产品规格

ONTAP 9 中的安全性功能

保护全世界最重要的资源：数据

主要优势

增强数据的机密性、完整性和可用性
使用 ONTAP Data Fabric 的安全性功能保护企业最重要的资源：数据。

加强企业的安全防护
为企业的 Data Fabric 建立安全根基，同时掌握打造安全基础架构的可见性功能和安全性功能。

应用 NetApp 和行业安全最佳实践
借助 NetApp 专业知识和行业知识建立一套审查严格的安全体系。

满足监管与合规性要求
使用成熟的安全最佳实践，遵守并支持行业法规和安全合规性要求。

在 NetApp® ONTAP® 数据管理软件的持续发展过程中，安全性是其不可或缺的一环。最新版本的 ONTAP 9 包含许多新的安全性功能，它们对于企业保护整个混合云中的数据以及遵循行业最佳实践具有宝贵的价值。这些新功能还支持企业向零信任 (Zero Trust) 模式转变。

要了解有关强化 ONTAP 9 解决方案的更多信息，请参见《TR-4569：NetApp ONTAP 9 安全性强化指南》。

挑战

如今，企业面临着数字化转型带来的重重压力。他们需要高效管理日益分散、瞬息万变且形态各异的数据。当今世界，安全威胁形势日益错综复杂，对 IT 环境的危险性也与日俱增。存储工程师作为数据和信息的管理员与操作者被寄予厚望，希望他们可以在数据的整个生命周期中以安全的方式管理和维护数据。

解决方案

NetApp ONTAP 9 软件对于保护数据和满足合规性要求至关重要。在为企业最重要的资源（数据）建立经行业验证的安全防护时，本产品规格以及《TR-4569：NetApp ONTAP 9 安全性强化指南》是必读内容。

