Introduction to iDRAC6

A Dell Technical White Paper

Dell | Systems Management

Brian Doty

Mark MacLean

Learn more at Dell.com/OpenManage

Revision 1 February 2011

Contents

Tables

Figures

Introduction

The Integrated Dell™ Remote Access Controller 6 (or iDRAC6) is Dell's sixth generation remote access controller. It is designed to increase server administrators' productivity, reduce the total cost of ownership (TCO) and increase overall server availability of Dell servers. The iDRAC6 achieves these goals by alerting administrators to server warnings and failures, enabling remote server management, and providing power monitoring and budgeting features. The iDRAC6 is an out-of-band device in that it functions independent of the server's operating system; unlike in-band server management tools that typically involve installed software agents, the iDRAC6 sits "outside" the operating system.

Ultimately, the goal of iDRAC6 is to provide powerful yet simple control over Dell PowerEdge™ servers, thus reducing the need for the administrator to make a server-side visit. This paper explores how the iDRAC6 can help you extend your management reach.

> **"It [iDRAC] allows us to troubleshoot customer issues four times faster than before, and we're saving two administrator hours per day."**
>
> Larry Boeck, Microsoft Windows System Administrator, BTInet
> http://i.dell.com/sites/content/corporate/case-studies/en/Documents/2010-btinet-10008245.pdf

Choosing the Right iDRAC6

The iDRAC6 is an upgrade for many of Dell's 11th generation servers and is available in three versions:

- iDRAC6 Express
- iDRAC6 Enterprise
- iDRAC6 Enterprise with vFlash

iDRAC6 Express offers a rich management feature set, including a browser-based GUI, command line access, advanced authentication, rich power management controls, and powerful diagnostic information. iDRAC6 Enterprise extends this feature set by providing "as if you were there" remote access including Virtual Console and Virtual Media; it also provides increased flexibility with scripting capabilities and a dedicated network port. Lastly, iDRAC6 Enterprise with vFlash enables additional automation features, including virtual flash partitions and advanced Lifecycle Controller features. For more information on the Dell Lifecycle Controller, see the Additional Information section of this document.

The iDRAC6 Express is a standard offering on Dell™ PowerEdge™ 600 series and higher rack and tower servers, while iDRAC6 Enterprise is standard on all Dell PowerEdge M-series (blade) servers. The Baseboard Management Controller (BMC) is offered on Dell entry-level servers (500 series servers and lower), and is limited to Intelligent Platform Management Interface (IPMI) 2.0 management. Table 1 below lists all of the iDRAC6 product offerings by server line while Table 2 provides a more detailed explanation on the differences between the iDRAC6 offerings.

Table 1. iDRAC6 Offerings by Server Line

	Server Line			
	100 Series	***200-500 Series***	***600-900 Series***	***Blades***
BMC	✓ Standard	✓ Standard	-	-
iDRAC6 Express[1, 2] (includes Lifecycle Controller)	✘ Not Available	☑ Upgrade	✓ Standard	-
iDRAC6 Enterprise[2] (includes Lifecycle Controller)	✘ Not Available	☑ Upgrade	☑ Upgrade	✓ Standard
vFlash (includes Lifecycle Controller)	✘ Not Available	☑ Upgrade	☑ Upgrade	☑ Upgrade

[1]The iDRAC6 Express does not support graphical console redirection; this feature, known as *Virtual Console*, is available in iDRAC6 Enterprise and higher versions.

[2]Any level of iDRAC6 can be added to 200+ series PowerEdge servers after the time of purchase.

Table 2. iDRAC6 Feature Matrix

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
Interface & Standards Support				
IPMI 2.0	✓	✓	✓	✓
Web-based GUI		✓	✓	✓
SNMP & IPMI Discovery		✓	✓	✓
WSMAN		✓	✓	✓
SMASH-CLP (SSH)		✓	✓	✓
RACADM command-line (SSH & local)		✓	✓	✓
RACADM command-line (remote)			✓	✓
Connectivity				
Shared/failover network modes	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN tagging	✓	✓	✓	✓

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
IPv6		✓	✓	✓
Dynamic DNS	✓	✓	✓	✓
Dedicated NIC			✓	✓
Security & Authentication				
Role-based authority	✓	✓	✓	✓
Local users	✓	✓	✓	✓
SSL Encryption	✓	✓	✓	✓
Active Directory		✓	✓	✓
"Generic" LDAP support		✓	✓	✓
Two-factor authentication[3]		✓	✓	✓
Single sign-on		✓	✓	✓
PK Authentication (for SSH)			✓	✓
Remote Management & Remediation				
Remote firmware update		✓	✓	✓
Server power control	✓ [1]	✓	✓	✓
Serial-over-LAN (with proxy)	✓	✓	✓	✓
Serial-over-LAN (no proxy)		✓	✓	✓
Power budgeting		✓	✓	✓
Last crash screen capture		✓	✓	✓
Boot capture		✓	✓	✓
Virtual Media[2]			✓	✓
Virtual Console[2]			✓	✓
Virtual Console sharing[2]			✓	✓
Remote Virtual Console Launch			✓	✓
Remote File Share			✓	✓
Virtual Flash				✓
Monitoring				
Sensor monitoring & alerting	✓ [1]	✓	✓	✓
Real-time power monitoring		✓	✓	✓
Real-time power graphing		✓	✓	✓
Historical power counters		✓	✓	✓

Feature	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media
Logging				
System Event Log	✓	✓	✓	✓
RAC Log		✓	✓	✓
Trace Log		✓	✓	✓
Lifecycle Controller				
Unified Server Configurator	✓ [4]	✓	✓	✓
Remote Services (using WSMAN)		✓	✓	✓
Part Replacement				✓

[1] Feature is available, but only through IPMI and not a Web GUI.
[2] Virtual Console and Virtual Media are available using both Java and ActiveX® plug-ins.
[3] Two-factor authentication is available using ActiveX, and therefore only supports Internet Explorer®.
[4] The Unified Server Configurator for BMC is limited to operating system installation and diagnostics only.

Getting Started

When a rack-mount or tower server with iDRAC6 is shipped from the factory it will have the default IP address of 192.168.0.120, and a default user name and password of “root” and ”calvin”; this configuration is meant to simplify deployment for when the system arrives in a user environment. The iDRAC6 in blade servers takes a slightly different approach by disabling the iDRAC6’s network interface. This is to prevent duplicate IP addresses. All M1000e blade chassis come equipped with a Chassis Management Controller (CMC) which allows users to manage all the iDRACs in the blade chassis.

Since August 2009, Dell has offered an option known as *Auto Discovery* with all its Lifecycle Controller-equipped servers. Lifecycle Controller is present on all servers that have iDRAC6 Express or higher. When servers are ordered with this option enabled, the iDRAC6 will arrive without user credentials and with DHCP enabled. Once power is applied to the server, the iDRAC6 will locate a provisioning server through the network. For more information on Auto Discovery and the Dell Lifecycle Controller, see the Additional Information section of this document.

The iDRAC6 Enterprise for rack-mount and tower servers offers three different configurations for its physical network connection. See Figure 1 below.

Did you know?

The CMC includes a feature that allows users to quickly assign network settings to all the iDRACs in the chassis? It also has a feature called QuickDeploy which allows users to assign these network settings to a blade slot for blade pre-deployment.

