ONTAP技术报告

ONTAP Technical Reports

NetApp
February 23, 2026

目录

ONTAP技术报告

ONTAP以及应用程序和数据库技术报告

ONTAP是许多企业级应用程序和数据库技术的数据管理和数据保护基础。以下技术报告提供了针对Microsoft SQL Server、MySQL、Oracle、PostgreSQL、SAP HANA和Epic的NetApp建议实践和实施过程的指导。

Microsoft SQL Server

SQL Server是Microsoft数据平台的基础、可通过内存技术提供任务关键型性能、并加快对任何数据(无论是内部数据还是云数据)的洞察力。

"采用ONTAP的Microsoft SQL Server最佳实践"了解存储管理员和数据库管理员如何在ONTAP存储上成功部署Microsoft SQL Server。

> 本文档将取代先前发布的技术报告_TR-4590：《采用ONTAP的Microsoft SQL Server最佳实践指南》

"TR-4976：《NetApp AFF A系列和C系列系统上的虚拟化Microsoft SQL Server性能》"
了解使用NetApp AFF A系列和C系列系统的Microsoft SQL Server性能特征、以及如何根据工作负载选择合适的系统的指导。

"TR-4714：《使用SnapCenter的Microsoft SQL Server最佳实践》"
立即了解如何使用SnapCenter技术在ONTAP存储上成功部署Microsoft SQL Server以实现数据保护。

MySQL

本文档介绍了在ONTAP上部署MySQL时的配置要求、并提供了有关调整和存储配置的指导。

"基于NetApp ONTAP的MySQL数据库最佳实践"MySQL及其变体(包括MariaDB和Percona)广泛用于许多企业级应用程序。这些应用程序包括全球社交网站和大型电子商务系统、以及包含数千个数据库实例的中小企业托管系统。了解在ONTAP上部署MySQL时的配置要求以及调整和存储配置指导。

> 本文档将取代先前发布的技术报告_TR-4722：《基于NetApp ONTAP的MySQL数据库最佳实践》。_

Oracle

ONTAP专为Oracle数据库而设计。几十年来、ONTAP针对关系数据库I/O的独特需求进行了优化、并专门为满足Oracle数据库的需求而创建了多种ONTAP功能、甚至是应Oracle Inc.本身的要求也是如此。

"基于ONTAP的Oracle数据库"了解可帮助存储管理员和数据库管理员在ONTAP存储上成功部署Oracle的建议做法。

"借助ONTAP实现Oracle数据保护"了解可帮助存储管理员和数据库管理员成功备份、恢复、复制基于ONTAP存储的Oracle并提供灾难恢复的建议做法。

"借助ONTAP实现Oracle灾难恢复"了解在MetroCluster和SnapMirror业务连续性上运行Oracle数据库的建议实践、测试过程和其他注意事项。

"将Oracle数据库迁移到ONTAP存储系统"了解规划迁移策略时的整体注意事项、进行数据移动的三个不同级别、并详细介绍了一些可用的过程。

> 上述链接的文档可替代先前发布的技术报告_TR-3633：《基于ONTAP的Oracle数据库》；TR-4591：《Oracle数据保护：备份、恢复、复制》；TR-4592：《基于MetroCluster的Oracle》；以及TR-4534：《将Oracle数据库迁移到NetApp存储系统》_

"TR-4969：《基于AFF A系列和C系列的Oracle数据库性能》"
ONTAP是一款功能强大的数据管理平台、具有本机功能、包括实时数据压缩、无中断硬件升级以及从外部存储阵列导入LUN的功能。最多可以将24个节点集群在一起、通过网络文件系统(NFS)、服务器消息块(SMB)、iSCSI、光纤通道(FC)和非易失性内存高速(NVMe)协议同时提供数据。此外、Snapshot技术是创建数万个联机备份和完全正常运行的数据库克隆的基础。除了ONTAP丰富的功能集之外、还有各种各样的用户要求、包括数据库大小、性能要求和数据保护需求。了解使用AFF存储系统(包括A系列和C系列)的裸机数据库性能、并介绍这两个AFF选项的最大值和实际差异。

"TR-4971：《基于AFF A系列和C系列的虚拟化Oracle数据库性能》"
ONTAP是一款功能强大的数据管理平台、具有本机功能、包括实时数据压缩、无中断硬件升级以及从外部存储阵列导入LUN的功能。最多可以将24个节点集群在一起、通过网络文件系统(NFS)、服务器消息块(SMB)、iSCSI、光纤通道(FC)和非易失性内存高速(NVMe)协议同时提供数据。此外、Snapshot技术是创建数万个联机备份和完全正常运行的数据库克隆的基础。除了ONTAP丰富的功能集之外、还有各种各样的用户要求、包括数据库大小、性能要求和数据保护需求。了解使用AFF存储系统(包括A系列和C系列)的虚拟化数据库性能、并介绍这两个AFF选项的最大值和实际差异。

"TR-4695：《使用FabricPool进行数据库存储层化》"
了解FabricPool在各种数据库(包括Oracle关系数据库管理系统(RDBMS))中的优势和配置选项。

"TR-4899：采用SnapMirror活动同步的Oracle数据库透明应用程序故障转移" SnapMirror主动同步(以前称为SM-BC)和Oracle Real Application Cluster (RAC)可以在发生站点中断和真正灾难时提供透明的应用程序故障转移(Application Failover、TAF)和连续性。了解将SnapMirror活动同步作为Oracle RAC存储组件的AFF存储阵列的配置指导和建议实践。

"TR-4876：《采用ONTAP 解决方案 的Oracle多租户和部署最佳实践》"
了解有关如何使用ONTAP存储配置、管理和保护Oracle多租户数据库以最大程度地发挥Oracle多租户数据库和ONTAP软件功能的优势的解决方案建议实践。

PostgreSQL

PostgreSQL附带的变体包括PostgreSQL、PostgreSQL Plus和EDB Postgrers Advanced Server (ePAS)。PostgreSQL通常部署为多层应用程序的后端数据库。对于运行PostgreSQL数据库来说、NetApp ONTAP的可靠性、高性能和高效的数据管理功能是一个绝佳的选择。

"基于ONTAP最佳实践的PostgreSQL数据库"PostgreSQL附带的变体包括PostgreSQL、PostgreSQL Plus和EDB Postgrers Advanced Server (ePAS)。PostgreSQL通常部署为多层应用程序的后端数据库。它受常见中间件包(如PHP、Java、Python、Tcl/Tk、ODBC、 和JDBC)、并且一直以来都是开源数据库管理系统的常用选择。了解在ONTAP上部署PostgreSQL时的配置要求以及有关调整和存储配置的指导。

> 本文档将取代先前发布的技术报告_TR-4770：《基于ONTAP最佳实践的PostgreSQL数据库》_。

SAP HANA

"基于ONTAP的SAP HANA数据库解决方案"有关配置、管理和自动化SAP解决方案的最佳实践、请参见NetApp SAP解决方案页面。

Epic

"ONTAP上的EPIC最佳实践"此指南旨在帮助您了解在内部和云中部署Epic的最佳实践、同时满足在ONTAP上正确部署的配置标准。

本文档将取代先前发布的技术报告_TR-3923：《适用于Epic_的NetApp最佳实践》。

业务连续性技术报告

NetApp提供了广泛的解决方案、可合理调整应用程序和数据的位置、从而经济高效地提高性能。数据保护、复制和持续可用性：ONTAP数据管理可通过"一劳永逸"策略管理简化数据保护、同时通过MetroCluster和SnapMirror活动同步实现业务连续性。

这些技术报告对和产品文档进行了扩展 "ONTAP SnapMirror活动同步" "ONTAP MetroCluster" 。

SnapMirror活动同步(原SM-BC)

"TR-4878：SnapMirror活动同步" SnapMirror主动同步是一种应用程序级粒度级别的持续可用存储解决方案、可用于在AFF或全SAN阵列(ASA)存储系统上运行的ONTAP、以满足最关键业务应用程序的RPO 0和RTO 0需求。

MetroCluster

"TR-4705：《NetApp MetroCluster 解决方案 架构和设计》"
本文档简要介绍了ONTAP中MetroCluster功能的架构和设计概念。

MetroCluster IP

"TR-4689：NetApp MetroCluster IP"MetroCluster是一款持续可用的存储解决方案、适用于在FAS和AFF系统上运行的ONTAP。MetroCluster IP是采用基于以太网的后端存储网络结构的最新版本。MetroCluster IP可提供高度冗余的配置、以满足最关键的业务应用程序的需求。MetroCluster IP包含在ONTAP中、可为使用ONTAP存储的客户端和服务器提供NAS和SAN连接。

MetroCluster FC

"TR-4375：《NetApp MetroCluster FC》"MetroCluster可在不同地理位置的数据中心为任务关键型应用程序提供持续的数据可用性。了解MetroCluster FC建议的实践、设计决策和支持的配置。

ONTAP数据保护和灾难恢复技术报告

SnapMirror是一种经济高效、易于使用的跨Data Fabric统一复制解决方案。它可以通过 LAN 或 WAN 高速复制数据。在虚拟和传统环境中、您可以为业务关键型应用程序(例如Microsoft Exchange、Microsoft SQL Server和Oracle)提供高数据可用性和快速数据复制。在将数据复制到一个或多个ONTAP存储系统并持续更新二级数据时、您的数据将保持最新、并可随时使用。不需要外部复制服务器。

这些技术报告对产品文档进行了扩展"ONTAP数据保护和灾难恢复"。

SnapMirror

SnapMirror异步

"TR-4015：《SnapMirror异步配置和最佳实践》"了解配置卷、一致性组和Storage Virtual Machine的SnapMirror异步(SM-A)复制(SVM灾难恢复)的建议实践。

"TR-4678：数据保护和备份ONTAP FlexGroup卷"
了解为FlexGroup卷建议的数据保护和备份。主题包括Snapshot副本、SnapMirror以及其他数据保护和备份解决方案。

SnapMirror同步

"TR-4733：《SnapMirror同步配置和最佳实践》"了解配置SnapMirror同步(SM-S)复制的建议做法。

SnapMirror三数据中心灾难恢复

"TR-4832：《使用适用于ONTAP 9.7的NetApp SnapMirror进行三数据中心灾难恢复》"了解使用ONTAP SnapMirror技术进行复制的三数据中心灾难恢复配置。

使用SnapMirror的应用程序和基础架构

"TR-4900:《采用ONTAP的VMware Site Recovery Manager》" 自2002年将ONTAP引入现代数据中心以来、它一直是VMware vSphere环境中领先的存储解决方案、并不断增加创新功能、以简化管理、同时降低成本。了解推荐的适用于VMware Site Recovery Manager (SRM)的ONTAP 解决方案，这是VMware行业领先的灾难恢复(DR)软件，包括最新的产品信息和建议的实践，以简化部署、降低风险和简化日常管理。

ONTAP网络存储

"ONTAP网络存储"NetApp基于ONTAP的网络存储为企业提供了一个全面灵活的解决方案、用于保护其最关键的数据资产。通过利用逻辑间隙和强大的强化方法、ONTAP可帮助您创建安全、隔离的存储环境、以抵御不断演变的网络威胁。借助ONTAP、您可以确保数据的机密性、完整性和可用性、同时保持存储基础架构的灵活性和效率。

ONTAP FlexCache和FlexGroup卷技术报告

NetApp NAS解决方案可简化数据管理、帮助您在优化成本的同时跟上增长步伐。ONTAP NAS解决方案可在一个统一架构中为您提供无中断运行、经验证的效率和无缝可扩展性。由ONTAP提供支持的横向扩展NAS利用了庞大的ONTAP生态系统、具有显著的创新领先优势、并对未来积极创新有着远见。

这些技术报告对和产品文档进行了扩展 "ONTAP FlexCache卷" "ONTAP FlexGroup卷" 。

FlexCache

"TR-4743： FlexCache in ONTAP"
FlexCache是一种缓存技术、可为相同或不同ONTAP集群上的卷创建稀疏可写副本。它可以使数据和文件更靠近用户、以更快的吞吐量和更小的占用空间。了解如何使用FlexCache、建议的实践、限制以及设计和实施注意事项。

FlexCache回写

"FlexCache回写" FlexCache回写是在ONTAP 9.151中推出的一种备用操作模式、用于在缓存中写入数据。回写允许将写入提交到缓存中的稳定存储、并向客户端确认、而无需等待数据传输到源站。数据会异步转储回源站。因此、可以构建一个全球分布式文件系统、使特定工作负载和环境能够以接近本地的速度执行写入、从而显著提高性能。

FlexGroup 卷

"TR-4571a：《FlexGroup十大最佳实践》"
本技术报告是TR-4571：《NetApp ONTAP FlexGroup卷最佳实践和快速实施指南》的精简版本。

"TR-4557：《NetApp ONTAP FlexGroup卷—技术概述》"
了解FlexGroup卷、这是一种ONTAP横向扩展NAS容器、可在元数据繁重的工作负载中将近乎无限的容量与可预测的低延迟性能完美地结合在一起。

"TR-4571：《NetApp ONTAP FlexGroup卷最佳实践和实施指南》"
了解FlexGroup卷、建议的实践和实施提示。FlexGroup卷是ONTAP横向扩展NAS容器的演变、在元数据繁重的工作负载中、它将几乎无限的容量与可预测的低延迟性能完美地结合在一起。

"TR-4678：《FlexGroup卷的数据保护和备份》"
了解FlexGroup卷的数据保护和备份、包括Snapshot副本、SnapMirror以及其他数据保护和备份解决方案。

ONTAP NAS技术报告

NetApp NAS解决方案可简化数据管理、帮助您在优化成本的同时跟上增长步伐。ONTAP NAS解决方案可在一个统一架构中实现无中断运行、高效率和无缝可扩展性。由NetApp ONTAP提供支持的横向扩展NAS利用了庞大的ONTAP生态系统、具有显著的创新领先优势、并对未来积极创新有着远见。

这些技术报告对和产品文档进行了扩展 "ONTAP NAS存储管理" "ONTAP S3存储管理" 。

NFS

"TR-4067：《ONTAP中的NFS最佳实践和实施指南》"
了解ONTAP中NFS的基本概念、支持信息、配置提示和建议实践。

"TR-4962：《NFSv4.2扩展属性》"
了解如何在ONTAP 9.12.1及更高版本中启用和使用NFSv4.2扩展属性。

SMB

"TR-4740：SMB 3.0多通道"
Microsoft在SMB 3.0协议中引入了多通道、其目标是通过解决SMB1和SMB2的性能和可靠性限制来改进SMB3协议。了解ONTAP中的多通道功能、包括其功能、建议的实践和性能测试结果。

多协议

"TR-4887：《ONTAP中的多协议NAS概述和最佳实践》"
了解多协议NAS访问在ONTAP中的工作原理、以及针对多协议环境的建议实践。

ONTAP S3

"TR-4814：《ONTAP中的S3最佳实践》" 了解将Amazon Simple Storage Service (S3)与ONTAP软件结合使用的建议实践、以及将ONTAP用作本机S3应用程序的对象存储或FabricPool的分层目标的功能和配置。

名称服务

"TR-4523：《ONTAP中的DNS负载平衡》"
了解如何配置ONTAP以与DNS负载平衡方法(包括ONTAP中的DNS)结合使用、各种配置方法以及建议的实践。

"TR-4668：《名称服务最佳实践指南》"
了解在ONTAP中实施网络连接存储(Network-连接 存储、NAS)解决方案(例如、CIFS或SMB和NFS)时的建议做法、限制和注意事项。

"TR-4835：《如何在ONTAP多协议NAS身份管理中配置LDAP》"
了解如何在适用于多协议NAS的ONTAP中配置轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)身份管理。

NAS安全性

"TR-4616： ONTAP 中的 NFS Kerberos"
了解ONTAP中的NFS Kerberos、包括Active Directory和Red Hat Enterprise Linux (RHEL)客户端的配置步骤。

ONTAP网络技术报告

ONTAP提供了各种不同的网络功能和配置、可满足要求最苛刻的横向扩展应用程序的要求。利用网络功能、企业可以安全可靠地访问其数据。

这些技术报告对产品文档进行了扩展"ONTAP网络管理"。

"TR-4949：《数据中心中采用ONTAP的BGP/VIP》"
了解如何在ONTAP中快速部署基本BGP配置。

ONTAP SAN技术报告

ONTAP SAN存储可提供简化的SAN体验、为您组织的任务关键型数据库和其他SAN工作负载提供高可用性。通过与Oracle、SAP和Microsoft SQL Server数据库以及VMware和其他领先虚拟机管理程序的同类最佳数据服务集成、ONTAP SAN可以加快企业级数据库应用程序的价值实现速度。

这些技术报告对产品文档进行了扩展"ONTAP SAN存储管理"。

"TR-4080：《ONTAP中现代SAN的最佳实践》"
了解ONTAP中的块协议以及建议实践。

"TR-4684：《使用基于网络结构的NVMe (NVMe-oF)实施和配置现代SAN》"
了解如何实施和配置基于网络结构的NVMe传输(基于光纤通道的NVMe和基于TCP的NVMe)。主题包括使用NVMe协议和传输构建高度可用、高性能现代SAN解决方案的设计、实施、配置、管理准则和建议实践。

"TR-4968：《NetApp全SAN阵列数据可用性和完整性》"
了解全SAN阵列系统的各种数据保护和数据完整性功能如何工作来最大程度地延长应用程序正常运行时间、以及建议的SAN网络设计、实施和管理实践。

"现代SAN云互联闪存解决方案"
这款经验证的NetApp架构由NetApp、VMware和Broadcom联合设计和验证。它采用最新的Brocade、Emulex和VMware vSphere技术解决方案以及NetApp全闪存存储、为企业级SAN存储和数据保护设定了新标准、可带来卓越的业务价值。

安全性

ONTAP安全技术报告

ONTAP不断发展、安全性是解决方案不可或缺的一部分。最新版本的ONTAP包含许多新的安全功能、这些功能对于您的组织保护混合云中的数据、防止勒索软件攻击以及遵守行业建议的实践至关重要。这些新功能还支持您的组织向零信任模式过渡。

这些技术报告对产品文档进行了扩展"ONTAP安全性和数据加密"。

ONTAP网络存储

"ONTAP网络存储"NetApp基于ONTAP的网络存储为企业提供了一个全面灵活的解决方案、用于保护其最关键的数据资产。通过利用逻辑间隙和强大的强化方法、ONTAP可帮助您创建安全、隔离的存储环境、以抵御不断演变的网络威胁。借助ONTAP、您可以确保数据的机密性、完整性和可用性、同时保持存储基础架构的灵活性和效率。

勒索软件

"TR-4572：《NetApp 解决方案for勒索软件》" 了解勒索软件的演变过程；以及如何使用NetApp勒索软件解决方案识别攻击、防止传播和尽快恢复。本文档中提供的指导和解决方案旨在帮助组织制定具有网络弹性的解决方案、同时满足其为信息系统机密性、完整性和可用性规定的安全目标。

"TR-4526：《使用NetApp SnapLock的兼容WORM存储》"
许多企业都依靠"一次写入、多次读取"(Write On一次 读取、Read M众多、WORM)数据存储来满足法规遵从性要求、或者只是为了在数据保护策略中增加另一层。了解如何将ONTAP中的WORM解决方案SnapLock集成到需要WORM数据存储的环境中。

零信任

"NetApp和零信任" 一直以来、零信任都是一种以网络为中心的方法、用于构建微核心和外围(MCAP)架构、以通过称为分段网关的控制来保护数据、服务、应用程序或资产。ONTAP采用以数据为中心的零信任方法、其中存储管理系统将成为保护和监控客户数据访问的分段网关。尤其是、FPolicy零信任引擎和FPolicy合作伙伴生态系统成为一个控制中心、可以详细了解正常和异常的数据访问模式、并识别内部威胁。

多因素身份验证

"TR-4647：《ONTAP最佳实践和实施指南中的多因素身份验证》"
了解ONTAP使用System Manager、Active IQ Unified Manager和ONTAP安全Shell (SSH)命令行界面身份验证为管理访问提供的多因素身份验证功能。

"TR-4717：《使用通用访问卡进行ONTAP SSH身份验证》"
了解如何配置和测试第三方SSH客户端以及ActivClient软件、以便在ONTAP中配置ONTAP存储管理员时、通过通用访问卡(CAC)上存储的公共密钥对其进行身份验证。

多租户

"TR-4160：《ONTAP中的安全多租户》"

了解如何在ONTAP中使用Storage VM实施安全多租户、包括设计注意事项和建议的实践。

标准

"TR-4401：PCI-DSS 4.0和ONTAP"
了解如何根据PCI DSS 4.0标准验证系统并满足适用于NetApp ONTAP系统的控制要求。

基于属性的访问控制

"使用ONTAP进行基于属性的访问控制"了解如何配置NFSv4.2安全标签和扩展属性(xattrs)以支持基于角色的访问控制(Role-Based Access Control、RBAC)和基于属性的访问控制(ABAC)、ABAC是一种根据用户、资源和环境属性定义权限的授权策略。

