

Updating the Dell PowerEdge 1855 Blade Server

Chassis and Server Blades

Many hardware components in the Dell™ PowerEdge™ 1855 blade server have been designed with a firmware upgrade option—including the Dell Remote Access Controller/Modular Chassis (DRAC/MC) management module; server baseboard management controllers; I/O modules; and keyboard, video, mouse modules. This article discusses standards-based frameworks for updating individual server blades and available software utilities as well as recommended methods and best practices for updating chassis component firmware.

BY NARAYAN DEVIREDDY AND RUOTING HUANG

Related Categories:

Blade servers

Dell PowerEdge blade servers

New-generation server technology

Visit www.dell.com/powersolutions
for the complete category index.

Equipped with 10 server blades and several I/O modules and management modules, the Dell PowerEdge 1855 blade server contains numerous system software components to update during the change-management process. Although best practices dictate careful planning and methodical implementation when deploying system software updates for the PowerEdge 1855 blade server, such change management need not be difficult. As is the case with other PowerEdge servers, administrators can manage software updates for the PowerEdge 1855 blade server using standards-based Dell OpenManage™ tools, third-party enterprise change-management tools, or both.

Updating server blades

The process for updating system software components on PowerEdge 1855 server blades is designed to be the same as on other PowerEdge servers. This similarity allows administrators to leverage existing change-management

processes in their IT organization to manage updates to PowerEdge 1855 server blades. On PowerEdge 1855 server blades, administrators can typically update firmware on the following system software components:

- Server system BIOS
- Baseboard management controller (BMC)
- PowerEdge Expandable RAID Controller 4, Integrated Mirroring (PERC 4/IM)
- Adaptec SCSI Card 39160
- SCSI hard disk drives
- OS-level drivers

As part of the change-management planning process, administrators must decide which update method best fits their environment. System software components on a PowerEdge 1855 server blade can be updated using one of two methods: offline updates or online updates.

Offline updates

To perform an offline update, administrators must schedule server downtime. Most offline update utilities boot into a pre-OS environment such as DOS to perform the update. These update utilities may also require multiple system reboots to complete the update process. Although the offline update process is time-consuming and requires several manual steps, this is a safe method to update system software on virtually any server because the network is not involved. In contrast, network traffic, Trivial FTP (TFTP) server response time, packet loss, and link loss can affect firmware updates that are performed over a network.

On a PowerEdge 1855 server blade, administrators can update BIOS, BMC firmware, RAID firmware, SCSI hard disk drive firmware, SCSI controller firmware, and OS-level drivers using DOS-based update utilities found on the Dell support Web site (support.dell.com). *Note:* The PERC 4/IM is integrated into the PowerEdge 1855 server blade motherboard, so PERC 4/IM firmware is included as part of the system BIOS update package.

Online updates

Unlike an offline update, the online update process minimizes server downtime by allowing the process to run in a normal OS environment. The greatest advantage of the online approach is its capability to automate the update process. Online updates enable organizations to update multiple server blades from a central console using Dell OpenManage change-management tools or third-party change-management frameworks.

Dell OpenManage change-management tools for the PowerEdge 1855 blade server comprise the following:

- Dell Update Packages
- Dell OpenManage Server Update Utility (SUU)
- Dell OpenManage IT Assistant (ITA) 7

Dell Update Packages. Dell Update Packages are self-contained, easy-to-use programs; each package updates a single system software component on the server on which it is executed. Each Dell Update

Although the offline update process is time-consuming and requires several manual steps, this is a safe method to update system software on virtually any server because the network is not involved.

Package contains the logic to verify that the update will work on a given system. Dell Update Packages support both a graphical user interface (GUI) and a command-line interface (CLI). BIOS and BMC firmware Dell Update Packages are available for PowerEdge 1855 server blades. Dell Update Packages are supported on Microsoft® Windows Server™ 2003 and Red Hat® Enterprise Linux® operating systems. In addition, Dell Update Packages can be integrated into third-party or custom software distribution application frameworks such as Microsoft Systems Management Server (SMS) 2003, Altiris® Deployment Solution, and others.¹

Dell OpenManage Server Update Utility. SUU is a comprehensive system update utility that provides a mechanism to update several system software components at once. It is a CD-based application that can identify systems and apply the appropriate updates. For example, on a PowerEdge 1855 blade server, administrators can use the SUU CD to update all system software on a server blade. The SUU update process requires administrators to update one server blade at a time.

