自主勒索软件保护
ONTAP 9

NetApp
August 31, 2024

目录

自主勒索软件保护

自主勒索软件保护概述

从ONTAP 9.10.1开始、自动勒索软件保护(ARP)功能使用NAS (NFS和SMB)环境中的工作负载分析功能主动检测并警告可能指示勒索软件攻击的异常活动。

如果怀疑发生攻击、ARP除了从计划的Snapshot副本中提供现有保护之外、还会创建新的Snapshot副本。

许可证和支持

ARP需要许可证。ARP可用于 "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、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	反勒索软件
ONTAP 9.10.1	MT_EK_Mgmt (多租户密钥管理)

- 如果您要升级到ONTAP 9.11.1或更高版本、并且您的系统上已配置ARP、则无需购买新的反勒索软件许可证。对于新的ARP配置、需要新的许可证。
- 如果您要从ONTAP 9.11.1或更高版本还原到ONTAP 9.10.1、并且已使用防勒索软件许可证启用ARP、则会看到一条警告消息、可能需要重新配置ARP。 "了解还原ARP的相关信息"。

您可以使用System Manager或ONTAP命令行界面按卷配置ARP。

ONTAP 勒索软件保护策略

有效的勒索软件检测策略应包括多个保护层。

一个比喻是车辆的安全特性。您不需要依靠安全带等单一功能来在发生事故时为您提供全面保护。安全袋，防抱死制动器和前向碰撞警告都是额外的安全功能，可以带来更好的结果。应以相同方式查看勒索软件保护。

虽然ONTAP 包括FPolicy、Snapshot副本、SnapLock 和Active IQ 数字顾问等功能来帮助防止勒索软件、但以下信息重点介绍了具有机器学习功能的ARP机载功能。

要了解有关ONTAP的其他反勒索软件功能的更多信息，请参见"勒索软件和NetApp的保护产品组合"。

ARP检测到的内容

ARP旨在防止攻击者在支付赎金之前扣留数据的拒绝服务攻击。ARP提供基于以下各项的实时勒索软件检测：

- 将传入数据标识为加密或纯文本。
- 分析，用于检测
  - 平均值：对文件中数据的随机性的评估

- 文件扩展名类型：不符合正常扩展名类型的扩展名
- 文件**IOP**：使用数据加密时卷活动异常激增(从ONTAP 9.11.1开始)

在对少量文件进行加密后、ARP可以检测到大多数勒索软件攻击的蔓延、并自动采取措施保护数据、并提醒您可疑攻击正在发生。

> 任何勒索软件检测或预防系统都无法完全保证免遭勒索软件攻击的安全。虽然攻击可能无法检测到、但如果防病毒软件未能检测到入侵、ARP则会作为一个重要的额外防御层。

学习和主动模式

ARP有两种模式：

- 学习(或"演练"模式)
- **Active**(或"已启用"模式)

启用ARP后、它将在_leARnLearning mode_下 运行。在学习模式下、ONTAP系统会根据分析区域(熵、文件扩展名类型和文件IOPS)开发警报配置文件。在学习模式下运行ARP并有足够的时间来评估工作负载特征后、您可以切换到活动模式并开始保护数据。ARP切换到活动模式后、ONTAP会创建ARP Snapshot副本、以便在检测到威胁时保护数据。

建议您将ARP保留在学习模式30天。从ONTAP 9.13.1开始、ARP会自动确定最佳学习周期间隔并自动执行交换机操作、这可能会在30天之前发生。

在活动模式下、如果文件扩展名被标记为异常、则应评估警报。您可以对警报采取措施来保护您的数据、也可以将警报标记为误报。将警报标记为误报可更新警报配置文件。例如、如果警报由新文件扩展名触发、而您将警报标记为误报、则下次观察到该文件扩展名时、您不会收到警报。命令 `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。)

