启用零信任模式
ONTAP 9

NetApp
July 12, 2024

目录

启用零信任模式

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-4015：《NetApp和零信任：启用以数据为中心的零信任模式》中的内容已与ONTAP产品文档的其余部分集成在一起、该报告先前以PDF格式发布。

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?

零信任模式最初由Forrester Research开发 "John Kindervag" 。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利用现有基础架构、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。

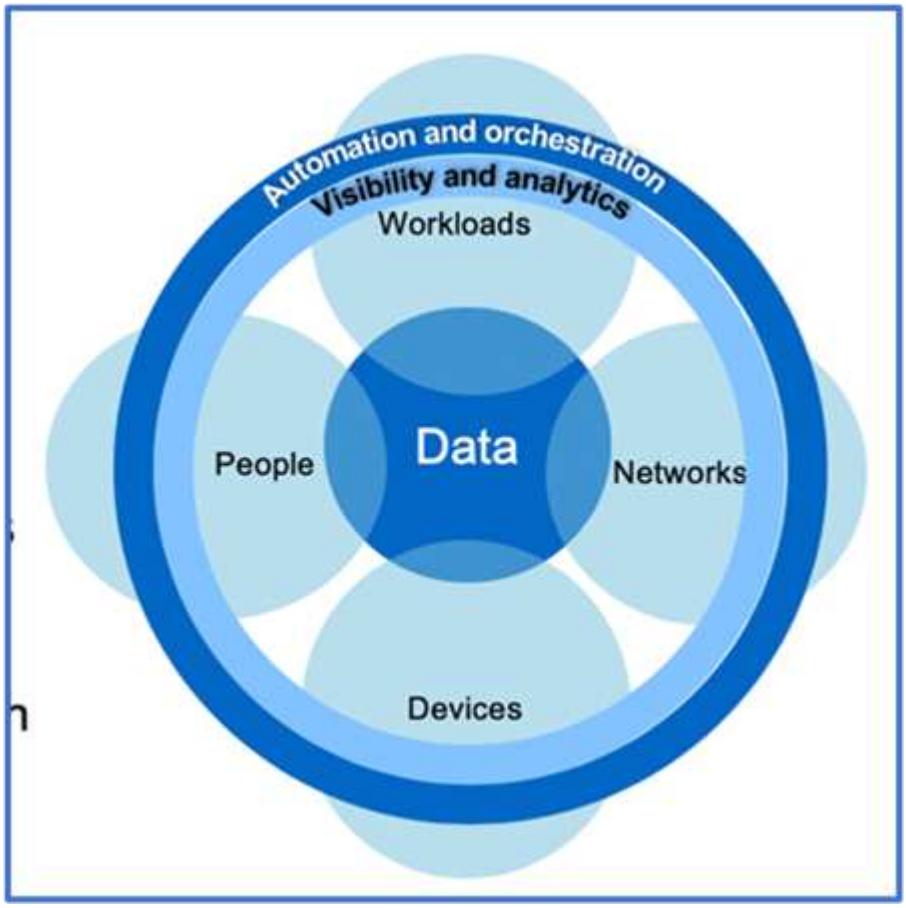
安全资源

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。有毒数据是指不打算在组织外部公开的敏感数据。泄露有毒数据可能会违反法规、并损害组织的声誉。在合规性方面，有毒数据包括的持卡人数据 "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)"或的医疗保健数据 "健康保险携带和责任法案(HIPAA)"。您可以使用AI驱动的工具包NetApp "BlueXP分类" (以前称为Cloud Data Sense)自动扫描、分析数据并对数据进行分类。

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Snapshot副本的另一种方法是使用ONTAP "Snapshot副本锁定"。Snapshot副本锁定是一项SnapLock功能、通过此功能、可以手动或自动将Snapshot副本呈现为不可删除的卷Snapshot副本策略保留期限。Snapshot副本锁定也称为防篡改Snapshot副本锁定。Snapshot副本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Snapshot系统上的Snapshot副本。可以快速恢复主系统上锁定的Snapshot副本、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。

