

iDRAC9 with Lifecycle Controller—Best in class management for Dell EMC 14th generation PowerEdge Servers

This technical white paper lists the enhancements that iDRAC9 with Lifecycle Controller provides the customers in the Dell EMC 14th generation PowerEdge servers. The method in which the cutting edge technologies offered by PowerEdge servers align with the four pillars of IT infrastructure management are discussed in brief.

Dell OpenManage Product Marketing
June 2017

Authors

Rick Hall

Raja Tamilarasan

Doug Iler

Sheshadri PR Rao (InfoDev)

Revisions

Date	Description
June 2017	Initial release

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © June-2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [10/11/2017] [Technical White Paper]

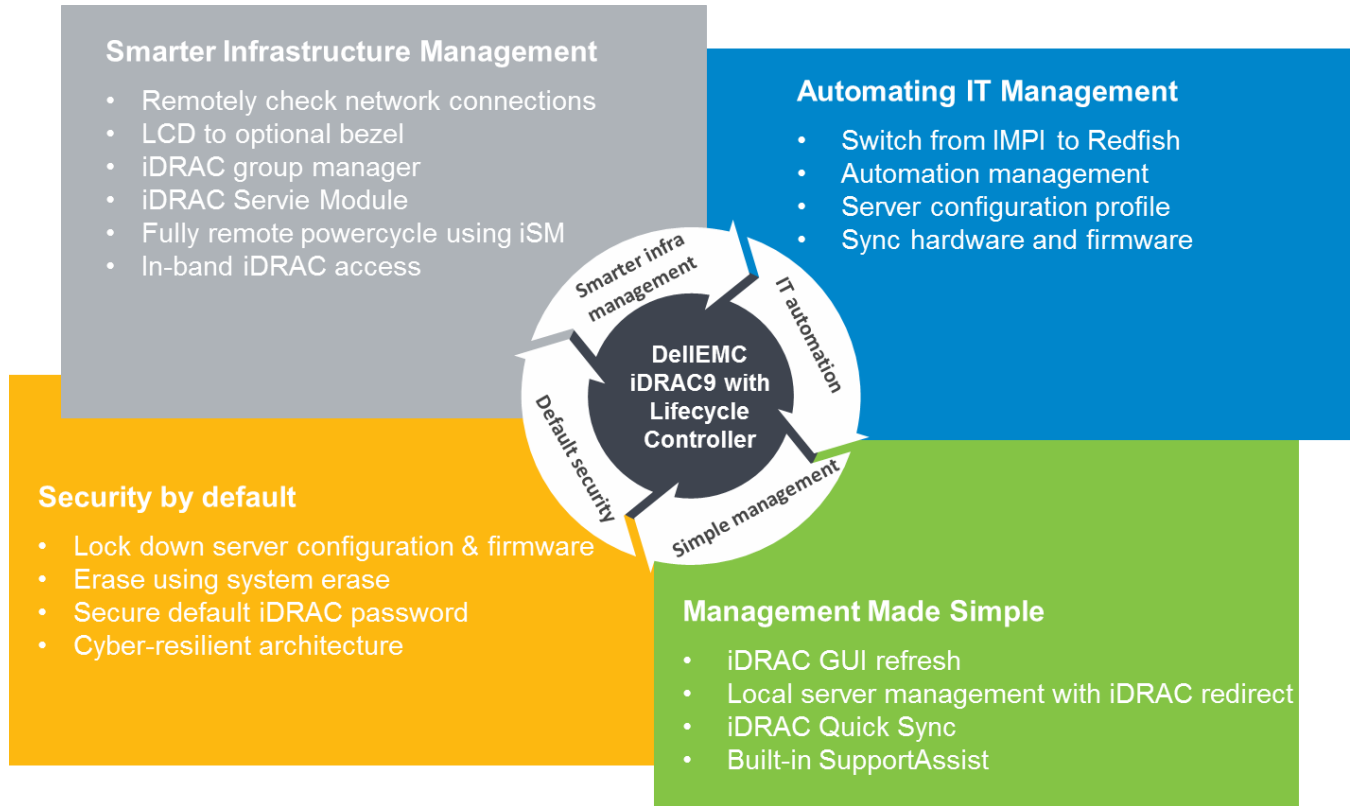
Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Revisions.....	2
Executive summary.....	4
Audience.....	4
1 iDRAC9—Server industry’s leading Embedded Management solution	5
1.1 Four pillars of Systems Management.....	5
1.1.1 Automating IT management	6
1.1.2 Management Made Simple.....	8
1.1.3 Security by Default	10
1.1.4 Smarter Infrastructure Management.....	11
1.1.5 iDRAC Security best practices	13
Additional resources	14