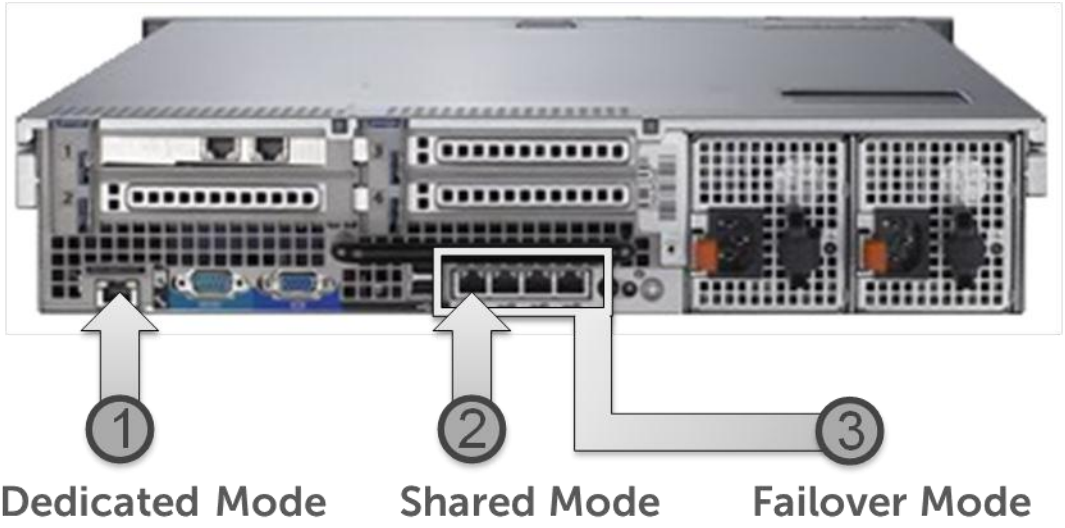

Figure 1. iDRAC6 Network Options

Shared and failover modes are the only options available for iDRAC6 Express. Shared mode allows a user to host two different MAC addresses on the first LAN on Motherboard (LOM) port; this separation at the MAC layer simplifies switch configuration and minimizes network ports. In addition, the LOM will constrain the iDRAC6 bandwidth during use and therefore minimize the impact to in-band traffic. For users that still want to maintain some separation between the in-band network and the iDRAC6, virtual LANs are supported on the device. Failover mode adds the ability to failover to other LOMs in case LOM1 loses network connectivity. Dedicated mode is available with the iDRAC6 Enterprise and higher, and although it requires a separate network port, the dedicated mode provides complete physical separation between the LOMs and the iDRAC6. The iDRAC6 dedicated network port is located on the rear of the server and labeled with a spanner icon.

Note: The iDRAC6 for blade servers is limited to a dedicated management port that is consolidated by an Ethernet switch that is on the Chassis Management Controller (CMC).

In each configuration, the iDRAC6 has a MAC and an IP address that is either statically set or obtained using DHCP; both IPv4 and IPv6 Internet protocols are supported on iDRAC6 individually or as a dual stack. When using the dual stack, the iDRAC6 can have multiple IP addresses: one IPv4 address and up to sixteen IPv6 addresses. The iDRAC6 IP address settings can be viewed and configured using <Ctrl><E> during the server POST, using local Command Line Interface (CLI) commands, using OpenManage™ Server administrator (OMSA), or the by accessing the server or blade chassis' interactive LCD panel.

To make the iDRAC6 easier to address, it also supports dynamic DNS registration. The default DNS name is equal to "idrac-" plus the system's unique service tag.

Did you know?

You can read and set the iDRAC6's IP address using the front panel LCD? This includes the ability to set the IP addresses of all the blades and CMC of an M1000e modular chassis.

iDRAC6 Essentials

Though the iDRAC6 Express has a robust feature set, it is geared towards more cost-sensitive environments. The iDRAC6 Express retails for $99 USD at publication of this paper. The focus of this paper is on the fully featured iDRAC6 Enterprise. The iDRAC6 operates independently from the server's CPU and operating system. The iDRAC6 functions even if the server is powered off, no operating system is installed, or the operating system is inoperable. This capability makes iDRAC6 a mainstay in remotely managed data centers and distant offices where remote desktop applications (such as RDP) are not sufficient due to their dependency on a running operating system.

One of the most important features of iDRAC6 is its SSL-protected Web GUI interface. Figure 2 below details the main page of the iDRAC6 Web GUI. The iDRAC6 home page provides quick access to the most commonly used information and tasks and is broken down into five distinct sections:

- Server Health
- Virtual Console Preview
- Server Information
- Quick Launch Tasks
- Recently Logged Events

Each of these sections plays an important role in managing a remote server. The Server Health section provides a snapshot of the overall server health by displaying the status of server hardware sensors. The Virtual Console Preview offers a snapshot of the remote server's console screen. Automatically updated every 30 seconds, this image quickly allows a remote administrator to determine the OS state and if there may be another user interacting with it. Because the Virtual Console feature is available with iDRAC6 Enterprise and higher, this section will not show up on the home page of an iDRAC6 Express. The Server Information section provides data commonly needed by administrators such as the server model, power state, operating system, and unique identifiers. The Quick Launch Tasks section is designed to provide easy access to common iDRAC6 features and setup options. Finally, the Recently Logged Events section provides the last ten events from the server's system event log (SEL); the SEL is an IPMI-based standard log that contains a history of server health events.