针对勒索软件的NetApp解决方案

勒索软件和NetApp的保护产品组合

2024年、勒索软件仍然是导致企业业务中断的最严重威胁之一。根据 "《RSoos的Rans要索状态2024》"、勒索软件攻击影响了72%的受调查对象。勒索软件攻击已经变得更加复杂、更具针对性、威胁行为者采用人工智能等先进技术来最大限度地提高其影响和利润。

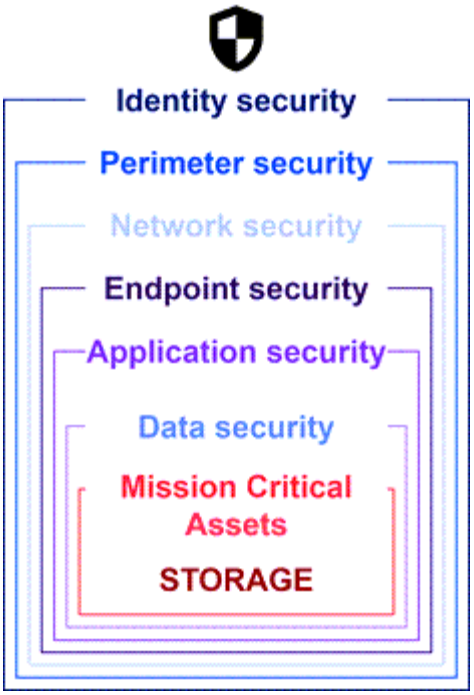
企业必须从外围、网络、身份、应用程序以及数据在存储级别的驻留位置全面审视其整个安全防护、并确保这些层的安全。在当今的威胁形势下、在存储层采用以数据为中心的网络保护方法至关重要。虽然没有一个解决方案可以抵御所有攻击、但使用合作伙伴和第三方等解决方案组合可提供分层防御。

NetApp产品组合提供了各种有效的可见性、检测和修复工具、可帮助您及早发现勒索软件、防止其蔓延、并在必要时快速恢复、以避免代价高昂的停机。传统的分层防御解决方案仍然很普遍、第三方和合作伙伴的可见性和检测解决方案也是如此。有效补救仍然是应对任何威胁的关键部分。利用不可固定的NetApp Snapshot技术和SnapLock逻辑空隙解决方案的独特行业方法是一项行业差异化优势、也是勒索软件修复功能的行业最佳实践。

> 从2024年7月开始、技术报告_TR-4572：《NetApp防兰软件保护》的内容(以前以PDF格式发布)可从docs.netapp.com上获取。

数据是主要目标

网络犯罪分子越来越多地直接将数据作为目标、认识到数据的价值。虽然外围、网络和应用程序安全非常重要、但可以绕过它们。专注于保护数据的源存储层、可提供关键的最后一道防线。勒索软件攻击的目标是访问生产数据并对其进行加密或使其无法访问。要达到这一目标、攻击者必须已经破破了当今组织部署的现有防御系统、从外围到应用程序安全。



遗憾的是、许多企业无法利用数据层的安全功能。这就是NetApp勒索软件保护产品组合的出现之处、可在最后一道防线为您提供保护。

勒索软件的实际成本

赎金本身并不是对企业的最大货币影响。虽然支付的费用不是微不足道的、但与遭受勒索软件事件的停机成本相比、它微不足道。

在处理勒索软件事件时、赎金只是恢复成本的一个要素。如果不包括支付的任何赎金、2024年、各组织报告从勒索软件攻击中恢复的平均成本为27.3亿美元、比该 "2024年：《RSoos的Rans潘 莫斯状态》"报告所报告的2023年的18.2亿美元增加了近100万美元。对于严重依赖IT可用性(例如电子商务、股票交易和医疗保健)的企业来说、成本可能会高出10倍甚至更多。

鉴于勒索软件攻击被保险公司的真实可能性、网络保险成本也持续上升。

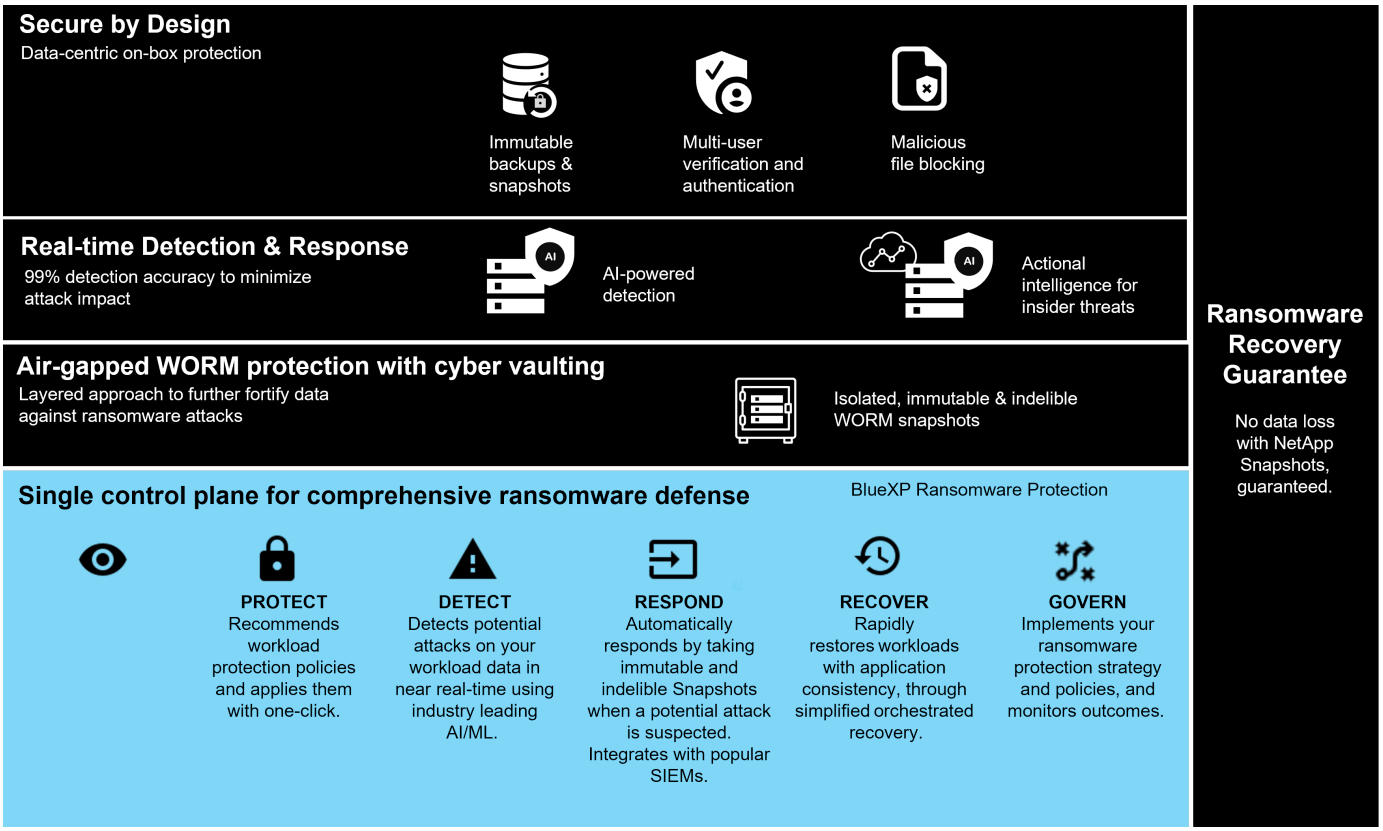
在数据层提供勒索软件保护

NetApp了解您的安全防护在整个组织中具有广泛而深入的作用、从外围到数据位于存储层的位置。您的安全堆栈非常复杂、应在技术堆栈的每个级别提供安全保护。

数据层的实时保护更加重要、并且具有独特的要求。为了有效、该层的解决方案必须提供以下关键属性：

- 设计安全，最大限度地减少攻击成功的可能性
- 实时检测和响应，最大限度地减少成功攻击的影响
- **Air-gapped WORM**保护，用于隔离关键数据备份
- *单一控制平台*实现全面的勒索软件防御

NetApp可以提供所有这些功能以及更多功能。



NetApp的勒索软件保护产品组合

NetApp"内置勒索软件保护"为您的关键数据提供实时、强大的多方面防御。其核心是由AI提供支持的高级检测算法、可持续监控数据模式、以99%的准确性快速识别潜在的勒索软件威胁。通过快速响应攻击、我们的存储可以快速创建数据快照并保护副本的安全、从而确保快速恢复。

为了进一步增强数据的安全、NetApp的"网络保险"功能可以隔离具有逻辑空隙的数据。通过保护关键数据、我们可以确保快速的业务连续性。

NetApp"NetApp勒索软件防护"通过单一控制平面智能协调和执行端到端以工作负载为中心的勒索软件防御，减轻运营负担，因此您只需单击即可识别和保护处于危险中的关键工作负载数据，准确、自动地检测和响应以限制潜在攻击的影响，并在几分钟内（而不是几天内）恢复工作负载，保护您宝贵的工作负载数据并最大限度地减少代价高昂的中断。

作为一款内置的本机ONTAP解决方案、可保护对数据的未经授权访问、它"多管理员验证(MAV)"具有一组强大的功能、可确保删除卷、创建额外管理用户或删除快照等操作只能在至少另一位指定管理员批准后才能执行。这样可以防止受到影响的管理员、恶意管理员或经验不足的管理员进行不希望的更改或删除数据。在删除快照之前、您可以根据需要配置任意数量的指定管理员批准者。

NetApp ONTAP满足了 "多因素身份验证(MFA)"System Manager中基于Web的身份验证和SSH命令行界面身份验证的要求。

NetApp的勒索软件保护功能可以让您在不断演变的威胁环境中高枕无忧。其全面的方法不仅可以抵御当前的勒索软件变体、还可以适应新出现的威胁、为您的数据基础架构提供长期的安全性。

了解其他保护选项

- "Digital Advisor勒索软件保护"

- "Data Infrastructure Insights存储工作负载安全"
- "FPolicy"
- "SnapLock和防篡改快照"

勒索软件恢复担保

NetApp保证在发生勒索软件攻击时还原快照数据。我们的保证：如果我们无法帮助您还原快照数据、我们会帮您解决问题。此担保适用于新购买的AFF A系列、AFF C系列、ASA和FAS系统。

了解更多信息。

- "恢复保证服务说明"
- "勒索软件恢复担保博客"(英文)

相关信息

- "NetApp支持站点资源页面"
- "NetApp产品安全性"

SnapLock和防篡改快照、用于勒索软件保护

SnapLock是NetApp Snap Arvanson中的一项重要武器、经验证、它在防范勒索软件威胁方面非常有效。通过防止未经授权的数据删除、SnapLock提供了额外的安全保护层、确保即使发生恶意攻击、关键数据也能保持完好并可访问。

SnapLock Compliance

SnapLock Compliance (SLC)可为您的数据提供不可替代的保护。即使管理员尝试重新初始化阵列、SLC也禁止删除数据。与其他竞争产品不同、SnapLock Compliance不容易通过这些产品的支持团队遭受社会工程黑客攻击。受SnapLock Compliance卷保护的数据在达到其到期日期之前是可恢复的。

要启用SnapLock、"ONTAP One"需要许可证。

了解更多信息。

- "SnapLock文档"

防篡改快照

防篡改Snapshot (TPS)副本提供了一种便捷快速的方法来保护数据免受恶意行为的影响。与SnapLock Compliance不同、TPS通常在主系统上使用、在主系统中、用户可以在确定的时间内保护数据、并将数据留在本地进行快速恢复、或者无需将数据复制出主系统。TPS使用SnapLock技术来防止主快照被使用相同SnapLock保留期限的ONTAP管理员删除。即使卷未启用SnapLock、也会阻止Snapshot删除、尽管快照与SnapLock Compliance卷的不可删除性质不同。

要使快照防篡改、"ONTAP One"需要许可证。

了解更多信息。

- "锁定快照以防止勒索软件攻击"(英文)

FPolicy文件阻止

FPolicy可阻止不需要的文件存储在企业级存储设备上。FPolicy还提供了一种阻止已知勒索软件文件扩展名的方法。用户仍对主文件夹拥有完全访问权限、但FPolicy不允许用户存储管理员标记为已阻止的文件。无论这些文件是MP3文件还是已知的勒索软件文件扩展名、都无关紧要。

使用**FPolicy**本机模式阻止恶意文件

NetApp FPolicy本机模式(名称"文件策略"的演变)是一个文件扩展名阻止框架、可用于阻止不需要的文件扩展名进入环境。它已成为ONTAP的一部分超过十年、在帮助您防范勒索软件方面非常有用。此零信任引擎非常有用、因为您可以获得超出访问控制列表(ACL)权限的额外安全措施。

在ONTAP系统管理器和NetApp Console中，有超过 3000 个文件扩展名的列表可供参考。

> 某些扩展在您的环境中可能是合法的、阻止它们可能会导致意外问题。在配置本机FPolicy之前、创建适合您环境的列表。

所有ONTAP许可证均包含FPolicy本机模式。

了解更多信息。

- "博客：应对网络软件：第三部分—ONTAP FPolicy、另一个功能强大的本机(也称为免费)工具"

在**FPolicy**外部模式下启用用户和实体行为分析**(UEA)**

FPolicy外部模式是一种文件活动通知和控制框架、可提供文件和用户活动的可见性。外部解决方案可以使用这些通知执行基于AI的分析以检测恶意行为。

也可以将FPolicy外部模式配置为等待FPolicy服务器批准、然后再允许执行特定活动。可以在一个集群上配置多个类似这样的策略、从而为您提供极大的灵活性。

> 如果FPolicy服务器配置为提供批准、则必须对FPolicy请求做出响应；否则、存储系统性能可能会受到负面影响。

FPolicy外部模式包括在中"所有ONTAP许可证"。

了解更多信息。

- "博客：应对异常：第四部分—采用FPolicy外部模式的UBA和ONTAP。"

Data Infrastructure Insights存储工作负载安全

存储工作负载安全 (SWS) 是NetAppData Infrastructure Insights的一项功能，可极大地增强ONTAP环境的安全态势、可恢复性和责任感。 SWS 采用以用户为中心的方法，跟踪环境中每个经过身份验证的用户的所有文件活动。它使用高级分析为每个用户建立正常和季节性的访问模式。这些模式用于快速识别可疑行为，而无需勒索软件签名。

当 SWS 检测到潜在的勒索软件或数据删除时，它可以采取自动措施，例如：

- 为受影响的卷创建快照。
- 阻止涉嫌恶意活动的用户帐户和IP地址。
- 向管理员发送警报。

由于SWS可以采取自动化操作来快速阻止内部威胁并跟踪每个文件活动、因此可以更轻松、更快速地从勒索软件事件中恢复。借助内置的高级审核和取证工具、用户可以立即查看受攻击影响的卷和文件、攻击来自哪个用户帐户以及执行了哪些恶意操作。自动快照可减少损坏并加快文件还原速度。

ONTAP的自动勒索软件保护(Autonomous Ransomware Protection、ARP)发出的警报也会显示在SWS中、从而为同时使用ARP和SWS的客户提供一个界面来防止勒索软件攻击。

了解更多信息。

- "NetAppData Infrastructure Insights"

NetApp ONTAP内置基于AI的内置检测和响应功能

随着勒索软件威胁变得越来越复杂、您的防御机制也会越来越复杂。NetApp的自主勒索软件保护(ARP)由AI提供支持、ONTAP内置智能异常检测功能。启用它可为您的网络故障恢复能力增加另一层防御。

ARP和ARP/AI可通过ONTAP内置管理界面System Manager进行配置、并按卷启用。

自主勒索软件保护(ARP)

自主勒索软件保护(ARP)是自9.10.1以来另一种内置的本机ONTAP解决方案、它关注NAS存储卷工作负载文件活动和数据熵、以自动检测潜在的勒索软件。ARP为管理员提供实时检测、洞察力和数据恢复点、实现前所未有的机载潜在勒索软件检测。

对于支持ONTAP 9的ARP.151及更早版本、ARP将从学习模式开始学习典型的工作负载数据活动。对于大多数环境、此操作可能需要七天时间。学习模式完成后、ARP将自动切换到活动模式、并开始查找可能是勒索软件的异常工作负载活动。

如果检测到异常活动、则会立即创建自动快照、这将提供一个尽可能接近攻击时间的恢复点、并且受感染数据最少。同时、系统会生成一个自动警报(可配置)、允许管理员查看异常文件活动、以便确定该活动是否确实是恶意活动并采取适当措施。

如果活动是预期工作负载、管理员可以轻松地将其标记为误报。ARP将此变化视为正常工作负载活动、不再将其标记为未来的潜在攻击。

要启用ARP、"ONTAP One"需要许可证。

了解更多信息。

- "自主勒索软件保护"

自主防兰森保护/AI (ARP/AI)

ARP/AI作为技术预览在ONTAP 9 15.1中推出、将NAS存储系统机载实时检测提升到一个新的水平。由AI提供支持的全新检测技术针对超过100万个文件和各种已知勒索软件攻击进行了训练。除了ARP中使用的信号之外、ARP/AI还会检测报头加密。AI的功率和附加信号使ARP/AI的检测精度超过99%。这已经过SE Labs的验证、SE Labs是一家独立的测试实验室、为ARP/AI提供了最高的AAA评级。

由于训练模型会在云中持续进行、因此ARP/AI不需要学习模式。它在打开时即处于活动状态。持续培训还意味着ARP/AI始终可以在新出现的勒索软件攻击类型中进行验证。ARP/AI还附带自动更新功能、可为所有客户提供新参数、以使勒索软件检测保持最新。ARP的所有其他检测、洞察和数据恢复点功能均为ARP/AI保留。

要启用ARP/AI、"ONTAP One"需要许可证。

了解更多信息。

- "博客：NetApp基于AI的实时勒索软件检测解决方案达到AAA评级"

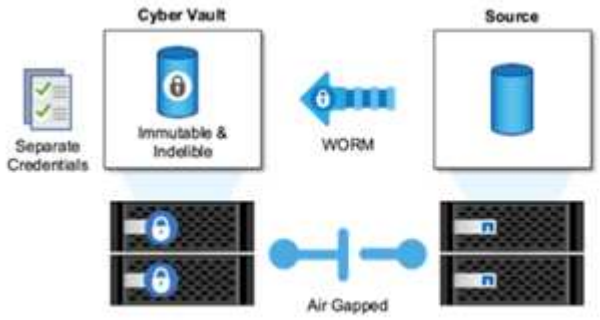
在ONTAP中通过网络存储实现无线WORM保护

NetApp的网络存储方法是一种专用参考架构、用于逻辑上隔离的网络存储。这种方法利用SnapLock等安全强化和合规性技术实现了不可变和不可删除的快照。

利用SnapLock Compliance进行网络存储、并形成合理的空隙

攻击者破坏备份副本的趋势越来越明显、在某些情况下甚至会对其进行加密。因此、网络安全行业的许多企业都建议将空隙备份作为整体网络弹性策略的一部分。

问题在于、传统的空隙(磁带和脱机介质)可以显著增加恢复时间、从而增加停机时间和整体相关成本。即使采用更现代化的方法来解决空隙问题也会有问题。例如、如果临时打开备份存储以接收新的备份副本、然后断开并关闭其与主数据的网络连接、以便再次"无线连接"、则攻击者可以利用临时打开的空间。在连接联机期间、攻击者可能会攻击以破坏或销毁数据。此类配置通常还会增加不必要的复杂性。逻辑空隙非常适合替代传统或现代空隙、因为它在保持备份联机的同时具有相同的安全保护原则。借助NetApp、您可以通过逻辑气隙来解决磁带或磁盘气隙的复杂性问题、而逻辑气隙可以通过不可变更的快照和NetApp SnapLock Compliance来实现。



NetApp在10多年前发布了SnapLock功能、旨在满足数据合规性要求、例如健康保险携带和责任法案(HIPAA)、萨班斯-奥克斯利法案以及其他法规数据规则。您还可以将主快照存储到SnapLock卷、以便将副本提交到

WORM、从而防止删除。SnapLock许可证有两个版本：SnapLock Compliance和SnapLock Enterprise。对于勒索软件保护、NetApp建议使用SnapLock Compliance、因为您可以设置一个特定的保留期限、在该期限内、即使ONTAP管理员或NetApp支持人员也无法删除快照。

了解更多信息。

- "博客：ONTAP网络存储概述"

防篡改快照

虽然利用SnapLock Compliance作为逻辑空隙可提供防止攻击者删除备份副本的终极保护、但它确实要求您使用SnapVault将快照移动到启用了SnapLock的二级卷。因此、许多客户都会在网络中的二级存储上部署此配置。与在主存储上还原主卷Snapshot相比、这可能会导致还原时间更长。

从ONTAP 9.12.1开始、防篡改快照可为主存储和主卷中的快照提供接近SnapLock Compliance级别的保护。无需使用SnapVault将快照存储到二级SnapLocked卷。防篡改快照使用SnapLock技术来防止主快照被删除、即使是使用相同SnapLock保留期限的完整ONTAP管理员也是如此。这样可以缩短还原时间、并可通过防篡改的受保护快照备份FlexClone卷、而传统的SnapLock Compliance存储快照则无法做到这一点。

