DELL Technologies

白皮书

技术白皮书：Dell EMC PowerEdge 服务器的网络弹性安全性

2020 年 12 月

修订记录

日期	描述
2018年1月	初始版本
2020 年 11 月	修订版本

中国印刷 [11/12/20] [技术白皮书]

目录

目录

执行摘要

Dell Technologies 安全方法与生俱来（内置，而非事后外接），而且集成到戴尔安全开发生命周期的每个步骤中。我们不断努力改进 PowerEdge 安全控制、功能和解决方案，以应对日益增长的威胁环境，并继续借助基于硅的信任根来巩固安全性。本文详细介绍了 PowerEdge 网络弹性平台中内置的安全功能，其中许多功能通过 Dell Remote Access Controller (iDRAC9) 启用。自从上一份 PowerEdge 安全白皮书发布以来，我们增加了许多新功能，从访问控制到数据加密，再到供应链保障，不一而足。具体包括：实时 BIOS 扫描、UEFI 安全启动自定义、RSA Secure ID MFA、Secure Enterprise Key Management (SEKM)、Secured Component Verification (SCV)、增强的系统擦除、自动证书登记和续订、密码选择和 CNSA 支持。所有功能都充分利用智能和自动化来帮助您提前应对威胁，并实现扩展以满足不断增长的使用模式要求。

1.简介

随着威胁环境的不断发展，IT 和安全专业人员在管理数据和资源风险方面日益艰难。数据的使用位置遍布许多设备、本地环境和云环境，并且影响重大的数据泄露事件不断增加。过去，安全重点一直放在操作系统、应用程序、防火墙、IPS 和 IDS 系统上。这些仍然是需要注意的重要领域。然而，鉴于过去一两年发生的事件已经表明硬件面临着诸多威胁，我们认为保护基于硬件的基础架构（如固件、BIOS、BMC 和其他像供应链保障之类的硬件保护）同样是至关重要的需求。

Dell Technologies 2020 数字化转型指数研究发现，数据隐私和网络安全问题是数字化转型的头号障碍。[1] 63% 的公司经历过因攻击者利用漏洞而导致数据泄露的情况[2]。到 2021 年，与网络犯罪相关的全球损失将达 6 万亿美元[3]。

随着服务器在软件定义的数据中心体系结构中变得越来越重要，服务器安全性成为企业整体安全的基础。服务器必须通过利用一个不可变的信任根来强调硬件和固件级别的安全性，该信任根可用于验证服务器内的后续操作。这就建立了一条贯穿于服务器整个生命周期（从部署到维护再到停用）的信任链。

采用 iDRAC9 的第 14 和 15 代 Dell EMC PowerEdge 服务器可提供此信任链，并将其与安全控制和全面的管理工具相结合，从而跨硬件和固件提供稳健的安全层。最终打造成一个网络弹性体系结构，延伸到服务器的各个方面，包括嵌入式服务器固件、存储在系统中的数据、操作系统、外围设备以及内部的管理操作。组织可以构建一个流程来保护其宝贵的服务器基础架构和内部的数据，检测任何异常、违规或未经授权的操作，以及从意外或恶意事件中恢复。

[1] Dell Technologies 2020 数字化转型指数

[2] 将当前安全威胁与 BIOS 级控制相匹配。受戴尔委托撰写的 Forrester Consulting 思想领袖白皮书，2019 年

[3] 预计会发生勒索软件攻击...The National Law Review，2020 年

2.通向安全服务器基础架构之路

Dell EMC PowerEdge 服务器的几代产品都具备强大的安全性，包括使用基于硅的数据安全性的创新。Dell EMC 14G PowerEdge 服务器扩展了基于硅的安全性，可在服务器启动过程中使用加密信任根来验证 BIOS 和固件。Dell EMC 产品团队在第 14 和 15 代 PowerEdge 服务器的设计过程中考虑到了几个关键要求，以应对现代 IT 环境中面临的安全威胁：

- **保护：**在生命周期的每一个阶段保护服务器，包括 BIOS、固件、数据和物理硬件
- **检测：**检测恶意网络攻击和未经批准的更改；主动接洽 IT 管理员
- **恢复：**将 BIOS、固件和操作系统恢复到已知良好状态；安全地淘汰服务器或调整其用途

Dell EMC PowerEdge 服务器符合本文所阐述的有关加密和安全性的主要行业标准，并对新漏洞进行持续跟踪和管理。

Dell EMC 已经实施了安全开发生命周期流程，将安全性作为开发、采购、制造、运输和支持等各个方面的关键要素，从而打造一个网络弹性体系结构。

2.1 安全开发生命周期

提供网络弹性体系结构需要在开发的每个阶段都具有安全意识和规范措施。此过程被称为安全开发生命周期 (SDL) 模型，其中安全性不是事后追加的，而是整个服务器设计过程中不可或缺的一部分。此设计过程涵盖整个服务器生命周期中安全需求的视图，如下面的要点列表和图 1 中所示：

- 在对功能进行构思、设计、制作原型、实施、投入生产、部署和维护时，优先考虑安全性
- 服务器固件经过精心设计，可在产品开发生命周期的各个阶段阻碍、阻止和抵制恶意代码入侵
  - » 设计过程中的威胁建模和渗透测试覆盖率
  - » 在固件开发的每个阶段都应用安全编码实践
- 对于关键技术，外部审核与内部 SDL 流程相辅相成，以确保固件遵循已知的安全最佳实践
- 使用全新的安全评估工具持续测试和评估新的潜在漏洞
- 快速响应关键的通用漏洞披露 (CVE)，包括在必要时建议采取的补救措施。

图 1：Dell EMC 的安全开发生命周期

2.2 网络弹性体系结构

Dell EMC 第 14 和 15 代 PowerEdge 服务器采用增强的网络弹性体系结构，可提供经过强化的服务器设计，以防范、检测网络攻击并从攻击中恢复。此体系结构的一些关键方面包括：

- **有效防范攻击**
  - 基于硅的信任根
  - 安全启动
  - 签名固件更新
  - 动态系统锁定
  - 硬盘加密和企业密钥管理
- **可靠的攻击检测**
  - 配置和固件偏差检测
  - 持久的事件日志记录
  - 审核日志记录和警报
  - 机箱防盗检测
- **快速恢复，几乎不会中断业务**
  - 自动化 BIOS 恢复
  - 快速操作系统恢复
  - 固件回滚
  - 快速系统擦除

2.3 当今的威胁

当今不断变化的环境中存在许多威胁矢量。表 1 总结了 Dell EMC 管理关键后端威胁的方法。

表 1：Dell EMC 如何解决常见的威胁矢量

服务器平台层		
安全层	**威胁矢量**	**Dell EMC 解决方案**
物理服务器	服务器/组件篡改	Secured Component Verification (SCV)、机箱入侵检测
固件和软件	固件损坏、恶意软件入侵	基于硅的信任根；Intel Boot Guard；AMD Secure Root-of-Trust；UEFI 安全启动自定义 经加密签名和验证的固件；
	软件	CVE 报告；按需修补
认证信任功能	服务器身份欺骗	TPM、TXT、信任链
服务器管理	恶意配置和更新、未经授权的开放端口攻击	iDRAC9，远程认证。

服务器环境层		
安全层	**威胁矢量**	**Dell EMC 解决方案**
数据	数据泄露	SED（自加密驱动器）— FIPS 或 Opal/TCG Secure Enterprise Key Management 仅 ISE（即时安全擦除）驱动器 安全的用户身份验证
供应链完整性	假冒组件 恶意软件威胁	所有全球服务器制造基地均通过 ISO9001 认证；安全组件验证；所有权证明 作为安全开发生命周期 (SDL) 流程的一部分实施的安全措施
供应链安全	制造基地的物理安全性 运输期间的被盗和篡改	货运资产保护协会 (TAPA) 设施安全要求 海关贸易合作反恐条例 (C-TPAT)；SCV

