安全性和数据加密

ONTAP 9

NetApp
April 24, 2024

目录

安全性和数据加密

System Manager 安全管理概述

从 ONTAP 9.7 开始，您可以使用 System Manager 管理集群安全性。

借助 System Manager ，您可以使用 ONTAP 标准方法来保护客户端和管理员对存储的访问，并防止病毒的侵害。高级技术可用于对空闲数据进行加密以及对 WORM 存储进行加密。

如果您使用的是经典 System Manager （仅适用于 ONTAP 9.7 及更早版本），请参见 "System Manager 经典版（ ONTAP 9.0 到 9.7 ）"

病毒扫描

您可以在存储系统上使用集成的防病毒功能，防止数据受到病毒或其他恶意代码的侵害。称为 *Vscan* 的 ONTAP 病毒扫描将同类最佳的第三方防病毒软件与 ONTAP 功能相结合，让您可以灵活地控制扫描哪些文件以及何时扫描。

加密

ONTAP 提供了基于软件和基于硬件的加密技术，可确保在存储介质被重新利用，退回，放置在不当位置或被盗时无法读取空闲数据。

WORM 存储

WORM 是一种高性能合规解决方案，适用于使用 _write once， _read many （ SnapLock ） _ 存储以未经修改的形式保留关键文件以满足监管要求的组织。

防范勒索软件

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 "TR-4572：《 NetApp 解决方案 for 勒索软件》。"

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提供基于以下方面的反勒索软件检测：

- 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 9.14.1	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	✓	✓	✓		

	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仍可创建主动快照、但如果文件扩展名未被外部篡改、则不会触发警报。

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` 参数。

   ```
   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 ... ⋮ 然后编辑**Ranson**要 程序事件严重性。
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，您可以通过以下两种方式之一来标记文件活动：

- 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，请单击链接或导航到*Volumes*概述的*Security*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` 运营需要额外的审批、每个MAV组审批人执行以下操作：

   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 … ⋮ 在要还原的Snapshot副本旁边，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 … ⋮ 他们选择 `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。
* arw.snap.create.interval.hours*	指定两个ARP Snapshot副本之间的间隔_in Hours_。如果怀疑发生攻击、并且之前创建的副本早于指定的时间间隔、则会创建一个新的Snapshot副本。

ARW设置	Description
* 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副本变为旧副本时、将删除在最新副本之前为达到此期限而创建的任何其他ARP Snapshot副本。任何ARP Snapshot副本都不能早于此持续时间。
* 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)。如果卷上未报告任何早于此持续时间的ARP Snapshot副本攻击、则此副本将被删除。 + ⓘ 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。
* 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。如果卷已包含最大数量的ARP Snapshot副本、则此选项中指定的时间间隔将用于下次创建ARP Snapshot副本、而不是arw.snap.create.interval.hours。
* arw.surge.snap.interval.days*	指定ARP激增Snapshot副本之间的间隔_in days 。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。此选项还指定*ARP*激增快照的保留期限_*in day*。

防范病毒

防病毒配置概述

Vscan是NetApp开发的防病毒扫描解决方案、支持客户保护其数据免受病毒或其他恶意代码的危害。

当客户端通过SMB访问文件时、Vscan会执行病毒扫描。您可以将Vscan配置为按需或按计划进行扫描。您可以使用ONTAP命令行界面(CLI)或ONTAP应用程序编程接口(API)与Vscan进行交互。

相关信息

"Vscan合作伙伴解决方案"

关于 **NetApp** 防病毒保护

关于 **NetApp** 病毒扫描

Vscan是NetApp开发的防病毒扫描解决方案、支持客户保护其数据免受病毒或其他恶意代码的危害。它将合作伙伴提供的防病毒软件与ONTAP功能相结合、为客户提供管理文件扫描所需的灵活性。

存储系统将扫描操作卸载到托管第三方供应商提供的防病毒软件的外部服务器。

根据活动扫描模式、当客户端按计划或立即(按需)通过SMB (实时)访问文件或访问特定位置的文件时、ONTAP会发送扫描请求。

- 当客户端通过 SMB 打开，读取，重命名或关闭文件时，您可以使用 _on-access scanning-来 检查病毒。文件操作将暂停、直到外部服务器报告文件的扫描状态为止。如果文件已扫描，则 ONTAP 允许执行文件操作。否则，它将从服务器请求扫描。

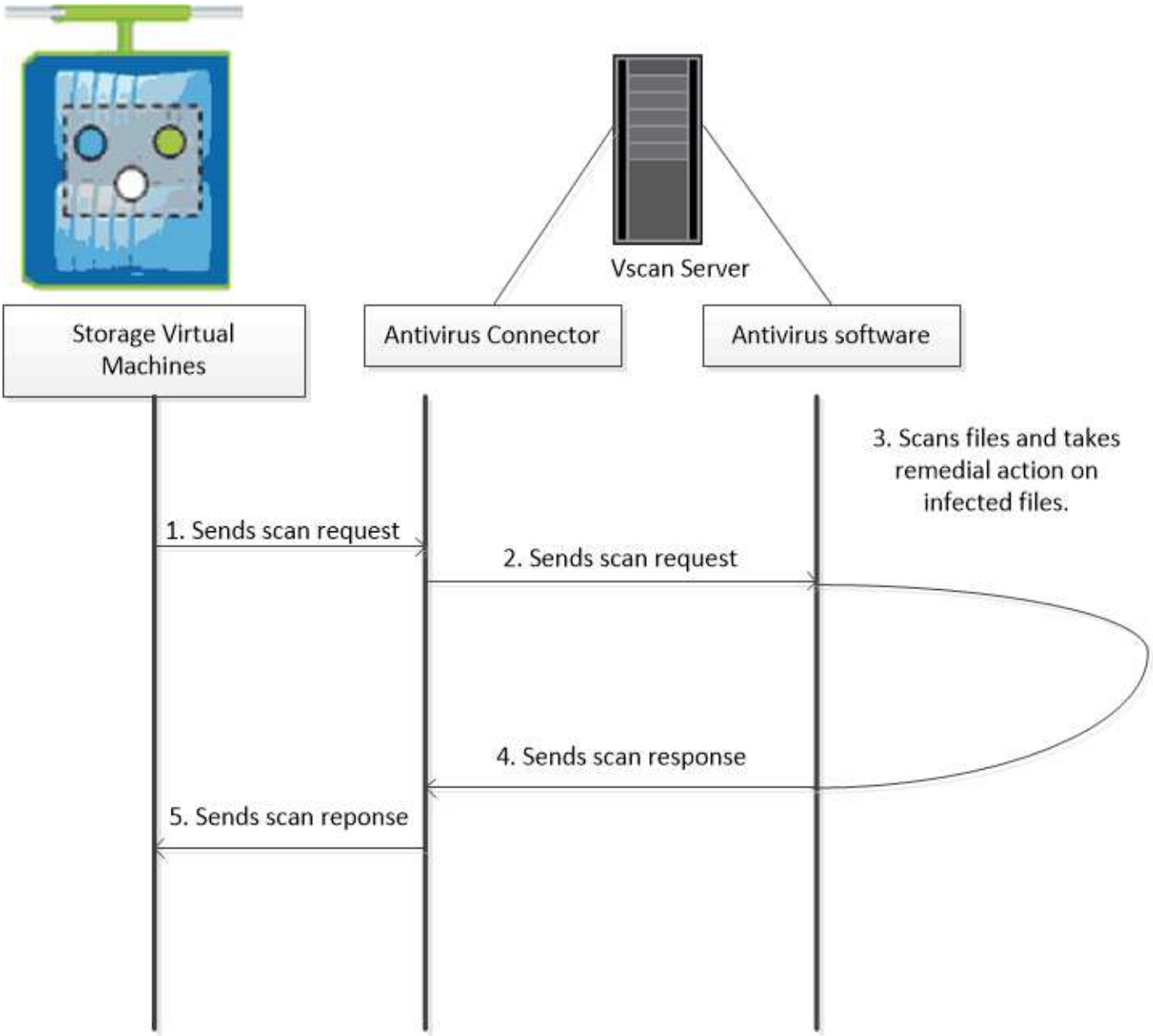
  NFS 不支持实时扫描。

- 您可以使用 _on-Demand scanning-立即 或按计划检查文件中的病毒。我们建议按需扫描只在非高峰时段运行、以避免现有AV基础架构过载、而现有AV基础架构的规模通常适合实时扫描。外部服务器会更新已检查文件的扫描状态、以便通过SMB减少文件访问延迟。如果进行了文件修改或软件版本更新、则会从外部服务器请求新的文件扫描。

  您可以对 SVM 命名空间中的任何路径使用按需扫描，即使是仅通过 NFS 导出的卷也是如此。

通常、您会在SVM上同时启用实时和按需扫描模式。在任一模式下、防病毒软件都会根据您的软件设置对受感染的文件采取补救措施。

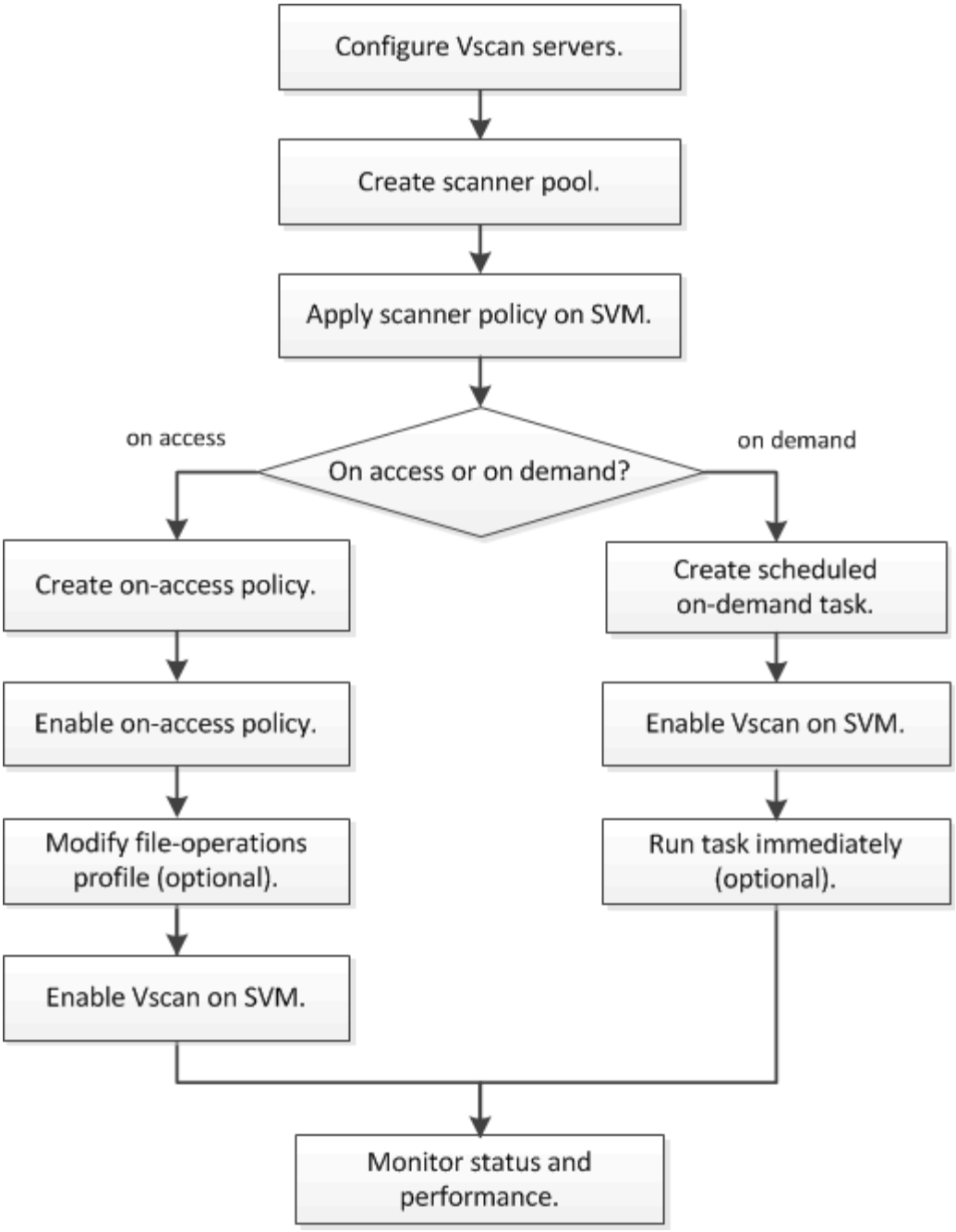
ONTAP 防病毒连接器由 NetApp 提供并安装在外部服务器上，用于处理存储系统与防病毒软件之间的通信。



病毒扫描工作流

您必须先创建扫描程序池并应用扫描程序策略，然后才能启用扫描。通常、您会在SVM上同时启用实时和按需扫描模式。

> 您必须已完成 CIFS 配置。



后续步骤

- 在单个集群上创建扫描程序池
- 在单个集群上应用扫描程序策略
- 创建实时策略

防病毒架构

NetApp防病毒架构由Vscan服务器软件和相关设置组成。

Vscan服务器软件

您必须在Vscan服务器上安装此软件。

- * ONTAP 防病毒连接器 *

  这是NetApp提供的软件、用于处理SVM与防病毒软件之间的扫描请求和响应通信。它可以在虚拟机上运行、但为了获得最佳性能、请使用物理机。您可以从NetApp 支持站点 下载此软件(需要登录)。

- * 防病毒软件 *

  这是合作伙伴提供的软件、用于扫描文件中的病毒或其他恶意代码。您可以指定在配置软件时对受感染文件采取的补救措施。

Vscan软件设置

您必须在Vscan服务器上配置这些软件设置。

- * 扫描程序池 *

  此设置用于定义可连接到SVM的Vscan服务器和有权限的用户。它还定义了扫描请求超时期限，之后，如果有备用 Vscan 服务器，则会将扫描请求发送到该服务器。

  > 您应将Vscan服务器上防病毒软件的超时期限设置为比扫描程序池扫描请求超时期限少五秒。这样可以避免因软件超时期限大于扫描请求超时期限而导致文件访问延迟或被完全拒绝的情况。

- * 特权用户 *

  此设置是Vscan服务器用于连接到SVM的域用户帐户。该帐户必须位于扫描程序池中的有权限用户列表中。

- * 扫描程序策略 *

  此设置确定扫描程序池是否处于活动状态。扫描程序策略是系统定义的、因此您无法创建自定义扫描程序策略。只有以下三种策略可用：

  - `Primary` 指定扫描程序池处于活动状态。
  - `Secondary` 指定扫描程序池仅在主扫描程序池中没有Vscan服务器连接时处于活动状态。
  - `Idle` 指定扫描程序池处于非活动状态。

- * 实时策略 *

  此设置定义实时扫描的范围。您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。

  默认情况下，仅扫描读写卷。您可以指定允许扫描只读卷或将扫描限制为使用执行访问打开的文件的筛选器：

  - `scan-ro-volume` 启用只读卷扫描。
  - `scan-execute-access` 限制对通过执行访问打开的文件的扫描。

  > “执行访问`"不同于"`执行权限。” 仅当可执行文件是使用"`execute intent`"打开时、给定客户端才会对该文件具有"`execute access`"。

您可以设置 `scan-mandatory` 选项设置为off、用于指定在没有可用于病毒扫描的Vscan服务器时允许文件访问。在实时模式下、您可以从以下两个互斥选项中进行选择：

- 必填：使用此选项、Vscan会尝试向服务器传送扫描请求、直到超时期限到期为止。如果服务器未接受扫描请求、则客户端访问请求将被拒绝。
- Non-Mandatory:使用此选项时，无论Vscan服务器是否可用于病毒扫描，Vscan始终允许客户端访问。

- * 按需任务 *

  此设置定义按需扫描的范围。您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。默认情况下会扫描子目录中的文件。

  您可以使用 cron 计划指定任务运行的时间。您可以使用 `vserver vscan on-demand-task run` 命令以立即运行任务。

- * Vscan 文件操作配置文件（仅限实时扫描） *

  。 `vscan-fileop-profile` 的参数 `vserver cifs share create` 命令用于定义触发病毒扫描的SMB文件操作。默认情况下、参数设置为 `standard`，这是NetApp最佳实践。在创建或修改SMB共享时、您可以根据需要调整此参数：

  - `no-scan` 指定从不为共享触发病毒扫描。
  - `standard` 指定病毒扫描由打开、关闭和重命名操作触发。
  - `strict` 指定病毒扫描由打开、读取、关闭和重命名操作触发。

    。 `strict` 如果多个客户端同时访问一个文件、则配置文件可增强安全性。如果一个客户端在向某个文件写入病毒后将其关闭、而同一文件在另一个客户端上保持打开状态、 `strict` 确保在关闭文件之前、对第二个客户端执行读取操作会触发扫描。

    您应小心限制 `strict` 配置文件到包含您预计将同时访问的文件的共享。由于此配置文件生成的扫描请求较多、因此可能会影响性能。

  - `writes-only` 指定仅在关闭修改后的文件时才触发病毒扫描。

    自此 `writes-only` 生成的扫描请求更少、通常可提高性能。

  如果使用此配置文件、则必须将扫描程序配置为删除或隔离不可修复的受感染文件、以便无法访问这些文件。例如、如果客户端在向某个文件写入病毒后关闭该文件、并且该文件未被修复、删除或被隔离、则访问该文件的任何客户端都是如此 `without` 写入数据将受到感染。

> 如果客户端应用程序执行重命名操作，则文件将使用新名称关闭，不会进行扫描。如果此类操作在您的环境中造成安全问题、则应使用 `standard` 或 `strict` 配置文件。

Vscan合作伙伴解决方案

NetApp与Trellix、Symantec、Trend Micro和Sentinel One合作、提供基于ONTAP Vscan技术构建的行业领先的反恶意软件和防病毒解决方案。这些解决方案可帮助您扫描文件中的恶意软件并修复任何受影响的文件。

如下表所示、NetApp互操作性表维护了Trellix、Symantec和Trend Micro的互操作性详细信息。有关Trellix

和Symantec的互操作性详细信息、请参见合作伙伴网站。Sentinel One和其他新合作伙伴的互操作性详细信息将由合作伙伴在其网站上维护。

合作伙伴	解决方案文档	互操作性详细信息
Trellix (前身为McAfee)	"Trellix产品文档"	• "NetApp 互操作性表工具" • "支持的端点安全存储保护平台(trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	• "NetApp 互操作性表工具" • "合作伙伴设备支持表—已通过网络连接存储(NAS) 9.x.x.x.x.x.x.z的Symantec保护引擎(Protection Engine、身份验证引擎)认证" • "获得网络连接存储(NAS) 8.x版Symantec保护引擎(SPE)认证的合作伙伴设备支持列表(broadcom.com)"
Trend Micro	"《Trend Micro Serverect for Storage 6.0入门指南》"	"NetApp 互操作性表工具"
Sentinel One	• "SentinelOne Singlity Cloud Data Security" • "SentinelOne支持" 此链接需要用户登录。您可以从Sentinel One申请访问权限。	深刻的直觉

Vscan 服务器安装和配置

Vscan 服务器安装和配置

设置一个或多个Vscan服务器、以确保系统上的文件已进行病毒扫描。按照供应商提供的说明在服务器上安装和配置防病毒软件。

按照NetApp提供的自述文件中的说明安装和配置ONTAP防病毒连接器。或者、按照上的说明进行操作 "安装ONTAP防病毒连接器页面"。

> 对于灾难恢复和MetroCluster配置、您必须为主/本地和二级/配对ONTAP集群设置和配置单独的Vscan服务器。

防病毒软件要求

- 有关防病毒软件要求的信息，请参见供应商文档。
- 有关 Vscan 支持的供应商，软件和版本的信息，请参见 "Vscan合作伙伴解决方案" 页面。

ONTAP 防病毒连接器要求

- 您可以从NetApp 支持站点 上的*软件下载*页面下载ONTAP防病毒连接器。 "NetApp 下载：软件"
- 有关ONTAP防病毒连接器支持的Windows版本和互操作性要求的信息、请参阅 "Vscan合作伙伴解决方案"。

> 您可以为集群中的不同 Vscan 服务器安装不同版本的 Windows 服务器。

- Windows 服务器上必须安装 .NET 3.0 或更高版本。
- 必须在 Windows 服务器上启用 SMB 2.0 。

安装**ONTAP**防病毒连接器

在Vscan服务器上安装ONTAP防病毒连接器、以启用运行ONTAP的系统与Vscan服务器之间的通信。安装ONTAP防病毒连接器后、防病毒软件可以与一个或多个Storage Virtual Machine (SVM)进行通信。

关于此任务

- 请参见 "Vscan合作伙伴解决方案" 页面、了解有关支持的协议、防病毒供应商软件版本、ONTAP版本、互操作性要求和Windows服务器的信息。
- 必须安装.NET 4.5.1或更高版本。
- ONTAP防病毒连接器可以在虚拟机上运行。但是、为了获得最佳性能、NetApp建议使用专用虚拟机进行防病毒扫描。
- 必须在要安装和运行ONTAP防病毒连接器的Windows服务器上启用SMB 2.0。

开始之前

- 从支持站点下载ONTAP防病毒连接器安装文件、并将其保存到硬盘驱动器上的目录中。
- 确认您满足安装ONTAP防病毒连接器的要求。
- 验证您是否具有安装防病毒连接器的管理员权限。

步骤

1. 运行相应的安装文件以启动防病毒连接器安装向导。
2. 选择_Next_。此时将打开目标文件夹对话框。
3. 选择_Next_将防病毒连接器安装到列出的文件夹中，或选择_Change_to install to a next folder。
4. 此时将打开ONTAP AV Connector Windows服务凭据对话框。
5. 输入您的Windows服务凭据或选择*Add*以选择用户。对于ONTAP系统、此用户必须是有效的域用户、并且必须位于SVM的扫描程序池配置中。
6. 选择 * 下一步 * 。此时将打开准备安装程序对话框。
7. 选择*Install*开始安装，或者如果要对设置进行任何更改，选择*Back*。
   此时将打开一个状态框，并显示安装进度，然后显示InstallShield向导已完成对话框。
8. 如果要继续配置ONTAP管理或数据、请选中配置ONTAP LUN复选框。
   要使用此Vscan服务器、必须至少配置一个ONTAP管理或数据LIF。
9. 如果要查看安装日志，请选中显示*Windows Installer log*复选框。

10. 选择*完成*以结束安装并关闭InstallShield向导。
配置ONTAP Lifs*图标保存在桌面上以配置ONTAP Lifs。

11. 将SVM添加到防病毒连接器。
您可以通过添加ONTAP管理LIF (轮询以检索数据LIF列表)或直接配置一个或多个数据LIF来将SVM添加到防病毒连接器。
如果配置了ONTAP管理LIF、则还必须提供轮询信息和ONTAP管理员帐户凭据。

    - 验证是否已为启用管理LIF或SVM的IP地址 `management-https`。仅在配置数据生命周期时、不需要执行此操作。
    - 验证是否已为HTTP应用程序创建用户帐户、并分配了对具有(至少是只读)访问权限的角色 `/api/network/ip/interfaces` REST API。
    有关创建用户的详细信息、请参见 "创建安全登录角色" 和 "创建安全登录" ONTAP手册页。

> 您还可以通过为管理SVM添加身份验证通道SVM来使用域用户作为帐户。有关详细信息，请参见 "安全登录域通道创建" ONTAP手册页或使用 `/api/security/acccounts` 和 `/api/security/roles` 用于配置管理员帐户和角色的REST API。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。
2. 在配置ONTAP LUN对话框中、选择首选配置类型、然后执行以下操作：

要创建此类型的LIF…	执行以下步骤 …
数据 LIF	a. 将"Role"设置为"data" b. 将"data protocol (数据协议)"设置为"CIFS (CIFS)" c. 将"Firewall policy"设置为"data" d. 将"service policy"设置为"default-data-files"
管理LIF	a. 将"Role*设置为"data" b. 将"data protocol (数据协议)"设置为"none (无)" c. 将"Firewall policy"设置为"mgmt" d. 将"service policy"设置为"default-management "

了解更多信息 "正在创建LIF"。

创建LIF后、输入要添加的SVM的数据或管理LIF或IP地址。您也可以输入集群管理LIF。如果指定集群管理LIF、则该集群中提供SMB的所有SVM都可以使用Vscan服务器。

> 如果Vscan服务器需要Kerberos身份验证、则每个SVM数据LIF都必须具有唯一的DNS名称、并且您必须将该名称注册为Windows Active Directory中的服务器主体名称(SPN)。如果没有为每个数据LIF提供唯一的DNS名称或将其注册为SPN、则Vscan服务器将使用NT LAN Manager机制进行身份验证。如果在连接Vscan服务器后添加或修改DNS名称和SPN、则必须在Vscan服务器上重新启动防病毒连接器服务以应用更改。

3. 要配置管理LIF、请输入轮询持续时间(以秒为单位)。轮询持续时间是指防病毒连接器检查SVM或集群LIF配置是否发生更改的频率。默认轮询间隔为60秒。

4. 输入ONTAP管理员帐户名称和密码以配置管理LIF。
5. 单击*Test*以检查连接并验证身份验证。仅验证管理LIF配置的身份验证。
6. 单击*更新*将LIF添加到要轮询或连接到的LIF列表中。
7. 单击*保存*以保存与注册表的连接。
8. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

请参见 "配置ONTAP防病毒连接器页面" 了解配置选项。

配置**ONTAP**防病毒连接器

通过输入ONTAP管理LIF、轮询信息和ONTAP管理员帐户凭据或仅输入数据LIF、配置ONTAP防病毒连接器以指定要连接到的一个或多个Storage Virtual Machine (SVM)。您还可以修改SVM连接的详细信息或删除SVM连接。默认情况下、如果配置了ONTAP管理LIF、ONTAP防病毒连接器将使用REST API检索数据LIF列表。

修改**SVM**连接的详细信息

您可以通过修改ONTAP管理LIF和轮询信息来更新已添加到防病毒连接器的Storage Virtual Machine (SVM)连接的详细信息。添加数据LUN后、您将无法对其进行更新。要更新数据LIF、您必须先将其删除、然后使用新的LIF或IP地址重新添加。

开始之前

验证是否已为HTTP应用程序创建用户帐户、并分配了对具有(至少是只读)访问权限的角色 `/api/network/ip/interfaces` REST API。
有关创建用户的详细信息、请参见 "创建安全登录角色" 和 "创建安全登录" 命令
您还可以通过为管理SVM添加身份验证通道SVM来使用域用户作为帐户。
有关详细信息，请参见 "安全登录域通道创建" ONTAP手册页。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。此时将打开配置ONTAP LUN对话框。
2. 选择SVM IP地址，然后单击*Update*。
3. 根据需要更新此信息。
4. 单击*保存*以更新注册表中的连接详细信息。
5. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。
如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

从防病毒连接器中删除**SVM**连接

如果您不再需要SVM连接、可以将其删除。

步骤

1. 右键单击完成防病毒连接器安装时保存在桌面上的*配置ONTAP Lifs*图标，然后选择*以管理员身份运行*。此时将打开配置ONTAP LUN对话框。
2. 选择一个或多个SVM IP地址，然后单击*Remove*。

3. 单击*保存*以更新注册表中的连接详细信息。
4. 如果要将连接列表导出到注册表导入或注册表导出文件，请单击*Export*。
   如果多个Vscan服务器使用一组相同的管理或数据生命周期、则此功能非常有用。

故障排除

开始之前

在此操作步骤中创建注册表值时、请使用右侧窗格。

您可以启用或禁用防病毒连接器日志以进行诊断。默认情况下、这些日志处于禁用状态。为了提高性能、您应禁用防病毒连接器日志、并仅在发生严重事件时启用这些日志。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。
2. 在*Registry Editor*中，找到ONTAP防病毒连接器的以下项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 通过提供下表所示的类型、名称和值来创建注册表值：

Type	Name	值
string	迹线	C：\avshim.log

   此注册表值可以是任何其他有效路径。

4. 通过提供下表所示的类型、名称、值和日志记录信息、创建另一个注册表值：

Type	Name	关键日志记录	中间日志记录	详细日志记录
DWORD	Tracellevel	1.	2或3	4.

   这将启用按照步骤3中的TracePath提供的路径值保存的防病毒连接器日志。

5. 通过删除在步骤3和4中创建的注册表值来禁用防病毒连接器日志。
6. 创建另一个类型为"multi_SZ"且名称为"LogRotation"(不带引号)的注册表值。在"LogRotation"中、提供"logFileSize：1"作为轮换大小的条目(其中1表示1MB)、并在下一行中提供"logFileCount：5"作为旋转限值条目(5为限值)。

   这些值是可选的。如果未提供、则会分别使用默认值20 MB和10个文件作为轮换大小和轮换限制。提供的整数值不提供小数值或小数值。如果提供的值高于默认值、则会改用默认值。

7. 要禁用用户配置的日志轮换、请删除您在步骤6中创建的注册表值。

可自定义的横幅

自定义横幅允许您在_Configure ONTAP LIF API_窗口中放置具有法律约束力的声明和系统访问免责声明。

步骤

1. 通过更新中的内容来修改默认横幅 `banner.txt` 文件、然后保存所做的更改。
   要查看横幅中反映的更改、必须重新打开配置ONTAP LIF API窗口。

启用扩展条例模式

您可以启用和禁用扩展法令(EO)模式以确保安全操作。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。
2. 在*Registry Editor*中，找到ONTAP防病毒连接器的以下项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 在右侧窗格中、创建名为"EO_Mode"(不带引号)且值为"1"(不带引号)的新注册表值"DWORD"、以启用"EO模式"或值"0"(不带引号)禁用"EO模式"。

> 默认情况下、如果是 `EO_Mode` 缺少注册表条目、已禁用EO模式。启用EO模式后、必须同时配置外部系统日志服务器和相互证书身份验证。

配置外部系统日志服务器

开始之前

请注意、在此操作步骤中创建注册表值时、请使用右侧窗格。

步骤

1. 选择*Start*，在搜索框中键入“regedit”，然后选择 `regedit.exe` 在程序列表中。
2. 在*Registry Editor*中，为系统日志配置的ONTAP防病毒连接器创建以下项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 通过提供类型、名称和值来创建注册表值、如下表所示：

Type	Name	价值
DWORD	syslog_enabled	1或0

   请注意、使用"1"值启用系统日志、使用"0"值禁用系统日志。

4. 通过提供下表所示的信息创建另一个注册表值：

Type	Name
REG_SZ	syslog_host

   为值字段提供系统日志主机IP地址或域名。

5. 通过提供下表所示的信息创建另一个注册表值：

Type	Name

REG_SZ	syslog_port

在Value字段中提供运行系统日志服务器的端口号。

6. 通过提供下表所示的信息创建另一个注册表值：

Type	Name
REG_SZ	syslog_protocol

在值字段中输入系统日志服务器上使用的协议、即"TCP"或"UDP"。

7. 通过提供下表所示的信息创建另一个注册表值：

Type	Name	Log_Rert	log_notice	LOG_INFO	log_ddebug
DWORD	syslog_level	2.	5.	6.	7.

8. 通过提供下表所示的信息创建另一个注册表值：

Type	Name	价值
DWORD	syslog_tls.	1或0

请注意、"1"值将启用采用传输层安全(Transport Layer Security、TLS)的系统日志、而"0"值将禁用采用TLS的系统日志。

确保已配置的外部系统日志服务器平稳运行

- 如果密钥不存在或具有空值：
  - 协议默认为"TCP"。
  - 对于纯"TCP/UDP"、此端口默认为"514"；对于TLS、此端口默认为"6514"。
  - 系统日志级别默认为5 (log_notice)。
- 您可以通过验证是否已启用系统日志来确认是否已启用 `syslog_enabled` 值为"1"。当 `syslog_enabled` 值为"1"、无论是否启用了EO模式、您都应该能够登录到已配置的远程服务器。
- 如果将EO模式设置为"1"、则更改 `syslog_enabled` 值从"1"到"0"、适用以下条件：
  - 如果未在EO模式下启用系统日志、则无法启动此服务。
  - 如果系统以稳定状态运行、则会显示一条警告、指出无法在EO模式下禁用系统日志、并且系统日志会强制设置为"1"、您可以在注册表中看到此信息。如果发生这种情况、您应先禁用EO模式、然后再禁用系统日志。
- 如果在启用了EO模式和系统日志后、系统日志服务器无法成功运行、则该服务将停止运行。出现此问题的原因可能如下：
  - 配置的syslog_host无效或未配置。

- 配置的协议无效、而不是UDP或TCP。
- 端口号无效。

- 对于TCP或基于TCP的TLS配置、如果服务器未侦听IP端口、则连接将失败、服务将关闭。

配置X.509相互证书身份验证

对于管理路径中防病毒连接器和ONTAP之间的安全套接字层(SSL)通信、可以使用基于X.509证书的相互身份验证。如果启用了EO模式、但未找到证书、AV Connector将终止。在防病毒连接器上执行以下操作步骤：

步骤

1. 防病毒连接器在其运行安装目录的目录路径中搜索NetApp服务器的防病毒连接器客户端证书和证书颁发机构(CA)证书。将证书复制到此固定目录路径中。
2. 以PKCS12格式嵌入客户端证书及其私钥、并将其命名为"AV_client.p12"。
3. 确保用于对NetApp服务器的证书签名的CA证书(以及任何中间签名颁发机构、直到根CA)采用隐私增强邮件(PEM)格式且名为"ONTAP CA。pEM"。将其放在防病毒连接器安装目录中。在NetApp ONTAP系统上、安装用于将ONTAP中的防病毒连接器客户端证书作为"client-ca"类型证书进行签名的CA证书(以及直到根CA的任何中间签名颁发机构)。

配置扫描程序池

配置扫描程序池概述

扫描程序池用于定义可连接到 SVM 的 Vscan 服务器和有权限的用户。扫描程序策略用于确定扫描程序池是否处于活动状态。

> 如果在SMB服务器上使用导出策略、则必须将每个Vscan服务器添加到此导出策略中。

在单个集群上创建扫描程序池

扫描程序池用于定义可连接到 SVM 的 Vscan 服务器和有权限的用户。您可以为单个SVM或集群中的所有SVM创建扫描程序池。

您需要的内容

- SVM 和 Vscan 服务器必须位于同一域或受信任域中。
- 对于为单个SVM定义的扫描程序池、您必须已为ONTAP防病毒连接器配置SVM管理LIF或SVM数据LIF。
- 对于为集群中的所有SVM定义的扫描程序池、您必须已使用集群管理LIF配置ONTAP防病毒连接器。
- 有权限的用户列表必须包含 Vscan 服务器用于连接到 SVM 的域用户帐户。
- 配置扫描程序池后、请检查与服务器的连接状态。

步骤

1. 创建扫描程序池：

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

- 为为为单个 SVM 定义的池指定数据 SVM ，并为为为集群中的所有 SVM 定义的池指定集群管理员 SVM 。
- 为每个 Vscan 服务器主机名指定 IP 地址或 FQDN 。
- 为每个有权限的用户指定域和用户名。
  有关完整的选项列表，请参见命令手册页。

  以下命令将创建名为的扫描程序池 `SP` 在上 `vs1` SVM：

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. 验证是否已创建扫描程序池：

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   有关完整的选项列表，请参见命令手册页。

   以下命令将显示的详细信息 `SP` 扫描程序池：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   您也可以使用 `vserver vscan scanner-pool show` 命令以查看SVM上的所有扫描程序池。有关完整的命令语法，请参见命令手册页。

在 **MetroCluster** 配置中创建扫描程序池

您必须在 MetroCluster 配置中的每个集群上创建主和二级扫描程序池，这些池对应于集群上的主和二级 SVM 。

您需要的内容

- SVM 和 Vscan 服务器必须位于同一域或受信任域中。

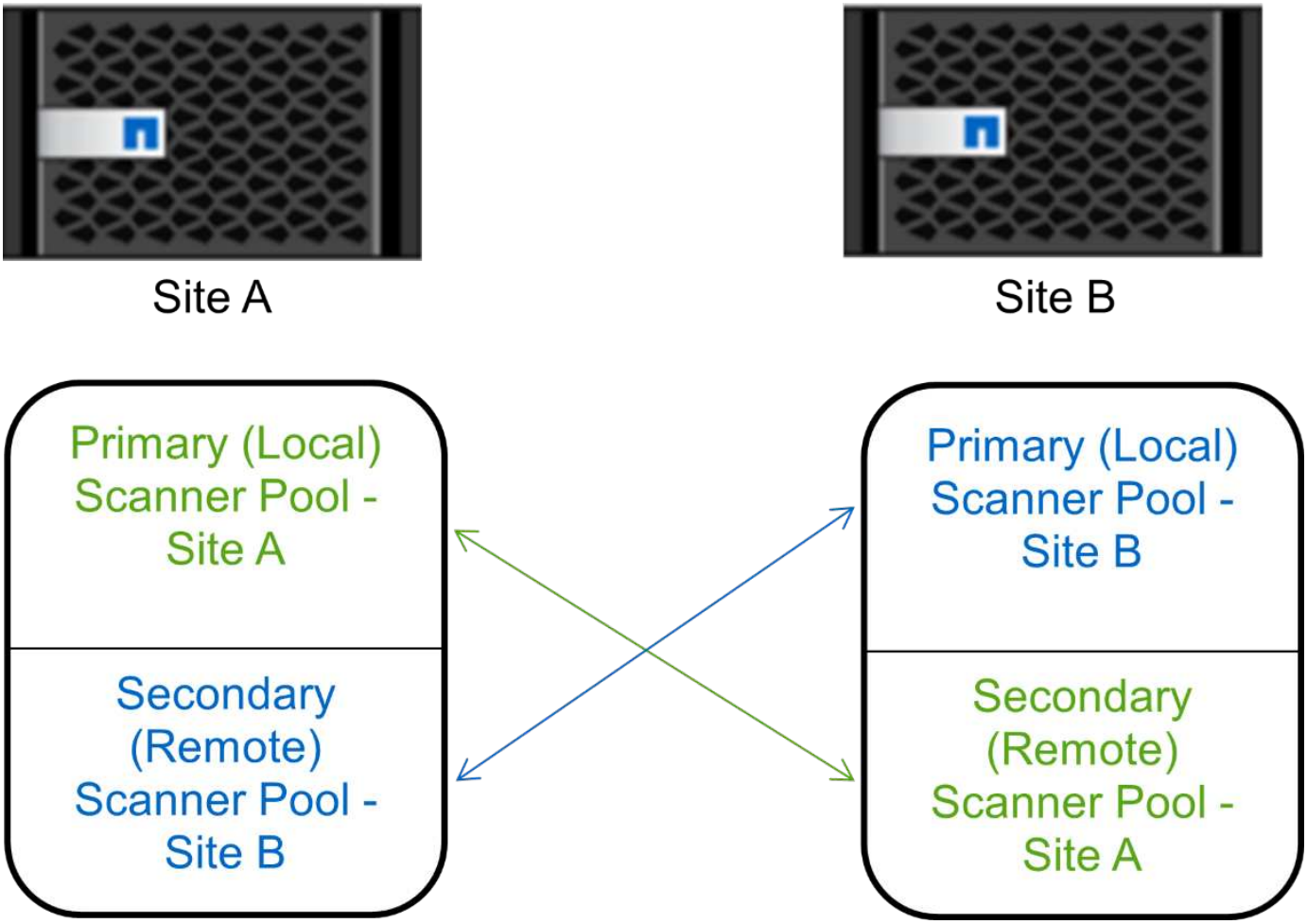
- 对于为单个SVM定义的扫描程序池、您必须已为ONTAP防病毒连接器配置SVM管理LIF或SVM数据LIF。
- 对于为集群中的所有SVM定义的扫描程序池、您必须已使用集群管理LIF配置ONTAP防病毒连接器。
- 有权限的用户列表必须包含 Vscan 服务器用于连接到 SVM 的域用户帐户。
- 配置扫描程序池后、请检查与服务器的连接状态。

关于此任务

MetroCluster 配置通过实施两个物理上独立的镜像集群来保护数据。每个集群会同步复制另一个集群的数据和 SVM 配置。当集群联机时，本地集群上的主 SVM 将提供数据。当远程集群脱机时，本地集群上的二级 SVM 将提供数据。

这意味着您必须在MetroCluster配置中的每个集群上创建主扫描程序池和二级扫描程序池、当集群开始从二级SVM提供数据时、二级池将变为活动状态。对于灾难恢复(Disaster Recovery、DR)、此配置与MetroCluster类似。

此图显示了典型的MetroCluster/DR配置。



步骤

1. 创建扫描程序池：

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

- 为为为单个 SVM 定义的池指定数据 SVM ，并为为为集群中的所有 SVM 定义的池指定集群管理员 SVM 。
- 为每个 Vscan 服务器主机名指定 IP 地址或 FQDN 。
- 为每个有权限的用户指定域和用户名。

> 您必须从包含主 SVM 的集群创建所有扫描程序池。

有关完整的选项列表，请参见命令手册页。

以下命令会在 MetroCluster 配置中的每个集群上创建主扫描程序池和二级扫描程序池：

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. 验证是否已创建扫描程序池：

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   有关完整的选项列表，请参见命令手册页。

   以下命令显示扫描程序池的详细信息 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

您也可以使用 `vserver vscan scanner-pool show` 命令以查看SVM上的所有扫描程序池。有关完整的命令语法，请参见命令手册页。

在单个集群上应用扫描程序策略

扫描程序策略用于确定扫描程序池是否处于活动状态。您必须先激活扫描程序池、然后它定义的Vscan服务器才能连接到SVM。

关于此任务

- 一个扫描程序池只能应用一个扫描程序策略。
- 如果为集群中的所有SVM创建了扫描程序池、则必须分别对每个SVM应用扫描程序策略。

步骤

1. 应用扫描程序策略：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   扫描程序策略可以具有以下值之一：

   - `Primary` 指定扫描程序池处于活动状态。
   - `Secondary` 指定只有在主扫描程序池中没有Vscan服务器连接时扫描程序池才处于活动状态。
   - `Idle` 指定扫描程序池处于非活动状态。

     以下示例显示名为的扫描程序池 `SP` 在上 `vs1` SVM处于活动状态：

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. 验证扫描程序池是否处于活动状态：

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 `SP` 扫描程序池：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

您可以使用 `vserver vscan scanner-pool show-active` 命令以查看SVM上的活动扫描程序池。有关完整的命令语法，请参见命令的手册页。

在 **MetroCluster** 配置中应用扫描程序策略

扫描程序策略用于确定扫描程序池是否处于活动状态。必须将扫描程序策略应用于MetroCluster 配置中每个集群上的主扫描程序池和二级扫描程序池。

关于此任务

- 一个扫描程序池只能应用一个扫描程序策略。
- 如果为集群中的所有SVM创建了扫描程序池、则必须分别对每个SVM应用扫描程序策略。
- 对于灾难恢复和MetroCluster配置、您必须将扫描程序策略应用于本地集群和远程集群中的每个扫描程序池。
- 在为本地集群创建的策略中、必须在中指定本地集群 `cluster` 参数。在为远程集群创建的策略中、必须在中指定远程集群 `cluster` 参数。然后、远程集群可以在发生灾难时接管病毒扫描操作。

步骤

1. 应用扫描程序策略：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   扫描程序策略可以具有以下值之一：

- `Primary` 指定扫描程序池处于活动状态。
- `Secondary` 指定只有在主扫描程序池中没有Vscan服务器连接时扫描程序池才处于活动状态。
- `Idle` 指定扫描程序池处于非活动状态。

> 您必须应用包含主 SVM 的集群中的所有扫描程序策略。

以下命令会将扫描程序策略应用于 MetroCluster 配置中每个集群上的主扫描程序池和二级扫描程序池：

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. 验证扫描程序池是否处于活动状态：

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   有关完整的选项列表，请参见命令手册页。

   以下命令显示扫描程序池的详细信息 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

您可以使用 `vserver vscan scanner-pool show-active` 命令以查看SVM上的活动扫描程序池。有关完整的命令语法，请参见命令手册页。

用于管理扫描程序池的命令

您可以修改和删除扫描程序池，以及管理扫描程序池的有权限用户和 Vscan 服务器。您还可以查看有关扫描程序池的摘要信息。

如果您要 ...	输入以下命令 ...
修改扫描程序池	`vserver vscan scanner-pool modify`
删除扫描程序池	`vserver vscan scanner-pool delete`
将有权限的用户添加到扫描程序池	`vserver vscan scanner-pool privileged-users add`
从扫描程序池中删除有权限的用户	`vserver vscan scanner-pool privileged-users remove`
将 Vscan 服务器添加到扫描程序池	`vserver vscan scanner-pool servers add`
从扫描程序池中删除 Vscan 服务器	`vserver vscan scanner-pool servers remove`
查看扫描程序池的摘要和详细信息	`vserver vscan scanner-pool show`
查看扫描程序池的有权限用户	`vserver vscan scanner-pool privileged-users show`
查看所有扫描程序池的 Vscan 服务器	`vserver vscan scanner-pool servers show`

有关这些命令的详细信息，请参见手册页。

配置实时扫描

创建实时策略

实时策略用于定义实时扫描的范围。您可以为单个 SVM 或集群中的所有 SVM 创建实时策略。如果您为集群中的所有 SVM 创建了实时策略，则必须分别在每个 SVM 上启用该策略。

关于此任务

- 您可以指定要扫描的最大文件大小、要包括在扫描中的文件扩展名和路径以及要从扫描中排除的文件扩展名和路径。

- 您可以设置 `scan-mandatory` 选项设置为off、用于指定在没有可用于病毒扫描的Vscan服务器时允许文件访问。
- 默认情况下、ONTAP会创建一个名为"default_CIFS"的实时策略、并为集群中的所有SVM启用该策略。
- 符合基于的扫描排除条件的任何文件 `paths-to-exclude`， `file-ext-to-exclude`或 `max-file-size` 扫描时不考虑参数、即使是 `scan-mandatory` 选项设置为on。(选中此项 "故障排除" 部分、了解与相关的连接问题 `scan-mandatory` 选项。)
- 默认情况下，仅扫描读写卷。您可以指定允许扫描只读卷或将扫描限制为使用执行访问打开的文件的筛选器。
- 如果持续可用参数设置为是、则不会对SMB共享执行病毒扫描。
- 请参见 "防病毒架构" 第节、了解有关_Vscan文件操作配置文件_的详细信息。
- 每个SVM最多可以创建十(10)个实时策略。但是、一次只能启用一个实时策略。
  - 在实时策略中、最多可以从病毒扫描中排除一百(100)个路径和文件扩展名。
- 一些文件排除建议：
  - 请考虑从病毒扫描中排除大型文件(可以指定文件大小)、因为它们可能会导致CIFS用户的响应速度较慢或扫描请求超时。要排除的默认文件大小为2 GB。
  - 请考虑排除文件扩展名、例如 `.vhd` 和 `.tmp` 因为具有这些扩展名的文件可能不适合扫描。
  - 请考虑排除一些文件路径、例如隔离目录或仅存储虚拟硬盘驱动器或数据库的路径。
  - 验证是否在同一策略中指定了所有排除项、因为一次只能启用一个策略。NetApp强烈建议使用在防病毒引擎中指定的一组相同排除项。
- 需要使用实时策略 按需扫描。要避免对进行实时扫描、您应设置 `-scan-files-with-no-ext` 设置为false、然后 `-file-ext-to-exclude` 至*以排除所有扩展名。

步骤

1. 创建实时策略：

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   - 为为为单个 SVM 定义的策略指定数据 SVM ，为为集群中的所有 SVM 定义的策略指定集群管理员 SVM 。
   - 。 `-file-ext-to-exclude` 设置将覆盖 `-file-ext-to-include` 设置。
   - 设置 `-scan-files-with-no-ext` 设置为true可扫描不带扩展名的文件。
     以下命令将创建一个名为的实时策略 `Policy1` 在上 `vs1` SVM：

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. 验证是否已创建实时策略：`vserver vscan on-access-policy show -instance *data_SVM|cluster_admin_SVM* -policy-name *name*`

   有关完整的选项列表，请参见命令手册页。

   以下命令将显示的详细信息 `Policy1` 策略：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

启用实时策略

实时策略用于定义实时扫描的范围。必须先在 SVM 上启用实时策略，然后才能扫描其文件。

如果您为集群中的所有 SVM 创建了实时策略，则必须分别在每个 SVM 上启用该策略。一次只能在 SVM 上启用一个实时策略。

步骤

1. 启用实时策略：

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   以下命令将启用名为的实时策略 `Policy1` 在上 `vs1` SVM：

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. 验证是否已启用实时策略：

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

有关完整的选项列表，请参见命令手册页。

以下命令将显示的详细信息 `Policy1` 实时策略：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

修改 **SMB** 共享的 **Vscan** 文件操作配置文件

SMB共享的_Vscan文件操作配置文件_用于定义共享上可触发扫描的操作。默认情况下、参数设置为 `standard`。创建或修改 SMB 共享时，您可以根据需要调整参数。

请参见 "防病毒架构" 第节、了解有关_Vscan文件操作配置文件_的详细信息。

> 不会对具有的SMB共享执行病毒扫描 `continuously-available` 参数设置为 `Yes`。

步骤

1. 修改SMB共享的Vscan文件操作配置文件的值：

   ```
   vserver cifs share modify -vserver data_SVM -share-name share -path share_path
   -vscan-fileop-profile no-scan|standard|strict|writes-only
   ```

   有关完整的选项列表，请参见命令手册页。

   以下命令将SMB共享的Vscan文件操作配置文件更改为 `strict`：

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

用于管理实时策略的命令

您可以修改，禁用或删除实时策略。您可以查看策略的摘要和详细信息。

如果您要 ...	输入以下命令 ...
创建实时策略	`vserver vscan on-access-policy create`
修改实时策略	`vserver vscan on-access-policy modify`
启用实时策略	`vserver vscan on-access-policy enable`
禁用实时策略	`vserver vscan on-access-policy disable`
删除实时策略	`vserver vscan on-access-policy delete`
查看实时策略的摘要和详细信息	`vserver vscan on-access-policy show`
添加到要排除的路径列表	`vserver vscan on-access-policy paths-to-exclude add`
从要排除的路径列表中删除	`vserver vscan on-access-policy paths-to-exclude remove`
查看要排除的路径列表	`vserver vscan on-access-policy paths-to-exclude show`
添加到要排除的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-exclude add`
从要排除的文件扩展名列表中删除	`vserver vscan on-access-policy file-ext-to-exclude remove`
查看要排除的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-exclude show`
添加到要包含的文件扩展名列表中	`vserver vscan on-access-policy file-ext-to-include add`
从要包含的文件扩展名列表中删除	`vserver vscan on-access-policy file-ext-to-include remove`
查看要包括的文件扩展名列表	`vserver vscan on-access-policy file-ext-to-include show`

有关这些命令的详细信息，请参见手册页。

配置按需扫描

配置按需扫描概述

您可以使用按需扫描立即或按计划检查文件中的病毒。

例如，您可能希望仅在非高峰时段运行扫描，或者您可能希望扫描从实时扫描中排除的非常大的文件。您可以使用cron计划指定任务运行的时间。

关于本主题

- 您可以在创建任务时分配计划。
- 一次只能在一个 SVM 上计划一个任务。
- 按需扫描不支持扫描符号链接或流文件。

> 按需扫描不支持扫描符号链接或流文件。

> 要创建按需任务、必须至少启用一个实时策略。它可以是默认策略、也可以是用户创建的实时策略。

创建按需任务

按需任务定义按需病毒扫描的范围。您可以指定要扫描的文件的最大大小，要包含在扫描中的文件的扩展名和路径，以及要从扫描中排除的文件的扩展名和路径。默认情况下会扫描子目录中的文件。

关于此任务

- 每个SVM最多可以有十(10)个按需任务、但只能有一个处于活动状态。
- 按需任务会创建一个报告、其中包含与扫描相关的统计信息。可通过命令或下载任务在定义的位置创建的报告文件来访问此报告。

开始之前

- 您必须拥有 已创建实时策略。此策略可以是默认策略、也可以是用户创建的策略。如果没有实时策略、则无法启用扫描。

步骤

1. 创建按需任务：

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
   -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
   -no-ext true|false -directory-recursion true|false
   ```