SnapLock Compliance与防篡改快照之间的主要区别在于、如果SnapLock Compliance卷中存储的快照尚未达到到期日期、则SnapLock Compliance不允许对ONTAP阵列进行初始化和擦除。要使快照防篡改、需要SnapLock Compliance许可证。

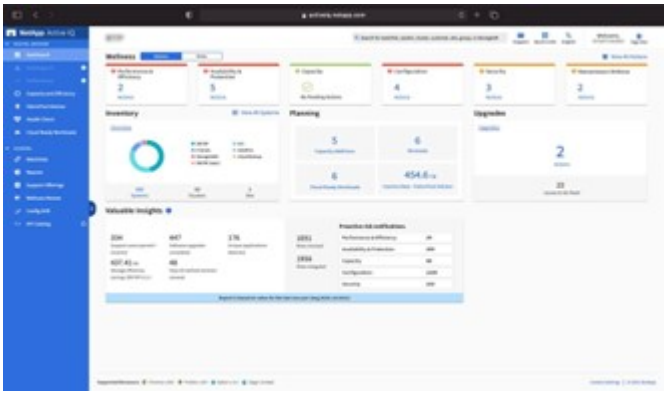
了解更多信息。

- "锁定快照以防止勒索软件攻击"

Digital Advisor勒索软件保护

由 Active IQ 提供支持的 Digital Advisor 简化了 NetApp 存储的主动护理和优化，通过可操作的智能实现最佳数据管理。凭借来自我们高度多样化的安装基础的遥测数据，它使用先进的 AI 和 ML 技术来发现机会，以降低风险并提高存储环境的性能和效率。

`https://www.netapp.com/services/support/active-iq/["NetApp数字顾问"^]`
`https://www.netapp.com/blog/fix-security-vulnerabilities-with-active-iq/["消除安全漏洞"^]`它不仅可以提供帮助，还提供针对勒索软件的防护的见解和指导。一张专用健康卡可显示所需的操作和已解决的风险、因此您可以确保您的系统符合这些最佳实践建议。



在"防兰索防健康"页面上跟踪的风险和操作包括以下(以及更多)：

- 卷快照计数较低、降低了潜在的勒索软件保护。
- 未为配置了NAS协议的所有Storage Virtual Machine (SVM)启用FPolicy。

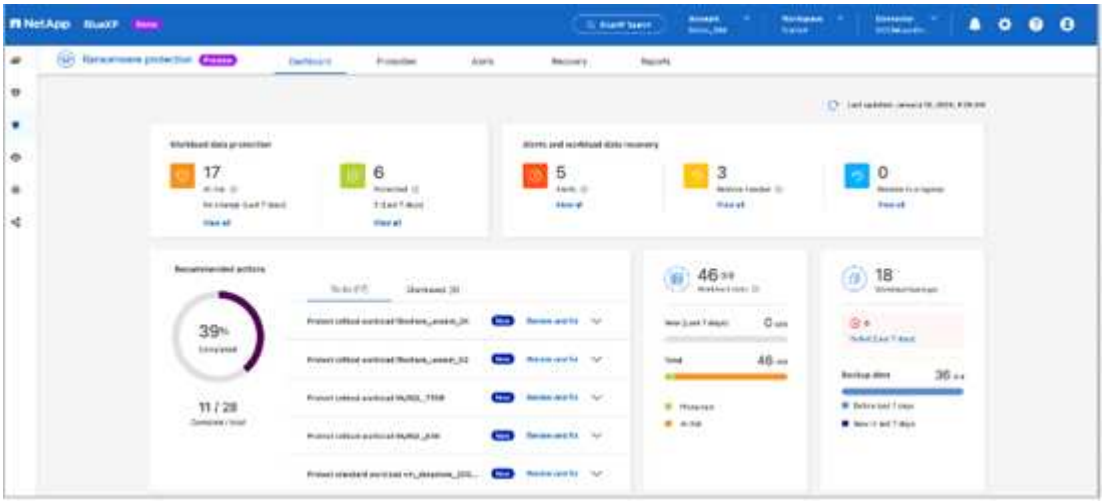
要了解勒索软件保护的实际操作，请参见"Digital Advisor"。

NetApp勒索软件防护提供全面的恢复能力

尽早检测勒索软件非常重要，这样才能防止其传播并避免代价高昂的停机。然而，有效的勒索软件检测策略应该包含多层保护。 NetApp 的勒索软件防护采用综合方法，包括使用NetApp Console扩展到数据服务的实时、机上功能以及用于网络保管的隔离、分层解决方案。

NetApp勒索软件防护

NetApp Console是一个单一控制平面，可以智能地协调全面的、以工作负载为中心的勒索软件防御。 NetApp勒索软件防护汇集了ONTAP强大的网络弹性功能（例如 ARP、FPolicy 和防篡改快照）以及NetApp数据服务（例如NetApp Backup and Recovery）。它还添加了自动化工作流程的建议和指导，以通过单一 UI 提供端到端防御。它在工作负载级别运行，以确保运行您业务的应用程序受到保护，并且在受到攻击时可以尽快恢复。



客户获益：

- 辅助防勒索软件可降低运营开销并提高效率
- 采用AI/ML技术的异常检测可提供更高的准确性和更快的响应来控制风险
- 借助应用程序一致的引导式还原、您可以在几分钟内更轻松地恢复工作负载

"NetApp勒索软件防护"使得这些 NIST 功能更容易实现：

- 自动*发现* NetApp存储中的数据并确定数据优先级*，重点关注基于应用程序的顶级工作负载*。
- *一键保护*顶级工作负载数据备份、不可变、安全配置、恶意文件阻止和不同的安全域。
- 使用*基于**AI**的下一代异常检测、尽可能*快速*准确检测*勒索软件
- 自动响应和工作流、并与顶级*暹粒和XDR解决方案集成。*
- 通过简化的*协调恢复*快速恢复数据，加快应用程序正常运行时间。

- 实施勒索软件保护*策略*和*策略*，并*监控结果*。

NetApp和零信任

NetApp和零信任

一直以来、零信任都是一种以网络为中心的方法、用于构建微核心和外围(MCAP)架构、以通过称为分段网关的控制来保护数据、服务、应用程序或资产。NetApp ONTAP正在采取以数据为中心的零信任方法、在这种方法中、存储管理系统将成为保护和监控客户数据访问的分段网关。尤其是、FPolicy零信任引擎和FPolicy合作伙伴生态系统成为一个控制中心、可以详细了解正常和异常的数据访问模式、并识别内部威胁。

从2024年7月开始、技术报告_TR-4829：《NetApp和零信任：启用以数据为中心的零信任模式》的内容(以前以PDF格式发布)可从docs.netapp.com获取。

数据是企业拥有的最重要资产。根据2022年的数据泄露、18%的数据泄露是由内部威胁造成 "Verizon数据泄露调查报告"的。企业可以通过NetApp ONTAP数据管理软件部署行业领先的零信任控制来提高警惕。

什么是零信任?

零信任模型最初由John Kindervag在Forrester Research开发。它设想从内到外而不是从外到外的网络安全。 由内而外的零信任方法可识别微核和外围(MCAP)。MCAP是一个内部定义、用于定义要通过一套全面的控制措施进行保护的数据、服务、应用程序和资产。安全外围的概念已经过时。然后、受信任并允许成功通过外围进行身份验证的实体会使组织容易受到攻击。根据定义、内部人员已经位于安全边界内。员工、承包商和合作伙伴都是内部人员、他们必须能够在适当的控制下运营、才能在组织的基础架构中履行其角色。

Zero Trust于2019年9月被视为一项为DoD带来承诺的技术 "2019财年—23财年DoD数字化现代化战略"。它将零信任定义为"一种网络安全战略、它在整个架构中内置安全性、以阻止数据泄露。这种以数据为中心的安全模式消除了可信或不可信网络、设备、用户身份或进程的想法、并转变为基于多属性的信任级别、从而在最低权限访问概念下启用身份验证和授权策略。实施零信任需要重新思考我们如何使用现有基础架构、以更简单、更高效的方式通过设计来实施安全性、同时实现不受阻碍的运营。"

2020年8月、NIST发布了 "特殊Pub 800-207零信任架构" (ZTA)。ZTA侧重于保护资源而非网段、因为网络位置不再被视为资源安全防护的主要组件。资源是数据和计算。ZTA策略适用于企业网络架构师。ZTA从最初的Forrester概念引入了一些新术语。称为策略决策点(PDP)和策略实施点(PEP)的保护机制类似于Forrester分段网关。ZTA引入了四种部署模式：

- 基于设备代理或网关的部署
- 基于区域的部署(有点类似于Forrester MCAP)
- 基于资源门户的部署
- 设备应用程序沙盒

在本文档中、我们使用Forrester Research的概念和术语、而不是NIST ZTA。

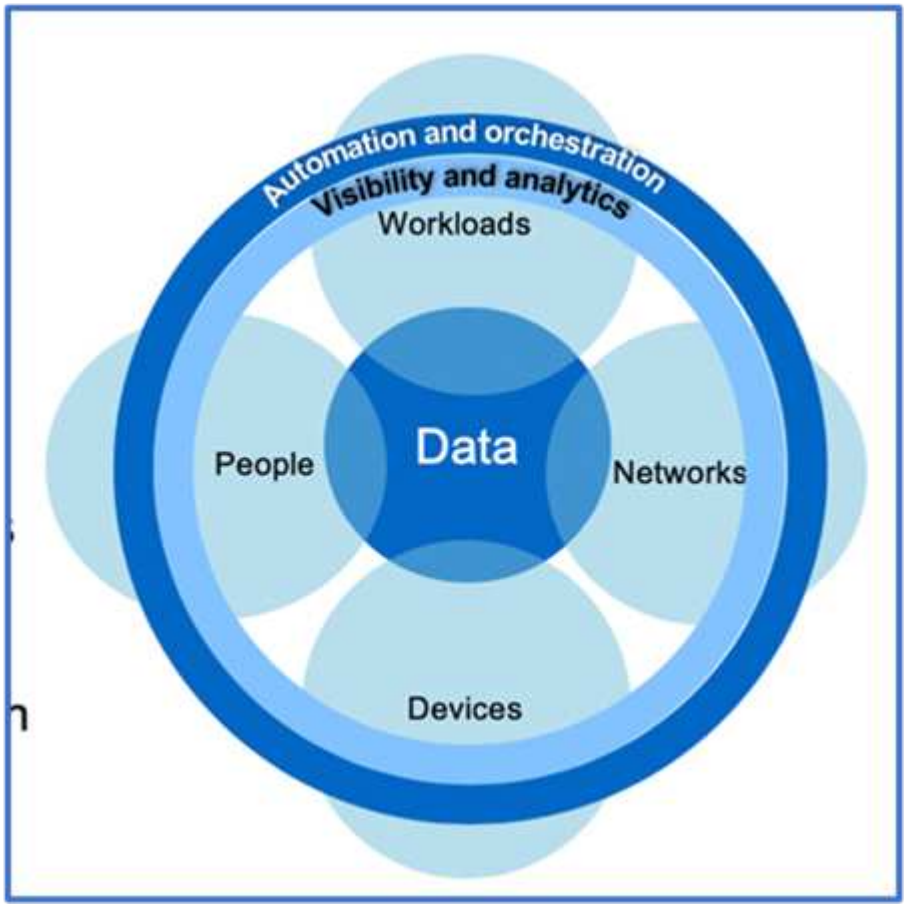
安全资源

有关报告漏洞和事件、NetApp安全响应以及客户机密性的信息，请参见 "NetApp安全门户"。

借助**ONTAP**设计以数据为中心的零信任方法

零信任网络由以数据为中心的方法定义、其中安全控制应尽可能接近数据。ONTAP的功能与NetApp FPolicy合作伙伴生态系统相结合、可以为以数据为中心的零信任模式提供必要的控制。

ONTAP是NetApp提供的安全丰富的数据管理软件、FPolicy零信任引擎是行业领先的ONTAP功能、可提供基于文件的粒度事件通知界面。NetApp FPolicy合作伙伴可以使用此接口更好地了解ONTAP中的数据访问。



构建以零信任数据为中心的**MCAP**

要构建以数据为中心的零信任MCAP、请执行以下步骤：

1. 确定所有组织数据的位置。
2. 对数据进行分类。
3. 安全地处置不再需要的数据。
4. 了解哪些角色应有权访问数据分类。
5. 应用最小特权原则以强制实施访问控制。
6. 对管理访问和数据访问使用多因素身份验证。
7. 对空闲数据和传输中的数据使用加密。
8. 监控和记录所有访问。

9. 对可疑访问或行为发出警报。

确定所有组织数据的位置

借助ONTAP的FPolicy功能以及FPolicy合作伙伴的NetApp联盟合作伙伴生态系统、您可以确定贵组织的数据位于何处以及谁有权访问这些数据。这是通过用户行为分析来实现的、该分析可确定数据访问模式是否有效。有关用户行为分析的更多详细信息、请参见监控和记录所有访问。如果您不了解数据位于何处以及谁有权访问数据、用户行为分析可以提供一个基线、用于根据经验观察结果构建分类和策略。

对数据进行分类

在零信任模型的术语中，数据分类涉及有毒数据的识别。有毒数据是不适合在组织外部暴露的敏感数据。泄露有毒数据可能会违反法规合规性并损害组织的声誉。在监管合规方面，有毒数据包括持卡人数据 "支付卡行业数据安全标准（ PCI-DSS ）"，欧盟的个人数据 "《一般数据保护条例》(GDPR)"或医疗保健数据 "健康保险携带和责任法案(HIPAA)"。您可以使用NetApp "NetApp Data Classification" （以前称为 Cloud Data Sense），一款人工智能驱动的工具包，可自动扫描、分析和分类您的数据。

安全地处置不再需要的数据

对组织的数据进行分类后、您可能会发现某些数据不再需要或与组织的功能无关。保留不必要的数据是一项责任、应删除此类数据。有关以加密方式擦除数据的高级机制、请参见空闲数据加密中的安全清除说明。

了解哪些角色应有权访问数据分类、并应用最小特权原则来强制实施访问控制

映射对敏感数据的访问权限并应用最小特权原则意味着、您的组织中的人员只能访问执行其工作所需的数据。此过程涉及基于角色的访问控制 ("RBAC"，适用于数据访问和管理访问。

借助ONTAP、可以使用Storage Virtual Machine (SVM)对ONTAP集群中租户的组织数据访问进行分段。RBAC可应用于对SVM的数据访问和管理访问。也可以在集群管理级别应用RBAC。

除了RBAC之外，您还可以使用ONTAP "多管理员验证" (MAV)来要求一个或多个管理员批准或等命令 `volume delete` `volume snapshot delete`。启用MAV后、修改或禁用MAV需要获得MAV管理员的批准。

保护快照的另一种方法是使用ONTAP"Snapshot锁定"。快照锁定是一种SnapLock功能、可通过卷快照策略上的保留期限手动或自动呈现不可删除的快照。快照锁定也称为防篡改快照锁定。快照锁定的目的是防止恶意或不可信的管理员删除主ONTAP系统和二级系统上的快照。可以快速恢复主系统上锁定的快照、以便还原被勒索软件损坏的卷。

对管理访问和数据访问使用多因素身份验证

除了集群管理RBAC之外、 "多因素身份验证(MFA)" 还可以部署ONTAP Web管理访问和安全Shell (SSH)命令行访问。对于美国公共部门组织或必须遵循PCI-DSS的组织、管理访问的MFA是一项要求。MFA使攻击者无法仅使用用户名和密码来攻击帐户。MFA需要两个或更多独立因素进行身份验证。双因素身份验证的一个示例是用户拥有的信息(例如私钥)和用户知道的信息(例如密码)。通过安全断言标记语言(SAML) 2.0、可以通过Web对ONTAP系统管理器或ActiveIQ统一管理器进行管理访问。SSH命令行访问使用具有公共密钥和密码的链式双因素身份验证。

您可以使用ONTAP中的身份和访问管理功能通过API控制用户和计算机访问：

- 用户：
  - *身份验证和授权。*通过适用于SMB和NFS的NAS协议功能。
  - *审计*访问和事件系统日志。CIFS协议的详细审核日志记录、用于测试身份验证和授权策略。对文件级

的详细NAS访问进行精细粒度FPolicy审核。

- 设备：
  - *身份验证。*基于证书的API访问身份验证。
  - *授权默认或自定义基于角色的访问控制(Role-Based Access Control、RBAC)。
  - *审计*已执行的所有操作的系统日志。

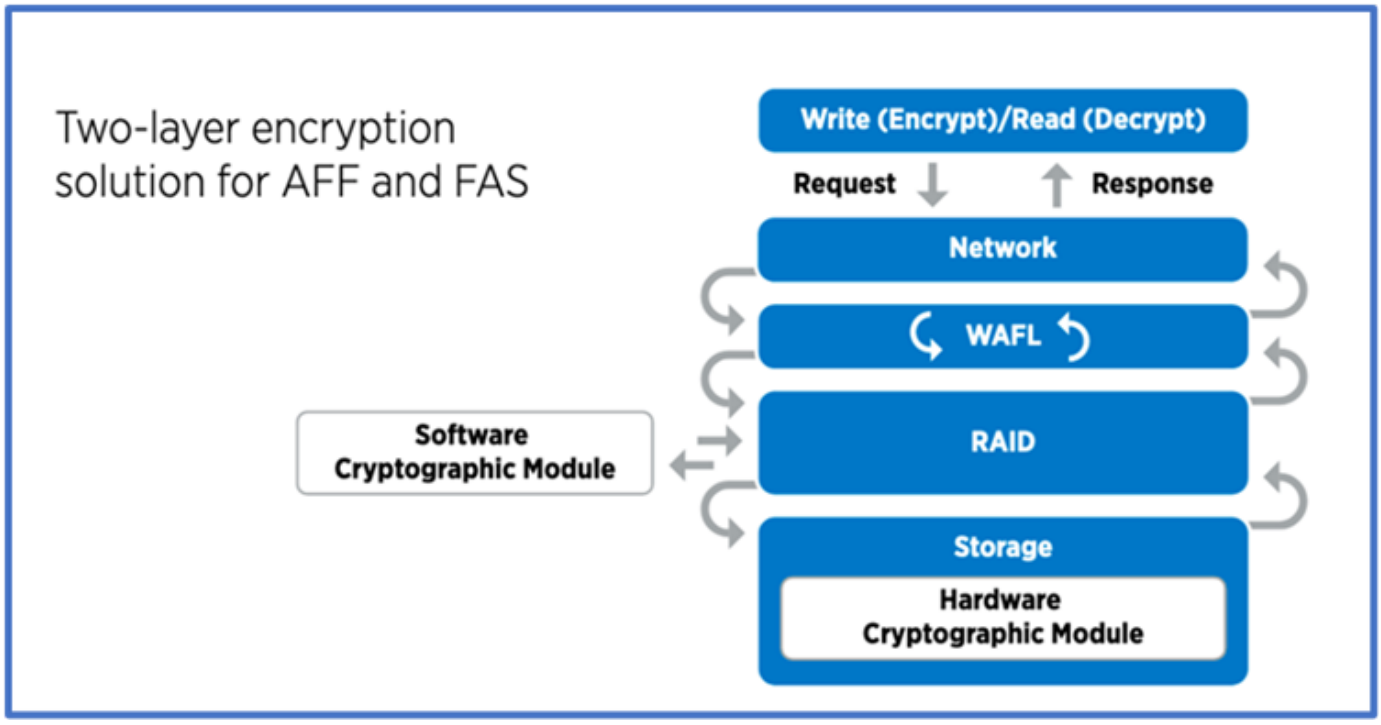
对空闲数据和传输中的数据使用加密

空闲数据加密

每天、当企业重新利用驱动器、退回有缺陷的驱动器或通过销售或以旧换新方式升级到更大的驱动器时、要缓解存储系统风险和基础架构缺口、都有新的要求。 作为数据管理员和操作员、存储工程师应在数据的整个生命周期内安全地管理和维护数据。 "NetApp存储加密(NSE)#44；NetApp卷加密(NVE)#44；以及NetApp聚合加密" 帮助您始终对空闲数据进行加密、无论数据是否有毒、而且不会影响日常运营。 "NSE" 是一款ONTAP硬件 "空闲数据" 解决方案、使用经过FIPS 140-2 2级验证的自加密驱动器。 "NVE和NAE" 是利用的ONTAP软件 "空闲数据" 解决方案 "FIPS 140-2 1级验证的NetApp加密模块"。使用NVE和NAE时、可以使用硬盘驱动器或固态驱动器进行空闲数据加密。此外、NSE驱动器可用于提供本机分层加密解决方案、以提供加密冗余和额外的安全性。如果违反了一个层、则第二个层仍可保护数据的安全。这些功能使ONTAP非常适合 "量子就绪加密"。

