安全性

ONTAP Technical Reports

NetApp
January 23, 2026

目录

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。

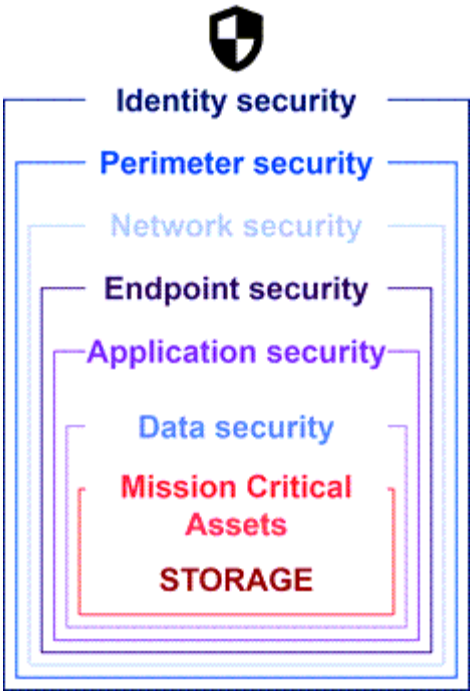
企业必须从外围、网络、身份、应用程序以及数据在存储级别的驻留位置全面审视其整个安全防护、并确保这些层的安全。在当今的威胁形势下、在存储层采用以数据为中心的网络保护方法至关重要。虽然没有一个解决方案可以抵御所有攻击、但使用合作伙伴和第三方等解决方案组合可提供分层防御。

