



# 开始使用

## NetApp virtualization solutions

NetApp  
January 12, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/netapp-solutions-virtualization/vmware/vmw-getting-started-overview.html> on January 12, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# 目录

|                                                         |    |
|---------------------------------------------------------|----|
| 开始使用 .....                                              | 1  |
| 核心概念 .....                                              | 1  |
| 了解适用于 VMware vSphere 的ONTAP .....                       | 1  |
| 了解适用于 VMware 的NetApp平台 .....                            | 4  |
| 了解NetApp和 VMware 的混合多云环境 .....                          | 7  |
| 管理工具和解决方案 .....                                         | 7  |
| 了解如何使用适用ONTAP tools for VMware vSphere管理虚拟机 .....       | 8  |
| 了解如何使用ONTAP和 VMware API 进行管理 .....                      | 8  |
| 了解如何使用NetApp Data Infrastructure Insights监控整个基础架构 ..... | 9  |
| 了解从 VMware vSphere 到ONTAP数据存储区的虚拟机 .....                | 10 |
| 数据保护解决方案 .....                                          | 10 |
| 了解如何使用MetroCluster和SnapMirror主动同步保护 VMware 环境 .....     | 10 |
| 了解如何降低 VMware 工作负载的安全和勒索软件风险 .....                      | 11 |
| 自主防御 NFS 和 VMFS 勒索软件 .....                              | 12 |
| 备份和灾难恢复解决方案 .....                                       | 19 |
| 了解如何使用适用于 VMware vSphere 的SnapCenter插件备份和还原虚拟机 .....    | 19 |
| 了解如何使用NetApp Disaster Recovery进行虚拟机灾难恢复 .....           | 19 |

# 开始使用

## 核心概念

### 了解适用于 **VMware vSphere** 的**ONTAP**

NetApp ONTAP是适用于 VMware vSphere 的领先存储解决方案，为数据存储和客户机连接存储用例提供近二十年的可靠性能。ONTAP支持 SAN 和 NAS 协议，允许独立扩展存储和计算资源，并从主机卸载存储任务。其优势包括强大的数据保护、高可用性以及先进的业务连续性功能，如SnapMirror和MetroCluster。

#### 简介

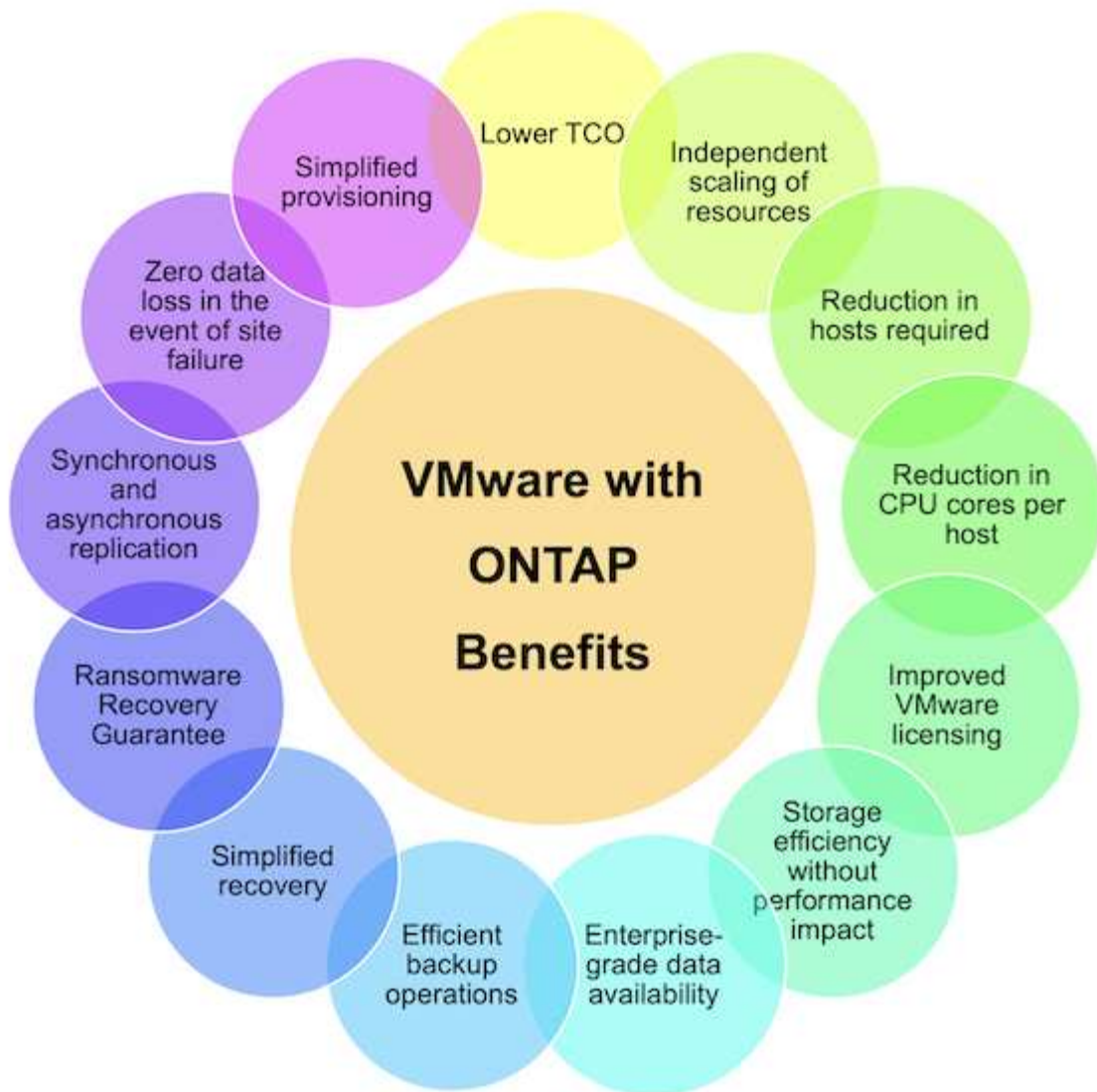
NetApp继续增加创新功能以简化存储管理，同时降低成本并增强对基于 VMware 的整合云虚拟基础架构的信心。该解决方案集合引入了适用于 VMware vSphere Foundation 和 VMware Cloud Foundation 的ONTAP产品，包括最新产品信息和最佳实践，以简化部署、降低风险和简化管理。

有关将ONTAP与 VMware vSphere 结合使用的更多信息，请参阅 ["搭载ONTAP 的VMware vSphere"](#)。

#### 为什么选择**ONTAP for VMware**

成千上万的客户选择ONTAP作为 vSphere 存储解决方案的原因有很多，例如支持 SAN 和 NAS 协议的统一存储系统、使用节省空间的快照的强大数据保护功能以及帮助您管理应用程序数据的丰富工具。使用与虚拟机管理程序分离的存储系统允许您卸载许多功能并最大化您对 vSphere 主机系统的投资。这种方法不仅可以确保您的主机资源专注于应用程序工作负载，还可以避免存储操作对应用程序的随机性能产生影响。

ONTAP与 vSphere 结合使用是一种很好的组合，可以让您减少主机硬件和 VMware 软件的费用。您还可以以较低的成本保护您的数据并保持始终如一的高性能。由于虚拟化工作负载是移动的，您可以探索使用 Storage vMotion 的不同方法在同一存储系统上跨 VMFS、NFS 或vVols数据存储移动虚拟机。



以下是NetApp和 VMware 客户的主要优势：

- \*第一天以及随着规模扩大而具有灵活性。\*任何架构都可能因各种原因而产生增长的需求。无论性能或容量需求如何变化，或者随着新主机的添加和网络或结构考虑的出现，选择一个允许独立扩展资源的存储平台至关重要。

借助ONTAP，您可以从所需的容量开始，根据需要增加容量并利用分层功能，而无需添加额外的计算主机。此外，单个ONTAP集群可与多个工作负载域一起使用，并避免创建存储孤岛。这些好处为组织带来了显著的成本节省。

- \*将存储任务卸载到ONTAP。\*在典型的 HCI 环境中，主机平台负责计算任务、存储操作和客户端的任何网络优化。例如，在确定计算节点的硬件要求时需要考虑 CPU 开销。这种开销通常很难预先确定范围，通常被接受为 10-15%，并且取决于工作负载的 I/O 配置文件。此外，考虑内存消耗也很重要。内存开销是强制性的，不应为了保持性能而牺牲内存开销。主机可以利用支持 RDMA 的 NIC 来抵消这一点，从而提高网络传输效率，但需要支付额外费用。最后，通过 HCI 平台，存储效率、RAID 和故障容忍度以及加密等存储功能由主机处理。