从ONTAP 9.11.1开始、您可以自定义ARP的检测参数。有关详细信息，请参见 管理ARP攻击检测参数。

威胁评估和**ARP Snapshot**副本

在主动模式下、ARP根据根据所学分析测量的传入数据评估威胁概率。当ARP检测到威胁时、将分配一个度量值：

- 低：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)。
- 中等：观察到多个文件具有相同的"从未见过"文件扩展名。
  - 在ONTAP 9.10.1中、升级到"中等"的阈值为100个或更多文件。从ONTAP 9.11.1开始、文件数量可进行编辑；其默认值为20。

在威胁较低的情况下、ONTAP会检测到一个非正常情况、并为此卷创建一个Snapshot副本、以创建最佳恢复点。ONTAP会在ARP Snapshot副本的名称前面附加 `Anti-ransomware-backup` 以使其易于识别、例如 `Anti_ransomware_backup.2022-12-20_1248`。

在ONTAP运行分析报告以确定此非正常情况是否与勒索软件配置文件匹配后、此威胁会升级为中等。系统会在System Manager的事件部分中记录并显示处于较低级别的威胁。当攻击概率为中等时、ONTAP 会生成EMS通知、提示您评估威胁。ONTAP不会发送有关低威胁的警报、但是、从ONTAP 9.14.1开始、您可以发送警报 修改警报设置。有关详细信息，请参见 应对异常活动。。

您可以在System Manager的事件部分中或使用查看有关威胁的信息，而不受威胁级别的限制 `security anti-ransomware volume show` 命令：

ARP Snapshot副本至少保留两天。从ONTAP 9.11.1开始、您可以修改保留设置。有关详细信息，请参见 修改Snapshot副本的选项。

如何在勒索软件攻击后在 **ONTAP** 中恢复数据

如果怀疑发生攻击，系统将在该时间点创建卷 Snapshot 副本并锁定该副本。如果稍后确认攻击、则可以使用ARP Snapshot副本还原卷。

无法正常删除已锁定的 Snapshot 副本。但是，如果您稍后决定将此攻击标记为误报，则锁定的副本将被删除。

了解受影响的文件和攻击时间后、可以有选择地从各种Snapshot副本恢复受影响的文件、而不是简单地将整个卷还原到其中一个Snapshot副本。

因此、ARP建立在经验证的ONTAP 数据保护和灾难恢复技术之上、可应对勒索软件攻击。有关恢复数据的详细信息，请参见以下主题。

- "从 Snapshot 副本恢复（ System Manager ）"
- "从 Snapshot 副本还原文件（命令行界面）"
- "智能勒索软件恢复"

自主勒索软件保护使用情形和注意事项

从ONTAP 9.10.1开始、可为NAS工作负载提供自主关系统软件保护(ARP)。在部署ARP之前、您应了解建议的用途和支持的配置以及对性能的影响。

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：

- NFS 存储上的数据库
- Windows 或 Linux 主目录

  由于用户可能会创建在学习期间未检测到扩展名的文件、因此在此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不适用于：

- 文件创建或删除频率较高的工作负载(几秒钟内即可创建数十万个文件；例如测试/开发工作负载)。
- ARP的威胁检测取决于其识别文件创建、重命名或删除活动异常激增的能力。如果应用程序本身是文件活动的源、则无法有效地将其与勒索软件活动区分开来。
- 应用程序或主机对数据进行加密的工作负载。
  ARP取决于将传入数据区分为已加密或未加密。如果应用程序本身正在对数据进行加密，则此功能的有效性将会降低。但是、该功能仍可根据文件活动(删除、覆盖或创建、或者使用新文件扩展名创建或重命名)和文件类型来工作。

