防范勒索软件攻击
ASA r2

NetApp
February 11, 2026

目录

防范勒索软件攻击

创建防篡改快照，以防止对ASA r2 存储系统的勒索软件攻击

为了增强对勒索软件攻击的防护、请将快照复制到远程集群、然后锁定目标快照以防止其篡改。锁定的快照不会被意外或恶意删除。如果某个存储单元受到勒索软件攻击的威胁、您可以使用锁定的快照来恢复数据。

初始化SnapLock Compliance时钟

在创建防篡改快照之前、您必须初始化本地和目标集群上的SnapLock Compliance时钟。

步骤

1. 选择 * 集群 > 概述 * 。
2. 在*N节点*部分中，选择*初 始化SnapLock Compliance Clock*。
3. 选择*初始化*。
4. 验证Compliance时钟是否已初始化。
   a. 选择 * 集群 > 概述 * 。
   b. 在*节点*部分中，选择；然后选择* SnapLock Compliance Clock*。

下一步是什么?

在本地集群和目标集群上初始化SnapLock Compliance时钟后，即可开始"使用锁定的快照创建复制关系"。

在ASA r2 存储系统上利用 AI 实现自主勒索软件防护

从ONTAP 9.17.1 开始，您可以使用人工智能自主勒索软件防护 (ARP/AI) 来保护ASA r2 系统上的数据。ARP/AI 可以快速检测潜在的勒索软件威胁，自动创建 ARP 快照来保护您的数据，并在系统管理器中显示警告消息，提醒您注意可疑活动。

ARP 通过采用反勒索软件分析的机器学习模型来提高网络弹性，该模型可检测 SAN 环境下不断变化的勒索软件形式，准确率高达 98%。ARP 的机器学习模型在模拟勒索软件攻击之前和之后都在大型文件数据集上进行了预训练。这种资源密集型训练是在 ONTAP 外部完成的，由此训练产生的预训练模型包含在 ONTAP 的盒内。此模型不可访问或修改。ARP/AI 在启用后立即激活；没有"学习期"。

> 没有勒索软件检测或防御系统可以完全保证免受勒索软件攻击的安全。虽然攻击可能未被检测到，但如果防病毒软件未能检测到入侵，ARP/AI 将充当重要的额外防御层。

关于此任务

- ARP/AI 支持包含在"ONTAP One 许可证" 。
- 受 SnapMirror 活动同步、SnapMirror 同步或 SnapLock 保护的存储单元不支持 ARP/AI。
- 从 ONTAP 9.18.1 开始，在升级到 ONTAP 9.18.1 或初始化新的 ONTAP 9.18.1 ASA r2 集群 12 小时后，默认在所有新创建的存储单元上启用 ARP/AI。

- 启用 ARP/AI 后，您应该"为您的安全文件启用自动更新"自动接收新的安全更新。

在集群中的所有存储单元上启用 ARP/AI

如果您正在运行 ONTAP 9.17.1，则可以默认在集群中创建的所有存储单元上启用 ARP/AI。

在 ONTAP 9.18.1 及更高版本中，默认情况下在所有新存储单元上启用 ARP/AI。如果您在 ONTAP 9.17.1 中创建的存储单元未启用 ARP/AI，则可以手动启用它。

步骤

1. 在System Manager中、选择*集群>设置*。
2. 在*反勒索软件*旁边，选择 ⋮，然后选择*在所有现有存储单元上启用*。
3. 选择*启用*。

在存储虚拟机中的所有存储单元上启用 ARP/AI

如果您正在运行 ONTAP 9.17.1，则可以在默认情况下在存储虚拟机 (VM) 中创建的所有存储单元上启用 ARP/AI。这意味着在存储虚拟机中创建的任何新存储单元都将自动启用 ARP/AI。您还可以将 ARP/AI 应用于存储虚拟机中的现有存储单元。

在 ONTAP 9.18.1 及更高版本中，默认情况下在所有新存储单元上启用 ARP/AI。如果您在 ONTAP 9.17.1 中创建的存储单元未启用 ARP/AI，则可以手动启用它。

步骤

1. 在系统管理器中，选择“集群”>“存储虚拟机”。
2. 选择要启用 ARP/AI 的存储虚拟机。
3. 在“安全”部分的“反勒索软件”旁边，选择 ⋮ ；然后选择*编辑反勒索软件设置*。
4. 选择*启用反勒索软件*。

   这将默认在所选存储虚拟机上创建的所有未来存储单元上启用 ARP/AI。

5. 要将 ARP 应用于所选存储虚拟机上的现有存储单元，请选择*将此更改应用于此存储虚拟机上所有适用的现有存储单元*。
6. 选择 * 保存 * 。

结果

默认情况下，您在存储 VM 上创建的所有新存储单元都受到保护，免受勒索软件攻击，可疑活动会在系统管理器中报告给您。

在存储虚拟机中的特定存储单元上启用 ARP/AI

如果正在运行 ONTAP 9.17.1，并且不希望在存储虚拟机中的所有存储单元上启用 ARP/AI，则可以选择要启用的特定单元。

在 ONTAP 9.18.1 及更高版本中，默认情况下在所有新存储单元上启用 ARP/AI。如果您在 ONTAP 9.17.1 中创建的存储单元未启用 ARP/AI，则可以手动启用它。

步骤

1. 在System Manager中，选择*Storage*。
2. 选择要启用 ARP/AI 的存储单元。
3. 选择 ⋮ ；然后选择*启用反勒索软件*。
4. 选择*启用*。