客户可以利用ONTAP来减轻对主机 CPU 资源的任何不利影响。此策略使主机能够专注于计算任务，同时允许ONTAP管理 CPU 密集型存储操作。该策略通过优化存储效率、加密、快照等来提高整体性能，同时降低总体拥有成本。它不仅可以提高主机性能并减少提供相同工作负载所需的主机数量，还可以减少每个主机所

需的核心数量，从而进一步节省成本。这些节省进一步扩展到节省能源效率、减少冷却要求、优化许可证成本等；所有这些都通过将 CPU 密集型存储任务卸载到ONTAP并减少对主机处理所有事情的依赖来实现。

- 存储效率 尽管NetApp是第一个为生产工作负载提供重复数据删除功能的公司，但这项创新并不是该领域的第一次或最后一次创新。它从快照开始，这是一种节省空间且不会影响性能的数据保护机制，同时结合FlexClone技术，可以立即为生产和备份使用制作虚拟机的读/写副本。NetApp继续提供内联功能，包括重复数据删除、压缩和零块重复数据删除，以从昂贵的 SSD 中榨取最多的存储空间。最近，ONTAP增加了使用压缩将较小的 I/O 操作和文件打包到磁盘块中的功能。这些功能的结合使客户看到 VSI 节省高达 5:1，VDI 节省高达 30:1。
- \*企业级数据可用性。\*对于任何 IT 组织来说，数据保护都是至关重要的。规划工作负载容错能力需要仔细考虑，以确保主机负责存储操作时有足够数量的节点可用。随着可容忍的故障数量的增加，对额外主机的需求以及为满足所需的虚拟机存储容量而配置的存储量也会增加。

ONTAP 的全面可用性功能可确保数据始终可访问、安全且具有弹性，使其成为各种规模的 VMware 部署的可靠选择。利用 VMware 环境中的共享存储有助于部署较小的 vSphere 集群，简化设置过程并实现跨集群的存储共享，增强容错能力。

ONTAP 的主要可用性功能包括：

- 高可用性 (HA) 架构：ONTAP支持包含集群部署模型的高可用性架构。
- 自动故障转移和故障恢复：如果发生硬件或软件故障，ONTAP允许自动故障转移到备用存储节点。一旦问题解决，就可以执行故障恢复以恢复原始配置，从而最大限度地减少停机时间。
- 内置数据保护：ONTAP包含内置数据保护功能，例如 RAID-DP 和RAID-TEC，它们可提供增强的磁盘故障保护并确保数据完整性和可用性。
- \*高效的备份和恢复操作。\*除了在发生各种故障时保护数据之外，我们还必须计划将虚拟机和工作负载备份作为常规 IT 操作的一部分。快照捕获特定时间点的虚拟机状态，包括虚拟机的磁盘、内存和设置。如果出现问题（例如更新失败、配置更改或成为勒索软件或病毒攻击的受害者），管理员可以将虚拟机恢复到以前的状态。在为 VMware 环境设计平衡解决方案时，应考虑快照消耗的存储。

虽然快照是一个重要的工具，但过度依赖基于 VMware 的快照会引发对频率和保留策略的担忧。此外，基于 VMware 的快照过多也会降低性能。考虑替代方案非常重要，例如NetApp快照副本和SnapCenter Plug-in for VMware vSphere。SnapCenter利用快照副本，即卷的只读、时间点映像，最初与活动文件系统共享磁盘块，不需要额外的空间和最少的存储空间。这些快照的性能开销可以忽略不计，仅捕获自上次快照以来的变化。SnapCenter Plug-in for VMware vSphere利用这些快照为虚拟机、数据存储区和 VMDK 提供高效、崩溃一致的备份和还原。这些操作无缝集成，并且不会对 vCenter 环境内的性能产生影响。此外，ONTAP还支持将快照卸载到对象存储以进行长期保留。

- \*整体业务连续性能力。\*除了标准的容错、备份和恢复之外，组织还必须为各种情况做好规划，例如灾难、勒索软件攻击和数据中心站点迁移。对于基于主机的存储，解决这些挑战通常需要依靠一系列第三方解决方案来有效地减轻灾难并确保业务连续性。此外，对于网络密集型场景，网络和存储设备规模不足可能会对性能造成严重影响。

ONTAP基于其可用性功能以及备份和恢复功能，是 VMware 环境全面业务连续性战略不可或缺的组成部分。组织需要虚拟机和工作负载在正常和维护操作期间无缝可用，并通过强大的保护和恢复功能进行保障，并且能够利用节省空间且经济高效的灾难恢复解决方案。

ONTAP业务连续性的主要功能包括：

- 使用SnapMirror进行数据复制：利用快照副本，SnapMirror可以将数据异步和同步复制到远程站点或云环境，以实现灾难恢复
- MetroCluster：ONTAP 的MetroCluster技术可在地理位置分散的站点之间提供同步复制，确保零数据丢失

失并在站点发生故障时快速恢复。

- 云分层：云分层自动识别主存储上的冷数据（不经常访问的数据）并将其移动到云端或本地的低成本对象存储。
- NetApp Disaster Recovery： NetApp Disaster Recovery是一个综合解决方案，旨在为企业提供强大的灾难恢复能力，确保在发生灾难时实现数据保护、快速恢复和业务连续性。

## 了解适用于 VMware 的NetApp平台

NetApp提供针对 VMware 环境量身定制的平台，包括用于经济高效存储的FAS、用于高性能工作负载的AFF、用于专用 SAN 部署的ASA以及用于混合和多云架构的云解决方案。这些平台由ONTAP提供支持，支持 VMware Cloud Foundation 和 VMware vSphere。

### 简介

这些产品增强了 VMware 管理员的性能、可扩展性和数据管理。此外，ONTAP可在这些平台上使用，提供统一、可扩展且高效的数据管理解决方案，支持各种存储协议、增强数据保护并优化不同工作负载的性能。

### NetApp平台的共同优势

- **VMware 集成**：所有NetApp平台都提供与 VMware 的深度集成，从而提高了存储环境的效率。内部部署解决方案可以利用插件、API、VAAI 和 VASA 来改善整体数据管理，同时提高基础设施的多功能性。
- **\*成本优化和存储效率**：\*利用NetApp存储可利用重复数据删除、压缩和精简配置等本机效率技术，显著降低存储消耗和成本，同时最大限度地提高容量利用率和性能。此外，这些存储节省还可以减轻计算资源的负担。
- **统一数据管理**：ONTAP为内部部署和基于云的存储提供单一管理界面，简化管理并降低复杂性。这允许在本地和云环境之间实现无缝的数据移动和管理，为 VMware 工作负载提供灵活性和可扩展性。
- **多协议支持**：ONTAP支持多种存储协议，包括 NFS、CIFS/SMB、iSCSI、FC 和 NVMe，允许组织在单一平台上整合工作负载或利用专用 SAN 产品，而无需创建数据孤岛。
- **\*自动化和编排**：\*支持 VMware Cloud Foundation Automation（以前称为 VMware Aria Automation）等自动化工具，并与 Ansible 和其他自动化框架集成，简化操作并减少管理开销。
- **安全性**：强大的安全功能，包括静态和传输中加密、安全多租户和基于角色的访问控制，确保 VMware 环境保持安全。
- **\*适用于 VMware 的ONTAP工具**：\* NetApp适用于 VMware 的ONTAP工具提供无缝集成和管理功能，通过统一直观的界面为 VMware 环境实现高效的存储配置、数据保护和增强性能。
- **\* SnapCenter for VMware vSphere**：\* NetApp SnapCenter for VMware vSphere 简化并集中了 VMware 环境的数据保护、备份和恢复操作，确保可靠、高效地管理虚拟机数据。
- **高可用性和弹性**：RAID-TEC和 RAID-DP 等功能提供强大的数据保护和高可用性，这对于 VMware 环境至关重要。
- **服务质量 (QoS)**：允许管理员为不同的虚拟机设置性能保证，确保关键工作负载获得必要的资源。

注意：NetApp云解决方案可能具有受云提供商限制的功能，但它们对于客户机连接和本机 NFS 数据存储的支持仍然非常强大。

## NetApp ASA（全 SAN 阵列）优势

- \*针对 SAN 进行优化：\*专为 SAN 工作负载而设计，为依赖块存储的 VMware 环境提供高性能和低延迟。
- 增强的高可用性：主动-主动控制器和同步复制等功能可确保持续可用性和数据保护。

ASA系列包括 A 系列和 C 系列型号。

NetApp A 系列全 NVMe 闪存阵列专为高性能工作负载而设计，提供超低延迟和高弹性，适用于关键任务应用程序。



C 系列 QLC 闪存阵列针对更高容量的用例，提供闪存的速度和混合闪存的经济性。



### 存储协议支持

ASA支持所有标准 SAN 协议，包括 iSCSI、光纤通道 (FC)、以太网光纤通道 (FCoE) 和 NVME over fabrics。

**iSCSI** - NetApp ASA为 iSCSI 提供强大的支持，允许通过 IP 网络对存储设备进行块级访问。它提供与 iSCSI 启动器的无缝集成，从而实现 iSCSI LUN 的高效配置和管理。ONTAP 的高级功能，例如多路径、CHAP 身份验证和 ALUA 支持。