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。

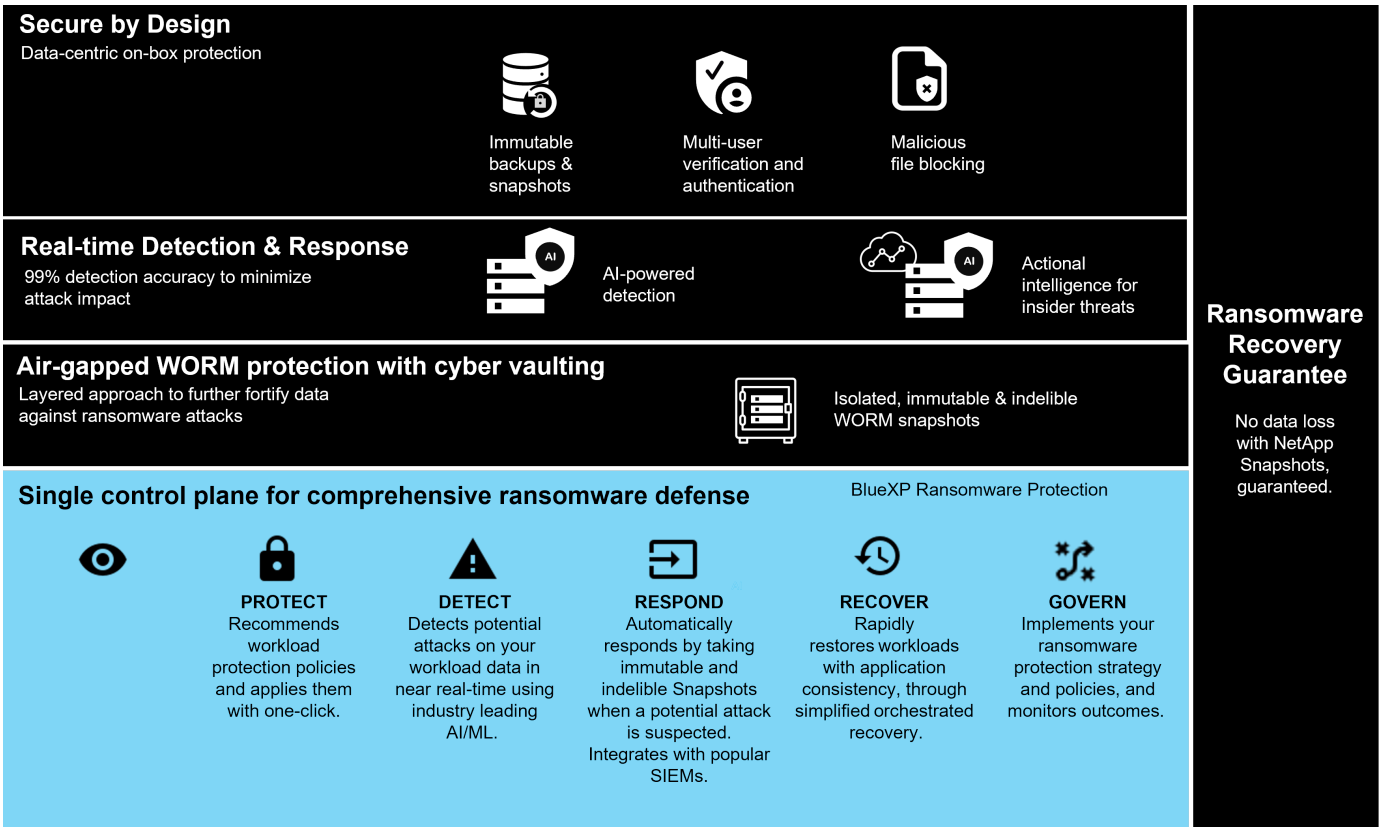
在数据层提供勒索软件保护

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"