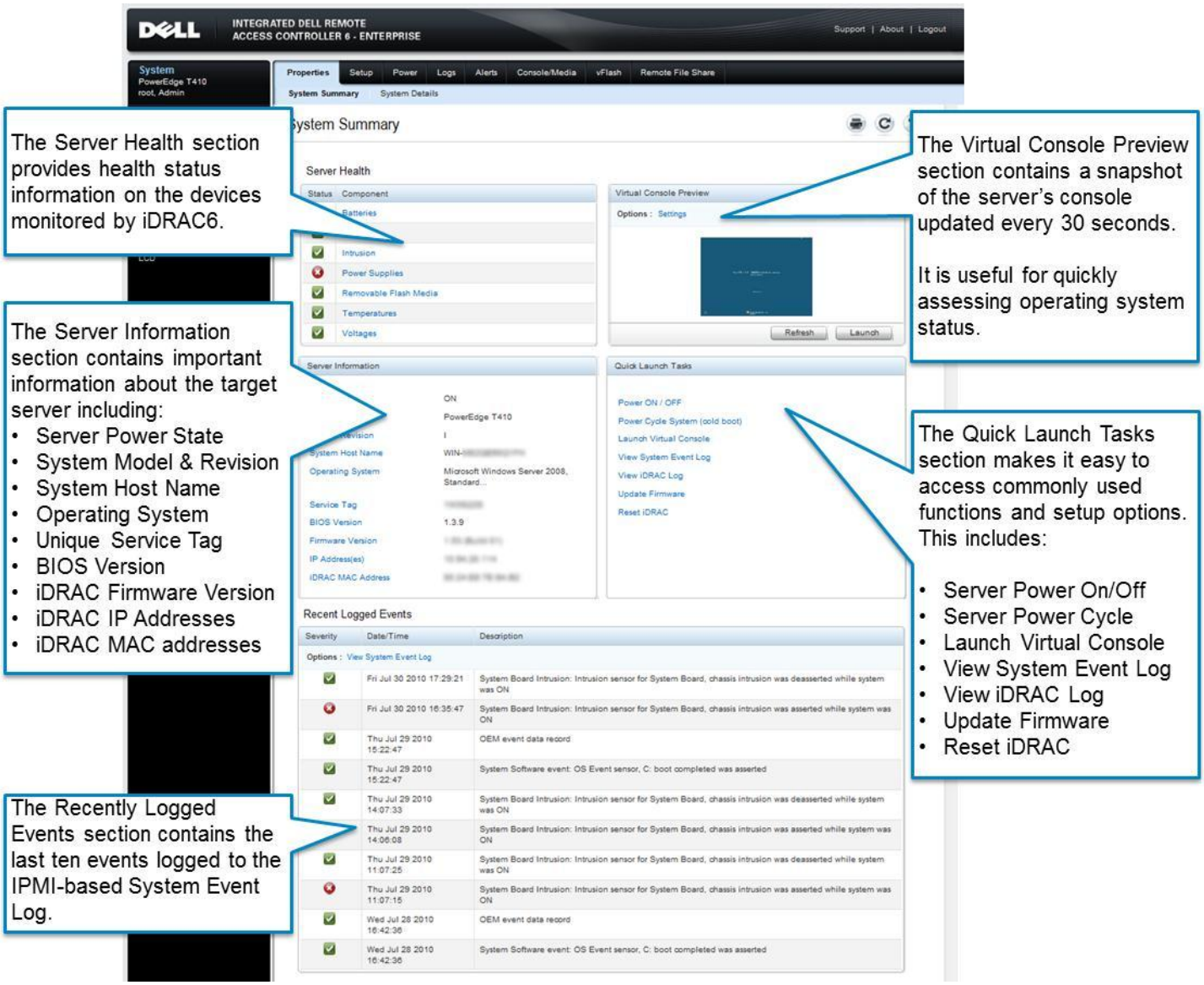

Figure 2. iDRAC6 Home Page

The iDRAC6 Enterprise features are designed to provide an "as if you were there" management experience; to accomplish this, iDRAC6 offers several remote management features briefly described in Table 3.

Table 3. iDRAC6 Enterprise Features

Feature	Benefit	Availability
Remote Power Control	One of the most fundamental remote management tasks is remote power control. This iDRAC6 feature allows administrators to remotely control the power state of the system. In the most severe case of server disruption, the iDRAC6 can allow an administrator to power cycle a server that is locked-up.	iDRAC6 Express and higher
Alerts & Filters	Not only does the iDRAC6 monitor the state of server hardware, it also offers the ability to send platform event traps (PETs), and follow up with emails to warn administrators when they occur. In addition, the iDRAC6 can be configured to automatically trigger certain platform actions (such as a power cycle) when a monitored event occurs.	iDRAC6 Express and higher
Virtual Console	The virtual console provides secure redirection of the keyboard, video, and mouse regardless of operating system state. This feature allows administrators to perform tasks securely from a remote site just as if they were local to the system.	iDRAC6 Enterprise and higher
Virtual Media	Virtual media provides a secure method for the user to share a CD, DVD, floppy, USB storage device, or ISO/IMG images from their own system as though they were devices directly attached to the server. Virtual media complements the virtual console by minimizing the need to physically visit a server for general management or resolution tasks (such as software installation). Virtual media is integrated into the virtual console and is available as a command line option.	iDRAC6 Enterprise and higher
Remote File Share	Remote file share is similar to virtual media, with one key difference; the ISO image used for the remote media is located on a file share eliminating the need to keep the Virtual Console client open. This is beneficial to administrators who are managing multiple servers, use images on distant file shares, or simply don't want to tie up their local client for long periods of time.	iDRAC6 Enterprise and higher
Virtual Flash	Virtual flash is also similar to virtual media, but the information is stored on the iDRAC6's 8GB vFlash media card. The iDRAC6 allows for up to 16 partitions, ranging in sizes from 1MB to 4GB. These partitions can be emulated as CDs, floppy disks, or as a traditional USB key that can be attached to and detached from the server under the control of a remote administrator.	iDRAC6 Enterprise with vFlash

Virtual Console

The Virtual Console is one of the most important features available in iDRAC6. Virtual Console redirects exactly what is shown on the server's video connector to the client regardless of the server state. Users can use it to view a power on self-test (POST), BIOS setup interaction, or operating system start up as if watching the server locally. All communications can be encrypted for secure use from any location.

Did you know?

You can use launch the iDRAC6 Virtual Console without even logging into the Web GUI? Simply type your iDRAC6's DNS name or IP address followed by "/console" (i.e., https://my_idrac_dns_name/console) into your browser and it will automatically launch the Virtual Console window.

The Virtual Console is supported using either Microsoft® ActiveX® or Java browser plug-ins on the client system. There is no need to go to www.dell.com to get the plug-ins, because the iDRAC6 stores them for direct download by the browser; by default, the iDRAC6 will use ActiveX® when the client browser is Internet Explorer and Java when the client browser is Firefox though this setting can be customized.