有关 iSCSI 配置的设计指导，请参阅 ["SAN 配置参考文档"](#)。

**光纤通道** - NetApp ASA为光纤通道 (FC) 提供全面支持，光纤通道是一种常用于存储区域网络 (SAN) 的高速网络技术。ONTAP与 FC 基础架构无缝集成，提供可靠、高效的存储设备块级访问。它提供分区、多路径和结构登录 (FLOGI) 等功能，以优化性能、增强安全性并确保 FC 环境中的无缝连接。

有关光纤通道配置的设计指导，请参阅 ["SAN 配置参考文档"](#)。

**NVMe over Fabrics** - NetApp ONTAP和ASA支持 NVMe over fabrics。NVMe/FC 支持通过光纤通道基础设施

使用 NVMe 存储设备，并通过存储 IP 网络使用 NVMe/TCP。

有关 NVMe 的设计指导，请参阅 ["NVMe 配置、支持和限制"](#)

## 双活技术

NetApp全闪存 SAN 阵列允许通过两个控制器实现主动-主动路径，从而无需主机操作系统等待主动路径发生故障后再激活备用路径。这意味着主机可以利用所有控制器上的所有可用路径，确保无论系统处于稳定状态还是正在进行控制器故障转移操作，活动路径始终存在。

此外，NetApp ASA还提供了一项独特的功能，可大大提高 SAN 故障转移的速度。每个控制器不断地将重要的 LUN 元数据复制到其配对控制器。因此，每个控制器都准备在其合作伙伴突然发生故障时接管数据服务责任。这种准备是可能的，因为控制器已经拥有开始利用先前由故障控制器管理的驱动器所需的信息。

通过主动-主动路径，计划内和计划外的接管的 IO 恢复时间均为 2-3 秒。

有关详细信息，请参阅 ["TR-4968，NetApp全 SAS 阵列 – NetApp ASA的数据可用性和完整性"](#)。

详细信息请参见 ["NetApp ASA登录页面"](#)。

## NetApp AFF（全闪存FAS）优势

- **极致性能：**利用全闪存存储提供亚毫秒级延迟和高 IOPS，非常适合性能敏感的 VMware 工作负载。
- **持续低延迟：**确保关键应用程序和虚拟机的可预测性能，这对于维护 SLA 至关重要。

有关NetApp AFF A 系列存储阵列的更多信息，请参阅["NetApp AFF A 系列"](#)登陆页面。

有关NetApp C 系列存储阵列的更多信息，请参阅["NetApp AFF C 系列"](#)登陆页面。

## NetApp FAS（光纤连接存储）优势

- **统一存储架构：**支持 SAN（块级）和 NAS（文件级）协议，使其适用于各种 VMware 工作负载。
- **经济高效：**非常适合需要在性能和成本之间取得平衡的环境，提供 HDD 和 SSD 的组合。

## 云解决方案的优势

- **云原生数据管理：**利用云原生产品增强 VMware 工作负载的数据移动性、备份和灾难恢复。对 VMware 云工作负载的原生 NFS 数据存储支持如下：
  - VMware Cloud on AWS 和Amazon FSx for NetApp ONTAP
  - 带有Azure NetApp Files的Azure VMware 服务
  - 带有 Google Cloud NetApp Volume 的 Google Cloud VMware Engine -
- **混合云灵活性：**内部部署和云环境之间的无缝集成，为跨多个位置的 VMware 工作负载提供灵活性。

## 摘要

总之，ONTAP和NetApp平台为 VMware 工作负载提供了全面的优势，增强了性能、可扩展性和数据管理。虽然常见的功能提供了坚实的基础，但每个平台都提供了针对特定需求的差异化优势，无论是通过FAS实现的经济

高效的存储、通过AFF实现的高性能、通过ASA实现的优化 SAN 性能，还是通过NetApp云产品实现的混合云灵活性。

## 了解NetApp和 VMware 的混合多云环境

了解NetApp和 VMware 如何通过将内部基础架构与公共云服务相集成来简化混合多云设置，从而实现工作负载迁移、资源优化和跨环境的一致操作。

### 简介

这种方法使企业能够轻松迁移工作负载、优化资源使用率并在两个环境中保持一致的操作。

有关 VMware 和NetApp混合云场景的更多信息，请参阅["NetApp与 VMware 的混合多云概述"](#)。

### NetApp的 VMware 部署场景

本节介绍跨本地和公共云的 VMware 环境的各种部署选项。每个云提供商都在其各自的公共云产品中支持 VMware 软件定义数据中心 (SDDC) 和/或 VMware 云基础 (VCF) 堆栈。

- **VMware 本地部署**

将 VMware 与NetApp存储结合使用可提供强大、可扩展且灵活的虚拟化环境。通过将 NetApp 的高级数据管理功能（如重复数据删除、压缩和高效快照）与由ONTAP提供支持的适当存储系统相结合，客户可以选择适合他们的平台。这种组合可确保虚拟化工作负载的高性能、可靠性和简化的管理，从而提高整体数据中心的效率。

- **Azure VMware 解决方案**

Azure VMware 解决方案是一种混合云服务，允许在 Microsoft Azure 公共云中完全运行 VMware SDDC。Azure VMware 解决方案是完全由 Microsoft 管理和支持的第一方解决方案，并由 VMware 利用 Azure 基础架构进行了验证。这意味着，当部署 Azure VMware 解决方案时，客户可以获得 VMware 的 ESXi 用于计算虚拟化、vSAN 用于超融合存储以及 NSX 用于网络和安全，同时利用 Microsoft Azure 的全球影响力、一流的数据中心设施以及靠近丰富的原生 Azure 服务和解决方案生态系统的优势。

- **AWS 上的 VMware 云**

VMware Cloud on AWS 将 VMware 的企业级 SDDC 软件引入 AWS 云，并优化了对原生 AWS 服务的访问。VMware Cloud on AWS 由 VMware Cloud Foundation 提供支持，集成了 VMware 的计算、存储和网络虚拟化产品（VMware vSphere、VMware vSAN 和 VMware NSX）以及 VMware vCenter Server 管理，并针对专用、弹性、裸机 AWS 基础架构上运行进行了优化。

- **Google Cloud VMware 引擎**

Google Cloud VMware Engine 是一款基础架构即服务 (IaaS) 产品，它基于 Google Cloud 高性能可扩展基础架构和 VMware Cloud Foundation 堆栈（VMware vSphere、vCenter、vSAN 和 NSX-T）构建。此服务可快速迁移至云端，将现有 VMware 工作负载从本地环境无缝迁移或扩展到 Google Cloud Platform，无需承担重构应用程序或重新调整运维的成本、精力或风险。这是一项由 Google 销售和支撑的服务，并与 VMware 密切合作。

## 管理工具和解决方案

## 了解如何使用适用**ONTAP tools for VMware vSphere**管理虚拟机

ONTAP tools for VMware vSphere简化了使用NetApp存储的虚拟机的生命周期管理。管理员可以直接从 vCenter Server 管理存储，从而简化操作并增强可扩展性。虚拟存储控制台 (VSC)、VASA 提供程序和存储复制适配器 (SRA) 等关键组件可优化配置、性能监控和灾难恢复。

### 简介

它使管理员能够直接管理 vCenter Server 内的存储，并简化 VMware 环境的存储和数据管理。VMware vSphere Client 插件工具旨在将插件功能集成到 vSphere Client 中，而无需在 vCenter Server 内部运行。这提供了插件隔离并支持在大型 vSphere 环境中运行的插件的横向扩展。

### ONTAP工具组件

- **虚拟存储控制台 (VSC)** VSC 包括与 vSphere 客户端集成的界面，您可以在其中添加存储控制器、配置数据存储库、监控数据存储库的性能以及查看和更新 ESXi 主机设置。
- **VASA** 提供程序 适用于ONTAP 的VMware vSphere APIs for Storage Awareness (VASA) 提供程序将有关 VMware vSphere 使用的存储的信息发送到 vCenter Server，从而实现 VMware 虚拟卷 (vVols) 数据存储的配置、存储功能配置文件的创建和使用、合规性验证以及性能监控。
- **存储复制适配器 (SRA)** 启用并与 VMware Site Recovery Manager (SRM) 一起使用时，SRA 可在发生故障时促进 vCenter Server 数据存储和虚拟机的恢复，从而允许配置受保护站点和恢复站点以进行灾难恢复。