   - 。 `-file-ext-to-exclude` 设置将覆盖 `-file-ext-to-include` 设置。

- 设置 `-scan-files-with-no-ext` 设置为true可扫描不带扩展名的文件。

  有关完整的选项列表、请参见 "命令参考"。

  以下命令将创建一个名为的按需任务 `Task1` 在`VS1`s虚拟机上：

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> 您可以使用 `job show` 命令以查看作业状态。您可以使用 `job pause` 和 `job resume` 用于暂停和重新启动作业的命令、或 `job stop` 命令以结束作业。

2. 验证是否已创建按需任务：

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   有关完整的选项列表，请参见命令手册页。

   以下命令将显示的详细信息 `Task1` 任务：

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                 List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

完成后

在计划运行任务之前，必须在 SVM 上启用扫描。

计划按需任务

您可以在不分配计划的情况下创建任务、然后使用 `vserver vscan on-demand-task schedule` 命令以分配计划；或者在创建任务时添加计划。

关于此任务

分配给的计划 `vserver vscan on-demand-task schedule` 命令会覆盖已使用分配的计划 `vserver vscan on-demand-task create` 命令：

步骤

1. 计划按需任务：

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   以下命令会计划一个名为的实时任务 `Task2` 在上 `vs2` SVM：

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

要查看作业状态、请使用 `job show` 命令：。 `job pause` 和 `job resume` 命令、分别暂停和重新启动作业； `job stop` 命令将终止作业。

2. 验证是否已计划按需任务：

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   有关完整的选项列表，请参见命令手册页。

   以下命令将显示的详细信息 `Task 2` 任务：

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                 List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
```

完成后

在计划运行任务之前，必须在 SVM 上启用扫描。

立即运行按需任务

无论是否分配了计划，您都可以立即运行按需任务。

开始之前

您必须已在 SVM 上启用扫描。

步骤

1. 立即运行按需任务：

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   以下命令将运行名为的实时任务 `Task1` 在上 `vs1` SVM：

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

> 您可以使用 `job show` 命令以查看作业状态。您可以使用 `job pause` 和 `job resume` 用于暂停和重新启动作业的命令、或 `job stop` 命令以结束作业。

用于管理按需任务的命令

您可以修改，删除或取消计划按需任务。您可以查看任务的摘要和详细信息，并管理任务的报告。

如果您要 ...	输入以下命令 ...
创建按需任务	`vserver vscan on-demand-task create`
修改按需任务	`vserver vscan on-demand-task modify`
删除按需任务	`vserver vscan on-demand-task delete`
运行按需任务	`vserver vscan on-demand-task run`
计划按需任务	`vserver vscan on-demand-task schedule`
取消计划按需任务	`vserver vscan on-demand-task unschedule`
查看按需任务的摘要和详细信息	`vserver vscan on-demand-task show`
查看按需报告	`vserver vscan on-demand-task report show`
删除按需报告	`vserver vscan on-demand-task report delete`

有关这些命令的详细信息，请参见手册页。

在**ONTAP**中配置机下防病毒功能的最佳实践

在ONTAP中配置机下功能时、请考虑以下建议。

- 限制有权限的用户执行病毒扫描操作。不应鼓励普通用户使用有权限的用户凭据。可以通过关闭Active Directory上有权限的用户的登录权限来实现此限制。

- 有权限的用户不必属于在域中拥有大量权限的任何用户组、例如管理员组或备份操作员组。有权限的用户只能通过存储系统进行验证、以便可以创建Vscan服务器连接并访问文件以进行病毒扫描。
- 运行Vscan服务器的计算机仅用于病毒扫描。为了阻止常规使用、请禁用这些计算机上的Windows终端服务和其他远程访问配置、并仅向管理员授予在这些计算机上安装新软件的权限。
- 将Vscan服务器专用于病毒扫描、不要将其用于备份等其他操作。您可能决定将Vscan服务器作为虚拟机(VM)运行。如果将Vscan服务器作为VM运行、请确保分配给该VM的资源不会共享、并且有足够的资源来执行病毒扫描。
- 为Vscan服务器提供足够的CPU、内存和磁盘容量、以避免资源分配过度。大多数Vscan服务器都设计为使用多个CPU核心服务器、并在CPU之间分布负载。
- NetApp建议使用具有专用VLAN的专用网络从SVM连接到Vscan服务器、以使扫描流量不受其他客户端网络流量的影响。创建一个单独的网络接口卡(Network Interface Card、NIC)、专用于Vscan服务器上的防病毒VLAN和SVM上的数据LIF。此步骤可简化出现网络问题时的管理和故障排除。防病毒流量应使用专用网络进行隔离。应将防病毒服务器配置为通过以下方式之一与域控制器(DC)和ONTAP进行通信：
  - DC应通过用于隔离流量的专用网络与防病毒服务器通信。
  - DC和防病毒服务器应通过不同的网络(而不是前面提到的专用网络)进行通信、这与CIFS客户端网络不同。
  - 要为防病毒通信启用Kerberos身份验证、请为专用LIF创建一个DNS条目、并在DC上创建一个与为专用LIF创建的DNS条目对应的服务主体名称。将LIF添加到防病毒连接器时、请使用此名称。DNS应该能够为连接到防病毒连接器的每个专用LIF返回一个唯一的名称。

> 如果Vscan流量的LIF配置在与客户端流量的LIF不同的端口上、则在发生端口故障时、Vscan LIF可能会故障转移到其他节点。此更改会使Vscan服务器无法从新节点访问、并且此节点上的文件操作的扫描通知将失败。验证Vscan服务器是否可通过节点上的至少一个LIF访问、以便它可以处理对该节点执行文件操作的扫描请求。

- 至少使用1GbE网络连接NetApp存储系统和Vscan服务器。
- 对于具有多个Vscan服务器的环境、请连接具有类似高性能网络连接的所有服务器。连接Vscan服务器可实现负载共享、从而提高性能。
- 对于远程站点和分支机构、NetApp建议使用本地Vscan服务器、而不是远程Vscan服务器、因为前者是实现高延迟的理想选择。如果考虑到成本因素、请使用笔记本电脑或PC进行中等程度的病毒防护。您可以通过共享卷或qtrees并从远程站点中的任何系统扫描它们来计划定期执行完整文件系统扫描。
- 使用多个Vscan服务器扫描SVM上的数据、以实现负载平衡和冗余。CIFS工作负载的数量以及生成的防病毒流量因SVM而异。监控存储控制器上的CIFS和病毒扫描延迟。监控结果随时间的变化趋势。如果由于Vscan服务器上的CPU或应用程序队列超过趋势阈值而导致CIFS延迟和病毒扫描延迟增加、则CIFS客户端可能会出现长时间等待。添加其他Vscan服务器
以分布负载。
- 安装最新版本的ONTAP防病毒连接器。
- 使防病毒引擎和定义保持最新。请咨询合作伙伴、了解有关更新频率的建议。
- 在多租户环境中、可以与多个SVM共享一个扫描程序池(Vscan服务器池)、但前提是Vscan服务器和SVM属于同一个域或受信任域。
- 受感染文件的防病毒软件策略应设置为"delete"或"隔离 区"、这是大多数防病毒供应商设置的默认值。如果"vscand-fileop-profile"设置为"write_only "、并且发现受感染的文件、则该文件将保留在共享中、并且可以打开、因为打开文件不会触发扫描。只有在关闭文件后、才会触发防病毒扫描。
- 。 `scan-engine timeout` 值应小于 `scanner-pool request-timeout` 价值。
如果设置为较高的值、则访问文件可能会延迟、并且最终可能会超时。

要避免这种情况、请配置 `scan-engine timeout` 比低5秒 `scanner-pool request-timeout` 价值。有关如何更改的说明，请参阅扫描引擎供应商的文档 `scan-engine timeout` 设置。。 `scanner-pool timeout` 可以在高级模式下使用以下命令并为提供适当的值来更改 `request-timeout` 参数：`vserver vscan scanner-pool modify`。

- 对于为实时扫描工作负载调整规模并需要使用按需扫描的环境、NetApp建议将按需扫描作业计划在非高峰时间进行、以避免现有防病毒基础架构产生额外负载。

要了解有关合作伙伴专用最佳实践的更多信息、请访问 "Vscan合作伙伴解决方案"。

在 SVM 上启用病毒扫描

必须先在 SVM 上启用病毒扫描，然后才能运行实时或按需扫描。

步骤

1. 在 SVM 上启用病毒扫描：

   `vserver vscan enable -vserver data_SVM`

   > 您可以使用 `vserver vscan disable` 命令以禁用病毒扫描(如果需要)。

   以下命令将在上启用病毒扫描 `vs1` SVM：

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. 验证是否已在 SVM 上启用病毒扫描：

   `vserver vscan show -vserver data_SVM`

   有关完整的选项列表，请参见命令手册页。

   以下命令将显示的Vscan状态 `vs1` SVM：

   ```
   cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                         Vscan Status: on
   ```

重置已扫描文件的状态

有时、您可能需要使用重置SVM上已成功扫描文件的扫描状态 `vserver vscan reset` 命令以丢弃文件的缓存信息。例如，如果扫描配置不当，您可能需要使用此命令重新启动病毒扫描处理。

关于此任务

运行之后 `vserver vscan reset` 命令时、所有符合条件的文件都会在下次访问时进行扫描。

此命令可能会对性能产生不利影响，具体取决于要重新扫描的文件的数量和大小。

您将需要什么

此任务需要高级权限。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 重置已扫描文件的状态：

   ```
   vserver vscan reset -vserver data_SVM
   ```

   以下命令将在上重置已扫描文件的状态 `vs1` SVM：

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

查看 Vscan 事件日志信息

您可以使用 `vserver vscan show-events` 命令以查看有关受感染文件、Vscan服务器更新等的事件日志信息。您可以查看集群或给定节点， SVM 或 Vscan 服务器的事件信息。

开始之前

要查看Vscan事件日志、需要高级权限。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 查看 Vscan 事件日志信息：

   ```
   vserver vscan show-events
   ```

   有关完整的选项列表，请参见命令手册页。

   以下命令显示集群的事件日志信息 `cluster1`：

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

监控连接问题并对其进行故障排除

与 **scan-mandatory** 选项相关的潜在连接问题

您可以使用 `vserver vscan connection-status show` 用于查看有关Vscan服务器连接的信息的命令、您可能会发现这些信息有助于对连接问题进行故障排除。

默认情况下、 `scan-mandatory` 当Vscan服务器连接不可用于扫描时、实时扫描选项会拒绝文件访问。虽然此选项提供了重要的安全功能，但在某些情况下可能会导致问题。

- 在启用客户端访问之前，您必须确保至少有一个 Vscan 服务器连接到每个具有 LIF 的节点上的 SVM 。如果在启用客户端访问后需要将服务器连接到SVM、则必须关闭 `scan-mandatory` 选项、以确保文件访问不会因Vscan服务器连接不可用而被拒绝。连接服务器后，您可以重新打开此选项。
- 如果目标 LIF 托管 SVM 的所有 Vscan 服务器连接，则迁移 LIF 后，服务器与 SVM 之间的连接将丢失。要确保不会因Vscan服务器连接不可用而拒绝文件访问、必须关闭 `scan-mandatory` 选项。迁移 LIF 后，您可以重新启用此选项。

每个 SVM 应至少分配两个 Vscan 服务器。最佳做法是，通过与客户端访问不同的网络将 Vscan 服务器连接到存储系统。

用于查看 **Vscan** 服务器连接状态的命令

您可以使用 `vserver vscan connection-status show` 用于查看有关Vscan服务器连接状态的摘要和详细信息的命令。

如果您要 ...	输入以下命令 ...
查看 Vscan 服务器连接的摘要	`vserver vscan connection-status show`
查看 Vscan 服务器连接的详细信息	`vserver vscan connection-status show-all`

如果您要 ...	输入以下命令 ...
查看已连接 Vscan 服务器的详细信息	`vserver vscan connection-status show-connected`
查看未连接的可用 Vscan 服务器的详细信息	`vserver vscan connection-status show-not-connected`

有关这些命令的详细信息，请参见 "ONTAP 手册页"。

对病毒扫描进行故障排除

对于常见的病毒扫描问题、可能的原因和解决方法是存在的。病毒扫描也称为Vscan。

问题描述	如何解决
Vscan服务器无法连接到集群模式ONTAP存储系统。	检查扫描程序池配置是否指定Vscan服务器IP地址。同时检查扫描程序池列表中允许的有权限用户是否处于活动状态。要检查扫描程序池、请运行 `vserver vscan scanner-pool show` 命令。如果Vscan服务器仍无法连接、则网络中可能存在问题描述。
客户端存在高延迟。	现在可能是向扫描程序池添加更多Vscan服务器的时候了。
触发的扫描次数过多。	修改的值 `vscan-fileop-profile` 用于限制因病毒扫描而监控的文件操作数的参数。
未扫描某些文件。	检查实时策略。这些文件的路径可能已添加到路径排除列表中、或者其大小超过为排除项配置的值。要检查实时策略、请运行 `vserver vscan on-access-policy show` 命令。
文件访问被拒绝。	检查是否在策略配置中指定了_scAN-MANUALIANDE_SETTING_设置。如果未连接Vscan服务器、则此设置将拒绝数据访问。根据需要修改设置。

监控状态和性能活动

您可以监控Vscan模块的关键方面、例如Vscan服务器连接状态、Vscan服务器的运行状况以及已扫描的文件数。此信息将有所帮助您可以诊断与Vscan服务器相关的问题。

查看**Vscan**服务器连接信息

您可以查看Vscan服务器的连接状态、以管理已在使用的连接以及可供使用的连接。各种命令可显示信息

关于Vscan服务器的连接状态。

命令…	显示的信息…
`vserver vscan connection-status show`	连接状态摘要
`vserver vscan connection-status show-all`	有关连接状态的详细信息
`vserver vscan connection-status show-not-connected`	可用但未连接的连接的状态
`vserver vscan connection-status show-connected`	有关已连接Vscan服务器的信息

有关这些命令的详细信息，请参见 "手册页"。

查看**Vscan**服务器统计信息

您可以查看Vscan服务器专用的统计信息、以监控性能并诊断与相关的问题
病毒扫描。您必须先收集数据样本、然后才能使用 `statistics show` 命令
显示Vscan服务器统计信息。
要完成数据样本、请完成以下步骤：

步骤

1. 运行 `statistics start` 命令和 `optional statistics` 停止命令。

查看有关**Vscan**服务器请求和持续时间的统计信息

您可以使用ONTAP `offbox_vscan` 每个SVM上的计数器、用于监控Vscan速率
每秒分派和接收的服务器请求以及所有Vscan的服务器时间
服务器。要查看这些统计信息、请完成以下步骤：

步骤

1. 运行统计信息show `object offbox_vscan -instance SVM` 命令
以下计数器：

计数器…	显示的信息…
`scan_request_dispatched_rate`	每秒从ONTAP发送到Vscan服务器的病毒扫描请求数
`scan_noti_received_rate`	ONTAP每秒从Vscan服务器收到的病毒扫描请求数
`dispatch_latency`	ONTAP中用于确定可用Vscan服务器并将请求发送到该Vscan服务器的延迟

scan_latency	从ONTAP到Vscan服务器的往返延迟、包括扫描运行时间

从**ONTAP**机下**vscan**计数器生成的统计信息示例

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
---------------------------------------------------------------
```

查看单个**Vscan**服务器请求和持续时间的统计信息

您可以使用ONTAP `offbox_vscan_server` 每个SVM、每个机下Vscan服务器上的计数器、并按节点监控已分派Vscan服务器请求的速率以及上的服务器延迟每个Vscan服务器单独。要收集此信息、请完成以下步骤：

步骤

1. 运行 `statistics show -object offbox_vscan -instance SVM:servername:nodename` 命令和以下计数器：

计数器…	显示的信息…
scan_request_dispatched_rate	从ONTAP发送的病毒扫描请求数
scan_latency	从ONTAP到Vscan服务器的往返延迟、包括扫描运行时间 每秒Vscan服务器数

ONTAP offbox_vscan_server计数器生成的统计信息示例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

查看**Vscan**服务器利用率的统计信息

您也可以使用ONTAP `offbox_vscan_server` 用于收集Vscan服务器端利用率的计数器统计信息。这些统计信息会按每个SVM、每个机下Vscan服务器和每个节点进行跟踪。他们包括Vscan服务器上的CPU利用率、Vscan服务器上扫描操作的队列深度(当前和最大)、已用内存和已用网络。
这些统计信息由防病毒连接器转发到ONTAP中的统计信息计数器。他们基于每20秒轮询一次的数据、为确保准确性、必须收集多次；否则、统计信息中显示的值仅反映上次轮询。CPU利用率和队列为尤其需要进行监控和分析。平均队列的值较高表示Vscan服务器存在瓶颈。
收集每个SVM上的Vscan服务器、每个机下Vscan服务器和每个节点的利用率统计信息请完成以下步骤：

步骤

1. 收集Vscan服务器的利用率统计信息

   运行 `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` 命令 `offbox_vscan_server` 计数器：

计数器…	显示的信息…
`scanner_stats_pct_cpu_used`	Vscan服务器上的CPU利用率
`scanner_stats_pct_input_queue_avg`	Vscan服务器上扫描请求的平均队列
`scanner_stats_pct_input_queue_hiwatermark`	Vscan服务器上扫描请求的峰值队列
`scanner_stats_pct_mem_used`	Vscan服务器上使用的内存
`scanner_stats_pct_network_used`	Vscan服务器上使用的网络

Vscan服务器利用率统计信息示例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------------
```

审核 SVM 上的 NAS 事件

SMB 和 NFS 审核和安全跟踪

您可以将 SMB 和 NFS 协议可用的文件访问审核功能与 ONTAP 结合使用，例如，使用 FPolicy 进行原生审核和文件策略管理。

在以下情况下，您应设计并实施 SMB 和 NFS 文件访问事件审核：

- 已配置基本 SMB 和 NFS 协议文件访问。
- 您希望使用以下方法之一创建和维护审核配置：
  - 原生 ONTAP 功能
  - 外部 FPolicy 服务器

审核 SVM 上的 NAS 事件

审核NAS事件是一种安全措施、可用于跟踪和记录Storage Virtual Machine (SVM)上的某些SMB和NFS事件。这有助于您跟踪潜在的安全问题，并提供任何安全违规的证据。您还可以暂存和审核 Active Directory 中央访问策略，以查看实施这些策略的结果。

SMB事件

您可以审核以下事件：

- SMB 文件和文件夹访问事件

  您可以审核存储在属于已启用审核的 SVM 的 FlexVol 卷上的对象上的 SMB 文件和文件夹访问事件。

- SMB登录和注销事件

  您可以审核SVM上SMB服务器的SMB登录和注销事件。

- 中央访问策略暂存事件

  您可以使用通过建议的中央访问策略应用的权限审核SMB服务器上对象的有效访问。通过对中央访问策略的暂存进行审核，您可以在部署之前查看中央访问策略的影响。

  中央访问策略暂存的审核是使用 Active Directory GPO 设置的；但是，必须配置 SVM 审核配置以审核中央访问策略暂存事件。

  虽然您可以在审核配置中启用中央访问策略暂存、而无需在SMB服务器上启用动态访问控制、但只有在启用动态访问控制后、才会生成中央访问策略暂存事件。动态访问控制可通过SMB服务器选项启用。默认情况下，不会启用此功能。

NFS事件

您可以对SVM上存储的对象使用NFSv4 ACL来审核文件和目录事件。

审核的工作原理

基本审核概念

要了解 ONTAP 中的审核，您应了解一些基本的审核概念。

- * 暂存文件 *

  整合和转换前存储审核记录的各个节点上的中间二进制文件。暂存文件包含在暂存卷中。

- * 暂存卷 *

  ONTAP 创建的用于存储暂存文件的专用卷。每个聚合有一个暂存卷。暂存卷由所有启用了审核的 Storage Virtual Machine （ SVM ）共享，用于存储该特定聚合中数据卷的数据访问审核记录。每个 SVM 的审核记录都存储在暂存卷中的一个单独目录中。

  集群管理员可以查看有关暂存卷的信息，但不允许执行大多数其他卷操作。只有 ONTAP 才能创建暂存卷。ONTAP 会自动为暂存卷分配一个名称。所有暂存卷名称均以开头 `MDV_aud_` 后跟包含该暂存卷的聚合的UUID (例如： `MDV_aud_1d0131843d4811e296fc123478563412`）

- * 系统卷 *

  包含特殊元数据的 FlexVol 卷，例如文件服务审核日志的元数据。管理 SVM 拥有系统卷，这些卷可在集群中显示。暂存卷是一种系统卷。

- * 整合任务 *

  启用审核时创建的任务。在每个 SVM 上运行的这一长时间任务会从 SVM 的成员节点上的暂存文件中获取审核记录。此任务将按时间顺序合并审核记录，然后将其转换为审核配置中指定的用户可读事件日志格式—evtx 或 XML 文件格式。转换后的事件日志存储在 SVM 审核配置中指定的审核事件日志目录中。

ONTAP 审核过程的工作原理

ONTAP 审核过程与 Microsoft 审核过程不同。在配置审核之前，您应了解 ONTAP 审核过程的工作原理。

审核记录最初存储在各个节点上的二进制暂存文件中。如果在 SVM 上启用了审核，则每个成员节点都会保留该 SVM 的暂存文件。它们会定期进行整合并转换为用户可读的事件日志，这些日志存储在 SVM 的审核事件日志目录中。

在 SVM 上启用审核时的过程

只能在 SVM 上启用审核。当存储管理员对 SVM 启用审核时，审核子系统会检查是否存在暂存卷。包含 SVM 所拥有的数据卷的每个聚合都必须存在一个暂存卷。如果不存在任何所需的暂存卷，则审核子系统会创建这些卷。

在启用审核之前，审核子系统还会完成其他前提条件任务：

- 审核子系统会验证日志目录路径是否可用且不包含符号链接。

  日志目录必须已作为路径存在于 SVM 的命名空间中。建议创建一个新卷或 qtree 来存放审核日志文件。审核子系统不会分配默认日志文件位置。如果在审核配置中指定的日志目录路径无效、则创建审核配置将失败、并显示 `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` 错误。

  如果目录存在但包含符号链接，则配置创建将失败。

- 审核会计划整合任务。

  计划此任务后，将启用审核。SVM审核配置和日志文件会在重新启动后或者NFS或SMB服务器停止或重新启动后保留下来。

事件日志整合

日志整合是一项计划的任务，在禁用审核之前会例行运行。禁用审核后，整合任务将验证所有剩余日志是否已整合。

有保障的审核

默认情况下，保证审核。ONTAP 保证记录所有可审核的文件访问事件（由配置的审核策略 ACL 指定），即使节点不可用也是如此。在将请求的文件操作的审核记录保存到永久性存储上的暂存卷之前，无法完成该操作。如果由于空间不足或其他问题而无法将审核记录提交到暂存文件中的磁盘，则会拒绝客户端操作。

> 管理员或具有权限级别访问权限的帐户用户可以使用 NetApp 易管理性 SDK 或 REST API 绕过文件审核日志记录操作。您可以通过查看中存储的命令历史记录日志来确定是否已使用NetApp易管理性SDK或REST API执行任何文件操作 `audit.log` 文件
>
> 有关命令历史记录审核日志的详细信息，请参见中的 " 管理管理活动的审核日志记录 " 一节 "系统管理"。

节点不可用时的整合过程

如果包含已启用审核的 SVM 中的卷的节点不可用，则审核整合任务的行为取决于节点的存储故障转移（

Storage Failover ， SFO ）配对节点（如果是双节点集群，则为 HA 配对节点）是否可用：

- 如果暂存卷可通过 SFO 配对节点使用，则会扫描最后从节点报告的暂存卷，并且整合将正常进行。
- 如果 SFO 配对节点不可用，则此任务将创建一个部分日志文件。

  如果某个节点不可访问，则整合任务会整合该 SVM 中其他可用节点的审核记录。要确定该操作未完成、此任务将添加后缀 `.partial` 到整合文件名。

- 当不可用节点可用后，该节点中的审核记录将与当时其他节点的审核记录整合在一起。
- 所有审核记录均会保留。

事件日志轮换

当审核事件日志文件达到已配置的阈值日志大小或按已配置的计划时，这些文件会进行轮换。轮换事件日志文件后，计划的整合任务会首先将活动转换的文件重命名为带时间戳的归档文件，然后创建一个新的活动转换的事件日志文件。

在 **SVM** 上禁用审核时的过程

在 SVM 上禁用审核后，将最后触发整合任务。记录的所有未完成审核记录均以用户可读格式记录。在 SVM 上禁用审核并可供查看时，不会删除存储在事件日志目录中的现有事件日志。

整合该 SVM 的所有现有暂存文件后，整合任务将从计划中删除。禁用 SVM 的审核配置不会删除审核配置。存储管理员可以随时重新启用审核。

启用审核时创建的审核整合作业会监控整合任务，如果整合任务因错误而退出，则会重新创建该任务。用户无法删除审核整合作业。

审核要求和注意事项

在 Storage Virtual Machine （ SVM ）上配置和启用审核之前，您需要了解某些要求和注意事项。

- 支持的已启用审核的SVM的最大数量取决于您的ONTAP版本：

ONTAP 版本	最大值
9.8及更早版本	50.
9.9.1 及更高版本	400

- 审核与SMB或NFS许可无关。

  即使集群上未安装SMB和NFS许可证、您也可以配置和启用审核。

- NFS 审核支持安全 ACE （ U 型）。
- 对于 NFS 审核，模式位与审核 ACE 之间没有映射。

  将 ACL 转换为模式位时，将跳过 ACE 审核。将模式位转换为 ACL 时，不会生成对 ACE 的审核。

- 审核配置中指定的目录必须存在。

如果不存在，则用于创建审核配置的命令将失败。

- 在审核配置中指定的目录必须满足以下要求：
  - 目录不能包含符号链接。

    如果在审核配置中指定的目录包含符号链接，则用于创建审核配置的命令将失败。

  - 必须使用绝对路径指定目录。

    您不应指定相对路径、例如 `/vs1/../`。

- 审核取决于暂存卷中是否有可用空间。

  您必须了解并计划确保包含已审核卷的聚合中有足够的空间用于暂存卷。

- 审核取决于卷中的可用空间，该卷包含已转换事件日志的存储目录。

  您必须了解并计划确保卷中有足够的空间用于存储事件日志。您可以使用指定要保留在审核目录中的事件日志数量 `-rotate-limit` 参数、此参数有助于确保卷中的事件日志具有足够的可用空间。

- 虽然您可以在审核配置中启用中央访问策略暂存、而无需在SMB服务器上启用动态访问控制、但要生成中央访问策略暂存事件、必须启用动态访问控制。

  默认情况下，不会启用动态访问控制。

启用审核时的聚合空间注意事项

创建审核配置并在集群中至少一个 Storage Virtual Machine （ SVM ）上启用审核后，审核子系统将在所有现有聚合以及创建的所有新聚合上创建暂存卷。在集群上启用审核时，您需要了解某些聚合空间注意事项。

由于聚合中的空间不可用，暂存卷创建可能会失败。如果您创建了审核配置，而现有聚合没有足够的空间来容纳暂存卷，则可能会发生这种情况。

在 SVM 上启用审核之前，应确保现有聚合上有足够的空间用于暂存卷。

暂存文件上审核记录大小的限制

暂存文件上的审核记录大小不能大于 32 KB 。

何时可能会出现大量审核记录

在以下情况之一的管理审核期间，可能会出现大量审核记录：

- 向具有大量用户的组添加或删除用户。
- 在具有大量文件共享用户的文件共享上添加或删除文件共享访问控制列表（ ACL ）。
- 其他情形。

禁用管理审核以避免此问题描述。为此，请修改审核配置并从审核事件类型列表中删除以下内容：

- 文件共享

- 用户帐户
- 安全组
- authorization-policy-change

  删除后，文件服务审核子系统将不会审核它们。

审核记录过大的影响

- 如果审核记录的大小过大（超过 32 KB ），则不会创建审核记录，而审核子系统会生成类似于以下内容的事件管理系统（ EMS ）消息：

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  如果保证审核，则文件操作将失败，因为无法创建其审核记录。

- 如果审核记录的大小超过 9 ， 999 字节，则会显示与上述相同的 EMS 消息。此时将创建一个部分审核记录，其中缺少较大的密钥值。
- 如果审核记录超过 2 ， 000 个字符，则会显示以下错误消息，而不是实际值：

  ```
  The value of this field was too long to display.
  ```

支持的审核事件日志格式是什么

转换后的审核事件日志支持的文件格式为 EVTX 和 XML 文件格式。

您可以在创建审核配置时指定文件格式的类型。默认情况下、ONTAP会将二进制日志转换为 EVTX 文件格式。

查看审核事件日志

您可以使用审核事件日志来确定您是否具有足够的文件安全性，以及是否有不正确的文件和文件夹访问尝试。您可以查看和处理保存在中的审核事件日志 EVTX 或 XML 文件格式。

- EVTX 文件格式

  您可以打开已转换的 EVTX 使用Microsoft事件查看器将事件日志作为已保存文件进行审核。

  使用事件查看器查看事件日志时，可以使用两个选项：

  - 常规视图

    系统将为此事件记录显示所有事件通用的信息。在此版本的 ONTAP 中，不会显示事件记录的特定于事件的数据。您可以使用详细视图显示事件特定的数据。

  - 详细视图

    提供友好的视图和 XML 视图。友好视图和 XML 视图可显示所有事件的通用信息以及事件记录的事件特

定数据。

- XML 文件格式

  您可以查看和处理 XML 支持的第三方应用程序上的审核事件日志 XML 文件格式。如果您具有 XML 架构以及 XML 字段定义的相关信息，则可以使用 XML 查看工具查看审核日志。有关 XML 架构和定义的详细信息，请参见 "《 ONTAP 审核架构参考》"。

如何使用事件查看器查看活动审核日志

如果审核整合过程正在集群上运行，则整合过程会将新记录附加到启用了审核的 Storage Virtual Machine （ SVM ）的活动审核日志文件中。可以在 Microsoft 事件查看器中通过 SMB 共享访问和打开此活动审核日志。

除了查看现有审核记录之外，事件查看器还提供了一个刷新选项，可用于刷新控制台窗口中的内容。是否可以在事件查看器中查看新附加的日志，取决于用于访问活动审核日志的共享是否已启用机会锁。

共享上的机会锁设置	行为
enabled	事件查看器将打开日志，其中包含截至该时间点写入到该日志中的事件。刷新操作不会刷新日志并附加整合过程中的新事件。
已禁用	事件查看器将打开日志，其中包含截至该时间点写入到该日志中的事件。刷新操作会使用整合过程附加的新事件刷新日志。

> 此信息仅适用于 EVTX 事件日志。 XML 可以在浏览器中通过SMB查看事件日志、也可以使用任何XML编辑器或查看器通过NFS查看事件日志。

可审核的 SMB 事件

可审核的 SMB 事件概述

ONTAP 可以审核某些 SMB 事件，包括某些文件和文件夹访问事件，某些登录和注销事件以及中央访问策略暂存事件。了解可以审核哪些访问事件有助于解释事件日志中的结果。

可以在 ONTAP 9.2 及更高版本中审核以下其他 SMB 事件：

事件 ID （ EVT/EVTX ）	事件	Description	类别
4670	对象权限已更改	对象访问：权限已更改。	文件访问
4907年	对象审核设置已更改	对象访问：审核设置已更改。	文件访问
4913.	对象中央访问策略已更改	对象访问： CAP 已更改。	文件访问

可以在 ONTAP 9.0 及更高版本中审核以下 SMB 事件：

事件 ID （EVT/EVTX）	事件	Description	类别
540/4624.	已成功登录帐户	登录/注销：网络(SMB)登录。	登录和注销
529/4625.	帐户无法登录	logon/logoff ： 用户名未知或密码错误。	登录和注销
530/4625	帐户无法登录	logon/logoff ： 帐户登录时间限制。	登录和注销
531/4625.	帐户无法登录	logon/logoff ： 帐户当前已禁用。	登录和注销
532/4625.	帐户无法登录	登录 / 注销：用户帐户已过期。	登录和注销
533/4625.	帐户无法登录	logon/logoff ： 用户无法登录到此计算机。	登录和注销
534/4625.	帐户无法登录	logon/logoff ： 此处未授予用户登录类型。	登录和注销
535/4625.	帐户无法登录	登录 / 注销：用户密码已过期。	登录和注销
5374625.	帐户无法登录	logon/logoff ： 由于上述原因，登录失败。	登录和注销
539/4625.	帐户无法登录	logon/logoff ： 帐户已锁定。	登录和注销
534/4634	已注销帐户	登录 / 注销：本地或网络用户注销。	登录和注销
560/4656	打开对象 / 创建对象	对象访问：打开对象（文件或目录）。	文件访问
563/4659.	打开要删除的对象	对象访问：已请求对对象（文件或目录）的句柄，其目的是删除。	文件访问
564/4660	删除对象	对象访问：删除对象（文件或目录）。当 Windows 客户端尝试删除对象（文件或目录）时， ONTAP 会生成此事件。	文件访问

567/463.	读取对象 / 写入对象 / 获取对象属性 / 设置对象属性	对象访问：对象访问尝试（读取，写入，获取属性，设置属性）。 • 注意： * 对于此事件， ONTAP 仅审核对象的第一个 SMB 读取和第一个 SMB 写入操作（成功或失败）。这样，当一个客户端打开一个对象并对同一个对象执行多次连续读写操作时， ONTAP 就不会创建过多的日志条目。	文件访问
NA/4664	硬链接	对象访问：尝试创建硬链接。	文件访问
NA/4818	建议的中央访问策略不会授予与当前中央访问策略相同的访问权限	对象访问：中央访问策略暂存。	文件访问
不适用 Data ONTAP 事件 ID 9999	重命名对象	对象访问：对象已重命名。这是一个 ONTAP 事件。目前， Windows 不支持将其作为单个事件。	文件访问
不适用/不适用Data ONTAP事件ID 9998	取消对象链接	对象访问：对象未链接。这是一个 ONTAP 事件。目前， Windows 不支持将其作为单个事件。	文件访问

追加信息关于事件 **4656**

。 `HandleID` 标记 `XML` event包含所访问对象(文件或目录)的句柄。。 `HandleID` 根据打开的事件是用于创建新对象还是用于打开现有对象、evtx 4656事件的标记包含不同的信息：

- 如果打开事件是创建新对象(文件或目录)的打开请求、则 `HandleID` 审核XML事件中的标记显示为空 `HandleID` (例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

  。 `HandleID` 为空、因为在实际创建对象之前和句柄存在之前、系统会审核打开(用于创建新对象)请求。同一对象的后续审核事件在中具有正确的对象句柄 `HandleID` 标记。

- 如果此打开事件是打开现有对象的OPEN请求、则此审核事件将在中为该对象分配句柄 `HandleID` 标记(例如： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>` ）。

确定已审核对象的完整路径

打印在中的对象路径 `<ObjectName>` 审核记录的标记包含卷的名称(用圆括号括起)以及从所属卷的根目录开始的相对路径。如果要确定已审核对象的完整路径，包括接合路径，则必须执行某些步骤。

步骤

1. 通过查看来确定卷名称以及经过审核的对象的相对路径 `<ObjectName>` 审核事件中的标记。

在此示例中、卷名称为`data1`、文件的相对路径为 `/dir1/file.txt`：

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

2. 使用上一步中确定的卷名称，确定包含已审核对象的卷的接合路径：

   在此示例中、卷名称为`data1`、包含已审核对象的卷的接合路径为 `/data/data1`：

   ```
   volume show -junction -volume data1
   ```

   ```
                                   Junction                      Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. 通过附加中的相对路径来确定经过审核的对象的完整路径 `<ObjectName>` 标记到卷的接合路径。

   在此示例中，卷的接合路径为：

   ```
   /data/data1/dir1/file.text
   ```

审核符号链接和硬链接时的注意事项

审核符号链接和硬链接时，必须牢记某些注意事项。

审核记录包含有关要审核的对象的信息、包括中标识的已审核对象的路径 `ObjectName` 标记。您应了解符号链接和硬链接的路径如何记录在中 `ObjectName` 标记。