3.保护

“保护”功能是 NIST 网络安全框架的关键组成部分，用于抵御网络安全攻击。此功能包括访问控制、数据安全、维护和保护技术等多个类别。重要的基本理念是，作为全面安全安装和计算环境的一部分，基础架构资产必须提供强有力的保护，防止未经授权访问资源和数据。这包括防止对 BIOS 和固件等关键组件进行未经授权的修改。该平台符合 NIST SP 800-193 中的现行建议。

PowerEdge 服务器中的网络弹性体系结构可提供高水平的平台保护，包括以下功能：

- 经过加密验证的可信启动
- 用户访问安全性
- 签名固件更新
- 加密数据存储
- 物理安全性
- 供应链完整性和安全性

3.1 经过加密验证的可信启动

服务器安全性最重要的一个方面是确保可以验证启动过程的安全性。此过程为所有后续操作（如启动操作系统或升级固件）提供一个可信赖的锚点。针对 iDRAC 凭证存储区（iDRAC 中用于存储敏感数据的加密安全内存）等功能，几代 PowerEdge 服务器都使用了基于硅的安全保护。使用基于硅的信任根对启动过程进行验证，以满足 NIST SP 800-147B（“适用于服务器的 BIOS 保护指南”）和 NIST SP 800-155（“BIOS 完整性衡量指南”）中的建议。

3.1.1 基于硅的信任根

第 14 和 15 代 PowerEdge 服务器（均基于英特尔或 AMD）现在使用一个不可变的基于硅的信任根，以加密方式证明 BIOS 和 iDRAC 固件的完整性。此信任根基于一次性可编程的只读公钥，以防止恶意软件篡改。BIOS 启动过程利用 Intel Boot Guard 技术或 AMD Root-of-Trust 技术，可以验证启动映像的加密哈希的数字签名是否与 Dell EMC 在出厂时存储在硅片中的签名一致。验证失败会导致服务器关闭，并且生命周期控制器日志中出现用户通知，然后用户可以启动 BIOS 恢复过程。如果 Boot Guard 成功验证，则使用信任链程序验证其余的 BIOS 模块，直到将控制权移交给操作系统或虚拟机管理程序为止。

除 Boot Guard 的验证机制外，iDRAC9 4.10.10.10 或更高版本还提供了一个信任根机制，以在主机启动时验证 BIOS 映像。只有成功验证 BIOS 映像后，主机才能启动。iDRAC9 还提供了一种机制，可在运行时、按需或按用户计划的时间间隔验证 BIOS 映像

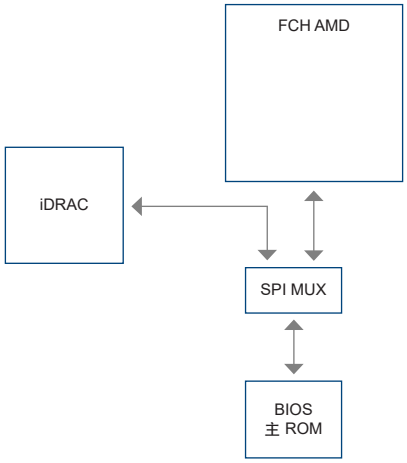
我们来详细了解一下信任链。每个 BIOS 模块都包含链中下一个模块的哈希值。BIOS 中的关键模块包括 IBB（初始启动块）、SEC（安全性）、PEI（EFI 前期初始化）、MRC（内存参考代码）、DXE（驱动程序执行环境）和 BDS（启动设备选择）。如果 Intel Boot Guard 对 IBB（初始启动块）进行身份验证，则 IBB 在将控制权移交给它之前会验证 SEC+PEI。SEC+PEI 然后验证 PEI+MRC，进一步验证 DXE+BDS 模块。此时，控制权将移交给 UEFI 安全启动，下一节将对此进行解释。

同样，对于基于 AMD EPYC 的 Dell EMC PowerEdge 服务器，AMD Secure Root-of-Trust 技术可确保服务器仅从可信赖的固件映像启动。此外，AMD Secure Run 技术旨在对主存进行加密，使其保持私密，防止恶意入侵者访问硬件。使用此功能无需修改任何应用程序，而且安全处理器从不在处理器之外公开加密密钥。

iDRAC 还承担着基于硬件的安全技术的角色，并且除了 AMD 的 Fusion Controller Hub (FCH) 之外，还通过 SPI 访问主 BIOS ROM，并执行 RoT 过程。

在以下情况下，iDRAC9 将恢复 BIOS。

1. BIOS 完整性检查失败。
2. BIOS 自检失败。
3. 使用 RACADM 命令 — **racadm recover BIOS.Setup.1-1**



iDRAC 启动流程使用自己独立的基于硅的信任根来验证 iDRAC 固件映像。iDRAC 信任根还提供关键的信任锚点，用于对 Dell EMC 固件更新包 (DUP) 的签名进行身份验证。

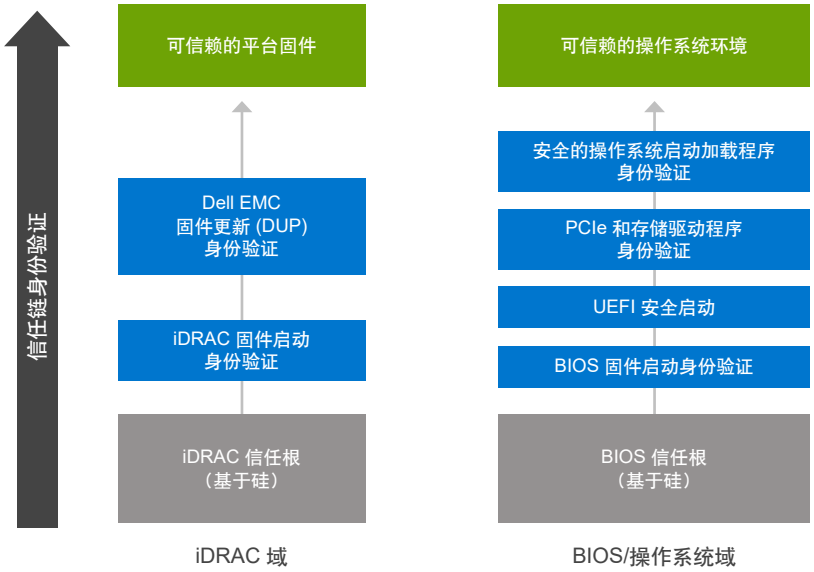


图 2：PowerEdge 服务器中基于硅的信任域根

3.1.2 BIOS 实时扫描

BIOS 实时扫描可在主机开机时（而不是在 POST 过程中）验证主 ROM 中 BIOS 映像的完整性和真实性。这是 AMD 特有的功能，仅适用于具有数据中心许可证的 iDRAC9 4.10.10.10 或更高版本。您必须拥有管理员权限，或拥有“执行调试命令”调试权限的管理员权限，才能执行此操作。您可以通过 iDRAC UI、RACADM 和 Redfish 接口来计划扫描

3.1.3 UEFI 安全启动自定义

PowerEdge 服务器还支持行业标准的 UEFI（统一可扩展固件接口）安全启动，它可以在操作系统运行之前检查 UEFI 驱动程序和其他已加载代码的加密签名。安全启动代表了预启动环境中的行业安全标准。计算机系统供应商、扩展卡供应商和操作系统提供商就该规范进行协作以提高互操作性。

