安全性
ONTAP 9

NetApp
February 12, 2026

目录

安全性 1
客户端身份验证和授权 1
身份验证 1
Authorization 1
使用SAML进行身份验证 2
OAuth2.0与ONTAP REST API客户端 2
管理员身份验证和 RBAC 2
身份验证 2
RBAC 2
病毒扫描 2
加密 3
NetApp 存储加密 4
NVMe 自加密驱动器 4
NetApp 聚合加密 5
NetApp 卷加密 5
WORM 存储 5

安全性

客户端身份验证和授权

ONTAP 使用标准方法来保护客户端和管理员对存储的访问，并防止病毒的侵害。高级技术可用于对空闲数据进行加密以及对 WORM 存储进行加密。

ONTAP 通过向可信源验证客户端计算机和用户的身份来对其进行身份验证。ONTAP 通过将用户凭据与文件或目录上配置的权限进行比较来授权用户访问文件或目录。

身份验证

您可以创建本地或远程用户帐户：

- 本地帐户是指帐户信息驻留在存储系统上的帐户。
- 远程帐户是指帐户信息存储在 Active Directory 域控制器， LDAP 服务器或 NIS 服务器上的帐户。

ONTAP 使用本地或外部名称服务查找主机名，用户，组，网络组和名称映射信息。ONTAP 支持以下名称服务：

- 本地用户
- DNS
- 外部 NIS 域
- 外部LDAP域

名称服务切换表 _ 用于指定搜索网络信息的源以及搜索这些源的顺序（提供 UNIX 系统上 /etc/nsswitch.conf 文件的等效功能）。当 NAS 客户端连接到 SVM 时， ONTAP 会检查指定的名称服务以获取所需的信息。

kerberos support Kerberos 是一种网络身份验证协议，可通过在客户端 - 服务器实施中加密用户密码来提供 " s强身份验证 " 。ONTAP 支持使用完整性检查的 Kerberos 5 身份验证（ krb5i ）和使用隐私检查的 Kerberos 5 身份验证（ krb5p ）。

Authorization

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估安全级别后，访问权限由有效权限决定：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

使用SAML进行身份验证

ONTAP支持使用安全断言标记语言(SAML)对远程用户进行身份验证。支持多种常见的身份提供程序(IDPs)。有关支持的IdPs的详细信息以及启用SAML身份验证的说明、请参见 "配置 SAML 身份验证"。

OAuth2.0与ONTAP REST API客户端

从ONTAP 9.14开始、可支持开放授权(OAuth2.0)框架。当客户端使用REST API访问ONTAP时、您只能使用OAuth2.0进行授权和控制访问决策。但是、您可以使用任何ONTAP管理界面(包括命令行界面、System Manager和REST API)配置和启用此功能。

标准OAuth2.0功能与多个常用授权服务器一起受支持。您可以使用基于相互TLS的受发件人限制的访问令牌进一步增强ONTAP安全性。此外、还提供了多种授权选项、包括独立范围以及与ONTAP REST角色和本地用户定义的集成。请参见 "ONTAP OAuth2.0实施概述" 有关详细信息 …

管理员身份验证和 RBAC

管理员可以使用本地或远程登录帐户向集群和 SVM 进行身份验证。基于角色的访问控制（ Role-Based Access Control ， RBAC ）可确定管理员有权访问的命令。

身份验证

您可以创建本地或远程集群和 SVM 管理员帐户：

- 本地帐户是指帐户信息，公有密钥或安全证书驻留在存储系统上的帐户。
- 远程帐户是指帐户信息存储在 Active Directory 域控制器， LDAP 服务器或 NIS 服务器上的帐户。

除了 DNS 之外， ONTAP 使用与对客户端进行身份验证相同的名称服务来对管理员帐户进行身份验证。

RBAC

分配给管理员的 *role* 用于确定管理员有权访问的命令。您可以在为管理员创建帐户时分配角色。您可以根据需要分配其他角色或定义自定义角色。

病毒扫描

您可以在存储系统上使用集成的防病毒功能，防止数据受到病毒或其他恶意代码的侵害。称为 *Vscan* 的 ONTAP 病毒扫描将同类最佳的第三方防病毒软件与 ONTAP 功能相结合，让您可以灵活地控制扫描哪些文件以及何时扫描。

存储系统将扫描操作卸载到托管第三方供应商提供的防病毒软件的外部服务器。ONTAP 防病毒连接器 _ 由 NetApp 提供并安装在外部服务器上，用于处理存储系统与防病毒软件之间的通信。

- 当客户端通过 SMB 打开，读取，重命名或关闭文件时，您可以使用 _on-access scanning-来 检查病毒。文件操作将暂停，直到外部服务器报告文件的扫描状态为止。如果文件已扫描，则 ONTAP 允许执行文件操作。否则，它将从服务器请求扫描。