符号链接

符号链接是一个具有单独索引节点的文件，其中包含指向目标对象（称为目标）位置的指针。通过符号链接访问对象时， ONTAP 会自动解释符号链接，并遵循卷中目标对象的实际不受规范协议限制的路径。

在以下示例输出中、有两个符号链接、它们都指向一个名为的文件 `target.txt`。其中一个符号链接是相对符号链接，一个符号链接是绝对符号链接。如果审核了其中任何一个符号链接、则 `ObjectName` 审核事件中的标记包含文件的路径 `target.txt`：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

硬链接

硬链接是指将名称与文件系统上的现有文件关联的目录条目。硬链接指向原始文件的索引节点位置。与 ONTAP 解释符号链接的方式类似， ONTAP 解释硬链接并遵循卷中目标对象的实际规范路径。审核对硬链接对象的访问时、审核事件会在中记录此绝对规范路径 `ObjectName` 标记、而不是硬链接路径。

审核备用 **NTFS** 数据流时的注意事项

在使用 NTFS 备用数据流审核文件时，必须牢记某些注意事项。

要审核的对象的位置会使用两个标记(即)记录在事件记录中 `ObjectName` 标记(路径)和 `HandleID` 标记(手柄)。要正确识别正在记录的流请求，您必须了解 NTFS 备用数据流的以下字段中的 ONTAP 记录：

- evtx ID： 4656 个事件（打开和创建审核事件）
  - 备用数据流的路径将记录在中 `ObjectName` 标记。
  - 备用数据流的句柄记录在中 `HandleID` 标记。
- evtx ID： 4663 个事件（所有其他审核事件，例如读取，写入， getattr 等）
  - 基础文件的路径(而不是备用数据流)会记录在中 `ObjectName` 标记。
  - 备用数据流的句柄记录在中 `HandleID` 标记。

示例

以下示例说明了如何使用确定备用数据流的evtx ID：4663个事件 `HandleID` 标记。即使 `ObjectName` 读取审核事件中记录的标记(路径)指向基本文件路径、即 `HandleID` 标记可用于将事件标识为备用数据流的审核记录。

流文件名采用以下格式 `base_file_name:stream_name`。在此示例中、将显示 `dir1` 目录包含一个基础文件、其中包含一个备用数据流、其路径如下：

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> 以下事件示例中的输出将被截断，如图所示；输出不会显示事件的所有可用输出标记。

对于evtx ID 4656 (打开审核事件)、备用数据流的审核记录输出将在中记录备用数据流名称 `ObjectName` 标记：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

对于evtx ID 4663 (读取审核事件)、同一备用数据流的审核记录输出将在中记录基本文件名 `ObjectName` 标记；但是、中的句柄 `HandleID` 标记是备用数据流的句柄、可用于将此事件与备用数据流相关联：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

可以审核的 **NFS** 文件和目录访问事件

ONTAP 可以审核某些 NFS 文件和目录访问事件。了解可以审核哪些访问事件有助于解释转换后的审核事件日志的结果。

您可以审核以下 NFS 文件和目录访问事件：

- 读取
- 打开
- 关闭
- 添加项
- 写入
- SETATTR
- 创建
- 链接。
- 操作
- 删除
- getattr
- 验证
- n 验证
- 重命名

要可靠地审核 NFS 重命名事件，您应在目录而不是文件上设置审核 ACE ，因为如果目录权限足够，则不会检查文件权限以执行重命名操作。

规划审核配置

在 Storage Virtual Machine （ SVM ）上配置审核之前，您必须了解哪些配置选项可用，并规划要为每个选项设置的值。此信息可帮助您配置满足业务需求的审核配置。

某些配置参数对于所有审核配置都是通用的。

此外，您还可以使用某些参数来指定在轮换整合和转换的审核日志时使用的方法。配置审核时，您可以指定以下三种方法之一：

- 根据日志大小轮换日志

  这是用于轮换日志的默认方法。

- 根据计划轮换日志
- 根据日志大小和计划轮换日志（以先发生的事件为准）
  F

> 应始终至少设置一种日志轮换方法。

所有审核配置通用的参数

创建审核配置时，必须指定两个必需参数。此外，您还可以指定三个可选参数。

信息类型	选项	Required	包括	您的价值
_SVM 名称 _ 要创建审核配置的 SVM 的名称。此 SVM 必须已存在。	`-vserver vserver_name`	是的。	是的。	
日志目标路径 _ 指定用于存储转换后的审核日志的目录，通常为专用卷或 qtree 。此路径必须已存在于 SVM 命名空间中。 路径长度最多可包含 864 个字符，并且必须具有读写权限。 如果路径无效，审核配置命令将失败。 如果 SVM 是 SVM 灾难恢复源，则日志目标路径不能位于根卷上。这是因为根卷内容不会复制到灾难恢复目标。 不能将 FlexCache 卷用作日志目标（ONTAP 9.7 及更高版本）。	`-destination text`	是的。	是的。	

要审核的事件的类别 _ 指定要审核的事件的类别。可以审核以下事件类别： • 文件访问事件（ SMB 和 NFSv4 ） • SMB登录和注销事件 • 中央访问策略暂存事件 从Windows 2012 Active Directory域开始、可以使用中央访问策略暂存事件。 • 文件共享类别事件 • 审核策略更改事件 • 本地用户帐户管理事件 • 安全组管理事件 • 授权策略更改事件 默认情况下会审核文件访问以及SMB登录和注销事件。 *注意：*在指定之前 `cap-staging` 作为事件类别、SVM上必须存在SMB服务器。虽然您可以在审核配置中启用中央访问策略暂存、而无需在SMB服务器上启用动态访问控制、但只有在启用动态访问控制后、才会生成中央访问策略暂存事件。动态访问控制可通过SMB服务器选项启用。默认情况下，不会启用此功能。	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change}`	否

		日志文件输出格式 _ 确定审核日志的输出格式。输出格式可以是特定于ONTAP的格式之一 XML 或Microsoft Windows EVTX 日志格式。默认情况下、输出格式为 EVTX。	-format {xml	evtx}
否			日志文件轮换限制 _ 确定在将最旧的日志文件转出之前要保留的审核日志文件数。例如、如果输入的值为 5，则会保留最后五个日志文件。 的值 0 指示保留所有日志文件。默认值为0。	-rotate -limit integer

用于确定何时轮换审核事件日志的参数

- 根据日志大小轮换日志 *

默认情况下，会根据大小轮换审核日志。

- 默认日志大小为 100 MB 。
- 如果要使用默认日志轮换方法和默认日志大小，则无需为日志轮换配置任何特定参数。
- 如果要仅根据日志大小轮换审核日志、请使用以下命令取消设置 `-rotate-schedule-minute` 参数：`vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

如果不想使用默认日志大小、则可以配置 `-rotate-size` 用于指定自定义日志大小的参数：

信息类型	选项	Required	包括	您的价值
日志文件大小限制 _ 确定审核日志文件大小限制。	`-rotate-size` {`integer`[KB	MB	GB	TB

- 根据计划轮换日志 *

如果您选择根据计划轮换审核日志，则可以通过使用基于时间的轮换参数的任意组合来计划日志轮换。

- 如果使用基于时间的旋转、则 `-rotate-schedule-minute` 参数为必填项。
- 所有其他基于时间的轮换参数均为可选参数。
- 轮换计划使用所有与时间相关的值进行计算。

  例如、如果仅指定 `-rotate-schedule-minute` 参数、审核日志文件将根据一周中所有日期指定的分钟数在一年中所有月份的所有时间内进行轮换。

- 如果您仅指定一个或两个基于时间的旋转参数(例如、 `-rotate-schedule-month` 和 `-rotate -schedule-minutes`)、日志文件将根据您在一周中的所有日期指定的分钟值进行轮换、在所有时间内、但仅在指定月份内。

  例如，您可以指定在 1 月， 3 月和 8 月期间，在所有星期一，星期三和星期六的上午 10： 30 轮换审核日志

- 指定这两者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`、它们会独立考虑。

  例如、如果指定 `-rotate-schedule-dayofweek` 作为星期五和 `-rotate-schedule-day` 如果为13、则审核日志将在每个星期五和指定月份的第13天轮换、而不仅仅是在每个星期五的第13天轮换。

- 如果要仅根据计划轮换审核日志、请使用以下命令取消设置 `-rotate-size` 参数： `vserver audit modify -vserver vs0 -destination / -rotate-size -`

您可以使用以下可用审核参数列表来确定用于配置审核事件日志轮换计划的值：

信息类型	选项	Required	包括	您的价值

日志轮换计划： month_ 确定轮换审核日志的每月计划。 有效值为 `January` 到 `December`，和 `all`。例如，您可以指定在 1 月， 3 月和 8 月期间轮换审核日志。	`-rotate-schedule-month chron_month`	否		
日志轮换计划：星期几 _ 确定轮换审核日志的每日（星期几）计划。 有效值为 `Sunday` 到 `Saturday`，和 `all`。例如，您可以指定在星期二和星期五或一周的所有日期轮换审核日志。	`-rotate-schedule -dayofweek chron_dayofweek`	否		
日志轮换计划： day_ 确定轮换审核日志的每月计划日期。 有效值范围为 `1` 到 `31`。例如，您可以指定在一个月的第 10 天和第 20 天或一个月的所有日期轮换审核日志。	`-rotate-schedule-day chron_dayofmonth`	否		
日志轮换计划： hour_ 确定轮换审核日志的每小时计划。 有效值范围为 `0` (午夜)至 `23` (晚上11：00)。指定 `all` 每小时轮换一次审核日志。例如，您可以指定在 6 （早上 6 点）和 18 （下午 6 点）轮换审核日志。	`-rotate-schedule-hour chron_hour`	否		
日志轮换计划： minute_ 确定轮换审核日志的分钟计划。 有效值范围为 `0` to `59`。例如，您可以指定在 30 分钟轮换审核日志。	`-rotate-schedule-minute chron_minute`	是，如果配置基于计划的日志轮换；否则，否		

- 根据日志大小和计划轮换日志 *

您可以通过同时设置来选择根据日志大小和计划轮换日志文件 `-rotate-size` 参数和基于时间的旋转参数的任意组合。例如：if `-rotate-size` 设置为10 MB、然后 `-rotate-schedule-minute` 设置为15时、日志文件将在日志文件大小达到10 MB时或每小时的15分钟(以先发生的事件为准)轮换。

在 SVM 上创建文件和目录审核配置

创建审核配置

在 Storage Virtual Machine （ SVM ）上创建文件和目录审核配置包括了解可用的配置选项，规划配置以及配置和启用配置。然后，您可以显示有关审核配置的信息，以确认生成的配置是所需的配置。

在开始审核文件和目录事件之前，必须在 Storage Virtual Machine （ SVM ）上创建审核配置。

开始之前

如果您计划为中央访问策略暂存创建审核配置、则SVM上必须存在SMB服务器。

- 虽然您可以在审核配置中启用中央访问策略暂存、而无需在SMB服务器上启用动态访问控制、但只有在启用动态访问控制后、才会生成中央访问策略暂存事件。

  动态访问控制可通过SMB服务器选项启用。默认情况下，不会启用此功能。

- 如果命令中某个字段的参数无效，例如字段的条目无效，条目重复以及条目不存在，则此命令将在审核阶段之前失败。

  此类故障不会生成审核记录。

关于此任务

如果 SVM 是 SVM 灾难恢复源，则目标路径不能位于根卷上。

步骤

1. 使用规划工作表中的信息，创建审核配置以根据日志大小或计划轮换审核日志：

审核日志轮换方式	输入 …
日志大小	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
计划	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

示例

以下示例将创建一个审核配置、该配置使用基于大小的轮换来审核文件操作以及SMB登录和注销事件(默认设置

)。日志格式为 EVTX (默认值)。日志存储在中 /audit_log 目录。日志文件大小限制为 200 MB。日志大小达到 200 MB 时会进行轮换。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

以下示例将创建一个审核配置、该配置使用基于大小的轮换来审核文件操作以及SMB登录和注销事件(默认设置)。日志格式为 EVTX (默认值)。日志存储在中 /cifs_event_logs 目录。日志文件大小限制为 100 MB (默认值)、日志轮换限制为 5：

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

以下示例将创建一个审核配置，该配置使用基于时间的轮换来审核文件操作， CIFS 登录和注销事件以及中央访问策略暂存事件。日志格式为 EVTX (默认值)。审核日志每月在中午 12： 30 轮换一次在一周的所有日期。日志轮换限制为 5：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

在 **SVM** 上启用审核

设置完审核配置后，必须在 Storage Virtual Machine （ SVM ）上启用审核。

您需要的内容

SVM 审核配置必须已存在。

关于此任务

首次启动 SVM 灾难恢复 ID 丢弃配置（在 SnapMirror 初始化完成后）且 SVM 具有审核配置时， ONTAP 会自动禁用审核配置。在只读 SVM 上禁用审核，以防止暂存卷填满。只有在 SnapMirror 关系中断且 SVM 为读写状态后，才能启用审核。

步骤

1. 在 SVM 上启用审核：

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

验证审核配置

完成审核配置后，您应验证是否已正确配置并启用审核。

步骤

1. 验证审核配置：

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   以下命令以列表形式显示 Storage Virtual Machine （ SVM ） vs1 的所有审核配置信息：

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                                Vserver: vs1
                       Auditing state: true
                 Log Destination Path: /audit_log
        Categories of Events to Audit: file-ops
                            Log Format: evtx
                   Log File Size Limit: 200MB
         Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                    Rotation Schedules: -
             Log Files Rotation Limit: 0
   ```

配置文件和文件夹审核策略

配置文件和文件夹审核策略

对文件和文件夹访问事件实施审核是一个两步过程。首先，您必须在 Storage Virtual Machine （ SVM ）上创建并启用审核配置。其次，必须对要监控的文件和文件夹配置审核策略。您可以配置审核策略以监控成功和失败的访问尝试。

您可以配置 SMB 和 NFS 审核策略。SMB 和 NFS 审核策略具有不同的配置要求和审核功能。

如果配置了适当的审核策略，则只有在 SMB 或 NFS 服务器正在运行时， ONTAP 才会按照审核策略中的指定监控 SMB 和 NFS 访问事件。

在 **NTFS** 安全模式文件和目录上配置审核策略

在审核文件和目录操作之前，您必须在要收集审核信息的文件和目录上配置审核策略。这是对设置和启用审核配置的补充。您可以使用 Windows 安全性选项卡或 ONTAP 命令行界面配置 NTFS 审核策略。

使用 **Windows** 安全性选项卡配置 **NTFS** 审核策略

您可以使用 Windows 属性窗口中的 * Windows 安全性 * 选项卡在文件和目录上配置 NTFS 审核策略。这与为驻留在 Windows 客户端上的数据配置审核策略时使用的方法相同，通过此方法，您可以使用您习惯使用的相同 GUI 界面。

您需要的内容

必须在包含要应用系统访问控制列表（ SACL ）的数据的 Storage Virtual Machine （ SVM ）上配置审核。

关于此任务

配置 NTFS 审核策略的方法是，向与 NTFS 安全描述符关联的 NTFS SACL 添加条目。然后，安全描述符将应用于 NTFS 文件和目录。这些任务由 Windows 图形用户界面自动处理。安全描述符可以包含用于应用文件和文件夹访问权限的随机访问控制列表（ DACL ），用于文件和文件夹审核的 SACL ，或者同时包含 SACL 和 DACL 。

要使用 Windows 安全性选项卡设置 NTFS 审核策略，请在 Windows 主机上完成以下步骤：

步骤

1. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 * 。
2. 完成 * 映射网络驱动器 * 框：

   a. 选择一个 * 驱动器 * 字母。

   b. 在*Folder*框中，键入包含共享的SMB服务器名称，其中包含要审核的数据以及共享的名称。

      您可以指定SMB服务器数据接口的IP地址、而不是SMB服务器名称。

      如果SMB服务器名称为`SMB_Server`、而共享名为`shre1`、则应输入 `\\SMB_SERVER\share1`。

   c. 单击 * 完成 * 。

   您选择的驱动器已挂载并准备就绪，此时将显示 Windows 资源管理器窗口，其中显示共享中包含的文件和文件夹。

3. 选择要为其启用审核访问的文件或目录。
4. 右键单击文件或目录，然后选择 * 属性 * 。
5. 选择 * 安全性 * 选项卡。
6. 单击 * 高级 * 。
7. 选择 * 审核 * 选项卡。
8. 执行所需的操作：

如果您要 …	执行以下操作：
为新用户或组设置审核	a. 单击 * 添加 * 。 b. 在输入对象名称以选择框中，键入要添加的用户或组的名称。 c. 单击 * 确定 * 。
从用户或组中删除审核	a. 在输入对象名称以选择框中，选择要删除的用户或组。 b. 单击 * 删除 * 。 c. 单击 * 确定 * 。 d. 跳过此操作步骤的其余部分。

更改用户或组的审核	a. 在输入对象名称以选择框中，选择要更改的用户或组。 b. 单击 * 编辑 * 。 c. 单击 * 确定 * 。

如果要对用户或组设置审核，或者更改现有用户或组的审核，则会打开 "<objecy> 的审核条目 " 框。

9. 在 * 应用于 * 框中，选择要如何应用此审核条目。

   您可以选择以下选项之一：

   - * 此文件夹，子文件夹和文件 *
   - * 此文件夹和子文件夹 *
   - * 仅此文件夹 *
   - * 此文件夹和文件 *
   - * 仅限子文件夹和文件 *
   - * 仅限子文件夹 *
   - 仅限文件
     如果要对单个文件设置审核，应用于*框不会处于活动状态。" 应用于 * " 框设置默认为 "* 仅此对象 * " 。

     由于审核会占用 SVM 资源，因此请仅选择可提供符合安全要求的审核事件的最低级别。

10. 在 * 访问 * 框中，选择要审核的内容以及要审核成功事件，失败事件还是同时审核这两者。

    - 要审核成功的事件，请选中成功框。
    - 要审核失败事件，请选中故障框。

      请仅选择您需要监控的操作以满足安全要求。有关这些可审核事件的详细信息，请参见 Windows 文档。
      您可以审核以下事件：

    - * 完全控制 *
    - * 遍历文件夹 / 执行文件 *
    - * 列出文件夹 / 读取数据 *
    - * 读取属性 *
    - * 读取扩展属性 *
    - * 创建文件 / 写入数据 *
    - * 创建文件夹 / 附加数据 *
    - * 写入属性 *
    - * 写入扩展属性 *
    - * 删除子文件夹和文件 *
    - * 删除 *
    - * 读取权限 *

- * 更改权限 *
- * 取得所有权 *

11. 如果不希望审核设置传播到原始容器的后续文件和文件夹，请选中 * 仅将这些审核条目应用于此容器中的对象和 / 或容器 * 框。
12. 单击 * 应用 * 。
13. 添加，删除或编辑完审核条目后，单击 * 确定 * 。

    此时， <objece> 的审核条目框将关闭。

14. 在 * 审核 * 框中，选择此文件夹的继承设置。

    请仅选择提供符合安全要求的审核事件的最低级别。您可以选择以下选项之一：

    - 选中包括此对象父级的可继承审核条目框。
    - 选中使用从此对象继承的审核条目替换所有后代上所有现有的可继承审核条目框。
    - 选择这两个框。
    - 不选择任何一个框。
      如果要在单个文件上设置 SACL ，则 " 审核 " 框中不会显示 " 将所有后代上的所有现有可继承审核条目替换为此对象的可继承审核条目 " 框。

15. 单击 * 确定 * 。

    此时将关闭审核框。

使用 **ONTAP** 命令行界面配置 **NTFS** 审核策略

您可以使用 ONTAP 命令行界面对文件和文件夹配置审核策略。这样，您就可以配置 NTFS 审核策略，而无需在 Windows 客户端上使用 SMB 共享连接到数据。

您可以使用配置NTFS审核策略 `vserver security file-directory` 命令系列。

您只能使用命令行界面配置 NTFS SACL 。此 ONTAP 命令系列不支持配置 NFSv4 SACL 。有关使用这些命令配置 NTFS SACL 并将其添加到文件和文件夹的详细信息，请参见手册页。

配置 **UNIX** 安全模式文件和目录的审核

您可以通过向 NFSv4.x ACL 添加审核 ACE 来配置 UNIX 安全模式文件和目录的审核。这样，您就可以出于安全目的监控某些 NFS 文件和目录访问事件。

关于此任务

对于 NFSv4.x ，随机 ACE 和系统 ACE 都存储在同一 ACL 中。它们不会存储在单独的 DACL 和 SACL 中。因此，在向现有 ACL 添加审核 ACE 时必须谨慎，以避免覆盖和丢失现有 ACL 。将审核 ACE 添加到现有 ACL 的顺序无关紧要。

步骤

1. 使用检索文件或目录的现有ACL `nfs4_getfacl` 或等效命令。

   有关操作 ACL 的详细信息，请参见 NFS 客户端的手册页。

2. 附加所需的审核 ACE 。
3. 使用将更新后的ACL应用于文件或目录 `nfs4_setfacl` 或等效命令。

显示有关应用于文件和目录的审核策略的信息

使用 **Windows** 安全性选项卡显示有关审核策略的信息

您可以使用 Windows 属性窗口中的安全性选项卡显示已应用于文件和目录的审核策略的信息。这与驻留在 Windows 服务器上的数据使用的方法相同，这样客户就可以使用他们习惯使用的相同图形用户界面。

关于此任务

通过显示应用于文件和目录的审核策略信息，您可以验证是否已在指定文件和文件夹上设置了适当的系统访问控制列表（ SACL ）。

要显示已应用于 NTFS 文件和文件夹的 SACL 的信息，请在 Windows 主机上完成以下步骤。

步骤

1. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 * 。
2. 完成 * 映射网络驱动器 * 对话框：
   a. 选择一个 * 驱动器 * 字母。
   b. 在*文件夹*框中，键入Storage Virtual Machine (SVM)的IP地址或SMB服务器名称，该共享包含要审核的数据和共享名称。

      如果SMB服务器名称为`SMB_Server`、而共享名为`shre1`、则应输入 `\\SMB_SERVER\share1`。

      > 您可以指定SMB服务器数据接口的IP地址、而不是SMB服务器名称。

   c. 单击 * 完成 * 。

   您选择的驱动器已挂载并准备就绪，此时将显示 Windows 资源管理器窗口，其中显示共享中包含的文件和文件夹。
3. 选择要显示其审核信息的文件或目录。
4. 右键单击文件或目录，然后选择 * 属性 * 。
5. 选择 * 安全性 * 选项卡。
6. 单击 * 高级 * 。
7. 选择 * 审核 * 选项卡。
8. 单击 * 继续 * 。

   此时将打开审核框。"* 审核条目 * " 框显示应用了 SACL 的用户和组的摘要。
9. 在 * 审核条目 * 框中，选择要显示其 SACL 条目的用户或组。
10. 单击 * 编辑 * 。

此时将打开 "<objecy> 的审核条目 " 框。

11. 在 * 访问 * 框中，查看应用于选定对象的当前 SACL 。
12. 单击 * 取消 * 以关闭 * 审核条目 < 对象 >* 框。
13. 单击 * 取消 * 关闭 * 审核 * 框。

使用命令行界面显示有关 **FlexVol** 卷上 **NTFS** 审核策略的信息

您可以显示有关 FlexVol 卷上的 NTFS 审核策略的信息，包括什么是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表的信息。您可以使用这些信息验证安全配置或对审核问题进行故障排除。

关于此任务

通过显示应用于文件和目录的审核策略信息，您可以验证是否已在指定文件和文件夹上设置了适当的系统访问控制列表（ SACL ）。

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其审核信息的文件或文件夹的路径。您可以摘要形式或详细列表形式显示输出。

- 对于审核策略， NTFS 安全模式卷和 qtree 仅使用 NTFS 系统访问控制列表（ SACL ）。
- 具有 NTFS 有效安全性的混合安全模式卷中的文件和文件夹可以应用 NTFS 审核策略。

  混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NTFS SACL 。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件和文件夹 NFSv4 SACL 以及存储级别访问防护 NTFS SACL 。
- 如果在命令中输入的路径指向采用 NTFS 有效安全模式的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。
- 显示有关具有 NTFS 有效安全性的文件和文件夹的安全信息时，与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。

  在确定文件访问权限时， NTFS 安全模式文件和文件夹仅使用 NTFS 文件权限以及 Windows 用户和组。

- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。

步骤

1. 显示具有所需详细级别的文件和目录审核策略设置：

要显示信息的项	输入以下命令 …

摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
作为详细列表	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示了路径的审核策略信息 `/corp` 在SVM VS1中。此路径具有 NTFS 有效安全性。NTFS 安全描述符包含成功和成功 / 失败 SACL 条目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

以下示例显示了路径的审核策略信息 `/datavol1` 在SVM VS1中。此路径包含常规文件和文件夹 SACL 以及存储级别访问防护 SACL 。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

显示有关文件安全性和审核策略信息的方式

您可以使用通配符（*）显示有关给定路径或根卷下所有文件和目录的文件安全和审核策略的信息。

通配符（*）可用作给定目录路径的最后一个子组件，在该路径下，您希望显示所有文件和目录的信息。

如果要显示名为 "*" 的特定文件或目录的信息，则需要在双引号（""）中提供完整路径。

示例

以下带有通配符的命令显示路径下所有文件和目录的信息 `/1/` SVM VS1：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
               Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
               Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

以下命令显示路径下名为"*"的文件的信息 `/vol1/a` SVM VS1。路径用双引号括起来（""）。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

可审核的 **CLI** 更改事件

可审核的 **CLI** 更改事件概述

ONTAP 可以审核某些命令行界面更改事件，包括某些 SMB 共享事件，某些审核策略事件，某些本地安全组事件，本地用户组事件和授权策略事件。了解可以审核哪些变更事件有助于解释事件日志中的结果。

您可以通过手动轮换审核日志，启用或禁用审核，显示有关审核更改事件的信息，修改审核更改事件以及删除审核更改事件来管理 Storage Virtual Machine （ SVM ）审核 CLI 更改事件。

作为管理员，如果您执行任何命令来更改与 SMB 共享，本地用户组，本地安全组，授权策略和审核策略事件相关的配置， 生成记录并审核相应的事件：

审核类别	事件	事件 IDs	运行此命令 …
Mhost 审核	策略更改	[4719] Audit configuration changed	`vserver audit disable
enable	modify`	文件共享	[5142] Network share was add得

vserver cifs share create	[5143] Network share was modified	vserver cifs share modify `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] Network share deleted	vserver cifs share delete
审核	用户帐户	[4720] 已创建本地用户	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722] 已启用本地用户	`vserver cifs users-and-groups local-user create	modify`	[4724] 本地用户密码重置
vserver cifs users-and-groups local-user set-password	[4725] 已禁用本地用户	`vserver cifs users-and-groups local-user create	modify`
[4726] 本地用户已删除	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] Local user Change.	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
【4781】本地用户重命名	vserver cifs users-and-groups local-user rename	安全组	【4731】已创建本地安全组
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734] Local Security Group deleted	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735] Local Security Group Modified
`vserver cifs users-and-groups local-group rename	modify` vserver services name-service unix-group modify	[4732] 已将用户添加到本地组	vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser

[4733] 已从本地组中删除此用户	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	authorization-policy-change	【4704】已分配用户权限
`vserver cifs users-and-groups privilege add-privilege`	【4705】已删除用户权限	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

管理文件共享事件

如果为 Storage Virtual Machine （SVM）配置了文件共享事件并启用了审核，则会生成审核事件。使用修改SMB网络共享时会生成文件共享事件 `vserver cifs share` 相关命令。

在为 SVM 添加，修改或删除 SMB 网络共享时，将生成事件 ID 为 5142 ， 5143 和 5144 的文件共享事件。可使用修改SMB网络共享配置 `cifs share access control create|modify|delete` 命令

以下示例显示了在创建名为 "audit_dest" 的共享对象时生成的文件共享事件， ID 为 5143：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

管理审核策略更改事件

为 Storage Virtual Machine （SVM）配置审核策略更改事件并启用审核后，将生成审核事件。使用修改审核策略时会生成audy-policy-change事件 `vserver audit` 相关命令。

无论何时禁用，启用或修改审核策略，都会生成事件 ID 为 4719 的审核策略更改事件，此事件有助于确定用户何时尝试禁用审核以覆盖这些跟踪。默认情况下，它已配置，需要诊断权限才能禁用。

以下示例显示了禁用审核时生成的审核策略更改事件， ID 为 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

管理用户帐户事件

如果为 Storage Virtual Machine （ SVM ）配置了用户帐户事件并启用了审核，则会生成审核事件。

事件ID为4720、4722、4724、4725、4726的用户帐户事件 在系统中创建或删除本地SMB或NFS用户、启用、禁用或修改本地用户帐户以及重置或更改本地SMB用户密码时、将生成4738和4781。使用修改用户帐户时会生成用户帐户事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令

以下示例显示创建本地SMB用户时生成ID为4720的用户帐户事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

以下示例显示了重命名在上述示例中创建的本地SMB用户时生成的ID为4781的用户帐户事件：

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

管理安全组事件

如果为 Storage Virtual Machine （ SVM ）配置了安全组事件并启用了审核，则会生成审核事件。

在系统中创建或删除本地SMB或NFS组时、系统会生成事件ID为4731、4732、4733、4734和4735的安全组事件、并在组中添加或删除本地用户。使用修改用户帐户时会生成secure-group-Events `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令

以下示例显示了创建本地 UNIX 安全组时生成的 ID 为 4731 的安全组事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

管理 **authorization-policy-change** 事件

如果为 Storage Virtual Machine （ SVM ）配置了 authorization-policy-change 事件并启用了审核，则会生成审核事件。

每当为 SMB 用户和 SMB 组授予或撤消授权权限时，都会生成事件 ID 为 4704 和 4705 的 authorization-policy-change 事件。使用分配或撤消授权权限时、将生成authorize-policy-change事件 `vserver cifs users-and-groups privilege` 相关命令。

以下示例显示了分配 SMB 用户组授权权限时生成的授权策略事件， ID 为 4704 ：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

管理审核配置

手动轮换审核事件日志

在查看审核事件日志之前，必须将日志转换为用户可读格式。如果要在 ONTAP 自动轮换日志之前查看特定 Storage Virtual Machine （ SVM ）的事件日志，则可以手动轮换 SVM 上的审核事件日志。

步骤

1. 使用轮换审核事件日志 `vserver audit rotate-log` 命令：

   ```
   vserver audit rotate-log -vserver vs1
   ```

   审核事件日志以审核配置指定的格式保存在SVM审核事件日志目录中 (`XML` 或 `EVTX`)、可使用相应的应用程序进行查看。

在 **SVM** 上启用和禁用审核

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用审核。您可能希望通过禁用审核来暂时停止文件和目录审核。您可以随时启用审核（如果存在审核配置）。

您需要的内容

在 SVM 上启用审核之前， SVM 的审核配置必须已存在。

"创建审核配置"

关于此任务

禁用审核不会删除审核配置。

步骤

1. 执行相应的命令：

审核条件	输入命令 ...
enabled	`vserver audit enable -vserver vserver_name`
已禁用	`vserver audit disable -vserver vserver_name`

2. 验证审核是否处于所需状态：

```
vserver audit show -vserver vserver_name
```

示例

以下示例将为 SVM vs1 启用审核：

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

以下示例将禁用 SVM vs1 的审核：

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                       Auditing state: false
                 Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                            Log Format: evtx
                   Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 10
```