启用 UEFI 安全启动后，可防止加载未签名（即不受信任）的 UEFI 设备驱动程序，显示错误消息，并且不允许设备运行。必须禁用安全启动，才能加载未签名的设备驱动程序。

此外，第 14 和 15 代 PowerEdge 服务器为客户提供了独特的灵活性，可以使用未经 Microsoft 签名的自定义启动加载程序证书。该功能主要面向那些希望为自己的操作系统启动加载程序签名的 Linux 环境管理员。可通过首选的 iDRAC API 上传自定义证书，以验证客户的特定操作系统启动加载程序。NSA 借助此 PowerEdge UEFI 自定义方法来缓解服务器中的 Grub2 漏洞。

3.1.4 TPM 支持

PowerEdge 服务器支持三种版本的 TPM：

- TPM 1.2 FIPS + Common Criteria + TCG 认证 (Nuvoton)
- TPM 2.0 FIPS + Common Criteria + TCG 认证 (Nuvoton)
- TPM 2.0 中国大陆地区 (NationZ)

TPM 可用于执行公钥加密功能；计算哈希功能；生成、管理和安全地存储密钥；以及进行认证。此外，还支持英特尔的 TXT（可信执行技术）功能和 Windows Server 2016 中的 Microsoft 平台保障功能。TPM 还可用于启用 Windows Server 2012/2016 中的 BitLocker™ 硬盘加密功能。

认证和远程认证解决方案可以使用 TPM 在服务器的硬件、虚拟机管理程序、BIOS 和操作系统启动时进行测量，并以加密安全的方式与存储在 TPM 中的基本测量值进行比较。如果它们不一致，则服务器身份可能已经泄露，系统管理员可以在本地或远程禁用服务器并断开连接。

可以订购带或不带 TPM 的服务器，但对于许多操作系统规定和其他安全规定来说，TPM 正成为一项标准配置。通过 BIOS 选项启用 TPM。它是一种插件模块解决方案，平面上有一个用于此插件模块的接口。

3.1.5 安全认证

Dell EMC 已获得 NIST FIPS 140-2 和 Common Criteria EAL-4 等标准的认证。这些对于遵守美国国防部 (DoD) 和其他政府要求非常重要。PowerEdge 服务器已获得以下认证：

- 服务器平台：通过 RHEL 的 Common Criteria EAL4+ 认证，也用于支持合作伙伴 CC 认证
- iDRAC 和 CMC FIPS 140-2 Level 1 认证
- OpenManage Enterprise-Modular 通过 EAL2+ 认证
- TPM 1.2 和 2.0 通过 FIPS 140-2 和 Common Criteria 认证

3.2 用户访问安全性

确保正确的身份验证和授权是任何现代访问控制策略的关键要求。PowerEdge 服务器的主要访问接口是通过 API、CLI 或嵌入式 iDRAC 的 GUI。用于自动化服务器管理的首选 API 和 CLI 包括：

- iDRAC Restful API with Redfish
- RACADM CLI
- SELinux

这些都提供了可靠的凭证，如用户名和密码安全，如果需要，可通过加密连接（如 HTTPS）传输凭证。SSH 通过使用一组匹配的加密密钥验证用户身份（因此无需输入安全性较低的密码）。支持旧协议（如 IPMI），但由于近年来发现的各种安全问题，不建议将其用于新部署。我们建议，如果您当前正在使用 IPMI，应评估并过渡到 iDRAC Restful API with Redfish。

可以将 **TLS/SSL 证书**上传到 iDRAC，以对网页浏览器会话进行身份验证。三种选择：

- **Dell EMC 自签名 TLS/SSL 证书** — 该证书由 iDRAC 自动生成并自签名。
  - » 优势：无需维护单独的证书颁发机构（请参阅 X.509/IETF PKIX 标准）。
- **自定义签名 TLS/SSL 证书** — 该证书自动生成，并使用已上传到 iDRAC 的私钥进行签名。
  - » 优势：单一可信 CA 适用于所有 iDRAC。您的内部 CA 可能已在您的管理站中受到信任。
- **CA 签名 TLS/SSL 证书** — 系统将生成一个证书签名请求 (CSR)，并将其提交给您的内部 CA 或第三方 CA（如 VeriSign、Thawte 和 Go Daddy）进行签名。
  - » 优势：可以使用商业证书颁发机构（请参阅 X.509/IETF PKIX 标准）。单一可信 CA 适用于所有 iDRAC。如果使用的是商业 CA，那么它很可能已经在您的管理站中受到信任。

iDRAC9 通过利用客户现有的身份验证和授权模式（已提供对 PowerEdge 服务器的安全访问），实现与 **Active Directory** 和 **LDAP** 的集成。它还支持**基于角色的访问控制 (RBAC)**，授予适当级别的访问权限（管理员、操作员或只读权限），以匹配人员在服务器操作中的角色。强烈建议以这种方式使用 RBAC，而不仅仅是向所有用户授予最高级别权限（即管理员权限）。

iDRAC9 还提供了其他方法来防止未经授权的访问，包括 **IP 阻塞和筛选**。IP 阻塞会动态地确定某个特定 IP 地址何时出现过多登录失败情况，并在预先选定的时间段内阻塞（或阻止）该地址登录到 iDRAC9。IP 筛选限制了访问 iDRAC 的客户端的 IP 地址范围。它将传入登录的 IP 地址与指定的地址范围进行比较，仅允许从源 IP 地址位于该范围内的管理站访问 iDRAC。所有其他登录请求都会被拒绝。

由于基于用户名和密码的单因素身份验证方案越来越容易受到攻击，因此如今**多因素身份验证 (MFA)** 的应用更加广泛。iDRAC9 允许使用智能卡进行远程 GUI 访问，并将支持 RSA 令牌。在这两种情况下，多因素均包括设备或卡的物理存在以及相关的 PIN。

3.2.1 RSA SecurID MFA

RSA SecurID 可用作对系统上的用户进行身份验证的另一种方法。iDRAC9 开始支持 RSA SecurID，使用数据中心许可证和固件 4.40.00.00 作为另一种双因素身份验证方法。

