使用文件权限确保文件访问安全

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/smb-admin/configure-ntfs-windows-security-tab-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

使用文件权限确保文件访问安全

使用 Windows 安全性选项卡配置高级 NTFS 文件权限

您可以使用 Windows 属性窗口中的 * Windows 安全性 * 选项卡配置文件和文件夹的标准 NTFS 文件权限。

开始之前

执行此任务的管理员必须具有足够的 NTFS 权限才能更改对选定对象的权限。

关于此任务

通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（ DACL ）添加条目，可以在 Windows 主机上配置 NTFS 文件权限。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。

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 * 对话框：
   a. 选择一个 * 驱动器 * 字母。
   b. 在 * 文件夹 * 框中，键入包含要应用权限的数据的共享的 CIFS 服务器名称以及共享的名称。

      如果CIFS服务器名称为"`CIFS_SERVER`"、而共享名为"`shre1`"、则应键入 `\\CIFS_SERVER\share1`。

      您可以为 CIFS 服务器指定数据接口的 IP 地址，而不是 CIFS 服务器名称。

   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. 选择要为其设置 NTFS 文件权限的文件或目录。
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。
   - 安全性 * 选项卡显示设置了 NTFS 权限的用户和组的列表。* 权限 * 框显示了对选定的每个用户或组有效的允许和拒绝权限列表。
6. 单击 * 高级 * 。

   Windows 属性窗口显示有关分配给用户和组的现有文件权限的信息。
7. 单击 * 更改权限 * 。

   此时将打开权限窗口。
8. 执行所需的操作：

如果您要 ...	执行以下操作 ...
为新用户或组设置高级 NTFS 权限	a. 单击 * 添加 * 。 b. 在 * 输入要选择的对象名称 * 框中，键入要添加的用户或组的名称。 c. 单击 * 确定 * 。
更改用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要更改其高级权限的用户或组。 b. 单击 * 编辑 * 。
删除用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要删除的用户或组。 b. 单击 * 删除 * 。 c. 跳至步骤 13 。

如果要为新用户或组添加高级 NTFS 权限，或者更改现有用户或组的 NTFS 高级权限，则会打开 < 对象 > 的权限条目框。

9. 在 * 应用于 * 框中，选择要如何应用此 NTFS 文件权限条目。

   如果要对单个文件设置 NTFS 文件权限，则 * 应用于 * 框不会处于活动状态。* 应用于 * 设置默认为 * 仅此对象 * 。

10. 在 * 权限 * 框中，为要对此对象设置的高级权限选择 * 允许 * 或 * 拒绝 * 框。

    - 要允许指定的访问，请选中 * 允许 * 框。
    - 要不允许指定的访问，请选中 * 拒绝 * 框。 您可以对以下高级权限设置权限：
    - * 完全控制 *

      如果选择此高级权限，则会自动选择所有其他高级权限（允许或拒绝权限）。

    - * 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 *

> 如果任何高级权限框不可选，则是因为权限是从父对象继承的。

11. 如果希望此对象的子文件夹和文件继承这些权限，请选中 * 仅将这些权限应用于此容器中的对象和 / 或容器 * 框。
12. 单击 * 确定 * 。
13. 添加，删除或编辑完 NTFS 权限后，请为此对象指定继承设置：
    - 选中 * 包括此对象父级的可继承权限 * 框。

      这是默认值。
    - 选中 * 将所有子对象权限替换为此对象的可继承权限 * 框。

      如果要对单个文件设置 NTFS 文件权限，则权限框中不存在此设置。

      > 选择此设置时请务必小心。此设置将删除所有子对象的所有现有权限，并将其替换为此对象的权限设置。您可能会无意中删除不希望删除的权限。在混合安全模式卷或 qtree 中设置权限时尤其重要。如果子对象采用 UNIX 有效安全模式，则将 NTFS 权限传播到这些子对象会导致 ONTAP 将这些对象从 UNIX 安全模式更改为 NTFS 安全模式，并且这些子对象上的所有 UNIX 权限将替换为 NTFS 权限。

    - 选择这两个框。
    - 不选择任何一个框。
14. 单击 * 确定 * 关闭 * 权限 * 框。
15. 单击 * 确定 * 以关闭 * 对象 * 的高级安全设置框。

有关如何设置高级 NTFS 权限的详细信息，请参见 Windows 文档。

相关信息

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

显示NTFS安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

使用 ONTAP 命令行界面配置 NTFS 文件权限

您可以使用 ONTAP 命令行界面为文件和目录配置 NTFS 文件权限。这样，您就可以配置 NTFS 文件权限，而无需使用 Windows 客户端上的 SMB 共享连接到数据。

您可以通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（ DACL ）添加条目来配置 NTFS 文件权限。然后，安全描述符将应用于 NTFS 文件和目录。

您只能使用命令行配置 NTFS 文件权限。您不能使用命令行界面配置 NFSv4 ACL 。

步骤

1. 创建NTFS安全描述符。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. 将DACL添加到NTFS安全描述符。

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. 创建文件/目录安全策略。

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

通过 SMB 访问文件时， UNIX 文件权限如何提供访问控制

FlexVol 卷可以采用以下三种安全模式之一： NTFS ， UNIX 或混合。无论安全模式如何，您都可以通过 SMB 访问数据；但是，要以 UNIX 有效安全模式访问数据，需要适当的 UNIX 文件权限。

通过 SMB 访问数据时，在确定用户是否有权执行请求的操作时，会使用多种访问控制：

- 导出权限

  配置 SMB 访问的导出权限是可选的。

- 共享权限
- 文件权限

  以下类型的文件权限可能会应用于用户要执行操作的数据：

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX 模式位

对于设置了 NFSv4 ACL 或 UNIX 模式位的数据，将使用 UNIX 模式权限来确定对数据的文件访问权限。SVM 管理员需要设置适当的文件权限，以确保用户有权执行所需的操作。

混合安全模式卷中的数据可能采用 NTFS 或 UNIX 有效安全模式。如果数据采用 UNIX 有效安全模式，则在确定数据的文件访问权限时会使用 NFSv4 权限或 UNIX 模式位。

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。