NVE还提供了一项功能、称为 "安全清除" 在将敏感文件写入非分类卷时以加密方式删除数据泄漏中的有毒数据。

"板载密钥管理器（ OKM ）"内置在ONTAP中的密钥管理器，或者 "已批准" 第三方 "外部密钥管理器" 可与NSE和NVE结合使用以安全地存储密钥材料。



如上图所示、基于硬件和软件的加密可以结合使用。通过此功能 "将ONTAP验证到NSA的分类计划商业解决方案中" 、可以存储顶级机密数据。

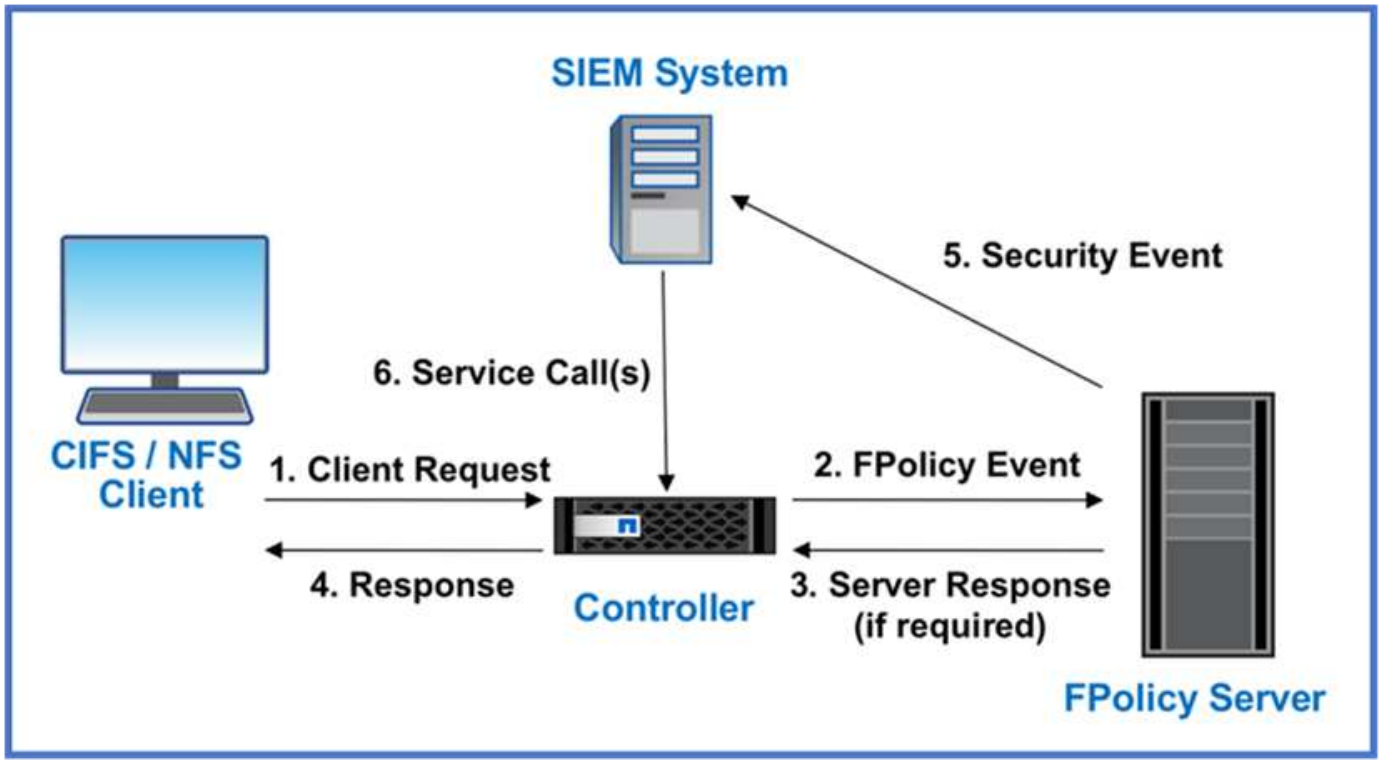
传输中数据加密

ONTAP传输中数据加密可保护用户数据访问和控制平台访问。对于Microsoft CIFS共享访问、可以使用SMB 3.0加密来加密用户数据访问；对于NFS Kerberos 5、可以使用krb5P来加密用户数据访问。对于CIFS、NFS和iSCSI、也可以使用加密用户数据访问 "IPsec" 。控制平面访问使用传输层安全(Transport Layer Security、TLS)进行加密。ONTAP为控制平面访问提供了"FIPS"合规模式、该模式可启用FIPS批准的算法、并禁用未经FIPS批准的算法。数据复制使用进行加密 "集群对等加密"。这样可以为ONTAP SnapVault和SnapMirror技术提供加密功能。

监控和记录所有访问

在实施RBAC策略后、您必须部署主动监控、审核和警报。NetApp ONTAP的FPolicy零信任引擎与相结合 "NetApp FPolicy合作伙伴生态系统"，为以数据为中心的零信任模型提供了必要的控制。NetApp ONTAP是一款安全丰富的数据管理软件、 "FPolicy" 是行业领先的ONTAP功能、可提供基于文件的粒度事件通知界面。NetApp FPolicy合作伙伴可以使用此接口更好地了解ONTAP中的数据访问。借助ONTAP的FPolicy功能以及FPolicy合作伙伴的NetApp联盟合作伙伴生态系统、您可以确定组织数据的位置以及谁有权访问这些数据。这是通过用户行为分析来实现的、该分析可确定数据访问模式是否有效。用户行为分析可用于针对异常模式下的可疑或异常数据访问发出警报、并在必要时采取措施拒绝访问。

FPolicy合作伙伴正在从用户行为分析转向机器学习(ML)和人工智能(AI)、以提高事件保真度并减少误报(如果有)。所有事件都应记录到系统日志服务器或安全信息和事件管理(SIEM)系统、该系统也可以使用ML和AI。



NetApp 的 "DII 存储工作负载安全"利用云和本地ONTAP存储系统上的 FPolicy 界面和用户行为分析，为您提供恶意用户行为的实时警报。存储工作负载安全通过先进的机器学习和异常检测保护组织数据不被恶意或受感染的用户滥用。存储工作负载安全可以识别勒索软件攻击或其他恶意行为，调用快照并隔离恶意用户。存储工作负载安全还具有取证功能，可以详细查看用户和实体活动。存储工作负载安全是NetAppData Infrastructure Insights的一部分。

除了存储工作负载安全性之外、ONTAP还具有板载勒索软件检测功能、称为 "自主勒索软件保护" (ARP)。ARP使用机器学习来确定异常文件活动是否指示正在进行勒索软件攻击、并调用快照并向管理员发出警报。存储工作负载安全性与ONTAP集成以接收ARP事件、并提供额外的分析和自动响应层。

有关此过程中所述命令的更多信息，请参见"ONTAP命令参考"。

ONTAP外部的NetApp安全自动化和业务流程控制

通过自动化、您可以在最少的人工协助下执行流程或程序。借助自动化、企业可以将零信任部署扩展到远远超出手动过程的范围、从而防止同时自动化的不当活动。

Ans还是 一款开源软件配置、配置管理和应用程序部署工具。它可以在许多类Unix系统上运行、并且可以配置类Unix系统以及Microsoft Windows。它包含自己的声明性语言来描述系统配置。《安赛威》由Michael DeHaan编写、并于2015年被Red Hat收购。Ansil可能 无代理、通过SSH或Windows远程管理临时远程连接(允许远程执行PowerShell)以执行任务。NetApp开发了更多产品 "150个适用于ONTAP软件的Ans负责 模块"，可进一步与Ans得 自动化框架集成。适用于NetApp的Ans得 模块提供了一组有关如何定义所需状态并将其中继到目标NetApp环境的说明。这些模块旨在支持设置许可、创建聚合和Storage Virtual Machine、创建卷和还原快照等任务。《NetApp DoD统一功能(UC)部署指南》专门指定了一个"Ands还是And"角色 "发布在GitHub上" 。

通过使用可用模块库、用户可以轻松地开发Ans得 游戏手册、并根据自己的应用程序和业务需求对其进行自定义、以自动执行日常任务。编写完播放手册后、您可以运行它来执行指定的任务、从而节省时间并提高工作效率。NetApp已创建并共享了可直接使用或根据您的需求定制的示例操作手册。

Data Infrastructure Insights是一种基础设施监控工具，可让您了解完整的基础设施。借助Data Infrastructure Insights，您可以监控、排除故障并优化所有资源，包括公共云实例和私有数据中心。Data Infrastructure Insights可以将平均解决时间缩短 90%，并防止 80% 的云问题影响最终用户。它还可以平均降低 33% 的云基础设施成本，并通过使用可操作的情报保护您的数据来减少您受到内部威胁的风险。Data Infrastructure Insights的存储工作负载安全功能支持通过 AI 和 ML 进行用户行为分析，以便在由于内部威胁而出现异常用户行为时发出警报。对于ONTAP，存储工作负载安全使用零信任 FPolicy 引擎。

零信任和混合云部署

NetApp是混合云的数据权威。NetApp提供了多种选项，可通过 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud 和其他领先的云提供商将内部部署数据管理系统扩展到混合云。NetApp混合云解决方案支持与本地ONTAP系统和ONTAP Select软件定义存储相同的零信任安全控制。

您可以使用适用于 AWS（FSxN）、Google Cloud（GCNV）和适用于 Microsoft Azure 的Azure NetApp Files 的企业级云原生文件服务，轻松扩展公共云的容量，而不受典型的资本支出限制。这些云数据服务非常适合分析和 DevOps 等数据密集型工作负载，它将NetApp的弹性按需存储即服务与ONTAP数据管理结合在一起，形成一个完全托管的产品。

ONTAP借助NetApp SnapMirror数据复制软件，支持在本地ONTAP系统与 AWS、Google Cloud 或 Azure 存储环境之间移动数据。

基于属性的访问控制

使用ONTAP进行基于属性的访问控制

从9.12.1开始、您可以为ONTAP配置NFSv4.2安全标签和扩展属性(xattrs)、以便使用属性和基于属性的访问控制(ABAC)支持基于角色的访问控制(Role-Based Access Control 、RBAC)。

ABAC是一种授权策略、可根据用户属性、资源属性和环境条件定义权限。ONTAP与NFS v4.2安全标签和xattt的集成符合NIST特刊800-162中规定的ABAC解决方案NIST标准。

您可以使用NFS v4.2安全标签和xattrs分配文件用户定义的属性和标签。ONTAP可以与面向ABAC的身份和访问管理软件集成、以根据这些属性和标签实施精细的文件和文件夹访问控制策略。

相关信息

- "使用ONTAP进行ABAC的方法"
- "NetApp ONTAP中的NFS：最佳实践和实施指南"

ONTAP中基于属性的访问控制(ABAC)的方法

ONTAP提供了多种可用于实现文件级基于属性的访问控制(ABAC)的方法、包括NFS v4.2安全标签和使用NFS的扩展属性(xattrs)。

NFS v4.2安全标签

从ONTAP 9.9.1开始、支持名为标记NFS的NFS v4.2功能。

NFS v4.2安全标签是一种使用SELinux标签和强制访问控制(Mandat强制 访问控制、MAC)管理精细文件和文件夹访问的方法。这些MAC标签与文件和文件夹存储在一起、并与UNIX权限和NFS v4.x ACL结合使用。

支持NFS v4.2安全标签意味着ONTAP现在可以识别和了解NFS客户端的SELinux标签设置。RFC 7204中介绍了NFS v4.2安全标签。

NFS v4.2安全标签的使用情形如下：

- 虚拟机(VM)映像的MAC标签
- 公共部门的数据安全分类(机密、最高机密和其他分类)
- 安全合规性
- 无磁盘 Linux

启用 NFS v4.2 安全标签

您可以使用以下命令启用或禁用NFS v4.2安全标签(需要高级权限)：

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

有关的详细信息 `vserver nfs modify`，请参见"ONTAP命令参考"。

NFS v4.2安全标签的强制实施模式

从ONTAP 9.9.1开始、ONTAP支持以下强制实施模式：

- 受限服务器模式：ONTAP无法强制执行标签，但可以存储和传输标签。

  更改MAC标签的功能由客户端实施。

- 来宾模式：如果客户端未标记为NFS感知型(v4.1或更低版本)，则不会传输MAC标签。

> ONTAP当前不支持完整模式(存储和强制实施MAC标签)。

NFS v4.2安全标签示例

以下配置示例演示了使用Red Hat Enterprise Linux 9.3 (Plow)的概念。

根据John R. Smith的凭据创建的用户 `jrsmith`具有以下帐户Privileges：

- 用户名= `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

角色有两个：具有特权的用户的管理员帐户和MLS Privileges表中所述的用户 `jrsmith`：

用户	角色	键入	级别
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

在此示例环境中，用户 `jrsmith`可以访问级别为的 `s3`文件 `s0`。我们可以加强现有的安全分类、如下所述、以确保管理员无权访问用户特定的数据。

- Shu =特权管理员用户数据
- Shu =未分类数据
- S1 =机密
- S2 =机密数据
- S3 =排名靠前的机密数据

使用MCS的NFS v4.2安全标签示例

除了多级别安全性(MLS)之外、另一项称为多类别安全性(MCS)的功能还允许您定义项目等类别。

NFS安全标签	价值
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

扩展属性(xatts)

从ONTAP 9.12.1开始、ONTAP支持xattr。xattr允许元数据与系统提供的范围以外的文件和目录相关联、例如访问控制列表(ACL)或用户定义的属性。

要实施xatts、您可以在Linux中使用 `setfattr`和 `getfattr`命令行实用程序。这些工具为管理文件和目录的其他元数据提供了一种强大的方式。使用时应小心、因为使用不当可能会导致意外行为或安全问题。有关详细的使用说

明、请始终参考 `setfattr`和 `getfattr`手册页或其他可靠的文档。

在ONTAP文件系统上启用xatts后、用户可以设置、修改和检索文件的任意属性。这些属性可用于存储有关标准文件属性集未捕获的文件的其他信息、例如访问控制信息。

在ONTAP中使用xattrs有多个要求和限制：

- Red Hat Enterprise Linux 8.4或更高版本
- Ubuntu 22.04或更高版本
- 每个文件最多可以包含128个xatts
- XATTR密钥限制为255字节
- 组合键或值大小为每个xattr 1、729字节
- 目录和文件可以包含xatts
- 要设置和检索xattr、 `w`必须为用户和组启用写入模式位

Xatts在用户命名空间中使用、对ONTAP本身没有任何内在意义。而是由与文件系统交互的客户端应用程序来确定和管理它们的实际应用程序。

XATTR用例示例：

- 记录负责创建文件的应用程序的名称
- 维护对从中获取文件的电子邮件的引用
- 建立用于组织文件对象的分类框架
- 使用原始下载源的URL标记文件

用于管理**xattrs**的命令

- `setfattr`设置文件或目录的扩展属性：

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  命令示例：

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`检索特定扩展属性的值或列出文件或目录的所有扩展属性：

  特定属性：
  ```
  getfattr -n <attribute_name> <file or directory name>
  ```

  所有属性：
  ```
  getfattr <file or directory name>
  ```

  命令示例：

```
getfattr -n user.comment example.txt
```

XATTR键值对示例

下表显示了两个xattr键值对示例：

xattr	价值
user.digitalIdentifier	CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US
user.countryOfAffiliations	USA

ACE for xatts的用户权限

访问控制条目(ACE)是ACL中的一个组件、用于定义为特定资源(例如文件或目录)授予单个用户或一组用户的访问权限。每个ACE都指定允许或拒绝的访问类型、并与特定安全主体(用户或组身份)相关联。

xatts需要访问控制条目**(ACE)**

- RetrievE xattr：用户读取文件或目录的扩展属性所需的权限。"R"表示需要读取权限。
- set xattr：修改或设置扩展属性所需的权限。"a"、"w"和"T"表示不同的权限示例、例如附加、写入以及与xatts相关的特定权限。
- files：用户需要附加、写入以及可能与xatts相关的特殊权限来设置扩展属性。
- 目录：设置扩展属性需要特定权限"T"。

文件类型	检索**xattr**	设置**xattrs.**
文件	R	A、W、T
目录	R	T

与**ABAC**身份和访问控制软件集成

为了充分利用ABAC的功能、ONTAP可以与面向ABAC的身份和访问管理软件集成。

在ABAC系统中、政策执行点(PEP)和政策决策点(PDP)发挥着关键作用。PEP负责实施访问控制策略、而PDP则根据策略决定是授予还是拒绝访问。

在实际环境中、组织会混合使用NFS安全标签和xatts。它们用于表示各种元数据、包括分类、安全性、应用程序和内容、这些都有助于ABAC决策。例如、xatts可用于存储PDP决策过程所使用的资源属性。可以定义一个属性来表示文件的分类级别(例如、"未分类"、"机密"、"机密"或"最高机密")。然后、PDP可以使用此属性来强制实施一项策略、该策略将限制用户仅访问分类级别等于或低于其间隙级别的文件。

> 此内容假定客户的身份、身份验证和访问服务至少包括PEP和PDP、它们充当文件系统访问的中间人。

ABAC流程示例

1. 用户提供系统访问PEP的凭据(例如PKI、OAuth、SAML)、并从PDP获取结果。

   PEP的角色是截获用户的访问请求并将其转发到PDP。

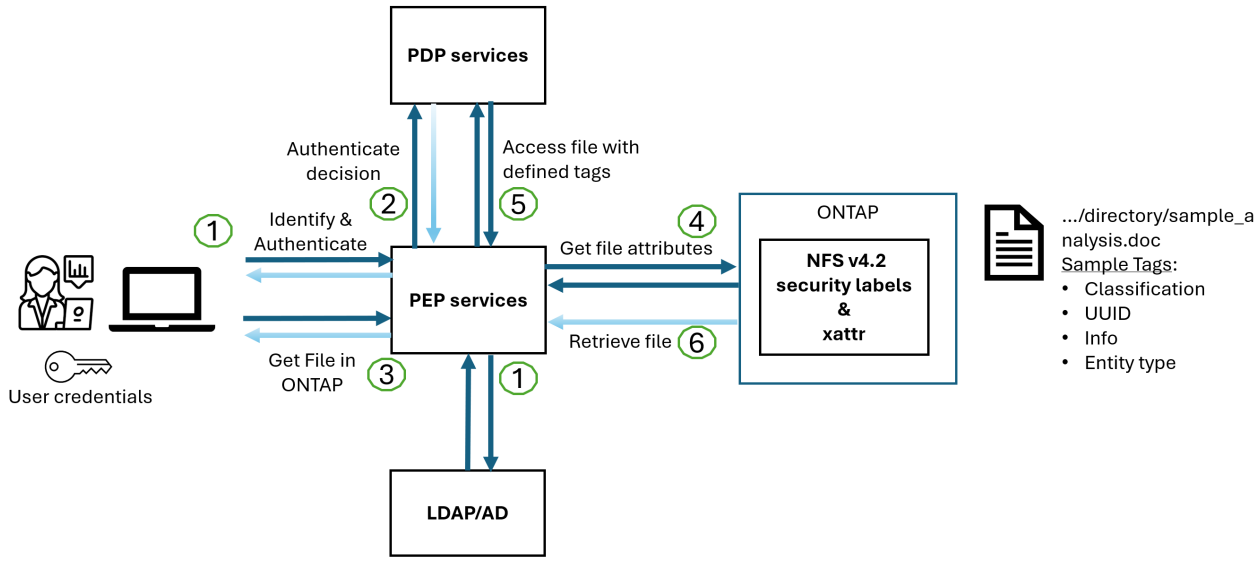
2. 然后、PDP会根据已建立的ABAC策略评估此请求。

   这些策略会考虑与用户、相关资源和周围环境相关的各种属性。根据这些政策、PDP做出允许或拒绝访问决定、然后将该决定传达给PEP。

   PDP为PEP提供了要强制实施的策略。然后、PEP会根据PDP的决定批准或拒绝用户的访问请求、从而强制执行此决定。

3. 请求成功后、用户将请求存储在ONTAP中的文件(例如AFF、AFF C)。
4. 如果请求成功、PEP将从文档中获取精细的访问控制标签。
5. PEP根据该用户的证明请求该用户的策略。
6. PEP根据策略和标记决定用户是否有权访问该文件、并允许用户检索该文件。

实际访问可能使用令牌完成。



ONTAP克隆和**SnapMirror**

ONTAP的克隆和SnapMirror技术旨在提供高效可靠的数据复制和克隆功能、确保文件数据的所有方面(包括xattrs)都与文件一起保留和传输。xattrs非常重要、因为它们存储与文件关联的其他元数据、例如安全标签、访问控制信息和用户定义的数据、这些对于维护文件的上下文和完整性至关重要。

使用ONTAP的FlexClone技术克隆卷时、系统会为该卷创建一个精确的可写副本。此克隆过程可瞬时完成、并且节省空间、其中包括所有文件数据和元数据、从而确保完全复制xatts。同样、SnapMirror可确保以完全保真的方式将数据镜像到二级系统。其中包括xatts、对于依赖此元数据的应用程序正常运行至关重要。

