自主勒索软件保护
ONTAP 9

NetApp
February 26, 2026

目录

自主勒索软件保护 1
- 了解ONTAP自动防兰软件保护 1
  - 许可证和支持 1
  - ONTAP 勒索软件保护策略 2
  - ARP检测到的内容 2
  - 了解 ARP 模式 2
  - 威胁评估和ARP快照 4
  - 如何在勒索软件攻击后在 ONTAP 中恢复数据 5
  - 为ARP提供多管理员验证保护 6
  - 利用人工智能(ARP/AI)实现自主防兰功能 6
  - ARP/AI 和 ARP 模型之间的差异一目了然 6
- ONTAP自主防网络软件保护的用例和注意事项 7
  - 支持和不支持的配置 7
  - ARP性能和频率注意事项 10
  - 按平台划分的 ARP 卷限制 11
  - 使用ARP保护的卷进行多管理员验证 11
- 启用 ARP 11
  - 在卷上启用 ONTAP 自主勒索软件保护 11
  - 默认情况下、在新卷中启用ONTAP自动防软件保护 17
  - 选择退出 ONTAP Autonomous Ransomware Protection 默认启用 19
- 学习一段时间后、在ONTAP ARP中切换到活动模式 21
  - 记忆期过后、手动切换到激活模式 21
  - 自动从学习模式切换到活动模式 22
- 了解 SAN 卷的ONTAP ARP 评估期 23
  - 理解熵评估 23
  - 合适的工作负荷和自适应阈值 24
- 暂停ONTAP自动防软件保护以从分析中排除工作负载事件 25
- 管理ONTAP自主防系统攻击检测参数 27
  - 攻击检测的工作原理 27
  - 修改攻击检测参数 27
  - 报告已知电涌 28
  - 配置ARP警报 29
- 对ONTAP ARP检测到的异常活动做出响应 31
- 在发生勒索软件攻击后从ONTAP ARP快照还原数据 35
- 调整自动生成的 ARP 快照的设置 39
- 使用AI更新ONTAP自动防软件保护(ARP/AI) 42
  - 选择ARP/AI的更新首选项 43
  - 使用最新的安全软件包手动更新ARP/AI 43
  - 验证ARP/AI更新 44

自主勒索软件保护

了解ONTAP自动防兰软件保护

从 ONTAP 9.10.1 开始，ONTAP 管理员可以启用自主勒索软件保护 (ARP) 来在 NAS (NFS 和 SMB) 环境中执行工作负载分析，以主动检测并警告可能表明勒索软件攻击的异常活动。从 ONTAP 9.17.1 开始，ARP 还支持块设备卷，包括包含 LUN 或 NVMe 命名空间的 SAN 卷，或包含来自虚拟机管理程序（如 VMware）的虚拟磁盘的 NAS 卷。从 ONTAP 9.17.1P5 开始，也支持 Hyper-V、KVM 和 OpenStack 虚拟机管理程序。

ARP 直接内置于 ONTAP 中，确保与 ONTAP 的其他功能实现集成控制和协调。ARP实时运行，在文件系统中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。

ARP 除了按计划创建快照外，还会定期创建锁定快照，以增加保护。它可以智能地管理快照的保存时长。如果没有检测到异常活动，快照将迅速回收利用。但是，如果检测到攻击，则会将攻击开始前创建的快照保留较长时间。有关更多信息，包括ONTAP版本添加的更改，请参阅 ARP Snapshot。

许可证和支持

您需要许可证才能使用 ARP。决定是在新卷上默认启用 ARP，还是在每个卷上手动启用 ARP。

ARP 的许可证选项

ARP 支持包含在内"ONTAP One 许可证"。如果您没有ONTAP One 许可证，则可以使用其他许可证来用于 ARP，具体取决于您的ONTAP版本。

ONTAP 版本	许可证
ONTAP 9.11.1及更高版本	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` （多租户密钥管理）

- 如果您要从ONTAP 9.10.1 升级到ONTAP 9.11.1 或更高版本，并且系统上已配置 ARP，则无需安装新的 `Anti-ransomware`许可证。对于新的 ARP 配置，需要新的许可证。
- 如果您从ONTAP 9.11.1 或更高版本恢复到ONTAP 9.10.1，并且已使用 Anti_ransomware 许可证启用 ARP，您将看到一条警告消息，可能需要重新配置 ARP。"了解还原ARP的相关信息" 。

ARP 的启用选项

ARP 在集群、SVM 和卷级别提供灵活的启用选项，允许您为新卷配置自动默认启用，或根据需要在现有卷上手动启用 ARP。

在新卷上自动默认启用

从 ONTAP 9.18.1 开始，默认情况下，AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系统的所有新卷都自动启用 ARP。此自动默认 ARP 启用不适用于"不受支持的卷或配置"。

新卷上的 ARP 默认启用在升级后的 12 小时宽限期后生效，或对新的 ONTAP 9.18.1 安装立即生效，前提是在

任何一种情况下都安装了 ARP 许可证。您必须在现有卷上手动启用 ARP。

在宽限期内，您可以"使用 System Manager 或 ONTAP CLI 在集群级别选择退出新卷的默认启用"。如果不选择退出，则会自动为宽限期结束后创建的所有新卷启用 ARP。如果在宽限期后需要更改，您还可以随时打开或关闭默认启用。

在新卷上手动启用默认设置

如果您在群集级别禁用了 ARP 的自动默认启用，您也可以选择在 SVM 级别"默认情况下，在所有新卷上手动启用 ARP"。对于 ONTAP 9.17.1 及更早版本，这是配置 ARP 在新卷上默认启用的唯一方法。

在所有或特定现有卷上启用 **ARP**

从 9.18.1 开始，您可以从集群级别手动在所有现有卷上启用 ARP（选择*集群 > 安全*和 在*反勒索软件*部分中，然后选择*在所有现有卷上启用*）。

如果您希望将 ARP 启用限制为特定卷，则可以"根据每个卷启用 ARP"。

ONTAP 勒索软件保护策略

有效的勒索软件防护需要多层防护协同工作。

虽然 ONTAP 包含 FPolicy、快照、SnapLock 和 Active IQ Digital Advisor（也称为 Digital Advisor）等功能，以帮助防范勒索软件，但 ARP 提供了额外的防御层。

要详细了解 NetApp 产品组合中防范勒索软件的其他功能，请参见：

- "勒索软件和NetApp的保护产品组合"
- "ONTAP 网络保险库加固与 PowerShell"

ARP检测到的内容

ONTAP ARP 旨在防御拒绝服务攻击，即攻击者扣留数据直至支付赎金。ARP基于以下方式提供实时勒索软件检测：

- 将传入数据识别为加密或纯文本。
- 可检测以下内容的分析：
  - 熵：（用于 NAS 和 SAN）对文件中数据随机性的评估
  - 文件扩展名类型：（仅在 NAS 中使用）不符合预期扩展名类型的文件扩展名
  - 文件 **IOPS**：（仅在ONTAP 9.11.1 开始的 NAS 中使用）数据加密时异常卷活动激增

ARP 只需少量文件被加密即可检测到大多数勒索软件攻击的传播，自动响应以保护数据，并提醒您疑似攻击正在发生。

> 没有任何勒索软件检测系统可以保证完全的安全。如果防病毒软件无法检测到入侵，ARP 可提供额外的防御层。

了解 **ARP** 模式

在为卷启用 ARP 后，它将进入学习期以建立基线。 ARP 在转换到主动检测模式之前会分析系统指标以制定警

报配置文件。在主动模式下，ARP 监控异常活动，如果检测到异常行为，则采取保护措施并生成警报。

对于 ARP，学习模式和主动模式行为因ONTAP版本、卷类型和协议（NAS 或 SAN）而异。

NAS 环境和模式类型

下表总结了ONTAP 9.10.1 与 NAS 环境的更高版本之间的差异。

对于采用早期 ARP 模型的版本，建议在开始主动监控之前先进行一段时间的学习。对于支持 NAS 的环境ARP/AI没有学习期，立即开始主动监控。

模式	Description	卷类型和版本
学习	对于某些版本的ONTAP和某些卷类型，启用 ARP 时，ARP 会自动设置为学习模式。在学习模式下， ONTAP系统会根据以下分析领域（熵、文件扩展名类型和文件 IOPS）制定警报配置文件。 建议您将 ARP 保持在学习模式 30 天。从ONTAP 9.13.1 开始，ARP 会自动确定最佳学习间隔并自动切换，切换可能在 30 天之前完成。对于ONTAP 9.13.1 之前的版本，您可以手动进行切换。 从ONTAP 9.16.1 开始， FlexVol卷仅存在活动模式，任何升级到此版本或更高版本的FlexVol卷都会自动从学习模式过渡到活动模式。 对于ONTAP 9.16.1 到 9.17.1，ARP/AI 尚不支持FlexGroup卷，并继续运行较旧的 ARP 模型。因此，对于这些带有FlexGroup卷的版本，仍然建议留出一段学习期。 从ONTAP 9.18.1 开始， FlexVol和FlexGroup卷都只有活动模式。任何升级后的卷都会自动切换到活动模式。 "了解有关从学习模式切换到主动模式的更多信息" 。 命令可 `security anti-ransomware volume workload-behavior show`显示在卷中检测到的文件扩展名。如果您在学习模式早期运行此命令、并且此命令显示了文件类型的准确表示、则不应将此数据用作迁移到活动模式的基础、因为ONTAP仍在收集其他指标。有关的详细信息 `security anti-ransomware volume workload-behavior show`，请参见"ONTAP 命令参考"。	• FlexVol卷（采用ONTAP 9.10.1 至 9.15.1） • FlexGroup卷，版本从ONTAP 9.13.1 到ONTAP 9.17.1
活动	在主动模式下，如果文件扩展名被标记为异常，您应该评估该警报。您可以根据警报采取行动来保护数据，也可以将警报标记为误报。将警报标记为误报会更新警报配置文件。例如，如果警报是由新的文件扩展名触发的，并且您将警报标记为误报，则下次观察到该文件扩展名时，您将不会收到警报。	所有受支持的ONTAP版本以及FlexVol和FlexGroup卷

