White Paper

Cyber Resilient Security in Dell EMC PowerEdge Servers

Abstract

This technical white paper covers the variety of security processes and features in the 14th and 15th generations PowerEdge Servers, featuring iDRAC9.

March 2021

Revisions

Date	Description
January 2018	Initial release
November 2020	First Revision
March 2021	Updated to include new features

Acknowledgments

Authors: Vandana Mallempati, Craig Phelps, Manoj Malhotra, Doug Iler

Table of contents

Revisions....2
Acknowledgments....2
Executive summary....5
1 Introduction....6
2 The Path to a Secure Server Infrastructure....7
2.1 Security Development Lifecycle....7
2.2 Cyber Resilient Architecture....8
2.3 Current Threats....9
3 Protect....10
3.1 Cryptographically verified Trusted Booting....10
3.1.1 Silicon based Root of Trust....10
3.1.2 BIOS Live Scanning....12
3.1.3 UEFI Secure Boot Customization DHCP—current and new configuration options....12
3.1.4 Trusted Platform Module Support....13
3.1.5 Security Certifications....13
3.2 User Access Security....13
3.2.1 RSA SecurID Multi Factor Authentication....14
3.2.2 Simplified Two Factor Authentication (2FA)....14
3.2.3 SELinux framework....15
3.2.4 Least Required Privilege....15
3.2.5 Automatic Certificate Enrollment and Renewal....15
3.2.6 Factory Generated Default Password....16
3.2.7 Server System Lockdown....16
3.2.8 Domain Isolation....17
3.3 Signed Firmware Updates....17
3.4 Encrypted Data Storage....17
3.4.1 iDRAC Credential Vault....18
3.4.2 Local Key Managements (LKM)....18
3.4.3 Secure Enterprise Key Manager (SEKM)....19
3.5 Hardware Security....20
3.5.1 Chassis Intrusion Alert....20
3.5.2 Dynamic USB Port Management....20
3.5.3 iDRAC Direct....20

3.5.4 iDRAC Connection View with Geolocation 20
3.6 Supply Chain Integrity and Security 21
3.6.1 Hardware and Software Integrity 21
3.6.2 Physical Security 21
3.6.3 Dell Technologies Secured Component Verification (SCV) for PowerEdge 22
4 Detect 23
4.1 Comprehensive Monitoring using iDRAC 23
4.1.1 Lifecycle Log 23
4.1.2 Alerts 24
4.2 Drift Detection 25
5 Recover 26
5.1 Rapid Response to New Vulnerabilities 26
5.2 BIOS and operating system Recovery 26
5.3 Firmware Rollback 27
5.4 Restoring Server Configuration after Hardware Servicing 27
5.4.1 Parts Replacement 28
5.4.2 Easy Restore (for System Board Replacement) 28
5.5 System Erase 29
5.6 iDRAC9 Cipher Suite 30
5.7 Commercial National Security Algorithm (CNSA) Support 30
5.8 Full Power Cycle 30
6 Conclusion 31
A Technical support and resources 32

Executive summary

The Dell Technologies approach to security is intrinsic in nature. Security is integrated, not bolted-on after the fact, and it is integrated into every step of the Dell EMC Secure Development Lifecycle. The PowerEdge team continuously evolves the security controls, features, and solutions to meet the ever-growing threat landscape. A key security foundation is Silicon Root of Trust.

This paper details the security features built into in the PowerEdge Cyber Resilient Platform, many enabled by the integrated Dell Remote Access Controller (iDRAC9). Many new security features have been added, which span from access control to data encryption to supply chain assurance. These features include:

- Live BIOS scanning
- UEFI Secure Boot Customization
- RSA SecurID Multi Factor Authentication
- Secure Enterprise Key Management (SEKM)
- Secured Component Verification (SCV)
- Enhanced System Erase
- Automatic Certificate Enrollment and Renewal
- Cipher Select
- Commercial National Security Algorithm (CNSA) support

All features make extensive use of intelligence and automation to help IT admins stay ahead of the threat curve.

1 Introduction

As the threat landscape evolves, IT and security professionals struggle to manage the risks to their data and resources. Data is being used across many devices, on premise, and in the cloud, and high impact data breaches continue to mount. Historically security emphasis has been placed on the operating system, on applications, and on firewalls. Another network infrastructure concern is Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). IDS analyses the network traffic for signatures that match known cyberattacks. IPS stops the packets from being delivered. These areas continue to be important areas to address. Threats to hardware continue to rise, which requires secure hardware-based infrastructure for firmware, BIOS, iDRAC, and overall supply chain assurance.

The Dell Technologies 2020 Digital Transformation Index found that data privacy and cybersecurity concerns are the Number One barrier to digital transformation.[1] Also, 63% of companies experienced a data compromise due to an exploited vulnerability[2].

As servers become more critical in a software-defined data center architecture, server security becomes the foundation of overall enterprise security. Servers must emphasize security at both the hardware and firmware level by leveraging an immutable Root of Trust. The Root of Trust is used to verify subsequent operations within the server. This verification establishes a chain of trust that extends throughout the server life cycle, from deployment through maintenance to decommissioning.

The 14th and 15th generations of Dell EMC PowerEdge servers with iDRAC9 deliver this chain of trust. This chain of trust, along with security controls and comprehensive management tools provides robust layers of security across hardware and firmware. The result is a Cyber Resilient Architecture that extends across every aspect of the server. Cyber Resilient Architecture includes the embedded server firmware, the data stored in the system, the operating system, peripheral devices, and the management operations within it. Organizations can build a process to protect their valuable server infrastructure and the data within it. They can detect any anomalies, breaches, unauthorized operations, and recover from unintended or malicious events.

[1] Dell Technologies 2020 Digital Transformation Index

[2] Match Present-Day Security threats with BIOS-Level Control. A Forrester Consulting Thought Leadership Paper commissioned by Dell, 2019

2 The Path to a Secure Server Infrastructure

Dell EMC PowerEdge servers have featured robust security for several generations, including the innovation of using silicon-based data security. Dell EMC PowerEdge servers extended silicon-based security to authenticate BIOS andfirmware with a cryptographic Root of Trust during server boot process. Dell EMC product team prioritizes features in PowerEdge servers to limit security threats faced in modern IT environments.

- **Protect:** Protect server during every aspect of life cycle, including BIOS, firmware, data, and physical hardware.
- **Detect:** Detect malicious cyberattacks and unapproved changes; engage IT administrators proactively.
- **Recover:** Recover BIOS, firmware, and operating system to a known good state; securely retire or repurpose servers.

Dell EMC PowerEdge servers conform to key industry standards on cryptography and security and performs on-going tracking and management of new vulnerabilities.

Dell EMC uses the Security Development Lifecycle process in every aspect of development, procurement, manufacturing, shipping, and support, resulting in a Cyber Resilient Architecture.

2.1 Security Development Lifecycle

Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development. The Security Development Lifecycle (SDL) model is a key part of the overall server design process. This design process encompasses a view of security needs throughout the entire server life cycle, as bulleted below and as shown in Figure 1:

- Features are conceived, designed, prototyped, implemented, set into production, deployed, and maintained, with security as a key priority.
- Server firmware is designed to obstruct, oppose, and counter the injection of malicious code during all phases of the product development life cycle.
    - Threat modeling and penetration testing coverage during the design process
    - Secure coding practices are applied at each stage of firmware development.
- For critical technologies, external audits supplement the internal SDL process to ensure that firmware adheres to known security best practices.
- On-going testing and evaluation of new potential vulnerabilities using the latest security assessment tools

- Rapid response to critical Common Vulnerabilities and Exposures (CVEs) including recommended remediation measures as needed.