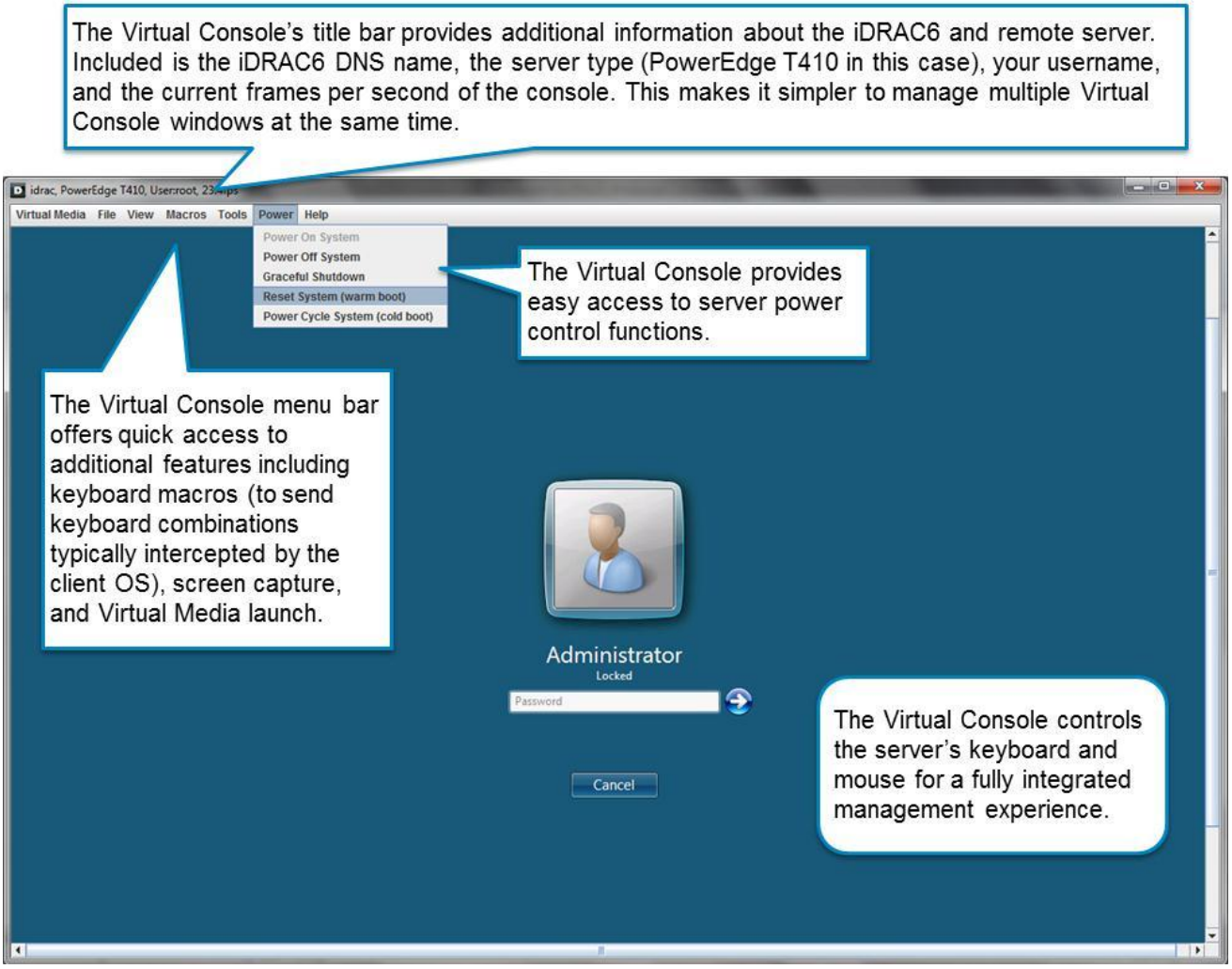

Figure 3. Virtual Console

Power control and virtual media support are also built-in to the Virtual Console for ease of use; this removes the need for users to switch to and from the iDRAC6 Web GUI to access these common management features. The Virtual Console also provides a "Macros" drop-down menu that allows users to send keyboard combinations that are often intercepted by the local client's operating system such as <Alt><Ctrl><Del>.

The Virtual Console allows for up to four users to collaborate on a single remote iDRAC6 Enterprise. The first user is considered

Did you know?

If you enable the keyboard pass-through mode under Tools —> General and Full Screen mode View —> Full Screen, you can send almost any keyboard combination without the use of the Macros menu?

the “master” user and can grant privileges (full access, read-only access, and no access) to additional users. This feature goes beyond “as if you were there” management, and brings together several administrators as if they were actually huddled in front of the server’s local console.

Remote Media Functions

The iDRAC6 offers three different types of remote media functions: Virtual Media, Remote File Share, and Virtual Flash Partitions (vFlash).

> **“The iDRAC is great because it lets us troubleshoot and upgrade software in our London datacentre from our office in Edinburgh. Tasks such as mounting a CD can be completed in two minutes as opposed to several hours if an employee had to be present onsite.”**
>
> Paul Redpath, Managing Director, Catalyst2
> http://content.dell.com/us/en/corp/d/corporate~case-studies~en/Documents~2010-catalyst2-10008457.pdf.aspx

Virtual Media

Similar to the Virtual Console’s redirection of the graphical console, Virtual Media redirects media devices and images. Users can share a CD or DVD in their local optical drive, share a floppy disk, LS120, or a zip file located in their local floppy drive, or share a local USB key or other USB mass storage device. (See Figure 4.) Users can also share ISO and IMG images with the remote server, which is useful as many current systems do not support any removable media devices.

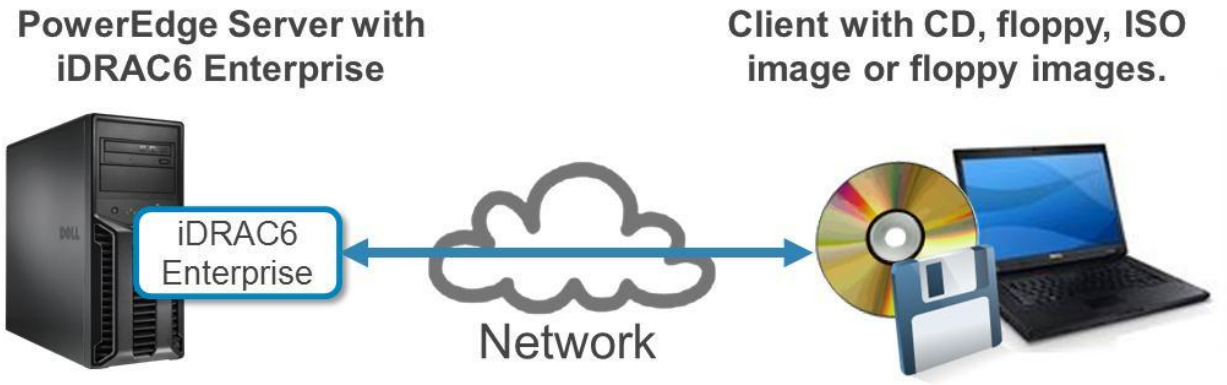

Figure 4. Virtual Media

The benefit that Virtual Media provides over simple file sharing with the remote operating system is that it is completely out-of-band. This means that Virtual Media can be used at boot time or pre-OS, such as in a DOS or UEFI environment, as well as in the operating system itself. This is made possible by the iDRAC6 that presents the remote client's device/images as a local physical device at the server. The Server OS will treat this as any other device and assign the appropriate drive letter. (See Figure 5.)