Executive summary

This technical white paper briefly describes the enhanced feature that iDRAC9 with Lifecycle Controller offers to enable you manage your servers to ensure that your business-critical services are available 24x7 globally. The key innovations designed to help IT teams securely and effectively deploy, update, and monitor the latest generation of Dell EMC PowerEdge Servers are discussed with its benefits. Enhancements made in the 14th generation servers are listed.



The 14th generation PowerEdge servers supplied with preinstalled iDRAC9 with Lifecycle Controller fulfill the requirements of four pillars of IT infrastructure management

Audience

This technical white paper is intended for server administrators, architects, and other stake holders in decision making capacities. The reader is expected to have basic knowledge about server management applications.

1 iDRAC9—Server industry’s leading Embedded Management solution





The integrated Dell Remote Access Controller 9 (iDRAC9) with Lifecycle Controller delivers advanced, agent-free, local and remote server administration. Embedded in every PowerEdge server, iDRAC9 provides a secure means to automate a multitude of common management tasks. Because iDRAC is embedded in every PowerEdge server, there is no additional software to install; just plug in power and network cables, and iDRAC with Lifecycle Controller is ready to go. Even before installing an operating system (OS) or hypervisor, IT administrators have a complete set of server management features at their fingertips—Maximize storage performance with up to 12 NVMe drives and ensure application performance scales easily.

With iDRAC9 in place across the Dell EMC PowerEdge portfolio, the same IT administration techniques and tools can be applied throughout. This consistent management platform allows easy scaling of PowerEdge servers as an organization’s infrastructure needs to grow. Customers will be able to use the iDRAC RESTful API for the latest in scalable administration methods of PowerEdge servers. With this API, iDRAC enables support for the Redfish standard and enhances it with Dell EMC extensions to optimize at-scale management of PowerEdge servers. Regardless of size, the entire OpenManage portfolio of Systems Management tools allows every customer to tailor an effective, affordable solution for their environment.

The iDRAC9 provides a faster and powerful processor compared to the iDRAC8. Driven by a dual-core processor and with twice the memory, the iDRAC9 provides almost 4X faster performance compared to its previous generations.

1.1 Four pillars of Systems Management

The top four pillars of Dell EMC systems management closely align with the issues and business challenges faced by many IT departments across the globe.

 <p>Automating IT management</p> <p>Dell EMC offers comprehensive automation management for reducing OPEX and increasing uptime and overall efficiency</p> <p>Comprehensive suite of tools to automate IT infrastructure “your way”</p>	 <p>Management made simple</p> <p>Simple but powerful tools for managing your Dell EMC servers</p> <p>Built-in tools that streamline support engagements</p> <p>Innovative “at-the-box” management features</p>	 <p>Security by default</p> <p>Dell EMC servers offer robust security defenses to thwart the next generation of malicious attacks</p> <p>Security is designed deep into the hardware and firmware architecture for optimal protection</p>	 <p>Smarter Infrastructure Management</p> <p>Dell EMC offers a next generation one-many console to manage your IT and server infrastructure</p> <p>Embedded intelligence which is “infrastructure-aware” to optimize troubleshooting and deployment</p>
---	---	---	---

This technical white paper showcases the prime new and greatly improved features of iDRAC9, and covers the various topics as they fit under the respective categories. All these tools are designed to drive simplicity, efficiency, and availability for Dell EMC PowerEdge Servers.

