配置安全模式

ONTAP 9

NetApp
April 24, 2024

目录

配置安全模式

安全模式如何影响数据访问

安全模式及其影响是什么

安全模式有四种： UNIX ， NTFS ，混合和统一。每个安全模式对处理数据权限的方式具有不同的影响。您必须了解不同的影响，以确保选择适合您的安全模式。

请务必了解，安全模式并不确定哪些客户端类型可以或不可以访问数据。安全模式仅确定 ONTAP 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

例如，如果某个卷使用 UNIX 安全模式，则由于 ONTAP 的多协议性质， SMB 客户端仍可访问数据（前提是它们正确进行身份验证和授权）。但是， ONTAP 使用的是 UNIX 权限，只有 UNIX 客户端才能使用原生工具进行修改。

安全风格	可以修改权限的客户端	客户端可以使用的权限	生成的有效安全模式	可以访问文件的客户端
"unix"	NFS	NFSv3 模式位	"unix"	NFS 和 SMB
NFSv4.x ACL	"unix"	NTFS	SMB	NTFS ACL
NTFS	混合	NFS 或 SMB	NFSv3 模式位	"unix"
NFSv4.x ACL	"unix"	NTFS ACL	NTFS	统一：
NFS 或 SMB	NFSv3 模式位	"unix"	NFSv4.1 ACL	"unix"
NTFS ACL	NTFS	统一： (仅限无限卷、在ONTAP 9.4及更早版本中。)	NFS 或 SMB	NFSv3 模式位
"unix"	NFSv4.1 ACL			NTFS ACL

FlexVol卷支持UNIX、NTFS和混合安全模式。混合或统一安全模式时，有效权限取决于上次修改权限的客户端类型，因为用户会逐个设置安全模式。如果修改权限的最后一个客户端是 NFSv3 客户端，则权限为 UNIX NFSv3 模式位。如果最后一个客户端是 NFSv4 客户端，则权限为 NFSv4 ACL 。如果最后一个客户端是 SMB 客户端，则权限为 Windows NTFS ACL 。

统一安全模式仅适用于无限卷，而 ONTAP 9.5 及更高版本不再支持无限卷。有关详细信息，请参见 "FlexGroup 卷管理概述"。

从ONTAP 9.2开始、 `show-effective-permissions` 参数 `vserver security file-directory` 命令用于显示为Windows或UNIX用户授予的对指定文件或文件夹路径的有效权限。此外、还有可选参数 `-share -name` 用于显示有效共享权限。

ONTAP 最初会设置一些默认文件权限。默认情况下， UNIX ，混合和统一安全模式卷中所有数据的有效安全模式为 UNIX ，有效权限类型为 UNIX 模式位（ 0755 ，除非另有指定），直到客户端按照默认安全模式进行配置为止。默认情况下， NTFS 安全模式卷中所有数据的有效安全模式为 NTFS ，并且具有一个 ACL ，允许对任何人进行完全控制。

设置安全模式的位置和时间

可以在 FlexVol 卷（根卷或数据卷）和 qtree 上设置安全模式。安全模式可以在创建时手动设置，自动继承或稍后更改。

确定要在 **SVM** 上使用的安全模式

为了帮助您确定要在卷上使用的安全模式，您应考虑两个因素。主要因素是管理文件系统的管理员类型。二级因素是访问卷上数据的用户或服务的类型。

在卷上配置安全模式时，应考虑环境的需求，以确保选择最佳安全模式并避免管理权限时出现问题。以下注意事项有助于您做出决定：

安全风格	选择条件
"unix"	• 文件系统由 UNIX 管理员管理。 • 大多数用户都是 NFS 客户端。 • 访问数据的应用程序使用 UNIX 用户作为服务帐户。
NTFS	• 文件系统由 Windows 管理员管理。 • 大多数用户都是SMB客户端。 • 访问数据的应用程序使用 Windows 用户作为服务帐户。
混合	文件系统由 UNIX 和 Windows 管理员管理，用户由 NFS 和 SMB 客户端组成。

安全模式继承的工作原理

如果在创建新的 FlexVol 卷或 qtree 时未指定安全模式，则它会以不同方式继承其安全模式。

安全模式按以下方式继承：

- FlexVol 卷继承其所属 SVM 的根卷的安全模式。
- qtree 继承其所属 FlexVol 卷的安全模式。
- 文件或目录会继承其所在 FlexVol 卷或 qtree 的安全模式。

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。

在 SVM 根卷上配置安全模式

您可以配置 Storage Virtual Machine （ SVM ）根卷安全模式，以确定 SVM 根卷上的数据所使用的权限类型。

步骤

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 用于定义安全模式的参数。

   根卷安全模式的可能选项为 `unix`， `ntfs``或 `mixed`。

2. 显示并验证配置，包括您创建的 SVM 的根卷安全模式： `vserver show -vserver vserver_name`

在 FlexVol 卷上配置安全模式

您可以配置 FlexVol 卷安全模式，以确定 Storage Virtual Machine （ SVM ）的 FlexVol 卷上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 FlexVol 卷 …	使用命令 …
尚不存在	`volume create` 并包括 `-security-style` 用于指定安全模式的参数。
已存在	`volume modify` 并包括 `-security-style` 用于指定安全模式的参数。

   FlexVol卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建 FlexVol 卷时未指定安全模式，则此卷将继承根卷的安全模式。

   有关的详细信息、请参见 `volume create` 或 `volume modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置，包括您创建的 FlexVol 卷的安全模式，请输入以下命令：

   ```
   volume show -volume volume_name -instance
   ```

在 qtree 上配置安全模式

您可以配置 qtree 卷安全模式，以确定 qtree 上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 **qtree…**	使用命令 **…**
尚不存在	`volume qtree create` 并包括 `-security -style` 用于指定安全模式的参数。
已存在	`volume qtree modify` 并包括 `-security -style` 用于指定安全模式的参数。

   qtree安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建qtree时未指定安全模式、则默认安全模式为 `mixed`。

有关的详细信息、请参见 `volume qtree create` 或 `volume qtree modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置(包括所创建的qtree的安全模式)、请输入以下命令： `volume qtree show -qtree qtree_name -instance`