Systems Management Techniques

for the Dell PowerEdge 1855 Blade Server

Systems management capabilities built into the Dell™ PowerEdge™ 1855 blade server allow administrators to manage individual server blades using the Dell OpenManage™ infrastructure, while also enabling management of the entire system through the Dell Remote Access Controller/Modular Chassis management module. This article provides a high-level overview of the deployment, monitoring, and change management capabilities of the PowerEdge 1855 blade server.

**BY STEVEN GRIGSBY AND NARAYAN DEVIREDDY**

The Dell PowerEdge 1855 blade server is a modular system consisting of a chassis, up to 10 independent server blades, and the infrastructure components shared by the server blades in the chassis. The shared infrastructure components include power supply modules; cooling modules; network I/O modules; the Dell Remote Access Controller/Modular Chassis (DRAC/MC) remote access management module; and a keyboard, video, mouse (KVM) switch module. Systems management of the PowerEdge 1855 blade server can be categorized into two key areas:

- **Server blade management:** Server blade management is accomplished through individual management features on the server blades and in the I/O modules.
- **Chassis management:** System-wide management of shared infrastructure components is accomplished through the DRAC/MC.

Managing Dell PowerEdge 1855 blade servers is similar to managing stand-alone Dell PowerEdge servers. Each server blade provides traditional in-band\(^1\) management features using the Dell OpenManage suite and out-of-band, agentless management using a built-in baseboard management controller (BMC)—and each server blade can be managed independently of the other server blades in the chassis.

Because all the server blades in the modular system share the common chassis infrastructure components, chassis management plays a critical role in overall Dell PowerEdge 1855 systems management. The Dell PowerEdge 1855 blade server chassis and its common infrastructure components are managed through the DRAC/MC component. The DRAC/MC monitors power supplies, power allocation, blade presence, and I/O module presence. The DRAC/MC provides the following management access points:

- Web-based graphical user interface (GUI) accessible through a browser
- Command-line interface (CLI) accessible through a Telnet connection
- CLI accessible through the DRAC/MC’s integrated serial port

---

\(^1\) In-band features are used when the operating system is present.
The DRAC/MC runs on low-wattage power and has a separate network connection to help ensure remote access to the system. The separate network connection provides a redundant path for the routing of network alerts.

Server blade configuration and deployment
Manually configuring the server blade hardware and deploying an operating system (OS) image on multiple blades may seem simple, but can become a daunting task when a large number of servers are involved. Several local and remote deployment options are available—ranging from local, attended deployment with CD media to remote, unattended deployment using Preboot Execution Environment (PXE) and custom scripts.

Local configuration
Manually configuring the server blades and deploying the OS requires administrators to physically interact with the blade server system. This may be practical in organizations that have relatively few servers if all the servers are physically accessible. One local deployment method is to repeat the configuration and deployment steps for each server blade. However, it may make more sense to perform the steps once, save the configuration data, and use the data to configure and deploy the remaining systems.

Local, attended configuration and deployment is accomplished by booting the Dell OpenManage Server Assistant (DSA) CD using a Universal Serial Bus (USB) CD drive attached to the front-panel dongle of the server. This requires the administrator to configure the boot order in the BIOS. Once the DSA CD boots, a DSA configuration wizard prompts the administrator with a series of questions to configure the server blade. As part of this configuration, the administrator must select an OS. DSA then prompts for the OS configuration data including network settings and time zone. To complete the installation, DSA prompts the administrator to insert the OS installation media.

To enable local, unattended installation, the administrator can choose to save the configuration data to a USB floppy disk drive attached to the front-panel dongle of the server and use this data to replicate subsequent installations on additional server blades. When the administrator moves the floppy disk containing the configuration data to the next server blade and boots the DSA CD, the configuration data is automatically read by DSA to complete the installation.

Remote configuration
When an organization has many servers to deploy, or when physical access is limited, administrators can opt to configure and deploy server blades remotely. The Dell OpenManage Deployment Toolkit contains several configuration tools for scripting tasks such as partitioning drives and configuring BIOS settings, BMC settings, and RAID controllers.

Using a combination of the Dell OpenManage Deployment Toolkit and third-party remote deployment products such as Altiris Deployment Solution, Microsoft® Automated Deployment Services (ADS), VERITAS OpForce, and Symantec ON iCommand, administrators can rapidly deploy remote PowerEdge 1855 server blades. The Dell OpenManage Deployment Toolkit provides configuration tools and sample scripts to configure hardware devices in a pre-OS environment. Scripts that configure BIOS, BMC, RAID, and disk devices can be leveraged in PXE to remotely configure the hardware and deploy the OS on the server blades.

Using PXE and remote deployment products is an excellent option for remotely deploying numerous servers. Although such techniques require additional time up-front to create the PXE image and script the configuration, the time investment is rewarded with the automatic, remote configuration and deployment of the server blades. Dell OpenManage Deployment Toolkit tools can also be leveraged in any custom deployment environment.