通过在克隆和复制操作中使用xatts、NetApp ONTAP可确保整个数据集及其所有特征在主存储系统和二级存储系统中可用且一致。这种全面的数据管理方法对于需要一致的数据保护、快速恢复以及遵守合规性和法规标准的组

织至关重要。同时、它还可以简化不同环境(无论是内部环境还是云环境)中的数据管理、让用户确信其数据在这些过程中是完整的、不会被更改。

NFS v4.2安全标签具有中定义的说明NFS v4.2安全标签。

审核标签更改

审核对xattr或NFS安全标签的更改是文件系统管理和安全性的一个关键方面。通过标准文件系统审核工具、可以监控和记录对文件系统的所有更改、包括对xattrs和安全标签的修改。

在Linux环境中、 `auditd`守护进程通常用于为文件系统事件建立审核。它允许管理员配置规则，以监视与`xattr`更改相关的特定系统调用，例如 `setxattr`、 `lsetxattr`以及 `fsetxattr`设置属性和 `removexattr`、 `lremovexattr`以及 `fremovexattr`删除属性。

ONTAP FPolicy通过提供一个用于实时监控和控制文件操作的强大框架、扩展了这些功能。可以对FPolicy进行配置、使其支持各种xattr事件、从而对文件操作进行精细控制、并能够实施全面的数据管理策略。

对于使用xattrs的用户、尤其是在NFS v3和NFS v4环境中、仅支持使用特定的文件操作和筛选器组合进行监控。下面详细列出了对NFS v3和NFS v4文件访问事件进行FPolicy监控时支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

setattr操作的**auditd**日志段示例：

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

为使用xatts的用户启用"ONTAP FPolicy"可提供一层可见性和控制、这对于维护文件系统的完整性和安全性至关重要。通过利用FPolicy的高级监控功能、企业可以确保跟踪、审核对xatts的所有更改、并使其符合其安全和合规性标准。这种主动式文件系统管理方法是强烈建议任何希望增强数据监管和保护策略的组织启用ONTAP FPolicy的原因。

控制数据访问的示例

以下John R. Smith的PKI证书中存储的数据条目示例显示了如何将NetApp的方法应用于文件并提供精细的访问控制。

这些示例仅用于说明目的、客户负责确定与NFS v4.2安全标签和xatts关联的元数据。为了简便起见、省略了有关更新和标签保留的详细信息。

示例**PKI**证书值

密钥	价值
实体SecurityMark	T：S01 =未分类

信息	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

规格	" DoD"
UUID	b4111349-7875-4115-AD30-0928565f2e15

管理组织	{
	"value": "DoD"
	}

密钥	价值

简报会	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

"Stat.shipStatus"	{
	"value": "US"
	}

间隙	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

国家或地区附属机构	[
	{
	"value": "USA"
	}
	]

密钥	价值

Digital标识 符	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

DissemTos	<pre>{
	  "value": "DoD"
	}</pre>

双重组织	<pre>{
	  "value": "DoD"
	}</pre>

实体类型	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControl	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

这些PKI授权显示John R. Smith的访问详细信息、包括按数据类型和属性进行的访问。

如果IC-TDF元数据与文件分开存储、则NetApp主张增加一层精细的访问控制。这涉及到在目录级别以及与每个文件关联的情况下存储访问控制信息。例如、请考虑以下链接到文件的标记：

- NFS v4.2安全标签：用于制定安全决策

- xatts：提供与文件和组织计划要求相关的补充信息

以下键-值对是可存储为xatts的元数据示例、并提供有关文件创建者和关联安全分类的详细信息。客户端应用程序可以利用这些元数据做出明智的访问决策、并根据组织标准和要求组织文件。

- xattr键值对的示例*

密钥	价值
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

密钥	价值

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

密钥	价值
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

相关信息

- "NetApp ONTAP中的NFS：最佳实践和实施指南"
- "ONTAP命令参考"
- 请求注释(RFC)
  - "RFC 7204：标记NFS的要求"
  - "RFC 2203：《RPCSEC_GSS协议规范》"
  - "RFC 3530：《网络文件系统(Network File System、NFS)版本4协议》"

加强安全性

ONTAP安全强化指南

这些技术报告提供了有关如何对NetApp ONTAP以及其他NetApp产品进行加密的指导。

这些技术报告对产品文档进行了扩展"ONTAP安全性和数据加密"。

强化指南

"TR-4569：《NetApp ONTAP安全强化指南》" 了解如何配置NetApp ONTAP以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

"适用于VMware vSphere的ONTAP工具安全强化指南" 了解如何为VMware vSphere配置ONTAP工具、以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

"TR-4957：《NetApp SnapCenter安全强化指南》"
了解如何配置NetApp SnapCenter软件以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

"TR-4963：安全强化指南： NetApp Backup and Recovery"了解如何配置NetApp Cloud Backup for Applications，以帮助组织满足信息系统机密性、完整性和可用性的规定安全目标。

"TR-4943：《NetApp Active IQ Unified Manager安全强化指南》"
了解如何配置NetApp Active IQ Unified Manager以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

"TR-4945：《NetApp易管理性SDK的安全强化指南》"
了解如何配置NetApp易管理性SDK (NMSDK)、以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

"MetroCluster Tieb破碎 机主机和数据库安全强化指南"了解如何配置NetApp MetroCluster Tieb破碎 机主机和数据库、以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

ONTAP安全强化准则

ONTAP安全强化概述

ONTAP提供了一组控件、可用于加强ONTAP存储操作系统(行业领先的数据管理软件)的安全。使用ONTAP的指导和配置设置帮助您的组织满足规定的信息系统机密性、完整性和可用性安全目标。

当前威胁格局的演变为企业在保护数据和信息等最有价值的资产方面提出了独特的挑战。我们面临的高级动态威胁和漏洞越来越复杂。随着模糊和侦察技术对潜在的侵入者的效用的提高、系统管理员必须主动解决数据和信息的安全问题。

从2024年7月开始、技术报告_TR-4569：《针对PDF_的安全强化指南》的内容(以前以ONTAP格式发布)可从docs.netapp.com上获取。

ONTAP映像验证

ONTAP提供了一些机制来确保ONTAP映像在升级和启动时有效。

升级映像验证

代码签名有助于验证通过无中断映像更新或自动化无中断映像更新、命令行界面或ONTAP API安装的ONTAP映像是否由NetApp真正生成且未被篡改。ONTAP 9.3引入了升级映像验证。

此功能是对ONTAP升级或恢复的非接触式安全增强功能。除了可以选择验证顶级签名之外、用户不应执行任何其他操作 `image.tgz` 。

启动时映像验证

从ONTAP 9.4开始、为NetApp AFF A800、AFF A220、FAS2750和FAS2720系统以及采用UEFI BIOS的后续下一代系统启用了统一可扩展固件接口(Unified可扩展固件接口、UEFI)安全启动。

启动期间、启动加载程序会验证安全启动密钥的白表数据库以及与所加载的每个模块关联的签名。验证并加载每个模块后、启动过程将继续进行ONTAP初始化。如果任何模块的签名验证失败，系统将重新启动。

这些项目适用于ONTAP映像和平台BIOS。

本地存储管理员帐户

ONTAP角色、应用程序和身份验证

ONTAP使注重安全的企业能够通过不同的登录应用程序和方法为不同的管理员提供细粒度访问权限。这有助于客户创建以数据为中心的零信任模式。

这些角色可供管理员和Storage Virtual Machine管理员使用。系统将指定登录应用程序方法和登录身份验证方法。

角色

借助基于角色的访问控制(Role-Based Access Control、RBAC)、用户只能访问其工作角色和职能所需的系统和选项。ONTAP中的RBAC解决方案将用户的管理访问权限限制为为为其定义的角色所授予的级别、从而使管理员可以按分配的角色管理用户。ONTAP提供了多种预定义角色。操作员和管理员可以创建、修改或删除自定义访问控制角色、并且可以为特定角色指定帐户限制。

集群管理员的预定义角色

此角色 …	具有此访问级别 …	访问以下命令或命令目录
`admin`	全部	所有命令目录(`DEFAULT`)

admin-no-fsa(从ONTAP 9.12.1开始提供)	读/写	• 所有命令目录(DEFAULT) • security login rest-role • security login role
只读	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	无
volume file show-disk-usage	autosupport	全部
• set • system node autosupport	无	所有其他命令目录(DEFAULT)
backup	全部	vserver services ndmp
只读	volume	无
所有其他命令目录(DEFAULT)	readonly	全部

• `security login password` 仅用于管理自己的用户帐户本地密码和密钥信息 • `set`	无	`security`
只读	所有其他命令目录(`DEFAULT`)	`none`

此 `autosupport`角色将分配给AutoSupport OnDemand使用的预定义 `autosupport`帐户。ONTAP会阻止您修改或删除此 `autosupport`帐户。此外、ONTAP还会阻止您将此角色分配 `autosupport`给其他用户帐户。

Storage Virtual Machine (SVM)管理员的预定义角色

角色名称	功能
`vsadmin`	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、但卷移动除外 • 管理配额、qtrees、快照和文件 • 管理LUN • 执行SnapLock操作、但特权删除除外 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 监控作业 • 监控网络连接和网络接口 • 监控SVM的运行状况
`vsadmin-volume`	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、但卷移动除外 • 管理配额、qtrees、快照和文件 • 管理LUN • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 监控网络接口 • 监控SVM的运行状况

vsadmin-protocol	• 管理自己的用户帐户本地密码和密钥信息 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 管理LUN • 监控网络接口 • 监控SVM的运行状况
vsadmin-backup	• 管理自己的用户帐户本地密码和密钥信息 • 管理NDMP操作 • 将已还原的卷设置为读/写卷 • 管理SnapMirror关系和快照 • 查看卷和网络信息
vsadmin-snaplock	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、但卷移动除外 • 管理配额、qtrees、快照和文件 • 执行SnapLock操作、包括以特权方式删除 • 配置协议：NFS和SMB • 配置服务：DNS、LDAP和NIS • 监控作业 • 监控网络连接和网络接口
vsadmin-readonly	• 管理自己的用户帐户本地密码和密钥信息 • 监控SVM的运行状况 • 监控网络接口 • 查看卷和LUN • 查看服务和协议

应用程序方法

应用程序方法用于指定登录方法的访问类型。可能的值包括 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 和 `telnet`。

将此参数设置为 `service-processor` 可授予用户对服务处理器的访问权限。如果此参数设置为 `service-processor`，则必须将该 `-authentication-method` 参数设置为 `password` ，因为服务处理器仅支持 `password` 身份验证。SVM用户帐户无法访问服务处理器。因此，当参数设置为时，操作员和管理员不能使用 `-vserver` 参数 `service-processor`。

要进一步限制对的访问， `service-processor` 请使用命令 `system service-processor ssh add-allowed-addresses`。命令 `system service-processor api-service` 可用于更新配置和证书。

出于安全原因、Telnet和远程Shell (RSH)默认处于禁用状态、因为NetApp建议使用安全Shell (SSH)进行安全远程访问。如果需要或唯一需要Telnet或RSH、则必须启用它们。

命令用于 `security protocol modify` 修改RSH和Telnet的现有集群范围配置。通过将已启用字段设置为，在集群中启用RSH和Telnet `true`。

身份验证方法

authentication方法参数用于指定用于登录的身份验证方法。

身份验证方法	说明
`cert`	SSL证书身份验证
`community`	SNMP 团体字符串
`domain`	Active Directory 身份验证
`nsswitch`	LDAP或NIS身份验证
`password`	密码
`publickey`	公共密钥身份验证
`usm`	SNMP用户安全模型

由于协议安全漏洞、不建议使用NIS。

从ONTAP 9.3开始、本地SSH帐户可以使用和作为两种身份验证方法来进行链式双因素身份验证 `admin publickey password`。除了 `-authentication-method` 命令中的字段 `security login` 之外、还添加了一个名为的新字段 `-second-authentication-method`。 `publickey`可以将或 `password` 指定为 `-authentication-method` 或 `-second-authentication-method`。但是、在SSH身份验证期间、顺序始终为 `publickey` 部分身份验证、然后是用于完全身份验证的密码提示。

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

从ONTAP 9.4开始， `nsswitch` 可用作的第二种身份验证方法 `publickey`。

从ONTAP 9.12.1开始、FIDO2也可用于使用YukiKey硬件身份验证设备或其他FIDO2兼容设备进行SSH身份验证。

从ONTAP 9.13.1.开始：

- `domain` 帐户可用作中的第二种身份验证方法 `publickey`。
- 基于时间的一次性密码是由算法生成的临时密码 (`totp`，该算法使用当前时间作为第二种身份验证方法的身份验证因素之一。

- SSH公共密钥以及证书均支持公共密钥撤消、这些证书将在SSH期间进行到期/撤消检查。

有关ONTAP系统管理器、Active IQ Unified Manager和SSH的多因素身份验证(MFA)的详细信息，请参见 "TR-4647：《ONTAP 9中的多因素身份验证》"。

默认管理帐户

应限制管理员帐户、因为管理员角色可以使用所有应用程序进行访问。diag帐户允许访问系统Shell、并且只能由技术支持人员保留以执行故障排除任务。

有两个默认管理帐户： `admin` 和 `diag`。

孤立帐户是一个主要的安全媒介、通常会导致漏洞、包括特权升级。这些帐户是用户帐户存储库中保留的不必要和未使用的帐户。它们主要是从未使用过的默认帐户、或者从未更新或更改过密码的默认帐户。为了解决此问题、ONTAP支持删除和重命名帐户。

> 无法删除或重命名内置帐户。如果管理员删除帐户，则在重新启动时，将重新创建内置帐户。*NetApp 建议*使用 lock 命令锁定任何不需要的内置帐户。

虽然孤立帐户是一个重大的安全问题，但 **NetApp** 强烈建议 测试从本地帐户存储库中删除帐户的效果。

列出本地帐户

要列出本地帐户、请运行命令。 `security login show`

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application  Method    Role Name         Locked Group
---------------- -----------  --------- ----------------- ------ -----------
admin            console      password  admin             no     no
admin            http         password  admin             no     no
admin            ontapi       password  admin             no     no
admin            service-processor password admin          no     no
admin            ssh          password  admin             no     no
autosupport      console      password  autosupport       no     no
6 entries were displayed.
```

设置诊断**(diag)**帐户密码

存储系统会提供一个名为的诊断帐户 `diag` 。您可以使用 `diag` 帐户在中执行故障排除任务 `systemshell`。该 `diag` 帐户是唯一可用于通过特权命令访问systemshell的帐户 `diag systemshell`。

> systemshell和关联 `diag` 帐户用于进行低级诊断。其访问需要诊断权限级别、并且仅在技术支持指导下使用、以执行故障排除任务。帐户和均不 `diag systemshell` 用于一般管理目的。

开始之前

在访问之前 `systemshell`，您必须使用命令设置 `diag` 帐户密码 `security login password`。您应使用强密码原则并定期更改 `diag` 密码。

步骤

1. 设置 `diag` 帐户用户密码：

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

多管理员验证

从ONTAP 9.11.1开始、您可以使用多管理员验证(MAV)来允许某些操作(例如删除卷或快照)仅在获得指定管理员批准后才能执行。这样可以防止受到影响的管理员、恶意管理员或经验不足的管理员进行不希望的更改或删除数据。

配置MAV包括以下内容：

- "创建一个或多个管理员批准组"(英文)
- "启用多管理员验证功能"(英文)
- "添加或修改规则"(英文)

完成初始配置后、只有MAV批准组中的管理员(MAV管理员)才能修改这些元素。

启用MAV后、完成每个受保护操作需要三个步骤：

1. 当用户启动操作时，会显示"已生成请求"。
2. 在执行之前，所需的数量"MAV管理员必须批准"。
3. 批准后、用户完成操作。

MAV不适用于涉及大量自动化的卷或工作流、因为每个自动化任务都需要经过批准才能完成操作。如果要同时使用自动化和MAV、NetApp建议您对特定MAV操作使用查询。例如、您只能将MAV规则应用 `volume delete` 于

不涉及自动化的卷、并且可以使用特定的命名方案来指定这些卷。

有关MAV的更多详细信息，请参见 "ONTAP多管理员验证文档"。

Snapshot锁定

快照锁定是一种SnapLock功能、可通过卷快照策略上的保留期限手动或自动呈现不可删除的快照。快照锁定的目的是防止恶意或不可信的管理员删除主或二级ONTAP系统上的快照。

ONTAP 9.12.1引入了快照锁定功能。快照锁定也称为防篡改快照锁定。虽然它确实需要SnapLock许可证并初始化Compliance时钟、但快照锁定与SnapLock Compliance或SnapLock Enterprise无关。没有值得信赖的存储管理员、就像SnapLock Enterprise一样、它无法像SnapLock Compliance那样保护底层物理存储基础架构。与将快照通过Snapvauling存储到二级系统相比、这是一项改进。可以快速恢复主系统上锁定的快照、以还原被勒索软件损坏的卷。

有关详细信息，请参见"Snapshot锁定文档"。

设置基于证书的**API**访问

必须使用基于证书的身份验证、而不是用于REST API或NetApp易管理性SDK API访问ONTAP的用户ID和密码身份验证。

作为REST API基于证书的身份验证的替代方法，请使用 "基于OAuth2.0令牌的身份验证"。）

您可以按以下步骤中所述在ONTAP上生成并安装自签名证书。

步骤

1. 使用OpenSSL、通过运行以下命令生成证书：

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
............................+++
writing new private key to 'test.key'
```

此命令将生成名为的公共证书和名为的 `test.pem` 专用密钥 `key.out`。公用名CN与ONTAP用户ID相对应。

2. 通过运行以下命令并在出现提示时粘贴公共证书的内容、在ONTAP中以隐私增强邮件(prom)格式安装此证书的内容：

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. 启用ONTAP以允许客户端通过SSL进行访问、并定义用于API访问的用户ID。

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

在以下示例中、用户ID `cert_user` 现在已启用、可使用经过证书身份验证的API访问。用于显示ONTAP版本的简单易管理性SDK Python脚本 `cert_user` 如下所示：

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

该脚本的输出将显示ONTAP版本。

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. 要使用ONTAP REST API执行基于证书的身份验证、请完成以下步骤：
   a. 在ONTAP中、定义http访问的用户ID：

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

   b. 在Linux客户端上、运行以下命令、以输出形式生成ONTAP版本：

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

更多信息

- "使用适用于ONTAP的NetApp易管理性SDK进行基于证书的身份验证"(英文)

适用于**REST API**的**ONTAP OAuth2.0**基于令牌的身份验证

作为基于证书的身份验证的替代方法、您可以对REST API使用基于OAuth2.0令牌的身份验证。

从ONTAP 9.14.1开始、您可以选择使用开放授权(OAuth2.0)框架控制对ONTAP集群的访问。您可以使用任何ONTAP管理界面配置此功能、包括ONTAP命令行界面、System Manager和REST API。但是、只有当客户端使用REST API访问ONTAP时、才能应用OAuth2.0授权和访问控制决策。

OAuth2.0令牌取代了用户帐户身份验证的密码。

有关使用OAuth2.0的详细信息，请参见 "有关使用OAuth2.0进行身份验证和授权的ONTAP文档"。

登录和密码参数

有效的安全防护符合既定的组织策略、准则以及适用于组织的任何监管或标准。这些要求的示例包括用户名生命周期、密码长度要求、字符要求以及此类帐户的存储。ONTAP解决方案提供了一些特性和功能来解决这些安全结构问题。

新的本地帐户功能

要支持组织的用户帐户策略、准则或标准(包括监管)、ONTAP支持以下功能：

- 配置密码策略以强制实施最少数字、小写字符或大写字符数
- 登录尝试失败后需要延迟
- 定义帐户非活动限制
- 使用户帐户过期
- 显示密码到期警告消息
- 登录无效通知

可配置的设置可使用security login Role config修改命令进行管理。

SHA-512支持

为了增强密码安全性、ONTAP 9支持SHA-2密码哈希函数、并默认使用SHA-512对新创建或更改的密码进行哈希。操作员和管理员还可以根据需要使帐户过期或锁定帐户。

升级到ONTAP 9.0或更高版本后、未更改密码的原有ONTAP 9用户帐户仍可使用MD5哈希函数。但是、NetApp强烈建议用户更改密码、将这些用户帐户迁移到更安全的SHA-512解决方案。

通过密码哈希功能、您可以执行以下任务：

- 显示与指定哈希函数匹配的用户帐户：

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 使使用指定哈希函数(例如MD5)的帐户过期、从而强制用户在下次登录时更改密码：

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 使用使用指定哈希函数的密码锁定帐户。

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

集群管理SVM中的内部用户无法识别密码哈希函数 `autosupport` 。此问题无关紧要。哈希函数未知、因为默认情况下、此内部用户未配置密码。

  - 要查看用户的密码哈希函数 `autosupport` 、请运行以下命令：

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

  - 要设置密码哈希函数(默认值：SHA512)、请运行以下命令：

```
::> security login password -username autosupport
```