有关适用于 VMware 的NetApp ONTAP工具的更多信息，请参阅 "[ONTAP tools for VMware vSphere文档](#)"。

## 了解如何使用**ONTAP**和 **VMware API** 进行管理

ONTAP和 VMware 提供用于实现存储和虚拟化平台之间无缝集成和自动化的 API。这使得配置、监控和数据保护得以简化，从而提高了工作流程的一致性。

### 简介

VMware 提供了一系列 API，允许管理员以编程方式与各种 VMware 产品和服务进行交互，从而提高操作的效率和一致性。此外，NetApp ONTAP API 提供了一套强大的工具，使管理员能够自动化、集成和优化存储环境的管理，尤其是与 VMware 工作负载结合使用时。这些 API 促进了ONTAP存储系统和 VMware 之间的无缝交互，从而提高了效率、性能和数据保护。

### 基于 **VMware** 的 API

- **VMware vSphere API:** vSphere API 是一个综合性的 API，允许管理员管理和自动化 VMware vSphere 环境。它提供对各种 vSphere 功能的访问，包括虚拟机配置、配置、监控和生命周期管理。
- **VMware vCenter Server REST API:** vCenter Server REST API 提供了一个现代化的 RESTful 界面来管理 vCenter Server 及其相关组件。它简化了自动化以及与其他系统和工具的集成。
- **\*VMware Cloud Foundation API:** \*VMware 软件定义数据中心 (SDDC) API 提供对 VMware SDDC 环境中各种组件和服务的编程访问。这些 API 使管理员和开发人员能够自动化、管理和集成数据中心的各个方面，包括计算、存储、网络和管理服务。
- **\*VMware vSphere 存储 API - 存储感知:** \*VASA 是一组 API，提供存储阵列与 vCenter 的集成，以便进行管理。该架构基于多个组件，包括处理 VMware vSphere 和存储系统之间的通信的 VASA 提供程序。借

助ONTAP，该提供程序作为ONTAP tools for VMware vSphere的一部分实现。

- \*VMware vSphere 存储 API - 阵列集成：\*VAAI 是一组支持 VMware vSphere ESXi 主机和存储设备之间通信的 API。API 包括一组主机用来将存储操作卸载到阵列的原始操作。VAAI 可以为存储密集型任务提供显著的性能改进。

## 基于ONTAP的 API

- \* NetApp ONTAP REST API：\* ONTAP REST API 提供了一个用于管理ONTAP存储系统的现代 RESTful 界面。它简化了配置、监控和配置等存储任务的自动化。它可以轻松与 VMware vSphere 和其他 VMware 管理工具集成，从而直接从 VMware 环境实现自动化存储操作。它支持广泛的操作，从基本的存储管理到高级数据保护和复制任务，实现可扩展和灵活的存储管理。
- \* 适用于 VMware vSphere 的ONTAP工具：\*ONTAP tools for VMware vSphere是一组用于集成ONTAP和 vSphere 的工具。它实现了 VASA API 框架的提供程序功能。ONTAP工具还包括 vCenter 插件、用于 VMware Site Recovery Manager 的存储复制适配器 (SRA) 以及可用于构建自动化应用程序的 REST API 服务器。

## 摘要

总之，借助ONTAP API，管理员可以编写脚本在 VMware 环境中创建和配置数据存储区，确保快速、一致的存储配置。此外，它们还可以自动创建、安排和删除 VMware 虚拟机的快照，提供高效的数据保护和恢复选项。SnapMirror API 促进了复制关系设置和管理的自动化，确保为 VMware 工作负载提供强大的灾难恢复解决方案。管理员还可以实施脚本来监控存储性能指标，并在超出性能阈值时触发警报或自动操作，确保 VMware 工作负载的最佳存储性能。通过将ONTAP API 与 VMware API（例如 vSphere 和 vRealize 提供的 API）相集成，管理员可以获得无缝且高度自动化的管理体验，从而提高其虚拟化基础架构的整体效率和可靠性。

## 了解如何使用NetApp Data Infrastructure Insights监控整个基础架构

NetApp Data Infrastructure Insights（以前称为Cloud Insights）可监控本地和云系统，提供对整个 IT 环境（包括 VMware vSphere 和ONTAP存储系统）的可视性。它支持跨公共和私有环境的性能跟踪、问题检测和资源优化等功能。

## 简介

借助Data Infrastructure Insights，您可以监控、排除故障并优化所有资源，包括公共云和私有数据中心。

有关Data Infrastructure Insights的更多信息，请参阅["Data Infrastructure Insights文档"](#)。

## Data Infrastructure Insights能力

- Data Infrastructure Insights提供混合多云监控，让您可以全栈观察基础设施和工作负载。
- 异构基础设施和工作负载的数据收集器，包括 Kubernetes
- 开放 Telegraf 收集器和开放 API，方便集成
- 全面的警报和通知
- 机器学习带来智能洞察
- 优化资源利用率
- 内置或可定制的仪表板，配有高级过滤器，可最大限度地减少显示噪音，从而回答问题
- 了解ONTAP存储操作的健康状况

- 保护您最宝贵的商业资产——数据——免受勒索软件或数据破坏攻击

## 了解从 **VMware vSphere** 到**ONTAP**数据存储区的虚拟机

VMware vSphere 管理员可以通过将工作负载迁移到NetApp ONTAP数据存储来增强其基础架构。ONTAP提供虚拟机感知快照、存储高效克隆和无缝 vMotion 操作，同时支持基于存储策略的管理 (SPBM)。无论是从 vSAN、传统存储迁移，还是实施混合云部署，ONTAP都能为 VMware 环境提供更高的性能和简化的存储操作。

这种迁移实现了无缝集成、改进的数据保护以及管理虚拟化环境的更大灵活性，确保了平稳过渡和最少的停机时间。

### 使用情形

在考虑迁移到ONTAP支持的数据存储时，在源和目标方面有许多迁移选项。

- 从第三方存储系统（包括 vSAN）迁移到ONTAP数据存储。
- 同一 vSphere 集群中的虚拟机迁移
- 跨多个 vSphere 集群迁移虚拟机
- 在同一 SSO 域中跨 vCenter 服务器迁移虚拟机
- 在不同 SSO 域中的 vCenter 服务器之间迁移虚拟机
- 跨数据中心位置迁移虚拟机
- 从第三方存储系统（包括 vSAN）迁移到ONTAP数据存储。
- 混合云环境中虚拟机的迁移

有关将 VMware 工作负载迁移到ONTAP支持的数据存储库的更多信息，请参阅["将虚拟机迁移到ONTAP数据存储库"](#)。

## 数据保护解决方案

### 了解如何使用**MetroCluster**和**SnapMirror**主动同步保护 **VMware** 环境

高级业务连续性对于保护 VMware 环境免受域内中断至关重要。NetApp和 VMware 提供NetApp MetroCluster、 SnapMirror active sync 和 VMware vSphere Metro Storage Cluster (vMSC) 等解决方案，以增强工作负载保护并确保高可用性。

### 简介

除了产品内置的可用性之外，VMware 和NetApp还提供高级配置，进一步保护分布在机架、建筑物、校园甚至城市等故障域中的工作负载。

### NetApp MetroCluster

NetApp MetroCluster使用 NetApp 的高可用性 (HA) 功能来防止控制器故障。MetroCluster还包括SyncMirror技术、按需集群故障转移 (CFOD)、硬件冗余和地理分离，以实现高可用性。SyncMirror在两个 plex 之间同步镜像数据：本地 plex 主动提供数据，远程 plex 作为备用。所有MetroCluster组件（例如控制器、存储、电缆、交

换机和适配器)都具有硬件冗余。

## NetApp SnapMirror主动同步

NetApp SnapMirror主动同步通过 FCP 和 iSCSI SAN 协议提供数据存储粒度保护,有选择地保护高优先级工作负载拓扑。与主动-备用MetroCluster不同,它提供对本地和远程站点的主动-主动访问。从ONTAP 9.15.1 开始, SnapMirror主动同步支持对称主动/主动功能,允许通过双向同步复制从受保护 LUN 的两个副本执行读写 I/O 操作。

## VMware vSphere Metro 存储群集

VMware vSphere Metro Storage Cluster (vMSC) 通过主动-主动延伸存储增强了 VMware HA。此经过认证的配置可保护虚拟机和容器免受故障影响。这是通过使用延伸存储概念以及 vSphere 主机集群来实现的。这些主机分布在不同的故障域中。NetApp MetroCluster和SnapMirror主动同步存储技术用于提供保护和支持的存储产品。通过利用 vMSC, NetApp认证的解决方案可跨故障域提供强大且具有弹性的 IT 运营。