支持的配置

从ONTAP 9.10.1开始、可对内部ONTAP系统中的NFS和SMB卷使用ARP。

以下ONTAP版本支持其他配置和卷类型：

	ONTAP 9.15.1.	**ONTAP 9.14.1**	**ONTAP 9.13.1**	**ONTAP 9.12.1**	**ONTAP 9.11.1**	**ONTAP 9.10.1**
使用异步SnapMirror保护的卷	✓	✓	✓	✓		
使用异步SnapMirror保护SVM (SVM灾难恢复)	✓	✓	✓	✓		
SVM 数据移动性 (`vserver migrate`)	✓	✓	✓	✓		
FlexGroup 卷	✓	✓	✓			
多管理员验证	✓	✓	✓			

SnapMirror和**ARP**互操作性

从ONTAP 9.12.1开始、异步SnapMirror目标卷支持ARP。SnapMirror同步**不支持ARP。

如果SnapMirror源卷已启用ARP、则SnapMirror目标卷会自动获取源卷的ARP配置状态(学习、已启用等)、ARP培训数据以及ARP创建的Snapshot。无需显式启用。

虽然目标卷包含只读(Read Only、RO) Snapshot副本、但不会对其数据执行ARP处理。但是、当SnapMirror目标卷转换为读写(rw)时、将自动在RW转换的目标卷上启用ARP。除了已记录在源卷上的内容之外、目标卷不需要任何其他学习操作步骤。

在ONTAP 9.10.1和9.11.1中、SnapMirror不会将ARP配置状态、培训数据和Snapshot副本从源卷传输到目标卷。因此、在将SnapMirror目标卷转换为RW后、必须在转换后的学习模式下明确启用目标卷上的ARP。

ARP和虚拟机

虚拟机(VM)支持ARP。对于VM内部和外部的更改、ARP检测的行为有所不同。建议不要对虚拟机中具有大量熵文件的工作负载使用ARP。

虚拟机外部的更改

如果新扩展进入加密卷、或者文件扩展名发生更改、ARP可以检测VM外部NFS卷上的文件扩展名更改。可检测到的文件扩展名更改包括：

- vmx
- vmxf
- vmdk
- -fl.vmdk
- .NVRAM
- .vmm
- vms
- vmsn
- .vswp
- vmss
- .log
- -\#.log

虚拟机内部的更改

如果勒索软件攻击以虚拟机为目标、而虚拟机内部的文件在未在虚拟机外部进行更改的情况下发生更改、则在虚拟机的默认熵较低(例如.txt、.DOCX或.mp4文件)时、ARP会检测到威胁。在此情形下、尽管ARP会创建一个保护性Snapshot、但它不会生成威胁警报、因为虚拟机外部的文件扩展名未被篡改。

默认情况下、如果文件的熵较高(例如.gzip或受密码保护的文件)、则ARP的检测功能会受到限制。在这种情况下、ARP仍可主动创建快照；但是、如果文件扩展名未被外部篡改、则不会触发任何警报。

不支持的配置

以下系统配置不支持ARP：

- ONTAP S3 环境
- SAN 环境

ARP不支持以下卷配置：

- FlexGroup卷(在ONTAP 9.10.1到9.12.1中。从ONTAP 9.131开始、支持FlexGroup卷)
- FlexCache卷(原始FlexVol卷支持ARP、但缓存卷不支持ARP)
- 使卷脱机
- SAN-only volumes
- SnapLock 卷
- SnapMirror 同步
- 异步SnapMirror (仅在ONTAP 9.10.1和9.11.1中不受支持。从ONTAP 9.12.1开始、支持异步SnapMirror。有关详细信息，请参见 [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

根据吞吐量和峰值IOPS衡量、ARP对系统性能的影响最小。ARP功能的影响取决于特定的卷工作负载。对于常见工作负载、建议遵循以下配置限制：

工作负载特征	每个节点的建议卷限制	超出每节点卷限制时性能下降传递：[*]
读取密集型数据或数据可以压缩。	150	最大IOPS的4%
写入密集型、无法压缩数据。	60	最大IOPS的10%

