配置文件和文件夹审核策略

ONTAP 9

NetApp
September 12, 2024

目录

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。

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 。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。