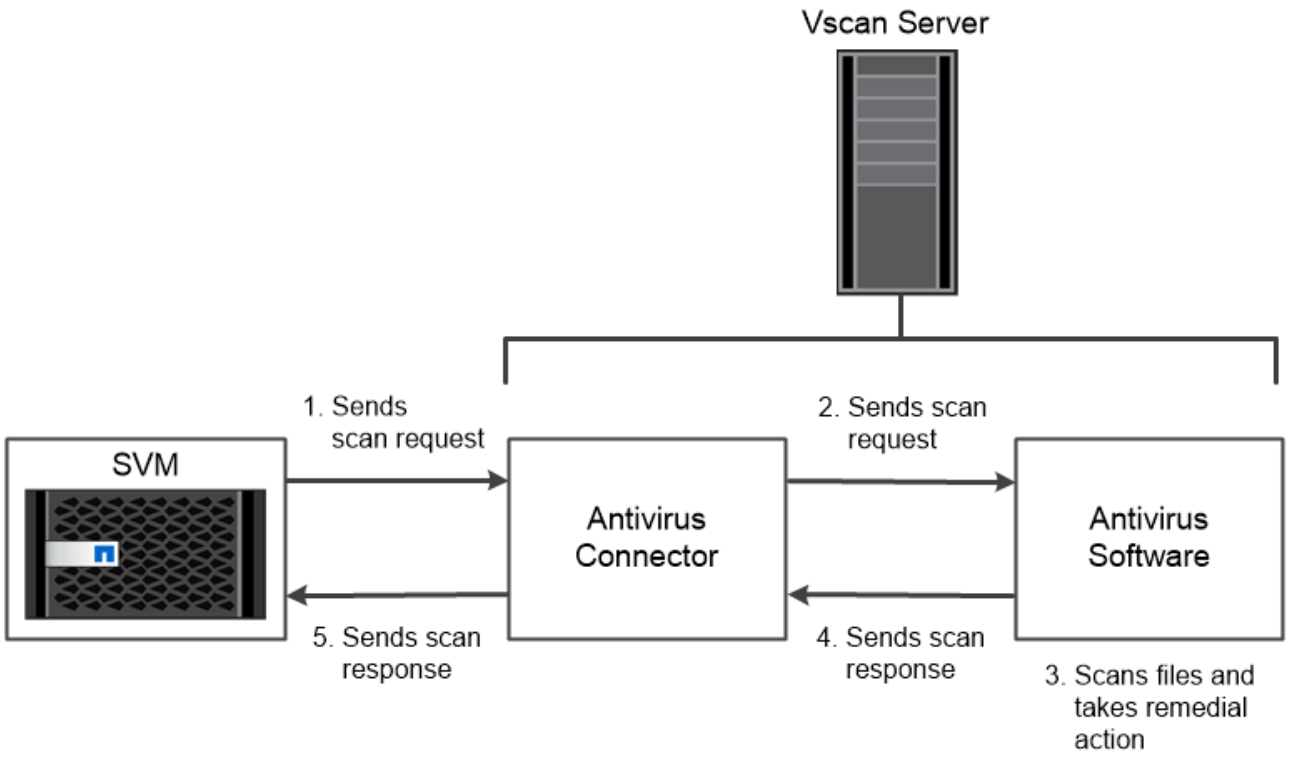
  NFS不支持实时扫描。

- 您可以使用 _on-Demand scanning-立即 或按计划检查文件中的病毒。例如，您可能只想在非高峰时段运行扫描。外部服务器会更新已检查文件的扫描状态，以便下次通过 SMB 访问这些文件时，通常会缩短这些文件的文件访问延迟（假设这些文件尚未修改）。

  您可以对 SVM 命名空间中的任何路径使用按需扫描，即使是仅通过 NFS 导出的卷也是如此。

通常，您可以在 SVM 上同时启用这两种扫描模式。在任一模式下，防病毒软件都会根据软件中的设置对受感染的文件采取补救措施。

灾难恢复和 MetroCluster 配置中的 * 病毒扫描 _* 对于灾难恢复和 MetroCluster 配置，您必须为本地集群和配对集群设置单独的 Vscan 服务器。



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

加密

ONTAP 提供了基于软件和基于硬件的加密技术，可确保在存储介质被重新利用，退回，放置在不当位置或被盗时无法读取空闲数据。

对于所有 SSL 连接， ONTAP 均符合联邦信息处理标准（ FIPS ） 140-2 的要求。您可以使用以下加密解决方案：

- 硬件解决方案：
  - NetApp 存储加密（ NSE ）

    NSE 是一种使用自加密驱动器（ SED ）的硬件解决方案。

  - NVMe SED

    ONTAP 为未获得 FIPS 140-2 认证的 NVMe SED 提供全磁盘加密。

- 软件解决方案：
  - NetApp 聚合加密（ NAE ）

    NAE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个聚合都使用唯一的密钥启用数据卷。

  - NetApp 卷加密（ NVE ）

    NVE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个卷都有一个唯一的密钥。

使用软件（ NAE 或 NVE ）和硬件（ NSE 或 NVMe SED ）加密解决方案实现空闲双加密。NAE或NVE加密不会影响存储效率。

NetApp 存储加密

NetApp 存储加密（ NetApp Storage Encryption ， NSE ）支持 SED 在写入数据时对数据进行加密。如果磁盘上未存储加密密钥，则无法读取数据。而加密密钥只能由经过身份验证的节点访问。