显示有关审核配置的信息

您可以显示有关审核配置的信息。这些信息可帮助您确定每个 SVM 的配置是否符合您的要求。通过显示的信息，您还可以验证是否已启用审核配置。

关于此任务

您可以显示有关所有 SVM 上审核配置的详细信息，也可以通过指定可选参数来自定义输出中显示的信息。如果未指定任何可选参数，则会显示以下内容：

- 审核配置所应用的 SVM 名称
- 审核状态、可以是 `true` 或 `false`

  如果审核状态为 `true`，已启用审核。如果审核状态为 `false`，已禁用审核。

- 要审核的事件的类别
- 审核日志格式
- 审核子系统用于存储整合和转换的审核日志的目标目录

步骤

1. 使用显示有关审核配置的信息 `vserver audit show` 命令：

   有关使用命令的详细信息，请参见手册页。

示例

以下示例显示了所有 SVM 的审核配置摘要：

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

以下示例以列表形式显示所有 SVM 的所有审核配置信息：

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 0
```

用于修改审核配置的命令

如果要更改审核设置，您可以随时修改当前配置，包括修改日志路径目标和日志格式，修改要审核的事件类别，如何自动保存日志文件以及指定要保存的最大日志文件数。

如果您要 ...	使用此命令 ...
修改日志目标路径	`vserver audit modify` 使用 `-destination` 参数
修改要审核的事件类别	`vserver audit modify` 使用 `-events` 参数 要审核中央访问策略暂存事件、必须在Storage Virtual Machine (SVM)上启用动态访问控制(DAC) SMB服务器选项。
修改日志格式	`vserver audit modify` 使用 `-format` 参数

根据内部日志文件大小启用自动保存	`vserver audit modify` 使用 `-rotate-size` 参数
根据时间间隔启用自动保存	`vserver audit modify` 使用 `-rotate-schedule-month`， `-rotate-schedule-dayofweek`， `-rotate-schedule-day`， `-rotate-schedule-hour`，和 `-rotate-schedule-minute` parameters
指定已保存日志文件的最大数量	`vserver audit modify` 使用 `-rotate-limit` 参数

删除审核配置

在中，您不再需要审核 Storage Virtual Machine （ SVM ）上的文件和目录事件，也不希望在 SVM 上保留审核配置，您可以删除审核配置。

步骤

1. 禁用审核配置：

   ```
   vserver audit disable -vserver vserver_name
   ```

   ```
   vserver audit disable -vserver vs1
   ```

2. 删除审核配置：

   ```
   vserver audit delete -vserver vserver_name
   ```

   ```
   vserver audit delete -vserver vs1
   ```

了解还原集群的含义

如果您计划还原集群，则应注意，当集群中存在启用了审核的 Storage Virtual Machine （ SVM ）时， ONTAP 会遵循以下还原过程。还原之前，必须执行某些操作。

还原到不支持审核**SMB**登录和注销事件以及中央访问策略暂存事件的**ONTAP**版本

从集群模式Data ONTAP 8.3开始、支持审核SMB登录和注销事件以及中央访问策略暂存事件。如果要还原到不支持这些事件类型的 ONTAP 版本，并且您的审核配置监控这些事件类型，则必须在还原之前更改已启用审核的 SVM 的审核配置。您必须修改配置，以便仅审核文件操作事件。

对审核和暂存卷空间问题进行故障排除

如果暂存卷或包含审核事件日志的卷上没有足够的空间，则可能会出现问题。如果空间不足，则无法创建新的审核记录，从而阻止客户端访问数据，并且访问请求将失败。您应了解如何对这些卷空间问题进行故障排除和解决。

对与事件日志卷相关的空间问题进行故障排除

如果包含事件日志文件的卷用尽空间，审核将无法将日志记录转换为日志文件。这会导致客户端访问失败。您必须了解如何对与事件日志卷相关的空间问题进行故障排除。

- Storage Virtual Machine （ SVM ）和集群管理员可以通过显示有关卷和聚合使用情况和配置的信息来确定卷空间是否不足。
- 如果包含事件日志的卷空间不足， SVM 和集群管理员可以通过删除某些事件日志文件或增加卷大小来解决空间问题。

> 如果包含事件日志卷的聚合已满，则必须先增加聚合的大小，然后才能增加卷的大小。只有集群管理员才能增加聚合的大小。

- 可以通过修改审核配置将事件日志文件的目标路径更改为另一个卷上的目录。

> 在以下情况下，数据访问被拒绝：
>
> - 删除目标目录时。
> - 如果托管目标目录的卷上的文件限制达到其最大级别。

详细了解：

- "如何查看有关卷和增加卷大小的信息"。
- "如何查看有关聚合和管理聚合的信息"。

对与暂存卷相关的空间问题进行故障排除

如果包含 Storage Virtual Machine （ SVM ）暂存文件的任何卷用尽空间，审核将无法将日志记录写入暂存文件。这会导致客户端访问失败。要对此问题描述进行故障排除，您需要通过显示有关卷使用情况的信息来确定 SVM 中使用的任何暂存卷是否已满。

如果包含整合事件日志文件的卷具有足够的空间，但由于空间不足仍存在客户端访问失败的情况，则暂存卷可能会空间不足。SVM 管理员必须与您联系，以确定包含 SVM 暂存文件的暂存卷是否空间不足。如果由于暂存卷空间不足而无法生成审核事件，则审核子系统将生成 EMS 事件。此时将显示以下消息： `No space left on device`。只有您才能查看暂存卷的相关信息； SVM 管理员无法查看此信息。

所有暂存卷名称均以开头 `MDV_aud_` 后跟该暂存卷所在聚合的UUID。以下示例显示了管理 SVM 上的四个系统卷，这些系统卷是在为集群中的数据 SVM 创建文件服务审核配置时自动创建的：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

如果暂存卷中的空间不足，您可以通过增加卷的大小来解决空间问题。

> 如果包含暂存卷的聚合已满，则必须先增加聚合的大小，然后才能增加卷的大小。只有您才能增加聚合的大小； SVM 管理员无法增加聚合的大小。

如果一个或多个聚合的可用空间小于 2 GB ，则 SVM 审核创建将失败。如果 SVM 审核创建失败，则已创建的暂存卷将被删除。

使用 FPolicy 在 SVM 上监控和管理文件

了解FPolicy

什么是 FPolicy 解决方案的两个部分

FPolicy是一个文件访问通知框架、用于通过合作伙伴解决方案监控和管理Storage Virtual Machine (SVM)上的文件访问事件。合作伙伴解决方案可帮助您应对各种用例、例如数据监管与合规性、勒索软件保护和数据移动性。

合作伙伴解决方案包括NetApp支持的第三方解决方案和NetApp产品工作负载安全性和云数据感知。

FPolicy 解决方案分为两部分。ONTAP FPolicy框架可管理集群上的活动、并向合作伙伴应用程序(也称为外部FPolicy服务器)发送通知。外部FPolicy服务器处理ONTAP FPolicy发送的通知、以满足客户使用情形的要求。

ONTAP 框架可创建和维护 FPolicy 配置，监控文件事件并向外部 FPolicy 服务器发送通知。ONTAP FPolicy 提供的基础架构允许外部 FPolicy 服务器与 Storage Virtual Machine （ SVM ）节点之间进行通信。

当由于客户端访问而发生某些文件系统事件时， FPolicy 框架会连接到外部 FPolicy 服务器，并向 FPolicy 服务

器发送有关这些事件的通知。外部 FPolicy 服务器会处理通知并将响应发送回节点。由于通知处理而发生的情况取决于应用程序以及节点与外部服务器之间的通信是异步还是同步。

什么是同步和异步通知

FPolicy 会通过 FPolicy 接口向外部 FPolicy 服务器发送通知。通知以同步或异步模式发送。通知模式可确定 ONTAP 在向 FPolicy 服务器发送通知后执行的操作。

- * 异步通知 *

  使用异步通知时，节点不会等待 FPolicy 服务器的响应，从而提高系统的整体吞吐量。此类通知适用于 FPolicy 服务器不要求在评估通知后执行任何操作的应用程序。例如，当 Storage Virtual Machine （ SVM ）管理员希望监控和审核文件访问活动时，会使用异步通知。

  如果在异步模式下运行的 FPolicy 服务器发生网络中断，则在中断期间生成的 FPolicy 通知将存储在存储节点上。当 FPolicy 服务器恢复联机时，它会收到存储的通知警报，并可从存储节点提取这些通知。在中断期间可以存储通知的时间长度可配置为长达 10 分钟。

  从ONTAP 9.14.1开始、您可以通过FPolicy设置永久性存储、以捕获SVM中异步非强制策略的文件访问事件。永久性存储有助于将客户端I/O处理与FPolicy通知处理分离、以减少客户端延迟。不支持同步(强制或非强制)和异步强制配置。

- * 同步通知 *

  如果配置为在同步模式下运行，则 FPolicy 服务器必须确认每个通知，然后才能继续执行客户端操作。如果根据通知评估结果需要执行操作，则会使用此类型的通知。例如，当 SVM 管理员希望根据外部 FPolicy 服务器上指定的标准允许或拒绝请求时，将使用同步通知。

同步和异步应用程序

FPolicy 应用程序有许多可能的用途，包括异步和同步应用程序。

异步应用程序是指外部 FPolicy 服务器不会更改对文件或目录的访问权限或修改 Storage Virtual Machine （ SVM ）上的数据的应用程序。例如：

- 文件访问和审核日志记录
- 存储资源管理

同步应用程序是指外部 FPolicy 服务器更改数据访问或修改数据的应用程序。例如：

- 配额管理
- 文件访问阻止
- 文件归档和分层存储管理
- 加密和解密服务
- 数据压缩和解压缩服务

FPolicy持久存储

从ONTAP 9.14.1开始、您可以通过FPolicy设置永久性存储、以捕获SVM中异步非强制策

略的文件访问事件。永久性存储有助于将客户端I/O处理与FPolicy通知处理分离、以减少客户端延迟。不支持同步(强制或非强制)和异步强制配置。

此功能仅在FPolicy外部模式下可用。您使用的合作伙伴应用程序需要支持此功能。您应与合作伙伴合作、确保此FPolicy配置受支持。

最佳实践

集群管理员需要在启用了FPolicy的每个SVM上为永久性存储配置一个卷。配置后、永久性存储将捕获所有匹配的FPolicy事件、这些事件将在FPolicy管道中进行进一步处理并发送到外部服务器。

如果发生意外重新启动或FPolicy被禁用并再次启用、则持久存储将保持上次收到事件时的状态。接管操作完成后、配对节点将存储和处理新事件。在执行了恢复操作之后、永久性存储将恢复处理节点接管发生后可能仍存在的任何未处理事件。实时事件的优先级高于不经过处理的事件。

如果永久性存储卷从同一SVM中的一个节点移至另一个节点、则尚未处理的通知也将移至新节点。您需要重新运行 `fpolicy persistent-store create` 命令、以确保将待定通知传送到外部服务器。

永久性存储卷会按SVM进行设置。对于每个启用了FPolicy的SVM、您需要创建一个永久性存储卷。

在包含预期Fpolicy监控的最大流量的生命周期的节点上创建永久性存储卷。

如果持久性存储中累积的通知超过所配置卷的大小、FPolicy将开始删除传入通知并显示相应的EMS消息。

创建卷时指定的永久性存储卷名称和接合路径应匹配。

将Snapshot策略设置为 `none` 而不是 `default`。这是为了确保不会意外还原快照而导致当前事件丢失、并防止可能发生重复的事件处理。

使持久存储卷无法用于外部用户协议访问(CIFS或NFS)、以避免意外损坏或删除保留的事件记录。为此、在启用FPolicy后、请在ONTAP中卸载卷以删除接合路径、这样用户协议访问就无法访问该路径。

有关详细信息，请参见 "创建持久性存储"。

FPolicy 配置类型

有两种基本的 FPolicy 配置类型。一种配置使用外部 FPolicy 服务器处理通知并对通知采取措施。另一种配置不使用外部 FPolicy 服务器，而是使用 ONTAP 内部原生 FPolicy 服务器根据扩展来简单地阻止文件。

- * 外部 FPolicy 服务器配置 *

  此通知将发送到 FPolicy 服务器，该服务器会筛选请求并应用规则来确定节点是否应允许所请求的文件操作。对于同步策略， FPolicy 服务器会向节点发送响应，以允许或阻止请求的文件操作。

- * 原生 FPolicy 服务器配置 *

  通知将在内部进行筛选。根据在 FPolicy 范围中配置的文件扩展名设置，允许或拒绝此请求。

  注：不会记录被拒绝的文件扩展名请求。

何时创建原生 **FPolicy** 配置

原生 FPolicy 配置使用 ONTAP 内部 FPolicy 引擎根据文件扩展名监控和阻止文件操作。此解决方案不需要外部 FPolicy 服务器（ FPolicy 服务器）。如果只需使用此简单解决方案，则可以使用原生文件阻止配置。

通过原生文件阻止，您可以监控与配置的操作和筛选事件匹配的任何文件操作，然后拒绝访问具有特定扩展名的文件。这是默认配置。

此配置提供了一种仅根据文件扩展名阻止文件访问的方法。例如、阻止包含的文件 `mp3` 扩展名、则可以配置一个策略、以便为具有目标文件扩展名的某些操作提供通知 `mp3`。此策略配置为deny `mp3` 生成通知的操作的文件请求。

以下适用场景原生 FPolicy 配置：

- 原生文件阻止也支持基于 FPolicy 服务器的文件筛选所支持的同一组筛选器和协议。
- 可以同时配置原生文件阻止和基于 FPolicy 服务器的文件筛选应用程序。

  为此，您可以为 Storage Virtual Machine （ SVM ）配置两个单独的 FPolicy 策略，其中一个策略配置为阻止原生文件，另一个策略配置为基于 FPolicy 服务器的文件筛选。

- 原生文件阻止功能仅根据扩展名而不是文件内容对文件进行筛选。
- 对于符号链接，原生文件阻止使用根文件的文件扩展名。

了解更多信息 "FPolicy：原生 文件阻止"。

何时创建使用外部 **FPolicy** 服务器的配置

使用外部 FPolicy 服务器处理和管理通知的 FPolicy 配置可为需要基于文件扩展名进行简单文件阻止的使用情形提供强大的解决方案。

如果要执行以下操作，您应创建一个使用外部 FPolicy 服务器的配置：监控和记录文件访问事件，提供配额服务，根据简单文件扩展名以外的标准执行文件阻止，使用分层存储管理应用程序提供数据迁移服务， 或者，提供一组细化策略，这些策略仅监控 Storage Virtual Machine （ SVM ）中的一部分数据。

集群组件在 **FPolicy** 实施中发挥的角色

集群，包含的 Storage Virtual Machine （ SVM ）和数据 LIF 都在 FPolicy 实施中发挥作用。

- * 集群 *

  集群包含 FPolicy 管理框架，并维护和管理有关集群中所有 FPolicy 配置的信息。

- * SVM*

  FPolicy 配置在 SVM 级别定义。此配置的范围是 SVM ，它仅在 SVM 资源上运行。一个 SVM 配置不能监控针对驻留在另一个 SVM 上的数据发出的文件访问请求并发送通知。

  可以在管理 SVM 上定义 FPolicy 配置。在管理 SVM 上定义配置后，可以在所有 SVM 中查看和使用这些配置。

- * 数据 LIF*

通过属于具有 FPolicy 配置的 SVM 的数据 LIF 连接到 FPolicy 服务器。用于这些连接的数据 LIF 可以按照用于正常客户端访问的数据 LIF 的方式进行故障转移。

FPolicy 如何与外部 FPolicy 服务器配合使用

在 Storage Virtual Machine （ SVM ）上配置并启用 FPolicy 后， FPolicy 将在 SVM 参与的每个节点上运行。FPolicy 负责与外部 FPolicy 服务器（ FPolicy 服务器）建立和维护连接，处理通知以及管理与 FPolicy 服务器之间的通知消息。

此外，在连接管理中， FPolicy 还负责以下职责：

- 确保文件通知通过正确的 LIF 流向 FPolicy 服务器。
- 确保当多个 FPolicy 服务器与一个策略关联时，在向 FPolicy 服务器发送通知时会执行负载平衡。
- 在与 FPolicy 服务器的连接断开时尝试重新建立连接。
- 通过经过身份验证的会话向 FPolicy 服务器发送通知。
- 管理由 FPolicy 服务器建立的直通读取数据连接，以便在启用直通读取时为客户端请求提供服务。

如何使用控制通道进行 FPolicy 通信

FPolicy 会从 Storage Virtual Machine （ SVM ）上参与的每个节点的数据 LIF 启动与外部 FPolicy 服务器的控制通道连接。FPolicy 使用控制通道传输文件通知；因此，根据 SVM 拓扑， FPolicy 服务器可能会看到多个控制通道连接。

如何将有权限的数据访问通道用于同步通信

对于同步使用情形， FPolicy 服务器会通过特权数据访问路径访问驻留在 Storage Virtual Machine （ SVM ）上的数据。通过特权路径进行访问会将整个文件系统公开给 FPolicy 服务器。它可以访问数据文件来收集信息，扫描文件，读取文件或写入文件。

由于外部 FPolicy 服务器可以通过有权限的数据通道从 SVM 的根目录访问整个文件系统，因此有权限的数据通道连接必须安全。

FPolicy 连接凭据如何用于有权限的数据访问通道

FPolicy 服务器使用随 FPolicy 配置一起保存的特定 Windows 用户凭据来与集群节点建立有权限的数据访问连接。SMB 是唯一支持建立有权限的数据访问通道连接的协议。

如果 FPolicy 服务器需要特权数据访问，则必须满足以下条件：

- 集群上必须启用SMB许可证。
- FPolicy 服务器必须在 FPolicy 配置中配置的凭据下运行。

建立数据通道连接时， FPolicy 会使用凭据作为指定的 Windows 用户名。通过管理共享 ontap_admin$ 进行数据访问。

为有权限的数据访问授予超级用户凭据的含义

ONTAP 使用在 FPolicy 配置中配置的 IP 地址和用户凭据的组合向 FPolicy 服务器授予超级用户凭据。

当 FPolicy 服务器访问数据时，超级用户状态会授予以下权限：

- 避免权限检查

  用户可避免检查文件和目录访问。

- 特殊锁定权限

  无论现有锁定如何， ONTAP 都允许对任何文件进行读取，写入或修改访问。如果 FPolicy 服务器对文件执行字节范围锁定，则会立即删除文件上的现有锁定。

- 绕过任何 FPolicy 检查

  访问不会生成任何 FPolicy 通知。

FPolicy 如何管理策略处理

可能会为 Storage Virtual Machine （ SVM ）分配多个 FPolicy 策略；每个策略的优先级各不相同。要在 SVM 上创建适当的 FPolicy 配置，请务必了解 FPolicy 如何管理策略处理。

系统会对每个文件访问请求进行初始评估，以确定哪些策略正在监控此事件。如果是受监控事件，则有关受监控事件的信息以及相关策略将传递到 FPolicy ，并在其中对其进行评估。系统将按分配的优先级顺序评估每个策略。

配置策略时，应考虑以下建议：

- 如果您希望某个策略始终在评估其他策略之前进行评估，请为该策略配置较高的优先级。
- 如果对受监控事件成功执行请求的文件访问操作是根据另一策略评估文件请求的前提条件，请为控制第一个文件操作成功或失败的策略指定较高的优先级。

  例如，如果一个策略管理 FPolicy 文件归档和还原功能，而另一个策略管理联机文件的文件访问操作， 管理文件还原的策略必须具有较高的优先级，以便在允许第二个策略管理的操作之前还原文件。

- 如果要评估可能应用于文件访问操作的所有策略，请为同步策略指定较低的优先级。

您可以通过修改策略序列号对现有策略的策略优先级重新排序。但是，要让 FPolicy 根据修改后的优先级顺序评估策略，您必须禁用并重新启用此策略并使用修改后的序列号。

什么是节点到外部 FPolicy 服务器通信过程

要正确规划 FPolicy 配置，您应了解节点到外部 FPolicy 服务器的通信过程是什么。

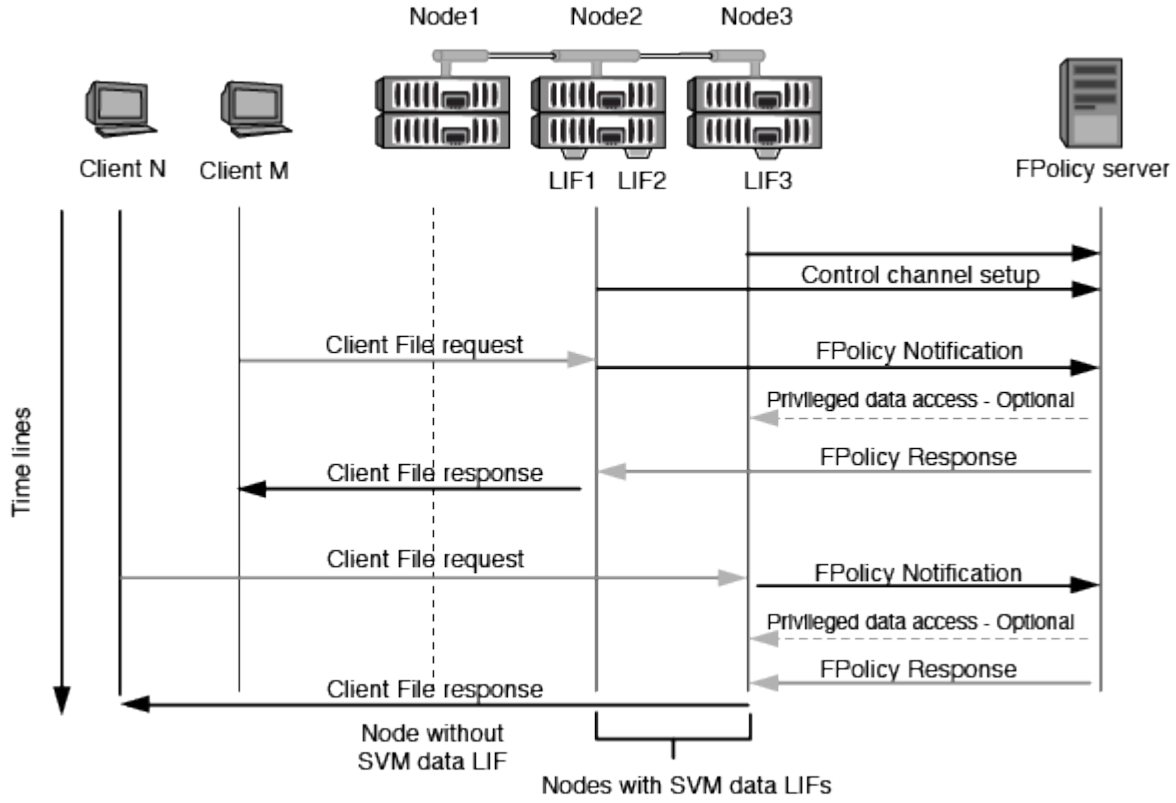
参与每个 Storage Virtual Machine （ SVM ）的每个节点都会使用 TCP/IP 启动与外部 FPolicy 服务器（ FPolicy 服务器）的连接。与 FPolicy 服务器的连接使用节点数据 LIF 进行设置；因此，只有当节点具有 SVM 的可操作数据 LIF 时，参与节点才能设置连接。

启用此策略后，参与节点上的每个 FPolicy 进程都会尝试与 FPolicy 服务器建立连接。它使用策略配置中指定的 FPolicy 外部引擎的 IP 地址和端口。

此连接将通过数据 LIF 从每个 SVM 上参与的每个节点建立一个控制通道，并连接到 FPolicy 服务器。此外，如果 IPv4 和 IPv6 数据 LIF 地址位于同一参与节点上，则 FPolicy 会尝试为 IPv4 和 IPv6 建立连接。因此，如果 SVM 扩展到多个节点，或者同时存在 IPv4 和 IPv6 地址，则在 SVM 上启用 FPolicy 策略后， FPolicy 服务器必

须已准备好处理来自集群的多个控制通道设置请求。

例如，如果集群有三个节点：节点 1 ，节点 2 和节点 3 ，并且 SVM 数据 LIF 仅分布在节点 2 和节点 3 上，则无论数据卷的分布如何，控制通道只会从节点 2 和节点 3 启动。假设 Node2 有两个属于 SVM 的数据 LIF - LIF1 和 LIF2 ，并且初始连接来自 LIF1 。如果 LIF1 发生故障， FPolicy 将尝试从 LIF2 建立控制通道。



FPolicy 如何在 **LIF** 迁移或故障转移期间管理外部通信

数据 LIF 可以迁移到同一节点中的数据端口或远程节点上的数据端口。

当数据 LIF 发生故障转移或迁移时，将与 FPolicy 服务器建立新的控制通道连接。然后， FPolicy 可以重试超时的 SMB 和 NFS 客户端请求，从而向外部 FPolicy 服务器发送新通知。节点拒绝 FPolicy 服务器对初始超时 SMB 和 NFS 请求的响应。

FPolicy 如何在节点故障转移期间管理外部通信

如果托管用于 FPolicy 通信的数据端口的集群节点发生故障， ONTAP 将中断 FPolicy 服务器与节点之间的连接。

可以通过配置故障转移策略将FPolicy通信中使用的数据端口迁移到另一个活动节点来缓解向FPolicy服务器进行集群故障转移所产生的影响。迁移完成后，将使用新的数据端口建立新的连接。

如果未将故障转移策略配置为迁移数据端口、则FPolicy服务器必须等待故障节点启动。节点启动后，将使用新会话 ID 从该节点启动新连接。

> FPolicy 服务器检测到连接断开并显示 Keep-alive 协议消息。清除会话 ID 的超时时间是在配置 FPolicy 时确定的。默认的保活超时为 2 分钟。

FPolicy 服务如何跨 **SVM** 命名空间工作

ONTAP 提供了一个统一的 Storage Virtual Machine （ SVM ）命名空间。集群中的卷通过接合连接在一起，以提供一个逻辑文件系统。FPolicy 服务器可以识别命名空间拓扑，并在命名空间中提供 FPolicy 服务。

此命名空间是 SVM 特有的，并且包含在 SVM 中；因此，您只能从 SVM 上下文中查看此命名空间。命名空间具有以下特征：

- 每个 SVM 中都有一个命名空间，命名空间的根是根卷，在命名空间中以斜杠（ / ）表示。
- 所有其他卷的接合点均位于根（ / ）下方。
- 卷接合对客户端是透明的。
- 一个 NFS 导出可以提供对整个命名空间的访问；否则，导出策略可以导出特定卷。
- SMB 共享可以在卷或卷中的 qtree 上创建，也可以在命名空间中的任何目录上创建。
- 命名空间架构非常灵活。

  典型命名空间架构的示例如下：

  - 根下具有一个分支的命名空间
  - 一个命名空间，其中包含多个根下的分支
  - 一个命名空间，其中包含多个从根部断开的卷

FPolicy 直通读取如何提高分层存储管理的可用性

通过直通读取， FPolicy 服务器（用作分层存储管理（ HSM ）服务器）可以对脱机文件进行读取访问，而无需将文件从二级存储系统重新调用到主存储系统。

如果将 FPolicy 服务器配置为向 SMB 服务器上的文件提供 HSM ，则会发生基于策略的文件迁移，其中，文件脱机存储在二级存储上，而只有存根文件保留在主存储上。即使存根文件在客户端中显示为普通文件，但它实际上是一个与原始文件大小相同的稀疏文件。稀疏文件设置了SMB脱机位、并指向已迁移到二级存储的实际文件。

通常，在收到脱机文件的读取请求时，必须将请求的内容重新调用回主存储，然后通过主存储进行访问。需要将数据重新调用回主存储会产生一些不希望出现的影响。其中一个不希望受到的影响是，由于需要在响应请求之前重新调用内容，客户端请求的延迟增加，并且主存储上重新调用的文件所需的空间消耗增加。

通过 FPolicy 直通读取， HSM 服务器（ FPolicy 服务器）可以对已迁移的脱机文件提供读取访问，而无需将文件从二级存储系统重新调用到主存储系统。可以直接从二级存储处理读取请求，而不是将文件重新调用回主存储。

> FPolicy 直通读取操作不支持副本卸载（ ODX ）。

直通读取通过提供以下优势增强了可用性：

- 即使主存储没有足够的空间将请求的数据重新调用回主存储，也可以处理读取请求。
- 当数据重新调用可能激增时，例如脚本或备份解决方案需要访问多个脱机文件时，可以更好地管理容量和性能。

- 可以处理 Snapshot 副本中脱机文件的读取请求。

  由于 Snapshot 副本是只读的，因此，如果存根文件位于 Snapshot 副本中，则 FPolicy 服务器将无法还原原始文件。使用直通读取可消除此问题。

- 可以设置策略来控制何时通过访问二级存储上的文件来处理读取请求，以及何时应将脱机文件重新调用到主存储。

  例如，可以在 HSM 服务器上创建一个策略，用于指定在将脱机文件迁移回主存储之前的指定时间段内可以访问该文件的次数。此类策略可避免调用很少访问的文件。

启用 **FPolicy** 直通读取时如何管理读取请求

您应了解启用 FPolicy 直通读取时如何管理读取请求，以便以最佳方式配置 Storage Virtual Machine （ SVM ）和 FPolicy 服务器之间的连接。

启用 FPolicy 直通读取后，如果 SVM 收到脱机文件请求，则 FPolicy 将通过标准连接通道向 FPolicy 服务器（ HSM 服务器）发送通知。

收到通知后， FPolicy 服务器将从通知中发送的文件路径读取数据，并通过 SVM 与 FPolicy 服务器之间建立的直通读取特权数据连接将请求的数据发送到 SVM 。

发送数据后， FPolicy 服务器将对读取请求做出响应，即允许或拒绝。根据读取请求是被允许还是被拒绝，ONTAP 会向客户端发送请求的信息或错误消息。

规划 **FPolicy** 配置

配置 **FPolicy** 的要求，注意事项和最佳实践

在SVM上创建和配置FPolicy配置之前、您需要了解配置FPolicy的某些要求、注意事项和最佳实践。

FPolicy功能可通过命令行界面(CLI)或REST API进行配置。

设置 **FPolicy** 的要求

在 Storage Virtual Machine （ SVM ）上配置和启用 FPolicy 之前，您需要了解某些要求。

- 集群中的所有节点都必须运行支持 FPolicy 的 ONTAP 版本。
- 如果您不使用 ONTAP 原生 FPolicy 引擎，则必须安装外部 FPolicy 服务器（ FPolicy 服务器）。
- FPolicy 服务器必须安装在可从启用了 FPolicy 策略的 SVM 的数据 LIF 访问的服务器上。

> 从ONTAP 9.8开始、ONTAP 通过添加为出站FPolicy连接提供客户端LIF服务 `data-fpolicy-client` 服务 "详细了解LIF和服务策略"。

- 必须在 FPolicy 策略外部引擎配置中将 FPolicy 服务器的 IP 地址配置为主服务器或二级服务器。
- 如果 FPolicy 服务器通过有权限的数据通道访问数据，则必须满足以下附加要求：
  - SMB 必须在集群上获得许可。

通过 SMB 连接实现有权限的数据访问。

  - 必须配置用户凭据才能通过有权限的数据通道访问文件。
  - FPolicy 服务器必须在 FPolicy 配置中配置的凭据下运行。
  - 必须将用于与FPolicy服务器通信的所有数据SIFs配置为具有 `cifs` 作为允许的协议之一。

    这包括用于直通读取连接的 LIF 。

- 从ONTAP 9.14.1开始、您可以通过FPolicy设置永久性存储、以捕获SVM中异步非强制策略的文件访问事件。永久性存储有助于将客户端I/O处理与FPolicy通知处理分离、以减少客户端延迟。不支持同步(强制或非强制)和异步强制配置。

设置 **FPolicy** 时的最佳实践和建议

在Storage Virtual Machine (SVM)上设置FPolicy时、请熟悉常规配置最佳实践和建议、以确保您的FPolicy配置提供稳定可靠的监控性能和结果、从而满足您的要求。

有关性能、规模估算和配置的具体准则、请使用您的FPolicy合作伙伴应用程序。

策略配置

为SVM配置FPolicy外部引擎、事件和范围可以改善整体体验和安全性。

- 为SVM配置FPolicy外部引擎：
  - 提供额外的安全性会降低性能成本。启用安全套接字层(SSL)通信会影响访问共享的性能。
  - FPolicy外部引擎应配置多个FPolicy服务器、以提供FPolicy服务器通知处理的故障恢复能力和高可用性。
- 为SVM配置FPolicy事件：

  监控文件操作会影响您的整体体验。例如、在存储端筛选不需要的文件操作可以改善您的体验。NetApp建议设置以下配置：

  - 监控最小文件操作类型并启用最大数量的筛选器、而不会违反使用情形。
  - 对getattr、读取、写入、打开和关闭操作使用筛选器。SMB和NFS主目录环境中的这些操作所占比例较高。
- 配置SVM的FPolicy范围：

  将策略的范围限制为相关存储对象、例如共享、卷和导出、而不是在整个SVM中启用这些对象。NetApp建议检查目录扩展名。如果 `is-file-extension-check-on-directories-enabled` 参数设置为 `true` ，目录对象将与常规文件一样进行扩展名检查。

网络配置：

FPolicy服务器和控制器之间的网络连接应具有低延迟。NetApp建议使用专用网络将FPolicy流量与客户端流量分隔开。

此外、您还应将外部FPolicy服务器(FPolicy服务器)放置在具有高带宽连接的集群附近、以实现最低延迟和高带宽连接。

> 如果将用于FPolicy流量的LIF配置在与用于客户端流量的LIF不同的端口上、则FPolicy LIF可能会因端口故障而故障转移到另一节点。因此、无法从节点访问FPolicy服务器、从而导致节点上文件操作的FPolicy通知失败。要避免出现此问题描述、请验证是否可通过节点上的至少一个LIF访问FPolicy服务器、以处理对该节点执行文件操作的FPolicy请求。

硬件配置

您可以将FPolicy服务器放置在物理服务器或虚拟服务器上。如果FPolicy服务器位于虚拟环境中、则应为此虚拟服务器分配专用资源(CPU、网络和内存)。

应优化集群节点与 FPolicy 服务器比率，以确保 FPolicy 服务器不会过载，这可能会在 SVM 响应客户端请求时导致延迟。最佳比率取决于使用FPolicy服务器的配对应用程序。NetApp建议与合作伙伴合作确定适当的价值。

多策略配置

无论序列号如何、用于本机阻止的FPolicy策略都具有最高优先级、而决策策略的优先级高于其他策略。策略优先级取决于使用情形。NetApp建议与合作伙伴合作确定适当的优先级。

大小注意事项

FPolicy对SMB和NFS操作执行实时监控、向外部服务器发送通知并等待响应、具体取决于外部引擎通信模式(同步或异步)。此过程会影响SMB和NFS访问以及CPU资源的性能。

要缓解任何问题、NetApp建议在启用FPolicy之前与合作伙伴一起评估环境并对其进行规模估算。性能受多种因素影响、包括用户数量、工作负载特征(例如每个用户的操作数和数据大小)、网络延迟以及故障或服务器速度减低。

监控性能

FPolicy是一个基于通知的系统。通知将发送到外部服务器进行处理、并生成对ONTAP的响应。此往返过程会增加客户端访问的延迟。

通过监控FPolicy服务器和ONTAP中的性能计数器、您可以发现解决方案中的瓶颈、并根据需要调整参数以获得最佳解决方案。例如、FPolicy延迟的增加会对SMB和NFS访问延迟产生级联影响。因此、您应同时监控工作负载(SMB和NFS)和FPolicy延迟。此外、您还可以在ONTAP中使用服务质量策略为启用了FPolicy的每个卷或SVM设置工作负载。

NetApp建议运行 `statistics show -object workload` 命令以显示工作负载统计信息。此外、您还应监控以下参数：

- 平均、读取和写入时间
- 操作总数
- 读取和写入计数器

您可以使用以下FPolicy计数器监控FPolicy子系统的性能。

> 您必须处于诊断模式才能收集与FPolicy相关的统计信息。

步骤

1. 收集FPolicy计数器：

a. `statistics start -object fpolicy -instance instance_name -sample-id ID`

b. `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. 显示FPolicy计数器：

a. `statistics show -object fpolicy –instance instance_name -sample-id ID`

b. `statistics show -object fpolicy_server –instance instance_name -sample-id ID`

。 `fpolicy` 和 `fpolicy_server` 计数器可提供有关下表中所述的多个性能参数的信息。

计数器	Description
"fpolicy"计数器	已中止请求
在SVM上中止处理的屏幕请求数量	event_count
生成通知的事件列表	max_request_延迟
最大屏幕请求延迟	未完成_请求
正在处理的屏幕请求总数	processed_requests
在SVM上执行fpolicy处理的屏幕请求总数	Request_延迟 历史记录
屏幕请求延迟的直方图	Requests_发放 率
每秒发送的屏幕请求数	Requests_received_rate
每秒接收的屏幕请求数	**"fpolicy_server"**计数器
max_request_延迟	屏幕请求的最大延迟
未完成_请求	等待响应的屏幕请求总数
request_延迟	屏幕请求的平均延迟
Request_延迟 历史记录	屏幕请求延迟的直方图
Request_sent率	每秒发送到FPolicy服务器的屏幕请求数
respony_received_rate	每秒从FPolicy服务器收到的屏幕响应数

管理**FPolicy**工作流以及对其他技术的依赖

NetApp建议在进行任何配置更改之前禁用FPolicy策略。例如、如果要在为已启用策略配置的外部引擎中添加或修改某个IP地址、请先禁用该策略。

如果将FPolicy配置为监控NetApp FlexCache卷、NetApp建议您不要将FPolicy配置为监控读取和getATTR文件操作。在ONTAP中监控这些操作需要检索索引节点到路径(i2P)数据。由于无法从FlexCache卷检索I2P数据、因此必须从初始卷检索这些数据。因此、监控这些操作会消除FlexCache可提供的性能优势。

部署FPolicy和机下防病毒解决方案后、防病毒解决方案会首先收到通知。FPolicy处理仅在防病毒扫描完成后开始。正确估算防病毒解决方案的规模非常重要、因为速度较慢的防病毒扫描程序可能会影响整体性能。

直通读取升级和还原注意事项

在升级到支持直通读取的 ONTAP 版本之前或还原到不支持直通读取的版本之前，您必须了解某些升级和还原注意事项。

升级

在将所有节点升级到支持 FPolicy 直通读取的 ONTAP 版本后，集群可以使用直通读取功能；但是，在现有 FPolicy 配置中，直通读取默认处于禁用状态。要对现有 FPolicy 配置使用直通读取，必须禁用 FPolicy 策略并修改配置，然后重新启用配置。

还原

还原到不支持FPolicy直通读取的ONTAP版本之前、您必须满足以下条件：

- 使用直通读取禁用所有策略、然后修改受影响的配置、使其不使用直通读取。
- 通过禁用集群上的每个FPolicy策略、在集群上禁用FPolicy功能。

在还原到不支持永久性存储的ONTAP版本之前、请确保所有Fpolicy策略均未配置永久性存储。如果配置了永久性存储、还原将失败。

设置 **FPolicy** 配置的步骤是什么

要监控文件访问，必须先在需要 FPolicy 服务的 Storage Virtual Machine （ SVM ）上创建并启用 FPolicy 配置。

在 SVM 上设置和启用 FPolicy 配置的步骤如下：

1. 创建 FPolicy 外部引擎。

   FPolicy 外部引擎可识别与特定 FPolicy 配置关联的外部 FPolicy 服务器（ FPolicy 服务器）。如果使用内部 "`FPolicy` " 原生引擎创建原生文件阻止配置，则无需创建 FPolicy 外部引擎。

2. 创建 FPolicy 事件。

   FPolicy 事件描述了 FPolicy 策略应监控的内容。事件由要监控的协议和文件操作组成，并且可以包含筛选器列表。事件使用筛选器缩小 FPolicy 外部引擎必须发送通知的受监控事件的列表范围。事件还指定策略是否监控卷操作。

3. 创建 FPolicy 策略。

   FPolicy 策略负责将需要监控的一组事件与相应的范围关联起来，以及必须将哪些受监控事件通知发送到指定的 FPolicy 服务器（如果未配置任何 FPolicy 服务器，则还必须发送到原生引擎）。该策略还定义是否允许 FPolicy 服务器对其接收通知的数据进行特权访问。如果 FPolicy 服务器需要访问数据，则需要进行特权访问。需要特权访问的典型使用情形包括文件阻止，配额管理和分层存储管理。您可以在此策略中指定此策略的配置是使用 FPolicy 服务器还是使用内部 "`原生` FPolicy 服务器。

   策略指定是否必须进行筛选。如果必须进行筛选，并且所有 FPolicy 服务器均已关闭，或者在定义的超时期限内未从 FPolicy 服务器收到任何响应，则会拒绝文件访问。

   策略的边界为 SVM 。一个策略不能应用于多个 SVM 。但是，一个特定 SVM 可以具有多个 FPolicy 策略，每个策略的范围，事件和外部服务器配置组合相同或不同。

4. 配置策略范围。

   FPolicy 范围用于确定该策略对哪些卷，共享或导出策略执行操作或排除在监控范围之外。范围还决定了应在 FPolicy 监控中包括或排除哪些文件扩展名。

   > 排除列表优先于包括列表。

5. 启用 FPolicy 策略。

   启用此策略后，控制通道以及（可选）有权限的数据通道将连接起来。SVM 参与的节点上的 FPolicy 进程开始监控文件和文件夹访问，对于符合已配置标准的事件，会向 FPolicy 服务器（如果未配置任何 FPolicy 服务器，则向原生引擎发送通知）。

   > 如果此策略使用原生文件阻止，则不会配置外部引擎或将其与此策略关联。

规划 **FPolicy** 外部引擎配置

规划 **FPolicy** 外部引擎配置

在配置 FPolicy 外部引擎（外部引擎）之前，您必须了解创建外部引擎的含义以及可用的配置参数。此信息可帮助您确定要为每个参数设置的值。

创建 **FPolicy** 外部引擎时定义的信息

外部引擎配置定义了 FPolicy 在建立和管理与外部 FPolicy 服务器（ FPolicy 服务器）的连接时所需的信息，其中包括以下信息：

- SVM name
- 引擎名称
- 主和二级 FPolicy 服务器的 IP 地址以及在连接到 FPolicy 服务器时要使用的 TCP 端口号
- 引擎类型是异步还是同步
- 如何对节点与 FPolicy 服务器之间的连接进行身份验证

  如果您选择配置相互 SSL 身份验证，则还必须配置提供 SSL 证书信息的参数。

- 如何使用各种高级权限设置管理连接

  其中包括用于定义超时值，重试值，保活值，最大请求值，已发送和接收缓冲区大小值以及会话超时值等内容的参数。

。 `vserver fpolicy policy external-engine create` 命令用于创建FPolicy外部引擎。

什么是基本外部引擎参数

您可以使用下表中的基本 FPolicy 配置参数来帮助您规划配置：

信息类型	选项

SVM 指定要与此外部引擎关联的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
引擎名称 _ 指定要分配给外部引擎配置的名称。您必须在稍后创建 FPolicy 策略时指定外部引擎名称。这会将外部引擎与策略相关联。 此名称最长可为 256 个字符。 ⓘ 如果在 MetroCluster 或 SVM 灾难恢复配置中配置外部引擎名称，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • `a` 到 `z` • `A` 到 `Z` • `0` 到 `9` • “_”、“-”, and "`.`Ω"	`-engine-name engine_name`
_ 主 FPolicy 服务器 _ 指定节点针对给定 FPolicy 策略向其发送通知的主 FPolicy 服务器。此值以逗号分隔的 IP 地址列表形式指定。 如果指定了多个主服务器 IP 地址，则 SVM 参与的每个节点都会在启用此策略时与每个指定的主 FPolicy 服务器创建一个控制连接。如果配置了多个主 FPolicy 服务器，则会以轮循方式向 FPolicy 服务器发送通知。 如果在 MetroCluster 或 SVM 灾难恢复配置中使用外部引擎，则应将源站点上 FPolicy 服务器的 IP 地址指定为主服务器。目标站点上 FPolicy 服务器的 IP 地址应指定为二级服务器。	`-primary-servers IP_address`、
端口号 _ 指定 FPolicy 服务的端口号。	`-port integer`

二级 FPolicy 服务器 _ 指定要将给定 FPolicy 策略的文件访问事件发送到的二级 FPolicy 服务器。此值以逗号分隔的 IP 地址列表形式指定。 只有在无法访问主服务器时，才会使用二级服务器。启用策略后，系统会建立与二级服务器的连接，但只有在无法访问任何主服务器时，才会向二级服务器发送通知。如果配置了多个二级服务器，则会以轮循方式向 FPolicy 服务器发送通知。	`-secondary-servers IP_address`、
外部引擎类型 _ 指定外部引擎是在同步模式还是异步模式下运行。默认情况下， FPolicy 在同步模式下运行。 设置为时 `synchronous`，文件请求处理会向FPolicy服务器发送通知，但只有在收到FPolicy服务器的响应后才会继续。此时，请求流将继续，或者处理将导致拒绝，具体取决于 FPolicy 服务器的响应是否允许所请求的操作。 设置为时 `asynchronous`，文件请求处理会向FPolicy服务器发送通知，然后继续。	`-extern-engine-type external_engine_type` 此参数的值可以是以下值之一： • `synchronous` • `asynchronous`
用于与 FPolicy server_ 通信的 _ssl 选项 指定用于与 FPolicy 服务器通信的 SSL 选项。这是必需的参数。您可以根据以下信息选择一个选项： • 设置为时 `no-auth`，则不进行身份验证。 通信链路通过 TCP 建立。 • 设置为时 `server-auth`，SVM使用SSL服务器身份验证对FPolicy服务器进行身份验证。 • 设置为时 `mutual-auth`，SVM和FPolicy服务器之间会进行相互身份验证；SVM会对FPolicy服务器进行身份验证，FPolicy服务器会对SVM进行身份验证。 如果选择配置相互SSL身份验证、则还必须配置 `-certificate -common-name`， `-certificate-serial`，和 `-certifcate-ca` parameters	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
证书 FQDN 或自定义公用名 _ 指定在 SVM 和 FPolicy 服务器之间配置 SSL 身份验证时使用的证书名称。您可以将证书名称指定为 FQDN 或自定义公用名。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-common-name` 参数。	`-certificate-common -name text`

证书序列号 _ 指定在 SVM 和 FPolicy 服务器之间配置了 SSL 身份验证时用于身份验证的证书的序列号。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-serial` 参数。	`-certificate-serial text`
证书颁发机构 _ 指定在 SVM 和 FPolicy 服务器之间配置了 SSL 身份验证时用于身份验证的证书的 CA 名称。 如果指定 `mutual-auth` 。 `-ssl-option` 参数、则必须为指定一个值 `-certificate-ca` 参数。	`-certificate-ca text`

什么是高级外部引擎选项

在计划是否使用高级参数自定义配置时，您可以使用下表中的高级 FPolicy 配置参数。您可以使用以下参数修改集群节点和 FPolicy 服务器之间的通信行为：

信息类型	选项
取消请求时超时 _ 指定时间间隔(以小时为单位) (`h`)、分钟 (`m`)或秒 (`s`)、表示节点等待FPolicy服务器的响应。 如果超时间隔已过，则节点会向 FPolicy 服务器发送取消请求。然后，节点会将通知发送到备用 FPolicy 服务器。此超时有助于处理无响应的 FPolicy 服务器，从而提高 SMB/NFS 客户端响应速度。此外，在超时期限后取消请求有助于释放系统资源，因为通知请求会从已关闭 / 错误的 FPolicy 服务器移至备用 FPolicy 服务器。 此值的范围为 `0` 到 `100`。如果此值设置为 `0`，选项已禁用，并且取消请求消息不会发送到FPolicy服务器。默认值为 `20s`。	`-reqs-cancel-timeout integer`[h
m	s]
中止请求时超时 _ 以小时为单位指定超时 (`h`)、分钟 (`m`)或秒 (`s`)以使请求发生abording。 此值的范围为 `0` 到 `200`。	`-reqs-abort-timeout` ` `integer`[h
m	s]

发送状态请求的间隔 _ 以小时为单位指定间隔 (h)、分钟 (m)或秒 (s)之后、状态请求将发送到FPolicy服务器。 此值的范围为 0 到 50。如果此值设置为 0，选项已禁用，并且状态请求消息不会发送到FPolicy服务器。默认值为 10s。	-status-req-interval integer[h
m	s]
FPolicy 服务器上的最大未处理请求数 _ 指定可在 FPolicy 服务器上排队的最大未处理请求数。 此值的范围为 1 到 10000。默认值为 500。	-max-server-reqs integer
断开无响应 FPolicy 服务器的超时 _ 指定时间间隔(以小时为单位) (h)、分钟 (m)或秒 (s)之后、与FPolicy服务器的连接将终止。 只有当 FPolicy 服务器的队列包含允许的最大请求且在超时期限内未收到响应时，此连接才会在超时期限后终止。允许的最大请求数为任一 50 (默认值)或指定的数字 max-server-reqs- 参数。 此值的范围为 1 到 100。默认值为 60s。	-server-progress -timeout integer[h
m	s]
向 FPolicy 服务器发送保活消息的 _Interval 指定时间间隔(以小时为单位) (h)、分钟 (m)或秒 (s)、在该位置、保活消息将发送到FPolicy服务器。 保持活动消息会检测半打开的连接。 此值的范围为 10 到 600。如果此值设置为 0，选项将被禁用，并阻止将保持活动消息发送到FPolicy服务器。默认值为 120s。	-keep-alive-interval- integer[h
m	s]
最大重新连接尝试次数 _ 指定在连接断开后 SVM 尝试重新连接到 FPolicy 服务器的最大次数。 此值的范围为 0 到 20。默认值为 5。	-max-connection-retries integer

接收缓冲区大小 _ 指定 FPolicy 服务器的已连接套接字的接收缓冲区大小。 默认值设置为 256 KB 。如果此值设置为 0 ，则接收缓冲区的大小将设置为系统定义的值。 例如，如果套接字的默认接收缓冲区大小为 65536 字节，则通过将可调值设置为 0 ，套接字缓冲区大小将设置为 65536 字节。您可以使用任何非默认值来设置接收缓冲区的大小（以字节为单位）。	`-recv-buffer-size integer`
发送缓冲区大小 _ 指定 FPolicy 服务器的已连接套接字的发送缓冲区大小。 默认值设置为 256 KB 。如果此值设置为 0 ，则发送缓冲区的大小将设置为系统定义的值。 例如，如果套接字的默认发送缓冲区大小设置为 65536 字节，则通过将可调值设置为 0 ，套接字缓冲区大小将设置为 65536 字节。您可以使用任何非默认值来设置发送缓冲区的大小（以字节为单位）。	`-send-buffer-size integer`
_Timeout ，用于在重新连接期间清除会话 ID 以小时为单位指定间隔 (`h`)、分钟 (`m`)或秒 (`s`)之后、新会话ID将在重新连接尝试期间发送到FPolicy服务器。 如果存储控制器与FPolicy服务器之间的连接终止、并在中重新建立连接 `-session-timeout` 间隔、旧会话ID将发送到FPolicy服务器、以便它可以发送对旧通知的响应。 默认值设置为10秒。	`-session-timeout [integerh][integerm][integer秒]`

追加信息关于配置 **FPolicy** 外部引擎以使用经过 **SSL** 身份验证的连接的信息

如果要将 FPolicy 外部引擎配置为在连接到 FPolicy 服务器时使用 SSL ，则需要了解一些追加信息。

SSL 服务器身份验证

如果选择为 SSL 服务器身份验证配置 FPolicy 外部引擎，则在创建外部引擎之前，必须安装对 FPolicy 服务器证书签名的证书颁发机构（ CA ）的公有证书。

相互身份验证

如果您将 FPolicy 外部引擎配置为在将 Storage Virtual Machine （ SVM ）数据 LIF 连接到外部 FPolicy 服务器时使用 SSL 相互身份验证，则在创建外部引擎之前， 您必须安装对 FPolicy 服务器证书签名的 CA 的公有证书以及公有证书和密钥文件，以便对 SVM 进行身份验证。当任何 FPolicy 策略使用已安装的证书时，不能删除此证书。

如果在连接到外部 FPolicy 服务器时 FPolicy 使用该证书进行相互身份验证时删除了该证书，则无法重新启用使用该证书的已禁用 FPolicy 策略。在这种情况下，即使在 SVM 上创建并安装了具有相同设置的新证书，也无法重新启用 FPolicy 策略。

如果证书已删除，则需要安装新证书，创建使用新证书的新 FPolicy 外部引擎，并通过修改 FPolicy 策略将新外部引擎与要重新启用的 FPolicy 策略相关联。

安装 **SSL** 证书

用于签署FPolicy服务器证书的CA的公共证书是使用安装的 `security certificate install` 命令 `-type` 参数设置为 `client-ca`。使用安装SVM身份验证所需的专用密钥和公共证书 `security certificate install` 命令 `-type` 参数设置为 `server`。

证书不会在具有非 **ID-preserve** 配置的 **SVM** 灾难恢复关系中进行复制

在连接到 FPolicy 服务器时用于 SSL 身份验证的安全证书不会复制到具有非 ID-preserve 配置的 SVM 灾难恢复目标。虽然会复制 SVM 上的 FPolicy 外部引擎配置，但不会复制安全证书。您必须在目标上手动安装安全证书。

在设置SVM灾难恢复关系时、您为选择的值 `-identity-preserve` 的选项 `snapmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则会复制所有FPolicy配置详细信息、包括安全证书信息。只有在将选项设置为时、才必须在目标上安装安全证书 `false` (不保留ID)。

具有 **MetroCluster** 和 **SVM** 灾难恢复配置的集群范围 **FPolicy** 外部引擎的限制

您可以通过将集群 Storage Virtual Machine （ SVM ）分配给外部引擎来创建集群范围的 FPolicy 外部引擎。但是，在 MetroCluster 或 SVM 灾难恢复配置中创建集群范围的外部引擎时，在选择 SVM 用于与 FPolicy 服务器进行外部通信的身份验证方法时，存在某些限制。

创建外部 FPolicy 服务器时，您可以选择三种身份验证选项：无身份验证， SSL 服务器身份验证和 SSL 相互身份验证。尽管在将外部 FPolicy 服务器分配给数据 SVM 时选择身份验证选项没有任何限制，但在创建集群范围的 FPolicy 外部引擎时仍存在一些限制：

Configuration	是否允许?
MetroCluster 或 SVM 灾难恢复以及集群范围的 FPolicy 外部引擎，不进行身份验证（未配置 SSL ）	是的。
MetroCluster 或 SVM 灾难恢复以及具有 SSL 服务器或 SSL 相互身份验证的集群范围 FPolicy 外部引擎	否

- 如果存在具有 SSL 身份验证的集群范围的 FPolicy 外部引擎，而您要创建 MetroCluster 或 SVM 灾难恢复配置，则必须先修改此外部引擎以不使用身份验证或删除外部引擎，然后才能创建 MetroCluster 或 SVM 灾难恢复配置。
- 如果 MetroCluster 或 SVM 灾难恢复配置已存在，则 ONTAP 会阻止您使用 SSL 身份验证创建集群范围的 FPolicy 外部引擎。

填写 **FPolicy** 外部引擎配置工作表

您可以使用此工作表记录 FPolicy 外部引擎配置过程中所需的值。如果需要参数值，您需要先确定要对这些参数使用的值，然后再配置外部引擎。

基本外部引擎配置的信息

您应记录是否要在外部引擎配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
引擎名称	是的。	是的。	
主 FPolicy 服务器	是的。	是的。	
端口号	是的。	是的。	
二级 FPolicy 服务器	否		
外部引擎类型	否		
用于与外部 FPolicy 服务器通信的 SSL 选项	是的。	是的。	
证书 FQDN 或自定义公用名	否		
证书序列号	否		
证书颁发机构	否		

有关高级外部引擎参数的信息

要使用高级参数配置外部引擎，必须在高级权限模式下输入配置命令。

信息类型	Required	包括	您的价值
取消请求超时	否		
中止请求超时	否		
发送状态请求的间隔	否		
FPolicy 服务器上的最大未处理请求数	否		

断开无响应 FPolicy 服务器的连接超时	否		
向 FPolicy 服务器发送保活消息的间隔	否		
最大重新连接尝试次数	否		
接收缓冲区大小	否		
发送缓冲区大小	否		
重新连接期间清除会话 ID 超时	否		

规划 **FPolicy** 事件配置

规划 **FPolicy** 事件配置概述

在配置 FPolicy 事件之前，您必须了解创建 FPolicy 事件的含义。您必须确定要监控事件的协议，要监控的事件以及要使用的事件筛选器。此信息有助于您规划要设置的值。

创建 **FPolicy** 事件的含义

创建 FPolicy 事件意味着定义 FPolicy 进程需要用于确定要监控的文件访问操作以及应将哪些受监控事件通知发送到外部 FPolicy 服务器的信息。FPolicy 事件配置定义了以下配置信息：

- Storage Virtual Machine （ SVM ）名称
- 事件名称
- 要监控的协议

  FPolicy 可以监控 SMB ， NFSv3 和 NFSv4 文件访问操作。

- 要监控的文件操作

  并非所有文件操作对每个协议都有效。

- 要配置的文件筛选器

  只有某些文件操作和筛选器组合有效。每个协议都有自己一组支持的组合。

- 是否监控卷挂载和卸载操作

> 其中三个参数具有相关性 (`-protocol`， `-file-operations`， `-filters`）。以下组合适用于这三个参数：
>
> - 您可以指定 `-protocol` 和 `-file-operations` parameters
> - 您可以指定所有三个参数。
> - 您不能指定任何参数。

FPolicy 事件配置包含的内容

您可以使用以下可用 FPolicy 事件配置参数列表来帮助您规划配置：

信息类型	选项
SVM 指定要与此 FPolicy 事件关联的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
事件名称 _ 指定要分配给 FPolicy 事件的名称。创建 FPolicy 策略时，您可以使用事件名称将 FPolicy 事件与策略相关联。 此名称最长可为 256 个字符。 ⓘ 如果在 MetroCluster 或 SVM 灾难恢复配置中配置事件，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • `a` 到 `z` • `A` 到 `Z` • `0` 到 `9` • " _ "、“-”, and "`.`Ω"	`-event-name event_name`
_ 协议 _ 指定要为 FPolicy 事件配置的协议。的列表 `-protocol` 可以包含以下值之一： • `cifs` • `nfsv3` • `nfsv4` ⓘ 如果指定 `-protocol`**则必须在中指定有效值** `-file-operations` 参数。协议版本发生变化时，有效值可能会发生变化。	`-protocol protocol`

File operations 指定 FPolicy 事件的文件操作列表。 此事件使用中指定的协议从所有客户端请求中检查此列表中指定的操作 `-protocol` 参数。您可以使用逗号分隔列表列出一个或多个文件操作。的列表 `-file-operations` 可以包含以下一个或多个值： • `close` 用于文件关闭操作 • `create` 用于文件创建操作 • `create-dir` 目录创建操作 • `delete` 用于文件删除操作 • `delete_dir` 目录删除操作 • `getattr` 获取属性操作 • `link` 用于链路操作 • `lookup` 查找操作 • `open` 用于文件打开操作 • `read` 用于文件读取操作 • `write` 用于文件写入操作 • `rename` 用于文件重命名操作 • `rename_dir` 目录重命名操作 • `setattr` 用于设置属性操作 • `symlink` 符号链接操作 ⓘ 如果指定 `-file-operations`，则必须在中指定有效的协议 `-protocol` 参数。	`-file-operations` `file_operations`、

Filters 指定指定协议的给定文件操作的筛选器列表。中的值 `-filters` 参数用于筛选客户端请求。此列表可以包括以下一项或多项： ⓘ 如果指定 `-filters` 参数、则还必须为指定有效值 `-file -operations` 和 `-protocol` parameters • `monitor-ads` 用于筛选客户端对备用数据流的请求的选项。 • `close-with-modification` 用于筛选客户端请求以关闭并修改的选项。 • `close-without-modification` 用于筛选客户端请求以进行关闭而不进行修改的选项。 • `first-read` 用于筛选客户端请求以进行首次读取的选项。 • `first-write` 用于筛选客户端请求以进行首次写入的选项。 • `offline-bit` 用于筛选脱机位集的客户端请求的选项。 设置此筛选器会使 FPolicy 服务器仅在访问脱机文件时收到通知。 • `open-with-delete-intent` 用于筛选客户端请求的选项、以用于具有删除意图的OPEN。 设置此筛选器后，只有在尝试打开要删除的文件时， FPolicy 服务器才会收到通知。当时、文件系统会使用此选项 `FILE_DELETE_ON_CLOSE` 已指定标志。 • `open-with-write-intent` 用于筛选具有写入意图的OPEN客户端请求的选项。 设置此筛选器后，只有在尝试打开文件并在其中写入内容时， FPolicy 服务器才会收到通知。 • `write-with-size-change` 用于筛选客户端写入请求并更改大小的选项。	`-filters filter, ...`

_Filters_continued • `setattr-with-owner-change` 用于筛选客户端SETATTR更改文件或目录所有者的请求的选项。 • `setattr-with-group-change` 用于筛选客户端SETATTR更改文件或目录组的请求的选项。 • `setattr-with-sacl-change` 用于筛选客户端SETATTR更改文件或目录上的SACL请求的选项。 此筛选器仅适用于SMB和NFSv4协议。 • `setattr-with-dacl-change` 用于筛选客户端SETATTR请求以更改文件或目录上的DACL的选项。 此筛选器仅适用于SMB和NFSv4协议。 • `setattr-with-modify-time-change` 用于筛选客户端SETATTR请求以更改文件或目录的修改时间的选项。 • `setattr-with-access-time-change` 用于筛选客户端setattr请求以更改文件或目录访问时间的选项。 • `setattr-with-creation-time-change` 用于筛选客户端SETATTR请求以更改文件或目录的创建时间的选项。 此选项仅适用于SMB协议。 • `setattr-with-mode-change` 用于筛选客户端setattr请求以更改文件或目录上的模式位的选项。 • `setattr-with-size-change` 用于筛选客户端setattr请求以更改文件大小的选项。 • `setattr-with-allocation-size-change` 用于筛选客户端SETATTR请求以更改文件分配大小的选项。 此选项仅适用于SMB协议。 • `exclude-directory` 用于筛选客户端目录操作请求的选项。 指定此筛选器后，不会监控目录操作。	`-filters filter, ...`
是否需要执行卷操作 _ 指定卷挂载和卸载操作是否需要监控。默认值为 `false`。	`-volume-operation {true`

false} -filters filter，…	*FPolicy*访问被拒绝通知 从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。这些通知对于安全性、勒索软件防护和监管非常重要。如果文件操作因缺少权限而失败、则会生成通知、其中包括： • 由于NTFS权限而失败。 • 由于Unix模式位而导致失败。 • 由于NFSv4 ACL而导致失败。
-monitor-fileop-failure {true	false}

FPolicy可以监控**SMB**的受支持文件操作和筛选器组合

在配置 FPolicy 事件时，您需要注意的是，监控 SMB 文件访问操作仅支持特定的文件操作和筛选器组合。

下表列出了用于监控 SMB 文件访问事件的 FPolicy 支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
关闭	监控器广告，脱机位，修改后接近，修改后关闭，读取后关闭， 排除目录
创建	监控器广告，脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	监控器广告，脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
getattr	offline-bit ， exclude-dir
打开	monitor-ad ， offline-bit ， open-wan-delete-intent ， open-write-intent ， exclude-dir
读取	监控器广告，脱机位，首次读取
写入	monitor-ad ， offline-bit ， first-write ， write-write-wing-write-size-change

重命名	监控器广告，脱机位
rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	monitor-ad， offline-bit， setattr_and_owner_change， setattr_and_group_change， setattr_and_mode_change， setattr_for_sacl_change， setattr_for_dacl_change， setattr_for_modify_time_change， setattr_for_access_time_change， setattr_for_creation_time_change， setattr_and_size_change， setattr_and_allocation_size_change， exclude_directory

从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。下表列出了在对SMB文件访问事件进行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器
打开	不适用

FPolicy可以监控**NFSv3**的受支持文件操作和筛选器组合

配置FPolicy事件时、需要注意、仅支持使用特定的文件操作和筛选器组合来监控NFSv3文件访问操作。

下表列出了对NFSv3文件访问事件执行FPolicy监控时支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
创建	脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
链接。	脱机位
查找	offline-bit， exclude-dir
读取	脱机位，首次读取
写入	脱机位，首次写入，写入时更改大小
重命名	脱机位

rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	脱机位， setattr_and_owner_change ， setattr_and_group_change ， setattr_and_mode_change ， setattr_and_modify_time_change ， setattr_and_access_time_change ， setattr_and_size_change ， exclude_directory
符号链接	脱机位

从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。下表列出了对NFSv3文件访问事件进行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器
访问	不适用
创建	不适用
create_dir	不适用
删除	不适用
delete_dir	不适用
链接。	不适用
读取	不适用
重命名	不适用
rename_dir	不适用
SETATTR	不适用
写入	不适用

FPolicy 可以监控 **NFSv4** 的受支持文件操作和筛选器组合

在配置 FPolicy 事件时，您需要注意，在监控 NFSv4 文件访问操作时，仅支持特定的文件操作和筛选器组合。

下表列出了用于监控 NFSv4 文件访问事件的 FPolicy 支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器

关闭	脱机位，排除目录
创建	脱机位
create_dir	目前，此文件操作不支持任何筛选器。
删除	脱机位
delete_dir	目前，此文件操作不支持任何筛选器。
getattr	脱机位，排除目录
链接。	脱机位
查找	脱机位，排除目录
打开	脱机位，排除目录
读取	脱机位，首次读取
写入	脱机位，首次写入，写入时更改大小
重命名	脱机位
rename_dir	目前，此文件操作不支持任何筛选器。
SETATTR	脱机位， setattr_and_owner_change ， setattr_and_group_change ， setattr_and_mode_change ， setattr_and_sacl_change ， setattr_and_dacl_change ， setattr_and_modify_time_change ， setattr_and_access_time_change ， setattr_and_size_change ， exclude_directory
符号链接	脱机位

从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。下表列出了对NFSv4文件访问事件进行FPolicy监控时支持的拒绝访问文件操作和筛选器组合：

支持拒绝访问文件操作	支持的筛选器
访问	不适用
创建	不适用

create_dir	不适用
删除	不适用
delete_dir	不适用
链接。	不适用
打开	不适用
读取	不适用
重命名	不适用
rename_dir	不适用
SETATTR	不适用
写入	不适用

填写 **FPolicy** 事件配置工作表

您可以使用此工作表记录 FPolicy 事件配置过程中所需的值。如果需要参数值，则需要先确定要对这些参数使用的值，然后再配置 FPolicy 事件。

您应记录是否要在 FPolicy 事件配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
事件名称	是的。	是的。	
协议	否		
文件操作	否		
筛选器	否		
卷操作	否		
拒绝访问事件+ (从ONTAP 9.13开始提供支持)	否		

规划 FPolicy 策略配置

规划 FPolicy 策略配置概述

在配置 FPolicy 策略之前，您必须了解创建策略时需要哪些参数，以及为什么要配置某些可选参数。此信息可帮助您确定要为每个参数设置的值。

创建 FPolicy 策略时，请将此策略与以下项相关联：

- Storage Virtual Machine （SVM）
- 一个或多个 FPolicy 事件
- FPolicy 外部引擎

您还可以配置多个可选策略设置。

FPolicy 策略配置包含哪些内容

您可以使用以下可用的 FPolicy 必需策略和可选参数列表来帮助您规划配置：

信息类型	选项	Required	Default
_SVM 名称 _ 指定要在其中创建 FPolicy 策略的 SVM 的名称。	`-vserver vserver_name`	是的。	无
策略名称 _ 指定 FPolicy 策略的名称。 此名称最长可为 256 个字符。 ⓘ 如果在 MetroCluster 或 SVM 灾难恢复配置中配置策略，则此名称的长度应最多为 200 个字符。 此名称可以包含以下 ASCII 范围字符的任意组合： • `a` 到 `z` • `A` 到 `Z` • `0` 到 `9` • “_”、“-”, and "`.`Ω"	`-policy-name policy_name`	是的。	无

事件名称 _ 指定要与 FPolicy 策略关联的事件的逗号分隔列表。 • 您可以将多个事件关联到一个策略。 • 事件是特定于协议的。 • 您可以使用一个策略来监控多个协议的文件访问事件，方法是为要策略监控的每个协议创建一个事件，然后将事件与策略关联。 • 事件必须已存在。	`-events event_name，...`	是的。	无
外部引擎名称 _ 指定要与 FPolicy 策略关联的外部引擎的名称。 • 外部引擎包含节点向 FPolicy 服务器发送通知所需的信息。 • 您可以将 FPolicy 配置为使用 ONTAP 原生外部引擎进行简单文件阻止，或者使用配置为使用外部 FPolicy 服务器（FPolicy 服务器）的外部引擎进行更复杂的文件阻止和文件管理。 • 如果要使用本机外部引擎、则不能为此参数指定值、也可以指定 `native` 作为值。 • 如果要使用 FPolicy 服务器，外部引擎的配置必须已存在。	`-engine engine_name`	是（除非策略使用内部 ONTAP 原生引擎）	`native`
Is mandatory screening required 指定是否需要强制文件访问筛选。 • 强制筛选设置用于确定在所有主服务器和二级服务器均已关闭或在给定超时期限内未从 FPolicy 服务器收到响应时对文件访问事件采取的操作。 • 设置为时 `true`，文件访问事件被拒绝。 • 设置为时 `false`，则允许文件访问事件。	`-is-mandatory {true`	`false}`	否

true	*allow privileged access* 指定是否希望 FPolicy 服务器通过使用有权限的数据连接对受监控的文件和文件夹具有访问权限。 如果已配置，则 FPolicy 服务器可以使用特权数据连接从 SVM 的根目录访问包含受监控数据的文件。 要进行有权限的数据访问、必须在集群上获得SMB的许可、并且必须将用于连接到FPolicy服务器的所有数据SIFs配置为具有 `cifs` 作为允许的协议之一。 如果要将策略配置为允许特权访问，则还必须为希望 FPolicy 服务器用于特权访问的帐户指定用户名。	`-allow -privileged -access` {`yes`	`no`}
否（除非启用直通读取）	`no`	特权用户名 _ 指定 FPolicy 服务器用于特权数据访问的帐户的用户名。 • 此参数的值应采用 `domain\user name` 格式。 • 条件 `-allow -privileged -access` 设置为 `no`，则会忽略为此参数设置的任何值。	`-privileged -user-name user_name`

否（除非启用了特权访问）	无	*allow passthrough-read* 指定 FPolicy 服务器是否可以为已由 FPolicy 服务器归档到二级存储（脱机文件）的文件提供直通读取服务： • 直通读取是一种在不将数据还原到主存储的情况下读取脱机文件数据的方法。 直通读取可减少响应延迟，因为在响应读取请求之前，无需将文件重新调用回主存储。此外，直通读取还可以通过消除仅为满足读取请求而重新调用的文件占用主存储空间的需求来优化存储效率。 • 启用后，FPolicy 服务器将通过专为直通读取打开的单独有权限的数据通道为文件提供数据。 • 如果要配置直通读取，则还必须将策略配置为允许特权访问。	`-is-passthrough-read-enabled {true`

FPolicy 策略使用原生引擎时的 **FPolicy** 范围配置要求

如果您将 FPolicy 策略配置为使用原生引擎，则需要明确说明如何定义为该策略配置的 FPolicy 范围。

FPolicy 范围定义了应用 FPolicy 策略的边界，例如 FPolicy 适用场景是否指定了卷或共享。有许多参数进一步限制了 FPolicy 策略的适用范围。其中一个参数、 `-is-file-extension-check-on-directories -enabled`，指定是否检查目录上的文件扩展名。默认值为 `false`，表示不检查目录上的文件扩展名。

在共享或卷以及上启用使用本机引擎的FPolicy策略时 `-is-file-extension-check-on-directories`

`-enabled` 参数设置为 `false` 对于策略范围、目录访问将被拒绝。使用此配置时，由于不会检查文件扩展名中是否存在目录，因此，如果任何目录操作属于此策略的范围，则会拒绝此操作。

要确保在使用本机引擎时成功访问目录、您必须设置 `-is-file-extension-check-on-directories -enabled parameter` to `true` 创建范围时。

将此参数设置为 `true`，将对目录操作进行扩展检查，并根据FPolicy范围配置中包含或排除的扩展来决定是允许还是拒绝访问。

填写 **FPolicy** 策略工作表

您可以使用此工作表记录 FPolicy 策略配置过程中所需的值。您应记录是否要在 FPolicy 策略配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	
Policy name	是的。	
事件名称	是的。	
外部引擎名称		
是否需要强制筛查?		
允许特权访问		
有权限的用户名		
是否已启用直通读取?		

规划 **FPolicy** 范围配置

规划 **FPolicy** 范围配置概述

在配置 FPolicy 范围之前，您必须了解创建范围的含义。您必须了解范围配置的内容。您还需要了解优先级范围规则的含义。此信息可帮助您规划要设置的值。

创建 **FPolicy** 范围的含义

创建 FPolicy 范围意味着定义适用 FPolicy 策略的边界。Storage Virtual Machine （ SVM ）是基本边界。在为 FPolicy 策略创建范围时，必须定义要应用此范围的 FPolicy 策略，并且必须指定要应用此范围的 SVM 。

有许多参数进一步限制了指定 SVM 中的范围。您可以通过指定要包含在范围中的内容或指定要从范围中排除的内容来限制范围。将范围应用于已启用的策略后，策略事件检查将应用于此命令定义的范围。

如果在 "`include` " 选项中找到匹配项，则会为文件访问事件生成通知。如果在 "`exclude` " 选项中找到匹配项，

则不会为文件访问事件生成通知。

FPolicy 范围配置定义了以下配置信息：

- SVM name
- Policy name
- 要包括或排除受监控内容的共享
- 要包括或排除受监控内容的导出策略
- 要包括或排除受监控内容的卷
- 要在受监控的内容中包含或排除的文件扩展名
- 是否对目录对象执行文件扩展名检查

> 有关集群 FPolicy 策略的范围，需要特别注意一些事项。集群 FPolicy 策略是集群管理员为管理 SVM 创建的策略。如果集群管理员还为该集群 FPolicy 策略创建了范围，则 SVM 管理员不能为同一策略创建范围。但是，如果集群管理员未为集群 FPolicy 策略创建范围，则任何 SVM 管理员都可以为该集群策略创建范围。如果 SVM 管理员为该集群 FPolicy 策略创建了范围，则集群管理员随后无法为同一集群策略创建集群范围。这是因为集群管理员不能覆盖同一集群策略的范围。

什么是优先级范围规则

以下优先级规则适用于范围配置：

- 当共享包含在中时 `-shares-to-include` 参数、共享的父卷包含在中 `-volumes-to-exclude` 参数、`-volumes-to-exclude` 优先于 `-shares-to-include`。
- 导出策略包含在中时 `-export-policies-to-include` 参数和导出策略的父卷包含在中 `-volumes-to-exclude` 参数、 `-volumes-to-exclude` 优先于 `-export-policies-to-include`。
- 管理员可以同时指定这两者 `-file-extensions-to-include` 和 `-file-extensions-to-exclude` 列表。

  。 `-file-extensions-to-exclude` 参数已在之前检查 `-file-extensions-to-include` 已检查参数。

FPolicy 范围配置包含的内容

您可以使用以下可用 FPolicy 范围配置参数列表来帮助您规划配置：

> 在配置要在范围中包括或排除的共享、导出策略、卷和文件扩展名时、include和exclude参数可以包括元字符、例如"`"?`" and “*”。 不支持使用正则表达式。

信息类型	选项

SVM 指定要创建 FPolicy 范围的 SVM 名称。 每个 FPolicy 配置都在一个 SVM 中定义。为创建 FPolicy 策略配置而组合在一起的外部引擎，策略事件，策略范围和策略都必须与同一 SVM 相关联。	`-vserver vserver_name`
策略名称 _ 指定要将范围附加到的 FPolicy 策略的名称。FPolicy 策略必须已存在。	`-policy-name policy_name`
要包含的共享 _ 指定要监控应用范围的 FPolicy 策略的共享列表，以逗号分隔。	`-shares-to-include share_name，…`
要排除的共享 _ 指定要从对应用了范围的 FPolicy 策略的监控中排除的共享的逗号分隔列表。	`-shares-to-exclude share_name，…`
要包含的卷 _ 指定要监控的卷列表，以确定应用了此范围的 FPolicy 策略。	`-volumes-to-include volume_name，…`
要排除的卷 _ 指定要从应用范围的 FPolicy 策略的监控中排除的卷的逗号分隔列表。	`-volumes-to-exclude volume_name，…`
导出要包含的策略 _ 指定一个以逗号分隔的导出策略列表，用于监控应用此范围的 FPolicy 策略。	`-export-policies-to -include export_policy_name，…`
导出要排除的策略 _ 指定要从对应用范围的 FPolicy 策略的监控中排除的导出策略的逗号分隔列表。	`-export-policies-to -exclude export_policy_name，…`
要包含的文件扩展名 _ 指定要监控应用范围的 FPolicy 策略的文件扩展名的逗号分隔列表。	`-file-extensions-to -include file_extensions ，…`
要排除的文件扩展名 _ 指定要从对应用范围的 FPolicy 策略的监控中排除的文件扩展名的逗号分隔列表。	`-file-extensions-to -exclude file_extensions ，…`

目录上的文件扩展名检查是否已启用？ _ 指定文件扩展名检查是否也应用于目录对象。如果此参数设置为 `true`，目录对象将接受与常规文件相同的扩展名检查。如果此参数设置为 `false`，目录名称与扩展名不匹配，即使目录的名称扩展名不匹配，也会为其发送通知。 如果将范围分配到的FPolicy策略配置为使用本机引擎、则必须将此参数设置为 `true`。	`-is-file-extension -check-on-directories -enabled {true`我们可以为您提供 `false`

填写 **FPolicy** 范围工作表

您可以使用此工作表记录在 FPolicy 范围配置过程中所需的值。如果需要参数值，则需要先确定要对这些参数使用的值，然后再配置 FPolicy 范围。

您应记录是否要在 FPolicy 范围配置中包括每个参数设置，然后记录要包括的参数的值。

信息类型	Required	包括	您的价值
Storage Virtual Machine （ SVM ）名称	是的。	是的。	
Policy name	是的。	是的。	
要包含的共享	否		
要排除的共享	否		
要包含的卷	否		
要排除的卷	否		
要包括的导出策略	否		
要排除的导出策略	否		
要包括的文件扩展名	否		
要排除的文件扩展名	否		
是否已启用目录文件扩展名检查?	否		

创建 **FPolicy** 配置

创建 **FPolicy** 外部引擎

您必须创建外部引擎才能开始创建 FPolicy 配置。外部引擎定义了 FPolicy 如何建立和管

理与外部 FPolicy 服务器的连接。如果您的配置使用内部 ONTAP 引擎（原生外部引擎）来简单地阻止文件，则无需配置单独的 FPolicy 外部引擎，也无需执行此步骤。

您需要的内容

。 "外部引擎" 应填写工作表。

关于此任务

如果在 MetroCluster 配置中使用外部引擎，则应将源站点上 FPolicy 服务器的 IP 地址指定为主服务器。目标站点上 FPolicy 服务器的 IP 地址应指定为二级服务器。

步骤

1. 使用创建FPolicy外部引擎 `vserver fpolicy policy external-engine create` 命令：

   以下命令将在 Storage Virtual Machine （ SVM ） vs1.example.com 上创建外部引擎。与 FPolicy 服务器的外部通信不需要身份验证。

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. 使用验证FPolicy外部引擎配置 `vserver fpolicy policy external-engine show` 命令：

   以下命令显示有关在 SVM vs1.example.com 上配置的所有外部引擎的信息：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                   Primary        Secondary
   External
   Vserver            Engine       Servers        Servers       Port Engine
   Type
   ---------------    -----------  -------------- ----------- ------
   -----------
   vs1.example.com    engine1      10.1.1.2,      -             6789
   synchronous
                                   10.1.1.3
   ```

