在 SVM 上创建文件和目录审核配置

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/nas-audit/create-auditing-config-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

目录

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
```

相关信息

- "在 SVM 上启用审核"
- "验证审核配置"

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。

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"

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。