密码：[*]无论添加的卷数是否超过建议的限制、系统性能均不会超过这些百分比。

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、在每个卷上运行分析的频率会降低。

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。了解操作方法 "为受ARP保护的卷启用MAV"。

您需要为MAV组定义管理员并为创建MAV规则 `security anti-ransomware volume disable`，`security anti-ransomware volume pause`，和 `security anti-ransomware volume attack clear-suspect` 要保护的ARP命令。MAV组中的每个管理员都必须批准每个新规则请求和 "再次添加MAV规则" 在MAV设置中。

从ONTAP 9.14.1开始、ARP提供有关创建ARP快照和观察新文件扩展名的警报。默认情况下、这些事件的警报处于禁用状态。可以在卷或SVM级别设置警报。您可以使用在SVM级别创建MAV规则 `security anti-ransomware vserver event-log modify` 或在卷级别使用 `security anti-ransomware volume event-log modify`。

后续步骤

- "启用自主勒索软件保护"
- "为受ARP保护的卷启用MAV"

启用自主勒索软件保护

从ONTAP 9.10.1开始、可以在新卷或现有卷上启用自动勒索软件保护(ARP)。您首先可以在学习模式下启用ARP、在此模式下、系统会分析工作负载以确定正常行为的特征。您可以在现有卷上启用ARP、也可以从头创建新卷并启用ARP。

关于此任务

您应始终在初始学习(或演练)模式下启用ARP。在活动模式下开始可能会导致误报报告过多。

建议您让ARP在学习模式下运行至少30天。从ONTAP 9.13.1开始、ARP会自动确定最佳学习周期间隔并自动执行交换机操作、这可能会在30天之前发生。有关详细信息，请参见 "学习和主动模式"。

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。

开始之前

- 您必须为NFS或SMB (或这两者)启用Storage VM (SVM)。
- 。 正确的许可证 必须为您的ONTAP 版本安装。
- 您必须已配置NAS工作负载和客户端。
- 要设置ARP的卷需要受到保护、并且必须具有活动卷 "接合路径"。
- 卷的容量必须小于100%。
- 建议您将EMS系统配置为发送电子邮件通知、其中包括ARP活动通知。有关详细信息，请参见 "配置 EMS 事件以发送电子邮件通知"。
- 从ONTAP 9.13.1开始、建议您启用多管理员验证(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"。

启用ARP

您可以使用System Manager或ONTAP命令行界面启用ARP。

System Manager

步骤

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，在*Anti-勒索 软件*框中选择*Status*，在学习模式下从Disabled切换为Enabled。
3. 学习期结束后、将ARP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执行交换机操作。您可以 "在关联的Storage VM上禁用此设置" 如果您要手动将学习模式控制为激活模式开关。

   a. 选择*存储>卷*，然后选择已准备好进入活动模式的卷。
   b. 在*卷*概述的*安全性*选项卡中，在防勒索软件框中选择*切换到活动模式。
4. 您可以在*Anti-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

如果要在现有卷上启用ARP、而要在新卷上启用ARP、则使用命令行界面启用ARP的过程会有所不同。

在现有卷上启用**ARP**

1. 修改现有卷以在学习模式下启用勒索软件保护：

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

   如果您运行的是ONTAP 9.13.1.或更高版本、则会启用自适应学习、以便自动更改为活动状态。如果您不希望自动启用此行为、请在所有关联卷上的SVM级别更改此设置：

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

2. 学习期结束后、如果尚未自动修改受保护卷以切换到活动模式、请将其修改为：

   ```
   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
   active
   ```

3. 验证卷的ARP状态。

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

在新卷上启用**ARP**

1. 在配置数据之前、创建一个启用了反勒索软件保护的新卷。

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   ```

```
nn -anti-ransomware-state dry-run -junction-path /path_name
```

如果您运行的是ONTAP 9.13.1.或更高版本、则会启用自适应学习、以便自动更改为活动状态。如果您不希望自动启用此行为、请在所有关联卷上的SVM级别更改此设置：

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

2. 学习期结束后、如果尚未自动修改受保护卷以切换到活动模式、请将其修改为：

```
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
active
```

