DELL Technologies

APEX Data Storage Services — 安全性最佳实践

戴尔公司安全性与弹性组织 • 版本 1.1 • 上次更新时间：2022 年 8 月 18 日

执行摘要

IT 组织在技术转型之旅中仍面临种种挑战，例如：

- 过量配置/配置不足
- 资本预算制约
- 冗长的采购周期
- 复杂的基础架构迁移
- 快节奏的技术变革
- 有限的 IT 人力资源和技能

IT 领导者正在寻求一种更简易、更敏捷的体验。APEX Data Storage Services 是一种以 “即服务” 形式提供的可扩展且富有弹性的存储资源产品组合，专为运营支出模式而设计。[1] 此产品/服务通过减少过量配置和配置不足的情况以及缩短复杂的采购和迁移周期，支持您进行优化，以确保简易性。您可以通过单个界面 — APEX Console — 轻松管理您的 “即服务” 体验。

本白皮书借鉴了安全开发战略，这些战略是戴尔设计和开发应用程序和计划的基础。本白皮书重点介绍本地 APEX Data Storage Services 部署方案。

本白皮书将探讨：

1. 组织应考虑的安全风险。
2. 通过 “共同责任矩阵” 明确与保护信息相关的责任。
3. APEX Data Storage Services 安全性战略和措施如何保护数据的安全性和完整性。

APEX Data Storage Services 安全性注意事项

若要将第三方基础架构集成到数据中心环境，组织务必要考虑由此可能会引发哪些风险。对于当前正在使用或计划使用以 “即服务” 模式交付的存储的组织而言，一些关键的安全考虑因素包括：

- **安全性治理：**安全性治理至关重要，因为它划分了服务提供商与客户各自的责任。戴尔拥有自己的安全性治理机制，这些机制对应于多个重要的行业框架和控制。在本文档后面的 “安全性和合规性” 部分可以找到这些信息。
- **数据保护注意事项：**将高度敏感的数据和信息存储在第三方存储系统上会给客户带来额外的风险。敏感数据的泄露可能导致有形和无形的损失（例如商业声誉），这可能对组织的盈利能力产生直接影响，也可能导致潜在的监管问题。因此，“即服务” 客户需要有保障的数据保护，包括但不限于确认服务提供商已实施风险缓解控制措施。
- **法律/合规性：**正在考虑采用私有或公有存储服务的组织，应确保了解与通过存储提供商存储的数据类型相关的法律含义。除此之外，适用法律（例如 GDPR 和 CCPA）以及所存储数据的敏感性也可能对与您的数据存储方法相关的隐含风险产生重大影响。

[1] 运营支出模式受客户内部会计审查和政策的制约。

戴尔将要缓解的风险与服务产品和支持基础架构的安全性相关联。客户则应负责管理与云端数据、系统和应用程序的运行有关的风险。

客户和戴尔在 APEX Data Storage Services 方面的责任

除了戴尔管理的数据块和文件服务选项，客户现在还拥有灵活性和控制权，可以选择由谁来执行日常管理操作。借助戴尔管理，您可以保持对工作负载和应用程序的操作控制，而由戴尔负责管理和维护本地基础架构。或者，寻求对 “即服务” 体验拥有更多控制权的 IT 组织可以选择 “客户管理” 选项，该选项旨在让您能够掌控监视容量利用率、基础架构管理和资源优化等任务。