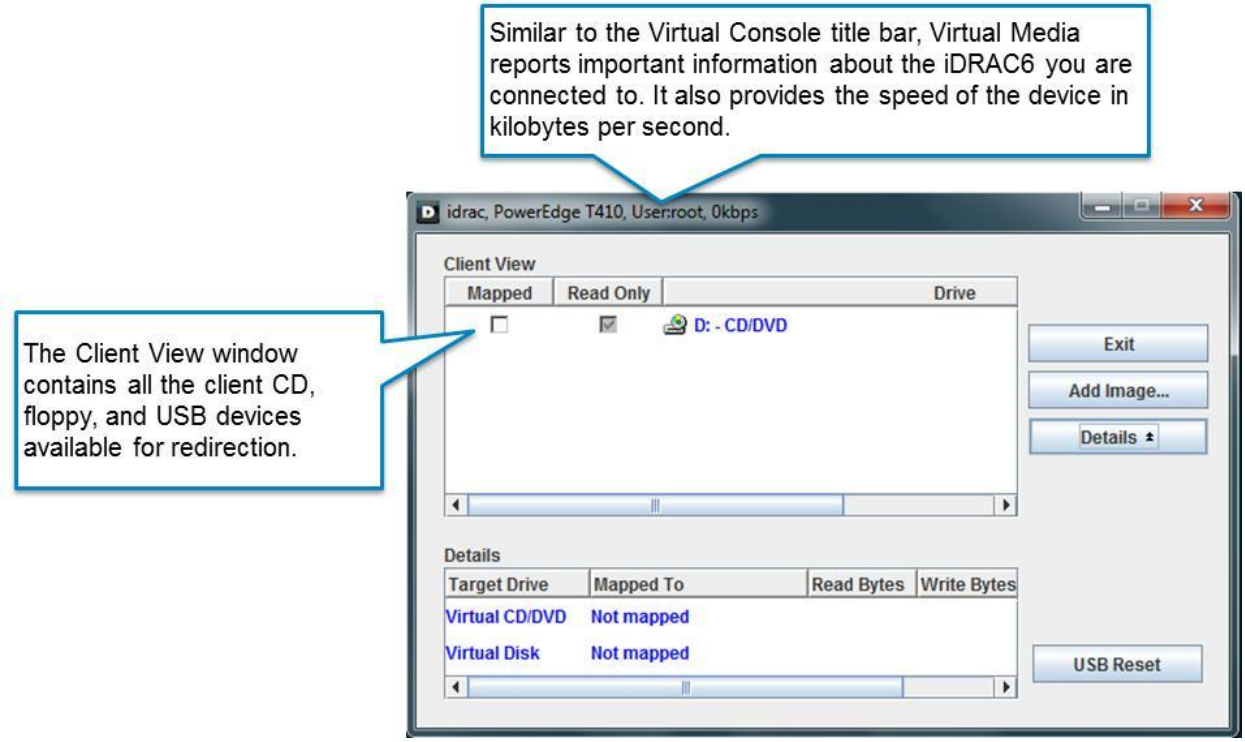

Figure 5. Virtual Media Control Window

One disadvantage of Virtual Media GUI, as you see it above, is that it does not scale beyond a single server and it cannot be scripted. To enable scripting, Dell offers a tool called Integrated Virtual Media CLI (iVMCLI). This command line tool makes it possible to access all of the Virtual Media features directly from a command line.

Remote File Share

To resolve the Virtual Media scaling, Dell took a different approach and offers a feature known as Remote File Share (see Figure 6). This feature does not require the presence of a client, and allows one or more iDRAC6s to connect to an ISO image on a network file share. Because Remote File Share is available from the RACADM command line (you can read more about this in the Command Line section), savvy do-it-yourselfers can script a mass deployment to many servers at the same time.

Did you know?

You can configure the iDRAC6 to boot to Virtual Media devices only on the next reboot using the boot once feature? This feature can be accessed using the iDRAC6 Web GUI under System —> Console/Media —> Virtual Media —> Enable Boot Once and at System —> Setup —> First Boot Device.

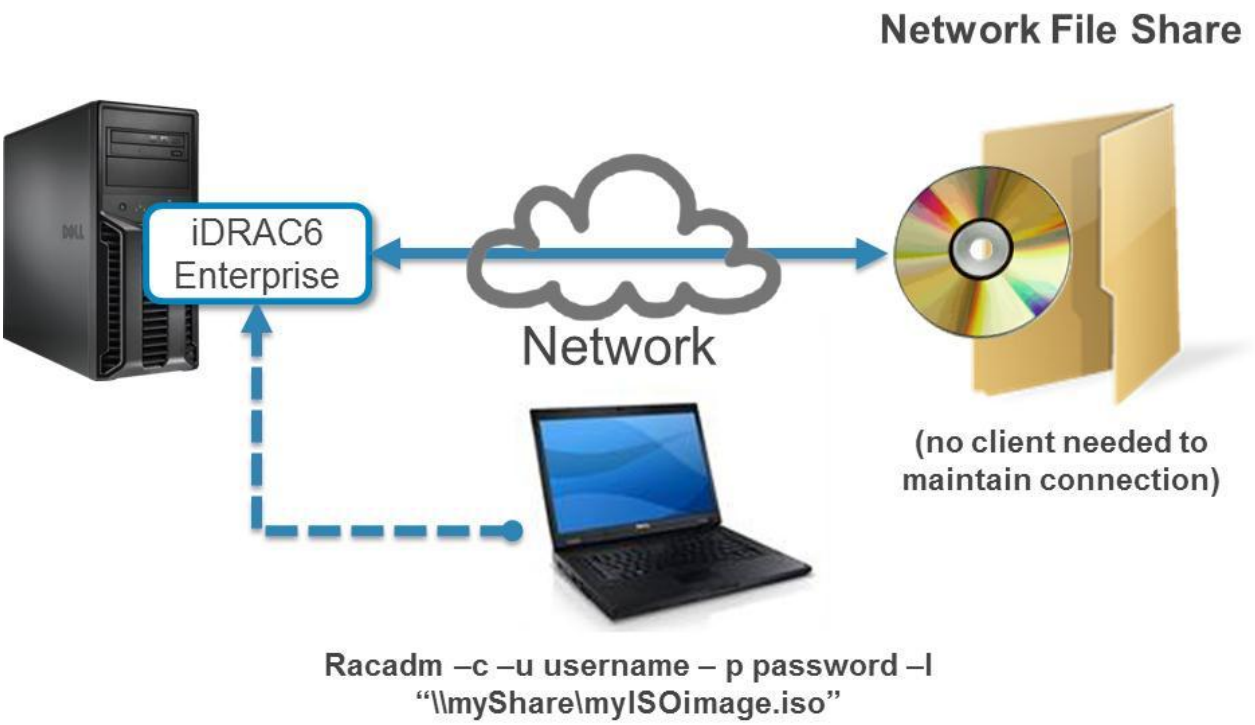

Figure 6. Remote File Share

vFlash

As explained in the Virtual Media section, the iDRAC6 has a number of capabilities with respect to remote media functions, and Virtual Flash adds in a few more. Unlike Virtual Media and Remote File Share where the virtualized image is stored on the client or on a file share, the image/data used for Virtual Media is stored local to the server on the Dell vFlash media card. See Figure 7.