3. 验证卷的ARP状态。

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

默认情况下、在新卷中启用自主勒索软件保护

从ONTAP 9.10.1开始、您可以配置Storage VM (SVM)、以便在学习模式下为自动勒索软件保护(ARP)默认启用新卷。

关于此任务

默认情况下、系统会在禁用ARP的情况下创建新卷。您可以在System Manager中使用命令行界面修改此设置。默认情况下、启用的卷会在学习(或演练)模式下设置为ARP。

只有在更改设置后、才会对在SVM中创建的卷启用ARP。现有卷不会启用ARP。了解操作方法 "在现有卷中启用ARP"。

从ONTAP 9.13.1开始、ARP分析中添加了自适应学习功能、并且会自动从学习模式切换到活动模式。有关详细信息，请参见 "学习和主动模式"。

开始之前

- 。 正确的许可证 必须为您的ONTAP 版本安装。
- 卷的容量必须小于100%。
- 接合路径必须处于活动状态。
- 从ONTAP 9.13.1开始、建议您启用多管理员验证(MAV)、以便反勒索软件操作需要两个或更多经过身份验证的用户管理员。 "了解更多信息。"。

将ARP从学习模式切换到活动模式

从ONTAP 9.131开始、ARP分析增加了自适应学习功能。自动完成从学习模式切换到活动模式的操作。ARP自动决定从学习模式切换到活动模式取决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
```

学习30天后、卷会自动切换到活动模式、即使其中一个或多个条件不满足也是如此。也就是说、如果启用了自动切换、则卷将在最长30天后切换到活动模式。30天的最大值是固定的、不可修改。

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"。

步骤

默认情况下、您可以使用System Manager或ONTAP命令行界面启用ARP。

System Manager

1. 选择*存储> Storage VM*、然后选择包含要使用ARP保护的卷的Storage VM。
2. 导航到*Settings*选项卡。在*安全性*下，找到反勒索软件磁贴，然后选择
3. 选中此框可为NAS卷启用ARP。选中附加框可在Storage VM中所有符合条件的NAS卷上启用ARP。

> 如果您已升级到ONTAP 9.13.1，*在充分学习后自动从学习模式切换到活动模式*设置将自动启用。这样、ARP就可以确定最佳学习周期间隔、并自动切换到活动模式。如果要手动过渡到活动模式、请关闭设置。

命令行界面

1. 修改现有SVM、以便在新卷中默认启用ARP：
   ```
   vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
   ```

   在CLI中、您还可以创建一个新的SVM、并为新卷默认启用ARP。
   ```
   vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
   ```

   如果您升级到ONTAP 9.13.1或更高版本、则会启用自适应学习、以便自动更改为活动状态。如果不希望自动启用此行为、请使用以下命令：

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

暂停自主勒索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 9.13.1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。 "了解更多信息。"。

关于此任务

在ARP暂停期间、不会记录任何事件、也不会对新写入执行任何操作。但是，分析操作仍会在后台对早期日志执行。

> 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. 在卷概述的安全性选项卡中，选择*反勒索软件*框中的*暂停反勒索软件*。

> 从ONTAP 9.13.1开始，如果使用MAV保护ARP设置，暂停操作将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审批组关联、否则操作将失败。

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
   ```