SAN 环境和模式类型

SAN 环境会使用评估期（类似于 NAS 环境中的学习模式），然后自动过渡到主动检测。下表总结了评估模式和主动模式。

模式	Description	卷类型和版本
评估	进行为期两到四周的评估期，以确定基线加密行为，同时 ARP/AI 在评估期内为 SAN 卷提供即时主动保护。在建立基线阈值期间，可以进行检测并发出警报。您可以通过运行以下命令来确定评估期是否结束： `security anti-ransomware volume show`命令和检查 `Block device detection status`。 "了解有关 SAN 卷和熵评估期的更多信息" 。	• 带有ONTAP 9.17.1 及更高版本的FlexVol 卷
活动	评估期结束后，您可以通过运行 `security anti-ransomware volume show`指挥和检查 `Block device detection status`.的状态 `Active_suitable_workload`表示可以成功监测到评估的熵值。ARP会根据评估过程中审查的数据自动调整自适应阈值。	• 带有ONTAP 9.17.1 及更高版本的FlexVol 卷

威胁评估和ARP快照

ARP 基于根据学习分析测量的传入数据评估威胁概率。当 ARP 检测到异常时，会分配一个测量值。ARP 可能会在检测时或定期分配快照。

ARP 阈值

- **Low**：检测到卷中存在异常的最早时间(例如、在卷中观察到新的文件扩展名)。此检测级别仅适用于ONTAP 9不具有ARP/AI的ARP.16.1之前的版本。
  - 从ONTAP 9.11.1 开始，您可以"自定义ARP检测参数" 。
  - 在ONTAP 9.10.1中、升级到"中等"的阈值为100个或更多文件。
- 中等：检测到高熵，或观察到多个具有相同前所未见文件扩展名的文件。这是ONTAP 9.16.1 及更高版本中带有 ARP/AI 的基准检测级别。

当ONTAP运行分析报告确定异常是否与勒索软件配置文件匹配时，威胁会升级为中等。当攻击概率为中等时，ONTAP会生成 EMS 通知，提示您评估威胁。ONTAPONTAP不会发送有关低威胁的警报；但是，从ONTAP9.14.1 开始，您可以 "修改默认警报设置"。"应对异常活动。" 。

您可以在System Manager的*事件*部分或使用命令查看有关中等威胁的信息 `security anti-ransomware volume show`。在不包含ARP/AI的9.16.1 9.161之前的版本中、也可以使用命令查看低威胁事件 `security anti-ransomware volume show`。有关的详细信息 `security anti-ransomware volume show`，请参见"ONTAP 命令参考"。

ARP Snapshot

当检测到攻击的早期迹象时，ARP 会创建快照。然后进行详细分析，以确认或排除潜在攻击。由于 ARP 快照是在攻击得到完全确认之前主动创建的，因此它们也可能会定期为某些合法应用程序生成。这些快照的存在不应被视为异常。如果确认发生攻击，则攻击概率将升级为 `Moderate`并生成攻击通知。

从ONTAP 9.17.1 开始，会定期为 NAS 和 SAN 卷生成 ARP 快照，并响应检测到的异常。ONTAP在 ARP 快照前添加一个名称，以便于识别。

从ONTAP 9.11.1 开始，您可以修改保留设置。有关更多信息，请参阅"修改快照选项" 。

下表总结了不同版本的 ARP 快照差异。

功能	**ONTAP 9.17.1** 及更高版本	**ONTAP 9.16.1** 及更早版本
创建触发器	• 快照以固定的 4 小时间隔创建，无论任何特定触发器如何 • 确认攻击 根据触发类型创建“定期”或“攻击”快照。	• 检测到高熵 • 检测到新的文件扩展名（9.15.1 及更早版本） • 检测到文件操作激增（9.15.1 及更早版本） 快照创建间隔基于触发器类型。
前缀名称约定	“反勒索软件定期备份” “反勒索软件攻击备份”	“反勒索软件备份”
删除行为	ARP快照被锁定，管理员无法删除	ARP快照被锁定，管理员无法删除
最大快照数	"六个快照可配置限制"	"六个快照可配置限制"
保留期	快照通常保留 12 小时。 • NAS 卷：如果通过文件分析确认了攻击，则攻击前创建的快照将保留，直到管理员将攻击标记为真或误报（明确怀疑）。 • SAN 卷或 VM 数据存储：如果通过块熵分析确认了攻击，则攻击前创建的快照将保留 10 天（可配置）。	• 根据触发条件确定（不固定） • 攻击之前创建的快照将保留，直到管理员将攻击标记为真或误报（明确嫌疑）。
明确嫌疑行动	管理员可以执行清除嫌疑的操作，该操作根据确认设置保留： • 误报保留时间为 24 小时 • 真实阳性保留时间为 7 天	管理员可以执行清除嫌疑的操作，该操作根据确认设置保留： • 误报保留时间为 24 小时 • 真实阳性保留时间为 7 天 此预防性保留行为在ONTAP 9.16.1 之前不存在
到期时间	所有快照均设置了到期时间	无

如何在勒索软件攻击后在 ONTAP 中恢复数据

ARP 基于成熟的ONTAP数据保护和灾难恢复技术，可有效应对勒索软件攻击。当检测到攻击的早期迹象时，ARP 会创建锁定快照。您需要首先确认攻击是真实攻击还是误报。如果您确认存在攻击，则可以使用 ARP 快照恢复卷。

锁定的快照无法通过正常方式删除。但是，如果您稍后决定将攻击标记为误报， ONTAP会删除锁定的副本。

您可以从选定的快照中恢复受影响的文件，而不必恢复整个卷。

有关应对攻击和恢复数据的更多信息，请参阅以下主题：

- "应对异常活动。"

- "从 ARP 快照恢复数据"
- "从ONTAP快照恢复"
- "智能勒索软件恢复"

为ARP提供多管理员验证保护

从ONTAP 9.13.1开始、建议启用多管理员验证(MAV)、以便需要两个或更多经过身份验证的用户管理员才能进行自动防病毒(ARP)配置。有关详细信息，请参见 "启用多管理员验证"。

利用人工智能(ARP/AI)实现自主防兰功能

从ONTAP 9.16.1 开始，ARP 采用机器学习模型进行反勒索软件分析，从而提升了网络弹性。该模型能够在 NAS 环境中以 99% 的准确率检测不断演变的勒索软件形式。的机器学习模型在模拟勒索软件攻击前后都基于大量文件数据集进行了预训练。这种资源密集型的训练是在ONTAP之外进行的，使用开源取证研究数据集来训练模型。整个建模流程不会使用客户数据，因此不存在隐私问题。此训练生成的预训练模型随ONTAP一起提供。但无法通过ONTAP CLI 或ONTAP API 访问或修改此模型。

立即过渡到主动防御ARP/AI

使用ARP/AI，就没有学习期。对于以下受支持的卷类型，ARP/AI 在安装或升级后立即激活：

- NAS FlexVol卷，支持ONTAP 9.16.1 及更高版本
- NAS FlexGroup卷， ONTAP9.18.1 及更高版本
- 使用ONTAP 9.17.1 及更高版本的 SAN 卷（立即激活，即使在期间）"评估期" ）

对于已启用 ARP 功能的现有卷和新卷，将集群升级到支持 ARP/AI 的ONTAP版本后，ARP/AI 保护将自动激活。

ARP/AI自动更新

为了持续提供针对最新勒索软件威胁的最新保护，ARP/AI 提供频繁的自动更新，这些更新在ONTAP常规升级和发布周期之外进行。如果您"已启用自动更新"在您选择安全文件自动更新后，您也将能够开始接收 ARP/AI 的自动安全更新。您还可以选择"手动进行这些更新"并控制更新发生的时间。

从System Manager.16.1开始、除了系统和固件更新之外、还可以使用ONTAP 9提供ARP/AI的安全更新。

"了解有关ARP/AI更新的更多信息"

ARP/AI 和 ARP 模型之间的差异一目了然

功能	ARP	ARP/AI
ONTAP 版本	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 和更高版本；9.15.1（技术预览）
检测方法	分析文件活动、数据熵和文件扩展名类型	在大型取证数据集上训练的人工智能/机器学习模型；分析熵和文件行为
学习期	NAS FlexVol 卷需要 30 天学习模式（9.13.1 及更高版本中提供自动切换）	无学习期；启用后立即激活

