审核的工作原理

ONTAP 9

NetApp
September 12, 2024

目录

审核的工作原理 1
基本审核概念 1
ONTAP 审核过程的工作原理 1

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。