1.1.1 Automating IT management

It is no secret that IT teams are continually challenged with increased workloads with reduced personnel. It is at this point when the focus shifts to automation. Having a streamlined process that yields quick and repeated successful results saves time and money. Dell EMC is committed to helping drive new innovation in regards to automation to provide both efficiency and scalability in datacenters around the globe.

Automation is not a new concept to the iDRAC; it is been in practice for multiple generations. However, here are some of the items we have enhanced in iDRAC9.

Make the switch from IPMI to Redfish

Redfish® is an open industry standard specification and schema that specifies a RESTful interface and utilizes JSON and OData to help customers integrate solutions within their existing tool chains. Refer to the [DMTF Redfish](#) page for more information.

- Benefits
 - REST-based API
 - More secure and scalable than IPMI
 - Easier to script
 - Multi-vendor support
- 14G Enhancements
 - Latest DMTF additions for server configuration and update
 - Support for Dell Server Configuration Profile (SCP)

Dell's 14th generation Lifecycle Controller improves automation management

Dell PowerEdge servers support automated configuration of device attributes for a variety of devices. For more information, see [BIOS and NIC Configuration whitepaper](#).

- Benefits
 - High Resolution Attributes: iDRAC continues to provide industry leading deep level details on components such as HDDs, PERC, NICs, and HBAs to help IT admins precisely and effectively manage details in scripts.
 - Reduce OPEX and increase availability
 - Extensive library of Python and PowerShell scripts
- 14G Enhancements
 - More Fibre Channel HBA attributes
 - Improved agent-free hardware and software RAID management without an OMSA agent
 - Gen 2 NVMe management

Speed up the server deployments using Dell's Server Configuration Profile (SCP)

The heart of embedded management in every Dell PowerEdge server, the iDRAC with Lifecycle Controller provides the ability to generate a human-readable snapshot of server configuration via a Server Configuration Profile. This single file contains all BIOS, iDRAC, Lifecycle Controller, Network, and Storage settings. After capturing, this file can be modified, as required, and then applied to other servers—even with different server models. However, this operation requires attention to details such as I/O identity, storage configuration, and other settings that could cause issues, if misconfigured.

Among the operational features of the Server Configuration Profile are “Clone” and “Replace” modes of Profile Export and a “Preview” mode for Profile Import. As these names suggest, these methods can save significant time in highly automated IT environments where multiple servers are to be configured, cloned, and in the future, reconfigured for different workloads. For more information, see the [server configuration profile](#) whitepaper.

- Benefits
 - Configure all the components in a Dell EMC PowerEdge server by using a single file—iDRAC, BIOS, Users, RAID, NICs, HBAs—everything in the server
 - Import or export to multiple servers
 - Script by using various CLIs or use console tools such as OpenManage Essentials
 - The SCP can also be loaded on a USB key. This allows for error free bare-metal configuration if ToR switch is not connected.
- 14G Enhancements
 - Adds firmware deployment
 - HTTP(S) support for iDRAC with Lifecycle Controller interfaces
 - Selectable JSON or XML format
 - HTTP file streaming
 - Configure all BIOS settings from the iDRAC GUI; set or stage

Automatically sync both hardware and firmware baselines using iDRAC9

Many companies are looking for ways to not only automate the initial setup of the server, but ways to keep it that way. They are concerned about “drift” or any changes to the configuration to hardware settings or firmware version. iDRAC9 provides options to automatically control both.

- Benefits
 - The [Zero Touch](#) configuration automatically pulls server settings from a network share you set up.
 - The [Auto Update](#) feature pulls firmware bundles from network repositories (built with Repository Manager).
- 14G Enhancements
 - HTTP support
 - Complex RAID support

1.1.2 Management Made Simple

13th Generation PowerEdge servers introduced multiple ground-breaking firsts for OEM servers. Dell EMC was the first to offer a mobile solution based on NFC to directly connect to the iDRAC to allow an easier method to “set the IP address” compared to the LCD panel—but with many more features such as setting passwords, and viewing logs.

