

Remotely Managing the Dell

PowerEdge 1855 Blade Server

Using the DRAC/MC

The Dell™ PowerEdge™ 1855 blade server provides two primary out-of-band interfaces for remote management: the Dell Remote Access Controller/Modular Chassis (DRAC/MC) for the blade server chassis, and a baseboard management controller for the individual server blades. This article discusses how to manage the blade server chassis using the DRAC/MC.

BY MICHAEL BRUNDRIDGE AND RYAN PUTMAN

The Dell PowerEdge 1855 system is Dell's new-generation blade server. In addition to providing a flexible, modular architecture, the PowerEdge 1855 blade server is designed to support advanced management features. The system enables high performance in a dense form factor and can include up to 10 server modules; the Dell Remote Access Controller/Modular Chassis (DRAC/MC) management module;¹ three or four hot-pluggable, redundant power supply modules; two cooling modules; up to four I/O module bays for I/O switches or pass-through modules; and a keyboard, video, mouse (KVM) switch module.

While the system's DRAC/MC is based on the standard Dell OpenManage™ feature set that is included in the eighth-generation Dell Remote Access Controller 4 (DRAC 4), the DRAC/MC has been enhanced to support the modular blade server system computing environment.

The DRAC/MC is a customer-serviceable module installed in the rear of the server chassis (see Figure 1). The module has a serial port and a 10/100 Mbps RJ-45 port. Two state LEDs are visible from the back of the module. The DRAC/MC is responsible for the management of the chassis and all of its shared components.

Introducing the DRAC/MC architecture and features

The DRAC/MC architecture provides autonomous monitoring of hardware, events, and recovery mechanisms. The DRAC/MC functions by using system standby power and is designed to be operational as long as AC power is available to the chassis, even if the chassis is powered down. Because the DRAC/MC works from standby power and runs its own real-time operating system (RTOS) and out-of-band interfaces, it can be used to manage and monitor the system even when the server module, chassis, or other shared components are powered down.

For example, when a problem occurs with power, temperature, fan speed, or the general health of the chassis, the system generates a system event log (SEL) event. If properly configured, the SEL event can be sent as an alert in the form of a Simple Network Management Protocol (SNMP) trap to a console such as Dell OpenManage IT Assistant or as an e-mail to one or more DRAC/MC users, or both.

The DRAC/MC offers the following key features:

- Remote power-up, shutdown, reset, or generation of a non-maskable interrupt (NMI) for each server module in the blade server chassis

¹Redundant DRAC/MC modules are planned for a future release.

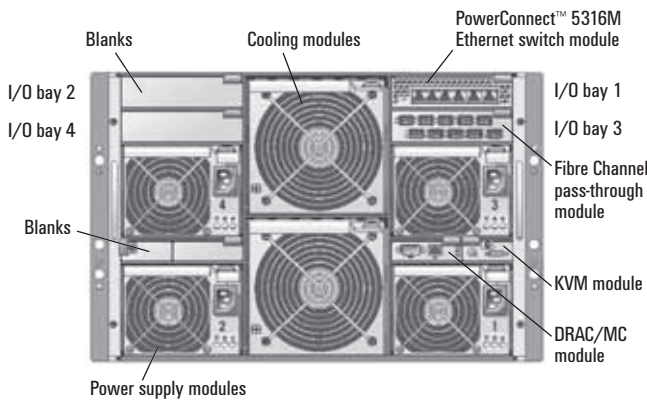


Figure 1. Rear view of the Dell PowerEdge 1855 modular blade server

- Remote power-up and shutdown of the complete chassis
- Monitoring of shared components, including power supplies, fans, voltage, and temperature
- Access protection by password and privilege-level security
- Remote upgrade of the DRAC/MC’s firmware through Trivial FTP (TFTP)
- Capability to deliver alerts by sending SNMP traps or e-mail messages
- Access to the chassis SEL and remote access controller (RAC) log
- Support for Dynamic Host Configuration Protocol (DHCP) of the DRAC/MC’s IP address
- Capability to provide an inventory of the chassis including server modules, switch service tags (if applicable), I/O module types, and Media Access Control (MAC) addresses (if applicable)
- Serial port multiplexing for serial console redirection in which one serial port is multiplexed to the server modules and I/O modules

Figure 2 shows the three ways to access the DRAC/MC:

- **Web-based GUI:** Using the out-of-band, Web-based graphical user interface (GUI) to connect remotely through a Web browser; the GUI supports Secure Sockets Layer (SSL) encryption
- **Telnet service:** Using a Telnet client to connect remotely to the out-of-band, text-based console
- **DRAC/MC serial port:** Attaching directly to the DRAC/MC local serial port and using a virtual terminal such as Hilgraeve HyperTerminal to connect to the out-of-band, text-based console