   以下命令显示有关 SVM vs1.example.com 上名为 "`Engine1` " 的外部引擎的详细信息：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                                Vserver: vs1.example.com
                                 Engine: engine1
               Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
        Port Number of FPolicy Service: 6789
             Secondary FPolicy Servers: -
                  External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
                Certificate Authority: -
```

创建 **FPolicy** 事件

在创建 FPolicy 策略配置过程中，您需要创建 FPolicy 事件。您可以在创建事件时将其与 FPolicy 策略相关联。事件定义要监控的协议以及要监控和筛选的文件访问事件。

开始之前

您应完成FPolicy事件 "工作表"。

创建 **FPolicy** 事件

1. 使用创建FPolicy事件 `vserver fpolicy policy event create` 命令：

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. 使用验证FPolicy事件配置 `vserver fpolicy policy event show` 命令：

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                     Event                 File                      Is Volume
   Vserver           Name      Protocols Operations    Filters   Operation
   ---------------   --------- --------- ------------- ---------
   ------------
   vs1.example.com   event1    cifs      open, close,  -         false
                                         read, write
   ```

创建**FPolicy**拒绝访问事件

从ONTAP 9.13.1开始、用户可以收到因缺少权限而导致文件操作失败的通知。这些通知对于安全性、勒索软件防护和监管非常重要。

1. 使用创建FPolicy事件 `vserver fpolicy policy event create` 命令：

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   ```

```
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

创建持久性存储

从ONTAP 9.14.1开始、FPolicy允许您设置 "永久性存储" 捕获SVM中异步非强制策略的文件访问事件。永久性存储有助于将客户端I/O处理与FPolicy通知处理分离、以减少客户端延迟。不支持同步(强制或非强制)和异步强制配置。

最佳实践

- 在使用永久性存储功能之前、请确保您的合作伙伴应用程序支持此配置。
- 永久性存储卷会按SVM进行设置。对于启用了FPolicy的每个SVM、您都需要一个永久性存储卷。
- 创建卷时指定的永久性存储卷名称和接合路径应匹配。
- 在包含预期Fpolicy监控的最大流量的生命周期的节点上创建永久性存储卷。
- 将Snapshot策略设置为 `none` 而不是 `default`。这是为了确保不会意外还原快照而导致当前事件丢失、并防止可能发生重复的事件处理。
- 使持久存储卷无法用于外部用户协议访问(CIFS或NFS)、以避免意外损坏或删除保留的事件记录。为此、在启用FPolicy后、请在ONTAP中卸载卷以删除接合路径、这样用户协议访问就无法访问该路径。

步骤

1. 在SVM上创建一个可为永久性存储配置的空卷：

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - 永久性存储卷的大小取决于您要使未传送到外部服务器(配对应用程序)的事件持久化的持续时间。

     例如、如果您希望在每秒容量为3万次通知的集群中持久保留30分钟的事件：

     所需卷大小= 30000 x 30 x 60 x 0.6 KB (平均通知记录大小)= 3240000 KB =~32 GB

   要了解大致的通知率、您可以联系您的FPolicy合作伙伴申请、也可以使用FPolicy计数器 `requests_dispatched_rate`。

   - 具有足够RBAC权限(用于创建卷)的管理员用户应使用volume CLI命令或REST API创建所需大小的卷、并将该卷的名称提供为 `-volume` 在永久性存储中、创建CLI命令或REST API。

2. 创建永久性存储：

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - 永久性存储：永久性存储名称
   - volume：永久性存储卷

3. 创建永久性存储后、您可以创建FPolicy策略并将此永久性存储名称添加到该策略中。
   有关详细信息，请参见 "创建 FPolicy 策略"。

创建 **FPolicy** 策略

创建 FPolicy 策略时，您需要将一个外部引擎以及一个或多个事件与此策略相关联。该策略还指定是否需要强制筛选， FPolicy 服务器是否有权访问 Storage Virtual Machine （SVM）上的数据，以及是否已启用对脱机文件的直通读取。

您需要的内容

- 应填写 FPolicy 策略工作表。
- 如果您计划配置策略以使用 FPolicy 服务器，则外部引擎必须存在。
- 您计划与 FPolicy 策略关联的至少一个 FPolicy 事件必须存在。
- 如果要配置有权限的数据访问、SVM上必须存在SMB服务器。
- 要为策略配置永久性存储，引擎类型必须为*async*，策略必须为*non-man强制*。

  有关详细信息，请参见 "创建持久性存储"。

步骤

1. 创建 FPolicy 策略：

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - 您可以将一个或多个事件添加到 FPolicy 策略中。
   - 默认情况下，强制筛选处于启用状态。
   - 如果要通过设置来允许特权访问 `-allow-privileged-access` 参数设置为 `yes`，您还必须为特权访问配置特权用户名。
   - 如果要通过设置来配置直通读取 `-is-passthrough-read-enabled` 参数设置为 `true`，您还必须配置有权限的数据访问。

     以下命令将创建一个名为 "`policy1` " 的策略，该策略会将事件命名为 "`EVENT1` " ，并将外部引擎命名为 "`Engine1` " 。此策略在策略配置中使用默认值：
     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
     -events event1 -engine engine1
     ```

     以下命令将创建一个名为 "`policy2` " 的策略，其中包含名为 "`event2` " 的事件以及名为 "`engine2` " 的外部引擎。此策略配置为使用指定的用户名进行特权访问。已启用直通读取：

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

     以下命令将创建一个名为 "`native1` " 的策略，该策略与名为 "`event3` " 的事件关联。此策略使用原生引擎并在策略配置中使用默认值：

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
   ```

```
-events event3 -engine native
```

2. 使用验证FPolicy策略配置 `vserver fpolicy policy show` 命令：

   以下命令显示有关已配置的三个 FPolicy 策略的信息，其中包括以下信息：

   - 与策略关联的 SVM
   - 与策略关联的外部引擎
   - 与策略关联的事件
   - 是否需要强制筛查
   - 是否需要特权访问
     `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

创建 **FPolicy** 范围

创建 FPolicy 策略后，您需要创建 FPolicy 范围。在创建范围时，您可以将此范围与 FPolicy 策略相关联。范围用于定义适用 FPolicy 策略的边界。范围可以根据共享，导出策略，卷和文件扩展名包括或排除文件。

您需要的内容

必须填写 FPolicy 范围工作表。FPolicy 策略必须与关联的外部引擎一起存在（如果将此策略配置为使用外部 FPolicy 服务器），并且必须至少具有一个关联的 FPolicy 事件。

步骤

1. 使用创建FPolicy范围 `vserver fpolicy policy scope create` 命令：

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. 使用验证FPolicy范围配置 `vserver fpolicy policy scope show` 命令：

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

启用 **FPolicy** 策略

配置完 FPolicy 策略配置后，可以启用 FPolicy 策略。启用此策略可设置其优先级并开始监控此策略的文件访问。

您需要的内容

FPolicy 策略必须与关联的外部引擎一起存在（如果将此策略配置为使用外部 FPolicy 服务器），并且必须至少具有一个关联的 FPolicy 事件。FPolicy 策略范围必须存在，并且必须分配给 FPolicy 策略。

关于此任务

如果在 Storage Virtual Machine （ SVM ）上启用了多个策略，并且多个策略已订阅同一文件访问事件，则会使用此优先级。对于任何其他引擎，使用原生引擎配置的策略的优先级都高于策略，无论启用策略时为其分配的序列号如何。

> 无法在管理 SVM 上启用策略。

步骤

1. 使用启用FPolicy策略 `vserver fpolicy enable` 命令：

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. 使用验证是否已启用FPolicy策略 `vserver fpolicy show` 命令：

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                       Sequence
   Vserver          Policy Name          Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                    1  on       engine1
   ```

管理FPolicy配置

修改 FPolicy 配置

用于修改 FPolicy 配置的命令

您可以通过修改构成 FPolicy 配置的元素来修改 FPolicy 配置。您可以修改外部引擎， FPolicy 事件， FPolicy 范围和 FPolicy 策略。您还可以启用或禁用 FPolicy 策略。禁用 FPolicy 策略后，该策略的文件监控将停止。

建议在修改配置之前禁用 FPolicy 策略。

要修改的内容	使用此命令 …
外部引擎	`vserver fpolicy policy external-engine modify`
事件	`vserver fpolicy policy event modify`
范围	`vserver fpolicy policy scope modify`
策略	`vserver fpolicy policy modify`

有关详细信息，请参见命令的手册页。

启用或禁用 FPolicy 策略

配置完成后，您可以启用 FPolicy 策略。启用此策略可设置其优先级并开始监控此策略的文件访问。如果要停止对策略的文件访问监控，可以禁用 FPolicy 策略。

您需要的内容

启用 FPolicy 策略之前，必须完成 FPolicy 配置。

关于此任务

- 如果在 Storage Virtual Machine （ SVM ）上启用了多个策略，并且多个策略已订阅同一文件访问事件，则会使用此优先级。
- 对于任何其他引擎，使用原生引擎配置的策略的优先级都高于策略，无论启用策略时为其分配的序列号如何。
- 如果要更改 FPolicy 策略的优先级，必须禁用该策略，然后使用新序列号重新启用它。

步骤

1. 执行相应的操作：

如果您要 …	输入以下命令 …
启用 FPolicy 策略	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`

禁用 FPolicy 策略	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

显示有关 **FPolicy** 配置的信息

show 命令的工作原理

在显示有关FPolicy配置的信息以了解如何配置时、这将非常有用 `show` 命令有效。

答 `show` 不带其他参数的命令以摘要形式显示信息。此外、每 `show` 命令具有两个相同的互斥可选参数：`-instance` 和 `-fields`。

使用时 `-instance` 参数、带 `show` 命令、则命令输出将以列表格式显示详细信息。在某些情况下，详细输出可能会很长，并且包含的信息可能比您需要的更多。您可以使用 `-fields fieldname[,fieldname…]` 参数、用于自定义输出、使其仅显示指定字段的信息。您可以通过输入来标识您可以指定的字段 `?` 之后 `-fields` 参数。

> 的输出 `show` 命令 `-fields` 参数可能会显示与请求的字段相关的其他必需字段。

每 `show` command具有一个或多个可选参数、用于筛选该输出、并可用于缩小命令输出中显示的信息范围。您可以通过输入来确定哪些可选参数可用于命令 `?` 之后 `show` 命令：

。 `show` command支持UNIX模式和通配符、可用于匹配命令参数中的多个值。例如，您可以在指定值时使用通配符（*），NOT 运算符（!），OR 运算符（=），范围运算符（integer…integer），小于运算符（<），大于运算符（>），小于或等于运算符（<=）以及大于或等于运算符（>=）。

有关使用UNIX模式和通配符的详细信息、请参见 使用 ONTAP 命令行界面。

用于显示有关 **FPolicy** 配置的信息的命令

您可以使用 `fpolicy show` 用于显示有关FPolicy配置的信息的命令、包括有关FPolicy外部引擎、事件、范围和策略的信息。

要显示有关 FPolicy… 的信息	使用此命令 …
外部引擎	`vserver fpolicy policy external-engine show`
事件	`vserver fpolicy policy event show`
范围	`vserver fpolicy policy scope show`
策略	`vserver fpolicy policy show`

有关详细信息，请参见命令的手册页。

您可以显示有关 FPolicy 策略状态的信息，以确定策略是否已启用，配置为使用的外部引擎，策略的序列号以及与 FPolicy 策略关联的 Storage Virtual Machine （SVM）。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Policy name
- 策略序列号
- 策略状态

除了显示集群或特定 SVM 上配置的 FPolicy 策略的策略状态信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 `-instance` 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 `-fields` 参数以仅显示命令输出中指示的字段、或 `-fields ?` 以确定您可以使用哪些字段。

步骤

1. 使用相应命令显示有关 FPolicy 策略状态的筛选信息：

要显示有关策略的状态信息的信息	输入命令 …
在集群上	`vserver fpolicy show`
具有指定状态的	`vserver fpolicy show -status {on
off}`	在指定的 SVM 上
`vserver fpolicy show -vserver vserver_name`	使用指定的策略名称
`vserver fpolicy show -policy-name policy_name`	使用指定外部引擎的

示例

以下示例显示了有关集群上 FPolicy 策略的信息：

```
cluster1::> vserver fpolicy show
                                          Sequence
Vserver             Policy Name             Number  Status      Engine
------------------- ------------------- --------  ---------   ---------
FPolicy             cserver_policy      -         off         eng1
vs1.example.com     v1p1                -         off         eng2
vs1.example.com     v1p2                -         off         native
vs1.example.com     v1p3                -         off         native
vs1.example.com     cserver_policy      -         off         eng1
vs2.example.com     v1p1                3         on          native
vs2.example.com     v1p2                1         on          eng3
vs2.example.com     cserver_policy      2         on          eng1
```

显示有关已启用的 **FPolicy** 策略的信息

您可以显示有关已启用 FPolicy 策略的信息，以确定配置为使用的 FPolicy 外部引擎，策略的优先级以及 FPolicy 策略与哪个 Storage Virtual Machine （SVM）关联。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Policy name
- 策略优先级

您可以使用命令参数按指定条件筛选命令的输出。

步骤

1. 使用相应的命令显示有关已启用的 FPolicy 策略的信息：

要显示有关已启用策略的信息 …	输入命令 …
在集群上	`vserver fpolicy show-enabled`
在指定的 SVM 上	`vserver fpolicy show-enabled -vserver vserver_name`
使用指定的策略名称	`vserver fpolicy show-enabled -policy-name policy_name`
具有指定的序列号	`vserver fpolicy show-enabled -priority integer`

示例

以下示例显示了有关集群上已启用的 FPolicy 策略的信息：

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

管理 **FPolicy** 服务器连接

连接到外部 **FPolicy** 服务器

要启用文件处理，如果先前已终止连接，则可能需要手动连接到外部 FPolicy 服务器。达到服务器超时后或由于某些错误，连接将终止。或者，管理员也可以手动终止连接。

关于此任务

如果发生致命错误，则可以终止与 FPolicy 服务器的连接。解决导致致命错误的问题描述后，您必须手动重新连接到 FPolicy 服务器。

步骤

1. 使用连接到外部FPolicy服务器 `vserver fpolicy engine-connect` 命令：

   有关命令的详细信息，请参见手册页。

2. 使用验证外部FPolicy服务器是否已连接 `vserver fpolicy show-engine` 命令：

   有关命令的详细信息，请参见手册页。

断开与外部 **FPolicy** 服务器的连接

您可能需要手动断开与外部 FPolicy 服务器的连接。如果 FPolicy 服务器在处理通知请求时出现问题，或者您需要对 FPolicy 服务器执行维护，则可能需要执行此操作。

步骤

1. 使用断开与外部FPolicy服务器的连接 `vserver fpolicy engine-disconnect` 命令：

   有关命令的详细信息，请参见手册页。

2. 使用验证外部FPolicy服务器是否已断开连接 `vserver fpolicy show-engine` 命令：

   有关命令的详细信息，请参见手册页。

显示有关连接到外部 **FPolicy** 服务器的信息

您可以显示有关与集群或指定 Storage Virtual Machine （ SVM ）的外部 FPolicy 服务器

（FPolicy 服务器）连接的状态信息。此信息可帮助您确定连接了哪些 FPolicy 服务器。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- Node name
- FPolicy policy name
- FPolicy 服务器 IP 地址
- FPolicy 服务器状态
- FPolicy 服务器类型

除了显示有关集群或特定 SVM 上的 FPolicy 连接的信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 `-instance` 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 `-fields` 参数、以便在命令输出中仅显示指示的字段。您可以输入 `?` 之后 `-fields` 用于确定可以使用哪些字段的参数。

步骤

1. 使用相应的命令显示有关节点与 FPolicy 服务器之间连接状态的筛选信息：

要显示有关 FPolicy 服务器的连接状态信息 …	输入 …
您指定的	`vserver fpolicy show-engine -server IP_address`
指定的 SVM	`vserver fpolicy show-engine -vserver vserver_name`
附加了指定策略的	`vserver fpolicy show-engine -policy-name policy_name`
指定的服务器状态	`vserver fpolicy show-engine -server-status status` 服务器状态可以是以下状态之一： • `connected` • `disconnected` • `connecting` • `disconnecting`

指定类型	`vserver fpolicy show-engine -server-type type` FPolicy 服务器类型可以是以下类型之一： • `primary` • `secondary`
已因指定原因断开连接的	`vserver fpolicy show-engine -disconnect-reason text` 断开连接的原因可能有多种。以下是断开连接的常见原因： • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

示例

此示例显示了有关 SVM vs1.example.com 上 FPolicy 服务器的外部引擎连接的信息：

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                                Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

此示例仅显示有关已连接 FPolicy 服务器的信息：

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

显示有关 **FPolicy** 直通读取连接状态的信息

您可以显示有关与集群或指定 Storage Virtual Machine （ SVM ）的外部 FPolicy 服务器（ FPolicy 服务器）的 FPolicy 直通读取连接状态的信息。此信息可帮助您确定哪些 FPolicy 服务器具有直通读取数据连接，以及哪些 FPolicy 服务器的直通读取连接已断开。

关于此任务

如果未指定任何参数，则此命令将显示以下信息：

- SVM name
- FPolicy policy name
- Node name
- FPolicy 服务器 IP 地址
- FPolicy 直通读取连接状态

除了显示有关集群或特定 SVM 上的 FPolicy 连接的信息之外，您还可以使用命令参数按其他条件筛选命令的输出。

您可以指定 `-instance` 用于显示有关列出策略的详细信息的参数。或者、您也可以使用 `-fields` 参数、以便在命令输出中仅显示指示的字段。您可以输入 `?` 之后 `-fields` 用于确定可以使用哪些字段的参数。

步骤

1. 使用相应的命令显示有关节点与 FPolicy 服务器之间连接状态的筛选信息：

要显示连接状态信息的对象	输入命令 ...
集群的 FPolicy 直通读取连接状态	`vserver fpolicy show-passthrough-read-connection`
指定 SVM 的 FPolicy 直通读取连接状态	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定策略的 FPolicy 直通读取连接状态	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定策略的详细 FPolicy 直通读取连接状态	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

指定状态的 FPolicy 直通读取连接状态	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` 服务器状态可以是以下状态之一： • `connected` • `disconnected`

示例

以下命令显示有关集群上所有 FPolicy 服务器的直通读取连接的信息：

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

以下命令显示有关在 "`pol_cifs_1` " 策略中配置的 FPolicy 服务器的直通读取连接的详细信息：

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                             Node: FPolicy-01
                                          Vserver: vs1.example.com
                                           Policy: pol_cifs_1
                                           Server: 1.1.1.1
                 Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                     Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

使用安全跟踪验证访问

安全跟踪的工作原理

您可以添加权限跟踪筛选器，以指示 ONTAP 记录有关 Storage Virtual Machine （SVM）上的 SMB 和 NFS 服务器为何允许或拒绝客户端或用户执行操作的请求的信息。如果要验证文件访问安全方案是否合适，或者要对文件访问问题进行故障排除，则此功能非常有用。

通过安全跟踪，您可以配置一个筛选器，以便通过 SMB 和 NFS 在 SVM 上检测客户端操作，并跟踪与该筛选器匹配的所有访问检查。然后，您可以查看跟踪结果，其中提供了允许或拒绝访问的原因的方便摘要。

如果要验证 SVM 上文件和文件夹的 SMB 或 NFS 访问安全设置，或者遇到访问问题，可以快速添加一个筛选器以启用权限跟踪。

以下列表概括了有关安全跟踪工作原理的重要信息：

- ONTAP 会在 SVM 级别应用安全跟踪。
- 系统会对每个传入请求进行筛选，以查看其是否符合任何已启用安全跟踪的筛选条件。
- 对文件和文件夹访问请求都执行跟踪。
- 跟踪可以根据以下条件进行筛选：
  - 客户端IP
  - SMB 或 NFS 路径
  - Windows 名称
  - UNIX名称
- 系统会对请求进行筛选，以查看 _allowed*and _denied* 访问响应结果。
- 已启用跟踪的每个请求匹配筛选条件都会记录在跟踪结果日志中。
- 存储管理员可以对筛选器配置超时以自动将其禁用。
- 如果某个请求与多个筛选器匹配，则会记录索引编号最高的筛选器的结果。
- 存储管理员可以打印跟踪结果日志中的结果，以确定允许或拒绝访问请求的原因。

访问类型会检查安全跟踪监控器

文件或文件夹的访问检查基于多个条件进行。安全跟踪可监控所有这些条件的操作。

安全跟踪所监控的访问检查类型包括：

- 卷和 qtree 安全模式
- 包含请求操作的文件和文件夹的文件系统的有效安全性
- 用户映射
- 共享级别权限
- 导出级别权限
- 文件级权限
- 存储级别访问防护安全性

创建安全跟踪时的注意事项

在 Storage Virtual Machine （ SVM ）上创建安全跟踪时，应牢记几个注意事项。例如，您需要了解可以创建跟踪的协议，支持的安全模式以及活动跟踪的最大数量。

- 您只能在 SVM 上创建安全跟踪。
- 每个安全跟踪筛选器条目都是特定于 SVM 的。

  您必须指定要在其中运行跟踪的 SVM 。

- 您可以为 SMB 和 NFS 请求添加权限跟踪筛选器。
- 您必须在要创建跟踪筛选器的SVM上设置SMB或NFS服务器。
- 您可以为 NTFS ， UNIX 以及混合安全模式卷和 qtree 上的文件和文件夹创建安全跟踪。
- 每个 SVM 最多可以添加 10 个权限跟踪筛选器。
- 创建或修改筛选器时，必须指定筛选器索引编号。

  筛选器将按索引编号的顺序进行考虑。索引编号较高的筛选器中的条件将在索引编号较低的条件之前进行考虑。如果要跟踪的请求与多个已启用筛选器中的条件匹配，则仅会触发索引编号最高的筛选器。

- 创建并启用安全跟踪筛选器后，您必须在客户端系统上执行一些文件或文件夹请求，以生成跟踪筛选器可以捕获并登录到跟踪结果日志的活动。
- 您应添加权限跟踪筛选器，以便进行文件访问验证或进行故障排除。

  添加权限跟踪筛选器对控制器性能的影响较小。

  完成验证或故障排除活动后，您应禁用或删除所有权限跟踪筛选器。此外，您选择的筛选条件应尽可能具体，以便 ONTAP 不会向日志发送大量跟踪结果。

执行安全跟踪

执行安全跟踪概述

执行安全跟踪涉及创建安全跟踪筛选器，验证筛选条件，在符合筛选条件的 SMB 或 NFS 客户端上生成访问请求以及查看结果。

在使用安全筛选器捕获跟踪信息后，您可以修改此筛选器并重复使用它，或者在不再需要时将其禁用。查看并分析筛选器跟踪结果后，如果不再需要，您可以将其删除。

创建安全跟踪筛选器

您可以创建安全跟踪筛选器来检测 Storage Virtual Machine （ SVM ）上的 SMB 和 NFS 客户端操作，并跟踪与此筛选器匹配的所有访问检查。您可以使用安全跟踪的结果来验证配置或对访问问题进行故障排除。

关于此任务

vserver security trace filter create 命令需要两个参数：

所需参数	Description

`-vserver vserver_name`	_SVM 名称 _ 包含要应用安全跟踪筛选器的文件或文件夹的 SVM 的名称。
`-index index_number`	筛选索引号 _ 要应用于筛选器的索引编号。每个 SVM 最多只能有 10 个跟踪筛选器。此参数允许的值为 1 到 10 。

您可以使用多个可选筛选器参数自定义安全跟踪筛选器，以便缩小安全跟踪生成的结果范围：

filter 参数	Description
`-client-ip IP_Address`	此筛选器指定用户从中访问 SVM 的 IP 地址。
`-path path`	此筛选器指定要应用权限跟踪筛选器的路径。的值 `-path` 可以使用以下格式之一： • 从共享或导出的根目录开始的完整路径 • 相对于共享根的部分路径 必须在路径值中使用 NFS 模式目录 UNIX 模式目录分隔符。
`-windows-name win_user_name` 或 `-unix -name``unix_user_name`	您可以指定要跟踪其访问请求的 Windows 用户名或 UNIX 用户名。用户名变量不区分大小写。您不能在同一筛选器中同时指定 Windows 用户名和 UNIX 用户名。 ⓘ 即使您可以跟踪 SMB 和 NFS 访问事件，在对混合或 UNIX 安全模式数据执行访问检查时，也可能会使用映射的 UNIX 用户和映射的 UNIX 用户组。
`-trace-allow {yes`	`no}`
对于安全跟踪筛选器，始终会启用对拒绝事件的跟踪。您可以选择跟踪允许事件。要跟踪允许事件、请将此参数设置为 `yes`。	`-enabled {enabled`
`disabled}`	您可以启用或禁用安全跟踪筛选器。默认情况下，安全跟踪筛选器处于启用状态。
`-time-enabled integer`	您可以为筛选器指定超时时间，超过此超时时间后将其禁用。

步骤

1. 创建安全跟踪筛选器：

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

`filter_parameters` 是可选筛选器参数的列表。

有关详细信息，请参见命令的手册页。

2. 验证安全跟踪筛选器条目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

示例

以下命令将为使用共享路径访问文件的任何用户创建安全跟踪筛选器 `\\server\share1\dir1\dir2\file.txt` 从IP地址10.10.10.7。筛选器将使用的完整路径 `-path` 选项用于访问数据的客户端 IP 地址为 10.10.10.7 。筛选器在 30 分钟后超时：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

以下命令使用的相对路径创建安全跟踪筛选器 `-path` 选项此筛选器会跟踪名为 "`Joe` " 的 Windows 用户的访问权限。Joe正在访问具有共享路径的文件 `\\server\share1\dir1\dir2\file.txt`。筛选器跟踪允许和拒绝事件：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                 Vserver: vs1
                            Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

显示有关安全跟踪筛选器的信息

您可以显示有关在 Storage Virtual Machine （ SVM ）上配置的安全跟踪筛选器的信息。

这样，您可以查看每个筛选器跟踪的访问事件类型。

步骤

1. 使用显示有关安全跟踪筛选器条目的信息 `vserver security trace filter show` 命令：

   有关使用此命令的详细信息，请参见手册页。

示例

以下命令显示有关 SVM vs1 上所有安全跟踪筛选器的信息：

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

显示安全跟踪结果

您可以显示为与安全跟踪筛选器匹配的文件操作生成的安全跟踪结果。您可以使用结果验证文件访问安全配置，或者对 SMB 和 NFS 文件访问问题进行故障排除。

您需要的内容

必须存在已启用的安全跟踪筛选器，并且必须已从与安全跟踪筛选器匹配的 SMB 或 NFS 客户端执行操作，才能生成安全跟踪结果。

关于此任务

您可以显示所有安全跟踪结果的摘要，也可以通过指定可选参数来自定义输出中显示的信息。如果安全跟踪结果包含大量记录，则此操作可能会很有用。

如果未指定任何可选参数，则会显示以下内容：

- Storage Virtual Machine （ SVM ）名称
- Node name
- 安全跟踪索引编号
- 安全风格
- 路径
- reason
- 用户名

  根据跟踪筛选器的配置方式显示用户名：

如果筛选器已配置 …	那么 …
使用 UNIX 用户名	安全跟踪结果将显示 UNIX 用户名。
使用 Windows 用户名	安全跟踪结果将显示 Windows 用户名。
没有用户名	安全跟踪结果将显示 Windows 用户名。

您可以使用可选参数自定义输出。可用于缩小命令输出中返回的结果范围的一些可选参数包括：

可选参数	Description
`-fields field_name，…`	显示所选字段的输出。您可以单独使用此参数，也可以与其他可选参数结合使用。
`-instance`	显示有关安全跟踪事件的详细信息。将此参数与其他可选参数结合使用可显示有关特定筛选器结果的详细信息。
`-node node_name`	仅显示有关指定节点上的事件的信息。
`-vserver vserver_name`	仅显示有关指定 SVM 上的事件的信息。
`-index integer`	显示有关因与指定索引编号对应的筛选器而发生的事件的信息。
`-client-ip IP_address`	显示有关从指定客户端 IP 地址访问文件而发生的事件的信息。
`-path path`	显示有关通过文件访问指定路径而发生的事件的信息。
`-user-name user_name`	显示有关指定 Windows 或 UNIX 用户访问文件时发生的事件的信息。
`-security-style security_style`	显示有关使用指定安全模式的文件系统上发生的事件的信息。

有关可与命令结合使用的其他可选参数的信息，请参见手册页。

步骤

1. 使用显示安全跟踪筛选器结果 `vserver security trace trace-result show` 命令：

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