3.2.2 简化的 2FA

提供的另一种身份验证方法是 Easy 2FA，它将在用户登录 iDRAC 时，向该用户的电子邮箱发送随机生成的令牌。

3.2.3 SELinux 框架

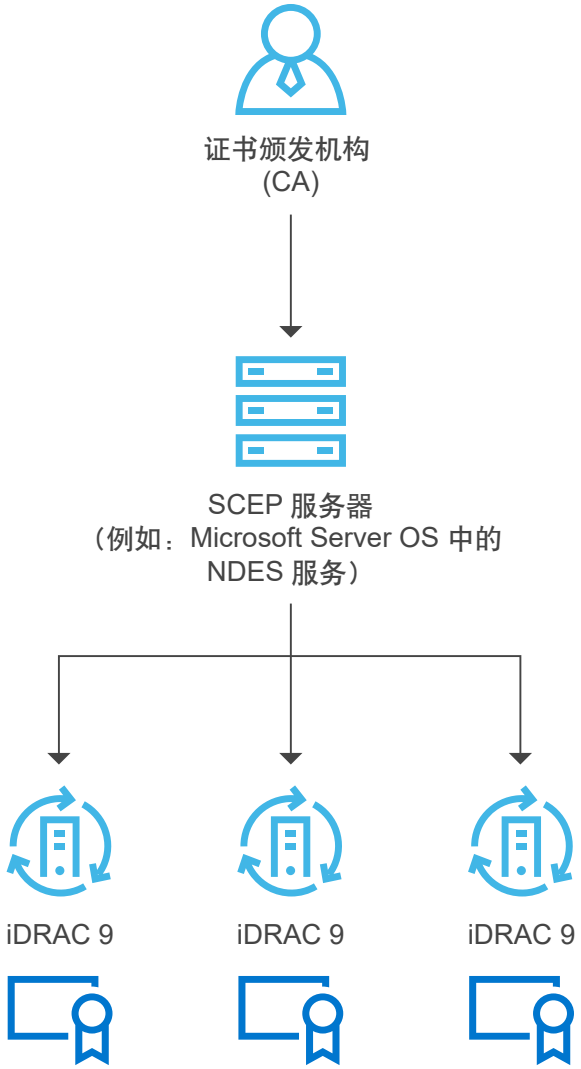
SELinux 在 iDRAC 上的核心内核级别运行，不需要用户提供任何输入或配置。SELinux 在检测到攻击时会记录安全消息。这些日志消息指明攻击者何时以及如何尝试侵入系统。目前，这些日志通过 SupportAssist 向注册此新功能的客户提供。在 iDRAC 的未来版本中，这些日志将在生命周期控制器日志中提供。

3.2.4 最低限度权限

在 iDRAC 内运行的所有内部进程都以最低限度权限运行；这是一个核心的 Unix 安全概念。这种保护可以确保可能受到攻击的系统进程不能访问该进程范围外的文件或硬件。例如，提供虚拟 KVM 支持的进程不得更改风扇速度。将这两个进程作为离散函数运行，有助于防止攻击从一个进程传播到另一个进程，从而保护系统。

3.2.5 自动证书登记和续订

iDRAC9 v4.0 添加了用于简单证书注册协议 (SCEP) 支持的客户端，并且需要数据中心许可证。SCEP 是一种协议标准，用于使用自动注册流程管理大量网络设备的证书。iDRAC 现在可与兼容 SCEP 的服务器（如 Microsoft ServerNDES 服务）集成，以自动维护 SSL/TLS 证书。该功能可用于注册和更新即将过期的 Web 服务器证书，并且可在 iDRAC GUI 中一对一地完成，通过 Server Configuration Profile 进行设置，或通过 RACADM 等工具编写脚本。



3.2.6 出厂默认密码

默认情况下，所有 14G PowerEdge 服务器都附带一个工厂生成的独特 iDRAC 密码，以提供额外的安全保护。该密码是在出厂时生成，位于机箱前端的拉出式信息标签上，该标签与服务器资产标签相邻。选择此默认选项的用户必须记下该密码，并在首次登录 iDRAC 时使用该密码，而不是使用通用默认密码。为了安全起见，Dell EMC 强烈建议更改默认密码。

3.2.7 动态系统锁定

iDRAC9 提供了一项新功能，可以“锁定”一台或多台服务器的硬件和固件配置，该功能需要企业或数据中心许可证。可以通过使用 GUI、CLI（如 RACADM）或作为 Server Configuration Profile 的一部分来启用此模式。具有管理权限的用户可以设置“系统锁定”模式，防止权限较低的用户对服务器进行更改。IT 管理员可以启用/禁用此功能。系统会在生命周期控制器日志中跟踪禁用“系统锁定”时进行的任何更改。通过启用锁定模式，您可以防止在使用 Dell EMC 工具和代理时数据中心出现配置偏差，以及防范在使用 Dell EMC Update Packages 时嵌入式固件遭受恶意攻击。可动态启用锁定模式，而无需重新启动系统。iDRAC9 v4.40 引入了增强功能，除了当前的系统锁定（仅使用 Dell Update Package (DUP) 控制更新）之外，此功能还扩展到特定 NIC。（注意：NIC 增强锁定仅包括固件锁定，以防止固件更新。）不支持配置 (x-UEFI) 锁定。当客户通过启用/设置任何受支持接口的属性将系统设置为锁定模式时，iDRAC 将根据系统配置执行其他操作。这些操作取决于在 iDRAC 发现过程中检测到的第三方设备。

3.2.8 域隔离

第 14 和 15 代 PowerEdge 服务器通过**域隔离**提供额外的安全保护，这是多租户托管环境的一项重要功能。为了确保服务器硬件配置的安全，托管提供商可能希望阻止租户进行任何重新配置。域隔离是一种配置选项，可确保主机操作系统中的管理应用程序无法访问带外 iDRAC 或英特尔芯片组功能，如管理引擎 (ME) 或创新引擎 (IE)。

3.3 签名固件更新

PowerEdge 服务器已经有多个代次在固件更新上使用数字签名，以确保仅在服务器平台上运行正版固件。我们使用 SHA-256 哈希和 2048 位 RSA 加密对所有固件程序包进行数字签名，以用于所有关键服务器组件的签名，包括适用于 iDRAC、BIOS、PERC、I/O 适配器和 LOM、PSU、存储驱动器、CPLD 和背板控制器的固件。iDRAC 将扫描固件更新，并将其签名与使用基于硅的信任根的预期内容进行比较；系统将中止任何无法验证的固件程序包，并在生命周期日志 (LCL) 中记录错误消息，以提醒 IT 管理员。

增强的固件身份验证嵌入在许多第三方设备中，这些设备使用它们自己的信任根机制提供签名验证。这样可防止可能使用受影响的第三方更新工具将恶意固件加载到 NIC 或存储驱动器（以及绕过使用签名的 Dell EMC Update Packages）的情况发生。与 PowerEdge 服务器一起发运的许多第三方 PCIe 和存储设备都使用硬件信任根来验证各自的固件更新。

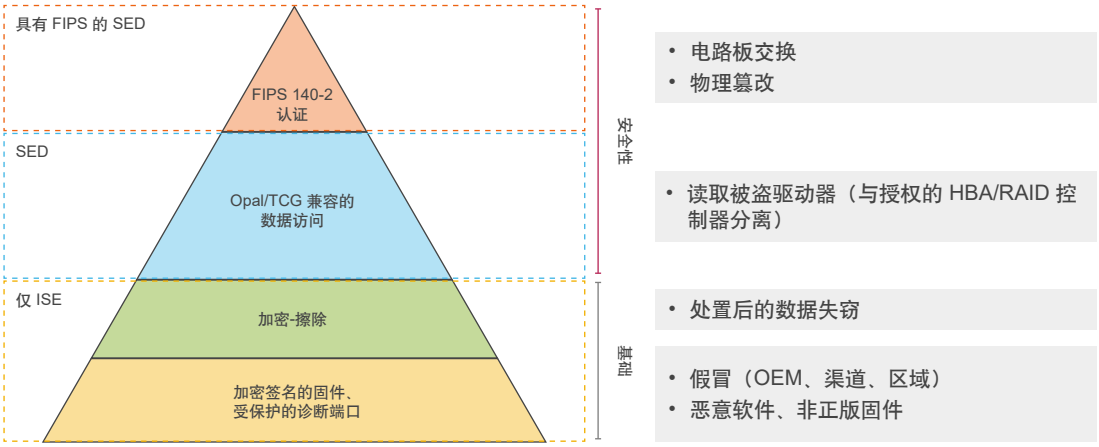
如果怀疑任何设备中的任何固件遭恶意篡改，IT 管理员可以将许多平台固件映像回滚到存储在 iDRAC 中的先前可信版本。我们在服务器上保留了 2 种版本的设备固件 — 现有的生产版本（“N”）和先前的可信版本（“N-1”）。