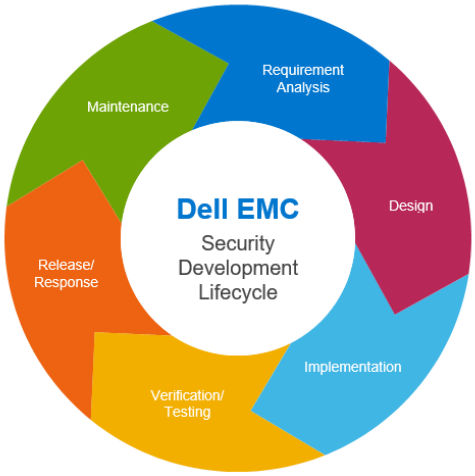


Figure 1: Security Development Lifecycle of Dell EMC

2.2 Cyber Resilient Architecture

Dell EMC servers feature an enhanced Cyber Resilient Architecture that provides a hardened server design to Protect, Detect, and Recover from cyberattacks. Some of the key aspects of this architecture are:

Effective Protection from attacks

- Silicon-based Root of Trust
- Secure Boot
- Signed Firmware Updates
- Dynamic System Lockdown
- Hard drive encryption and enterprise key management

Reliable Detection of attacks

- Configuration and Firmware Drift Detection
- Persistent Event Logging
- Audit Logging and Alerts
- Chassis Intrusion Detection

Rapid Recovery with little to no business interruption

- Automated BIOS recovery
- Rapid operating system Recovery
- Firmware Rollback
- Rapid System Erase

2.3 Current Threats

There are many threat vectors in the ever-changing IT landscape. Table 1 summarizes the Dell EMC approach to managing critical backend threats.

Server Platform Layers		
Security layer	**Threat vector**	**Dell EMC solution**
Physical server	Server/component tampering	Secured Component Verification (SCV), Chassis Intrusion Detection
Firmware and software	Firmware corruption, malware injection	Silicon-based Root of Trust; Intel Boot Guard; AMD Secure Root of Trust; UEFI Secure Boot Customization Cryptographically signed and validated firmware;
	Software	CVE reporting; Patching as required
Attestation trust features	Server identity spoofing	TPM, TXT, Chain of trust
Server management	Rogue configuration and updates, unauthorized open-port attacks	iDRAC9; Remote attestation

Server Environment Layers		
Security layer	**Threat vector**	**Dell EMC solution**
Data	Data breach	Self-Encrypting Drives (SED) – FIPS or Opal/TCG Secure Enterprise Key Management ISE – only (Instant Secure Erase) drives Secure User Authentication
Supply Chain Integrity	Counterfeit components Malware Threats	ISO9001 certification for all global server manufacturing sites; Secured ComponentVerification; proof of possession Security measures implemented as part of Secure Development Lifecycle (SDL) process
Supply Chain Security	Physical security in Manufacturing sites Theft and tempering during transport	Transported Asset Protection Association(TAPA) facility security requirements Customs-Trade Partnership Against Terrorism(C-TPAT); SCV

3 Protect

The “protect” function is a key component of the NIST Cybersecurity Framework and serves to guard against cybersecurity attacks. This function consists of several categories including access control, data security, maintenance, and protective technology. The key underlying philosophy is that infrastructure assets must provide robust protection against unauthorized access to resources and data. This philosophy includes protecting against unauthorized modifications of critical components such as BIOS and firmware. The platform meets the current recommendations in NIST SP 800-193.

The Cyber Resilient Architecture in PowerEdge servers offers a high level of platform protection that includes the following capabilities:

- Cryptographically verified Trusted Booting
- User Access Security
- Signed Firmware Updates
- Encrypted Data Storage
- Physical Security
- Supply Chain Integrity and Security

3.1 Cryptographically verified Trusted Booting

One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an operating system or updating firmware.

PowerEdge servers have used silicon-based security for several generations for features such as iDRAC Credential Vault, an encrypted secure memory in iDRAC for storing sensitive data. The boot process is verified using a silicon-based Root of\Trust to meet the following recommendations:

- NIST SP 800-147B “BIOS Protection Guidelines for Servers”
- NIST SP 800-155 “BIOS Integrity Measurement Guidelines”

3.1.1 Silicon based Root of Trust

PowerEdge servers use an immutable, silicon-based Root of Trust to cryptographically attest to the integrity of BIOS and iDRAC9 firmware. This Root of Trust is based on one time programmable, read-only public keys that provide protection against malware tampering. The BIOS boot process leverages Intel Boot Guard technology or AMD Root of Trust technology. This technology verifies the digital signature of the cryptographic hash of the boot image matches to the signature stored in silicon by Dell EMC in factory. A verification failure results in a shutdown of the server, and user notification in the Lifecycle Controller Log. Then, the user can initiate the BIOS recovery process. If Boot Guard validates successfully, the rest of the BIOS modules are validated by using a chain of trust procedure. Then, control is handed off to the operating system or hypervisor.

In addition to Boot Guard, iDRAC9 4.10.10.10 or higher provides a Root of Trust mechanism which verifies the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time, on demand, or at user-scheduled intervals.

Next is a detailed review of the chain of trust. Each BIOS module contains a hash of the next module in the chain. The key modules in BIOS are:

- Initial Boot Block (IBB)
- Security (SEC)
- Pre-EFI Initialization (PEI)
- Memory Reference Code (MRC)
- Driver Execution Environment (DXE)
- Boot Device Selection (BDS)

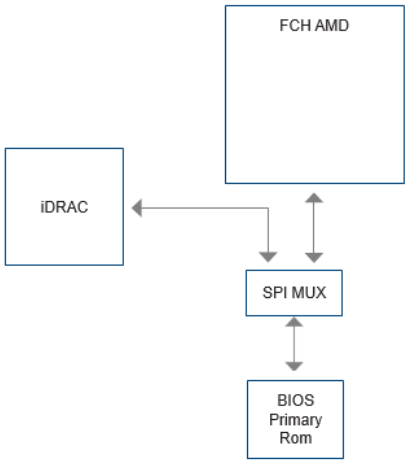
If Intel Boot Guard authenticates the Initial Boot Block (IBB), then the IBB validates SEC+PEI before handing control to it. SEC+PEI then validates PEI+MRC which further validates the DXE+BDS modules. Next, control is handed over to UEFI Secure Boot as explained in the next section.

Similarly, for Dell EMC PowerEdge AMD EPYC based servers, AMD Secure Root of Trust technology ensures that servers boot only from trusted firmware images. AMD Secure Run Technology is designed to encrypt main memory, keeping it private from malicious intruders having access to the hardware. No application modifications are required to use this feature, and the security processor never exposes the encryption keys outside of the processor.