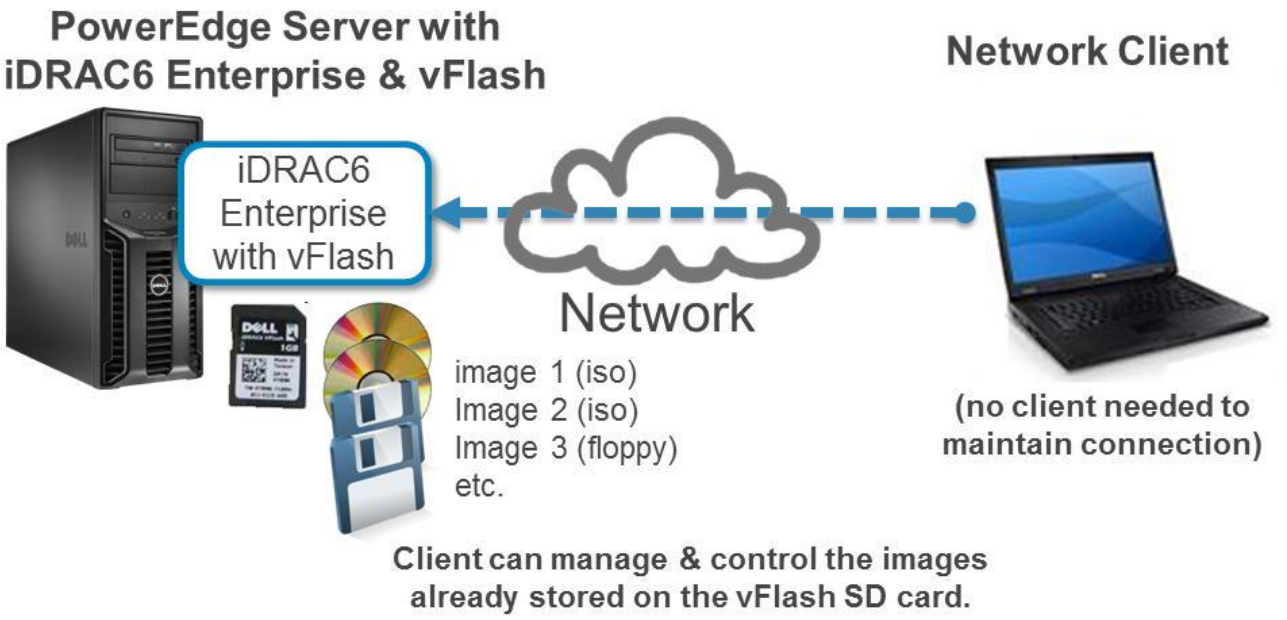

Figure 7. vFlash

The Dell vFlash media card is a custom SD card that can be plugged into the dedicated SD slot on the iDRAC6 Enterprise on the back of a rack-mount or tower server near the management Ethernet port. On blade servers, the slot is located internally near the mid-plane connector. vFlash can be managed from the vFlash tab in the iDRAC6 Web GUI. From the vFlash tab, users can create up to 16 independent partitions from 1MB to 4GB in size. These partitions can be created as empty partitions and formatted as FAT16, FAT32, EXT2, and EXT3, and emulated as CDs, floppy disks, and hard disks. Partitions can also be created by uploading an ISO or IMG image. Additionally, partitions can be downloaded when a remote administrator needs to access information that the operating system has written to the partition. See Figure 8.

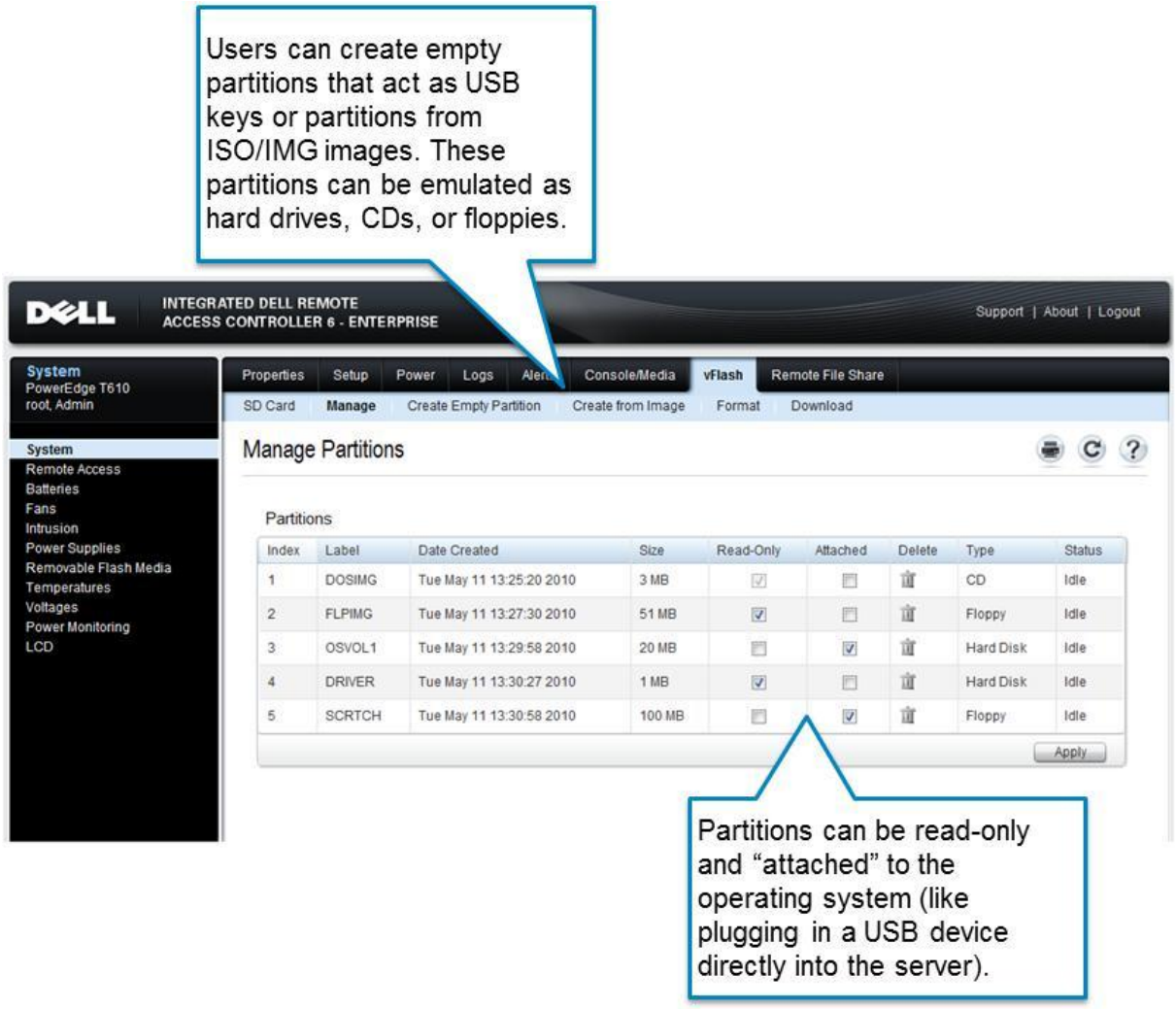

Figure 8. vFlash Manage Partitions Screen

Just like Virtual Media and Remote File Share, any attached vFlash partition can be set as a temporary boot device using the “boot once” feature. For more information on vFlash, including potential use cases, see the Additional Information section.

Note: SD Cards provided by vendors other than Dell will function but have a significantly reduced feature set; they are limited to one partition that is no larger than 256 MB.

Power Management

The iDRAC6 not only provides the ability to control the server power state, it also reports a host of real time and historical power usage counters; this information is provided to aid users with power capacity planning. These counters are also available from the CLI and allow users to analyze this information across multiple servers. See Figure 9 for more information.

