

Maximizing Remote Management Security

on Eighth-Generation Dell PowerEdge Servers

IT administrators can take advantage of a powerful option for managing remote servers through out-of-band connections by using the Intelligent Platform Management Interface (IPMI) together with the integrated baseboard management controller in eighth-generation Dell™ PowerEdge™ servers. This article discusses key security features that are part of the IPMI 1.5 standard, and examines how the latest Dell remote access controllers can help administrators enhance remote server management.

BY CHANDRA S. MUGUNDA, WEIMIN PAN, AND HAIHONG ZHUO

Related Categories:

Baseboard management controller (BMC)

Dell OpenManage

Dell PowerEdge servers

Dell Remote Access Controller (DRAC)

Intelligent Platform Management Interface (IPMI)

Out-of-band (OOB) management

Security

Systems management

Virtual media

Visit www.dell.com/powersolutions for the complete category index to all articles published in this issue.

The Intelligent Platform Management Interface (IPMI) 1.5 specification describes a standard way of managing remote servers through out-of-band connections. However, while out-of-band connections provide IT administrators with a rich set of capabilities, they also introduce security challenges. To enable secure management of IPMI 1.5-compliant, eighth-generation Dell PowerEdge servers using out-of-band connections, administrators must properly configure the integrated baseboard management controller (BMC). This article explains how administrators can configure security features of the Dell Remote Access Controller 4 (DRAC 4) to help ensure tight security.

IPMI security features

When a BMC remote management connection is configured on a server—via serial, LAN, or serial over LAN

(SOL) links—an application or utility that complies with the IPMI 1.5 specification can access the server through that connection. Although the IPMI specification allows the Anonymous setting to be enabled by default, eighth-generation Dell PowerEdge servers are shipped with the Anonymous setting disabled to help protect against potential security breaches.¹

IPMI 1.5 helps provide security through user authentication; the BMC maintains a local database of remote access users and their privileges. Individual users in the BMC local user database are assigned a privilege limit that dictates the type of rights they have on the BMC. Administrators can use the Dell OpenManage™ Server Administrator (OMSA) interface to manage BMC user accounts (see Figure 1).

Access to servers can be restricted through connection-level, or *channel-level*, privileges; through user-level

¹ For more information about how to configure Dell PowerEdge server BMCs to enable server management through supported out-of-band connections, see "Remote Management with the Baseboard Management Controller in Eighth-Generation Dell PowerEdge Servers" by Haihong Zhuo; Jianwen Yin, Ph.D.; and Anil V. Rao; in *Dell Power Solutions*, October 2004.

privileges; or both. Each channel can be limited to operate at one of three different privilege levels: User, Operator, or Administrator. Similarly, each user can be created with one of these three privileges. For example, when a particular channel is limited to Operator level, only Operator-level operations can be performed on that channel.²

IPMI BMC authentication mechanism

Authenticated IPMI communication to the BMC is accomplished by establishing a session. Each session connection includes a user authentication phase that precedes IPMI messaging. The BMC verifies the packets that it receives. Authenticated packets are silently discarded if the authentication signature is invalid or the authentication type does not match the authentication type that was negotiated when the session was activated.

DRAC 4 security features

The DRAC 4 enhances current Dell remote access controller (RAC) offerings by providing features such as role-based user authentication, Racadm utility security, virtual media security, and console redirection security.

Role-based user authentication

The DRAC 4 supports privileged user-based and role-based access to a RAC device. Each DRAC 4 user entered in the RAC local user database or Microsoft® Active Directory® directory service user database is assigned a set of privileges. These privileges determine which rights the user has on the RAC device.