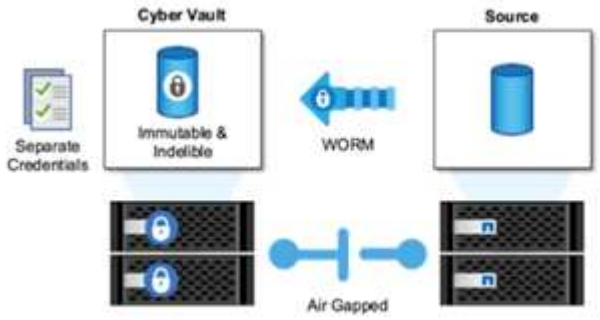
在ONTAP中通过网络存储实现无线WORM保护

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。

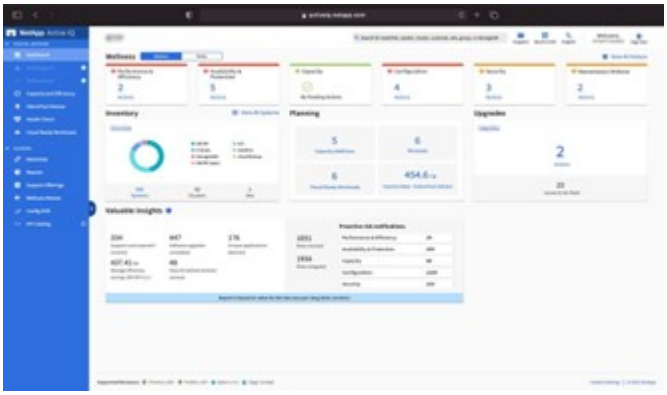
了解更多信息。

- "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。

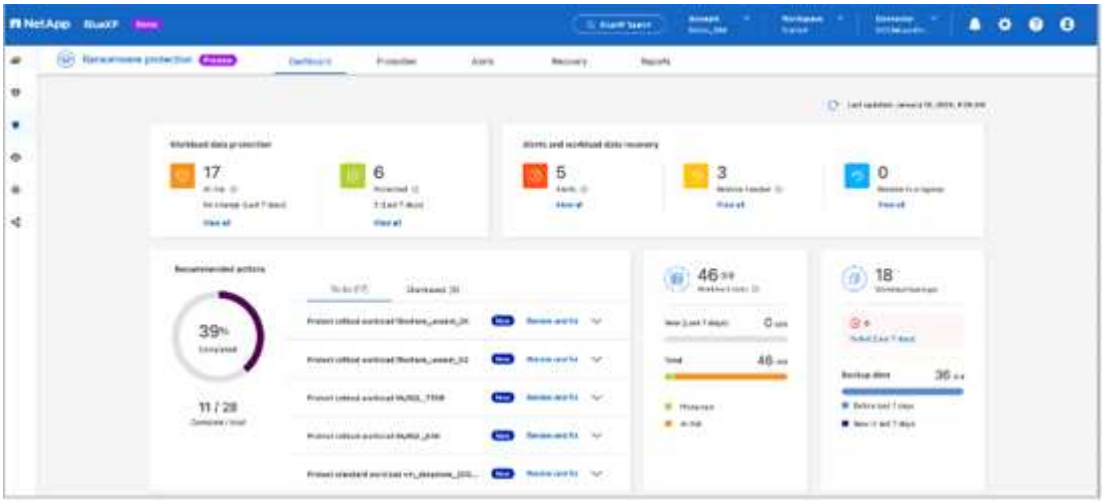