功能	ARP	ARP/AI
卷类型支持	• FlexVol: 9.10.1 及更高版本 • FlexGroup: 9.13.1 及更高版本 • SAN：不支持	• FlexVol: 9.16.1 及更高版本 • FlexGroup: 9.18.1 及更高版本 • SAN：9.17.1 及更高版本（含评估期）
Snapshot 创建	由高熵、新文件扩展名或文件操作浪涌触发	以固定的 4 小时间隔创建，并在攻击确认时创建
Snapshot 保留	保留至管理员清除可疑活动	12 小时默认值；根据攻击确认延长（误报 24 小时，确认为阳性 7 天）
更新	静态检测逻辑（仅通过 ONTAP 升级更新）	独立于 ONTAP 版本的自动安全更新
部署	每个卷的手动启用或 SVM 级别的默认设置	手动启用每个卷或 SVM 级别的默认设置；在 9.18.1 及更高版本中支持的系统上，在集群级别的所有新卷上默认启用
评估期间	不适用	SAN 卷（2-4 周）需要建立基准加密阈值

相关信息

- "ONTAP 命令参考"

ONTAP自主防网络软件保护的用例和注意事项

自主勒索软件防护 (ARP) 适用于从ONTAP 9.10.1 开始的 NAS 工作负载和从ONTAP 9.17.1 开始的 SAN 工作负载。在部署 ARP 之前，您应该了解其推荐用途、支持的配置以及性能影响。

支持和不支持的配置

在决定使用ARP时、请务必确保卷的工作负载适合ARP并满足所需的系统配置。

合适的工作负载

ARP 适用于以下类型的工作负载：

- NFS 或 SAN 存储上的数据库
- Windows 或 Linux 主目录

  对于没有 ARP/AI 的环境，用户可能会创建一些在学习期间无法检测到的扩展名的文件。因此，此类工作负载中出现误报的可能性更大。

- 图像和视频

  例如、医疗保健记录和电子设计自动化(Electronic Design Automation、EDA)数据

不适合的工作负载

ARP 不适合以下类型的工作负载：

- 具有高频率文件创建或删除操作的工作负载（几秒钟内数十万个文件；例如，测试/开发工作负载）。
- ARP 的威胁检测依赖于其识别文件创建、重命名或删除操作异常激增的能力。如果应用程序本身是文件活动的来源，则无法有效区分勒索软件活动。
- 应用程序或主机加密数据的工作负载。

  ARP 依赖于区分传入数据是加密的还是未加密的。如果应用程序本身正在加密数据，则该功能的有效性会降低。但是，ARP 仍然可以根据文件活动（删除、覆盖、创建，或者创建文件或使用新的文件扩展名重命名）和文件类型进行工作。

支持的配置

从ONTAP 9.10.1 开始，ARP 可用于 NAS NFS 和 SMB FlexVol卷。从 9.17.1 开始，ARP 可用于 iSCSI、FC 和带有 SAN 存储的 NVMe 的 SAN FlexVol卷。

从 ONTAP 9.10.1 开始，MetroCluster 配置支持 ARP。

以下ONTAP版本支持其他配置和卷类型：

	ONTAP 9.18.1	**ONTAP 9.17.1**	**ONTAP 9.16.1.**	**ONTAP 9.15.1.**	**ONTAP 9.14.1**	**ONTAP 9.13.1**	**ONTAP 9.12.1**	**ONTAP 9.11.1**	**ONTAP 9.10.1**
使用SnapMirror异步保护的卷	✓	✓	✓	✓	✓	✓	✓		
使用SnapMirror异步保护SVM(SVM灾难恢复)	✓	✓	✓	✓	✓	✓	✓		
SVM 数据移动性(`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
FlexGroup卷[1]	✓	✓	✓	✓	✓	✓			
多管理员验证	✓	✓	✓	✓	✓				
ARP/AI、具有自动更新功能	✓	✓	✓						

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1.	ONTAP 9.15.1.	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
ARP/AI 默认启用[2]	✓								

[1] ONTAP 9.16.1 和 9.17.1 不提供对FlexGroup卷的 ARP/AI 支持。升级到这些版本后，启用 ARP 的FlexGroup卷将继续使用 ARP/AI 之前使用的相同 ARP 模型运行。从ONTAP 9.18.1 开始， FlexGroup卷使用 ARP/AI 模型。

[2] 从 ONTAP 9.18.1 开始，ARP/AI 默认启用行为可用于 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系统。此行为在升级后的 12 小时宽限期后或对于新的 ONTAP 9.18.1 安装会自动在所有新卷上启用 ARP/AI。您需要在 "现有卷" 上手动启用 ARP。

SnapMirror和ARP互操作性

从ONTAP 9.12.1 开始， SnapMirror异步目标卷支持 ARP。SnapMirrorSnapMirror同步或SnapMirror主动同步不支持 ARP。

如果SnapMirror源卷启用了 ARP，则SnapMirror目标卷会自动获取 ARP 配置状态（例如 `dry-run`或者 `enabled`）、ARP 训练数据以及 ARP 创建的源卷快照。无需明确启用。

尽管目标卷包含只读 (RO) 快照，但其数据不会进行任何 ARP 处理。但是，当SnapMirror目标卷转换为读写 (RW) 时，ARP 会在已转换为 RW 的目标卷上自动启用。除了源卷上已记录的内容外，目标卷不需要任何其他学习过程。

在ONTAP 9.10.1 和 9.11.1 中， SnapMirror不会将 ARP 配置状态、训练数据和快照从源卷传输到目标卷。因此，当SnapMirror目标卷转换为 RW 时，必须在转换后在学习模式下明确启用目标卷上的 ARP。

ARP和虚拟机

VMware 上的虚拟机 (VM) 支持 ARP。检测对于虚拟机内部和外部的更改有不同的行为。对于虚拟机中涉及大量高度压缩文件（例如 7z 和 ZIP）或加密文件（例如受密码保护的 PDF、DOC 或 ZIP）的工作负载，不建议使用 ARP。

虚拟机外部的更改

如果新扩展名以加密状态进入卷或文件扩展名发生变化，ARP 可以检测到 VM 外部 NFS 卷上的文件扩展名变化。

虚拟机内部的更改

如果勒索软件攻击更改了虚拟机内部的文件，而没有更改虚拟机外部的文件，并且虚拟机的默认熵较低（例如 .txt、.docx 或 .mp4 文件），ARP 就会检测到威胁。对于ONTAP 9.16.1 及更早版本，ARP 会在这种情况下创建保护性快照，但不会生成威胁警报，因为虚拟机外部的文件扩展名未被篡改。从ONTAP 9.17.1 中的 SAN 支持开始，如果 ARP 检测到虚拟机内部的熵异常，还会生成威胁警报。

如果文件默认为高熵文件（例如 .gzip 文件或受密码保护的文件），ARP 的检测能力就会受到限制。在这种情况下，ARP 仍然可以主动拍摄快照；但是，如果文件扩展名未被外部篡改，则不会触发警报。

对于 SAN，ARP 在卷级别分析熵统计数据，并在发现熵异常时触发检测。

> 在ONTAP 9.18.1 及更高版本中，仅FlexVol卷可检测 VM 内发生的攻击，如果 VM 数据存储配置在FlexGroup卷上，则无法检测 VM 内发生的攻击。

不支持的配置

ONTAP S3 环境不支持 ARP。

ARP不支持以下卷配置：

- FlexGroup卷（在ONTAP 9.10.1 至 9.12.1 中）。

> 从ONTAP 9.13.1 到ONTAP 9.17.1，支持FlexGroup卷，但仅限于 ARP/AI 之前使用的 ARP 模型。 ONTAP 9.18.1 开始支持 ARP/AI 的FlexGroup卷。

- FlexCache卷(原始FlexVol卷支持ARP、但缓存卷不支持ARP)
- 使卷脱机
- SnapLock 卷
- SnapMirror活动同步
- SnapMirror同步
- SnapMirror异步（在ONTAP 9.10.1 和 9.11.1 中）。从ONTAP 9.12.1 开始支持SnapMirror异步。有关更多信息，请参阅[SnapMirror] 。
- 受限卷
- Storage VM的根卷
- 已停止Storage VM的卷

ARP性能和频率注意事项

ARP 对系统性能（以吞吐量和峰值 IOPS 衡量）的影响极小。ARP功能的影响取决于具体的卷工作负载。对于常见工作负载，建议采用以下配置限制：

工作负载特征	每个节点的建议卷限制	当每个节点的卷限制超过上限时，性能会下降[1]
读取密集型或数据可以压缩	150	最大IOPS的4%
写入密集且数据无法压缩	60	• NAS： ONTAP 9.15.1 及更早版本的最大 IOPS 的 10% • NAS：ONTAP 9.16.1 及更高版本最大 IOPS 的 5% • SAN： ONTAP 9.17.1 及更高版本的最大 IOPS 的 5%

[1] 无论添加的卷数量超过建议的限制多少，系统性能都不会下降超过这些百分比。

由于 ARP 分析按优先级顺序运行，因此随着受保护卷数量的增加，每个卷上运行的分析频率会降低。

> 在大量新卷上默认启用 ARP 可能会增加系统资源使用率。在卷上启用 ARP 时，请考虑快照等竞争流程的空间需求。

按平台划分的 **ARP** 卷限制

从 ONTAP 9.18.1 开始，ARP 支持根据平台类型和 CPU 核心数量增加卷限制。

平台类型	每个节点支持 **ARP** 的最大卷数
低端（最多 20 个 CPU 内核的系统）	250
中（最多 64 个 CPU 内核的系统）	500
高端（CPU 内核超过 64 个的系统）	1000

CPU 核心计数适用于双节点 HA 对中的每个单独节点。

使用**ARP**保护的卷进行多管理员验证

从ONTAP 9.13.1开始、您可以使用ARP启用多管理员验证(MAV)、以提高安全性。MAV可确保至少需要两个或更多经过身份验证的管理员在受保护的卷上关闭ARP、暂停ARP或将可疑攻击标记为误报。了解如何"为受ARP保护的卷启用MAV"。