We also introduced the notion of a front panel access to the iDRAC—no need to enter the hot-aisle and sort-through cables to connect a crash cart.

Added the ability to collect logs and reports required to open a ticket with Tech Support—reducing the need to install anything on the server, and greatly reducing the time spent on the phone.

DellEMC was the first major OEM to add an alternative to Java and ActiveX when accessing the virtual console. iDRAC8 and iDRAC7 both provide the option to connect to the virtual console by using HTML5—nothing to load, no certificates to accept, and no updates to stay on top of, for better security.

Thanks to feedback from our customers, we continued to improve on all of these features.

Securely manage Dell EMC servers from your mobile device using iDRAC Quick Sync 2

New for 14th generation PowerEdge servers, the optional Quick Sync 2 module provides wireless server management when used with the OpenManage Mobile 2.0 (OMM) app for your compatible phone or tablet. Choose Quick Sync 2 module for secure server configuration, monitoring, and remediation.

Quick Sync 2 utilizes both Bluetooth Low Energy (BLE) and Wi-Fi. OMM primarily connects to Quick Sync 2 over an encrypted BLE connection. Features that require higher bandwidth use encrypted Wi-Fi. An iDRAC administrator has the option to disable Wi-Fi or disable Quick Sync 2 completely.

- Benefits
 - Capture critical server information in seconds
 - Provision key server settings in a single click
 - Send diagnostic reports direct to Dell support
- 14G Enhancements
 - IOS and Android support
 - Supported on all rack/tower PowerEdge servers
 - Embedded upsell option, not bezel-based
 - “Touch and roam” up to five meters

SupportAssist built into every PowerEdge Server

One area where Dell EMC is constantly improving is the experience when calling into Tech Support. We are constantly looking for ways to improve and streamline the process so IT admins spend less time on the phone and more time working on projects that have a positive impact on their company's bottom line. During our 12th generation iDRAC7, we introduced a tool called "Tech Support Report" which encapsulated the tool used by Tech Support to gather logs used for troubleshooting. Now, it is a part of the larger SupportAssist solution.

Typically, a "phone home" solution was something large corporations used; and required a separate console to set up. But with iDRAC9, the code required to set up a direct, secure, proxy to Dell EMC Tech Support is part of every 14th generation PowerEdge server. Now, companies of all sizes can take advantage of streamlined support case generation and resolution.

- Benefits
 - No need to download special diagnostic tools such as DSET
 - Spend less time on the phone, more time on IT service delivery
 - Predictive alerting and auto-case creation reduce the down time
 - Phone home direct to Dell Support without the need for a proxy server

New iDRAC GUI Refresh for easier navigation

- Benefits
 - Modern Web GUI, based on latest HTML5 technology for improved speed and customization
 - Navigate quicker and easier to key features
 - No Java plugins required for virtual console or media operation (although Java and ActiveX are still supported)

Simplify local server management with iDRAC Direct

When 13th generation PowerEdge servers were launched, customers were introduced to a new feature that provided quick and secure connection to the iDRAC without having to enter the "hot aisle" to plug in a crash cart. The iDRAC Direct port has the "wrench" icon near the USB port on the front of the server.

iDRAC Direct has many uses—It can be used for bare-metal configuration of the server by using an SCP on a USB key; or, can connect to a laptop directly, creating a unique private network between the iDRAC and the laptop. After connecting, the user can interact by using the GUI or any of the scripting tools such as Redfish and RACADM.

- Benefits
 - Connect a laptop via a USB cable to access the iDRAC GUI for easier "at-the-box" server troubleshooting
 - Also supports uploading configuration templates via USB key
- 14G Enhancements
 - Uses industry standard micro-B to Type-A USB cable
 - Secure, dedicated port to iDRAC (not shared with Host USB ports)

1.1.3 Security by Default

Security is a critical component for any IT department. There is tremendous focus on security at the OS and application layer. Dell EMC is also focuses on security at the hardware, BIOS and firmware levels. Here are some of the features Dell EMC provides to further secure PowerEdge Servers.