```
Vserver: vs1

Node     Index   Filter Details         Reason
-------- ------- ---------------------  ------------------------------
node1    3       User:domain\user       Access denied by explicit ACE
                 Security Style:mixed
                 Path:/dir1/dir2/

node1    5       User:domain\user       Access denied by explicit ACE
                 Security Style:unix
                 Path:/dir1/
```

修改安全跟踪筛选器

如果要更改用于确定跟踪哪些访问事件的可选筛选器参数，可以修改现有的安全跟踪筛选器。

关于此任务

您必须指定要修改的安全跟踪筛选器，方法是指定应用此筛选器的 Storage Virtual Machine （ SVM ）名称以及此筛选器的索引编号。您可以修改所有可选筛选器参数。

步骤

1. 修改安全跟踪筛选器：

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` 是要应用安全跟踪筛选器的SVM的名称。
   - `index_number` 是要应用于筛选器的索引编号。此参数允许的值为 1 到 10 。
   - `filter_parameters` 是可选筛选器参数的列表。

2. 验证安全跟踪筛选器条目：

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

示例

以下命令将使用索引编号 1 修改安全跟踪筛选器。筛选器可跟踪使用共享路径访问文件的任何用户的事件 `\\server\share1\dir1\dir2\file.txt` 从任何IP地址。筛选器将使用的完整路径 `-path` 选项筛选器跟踪允许和拒绝事件：

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                 Vserver: vs1
                            Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                      Windows User Name: -
                         UNIX User Name: -
                     Trace Allow Events: yes
                         Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

删除安全跟踪筛选器

如果不再需要安全跟踪筛选器条目，可以将其删除。由于每个 Storage Virtual Machine （SVM ）最多可以有 10 个安全跟踪筛选器，因此，如果已达到最大值，则可以通过删除不需要的筛选器来创建新筛选器。

关于此任务

要唯一标识要删除的安全跟踪筛选器，必须指定以下内容：

- 应用跟踪筛选器的 SVM 的名称
- 跟踪筛选器的筛选器索引编号

步骤

1. 确定要删除的安全跟踪筛选器条目的筛选器索引编号：

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  -----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. 使用上一步中的筛选器索引编号信息删除筛选器条目：

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. 验证是否已删除安全跟踪筛选器条目：

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

```
Vserver   Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

删除安全跟踪记录

在使用筛选器跟踪记录验证文件访问安全性或对 SMB 或 NFS 客户端访问问题进行故障排除后，您可以从安全跟踪日志中删除此安全跟踪记录。

关于此任务

在删除安全跟踪记录之前，您必须知道该记录的序列号。

> 每个 Storage Virtual Machine （ SVM ）最多可存储 128 条跟踪记录。如果 SVM 上达到最大值，则添加新跟踪记录时，最早的跟踪记录将自动删除。如果您不想手动删除此 SVM 上的跟踪记录，可以让 ONTAP 在达到最大值后自动删除最旧的跟踪结果，以便为新结果腾出空间。

步骤

1. 确定要删除的记录的序列号：

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. 删除安全跟踪记录：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer

vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

   - `-node node_name` 是发生要删除的权限跟踪事件的集群节点的名称。

     这是必需的参数。

   - `-vserver vserver_name` 是发生要删除的权限跟踪事件的SVM的名称。

     这是必需的参数。

- `-seqnum integer` 是要删除的日志事件的序列号。

  这是必需的参数。

删除所有安全跟踪记录

如果您不想保留任何现有安全跟踪记录，则只需使用一个命令即可删除节点上的所有记录。

步骤

1. 删除所有安全跟踪记录：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

   - `-node node_name` 是发生要删除的权限跟踪事件的集群节点的名称。
   - `-vserver vserver_name` 是发生要删除的权限跟踪事件的Storage Virtual Machine (SVM)的名称。

解释安全跟踪结果

安全跟踪结果提供了允许或拒绝请求的原因。输出将结果显示为允许或拒绝访问的原因以及访问检查路径中允许或拒绝访问的位置的组合。您可以使用结果隔离并确定允许或不允许执行操作的原因。

查找有关结果类型列表和筛选器详细信息的信息

您可以在的手册页中找到可包含在安全跟踪结果中的结果类型和筛选器详细信息列表 `vserver security trace trace-result show` 命令：

的输出示例 `Reason` 字段 `Allow` 结果类型

以下是的输出示例 `Reason` 中的跟踪结果日志中显示的字段 `Allow` 结果类型：

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

的输出示例 `Reason` 字段 `Allow` 结果类型

以下是的输出示例 `Reason` 中的跟踪结果日志中显示的字段 `Deny` 结果类型：

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

的输出示例 `Filter details` 字段

以下是的输出示例 `Filter details` 跟踪结果日志中的字段、其中列出了文件系统的有效安全模式、该文件系统包含与筛选条件匹配的文件和文件夹：

```
Security Style: MIXED and ACL
```

从何处查找追加信息

成功测试SMB客户端访问之后、您可以执行高级SMB配置或添加SAN访问。成功测试NFS 客户端访问后，您可以执行高级 NFS 配置或添加 SAN 访问。协议访问完成后，您应保护 SVM 的根卷。

SMB配置

您可以使用以下命令进一步配置SMB访问：

- "SMB管理"

  介绍如何使用SMB协议配置和管理文件访问。

- "NetApp 技术报告 4191 ：《集群模式 Data ONTAP 8.2 Windows 文件服务最佳实践指南》"

  简要概述 SMB 实施和其他 Windows 文件服务功能，并提供有关 ONTAP 的建议和基本故障排除信息。

- "NetApp 技术报告 3740 ：《 Data ONTAP 中的 SMB 2 下一代 CIFS 协议》"

  介绍 SMB 2 的功能，配置详细信息及其在 ONTAP 中的实施。

NFS配置

您可以使用以下命令进一步配置NFS访问：

- "NFS 管理"

  介绍如何使用 NFS 协议配置和管理文件访问。

- "NetApp 技术报告 4067 ：《 NFS 最佳实践和实施指南》"

  可作为 NFSv3 和 NFSv4 操作指南，简要介绍 ONTAP 操作系统，重点介绍 NFSv4 。

- "NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

  提供了一个全面的最佳实践，限制，建议和注意事项列表，用于配置 LDAP ， NIS ， DNS 以及本地用户和组文件以进行身份验证。

- "NetApp 技术报告 4616 ：《采用 Microsoft Active Directory 的 ONTAP 中的 NFS Kerberos 》"
- "NetApp 技术报告 4835 ：《如何在 ONTAP 中配置 LDAP 》"
- "NetApp 技术报告 3580 ：《 NFSv4 增强功能和最佳实践指南： Data ONTAP 实施》"

介绍在连接到运行 ONTAP 的系统的 AIX， Linux 或 Solaris 客户端上实施 NFSv4 组件时应遵循的最佳实践。

根卷保护

在 SVM 上配置协议后，您应确保其根卷受到保护：

- "数据保护"

  介绍如何创建负载共享镜像以保护 SVM 根卷，这是适用于已启用 NAS 的 SVM 的 NetApp 最佳实践。此外，还介绍如何通过从负载共享镜像提升 SVM 根卷来快速从卷故障或丢失中恢复。

使用 System Manager 管理加密

使用基于软件的加密对存储的数据进行加密

使用卷加密可确保在底层设备被重新利用，退回，放置在不当位置或被盗时无法读取卷数据。卷加密不需要特殊磁盘；它适用于所有 HDD 和 SSD 。

卷加密需要密钥管理器。您可以使用 System Manager 配置板载密钥管理器。您也可以使用外部密钥管理器，但需要先使用 ONTAP 命令行界面进行设置。

配置密钥管理器后，新卷会默认加密。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在 * 加密 * 下，单击 首次配置板载密钥管理器。
3. 要对现有卷进行加密，请单击 * 存储 > 卷 * 。
4. 在所需卷上，单击 然后单击 * 编辑 * 。
5. 选择 * 启用加密 * 。

使用自加密驱动器对存储的数据进行加密

使用磁盘加密可确保在底层设备被重新利用，退回，放置在不当位置或被盗时无法读取本地层中的所有数据。磁盘加密需要特殊的自加密 HDD 或 SSD 。

磁盘加密需要密钥管理器。您可以使用 System Manager 配置板载密钥管理器。 您也可以使用外部密钥管理器，但需要先使用 ONTAP 命令行界面进行设置。

如果 ONTAP 检测到自加密磁盘，则会在创建本地层时提示您配置板载密钥管理器。

步骤

1. 在 * 加密 * 下，单击 配置板载密钥管理器。
2. 如果您看到需要重新设置磁盘密钥的消息，请单击 ，然后单击 * 重新设置磁盘密钥 * 。

使用 CLI 管理加密

NetApp加密概述

NetApp 提供了基于软件和基于硬件的加密技术，可确保在存储介质被重新利用，退回，放置在不当位置或被盗时无法读取空闲数据。

- 使用NetApp卷加密(NVE)的基于软件的加密支持一次对一个卷进行数据加密
- 使用NetApp存储加密(NetApp Storage Encryption、NSE)的基于硬件的加密支持在数据写入时对其进行全磁盘加密(FDE)。

配置 NetApp 卷加密

配置 NetApp 卷加密概述

NetApp 卷加密（ NVE ）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。只有存储系统可以访问的加密密钥可确保在底层设备被重新利用，退回，放置在不当位置或被盗时无法读取卷数据。

了解 NVE

使用NVE时、元数据和数据(包括Snapshot副本)均会加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。外部密钥管理服务器或板载密钥管理器(Onboard Key Manager、OKM)为节点提供密钥：

- 外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供密钥。最佳做法是，在与数据不同的存储系统上配置外部密钥管理服务器。
- 板载密钥管理器是一个内置工具，可为数据所在存储系统中的节点提供密钥。

从 ONTAP 9.7 开始，如果您拥有卷加密（ Volume Encryption ， VE ）许可证并使用板载或外部密钥管理器，则默认情况下会启用聚合和卷加密。VE许可证随一起提供 "ONTAP One"。每当配置外部或板载密钥管理器时，为全新聚合和全新卷配置空闲数据加密的方式都会发生变化。默认情况下，全新聚合将启用 NetApp 聚合加密（ NAE ）。默认情况下，不属于 NAE 聚合的全新卷将启用 NetApp 卷加密（ NVE ）。如果使用多租户密钥管理为数据存储虚拟机（ SVM ）配置了自己的密钥管理器，则为该 SVM 创建的卷将自动配置 NVE 。

您可以对新卷或现有卷启用加密。NVE 支持所有存储效率功能，包括重复数据删除和数据压缩。从ONTAP 9.14.1开始、您可以执行此操作 在现有SVM根卷上启用NVE。

> 如果您使用的是 SnapLock ，则只能对新的空 SnapLock 卷启用加密。您不能在现有 SnapLock 卷上启用加密。

您可以在任何类型的聚合（ HDD ， SSD ，混合，阵列 LUN ）上使用任何 RAID 类型以及任何受支持的 ONTAP 实施（包括 ONTAP Select ）中使用 NVE 。您还可以将 NVE 与基于硬件的加密结合使用，在 d自加密驱动器上 " 双重加密 " 数据。

启用NVE后、核心转储也会进行加密。

聚合级加密

通常，每个加密卷都分配有一个唯一的密钥。删除卷后，此密钥将随之删除。

从 ONTAP 9.6 开始，您可以使用 _NetApp 聚合加密（ NAE ） _ 为要加密的卷所在的聚合分配密钥。删除加密卷后，聚合的密钥将保留下来。如果删除整个聚合、则这些密钥将被删除。

如果计划执行实时或后台聚合级重复数据删除，则必须使用聚合级加密。否则， NVE 不支持聚合级重复数据删除。

从 ONTAP 9.7 开始，如果您拥有卷加密（ Volume Encryption ， VE ）许可证并使用板载或外部密钥管理器，则默认情况下会启用聚合和卷加密。

NVE 和 NAE 卷可以同时位于同一聚合上。默认情况下，在聚合级别加密下加密的卷为 NAE 卷。对卷进行加密时，您可以覆盖默认值。

您可以使用 `volume move` 命令将NVE卷转换为NAE卷、反之亦然。您可以将 NAE 卷复制到 NVE 卷。

您不能使用 `secure purge` NAE卷上的命令。

何时使用外部密钥管理服务器

尽管使用板载密钥管理器成本较低且通常更方便，但如果满足以下任一条件，则应设置 KMIP 服务器：

- 您的加密密钥管理解决方案必须符合联邦信息处理标准（ FIPS ） 140-2 或 OASIS KMIP 标准。
- 您需要一个具有集中管理加密密钥的多集群解决方案。
- 您的企业需要将身份验证密钥存储在系统或与数据不同的位置，从而提高安全性。

外部密钥管理的范围

外部密钥管理的范围决定了密钥管理服务器是保护集群中的所有 SVM 还是仅保护选定 SVM ：

- 您可以使用 *cluster scopter* 为集群中的所有 SVM 配置外部密钥管理。集群管理员可以访问存储在服务器上的每个密钥。
- 从 ONTAP 9.6 开始，您可以使用 *SVM scopter* 为集群中的指定 SVM 配置外部密钥管理。这最适合多租户环境，其中每个租户都使用不同的 SVM （或一组 SVM ）来提供数据。只有给定租户的 SVM 管理员才能访问该租户的密钥。
- 从 ONTAP 9.10.1 开始，您可以使用 Azure 密钥存储和 Google Cloud KMS 仅保护数据SVM的NVE密钥。从9.12.0开始、此功能可用于AWS的KMS。

您可以在同一集群中使用这两个范围。如果为 SVM 配置了密钥管理服务器，则 ONTAP 仅使用这些服务器来保护密钥。否则， ONTAP 将使用为集群配置的密钥管理服务器来保护密钥。

中提供了经过验证的外部密钥管理器列表 "NetApp 互操作性表工具（ IMT ）"。您可以通过在IMT的搜索功能中输入术语"密钥管理器"来查找此列表。

支持详细信息

下表显示了 NVE 支持详细信息：

资源或功能	支持详细信息

平台	需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 NVE 和 NAE 。

加密	从 ONTAP 9.7 开始，在添加卷加密（ Volume Encryption ， VE ）许可证并配置板载或外部密钥管理器时，新创建的聚合和卷会默认加密。如果需要创建未加密的聚合，请使用以下命令：
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	如果需要创建纯文本卷，请使用以下命令：
	
	`volume create -encrypt false`
	
	在以下情况下，默认情况下不启用加密：
	
	• 未安装 Ve 许可证。
	• 未配置密钥管理器
	• 平台或软件不支持加密
	• 已启用硬件加密

ONTAP	所有 ONTAP 实施。ONTAP 9.5 及更高版本支持 ONTAP 云。
设备	HDD ， SSD ，混合，阵列 LUN 。
RAID	RAID0 ， RAID4 ， RAID-DP ， RAID-TEC 。
Volumes	数据卷和现有SVM根卷。您不能对MetroCluster元数据卷上的数据进行加密。在9.14.1之前的ONTAP版本中、不能使用NVE对SVM根卷上的数据进行加密。从ONTAP 9.14.1开始、ONTAP支持 SVM根卷上的NVE。
聚合级加密	从 ONTAP 9.6 开始， NVE 支持聚合级加密（ Aggregate-Level Encryption ， NAE ）： • 如果计划执行实时或后台聚合级重复数据删除，则必须使用聚合级加密。 • 您不能为聚合级别的加密卷重新设置密钥。 • 聚合级加密卷不支持安全清除。 • 除了数据卷之外， NAE 还支持对 SVM 根卷和 MetroCluster 元数据卷进行加密。NAE 不支持对根卷进行加密。
SVM 范围	从 ONTAP 9.6 开始， NVE 仅支持用于外部密钥管理的 SVM 范围，而不支持板载密钥管理器。从 ONTAP 9.8 开始，支持 MetroCluster 。

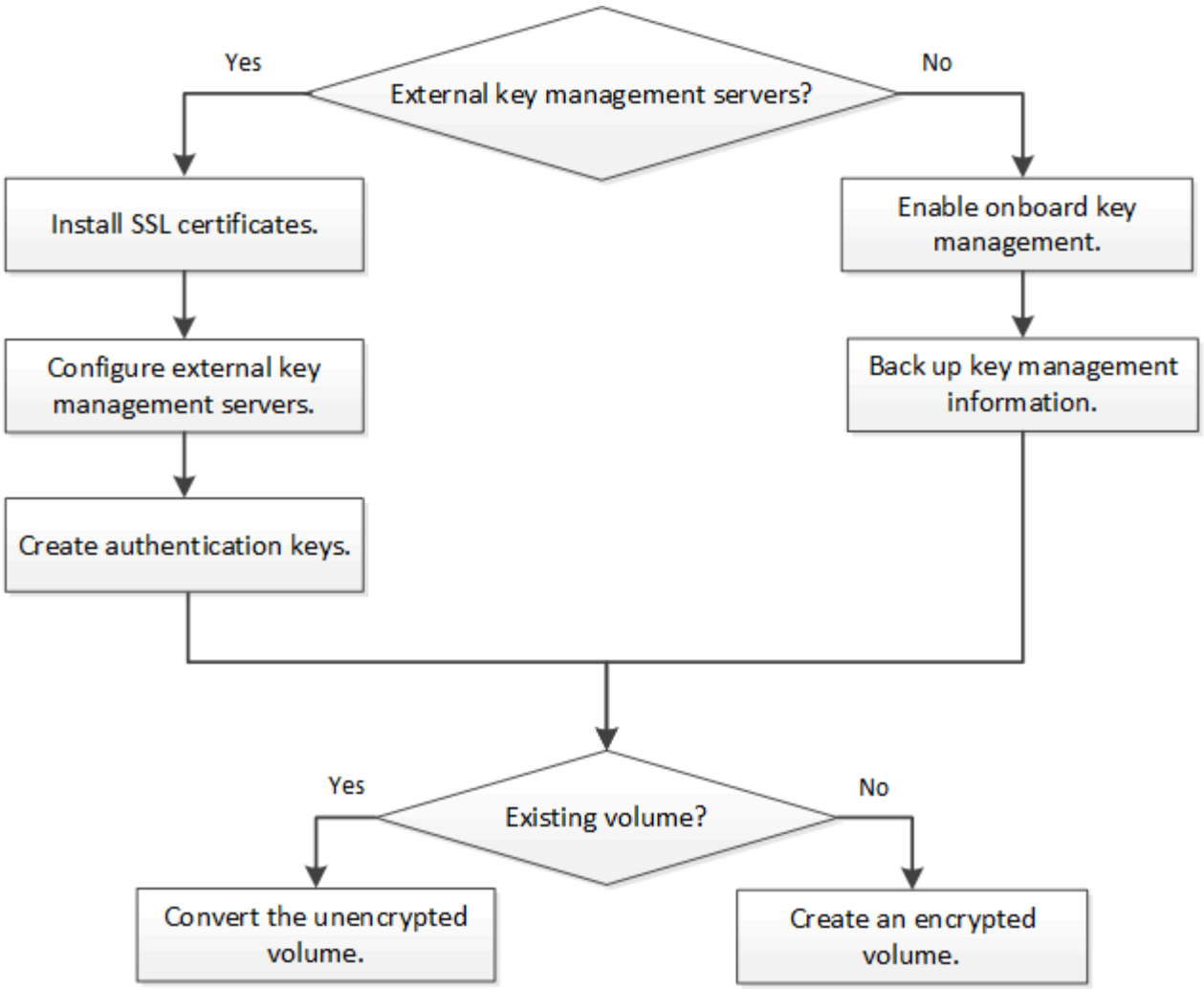
存储效率	重复数据删除，数据压缩，数据缩减， FlexClone 。 即使从父级拆分克隆后，克隆也会使用与父级相同的密钥。您应执行 `volume move` 在拆分的克隆上、之后、拆分的克隆将具有不同的密钥。
Replication	• 对于卷复制、源卷和目标卷可以具有不同的加密设置。可以为源配置加密，也可以为目标取消配置加密，反之亦然。 • 对于 SVM 复制，目标卷会自动加密，除非目标卷不包含支持卷加密的节点（在这种情况下复制成功，但目标卷不会加密）。 • 对于 MetroCluster 配置，每个集群从其配置的密钥服务器中提取外部密钥管理密钥。配置复制服务会将 OKM 密钥复制到配对站点。
合规性	从 ONTAP 9.2 开始， SnapLock 在合规和企业模式下均受支持，仅适用于新卷。您不能在现有 SnapLock 卷上启用加密。
FlexGroup	从 ONTAP 9.2 开始，支持 FlexGroup 。目标聚合的类型必须与源聚合相同，可以是卷级聚合，也可以是聚合级聚合。从 ONTAP 9.5 开始，支持对 FlexGroup 卷进行原位重新设置密钥。
7- 模式过渡	从 7- 模式过渡工具 3.3 开始，您可以使用 7- 模式过渡工具命令行界面对集群系统上启用了 NVE 的目标卷执行基于副本的过渡。

相关信息

"常见问题解答—NetApp卷加密和NetApp聚合加密"

NetApp 卷加密工作流

必须先配置密钥管理服务，然后才能启用卷加密。您可以对新卷或现有卷启用加密。



"您必须安装VE许可证" 并配置密钥管理服务、然后才能使用NVE加密数据。 在安装许可证之前，您应先执行此操作 "确定您的 ONTAP 版本是否支持 NVE"。

配置NVE

确定您的集群版本是否支持 NVE

在安装许可证之前，您应确定集群版本是否支持 NVE 。您可以使用 `version` 命令以确定集群版本。

关于此任务

集群版本是集群中任何节点上运行的最低 ONTAP 版本。

步骤

1. 确定您的集群版本是否支持 NVE ：

   ```
   version -v
   ```

   如果命令输出显示文本 "`1Ono-dare` " （对于 "`no Data at Rest Encryption` " ），或者您使用的平台未在中列出，则不支持 NVE "支持详细信息"。

以下命令可确定上是否支持NVE `cluster1`。

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

的输出 `1Ono-DARE` 表示您的集群版本不支持NVE。

安装许可证

VE 许可证使您有权在集群中的所有节点上使用此功能。要使用NVE对数据进行加密、必须先获得此许可证。随一起提供 "ONTAP One"。

在ONTAP One之前、加密包附带VE许可证。加密包不再提供、但仍然有效。虽然目前不需要、但现有客户可以选择这样做 "升级到ONTAP One"。

开始之前

- 您必须是集群管理员才能执行此任务。
- 您必须已从销售代表处收到VE许可证密钥、或者已安装ONTAP One。

步骤

1. "验证是否已安装VE许可证"。

   VE许可证包名称为 `VE`。

2. 如果未安装许可证、 "使用System Manager或ONTAP命令行界面安装它"。

配置外部密钥管理

配置外部密钥管理概述

您可以使用一个或多个外部密钥管理服务器来保护集群用于访问加密数据的密钥。外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）为节点提供密钥。

> 对于 ONTAP 9.1 及更早版本，必须先将节点管理 LIF 分配给已配置节点管理角色的端口，然后才能使用外部密钥管理器。

NetApp 卷加密（NVE）在 ONTAP 9.1 及更高版本中支持板载密钥管理器。从ONTAP 9.3开始、NVE支持外部密钥管理(KMIP)和板载密钥管理器。从 ONTAP 9.10.1 开始，您可以使用 Azure密钥存储或Google Cloud密钥管理器服务 保护NVE密钥。从ONTAP 9.11.1开始、您可以在一个集群中配置多个外部密钥管理器。请参见 配置集群模式密钥服务器。

使用**System Manager**管理外部密钥管理器

从ONTAP 9.7开始、您可以使用板载密钥管理器存储和管理身份验证和加密密钥。从ONTAP 9.131开始、您还可以使用外部密钥管理器来存储和管理这些密钥。

板载密钥管理器将密钥存储在集群内部的安全数据库中并对其进行管理。其范围为集群。外部密钥管理器可在集群外部存储和管理密钥。其范围可以是集群或Storage VM。可以使用一个或多个外部密钥管理器。需满足以下条件：

- 如果启用了板载密钥管理器、则无法在集群级别启用外部密钥管理器、但可以在Storage VM级别启用外部密钥管理器。
- 如果在集群级别启用了外部密钥管理器、则无法启用板载密钥管理器。

使用外部密钥管理器时、每个Storage VM和集群最多可以注册四个主密钥服务器。每个主密钥服务器最多可与三个二级密钥服务器组成集群。

配置外部密钥管理器

要为Storage VM添加外部密钥管理器、您应在为Storage VM配置网络接口时添加可选网关。如果创建的Storage VM没有网络路由、则必须为外部密钥管理器明确创建路由。请参见 "创建LIF (网络接口)"。

步骤

您可以从System Manager中的不同位置开始配置外部密钥管理器。

1. 要配置外部密钥管理器、请执行以下开始步骤之一。

工作流	导航	开始步骤
配置密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下、选择 ⚙。选择*外部密钥管理器*。
添加本地层	存储>*层*	选择*+添加本地层*。选中标有"配置密钥管理器"的复选框。选择*外部密钥管理器*。
准备存储	信息板	在*容量*部分中，选择*准备存储*。 然后、选择"配置密钥管理器"。选择*外部密钥管理器*。
配置加密(仅限Storage VM范围的密钥管理器)	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*安全性*下的*加密*部分中，选择 ⚙。

2. 要添加主密钥服务器、请选择 + Add ，然后填写“* IP地址或主机名*”和“端口”字段。
3. 已安装的现有证书列在*KMIP服务器CA证书*和*KMIP客户端证书*字段中。 您可以执行以下任一操作：
   - 选择 … ⌄ 选择要映射到密钥管理器的已安装证书。(可以选择多个服务CA证书、但只能选择一个客户端证书。)
   - 选择*添加新证书*以添加尚未安装的证书并将其映射到外部密钥管理器。
   - 选择 … × 旁边的证书名称可删除不想映射到外部密钥管理器的已安装证书。
4. 要添加辅助密钥服务器，请在*辅助密钥服务器*列中选择*Add*，并提供其详细信息。
5. 选择*保存*以完成配置。

编辑现有外部密钥管理器

如果您已配置外部密钥管理器、则可以修改其设置。

步骤

1. 要编辑外部密钥管理器的配置、请执行以下开始步骤之一。

范围	导航	开始步骤
集群范围外部密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下、选择 ⋮，然后选择*编辑外部密钥管理器*。
Storage VM范围外部密钥管理器	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*安全性*下的*加密*部分中，选择 ⋮，然后选择*编辑外部密钥管理器*。

2. 现有密钥服务器列在*密钥服务器*表中。您可以执行以下操作：
   - 通过选择添加新密钥服务器 + Add 。
   - 通过选择删除密钥服务器 ⋮ 位于包含密钥服务器名称的表单元格的末尾。与该主密钥服务器关联的辅助密钥服务器也会从配置中删除。

删除外部密钥管理器

如果卷未加密、则可以删除外部密钥管理器。

步骤

1. 要删除外部密钥管理器、请执行以下步骤之一。

范围	导航	开始步骤
集群范围外部密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下、选择选择 ⋮，然后选择*删除外部密钥管理器*。
Storage VM范围外部密钥管理器	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*安全性*下的*加密*部分中，选择 ⋮，然后选择*删除外部密钥管理器*。

在密钥管理器之间迁移密钥

如果在集群上启用了多个密钥管理器、则必须将密钥从一个密钥管理器迁移到另一个密钥管理器。此过程可通过System Manager自动完成。

- 如果在集群级别启用了板载密钥管理器或外部密钥管理器、并且某些卷已加密、 然后、在Storage VM级别配置外部密钥管理器时、必须将这些密钥从集群级别的板载密钥管理器或外部密钥管理器迁移到Storage VM级别的外部密钥管理器。 此过程由System Manager自动完成。
- 如果在Storage VM上创建卷时未进行加密、则不需要迁移密钥。

在集群上安装 SSL 证书

集群和 KMIP 服务器使用 KMIP SSL 证书来验证彼此的身份并建立 SSL 连接。在配置与 KMIP 服务器的 SSL 连接之前，必须为集群安装 KMIP 客户端 SSL 证书，并为 KMIP 服务器的根证书颁发机构（CA）安装 SSL 公有证书。

关于此任务

在 HA 对中，两个节点必须使用相同的公有和专用 KMIP SSL 证书。如果将多个 HA 对连接到同一个 KMIP 服务器，则 HA 对中的所有节点都必须使用相同的公有和专用 KMIP SSL 证书。

开始之前

- 创建证书的服务器， KMIP 服务器和集群上的时间必须同步。
- 您必须已获取集群的公有 SSL KMIP 客户端证书。
- 您必须已获取与集群的 SSL KMIP 客户端证书关联的专用密钥。
- SSL KMIP 客户端证书不能受密码保护。
- 您必须已为 KMIP 服务器的根证书颁发机构（CA）获取 SSL 公有证书。
- 在MetroCluster环境中、您必须在两个集群上安装相同的KMIP SSL证书。

> 在集群上安装客户端和服务器证书之前或之后，您可以在 KMIP 服务器上安装这些证书。

步骤

1. 为集群安装 SSL KMIP 客户端证书：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系统将提示您输入 SSL KMIP 公有和专用证书。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 为 KMIP 服务器的根证书颁发机构（CA）安装 SSL 公有证书：

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

在 ONTAP 9.6 及更高版本（NVE）中启用外部密钥管理

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。从ONTAP 9.6开始、您可以选择配置一个单独的外部密钥管理器、以保护数据SVM用于访问加密数据的密钥。

从ONTAP 9.11.1开始、您可以为每个主密钥服务器最多添加3个二级密钥服务器、以创建集群模式密钥服务器。有关详细信息，请参见 配置集群模式外部密钥服务器。

关于此任务

您最多可以将四个 KMIP 服务器连接到一个集群或 SVM 。建议至少使用两台服务器来实现冗余和灾难恢复。

外部密钥管理的范围决定了密钥管理服务器是保护集群中的所有 SVM 还是仅保护选定 SVM：

- 您可以使用 *cluster scopter* 为集群中的所有 SVM 配置外部密钥管理。集群管理员可以访问存储在服务器上的每个密钥。
- 从 ONTAP 9.6 开始，您可以使用 *SVM scopter* 为集群中的数据 SVM 配置外部密钥管理。这最适合多租户环境，其中每个租户都使用不同的 SVM （或一组 SVM ）来提供数据。只有给定租户的 SVM 管理员才能访问该租户的密钥。
- 对于多租户环境，请使用以下命令为 *MT_EK_MGMT* 安装许可证：

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  有关完整的命令语法，请参见命令手册页。

您可以在同一集群中使用这两个范围。如果为 SVM 配置了密钥管理服务器，则 ONTAP 仅使用这些服务器来保护密钥。否则， ONTAP 将使用为集群配置的密钥管理服务器来保护密钥。

您可以在集群范围配置板载密钥管理，并在 SVM 范围配置外部密钥管理。您可以使用 `security key-manager key migrate` 命令将密钥从集群范围的板载密钥管理迁移到SVM范围的外部密钥管理器。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 要执行此任务，您必须是集群或 SVM 管理员。
- 如果要为 MetroCluster 环境启用外部密钥管理，则必须在启用外部密钥管理之前完全配置 MetroCluster 。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 配置集群的密钥管理器连接：

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ◦ 。 `security key-manager external enable` 命令用于替换 `security key-manager setup` 命令：如果在集群登录提示符处运行命令、 *`admin_SVM`* 默认为当前集群的管理SVM。 您必须是集群管理员才能配置集群范围。您可以运行 `security key-manager external modify` 用于更改外部密钥管理配置的命令。
   > ◦ 在MetroCluster 环境中、如果要为管理SVM配置外部密钥管理、则必须重复 `security key-manager external enable` 命令。

   以下命令将为启用外部密钥管理 `cluster1` 使用三个外部密钥服务器。第一个密钥服务器使用其主机名和端口指定，第二个密钥服务器使用 IP 地址和默认端口指定，第三个密钥服务器使用 IPv6 地址和端口指定：

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 配置密钥管理器 SVM：

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   > ◦ 如果在SVM登录提示符处运行命令、 `SVM` 默认为当前SVM。 您必须是集群或 SVM 管理员才能配置 SVM 范围。您可以运行 `security key-manager external modify` 用于更改外部密钥管理配置的命令。
   > ◦ 在MetroCluster 环境中、如果要为数据SVM配置外部密钥管理、则不必重复 `security key-manager external enable` 命令。

   以下命令将为启用外部密钥管理 `svm1` 使用单密钥服务器侦听默认端口5696：

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 对任何其他 SVM 重复最后一步。

   > 您也可以使用 `security key-manager external add-servers` 命令以配置其他 SVM。。 `security key-manager external add-servers` 命令用于替换 `security key-manager add` 命令：有关完整的命令语法，请参见手册页。

4. 验证所有已配置的 KMIP 服务器是否均已连接：

   `security key-manager external show-status -node node_name`

   > 。 `security key-manager external show-status` 命令用于替换 `security key-manager show -status` 命令：有关完整的命令语法，请参见手册页。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

   转换卷之前、必须完全配置外部密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置外部密钥管理器。

在 **ONTAP 9.5** 及更早版本中启用外部密钥管理

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。最多可以将四个 KMIP 服务器连接到一个节点。建议至少使用两台服务器来实现冗余和灾难恢复。

关于此任务

ONTAP 为集群中的所有节点配置 KMIP 服务器连接。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 您必须是集群管理员才能执行此任务。
- 在配置外部密钥管理器之前，您必须配置 MetroCluster 环境。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 为集群节点配置密钥管理器连接：

   ```
   security key-manager setup
   ```

   此时将启动密钥管理器设置。

   > 在MetroCluster 环境中、必须在两个集群上运行此命令。

2. 在每个提示符处输入相应的响应。
3. 添加 KMIP 服务器：

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > 在MetroCluster 环境中、必须在两个集群上运行此命令。

4. 添加额外的 KMIP 服务器以实现冗余：

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > 在MetroCluster 环境中、必须在两个集群上运行此命令。

5. 验证所有已配置的 KMIP 服务器是否均已连接：

   ```
   security key-manager show -status
   ```

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> security key-manager show -status