Dell OpenManage IT Assistant. ITA 7 provides centralized software update capability for Dell servers. IT Assistant allows administrators to load Dell Update Packages and Dell System Update Sets into a central repository and then compare the packages to the software versions currently running on PowerEdge systems. Administrators can then decide whether to update systems that are not in compliance, either immediately or according to an administrator-defined schedule.

BMC flash updates

The BMC does not disable the power button on the front of an individual PowerEdge 1855 server blade during a flash update. If an administrator presses the power button during a flash update, the server blade will power off and leave the BMC in an unknown state. To recover the server blade, an administrator should remove the server blade from the PowerEdge blade server chassis, wait five seconds, reinsert the server blade, and allow the server blade to boot. Then the flash update can be performed again.

Note: Keyboard, video, mouse (KVM) hot-key keyboard sequences are not supported during a BMC flash update. If an administrator attempts a hot-key sequence from a server blade that is performing a BMC flash update, the flash update may fail. To recover, the administrator must execute the flash update again.

Updating chassis components

Because individual server blades in the PowerEdge 1855 blade server share common chassis infrastructure components, keeping the system software of the chassis components up-to-date can play a critical role in

¹ For more information about how Dell Update Packages are designed to work in third-party software distribution applications, see "Scripting Dell Update Packages on Windows and Linux" by Manoj Gujarathi, Pritesh Prabhu, and Subbu Ganesan in *Dell Power Solutions*, October 2004, www.dell.com/downloads/global/power/ps4q04-20040125-Gujarathi.pdf; and "Deploying Dell Update Packages Using Microsoft Systems Management Server 2003" by Sandeep Karandikar and Manoj Gujarathi in *Dell Power Solutions*, February 2005, www.dell.com/downloads/global/power/ps1q05-20040111-Gujarathi.pdf.

the overall PowerEdge 1855 blade server change-management process. However, the frameworks that are used to update individual server blades do not scale to manage the updates of chassis components. This section describes how to update components in the PowerEdge 1855 blade server chassis that have administrator-upgradeable system software. These firmware components include:

- Management modules
- KVM modules
- I/O modules

Administrators can update the PowerEdge 1855 blade server chassis module firmware using either the GUI or the CLI of the Dell Remote Access Controller/Modular Chassis (DRAC/MC). Both interfaces require administrators to download the firmware image from a TFTP or an FTP server. The updated firmware image should be made available in a designated directory on the TFTP or FTP server. *Note:* The *Dell Remote Access Controller/Modular Chassis User's Guide* provides specific instructions on how to set up the TFTP or FTP server for a firmware update at support.dell.com/support/edocs/software/smdrac3/dracmc.

Management module firmware updates

The DRAC/MC is the management module that allows administrators to monitor and manage chassis components in a Dell PowerEdge 1855 blade server. The PowerEdge 1855 blade server offers two different configurations for management module firmware:

- Single DRAC/MC
- Redundant DRAC/MC

Single DRAC/MC firmware. DRAC/MC firmware can be upgraded using the GUI, CLI, or DRAC/MC firmware recovery console.² The DRAC/MC firmware update is a TFTP-based update process. For all three DRAC/MC firmware update methods, administrators must complete the following setup procedures before starting the firmware update process:

1. Set up a TFTP server and copy the firmware image to the root of the TFTP server.
2. Record the IP address of the TFTP server and the file name of the updated firmware image.
3. Log in to the DRAC/MC, using either the GUI or CLI.

To update the firmware using the GUI, administrators should navigate to the Update tab and select “Firmware Update.” Next,

they should enter the TFTP IP address of the firmware image file name and start the DRAC/MC firmware update process by clicking “Update Firmware.”

To update the firmware using the CLI, administrators should enter the following Racadm command at the DRAC/MC console prompt:

```
DRAC/MC: racadm fwupdate -a TFTP_IP_ADDRESS
        -d mgmt.bin
```

where *TFTP_IP_ADDRESS* is the IP address of the TFTP server and *mgmt.bin* is the name of the firmware image file.