3.4 加密数据存储

第 14 和 15 代 PowerEdge 服务器提供了几种用于保护数据的存储驱动器选项。如下图所示，这些选项首先是支持即时安全擦除 (ISE) 的驱动器。ISE 是一项新技术，可即时且安全地擦除用户数据。第 14 和 15 代服务器默认提供支持 ISE 的驱动器。本文稍后将在系统擦除功能描述中更详细地讨论 ISE。

下一个安全性更高的选项是自加密驱动器 (SED)，它提供锁定保护，将存储驱动器与服务器和使用的 RAID 卡绑定在一起。这可防止所谓的“打砸抢掠”式驱动器盗窃以及随后的敏感用户数据丢失。当小偷试图使用驱动器时，因为不知道所需的锁定密钥密码，因此无法访问加密的驱动器数据。客户可以使用本文稍后讨论的 Secure Enterprise key Manager (SEKM) 防范整台服务器被盗。

NIST FIPS 140-2 认证的 SED 提供最高级别的保护。符合此标准的驱动器已通过测试实验室的认证，并在驱动器上贴有防篡改贴纸。Dell EMC SED 驱动器默认具有 FIPS 140-2 认证。



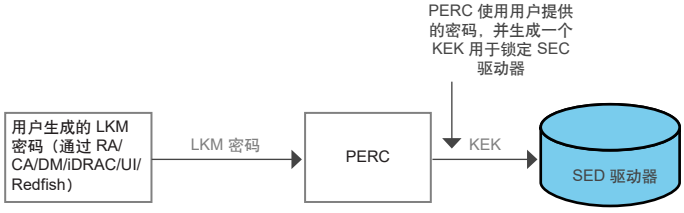
3.4.1 iDRAC 凭证存储区

iDRAC 服务处理器提供安全的存储内存，可保护各种敏感数据，如用于自签名 SSL 证书的 iDRAC 用户凭据和私钥。基于硅的安全性的另一个示例是，此内存使用唯一的不可变根密钥进行加密，该密钥在制造时编程到每个 iDRAC 芯片中。 这可防止攻击者为了获取数据访问权限而对芯片进行脱焊的物理攻击。

3.4.2 本地密钥管理 (LKM)

借助当前的 PowerEdge 服务器，用户可以使用“本地密钥管理”来保护连接到 PERC 控制器的 SED 驱动器。

为了在驱动器被盗时确保用户数据受到保护，需要用一个单独的密钥锁定 SED，如此一来，除非提供该密钥，否则 SED 不会解密用户数据 — 该密钥称为密钥加密密钥 (KEK)。为此，用户在 SED 所连接的 PERC 控制器上设置 keyId/密码，PERC 控制器使用该密码生成一个 KEK，然后用它来锁定 SED。现在，当驱动器通电时，它会显示为锁定的 SED，并且只有在提供 KEK 来解锁时才会加密/解密用户数据。PERC 向该驱动器提供 KEK 以将其解锁 — 这样的话，如果驱动器被盗，它会显示为“已锁定”，并且如果攻击者无法提供 KEK，则用户数据将受到保护。由于密码和 KEK 存储在 PERC 的本地，所以将其称为“本地”密码。下图显示了 LKM 解决方案。

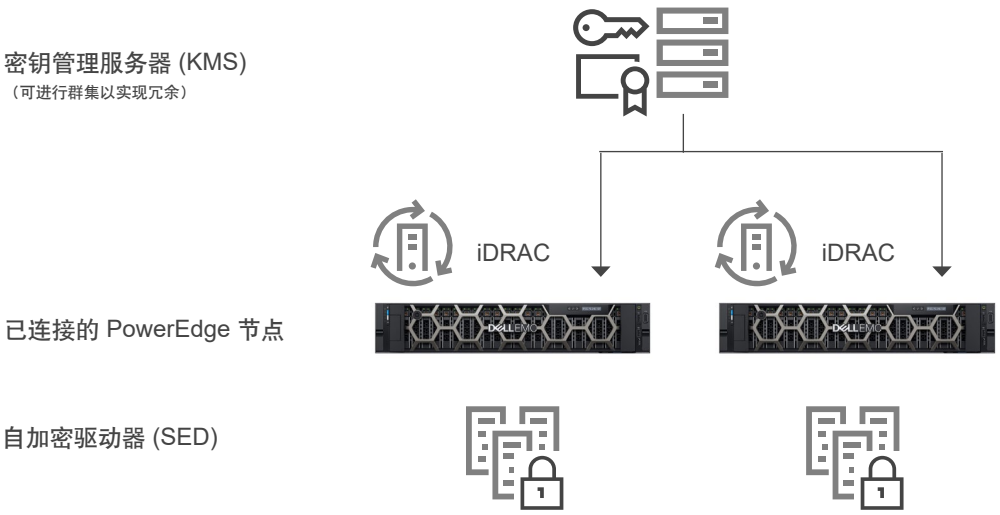


3.4.3 Secure Enterprise Key Manager (SEKM)

OpenManage SEKM 提供了一个中央密钥管理解决方案，以管理整个组织的静态数据。它使客户能够使用外部密钥管理服务器 (KMS) 来管理密钥，iDRAC 可以使用这些密钥来锁定和解锁 Dell EMC PowerEdge 服务器上的存储设备。使用通过特殊许可证激活的嵌入式代码，iDRAC 要求 KMS 为每个存储控制器创建密钥，它在每次主机启动时获取该密钥并提供给存储控制器，以便存储控制器可以解锁自加密驱动器 (SED)。

与本地密钥管理 (LKM) 相比，使用 SEKM 的优势包括：

- 防止“服务器被盗”，因为密钥不是存储在服务器上，而是存储在外部，并由连接的 PowerEdge 服务器节点检索（通过 iDRAC）。
- 针对具有高可用性的加密设备的集中式和可扩展密钥管理
- 支持行业标准 KMIP 协议，从而支持使用其他与 KMIP 兼容的设备
- 当驱动器或整个服务器受到威胁时，保护静态数据的安全
- 随驱动器数量扩展的驱动器级加密性能



3.5 硬件安全性

硬件安全性是任何全面的安全解决方案不可或缺的一部分。有些客户希望限制对入口端口（如 USB）的访问。服务器机箱在投入生产后通常不需要打开。在所有情况下，客户至少要跟踪和记录任何此类活动。总体目标是阻止和限制任何物理入侵。

3.5.1 机箱防盗警报

PowerEdge 服务器提供硬件入侵检测和日志记录功能，即使在交流电断电情况下检测功能也能正常工作。即使在运输过程中，当有人打开机箱或者对其做手脚时，机箱上的传感器都能够检测到。一旦通电，在运输途中曾被打开过的服务器即在 iDRAC 生命周期日志中生成一个条目。

3.5.2 动态 USB 端口管理

为了提高安全性，您可以完全禁用 USB 端口。您还可以选择仅禁用前部 USB 端口。例如，可以禁用 USB 端口以供生产使用，然后临时启用，授予对急救车的访问权限以进行调试。

3.5.3 iDRAC Direct

iDRAC Direct 是一种硬连接到 iDRAC 服务处理器的特殊 USB 端口，可从服务器前端（冷通道）进行服务器调试和管理。它允许用户将标准 Micro-AB USB 线缆连接到此端口，另一端 (Type A) 连接到笔记本电脑。然后，标准网页浏览器可以访问 iDRAC GUI，以便对服务器进行广泛的调试和管理。如果安装了 iDRAC Enterprise 许可证，则用户甚至可以通过 iDRAC 的虚拟控制台功能访问操作系统桌面。