   Node             Port      Registered Key Manager  Status
   --------------   ----      ----------------------  ---------------
   cluster1-01      5696      20.1.1.1                available
   cluster1-01      5696      20.1.1.2                available
   cluster1-02      5696      20.1.1.1                available
   cluster1-02      5696      20.1.1.2                available
   ```

6. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

转换卷之前、必须完全配置外部密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置外部密钥管理器。

通过云提供商管理密钥

从 ONTAP 9.10.1 开始，您可以使用 "Azure 密钥存储（AKV）" 和 "Google Cloud Platform 的密钥管理服务（Cloud KMS）" 保护云托管应用程序中的ONTAP加密密钥。从ONTAP 9.12.0开始、您还可以使用保护NVE密钥 "AWS的KMS"。

AWS KMS、AKV和Cloud KMS可用于保护 "NetApp 卷加密（NVE）密钥" 仅适用于数据SVM。

关于此任务

可以使用命令行界面或ONTAP REST API启用云提供程序的密钥管理。

在使用云提供商保护密钥时、请注意、默认情况下、数据SVM LIF用于与云密钥管理端点进行通信。节点管理网络用于与云提供商的身份验证服务进行通信（适用于 Azure 的 login.microsoftonline.com；适用于 Cloud KMS 的 oauth2.googleapis.com）。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

在使用云提供商密钥管理服务时、您应注意以下限制：

- 云提供商密钥管理不适用于NetApp存储加密(NSE)和NetApp聚合加密(NAE)。 "外部 KMIP" 可以改为使用。
- 云提供商密钥管理不适用于MetroCluster配置。
- 只能在数据SVM上配置云提供程序密钥管理。

开始之前

- 您必须已在相应的云提供程序上配置KMS。
- ONTAP集群的节点必须支持NVE。
- "您必须已安装卷加密(VE)和多租户加密密钥管理(MTEKM)许可证"。这些许可证包含在中 "ONTAP One"。
- 您必须是集群或SVM管理员。
- 数据SVM不能包含任何加密卷、也不能使用密钥管理器。如果数据SVM包含加密卷、则必须先迁移这些卷、然后再配置KMS。

启用外部密钥管理

启用外部密钥管理取决于您使用的特定密钥管理器。选择相应密钥管理器和环境的选项卡。

AWS

开始之前

- 您必须为管理加密的IAM角色要使用的AWS KMS密钥创建授权。IAM角色必须包含一个允许执行以下操作的策略：
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  有关详细信息、请参见的AWS文档 "赠款"。

在**ONTAP SVM**上启用**AWS KMV**

1. 开始之前、请从AWS KMS获取访问密钥ID和机密密钥。
2. 将权限级别设置为高级：
   `set -priv advanced`
3. 启用AWS KMS：
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出现提示时、输入机密密钥。
5. 确认已正确配置AWS KMS：
   `security key-manager external aws show -vserver` *`svm_name`*

Azure 酒店

在**ONTAP SVM**上启用**Azure**密钥存储

1. 开始之前，您需要从 Azure 帐户获取适当的身份验证凭据，即客户端密钥或证书。
   此外，还必须确保集群中的所有节点运行状况良好。您可以使用命令来检查此情况 `cluster show`。
2. 将权限级别设置为高级
   `set -priv advanced`
3. 在SVM上启用AKV
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   出现提示时，输入 Azure 帐户的客户端证书或客户端密钥。
4. 验证是否已正确启用AKV：
   `security key-manager external azure show vserver` *`svm_name`*
   如果服务可访问性不正常、请通过数据SVM LIF建立与AKV密钥管理服务的连接。

Google Cloud

在**ONTAP SVM**上启用云**KMS**

1. 开始之前、请以JSON格式获取Google Cloud KMS帐户密钥文件的专用密钥。您可以在 GCP 帐户中找到此信息。
   此外，还必须确保集群中的所有节点运行状况良好。您可以使用命令来检查此情况 `cluster show`。
2. 将权限级别设置为高级：
   `set -priv advanced`

3. 在SVM上启用Cloud KMS
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   出现提示时，使用服务帐户专用密钥输入 JSON 文件的内容
4. 验证Cloud KMS是否配置了正确的参数：
   `security key-manager external gcp show vserver svm_name`
   的状态 `kms_wrapped_key_status` 将是 "`UNKNOWN`" 如果尚未创建加密卷。
   如果服务可访问性不正常、请通过数据SVM LIF与GCP密钥管理服务建立连接。

如果已为数据SVM配置一个或多个加密卷、并且相应的NVE密钥由管理SVM板载密钥管理器管理、则这些密钥应迁移到外部密钥管理服务。要使用命令行界面执行此操作、请运行以下命令：
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
只有在成功迁移数据SVM的所有NVE密钥之后、才能为租户的数据SVM创建新的加密卷。

相关信息

- "使用适用于Cloud Volumes ONTAP的NetApp加密解决方案加密卷"

在 **ONTAP 9.6** 及更高版本（**NVE**）中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager onboard sync` 命令。

如果您使用的是MetroCluster配置、则必须运行 `security key-manager onboard enable` 命令、然后运行 `security key-manager onboard sync` 命令、并在每个上使用相同的密码短语。运行时 `security key-manager onboard enable` 命令、然后在远程集群上同步、则不需要运行 `enable` 命令。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。您可以使用 `cc-mode-enabled=yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `cc-mode-enabled=yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

配置 ONTAP 空闲数据加密时，为了满足分类商业解决方案（CSFC）的要求，您必须将 NSE 与 NVE 结合使用，并确保在通用标准模式下启用板载密钥管理器。请参见 "CSFC 解决方案简介" 有关 CSFC 的详细信息，请参见。

在通用标准模式下启用板载密钥管理器时 (`cc-mode-enabled=yes`)、系统行为将通过以下方式进行更改：

- 在通用标准模式下运行时，系统会监控连续失败的集群密码短语尝试。

  如果在启动时未输入正确的集群密码短语，则不会挂载加密卷。要更正此问题，您必须重新启动节点并输入正确的集群密码短语。启动后，对于需要使用集群密码短语作为参数的任何命令，系统最多允许连续 5 次尝试在 24 小时内正确输入集群密码短语。如果已达到限制（例如，您连续 5 次未正确输入集群密码短语），则必须等待 24 小时超时期限过后，或者重新启动节点，才能重置此限制。

- 系统映像更新使用 NetApp RSA-3072 代码签名证书以及 SHA-384 代码签名摘要来检查映像完整性，而不是使用通常的 NetApp RSA-2048 代码签名证书和 SHA-256 代码签名摘要。

  upgrade 命令可通过检查各种数字签名来验证映像内容是否未被更改或损坏。如果验证成功，映像更新过程将继续执行下一步；否则，映像更新将失败。请参见 `cluster image` 有关系统更新的信息、请参见手册页。

板载密钥管理器将密钥存储在易失性内存中。系统重新启动或暂停后，易失性内存内容将被清除。在正常运行条件下，系统暂停后，易失性内存内容将在 30 秒内清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置：

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   设置 `cc-mode-enabled=yes` 要求用户在重新启动后输入密钥管理器密码短语。对于NVE (如果已设置) `cc-mode-enabled=yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。。 - `cc-mode-enabled` 选项在MetroCluster配置中不受支持。。 `security key-manager onboard enable` 命令用于替换 `security key-manager setup` 命令：

   以下示例将在 cluster1 上启动密钥管理器设置命令，而无需在每次重新启动后输入密码短语：

   ```
   cluster1::> security key-manager onboard enable

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` "，输入 64 到 256 个字符的密码短语。

> 如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

3. 在密码短语确认提示符处，重新输入密码短语。
4. 验证是否已创建身份验证密钥：

   ```
   security key-manager key query -key-type NSE-AK
   ```

   > 。 `security key-manager key query` 命令用于替换 `security key-manager query key` 命令：有关完整的命令语法，请参见手册页。

   以下示例将验证是否已为创建身份验证密钥 `cluster1`：

   ```
   cluster1::> security key-manager key query -key-type NSE-AK
                  Node: node1
               Vserver: cluster1
           Key Manager: onboard
      Key Manager Type: OKM
    Key Manager Policy: -

    Key Tag                                  Key Type Encryption   Restored

   ------------------------------------  -------- ------------ --------

   node1                                   NSE-AK   AES-256      true

       Key ID:
   00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
   00000000

   node1                                   NSE-AK   AES-256      true

       Key ID:
   00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
   00000000

   2 entries were displayed.
   ```

5. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

   转换卷之前、必须完全配置板载密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置板载密钥管理器。

完成后

将密码短语复制到存储系统以外的安全位置，以供将来使用。

配置板载密钥管理器密码短语时，您还应手动将信息备份到存储系统以外的安全位置，以便在发生灾难时使用。请参见 "手动备份板载密钥管理信息"。

在 ONTAP 9.5 及更早版本（ NVE ）中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager setup` 命令。

如果您使用的是 MetroCluster 配置，请查看以下准则：

- 在ONTAP 9.5中、必须运行 `security key-manager setup` 在本地集群上、然后 `security key-manager setup -sync-metrocluster-config yes` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5之前的版本中、您必须运行 `security key-manager setup` 在本地集群上、等待大约20秒、然后运行 `security key-manager setup` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

> 密码短语尝试失败后，必须重新启动节点。

开始之前

- 如果将NSE或NVE与外部密钥管理(KMIP)服务器结合使用、则必须事先删除外部密钥管理器数据库。

  "从外部密钥管理过渡到板载密钥管理"

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > 从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 此选项要求用户在重新启动后输入密钥管理器密码短语。对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。

   以下示例将开始在 cluster1 上设置密钥管理器，而无需在每次重新启动后输入密码短语：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 输入 ... `yes` 在提示符处配置板载密钥管理。
3. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` "，输入 64 到 256 个字符的密码短语。

> 如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

4. 在密码短语确认提示符处，重新输入密码短语。
5. 验证是否已为所有节点配置密钥：

   ```
   security key-manager key show
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

   转换卷之前、必须完全配置板载密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置板载密钥管理器。

完成后

将密码短语复制到存储系统以外的安全位置，以供将来使用。

配置板载密钥管理器密码短语时，您还应手动将信息备份到存储系统以外的安全位置，以便在发生灾难时使用。请参见 "手动备份板载密钥管理信息"。

在新添加的节点中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

> 对于ONTAP 9.5及更早版本、必须运行 `security key-manager setup` 命令。
>
> 对于ONTAP 9.6及更高版本、必须运行 `security key-manager sync` 命令。
>
> 如果要将节点添加到配置了板载密钥管理的集群中，您将运行此命令刷新缺少的密钥。

如果您使用的是 MetroCluster 配置，请查看以下准则：

- 从ONTAP 9.6开始、您必须运行 `security key-manager onboard enable` 首先在本地集群上运行 `security key-manager onboard sync` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5中、必须运行 `security key-manager setup` 在本地集群上、然后 `security key-manager setup -sync-metrocluster-config yes` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5之前的版本中、您必须运行 `security key-manager setup` 在本地集群上、等待大约20秒、然后运行 `security key-manager setup` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

> 密码短语尝试失败后，必须重新启动节点。

使用 **NVE** 对卷数据进行加密

使用 **NVE** 概述对卷数据进行加密

从 ONTAP 9.7 开始，如果您拥有 VE 许可证以及板载或外部密钥管理，则默认情况下会启用聚合和卷加密。对于 ONTAP 9.6 及更早版本，您可以对新卷或现有卷启用加密。您必须

先安装VE许可证并启用密钥管理、然后才能启用卷加密。NVE 符合 FIPS-140-2 1 级标准。

使用**VE**许可证启用聚合级加密

从ONTAP 9.7开始、如果您有、则新创建的聚合和卷会默认进行加密 "VE许可证" 以及板载或外部密钥管理。从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。

关于此任务

如果计划执行实时或后台聚合级重复数据删除，则必须使用聚合级加密。否则， NVE 不支持聚合级重复数据删除。

启用聚合级别加密的聚合称为 *NAE aggregate* （适用于 NetApp 聚合加密）。NAE聚合中的所有卷都必须使用NAE或NVE加密进行加密。默认情况下、使用聚合级别加密时、在聚合中创建的卷会使用NAE加密进行加密。您可以覆盖默认值以改用NVE加密。

NAE 聚合不支持纯文本卷。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 启用或禁用聚合级别加密：

至 …	使用此命令 …
使用 ONTAP 9.7 或更高版本创建 NAE 聚合	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
使用 ONTAP 9.6 创建 NAE 聚合	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
将非 NAE 聚合转换为 NAE 聚合	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
将 NAE 聚合转换为非 NAE 聚合	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

有关完整的命令语法，请参见手册页。

以下命令将在上启用聚合级别加密 `aggr1`：

- ONTAP 9.7 或更高版本

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 或更早版本：

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. 验证是否已为聚合启用加密：

   `storage aggregate show -fields encrypt-with-aggr-key`

   有关完整的命令语法，请参见手册页。

   以下命令将对此进行验证 `aggr1` 已启用加密：

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

完成后

运行 `volume create` 命令以创建加密卷。

如果您使用 KMIP 服务器存储节点的加密密钥，则在对卷进行加密时， ONTAP 会自动 "`推送` " 加密密钥到服务器。

在新卷上启用加密

您可以使用 `volume create` 命令以对新卷启用加密。

关于此任务

您可以使用NetApp卷加密(NVE)对卷进行加密、从ONTAP 9.6开始、还可以使用NetApp聚合加密(NAE)对卷进行加密。要了解有关NAE和NVE的更多信息、请参见 卷加密概述。

在ONTAP 中为新卷启用加密的操作步骤 会根据您使用的ONTAP 版本和特定配置而有所不同：

- 从ONTAP 9.4开始、如果您启用了 `cc-mode` 设置板载密钥管理器时、您使用创建的卷 `volume create` 无论是否指定、命令都会自动加密 `-encrypt true`。
- 在ONTAP 9.6及更早版本中、您必须使用 `-encrypt true` 使用 `volume create` 用于启用加密的命令(前提是您未启用 `cc-mode`）。
- 如果要在ONTAP 9.6中创建NAE卷、则必须在聚合级别启用NAE。请参见 使用VE许可证启用聚合级别加密 了解有关此任务的更多详细信息。

- 从ONTAP 9.7开始、如果具有、则新创建的卷会默认进行加密 "VE许可证" 以及板载或外部密钥管理。默认情况下、在NAE聚合中创建的新卷的类型为NAE、而不是NVE。
  - 在ONTAP 9.7及更高版本中、如果您添加了 `-encrypt true` 到 `volume create` 命令要在NAE聚合中创建卷、此卷将采用NVE加密、而不是NAE加密。NAE聚合中的所有卷都必须使用NVE或NAE进行加密。

> NAE 聚合不支持纯文本卷。

步骤

1. 创建新卷并指定是否在卷上启用加密。如果新卷位于NAE聚合中、则默认情况下、此卷将为NAE卷：

要创建 ...	使用此命令 ...
NAE卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
NVE卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + 在不支持NAE的ONTAP 9.6及更早版本中、 `-encrypt true` 指定应使用NVE对卷进行加密。在ONTAP 9.7及更高版本中、如果在NAE聚合中创建卷、 `-encrypt true` 覆盖默认的NAE加密类型以创建NVE卷。
纯文本卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   有关完整的命令语法、请参见命令参考页面上的链接：https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[`volume create`^。

2. 验证是否已为卷启用加密：

   ```
   volume show -is-encrypted true
   ```

   有关完整的命令语法，请参见 "命令参考"。

结果

如果使用KMIP服务器存储节点的加密密钥、则在对卷进行加密时、ONTAP 会自动将加密密钥"推送"到服务器。

=
:allow-uri-read:

对现有卷启用加密

您可以使用 `volume move start` 或 `volume encryption conversion start` 命令以对现有卷启用加密。

关于此任务

- 从ONTAP 9.3开始、您可以使用 `volume encryption conversion start` 命令以"原位"加密现有卷、而无需将卷移动到其他位置。或者、您也可以使用 `volume move start` 命令：
- 对于ONTAP 9.2及更早版本、只能使用 `volume move start` 命令以通过移动现有卷启用加密。

使用 **volume encryption conversion start** 命令在现有卷上启用加密

从ONTAP 9.3开始、您可以使用 `volume encryption conversion start` 命令以"原位"加密现有卷、而无需将卷移动到其他位置。

启动转换操作后、必须完成该操作。如果您在操作期间遇到性能问题描述、则可以运行 `volume encryption conversion pause` 命令以暂停操作、以及 `volume encryption conversion resume` 命令以恢复操作。

> 您不能使用 `volume encryption conversion start` 转换SnapLock卷。

步骤

1. 在现有卷上启用加密：

   ```
   volume encryption conversion start -vserver SVM_name -volume volume_name
   ```

   有关整个命令语法、请参见命令的手册页。

   以下命令将对现有卷启用加密 `vol1`：

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   系统会为卷创建加密密钥。卷上的数据已加密。

2. 验证转换操作的状态：

   ```
   volume encryption conversion show
   ```

   有关整个命令语法、请参见命令的手册页。

   以下命令显示转换操作的状态：

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ----------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 转换操作完成后、验证卷是否已启用加密：

   ```
   volume show -is-encrypted true
   ```

   有关整个命令语法、请参见命令的手册页。

以下命令将显示上的加密卷 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----  ---------  ----
vs1       vol1     aggr2      online     RW   200GB    160.0GB   20%
```

结果

如果您使用 KMIP 服务器存储节点的加密密钥，则在对卷进行加密时， ONTAP 会自动 "`推送` " 加密密钥到服务器。

使用 **volume move start** 命令在现有卷上启用加密

您可以使用 `volume move start` 命令以通过移动现有卷启用加密。您必须使用 `volume move start` 在ONTAP 9.2及更早版本中。您可以使用同一个聚合或不同的聚合。

关于此任务

- 从ONTAP 9.8开始、您可以使用 `volume move start` 在SnapLock或FlexGroup卷上启用加密。
- 从ONTAP 9.4开始、如果在设置板载密钥管理器时启用"`cc-mode`"、则会显示使用创建的卷 `volume move start` 命令会自动加密。您无需指定 `-encrypt-destination true`。
- 从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要移动的卷所在的聚合分配密钥。使用唯一密钥加密的卷称为_NVE卷_(表示它使用NetApp卷加密)。使用聚合级别密钥加密的卷称为 *NAE volume* （适用于 NetApp 聚合加密）。NAE 聚合不支持纯文本卷。
- 从ONTAP 9.14.1开始、您可以使用NVE对SVM根卷进行加密。有关详细信息，请参见 在SVM根卷上配置NetApp卷加密。

开始之前

要执行此任务，您必须是集群管理员，或者集群管理员已向其委派权限的 SVM 管理员。

"委派权限以运行 volume move 命令"

步骤

1. 移动现有卷并指定是否在卷上启用加密：

要转换 …	使用此命令 …
纯文本卷到 NVE 卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
将 NVE 或纯文本卷连接到 NAE 卷（假设目标上启用了聚合级别加密）	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`

NAE 卷到 NVE 卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
NAE 卷到纯文本卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
NVE卷转换为纯文本卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

有关整个命令语法、请参见命令的手册页。

以下命令将转换名为的纯文本卷 `vol1` 到NVE卷：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

假设在目标上启用了聚合级加密、则以下命令将转换名为的NVE或纯文本卷 `vol1` 到NAE卷：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

以下命令将转换名为的NAE卷 `vol2` 到NVE卷：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

以下命令将转换名为的NAE卷 `vol2` 纯文本卷：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

以下命令将转换名为的NVE卷 `vol2` 纯文本卷：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 查看集群卷的加密类型：

```
volume show -fields encryption-type none|volume|aggregate
```

。 `encryption-type` 字段在ONTAP 9.6及更高版本中可用。

有关整个命令语法、请参见命令的手册页。

以下命令显示中卷的加密类型 `cluster2`：

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 验证是否已为卷启用加密：

   ```
   volume show -is-encrypted true
   ```

   有关整个命令语法、请参见命令的手册页。

   以下命令将显示上的加密卷 `cluster2`：

   ```
   cluster2::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
   ```

结果

如果您使用KMIP服务器存储节点的加密密钥、则在对卷进行加密时、ONTAP会自动将加密密钥推送到服务器。

在SVM根卷上配置NetApp卷加密

从ONTAP 9.14.1开始、您可以在Storage VM (SVM)根卷上启用NetApp卷加密(NVE)。使用NVE时、根卷会使用唯一密钥进行加密、从而提高SVM的安全性。

关于此任务

只有在创建SVM之后、才能在SVM根卷上启用NVE。

开始之前

- SVM根卷不能位于使用NetApp聚合加密(NAE)加密的聚合上。
- 您必须已使用板载密钥管理器或外部密钥管理器启用加密。

- 必须运行ONTAP 9.14.1或更高版本。
- 要迁移包含使用NVE加密的根卷的SVM、您必须在迁移完成后将SVM根卷转换为纯文本卷、然后对SVM根卷重新加密。
  - 如果SVM迁移的目标聚合使用NAE、则默认情况下、根卷会继承NAE。
- 如果SVM处于SVM灾难恢复关系中：
  - 镜像SVM上的加密设置不会复制到目标。如果在源或目标上启用NVE、则必须在镜像的SVM根卷上单独启用NVE。
  - 如果目标集群中的所有聚合都使用NAE、则SVM根卷将使用NAE。

步骤

您可以使用ONTAP命令行界面或System Manager在SVM根卷上启用NVE。

命令行界面

您可以在SVM根卷上原位启用NVE、也可以通过在聚合之间移动卷来启用NVE。

对根卷进行原位加密

1. 将根卷转换为加密卷：

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 确认加密成功。。 `volume show -encryption-type volume` 显示使用NVE的所有卷的列表。

通过移动**SVM**根卷对其进行加密

1. 启动卷移动：

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   有关的详细信息、请参见 `volume move`，请参阅 移动卷。

2. 确认 `volume move` 操作成功、使用 `volume move show` 命令：。 `volume show -encryption -type volume` 显示使用NVE的所有卷的列表。

System Manager

1. 导航到存储>卷。
2. 在要加密的SVM根卷的名称旁边、选择 ⋮ 然后编辑。
3. 在存储和优化标题下，选择启用加密。
4. 选择保存。

启用节点根卷加密

从 ONTAP 9.8 开始，您可以使用 NetApp 卷加密来保护节点的根卷。

关于此任务

此操作步骤适用场景为节点根卷。它不适用于 SVM 根卷。SVM根卷可通过聚合级加密进行保护、 从ONTAP 9.14.1开始、为NVE。

根卷加密开始后，必须完成。您不能暂停此操作。加密完成后，您不能为根卷分配新密钥，也不能执行安全清除操作。

开始之前

- 您的系统必须使用 HA 配置。
- 必须已创建节点根卷。
- 您的系统必须具有使用密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）的板载密钥管理器或外部密钥管理服务器。

步骤

1. 对根卷进行加密：

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 验证转换操作的状态：

   ```
   volume encryption conversion show
   ```

3. 转换操作完成后，验证卷是否已加密：

   ```
   volume show -fields
   ```

   下面显示了加密卷的示例输出。

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

配置基于 NetApp 硬件的加密

配置 NetApp 基于硬件的加密概述

NetApp 基于硬件的加密支持在数据写入时对其进行全磁盘加密（FDE）。如果固件上未存储加密密钥，则无法读取数据。而加密密钥只能由经过身份验证的节点访问。

了解 NetApp 基于硬件的加密

节点使用从外部密钥管理服务器或板载密钥管理器检索的身份验证密钥向自加密驱动器进行自我身份验证：

- 外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）为节点提供密钥。最佳做法是，在与数据不同的存储系统上配置外部密

钥管理服务器。

- 板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。

您可以将 NetApp 卷加密与基于硬件的加密结合使用，在 d自加密驱动器上 " 双重加密 " 数据。

启用自加密驱动器后、核心转储也会进行加密。

> 如果 HA 对使用加密 SAS 或 NVMe 驱动器（ SED ， NSE ， FIPS ），则必须按照主题中的说明进行操作 将 FIPS 驱动器或 SED 恢复到未受保护的模式 初始化系统之前 HA 对中的所有驱动器（启动选项 4 或 9 ）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

支持的自加密驱动器类型

支持两种类型的自加密驱动器：

- 所有 FAS 和 AFF 系统均支持自加密 FIPS 认证的 SAS 或 NVMe 驱动器。这些驱动器称为 _fips drives ， _ 符合联邦信息处理标准出版物 140-2 第 2 级的要求。经过认证的功能除了加密之外，还可以提供保护，例如防止驱动器受到拒绝服务攻击。不能在同一节点或 HA 对上将 FIPS 驱动器与其他类型的驱动器混合使用。
- 从ONTAP 9.6开始、AFF A800、A320及更高版本的系统支持未经过FIPS测试的自加密NVMe驱动器。这些驱动器称为_SED、可提供与FIPS驱动器相同的加密功能、但可以与同一节点或HA对上的非加密驱动器混合使用。
- 所有经过FIPS验证的驱动器都使用经过FIPS验证的固件加密模块。 FIPS驱动器加密模块不使用在驱动器外部生成的任何密钥(驱动器的固件加密模块使用输入到驱动器的身份验证密码短语来获取密钥加密密钥)。

> 非加密驱动器是指非SED或FIPS驱动器的驱动器。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

何时使用外部密钥管理

尽管使用板载密钥管理器成本较低且通常更方便、但如果满足以下任一条件、则应使用外部密钥管理：

- 贵组织的策略要求密钥管理解决方案 使用FIPS 140-2 2级(或更高)加密模块。
- 您需要一个具有集中管理加密密钥的多集群解决方案。
- 您的企业需要将身份验证密钥存储在系统或与数据不同的位置，从而提高安全性。

支持详细信息

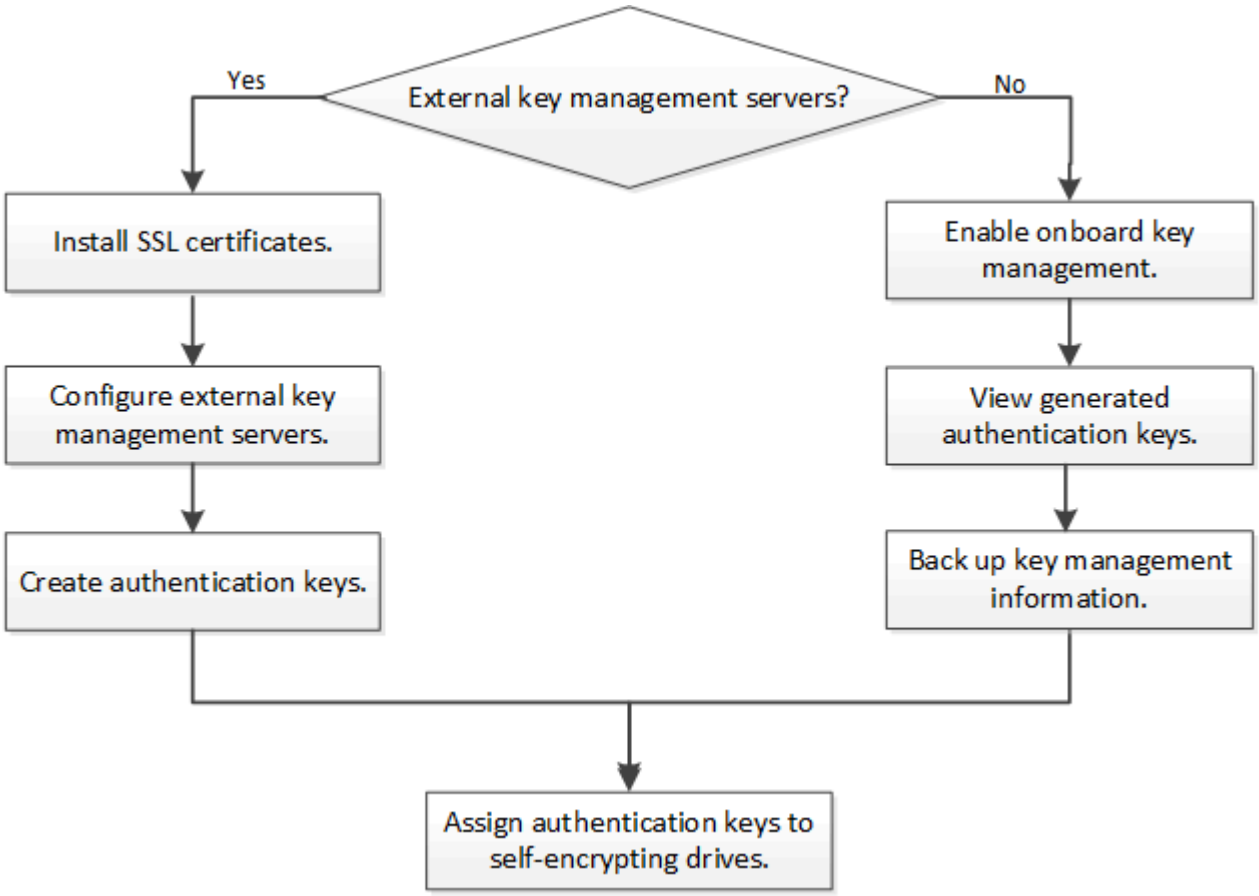
下表显示了重要的硬件加密支持详细信息。有关受支持的 KMIP 服务器，存储系统和磁盘架的最新信息，请参见互操作性表。

资源或功能	支持详细信息
非同构磁盘集	• 不能在同一节点或 HA 对上将 FIPS 驱动器与其他类型的驱动器混合使用。在同一集群中，遵从的 HA 对可以与不遵从的 HA 对共存。 • SED可以与同一节点或HA对上的非加密驱动器混合使用。

驱动器类型	• FIPS 驱动器可以是 SAS 或 NVMe 驱动器。 • SED 必须是 NVMe 驱动器。
10 Gb 网络接口	从 ONTAP 9.3 开始， KMIP 密钥管理配置支持使用 10 Gb 网络接口与外部密钥管理服务器进行通信。
用于与密钥管理服务器通信的端口	从 ONTAP 9.3 开始，您可以使用任何存储控制器端口与密钥管理服务器进行通信。否则、您应使用端口e0M与密钥管理服务器进行通信。根据存储控制器型号，某些网络接口在启动过程中可能不可用，无法与密钥管理服务器进行通信。
MetroCluster （ MCC ）	• NVMe 驱动器支持 MCC 。 • SAS 驱动器不支持 MCC 。

基于硬件的加密工作流

您必须先配置密钥管理服务，然后集群才能向自加密驱动器进行身份验证。您可以使用外部密钥管理服务器或板载密钥管理器。



相关信息

- "NetApp Hardware Universe"
- "NetApp 卷加密和 NetApp 聚合加密"

配置外部密钥管理概述

您可以使用一个或多个外部密钥管理服务器来保护集群用于访问加密数据的密钥。外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）为节点提供密钥。

对于 ONTAP 9.1 及更早版本，必须先将节点管理 LIF 分配给已配置节点管理角色的端口，然后才能使用外部密钥管理器。

在 ONTAP 9.1 及更高版本中，可以使用板载密钥管理器实施 NetApp 卷加密（NVE）。在 ONTAP 9.3 及更高版本中， NVE 可通过外部密钥管理（KMIP）和板载密钥管理器来实施。从ONTAP 9.11.1开始、您可以在一个集群中配置多个外部密钥管理器。请参见 配置集群模式密钥服务器。

在 **ONTAP 9.2** 及更早版本中收集网络信息

如果您使用的是 ONTAP 9.2 或更早版本，则应先填写网络配置工作表，然后再启用外部密钥管理。

从 ONTAP 9.3 开始，系统会自动发现所有需要的网络信息。

项目	注释：	价值
密钥管理网络接口名称		
密钥管理网络接口 IP 地址	节点管理 LIF 的 IP 地址，采用 IPv4 或 IPv6 格式	
密钥管理网络接口 IPv6 网络前缀长度	如果使用的是 IPv6 ，则为 IPv6 网络前缀长度	
密钥管理网络接口子网掩码		
密钥管理网络接口网关 IP 地址		
集群网络接口的 IPv6 地址	只有在对密钥管理网络接口使用 IPv6 时才需要此参数	
每个 KMIP 服务器的端口号	可选。所有 KMIP 服务器的端口号必须相同。如果不提供端口号，则默认为端口 5696 ，即为 KMIP 的 Internet 分配的编号颁发机构（IANA）分配的端口。	

密钥标记名称	可选。密钥标记名称用于标识属于某个节点的所有密钥。默认密钥标记名称是节点名称。	

相关信息

"NetApp 技术报告 3954：《适用于 IBM Tivoli Lifetime Key Manager 的 NetApp 存储加密安装前要求和过程》"

"NetApp 技术报告 4074：《 SafeNet KeySecure 的 NetApp 存储加密安装前要求和过程》"

在集群上安装 **SSL** 证书

集群和 KMIP 服务器使用 KMIP SSL 证书来验证彼此的身份并建立 SSL 连接。在配置与 KMIP 服务器的 SSL 连接之前，必须为集群安装 KMIP 客户端 SSL 证书，并为 KMIP 服务器的根证书颁发机构（CA）安装 SSL 公有证书。

关于此任务

在 HA 对中，两个节点必须使用相同的公有和专用 KMIP SSL 证书。如果将多个 HA 对连接到同一个 KMIP 服务器，则 HA 对中的所有节点都必须使用相同的公有和专用 KMIP SSL 证书。

开始之前

- 创建证书的服务器， KMIP 服务器和集群上的时间必须同步。
- 您必须已获取集群的公有 SSL KMIP 客户端证书。
- 您必须已获取与集群的 SSL KMIP 客户端证书关联的专用密钥。
- SSL KMIP 客户端证书不能受密码保护。
- 您必须已为 KMIP 服务器的根证书颁发机构（CA）获取 SSL 公有证书。
- 在MetroCluster环境中、您必须在两个集群上安装相同的KMIP SSL证书。

> 在集群上安装客户端和服务器证书之前或之后，您可以在 KMIP 服务器上安装这些证书。

步骤

1. 为集群安装 SSL KMIP 客户端证书：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系统将提示您输入 SSL KMIP 公有和专用证书。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 为 KMIP 服务器的根证书颁发机构（CA）安装 SSL 公有证书：

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。最多可以将四个 KMIP 服务器连接到一个节点。建议至少使用两台服务器来实现冗余和灾难恢复。

从ONTAP 9.11.1开始、您可以为每个主密钥服务器最多添加3个二级密钥服务器、以创建集群模式密钥服务器。有关详细信息，请参见 配置集群模式外部密钥服务器。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 您必须是集群管理员才能执行此任务。
- 在配置外部密钥管理器之前，您必须配置 MetroCluster 环境。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 配置集群的密钥管理器连接：

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ℹ
   > - 。 `security key-manager external enable` 命令用于替换 `security key-manager setup` 命令：您可以运行 `security key-manager external modify` 用于更改外部密钥管理配置的命令。有关完整的命令语法，请参见手册页。
   > - 在MetroCluster 环境中、如果要为管理SVM配置外部密钥管理、则必须重复 `security key-manager external enable` 命令。

   以下命令将为启用外部密钥管理 `cluster1` 使用三个外部密钥服务器。第一个密钥服务器使用其主机名和端口指定，第二个密钥服务器使用 IP 地址和默认端口指定，第三个密钥服务器使用 IPv6 地址和端口指定：

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. 验证所有已配置的 KMIP 服务器是否均已连接：

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   > ℹ
   > 。 `security key-manager external show-status` 命令用于替换 `security key-manager show -status` 命令：有关完整的命令语法，请参见手册页。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

在 **ONTAP 9.5** 及更早版本中启用外部密钥管理

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。最多可以将四个 KMIP 服务器连接到一个节点。建议至少使用两台服务器来实现冗余和灾难恢复。

关于此任务

ONTAP 为集群中的所有节点配置 KMIP 服务器连接。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 您必须是集群管理员才能执行此任务。
- 在配置外部密钥管理器之前，您必须配置 MetroCluster 环境。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 为集群节点配置密钥管理器连接：

   ```
   security key-manager setup
   ```

   此时将启动密钥管理器设置。

   > 在MetroCluster 环境中、必须在两个集群上运行此命令。

2. 在每个提示符处输入相应的响应。
3. 添加 KMIP 服务器：

```
security key-manager add -address key_management_server_ipaddress
```

```
clusterl::> security key-manager add -address 20.1.1.1
```

> 在MetroCluster 环境中、必须在两个集群上运行此命令。

4. 添加额外的 KMIP 服务器以实现冗余：

```
security key-manager add -address key_management_server_ipaddress
```

```
clusterl::> security key-manager add -address 20.1.1.2
```

> 在MetroCluster 环境中、必须在两个集群上运行此命令。

5. 验证所有已配置的 KMIP 服务器是否均已连接：

```
security key-manager show -status
```

有关完整的命令语法，请参见手册页。

```
cluster1::> security key-manager show -status

Node             Port      Registered Key Manager  Status
--------------   ----      -----------------------  ---------------
cluster1-01      5696      20.1.1.1                 available
cluster1-01      5696      20.1.1.2                 available
cluster1-02      5696      20.1.1.1                 available
cluster1-02      5696      20.1.1.2                 available
```

6. (可选)将纯文本卷转换为加密卷。

```
volume encryption conversion start
```

转换卷之前、必须完全配置外部密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置外部密钥管理器。

配置集群模式外部密钥服务器

从ONTAP 9.11.1开始、您可以配置与SVM上的集群模式外部密钥管理服务器的连接。使用集群模式密钥服务器、您可以在SVM上指定主密钥服务器和二级密钥服务器。注册密钥时、ONTAP 会先尝试访问主密钥服务器、然后再按顺序尝试访问二级服务器、直到操作成功完成、从而防止密钥重复。

外部密钥服务器可用于NSE、NVE、NAE和SED密钥。一个SVM最多可支持四个主外部KMIP服务器。每个主服

务器最多可支持三个二级密钥服务器。

开始之前

- "必须为SVM启用KMIP密钥管理"。
- 此过程仅支持使用KMIP的密钥服务器。有关支持的密钥服务器列表、请查看 "NetApp 互操作性表工具"。
- 集群中的所有节点都必须运行ONTAP 9.11.1或更高版本。
- 服务器的顺序列出中的参数 `-secondary-key-servers` 参数反映外部密钥管理(KMIP)服务器的访问顺序。

创建集群密钥服务器

配置操作步骤 取决于您是否配置了主密钥服务器。

将主密钥服务器和二级密钥服务器添加到**SVM**

1. 确认尚未为集群启用密钥管理：
   `security key-manager external show -vserver` *`svm_name`*
   如果SVM已启用最多四个主密钥服务器、则必须先删除其中一个现有主密钥服务器、然后再添加新的主密钥服务器。
2. 启用主密钥管理器：
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. 修改主密钥服务器以添加二级密钥服务器。。 `-secondary-key-servers` 参数可接受最多包含三个密钥服务器的逗号分隔列表。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

将二级密钥服务器添加到现有主密钥服务器

1. 修改主密钥服务器以添加二级密钥服务器。。 `-secondary-key-servers` 参数可接受最多包含三个密钥服务器的逗号分隔列表。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   有关二级密钥服务器的详细信息、请参见 [mod-secondary]。

修改集群模式密钥服务器

您可以通过更改特定密钥服务器的状态(主或二级)、添加和删除二级密钥服务器或更改二级密钥服务器的访问顺序来修改外部密钥服务器集群。

转换主密钥服务器和辅助密钥服务器

要将主密钥服务器转换为二级密钥服务器、必须先使用将其从SVM中删除 `security key-manager external remove-servers` 命令：

要将二级密钥服务器转换为主密钥服务器、必须先从其现有主密钥服务器中删除二级密钥服务器。请参见 [mod-secondary]。如果在删除现有密钥的同时将二级密钥服务器转换为主服务器、则在完成删除和转换之前尝试添加

新服务器可能会导致密钥重复。

修改二级密钥服务器

二级密钥服务器通过进行管理 `-secondary-key-servers` 的参数 `security key-manager external modify-server` 命令：。 `-secondary-key-servers` 参数接受逗号分隔列表。此列表中二级密钥服务器的指定顺序决定了二级密钥服务器的访问顺序。可以通过运行命令来修改访问顺序 `security key-manager external modify-server` 次密钥服务器按不同顺序输入。

要删除辅助密钥服务器、请 `-secondary-key-servers` 参数应包括要保留的密钥服务器、而不包括要删除的密钥服务器。要删除所有辅助密钥服务器、请使用参数 `-`，表示无。

对于追加信息 、请参见 `security key-manager external` 页面 "ONTAP 命令参考"。

在 ONTAP 9.6 及更高版本中创建身份验证密钥

您可以使用 `security key-manager key create` 命令为节点创建身份验证密钥并将其存储在已配置的KMIP服务器上。

关于此任务

如果您的安全设置要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证，则应为每个密钥创建一个单独的密钥。否则、您可以使用与数据访问相同的身份验证密钥来满足FIPS合规性要求。

ONTAP 会为集群中的所有节点创建身份验证密钥。

- 启用板载密钥管理器后，不支持此命令。但是，启用板载密钥管理器后，系统会自动创建两个身份验证密钥。可以使用以下命令查看这些密钥：

  ```
  security key-manager key query -key-type NSE-AK
  ```

- 如果已配置的密钥管理服务器已存储超过 128 个身份验证密钥，则会收到警告。
- 您可以使用 `security key-manager key delete` 命令以删除任何未使用的密钥。。 `security key-manager key delete` 如果给定密钥当前正由ONTAP使用、则命令将失败。（要使用此命令，您的权限必须大于 "`admin` "。）

> 在MetroCluster 环境中、删除密钥之前、必须确保配对集群上未使用此密钥。您可以在配对集群上使用以下命令来检查此密钥是否未被使用：
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 为集群节点创建身份验证密钥：

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

> 正在设置 ... `prompt-for-key=true` 使系统提示集群管理员在对加密驱动器进行身份验证时使用密码短语。否则，系统将自动生成 32 字节密码短语。 。 `security key-manager key create` 命令用于替换 `security key-manager create-key` 命令：有关完整的命令语法，请参见手册页。

以下示例将为创建身份验证密钥 `cluster1`，自动生成32字节密码短语：

```
cluster1::> security key-manager key create
Key ID:
00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. 验证是否已创建身份验证密钥：

   `security key-manager key query -node node`

   > 。 `security key-manager key query` 命令用于替换 `security key-manager query key` 命令：有关完整的命令语法，请参见手册页。 输出中显示的密钥 ID 是用于引用身份验证密钥的标识符。它不是实际的身份验证密钥或数据加密密钥。

   以下示例将验证是否已为创建身份验证密钥 `cluster1`：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

在 **ONTAP 9.5** 及更早版本中创建身份验证密钥

您可以使用 `security key-manager create-key` 命令为节点创建身份验证密钥并将其存储在已配置的KMIP服务器上。

关于此任务

如果您的安全设置要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证，则应为每个密钥创建一个单独的密钥。否则，您可以使用与数据访问相同的身份验证密钥来满足 FIPS 合规性要求。

ONTAP 会为集群中的所有节点创建身份验证密钥。

- 启用板载密钥管理后，不支持此命令。
- 如果已配置的密钥管理服务器已存储超过 128 个身份验证密钥，则会收到警告。

您可以使用密钥管理服务器软件删除任何未使用的密钥，然后再次运行命令。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 为集群节点创建身份验证密钥：

   `security key-manager create-key`

   有关完整的命令语法，请参见命令手册页。

   > 输出中显示的密钥 ID 是用于引用身份验证密钥的标识符。它不是实际的身份验证密钥或数据加密密钥。

   以下示例将为创建身份验证密钥 `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 验证是否已创建身份验证密钥：

   `security key-manager query`

   有关完整的命令语法，请参见手册页。

   以下示例将验证是否已为创建身份验证密钥 `cluster1`：

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

将数据身份验证密钥分配给 **FIPS** 驱动器或 **SED** （外部密钥管理）

您可以使用 `storage encryption disk modify` 用于将数据身份验证密钥分配给FIPS驱动器或SED的命令。集群节点使用此密钥锁定或解锁驱动器上的加密数据。

关于此任务

只有当自加密驱动器的身份验证密钥 ID 设置为非默认值时，才会保护其免遭未经授权的访问。密钥 ID 为 0x0 的制造商安全 ID （ MSID ）是 SAS 驱动器的标准默认值。对于 NVMe 驱动器，标准默认值为空密钥，表示为空密钥 ID 。将密钥 ID 分配给自加密驱动器时，系统会将其身份验证密钥 ID 更改为非默认值。

此操作步骤 不会造成中断。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将数据身份验证密钥分配给 FIPS 驱动器或 SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   有关完整的命令语法，请参见命令手册页。

您可以使用 `security key-manager query -key-type NSE-AK` 用于查看密钥ID的命令。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 验证是否已分配身份验证密钥：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

配置板载密钥管理

在 ONTAP 9.6 及更高版本中启用板载密钥管理

您可以使用板载密钥管理器向 FIPS 驱动器或 SED 验证集群节点的身份。板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。板载密钥管理器符合 FIPS-140-2 1 级标准。

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager onboard enable` 命令。在MetroCluster配置中、您必须运行 `security key-manager onboard enable` 首先在本地集群上运行 `security key-manager onboard sync` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。除了在MetroCluster中、您可以使用 `cc-mode-enabled=yes` 选项、要求用户在重新启动后输入密码短语。

在通用标准模式下启用板载密钥管理器时 (`cc-mode-enabled=yes`)、系统行为将通过以下方式进行更改：

- 在通用标准模式下运行时，系统会监控连续失败的集群密码短语尝试。

  如果启用了 NetApp 存储加密（NSE），但在启动时未输入正确的集群密码短语，则系统将无法向其驱动器进行身份验证并自动重新启动。要更正此问题，您必须在启动提示符处输入正确的集群密码短语。启动后，对于需要使用集群密码短语作为参数的任何命令，系统最多允许连续 5 次尝试在 24 小时内正确输入集群密码短语。如果已达到限制（例如，您连续 5 次未正确输入集群密码短语），则必须等待 24 小时超时期限过后，或者重新启动节点，才能重置此限制。

- 系统映像更新使用 NetApp RSA-3072 代码签名证书以及 SHA-384 代码签名摘要来检查映像完整性，而不是使用通常的 NetApp RSA-2048 代码签名证书和 SHA-256 代码签名摘要。

  upgrade 命令可通过检查各种数字签名来验证映像内容是否未被更改或损坏。如果验证成功，映像更新过程将继续执行下一步；否则，映像更新将失败。有关系统更新的信息，请参见 "`cluster image` " 手册页。

板载密钥管理器将密钥存储在易失性内存中。系统重新启动或暂停后，易失性内存内容将被清除。在正常运行条件下，系统暂停后，易失性内存内容将在 30 秒内清除。

开始之前

- 如果将 NSE 与外部密钥管理（KMIP）服务器结合使用，则必须已删除外部密钥管理器数据库。

  "从外部密钥管理过渡到板载密钥管理"

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须先配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置命令：

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   设置 `cc-mode-enabled=yes` 要求用户在重新启动后输入密钥管理器密码短语。。 `- cc-mode-enabled` 选项在MetroCluster配置中不受支持。。 `security key-manager onboard enable` 命令用于替换 `security key-manager setup` 命令：

   以下示例将在 cluster1 上启动密钥管理器设置命令，而无需在每次重新启动后输入密码短语：

   ```
   cluster1::> security key-manager onboard enable