您需要为MAV组定义管理员，并为要保护的、 `security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect`ARP命令创建MAV规则 `security anti-ransomware volume disable`。MAV组中的每个管理员都必须在MAV设置范围内批准每个新规则请求"再次添加MAV规则"。

有关、 `security anti-ransomware volume pause`和的详细信息 `security anti-ransomware volume disable`， `security anti-ransomware volume attack clear-suspect`请参见"ONTAP 命令参考"。

从ONTAP 9.14.1 开始，ARP 会在创建 ARP 快照和发现新文件扩展名时发出警报。这些事件的警报默认处于禁用状态。警报可以在卷或 SVM 级别设置。您可以使用以下命令启用警报 `security anti-ransomware vserver event-log modify`或使用 `security anti-ransomware volume event-log modify`。

有关和的 `security anti-ransomware volume event-log modify`详细信息 `security anti-ransomware vserver event-log modify`，请参见"ONTAP 命令参考"。

后续步骤

- "启用自主勒索软件保护"
- "为受ARP保护的卷启用MAV"

启用 **ARP**

在卷上启用 **ONTAP** 自主勒索软件保护

从ARP.10.1开始、您可以在现有卷上启用自动防兰软件保护(Autonomous Ransmor Protection、ONTAP 9)、也可以创建新卷并从头开始启用ARP.10.1。

关于此任务

要启用 ARP，请按照与您的环境相匹配的步骤操作。您确保您的环境满足某些要求：

- 带有FlexVol卷的 NAS
- 带有FlexGroup卷的 NAS
- SAN卷

启用 ARP 后，ARP 可能会进入过渡期，具体取决于您的环境和ONTAP版本：

Volume type	ONTAP 版本	启用后的行为
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 无需学习期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP启动后将进入学习模式，持续30天。
NAS FlexVol	ONTAP 9.16.1 及更高版本	ARP/AI 无需学习期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP启动后将进入学习模式，持续30天。
SAN卷	ONTAP 9.17.1 及更高版本	ARP/AI 立即启动，启动评估期，以确定合适的警报阈值，然后再从初始的保守阈值过渡。

开始之前

启用 ARP 之前，请确保您的环境具备以下条件：

NAS 特定要求

- 启用了 NFS 或 SMB（或两者）协议的存储虚拟机 (SVM)。
- 已配置客户端的 NAS 工作负载。
- 积极"接合路径"就音量而言。

SAN 特定要求

- 启用了 iSCSI、FC 或 NVMe 协议的存储虚拟机 (SVM)。
- 已配置客户端的 SAN 工作负载。

一般要求

- 这"正确的许可证"适用于您的ONTAP版本。
- （推荐）启用多管理员验证 (MAV)（ONTAP 9.13.1 及更高版本）。看"启用多管理员验证"。

在 **NAS FlexVol**卷上启用 **ARP**

您可以使用系统管理器或ONTAP CLI 在 NAS FlexVol卷上启用 ARP。具体流程会根据您的ONTAP版本而有所不同。

ONTAP 9.16.1 及更高版本

从ONTAP 9.16.1 开始，ARP/AI 可立即激活，无需学习期。

System Manager

1. 选择*存储>卷*，然后选择要保护的卷。
2. 在*Volumes*概述的*Security*选项卡中，选择*Status*从Disabled切换为Enabled。
3. 在“反勒索软件”框中验证卷的 ARP 状态。

   要显示所有卷的ARP状态：在*卷*窗格中，选择*显示/隐藏*，然后确保选中*反勒索软件*状态。

命令行界面

在现有卷上启用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

创建启用 **ARP** 的新卷：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

验证**ARP**状态：

```
security anti-ransomware volume show
```

有关的详细信息 `security anti-ransomware volume show`，请参见"ONTAP 命令参考"。

ONTAP 9.10.1 至 **9.15.1**

对于ONTAP 9.10.1 至 9.15.1 版本，您应该首先启用 ARP。"学习模式" （或“试运行”状态）。该系统通过分析工作负载来描述正常行为。以主动模式启动可能会导致过多的误报。

建议让 ARP 以学习模式运行至少 30 天。从ONTAP 9.13.1 开始，ARP 会自动确定最佳学习间隔并自动切换，切换可能在 30 天之前完成。

System Manager

1. 选择*存储>卷*，然后选择要保护的卷。
2. 在*Volumes*概述的*Security*选项卡中，选择*Status*从Disabled切换为Enabled。
3. 在“反勒索软件”框中选择“在学习模式下启用”。

> 你可以"禁用关联存储虚拟机上的自动学习活动模式转换"如果您想手动控制学习模式到主动模式的转换。

在现有卷中、学习和活动模式仅适用于新写入的数据、而不适用于卷中已有的数据。不会扫描和分析现有数据、因为在为卷启用ARP后、系统会根据新数据假设先前正常数据流量的特征。

4. 在“反勒索软件”框中验证卷的 ARP 状态。

   要显示所有卷的ARP状态：在*卷*窗格中，选择*显示/隐藏*，然后确保选中*反勒索软件*状态。

命令行界面

在现有卷上启用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

有关的详细信息 `security anti-ransomware volume dry-run`，请参见"ONTAP 命令参考"。

创建启用 **ARP** 的新卷：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

禁用自动切换（可选）：

如果您已将ONTAP升级到 ONTAP 9.13.1 至ONTAP 9.15.1，并且想要手动控制所有关联卷从学习模式切换到活动模式，则可以从 SVM 执行此操作：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

验证**ARP**状态：

```
security anti-ransomware volume show
```

在 **NAS FlexGroup**卷上启用 **ARP**

您可以使用系统管理器或ONTAP CLI 在 NAS FlexGroup卷上启用 ARP。具体流程会根据您的ONTAP版本而有所不同。

ONTAP 9.18.1 及更高版本

从ONTAP 9.18.1 开始，ARP/AI 对FlexGroup卷立即生效，无需学习期。

System Manager

1. 选择“存储 > 卷”，然后选择要保护的FlexGroup卷。
2. 在*Volumes*概述的*Security*选项卡中，选择*Status*从Disabled切换为Enabled。
3. 在“反勒索软件”框中验证卷的 ARP 状态。

   要显示所有卷的ARP状态：在*卷*窗格中，选择*显示/隐藏*，然后确保选中*反勒索软件*状态。

命令行界面

在现有**FlexGroup**卷上启用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

创建启用 **ARP** 的新**FlexGroup**卷：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

验证**ARP**状态：

```
security anti-ransomware volume show
```

ONTAP 9.13.1 至 **9.17.1**

对于ONTAP 9.13.1 至 9.17.1 版本， FlexGroup卷的起始版本为："学习模式" 。该系统通过分析工作负载来描述正常行为。

建议让 ARP 以学习模式运行至少 30 天。ARP 会自动确定最佳学习周期间隔并自动切换，切换可能在 30 天之前发生。

System Manager

1. 选择“存储 > 卷”，然后选择要保护的FlexGroup卷。
2. 在*Volumes*概述的*Security*选项卡中，选择*Status*从Disabled切换为Enabled。
3. 在“反勒索软件”框中选择“在学习模式下启用”。

   你可以"禁用自动学习到活动模式的转换"如果您想手动控制学习模式到主动模式的转换。

4. 在“反勒索软件”框中验证卷的 ARP 状态。

命令行界面

在现有**FlexGroup**卷上启用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

创建启用 **ARP** 的新**FlexGroup**卷：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

禁用自动切换（可选）：

如果您想手动控制从学习模式到活动模式的切换：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

验证**ARP**状态：

```
security anti-ransomware volume show
```

在**SAN**卷上启用**ARP**

从ONTAP 9.17.1 开始，您可以在 SAN 卷上启用 ARP。 ARP/AI 功能会自动启用，并在 SAN 卷维护期间立即开始主动监控和保护 SAN 卷。"评估期"同时确定工作负载是否适合 ARP，并设置最佳加密检测阈值。

您可以使用系统管理器或ONTAP CLI 在 SAN 卷上启用 ARP。

System Manager

步骤

1. 选择“存储 > 卷”，然后选择要保护的 SAN 卷。
2. 在*Volumes*概述的*Security*选项卡中，选择*Status*从Disabled切换为Enabled。
3. ARP/AI自动进入评估期。
4. 在“反勒索软件”框中验证 ARP 状态和评估状态。

   要显示所有卷的ARP状态：在*卷*窗格中，选择*显示/隐藏*，然后确保选中*反勒索软件*状态。

命令行界面

在现有 **SAN** 卷上启用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

创建启用 **ARP** 的新 **SAN** 卷：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

验证**ARP**状态和评估状态：

```
security anti-ransomware volume show
```

检查 `Block device detection status`现场监测评估期进展情况。

有关的详细信息 `security anti-ransomware volume show`，请参见"ONTAP 命令参考"。

相关信息

- "学习一段时间后切换到活动模式"

默认情况下、在新卷中启用**ONTAP**自动防软件保护

从 ONTAP 9.10.1 开始，您可以配置存储虚拟机 (SVM)，以便在默认情况下使用 Autonomous Ransomware Protection (ARP) 启用新卷。您可以使用 System Manager 或 ONTAP CLI 修改此设置。

从 ONTAP 9.18.1 开始，在群集升级或新安装后的 12 小时宽限期之后，默认情况下在 "支持的系统" 的群集级别的所有新卷上都启用 ARP。如果在群集级别禁用 ARP 的自动默认启用，您仍然可以选择在 SVM 级别的所有新卷上默认手动启用 ARP。