Setting up the DRAC/MC through the serial port

Using the local serial command-line interface (CLI), administrators can perform all actions on the DRAC/MC with the exception of the

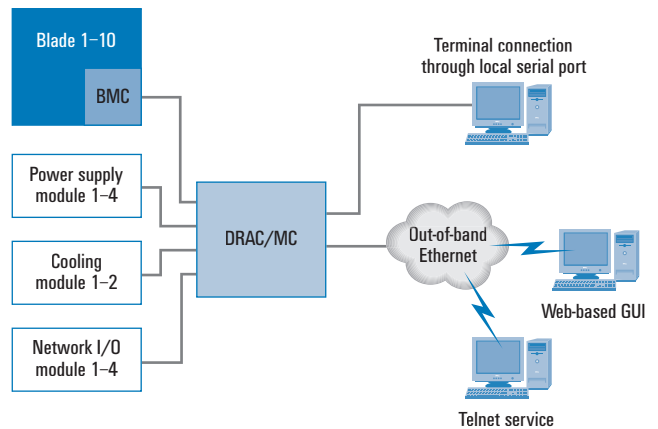


Figure 2. DRAC/MC management architecture

items listed in Figure 3. This article assumes the use of the DRAC/MC serial port for initial setup.

Factory defaults for the DRAC/MC include the creation of a default administrator user and settings for many of the database object properties. Refer to Appendix C of the *DRAC/MC User’s Guide*, located on the Dell OpenManage Documentation CD, for a quick reference guide to the object default properties.²

To view the basic syntax for the serial console commands, enter the following command at the CLI:

```
help (for a list of available commands)
```

or

```
help subcommand (for a list of the syntax statements for the specified subcommand)
```

To view the basic syntax for the `racadm` CLI commands, enter the following command at the CLI:

```
racadm help (for a list of available commands)
```

or

```
racadm help subcommand (for a list of the syntax statements for the specified subcommand)
```

Description	Management interface
Network physical control	Web only
Time zone	Web only
Web GUI time-out	Web only
Date/time format (12/24 hours)	Web only
User group	Web only

Figure 3. Configuration objects not supported in the local serial CLI

²The *DRAC/MC User’s Guide* is also available online at support.dell.com/support/systemsinfo/documentation.aspx?c=us&cs=04&l=en&s=bsd&cat=66&subcat=111.

For detailed information about serial console or racadm CLI commands, refer to the *DRAC/MC User's Guide*.

Configuring the DRAC/MC network

The DRAC/MC network configuration consists of a network interface card (NIC), Telnet configuration, and Simple Mail Transport Protocol (SMTP) e-mail alert configuration. The DRAC/MC default network settings are as follows:

- DHCP disabled; static IP address 192.168.0.120; subnet mask 255.255.255.0; gateway 192.168.0.120
- Physical control auto-negotiation (enabling the NIC to automatically detect the correct speed and duplex at which it should be running)
- SMTP enabled; SMTP server IP address 127.0.0.1
- Telnet disabled; port 23 Telnet default

The IP address of the DRAC/MC is used to gain access to its remote interfaces over the out-of-band network. When using DHCP, administrators should configure the DHCP server to use a nonexpiring, MAC-based IP address reservation. The current DHCP-assigned IP address can be determined either by using the Dell OpenManage IT Assistant discovery feature to locate the DRAC/MC or by attaching to the DRAC/MC serial interface.

Configuration using the DRAC/MC CLI

To display the DHCP-assigned IP address, enter the following command at the CLI for the DRAC/MC:

```
racadm getniccfg
```

To enable DHCP, enter the following command at the CLI:

```
racadm setniccfg -d
```

To change the network configuration of the DRAC/MC to use a static IP address, enter the following command at the CLI for the DRAC/MC:

```
racadm setniccfg -s ipaddress subnetmask gateway
```

To enable the Telnet service, enter the following command at the CLI:

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

To change the Telnet port, enter the following command at the CLI:

```
racadm config -g cfgRacTuning -o  
cfgRacTuneTelnetPort value
```

Note: In the preceding command, the value for the Telnet port must be entered in hexadecimal format. The hexadecimal format for port 23 is 0x17.

Changing the network configuration does not require the DRAC/MC to be reset. However, users attached to the DRAC/MC over the network will lose the connection and be required to reestablish the connection when the network configuration is changed. Once the IP address is known, DRAC/MC users can connect to the DRAC/MC over the network using the GUI or a Telnet service.

Configuration using DRAC/MC database objects

The network settings can also be set by using the DRAC/MC database objects. To enable or disable DHCP, enter the following command at the CLI:

```
racadm config -g cfgLanNetworking -o  
cfgNicUseDhcp value
```

Note: In the preceding command, the value is either 0 to disable or 1 to enable.