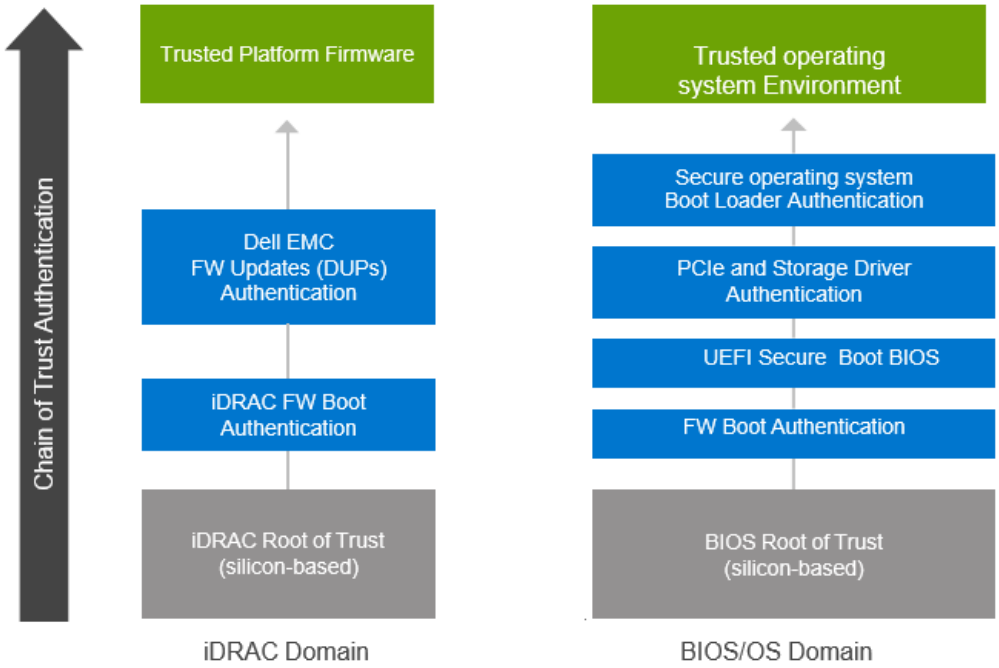
iDRAC takes on the role of hardware-based security technologies and accesses the primary BIOS ROM through SPI. iDRAC, along with the AMD fusion controller hub (FCH) performs the Root of Trust process.

Under the following conditions, iDRAC9 recovers the BIOS.

- BIOS integrity check failed.
- BIOS self-check failed.
- Using RACADM command - **racadm recover BIOS.Setup.1-1**



The iDRAC boot process uses its own independent silicon-based Root of Trust that verifies the iDRAC firmware image. The iDRAC Root of Trust also provides a critical trust anchor for authenticating the signatures of Dell EMC firmware update packages (DUPs).



3.1.2 BIOS Live Scanning

BIOS live scanning verifies the integrity and authenticity of the BIOS image in the primary ROM when the host is powered on. BIOS Live Scanning does not include the POST process. This AMD only feature and is available only with iDRAC9 4.10.10.10 or higher with the Datacenter license. This feature requires administrator privileges, or operator privileges with “Execute Debug Commands” debug privilege. This scan can be scheduled through the iDRAC UI, RACADM, and Redfish interfaces.

3.1.3 UEFI Secure Boot Customization DHCP—current and new configuration options

PowerEdge servers support Unified Extensible Firmware Interface (UEFI) Secure Boot. UEFI Secure Boot checks the cryptographic signatures of UEFI drivers and code that is loaded before the operating system. Secure Boot represents an industry-wide standard for security in the preboot environment. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability.

When enabled, UEFI Secure Boot prevents unsigned (untrusted) UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. Secure Boot must be disabled to load unsigned device drivers.

In addition, 14th and 15th generation PowerEdge servers offer customers the unique flexibility of using a customized boot loader certificate that is not signed by Microsoft. This feature is primarily for Linux administrators that want to sign their own operating system boot loaders. Custom certificates can be uploaded using the preferred iDRAC API to authenticate a customer specific operating system boot loader. The NSA cites this PowerEdge UEFI customization method for mitigating against Grub2 vulnerabilities in servers.

3.1.4 Trusted Platform Module Support

PowerEdge servers support three versions of the Trusted Platform Module (TPM):

- TPM 1.2 FIPS + Common Criteria+ TCG certified (Nuvoton)
- TPM 2.0 FIPS + Common Criteria+ TCG certified (Nuvoton)
- TPM 2.0 China (NationZ)

TPM can be used to perform public key cryptographic functions, compute hash functions, generate, manage, and securely store keys, and do attestation. Intel Trusted Execution Technology (TXT) functionality and Microsoft Platform Assurance feature in Windows Server 2016 are also supported. TPM can also be used to enable the BitLocker™ hard drive encryption feature in Windows Server 2012 and 2016.

Attestation and remote attestation solutions can use the TPM to take measurements at boot time of a server hardware, hypervisor, BIOS, and operating system. These measurements are compared in a cryptographically secure manner against base measurements that are stored in TPM. If they are not identical, the server identity may have been compromised and system administrators can disable and disconnect the server either locally or remotely.

Servers can be ordered with or without TPM, but for many operating systems and other security provisions it is becoming a standard.

TPM is enabled through a BIOS option. It is a Plug-In Module solution, the planar has a connector for this plug-in module.

3.1.5 Security Certifications

Dell EMC has received certifications for standards such as NIST FIPS 140-2 and Common Criteria EAL-4. These certifications are for complying with US Department of Defense (DoD) and other governmental requirements. The following certifications have been received for PowerEdge servers:

- Server platform: Common Criteria EAL4+ certified with Red Hat Enterprise Linux and are also being used to support the partner CC certifications.
- iDRAC and CMC FIPS 140-2 Level 1 certification
- OpenManage Enterprise – Modular is EAL2+ certified.
- FIPS 140-2 and Common Criteria certification for TPM 1.2 & 2.0

3.2 User Access Security

Ensuring proper authentication and authorization is a key requirement of any modern access control policy. The primary access interfaces for PowerEdge servers are using the APIs, CLIs, or the UI of the embedded iDRAC. The preferred APIs and CLIs for automating server management are:

- iDRAC Restful API with Redfish
- RACADM CLI
- SELinux

Each of these interfaces provides for robust credentials like username and password security, transported over an encrypted connection, such as HTTPS. SSH authenticates a user by using a matching set of cryptographic keys, eliminating the use of less than secure passwords. Older protocols, such as IPMI, are

supported but are not recommended for new deployments due to the various security issues uncovered in recent years. Dell EMC recommends IPMI users to evaluate and transition to iDRAC Restful API with Redfish.

TLS/SSL certificates can be uploaded to iDRAC to authenticate web browser sessions. Three options:

- **Dell EMC Self-Signed TLS/SSL Certificate**: The certificate is autogenerated and self-signed by iDRAC.
  - Advantage: No must maintain a separate Certification Authority (see X.509/IETF PKIX standard).
- **Custom Signed TLS/SSL Certificate:** The certificate is autogenerated and signed with a private key that has already been uploaded to iDRAC.
  - Advantage: Single trusted CA for all iDRACs. It is possible that the in house Certificate Authority (CA) is already trusted on the management stations.
- **CA Signed TLS/SSL Certificate:** A certificate signing request (CSR) generated and submitted to the in house CA or by a third party CA such as VeriSign, Thawte, and Go Daddy.
  - Advantages: Can use a commercial Certification Authority (see X.509/IETF PKIX standards). Single trusted CA for all the iDRACs. If a commercial CA is used, it is likely to be already trusted on the management stations.

iDRAC9 enables integration with Active Directory and LDAP by leveraging an existing authentication and authorization schemas that already provide secure access to PowerEdge servers. It also supports Role Based Access Control (RBAC) to grant the proper level of access. Roles include Administrator, Operator, or Read Only and match the role of the person in server operations. It is highly recommended to use RBAC in this manner and not grant the highest level (that is Administrator) to all users.

iDRAC9 also provides additional ways to protect against unauthorized access including IP blocking and filtering. IP blocking dynamically determines when excessive login failures occur from an IP address and blocks the address from logging in for a preselected time span. IP filtering limits the IP address range of the clients accessing iDRAC. It compares the IP address of an incoming login against the specified range and allows iDRAC access only source IP address is within the range. All other login requests are denied.

Multi Factor authentication (MFA) is used more widely today because of the growing vulnerability of single-factor authentication schemes that are based on username and password. iDRAC9 allows use of smart cards for remote user interface access and support RSA tokens. In both cases, the multiple factors include the are the physical presence of device or card and the associated PIN.