密码设置为什么无关紧要。

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

密码参数

ONTAP 解决方案提供满足并支持企业策略要求和准则的密码参数。

从9.14.1开始、密码的复杂性和锁定规则会增加、而这些规则仅适用于新安装的ONTAP。

所有密码必须与用户名不同。

属性	说明	默认	范围
username-minlength	最短用户名长度限制	3	3-16
username-alphanum	用户名字母数字	已禁用	启用/禁用
passwd-minlength	最短密码长度限制	8	3-64
passwd-alphanum	密码字母数字	已启用	启用/禁用
passwd-min-special-chars	密码中的最少特殊字符数限制	0	0-64
passwd-expiry-time	密码到期时间（天）	无限制，表示密码永不过期	0-unlimited 0 == 立即过期
require-initial-passwd-update	需要在首次登录时更新初始密码	已禁用	启用/禁用 允许通过控制台或SSH进行更改
max-failed-login-attempts	尝试失败的最大次数	0，不锁定帐户	-
lockout-duration	最大锁定期限（天）	默认值为 0，表示帐户锁定一天	-
disallowed-reuse	禁止使用最后N个密码	6	最小为 6

属性	说明	默认	范围
change-delay	密码更改之间的延迟（天）	0	-
delay-after-failed-login	每次登录尝试失败后的延迟（秒）	4	-
passwd-min-lowercase-chars	密码中的最少小写字母字符数限制	0，表示不需要小写字母字符	0-64
passwd-min-uppercase-chars	最少大写字母字符数限制	0，表示不需要大写字母字符	0-64
passwd-min-digits	密码中的最小数字字符数限制	0，表示不需要数字字符	0-64
passwd-expiry-warn-time	在帐户到期之前显示警告消息（天）	无限制，表示从不发出密码过期警告	0，表示每次成功登录时均提醒用户密码即将过期
account-expiry-time	帐户将在N天后过期	无限制，表示帐户永不过期	帐户到期时间必须大于帐户非活动限制
account-inactive-limit	帐户过期之前处于非活动状态的最大持续时间（天）	无限制，表示非活动帐户永不过期	帐户非活动限制必须小于帐户到期时间

示例

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                        Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                         Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

系统管理方法

这些参数是加强ONTAP系统管理的重要参数。

命令行访问

建立对系统的安全访问是维护安全解决方案的关键部分。最常见的命令行访问选项包括SSH、Telnet和RSH。其中、SSH是远程命令行访问最安全的行业标准最佳实践。NetApp强烈建议使用SSH通过命令行访问ONTAP解决方案。

SSH配置

命令可 `security ssh show` 显示集群和SVM的SSH密钥交换算法、密码和MAC算法配置。密钥交换方法使用这些算法和密码来指定如何为加密和身份验证生成一次性会话密钥以及如何进行服务器身份验证。

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

登录横幅

通过登录横幅、组织可以向任何操作员、管理员甚至入侵者提供可接受使用的条款和条件、并指明允许谁访问系统。这种方法有助于建立对系统访问和使用的预期。命令用于 `security login banner modify` 修改登录横幅。在SSH和控制台设备登录过程中、登录横幅显示在身份验证步骤的前面。横幅文本必须用双引号("")括起来、如以下示例所示。

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

登录横幅参数

参数	说明
`vserver`	使用此参数指定带有已修改横幅的SVM。使用集群管理SVM的名称修改集群级别的消息。集群级别的消息用作未定义消息的数据SVM的默认消息。
`message`	此可选参数可用于指定登录横幅消息。如果集群设置了登录横幅消息、则所有数据SVM也会使用集群登录横幅。设置数据SVM的登录横幅将覆盖集群登录横幅的显示。要将数据SVM登录横幅重置为使用集群登录横幅、请将此参数与值"-"结合使用。 如果使用此参数、则登录横幅不能包含换行符(也称为行尾[EOLS]或换行符)。要输入包含换行符的登录横幅消息、请勿指定任何参数。系统将提示您以交互方式输入消息。以交互方式输入的消息可以包含换行符。 非ASCII字符必须使用Unicode UTF-8。
`uri`	`(ftp

参数	说明
http):///(hostname	IPv4` 使用此参数指定从中下载登录横幅的URI。 消息长度不得超过2048字节。非ASCII字符必须以Unicode UTF-8格式提供。

每日消息

`security login motd modify`命令用于更新每日消息(Message of the Day、MOTD)。

MOTD分为两类：集群级别的MOTD和数据SVM级别的MOTD。登录到数据SVM的集群Shell的用户可能会看到两条消息：集群级别的MOTD、后跟该SVM的SVM级别的MOTD。

如果需要、集群管理员可以在每个SVM上单独启用或禁用集群级别的MOTD。如果集群管理员为SVM禁用了集群级别的MOTD、则登录到此SVM的用户不会看到集群级别的消息。只有集群管理员才能启用或禁用集群级别的消息。

MOTD参数	说明
Vserver	使用此参数指定要修改其MOTD的SVM。使用集群管理SVM的名称修改集群级别的消息。

MOTD参数	说明
message	此可选参数可用于指定消息。如果使用此参数、则MOTD不能包含换行符。如果未指定除参数以外的任何参数 `-vserver` 、系统将提示您以交互方式输入消息。以交互方式输入的消息可以包含换行符。非ASCII字符必须以Unicode UTF-8格式提供。消息可以包含使用以下转义序列动态生成的内容： • `\\` -单个反冲字符 • `\b` -无输出(仅支持与Linux兼容) • `\C` -集群名称 • `\d` -在登录节点上设置的当前日期 • `\t` -在登录节点上设置的当前时间 • `\I` -传入LIF IP地址(输出控制台以进行 `console` 登录) • `\l` -登录设备名称(打印登录控制台 `console`) • `\L` -用户在集群中任何节点上的上次登录 • `\m` -机器架构 • `\n` -节点或数据SVM名称 • `\N` -登录用户的名称 • `\o` -与\O相同用于实现Linux兼容性。 • `\O` -节点的DNS域名。请注意、输出取决于网络配置、可能为空。 • `\r` -软件版本号 • `\s` -操作系统名称 • `\u` 本地节点上活动的集群Shell会话数。对于集群管理员：所有clustershell用户。对于数据SVM管理员：仅限该数据SVM的活动会话。 • `\U` -与相同 `\u`，但已 `user` 附加或 `users` 附加 • `\v` -有效的集群版本字符串 • `\W` -登录用户在集群中的活动会话 (`who`)

有关在ONTAP中配置每日消息的详细信息，请参见 "有关每日消息的ONTAP文档"。

命令行界面会话超时

默认命令行界面会话超时为30分钟。超时对于防止陈旧会话和会话备份非常重要。

使用 `system timeout show` 命令查看当前命令行界面会话超时。要设置超时值、请使用 `system timeout modify -timeout <minutes>` 命令。

使用NetApp ONTAP系统管理器进行Web访问

如果ONTAP管理员更喜欢使用图形界面而不是命令行界面来访问和管理集群、请使用NetApp ONTAP系统管理器。它作为Web服务随ONTAP附带、默认情况下处于启用状态、并可通过浏览器进行访问。如果使用的是DNS

或IPv4或IPv6地址，请通过将浏览器指向主机名 `https://cluster-management-LIF`。

如果集群使用自签名数字证书，浏览器可能会显示一条警告，指示此证书不可信。您可以确认风险以继续访问、也可以在集群上安装证书颁发机构(CA)签名的数字证书以进行服务器身份验证。

从ONTAP 9.3开始、ONTAP系统管理器可以选择使用安全断言标记语言(SAML)身份验证。

ONTAP系统管理器的SAML身份验证

SAML 2.0是一种广泛采用的行业标准、它允许任何符合SAML的第三方身份提供程序(Identity Provider、Idp)使用企业所选Idp独有的机制执行MFA、并将其作为单点登录(Single Sign On、SSO)的源。

SAML规范中定义了三个角色：主体、Idp和服务提供商。在ONTAP实施中、主体是通过ONTAP系统管理器或NetApp Active IQ Unified Manager访问ONTAP的集群管理员。Idp是第三方Idp软件。从ONTAP 9.3开始、支持Microsoft Active Directory联合服务(ADFS)和开源Shbboleth Idp。从ONTAP 9.12.1开始、Cisco双核是受支持的Idp。服务提供商是内置在ONTAP中的SAML功能、可供ONTAP系统管理器或Active IQ Unified Manager Web应用程序使用。

与SSH双因素配置过程不同、在激活SAML身份验证后、ONTAP系统管理器或ONTAP服务处理器访问要求所有现有管理员通过SAML Idp进行身份验证。不需要更改集群用户帐户。启用SAML身份验证后、将向具有和应用程序管理员角色的现有用户添加新的身份验证方法 `saml http ontapi` 。

启用SAML身份验证后、应在ONTAP中使用管理员角色以及和应用程序的SAML身份验证方法定义需要SAML Idp访问的其他新帐户 `http ontapi` 。如果在某个时刻禁用了SAML身份验证、则这些新帐户需要 `password` 使用和应用程序的管理员角色定义身份验证方法 `http ontapi` 、并将用于本地ONTAP身份验证的应用程序添加 `console` 到ONTAP系统管理器中。

启用SAML IdP后、IdP将使用IdP可用的方法(例如轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)、Active Directory (AD)、Kerberos、密码等)执行ONTAP System Manager访问身份验证。可用方法对于Idp是唯一的。请务必确保在ONTAP中配置的帐户具有映射到Idp身份验证方法的用户ID。

已通过NetApp验证的IdPs包括Microsoft ADFS、Cisco Duo和开源Shbboleth IdP.

从ONTAP 9.14.1开始、Cisco Duo可用作SSH的第二个身份验证因素。

有关适用于ONTAP系统管理器、Active IQ Unified Manager和SSH的MFA的详细信息，请参见 "TR-4647：《ONTAP 9中的多因素身份验证》"。

ONTAP System Manager洞察力

从ONTAP 9.11.1开始、ONTAP系统管理器可提供深入见解、帮助集群管理员简化日常任务。这些安全洞察基于本技术报告中的建议。

Security Insight	决心
已启用Telnet	NetApp 建议使用安全 Shell （ SSH ）进行安全远程访问。
已启用远程Shell (RSH)	NetApp建议使用SSH进行安全远程访问。
AutoSupport正在使用不安全协议	AutoSupport未配置为通过链路：HTTPS发送。
集群级别未配置登录横幅	如果未为集群配置登录横幅、则显示警告。
SSH 正在使用不安全密码	如果SSH使用不安全的用户身份验证、则显示警告。

Security Insight	决心
配置的NTP服务器太少	如果配置的NTP服务器数量小于3、则显示警告。
默认管理员用户未锁定	如果不使用任何默认管理帐户(admin或diag)登录到System Manager、并且这些帐户未锁定、则建议将其锁定。
勒索软件防御：卷没有Snapshot策略	一个或多个卷未附加足够的Snapshot策略。
勒索软件防御：禁用Snapshot自动删除	已为一个或多个卷设置Snapshot自动删除。
不会监控卷的勒索软件攻击	多个卷支持自主勒索软件保护、但尚未进行配置。
没有为SVM配置自主勒索软件保护	多个SVM支持自主勒索软件保护、但尚未进行配置。
未配置本机FPolicy	未为NAS SVM设置FPolicy。
启用自主勒索软件保护活动模式	多个卷已完成其学习模式、您可以打开活动模式
已禁用全局FIPS 140-2合规性	未启用全局FIPS 140-2合规性。
没有为集群配置通知	电子邮件、webhook或SNMP陷阱主机未配置为接收通知。

有关ONTAP System Manager洞察的详细信息，请参见 "ONTAP System Manager洞察力文档"。

System Manager会话超时

您可以更改System Manager会话非活动超时。默认非活动超时时间为30分钟。超时对于防止陈旧会话和会话备份非常重要。

如果配置了SAML、则非活动超时由Idp上的设置控制。

步骤

1. 选择*集群>设置*。
2. 在*UI设置*中，选择 。
3. 在*非活动超时*框中，键入一个介于2到180之间的分钟值，或者输入“0”禁用超时。
4. 选择 * 保存 * 。

ONTAP自主勒索软件保护

为了对存储工作负载安全性的用户行为分析进行补充、ONTAP自主勒索软件保护功能可分析卷工作负载和熵、以检测勒索软件并创建快照、并在怀疑发生攻击时通知管理员。

除了使用外部 FPolicy 用户行为分析 (UBA) 结合NetApp Data Infrastructure Insights Storage Workload Security和NetApp FPolicy 合作伙伴生态系统进行勒索软件检测和预防之外， ONTAP 9.10.1 还引入了自主勒索软件防护。 ONTAP自主勒索软件防护使用内置的机上机器学习 (ML) 功能，该功能可查看批量工作负载活动和数据熵来自动检测勒索软件。它监控与 UBA 不同的活动，以便能够检测到 UBA 无法检测到的攻击。

有关此功能的更多详细信息，请参见"针对勒索软件的NetApp解决方案"或"ONTAP自主勒索软件保护文档"。

存储管理系统审核

通过将ONTAP事件卸载到远程系统日志服务器来确保事件审核的完整性。此服务器可以

是Splunk等安全信息事件管理系统。

发送系统日志

从支持和可用性角度来看、日志和审核信息对于企业来说非常重要。此外、日志(系统日志)以及审核报告和输出中包含的信息和详细信息通常具有敏感性。为了保持安全控制和防护、企业必须以安全的方式管理日志和审核数据。

要将违规范围或占用空间限制为单个系统或解决方案 、必须卸载系统日志信息。因此、NetApp建议将系统日志信息安全地卸载到安全的存储或保留位置。

创建日志转发目标位置

使用 `cluster log-forwarding create` 命令为远程日志记录创建日志转发目标。

参数

使用以下参数配置 `cluster log-forwarding create` 命令：

- *目标主机。*此名称是要将日志转发到的服务器的主机名或IPv4或IPv6地址。

```
-destination <Remote InetAddress>
```

- *目标端口。*这是目标服务器侦听的端口。

```
[-port <integer>]
```

- *日志转发协议。*此协议用于向目标发送消息。

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  日志转发协议可以使用以下值之一：

  - `udp-unencrypted`(英文)无安全保障的用户数据报协议。
  - `tcp-unencrypted`(英文)无安全性的TCP。
  - `tcp-encrypted`(英文)采用传输层安全(Transport Layer Security、TLS)的TCP。

- *验证目标服务器标识。*如果此参数设置为true、则会通过验证日志转发目标的证书来验证其身份。仅当在协议字段中选择了值时、该值才能设置为true `tcpencrypted` 。

```
[-verify-server \{true|false}]
```

- *系统日志工具。*此值是用于转发日志的系统日志工具。

```
[-facility <Syslog Facility>]
```

- *跳过连接测试。*通常、该 `cluster log-forwarding create` 命令会通过发送Internet控制消息协议(Internet Control Message Protocol、ICMP) ping检查目标是否可访问、如果无法访问、则该命令将失败。将此值设置为 `true` 可绕过ping检查、以便在无法访问目标时配置目标。

```
[-force [true]]
```

NetApp建议使用 `cluster log-forwarding` 命令强制连接到 `-tcp-encrypted` 类型。

事件通知

保护离开系统的信息和数据对于维护和管理系统的安全防护至关重要。ONTAP解决方案生成的事件提供了大量有关解决方案遇到的情况、处理的信息等信息。这些数据的活力凸显了以安全方式管理和迁移数据的必要性。

`event notification create`命令会将事件筛选器定义的一组事件的新通知发送到一个或多个通知目标。以下示例显示了事件通知配置和 `event notification show` 命令、其中显示了已配置的事件通知筛选器和目标。

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

ONTAP中的存储加密

要在磁盘被盗、退回或重新利用时保护敏感数据、请使用基于硬件的NetApp存储加密或基于软件的NetApp卷加密/NetApp聚合加密。这两种机制均经过FIPS-140-2验证、如果将基于硬件的机制与基于软件的机制结合使用、该解决方案符合分类商业解决方案(CSFC)计划的要求。它可以为硬件层和软件层的机密和顶级机密空闲数据提供增强的安全保护。

空闲数据加密对于在磁盘被盗、退回或重新利用时保护敏感数据非常重要。

ONTAP 9具有三个符合联邦信息处理标准(Federal Information Processing Standard、FIPS) 140-2的空闲数据加密解决方案：

- NetApp存储加密(NSE)是一种使用自加密驱动器的硬件解决方案。
- NetApp 卷加密 (NVE) 是一种软件解决方案，支持对任何驱动器类型上的任何数据卷进行加密，在这种情况

下，每个卷都有一个唯一密钥。

- NetApp 聚合加密 (NAE) 是一种软件解决方案，支持对任何驱动器类型上的任何数据卷进行加密，在这种情况下，每个聚合都有唯一密钥。

NSE、NVE和NAE可以使用外部密钥管理或板载密钥管理器(OKM)。NSE、NVE 和 NAE 的使用不影响 ONTAP 的存储效率功能。但是，NVE 卷将从聚合重复数据删除中排除。NAE 卷参与聚合重复数据消除并从中受益。

借助 NSE、NVE 或 NAE，OKM 为空闲数据提供了独立的加密解决方案。

NVE、NAE和OKM使用ONTAP加密模块。CryptoMod列在CMVP FIPS 140-2验证模块列表中。请参阅。 "FIPS 140-2证书编号4144"

要开始OKM配置、请使用 `security key-manager onboard enable` 命令。要配置外部密钥管理互操作性协议(Key Management互操作性协议、KMIP)密钥管理器、请使用 `security key-manager external enable` 命令。从ONTAP 9.6开始、外部密钥管理器支持多租户。使用 `-vserver <vserver name>` 参数为特定SVM启用外部密钥管理。在9.6之前的版本中、此 `security key-manager setup` 命令用于配置OKM和外部密钥管理器。对于板载密钥管理、此配置将引导操作员或管理员完成用于配置OKM的密码短语设置和其他参数。

以下示例提供了部分配置：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

从ONTAP 9.4开始、您可以将true选项与结合使用 `-enable-cc-mode` `security key-manager setup` 、以要求用户在重新启动后输入密码短语。对于ONTAP 9.6及更高版本，命令语法为 `security key-manager onboard enable -cc-mode-enabled yes`。

从ONTAP 9.4开始、您可以使用具有高级权限的 `secure-purge` 功能无故障"擦除"启用了NVE的卷上的数据。擦洗加密卷上的数据可确保无法从物理介质中恢复数据。以下命令可安全清除SVM VS1上vol1上已删除的文件：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

从ONTAP 9.7开始、如果已安装VE许可证、已配置OKM或外部密钥管理器、但未使用NSE、则默认情况下会启用NAE和NVE。默认情况下、会在NAE聚合上创建NAE卷、而在非NAE聚合上会默认创建NVE卷。您可以输入以下命令来覆盖此设置：

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

从ONTAP 9.6开始、您可以使用SVM范围为集群中的数据SVM配置外部密钥管理。如果多租户环境中的每个租户都使用一个或一组不同的SVM来提供数据、则此方法最适合此环境。只有给定租户的 SVM 管理员才能访问该租户的密钥。有关详细信息、请参见 "在ONTAP 9.6及更高版本中启用外部密钥管理" ONTAP文档中的。

从ONTAP 9.11.1开始、您可以通过在SVM上指定主密钥服务器和二级密钥服务器来配置与集群模式外部密钥管理服务器的连接。有关详细信息、请参见 "配置集群模式外部密钥服务器" ONTAP文档中的。

从ONTAP 9.13.1开始、您可以在System Manager中配置外部密钥管理器服务器。有关详细信息、请参见 "管理外部密钥管理器" ONTAP文档中的。

数据复制加密

要补充静态数据加密，您可以使用带有预共享密钥的 TLS 加密集群之间的 ONTAP 数据复制流量，适用于 SnapMirror、SnapVault 或 FlexCache。

在为灾难恢复、缓存或备份复制数据时、您必须在通过线缆从一个ONTAP 集群传输到另一个集群期间保护这些数据。这样可以防止在敏感数据传输过程中对其进行恶意中间人攻击。

从 ONTAP 9.6 开始，集群对等加密为 ONTAP 数据复制功能（例如 SnapMirror、SnapVault 和 FlexCache）提供 TLS 1.2 AES-256 GCM 加密支持。加密通过两个集群对等体之间的预共享密钥（PSK）进行设置。

从 ONTAP 9.15.1 开始，集群对等加密为 ONTAP 数据复制功能（例如 SnapMirror、SnapVault 和 FlexCache）提供 TLS 1.3 AES-256 GCM 加密支持。加密通过两个集群对等体之间的预共享密钥 (PSK) 进行设置。

使用 NSE、NVE 和 NAE 等技术来保护静态数据的客户也可以使用端到端的数据加密，方法是升级到 ONTAP 9.6 或更高版本以使用集群对等加密。

集群对等加密集群对等之间的所有数据。例如，在使用 SnapMirror 时，所有对等信息以及源和目标集群对等之间的所有 SnapMirror 关系都会被加密。无法在启用集群对等加密的集群对等之间发送明文数据。