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` "，输入 64 到 256 个字符的密码短语。

> 如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

3. 在密码短语确认提示符处，重新输入密码短语。
4. 验证是否已创建身份验证密钥：

```
security key-manager key query -node node
```

> 。 `security key-manager key query` 命令用于替换 `security key-manager query key` 命令：有关完整的命令语法，请参见手册页。

以下示例将验证是否已为创建身份验证密钥 `cluster1`：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

完成后

将密码短语复制到存储系统以外的安全位置，以供将来使用。

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。您还应手动备份此信息，以便在发生灾难时使用。

在 ONTAP 9.5 及更早版本中启用板载密钥管理

您可以使用板载密钥管理器向 FIPS 驱动器或 SED 验证集群节点的身份。板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。板载密钥管理器符合 FIPS-140-2 1 级标准。

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager setup` 命令。

如果您使用的是 MetroCluster 配置，请查看以下准则：

- 在ONTAP 9.5中、必须运行 `security key-manager setup` 在本地集群上、然后 `security key-manager setup -sync-metrocluster-config yes` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5之前的版本中、您必须运行 `security key-manager setup` 在本地集群上、等待大约20秒、然后运行 `security key-manager setup` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

> 密码短语尝试失败后，必须重新启动节点。

开始之前

- 如果将 NSE 与外部密钥管理（ KMIP ）服务器结合使用，则必须已删除外部密钥管理器数据库。

  "从外部密钥管理过渡到板载密钥管理"

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须先配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > 从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 此选项要求用户在重新启动后输入密钥管理器密码短语。对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。

   以下示例将开始在 cluster1 上设置密钥管理器，而无需在每次重新启动后输入密码短语：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 输入 ... `yes` 在提示符处配置板载密钥管理。
3. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` "，输入 64 到 256 个字符的密码短语。

> 如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

4. 在密码短语确认提示符处，重新输入密码短语。
5. 验证是否已为所有节点配置密钥：

   ```
   security key-manager key show
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

完成后

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。

配置板载密钥管理器密码短语时，您还应手动将信息备份到存储系统以外的安全位置，以便在发生灾难时使用。请参见 "手动备份板载密钥管理信息"。

将数据身份验证密钥分配给 FIPS 驱动器或 SED （板载密钥管理）

您可以使用 `storage encryption disk modify` 用于将数据身份验证密钥分配给FIPS驱动器或SED的命令。集群节点使用此密钥访问驱动器上的数据。

关于此任务

只有当自加密驱动器的身份验证密钥 ID 设置为非默认值时，才会保护其免遭未经授权的访问。密钥 ID 为 0x0 的制造商安全 ID （MSID）是 SAS 驱动器的标准默认值。对于 NVMe 驱动器，标准默认值为空密钥，表示为空密钥 ID 。将密钥 ID 分配给自加密驱动器时，系统会将其身份验证密钥 ID 更改为非默认值。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将数据身份验证密钥分配给 FIPS 驱动器或 SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   有关完整的命令语法，请参见命令手册页。

   > 您可以使用 `security key-manager key query -key-type NSE-AK` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. 验证是否已分配身份验证密钥：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

将 **FIPS 140-2** 身份验证密钥分配给 **FIPS** 驱动器

您可以使用 `storage encryption disk modify` 命令 `-fips-key-id` 用于将FIPS 140-2身份验证密钥分配给FIPS驱动器的选项。集群节点将此密钥用于数据访问以外的驱动器操作，例如防止驱动器受到拒绝服务攻击。

关于此任务

您的安全设置可能要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证。否则，您可以使用与数据访问相同的身份验证密钥来满足 FIPS 合规性要求。

此操作步骤 不会造成中断。

开始之前

驱动器固件必须支持 FIPS 140-2 合规性。。 "NetApp 互操作性表工具" 包含有关支持的驱动器固件版本的信息。

步骤

1. 您必须首先确保已分配数据身份验证密钥。可以使用来完成此操作 外部密钥管理器 或 板载密钥管理器。使用命令验证是否已分配密钥 `storage encryption disk show`。
2. 将 FIPS 140-2 身份验证密钥分配给 SED：

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D8000000000100000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 验证是否已分配身份验证密钥：

```
storage encryption disk show -fips
```

有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

为 **KMIP** 服务器连接启用集群范围 **FIPS** 兼容模式

您可以使用 `security config modify` 命令 `-is-fips-enabled` 用于为传输中的数据启用集群范围FIPS兼容模式的选项。这样做会强制集群在连接到 KMIP 服务器时在 FIPS 模式下使用 OpenSSL 。

关于此任务

启用集群范围 FIPS 兼容模式后，集群将仅自动使用 TLS1.2 和 FIPS 验证的密码套件。默认情况下，集群范围 FIPS 兼容模式处于禁用状态。

修改集群范围的安全配置后，您必须手动重新启动集群节点。

开始之前

- 存储控制器必须配置为 FIPS 兼容模式。
- 所有 KMIP 服务器都必须支持 TLSv1.2 。启用集群范围 FIPS 兼容模式后，系统需要使用 TLSv1.2 完成与 KMIP 服务器的连接。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 验证是否支持 TLSv1.2：

   ```
   security config show -supported-protocols
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. 启用集群范围 FIPS 兼容模式：

   `security config modify -is-fips-enabled true -interface SSL`

   有关完整的命令语法，请参见手册页。

4. 手动重新启动集群节点。
5. 验证是否已启用集群范围 FIPS 兼容模式：

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

管理 NetApp 加密

取消卷数据加密

您可以使用 `volume move start` 用于移动和取消加密卷数据的命令。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行 volume move 命令的权限"。

步骤

1. 移动现有加密卷并取消对卷上的数据加密：

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   有关完整的命令语法，请参见命令手册页。

   以下命令将移动名为的现有卷 `vol1` 目标聚合 `aggr3` 并对卷上的数据取消加密：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   系统将删除卷的加密密钥。卷上的数据未加密。

2. 验证卷是否已禁用加密：

   `volume show -encryption`

   有关完整的命令语法，请参见命令手册页。

   以下命令将显示卷是否位于上 `cluster1` 已加密：

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

移动加密卷

您可以使用 `volume move start` 命令以移动加密卷。移动的卷可以位于同一聚合或不同聚合上。

关于此任务

如果目标节点或目标卷不支持卷加密，则移动操作将失败。

。 `-encrypt-destination` 选项 `volume move start` 对于加密卷、默认为true。指定您不希望对目标卷进行加密的要求可确保您不会无意中对卷上的数据取消加密。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。

步骤

1. 移动现有加密卷并保持卷上的数据处于加密状态：

`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

有关完整的命令语法，请参见命令手册页。

以下命令将移动名为的现有卷 `vol1` 目标聚合 `aggr3` 并保持卷上的数据处于加密状态：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

2. 验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关完整的命令语法，请参见命令手册页。

   以下命令将显示上的加密卷 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

委派运行 **volume move** 命令的权限

您可以使用 `volume move` 用于对现有卷进行加密、移动加密卷或取消卷加密的命令。集群管理员可以运行 `volume move` 命令本身、也可以将运行命令的权限委派给SVM管理员。

关于此任务

默认情况下、系统会为SVM管理员分配 `vsadmin` 角色、不包括移动卷的权限。您必须分配 `vsadmin-volume` SVM管理员的角色、以使其能够运行 `volume move` 命令：

步骤

1. 委派运行的权限 `volume move` 命令：

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

   有关完整的命令语法，请参见命令手册页。

   以下命令授予SVM管理员运行的权限 `volume move` 命令：

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

使用 **volume encryption rekey start** 命令更改卷的加密密钥

安全最佳做法是定期更改卷的加密密钥。从ONTAP 9.3开始、您可以使用 `volume encryption rekey start` 命令以更改加密密钥。

关于此任务

启动重新设置密钥操作后，该操作必须完成。不会返回到旧密钥。如果您在操作期间遇到性能问题描述、则可以运行 `volume encryption rekey pause` 命令以暂停操作、以及 `volume encryption rekey resume` 命令以恢复操作。

在重新设置密钥操作完成之前，卷将具有两个密钥。新写入及其相应读取将使用新密钥。否则，读取将使用旧密钥。

> 您不能使用 `volume encryption rekey start` 重新设置SnapLock卷密钥。

步骤

1. 更改加密密钥：

   ```
   volume encryption rekey start -vserver SVM_name -volume volume_name
   ```

   以下命令将更改的加密密钥 `vol1` 在SVM上`vs1`：

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. 验证重新设置密钥操作的状态：

   ```
   volume encryption rekey show
   ```

   有关完整的命令语法，请参见命令手册页。

   以下命令显示重新设置密钥操作的状态：

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 重新设置密钥操作完成后，验证卷是否已启用加密：

   ```
   volume show -is-encrypted true
   ```

有关完整的命令语法，请参见命令手册页。

以下命令将显示上的加密卷 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

使用 **volume move start** 命令更改卷的加密密钥

安全最佳做法是定期更改卷的加密密钥。您可以使用 `volume move start` 命令以更改加密密钥。您必须使用 `volume move start` 在ONTAP 9.2及更早版本中。移动的卷可以位于同一聚合或不同聚合上。

关于此任务

您不能使用 `volume move start` 重新设置SnapLock或FlexGroup卷的密钥。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。

步骤

1. 移动现有卷并更改加密密钥：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   有关完整的命令语法，请参见命令手册页。

   以下命令将移动名为的现有卷 **`vol1`** 目标聚合 **`aggr2`** 并更改加密密钥：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   此时将为此卷创建一个新的加密密钥。卷上的数据将保持加密状态。

2. 验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关完整的命令语法，请参见命令手册页。

   以下命令将显示上的加密卷 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----  --------- ----
vs1       vol1     aggr2      online     RW   200GB    160.0GB   20%
```

轮换 **NetApp** 存储加密的身份验证密钥

使用 NetApp 存储加密（NetApp Storage Encryption， NSE）时，您可以轮换身份验证密钥。

关于此任务

如果您使用的是外部密钥管理器（KMIP），则支持在 NSE 环境中轮换身份验证密钥。

> 板载密钥管理器（OKM）不支持在 NSE 环境中轮换身份验证密钥。

步骤

1. 使用 `security key-manager create-key` 命令生成新的身份验证密钥。

   您需要先生成新的身份验证密钥，然后才能更改身份验证密钥。

2. 使用 `storage encryption disk modify -disk * -data-key-id` 命令以更改身份验证密钥。

删除加密卷

您可以使用 `volume delete` 命令以删除加密卷。

开始之前

- 您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。
- 卷必须处于脱机状态。

步骤

1. 删除加密卷：

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   有关完整的命令语法，请参见命令手册页。

   以下命令将删除名为的加密卷 `vol1`：

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   输入 ... `yes` 系统提示您确认删除时。

系统将在 24 小时后删除卷的加密密钥。

使用 ... `volume delete` 使用 `-force true` 可选择立即删除卷并销毁相应的加密密钥。此命令需要高级权限。有关详细信息，请参见手册页。

完成后

您可以使用 `volume recovery-queue` 命令以在发出后的保留期限内恢复已删除的卷 `volume delete` 命令：

```
volume recovery-queue SVM_name -volume volume_name
```

"如何使用卷恢复功能"

安全地清除加密卷上的数据

安全清除加密卷上的数据概述

从 ONTAP 9.4 开始，您可以使用安全清除功能无中断擦洗启用了 NVE 的卷上的数据。擦除加密卷上的数据可确保无法从物理介质恢复数据，例如，在 " s占用， " 的情况下，覆盖块时可能会留下数据跟踪，或者用于安全删除空出租户的数据。

安全清除仅适用于启用了 NVE 的卷上先前删除的文件。您不能擦除未加密的卷。您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

使用安全清除的注意事项

- 在为NetApp聚合加密(NAE)启用的聚合中创建的卷不支持安全清除。
- 安全清除仅适用于启用了 NVE 的卷上先前删除的文件。
- 您不能擦除未加密的卷。
- 您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

安全清除功能因 ONTAP 版本而异。

ONTAP 9.8及更高版本

- MetroCluster 和 FlexGroup 支持安全清除。
- 如果要清除的卷是 SnapMirror 关系的源，则无需中断 SnapMirror 关系即可执行安全清除。
- 对于使用 SnapMirror 数据保护的卷，重新加密方法与不使用 SnapMirror 数据保护（ DP ）或使用 SnapMirror 扩展数据保护的卷不同。
  - 默认情况下，使用 SnapMirror 数据保护（ DP ）模式的卷使用卷移动重新加密方法重新加密数据。
  - 默认情况下，未使用 SnapMirror 数据保护的卷或使用 SnapMirror 扩展数据保护（ XDP ）模式的卷使用原位重新加密方法。
  - 可以使用更改这些默认值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令：
- 默认情况下， FlexVol 卷中的所有 Snapshot 副本都会在安全清除操作期间自动删除。默认情况下，在安全清除操作期间，不会自动删除使用 SnapMirror 数据保护的 FlexGroup 卷和卷中的快照。可以使用更改这些默认值 `secure purge delete-all-snapshots [true|false]` 命令：

ONTAP 9.7及更早版本：

- 安全清除不支持以下内容：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的卷是 SnapMirror 关系的源，则必须先断开 SnapMirror 关系，然后才能清除该卷。

  如果卷中的 Snapshot 副本繁忙，则必须先释放 Snapshot 副本，然后才能清除卷。例如，您可能需要将 FlexClone 卷从其父卷拆分。
- 成功调用安全清除功能将触发卷移动，以便使用新密钥重新加密其余未清除的数据。

  移动的卷将保留在当前聚合上。旧密钥会自动销毁，以确保已清除的数据无法从存储介质恢复。

安全地清除加密卷上的数据，而不存在 **SnapMirror** 关系

从 ONTAP 9.4 开始，您可以使用安全清除功能在启用了 NVE 的卷上无中断地生成 " `scrub` " 数据。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
2. 在存储系统上，更改为高级权限级别：

   ```
   set -privilege advanced
   ```

3. 如果要安全清除的文件位于快照中，请删除这些快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 安全清除已删除的文件：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   以下命令可安全清除上已删除的文件 `vol1` 在SVM上`vs1`：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 验证安全清除操作的状态：

   ```
   volume encryption secure-purge show
   ```

使用异步 **SnapMirror** 关系安全地清除加密卷上的数据

从 ONTAP 9.8 开始，您可以使用安全清除功能在具有异步 SnapMirror 关系且已启用 NVE 的卷上无中断地传输 " `scrub` " 数据。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

步骤

1. 在存储系统上、切换到高级权限级别：

   ```
   set -privilege advanced
   ```

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。

3. 准备异步关系中要安全清除的目标卷：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   对异步 SnapMirror 关系中的每个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 如果要安全清除的文件位于基本 Snapshot 副本中，请执行以下操作：

   a. 在异步 SnapMirror 关系中的目标卷上创建 Snapshot 副本：

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. 更新 SnapMirror 以将基本 Snapshot 副本向前移动：

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   对异步 SnapMirror 关系中的每个卷重复此步骤。

   a. 重复步骤（a）和（b），使其等于基本 Snapshot 副本数加 1 。

      例如，如果您有两个基本 Snapshot 副本，则应重复步骤（a）和（b）三次。

   b. 验证是否存在基本Snapshot副本：

      ```
      snapshot show -vserver SVM_name -volume volume_name
      ```

   c. 删除基本Snapshot副本：

      ```
      snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
      ```

6. 安全清除已删除的文件：

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

对异步 SnapMirror 关系中的每个卷重复此步骤。

以下命令可安全清除 SVM "`vs1` " 上 "`vol1` " 上的已删除文件：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. 验证安全清除操作的状态：

```
volume encryption secure-purge show
```

擦除具有同步 **SnapMirror** 关系的加密卷上的数据

从ONTAP 9.8开始、您可以使用安全清除功能无故障"擦除"启用了NVE且具有同步SnapMirror关系的卷上的数据。

关于此任务

安全清除可能需要几分钟到几小时才能完成，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 在存储系统上，更改为高级权限级别：

```
set -privilege advanced
```

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
3. 准备异步关系中要安全清除的目标卷：

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

对同步 SnapMirror 关系中的另一个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. 如果安全清除文件位于基本 Snapshot 副本或通用 Snapshot 副本中，请更新 SnapMirror 以将通用 Snapshot 副本前移：

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   有两个通用 Snapshot 副本，因此必须发出此命令两次。

6. 如果安全清除文件位于应用程序一致的 Snapshot 副本中，请删除同步 SnapMirror 关系中两个卷上的 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   对两个卷执行此步骤。

7. 安全清除已删除的文件：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   对同步 SnapMirror 关系中的每个卷重复此步骤。

   以下命令可安全清除 SMV"`vs1` " 上 "`vol1` " 上已删除的文件。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. 验证安全清除操作的状态：

   ```
   volume encryption secure-purge show
   ```

更改板载密钥管理密码短语

安全最佳做法是定期更改板载密钥管理密码短语。您应将新的板载密钥管理密码短语复制到存储系统以外的安全位置，以供将来使用。

开始之前

- 要执行此任务，您必须是集群或 SVM 管理员。
- 此任务需要高级权限。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 更改板载密钥管理密码短语：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard update-passphrase`
ONTAP 9.5 及更早版本	`security key-manager update-passphrase`

有关完整的命令语法，请参见手册页。

以下ONTAP 9.6命令可用于更改的板载密钥管理密码短语 `cluster1`：

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. 输入 … `y` 在提示更改板载密钥管理密码短语时。
4. 在当前密码短语提示符处输入当前密码短语。
5. 在新的密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` "，输入 64 到 256 个字符的密码短语。

   如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

6. 在密码短语确认提示符处，重新输入密码短语。

完成后

在 MetroCluster 环境中，您必须更新配对集群上的密码短语：

- 在ONTAP 9.5及更早版本中、必须运行 `security key-manager update-passphrase` 在配对集群上使用相同密码短语。
- 在ONTAP 9.6及更高版本中、系统会提示您运行 `security key-manager onboard sync` 在配对集群上使用相同密码短语。

您应将板载密钥管理密码短语复制到存储系统以外的安全位置，以供将来使用。

更改板载密钥管理密码短语时，您应手动备份密钥管理信息。

"手动备份板载密钥管理信息"

手动备份板载密钥管理信息

配置板载密钥管理器密码短语时，应将板载密钥管理信息复制到存储系统外的安全位置。

您需要的内容

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

关于此任务

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。您还应手动备份密钥管理信息，以便在发生灾难时使用。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 显示集群的密钥管理备份信息：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard show-backup`
ONTAP 9.5 及更早版本	`security key-manager backup show`

有关完整的命令语法，请参见手册页。

+
以下9.6命令显示的密钥管理备份信息 `cluster1`：

+

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. 将备份信息复制到存储系统以外的安全位置，以便在发生灾难时使用。

还原板载密钥管理加密密钥

根据您的ONTAP版本、您还原板载密钥管理加密密钥所遵循的操作步骤会有所不同。

开始之前

- 如果将 NSE 与外部密钥管理（ KMIP ）服务器结合使用，则必须已删除外部密钥管理器数据库。有关详细信息，请参见 "从外部密钥管理过渡到板载密钥管理"
- 您必须是集群管理员才能执行此任务。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

具有加密根卷的**ONTAP 9.8**及更高版本

> 如果您运行的是ONTAP 9.8或更高版本、并且根卷未加密、请遵循适用于ONTAP 9.6或更高版本的操作步骤。

如果您运行的是 ONTAP 9.8 及更高版本，并且根卷已加密，则必须在启动菜单中设置板载密钥管理恢复密码短语。如果要更换启动介质、也需要执行此过程。

1. 将节点启动至启动菜单、然后选择选项 `(10) Set onboard key management recovery secrets`。
2. 输入 … `y` 以使用此选项。
3. 在提示符处，输入集群的板载密钥管理密码短语。
4. 在提示符处，输入备份密钥数据。

   节点将返回到启动菜单。

5. 从启动菜单中、选择选项 `(1) Normal Boot`。

ONTAP 9.6 及更高版本

1. 验证是否需要还原密钥：+
   `security key-manager key query -node` *`node`*
2. 还原密钥：+
   `security key-manager onboard sync`

   有关完整的命令语法，请参见手册页。

   以下 ONTAP 9.6 命令可同步板载密钥层次结构中的密钥：

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

3. 在密码短语提示符处，输入集群的板载密钥管理密码短语。

ONTAP 9.5 及更早版本

1. 验证是否需要还原密钥：+
   `security key-manager key show`
2. 如果您运行的是 ONTAP 9.8 及更高版本，并且根卷已加密，请完成以下步骤：

   如果您运行的是 ONTAP 9.6 或 9.7 ，或者运行的是 ONTAP 9.8 或更高版本，并且根卷未加密，请跳过此步骤。

3. 还原密钥：+
   `security key-manager setup -node node`

   有关完整的命令语法，请参见手册页。

4. 在密码短语提示符处，输入集群的板载密钥管理密码短语。

还原外部密钥管理加密密钥

您可以手动还原外部密钥管理加密密钥并将其推送到其他节点。如果要重新启动在为集群创建密钥时临时关闭的节点，则可能需要执行此操作。

关于此任务

在ONTAP 9.6及更高版本中、您可以使用 `security key-manager key query -node node_name` 命令以验证是否需要还原密钥。

在ONTAP 9.5及更早版本中、您可以使用 `security key-manager key show` 命令以验证是否需要还原密钥。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 如果您运行的是 ONTAP 9.8 或更高版本，并且根卷已加密，请执行以下操作：

   如果您运行的是 ONTAP 9.7 或更早版本，或者运行的是 ONTAP 9.8 或更高版本，并且根卷未加密，请跳过此步骤。

   a. 设置Bootargs：

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. 将节点启动至启动菜单、然后选择选项 `(11) Configure node for external key management`。

   c. 按照提示输入管理证书。

      输入所有管理证书信息后，系统将返回到启动菜单。

   d. 从启动菜单中、选择选项 `(1) Normal Boot`。

2. 还原密钥：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 及更早版本

> node 默认为所有节点。有关完整的命令语法，请参见手册页。启用板载密钥管理后，不支持此命令。

以下ONTAP 9.6命令可将外部密钥管理身份验证密钥还原到中的所有节点 `cluster1`：

```
clusterl::> security key-manager external restore
```

替换 **SSL** 证书

所有 SSL 证书都具有到期日期。您必须在证书到期之前对其进行更新，以防止对身份验证密钥的访问丢失。

开始之前

- 您必须已获取集群的替代公有证书和专用密钥（ KMIP 客户端证书）。
- 您必须已获取 KMIP 服务器的替代公有证书（ KMIP server-ca 证书）。
- 要执行此任务，您必须是集群或 SVM 管理员。
- 在MetroCluster 环境中、必须替换两个集群上的KMIP SSL证书。

> 在集群上安装证书之前或之后，您可以在 KMIP 服务器上安装替代客户端和服务器证书。

步骤

1. 安装新的 KMIP server-ca 证书：

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. 安装新的 KMIP 客户端证书：

   ```
   security certificate install -type client -vserver <>
   ```

3. 更新密钥管理器配置以使用新安装的证书：

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   如果您在MetroCluster 环境中运行ONTAP 9.6或更高版本、并且要修改管理SVM上的密钥管理器配置、则必须在配置中的两个集群上运行命令。

> 如果新客户端证书的公共 / 专用密钥与先前安装的密钥不同，则更新密钥管理器配置以使用新安装的证书将返回错误。请参见知识库文章 "新的客户端证书公有 或专用密钥与现有客户端证书不同" 有关如何覆盖此错误的说明。

更换 **FIPS** 驱动器或 **SED**

您可以像替换普通磁盘一样更换 FIPS 驱动器或 SED 。确保为替代驱动器分配新的数据身份验证密钥。对于 FIPS 驱动器，您可能还需要分配新的 FIPS 140-2 身份验证密钥。

> HA 对使用时 "加密 SAS 或 NVMe 驱动器（ SED， NSE， FIPS）"，您必须按照主题中的说明进行操作 "将 FIPS 驱动器或 SED 恢复到未受保护的模式" 初始化系统之前 HA 对中的所有驱动器（启动选项 4 或 9）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

开始之前

- 您必须知道驱动器使用的身份验证密钥的密钥 ID 。
- 您必须是集群管理员才能执行此任务。

步骤

1. 确保磁盘已标记为故障：

   ```
   storage disk show -broken
   ```

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                    Usable
   Physical
       Disk    Outage Reason HA Shelf Bay Chan    Pool  Type     RPM      Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. 按照适用于您的磁盘架型号的硬件指南中的说明，删除故障磁盘并将其更换为新的 FIPS 驱动器或 SED 。
3. 分配新更换磁盘的所有权：

   ```
   storage disk assign -disk disk_name -owner node
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 确认已分配新磁盘：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. 将数据身份验证密钥分配给 FIPS 驱动器或 SED 。

   "将数据身份验证密钥分配给 FIPS 驱动器或 SED （外部密钥管理）"

6. 如有必要，请为 FIPS 驱动器分配 FIPS 140-2 身份验证密钥。

   "将 FIPS 140-2 身份验证密钥分配给 FIPS 驱动器"

使 **FIPS** 驱动器或 **SED** 上的数据无法访问

使 **FIPS** 驱动器或 **SED** 上的数据无法访问概述

如果要使 FIPS 驱动器或 SED 上的数据永久不可访问，但要为新数据保留驱动器的未用空间，则可以对磁盘进行清理。如果要使数据永久不可访问且无需重复使用驱动器，可以将其销毁。

- 磁盘清理

  清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 false ，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0 （ SAS 驱动器）或空密钥（ NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

- 磁盘销毁

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定磁盘。这样做会使磁盘永久不可用，并且磁盘上的数据永久不可访问。

您可以清理或销毁节点的单个自加密驱动器或所有自加密驱动器。

清理 FIPS 驱动器或 SED

如果要使FIPS驱动器或SED上的数据永久不可访问、并使用该驱动器存储新数据、则可以使用 `storage encryption disk sanitize` 命令以对驱动器进行磁盘管理。

关于此任务

清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 false ，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0 （ SAS 驱动器）或空密钥（ NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要清理的 FIPS 驱动器或 SED 上的聚合：

   `storage aggregate delete -aggregate` *`aggregate_name`*

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. 确定要清理的 FIPS 驱动器或 SED 的磁盘 ID ：

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. 如果 FIPS 驱动器以 FIPS 兼容模式运行，请将节点的 FIPS 身份验证密钥 ID 设置回默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. 清理驱动器：

   `storage encryption disk sanitize -disk disk_id`

   您只能使用此命令清理热备用磁盘或损坏的磁盘。要清理所有磁盘、而不管其类型如何、请使用 `-force -all-state` 选项有关完整的命令语法，请参见手册页。

   ONTAP将提示您输入确认短语、然后再继续。输入屏幕上所示的短语。

   ```
   cluster1::> storage encryption disk sanitize -disk 1.10.2

   Warning: This operation will cryptographically sanitize 1 spare or
   broken self-encrypting disk on 1 node.
            To continue, enter sanitize disk: sanitize disk

   Info: Starting sanitize on 1 disk.
         View the status of the operation using the
         storage encryption disk show-status command.
   ```

销毁 **FIPS** 驱动器或 **SED**

如果要使FIPS驱动器或SED上的数据永久不可访问、并且不需要重复使用该驱动器、则可以使用 `storage encryption disk destroy` 命令销毁磁盘。

关于此任务

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定该驱动器。这样做会使磁盘几乎不可用，并且磁盘上的数据永远不可访问。但是，您可以使用磁盘标签上印有的物理安全 ID （ PSID ）将磁盘重置为出厂配置的设置。有关详细信息，请参见 "丢失身份验证密钥后，使 FIPS 驱动器或 SED 恢复正常运行"。

除非您拥有不可退回的磁盘加载服务（ NRD Plus ），否则不应销毁 FIPS 驱动器或 SED 。销毁磁盘将使其保修失效。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要销毁的 FIPS 驱动器或 SED 上的聚合：

   `storage aggregate delete -aggregate aggregate_name`

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. 确定要销毁的 FIPS 驱动器或 SED 的磁盘 ID：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. 销毁磁盘：

   `storage encryption disk destroy -disk disk_id`

   有关完整的命令语法，请参见手册页。

   系统将提示您输入确认短语，然后再继续。输入屏幕上所示的短语。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

紧急粉碎**FIPS**驱动器或**SED**上的数据

在发生安全紧急情况时，您可以立即阻止访问 FIPS 驱动器或 SED ，即使存储系统或 KMIP 服务器没有电源也是如此。

开始之前

- 如果您使用的 KMIP 服务器没有电源，则必须为 KMIP 服务器配置一个易于销毁的身份验证项（例如，智能卡或 USB 驱动器）。
- 您必须是集群管理员才能执行此任务。

步骤

1. 对 FIPS 驱动器或 SED 上的数据执行紧急粉碎：

条件	那么 ...

存储系统已通电，您有时间使存储系统正常脱机	a. 如果存储系统配置为 HA 对，请禁用接管。
	b. 使所有聚合脱机并将其删除。
	c. 将权限级别设置为高级：
	`set -privilege advanced`
	d. 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID：
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. 暂停存储系统。
	f. 启动至维护模式：
	g. 清理或销毁磁盘：
	◦ 如果要使磁盘上的数据无法访问、并且仍然能够重复使用这些磁盘、请清理这些磁盘：
	`disk encrypt sanitize -all`
	◦ 如果要使磁盘上的数据无法访问、并且不需要保存磁盘、请销毁磁盘：
	`disk encrypt destroy disk_id1 disk_id2 …`
	ⓘ ◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令仅保留用于维护模式。这些命令必须在每个 HA 节点上运行，并且不适用于损坏的磁盘。
	h. 对配对节点重复上述步骤。这会使存储系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。
		存储系统已通电，您必须立即粉碎数据

a. * 如果要使磁盘上的数据无法访问且仍能重复使用这些磁盘，请清理磁盘： *
b. 如果存储系统配置为 HA 对，请禁用接管。
c. 将权限级别设置为高级：
`set -privilege advanced`
d. 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID：
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. 清理磁盘：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. * 如果要使磁盘上的数据无法访问，并且不需要保存磁盘，请销毁磁盘： *
	b. 如果存储系统配置为 HA 对，请禁用接管。
	c. 将权限级别设置为高级：
	`set -privilege advanced`
	d. 销毁磁盘：
	`storage encryption disk destroy -disk * -force-all-states true`
		存储系统崩溃，使系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。

KMIP 服务器可以通电，但存储系统不能通电	a. 登录到KMIP服务器。 b. 销毁与包含要阻止访问的数据的 FIPS 驱动器或 SED 关联的所有密钥。 这样会阻止存储系统访问磁盘加密密钥。	KMIP 服务器或存储系统不能通电

有关完整的命令语法，请参见手册页。

如果身份验证密钥丢失，请将 **FIPS** 驱动器或 **SED** 恢复使用

如果您永久丢失 FIPS 驱动器或 SED 的身份验证密钥，并且无法从 KMIP 服务器检索这些密钥，则系统会将其视为已损坏。虽然您无法访问或恢复磁盘上的数据，但可以采取措施使 SED 的未用空间再次可用于数据。

开始之前

您必须是集群管理员才能执行此任务。

关于此任务

只有在确定 FIPS 驱动器或 SED 的身份验证密钥永久丢失且无法恢复时，才应使用此过程。

如果磁盘已分区、则必须先取消分区、然后才能启动此过程。

取消磁盘分区的命令只能在diag级别使用、并且只能在NetApp支持监督下执行。强烈建议您在继续操作之前联系**NetApp**支持部门。您也可以参考知识库文章 "如何在ONTAP 中取消对备用驱动器的分区"。

步骤

1. 将 FIPS 驱动器或 SED 恢复正常运行：

SED 是否为 …	请执行以下步骤 …

不在 FIPS 兼容模式或 FIPS 兼容模式下，并且 FIPS 密钥可用	a. 将权限级别设置为高级：
	`set -privilege advanced`
	b. 将FIPS密钥重置为默认制造安全ID 0x0：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 验证操作是否成功：
	`storage encryption disk show-status`
	如果操作失败、请使用本主题中的PSID过程。
	d. 对已损坏的磁盘进行分区：
	`storage encryption disk sanitize -disk disk_id`
	使用命令验证操作是否成功 `storage encryption disk show-status` 然后再继续下一步。
	e. 使已清除的磁盘恢复失败：
	`storage disk unfail -spare true -disk disk_id`
	f. 检查磁盘是否具有所有者：
	`storage disk show -disk disk_id`
	如果磁盘没有所有者、请分配一个。
	`storage disk assign -owner node -disk disk_id`
	i. 输入拥有要清理的磁盘的节点的 nodeshell ：
	`system node run -node node_name`
	运行 `disk sanitize release` 命令：
	g. 退出nokeshell。再次解除磁盘故障：
	`storage disk unfail -spare true -disk disk_id`
	h. 验证磁盘现在是否为备用磁盘并可在聚合中重复使用：
	`storage disk show -disk disk_id`

在 FIPS 兼容模式下，FIPS 密钥不可用， SED 的标签上印有 PSID	a. 从磁盘标签中获取磁盘的 PSID 。 b. 将权限级别设置为高级： `set -privilege advanced` c. 将磁盘重置为出厂配置设置： `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* 使用命令验证操作是否成功 `storage encryption disk show-status` 然后再继续下一步。 d. 如果您运行的是ONTAP 9.8P5或更早版本、请跳至下一步。如果您运行的是ONTAP 9.8p6或更高版本、请使已检查的磁盘恢复故障。 `storage disk unfail -disk` *`disk_id`* e. 检查磁盘是否具有所有者： `storage disk show -disk` *`disk_id`* 如果磁盘没有所有者、请分配一个。 `storage disk assign -owner node -disk` *`disk_id`* i. 输入拥有要清理的磁盘的节点的 nodeshell ： `system node run -node` *`node_name`* 运行 `disk sanitize release` 命令： f. 退出nokeshell。再次解除磁盘故障： `storage disk unfail -spare true -disk` *`disk_id`* g. 验证磁盘现在是否为备用磁盘并可在聚合中重复使用： `storage disk show -disk` *`disk_id`*

有关完整的命令语法，请参见 "命令参考"。

将 **FIPS** 驱动器或 **SED** 恢复到未受保护的模式

只有当节点的身份验证密钥 ID 设置为非默认值时， FIPS 驱动器或 SED 才会受到保护，防止未经授权的访问。您可以使用将FIPS驱动器或SED返回到未受保护的模式 `storage encryption disk modify` 命令将密钥ID设置为默认值。

如果 HA 对使用加密 SAS 或 NVMe 驱动器（ SED ， NSE ， FIPS ），则必须在初始化系统之前对 HA 对中的所有驱动器执行此过程（启动选项 4 或 9 ）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 如果 FIPS 驱动器以 FIPS 兼容模式运行，请将节点的 FIPS 身份验证密钥 ID 设置回默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用命令确认操作成功：

   `storage encryption disk show-status`

   重复show-status命令、直到"磁盘已开始"和"磁盘已完成"中的数字相同为止。

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. 将节点的数据身份验证密钥 ID 重新设置为默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   的值 `-data-key-id` 无论您要将SAS或NVMe驱动器返回到未受保护的模式、都应设置为0x0。

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

使用命令确认操作成功：

```
storage encryption disk show-status
```

重复 show-status 命令，直到数字相同为止。如果"disks"(磁盘开始)和"disks Done (磁盘完成)"中的数字相同、则操作完成。

维护模式

从ONTAP 9.7开始、您可以从维护模式重新为FIPS驱动器设置密钥。只有在无法使用上一节中的ONTAP 命令行界面说明时、才应使用维护模式。

步骤

1. 将节点的FIPS身份验证密钥ID重新设置为默认MSID 0x0：

   ```
   disk encrypt rekey_fips 0x0 disklist
   ```

2. 将节点的数据身份验证密钥 ID 重新设置为默认 MSID 0x0 ：

   ```
   disk encrypt rekey 0x0 disklist
   ```

3. 确认已成功重新设置FIPS身份验证密钥密钥：

   ```
   disk encrypt show_fips
   ```

4. 确认已使用成功重新设置数据身份验证密钥密钥：

   ```
   disk encrypt show
   ```

   您的输出可能会显示默认的MSID 0x0密钥ID或密钥服务器持有的64字符值。。 `Locked?` 字段是指数据锁定。

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

删除外部密钥管理器连接

当您不再需要 KMIP 服务器时，可以将其从节点断开。例如，在过渡到卷加密时，您可能会断开 KMIP 服务器的连接。

关于此任务

当您从 HA 对中的一个节点断开 KMIP 服务器的连接时，系统会自动断开此服务器与所有集群节点的连接。

> 如果您计划在断开 KMIP 服务器连接后继续使用外部密钥管理，请确保另一个 KMIP 服务器可用于提供身份验证密钥。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 断开 KMIP 服务器与当前节点的连接：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 及更早版本

在MetroCluster 环境中、必须对管理SVM的两个集群重复这些命令。

有关完整的命令语法，请参见手册页。

以下ONTAP 9.6命令将禁用与两个外部密钥管理服务器的连接 `cluster1`，第一个名为 `ks1`，侦听默认端口5696，第二个端口IP地址为10.0.0.20，侦听端口24482：

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

修改外部密钥管理服务器属性

从ONTAP 9.6开始、您可以使用 `security key-manager external modify-server` 用于更改外部密钥管理服务器的I/O超时和用户名的命令。

开始之前

- 要执行此任务，您必须是集群或 SVM 管理员。
- 此任务需要高级权限。
- 在MetroCluster 环境中、必须对管理SVM的两个集群重复这些步骤。

步骤

1. 在存储系统上，更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 修改集群的外部密钥管理器服务器属性：

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> 超时值以秒为单位。如果您修改了用户名，系统将提示您输入新密码。 如果在集群登录提示符处运行命令、 *admin_SVM* 默认为当前集群的管理SVM。您必须是集群管理员才能修改外部密钥管理器服务器属性。

以下命令会将的超时值更改为45秒 `cluster1` 侦听默认端口5696的外部密钥管理服务器：

```
clusterl::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. 修改 SVM 的外部密钥管理器服务器属性（仅限 NVE ）：

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> 超时值以秒为单位。如果您修改了用户名，系统将提示您输入新密码。 如果在SVM登录提示符处运行命令、 *SVM* 默认为当前SVM。您必须是集群或 SVM 管理员才能修改外部密钥管理器服务器属性。

以下命令将更改的用户名和密码 `svm1` 侦听默认端口5696的外部密钥管理服务器：

```
svml::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. 对任何其他 SVM 重复最后一步。

从板载密钥管理过渡到外部密钥管理

如果要从板载密钥管理切换到外部密钥管理，则必须先删除板载密钥管理配置，然后才能启用外部密钥管理。

开始之前

- 对于基于硬件的加密，必须将所有 FIPS 驱动器或 SED 的数据密钥重置为默认值。

  "将 FIPS 驱动器或 SED 恢复到未受保护的模式"

- 对于基于软件的加密，您必须取消对所有卷的加密。

  "取消卷数据加密"

- 您必须是集群管理员才能执行此任务。

步骤

1. 删除集群的板载密钥管理配置：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 及更早版本	`security key-manager delete-key-database`

有关完整的命令语法，请参见 "ONTAP 手册页"。

从外部密钥管理过渡到板载密钥管理

如果要从外部密钥管理切换到板载密钥管理，则必须先删除外部密钥管理配置，然后才能启用板载密钥管理。

开始之前

- 对于基于硬件的加密，必须将所有 FIPS 驱动器或 SED 的数据密钥重置为默认值。

  "将 FIPS 驱动器或 SED 恢复到未受保护的模式"

- 您必须已删除所有外部密钥管理器连接。

  "删除外部密钥管理器连接"

- 您必须是集群管理员才能执行此任务。

操作步骤

过渡密钥管理的步骤取决于您使用的ONTAP版本。

ONTAP 9.6 及更高版本

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 使用命令：

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   在MetroCluster 环境中、必须对管理SVM的两个集群重复此命令。

ONTAP 9.5 及更早版本

使用命令：

```
security key-manager delete-kmip-config
```

启动过程中无法访问密钥管理服务器时会发生什么情况

如果为 NSE 配置的存储系统在启动过程中无法访问任何指定的密钥管理服务器，则 ONTAP 会采取某些预防措施来避免发生意外行为。

如果存储系统配置了 NSE ， SED 已重新设置密钥并锁定，并且 SED 已启动，则存储系统必须从密钥管理服务器检索所需的身份验证密钥，以便向 SED 进行身份验证，然后才能访问数据。

存储系统会尝试联系指定的密钥管理服务器，最长三小时。如果存储系统在该时间后无法访问其中任何一个，则启动过程将停止，存储系统将暂停。

如果存储系统成功联系任何指定的密钥管理服务器，则会尝试建立 SSL 连接，时间最长为 15 分钟。如果存储系统无法与任何指定的密钥管理服务器建立 SSL 连接，则启动过程将停止，存储系统将暂停。

当存储系统尝试联系并连接到密钥管理服务器时，它会在 CLI 中显示有关失败的联系尝试的详细信息。您可以随时按 Ctrl-C 中断联系尝试

作为一项安全措施， SED 仅允许有限数量的未授权访问尝试，之后，它们将禁用对现有数据的访问。如果存储系统无法联系任何指定的密钥管理服务器以获取正确的身份验证密钥，则只能尝试使用默认密钥进行身份验证，从而导致尝试失败并发生崩溃。如果存储系统配置为在发生崩溃时自动重新启动，则它将进入启动环路，从而导致 SED 上的身份验证尝试持续失败。

在这些情况下，暂停存储系统的设计是为了防止存储系统进入启动环路，并防止因连续失败身份验证尝试次数超过安全限制而永久锁定 SED 而可能导致意外数据丢失。锁定保护的限制和类型取决于 SED 的制造规格和类型：

SED类型	导致锁定的连续身份验证尝试失败次数	达到安全限制时的锁定保护类型
HDD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。
X440_PHM2800MCTO 800 GB NSE SSD ，固件版本为 NA00 或 NA01	5.	临时。只有在磁盘重新启动之前，锁定才有效。
X577_PHM2800MCTO 800 GB NSE SSD、固件版本为NA00或NA01	5.	临时。只有在磁盘重新启动之前，锁定才有效。
具有更高固件版本的 X440_PHM2800MCTO 800 GB NSE SSD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。
具有更高固件版本的 X567_PHM2800MCTO 800 GB NSE SSD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。
所有其他 SSD 型号	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。

对于所有 SED 类型，成功的身份验证会将尝试次数重置为零。

如果您遇到存储系统因无法访问任何指定密钥管理服务器而暂停的情况，则必须先确定并更正通信失败的发生原因，然后再尝试继续启动存储系统。

默认情况下禁用加密

从 ONTAP 9.7 开始，如果您拥有卷加密（Volume Encryption， VE）许可证并使用板载或外部密钥管理器，则默认情况下会启用聚合和卷加密。如有必要、您可以默认为整个集群禁用加密。

开始之前

要执行此任务，您必须是集群管理员，或者集群管理员已向其委派权限的 SVM 管理员。

步骤

1. 要在 ONTAP 9.7 或更高版本中默认对整个集群禁用加密，请运行以下命令：

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```