3.2.1 RSA SecurID Multi Factor Authentication

RSA SecurID can be used as another means of authenticating a user on a system. The iDRAC9 starts to support RSA SecurID with the Datacenter license and firmware 4.40.00.00 as another two-factor authentication method. For more information about RSA SecurID, see the white paper on www.dell.com/support/idrac.

3.2.2 Simplified Two Factor Authentication (2FA)

Another authentication method that is offered is Easy 2FA, which sends a randomly generated token to a user email when logging into iDRAC9.

3.2.3 SELinux framework

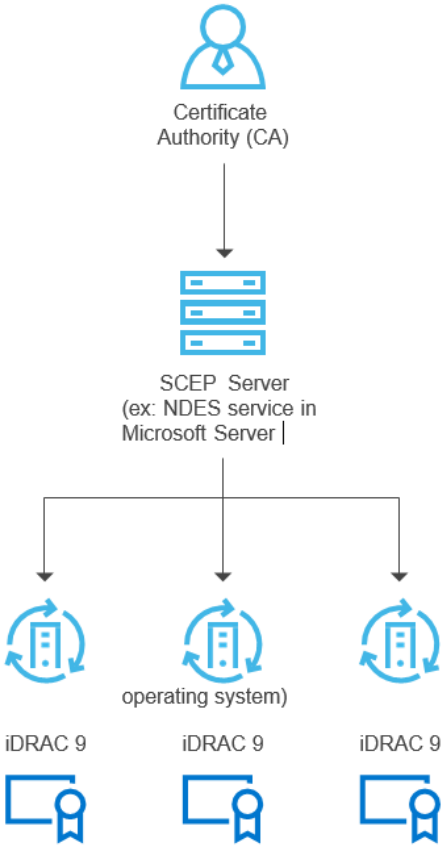
SELinux operates at the core kernel level on the iDRAC and does not need any input or configuration from users. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to customers enrolled in this new feature. In future release of iDRAC, these logs are available in the Lifecycle Controller Logs.

3.2.4 Least Required Privilege

SELinux operates at the core kernel level on the iDRAC and does not need any input or configuration from users. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to customers enrolled in this new feature. In future release of iDRAC, these logs are available in the Lifecycle Controller Logs.

3.2.5 Automatic Certificate Enrollment and Renewal

iDRAC9 v4.0 has added a client for Simple Certificate Enrollment Protocol (SCEP) support and requires Datacenter License. SCEP is a protocol standard that is used for managing certificates to large numbers of network devices using an automatic enrollment process. The iDRAC can now integrate with SCEP-compatible servers like the Microsoft Server NDES service to maintain SSL/TLS Certificates automatically. This feature can be used to enroll and refresh a soon to be expired web server certificate. This process can be done on a one-to-one basis in the iDRAC user interface, using Server Configuration Profile, or scripted using tools such as RACADM.



3.2.6 Factory Generated Default Password

By default, all 14G PowerEdge servers ship with a unique, factory-generated iDRAC password to provide additional security. This password is generated at the factory and is printed on the pull out Information Tag. This tag is on the front of the chassis, next to the server asset label. Users who choose this default option must note this password and use it to log in to iDRAC for the first time. For security purposes, Dell EMC strongly recommends changing the default password.

3.2.7 Server System Lockdown

iDRAC9 offers a feature that 'locks down' the hardware and firmware configuration of a server or servers and requires Enterprise or Datacenter license. This mode can be enabled by using the user interface, CLIs such as RACADM, or as part of the Server Configuration Profile. Users with administrative privileges can set System Lockdown mode which prevents users with lesser privileges from making changes to the server. IT administrators with 'root' access can enable and disable this feature.

Any changes made when System Lockdown is disabled are tracked in the Lifecycle Controller Log. Users can prevent configuration drift by enabling Lockdown Mode. System lockdown helps protect against malicious attacks against embedded firmware when using Dell EMC Update Packages. Lockdown mode can be enabled dynamically, without requiring a system reboot. iDRAC9 v4.40 introduces enhancements System Lockdown which extends beyond the Dell Update Package (DUP) to select network cards. Enhanced Lockdown for NICs only includes firmware lockdown to prevent firmware updates. Configuration (x-UEFI)

lockdown is not supported. These actions depend on the third party devices that are detected as part of the iDRAC discovery process.

3.2.8 Domain Isolation

14th and 15th generation PowerEdge servers provide additional security using Domain Isolation, an important feature for multitenant hosting environments. In order to secure the server hardware configuration, hosting providers may want to block any reconfiguration by tenants. Domain isolation ensures that management applications in the host operating system have no access to the out-of-band iDRAC. This isolation includes Intel chipset functions, such as Management Engine (ME) or Innovation Engine (IE).

3.3 Signed Firmware Updates

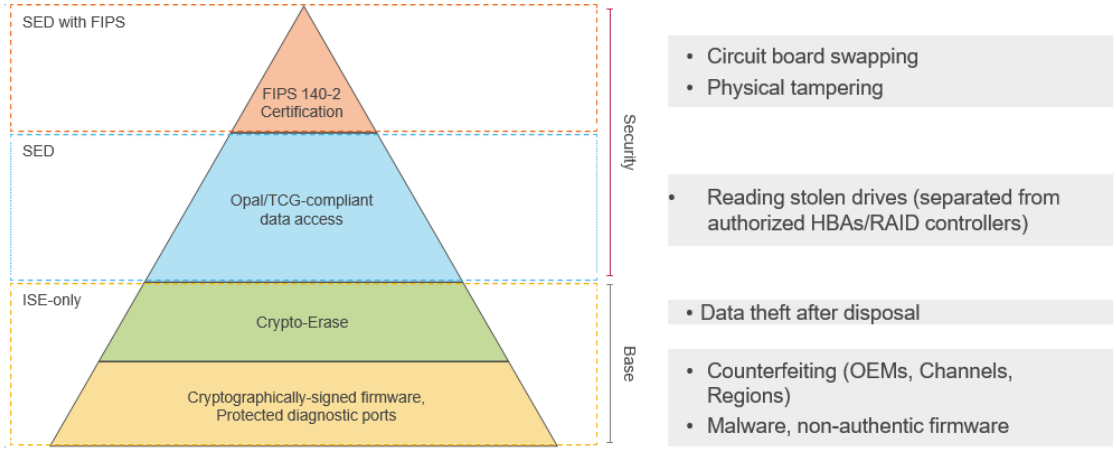
PowerEdge servers have used digital signatures on firmware updates for several generations to assure that only authentic firmware is running on the server platform. Dell EMC digitally signs all firmware packages using SHA-256 hashing with 2048-bit RSA encryption for the signature for all key server components. These components include firmware for iDRAC, BIOS, PowerEdge RAID Controller (PERC), I/O adapters and LOMs, PSUs, storage drives, CPLD, and backplane controllers. iDRAC scans firmware updates and compares their signatures to what is expected using the silicon-based Root of Trust. Any firmware package that fails validation is aborted and an error message is logged into the Lifecycle Log (LCL) to alert IT administrators.

Enhanced firmware authentication is embedded within many third-party devices which provide signature validation using their own Root of Trust mechanisms. This authentication prevents the use of a compromised third-party tool to load malicious firmware which bypasses the signed update package. Many of the third-party PCIe and storage devices that are shipped with PowerEdge servers use a hardware Root of Trust to validate their respective firmware updates.

If device firmware is suspected of malicious tampering, IT administrators can roll back the firmware images to a prior trusted version stored in iDRAC. iDRAC keeps two versions of device firmware on the server – the existing production version (“N”) and a prior trusted version (“N-1”).