Note: This Racadm command can be entered at the DRAC/MC serial console or at a Telnet session. Best practices recommend using the serial console because, if a TFTP download fails, administrators will lose Web access and network connections such as Telnet. DRAC/MC will boot to the DRAC/MC firmware recovery console, which can be accessed only at the serial console. The firmware recovery console provides the following options:

- Upgrade firmware from the serial port
- Upgrade firmware from the network
- Configure network parameters

Using the DRAC/MC firmware recovery console, administrators can restart the firmware update process either via serial port or the network.

Note: While in recovery mode, the DRAC/MC does not monitor chassis components of the PowerEdge 1855 blade server. For that reason, administrators should take extra care to minimize the amount of time that the DRAC/MC spends in recovery mode.

Redundant DRAC/MC firmware. In a redundant configuration, two separate DRAC/MC modules are installed in a chassis:

- A primary DRAC/MC module, which actively monitors the chassis
- A standby DRAC/MC module, which monitors the active signal from the primary DRAC/MC module (If a failure in the primary DRAC/MC module occurs for more than five seconds, the standby DRAC/MC module is designed to become the active, primary DRAC/MC module.)

The PowerEdge 1855 blade server supports redundant DRAC/MC mode if the DRAC/MC is running firmware version 1.1 or higher. Although redundant DRAC/MC modules can be updated with a single firmware package, the DRAC/MC goes through the following steps to complete the firmware update process once the administrator

² For more information about how to access the DRAC/MC GUI and the CLI (also known as the Racadm command-line utility), refer to the *Dell Remote Access Controller/Modular Chassis User's Guide* at support.dell.com/support/edocs/software/smdrac3/dracmc.

initiates a firmware update task, using either the GUI or the `racadm fwupdate` command from the CLI:

1. The primary DRAC/MC module starts the TFTP firmware update.
2. The standby DRAC/MC module monitors the chassis while the primary DRAC/MC module is updated. At this time, neither DRAC/MC is accessible, either through Telnet or the GUI.
3. When the primary DRAC/MC module completes the TFTP update, the TFTP update on the standby DRAC/MC module begins. The primary DRAC/MC module continues to monitor the chassis while the standby module is updating the firmware. At this time, neither DRAC/MC is accessible, either through Telnet or the GUI.
4. When the standby DRAC/MC module completes the firmware update process, the primary DRAC/MC module is available for network access. Telnet and the GUI become available.

KVM module firmware updates

The KVM module enables administrators to access server blades in the PowerEdge 1855 blade server by providing keyboard, monitor, and mouse functions as if the administrator were directly connected to the module. The PowerEdge 1855 blade server provides a built-in analog KVM module and an optional digital KVM module. Both KVM modules are flash-upgradeable.

Analog or digital KVM module firmware can also be updated using the DRAC/MC GUI or CLI. For both firmware update methods, administrators must complete the following setup procedures before starting the firmware update process:

1. Set up a TFTP server, and copy the firmware image to the root of the TFTP server.
2. Record the IP address of the TFTP server and the file name of the new firmware image.
3. Log in to the DRAC/MC, using either the GUI or CLI.

To update the firmware using the GUI, administrators should navigate to the Update tab and select “KVM Firmware Update.” They should then enter the TFTP server IP address of the firmware image file name, and start the KVM firmware update process by clicking “Update Firmware.” The TFTP download and firmware update process may take up to six minutes. After the update completes, the KVM will reset.

To update the firmware using the CLI, administrators should enter the following `Racadm` command at the DRAC/MC console prompt:

```
DRAC/MC: racadm fwupdate -a TFTP_IP_ADDRESS
-d kvm_firmware_name -mkvm
```

I/O module firmware updates

The PowerEdge 1855 blade server chassis provides extensible I/O functionality such as networking, Fibre Channel, or InfiniBand connectivity. The McDATA 4314 Fibre Channel switch and Brocade SilkWorm 3014 Fibre Channel switch provide Fibre Channel connectivity. The Dell PowerConnect™ 5316M Ethernet switch, a managed Layer 2 network switch, provides network functionality.