对于 ONTAP 9.17.1 及更早版本，在 SVM 级别进行配置是默认情况下在新卷上启用 ARP 的唯一方法。

关于此任务

默认情况下，新建卷的 ARP 功能是禁用的。您需要启用 ARP 功能，并将其设置为在 SVM 中创建的新卷上默认启用。

当您更改 SVM 的默认设置时，未启用 ARP 的现有卷不会自动更改 ARP 启用状态。本程序中描述的 SVM 设置更改仅影响新生成的卷。学习如何"为现有卷启用ARP"。

启用 ARP 后，ARP 可能会进入过渡期，具体取决于您的环境和ONTAP版本：

Volume type	**ONTAP** 版本	启用后的行为
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 无需学习期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP启动后将进入学习模式，持续30天。
NAS FlexVol	ONTAP 9.16.1 及更高版本	ARP/AI 无需学习期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP启动后将进入学习模式，持续30天。
SAN卷	ONTAP 9.17.1 及更高版本	ARP/AI 立即启动，启动评估期，以确定合适的警报阈值，然后再从初始的保守阈值过渡。

开始之前

启用 ARP 之前，请确保您的环境具备以下条件：

NAS 特定要求

- 启用了 NFS 或 SMB（或两者）协议的存储虚拟机 (SVM)。
- 积极"接合路径"就音量而言。

SAN 特定要求

- 启用了 iSCSI、FC 或 NVMe 协议的存储虚拟机 (SVM)。

一般要求

- 这"正确的许可证"适用于您的ONTAP版本。
- （推荐）启用多管理员验证（MAV）（ONTAP 9.13.1+）。看"启用多管理员验证"。

步骤

默认情况下、您可以使用System Manager或ONTAP命令行界面在新卷上启用ARP。

System Manager

1. 选择“存储”或“集群”（取决于您的环境），选择“存储虚拟机”，然后选择将包含要使用 ARP 保护的卷的存储虚拟机。
2. 导航到“设置”选项卡。在“安全”下，找到“反勒索软件”磁贴，然后选择 。
3. 勾选此框以启用反勒索软件 (ARP)。勾选附加框可在存储虚拟机中所有符合条件的卷上启用 ARP。
4. 对于有建议学习期的ONTAP版本，请选择“学习足够时间后自动从学习模式切换到活动模式”。这允许 ARP 确定最佳学习间隔并自动切换到主动模式。

命令行界面

修改现有**SVM**，使其在新卷中默认启用**ARP**。

选择 `dry-run`如果您的 `ARP` 版本需要学习期。否则，请选择 `enabled。

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

创建一个新的**SVM**，并默认为新卷启用**ARP**。

选择 `dry-run`如果您的 `ARP` 版本需要学习期。否则，请选择 `enabled。

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

修改现有**SVM**，禁用自动学习到主动模式的转换

如果您已从ONTAP 9.13.1 升级到ONTAP 9.15.1，并且默认状态为 `dry-run`（学习模式），启用自适应学习，以便进行更改 `enabled`状态（活动模式）是自动完成的。您可以禁用此自动切换功能，以便手动控制所有关联音量从学习模式切换到活动模式：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

验证 **ARP** 状态

```
security anti-ransomware volume show
```

相关信息

- "学习一段时间后切换到活动模式"
- "安全反勒索软件卷显示"

选择退出 **ONTAP Autonomous Ransomware Protection** 默认启用

从 ONTAP 9.18.1 开始，如果安装了 ARP 许可证，则在升级或新安装后 12 小时的预热期

后，自主勒索软件保护 (ARP) 会在 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系统的所有新卷上默认自动启用。您可以在 12 小时宽限期内或之后使用 System Manager 或 ONTAP CLI 选择退出此默认启用。

现有卷必须"手动启用"用于 ARP。

关于此任务

您可以稍后更改为此过程选择的设置。宽限期结束后，您可以随时灵活开启或关闭默认启用功能：

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

步骤

您可以使用 System Manager 或 ONTAP CLI 管理 ARP 默认启用选项。

System Manager

1. 选择*集群>设置*。
2. 执行以下操作之一：
   - 在活动宽限期内禁用：
     i. 在 **Anti-ransomware** 部分，您将看到一条消息，指示启用 ARP 之前的剩余小时数。选择 **Don't enable**。
     ii. 在下一个对话框中选择*禁用*，以确认新卷的默认 ARP 启用已关闭。
   - 宽限期后禁用：
     i. 在 **Anti-ransomware** 部分，选择 。
     ii. 选中复选框，然后 保存 以禁用新卷的默认 ARP 启用。

命令行界面

1. 检查默认启用状态：

   ```
   security anti-ransomware auto-enable show
   ```

2. 禁用新卷的默认启用：

   ```
   security anti-ransomware auto-enable modify -new-volume-auto-enable
   false
   ```

相关信息

- "在单个卷上启用 ONTAP 自主勒索软件保护"

学习一段时间后、在ONTAP ARP中切换到活动模式

对于 NAS 环境，手动或自动将启用 ARP 的卷从学习模式切换到活动模式。如果您在ONTAP 9.15.1 及更早版本中使用 ARP，或者在ONTAP 9.17.1 及更早版本的FlexGroup卷上运行 ARP，则需要切换模式。

ARP 完成建议至少 30 天的学习模式运行后，您可以手动切换到活动模式。从ONTAP 9.13.1 开始，ARP 会自动确定最佳学习周期间隔并自动切换，切换可能在 30 天之前发生。

如果您将 ARP 与 ARP/AI 保护结合使用，则 ARP 会自动激活。无需学习期。

> 在现有卷中、学习和活动模式仅适用于新写入的数据、而不适用于卷中已有的数据。不会扫描和分析现有数据、因为在为卷启用ARP后、系统会根据新数据假设先前正常数据流量的特征。

记忆期过后、手动切换到激活模式

对于ONTAP 9.10.1 至 9.15.1（ONTAP 9.17.1 及更早版本，带FlexGroup卷），学习期结束后，您可以使用系统管理器或ONTAP CLI 手动将 ARP 学习模式转换为活动模式。

关于此任务

本过程中描述的学习期后手动过渡到主动模式特定于 NAS 环境。

步骤

您可以使用系统管理器或ONTAP CLI 从学习模式切换到主动模式。

System Manager

1. 选择*存储>卷*，然后选择已准备好进入活动模式的卷。
2. 在*Volumes*概述的*Security*选项卡中，在Anti-勒索 软件框中选择*切换到活动模式*。
3. 您可以在*Anti-勒索 软件*框中验证卷的ARP状态。

命令行界面

1. 如果尚未自动完成，则修改受保护的卷以切换到活动模式：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

   您也可以使用 modify volume 命令切换到活动模式：

```
volume modify -volume <vol_name> -vserver <svm_name> -anti
-ransomware-state enabled
```

2. 验证卷的ARP状态。

```
security anti-ransomware volume show
```

自动从学习模式切换到活动模式

从ONTAP 9.13.1 开始，自适应学习已添加到 ARP 分析中，并且可以自动从学习模式切换到主动模式。ARP自动从学习模式切换到主动模式的自主决策基于以下选项的配置设置：

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

如果启用自动切换功能，即使未满足所有条件，卷也会在最多 30 天后自动切换到活动模式。此 30 天的限制是固定的，无法更改。

有关ARP配置选项(包括默认值)的详细信息、请参见 "ONTAP 命令参考"。

相关信息

- "安全反勒索软件量"

了解 SAN 卷的ONTAP ARP 评估期

从ONTAP 9.17.1 开始，ARP 需要一段评估期来确定 SAN 卷工作负载的熵级别是否适合勒索软件防护。在 SAN 卷上启用 ARP 后，ARP/AI 会在评估期间主动监控和保护该卷，同时确定最佳加密阈值。在评估期间，可以使用保守阈值进行检测和发出警报，同时建立基线阈值。会区分评估后的 SAN 卷中适用和不适用的工作负载，如果确定工作负载适合防护，则会根据评估期统计数据自动设置加密阈值。

理解熵评估

系统每隔 10 分钟收集一次连续的加密统计信息。在评估期间，还会每四小时持续创建一次 ARP 定期快照。如果某个时间间隔内的加密百分比超过了为该卷确定的最佳加密阈值，则会触发警报，`Anti_ransomware_attack_backup`创建快照，并且任何定期 ARP 快照的快照保留时间都会增加。

确认评估期有效

运行以下命令并确认状态为 `evaluation_period`。如果卷不符合评估条件，则不会显示评估状态。

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

响应示例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

监测评估期数据收集

您可以通过运行以下命令来实时监控加密检测。该命令将返回一个直方图，显示每个加密百分比范围内的数据量。该直方图每 10 分钟更新一次。

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

响应示例：

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

合适的工作负荷和自适应阈值

评估以下列结果之一结束：

- 该工作负载适用于 **ARP**。ARP会自动将自适应阈值设置为高于评估期内最大加密百分比的 10%。ARP还会持续收集统计信息并定期创建 ARP 快照。
- 该工作负载不适合 **ARP**。ARP会自动将自适应阈值设置为评估期内可见的最大加密百分比。ARP还会继续收集统计信息并定期创建 ARP 快照，但系统最终会建议在该卷上禁用 ARP。