3.4 Encrypted Data Storage

Encrypted data storage is built on the foundation of Signed Firmware Updates. The following diagram shows the levels. The following sections discuss these levels.



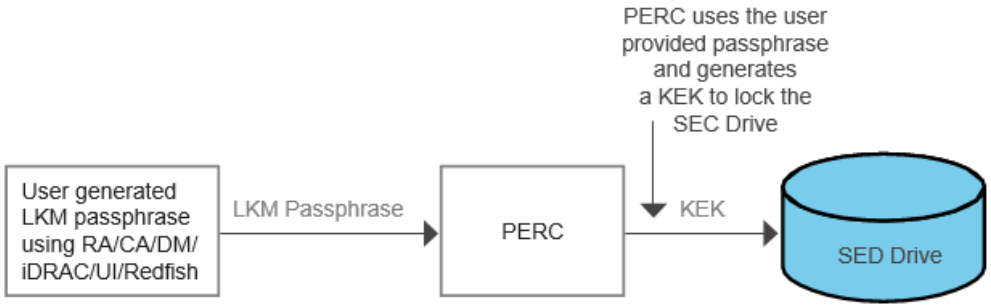
3.4.1 iDRAC Credential Vault

The iDRAC service processor provides a secure storage memory that protects various sensitive data such as iDRAC user credentials and private keys for self-signed SSL certificates. The Credential Vault is another example of silicon-based security. The memory is encrypted with a unique immutable root key that is programmed into each iDRAC chip at the time of manufacture. This check protects against physical attacks where the attacker unsolders the chip to gain access to the data.

3.4.2 Local Key Managements (LKM)

Current PowerEdge servers provide users the ability to secure SED drives connected to a PowerEdge RAID Controller (PERC) controller using Local Key Management.

LKM helps ensure that user data protection is safe, even when a drive is stolen. The SED must be locked with a separate key so that it does not decrypt user data unless that key is provided. This key is the Key Encryption Key (KEK). A user sets a key ID or passphrase on the PERC controller to which the SED is connected. The PERC controller generates a KEK using the passphrase and uses it to lock the SED. When the drive is powered on, it comes up as a locked SED. The drive encrypts and decrypts user data only when the KEK is provided to unlock it. The PERC provides the KEK to the drive to unlock it. If the drive is stolen, it comes up as “Locked.” the user data is protected. It is termed Local as the passphrase and the KEK are stored locally on the PERC. The following diagram shows the LKM solution.

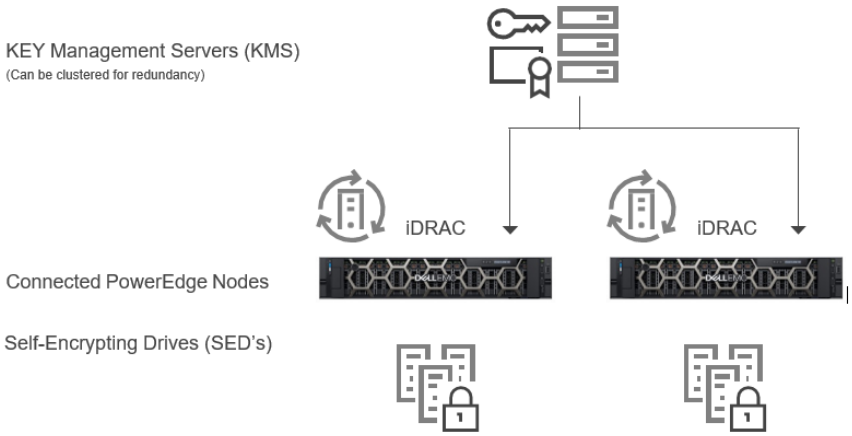


3.4.3 Secure Enterprise Key Manager (SEKM)

OpenManage SEKM delivers a central key management solution to manage data-at-rest across the organization. SEKM uses an external Key Management Server (KMS) to manage keys that iDRAC uses to lock and unlock storage devices.

The advantages of using SEKM over Local key Management (LKM) are:

- SEKM protects “theft of a server” since the keys are not stored on the server and are stored externally. Only authenticated iDRACs can retrieve the key from the external server.
- Centralized and scalable key management for encrypted devices with high availability.
- Supports industry standard KMIP protocol, which enables the use of other KMIP compatible devices.
- Protects data at rest when drives or entire server are compromised.
- On-drive encryption performance scales with drive count.



3.5 Hardware Security

Hardware security is an integral part of any comprehensive security solution. Some customers want to limit access to ports of entry, such as USB. A server chassis need not be opened in general after it has been put into production, except for a part failure. Customers want to track and log any hardware security activities. The goal is to alert on any unwanted physical intrusion.

3.5.1 Chassis Intrusion Alert

PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available. Sensors on the chassis detect when anyone opens or tampers with the chassis, even during transit. A server that has been opened while in transit generates an entry in the iDRAC Lifecycle log after power is supplied.

3.5.2 Dynamic USB Port Management

For more security, all USB ports can be programmatically disabled. There is also an option to disable only the USB ports on the front of the server. For example, USB ports can be disabled for production use and then temporarily enabled to grant access to a crash cart for debugging purposes.

3.5.3 iDRAC Direct

iDRAC Direct is a special USB port that is hardwired to the iDRAC service processor. iDRAC Direct uses one cable to connect to a data center crash cart. It allows a user to attach a standard Micro-AB USB cable to this port and the other end (Type A) to a laptop. A standard web browser can then access iDRAC UI for extensive debugging and management of the server. If iDRAC Enterprise or Datacenter license is installed, the user can also access the operating system using the iDRAC Virtual Console feature.

iDRAC Direct requires valid credentials and works as a secure crash cart with the advantage of extensive hardware management and service diagnostics. For added physical security in remote locations, host USB ports and VGA outputs can be disabled, while iDRAC Direct remains functional.

3.5.4 iDRAC Connection View with Geolocation

Connection View provides the ability for iDRAC to report the external switches and ports that are connected to Server I/O. It is a feature on select networking devices and requires Link Layer Discovery Protocol (LLDP) be enabled on the switches connected.

Some of the benefits of Connection View are:

- Remotely and quickly check if server I/O modules (LOMs, NDCs, and add-in PCIe cards) are connected to the correct switches and ports
- Avoid costly remote dispatch of technicians to remediate wiring errors
- No more tracing of cables in the server room hot aisles
- Can be done using the UI, or RACADM commands can provide information for all 14G connections

Beyond the obvious time and monetary savings, there is an additional benefit Connection View provides – providing real time geolocation of a physical server or virtual machine. IT admins can iDRAC Connection View to pinpoint which switch and port a server is connected to. This detail helps in securing servers from being connected to networks and devices that do not comply with corporate security guidelines or best practices.

Connection View validates the location of the server indirectly by reporting details about the switch it is connected to. The switch identity provides geolocation to assure that the server is not a “rogue server” in a nonauthorized site, providing another layer of physical security. Geolocation also provides validation that an application or VM has not “crossed” country or region borders, and that it is running in an approved, secure environment.

3.6 Supply Chain Integrity and Security

Supply Chain Integrity focuses on two key challenges:

- Maintaining **Hardware** Integrity: Ensuring that there is no product tampering or insertion of counterfeit components before shipping product to customers.
- Maintaining **Software** Integrity: Ensuring that no malware gets inserted in firmware or device drivers before shipping product to customers and preventing any coding vulnerabilities.

Dell EMC defines supply chain security as “the practice and application of prevention and detection control measures that protect physical assets, inventory, information, intellectual property, and people.” These security measures provide supply chain assurance and integrity by reducing opportunities for malicious or negligent introduction of malware and counterfeit components into the supply chain.