To change the network configuration of the DRAC/MC to use a static IP address, enter the following command at the CLI:

```
racadm config -g cfgLanNetworking -o  
cfgNicIpAddress ipaddress  
racadm config -g cfgLanNetworking -o  
cfgNicNetmask subnetmask  
racadm config -g cfgLanNetworking -o  
cfgNicGateway gateway
```

For more information on configuring the DRAC/MC network using the DRAC/MC serial interface or DRAC/MC database objects, visit *Dell Power Solutions* online at www.dell.com/powersolutions.

Managing the DRAC/MC through the GUI

The DRAC/MC has an embedded SSL-encrypted Web server from which it delivers an out-of-band GUI for remotely accessing the DRAC/MC. After configuring the network settings, administrators can launch the GUI by entering the DRAC/MC's IP address in a Web browser's URL address field. Then they can securely log in with a valid DRAC/MC username and password. After the username and password have been validated, the DRAC/MC Status page will appear. Because each DRAC/MC user can have a different privilege level, the GUI might appear different to each user based on those privileges. For instance, a user who does not have the Server Actions privilege will not see the Power tab or any of the other associated

User-level privilege	Bit mask*
Log in to DRAC/MC	0x80000001
Configure DRAC/MC	0x80000002
Configure users	0x80000004
Clear logs	0x80000008
Execute server control commands	0x80000010
Access console redirection	0x80000020
Test alerts	0x80000080
Execute debug commands	0x80000100

*Bit mask 0x80000040 is not currently used.

Figure 4. User-level privileges and associated bit masks

features that require the Server Actions privilege. Figure 4 indicates the level of permissions that a user must have to be able to perform actions with the DRAC/MC.

Accessing chassis information. The Properties tab of the GUI displays access information about the DRAC/MC, session status, shared components, and server modules. The GUI tabs and their associated links are available only if the user has the corresponding user privilege required for the feature. Information is shown on three separate pages:

- **Chassis Summary:** This page provides chassis, or *enclosure*, information, which includes the DRAC/MC's time, firmware version and date when firmware was last updated, current network settings, IP address, system model, service tag, asset tag, and chassis name and location. This page also provides session status, including the number of unused sessions, preliminary sessions, invalidated sessions, valid sessions, the current session ID, username, user's IP address, and login time.
- **Chassis Status:** This page provides information about all shared modules and server modules. Administrators can use this page to determine which modules are currently running in the Dell PowerEdge 1855 blade server as well as the service tags, power status, and overall health status of these modules.
- **Power Budget Status:** This page provides information about the current power budget status in the system. The page shows the current amount of power available along with the current amount of power currently being used. *Note:* The power values listed in the Power Budget Status page are static, maximum values; they do not reflect the actual power consumption of the system.

Monitoring chassis sensors. The Sensors tab shows sensor readings for the Dell PowerEdge 1855 blade server's temperature, cooling fan speed, and power supply status. This page also provides warning and failure thresholds for temperature and fan speed.

Managing the SEL and RAC log. The DRAC/MC maintains two persistent logs. The RAC log contains a list of user actions such as login and logout as well as alerts issued by the DRAC/MC. The oldest entries are overwritten when the log becomes full. Each log entry includes a brief description and information about severity, date and time, user, and ID of each event.

The SEL displays system-critical events that occur on the DRAC/MC and shared chassis components. This log includes the date, time, and a description of each event. To export both the DRAC/MC and SEL logs, administrators can click the Save As button in the GUI. Refreshing the logs in the GUI by selecting the Refresh button on the Web page before saving helps ensure that the latest logs are exported. Both logs can be cleared by clicking the Clear Log button.

Configuring chassis information. The Configuration tab enables many remote configuration tasks including configuring the chassis, creating and modifying users, creating and modifying alerts, configuring security for the DRAC/MC, configuring the network interface, and configuring the date and time.

Performing diagnostics. The Diagnostic tab allows administrators to display and execute basic network diagnostics, including:

- The Address Resolution Protocol (ARP) button displays the contents of the ARP table.
- `ping` verifies that the destination IP address is reachable from the DRAC/MC with the current routing-table contents.
- `ipconfig` displays the contents of the network interface table.
- `netstat` prints the contents of the routing table.

Updating the system firmware. The Update tab allows administrators to remotely update the DRAC/MC firmware image by using the DRAC/MC Flash function. Before performing the firmware update, administrators must download the latest firmware version from support.dell.com and then upload it to a TFTP server. The controller resets after the firmware update is complete.