3. *如果您使用MAV (从ONTAP 9.13.1开始可用于ARP)来保护ARP设置，*暂停操作将提示您获得一个或多个额外管理员的批准。必须从与MAV批准组关联的所有管理员处获得批准、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]
```

管理自主防系统攻击检测参数

从ONTAP 9.11.1开始、您可以修改已启用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

当自动防兰软件保护(ARP)处于学习模式时、它会为卷行为制定基线值。它们分别是熵、文件扩展名以及从ONTAP 9.11.1开始的IOPS。这些基线用于评估勒索软件威胁。有关这些条件的详细信息、请参见 ARP检测到的内容。

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、则ARP会将此类文件归类为所观察到的熵的威胁_thw考虑_。(24小时和20个文件值为默认值、可以进行修改。)

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]

某些卷和工作负载需要使用不同的检测参数。例如、启用了ARP的卷可能会托管多种类型的文件扩展名、在这种情况下、您可能需要将前所未见文件扩展名的阈值计数修改为大于默认值20的数字、或者禁用基于前所未见文件扩展名的警告。从ONTAP 9.11.1开始、您可以修改攻击检测参数、使其更适合您的特定工作负载。

修改攻击检测参数

根据启用了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
              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 : 20
         Never Seen before File Extensions Duration in Hour : 24
   ```

2. 显示的所有字段均可使用布尔值或整数值进行可订。要修改字段、请使用 `security anti-ransomware volume attack-detection-parameters modify` 命令：

   有关完整的参数列表、请参见 "ONTAP 命令参考"。

报告已知电涌

即使在活动模式下、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(一次性电涌或新正常值的电涌)，您应该将其报告为安全。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。

报告一次性电涌

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
   ```

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
   ```

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。有关详细信息，请参见 使用ARP保护的卷进行多管理员验证。

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. 选择安全性选项卡，然后选择事件安全性设置。
3. 要接收有关检测到新文件扩展名和已创建的异常快照的警报，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 **Storage VM**，然后选择要为其启用设置的SVM。
2. 在“安全”标题下，找到“反勒索软件卡”。选择，然后选择 ⋮ 编辑**Ranson**要 索事件严重性。
3. 要接收有关检测到新文件扩展名和已创建的异常快照的警报，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 -is
-enabled-on-new-file-extension-seen true
```

- 要为创建ARP Snapshot设置警报、请执行以下操作：

```
security anti-ransomware volume event-log modify -vserver svm_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 Snapshot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：

更多信息

- "了解自动防兰索防攻击和自动防兰索防快照"

应对异常活动。

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。

关于此任务

如果ARP检测到高数据容量、具有数据加密的异常卷活动以及异常文件扩展名的任意组合、则会显示可疑文件的列表。

发出警告后、通过以下两种方式之一指定文件活动来进行响应：

- 误报

  您的工作负载应具有已标识的文件类型，可以忽略此文件类型。

- 潜在的勒索软件攻击

  确定的文件类型在工作负载中是意外的，应视为潜在攻击。

在这两种情况下、在更新和清除通知后、正常监控将恢复。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必须在活动模式下运行。

步骤

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

System Manager

1. 当您收到"异常活动"通知时、请单击链接。或者，导航到*卷*概述的*安全性*选项卡。

   警告显示在*Events*菜单的*Overview*窗格中。

2. 显示 " 检测到异常卷活动 " 消息时，请查看可疑文件。

   在*安全性*选项卡中，选择*查看可疑文件类型*。

3. 在 * 可疑文件类型 * 对话框中，检查每个文件类型并将其标记为 " 误报 " 或 " 潜在勒索软件攻击 " 。

如果选择此值 …	执行此操作…
误报	选择*更新*和*清除可疑文件类型*以记录您的决定并恢复正常ARP监控。 从ONTAP 9.13.1开始、如果使用MAV保护ARP设置、则清除可疑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审批组关联、否则操作将失败。
潜在勒索软件攻击	应对攻击并还原受保护的数据。然后选择*更新*和*清除可疑文件类型*以记录您的决定并恢复正常ARP监控。 如果还原了整个卷、则不需要清除任何可疑文件类型。

命令行界面

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: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   您还可以检查 EMS 消息：

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

2. 生成攻击报告并记下输出位置：

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   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：