由于正常的 iDRAC 凭证用于登录，因此 iDRAC Direct 可作为安全急救车使用，并具有广泛的硬件管理和服务诊断的额外优势。对于确保远程访问服务器的物理访问而言，这会是一个极具吸引力的选择（在本例中可以禁用主机 USB 端口和 VGA 输出）。

3.5.4 带地理位置的 iDRAC 连接视图

连接视图使 iDRAC 能够报告连接到服务器 I/O 的外部交换机和端口。它是特定网络设备上的一项功能，需要在已连接的交换机上启用 LLDP（链路层发现协议）。

连接视图的一些优势包括：

- 快速远程检查服务器 I/O 模块（LOM、NDC 和附加 PCIe 卡）是否连接到正确的交换机和端口
- 无需派遣技术工程师到现场修复布线错误，节省相应开支
- 无需在机房的热通道中追踪线缆走向
- 可通过 GUI 完成，或者 RACADM 命令可以提供所有 14G 连接的信息

除了明显的时间和成本节约之外，连接视图还有一个额外的优势 — 提供物理服务器或虚拟机的实时地理位置。使用 iDRAC 连接视图，管理员可以精确定位服务器，以准确查看服务器连接的交换机和端口，这有助于保护服务器的安全，防止其连接到不符合企业安全准则或最佳实践的网络和设备。

连接视图通过报告服务器所连接的交换机标识来间接验证该服务器的位置。交换机标识有助于确定地理位置，并确保该服务器不是非授权站点中的流氓服务器，从而提供另一层物理安全。这也验证了应用程序或虚拟机没有“越过”国家/地区边界，并且是在经批准的安全环境中运行。

3.6 供应链完整性和安全性

供应链完整性关注两项主要挑战：

1. 维护硬件完整性：确保在向客户交付产品之前，没有产品遭篡改或插入假冒组件
2. 维护软件完整性：确保在将产品交付给客户之前，没有恶意软件插入到固件或设备驱动程序中，并防止任何编码漏洞

Dell EMC 将供应链安全定义为保护物理资产、库存、信息、知识产权和人员的预防和检测控制措施的做法和应用。这些安全措施还可减少恶意或疏忽地将恶意软件和假冒组件引入供应链的机会，有助于提供供应链保障并确保完整性。

3.6.1 硬件和软件完整性

Dell EMC 专注于确保质量控制流程到位，以帮助更大限度地减少假冒组件渗入我们供应链的机会。Dell EMC 的控制措施涵盖了供应商选择、采购、生产流程和治理，直至审核和测试。一旦选择了供应商，新产品引入流程将验证所有构建阶段中使用的所有材料是否都来自经批准的供应商列表，并与物料清单相匹配（视情况而定）。生产过程中的材料检验有助于识别出有误标识、偏离正常性能参数或包含错误电子标识符的部件。

在可能的情况下，直接从原始设计制造商 (ODM) 或原始组件制造商 (OCM) 采购部件。在新产品引入过程中进行的材料检验提供了多个机会来识别可能进入供应链的假冒或损坏组件。

此外，Dell EMC 在全球的所有制造基地都通过了 ISO 9001 认证。严格遵守这些流程和控制措施有助于更大限度地降低假冒组件嵌入 Dell EMC 产品，或将恶意软件插入固件或设备驱动程序中的风险。这些措施作为软件开发生命周期 (SDL) 流程的一部分而实施。

3.6.2 物理安全性

Dell EMC 在建立和维护制造设施和物流网络的安全性方面有几项长期的关键实践。例如，我们要求某些生产 Dell EMC 产品的工厂满足指定的货运资产保护协会 (TAPA) 设施安全要求，包括重点区域使用闭路监控摄像头，安装门禁系统，以及在出入口不间断地安排人员值守。作为行业先进的物流计划的一部分，我们还采取了保护措施防止产品在运输过程中被盗和遭篡改。该计划提供了一个不间断配备人员的指挥中心，以监控全球范围内的特定入港及出港装运情况，确保无中断地将货物从一个目的地运往另一目的地。

Dell EMC 还积极参与多项自愿性供应链安全计划和倡议。其中一项倡议是美国政府在 9/11 之后推出的海关贸易合作反恐条例 (C-TPAT)，旨在通过增强的边境和供应链安全措施来帮助降低恐怖主义的可能性。作为这项倡议的一部分，美国海关和边境保护局要求参与成员确保其安全实践的完整性，并向供应链内的业务合作伙伴传达其安全准则。自 2002 年以来，Dell EMC 一直积极参与其中，并保持着较高级别的成员身份。

3.6.3 专为 PowerEdge 服务器设计的 Dell Technologies Secured Component Verification (SCV)

适用于 PowerEdge 的 Dell Technologies Secured Component Verification (SCV) 是一项供应链保障服务，该服务使 Dell EMC 客户能够验证其收到的 PowerEdge 服务器是否与工厂生产的服务器相匹配。为了以加密安全的方式验证组件，在制造过程中，工厂会生成一个证书，其中包含特定服务器的唯一组件 ID。此证书在 Dell Technologies 工厂中签名，并存储在 iDRAC 中，之后由客户在 SCV 应用程序中使用。客户使用 SCV 应用程序收集当前系统清单（包括唯一组件 ID），并根据 SCV 证书中的清单对其进行验证。

SCV 应用程序生成的报告将验证哪些组件与工厂中安装的组件匹配，哪些组件与工厂中安装的组件不匹配。它还验证证书和信任链，以及 iDRAC 对于 SCV 私钥的拥有证明。当前的实施支持直接发货客户，不包括 VAR 或部件更换场景。

4.检测

关键是要拥有检测能力，能够全面了解服务器系统中的配置、运行状况和更改事件。这种可见性还必须检测启动和操作系统运行过程中对 BIOS、固件和 Option ROM 的恶意或其他更改。主动轮询必须与为系统中的任意和所有事件发送警报的能力相结合。日志必须提供有关服务器访问和更改的完整信息。更重要的是，服务器必须将这些功能扩展到所有组件。

4.1 通过 iDRAC 进行全面监控

iDRAC 不依赖操作系统代理与服务器中的托管资源进行通信，而是采用通向每个设备的直接边带路径。Dell EMC 已利用行业标准协议（如 MCTP、NC-SI 和 NVMe-MI）与外围设备（如 PERC RAID 控制器、以太网 NIC、光纤通道 HBA、SAS HBA 和 NVMe 驱动器）进行通信。此体系结构是与业界先进的供应商长期、多年合作的成果，可在我们的 PowerEdge 服务器中提供免代理设备管理。配置和固件更新操作还利用 Dell EMC 和合作伙伴支持的强大的 UEFI 和 HII 功能。

借助此功能，iDRAC 可以监控系统的配置事件、入侵事件（如前文提到的机箱入侵检测）和运行状况更改。配置事件直接与发起更改的用户的身份绑定，无论是 GUI 用户、API 用户还是控制台用户。

4.1.1 生命周期日志

生命周期日志是一段时间内在服务器中发生的事件的集合。生命周期日志提供事件描述，包括时间戳、严重程度、用户 ID 或来源、建议操作，以及其他可能非常方便地用于跟踪或提醒的技术信息。

以下是生命周期日志 (LCL) 中记录的各种信息类型：

- 系统硬件组件上的配置更改
- iDRAC、BIOS、NIC 和 RAID 配置更改
- 所有远程操作的日志
- 基于设备、版本和日期的固件更新历史记录
- 有关更换部件的信息
- 有关故障部件的信息
- 事件和错误消息 ID
- 与主机电源相关的事件
- POST 错误
- 用户登录事件
- 传感器状态更改事件