Integrating the DRAC/MC with other management applications

The DRAC/MC offers a mechanism to integrate its own management capabilities with those of other management applications such as Dell OpenManage IT Assistant. An SNMP agent is embedded in the DRAC/MC; this agent implements SNMP management information bases (MIBs) and SNMP traps. The SNMP MIB is a hierarchical set of variables that can be read and written over the network. These variables contain information about the managed platform, including status, settings, and so on.

The DRAC/MC implements the MIB-II standard, which defines characteristics of the system and network interface. The DRAC/MC also implements an enterprise-specific MIB that provides management data specific to the server module system and devices such

as service tags for the enclosure and server modules, health status for shared components, and so on.

The DRAC/MC uses SNMP version 1.0. Because this version does not provide complete security, the DRAC/MC SNMP agent does not support SNMP *set* operations and is disabled by default. The agent can be enabled by entering the following command:

```
racadm config -g cfg0obSnmp -o cfg0obSnmpAgentEnable 1
```

The MIB objects in the DRAC/MC are read-only. The *get* and *get next* commands can be performed on MIB objects.

SNMP is often used to monitor systems for fault conditions such as voltage failure or fan malfunction. Management applications such as IT Assistant can monitor faults by polling the appropriate object identifiers (OIDs) with the *get* command and analyzing the returned data. However, this polling method has its challenges. Performed frequently, polling can consume significant amounts of network bandwidth. Performed infrequently, this method may not allow administrators to respond quickly enough to the fault condition.

SNMP agents, supported by the DRAC/MC, can overcome such limitations by sending alerts or SNMP traps to designated recipients. The DRAC/MC can notify administrators when a system fails or is going to fail. To receive DRAC/MC SNMP traps at a management station running IT Assistant, the DRAC/MC must be configured for the trap destination, trap community name, and so on.

The DRAC/MC can also be configured to notify different trap destinations for different events by setting the proper SNMP trap filter. When the DRAC/MC detects a new event, the DRAC/MC inspects the event against each destination's trap filter and sends an SNMP trap to the appropriate destination.

Configuring alerts

DRAC/MC alerts consist of e-mail alerts and SNMP traps. The e-mail alert contains the following information: message, event description, date, time, severity, system ID, model, asset tag, service tag, managed system host name, and Embedded Server Management (ESM) version. The SNMP trap provides specific information describing the cause and source of the event. This information includes sensor identification, entity or Intelligent Platform Management Bus (IPMB) slave address, sensor number, sensor ID string (if possible), current sensor reading, range, and threshold values.

Adding a user with alert capabilities. To add a user who can receive e-mail notification, first locate the appropriate user index by entering `racadm getconfig -u username` command. Then, enter the following commands:

```
racadm config -g cfgUserAdmin -o
  cfgUserAdminEmailEnable -i index 1
```

```
racadm config -g cfgUserAdmin -o
  cfgUserAdminEmailAddress -i
  userindex email_address
racadm config -g cfgUserAdmin -o
  cfgUserAdminEmailCustomMsg -i
  userindex Custom Message
racadm config -g cfgRemoteHosts -o
  cfgRhostsSmtptServerIpAddr SMTP_Server_IP
```

Enabling SNMP traps. Up to 16 SNMP trap entries can be stored in the DRAC/MC MIB. To locate an available index to add a new SNMP trap, execute the following command for each index from 1 through 16 until an available index is located:

```
racadm getconfig -g cfgTraps -i trapindex
```


After an available index is located, enter the following command to enable an SNMP trap:

```
racadm config -g cfgTraps -o cfgTrapsEnable
  -i trapindex 1
racadm config -g cfgTraps -o cfgTrapsDestIpAddr
  -i trapindex IP_Address
racadm config -g cfgTraps -o cfgTrapsSnmpCommuni-
  -ity -i trapindex Community_Name
```

To create a test trap, enter the following command:

```
racadm testtrap -i trapindex
```

Enabling powerful and flexible management of modular systems

Dell provides several methods for accessing the DRAC/MC, enhancing management of the Dell PowerEdge 1855 blade server. Using the serial console CLI, `racadm` CLI, and the Web-based GUI, administrators can configure, monitor, and manage the Dell PowerEdge 1855 blade server both locally and remotely. By offering powerful and flexible management options for the modular Dell PowerEdge 1855 blade server, Dell helps simplify the management of multiple server blades through a single management interface that seamlessly integrates into an existing management network. 

Michael Brundridge is a technologist in the Dell Enterprise Software Development Group. He attended Texas State Technical College and has a technical degree from Southwest School of Electronics.

Ryan Putman is a platform developer for the Dell Enterprise Server Group. He has a bachelor's degree in Electrical Engineering from Vanderbilt University and a master's degree in Computer Engineering from North Carolina State University.