The DRAC 4 card supports nine privileges, which enable users to do the following:

- **RAC Login User:** Log in to the DRAC 4. Administrators can easily disable a user by removing this privilege. Removing the login privilege to disable a user is more straightforward than deleting a user. After a user's RAC Login User privilege is removed, that user still exists in the RAC or Active Directory user database. To re-enable the user at a later time, an administrator can simply grant the RAC Login User privilege again; there is no need to completely reconfigure the user in the database, as would be the case if the user were deleted.
- **RAC Card Configuration:** Change the DRAC 4 configuration—including out-of-band network interface card (NIC) configuration, Simple Network Management Protocol (SNMP) trap configuration, and Secure Sockets Layer (SSL) certificate configuration—with the exception of user configurations.

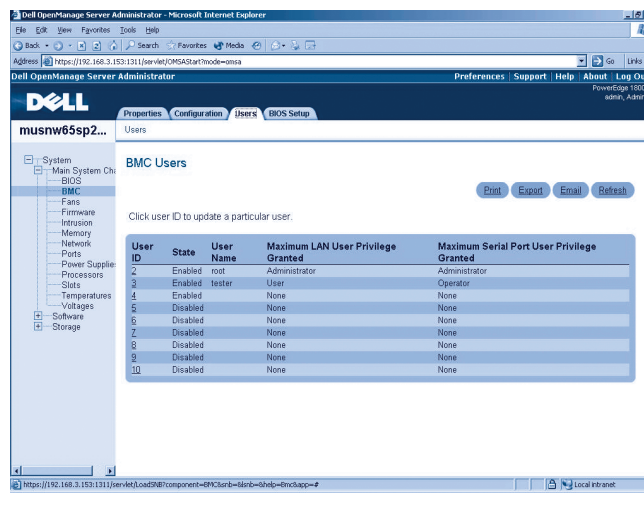


Figure 1. BMC user account management

- **RAC User Configuration:** Add or delete users, or change existing users' privileges.
- **RAC Log Clear:** Clear the system event log (SEL), RAC log, or last-crash screen log.
- **RAC Server Reset and Power-On/Off:** Perform power management operations on a system, such as reset, power up, or power down.
- **RAC Console Redirect:** Use the console redirection feature.
- **RAC Virtual Media:** Use the virtual media feature.
- **RAC Test SNMP Alert:** Set up the DRAC 4 to send a test SNMP trap alert to a preconfigured destination.
- **RAC Debug Command:** Issue debug commands. Most debug commands are used to help debug or diagnose the DRAC 4 and are normally used only by administrators or support technicians.

The DRAC 4 card supports five predefined user groups, which enable the following privileges:

- **Administrator:** A user in the Administrator group has all nine DRAC 4 privileges and can fully use all the features in the DRAC 4.
- **Power User:** A user in the Power User group has all DRAC 4 privileges except for RAC User Configuration and RAC Card Configuration. Thus, a member of the Power User group can use the DRAC 4 remote management features but cannot change any RAC configurations or user configurations.
- **Guest User:** A user in the Guest User group has only the RAC Login User privilege. A guest user can log in and view the various logs, system information, and session information.

²For more information about user privileges and which operations can be performed at each privilege level, refer to Appendix G of the IPMI 1.5 specification at www.intel.com/design/servers/ipmi/index.htm.

- **E-mail Alerts Only:** A user in the E-mail Alerts Only group can receive e-mail alerts but cannot log in to the DRAC 4.
- **Custom:** A user in the Custom group can be assigned any combination of privileges.

Configuring a RAC local user. Administrators can manage a DRAC 4 user through the supplied RAC GUI or the Racadm command-line interface (CLI). The Racadm utility is available on the Dell OpenManage CD. A user with the RAC User Configuration privilege—for example, a member of the Administrator group—can configure users. After logging in through a browser, the administrator must click the Configuration tab, then click the Users subtab to open a Remote Access Controller Users page. The DRAC 4 allows a maximum of 16 RAC local users. The DRAC 4 ships from Dell with a default user called root preconfigured in its first user slot; the other 15 slots are available. The root user has Administrator group privileges.

To add a user, the administrator can click on one of the available user slots to open the Add/Configure RAC User page. Three types of information need to be configured on that page: general information (including username and password), privileges, and e-mail alerts.