3.6.1 Hardware and Software Integrity

Dell EMC is focused on ensuring that quality control processes are in place to help minimize the opportunity for counterfeit components to infiltrate the supply chain. The controls Dell EMC has in place span supplier selection, sourcing, production processes, and governance through auditing and testing. The “product introduction process” verifies that all materials used during all build stages are sourced from the approved vendor list and match the bill of materials. Material inspections during production help identify components that are mismarked, deviate from normal performance parameters, or contain an incorrect electronic identifier.

Parts are procured directly from the Original Design Manufacturer (ODM) or Original Component Manufacturer (OCM) when possible. The material inspection that occurs during the product introduction process provides multiple opportunities to identify counterfeit or corrupted components that may have entered the supply chain.

Dell EMC maintains ISO 9001 certification for all global manufacturing sites. Strict adherence to these processes and controls helps minimize the risk of counterfeit components being embedded among the Dell EMC products. This standard also protects against malware getting inserted into firmware or device drivers. These measures are implemented as part of Software Development Lifecycle (SDL) process.

3.6.2 Physical Security

Dell EMC has several long-standing, key practices that establish and maintain security in manufacturing facilities and logistical networks. Factories where Dell EMC products are built must meet specified Transported Asset Protection Association (TAPA) facility security requirements. These requirements include the use of monitored closed circuit cameras in key areas, access controls, and continuously guarded entries and exits. Protective measures have also been put in place to guard products against theft and tampering during transport as part of an industry-leading logistics program. This program provides a continuously staffed command center to monitor select inbound and outbound shipments across the globe. This process ensures that shipments make it from one destination to another securely and without disruption.

Dell EMC is engaged in several voluntary supply chain security programs and initiatives. One such initiative is the Customs-Trade Partnership Against Terrorism (C-TPAT), introduced by the United States government after the September 11 attack. This initiative helps reduce the potential for terrorism through strengthened border and supply chain security measures. As part of this initiative, the U.S. Customs and Border Protection agency asks participating members to ensure the integrity of their security practices. They also ask members to communicate their security guidelines to their business partners within the supply chain. Dell EMC has been an active participant since 2002 and maintains the highest membership status.

3.6.3 Dell Technologies Secured Component Verification (SCV) for PowerEdge

In 2020, Dell Technologies introduced Secured Component Verification (SCV) for PowerEdge. SCV is a supply chain assurance offering that verifies that a PowerEdge server a customer receives matches the factory configuration. The factory generates a certificate that contains unique component IDs for a specific server. This cryptographically secure certificate is stored in iDRAC. The customer uses the SCV application to collect the current system inventory, including unique component IDs, and validates it against the inventory in the SCV certificate.

The SCV application generates a report which verifies which components match, and which components are a mismatch from what was installed in the factory. It also verifies the certificate and Chain of Trust along with the Proof of Possession of the SCV Private key for iDRAC. Current implementation supports direct ship customers and does not include Value Added Reseller (VAR) or Part Replacement scenarios.

4 Detect

It is critical to have a detection capability that provides complete visibility into the configuration, health status, and change events within a server system. This visibility must also detect malicious or other changes to BIOS, firmware, and Option ROMs within the boot and operating system runtime process. Proactive polling must be coupled with the ability to send alerts for any events within the system. Logs must provide complete information about access and changes to the server. Most importantly, the server must extend these capabilities to all components.

4.1 Comprehensive Monitoring using iDRAC

Rather than depending upon operating system agents to communicate with managed resources in a server, iDRAC employs a direct side-band path to each device. Dell EMC uses industry standard protocols such as MCTP, NC-SI, and NVMe- MI. These protocols communicate to peripheral devices such as PERC RAID controllers, Ethernet NICs, Fibre Channel HBAs, SAS HBAs, and NVMe drives. This architecture is the result of lengthy, multi-year partnerships with industry-leading vendors to provide agent-free device management in PowerEdge servers. Configuration and firmware update operations also leverage the powerful UEFI and HII features that Dell EMC and partners support.

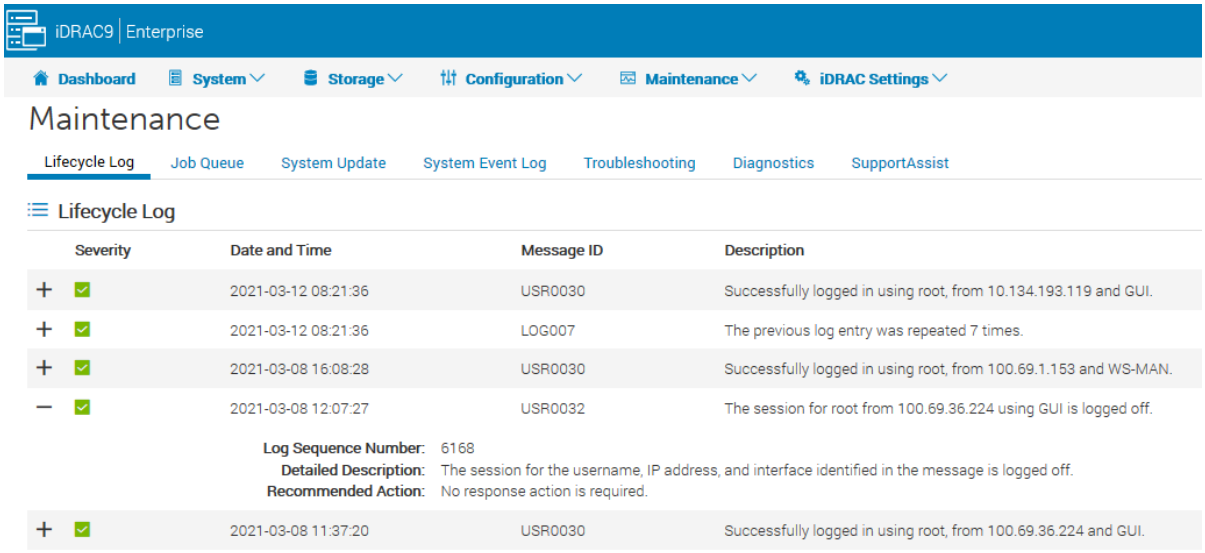
With this capability, iDRAC can monitor the system for configuration events, intrusion events (such as chassis intrusion detection mentioned earlier in this paper), and health changes. Configuration events are tied directly to the identity of the user that initiated the change, whether it is from a UI, API, or console.

4.1.1 Lifecycle Log

Lifecycle log is a collection of events that occur in a server over a period. Lifecycle log provides a description of events with timestamps, severity, user ID or source, and recommended actions. This technical information aids in security tracking and other hardware alerts.

The following are the various types of information that is recorded in the Lifecycle Log (LCL) are:

- Configuration Changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events



4.1.2 Alerts

iDRAC provides the capability to configure different event alerts and actions to be performed when a Lifecycle Logs event occurs. When an event is generated, it is forwarded to the configured destinations by using the selected alert type mechanisms. Users can enable or disable alerts through the iDRAC web interface, RACADM, or with iDRAC settings utility.

iDRAC supports different types of alerts such as:

- Email or IPMI alert
- SNMP trap
- Operating system and Remote System logs
- Redfish event

Alerts are categorized by severity – Critical, Warning, or Informational. Following filters can be applied to alerts:

- System health – For Example, Temperature, Voltage, or Device errors
- Storage health – For Example, Controller errors, physical or virtual disk errors
- Configuration changes – For Example, Change in RAID configuration, PCIe card removal
- Audit logs – For Example, Password authentication failure
- Firmware – For Example, Upgrades or Downgrade

Finally, IT Administrator can set different actions for alerts – Reboot, Power Cycle, Power Off, or No action.