确定评估结果

评估期结束后，ARP根据评估结果自动设置自适应阈值。

您可以通过运行以下命令来确定评估结果。卷适用性显示在 `Block device detection status`场地：

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

响应示例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

您还可以显示评估结果所采用的值阈值：

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

响应示例：

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

暂停ONTAP自动防软件保护以从分析中排除工作负载事件

如果您预期会发生异常工作负载事件、您可以随时临时暂停和恢复自主勒索软件保护(ARP)分析。

从ONTAP 9.131开始、您可以启用多管理员验证(MAV)、以便需要两个或更多经过身份验证的用户管理员来暂停ARP。

"了解有关MAV的更多信息"(英文)

关于此任务

在 ARP 暂停期间， ONTAP不会记录新写入的事件或操作；但是，对早期日志的分析会在后台继续进行。

> 请勿使用ARP禁用功能暂停分析。这样做会禁用卷上的ARP、并且与所了解的工作负载行为相关的所有现有信息都将丢失。这需要重新开始学习。

步骤

您可以使用System Manager或ONTAP命令行界面暂停ARP。

System Manager

1. 选择*存储>卷*，然后选择要暂停ARP的卷。
2. 在卷概览的“安全”选项卡中，选择“反勒索软件”框中的“暂停反勒索软件”。

> 从ONTAP 9.13.1 开始，如果您使用 MAV 来保护 ARP 设置，则暂停操作会提示您获得一个或多个其他管理员的批准。"必须获得所有管理员的批准"与 MAV 审批小组相关，否则操作将会失败。

3. 要恢复监控，请选择*恢复反勒索软件*。

命令行界面

1. 暂停卷上的ARP：

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. 要恢复处理、请使用 `resume` 命令：

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

有关的详细信息 `security anti-ransomware volume`，请参见"ONTAP 命令参考"。

3. 如果您使用 MAV（从ONTAP 9.13.1 开始与 ARP 一起使用）来保护 ARP 设置，则暂停操作会提示您获得一个或多个其他管理员的批准。必须获得与 MAV 审批组相关的所有管理员的批准，否则操作将失败。

   如果您正在使用MAV、并且预期的暂停操作需要额外的审批、则每个MAV组审批人将执行以下操作：

   a. 显示请求：

```
security multi-admin-verify request show
```

   b. 批准申请：

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

   最后一个组批准者的响应指示卷已修改、并且ARP状态已暂停。

   如果您正在使用MAV、并且您是MAV组批准者、则可以拒绝暂停操作请求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
有关的详细信息 `security multi-admin-verify request`，请参见"ONTAP 命令参考"。

管理ONTAP自主防系统攻击检测参数

从ONTAP 9.11.1开始、您可以修改启用了自动勒索软件保护的特定卷上的勒索软件检测参数、并将已知激增报告为正常文件活动。根据您的特定卷工作负载调整检测参数有助于提高报告的准确性。

攻击检测的工作原理

当自主勒索软件防护 (ARP) 处于学习或评估模式时，它会为卷行为制定基准值。这些基准值包括熵、文件扩展名以及（从ONTAP 9.11.1 开始的）IOPS。这些基准用于评估勒索软件威胁。有关这些标准的更多信息，请参阅"ARP检测到的内容" 。

不同的数据量和工作负载需要不同的检测参数。例如，启用 ARP 的卷可能托管多种类型的文件扩展名，在这种情况下，您可能需要将从未见过的文件扩展名的阈值计数修改为大于默认值 20 的数字，或者禁用基于从未见过的文件扩展名的警告。从ONTAP 9.11.1 开始，您可以修改攻击检测参数，使其更好地适应您的特定工作负载。

从ONTAP 9.14.1开始、您可以在ARP发现新文件扩展名以及创建快照时配置警报。有关详细信息，请参见[modify-alerts]。

NAS 环境中的攻击检测

在ONTAP 9.10.1中、如果ARP同时检测到以下两种情况、则会发出警告：

- 超过20个文件、其文件扩展名先前未在卷中发现
- 高熵数据

从ONTAP 9.11.1开始、如果满足_only一个条件、ARP将发出威胁警告。例如、如果在24小时内观察到20个以上的文件具有以前在卷中未观察到的文件扩展名、ARP会将此情况归类为所观察到的熵的威胁_th考虑_。24小时值和20文件值为默认值、可以进行修改。

> 要减少大量误报，请转到“存储”>“卷”>“安全”>“配置工作负载特征”，并禁用“监控新文件类型”。此设置在ONTAP 9.14.1 P7、9.15.1 P1、9.16.1 及更高版本中默认禁用。

SAN 环境中的攻击检测

从ONTAP 9.17.1 开始，如果 ARP 检测到超过自动学习阈值的高加密速率，则会发出警告。此阈值是在"评估期"但可以修改。

修改攻击检测参数

根据启用 ARP 的卷的预期行为，您可能需要修改攻击检测参数。

步骤

1. 查看现有攻击检测参数：

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
           Block Device Auto Learned Encryption Threshold : 10
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                 Is Detection Based on File Create Rate? : true
                 Is Detection Based on File Rename Rate? : true
                 Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 5
       Never Seen before File Extensions Duration in Hour : 48
```

2. 所有显示的字段均可使用布尔值或整数值进行修改。要修改字段，请使用 `security anti-ransomware volume attack-detection-parameters modify`命令。

   有关的详细信息 `security anti-ransomware volume attack-detection-parameters modify`，请参见"ONTAP 命令参考"。

报告已知电涌

即使处于活动状态、ARP也会继续修改检测参数的基线值。如果您知道音量活动中的电涌、无论是一次性电涌还是新常态的特征性电涌、您应将其报告为安全。手动将这些激增报告为安全状态有助于提高ARP威胁评估的准确性。

报告一次性激增

1. 如果在已知情况下发生一次性激增、而您希望ARP在未来情况下报告类似的激增、请从工作负载行为中清除该激增：

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

   有关的详细信息 `security anti-ransomware volume workload-behavior clear-surge`，请参

见"ONTAP 命令参考"。

修改基线喘振

1. 如果报告的浪涌应视为正常应用行为、则报告此浪涌以修改基线浪涌值。

```
security anti-ransomware volume workload-behavior update-baseline-from-
surge -vserver <svm_name> -volume <volume_name>
```

详细了解 `security anti-ransomware volume workload-behavior update-baseline-from-surge`在"ONTAP 命令参考" 。

配置ARP警报

从ONTAP 9.14.1开始、您可以使用ARP为两个ARP事件指定警报：

- 观察卷上的新文件扩展名
- 创建ARP快照

可以在单个卷上或为整个SVM设置这两个事件的警报。如果为SVM启用警报、则只有在启用警报之后创建的卷才会继承警报设置。默认情况下、任何卷都不会启用警报。

事件警报可通过多管理员验证进行控制。有关更多信息，请参阅"使用ARP保护的卷进行多管理员验证" 。

步骤

您可以使用系统管理器或ONTAP CLI 设置 ARP 事件警报。

System Manager

为卷设置警报

1. 导航到“卷”。选择要修改设置的单个卷。
2. 选择“安全”选项卡，然后选择“事件严重性设置”。
3. 要接收“检测到新文件扩展名”和“已创建勒索软件快照”的警报，请选择“严重性”标题下的下拉菜单。将设置从“不生成事件”修改为“通知”。
4. 选择 * 保存 * 。

为**SVM**设置警报

1. 导航到 存储虚拟机，然后选择要启用设置的 SVM。
2. 在“安全”标题下，找到“反勒索软件”选项卡。选择 然后*编辑勒索软件事件严重性*。
3. 要接收“检测到新文件扩展名”和“已创建勒索软件快照”的警报，请选择“严重性”标题下的下拉菜单。将设置从“不生成事件”修改为“通知”。
4. 选择 * 保存 * 。

命令行界面

为卷设置警报

- 要为新文件扩展名设置警报、请执行以下操作：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-new-file-extension-seen true`
```

- 要为创建ARP快照设置警报、请执行以下操作：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用确认设置 `anti-ransomware volume event-log show` 命令：