An administrator can place a user in a predefined group by selecting a group from the User Group list. Alternatively, the administrator can assign any set of privileges to a user by clicking the Privilege check box and placing the user in the Custom group.

If the user needs to receive e-mail alerts, the administrator must check the Enable E-mail Alert check box and configure a valid user e-mail address. The e-mail alert filter can also be configured by checking or unchecking boxes pertaining to different sensor types and severity levels. Only the alerts that pass this filter checking are sent to the user.

Users can also be added from the CLI using the Racadm utility, as follows:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 1 username
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 1 password
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege
-i 1 privileges
```

A user's e-mail alert can be configured from the CLI as follows:

```
racadm config -g cfgUserAdmin -o cfgUserAdminEmailEnable
-i 1 1
racadm config -g cfgUserAdmin -o cfgUserAdminEmailAddress
-i 1 email_address
```

Checking user privileges. When a user logs in from a browser, the DRAC 4 checks the user's privileges during the user authentication phase. After login, the user's privileges determine which tabs and associated subtabs are displayed on the screen. The user authentication process is designed to prevent a user who does not have sufficient privileges from using certain features. For example, a user in the Administrator group can view the tabs and subtabs of all available features after login (see Figure 2). By contrast, a user in the Guest User group is limited to seeing only the tabs and subtabs associated with the Guest User group.

When a BMC remote management connection is configured on a server—via serial, LAN, or SOL links—an application or utility that complies with the IPMI 1.5 specification can access the server through that connection.

When an administrator uses the remote Racadm utility to manage a system, user authentication and privilege checking are also required. A user who lacks sufficient privileges will fail to execute any command that requires that type of privilege. For example, the configuration command issued by a user without RAC Card Configuration and RAC User Configuration privileges will fail, and the error message will indicate that the user does not have the privilege to execute the command.

Racadm utility security

The Racadm utility is a CLI-based tool that can be used to configure and manage the DRAC 4. This scriptable utility can be

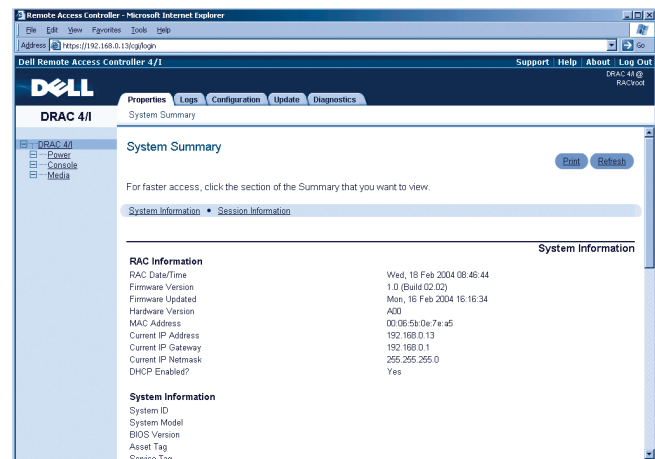


Figure 2. Main GUI page for a user in the Administrator group

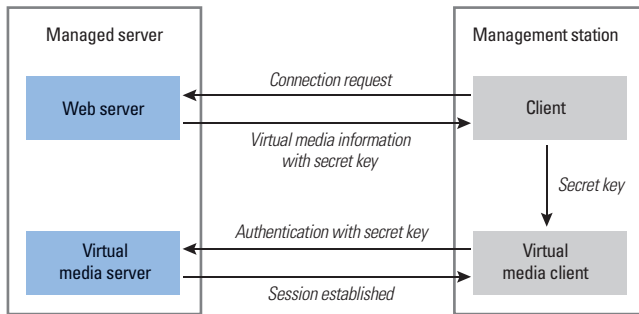


Figure 3. Virtual media security architecture

installed on the managed server or installed on a remote management station client system. The Racadm utility installed on the local managed server is called the local Racadm. The Racadm utility installed on the remote management station is called the remote Racadm.

