



## PowerEdge 服务器的 完全访问管理

### 借助 Dell EMC PowerEdge 产品组合实现现代化

Integrated Dell Remote Access Controller (iDRAC) 提供高级、免代理的本地和远程服务器管理。iDRAC 提供安全的方法来自动执行大量管理任务。由于每台 PowerEdge 服务器都嵌入了 iDRAC，因此无需安装其他软件。启用 iDRAC 后，您将拥有一整套服务器管理功能，随时可供您使用。

### 管理更多任务

通过在 PowerEdge 产品组合中使用 iDRAC，您可以在整个产品组合中应用相同的 IT 管理技术和工具。这个统一的管理平台支持随着组织基础架构需求的增长轻松扩展 PowerEdge 服务器。借助 iDRAC RESTful API，iDRAC 可实现对 Redfish 标准的支持，还可通过 Dell EMC 扩展程序对其进行增强，从而优化大规模管理。利用这一整套 OpenManage 系统管理工具产品组合，每位客户都可以为其环境量身定制一款经济实惠而又高效的解决方案。该产品组合包括利用 iDRAC 来简化管理的工具、控制台和集成。通过将覆盖范围扩展到更多服务器，您可以提高工作效率并降低组织成本。

### 智能自动化

iDRAC 的免代理管理可让您控制起来得心应手。在 PowerEdge 服务器开机和联网后，无论您是本地访问还是通过网络远程访问服务器，都可以对该系统进行监视和全面托管。实际上，由于 iDRAC 是免代理的，因此您可以监视、管理、更新、修复 Dell EMC 服务器，并对其进行故障处理。iDRAC 提供零接触部署和配置、组管理器以及系统锁定等功能，旨在使服务器管理变得简单高效。如果您已经拥有利用带内管理的现有管理平台，Dell EMC 将提供 iDRAC 服务模块，这是一项轻量级服务，可与 iDRAC 和主机操作系统进行交互，以支持传统管理平台。

### 安全的本地和远程管理

无论是通过已更新的 eHTML5 Web 界面、命令行界面还是一组强大的 API（如 iDRAC RESTful API）来使用 iDRAC，安全性都能得到保障。SELinux 和可配置的选项（如 HTTPS、TLS 1.2、智能卡身份验证、LDAP 和 Active Directory 集成）可在您的工作环境中提供安全保护。通过提供对远程服务器的安全访问权限，您可以执行关键管理功能，同时保持数据的完整性和安全性。其他的 iDRAC 安全功能包括：

- iDRAC 允许您通过系统锁定模式使您的系统免受不必要的配置更改。
- 除了 TLS 1.2 和 256 位加密强度之外，iDRAC Cipher Select 还为通信提供了更精细的密码控制。
- iDRAC 固件配有默认安全证书，该证书可以自动替换为受信任的证书。

## 利用遥测数据

借助全新的 iDRAC9 Datacenter 许可证, 您可以使用超过 180 个独特的监视指标来启用硬件指标的遥测流式传输, 以进行高级分析。这项全新的 iDRAC9 数据流功能与轮询方法相比, 其效率提升高达 10000 倍, 并且可以轻松集成到热门的分析解决方案 (如 Splunk 和 ELK 堆栈) 中。<sup>1</sup> 通过访问此高价值数据, 您可以对基础架构进行深入分析并提高运营效率。遥测流式传输可用于系统自定义、优化、风险管理和预测性分析。

iDRAC9 特性和优点	
网站特色	利益
遥测流式传输	对服务器遥测 (包括 CPU、GPU、SFP IO、电源、散热存储、网络、内存等) 进行深入分析。需要 iDRAC9 Datacenter 许可证。
散热管理	在机架和服务器级别定制散热和通风管理。需要 iDRAC9 Datacenter 许可证。
自动证书注册	使用受信任的 CA 证书自动注册 SSL 证书和续订 iDRAC 自签名证书。需要 iDRAC9 Datacenter 许可证。
零接触部署和配置	在 PowerEdge 服务器首次连接到网络时自动对其进行配置。此过程使用服务器配置文件来设置硬件、更新固件和安装操作系统。需要 iDRAC9 Enterprise 或 Datacenter 许可证。
虚拟剪贴板	在 HTML5 vConsole 中提供易于输入的复杂密码等内容。用户可以将文本/密码复制到本地剪贴板, 然后粘贴到远程控制台视图中。需要 iDRAC9 Datacenter 许可证。
连接视图	iDRAC 向外部交换机发送标准 LLDP 数据包, 从而提供在网络上发现 iDRAC 的选项。iDRAC 向出站网络发送两种类型的 LLDP 数据包: 拓扑数据包和发现数据包。此外, iDRAC 还可以显示交换机和端口信息。
系统锁定	在对选定的网卡使用戴耳工具甚至是供应商工具时, 有助于防止对服务器进行配置或固件更改。需要 iDRAC Enterprise 或 Datacenter 许可证。
RSA SecurID 2FA	将 RSA SecurID 客户端软件添加到 iDRAC 中, 以提供对 RSA 2FA 解决方案的原生支持。需要 Datacenter 许可证。
DRAC RESTful API	借助此 API, iDRAC 可实现对 Redfish 标准的支持, 还可通过戴耳扩展程序进行优化。
Cipher Select	Cipher Select 是一种高级用户设置, 用户可以在其中选择阻止由 iDRAC 协商的不需要的密码, 从而提高安全性。
Secured Component Verification	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。
系统擦除	通过正确的身份验证, 管理员可以安全地擦除本地存储 (硬盘、SSD、NVMe) 中的数据。
iDRAC Direct	可使用与 iDRAC Web 界面相连的安全前置 USB 端口, 无需使用“急救车”或前往数据中心的热通道。您可使用同一端口插入 USB 闪存盘, 以便上传新的系统配置文件, 确保安全、快速地进行系统配置。

要查看功能和许可证的完整列表, 请参阅 [iDRAC 用户指南](#)

<sup>1</sup> 基于 Dell EMC 委托 The Tolly Group 进行的调查报告, “iDRAC 遥测流式传输: 评估全新 iDRAC9 v4.0 中的遥测流式传输的性能和效率”, 2020 年 2 月。实际结果可能有所不同。  
完整报告: <https://reports.tolly.com/DocDetail.aspx?DocNumber=220101>。

## 了解有关 PowerEdge 服务器的详细信息



详细了解 Dell EMC OpenManage Secure Enterprise Key Management



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