使用本地用户和组进行身份验证和授权

ONTAP 9

NetApp
April 24, 2024

目录

使用本地用户和组进行身份验证和授权

ONTAP 如何使用本地用户和组

本地用户和组概念

在确定是否在环境中配置和使用本地用户和组之前，您应了解什么是本地用户和组以及有关它们的一些基本信息。

- * 本地用户 *

  具有唯一安全标识符（ SID ）的用户帐户，仅在创建该帐户的 Storage Virtual Machine （ SVM ）上可见。本地用户帐户具有一组属性，包括用户名和 SID 。本地用户帐户使用 NTLM 身份验证在 CIFS 服务器上进行本地身份验证。

  用户帐户有多种用途：

  - 用于向用户授予 *User Rights Management* 权限。
  - 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。

- * 本地组 *

  具有唯一 SID 的组只能在其创建所在的 SVM 上显示。组包含一组成员。成员可以是本地用户，域用户，域组和域计算机帐户。可以创建，修改或删除组。

  组有多种用途：

  - 用于向其成员授予 *User Rights Management* 权限。
  - 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。

- * 本地域 *

  具有本地作用域的域，该域受 SVM 的限制。本地域的名称是 CIFS 服务器名称。本地用户和组包含在本地域中。

- * 安全标识符（ SID ） *

  SID 是一个可变长度的数值，用于标识 Windows 模式的安全主体。例如，典型的 SID 采用以下形式： S-1-5-21-3139654847-1303905135-2517279418-123456 。

- * NTLM 身份验证 *

  一种 Microsoft Windows 安全方法，用于对 CIFS 服务器上的用户进行身份验证。

- * 集群复制数据库（ RDB ） *

  一个复制的数据库，其中集群中的每个节点上都有一个实例。本地用户和组对象存储在 RDB 中。

创建本地用户和本地组的原因

在 Storage Virtual Machine （ SVM ）上创建本地用户和本地组的原因有多种。例如，如果域控制器（ DC ）不可用，您可能希望使用本地组分配权限或 SMB 服务器位于工作组中，则可以使用本地用户帐户访问 SMB 服务器。

您可以出于以下原因创建一个或多个本地用户帐户：

- SMB 服务器位于工作组中，域用户不可用。

  在工作组配置中需要本地用户。

- 您希望在域控制器不可用时能够进行身份验证并登录到 SMB 服务器。

  当域控制器关闭或网络问题导致 SMB 服务器无法联系域控制器时，本地用户可以使用 NTLM 身份验证向 SMB 服务器进行身份验证。

- 您希望将 *User Rights Management* 权限分配给本地用户。

  User Rights Management 是 SMB 服务器管理员控制用户和组对 SVM 拥有的权限的能力。您可以通过为用户的帐户分配权限或使用户成为具有这些权限的本地组的成员来为用户分配权限。

您可以出于以下原因创建一个或多个本地组：

- SMB 服务器位于工作组中，并且域组不可用。

  工作组配置不需要本地组，但它们对于管理本地工作组用户的访问权限非常有用。

- 您希望通过使用本地组进行共享和文件访问控制来控制对文件和文件夹资源的访问。
- 您希望使用自定义的 *User Rights Management* 权限创建本地组。

  某些内置用户组具有预定义的权限。要分配一组自定义权限，您可以创建一个本地组并为该组分配必要的权限。然后，您可以将本地用户，域用户和域组添加到本地组。

相关信息

本地用户身份验证的工作原理

支持的权限列表

本地用户身份验证的工作原理

本地用户必须先创建经过身份验证的会话，然后才能访问 CIFS 服务器上的数据。

由于 SMB 基于会话，因此首次设置会话时，只需确定一次用户身份即可。CIFS 服务器在对本地用户进行身份验证时使用基于 NTLM 的身份验证。支持 NTLMv1 和 NTLMv2 。

ONTAP 在三种使用情形下使用本地身份验证。每个用例取决于用户名的域部分（采用 domain\user 格式）是否与 CIFS 服务器的本地域名（ CIFS 服务器名称）匹配：

- 域部分匹配

请求访问数据时提供本地用户凭据的用户将在 CIFS 服务器上进行本地身份验证。

- 域部分不匹配

  ONTAP 尝试对 CIFS 服务器所属域中的域控制器使用 NTLM 身份验证。如果身份验证成功，则登录完成。如果失败，接下来会发生什么情况取决于身份验证失败的原因。