有关详细信息,请参阅 ["采用ONTAP 的vSphere Metro 存储集群"](#)。

## 了解如何降低 VMware 工作负载的安全和勒索软件风险

ONTAP通过加密、快照和高级访问控制增强了 VMware 环境中的安全性和勒索软件防护,补充了 VMware 的安全功能以保护数据。

### 简介

通过在 VMware 环境中利用NetApp ONTAP的高级功能,组织可以确保其数据的完整性、可用性和安全性。

请参阅下文,详细了解这些技术如何协同工作以提供\*安全\*和\*备份优势\*。

### 安全和勒索软件

安全性是虚拟化环境中的首要关注点,而NetApp ONTAP提供了强大的功能来增强 VMware 基础架构内的安全性。ONTAP为静态数据和传输中的数据提供加密,确保敏感信息免遭未经授权的访问。加密密钥得到安全管理,并且ONTAP支持基于软件和基于硬件的加密解决方案。通过与 VMware 的安全工具(例如 vSphere 的内置安全功能和第三方安全解决方案)集成, ONTAP有助于创建安全且合规的环境。

### 勒索软件防御

勒索软件攻击对组织构成重大威胁,而 VMware 与ONTAP的结合提供了强大的防御机制。ONTAP 的快照技术允许创建不可变的快照,勒索软件无法更改或删除。如果发生攻击,这些快照可用于快速将受影响的虚拟机和数据存储恢复到攻击前的状态,从而最大限度地减少停机时间和数据丢失。此外,ONTAP 与安全信息和事件管理(SIEM)系统的集成实现了对可疑活动的主动监控和警报。ONTAP还支持多因素身份验证(MFA)和基于角色的访问控制(RBAC),以进一步增强安全性。

### 勒索软件恢复保证

NetApp勒索软件保障为组织提供了强大而可靠的解决方案,以防止勒索软件攻击。通过利用NetApp ONTAP的先进功能,组织可以确保其数据的安全性和可用性。该保证让您安心,因为您知道,如果发生勒索软件攻击,数据可以快速有效地恢复,最大限度地减少停机时间、数据丢失和财务影响。对数据安全和弹性的承诺使NetApp成为希望保护其关键资产免受不断演变的网络威胁的组织的理想合作伙伴。

## 高级安全功能

ONTAP 包括高级安全功能，例如安全多租户（可在多租户环境中隔离数据和资源）和合规性审计（可跟踪和记录对敏感数据的访问）。这些功能可确保数据安全，并且组织可以证明符合行业法规和标准。

## 摘要

ONTAP 的安全功能（例如加密、不可变快照和高级访问控制）与 VMware 工具的集成提供了对包括勒索软件在内的网络威胁的强大防御。ONTAP 对安全多租户和合规性审计的支持可确保数据保护和法规遵从性。

NetApp ONTAP 和 VMware 共同提供了用于保护虚拟化环境的全面解决方案，使组织能够保护数据、最大限度地减少停机时间并保持业务连续性。实施这些技术有助于企业应对现代 IT 挑战并保护关键资产免受不断演变的安全威胁。

## 自主防御 NFS 和 VMFS 勒索软件

了解 NetApp ONTAP 的自主勒索软件防护 (ARP) 如何使用机器学习来保护 VMware 环境中的 NFS 和 VMFS 数据存储，提供早期威胁检测、防篡改快照和快速恢复，以增强虚拟化和云工作负载的数据弹性。

## 概述

勒索软件威胁正在迅速演变，变得更加复杂和具有破坏性。传统的安全措施往往无法保护关键数据资产。NetApp ONTAP 存储提供内置安全功能，可主动保护数据。如果发生安全漏洞，ONTAP 会提供实时警报和快速恢复选项，以减少停机时间并限制数据丢失。ONTAP 使客户能够保护、恢复和移动其数据和应用程序，从而增强勒索软件的抵御能力。

## 用例 – 保护 VMware 虚拟机及其文件

在 VMware 环境中尽早检测勒索软件对于阻止其传播和最大限度地减少停机时间至关重要。有效的策略是在 ESXi 主机和客户虚拟机之间使用多层保护。虽然许多安全控制措施有助于建立强大的防御，但 NetApp ONTAP 增加了必要的存储级别保护措施，进一步加强了保护。

ONTAP 的主要功能包括用于时间点恢复的快照技术、由内置机器学习提供支持的自主勒索软件保护 (ARP)、多管理员验证和可保持数据完整性的防篡改快照。这些功能协同作用，增强了勒索软件的抵御能力，并在需要时实现快速恢复。

保护 vSphere 环境和客户虚拟机需要采取全面的方法。关键措施包括网络分段、部署 EDR/XDR/SIEM 解决方案进行端点监控、及时应用安全更新以及遵循既定的强化指南。每个虚拟机通常都运行一个标准操作系统，因此作为多层勒索软件防御策略的一部分，安装和定期更新企业级反恶意软件解决方案至关重要。

## ONTAP 如何提供帮助

ONTAP 通过多层防御加强数据保护。主要功能包括快照、自主勒索软件保护 (ARP)、防篡改快照、多管理员验证等。本文档重点介绍 9.17.1 版本中引入的 ARP 增强功能。

您可以在支持 VMware 数据存储区的 NAS 或 SAN 卷上启用 ARP。ARP 使用 ONTAP 的内置机器学习来监控工作负载模式和数据熵，自动检测勒索软件活动的迹象，并提供智能、主动的安全层。使用 ONTAP 的 CLI 或系统管理器界面配置每个卷的 ARP。

## ARP特性演进

从ONTAP版本 9.10.1 开始, ARP 可用于现有卷或新卷。在ONTAP版本 9.16.1 中, 您可以使用系统管理器或 CLI 启用 ARP。ARP/AI 保护立即生效, 无需学习期。在 9.17.1 版本中, ARP 支持 SAN 卷。当您在 SAN 卷上启用 ARP 时, ARP/AI 会在评估期间持续监控数据, 以确定工作负载的适用性并设置最佳检测加密阈值。

ARP 内置于ONTAP中, 提供与其他ONTAP功能的集成控制和协调。ARP 实时工作, 在写入或读取数据时进行处理, 并快速检测和响应潜在的勒索软件攻击。它会定期创建锁定快照以及预定的快照, 并在未检测到异常时通过回收快照来智能地管理快照保留。如果 ARP 检测到可疑活动, 它会将攻击前拍摄的快照保存较长时间, 以确保可靠的恢复点。

有关详细信息, 请参阅["ARP 检测到什么"](#)。

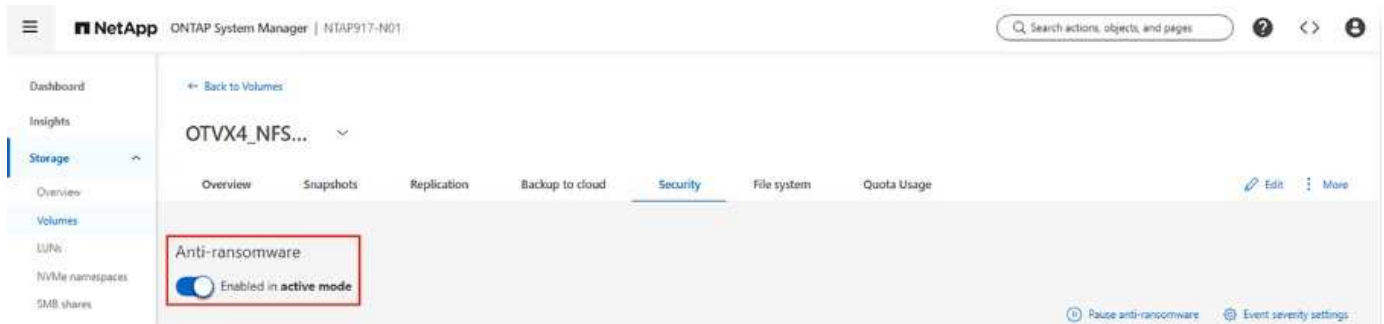


ONTAP ONE 许可证包含 ARP 支持。

### 在 NAS 卷上配置 ARP 并模拟对 VM 的攻击

了解如何在用于 VMware 数据存储区的 NAS 和 SAN 卷上启用NetApp ONTAP自主勒索软件防护 (ARP), 并模拟勒索软件攻击以了解 ARP 如何检测威胁并促进快速恢复。