为**SVM**设置警报

- 要为新文件扩展名设置警报、请执行以下操作：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-new-file-extension-seen true
```

- 要为创建ARP快照设置警报、请执行以下操作：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用确认设置 `security anti-ransomware vserver event-log show` 命令：

详细了解 `security anti-ransomware vserver event-log`命令"ONTAP 命令参考" 。

相关信息

- "了解自动防兰索防攻击和自动防兰索防快照"(英文)
- "ONTAP 命令参考"

对ONTAP ARP检测到的异常活动做出响应

当自主勒索软件保护(ARP)检测到受保护卷中的异常活动时、它会发出警告。您应评估通知以确定活动是否可接受(误报)或攻击是否看起来是恶意的。对攻击进行分类后、您可以清除有关可疑文件的警告和通知。

对攻击进行分类时，ARP 快照要么在分类操作启动后保留一段较短的时间（ONTAP 9.16.1 及更高版本），要么立即删除（ONTAP 9.15.1 及更早版本）。

从ONTAP 9.11.1 开始，您可以修改"保留设置"用于 ARP 快照。

关于此任务

当 ARP 检测到高数据熵、包含数据加密的异常卷活动以及异常文件扩展名的任意组合时，它会显示可疑文件列表。从适用于 NAS 和 SAN 环境的ONTAP 9.17.1 开始，系统管理器中的“反勒索软件”页面还会报告熵峰值的详细信息。

当发出 ARP 警告通知时，请通过以下两种方式之一指定活动进行响应：

- 误报

  已识别的文件类型或熵峰值是您的工作负载中预期会出现的，可以忽略。

- 潜在勒索软件攻击

  所识别的文件类型或熵峰值在您的工作负载中是意外的，应被视为潜在攻击。

在您更新您的决定并清除 ARP 通知后，系统将恢复正常监控。ARP会将您的评估记录到威胁评估配置文件中，并使用您的选择来监控后续的文件活动。

如果发生可疑攻击、您必须确定是否为攻击、如果是、则对其做出响应、并在清除通知之前还原受保护的数据。"详细了解如何从勒索软件攻击中恢复"。

如果还原整个卷、则不需要清除任何通知。

开始之前

ARP 必须主动保护卷，而不是处于学习或评估模式。

步骤

您可以使用System Manager或ONTAP命令行界面来响应异常活动。

System Manager

1. 当您收到“异常活动”通知时，请点击链接。或者，导航到“卷”概览的“安全”选项卡。

   警告显示在*Events*菜单的*Overview*窗格中。

2. 在“安全”选项卡中，查看可疑文件类型或熵峰值报告。
   - 对于可疑文件，请检查“可疑文件类型”对话框中的每种文件类型，并分别标记。
   - 对于熵峰值，请检查熵报告。
3. 记录你的回答：

如果选择此值…	执行此操作 …
误报	a. 执行以下操作之一： ◦ 对于文件类型警告，选择*更新并清除可疑文件类型*。 ◦ 对于熵尖峰，选择*标记为假阳性*。 这些操作可清除有关可疑文件或活动的警告通知。ARP随后将恢复对卷的正常监控。对于ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照会在分类操作触发的缩短保留期后自动删除。对于ONTAP 9.15.1 及更早版本，清除可疑文件类型后，相关的 ARP 快照会自动删除。 从ONTAP 9.13.1 开始，如果您使用 MAV 来保护 ARP 设置，清除可疑项操作会提示您获得一个或多个其他管理员的批准。"必须获得所有管理员的批准"与 MAV 审批小组相关，否则操作将会失败。
潜在勒索软件攻击	a. 回应攻击： ◦ 对于文件类型警告，将选定的文件标记为*潜在勒索软件攻击*，并"还原受保护的数据" 。 ◦ 对于表示攻击的熵峰值，选择“标记为潜在勒索软件攻击”并"还原受保护的数据" 。 b. 数据恢复完成后，记录您的决定并恢复正常的ARP监控： ◦ 对于文件类型警告，选择*更新并清除可疑文件类型*。 ◦ 对于熵峰值，选择*标记为潜在勒索软件攻击*并选择*保存并关闭*。 如果您已恢复整个卷，则无需清除任何可疑文件类型通知。 记录您的决定将清除攻击报告。对于ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照会在分类操作触发的缩短保留期后自动删除。对于ONTAP 9.15.1 及更早版本，还原卷后，ARP 快照将自动删除。

命令行界面

验证攻击

1. 收到可疑勒索软件攻击的通知后，请验证此攻击的时间和严重性：

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

示例输出：

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

您还可以检查 EMS 消息：

```
event log show -message-name callhome.arw.activity.seen
```

2. 生成攻击报告并指定保存位置：

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

命令示例：

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

示例输出：

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. 在管理客户端系统上查看报告。例如：

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

采取行动

1. 根据您对文件扩展名或熵峰值的评估，执行以下操作之一：

   - 误报

     运行以下命令之一来记录您的决定并恢复正常的自主勒索软件防护监控：

     - 对于文件扩展名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension_identifiers>] -false
       -positive true
       ```

       使用以下可选参数仅将特定扩展识别为误报：

       - `[-extension <text>, … ]`：文件扩展名

     - 对于熵尖峰：

       ```
       security anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
       HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
       ```

   - 潜在的勒索软件攻击

     应对攻击和 "从ARP创建的备份快照恢复数据"。运行以下命令之一记录您的决定并恢复正常的 ARP 监控：

     - 对于文件扩展名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension identifiers>] -false
       -positive false
       ```

       使用以下可选参数仅将特定扩展识别为潜在勒索软件：

       - `[-extension <text>, … ]`：文件扩展名

     - 对于熵尖峰：

       ```
       security anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
       HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
       false
       ```

这 `clear-suspect`操作会清除攻击报告。如果您还原了整个卷，则无需清除任何可疑文件类型通知。对于ONTAP 9.16.1 及更高版本中的 ARP/AI，ARP 快照会在分类操作触发的缩短保留期后自动删除。对于ONTAP 9.15.1 及更早版本，还原卷或清除可疑事件后，ARP 快照会自动删除。

2. 从 9.18.1 版本开始，您可以确定以下状态： `clear-suspect`手术：

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

MAV选项

1. 如果您使用的是MAV和预期的 `clear-suspect` 运营需要额外批准、每个MAV组批准人必须：

   a. 显示请求：

   ```
   security multi-admin-verify request show
   ```

   b. 批准恢复正常反勒索软件监控的请求：

   ```
   security multi-admin-verify request approve -index[<number
   returned from show request>]
   ```

   最后一个组批准者的响应指示卷已修改、并记录误报。

2. 如果您正在使用MAV、并且您是MAV组批准者、您还可以拒绝可疑交易请求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

相关信息

- "NetApp知识库：了解自主勒索软件防护攻击和自主勒索软件防护快照"
- "修改自动快照选项"
- "安全反勒索软件量"
- "安全多管理员验证请求"

在发生勒索软件攻击后从ONTAP ARP快照还原数据

自主勒索软件防护 (ARP) 会创建快照来防御潜在的勒索软件威胁。您可以使用其中一个 ARP 快照或卷的其他快照来恢复数据。

关于此任务

ARP 使用以下前缀名称之一创建快照：

- `Anti_ransomware_periodic_backup`：在ONTAP 9.17.1 及更高版本中用于定期创建的快照。例如，`Anti_ransomware_periodic_backup.2025-06-01_1248`。
- `Anti_ransomware_attack_backup`：在ONTAP 9.17.1 及更高版本中用于响应异常而创建的快照。例如，`Anti_ransomware_attack_backup.2025-08-25_1248`。
- `Anti_ransomware_backup`：在ONTAP 9.16.1 及更早版本中，用于为应对异常而创建的快照。例如，`Anti_ransomware_backup.2022-12-20_1248`。

要从快照中恢复，`Anti_ransomware`快照 在识别出系统攻击后，必须先释放ARP快照。

如果没有报告系统攻击，您必须首先从 `Anti_ransomware`快照，然后从您选择的快照完成卷的后续恢复。

> 如果受 ARP 保护的卷属于SnapMirror关系，则从快照还原卷后，您需要手动更新该卷的所有镜像副本。如果跳过此步骤，镜像副本可能会变得不可用，需要删除并重新创建。

开始之前

"您必须将攻击标记为潜在的勒索软件攻击"从快照恢复数据之前。

步骤

您可以使用System Manager或ONTAP 命令行界面还原数据。

System Manager

在系统受到攻击后恢复

1. 要从ARP快照还原、请跳至步骤二。要从早期的快照还原、必须先释放ARP快照上的锁定。
   a. 选择 * 存储 > 卷 * 。
   b. 选择*安全性*，然后选择*查看可疑文件类型*。
   c. 将文件标记为"潜在勒索软件攻击"。
   d. 选择*更新*和*清除可疑文件类型*。
2. 显示卷中的快照：

   选择*存储>卷*，然后选择卷和*Snapshot副本*。
3. 选择要还原的快照旁边的，然后选择**Restore**。

如果未发现系统攻击、则还原

1. 显示卷中的快照：

   选择*存储>卷*，然后选择卷和*Snapshot副本*。
2. 选择然后选择 `Anti_ransomware`快照。
3. 选择 * 还原 * 。
4. 返回到*Snapshot副本*菜单，然后选择要使用的快照。选择 * 还原 * 。

命令行界面

在系统受到攻击后恢复

要从ARP快照还原、请跳至步骤二。要从早期快照还原数据、必须解除对ARP快照的锁定。

> 只有在使用以下命令时、才需要在从早期快照还原之前释放反勒索软件SnapLock `volume snapshot restore`。如果使用FlexClone、单文件Snap Restore或其他方法还原数据、则无需执行此操作。

1. 将攻击标记为潜在的勒索软件攻击(`-false-positive false` ）并清除可疑文件(`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   使用以下参数之一来识别扩展：

   - `[-seq-no` *`integer`*`]` ： 可疑列表中文件的序列号。
   - `[-extension` *`text, … ]`* ： 文件扩展名
   - `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` ： 需要清除的文件范围的开始和结束时间，格式为“MM/DD/YYYY HH:MM:SS”。

2. 列出卷中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下示例显示了中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ------------ ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. 从快照还原卷的内容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

以下示例将还原的内容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

如果未发现系统攻击、则还原

1. 列出卷中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下示例显示了中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 从快照还原卷的内容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

以下示例将还原的内容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

有关的详细信息 `volume snapshot`，请参见"ONTAP 命令参考"。

相关信息

- "NetApp知识库： ONTAP中的勒索软件预防和恢复"
- "ONTAP 命令参考"

调整自动生成的 ARP 快照的设置

从Ransomware 11.1开始、您可以使用命令行界面来控制在发生可疑勒索软件攻击时自动生成的自动保护(Autonomous ONTAP 9 Protection、ARP)快照的保留设置。

开始之前

您只能修改"节点SVM"而不适用于其他类型的 SVM。

步骤

1. 显示所有当前ARP快照设置：