Local Racadm security. The local Racadm utility communicates with the DRAC 4 through its in-band Peripheral Component Interconnect (PCI) virtual universal asynchronous receiver-transmitter (UART) interface. Because it is installed on the local managed server, administrators need to log in to the managed server to run this utility.

The local Racadm utility enforces security by requiring the user to have either Administrator group or root user privileges to run the utility and access the DRAC 4. On a server running the Microsoft Windows® OS, a user must have Administrator group privileges on the system to run the local Racadm utility; otherwise, an error message is displayed. On a server running the Linux® OS, a user must log in to the system as a root user to have sufficient rights to run the local Racadm utility.

Remote Racadm security. The remote Racadm communicates with the DRAC 4 through its out-of-band NIC. Remote Racadm utility security has been enhanced through the use of an SSL channel to the DRAC 4. A user must successfully pass SSL and user authentication and also have sufficient privileges to execute a Racadm command. Because the remote Racadm utility uses an SSL channel, the commands and data are encrypted by SSL. The RSA (1,024-bit), RC4 (128-bit), and MD5 cipher suite is used in remote Racadm and DRAC 4 SSL communication.

Virtual media security

Virtual media is a powerful remote access feature that provides eighth-generation Dell PowerEdge servers with a virtual CD drive and a virtual floppy disk drive that can use standard media connected anywhere on the network. Administrators can use the virtual media feature from any client on the network to perform various administrative tasks such as OS installation, remote diagnostics, and remote driver and software application installation. To help prevent

an attack on a virtual media server, the DRAC 4 uses a security exchange protocol in the virtual media connection.

When a user logs in to the DRAC 4 Web server and selects the Virtual Media subtab, a request-for-connection command is sent to the DRAC 4 firmware (see Figure 3). The DRAC 4 firmware responds by sending virtual media configuration information along with a secret key via a secure SSL channel. Virtual media client software starts a connection and sends its secret key to the virtual media server for authentication. If the secret key passes the virtual media server authentication, a virtual media session is established. Otherwise, a message is sent back to the client indicating that the authentication failed, in which case the connection

is dropped. To prevent a replay attack, the secret key is a sufficiently long random number that is dynamically generated by the DRAC 4 firmware each time a request-for-connection command received.

To use the virtual media feature, a user needs the RAC Virtual Media privilege. A user who does not have this privilege will not be able to see the Virtual Media subtab after login.

Dell's virtual media server port number is configurable to help organizations meet their firewall criteria. An administrator can use the Racadm utility to easily configure the port number. The command syntax is as follows:

```
racadm config -g cfgRacVirtual -o cfgVirAtapiSvrPort
port_number
```

Console redirection security

The DRAC 4 can continuously redirect a managed server's video data to a management station and a management station's keyboard and mouse control to a managed server. The console redirection feature is easy to use and does not require the installation of any special software on either the managed server or the management station. The console redirection feature enables administrators to control a geographically distant server while at a remote management station just as if they were physically present at the managed server.

A security protocol has been implemented in the console redirection design to help keep clients that have not been authenticated

The DRAC 4 enhances current Dell RAC offerings

by providing features

such as role-based user

authentication, Racadm

utility security, virtual media

security, and console

redirection security.

through the DRAC 4 Web server login from accessing the console redirection path. This design helps prevent a hostile party from interpreting keyboard keystrokes by snooping on the network traffic during remote console redirection.

The following sequence of security protocol operations establishes a console redirection session:

1. The administrator logs in to the main GUI and clicks the Open Console button (see Figure 4). The main GUI sends a preauthentication request to the DRAC 4's embedded Web server via a secure SSL channel (see Figure 5).
2. The DRAC 4 Web server returns secret information including an encryption key via an SSL channel. The console redirection secret information and encryption key are dynamically generated to prevent a replay attack.
3. The console redirection client sends a login command to the console redirection server for authentication. If the authentication is successful, a console redirection session and a console redirection pipe are established. Video, mouse, and keyboard data are redirected in this pipe. Keyboard and mouse data is encrypted on the management station side using an encryption key, and the data is decrypted by the DRAC 4 console redirection server. This makes a network snooping attack virtually impossible.

Enhanced remote management capabilities and security compliance

IT administrators can take advantage of enhanced remote management capabilities by using the on-board BMC on IPMI 1.5-compliant, eighth-generation Dell PowerEdge servers and by properly configuring and maintaining the BMC's remote management connection. At the same time, enhanced DRAC 4 capabilities

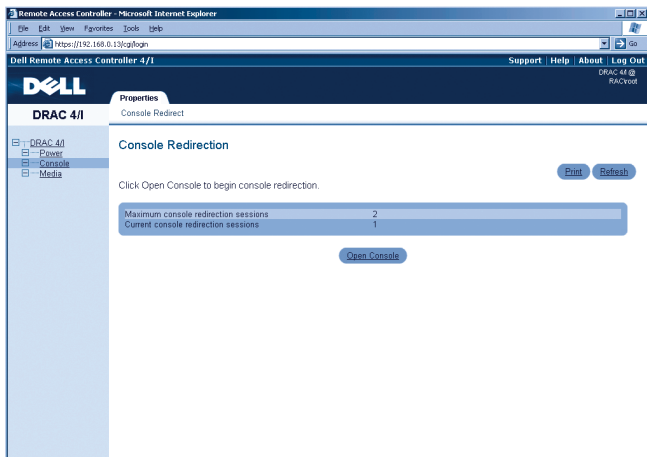


Figure 4. Main GUI Console Redirection page

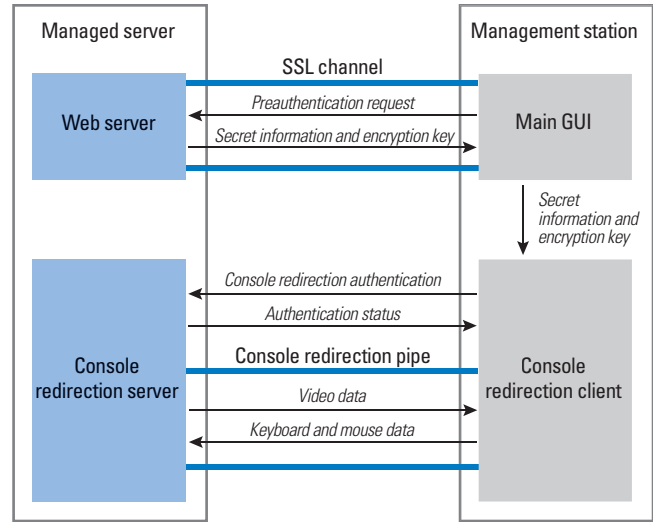


Figure 5. Console redirection security architecture

can further enhance remote server management through informed use of the latest built-in security features. [🔗](#)

Chandra S. Mugunda is a senior development engineer on the Dell Instrumentation Software team. Chandra has an M.S. in Computer Science from the India Institute of Technology, Roorkee, and a B.S. in Electrical Engineering from Andhra University in India.

Weimin Pan is a senior development engineer in the Dell Remote Management Group. He has worked as a senior systems engineer in the Dell Storage Enclosure Subsystem Group. Weimin has an M.S. in Electrical Engineering from the University of Utah and an M.S. in Computer Engineering from Shanghai Jiao Tong University in China.

Haihong Zhuo is a software engineer consultant in the Dell Enterprise Software Development Group. She has worked on systems management solutions and is currently on the Systems Management Instrumentation team. Haihong has an M.S. in Computer Engineering from The University of Texas at Austin and a B.S. in Electrical Engineering from Tsinghua University in China.

FOR MORE INFORMATION

IPMI 1.5 overview and specification:
www.intel.com/design/servers/ipmi/index.htm