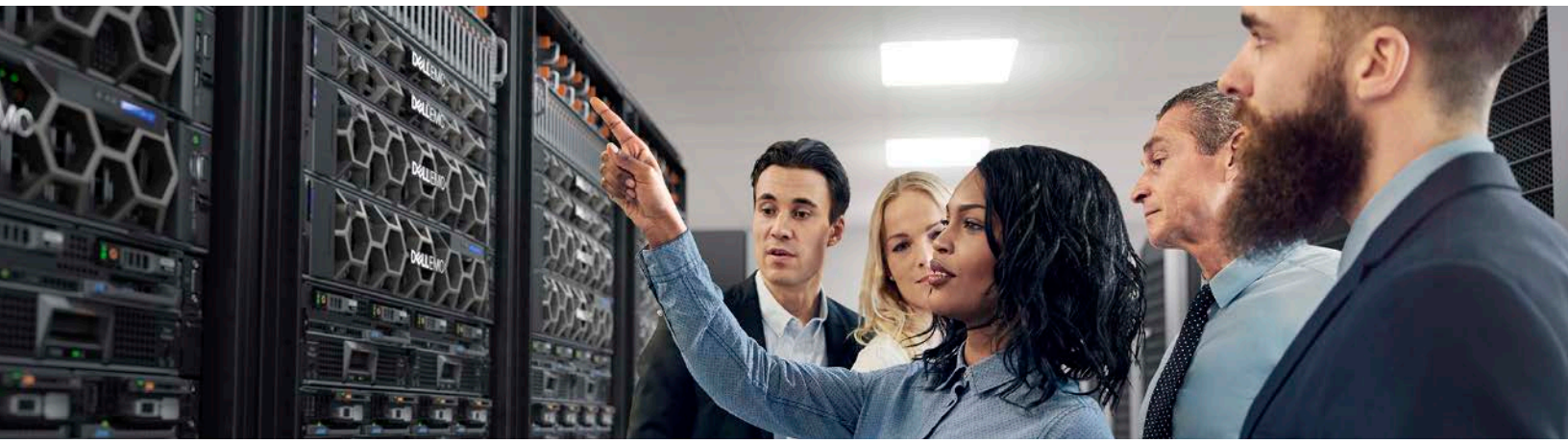
我们制定了一种共同责任模式，该模式按功能清晰地划分了客户与戴尔各自的角色，以及共同责任级别。它强调了一种应用程序交付战略，依据此战略，客户团队可以专注于日常运营，而不必担心用于服务的底层基础架构。

有关角色和职责的详细信息，请查看此处的文档：
https://www.dell.com/support/home/zh-cn/product-support/product/apex-data-storage-service/docs

类别	服务活动	客户管理		戴尔管理	
		客户	戴尔	客户	戴尔
部署	电源、空间、HVAC、访问客户数据和管理网络*	✓		✓	
	远程连接 — 提供对遥测数据的访问以监视使用情况和运行状况*	✓	✓	✓	✓
	安装和初始资源调配		✓		✓
监视	系统性能、容量和可用性	✓			✓
	配置更改以维持性能和正常运行时间承诺	✓			✓
运营	实施固件和系统软件更新（系统维护）**	✓			✓
	定义和维护数据保护、同步和快照策略	✓		✓	
	管理数据访问 — 卷、NFS 导出和 SMB 共享	✓		✓	
优化	性能和配置建议	✓			✓
	主动容量扩展和缓冲容量管理	✓			✓
支持	全天候主动硬件和系统软件支持以及现场更换部件		✓		✓
	操作方法指导		✓		✓
淘汰	与客户协调进行现场数据清理和资产回收		✓		✓

*对于戴尔管理的托管设施，戴尔对这些活动负有主要责任

**对于 “客户管理” 选项，客户负责发起半年一次的系统维护。对于 “戴尔管理” 选项，根据需要持续提供系统维护



如何保护信息

对于客户管理的解决方案，客户负责实施、维护和支持对部署到客户位置的基础架构产生影响的所有安全配置和活动，以实现安全性和合规性、访问控制、威胁和漏洞管理、数据加密和事件响应。

APEX Console

该自助式 IT 管理控制台可降低复杂性，让您能够更轻松地快速识别、部署、监视和扩展解决方案，在满足业务要求的同时降低运营风险。通过控制台来降低复杂性和运营风险，这种做法提供了一种简单而安全的服务管理方式。

安全性和合规性

APEX Data Storage Services 在既有框架中利用各种策略和战略来保护戴尔和客户数据。这可以帮助客户满足他们自己的合规性计划要求。 在适用的情况下，戴尔的应用程序和产品开发会利用与这些既有框架和法规之间的对应关系，帮助确保在开发生命周期中体现相应的安全性原则和要求。在 CCM、ISO 和 NIST 标准、法规和控制框架的启发之下，制定了保护 APEX 的安全措施以确保安全保障。

- 面向联邦信息系统和组织的 NIST 安全性和隐私控制
- ISO 27000 信息安全性管理系统
- CCM 云控制矩阵

访问控制

对于 APEX Data Storage Services 底层基础架构中存储的信息，必须采取保护措施，以防止未经授权的访问、披露和修改。以下访问控制实践有助于维护数据访问的安全性：