在发出 I/O 请求时，节点会使用从外部密钥管理服务器或板载密钥管理器检索到的身份验证密钥向 SED 进行自我身份验证：

- 外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供身份验证密钥。
- 板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。

NSE 支持自加密 HDD 和 SSD 。您可以将 NetApp 卷加密与 NSE 结合使用，对 NSE 驱动器上的数据进行双重加密。

如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

NVMe 自加密驱动器

NVMe SED不具有FIPS 140-2认证；但是、这些磁盘使用AES 256位透明磁盘加密来保护空闲数据。

数据加密操作（例如生成身份验证密钥）在内部执行。存储系统首次访问磁盘时会生成身份验证密钥。之后，磁盘将通过在每次请求数据操作时要求存储系统身份验证来保护空闲数据。

NetApp 聚合加密

NetApp 聚合加密（ NAE ）是一种基于软件的技术，用于对聚合上的所有数据进行加密。NAE 的一个优势是，卷包含在聚合级别重复数据删除中，而 NVE 卷则不包括在内。

启用 NAE 后，可以使用聚合密钥对聚合中的卷进行加密。

从ONTAP 9．7开始，如果已"NVE许可证"管理和板载密钥或外部密钥，则新创建的聚合和卷将默认进行加密。

NetApp 卷加密

NetApp 卷加密（ NVE ）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。只有存储系统可以访问的加密密钥可确保在底层设备与系统分离时无法读取卷数据。

数据(包括快照)和元数据都会进行加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。内置的板载密钥管理器可保护数据所在系统上的密钥。

您可以在任何类型的聚合（ HDD ， SSD ，混合，阵列 LUN ）上使用任何 RAID 类型以及任何受支持的 ONTAP 实施（包括 ONTAP Select ）中使用 NVE 。您还可以将 NVE 与 NetApp 存储加密（ NetApp Storage Encryption ， NSE ）结合使用，对 NSE 驱动器上的数据进行双重加密。

When to use KMIP servers 尽管使用板载密钥管理器成本较低且通常更方便，但如果满足以下任一条件，则应设置 KMIP 服务器：

- 您的加密密钥管理解决方案必须符合联邦信息处理标准（ FIPS ） 140-2 或 OASIS KMIP 标准。
- 您需要一个多集群解决方案。KMIP 服务器支持多个集群，并可集中管理加密密钥。

  KMIP 服务器支持多个集群，并可集中管理加密密钥。
- 您的企业需要将身份验证密钥存储在系统或与数据不同的位置，从而提高安全性。

  KMIP 服务器将身份验证密钥与数据分开存储。

相关信息

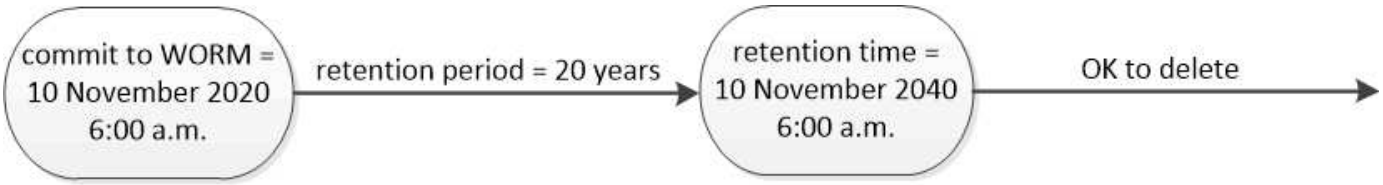
"常见问题解答—NetApp卷加密和NetApp聚合加密"

WORM 存储

WORM 是一种高性能合规解决方案，适用于使用 _write once ， read many （ SnapLock ） _ 存储以未经修改的形式保留关键文件以满足监管要求的组织。

只需一个许可证、您就可以在"严格合规性"模式下使用来满足SEC规则17a-4 (f)等外部要求、并在"宽松的企业"模式下使用SnapLock来满足内部数字资产保护法规的要求。SnapLock 使用防篡改 *ComplianceClock* 来确定 WORM 文件的保留期限何时已过。

您可以使用_WORM SnapLock for SnapVault _来保护二级存储上的快照。您可以使用 SnapMirror 将 WORM 文件复制到其他地理位置，以实现灾难恢复和其他目的。



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.