要了解勒索软件保护的实际操作，请参见"Digital Advisor"。

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。

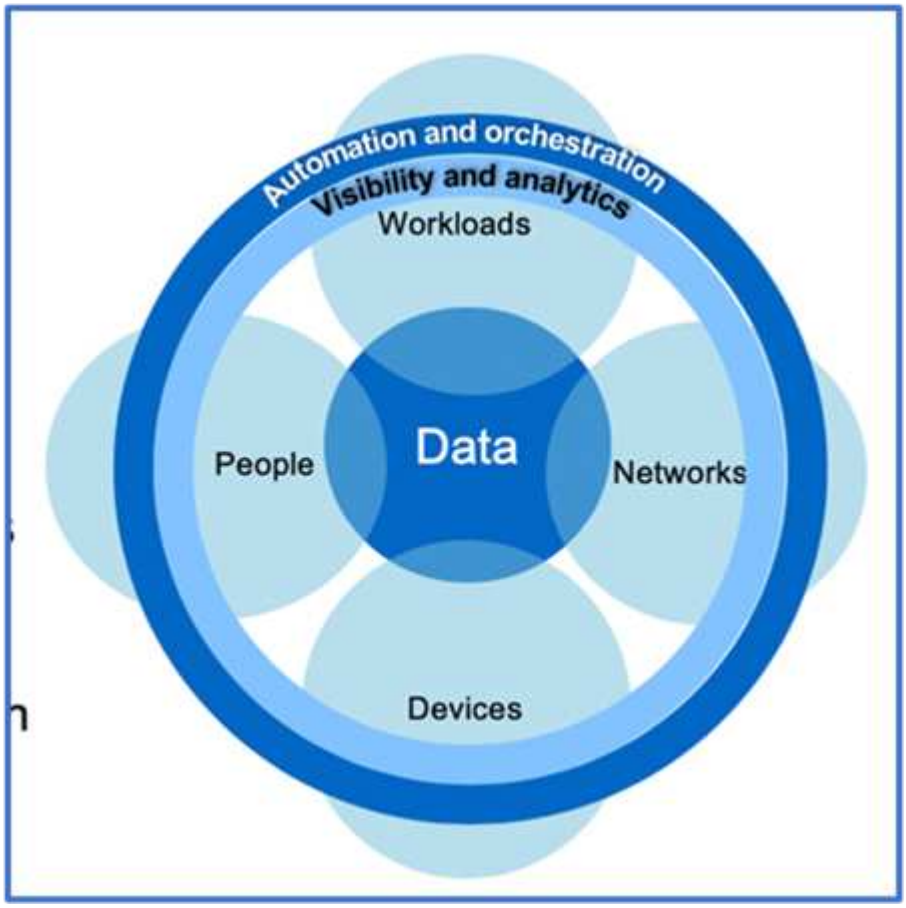
安全资源

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。

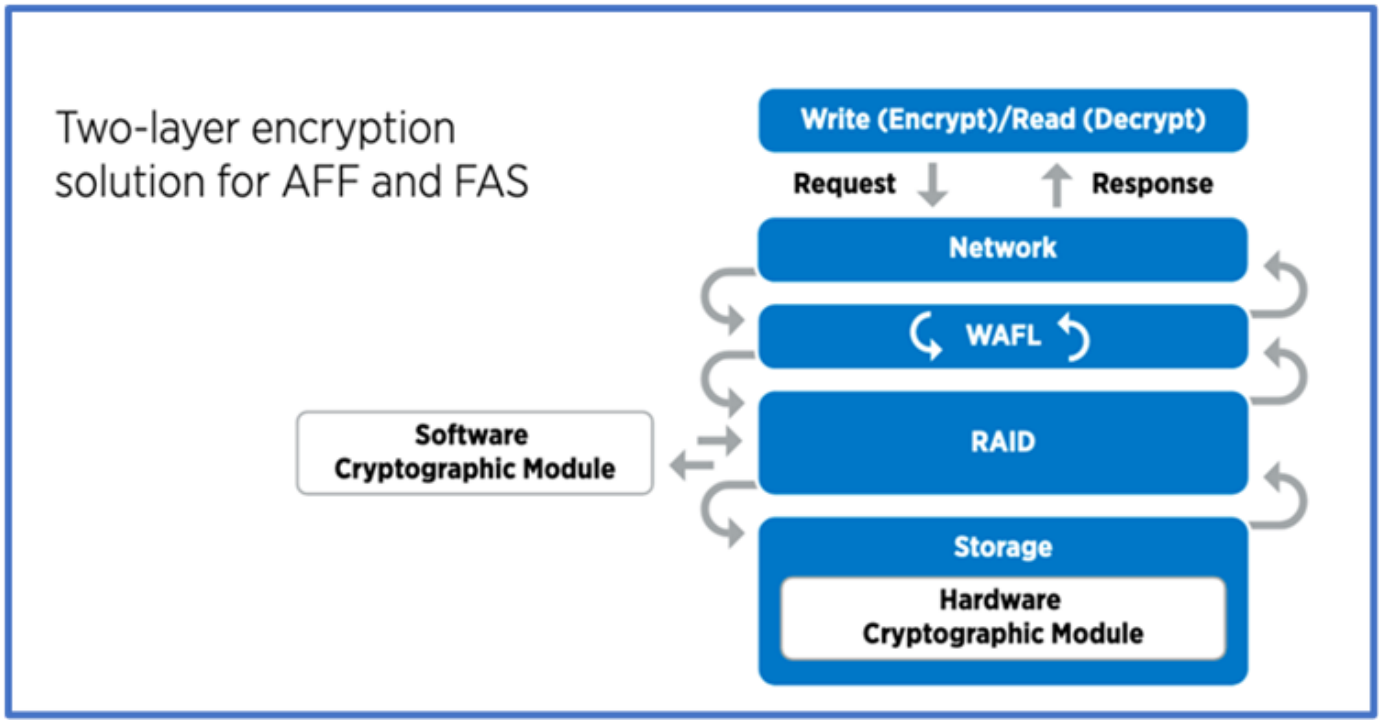
对空闲数据和传输中的数据使用加密