4.2 Drift Detection

Organizations can reduce the potential for exploitation by enforcing standardized configurations and adopting a “zero tolerance” policy for any changes. Dell EMC OpenManage Enterprise Console allows customer to define their own server configuration baseline and then monitoring the drift of their production servers from those baselines. The baseline can be built based on different criteria to fit different production enforcement, such as security and performance.

OpenManage Enterprise can report any deviations from the baseline and optionally repair the drift with a simple workflow to stage the changes on iDRAC9. The changes can then take place at the next maintenance windows while servers rebooting to make the production environment compliance again. This staged process enables customer to deploy configuration changes to production without any server downtime during non-maintenance hours. It increases the server availability without compromising on the serviceability or security.

5 Recover

Server solutions must support recovery to a known, consistent state as a response to various events:

- Newly discovered vulnerabilities
- Malicious attacks and data tampering
- Corruption of firmware due to memory failures or improper update procedures
- Replacement of server components
- Retiring or repurposing a server

The following section discusses responses to new vulnerabilities and corruption issues, and how to recover the server to its original state if needed.

5.1 Rapid Response to New Vulnerabilities

Common Vulnerabilities and Exposures (CVEs) are newly discovered attack vectors that compromise software and hardware products. Timely responses to CVEs are critical to most companies so they can swiftly assess their exposure and take appropriate action.

CVEs can be issued in response to new vulnerabilities identified in many items including the following:

- Open Source code such as OpenSSL
- Web browsers and other Internet access software
- Vendor product hardware and firmware
- Operating systems and hypervisors

Dell EMC works aggressively to quickly respond to new CVEs in PowerEdge servers and provide customers timely information including the following:

- Which products are affected?
- What remediation steps may be taken.
- If needed, when updates are available to address the .VE.

5.2 BIOS and operating system Recovery

Dell EMC 14th and 15th generation PowerEdge servers include two types of recovery: BIOS Recovery and Rapid Operating System Recovery. These features enable rapid recovery from corrupted BIOS or operating system images. In both cases, a special storage area is hidden from run-time software (BIOS, operating system, device firmware, so on). These storage areas contain pristine images that can be used as alternatives to the compromised primary software.

Rapid Operating System Recovery enables rapid recovery from a corrupted operating system image or an operating system image that is suspected of malicious tampering. The recovery media can be using internal SD card, SATA ports, M.2 drives, or internal USB. A recovery image of the operating system can be installed on the selected device. That device can then be disabled and hidden from the boot list and operating system. In the hidden state, BIOS disables the device making it inaccessible by the operating system. If the operating system is corrupted, the recovery location can then be enabled for boot. These settings can be accessed through BIOS or the iDRAC interface.

In extreme case of BIOS corruption, users must have a way to recover the BIOS to its original state. BIOS corruption can be caused by a malicious attack, power loss during the update process, or any other unforeseen event. A backup BIOS image is stored in iDRAC so it can be used to recover the BIOS image. iDRAC orchestrates the entire end to end recovery process. There are two options for BIOS recovery:

- Automatic BIOS recovery is when the BIOS initiates the process.
- On-demand BIOS recovery is when a user initiates the process using the RACADM CLI command.

5.3 Firmware Rollback

Dell EMC recommends keeping firmware up to date to maintain the latest features and security updates. If there is an issue after an update, it is possible to rollback an update or install an earlier version. Firmware rollbacks are verified against its signature.

Firmware Rollback from existing production version “N” to a previous version “N-1” is supported for the following firmware images:

- BIOS
- iDRAC
- Network Interface Card (NIC)
- PowerEdge RAID Controller (PERC)
- Power Supply Unit (PSU)
- Backplane

Firmware Rollback can be performed using any of the following methods:

- iDRAC web interface
- CMC web interface
- RACADM CLI – iDRAC and CMC
- Lifecycle Controller User Interface
- Lifecycle Controller Remote Services

Users can roll back the firmware for iDRAC or any device that iDRAC supports, even if the upgrade was previously performed using another interface. For example, if the firmware was upgraded using the Lifecycle Controller (F10) interface, the iDRAC web interface can roll it back. Multiple firmware rollbacks can be performed with one system reboot.

5.4 Restoring Server Configuration after Hardware Servicing

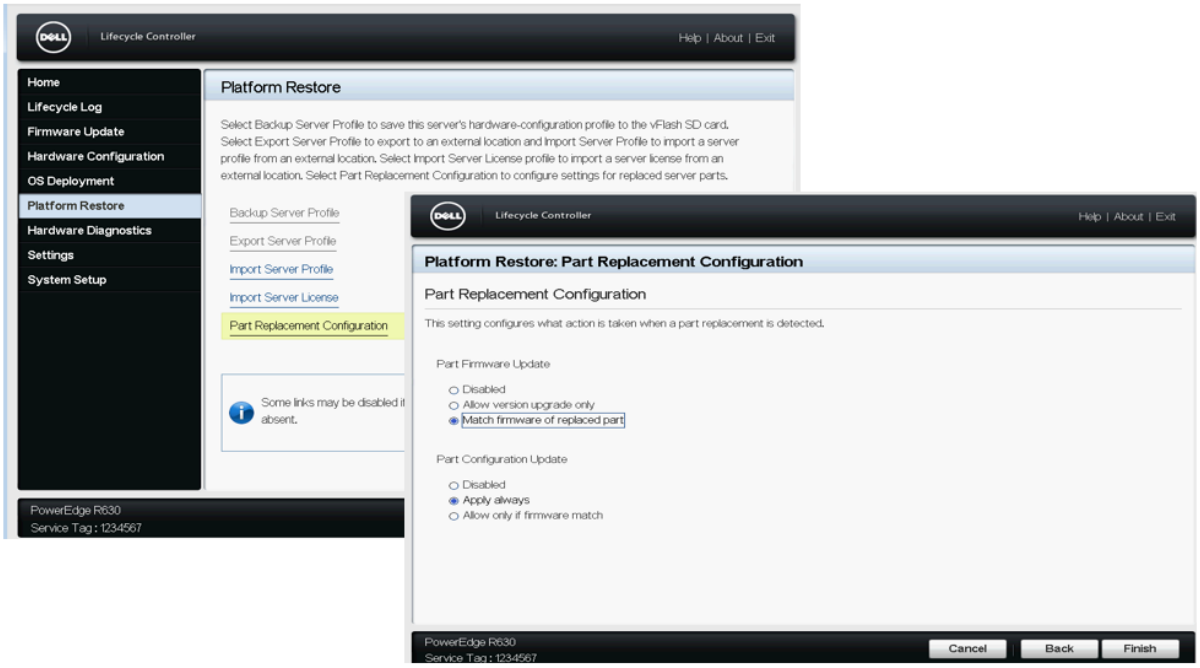
Remediating service events is a critical part of any IT operation. The ability to meet recovery time objectives and recovery point objectives has direct implications on the security of the solution. Restoring server configuration and firmware assures that security policies for server operation are automatically met.

PowerEdge servers provide functionality that quickly restores server configuration in the following situations:

- Individual part replacement
- System board replacement (Easy Restore)

5.4.1 Parts Replacement

iDRAC automatically saves both the firmware image and configuration settings for NIC cards, RAID controllers, and Power Supply Units (PSUs). After a field replacement of these parts, the user can select the “Parts Replacement” option in F10. This option restores the firmware and configuration to the replaced item. This functionality saves critical time and ensures a consistent configuration and security policy.



5.4.2 Easy Restore (for System Board Replacement)

System board replacements can be time-consuming and affect productivity. iDRAC offers the ability to backup and restore a PowerEdge server configuration to minimize the effort to replace a failed system board.