NetApp®

ONTAP 9 的安全性功能

表 1 介绍了 ONTAP 9 的安全性功能。

软件或特性	功能	影响
NetApp 卷加密 (NVE)	NVE 是一套基于软件的加密机制，支持在任何类型的磁盘上加密数据，每个卷使用一个唯一密钥。	空闲数据加密仍然是行业关注的一个焦点。NVE 在满足空闲数据加密需求的同时，还在整个混合云中保持高级别的安全防护。
NVE 安全清除	此功能通过一个命令移走未受影响的文件并删除用于加密受感染文件的密钥，以加密方式粉碎 NVE 卷上被删除的文件。	即使系统处于使用中，您也可以联机修复数据泄漏。此功能还提供一流的“立即擦除”(right-to-erasure) 功能，从而满足《一般数据保护条例》(GDPR) 的要求。
NetApp 聚合加密 (NAE)	NAE 是一套基于软件的加密机制，在加密卷之间共享的每一个聚合都有唯一的密钥，因此您可以对任何类型磁盘上的数据进行加密。	与 NVE 一样，NAE 也支持空闲数据加密。由于卷在整个聚合上共享密钥，因此可以利用 NAE 对聚合进行重复数据删除，并最终提高存储效率。
默认空闲数据 (DAR) 加密	如果定义了外部密钥管理器或板载密钥管理器，则会默认启用 DAR 加密。这种情况下将使用 NVE 或 NAE 基于软件的加密。如果 NSE 驱动器属于集群配置的一部分，仍支持 DAR 加密，但默认不使用基于软件的加密。	默认 DAR 加密可简化对整个混合云中高级别安全防护的维护工作。
NetApp 存储加密 (NSE)	NSE 是 NetApp 使用 FIPS-140-2 2 级自加密驱动器实施的全磁盘加密 (Full Disk Encryption, FDE)。而且，NSE 还支持对全套 NetApp 存储效率技术进行无中断加密。	空闲数据加密仍然是行业关注的一个焦点。NSE 提供可满足这一焦点需求的 FDE。NetApp Data Fabric 维护端到端的高级别安全防护。
采用 Intel AES 新指令 (AES-NI) 加速的 SMB 加密	在支持的处理器系列中，Intel AES-NI 可改进 AES 算法并加快数据加密的速度。	加速安全性功能可提升效率。高效使用资源对提供成功的安全性解决方案至关重要。
NetApp 加密安全性模块	此模块为基于安全套接字层 (Secure Sockets Layer, SSL) 的部分管理服务提供经 FIPS 140-2 验证的加密运算。	专用安全性模块可提高资源的使用效率。此外，FIPS 140-2 也是行业认可的产品与解决方案加密标准。
NetApp CryptoMod	此模块为 NVE、NAE 和板载密钥管理器 (OKM) 提供经 FIPS 140-2 验证的加密运算。	FIPS 140-2 是行业认可的产品与解决方案加密标准。
SHA-2 (SHA-512) 支持	为增强密码的安全性，ONTAP 9 提供了对 SHA-2 密码哈希函数的支持，并默认对散列新建密码或更改后的密码使用 SHA-512。	SHA-2 因其相对 SHA-1 标准（经常被破解）更严密的安全防护，现已成为哈希函数的行业标准。
安全日志转发（基于传输层安全协议 [Transport Layer Security, TLS] 的系统日志）	通过该日志转发功能，管理员可以对目标对象或地址进行配置，以便对方接收到系统日志和审计信息。由于系统日志和审计信息对安全性要求较高，ONTAP 9 可以使用 TCP 加密参数通过 TLS 发送此类信息，以确保安全。	从支持和可用性角度来看，日志和审计信息对于企业的价值不可估量。此外，日志（系统日志）以及审计报告和输出中包含的信息在本质上通常高度敏感。为了保持安全控制和安全防护，您必须对日志和审计数据加以管理，确保安全。
TLS 1.1 和 TLS 1.2	ONTAP 9 使用 TLS 1.1 和 TLS 1.2 保证安全通信和管理功能。	NetApp 不建议使用 TLS 1.0，因为此版本存在严重的安全漏洞，不符合 PCI-DSS 等合规性标准。NetApp 强烈建议使用 TLS 1.1 和 TLS 1.2 这两个强大而完整的版本。
在线证书状态协议 (OCSP)	启用 OCSP 后，使用 TLS 通信（例如 LDAP 或 TLS）的 ONTAP 9 应用程序可以接收数字证书状态。应用程序会收到一个签名响应，指示所请求证书的状态是良好、被撤消还是未知。	OCSP 无需证书撤消列表 (Certificate Revocation List, CRL) 便可帮助确定数字证书当前的状态。
板载密钥管理器 (OKM)	ONTAP 9 中的 OKM 为空闲数据提供了独立的加密解决方案。OKM 支持与 NVE 搭配使用，NVE 是一套基于软件的加密机制，支持您在任何类型的磁盘上加密数据。OKM 也支持与 NSE 搭配使用，NSE 使用自加密驱动器进行 FDE。	OKM 为 NSE 和 NVE 提供密钥管理功能。此外，在 ONTAP 9 中使用这种加密技术可以保护空闲数据，这提供了一个关键的数据安全解决方案。
OKM 安全启动	此项安全技术要求在重启节点后使用密码解锁驱动器和解密卷。	当 NSE 和 NVE 使用 OKM 时，安全重启可防止整个存储阵列（而不仅仅是驱动器）被窃。它还支持安全搬运整个集群和安全返还设备。