Lock down the server configuration and firmware

iDRAC9 offers a new feature that 'locks down' the hardware and firmware configuration of a server or servers. This mode can be enabled one by one by using the GUI, and CLIs such as RACADM, or as part of the Server Configuration Profile. This mode is set with root privilege, and prevents lower classes from making changes to the server. This feature can be enabled/disabled by root, and any changes made when disabled are tracked in the Lifecycle Controller Log.

- Benefits
 - Prevent configuration "drift" in your datacenter when using Dell tools.
 - Protect against malicious attacks against embedded FW when using Dell Update Package

Securely erase server storage content with System Erase

Often times, servers get 'repurposed' from one department to another. But concerns over residual data and information implies added work for the IT admin. Dell EMC servers now offer a quick and thorough process to remove existing data, users, passwords, and more with a few clicks of a mouse. Admins can choose to wipe all components, or select which items to keep. Hard drive (HDD) data is usually the primary concern. With drive sizes in the TB range, writing 0's and 1's can take weeks. For 14th generation, all drives in the servers support the industry standard "Instant Secure Erase" to help quickly remove the key that contains the information to the data location on the drive. Once the key is removed, the data is no longer accessible, and the system is ready for use in its new role.

- Benefits
 - Quickly and securely erase 14G server storage devices including HDD and SSD/NVMe drives
 - Repurpose or retire servers in minutes rather than hours or days

Factory-generated default password for iDRAC

The iDRAC password is well known and documented. However, some IT administrators forget to change this, and leave their systems to potential vulnerabilities. Beginning with 14G, all PowerEdge servers will ship with a factory-generated password, by default.

- iDRAC at 14G will ship with a factory-generated password string located on the server's information tag
- Customers can request "calvin" as the default password.
- Benefits
 - Prevents against accidental exposure of new iDRAC's on unprotected networks (DHCP is on by default in 14G)
 - Helps encourage effective password usage

Note: For security purposes, Dell EMC strongly recommends changing any initial password as part of the server deployment.

Cyber-Resilient architecture

Cyber security is increasingly top of mind for many IT managers. But most of the focus is on protecting the OS and applications from malicious attacks; little thought or planning is given to how secure the underlying server infrastructure is including the hardware and the firmware. 14G PowerEdge servers offer embedded security via a robust Cyber-Resilient Architecture which includes:

- Immutable hardware root of trust that authenticates BIOS and iDRAC firmware
- UEFI Secure Boot support with option of using customized certificates
- Rapid recovery after detection of malicious firmware and operating system attacks
- Signed SHA-256 firmware updates for all key server components
- Dynamically controlled USB ports for authenticated usage
- FIPS 140-2 Certification (iDRAC, CMC)

1.1.4 Smarter Infrastructure Management

Time is valuable. We have heard from many IT departments that "there has to be an easier way." At which point the planners and architects for iDRAC stepped back, and came up with a many new ways to 'get things done' with minimal effort required by the IT admin.

Remotely check your server's networking connections

iDRAC9 introduces a new item called "Connection View" which provides both the switch and port information to which the iDRAC9 is connected. Also, it will provide the same information for the LOMs and supported PCIe network cards.

- Benefits

- Remotely and quickly check if server LOMs or NDCs and iDRAC are connected to the correct switches and ports
- Avoid costly remote dispatch of technicians to remediate wiring errors
- No more tracing cables in the hot aisle
- Can be done via the GUI, or RACADM commands can provide information for all 14G connections
- Details
 - iDRAC parses LLDP messages from external switches to LOM/NDC ports
 - Requires LLDP enabled in networking environment

LCD panel is now an Optional Bezel

The LCD panel is old favorite used by IT teams across the planet. It is a simple way to set up IP addresses and view basic error messages. However, the demand for increase drive density has created a shift in the actual location of the LCD panel.

