



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 1
 - 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 1
 - 启用或禁用为 UNIX 安全模式数据提供 NTFS ACL 1
 - ONTAP 如何保留 UNIX 权限 2
 - 使用 Windows 安全性选项卡管理 UNIX 权限..... 2

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：

- 您只能通过通过 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。

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。