结果

您选择的存储单元受到保护，免受勒索软件攻击，并且可疑活动会在系统管理器中向您报告。

在您的 ASA r2 存储系统上禁用默认自主勒索软件保护

当您初始化新的 ONTAP 9.18.1 ASA r2 群集或将您的群集升级到 ONTAP 9.18.1 时，ARP/AI 在 12 小时宽限期后默认在所有新存储单元上自动启用。如果您在宽限期内未禁用 ARP/AI，则在宽限期结束时将为新存储单元启用群集范围的 ARP/AI。

在 ONTAP 9.17.1 中创建的存储单元必须"手动启用"用于 ARP/AI。

步骤

您可以在最初的 12 小时宽限期内或之后禁用默认启用。

System Manager

1. 选择*集群>设置*。
2. 禁用 ARP：
   - 要在 12 小时宽限期内禁用：
     i. 在*反勒索软件*下，选择*不启用*，然后选择*禁用*。
   - 若要在 12 小时宽限期后禁用：
     i. 在*反勒索软件*下，选择 ✎ 并取消选择*为新存储单元启用*。
     ii. 选择 **Save**

命令行界面

1. 检查默认启用状态：

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

2. 禁用现有卷和新卷的默认启用：

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

修改ASA r2 存储系统上的 ARP/AI 快照保留期

如果人工智能自主勒索软件防护 (ARP/AI) 检测到您的一个或多个ASA r2 系统存储单元出现异常活动，它会自动创建 ARP 快照来保护存储单元的数据。根据您的存储容量和数据的业务需求，您可能需要增加或减少默认 ARP 快照保留期。例如，您可能希望增加业务关键型应用程序的保留期，以便在需要时获得更长的数据恢复保留期；或者，您可能希望减少非关键型应用程序的保留期以节省存储空间。

ARP 快照的默认保留期取决于您针对异常活动采取的措施。

如果您采取此行动...	**ARP** 快照默认保留...
标记为误报	12 小时
标记为潜在勒索软件攻击	7天
不立即采取行动	10天

您可以使用ONTAP命令行界面 (CLI) 修改默认保留期。请参阅 "修改ONTAP自动快照的选项"了解更改默认保留期的步骤。

使用ASA r2 存储系统上的 AI 警报来响应自主勒索软件防护

如果人工智能自主勒索软件防护 (ARP/AI) 检测到您的一个或多个ASA r2 系统存储单元存在异常活动，系统管理器仪表板上会生成警告。您应该查看警告，验证活动，并在必要时采取措施阻止任何对您数据的潜在威胁。

如果显示 ARP/AI 警告消息，则在采取措施之前，您应该使用适当的应用程序完整性检查器来验证存储单元上数据的完整性。验证存储单元的数据完整性有助于您确定该活动是否可接受，或者是否是潜在的勒索软件攻击。

如果出现异常活动...	操作
可接受	将该活动标记为误报。
潜在的勒索软件攻击	将该活动标记为潜在的勒索软件攻击。
不确定	请勿立即采取措施。请监控存储单元最多 7 天。如果存储单元继续正常运行，则将该活动标记为误报。如果存储单元继续表现出异常活动，则将该活动标记为潜在的勒索软件攻击。

步骤

1. 在 System Manager 中，选择 * 信息板 * 。

   如果 ARP 在一个或多个存储单元上检测到异常活动，则会在 警告 下显示一条消息。

2. 选择警告消息。
3. 在“事件概览”下，选择指示具有异常活动的存储单元数量的“警告”消息。
4. 在*具有异常活动的存储单元*下，选择存储单元。
5. 选择*安全*。

如果存储单元上存在异常活动，则会在“反勒索软件”下显示一条消息。

6. 选择*选择一个操作*。
7. 选择*标记为误报*或选择*标记为潜在勒索软件攻击*。

下一步是什么？

如果您知道存储单元活动出现浪涌，无论是一次性浪涌还是具有新常态特征的浪涌，您都应将其报告为安全。手动将这些浪涌报告为安全有助于提高 ARP 威胁评估的准确性。了解如何"报告已知的 ARP/AI 浪涌"。

在ASA r2 存储系统上使用 AI 暂停或恢复自主勒索软件防护

从ONTAP 9.17.1 开始，您可以使用人工智能自主勒索软件防护 (ARP/AI) 来保护ASA r2 系统上的数据。如果您正在计划异常工作负载事件，可以暂时暂停 ARP/AI 分析，以防止误报勒索软件攻击。工作负载事件完成后，您可以恢复 ARP/AI 分析。

暂停ARP/AI

在开始异常工作负载事件之前，您可能需要暂时暂停 ARP/AI 分析，以防止对勒索软件攻击的误报检测。

步骤

1. 在System Manager中，选择*Storage*。
2. 选择要暂停 ARP/AI 的存储单元。
3. 选择*暂停反勒索软件*。

结果

所选存储单元的 ARP/AI 分析已暂停，并且在您恢复 ARP/AI 之前，系统管理器不会向您报告任何可疑活动。

恢复ARP/AI

如果您在异常工作负载期间暂停 ARP/AI，则在工作负载完成后，您应该恢复它以保护您的数据免受勒索软件攻击。

步骤

1. 在System Manager中，选择*Storage*。
2. 选择要恢复 ARP/AI 的存储单元。
3. 选择*恢复反勒索软件*。

结果

对潜在勒索软件攻击的分析已恢复，可疑活动将在系统管理器中向您报告。