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
```

4. 根据对文件扩展名的评估，执行以下操作之一：

   - 误报

     输入以下命令记录您的决定、将新扩展名添加到允许的扩展名列表中、并恢复正常的反勒索软件监控：
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     使用以下参数之一标识扩展：
     `[-seq-no integer]` 可疑列表中的文件序列号。
     `[-extension text, … ]` 文件扩展名
     `[-start-time date_time -end-time date_time]` 要清除的文件范围的开始时间和结束时间、格式为"MM/DD/YYYY HH：MM：SS"。

   - 潜在的勒索软件攻击

     应对攻击、然后 "从ARP创建的备份快照恢复数据"。恢复数据后、输入以下命令记录您的决定并恢复正常ARP监控：

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

     使用以下参数之一标识扩展：
     `[-seq-no integer]` 可疑列表中的文件序列号
     `[-extension text, … ]` 文件扩展名
     `[-start-time date_time -end-time date_time]` 要清除的文件范围的开始时间和结束时间、格式为"MM/DD/YYYY HH：MM：SS"。

   如果还原了整个卷、则不需要清除任何可疑文件类型。系统将删除ARP创建的备份快照、并清除攻击报告。

5. 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。

6. 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]
```

更多信息

- "知识库文章：了解自动防系统攻击和自动防系统攻击快照"。

在勒索软件攻击后还原数据

自动防兰森(ARP)会创建名为的Snapshot副本 `Anti_ransomware_backup` 检测到潜在的勒索软件威胁时。您可以使用这些ARP Snapshot副本之一或卷的另一个Snapshot副本还原数据。

关于此任务

如果卷具有 SnapMirror 关系，请在从 Snapshot 副本还原后立即手动复制卷的所有镜像副本。否则，可能会导致镜像副本不可用，必须删除并重新创建这些副本。

从以外的Snapshot还原 `Anti_ransomware_backup` Snapshot在确定系统攻击后、必须先释放ARP Snapshot。

如果未报告系统攻击、则必须先从还原 `Anti_ransomware_backup` 然后、Snapshot副本会从您选择的Snapshot副本完成卷的后续还原。

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Snapshot副本还原、必须先释放ARP Snapshot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. 将这些文件标记为"Falseal"。
   d. 选择*更新*和*清除可疑文件类型*
2. 显示卷中的Snapshot副本：

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

如果未发现系统攻击、则还原

1. 显示卷中的Snapshot副本：

   选择*存储>卷*，然后选择卷和*Snapshot副本*。
2. 选择 它们并选择 `Anti_ransomware_backup` Snapshot。
3. 选择 * 还原 * 。
4. 返回到*Snapshot副本*菜单，然后选择要使用的Snapshot副本。选择 * 还原 * 。

命令行界面

在系统受到攻击后恢复

1. 要从ARP Snapshot副本还原、请跳至步骤二。要从早期的Snapshot副本还原数据、您必须解除对ARP Snapshot的锁定。

   只有在使用时、才需要在从早期Snapshot副本还原之前释放反勒索软件SnapLock `volume snap restore` 命令。 如果使用Flex Clone、Single File Snap Restore或其他方法还原数据、则无需执行此操作。

   将攻击标记为"误报"和"明确怀疑"：
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   使用以下参数之一标识扩展：
   `[-seq-no` *`integer`*`]` 可疑列表中的文件序列号。
   `[-extension` *`text`*`, … ]` 文件扩展名
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` 要清除的文件范围的开始时间和结束时间、格式为"MM/DD/YYYY HH：MM：SS"。
2. 列出卷中的 Snapshot 副本：

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

以下示例显示了中的Snapshot副本 `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 Snapshot 副本还原卷的内容：

```
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 Snapshot 副本：

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

以下示例显示了中的Snapshot副本 `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 Snapshot 副本还原卷的内容：