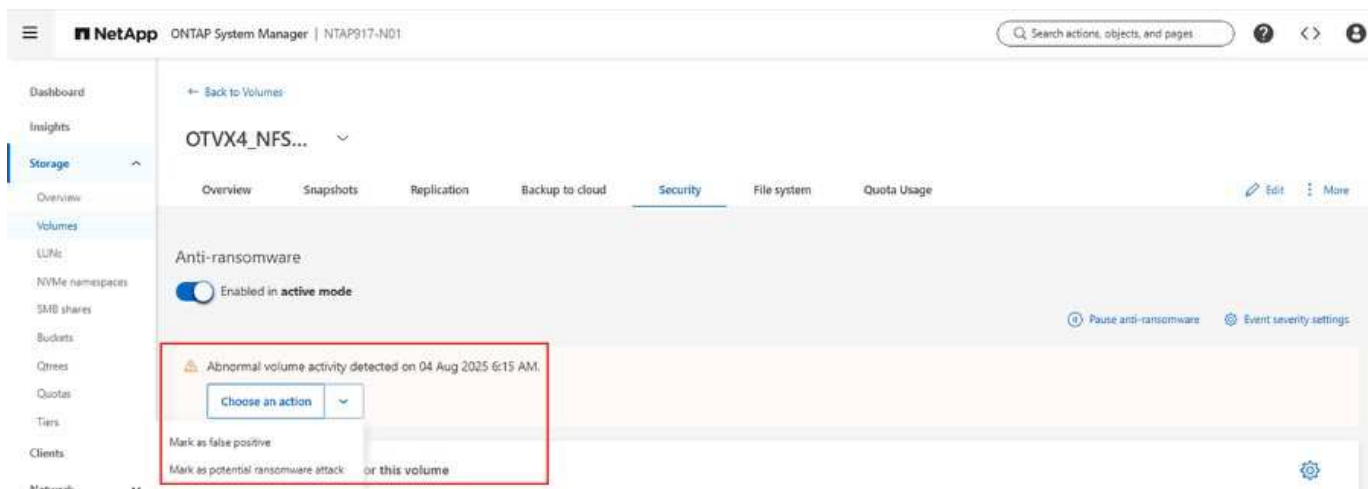
当使用系统管理器或 CLI 在 NAS 卷上启用 ARP 时, ARP/AI 保护将立即启用并处于活动状态。无需学习期。



在此示例中, 使用脚本修改文件或通过修改文件扩展名来触发模拟, 以模拟驻留在作为数据存储附加到 vCenter 的 NFS 卷上的 VM 内的攻击。

| Name                                | Date modified    | Type           | Size     |
|-------------------------------------|------------------|----------------|----------|
| Acorn Missouri River.pptx.encrypted | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Moon.pdf.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Moon.xls.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Panthers.doc.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Pheasant.docx.encrypted       | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Pheasant.pdf.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Pheasant.ppt.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Pig.pptx.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Pig.txt.encrypted             | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Ridge.doc.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Ridge.docx.encrypted          | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Ridge.pdf.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Ridge.ppt.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Ridge.txt.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn River.doc.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn River.pdf.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Rosa arkansana.doc.encrypted  | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Rosa arkansana.docx.encrypted | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Rosa arkansana.pdf.encrypted  | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soil.doc.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soil.docx.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soil.ppt.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soil.txt.encrypted            | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soybean.doc.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soybean.pdf.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Soybean.xls.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Sun.xls.encrypted             | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tornado.docx.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tornado.ppt.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tractor.docx.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tractor.ppt.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tractor.pptx.encrypted        | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Tractor.txt.encrypted         | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Water.pdf.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Wheat.doc.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |
| Acorn Wheat.pdf.encrypted           | 8/4/2025 1:15 PM | ENCRYPTED File | 1,680 KB |

如下所示，ARP检测到了异常活动。



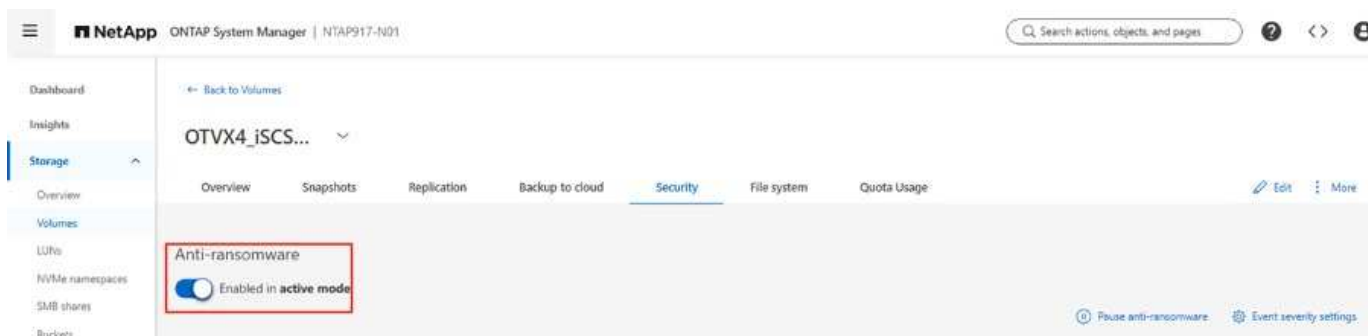
ARP 可提前检测到攻击，并能够从接近攻击时间的快照中恢复数据。要回滚，请使用事件触发之前生成的 ARP 定期快照。下面的屏幕截图显示了创建的快照：

|                                                 |                     |          |
|-------------------------------------------------|---------------------|----------|
| Anti_ransomware_periodic_backup.2025-08-13_0421 | Aug/12/2025 9:21 PM | 29 GiB   |
| hourly.2025-08-13_0405                          | Aug/12/2025 9:05 PM | 28.9 GiB |
| Anti_ransomware_periodic_backup.2025-08-13_0021 | Aug/12/2025 5:21 PM | 29.1 GiB |

