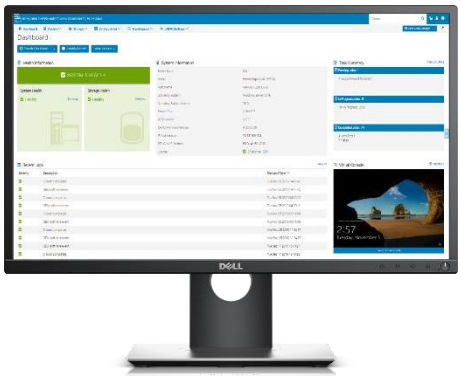
The integrated Dell Remote Access Controller 9 (iDRAC9) Solution Brief



Full Access Management of PowerEdge Servers

Modernize with Dell EMC PowerEdge portfolio

The integrated Dell Remote Access Controller (iDRAC) delivers advanced, agent-free local and remote server administration. The iDRAC provides a secure means to automate a multitude of management tasks. Given that iDRAC is embedded in every PowerEdge server, there's no additional software to install. Once iDRAC has been enabled, you will have a complete set of server management features at your fingertips.

Manage More

With iDRAC in place across the PowerEdge portfolio, the same IT administration techniques and tools can be applied throughout. This consistent management platform allows easy scaling of PowerEdge servers as your organization's infrastructure grows. With iDRAC RESTful API, iDRAC enables support for the Redfish standard and enhances it with Dell EMC extensions to optimize at-scale management. The entire OpenManage portfolio of systems management tools allows every customer to tailor an effective, affordable solution for their environment. This portfolio includes tools, consoles and integrations that leverage iDRAC to make management easy. By extending the reach to larger numbers of servers, you can be more productive and drive down organizational costs.

Intelligent Automation

The iDRAC's agent-free management puts you in control. Once a PowerEdge server is connected to power and networking, that system can be monitored and fully managed, whether you're standing in front of the server or remotely over a network. In fact, since iDRAC is agent free, you can monitor, manage, update, troubleshoot and remediate Dell EMC servers. With features like zero-touch deployment and provisioning, Group Manager, and System Lockdown, iDRAC is purpose-built to make server administration quick and easy. If you already have an existing management platform that utilizes in-band management, Dell EMC provides iDRAC Service Module, a lightweight service that can interact with both iDRAC and the host operating system to support legacy management platforms.

Secure Local and Remote Management

Whether iDRAC is used via the updated, eHTML5 web interface, command line interface, or a set of robust APIs such as the iDRAC RESTful API, security is ensured. SELinux and configurable options like HTTPS, TLS 1.2, Smart Card authentication, LDAP, and Active Directory integration provide security in your working environment. By providing secure access to remote servers, you can carry out critical management functions while maintaining the integrity and security of the data. Additional iDRAC security features include:

- The iDRAC allows you to protect your system from unwanted configuration changes via system lockdown mode.
- In addition to TLS 1.2 and 256-bit encryption strength, iDRAC Cipher Select provides further granular controls of the ciphers for communication.
- The iDRAC firmware is equipped with a default security certificate, which can be replaced automatically by a trusted certificate.

Leveraging Telemetry Data

With the new iDRAC9 Datacenter license, you can enable telemetry streaming of hardware metrics with over 180 unique monitoring metrics for advanced analytics. This new iDRAC9 data streaming feature delivers up to 10.000 times more efficiency than polling and can be easily integrated into popular analytics solutions like Splunk and ELK stack.[1] Having access to this high value data allows you to perform deep analysis of your infrastructure and increase operational efficiencies. Telemetry streaming can be used for system customization, optimization, risk management, and predictive analytics.

iDRAC9 Features and Benefits

Features	Benefits
Telemetry Streaming	Perform deep analysis of server telemetry including CPU, GPU, SFP IO, power, thermals storage, networking, memory and more. Requires iDRAC9 Datacenter license.
Thermal Manage	Customize thermal and airflow management at the rack and server level. Requires iDRAC9 Datacenter license.
Automatic Certificate Enrollment	Automatic SSL certificate enrollment and renewal of the iDRAC self-signed certificated with a trusted CA certificate. Requires iDRAC9 Datacenter license.
Zero touch deployment and provisioning	Automatically configure PowerEdge servers when they are initially connected to your network. This process uses a Server Configuration Profile to set hardware, update firmware, and install OS. Requires iDRAC9 Enterprise or Datacenter license.
Virtual Clipboard	Provides an easy to enter complex passwords and more in the HTML5 vConsole. Users can copy text/passwords to local clipboard and paste into remote console view. Requires iDRAC9 Datacenter license.
Connection View	iDRAC sends standard LLDP packets to external switches, which provides the option to discover iDRACs on the network. iDRAC sends two types of LLDP packets to the outbound network; Topology and Discovery. Also, iDRAC can also display switch and port information.
System Lockdown	Helps to prevent configuration or firmware changes to a server when using Dell tools and even vendor tools for selected network cards. Requires iDRAC Enterprise or Datacenter License.
RSA SecurID 2FA	Add the RSA SecurID client software into iDRAC to provide native support for RSA 2FA solutions. Requires Datacenter license.
DRAC RESTful API	With this API, iDRAC enables support for the Redfish standard and enhances it with Dell extensions.
Cipher Select	Cipher Select is an advanced user setting where the user can choose to block undesired ciphers negotiated by iDRAC, providing increased security.
Secured Component Verification	Secured Component Verification (SCV) is a Supply chain assurance offering that enables Dell EMC customers to verify that a PowerEdge server received by the customer matches what was manufactured in the factory.
System Erase	With proper authentication, administrators can securely erase data from local storage (HDDs, SSDs, NVMes).
iDRAC Direct	Secure front-panel USB connection to iDRAC web interface, which eliminates the need for crash carts or a trip to the hot aisle of your data center. You can use the same port to insert a USB key to upload new system profile for secure, rapid system configuration.

To view full list of features and license, see the iDRAC User Guide

[1] Based on a The Tolly Group report commissioned by Dell EMC, "iDRAC Telemetry Streaming: Evaluation of The Performance and Efficiency of Telemetry Streaming in the New iDRAC9 v4.0 Release," February 2020. Actual results may vary. Full report: https://reports.tolly.com/DocDetail.aspx?DocNumber=220101 .

Learn more about iDRAC

Contact
a Dell EMC Expert

View more resources

Join the conversation with

#HashTag

DELL EMC OpenManage