4.1.2 警报

iDRAC 提供了配置不同事件警报以及在特定生命周期日志事件发生时要执行的操作的功能。生成事件时，它将使用选定的警报类型机制转发到所配置的目标位置。您可以通过 iDRAC Web 界面、RACADM 或 iDRAC 设置实用程序来启用或禁用警报。

iDRAC 支持不同类型的警报，例如：

- 电子邮件或 IPMI 警报
- SNMP 陷阱
- 操作系统和远程系统日志
- Redfish 事件

也可以按严重程度（关键、警告或说明）对警报进行分类。

可对警报应用以下筛选条件：

- 系统运行状况 — 例如，温度、电压或设备错误
- 存储运行状况 — 例如，控制器错误、物理或虚拟磁盘错误
- 配置更改 — 例如，RAID 配置更改、PCIe 卡移除
- 审核日志 — 例如，密码验证失败
- 固件/驱动程序 — 例如，升级或降级

最后，IT 管理员可以针对警报设置不同的操作 — 重新启动、功率循环、关闭电源或无操作。

4.2 偏差检测

通过实施标准化配置并对任何更改采用“零容忍”策略，组织可以降低被利用的可能性。Dell EMC OpenManage Enterprise Console 允许客户定义他们自己的服务器配置基准，然后监视其生产服务器偏离这些基准的情形。可以根据不同的标准建立基准以适合不同的生产执行，例如安全性和性能。OpenManage Enterprise 可以报告任何偏离基准的情况，（可选）并通过一个简单的工作流以带外方式将更改加载到 iDRAC 上以修复这一偏离。然后，这些更改可以在服务器重新启动时的下一个维护时段内进行，以使生产环境再次合规。这种分阶段的流程使客户能够在非维护时段内将配置更改部署到生产环境，而不会出现严重的停机。它可以提高服务器的可用性，而不影响可服务性或安全性。

5.恢复

服务器解决方案必须支持恢复到已知的一致状态，作为对以下各种事件的响应：

- 新发现的漏洞
- 恶意攻击和数据篡改
- 由于内存故障或不正确的更新程序而导致固件损坏
- 更换服务器组件
- 服务器停用或重新利用

下面我们将详细讨论如何应对新的漏洞和损坏问题，以及如何将服务器恢复到其初始状态（如果需要）。

5.1 对新漏洞的快速响应

通用漏洞披露 (CVE) 是新发现的可破坏软件和硬件产品的攻击矢量。对大多数公司来说，及时应对 CVE 至关重要，这样他们就可以快速评估自身风险，并采取适当的行动。

可以针对许多项目中发现的新漏洞发布 CVE，包括以下项目：

- 开放源代码（如 OpenSSL）
- 网页浏览器和其他互联网访问软件
- 供应商产品硬件和固件
- 操作系统和虚拟机管理程序

Dell EMC 积极开展工作，快速响应 PowerEdge 服务器中的新 CVE，及时向客户提供以下信息：

- 哪些产品受到影响
- 可以采取哪些补救措施
- 如有必要，将在何时提供更新以解决 CVE

5.2 BIOS 和操作系统恢复

Dell EMC 第 14 和 15 代 PowerEdge 服务器包括两种类型的恢复：BIOS 恢复和快速操作系统 (OS) 恢复。这些功能可帮助实现从损坏的 BIOS 或操作系统映像中快速恢复。在这两种情况下，均针对运行时软件（BIOS、操作系统、设备固件等）隐藏了一个特殊存储区域。这些存储区域包含原始映像，可用于替代受损的主要软件。

快速的操作系统恢复可实现从损坏的操作系统映像（或涉嫌恶意篡改的操作系统映像）快速恢复。恢复介质可以通过内置 SD 卡、SATA 端口、M.2 驱动器或内置 USB。所选设备可以显示在启动列表和操作系统中，以便安装恢复映像。然后可以在启动列表和操作系统中将其禁用和隐藏。在隐藏状态下，BIOS 将禁用该设备，使操作系统无法访问它。如果操作系统映像损坏，则可以启用恢复位置以进行启动。可通过 BIOS 或 iDRAC 界面访问这些设置。

在极端情况下，如果 BIOS 损坏（由于恶意攻击，或由于更新过程中断电，或由于任何其他意外事件而导致损坏），则提供一种方法将 BIOS 恢复到其初始状态非常重要。备份 BIOS 映像存储在 iDRAC 中，可在需要时用来恢复 BIOS 映像。iDRAC 编排整个端到端恢复过程。

- 自动 BIOS 恢复由 BIOS 本身启动。
- 用户可以使用 RACADM CLI 命令启动按需 BIOS 恢复。

5.3 固件回滚

建议保持固件更新，以确保拥有新功能和安全更新。但是，如果在更新后遇到问题，可能需要回滚更新或安装一个较早版本。如果回滚到先前版本，也会根据其签名进行验证。

以下固件映像目前支持从现有生产版本“N”回滚到先前版本“N-1”：

- BIOS
- 带生命周期控制器的 iDRAC
- 网卡(NIC)
- PowerEdge RAID控制器(PERC)
- 电源装置 (PSU)
- 底板

可以使用以下任一方法将固件回滚到之前安装的版本（“N-1”）：

- iDRAC Web 界面
- CMC Web 界面
- RACADM CLI — iDRAC 和 CMC
- 生命周期控制器 GUI
- 生命周期控制器远程服务

您可以对 iDRAC 或生命周期控制器支持的任何设备的固件进行回滚（即使之前使用其他接口对固件进行了升级）。例如，如果使用生命周期控制器 GUI 对固件进行了升级，则可以使用 iDRAC Web 界面回滚该固件。您可以通过一次系统重新启动，对多台设备执行固件回滚。

在具有单个 iDRAC 和生命周期控制器固件的第 14 和 15 代 PowerEdge 服务器上，回滚 iDRAC 固件也会回滚生命周期控制器固件。

5.4 硬件维修后恢复服务器配置

修正服务事件是任何 IT 运营的关键部分。满足恢复时间目标和恢复点目标的能力直接影响解决方案的安全性。恢复服务器配置和固件可确保自动满足服务器运营的安全策略。

PowerEdge 服务器提供的功能可在以下情况下快速恢复服务器配置：

- 单个部件更换
- 主板更换（完整的服务器配置文件备份与恢复）
- 主板更换 (Easy Restore)

5.4.1 部件更换

iDRAC 可自动保存网卡、RAID 控制器和电源装置 (PSU) 的固件映像和配置设置。在对这些部件进行现场更换时，iDRAC 会自动检测新卡，并将固件和配置恢复到已更换的卡上。此功能可节省关键时间并确保一致的配置和安全策略。更换受支持的部件后，系统重新启动时将自动进行更新。

5.4.2 Easy Restore（适用于主板更换）

更换主板可能非常耗时并且会影响工作效率。iDRAC 能够备份和恢复 PowerEdge 服务器的配置和固件，以更大限度减少更换故障主板所需的工作量。

PowerEdge 服务器可通过以下两种方式进行备份和恢复：

1. PowerEdge 服务器会自动将系统配置设置（BIOS、iDRAC、NIC）、服务编号、UEFI 诊断应用程序和其他许可的数据备份到闪存。

   更换服务器上的主板后，Easy Restore 将提示您自动恢复此数据。

2. 要进行更全面的备份，用户可以备份系统配置，包括各种组件（如 BIOS、RAID、NIC、iDRAC、生命周期控制器和网络子卡 (NDC)）上安装的固件映像以及这些组件的配置设置。备份操作还包括硬盘配置数据、主板和更换部件。备份会创建一个文件，您可以将其保存到 vFlash SD 卡或网络共享（CIFS、NFS、HTTP 或 HTTPS）中。