从 ONTAP 9.6 开始，新的集群对等关系默认情况下启用加密。要对 ONTAP 9.6 之前创建的集群对等关系启用加密，必须将源集群和目标集群升级到 9.6。此外，必须使用 `cluster peer modify` 命令更改源和目标集群

对等体才能使用集群对等加密。

您可以在 ONTAP 9.6 中将现有对等关系转换为使用集群对等加密，如以下示例所示：

```
On the destination cluster peer:

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the source cluster peer:

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

IPsec传输中数据加密

现在、如果客户对数据复制流量使用NetApp存储加密(NSE)或NetApp卷加密(NVE)和集群对等加密(CPE)等空闲数据加密技术、则可以升级到ONTAP 9.8或更高版本并使用、从而在混合多云Data Fabric中的客户端和存储之间使用端到端加密 IPsec。IPsec提供了NFS或SMB/CCIFS加密的替代方案、并且是iSCSI流量唯一的加密传输中选项。

在某些情况下、可能需要保护通过缆线(或传输中)传输到ONTAP SVM的所有客户端数据。这样可以防止对传输中的敏感数据进行重放和恶意中间人攻击。

从ONTAP 9.8开始、互联网协议安全性(Internet Protocol Security、IPsec)为客户端和ONTAP SVM之间的所有IP流量提供端到端加密支持。所有 IP 流量的 IPsec 数据加密包括 NFS ， iSCSI 和 SMB/CIFS 协议。IPsec 为 iSCSI 流量提供了唯一的传输加密选项。

通过缆线提供NFS加密是IPsec的主要用例之一。在ONTAP 9.8之前的版本中、NFS线上加密需要设置和配置Kerberos、才能使用krb5p对传输中的NFS数据进行加密。在每个客户环境中、这并不总是简单或容易实现的。

现在、如果客户对数据复制流量使用NetApp存储加密(NSE)或NetApp卷加密(NVE)和集群对等加密(CPE)等空闲数据加密技术、则可以升级到ONTAP 9.8或更高版本并使用、从而在混合多云Data Fabric中的客户端和存储之间使用端到端加密 IPsec。

IPsec是IETF标准。ONTAP在传输模式下使用IPsec。它还利用Internet密钥交换(Internet Key Exchange、IKE)协议版本2、该协议使用预共享密钥(PSK)在客户端与使用IPv4或IPv6的ONTAP之间协商密钥材料。默认情况下，IPsec使用Suite-B AES-GCM 256位加密。此外、还支持采用256位加密的Suite B AES-GMAC256和AES-CBC256。

尽管必须在集群上启用IPsec功能、但它通过使用安全策略数据库(SPD)条目应用于单个SVM IP地址。策略(SPD)条目包含客户端IP地址(远程IP子网)、SVM IP地址(本地IP子网)、要使用的加密密码套件以及通过IKEv2进行身份验证并建立IPsec连接所需的预共享密钥(PSK)。除了IPsec策略条目之外，还必须为客户端配置相同的信息(本地和远程IP、PSK和密码套件)，然后流量才能通过IPsec连接进行传输。从ONTAP 9.10.1开始，增加了

对IPsec证书身份验证的支持。这将删除IPsec策略限制并启用Windows操作系统对IPsec的支持。

如果客户端和SVM IP地址之间存在防火墙、则必须允许ESP和UDP (端口500和4500)协议(入站(入站)和出站(出站))、以便成功进行I可 得2协商、从而允许IPsec流量。

对于 NetApp SnapMirror 和集群对等流量加密，仍然建议使用基于 IPsec 的集群对等加密（ Cluster peering encryption ， CPE ），以便通过线缆安全地进行传输。CPE对这些工作负载的性能优于IPsec。您不需要IPsec许可证，并且没有导入或导出限制。

您可以在集群上启用IPsec、并为单个客户端和单个SVM IP地址创建SPD条目、如以下示例所示：

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

相关信息

"准备在ONTAP网络上使用IP安全性"

ONTAP中的FIPS模式以及TLS和SSL管理

FIPS 140-2标准规定了安全系统中加密模块的安全要求、用于保护计算机和电信系统中的敏感信息。FIPS 140-2标准适用于加密模块、而不是产品、架构、数据或生态系统。加密模块是实施NIST批准的安全功能的特定组件(硬件、软件、固件或这三者的组合)。

启用FIPS 140-2合规性会影响ONTAP 9内部和外部的其他系统和通信。NetApp强烈建议在具有控制台访问权限的非生产系统上测试这些设置。

从ONTAP 9.11.1和TLS 1.3支持开始、您可以验证FIPS 140-2。

FIPS配置适用于ONTAP和平台BMC。

NetApp ONTAP的FIPS模式配置

NetApp ONTAP具有FIPS模式配置、可为控制平面例化增加的安全级别：

- 从9.11.1 9.11.1开始、如果启用了FIPS 140-2合规性模式、则TLSv1、TLSv1.1和SSLv3将被禁用、只有TSLv1.2和TSLv1.3保持启用状态。它会影响ONTAP 9内部和外部的其他系统和通信。如果启用FIPS 140-2合规模式、然后再禁用、TLSv1、TLSv1.1和SSLv3将保持禁用状态。TLSv1.2或TLSv1.3将保持启用状态、具体取决于先前的配置。
- 对于9.11.1之前的ONTAP版本、如果启用了FIPS 140-2合规性模式、则TLSv1和SSLv3都将被禁用、只有TLSv1.1和TLSv1.2保持启用状态。启用 FIPS 140-2 合规模式后， ONTAP 会阻止您同时启用 TLSv1 和 SSLv3 。如果启用 FIPS 140-2 合规模式，然后将其禁用， TLSv1 和 SSLv3 将保持禁用状态，但 TLSv1.2 或 TLSv1.1 和 TLSv1.2 均已启用，具体取决于先前的配置。

- "NetApp加密安全模块(NCSM)"已通过FIPS 140-2 1级验证，可提供基于软件的合规性。

> NIST已提交FIPS-140-2标准、NCSM将进行FIPS-140-2和FIPS-140-2验证。所有FIPS 140-2验证将于2026年9月21日变为历史状态、即新证书提交的最后一天之后五年。

启用**FIPS-140-2**和**FIPS-140-2**合规模式

从ONTAP 9开始、您可以为集群范围的控制面板接口启用FIPS-140-2和FIPS-140-2合规性模式。

- "启用FIPS"
- "查看FIPS状态"

FIPS支持和协议

`security config modify`命令可用于修改现有集群范围的安全配置。如果启用FIPS兼容模式、则集群将自动仅选择TLS协议。

- 使用 `-supported-protocols` 参数可独立于FIPS模式包含或排除TLS协议。默认情况下、FIPS模式处于禁用状态、TLSv1.3 (从ONTAP 9.11.1开始)和TLSv1.2协议处于启用状态。
- 默认情况下、先前版本的ONTAP启用了以下TLS协议：
  - TLSv1.1 (从ONTAP 9.12.1开始、默认情况下处于禁用状态)
  - TLSv1 (从ONTAP 9.8开始、默认情况下处于禁用状态)
- 为了实现向后兼容性、ONTAP支持在FIPS模式处于禁用状态时将SSLv3添加到支持的协议列表中。

FIPS支持和加密

- 使用 `-supported-cipher-suites` 参数仅配置高级加密标准(Advanced Encryption Standard、AES)或AES和3DES。
- 您可以通过指定来禁用RC4等弱加密 `!RC4`。默认情况下，支持的密码设置为 `ALL:!LOW:!aNULL:!EXP:!eNULL`。此设置意味着、协议支持的所有密码套件均已启用、但使用64位或56位加密算法且无身份验证、无加密、无导出的密码套件以及低加密密码套件除外。
- 选择可与相应选定协议一起使用的密码套件。配置无效可能会导致某些功能无法正常运行。
- 有关正确的密码字符串语法、请参见 ""使用"页面"OpenSSL上的(由OpenSSL软件基金会发布)。从ONTAP 9.9.1及更高版本开始、您无需在修改安全配置后手动重新启动所有节点。

SSH和**TLS**安全强化

通过SSH管理ONTAP 9需要使用OpenSSH客户端5.7或更高版本。SSH客户端必须使用椭圆曲线数字签名算法(ECDSA)公共密钥算法协商、才能成功建立连接。

要增强TLS安全性、请仅启用TLS 1.2、并使用支持完全正向保密(PFS)的密码套件。PFS是一种密钥交换方法、与TLS 1.2等加密协议结合使用时、有助于防止攻击者解密客户端和服务器之间的所有网络会话。

启用**TLSv1.2**和支持**PFS**的密码套件

要仅启用TLS 1.2和支持PFS的密码套件、请 `security config modify`在高级权限级别使用命令。

> 在更改SSL接口配置之前、请确保客户端在连接到ONTAP以保持与ONTAP的连接时支持密码DHE和ECDHE。

示例

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

确认 `y` 每个提示。有关PFS的详细信息，请参见此 "NetApp 博客"。

相关信息

"联邦信息处理标准(FIPS)出版物140"

创建**CA**签名的数字证书

对于许多组织而言、用于ONTAP Web访问的自签名数字证书不符合其InfoSec策略。在生产系统上、NetApp最佳做法是安装CA签名的数字证书、以便将集群或SVM作为SSL服务器进行身份验证。

您可以使用 `security certificate generate-csr` 命令生成证书签名请求(CSR)、并使用 `security certificate install` 命令安装从CA收到回的证书。

步骤

1. 要创建由组织的CA签名的数字证书、请执行以下操作：
   a. 生成CSR。
   b. 按照组织的过程从组织的CA使用CSR请求数字证书。例如、使用Microsoft Active Directory证书服务Web界面、转到 `<CA_server_name>/certsrv` 并请求证书。
   c. 在ONTAP中安装数字证书。

联机证书状态协议

启用联机证书状态协议(Online Certificate Status Protocol、OCSP)后、使用TLS通信(例如LDAP或TLS)的ONTAP应用程序可以接收数字证书状态。应用程序将收到签名响应、表示请求的证书正常、已撤销或未知。

OCSP无需证书吊销列表(Certificate Revocation List、CRL)即可确定数字证书的当前状态。

默认情况下， OCSP 证书状态检查处于禁用状态。可以使用命令打开 `security config ocsp enable -app name`**应用程序，其中应用程序名可以是** `autosupport`、、 `audit_log`、 `fabricpool`、 `ems`、 `kmip` `ldap_ad` `ldap_nis_namemap`**或** `all`。此命令需要高级权限级别。

SSHv2管理

`security ssh modify`命令会将集群或SVM的SSH密钥交换算法、密码或MAC算法的现有配置替换为您指定的配置设置。

NetApp建议执行以下操作：

- 对用户会话使用密码。
- 使用公共密钥访问计算机。

支持的密码和密钥交换

密码	密钥交换
aes256-ctr	迪夫-赫尔曼-组-交换- SHA256 (SHA-2)
aes192-ctr	迪比-赫尔曼-组-交换- SHA1 (SH-1)
aes128-ctr	迪比-赫尔曼-组14-SHA1 (SHA-1)
aes256-cbc	迪夫-赫尔曼-组1-SHA1 (SH-1)
aes192-cbc	-
aes128-cbc	-
ES128-GCM	-
ES256-GCM	-
3des-cbc	-

支持**AES**和**3DES**对称加密

ONTAP还支持以下类型的AES和3DES对称加密(也称为密码)：

- HMAC-SHA1
- hmac-sha1-96
- HMAC-MD5
- hmac-md5-96
- HMAC-里 布姆德160
- UMAC-64
- UMAC-64
- UMAC-128
- hmac-sha2-256
- hmac-sha2-512
- HMAC-SHA1-ETM
- HMAC-SHA1-96-ETM

- HMAC-SHA2-256-ETM
- HMAC-SHA2-512 ETM
- HMAC-MD5-ETM
- HMAC-MD5-96-ETM
- HMAC-提供160-ETM
- UMAC-64-ETM
- UMAC-128-ETM

SSH管理配置适用于ONTAP和平台BMC。

NetApp AutoSupport

通过ONTAP的AutoSupport功能、您可以主动监控系统的运行状况、并自动向NetApp技术支持、组织的内部支持团队或支持合作伙伴发送消息和详细信息。默认情况下、首次配置存储系统时、系统会启用向NetApp技术支持发送的AutoSupport消息。此外、AutoSupport在启用后24小时开始向NetApp技术支持发送消息。此24小时时间段是可配置的。要利用与组织内部支持团队的通信、必须完成邮件主机配置。

只有集群管理员才能执行AutoSupport管理(配置)。SVM 管理员没有 AutoSupport 访问权限。可以禁用 AutoSupport 功能。但是、NetApp建议启用此功能、因为AutoSupport有助于在存储系统出现问题时加快问题识别和解决速度。默认情况下、即使禁用AutoSupport、系统也会收集AutoSupport信息并将其存储在本地。

有关AutoSupport消息的更多详细信息、包括各种消息中包含的内容以及不同类型的消息的发送位置、请参见文档。 "NetApp数字顾问"

AutoSupport消息包含敏感数据、包括但不限于以下各项：

- 日志文件
- 有关特定子系统的上下文相关数据
- 配置和状态数据
- 性能数据

AutoSupport支持使用HTTPS和SMTP传输协议。由于 AutoSupport 消息的敏感性， NetApp 强烈建议使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。

此外、您还应利用 `system node autosupport modify` 命令指定AutoSupport数据的目标(例如、NetApp技术支持、组织的内部运营或合作伙伴)。此命令还允许您指定要发送的特定AutoSupport详细信息(例如性能数据、日志文件等)。

要完全禁用AutoSupport、请使用 `system node autosupport modify -state disable` 命令。

网络时间协议

尽管您可以通过ONTAP手动设置集群上的时区、日期和时间、但您必须配置网络时间协议(NTP)服务器、以便至少与三个外部NTP服务器同步集群时间。

如果集群时间不准确，可能会出现问题。尽管您可以通过ONTAP手动设置集群上的时区、日期和时间、但您必须配置网络时间协议(NTP)服务器、以便将集群时间与外部NTP服务器同步。

从 ONTAP 9.5 开始，您可以为 NTP 服务器配置对称身份验证。

使用命令最多可以关联10个外部NTP服务器 `cluster time-service ntp server create` 。为了保证冗余和时间服务质量、应至少将三个外部NTP服务器与集群相关联。

有关在ONTAP中配置NTP的详细信息，请参见 "管理集群时间（仅限集群管理员）"。

NAS文件系统本地帐户(CIFS工作组)

工作组客户端身份验证为ONTAP解决方案提供了与传统域身份验证态势一致的额外一层安全保护。使用 `vserver cifs session show` 命令可显示许多与状态相关的详细信息、包括IP信息、身份验证机制、协议版本和身份验证类型。

从ONTAP 9开始、您可以在工作组中配置CIFS服务器、其中CIFS客户端会使用本地定义的用户和组向该服务器进行身份验证。工作组客户端身份验证为ONTAP解决方案提供了与传统域身份验证态势一致的额外一层安全保护。要配置CIFS服务器、请使用 `vserver cifs create` 命令。创建CIFS服务器后、您可以将其加入CIFS域或工作组。要加入工作组、请使用 `-workgroup` 参数。示例配置如下：

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

工作组模式下的CIFS服务器仅支持Windows NT LAN Manager (NTLM)身份验证、而不支持Kerberos身份验证。

NetApp建议对CIFS工作组使用NTLM身份验证功能、以维护组织的安全防护。要验证CIFS安全防护、NetApp建议使用 `vserver cifs session show` 命令显示与防护相关的大量详细信息、包括IP信息、身份验证机制、协议版本和身份验证类型。

NAS文件系统审核

NAS文件系统在当今的威胁形势下占用的空间越来越大、审核功能对于支持可见性至关重要。

安全需要验证。ONTAP 在整个解决方案中提供了更多的审核事件和详细信息。由于 NAS 文件系统在当今的威胁环境中占据了越来越大的空间，审核功能对于支持可见性至关重要。由于 ONTAP 中改进的审核功能，CIFS 审核详细信息比以往任何时候都更加丰富。关键详细信息（包括以下内容）会与创建的事件一起记录：

- 文件、文件夹和共享访问
- 创建、修改或删除的文件
- 文件读取访问成功
- 读取或写入文件的尝试失败
- 文件夹权限更改

创建审核配置

您必须启用CIFS审核才能生成审核事件。使用 `vserver audit create` 命令创建审核配置。默认情况下、审核日志会根据大小使用轮换方法。如果在"旋转参数"字段中指定了基于时间的旋转选项、则可以使用该选项。其他日志审核轮换配置详细信息包括轮换计划、轮换限制、一周的轮换日期和轮换大小。以下文本提供了一个示例配置、其中描述了一个审核配置、该配置使用基于时间的每月轮换、计划在一周中的所有日期的12：30进行轮换。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS审核事件

CIFS审核事件如下：

- 文件共享：在使用相关命令添加、修改或删除CIFS网络共享时生成审核事件 `vserver cifs share` 。
- **Audit policy change**：使用相关命令禁用、启用或修改审核策略时生成审核事件 `vserver audit` 。
- 用户帐户：在创建或删除本地CIFS或UNIX用户、启用、禁用或修改本地用户帐户或重置或更改密码时生成审核事件。此事件使用 `vserver cifs users-and-groups local-group` 命令或相关 `vserver services name-service unix-user` 命令。
- 安全组：使用命令或相关命令创建或删除本地CIFS或UNIX安全组时、生成审核事件 `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- 授权策略更改：在使用命令授予或撤消CIFS用户或CIFS组的权限时生成审核事件 `vserver cifs users-and-groups privilege` 。

此功能基于系统审核功能、管理员可以通过此功能从数据用户的角度查看系统允许执行的操作。

REST API对**NAS**审核的影响

ONTAP允许管理员帐户使用REST API访问和操作SMB/CIFS/NFS或NFS文件。虽然REST API只能由ONTAP管理员运行、但REST API命令会绕过系统NAS审核日志。此外、使用REST API时、ONTAP管理员也可以绕过文件权限。但是、系统命令历史记录日志中会捕获管理员对文件使用REST API执行的操作。

创建无访问权限**REST API**角色

您可以通过创建不能通过REST访问ONTAP卷的REST API角色来防止ONTAP管理员使用REST API进行文件访问。要配置此角色、请完成以下步骤。

/api/storage/volumes REST API 不仅仅用于文件访问。System Manager 和其他 GUI 界面使用它来创建、查看和修改卷。

步骤

1. 创建一个新的REST角色、此角色不能访问存储卷、但可以访问所有其他REST API。

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 将管理员帐户分配给您在上一步中创建的新REST API角色。

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

如果要阻止内置ONTAP集群管理员帐户使用REST API进行文件访问，则需要首先 "创建新的管理员帐户并禁用或删除此内置帐户"。

配置和启用CIFS SMB签名和签章

您可以配置和启用SMB签名、通过确保存储系统和客户端之间的流量不会受到重放攻击或中间人攻击的影响来保护Data Fabric的安全性。SMB签名通过验证SMB消息是否具有有效签名来进行保护。

关于此任务

SMB协议是文件系统和架构的一个常见威胁媒介。为了应对这一载体、ONTAP 9解决方案使用行业标准SMB签名和密封。SMB签名可确保存储系统和客户端之间的流量不会受到重放攻击或中间人攻击的影响、从而保护Data Fabric的安全性。它通过验证SMB消息是否具有有效签名来实现此目的。

虽然出于性能考虑、默认情况下会禁用SMB签名、但NetApp强烈建议启用它。此外、ONTAP解决方案还支持SMB加密、也称为密封。这种方法可以在共享的基础上安全地传输数据。默认情况下， SMB 加密处于禁用状态。但是、NetApp建议您启用SMB加密。

SMB 2.0及更高版本现在支持LDAP签名和签章。签名(防止篡改)和签章(加密)可确保SVM和Active Directory服务器之间的安全通信。SMB 3.0及更高版本现在支持加速AES新指令(Intel AES NI)加密。Intel AES NI改进了AES算法、并在支持的处理器系列中加快了数据加密速度。

步骤

1. 要配置和启用SMB签名，请使用 `vserver cifs security modify` 命令并验证参数是否 `-is-signing-required` 设置为 `true`。请参见以下配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. 要配置和启用SMB密封和加密，请使用 `vserver cifs security modify` 命令并验证参数是否 `-is-smb-encryption-required` 设置为 `true`。请参见以下配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFS安全

导出规则是导出策略的功能要素。导出规则会将卷的客户端访问请求与您配置的特定参数进行匹配、以确定如何处理客户端访问请求。导出策略必须至少包含一个导出规则，才能访问客户端。如果导出策略包含多个规则，则这些规则将按照它们在导出策略中的显示顺序进行处理。

访问控制是保持安全防护的核心。因此、ONTAP会使用导出策略功能限制NFS卷访问权限、使其只能访问与特定参数匹配的客户端。导出策略包含一个或多个导出规则，用于处理每个客户端访问请求。导出策略与每个卷关联、用于配置客户端对卷的访问。此过程的结果将确定是授予还是拒绝(并显示权限被拒绝的消息)客户端对卷的访问权限。此过程还会确定为卷提供的访问级别。

要使客户端能够访问数据、SVM上必须存在具有导出规则的导出策略。一个SVM可以包含多个导出策略。

规则顺序由规则索引编号决定。如果某个规则与客户端匹配、则会使用该规则的权限、而不会处理其他规则。如果没有匹配的规则，客户端将被拒绝访问。

导出规则通过应用以下条件来确定客户端访问权限：

- 发送请求的客户端使用的文件访问协议(例如、NFSv4或SMB)
- 客户端标识符（例如，主机名或 IP 地址）
- 客户端用于进行身份验证的安全类型(例如、Kerberos v5、NTLM或AUATT_SYS)

如果某个规则指定了多个条件、而客户端与其中一个或多个条件不匹配、则该规则不适用。

示例导出策略包含具有以下参数的导出规则：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

安全类型决定了客户端接收的访问级别。这三个访问级别分别为只读、读写和超级用户(对于具有用户ID的客户端 `0`)。由于按此顺序评估由安全类型确定的访问级别、因此您必须遵守列出的规则：

导出规则中访问级别参数的规则

使客户端能够获得以下访问级别	这些访问参数必须与客户端的安全类型匹配
普通用户只读	只读(`-rorule`)
普通用户读写	只读(`-rorule`)和读写(`-rwrule`()
超级用户只读	只读(`-rorule`)和 `-superuser`
超级用户读写	只读(`-rorule`)和读写(`-rwrule`)和 `-superuser`

以下是这三个访问参数中每一个参数的有效安全类型：

- 任意
- 无
- 从不

以下安全类型不适用于 `-superuser` 参数：

- krb5
- NTLM
- 系统

访问参数结果的规则

如果客户端的安全类型...	然后...
与访问参数中指定的安全类型匹配。	客户端使用自己的用户ID接收该级别的访问。
与指定的安全类型不匹配，但访问参数包括选项 `none`。	客户端接收该级别的访问权限、并接收用户ID由参数指定的匿名用户 `-anon` 。
与指定的安全类型不匹配，并且访问参数不包括选项 `none`。	客户端不会收到该级别的任何访问权限。 此限制不适用于 `-superuser` 参数、因为此参数始终包括none、即使未指定也是如此。

Kerberos 5和Krb5p

从 ONTAP 9 开始，支持具有隐私服务的 Kerberos 5 身份验证 (krb5p)。Krbp5 身份验证模式具有较高的安全性，可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，达到保护目的。ONTAP解决方案支持Kerberos 128位和256位AES加密。隐私服务包括验证所接收数据的完整性、对用户进行身份验证以及在传输之前对数据进行加密。

krb5p选项在导出策略功能中最常用、并设置为加密选项。krb5p身份验证方法可用作身份验证参数、如以下示例所示：

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

启用轻型目录访问协议签名和签章

支持签名和签章、以便对LDAP服务器的查询启用会话安全性。此方法提供了一种替代基于TLS的LDAP会话安全性的方法。

签名功能使用密钥技术确认LDAP有效负载数据的完整性。密封功能会对LDAP有效负载数据进行加密、以避免以明文形式传输敏感信息。SVM上的会话安全设置与LDAP服务器上可用的设置相对应。默认情况下、LDAP签名和签章处于禁用状态。

步骤

1. 要启用此功能、请使用参数运行 `vserver cifs security modify` 命令 `session-security-for-ad-ldap` 。

   LDAP安全功能选项：

   - 无：默认值，无签名或签章
   - **Sign**：对LDAP流量进行签名
   - **Seal**：对LDAP流量进行签名和加密

   > 符号和签章参数是累积的、这意味着如果使用签名选项、则结果为LDAP与签名。但是、如果使用了密封选项、则结果为符号和密封。此外、如果未为此命令指定参数、则默认值为none。

   以下是配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

创建并使用NetApp FPolicy

您可以创建和使用FPolicy、这是ONTAP解决方案的基础架构组件、支持合作伙伴应用程序监控和设置文件访问权限。更强大的应用程序之一是存储工作负载安全性、这是一款NetApp SaaS应用程序、可集中查看和控制混合云环境中的所有企业数据访问、以确保满足安全性和合规性目标。

访问控制是一个关键的安全概念。可见性以及对文件访问和文件操作的响应能力对于维护您的安全防护至关重要。为了提供文件可见性和访问控制、ONTAP解决方案使用NetApp FPolicy功能。

可以根据文件类型设置文件策略。FPolicy用于确定存储系统如何处理来自各个客户端系统的操作请求、例如创建、打开、重命名和删除。从ONTAP 9开始、FPolicy文件访问通知框架得到了增强、具有筛选控件和短时网络

中断故障恢复能力。

步骤

1. 要利用FPolicy功能、必须先使用命令创建FPolicy策略 `vserver fpolicy policy create` 。

   此外、如果使用FPolicy查看和收集事件、请使用 `-events` 参数。通过ONTAP提供的额外粒度、可以筛选和访问用户名级别的控制。要使用用户名控制权限和访问、请指定 `-privilege-user-name` 参数。

   以下文本提供了创建FPolicy的示例：

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. 创建FPolicy策略后、必须使用命令启用它 `vserver fpolicy enable` 。此命令还会设置FPolicy条目的优先级或顺序。

   FPolicy顺序非常重要、因为如果多个策略订阅了同一个文件访问事件、则该顺序指示授予或拒绝访问的顺序。

   以下文本提供了用于启用FPolicy策略并使用命令验证配置的示例配置 `vserver fpolicy show` ：

   ```
   cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
   vs2_pol -sequence-number 5