表 1) 安全性功能。

软件或特性	功能	影响
外部密钥管理	在存储环境中使用第三方系统管理外部密钥。该第三方系统安全地管理存储系统中 NSE、NVE 或 NAE 等加密功能使用的身份验证密钥和加密密钥。存储系统使用 SSL 连接联系外部密钥管理服务器，以通过密钥管理互操作性协议 (KMIP) 存储和检索身份验证密钥或卷数据加密密钥。	借助外部密钥管理，您可以将自己企业的密钥管理功能集中起来，而且从本质上确认密钥并未存放在资产附近。这种方法大大降低了泄密的可能性。
多租户外部密钥管理	多租户外部密钥管理功能支持单个租户或存储虚拟机 (SVM) 通过 KMIP 为 NVE 维护自己的密钥。	借助多租户外部密钥管理，您可以将自己企业的密钥管理功能按部门或租户集中起来，而且从本质上确认密钥并未存放在资产附近。这种方法大大降低了泄密的可能性。
增强文件系统审计	ONTAP 9 提高了审计事件的数量，并扩大了解决方案报告的详细信息的覆盖范围。事件创建时将在日志中记录以下重点详细信息： • 文件 • 文件夹 • 共享访问 • 创建、修改或删除的文件 • 成功的文件读取访问 • 读取字段或写入文件的失败尝试 • 文件夹权限变更	从当今整体网络安全威胁形势来看，NAS 文件系统的涉及范围在扩大。因此，审计功能提供的可见性依然至关重要，而 ONTAP 9 中增强的审计功能提供比以往更多的 CIFS 审计详细信息。
CIFS SMB 签名和密封	通过保护存储系统和客户端之间的流量，避免重放攻击或中间人攻击，SMB 签名功能可帮助保护 Data Fabric 的安全。它还可确认 SMB 消息具有有效签名。此外，ONTAP 9 支持 SMB 加密（即密封）。	SMB 协议中有一个常见的文件系统和架构入侵载体。除了基于份额保证数据传输的安全之外，签名和密封还能实现纯粹的流量验证。
Kerberos 5 和 krb5p 支持	ONTAP 9 支持 Kerberos 128 位和 256 位 AES 加密。隐私服务包括接收数据完整性验证、用户身份验证和数据传输前加密。	Krb5p 身份验证通过使用校验和对客户端和服务器之间的所有流量进行加密，避免数据被篡改和窃听，从而达到保护目的。
轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) SMB 签名和密封	ONTAP 9 支持签名和密封功能，以保护 LDAP 服务器查询对话安全。	签名功能使用密钥技术确认 LDAP 负载数据的完整性。密封功能对 LDAP 负载数据进行加密，以避免以明文形式传输敏感信息。
安全 Shell (SSH) 中的 Ed25519 和 NIST 曲线（更新的算法和基于哈希的方法身份验证代码 [HMAC]）	ONTAP 9 提供更新的 SSH 密码和密钥交换功能，包括 AES、3DES、SHA-256 和 SHA-512。	随着网络威胁不断演变，协议算法、密码和密钥交换的强度对于协议完整性和产品功能的意义更加重大。
支持配置成功登录 SSH 前的最大尝试次数	ONTAP 9 为安全 ssh 修改命令增加了 parameter-max-authentication-retry-count 参数，用于设置最大登录尝试次数。每个 SSH 连接允许的默认最大次数为六次，不过 NetApp 从最佳安全实践的角度出发建议将此参数设置为三次。	此功能有助于防止暴力攻击。
多因素身份验证 (MFA)	为 NetApp ONTAP System Manager 和 NetApp Active IQ® Unified Manager 启用了 MFA，用于通过安全断言标记语言 (Security Assertion Markup Language, SAML) 和外部身份提供程序进行管理性网络访问。通过使用用户 ID/密码和公钥作为两个因素的本地双因素身份验证方法，可以通过管理命令行访问 ONTAP。您可以使用含公钥的 nsswitch 作为其中一个因素来实现 SSH 命令行管理访问。	管理访问凭据过于简单是大多数系统遭受威胁的原因所在。MFA 消除了使用简单密码帐户进行管理访问的可能性。