To update the firmware of the preceding I/O modules, administrators need to procure the IP addresses of the switches. As part of the installation of the McDATA, Brocade, and PowerConnect switches, administrators must configure the IP address using the corresponding switch configuration application. However, administrators can obtain the IP address of the Brocade switch using the DRAC/MC CLI as follows:

1. Log in to the DRAC/MC and connect to the switch using the `DRAC/MC: connect switch-N` command.
2. Log in to the switch with the username “admin” and password “password.”
3. Enter the `ipaddrshow` command to obtain the IP address.

Unlike the TFTP-based DRAC/MC firmware update process, the McDATA and Brocade Fibre Channel switch module firmware update process is FTP based. Administrators must complete the following setup procedures before starting the firmware update process:

1. Set up an FTP server on the management station, and unzip the firmware in a local directory.
2. Record the IP address of the switch and the FTP server.
3. Ensure that the switch is in normal operation mode by inspecting the status LEDs.

McDATA 4314 Fibre Channel switch firmware. To provide consistent performance throughout the fabric, administrators should ensure that all switch modules are running the same version of firmware. Installing updated firmware requires a switch reset. A stable fabric is required to successfully activate the firmware on a switch without disrupting traffic. Therefore, administrators must ensure that no administrative changes are in progress anywhere in the fabric before installing the Fibre Channel switch firmware.

McDATA provides management station software called Enterprise Fabric Connectivity Manager (EFCM), which provides a GUI to update the switch firmware. Detailed instructions on how to use EFCM can be found in the McDATA 4314 switch documentation.³

³For more information about EFCM, refer to the *EFCM Management Guide* on the CD that ships with the McDATA 4314 Fibre Channel switch.

For the firmware update process, the McDATA management interface requires administrators to log in to the switch using the “admin” account and access the advanced configuration console mode using the `admin start` command.⁴

Brocade Silkworm 3014 Fibre Channel switch firmware. Brocade Fibre Channel switch firmware can be upgraded using either a Web-based GUI or a CLI. To update the fabric OS in command-line mode, administrators should execute the `firmwaredownload` command from an FTP server or from a local Network File System (NFS) directory while in `admin` mode:

```
firmwaredownload options host_or_IP,user,
/path/to/the/file,passwd
```

The updated firmware is in the form of Red Hat® Package Manager (RPM™) packages with names defined in `pfile`, a binary file that contains specific firmware information and the names of firmware packages to be downloaded.

In dual-domain systems, the `firmwaredownload` command downloads the firmware image by default to both control processors (CPs) in rollover mode, which helps prevent disruption to application services. This operation depends on support for the High-Availability (HA) feature, which can be enabled through the `haenable` command in the switch CLI. If HA support is not available, administrators can still upgrade the CPs one at a time, using the `-s` option.⁵

Systems supported by the Brocade firmware have two partitions of nonvolatile storage areas—a primary and a secondary partition—to store two firmware images. The `firmwaredownload` command loads the updated image into the secondary partition and swaps the secondary partition to be the primary partition. The command then reboots the CP and activates the updated image. Finally, it performs the `firmwarecommit` procedure automatically to copy the updated image to the other partition (unless the `-n` option is used).

To update the firmware using the GUI, administrators should launch the Brocade Web console by entering the IP address of the switch in the browser address line. They should then log in

as “admin” and navigate to the Firmware tab. On the Firmware page, administrators should enter the FTP server’s IP address and the path to the firmware image file, then begin the firmware update process.

At the switch console, administrators can use the `firmwaredownloadstatus` command to monitor the download process. After the download is finished, administrators can enter the `firmwaredownloadshow` command to verify that the firmware update completed successfully.

Dell PowerConnect 5316M Ethernet switch firmware. Two firmware images can be stored in the flash memory of the PowerConnect 5316M switch module. The images are called active and nonactive, depending on which image the switch is currently running. The switch also supports two protocols to download the images: network-based TFTP and serial port-based xmodem.

