管理审核配置

ONTAP 9

NetApp
April 24, 2024

目录

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。