```
options -option-name arw*
```

2. 显示选定的当前ARP快照设置：

```
options -option-name <arw_setting_name>
```

3. 修改ARP快照设置：

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

您可以修改以下设置：

> 从ONTAP 9.17.1 开始，部分所述命令已弃用。ONTAPONTAP中引入的命令同时支持 NAS 和 SAN 环境。

正在设置 ...	Description	支持的版本
`arw.snap.max.count`	指定任意给定时间卷中可存在的 ARP 快照的最大数量。系统会删除较旧的副本，以确保 ARP 快照的总数不超过此指定限制。	ONTAP 9.11.1及更高版本
`arw.snap.create.interval.hours`	指定 ARP 快照之间的间隔（以小时为单位）。当怀疑存在基于数据熵的攻击且最近创建的 ARP 快照早于指定间隔时，将创建新的 ARP 快照。	ONTAP 9.11.1及更高版本
`arw.snap.normal.retain.interval.hours`	指定 ARP 快照的保留时长（以小时为单位）。当 ARP 快照达到保留阈值时，将被删除。	• ONTAP 9.11.1 升级至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已弃用
`arw.snap.max.retain.interval.days`	指定可以保留ARP快照的最长持续时间_in days_。如果卷上未报告攻击、则会删除早于此持续时间的任何ARP快照。 > 如果检测到中等威胁、则会忽略ARP快照的最大保留间隔。为响应威胁而创建的ARP快照将保留、直到您对威胁做出响应为止。将威胁标记为误报后、ONTAP将删除卷的ARP快照。	• ONTAP 9.11.1 升级至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已弃用

正在设置 ...	Description	支持的版本
`arw.snap.create.interval.hours.post.max.count`	当卷已包含最大数量的 ARP 快照时，指定 ARP 快照之间的间隔（以小时为单位）。达到最大数量时，将删除一个 ARP 快照，为新副本腾出空间。使用此选项可以降低新 ARP 快照的创建速度，以保留旧副本。如果卷已包含最大数量的 ARP 快照，则下次创建 ARP 快照时将使用此选项中指定的间隔，而不是 `arw.snap.create.interval.hours` 。	• ONTAP 9.11.1 至 9.16.1 • 在ONTAP 9.17.1 及更高版本中已弃用
`arw.snap.low.encryption.retain.duration.hours`	指定在加密活动较少期间创建的 ARP 快照的保留时间（以小时为单位）。	• ONTAP 9.17.1 及更高版本
`arw.snap.new.extns.interval.hours`	指定检测到新文件扩展名时创建 ARP 快照的间隔（以小时为单位）。检测到新文件扩展名时会创建一个新的 ARP 快照；上一个在检测到新文件扩展名时创建的快照早于此指定的间隔。在频繁创建新文件扩展名的工作负载上，此间隔有助于控制 ARP 快照的频率。此选项独立于 `arw.snap.create.interval.hours` ，指定基于数据熵的 ARP 快照的间隔。	• ONTAP 9.11.1 升级至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已弃用
`arw.snap.retain.hours.after.clear.suspect.false.alert`	指定在管理员将攻击事件标记为误报后，ARP 快照作为预防措施保留的时间间隔（以小时为单位）。在此预防性保留期到期后，可能会根据选项定义的标准保留期限删除快照 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更高版本
`arw.snap.retain.hours.after.clear.suspect.real.attack`	指定管理员将攻击事件标记为真实攻击后，ARP 快照作为预防措施保留的时间间隔（以小时为单位）。在此预防性保留期到期后，可能会根据选项定义的标准保留期限删除快照。 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更高版本
`arw.snap.surge.interval.days`	指定为响应IO激增而创建的ARP快照之间的间隔_天_。如果IO流量激增、而上次创建的ARP快照早于此指定间隔、则ONTAP会创建一个ARP快照激增副本。此选项还指定ARP激增快照的保留期限_in day_。	ONTAP 9.11.1及更高版本
`arw.high.encryption.alert.enabled`	启用高级别加密警报。当此选项设置为 `on` （默认），当ONTAP百分比超过 `arw.high.encryption.percentage.threshold` 。	ONTAP 9.17.1 及更高版本
`arw.high.encryption.percentage.threshold`	指定卷的最大加密百分比。如果加密百分比超过此阈值，则ONTAP会将加密百分比的增加视为攻击，并创建 ARP 快照。 `arw.high.encryption.alert.enabled`必须设置为 `on`以使此选项生效。	ONTAP 9.17.1 及更高版本

正在设置 ...	Description	支持的版本
`arw.snap.high.encryption.retain.duration.hours`	指定在高加密阈值事件期间创建的快照的保留持续时间间隔（以小时为单位）。	ONTAP 9.17.1 及更高版本

4. 如果您在 SAN 环境中使用 ARP，您还可以修改以下评估期设置：

正在设置 ...	Description	支持的版本
`arw.block_device.auto.learn.threshold.min_value`	指定块设备评估的自动学习阶段的最小加密阈值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.auto.learn.threshold.max_value`	指定块设备评估的自动学习阶段的最大加密阈值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_hours`	指定在设置加密阈值之前评估阶段必须运行的最小间隔（以小时为单位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.max_hours`	指定在设置加密阈值之前评估阶段必须运行的最大间隔（以小时为单位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	指定在设置加密阈值之前评估阶段必须提取的最小数据量（以 GB 为单位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.enabled`	指定是否在块设备上启用 ARP 评估阶段的警报。默认值为 `True`。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.threshold`	指定块设备上 ARP 评估阶段的阈值百分比。如果加密百分比超过此阈值，则会触发警报。	ONTAP 9.17.1 及更高版本

相关信息

- "威胁评估和ARP快照"
- "SAN熵评估期"

使用AI更新ONTAP自动防软件保护(ARP/AI)

为了及时防范最新的勒索软件威胁、ARP/AI提供了常规ONTAP版本周期之外的自动更新。

从ONTAP 9.16.1 开始，除系统和固件更新外，系统管理器软件下载中还提供 ARP/AI 安全更新。如果您

的ONTAP集群已注册"自动更新系统和固件"，当 ARP/AI 安全更新可用时，系统会自动通知您。您还可以更改您的更新偏好以便ONTAP自动安装安全更新。

如果需要手动更新ARP/AI，您可以从NetApp支持站点下载更新并使用System Manager进行安装。

关于此任务

您只能使用系统管理器更新 ARP/AI。

选择ARP/AI的更新首选项

在系统管理器中，安全文件的启用自动更新页面上的设置被设置为 `Show notifications`如果您已注册自动固件和系统更新，您可以更改更新设置以 `Automatically update`如果您希望ONTAP自动应用最新更新。如果您使用暗网或希望手动执行更新，您可以选择显示通知或自动关闭安全更新。

开始之前

对于自动安全更新，"应启用AutoSupport和AutoSupport OnDemand、并将传输协议设置为HTTPS"。

步骤

1. 在System Manager中、单击*集群>设置>软件更新*。
2. 在*软件更新*部分中，选择 →。
3. 从*软件更新*页面中，选择*所有其他更新*选项卡。
4. 选择*所有其他更新*选项卡，然后单击*更多*。
5. 选择*编辑自动更新设置*。
6. 从“自动更新设置”页面中，选择*安全文件*。
7. 指定要对安全文件执行的操作(ARP/AI更新)。

   您可以选择自动更新、显示通知或自动取消更新。

   > ⓘ 要使安全更新自动更新、应启用AutoSupport和AutoSupport OnDemand、并将传输协议设置为HTTPS。

8. 接受条款和条件并选择*保存*。

使用最新的安全软件包手动更新ARP/AI

根据您是否已向Active IQ Unified Manager注册、按照相应的过程进行操作。

> ⓘ 请确保仅安装比当前版本更新的ARP更新、以避免意外的ARP降级。

采用**ONTAP 9**的数字顾问**.161**及更高版本

1. 在System Manager中，转至*"DardManager*(仪表板*)"。

   在*Health*部分中，如果有任何建议的集群安全更新，则会显示一条消息。

2. 单击警报消息。

3. 在建议更新列表中的安全更新旁边，选择*Actions*。
4. 单击*Update*立即安装更新，或单击*Schedule *安排以后安装。

   如果已计划更新，您可以*编辑*或*取消*更新。

不带**ONTAP 9**的数字顾问**.16.1**及更高版本

1. 导航到"NetApp 支持站点"并登录。
2. 完成提示并下载要用于更新集群ARP/AI的安全软件包。
3. 将文件复制到网络上的HTTP或FTP服务器、或者复制到集群可使用ARP/AI访问的本地文件夹。
4. 在System Manager中、单击*集群>设置>软件更新*。
5. 在*软件更新*中，选择*所有其他更新*选项卡。
6. 在*手动更新*窗格中，单击*添加安全文件*并使用以下首选项之一添加文件：
   - 从服务器下载：输入安全文件包的URL。
   - 从本地客户端上传：导航到下载的TGZ文件。

   确保文件名以开头、并 `.tgz`作为文件扩展名 `ontap_security_file_arpai_`。
7. 单击*Add*以应用更新。

验证**ARP/AI**更新

要查看已取消或无法安装的自动更新的历史记录、请执行以下操作：

1. 在System Manager中、单击*集群>设置>软件更新*。
2. 在*软件更新*部分中，选择→。
3. 从“软件更新”页面中，选择“所有其他更新”选项卡，然后单击“更多*”。
4. 选择*查看所有自动更新*。

相关信息

- "了解ARP/AI"
- "通过电子邮件订阅软件更新"