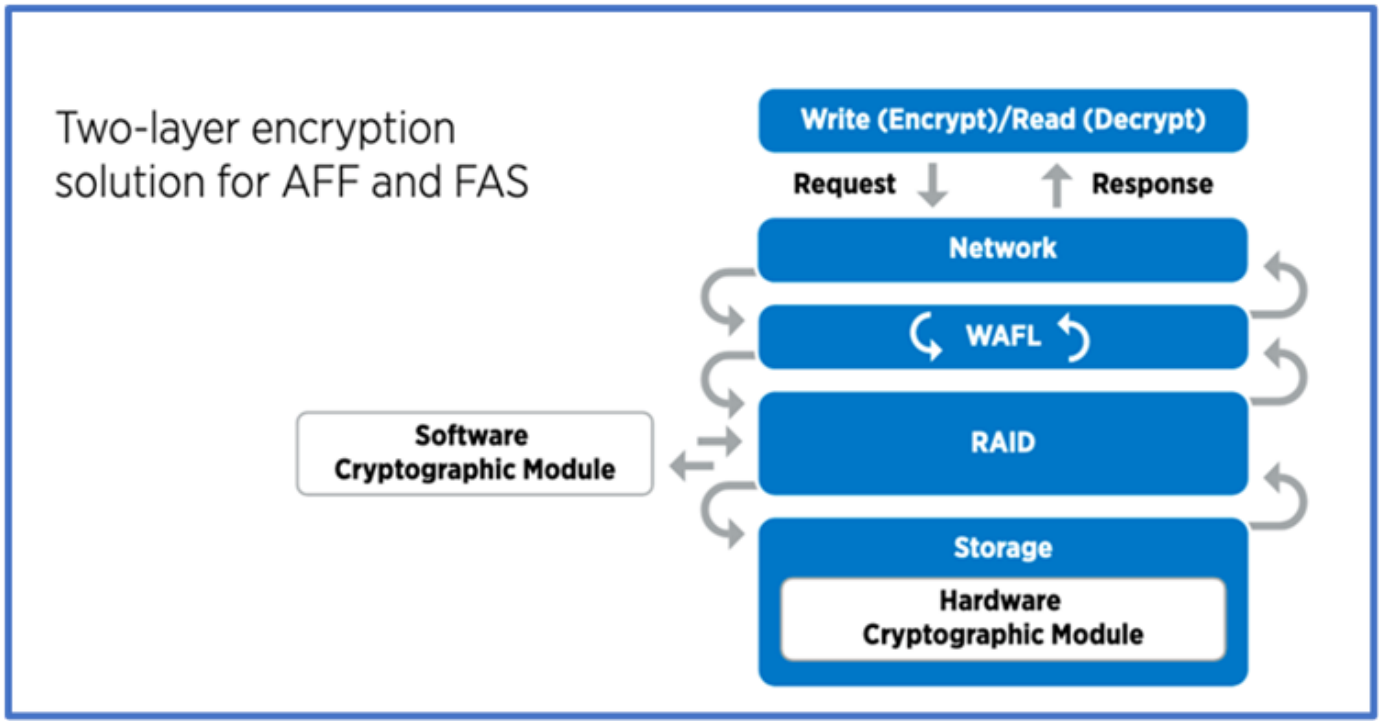
对空闲数据和传输中的数据使用加密

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ONTAP空闲数据硬件解决方案、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。

作为ONTAP内置的密钥管理器的 "板载密钥管理器（ OKM ）"，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。