有关在用作数据存储的 NFS 卷上启用 ARP 并在发生攻击时恢复的详细指导，请参阅["NFS 存储的 ARP"](#)。

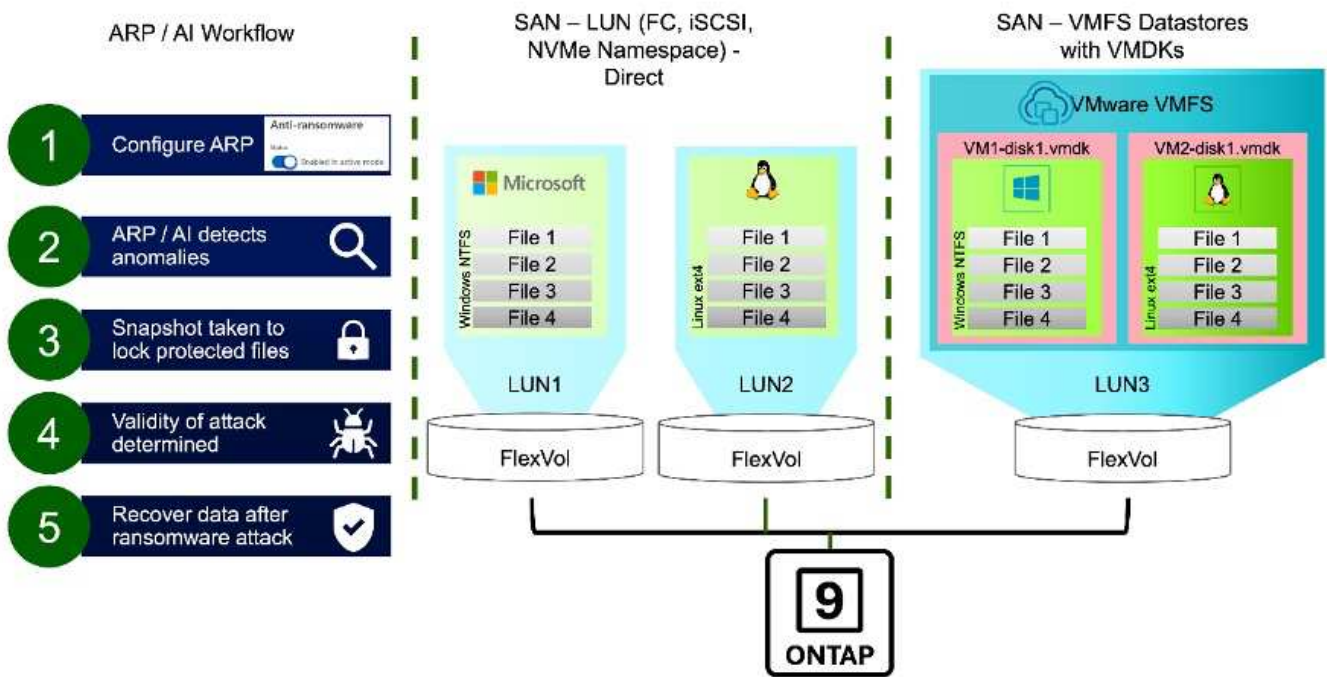
在 **SAN** 卷上配置 **ARP** 并模拟对 **VM** 的攻击

当在 SAN 卷上启用 ARP 时，它会从评估阶段开始，类似于 NAS 环境中使用的学习模式，然后自动转换为主动检测。



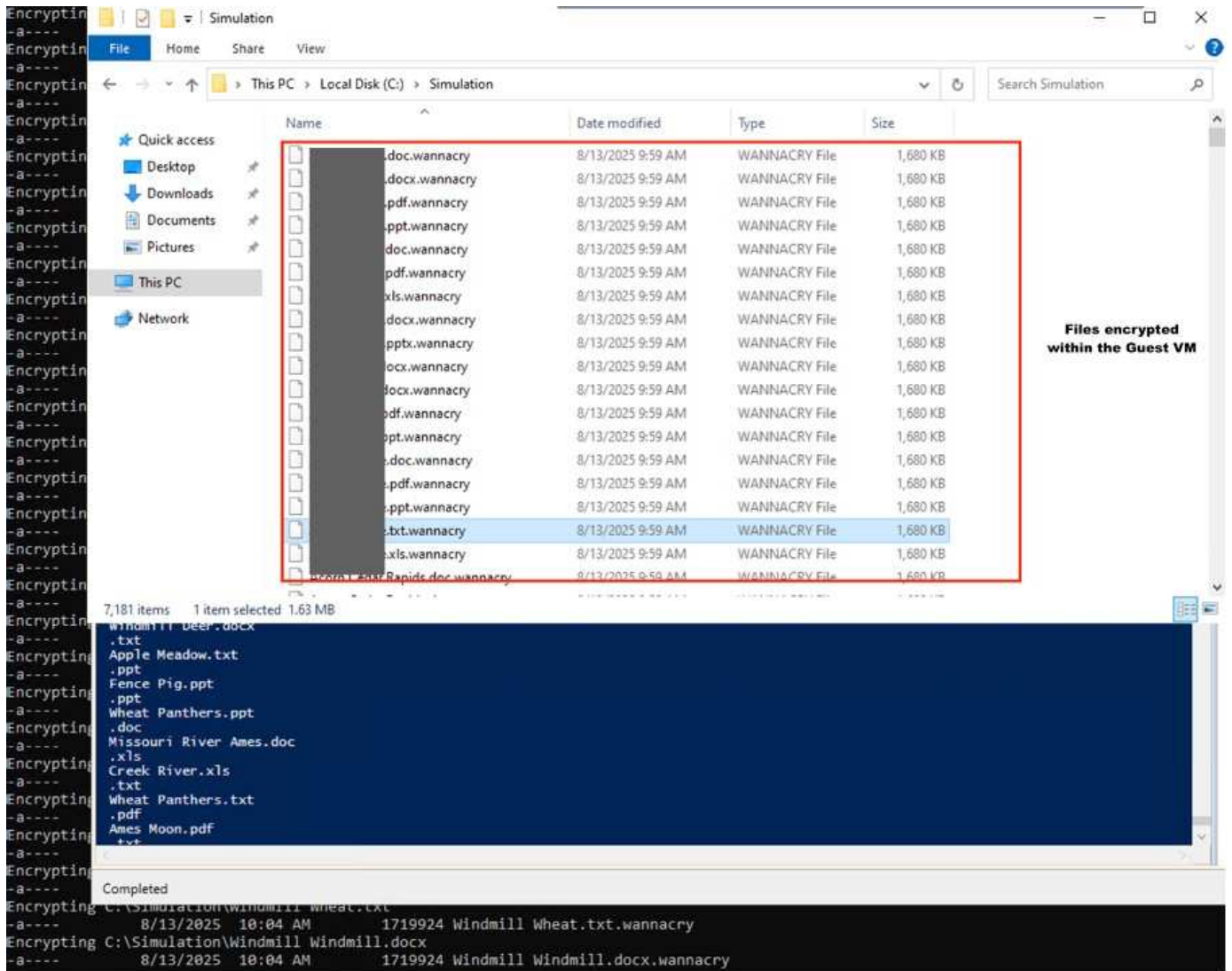
ARP 启动为期两到四周的评估期，阈值为 75%，以建立加密行为的基线。可以使用以下方式监控此阶段的进度  
``security anti-ransomware volume show`` 通过检查\*块设备检测状态\*命令。评估完成后，**Active\_suitable\_workload** 状态确认观察到的熵水平适合持续监控。根据收集的数据，ARP 会自动调整其自适应阈值，以确保准确、灵敏的威胁检测。根据需求，快照创建间隔可以从默认的 4 小时更改为 1 小时。请谨慎执行此修改。

从 ONTAP 9.17.1 开始，NAS 和 SAN 卷都会定期生成 ARP 快照。ONTAP

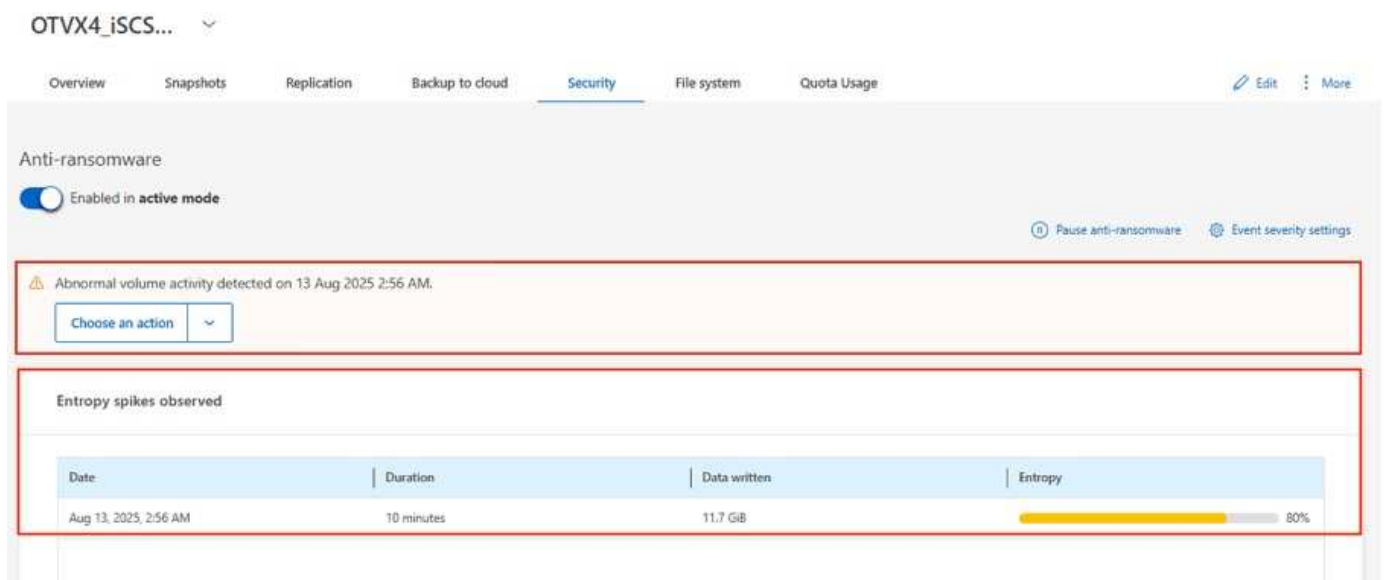


有关详细信息，请参阅["SAN 环境和模式类型"](#)

现在是模拟攻击的时候了。为了演示目的，文件在基于 iSCSI 的数据存储上运行的虚拟机内进行加密。生成的文件接近 7000 个，不幸的是，这些文件受到了勒索软件攻击的影响。