软件或特性	功能	影响
NetApp SnapLock® 技术与 NSE 和 NVE 相结合	ONTAP 9 通过 SnapLock 功能提供对 NSE 和 NVE 的支持，SnapLock 功能可用于管理和存储“一次写入，多次读取”(write once read many, WORM) 数据。	SnapLock 技术可用于创建专用卷，卷中可以存储文件，并设置为不可擦除、不可复写状态。SnapLock 可以在保持 NSE 和 NVE 解决方案的安全状态（加密）的同时，无限期地或在指定的保留期内保持这种状态。
升级映像验证	ONTAP 升级进程可在升级时验证映像是否为正版 ONTAP。	此项验证可检测出升级过程中使用的映像是否损坏或是否为伪造。
统一可扩展固件接口 (Unified Extensible Firmware Interface, UEFI) 安全启动	系统每次启动时都会进行映像验证。	启动加载程序会对签名 ONTAP 映像进行验证，从而在每次启动时防止伪造映像。
集群对等加密	集群对等加密使用 TLS 1.2 为对等集群之间通过线缆传输的所有数据进行加密，并对使用集群对等执行数据复制的底层 ONTAP 功能（NetApp SnapMirror®、SnapVault®、FlexCache®）进行加密。	需要复制数据的 ONTAP 功能特性可使用传输中数据加密。此外，使用空闲数据加密 (NVE/NSE) 的客户也可以在采用集群对等加密的 ONTAP 集群之间使用端到端加密。
基于角色的访问控制 (Role-based access control, RBAC)	管理员可以使用 ONTAP 中基于角色的访问控制 (RBAC) 将用户的管理访问限制在为其角色授予的级别。借助该功能，管理员可以根据分配给用户的角色管理用户。	访问控制是打造安全防护的根基。借助 RBAC 等功能，企业可以决定将数据访问权限赋予给谁，以及授予多大的权限。该功能有助于限制包括数据泄漏和权限升级在内的漏洞和利用机会。
Antivirus Connector（病毒扫描）	病毒扫描在运行 Antivirus Connector 和防病毒软件的 Vscan 服务器上执行。运行 ONTAP 的系统通常被配置为在客户端修改或访问文件时对文件进行扫描。	威胁和攻击途径层出不穷。因此，文件被访问或修改时对文件进行实时病毒扫描有助于保护企业文件的完整性。
登录横幅和每日消息 (MOTD) 横幅	进行身份验证之前，首先会显示登录横幅。企业和管理员可以利用这些横幅与系统用户进行沟通。	企业可以利用登录横幅将需要确认接受的系统使用条款与条件呈现给操作员、管理员乃至入侵者。这些横幅也会指明谁有权访问系统。
磁盘清理	利用磁盘清理功能，您可以从一个磁盘或一组磁盘中删除数据，使数据永远无法恢复。	安全性协议通常要求磁盘中的数据不可恢复。磁盘清理功能便为您提供了这种能力。
NetApp FPolicy™ 技术	FPolicy 是 ONTAP 的一个基础架构组件，它支持通过合作伙伴的应用程序监控和设置文件访问权限。文件策略可以根据文件类型设置。FPolicy 决定了存储系统如何处理来自独立客户端系统的操作请求，例如创建、打开、重命名和删除等。 **注意：**在 ONTAP 9 中，FPolicy 文件访问通知框架有所增强，加入了用于应对短期网络中断问题的筛选控制和故障恢复功能。	访问控制是一项关键的安全性功能。因此，对文件访问和文件操作的可见性和响应能力是维持安全防护的重要方面。ONTAP 解决方案使用 FPolicy 功能提供文件可见性和访问控制。

表 1) 安全性功能。

关于 NetApp

NetApp 是混合云数据管理领域的权威企业。我们提供一系列混合云数据服务，旨在简化云端和内部环境中的应用程序及数据管理，加速推进数字化转型。NetApp 携手合作伙伴，赋予全球企业充分释放数据的全部潜能、增加客户接触点、扶植创新和优化企业运营的能力。有关详细信息，请访问 www.netapp.com/cn。#DataDriven

全国销售热线：4008-1818-11