There are two ways the PowerEdge server can backup and restore:

- PowerEdge servers automatically backs up system configuration settings.
  - These items include BIOS, iDRAC, NIC, Service Tag, licenses, Credential Vault, and UEFI diagnostics.
  - These items are securely stored in memory on the control panel.
  - Firmware is not backed up due to space limitations.
  - After a system board replacement, Easy Restore prompts the user at boot to restore the data.
  - If no reply is entered, the iDRAC automatically restores the information.
- For a more comprehensive backup, a user can back up the system configuration, including the **installed firmware.**
  - Configuration and firmware are backed up for BIOS, RAID, NIC, iDRAC, and other components.
  - The backup operation also includes the hard disk configuration data, system board, and replaced parts.
  - The backup creates a single file that can be stored on local or network share (CIFS, NFS, HTTP, or HTTPS).

5.5 System Erase

At the end of a system life cycle, it either can be retired or repurposed. For either scenario, System Erase removes sensitive data and settings from the server. Secure Erase wipes storage devices and server nonvolatile stores such as caches and logs so that no confidential information unintentionally leaks. It is a utility in Lifecycle Controller (F10) that erases logs, configuration data, storage data, and cache.

The following devices, configuration settings, and applications can be erased by using the System Erase feature:

- iDRAC is reset to default settings, erasing all data and settings.
- Lifecycle Controller (F10) data
- BIOS
- Embedded diagnostics and operating system driver packs
- iDRAC Service Module (iSM)
- SupportAssist Collection reports

The following components can also be erased:

- Hardware Cache (clear PERC NVCache)
- vFlash SD Card (initialize card) (Note: vFlash not available on servers 15G or later.)

Data on the following components are cryptographically disposed of by System Erase as described below:

- Self Encrypting Drives (SED)
- Instant Secure Erase drives (ISE drives)
- NVM devices such as Intel Apache Pass and NVDIMMs

Data overwrite can erase non-ISE SATA hard drives.

Instant Secure Erase (ISE) destroys the internal encryption key that is used in 14th and 15th generation drives thus rendering the user data unrecoverable. ISE is a recognized method of data erasure on storage drives as seen in NIST Special Publication 800-88 “Guidelines for Media Sanitization.”

Advantages of the new ISE feature with System Erase are the following:

- Speed: Faster than data overwriting techniques like DoD 5220.22-M (seconds compare with hours)
- Effectiveness: ISE renders all the data on the drive, including reserved blocks, unreadable.
- Better TCO: Storage devices can be reused instead of being crushed or otherwise physically destroyed.

System Erase can be performed by the following methods:

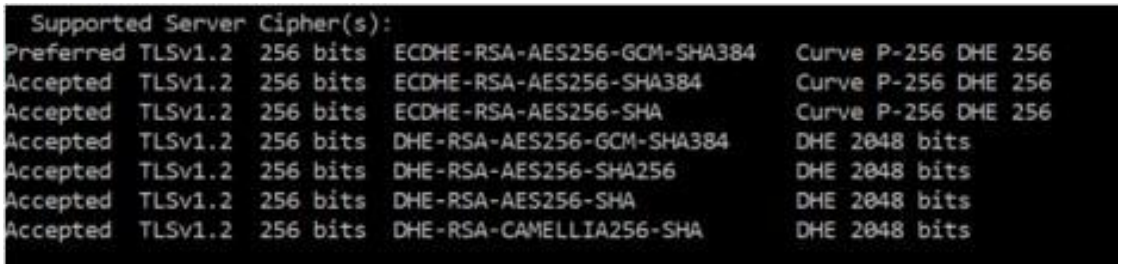
- Lifecycle Controller interface (F10)
- RACADM CLI
- Redfish

5.6 iDRAC9 Cipher Suite

The Cipher Suite Selection can be used to limit the ciphers the web browser can use to communicate with iDRAC. Also, it can determine how secure the connection is. These settings can be configured through iDRAC web interface, RACADM, and Redfish. This functionality is available across several iDRAC releases – iDRAC7, iDRAC8 (2.60.60.60 and higher), and the current iDRAC9 (3.30.30.30 and higher).

5.7 Commercial National Security Algorithm (CNSA) Support

The supported ciphers available in iDRAC9 with TLS1.2 and 256 Bit Encryption are shown in the screenshot image below. The ciphers available are inclusive of the ciphers in the CNSA approved set.



5.8 Full Power Cycle

In a Full Power Cycle, the server and all its components are rebooted. It drains main and auxiliary power from the server and all components. All data in volatile memory is also erased.

A physical Full Power Cycle requires taking out the AC power cable, waiting for 30 seconds, and then putting the cable back. This process poses a challenge when working with a remote system. A new feature in 14G and 15G servers performs a Full Power Cycle from iSM, IDRAC UI, BIOS, or a script. Full Power Cycle takes effect at the next power cycle.

Full Power Cycle feature eliminates the need for anyone to be physically present in the data center, thus reducing time to troubleshoot. It can also eliminate any malware resident in memory.

6 Conclusion

Data center security is paramount to business success, and the security of the underlying server infrastructure is critical. Cyberattacks have the potential for extended system and business downtime, lost revenue and customers, legal damages and tarnished corporate reputation. To protect, detect, and recover from hardware-targeted cyberattacks, security must be built into server hardware design, not added on after the fact.

Dell EMC has been a leader in leveraging silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. The 14th and 15th generation PowerEdge Servers feature an enhanced Cyber Resilient Architecture that uses silicon based Root of Trust to further harden server security. Other features are:

- **Cryptographically verified Trusted Booting** that anchors end-to-end server safety and overall data center security. It includes features like silicon-based Root of Trust, digitally signed firmware, and automatic BIOS recovery.
- **Secure Boot** which checks the cryptographic signatures of UEFI drivers and other code that is loaded before the operating system is running.
- **iDRAC Credential Vault** is a secure storage space for credentials, certificates, and other sensitive data. The Credential Vault is encrypted with a silicon based key that is unique for every server.
- **Server System Lockdown** helps secure any system configuration and firmware from malicious or unintended configuration changes, and alerts users to any attempted system changes.
- **Secure Enterprise Key Management** delivers a central key management solution to manage data-at-rest across the organization.
- **System Erase** allows users to easily retire or repurpose 14th and 15th generation servers by securely and quickly wiping data from various devices.
- **Supply Chain Security** provides supply chain assurance by ensuring there is no product tampering or counterfeit components before shipping products to the customers.

Dell EMC 14th and 15th generation PowerEdge servers are the trusted foundation for IT administrators to securely run their data center operations and workloads.

A Technical support and resources

http://www.dell.com/support Dell Technical Support

http://www.dell.com/support/idrac: The iDRAC support home page provides access to product documents, technical white papers, how-to videos, and more.

http://www.dell.com/idracmanuals: iDRAC User Guide and other manuals

Other documents

System Erase on PowerEdge Servers

Securing 14th generation Dell EMC PowerEdge servers with System Erase

Security in Server Design

Cyber Resiliency Starts at the Chipset and BIOS

Improved Server Security with iDRAC9 and SELinux

Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

Factory Generated Default iDRAC9 Password

Improved security with iDRAC9 via Root of Trust and BIOS Live Scanning

Secure Boot Management on Dell EMC PowerEdge Servers

Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers

iDRAC Automatic Certificate Enrollment

Rapid Operating System Recovery

RSA SecurID and iDRAC9

iDRAC9 Cipher Select – Improved Security for Dell EMC PowerEdge Server

UEFI Secure Boot Customization

Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers

(Video) Secure Boot Configuration and Certificate Management using RACADM