For 14th generation servers, the LCD panel is now an optional bezel choice—no bezel, standard bezel, or bezel with LCD. There are now many ways to configure and manage a server locally—using the bezel, iDRAC Direct, or OpenManage Mobile.

- Benefits
 - LCD is available across 14G rack and tower servers (even XD servers)
 - Consistent, optimized viewing across all rack and tower servers
 - Allows maximum storage options on all servers
 - Bezel is stateless—can be kept at ToR or on crash cart and used as needed

iDRAC Group Manager

iDRAC Group Manager is a “built-in” one-to-many console that allows all iDRAC9 servers to communicate to other iDRAC9 servers on the same physical IPv6 link local network. iDRACs will provide a global health status to the primary iDRAC9 of the Group. This feature is enabled by default when the iDRAC9 Enterprise license is selected. Other key features include:

- Benefits
 - No software to install (runs entirely on iDRACs)
 - Auto-discovers and monitors other servers on the same sub-net
 - Link and launch to other iDRAC GUIs or associated virtual consoles

iDRAC Service Module—Remote Full Power Cycle

Many customers are familiar with the OS agent known as OMSA – OpenManage Server Administrator. Since 12G, the need for OMSA has declined rapidly because iDRAC with Lifecycle Controller has taken over the tasks of discovery, configuration, updates, and monitoring.

iDRAC is OS- or hypervisor-agnostic, but there are still a few reasons to have a connection between the OS and iDRAC—such as the watchdog timer in the OS which advises iDRAC to start a crash video. In that timeframe, a smaller, lightweight replace for OMSA came around—the iDRAC Service Module (iSM) was introduced. Using only 3–5MB of running memory (compared to the 150–200 used by OMSA,) iSM provides additional solutions that OMSA cannot provide. For example, iSM can reset an iDRAC8 iDRAC9 remotely, if the iDRAC is not responsive by using the GUI or RACADM commands. Coming for iDRAC9, iSM offers additional functionality, such as:

Full Remote Power Cycle by using iSM

- Remotely drain all DC power from the server (including auxiliary power) and all its internal nodes for server troubleshooting
- Benefits
 - No need for support personnel to be present at server to pull power cables and plug back in
 - Power is restored back automatically in about 20 seconds.
 - Significantly reduces time for remotely troubleshooting hardware

In-band iDRAC Access using host OS IP using iSM

- iDRAC interfaces can be accessed by using in-band Host IP addresses (iDRAC GUI, Redfish, WS-Man, and SNMP traps)
- Benefits
 - Helps customers to get to iDRAC by using the host's in-band network without creating a separate dedicated network
 - Helps OMSA customers to migrate to iSM

1.1.5 iDRAC Security best practices

The iDRAC Security Best practice recommendations:

- iDRACs are intended to be on a separate management network; they are neither designed nor intended to be placed on or connected to the internet. Doing so could expose the connected system to security and other risks for which Dell is not responsible.
- Along with locating iDRACs on a separate management subnet, users should isolate the management subnet or vLAN with technologies such as firewalls, and limit access to the subnet or vLAN to authorized server administrators.
- Dell EMC also recommends:
 - Continually upgrading to the latest version of iDRAC firmware
 - Set the “SSL Encryption” to “256 bit or higher”
 - Set the “TLS Protocol” to “TLS 1.2 or higher”

Additional resources

- [Dell.com/support](https://dell.com/support) is focused on meeting customers' requirements with proven services and support.
- [Dell TechCenter](https://delltechcenter.com) is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware, and services.
- [DellTechCenter/iDRAC](https://delltechcenter.com/iDRAC) provides up to date links to firmware downloads, manuals, and white papers for iDRAC and CLI tools such as RACADM and Redfish.
- [DellTechCenter/OMM](https://delltechcenter.com/OMM) contains more information, white papers, and videos about the OpenManage Mobile.