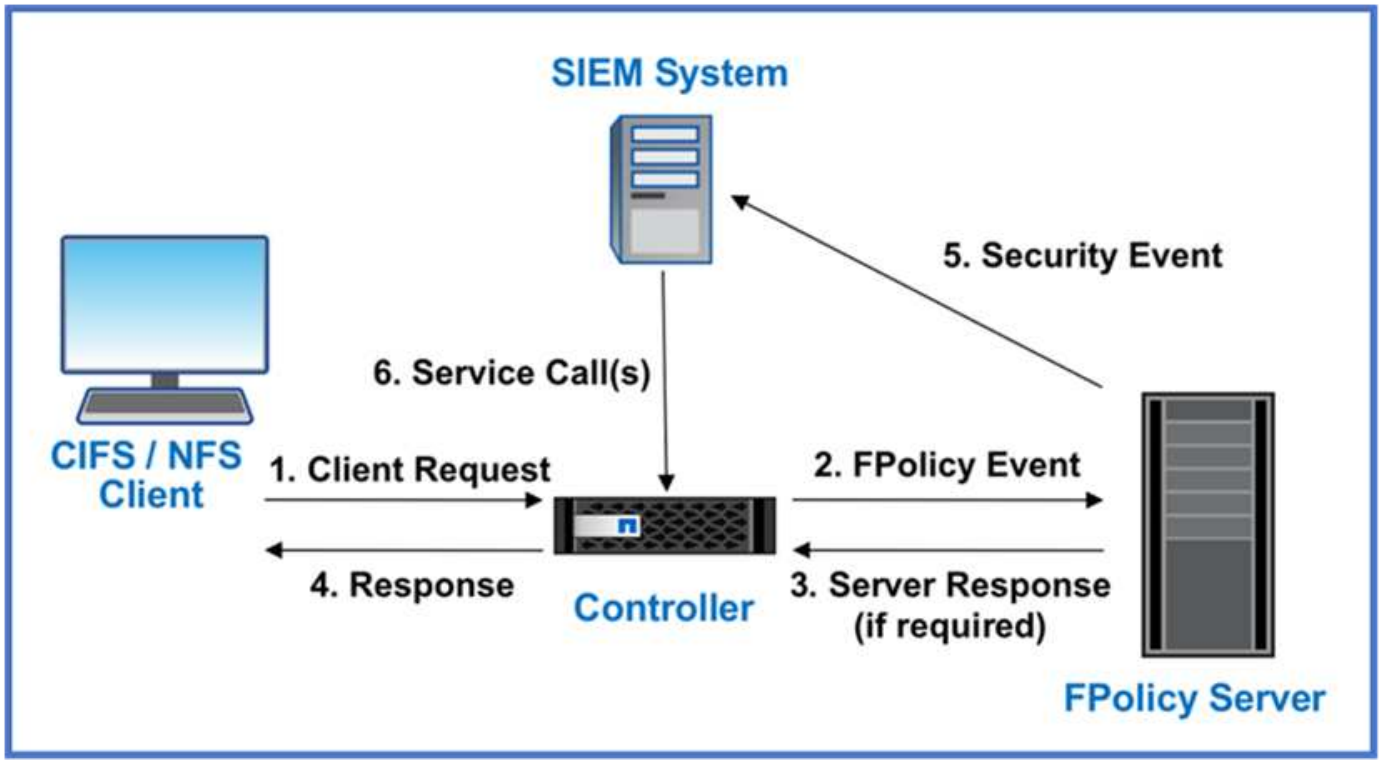
传输中数据加密

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的存储工作负载安全性(以前称为 "Cloud Secure")可利用FPolicy界面以及云端和内部ONTAP存储系统上的用户行为分析、为您提供有关恶意用户行为的实时警报。存储工作负载安全性通过高级机器学习和异常检测、防止组织数据被恶意用户或被入侵用户滥用。存储工作负载安全性可以识别勒索软件攻击或其他不当行为、调用Snapshot副本并隔离恶意用户。存储工作负载安全性还具有取证功能、可查看用户和实体活动的详细信息。存储工作负载安全性是NetApp Cloud 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发生勒索软件攻击、并调用Snapshot副本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。

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" 。

使用可用模块库、用户可以轻松开发Ans得 易操作手册、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。

Cloud Insights是一款基础架构监控工具、可让您深入了解整个基础架构。借助Cloud Insights、您可以监控和优化所有资源、包括公有云实例和私有数据中心、并对其进行故障排除。Cloud 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。此外、它还可以利用可指导行动的智能信息保护您的数据、从而将云基础架构成本平均降低33%、并降低您遭受内部威胁的风险。通过Cloud Insights的存储工作负载安全性功能、可以使用AI和ML进行用户行为分析、以便在内部威胁导致出现异常用户行为时发出警报。对于ONTAP、存储工作负载安全性使用零信任FPolicy引擎。

零信任和混合云部署

NetApp 是混合云数据管理领域的权威企业。NetApp提供了多种选项、用于通过Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)和其他领先的云提供商将内部数据管理系统扩展到混合云。NetApp混合云解决方案支持与内部ONTAP系统和ONTAP Select软件定义的存储相同的零信任安全控制。

您可以使用适用于AWS和GCP的首款企业级云原生文件服务NetApp Cloud Volumes Service以及适用于Microsoft Azure的Azure NetApp Files轻松扩展公有云中的容量、而不会受到典型的容量限制。这些云数据服务是分析和开发运营等数据密集型工作负载的理想选择、可将NetApp的弹性按需存储即服务与ONTAP数据管理功能结合到一个完全托管的产品中。

对于那些寻求云块或对象存储服务(如AWS EBS和S3或Azure存储)高级数据服务的客户、Cloud Volumes ONTAP通过一个通用视图在内部环境和公共云之间提供数据管理。Cloud Volumes ONTAP作为按需实例在AWS或Azure中运行、可提供ONTAP软件的存储效率、可用性和可扩展性。ONTAP支持使用NetApp SnapMirror数据复制软件在内部ONTAP系统与AWS或Azure存储环境之间移动数据。

详细了解ONTAP零信任内容

要了解有关ONTAP零信任内容中所述信息的更多信息、请参阅以下文档和/或网站：

- "Verizon数据泄露调查报告"
- "DoD数字化现代化战略"
- "NIST SP 800-207零信任架构"

- "NetApp合作伙伴联系：安全联盟合作伙伴"
- "使用FPolicy在SVM上监控和管理文件"
- "PCI-DSS 3.2 ONTAP 9."
- "《一般数据保护条例》(GDPR)"
- "HIPPA隐私规则摘要"
- "NetApp BlueXP分类"
- "多管理员验证"
- "防篡改Snapshot副本锁定"
- "ONTAP 9中的多因素身份验证"
- "NetApp 存储加密， NVMe 自加密驱动器， NetApp 卷加密和 NetApp 聚合加密"
- "NetApp 存储加密"
- "NetApp 卷加密和 NetApp 聚合加密"
- "NetApp加密模块FIPS-140-2证书"
- "NetApp提供的量子就绪空闲数据加密"
- "安全创新：NetApp和Ontrack荣获闪存峰会大奖"
- "启用板载密钥管理"
- "NetApp 互操作性表工具"
- "配置外部密钥管理"
- "分类的商业解决方案"
- "ONTAP IPSEC"
- "修改security config以启用FIPS模式"
- "在现有对等关系上启用集群对等加密"
- "存储工作负载安全性(Cloud Secure)"
- "利用NetApp和Ans得 开始自动化您的开发工作流"
- "专用于NetApp DoD统一功能(UC)部署指南的"Ansabile"模块"
- "管理员身份验证和RBAC"
- "ONTAP空闲数据加密"
- "TR-4569《NetApp ONTAP 9安全加强指南》"