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。

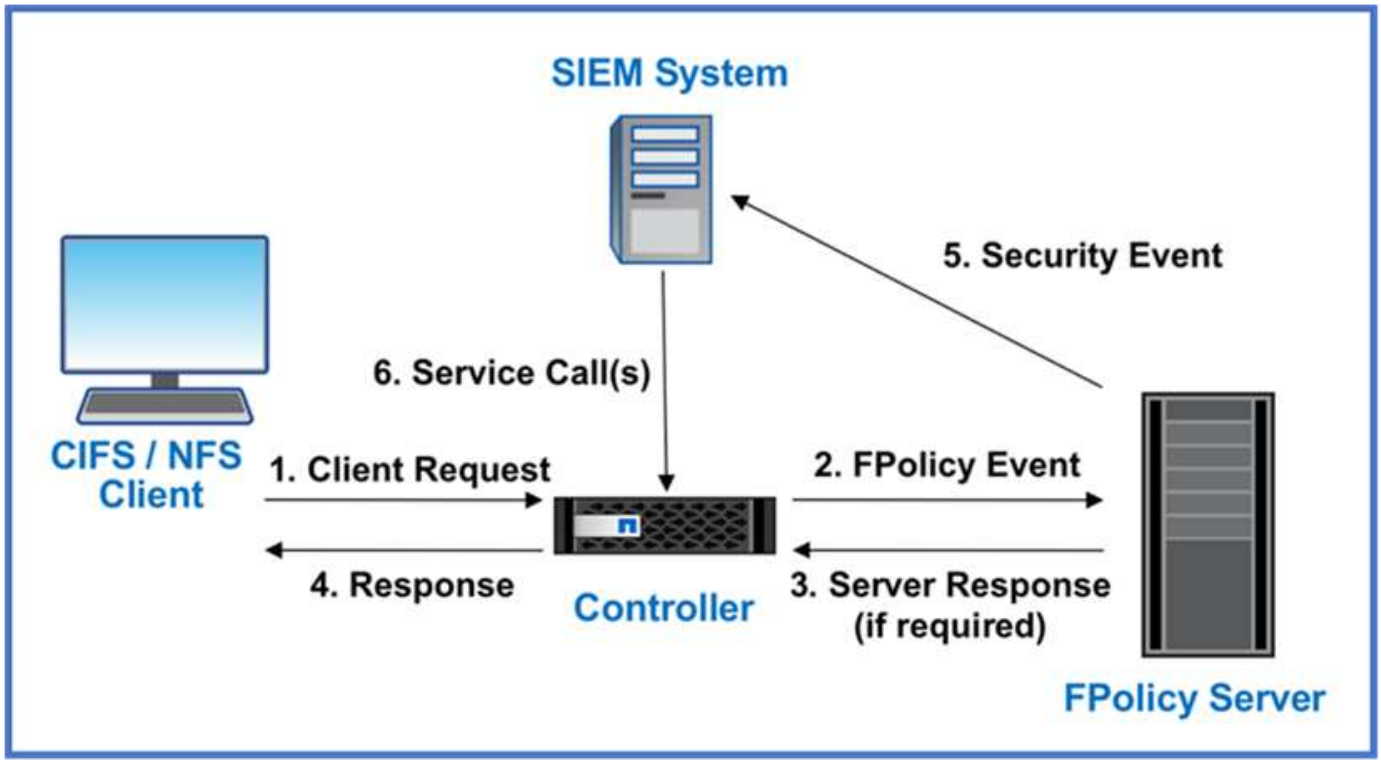
传输中数据加密

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。

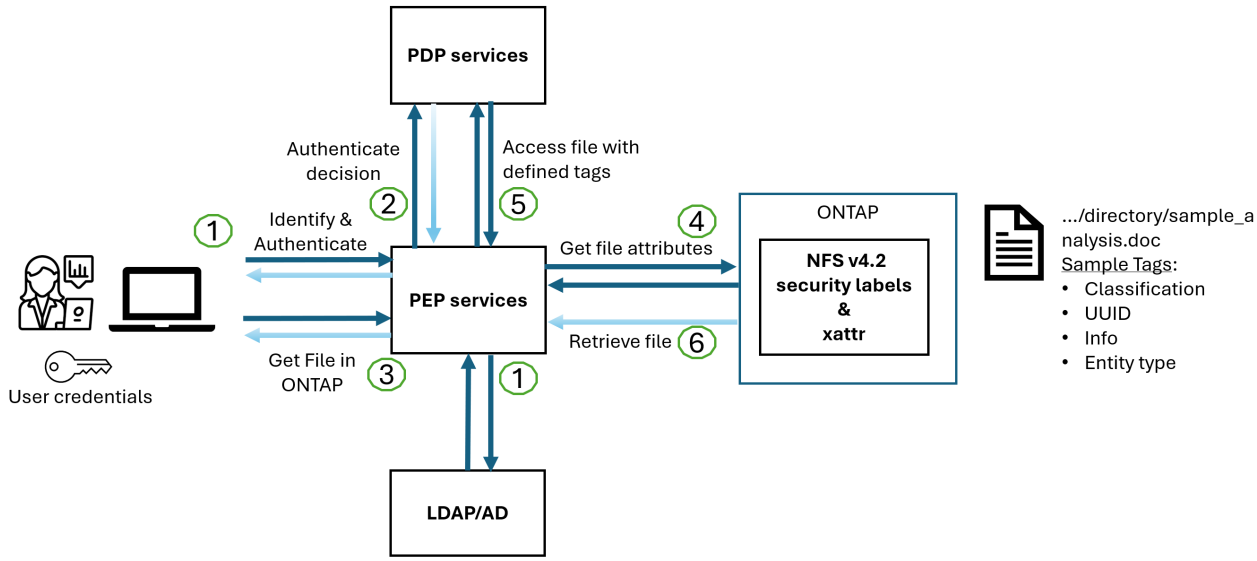
2. 然后、PDP会根据已建立的ABAC策略评估此请求。

   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》"