- 充分考虑业务案例，以实现更高级别的保障
- 身份信任验证和信息处理互操作性（例如 SSO）
- 通过权限和辅助功能，支持客户基于针对访问数据和会话的身份验证、授权和记帐 (AAA) 规则实现控制

威胁和漏洞管理

APEX Data Storage Services 支持威胁和漏洞管理战略，以确保基础架构受到保护，免遭已识别的风险和漏洞的影响。这些威胁和漏洞管理战略源自戴尔安全开发生命周期中使用的方法，包括：

1. 在修补底层基础架构时保持一致性，以确保实施最新和经过更新的功能及安全缺陷修复。戴尔使用一种规范的方法扫描 APEX Data Storage Services 的底层基础架构。
2. 将识别安全风险/漏洞的方法部署为 APEX 数据存储系统的组件。这些方法包括安全扫描和安全测试。

注意：客户有责任确保连接到 APEX Data Storage Services 基础架构的应用程序得到一致的管理和更新，以防止它们被用作攻击载体。

加密

APEX Data Storage Services 能够使用根据 NIST 特别出版物 800-131Ar2 定义的经 NIST 批准的算法对数据进行加密。NIST 加密算法定义了加密算法的使用和密钥长度。以下是为了保护资产和信息，戴尔在考虑公钥基础架构时所依据的标准：

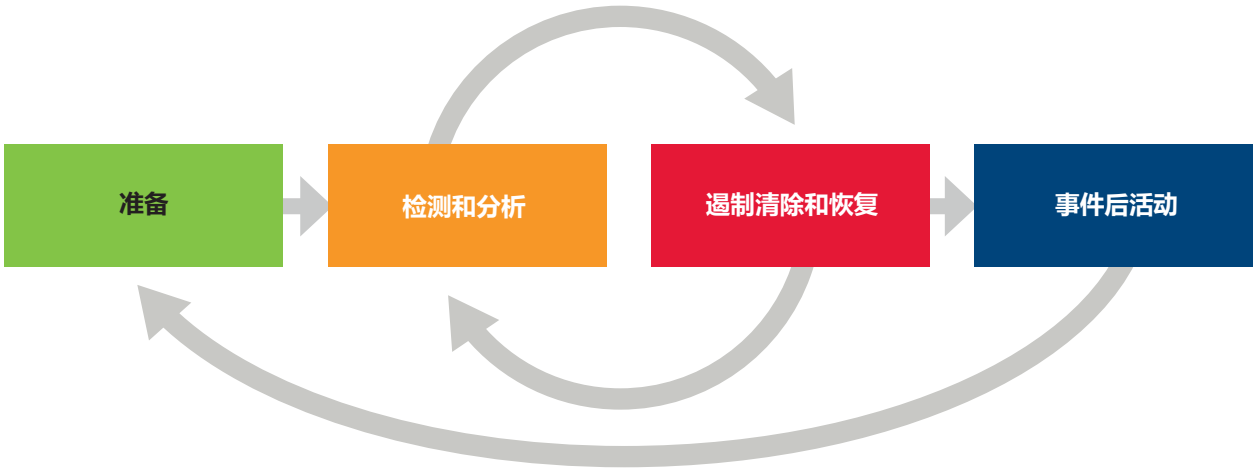
- 已弃用的加密算法默认处于禁用状态
- 在传输期间和静态条件下被归类为敏感数据的数据可以并且应该进行加密
- 对称密钥的密钥长度不得少于 256 位
- 对于非对称密钥，RSA 和 DSA 算法的密钥长度不得少于 2048 位，对于椭圆曲线 (EC) 算法，则不得少于 256 位
- 对于所有应用程序，必须将 TRIPLE DES (3DES) 增强为 AES 256 位基线

事件响应

戴尔依据记录的报告和管理方法处理安全事故和事件。此流程确保在必要时及时通知客户，并采取适当的步骤解决事件。

戴尔遵循以下事件响应流程：

- 准备
- 检测/分析
- 遏制/清除
- 恢复



• 报告

系统审核和问责制

APEX Data Storage Services 利用合规性和保障流程，持续评估平台上保护数据和信息的安全控制措施的有效性。其中包括定期审核和评估，以识别和修正不合规的情况。