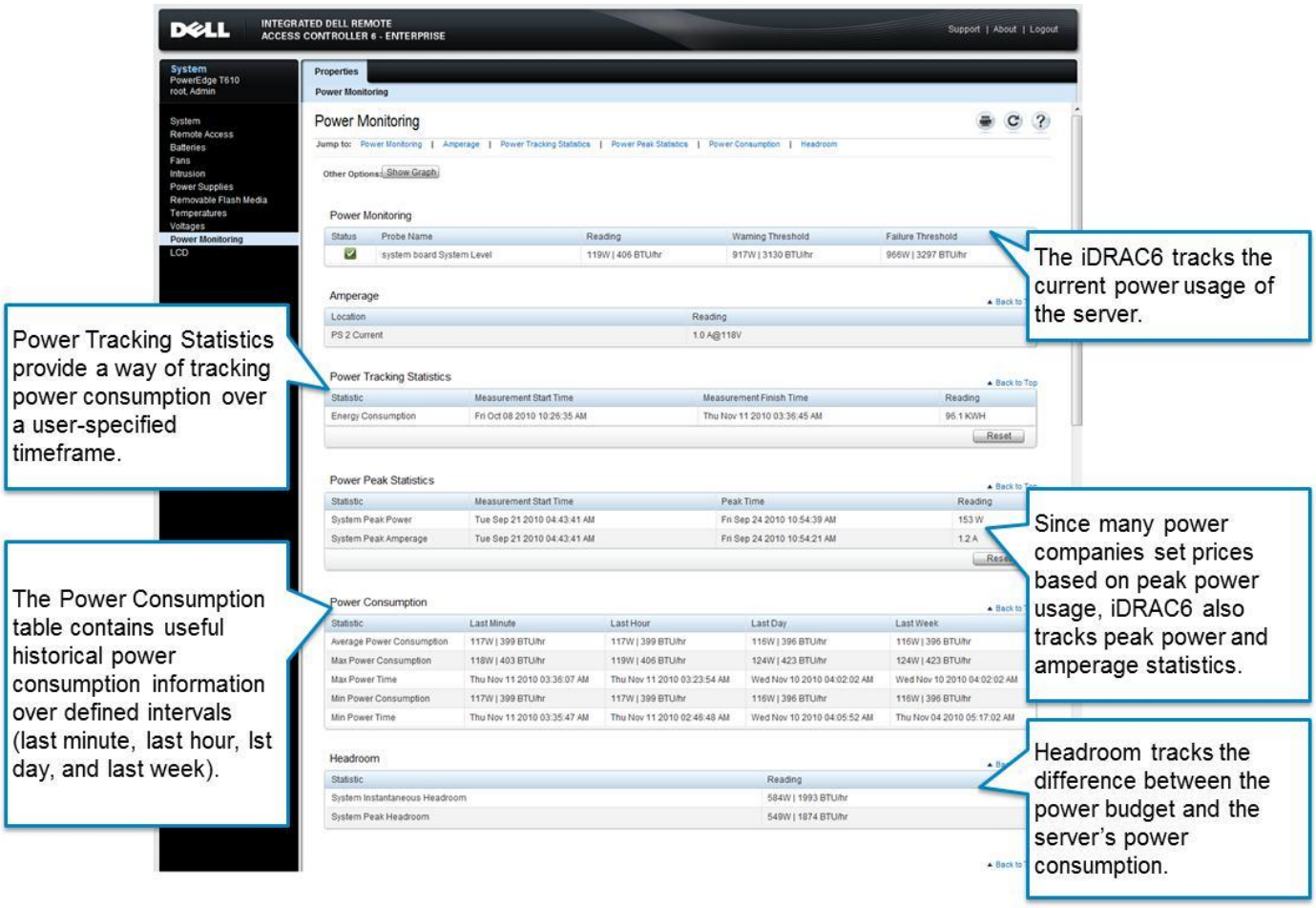

Figure 9. Power Monitoring

The iDRAC6 also supports the ability to graph power consumption and amperage over several time ranges. These graphs allow users to visually inspect the power usage, as far back as one week, to better understand the peaks and valleys of power usage. See Figure 10 for an example of iDRAC6's power-graphing capabilities.

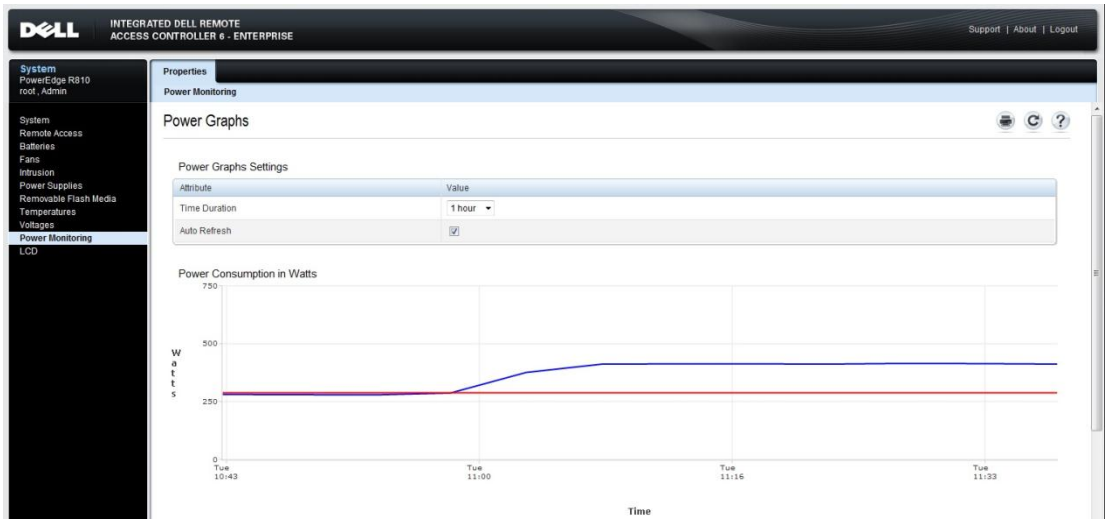

Figure 10. Power Graphing

The iDRAC6 for rack and tower servers provides additional capabilities beyond monitoring power usage, including a method to limit the power that the server can use. This feature, called Power Budgeting, enforces a user-defined power cap on the server and reduces the impact of peak usage and reducing overall sustained power consumption.

Note: Because blade servers make use of shared infrastructure and power, the CMC controls the power-budgeting aspects for the entire chassis and iDRAC6 provides power control and monitoring capabilities.

Command Line

The iDRAC6's supports several command line interfaces, but the standard CLI is known as RACADM (Remote Access Controller ADMinistrator). iDRAC6 also supports IPMI and SMASH CLP. These command lines are designed to be used interactively, as well as in scripted applications, and are available in a variety of different interfaces. Table 4 below describes each interface and how it can be accessed by the user.

Table 4. Command Line Protocols

Command Line Protocol	Direct Serial	Local on Host OS	Telnet/SSH	Remotely over IP
IPMI	✓	✓		✓
SMASH CLP	✓		✓	
RACADM	✓	✓	✓	✓

RACADM is the preferred command line for iDRAC6 due to the number of supported interfaces, its exhaustive feature set, and its support across all Dell remote access controllers.

Below is an example RACADM command that sets the iDRAC6 IP address:

```
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.1
```

For more information on RACADM, see the Command Line Reference Guide available on support.dell.com. This guide details RACADM usage, as well as all available commands for remote access products, including iDRAC6 for racks and towers, iDRAC6 for blades, and the Chassis Management Controller.

The iDRAC6 offers two other command line interfaces that extend its versatility: IMPI and SMASH CLP

IPMI (or Intelligent Platform Management Interface) version 2.0 is supported by the iDRAC6 and allows for a powerful set of commands. Many of these commands conform to available industry standards making it simple for users to build scripts for heterogeneous environments. The most common way to access IPMI is by using the Open Source IPMI Tool. This tool converts English-based commands into low-level hex commands understood by iDRAC6's IPMI parser. IPMI Tool will work direct serial or locally on the host OS, as well as remotely.

The standards based SMASH CLP can be accessed using ssh and telnet sessions to the iDRAC6. Supported SM-CLP commands are documented in the *iDRAC6 User's Guide* on support.dell.com.

Security

The iDRAC6 is a feature-rich tool, but these features would not be useful without high security standards; iDRAC6's remote access monitoring and remediation features make secure access all the more important. Customers, small-business and enterprises alike, require the iDRAC6 to handle security so they don't have to.

The following features are provided by iDRAC6 to provide secure remote access.