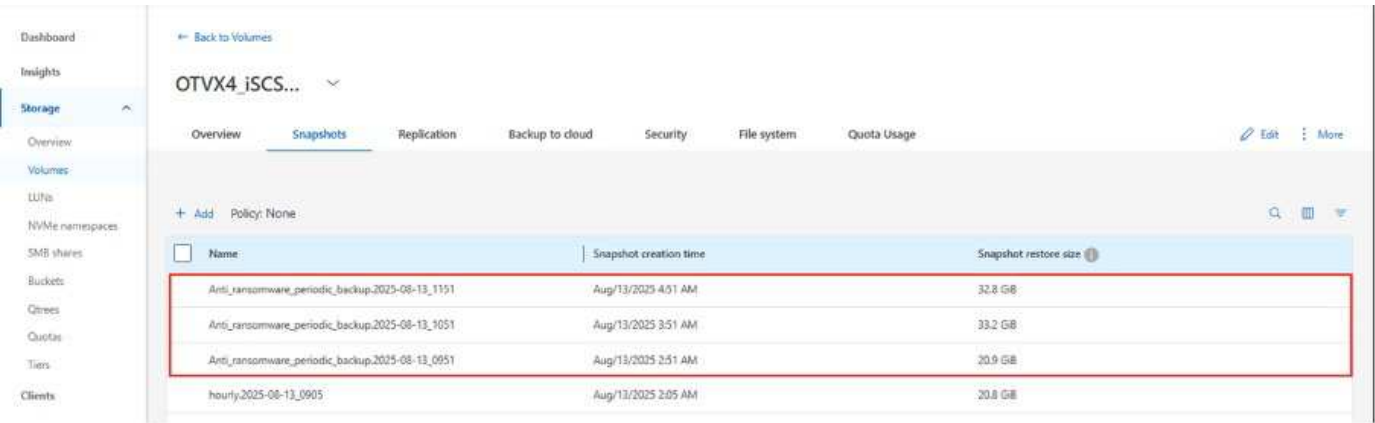


在 10 分钟内，根据高熵数据检测到卷上的异常活动，并且 ARP 生成威胁警报，因为它检测到 VM 内部的熵异常。

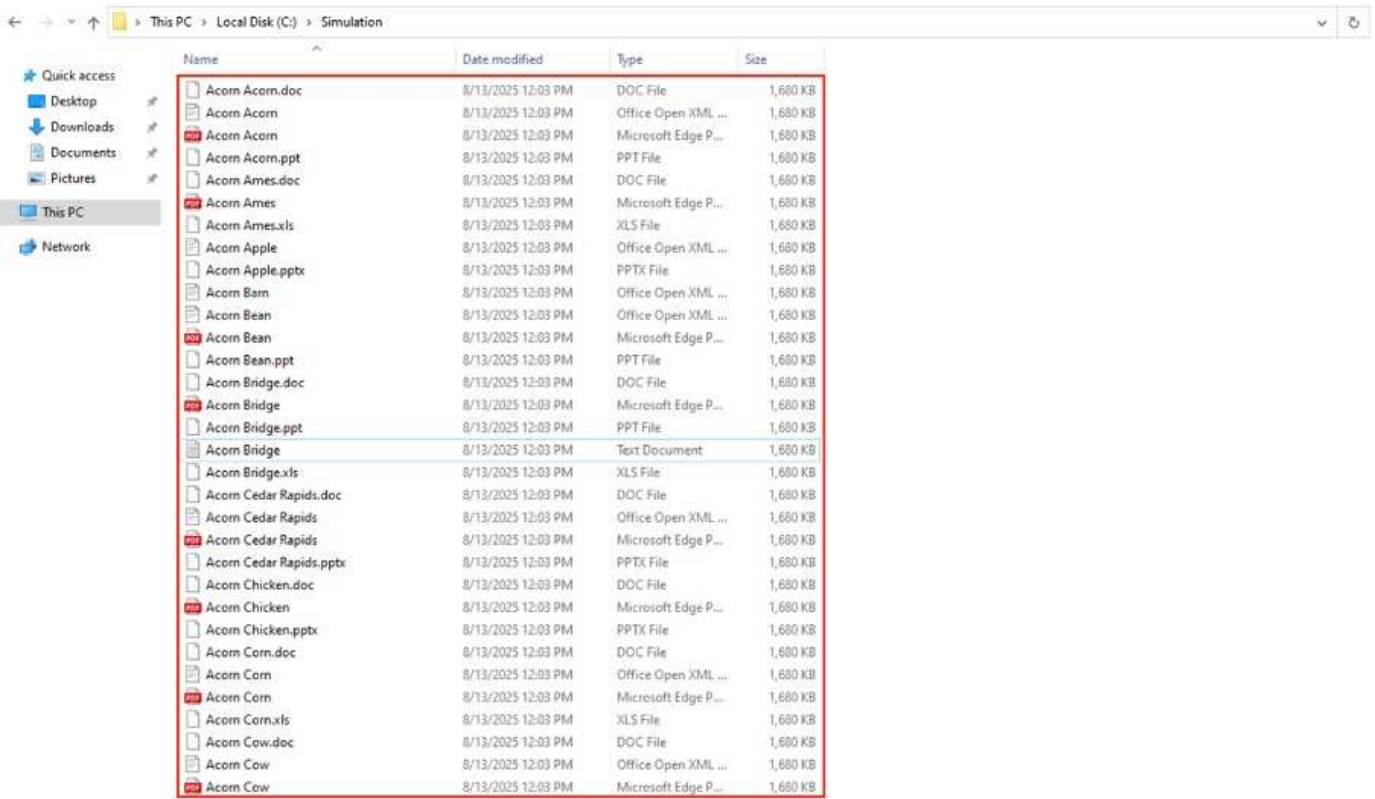


勒索软件攻击后恢复虚拟机及其数据

根据上述步骤确认攻击后，使用其中一个 ARP 快照或卷的另一个快照来恢复数据。



一旦恢复，文件就全部恢复了。



有关详细指导，请参阅["勒索软件攻击后从 ARP 快照恢复数据"](#)

ONTAP作为 VMware 及其他系统的防御层

只需点击几下，企业就可以无缝增强其数据保护策略。 ONTAP采用基于机器学习的先进检测机制，在 VMware 环境中引入了强大的防御层。这种智能保护不仅可提前识别威胁，而且还可帮助在威胁升级之前减轻潜在损害。

此用例不仅适用于 VMware。您可以将相同的原则扩展到任何基于 NAS 或 SAN 的应用程序，以构建多层安全架构。攻击者被迫穿越多个强化层，大大降低了成功入侵的风险。

ONTAP不仅仅保护数据，它还能帮助组织在不断演变的威胁面前保持弹性。

# 备份和灾难恢复解决方案

了解如何使用适用于 **VMware vSphere** 的**SnapCenter**插件备份和还原虚拟机

SnapCenter Plug-in for VMware vSphere可对虚拟机、数据存储空间和 VMDK 文件实现快速、虚拟机一致的备份和还原操作。此 VMware 插件与SnapCenter Server 集成，以支持基于应用程序的备份和SnapCenter特定应用程序插件的恢复。

## 文档资源

有关详细信息，请参阅以下文档资源。

- ["SnapCenter Plug-in for VMware vSphere文档"](#)

## 解决方案资源

请参阅以下 3-2-1 备份解决方案，该方案包含SnapCenter Plug-in for VMware vSphere以及适用于虚拟机的NetApp备份和恢复功能。

技术报告：["使用SnapCenter插件和NetApp Backup and RecoveryVMware 的 3-2-1 数据保护"](#)

Tech ONTAP博客：["使用SnapCenter插件和NetApp Backup and RecoveryVMware 的 3-2-1 数据保护"](#)

## 视频资源

[SnapCenter Plug-in for VMware vSphere- 解决方案先决条件](#)

[SnapCenter Plug-in for VMware vSphere- 部署](#)

[SnapCenter Plug-in for VMware vSphere- 备份 workflow](#)

[SnapCenter Plug-in for VMware vSphere- 还原 workflow](#)

[SnapCenter - SQL 还原 workflow](#)

了解如何使用**NetApp Disaster Recovery**进行虚拟机灾难恢复

NetApp Disaster Recovery利用ONTAP存储自动复制和恢复 VMware 虚拟机。它支持从本地设置恢复到 VMware Cloud on AWS，并使用Amazon FSx for NetApp ONTAP或其他本地 VMware 环境。

## 简介

成功的计划和技术组合可确保关键数据、应用程序和虚拟机的保护。DR 的挑战在于确定适当的保护级别和相关成本。

ONTAP阵列提供内置复制功能，可将卷数据（以及驻留在指定数据存储空间 LUN 上的虚拟机）从一个站点传输到另一个站点。NetApp Disaster Recovery与 vSphere 集成，并可自动执行整个工作流程，以便在发生灾难时实现无缝故障转移和故障恢复。

有关NetApp Disaster Recovery的更多信息，请参阅["NetApp Disaster Recovery概述"](#)。

## 注意事项

VMware vSphere 环境中 DR 故障转移最耗时的部分是在 DR 站点执行清点、注册、重新配置和启动虚拟机所需的步骤。理想的解决方案既具有低 RPO（以分钟为单位），又具有低 RTO（以分钟到小时为单位）。DR 解决方案中经常被忽视的一个因素是定期有效地测试 DR 解决方案的能力。

要构建 DR 解决方案，请牢记以下因素：

- 恢复时间目标 (RTO)。RTO 是指企业从灾难中恢复的速度，或者更具体地说，是执行恢复过程以使业务服务再次可用所需的时间。
- 恢复点目标 (RPO)。RPO 是指恢复的数据相对于灾难发生的时间而言，可供使用的时间。
- 可扩展性和适应性。该因素包括随着需求的增加而逐步增加存储资源的能力。

有关可用解决方案的更多技术信息，请参阅：

- ["使用NetApp Disaster Recovery技术为 NFS 数据存储提供灾难恢复服务"](#)
- ["使用NetApp Disaster Recovery技术为 VMFS 数据存储提供灾难恢复服务"](#)

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 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。