   cluster1::> vserver fpolicy show
   Vserver                 Policy Name                  Sequence  Status
   Engine
   ----------------------- ---------------------------- --------  -------
   -------
   vs1.example.com         vs1_pol
   vs2.example.com         vs2_pol
    external
   2 entries were displayed.
   ```

FPolicy增强功能

ONTAP 9包括以下各节所述的FPolicy增强功能。

筛选控件

新筛选器可用于 `SetAttr` 和删除有关目录活动的通知。

如果在异步模式下运行的 FPolicy 服务器发生网络中断，则在中断期间生成的 FPolicy 通知将存储在存储节点上。当 FPolicy 服务器恢复联机时，它会收到存储的通知警报，并可从存储节点提取这些通知。在中断期间可以存储通知的时间长度可配置为长达 10 分钟。

ONTAP中LIF角色的安全特征

LIF是具有相关特征的IP地址或全球通用端口名称(WWPN)、例如角色、主端口、主节点、要故障转移到的端口列表以及防火墙策略。您可以在集群通过网络发送和接收通信的端口上配置 LIF 。了解每个LIF角色的安全特征至关重要。

LIF角色

LIF角色可以是以下角色：

- 数据**LIF**：与SVM关联的用于与客户端通信的LIF。
- 集群**LIF**：用于在集群中的节点之间传输集群内流量的LIF。
- 节点管理**LIF**：提供专用IP地址以管理集群中的特定节点的LIF。
- 集群管理**LIF**：为整个集群提供单一管理接口的LIF。
- 集群间**LIF**：用于跨集群通信、备份和复制的LIF。

每个**LIF**角色的安全特征

	Data LIF	集群LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
是否需要专用IP子网？	否	是	否	否	否
是否需要安全网络?	否	是	否	否	是
默认防火墙策略	限制性很强	完全开放	中	中	限制性很强
防火墙是否可自定义？	是	否	是	是	是

- 由于集群LIF已完全打开、没有可配置的防火墙策略、因此它必须位于安全隔离网络上的专用IP子网上。
- LIF角色永远不应暴露在互联网上。

要了解有关保护 LIF 的更多信息，请参阅 "为 LIF 配置防火墙策略"。本页面还提供了从ONTAP 9.10.1 开始的 LIF 服务策略的详细信息。

要了解有关如何创建新服务策略的更多信息，请参阅 `network interface service-policy create` 命令 "命令参考。"

协议和端口安全性

除了执行机载安全操作和功能之外、解决方案的强化还必须包括机下安全机制。利用防火

墙、入侵防御系统(IPS)和其他安全设备等其他基础架构设备来过滤和限制对ONTAP的访问、是建立和保持严格安全防护的有效方法。此信息是筛选和限制对环境及其资源的访问的关键组成部分。

常用协议和端口

服务	端口 / 协议	说明
SSH	22/TCP	SSH登录
telnet	23/TCP	远程登录
Domain	53/TCP	域名服务器
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	远程操作步骤调用
NTP	123/UDP	网络时间协议
msrpc	135/TCP	Microsoft远程过程调用
Netbios-name	137/TCP 137/UDP	NetBIOS 名称服务
netbios-ssn	139/TCP	NetBIOS 服务会话
SNMP	161/UDP	SNMP
HTTPS	443/TCP	安全链接：http
microsoft-ds	445/TCP	Microsoft目录服务
IPsec	500/UDP	互联网协议安全性
mount	635/UDP	NFS 挂载
named	953/UDP	名称守护进程
NFS	2049/UDP 2049/TCP	NFS 服务器守护进程
nrv	2050/TCP	NetApp远程卷协议
iscsi	3260/TCP	iSCSI 目标端口
Lockd	4045/TCP 4045/UDP	NFS 锁定守护进程
NFS	4046/TCP	NFS mountf协议
acp-proto	4046/UDP	记帐协议
rquotad	4049/UDP	NFS Rquotad 协议
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	互联网协议安全性

服务	端口 / 协议	说明
acp	5125/UDP 5133/UDP 5144/TCP	磁盘的备用控制端口
Mdns	5353/UDP	多播 DNS
HTTPS	5986/UDP	HTTPS端口：侦听二进制协议
TELNET	8023/TCP	节点范围Telnet
HTTPS	8443/TCP	通过链接：HTTPS使用7MTT图形用户界面工具
RSH	8514/TCP	节点范围 RSH
KMIP	9877/TCP	KMIP客户端端口(仅限内部本地主机)
ndmp	10000/TCP	NDMP
cifs 见证端口	40001/TCP	CIFS见证端口
TLS	50000/TCP	传输层安全性
Iscsi	65200/TCP	iSCSI端口
SSH	65502/TCP	安全外壳
vsun	65503/TCP	vsun

NetApp内部端口

端口 / 协议	说明
900	NetApp 集群 RPC
902	NetApp 集群 RPC
904	NetApp 集群 RPC
905	NetApp 集群 RPC
910	NetApp 集群 RPC
911	NetApp 集群 RPC
913	NetApp 集群 RPC
914	NetApp 集群 RPC
915	NetApp 集群 RPC
918	NetApp 集群 RPC
920	NetApp 集群 RPC
921	NetApp 集群 RPC
924	NetApp 集群 RPC
925	NetApp 集群 RPC
927	NetApp 集群 RPC
928	NetApp 集群 RPC

端口 / 协议	说明
929	NetApp 集群 RPC
931	NetApp 集群 RPC
932	NetApp 集群 RPC
933	NetApp 集群 RPC
934	NetApp 集群 RPC
935	NetApp 集群 RPC
936	NetApp 集群 RPC
937	NetApp 集群 RPC
939	NetApp 集群 RPC
940	NetApp 集群 RPC
951	NetApp 集群 RPC
954	NetApp 集群 RPC
955	NetApp 集群 RPC
956	NetApp 集群 RPC
958	NetApp 集群 RPC
961	NetApp 集群 RPC
963	NetApp 集群 RPC
964	NetApp 集群 RPC
966	NetApp 集群 RPC
967	NetApp 集群 RPC
7810	NetApp 集群 RPC
7811	NetApp 集群 RPC
7812	NetApp 集群 RPC
7813	NetApp 集群 RPC
7814	NetApp 集群 RPC
7815	NetApp 集群 RPC
7816	NetApp 集群 RPC
7817	NetApp 集群 RPC
7818	NetApp 集群 RPC
7819	NetApp 集群 RPC
7820	NetApp 集群 RPC
7821	NetApp 集群 RPC
7822	NetApp 集群 RPC

端口 / 协议	说明
7823	NetApp 集群 RPC
7824	NetApp 集群 RPC

ONTAP SnapCenter技术报告

SnapCenter为应用程序一致的数据保护和克隆管理提供了一个统一平台。SnapCenter通过应用程序集成的工作流简化备份、还原和克隆生命周期管理。SnapCenter利用基于存储的数据管理功能、提高了性能和可用性、缩短了测试和开发时间。

这些技术报告对产品文档进行了扩展"SnapCenter"。

SnapCenter for Oracle

"TR-4700：《适用于Oracle数据库的SnapCenter插件最佳实践》"
NetApp SnapCenter是一个统一的可扩展平台、用于实现Oracle一致的数据保护、可通过集中控制和监管自动执行复杂操作。了解使用SnapCenter部署Oracle数据库的建议实践。

"TR-4964：《使用SnapCenter 服务备份、还原和克隆Oracle数据库》"了解如何设置SnapCenter服务以备份、还原和克隆部署到Amazon FSx for ONTAP存储和EC2计算实例的Oracle数据库。虽然设置和使用起来容易得多、但SnapCenter服务可通过SnapCenter界面提供关键功能。

SnapCenter for Microsoft SQL Server

"TR-4714：《使用NetApp SnapCenter的Microsoft SQL Server最佳实践》"
了解如何使用SnapCenter在NetApp存储上成功部署Microsoft SQL Server以实现数据保护。

SnapCenter for Microsoft Exchange Server

"TR-4681：《使用NetApp SnapCenter的Microsoft Exchange Server最佳实践》"
了解如何使用SnapCenter在NetApp存储上成功部署Microsoft Exchange Server以实现数据保护。

适用于SAP HANA的SnapCenter

"TR-4614：《使用 SnapCenter 实现 SAP HANA 备份和恢复》"SnapCenter是一个统一的可扩展平台、可为SAP HANA和其他数据库提供应用程序一致的数据保护。SnapCenter 提供集中控制和监管，同时委派用户管理应用程序专用的备份，还原和克隆作业。借助 SnapCenter ，数据库和存储管理员可以通过一种工具来管理各种应用程序和数据库的备份，还原和克隆操作。

"TR-4926：《基于Amazon FSX的SAP HANA for NetApp ONTAP —使用SnapCenter 进行备份和恢复》"了解在Amazon FSx for NetApp ONTAP和SnapCenter上实施SAP HANA数据保护的建议实践。主题包括SnapCenter概念、配置建议和操作工作流、包括配置、备份操作、 以及还原和恢复操作。

"TR-4667：《借助SnapCenter自动执行SAP HANA系统复制和克隆操作》"借助SnapCenter存储克隆以及灵活定义克隆前和克隆后操作的选项、SAP基础管理员可以加快和自动执行SAP系统复制、克隆或刷新操作。立即了解在任何主存储或二级存储上选择任何SnapCenter Snapshot备份、让您可以解决最重要的使用情形、包括逻辑损坏、灾难恢复测试或SAP QA系统更新。

"TR-4719：《使用SnapCenter进行SAP HANA系统复制备份和恢复》"
了解如何在SAP HANA系统复制环境中使用SnapCenter技术和SAP HANA插件进行备份和恢复。

"TR-4667：《借助SnapCenter自动执行SAP HANA系统复制和克隆操作》"在存储层创建应用程序一致

的NetApp Snapshot备份的能力是系统复制和系统克隆操作的基础。基于存储的Snapshot备份是使用适用于SAP HANA的NetApp SnapCenter 插件以及SAP HANA数据库提供的接口创建的。SnapCenter 会将Snapshot备份注册到SAP HANA备份目录中、以便这些备份可用于还原和恢复以及克隆操作。

SnapCenter强化指南

"TR-4957：《NetApp SnapCenter安全强化指南》"
了解如何配置SnapCenter以帮助组织满足规定的信息系统机密性、完整性和可用性安全目标。

ONTAP技术报告

借助FabricPool数据分层解决方案、企业的整体闪存系统用户体验得以改善、同时避免了为提高存储效率而重新构建应用程序所带来的麻烦。FabricPool可减少系统环境的存储占用空间和相关成本。活动数据保留在高性能SSD上。非活动数据分层到低成本对象存储、同时保持存储效率。

这些技术报告对产品文档进行了扩展"ONTAP FabricPool"。

"TR-4598：FabricPool 最佳实践"
了解FabricPool的功能、要求、实施和建议实践。

"TR-4826：《采用StorageGRID的NetApp FabricPool建议指南》"
了解将StorageGRID作为ONTAP组件FabricPool的容量层进行部署和规模估算的建议做法。本文档还介绍了使用StorageGRID时的核心功能、要求、实施和建议实践。

"TR-4695：《使用NetApp FabricPool进行数据库存储层化》"
了解FabricPool在各种数据库(包括Oracle关系数据库管理系统(RDBMS))中的优势和配置选项。

ONTAP虚拟化技术报告

NetApp虚拟化解决方案可帮助您从服务器中实现最大价值。借助基于开创性的高性能ONTAP闪存系统构建的响应式虚拟服务器基础架构、您可以更快地访问数据。您的粒度虚拟基础架构可在不中断运行的情况下扩展到数PB的数据、从而为您提供共享访问多个工作负载所需的性能。ONTAP通过关键合作伙伴关系、部署指导、应用程序集成和卓越的设计、帮助简化虚拟服务器基础架构部署并降低其复杂性。ONTAP为内部和云端的强大虚拟化环境提供了许多建议的实践和解决方案。

这些技术报告对产品文档进行了扩展"适用于 VMware vSphere 的 ONTAP 工具"。

"TR-4597 ：适用于 ONTAP 的 VMware vSphere"近20年来、ONTAP一直是适用于VMware vSphere环境的领先存储解决方案、并不断增加创新功能、以简化管理并降低成本。本文档介绍适用于vSphere的ONTAP 解决方案、包括最新的产品信息和建议的实践、以简化部署、降低风险和管理。

"TR-4400：《采用NetApp ONTAP 的VMware vSphere虚拟卷(vvol)》"二十年来、ONTAP一直是适用于VMware vSphere环境的领先存储解决方案、并不断增加创新功能、以简化管理并降低成本。本文档介绍了适用于VMware vSphere虚拟卷(vvol)的ONTAP功能、包括最新的产品信息和用例、建议的实践以及其他可简化部署和减少错误的信息。

"TR-4900:《采用NetApp ONTAP的VMware Site Recovery Manager》" 自2002年将ONTAP引入现代数据中心以来、它一直是VMware vSphere环境中领先的存储解决方案、并不断增加创新功能、以简化管理、同时降低成本。本文档介绍了VMware行业领先的灾难恢复(Disaster Recovery、DR)软件ONTAP 解决方案for VMware Site Recovery Manager (SRM)、其中包括最新的产品信息和建议的实践、用于简化部署、降低风险并简化日常管理。

"ONTAP 和 vSphere 自动化简介"自VMware ESX问世以来、自动化一直是管理VMware环境不可或缺的一部分。能够将基础架构作为代码进行部署，并将实践扩展到私有云操作，有助于缓解对规模，灵活性，自行配置和效率的顾虑。本文档介绍了用于自动执行ONTAP和VMware vSphere环境的ONTAP 解决方案。

"WP-7353：《适用于VMware vSphere的ONTAP工具—产品安全性》"本文档介绍了用于保护适用于VMware vSphere 9.X的ONTAP工具免受产品环境中现有威胁和新出现威胁的技术。

"WP-7355：SnapCenter插件VMware vSphere -产品安全性"本文档介绍了用于保护适用于VMware vSphere 4.X的NetApp SnapCenter插件免受产品环境中现有威胁和新出现威胁的技术。

"TR-4568：《适用于Windows Server的NetApp部署准则和存储最佳实践》"Microsoft Windows Server是一款企业级操作系统、涵盖网络、安全性、虚拟化、云、虚拟桌面基础架构、访问保护、信息保护、Web服务、应用程序平台基础架构等。本文档重点介绍Microsoft Windows、其中特别强调Hyper-V虚拟化技术、包括最新的产品信息和建议的实践、以简化部署、降低风险和管理。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 NetApp 、 Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

有关 NetApp 拥有的专利的最新列表，请访问：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

ONTAP

"9.16.1 9.16.0的通知" "9.16.0 9.16.0的通知" "9.15.1 9.16.0的通知" "9.15.0 9.16.0的通知" "ONTAP 9.14.1通知" "ONTAP 9.14.0的通知" "ONTAP 9.13.1的注意事项" "ONTAP 9.12.1的通知" "ONTAP 9.12.0通知" "ONTAP 9.11.1注意事项" "ONTAP 9.10.1 的通知" "ONTAP 9.10.0的通知" "ONTAP 9.9.1 注意事项" "ONTAP 9.8 注意事项" "ONTAP 9.7通知" "ONTAP 9.6的通知" "ONTAP 9.5通知" "ONTAP 9.4通知" "ONTAP 9.3通知" "ONTAP 9.2通知" "ONTAP 9.1通知"

适用于**MetroCluster IP**配置的**ONTAP**调解器

"9.9.1有关适用于MetroCluster IP配置的ONTAP调解器的通知" "9.8关于MetroCluster IP配置的ONTAP调解器的通知" "9.7关于MetroCluster IP配置的ONTAP调解器的通知"