   用户可以随时恢复此配置文件备份。Dell EMC 建议您对您认为可能要在某个时刻恢复的每个系统配置文件执行备份操作。

5.5 系统擦除

在系统的生命周期结束时，它需要淘汰或者重新调整用途。系统擦除的目标是从服务器存储设备和服务器非易失性存储中擦除敏感数据和设置（如高速缓存和日志），以避免机密信息无意中泄露。它是生命周期控制器中的一个应用工具，用于擦除日志、配置数据、存储数据、缓存和任何嵌入式应用程序。

通过使用系统擦除功能，可以擦除以下设备、配置设置和应用程序：

- iDRAC 重置为默认值
- 生命周期控制器 (LC) 数据
- BIOS
- 嵌入式诊断和操作系统驱动程序包
- iSM
- SupportAssist Collection 报告

此外，还可以擦除以下组件：

- 硬件高速缓存（清除 PERC NVCache）
- vFlash SD 卡（将卡初始化）（注：15G 或更高版本的服务器上不提供 vFlash。）

以下组件上的数据通过系统擦除进行了加密处理，如下所述：

- SED（自加密驱动器）
- 仅 ISE 驱动器（即时安全擦除驱动器）
- NVM 设备（Apache Pass、NVDIMM）

此外，还可以使用数据覆盖来擦除非 ISE SATA 硬盘。

请注意，即时安全擦除 (ISE) 会销毁第 14 和 15 代驱动器中使用的内部加密密钥，从而导致用户数据不可恢复。ISE 是 NIST Special Publication 800-88“介质清除指南”中提到的一种公认的存储驱动器数据清除方法。

新的 ISE 系统擦除功能的优势如下：

- **速度**：比 DoD 5220.22-M 等数据覆盖技术的速度快得多（几秒，而不是数小时）
- **有效性**：ISE 会导致驱动器上的所有数据（包括保留区块）完全无法读取
- **更高 TCO**：存储设备可重用，而不是被粉碎或以其他方式物理销毁

可通过以下方法执行系统擦除：

- 生命周期控制器 GUI (F10)
- RACADM CLI
- Redfish

5.6 iDRAC9 密码选择

可以使用密码套件来限制网页浏览器可用于与 iDRAC 通信的密码。另外，它还可以确定连接的安全程度。可通过 iDRAC Web 界面、RACADM 和 Redfish 来配置这些设置。此功能可跨多个 iDRAC 版本使用 — iDRAC7、iDRAC8（2.60.60.60 及更高）以及当前的 iDRAC9（3.30.30.30 及更高）。

5.7 CNSA 支持

下面的屏幕快照图像显示了 iDRAC9 中可用的受支持的 TLS1.2 位和 256 位加密密码。可用的密码包括 CNSA 批准的密码集里的密码。

```
pported Server Cipher(s):
erred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
pted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
pted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
pted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
pted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
pted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
pted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
```

5.8 完整电源周期

在完整电源周期中，服务器及其所有组件都将重新启动。它将耗尽服务器和所有组件的主电源和辅助电源。易失性内存中的所有数据也会被擦除。

物理完整电源周期需要拔掉交流电源线，等待 30 秒，然后再重新插入线缆。这给远程系统工作带来了挑战。14G 和 15G 服务器中的一项新功能允许您从 iSM、iDRAC GUI、BIOS 或脚本执行有效的完整电源周期。完整电源周期将在下一个电源周期时生效。

完整电源周期功能无需任何人亲临数据中心，因此缩短了故障处理时间。例如，它可以消除任何仍驻留在内存中的恶意软件。

6.摘要

确保数据中心的安全是业务成功的首要条件，而确保底层服务器基础架构的安全也至关重要。网络攻击可能会导致系统和业务停机时间延长、收入和客户损失、法律损害和企业声誉受损。要防范、检测针对硬件的网络攻击并从中恢复，需要将安全性构建到服务器硬件设计中，而不是在事后添加。

在过去的两代 PowerEdge 服务器中，Dell EMC 一直致力于利用基于硅的安全性来保护 PowerEdge 服务器中的固件和敏感的用户数据。第 14 和 15 代 PowerEdge 产品系列具有增强的网络弹性体系结构，该体系结构利用基于硅的信任根来进一步强化服务器安全性，包括以下功能：

- **经过加密验证的可信启动**，可确保端到端服务器安全性和总体数据中心安全性。它包括基于硅的信任根、数字签名固件和自动 BIOS 恢复等功能
- **安全启动**，可在操作系统运行之前，检查 UEFI 驱动程序和加载的其他代码的加密签名。
- **iDRAC 凭证存储区**，是凭证、证书和其他敏感数据的一个安全存储空间，使用每台服务器特有的基于硅的密钥进行加密
- **动态系统锁定**，是 PowerEdge 特有的功能，可帮助保护任何系统配置和固件免遭恶意或无意的更改，同时在出现任何试图更改系统的行为时提醒用户
- **企业密钥管理**，提供了一个中央密钥管理解决方案，以管理整个组织的静态数据。
- **系统擦除**，通过安全、快速地擦除存储驱动器和其他嵌入式非易失性内存中的数据，用户可以轻松地停用或重新利用第 14 和 15 代 PowerEdge 服务器
- **供应链安全性**，可确保在向客户运送产品之前产品没有遭篡改，也没有假冒组件，从而提供供应链保障。

总之，第 14 和 15 代 PowerEdge 服务器具有业界卓越的安全性，为 IT 转型奠定了值得信赖的基础，客户将在此基础上安全地运行其 IT 业务和工作负载。

A. 附录：延伸阅读

安全白皮书及附属文件

- （直接来自开发人员）PowerEdge 服务器上的系统擦除
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- 使用系统擦除功能保护第 14 代 Dell EMC PowerEdge 服务器
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- （直接来自开发人员）服务器设计中的安全性
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- （直接来自开发人员）网络弹性始于芯片组和 BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- 出厂默认 iDRAC9 密码
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- Dell EMC iDRAC 对 CVE-2017-1000251“BlueBorne”的响应
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- （视频）使用 RACADM 进行安全启动配置和证书管理
  https://youtu.be/mrIIN4X380c
- Dell EMC PowerEdge 服务器上的安全启动管理
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- 在第 14 和 15 代以及更高版本的 Dell EMC PowerEdge 服务器上为安全启动功能进行 UEFI 映像签名
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- 操作系统快速恢复
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- 管理第 14 代 (14G) Dell EMC PowerEdge 服务器上的 iDRAC9 事件警报
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFI 安全启动自定义
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

PowerEdge 白皮书

- iDRAC 概述
  http://www.DellTechCenter.com/iDRAC
- OpenManage 控制台概述
  http://www.DellTechCenter.com/OME
- OpenManage Mobile 概述
  http://www.DellTechCenter.com/OMM
- 生命周期控制器部件更换
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- 主板更换
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC 自动证书注册
  https://www.dellemc.com/resources/zh-cn/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- 使用 SELinux 改进了 iDRAC9 中的服务器安全功能
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 密码选择 — 提高了 Dell EMC PowerEdge 服务器的安全性
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

了解有关 PowerEdge 服务器的详细信息

详细了解我们的 PowerEdge 服务器

详细了解 我们的系统管理解决方案

搜索我们的资源库

关注 Twitter 上的 PowerEdge 服务器

联系 Dell Technologies 销售或支持专家

DELL Technologies