```
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
```

3. 重复步骤1和2、使用所需的Snapshot副本还原卷。

更多信息

- "知识库文章：ONTAP中的勒索软件预防和恢复"

修改自动Snapshot副本的选项

从ONTAP 9.11.1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勒索软件保护(Autonomous Ransomware Protection、ARP) Snapshot副本的保留设置。

开始之前

您只能修改节点SVM上的ARP Snapshot选项。

步骤

1. 要显示所有当前ARP Snapshot副本设置、请输入：
   `vserver options -vserver` *`svm_name`* `arw*`

。 `vserver options` command是一个隐藏命令。要查看手册页、请输入 `man vserver options` 在ONTAP 命令行界面上。

2. 要显示选定的当前ARP Snapshot副本设置、请输入：
`vserver options -vserver svm_name -option-name arw_setting_name`
3. 要修改ARP Snapshot副本设置、请输入：
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

以下设置可修改：

ARW设置	Description
`arw.snap.max.count`	指定在任何给定时间卷中可以存在的最大ARP Snapshot副本数。系统会删除较早的副本、以确保ARP Snapshot副本总数不超过此指定限制。 。 `-option-value` 参数接受3到8之间的整数(含3到8)。默认值为6。
`arw.snap.create.interval.hours`	指定两个ARP Snapshot副本之间的间隔_in Hours_。如果怀疑发生了基于数据熵的攻击、并且最近创建的ARP Snapshot副本早于指定的时间间隔、则会创建一个新的ARP Snapshot副本。 。 `-option-value` 参数接受1到48之间的整数(包括1和48)。默认值为4。
`arw.snap.normal.retain.interval.hours`	指定保留ARP Snapshot副本的持续时间_以小时为单位_。当ARP Snapshot副本达到保留阈值时、删除之前创建的任何其他ARP Snapshot副本。保留阈值之前的ARP Snapshot副本不能超过一个。 。 `-option-value` 参数接受4到96之间的整数(含4和96)。默认值为48。
`arw.snap.max.retain.interval.days`	指定可以保留ARP Snapshot副本的最长持续时间(以天为单位)。如果卷上未报告攻击、则会删除早于此持续时间的任何ARP Snapshot副本。 如果检测到中等威胁、则会忽略ARP Snapshot副本的最大保留间隔。为响应威胁而创建的ARP Snapshot副本将保留、直到您对威胁做出响应为止。将威胁标记为误报删除卷上的ARP Snapshot副本。 。 `-option-value` 参数接受1到365之间的整数(包括1和365)。默认值为5。
`arw.snap.create.interval.hours.post.max.count`	指定卷已包含最大ARP Snapshot副本数时两个ARP Snapshot副本之间的间隔_in Hours_。达到最大数量后、将删除ARP Snapshot副本、以便为新副本腾出空间。可以使用此选项降低新的ARP Snapshot副本创建速度、以保留旧副本。如果卷中的ARP Snapshot副本数已达到上限、则下次创建ARP Snapshot副本时将使用此选项中指定的间隔、而不是 `arw.snap.create.interval.hours`。 。 `-option-value` 参数接受4到48之间的整数(含4和48)。默认值为8。

ARW设置	Description
`arw.surge.snap.interval.days`	指定为响应IO激增而创建的ARP Snapshot副本之间的间隔_天_。如果IO流量激增、而上次创建的ARP Snapshot副本早于此指定间隔、则ONTAP会创建一个ARP Snapshot激增副本。此选项还会为ARP激增的Snapshot副本指定保留期限_in day_。 。 `-option-value` 参数接受1到365之间的整数(包括1和365)。默认值为5。
`arw.snap.new.extns.interval.hours`	此选项用于指定检测到新文件扩展名时创建ARP Snapshot副本的间隔_in Hours_。创建新的ARP Snapshot副本的时间系统会观察到新的文件扩展名；在观察到新文件扩展名后创建的上一个Snapshot早于此指定间隔。对于频繁创建新文件扩展名的工作负载、此间隔有助于控制ARP Snapshot副本的频率。此选项独立于而存在 `arw.snap.create.interval.hours`，用于指定基于数据熵的ARP Snapshot副本的间隔。 。 `-option-value` 参数接受24到8760之间的整数。默认值为48。

版权信息

商标信息