由戴尔进行独立审查和评估，以确保 APEX 符合既定的行业政策和标准。APEX 建立在云安全联盟的 CCM 等既定框架之上。

评估包括以下内容：

- 主机评估
- Web 应用程序评估
- Web 服务评估
- 移动评估
- 二进制评估（如果适用）

安全连接网关

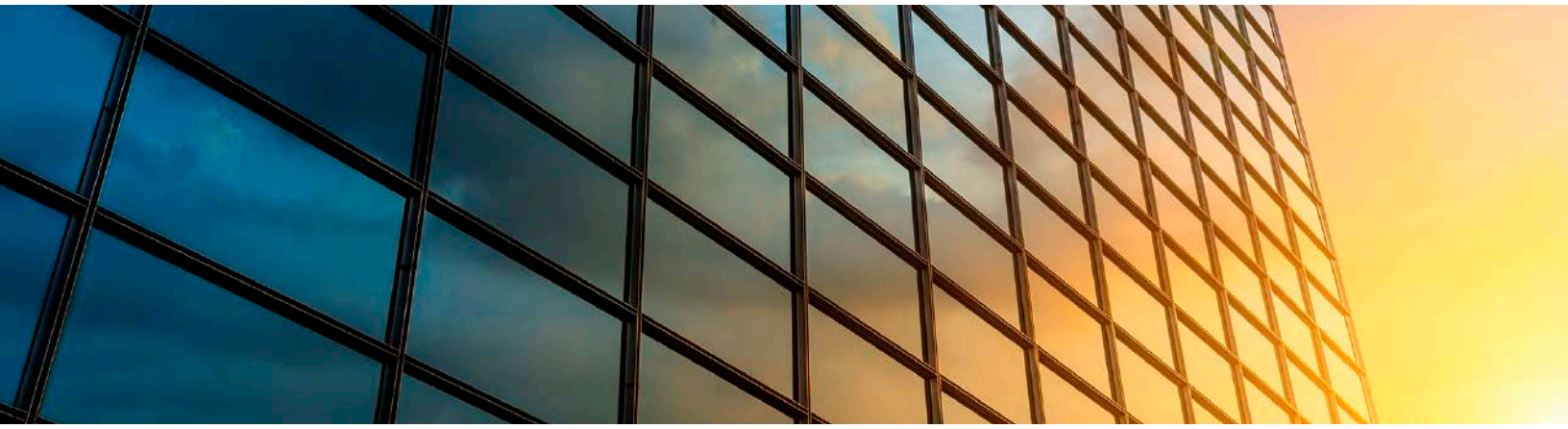
安全连接网关是 APEX Data Storage Services 与客户基础架构之间的安全双向连接。建立安全连接网关工具将创建安全的数据传输，并且仅供授权用户/设备使用。此解决方案可主动监控运行状况并预防问题。

客户负责维护用户及其相应的属性，并在自己的基础架构中建立连接。戴尔将负责管理支持通信的支持服务器和网络。这些服务需要戴尔和客户采用高度安全的协议来进行所有通信。戴尔还将在部署期间提供配置指南。

总结

APEX Data Storage Services 作为一款强大的 “存储即服务” 解决方案，将成为您转型之旅的推动因素，助力您挖掘和扩大存储需求。戴尔致力于为 APEX Data Storage Services 基础架构内的数据收集、通信、传输、使用和存储提供可靠、私密和安全的体验，让客户放心无忧。

有关 APEX Data Storage Services 的更多信息，请访问 Dell.com/APEX-Storage



术语表

术语定义

APEX	APEX 是 Dell Technologies 的 “即服务” 解决方案产品组合，可通过提高 IT 敏捷性和可控性来简化数字化转型。
NIST	美国国家标准与技术研究院
EC	椭圆曲线
RSA	Rivest–Shamir–Adleman
AAA	身份验证、授权和记帐
CCM	云控制矩阵
DSA	数字签名算法
SSO	单点登录
OpEx	运营支出
GDPR	通用数据保护条例
CCPA	加利福尼亚州消费者隐私法案
AICPA	美国注册会计师协会
PCI DSS	支付卡行业数据安全标准
CSP	云服务提供商