审核 **SVM** 上的 **NAS** 事件

ONTAP 9

NetApp
February 12, 2026

目录

审核 SVM 上的 NAS 事件

了解如何对SMB和NFS协议使用ONTAP审核文件访问

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

了解基本的**ONTAP**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。

了解**ONTAP**审核过程的运行情况

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。

ONTAP审核的前提条件

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。

- 启用了NFS和S3审核的SVM的综合限制取决于您的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。

对ONTAP审核记录的暂存文件大小的限制

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.
  ```

了解ONTAP审核事件日志支持的格式

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。

查看和处理ONTAP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

了解ONTAP可以审核以解释结果的SMB事件

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。

可以审核以下附加 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ONTAP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
```

了解ONTAP对符号链接和硬链接的审核

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。

了解ONTAP对备用NTFS数据流的审核

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>
```

了解ONTAP对NFS文件和目录访问事件的审核

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ONTAP SVM上的审核配置

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）

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。 • 异步删除 • 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`	`async-delete}`

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。

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

在ONTAP SVM上创建文件和目录审核配置

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
```

相关信息

- "在 SVM 上启用审核"
- "验证审核配置"

设置审核配置后、在ONTAP 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。

开始之前

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
```

相关信息

- "创建审核配置"
- "验证审核配置"

验证ONTAP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
   ```

相关信息

- "创建审核配置"
- "在 SVM 上启用审核"

配置文件和文件夹审核策略

在ONTAP SVM上启用审核配置并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**ONTAP**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。

开始之前

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 。要了解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"ONTAP 命令参考"。

为UNIX安全模式文件和目录配置ONTAP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"ONTAP 命令参考"。

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

通过访问ONTAP安全性选项卡查看Windows审核策略信息

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。

显示有关**ONTAP FlexVol**卷上的**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
```

使用通配符显示有关**ONTAP**文件安全性和审核策略的信息

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

了解可审核的ONTAP命令行界面更改事件

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`

相关信息

- "vserver"

管理文件共享ONTAP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audy-policy-change ONTAP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**ONTAP**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ONTAP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authorizy-policy-change ONTAP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以查看特定的ONTAP SVM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ONTAP SVM上启用或禁用审核

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）。

开始之前

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ONTAP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：

   有关的详细信息 `vserver audit show`，请参见"ONTAP 命令参考"。

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ONTAP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ONTAP SVM上的审核配置

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
```

了解还原经过审核的ONTAP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ONTAP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及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：
>
> - 目标目录将被删除。
> - 托管目标目录的卷上的文件限制已达到其最大级别。

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          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
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 (在ONTAP 9.14.1及更早版本中)或5 GB (从ONTAP 9.151开始)、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。