To use the TFTP method, administrators must complete the following setup procedures before starting the firmware update process:

1. Set up a TFTP server.
2. Install the updated firmware image on the TFTP server.
3. Log in to the switch, and enter the privileged EXEC mode.⁶

After logging in, administrators can execute the following command in privileged EXEC mode to copy the file named “image” to the nonactive image file:

```
console# copy tftp://hostname/path/to/the/
systemimage flash
```

After the flash update is complete, the switch can be instructed to boot from either of the two images by executing the following command in privileged EXEC mode:

```
console# boot system {image1 | image2}
```

Administrators should enter the following command to verify whether the switch successfully booted into the updated system image:

```
console# show version
```

Although administrators may never need to upgrade the switch boot image, they can do so by executing the following command:

To provide consistent performance throughout the fabric, administrators should ensure that all switch modules are running the same version of firmware.

⁴For more information about the CLI-based firmware update process for the McDATA 4314 switch, refer to the *McDATA 4314 Command Line Interface Guide* on the CD that ships with the McDATA switch.

⁵For more information about command options for Brocade Silkworm 3014 Fibre Channel switch firmware, refer to the *Brocade Fabric Operating System (FOS) Reference Manual* on the CD that ships with the Brocade switch.

⁶For more information about the operation modes of the PowerConnect 5316M switch and how to configure the system identity, refer to the *Dell PowerConnect 5316M Ethernet Switch Module User's Guide* and the *Dell PowerConnect CLI 5316M Reference Guide* at support.dell.com/support/edocs/network/PC5316M/en.

```
console# copy tftp://hostname/path/to/the/
bootimage boot
```

Note: Best practices recommend saving extra copies of the switch configurations on a TFTP server, especially before a firmware upgrade.

The PowerConnect 5316M Ethernet switch module used in the PowerEdge 1855 blade server chassis does not come equipped with its own serial console port. Instead, the serial console can be accessed as a module to which the DRAC/MC is connected. Therefore, to use xmodem as the source for the management station where the firmware image is stored, administrators must perform the following steps from the DRAC/MC:

1. Ensure that the current shell interface is already at the DRAC/MC command prompt. If not, switch back to the context of the DRAC/MC command prompt by pressing the Enter key, the tilde key, and the period key. *Note:* Press the Shift key if the tilde character is located in the upper register of the keyboard, and then press the period key.
2. At the DRAC/MC command prompt, issue the following command:

```
DRAC/MC: racadm config -g cfgSerial
-o cfgSerialConsoleIdleTimeout 0x3000
```

3. Redirect the DRAC/MC serial console to the internal serial console interface of the PowerConnect 5316M Ethernet switch module in binary mode by entering the following command:

```
DRAC/MC: connect -b switch-N
```

where *N* is the chassis I/O module bay number in which the PowerConnect 5316M Ethernet switch module is inserted. Press the Enter key several times to ensure that the terminal connection is successfully established and that the Ethernet switch module prompt appears.

Note: To terminate the binary mode connection to the PowerConnect 5316M Ethernet switch module's serial console, disconnect the current session of the terminal.⁷

Keeping blade server system software components up-to-date

The modular design of blade servers, such as the Dell PowerEdge 1855 blade server, brings an added dimension to the traditional change-management process. Today's industry-leading change-management and software distribution frameworks such as Altiris Patch Management Solution and Microsoft SMS are designed to provide robust automated tools to manage updates on modules that reside on server blades. Because these frameworks do not scale to manage the updates of chassis management modules and I/O modules, updating blade server chassis modules requires careful planning and deployment such as the approach described in this article. [↪](#)

Narayan Devireddy is a development manager in the Dell Enterprise Systems Management Software organization. He has 14 years of systems management product development experience. Before joining Dell, Narayan worked for Novell, Compaq, and Computer Associates in different capacities. He has an M.S. in Computer Science from Alabama A&M University.

Ruoting Huang is a development engineer in the Dell Enterprise Systems Management Software organization. He focuses on parallel processing and internetworking. Ruoting has an M.S. in Computer Science from the Asian Institute of Technology.

FOR MORE INFORMATION

Dell PowerEdge 1855 Systems User's Guide:
support.dell.com/support/edocs/systems/pe1855

Dell OpenManage:
www.dell.com/openmanage

Dell servers:
www.dell.com/servers

⁷For more information about configuring and using the DRAC/MC, refer to the *Dell Remote Access Controller/Modular Chassis User's Guide* at support.dell.com/support/edocs/software/smdrac3/dracmc.