PowerEdge 1855 blade server monitoring capabilities
Hardware monitoring and alerting on a PowerEdge 1855 blade server can be accomplished with the following components:

- On-board BMC on each server blade
- Dell OpenManage Server Administrator (OMSA) running on each server blade
- DRAC/MC management module in the chassis

The embedded BMC is designed to work in conjunction with the DRAC/MC (which resides in the chassis) and OMSA (which runs on the server blade OS) to log and send alerts on the network. The BMC is responsible for monitoring the status of the voltage and temperature probes on individual server blades. When the BMC detects an event, the event is written to the BMC hardware log and sent to the DRAC/MC using the Intelligent Platform Management Interface (IPMI). The DRAC/MC then writes a corresponding event to the system event log (SEL) and sends a corresponding Simple Network Management Protocol (SNMP) trap to the configured recipient. The DRAC/MC can also be configured to send an e-mail alert using Simple Mail Transport Protocol (SMTP).
NEW GENERATION SERVER TECHNOLOGY

If Dell OpenManage software agents are installed on the server blade OS, the event will also be handed off to OMSA for user notification. OMSA can be configured to send SNMP traps and SMTP e-mail alerts to multiple recipients.

The combination of the DRAC/MC, the server blade’s BMC, and Dell OpenManage agents is designed to provide a redundant notification path and redundant logging. The DRAC/MC can send an SNMP trap, an SMTP e-mail alert, or both through its own network connection; at the same time, Dell OpenManage agents can send an SNMP trap and an SMTP e-mail alert through the server blade’s network connection. The event is logged in both the DRAC/MC SEL and the BMC hardware log.

In addition, Dell OpenManage agents can provide enhanced logging capabilities in the OMSA Alert log and Command log—the same level of logging provided by Dell OpenManage agents on stand-alone Dell servers.

The DRAC/MC also monitors the presence and health of the I/O modules, cooling modules, KVM switch module, and power supply modules in the chassis. When an event occurs on one of these modules, the DRAC/MC handles the event exactly as it would handle an event on a server blade. The event is written to the DRAC/MC SEL and—if configured—an SNMP trap, SMTP e-mail alert, or both are sent over the DRAC/MC out-of-band network.

The PowerEdge 1855 blade server can also be remotely monitored and managed with Dell OpenManage IT Assistant (ITA), which is included in the Dell OpenManage suite. When ITA discovers the PowerEdge 1855 system, it groups PowerEdge server blades, Dell PowerConnect™ switches, and the DRAC/MC into a Chassis group—providing an overall system view that allows administrators to survey the individual server blades and components.

Access to the logs from the DRAC/MC and the server blades is available from the ITA console. When OMSA is installed on the server blades, OMSA can be configured to send server blade-related SNMP traps to the ITA console. Additionally, the DRAC/MC and PowerConnect switches can be configured to send SNMP traps to the ITA console. ITA can decode and report the traps and update the component and system status accordingly on the Status page of the system view.

PowerEdge 1855 blade server change management

Knowing server blade drivers, firmware, and BIOS updated can be challenging in organizations that have many servers to update. Using Dell Update Packages, administrators can update these components one at a time, or simultaneously apply the updates to many servers using management frameworks such as Microsoft Systems Management Server (SMS) or Altiris Deployment Solution. Dell Update Packages for the PowerEdge 1855 blade server are available for download from the Dell support website at support.dell.com. For single-server updates, a Dell Update Package can be either downloaded and executed or run from the Update tab of the OMSA GUI.

DRAC/MC firmware can be updated using the Trivial FTP (TFTP) protocol over the local area network. To update the firmware in this manner, administrators must install a TFTP server on a system that resides on the same network segment as the DRAC/MC. The firmware image can then be updated from the TFTP server using either the DRAC/MC CLI or GUI.

I/O module firmware can be updated through the interfaces provided by the I/O modules themselves. For example, the Dell PowerConnect 5316M Gigabit Ethernet switch provides for firmware updates from the switch GUI. In addition, firmware can be updated using the TFTP protocol in a manner similar to that previously described for DRAC/MC firmware.

A different management paradigm for modular blade servers

Managing the modular Dell PowerEdge 1855 blade server requires a somewhat different management paradigm compared to the traditional method of managing stand-alone servers. While managing a server blade is similar to managing a stand-alone server, management of the overall blade server system—including chassis infrastructure components and individual server blades—requires a combination of the DRAC/MC, the server blade BMC, and Dell OpenManage software agents. These components work together to provide a robust, redundant management environment—providing a holistic view of the entire system for optimal monitoring as well as redundant notification paths to help ensure that administrators are alerted when events occur.

Steven Grigsby is a test engineer in the Dell OpenManage Product Test organization. He has a B.S. in Computer Science from the University of Oklahoma.

Narayan Devireddy is a development manager in the Dell OpenManage Development organization. He has an M.S. in Computer Science from Alabama A&M University.

FOR MORE INFORMATION

Dell OpenManage:
www.dell.com/openmanage