管理如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性

ONTAP 9

NetApp
September 12, 2024

目录

管理如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性

管理如何向 SMB 客户端提供文件安全性以了解 UNIX 安全模式数据概述

您可以通过启用或禁用向 SMB 客户端提供 NTFS ACL 来选择如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性。每个设置都有一些优势，您应了解这些优势，才能选择最适合您业务需求的设置。

默认情况下， ONTAP 会将 UNIX 安全模式卷上的 UNIX 权限作为 NTFS ACL 提供给 SMB 客户端。在某些情况下，这种做法是可取的，其中包括以下情形：

- 要查看和编辑 UNIX 权限，请使用 Windows 属性框中的 * 安全性 * 选项卡。

  如果 UNIX 系统不允许修改 Windows 客户端的权限，则不能修改此操作。例如，您不能更改不拥有的文件的所有权，因为 UNIX 系统不允许执行此操作。此限制可防止 SMB 客户端绕过对文件和文件夹设置的 UNIX 权限。

- 用户正在使用某些 Windows 应用程序编辑和保存 UNIX 安全模式卷上的文件，例如 Microsoft Office ，在这些应用程序中， ONTAP 必须在保存操作期间保留 UNIX 权限。
- 您的环境中有一些 Windows 应用程序希望对其使用的文件读取 NTFS ACL 。

在某些情况下，您可能需要禁用将 UNIX 权限作为 NTFS ACL 呈现。如果禁用此功能，则 ONTAP 会将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端。您可能希望将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端的具体原因如下：

- 您只能通过在 UNIX 客户端上使用挂载来更改 UNIX 权限。

  在 SMB 客户端上映射 UNIX 安全模式卷时， " 安全 " 选项卡不可用。映射的驱动器似乎已使用 FAT 文件系统进行格式化，该文件系统没有文件权限。

- 您正在通过 SMB 使用应用程序，这些应用程序会对访问的文件和文件夹设置 NTFS ACL ，如果数据驻留在 UNIX 安全模式卷上，则这些应用程序可能会失败。

  如果 ONTAP 将卷报告为 FAT ，则应用程序不会尝试更改 ACL 。

相关信息

在 FlexVol 卷上配置安全模式

在 qtree 上配置安全模式

启用或禁用为 UNIX 安全模式数据提供 NTFS ACL

您可以为 UNIX 安全模式数据（ UNIX 安全模式卷和具有 UNIX 有效安全性的混合安全模式卷）启用或禁用向 SMB 客户端提供 NTFS ACL 。

关于此任务

如果启用此选项，则 ONTAP 会将具有有效 UNIX 安全模式的卷上的文件和文件夹作为具有 NTFS ACL 提供给 SMB 客户端。如果禁用此选项，这些卷将作为 FAT 卷呈现给 SMB 客户端。默认情况下，将 NTFS ACL 提供给 SMB 客户端。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置UNIX NTFS ACL选项设置： `vserver cifs options modify -vserver` *`vserver_name`* `-is -unix-nt-acl-enabled {true|false}`
3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

ONTAP 如何保留 UNIX 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 Windows 安全性选项卡管理 UNIX 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用 Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

  如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。