- Role-based authority: Enables administrators to configure specific privileges for each user.
- Password-protected local users: Supports up to 16 IPMI-based local user accounts protected by passwords.
- PK Authentication: Allows for the use of a private key to authenticate over SSH instead of the typical user name/password authentication.
- LDAP integration: Enables users to centralize user management into an LDAP service, such as Microsoft Active Directory with standard/extended schema, Open DS, Novell® eDirectory™, and others. The iDRAC6 also supports Single Sign-On with Microsoft Active Directory.
- Session time-out: Provides automatic session time-out for inactivity.
- Configurable TCP and UDP ports: Allows administrators to customize the ports used by many of the iDRAC6 services.
- Login failure limits with IP blocking: Blocks access by a range of IP addresses if too many failed login attempts are made.
- Limited IP address range: Enables administrators to restrict the IP addresses of clients connecting to the iDRAC6.
- Web-browser secured with 256-bit Secure Sockets Layer (SSL) (limited to 40-bit encryption for certain countries).
- SSH: Supports 128-bit Secure Sockets Layer (SSL) (limited to 40-bit encryption for certain countries).

- VLAN support: Enables iDRAC6 traffic to be located in a private "management VLAN" in both dedicated and shared network modes.
- Smart card login: Enhances security by enabling two-factor authentication with smart card authentication.
- Encryption services: Supports Virtual Console and Virtual Media encryption.

In addition to the security features listed above, the iDRAC6 supports several audit controls including a boot capture feature which allows customers to play back a video of the last three instances of the BIOS POST. It also supports two logs to aid in troubleshooting and internal auditing; the system event log (SEL) is an IPMI-based log maintained by iDRAC6 that tracks hardware failures. The remote access controller log (RAC Log) is also maintained by iDRAC6, and tracks administrative events such as login attempts, configuration changes, and other such items. Both of these logs are accessible using each of the iDRAC6 interfaces, and users can configure iDRAC6 to send log entries to a Linux® remote syslog server for consolidation and additional auditing measures.

Note: Unless the iDRAC6 is ordered with Auto Discovery enabled, it will use a default user name and password of "root" and "calvin." It is important to set a new password for the root account during server deployment.

For more information about iDRAC6 security, please see the *Integrated Dell Remote Access Controller 6 Security* white paper on DellTechCenter.com.

Value-Add Tools

Dell offers several tools that simplify the management of iDRAC6 as well as allow users to extend its functionality. These tools can be downloaded from support.dell.com at no additional charge.

Dell Remote Access Configuration Tool

The Dell Remote Access Configuration Tool (DRACT) is designed to make the complexities of deploying Microsoft Active Directory (AD) on a Dell remote access device a simple endeavor. DRACT does this by discovering DRACs in a given IP address range, and then guiding a user through the process of deploying a standard or extended AD schema or migrating Dell remote access controllers from one schema to another. At publication date of this paper, the tool supports DRAC4, DRAC5, iDRAC6, and CMC. DRACT is also able to perform a firmware update of supported Dell remote access controllers in a 1-to-many situation.

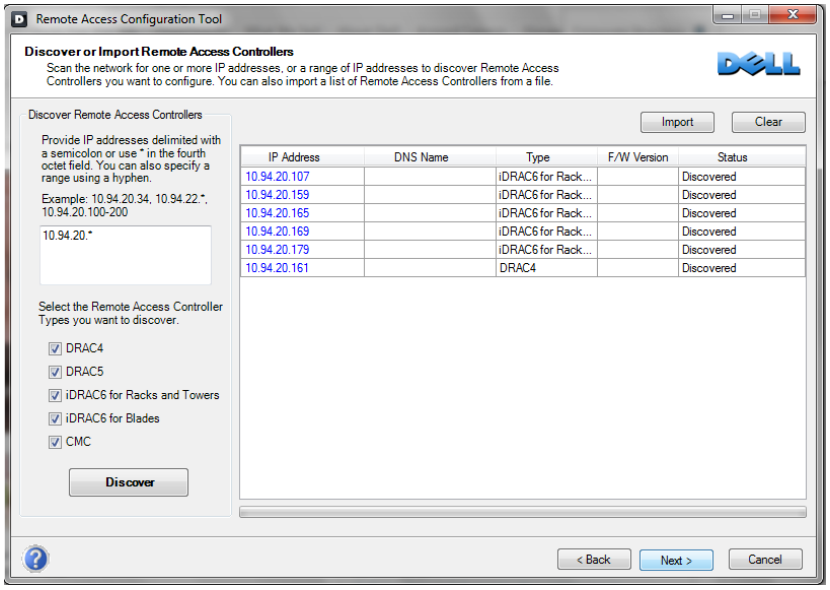

Figure 11. Dell Remote Access Configuration Tool

For more information on DRACT see the *Dell Remote Access Configuration Tool* white paper on delltechcenter.com.

To download the DRACT, see the Dell Remote Access Configuration Tool on support.dell.com.

Dell Remote Windows Debugger Utility

Using Windows Debugger (WinDbg) or (Kernel Debugger (KD), Dell Remote Windows Debugger Utility (DWDU) provides the remote debugging capability of Microsoft® Windows® operating systems by virtualizing the server's serial port. This virtualization capability is provided by DRAC, and allows the user to redirect WindDbg and Kernel Debugger data to any remote client with DWDU installed. At publication of this paper, DWDU supports DRAC5 and iDRAC6.

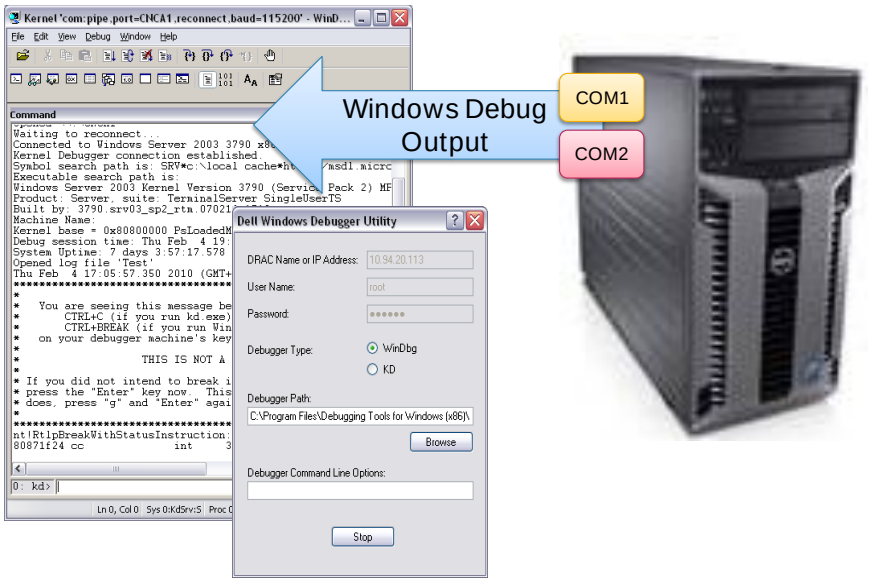

Figure 12. Dell Remote Windows Debugger Utility

For more information on DWDU see the *Remote Microsoft Windows Server OS Kernal Debugging Using Dell Windows Debugger Utility (DWDU)* white paper on delltechcenter.com.

To download the DWDU, see the Dell Remote Windows Debugger Utility on support.dell.com.

Additional Information

For more information on items such as AD integration and the RACADM CLI command set, refer to *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* located at support.dell.com. User Guides for Lifecycle Controller, the Chassis Management Controller (CMC), and other Dell Systems Management products can also be found on support.dell.com.

Looking for more iDRAC6 white papers? See OpenManage white papers on Dell TechCenter.

Join Dell's technical community at Dell TechCenter to learn more about iDRAC6 and other Dell products.

Learn what customers are saying about iDRAC6 and other Dell products at www.dell.com/casestudies.