  例如，如果用户位于 Active Directory 中，但密码无效或已过期，则 ONTAP 不会尝试使用 CIFS 服务器上的相应本地用户帐户。相反，身份验证将失败。在其他情况下， ONTAP 会使用 CIFS 服务器上的相应本地帐户（如果存在）进行身份验证，即使 NetBIOS 域名不匹配也是如此。例如，如果存在匹配的域帐户，但该帐户已禁用，则 ONTAP 会使用 CIFS 服务器上的相应本地帐户进行身份验证。

- 未指定域部分

  ONTAP 首先尝试以本地用户身份进行身份验证。如果以本地用户身份进行身份验证失败，则 ONTAP 会使用 CIFS 服务器所属域中的域控制器对用户进行身份验证。

成功完成本地或域用户身份验证后， ONTAP 将根据本地组成员资格和权限构建完整的用户访问令牌。

有关本地用户的 NTLM 身份验证的详细信息，请参见 Microsoft Windows 文档。

相关信息

启用或禁用本地用户身份验证

如何构建用户访问令牌

当用户映射共享时，将建立经过身份验证的 SMB 会话，并构建用户访问令牌，其中包含有关用户，用户的组成员资格和累积权限以及映射的 UNIX 用户的信息。

除非禁用此功能，否则本地用户和组信息也会添加到用户访问令牌中。构建访问令牌的方式取决于登录用户是本地用户还是 Active Directory 域用户：

- 本地用户登录

  尽管本地用户可以是不同本地组的成员，但本地组不能是其他本地组的成员。本地用户访问令牌由分配给特定本地用户所属组的所有权限组成。

- 域用户登录

  域用户登录时， ONTAP 会获取一个用户访问令牌，该令牌包含用户所属的所有域组的用户 SID 和 SID 。ONTAP 使用域用户访问令牌与用户域组的本地成员资格（如果有）提供的访问令牌以及分配给域用户或其任何域组成员资格的任何直接权限进行联合。

对于本地和域用户登录，还会为用户访问令牌设置主组 RID 。默认RID `Domain Users` (里德513)。您不能更改默认值。

Windows 到 UNIX 和 UNIX 到 Windows 名称映射过程会对本地帐户和域帐户遵循相同的规则。

> 从 UNIX 用户到本地帐户没有隐含的自动映射。如果需要，必须使用现有名称映射命令指定显式映射规则。

在包含本地组的 **SVM** 上使用 **SnapMirror** 的准则

在包含本地组的 SVM 所拥有的卷上配置 SnapMirror 时，应了解相关准则。

您不能在应用于 SnapMirror 复制到另一个 SVM 的文件，目录或共享的 ACE 中使用本地组。如果您使用 SnapMirror 功能为另一个 SVM 上的卷创建 DR 镜像，并且该卷具有本地组的 ACE ，则 ACE 在该镜像上无效。如果将数据复制到其他 SVM ，则数据会有效地跨越到其他本地域。授予本地用户和组的权限仅在最初创建这些用户和组的 SVM 的范围内有效。

删除 **CIFS** 服务器时本地用户和组会发生什么情况

默认的本地用户和组集是在创建 CIFS 服务器时创建的，它们与托管 CIFS 服务器的 Storage Virtual Machine （ SVM ）相关联。SVM 管理员可以随时创建本地用户和组。您需要了解删除 CIFS 服务器时本地用户和组会发生什么情况。

本地用户和组与 SVM 关联；因此，出于安全考虑，删除 CIFS 服务器时不会删除它们。虽然删除 CIFS 服务器时不会删除本地用户和组，但它们是隐藏的。在 SVM 上重新创建 CIFS 服务器之前，您无法查看或管理本地用户和组。

> CIFS 服务器管理状态不会影响本地用户或组的可见性。

如何对本地用户和组使用 **Microsoft** 管理控制台

您可以从 Microsoft 管理控制台查看有关本地用户和组的信息。使用此版本的 ONTAP ，您无法从 Microsoft 管理控制台为本地用户和组执行其他管理任务。

还原准则

如果您计划将集群还原到不支持本地用户和组的 ONTAP 版本，并且正在使用本地用户和组管理文件访问或用户权限，则必须了解某些注意事项。

- 由于安全原因，在将 ONTAP 还原到不支持本地用户和组功能的版本时，不会删除有关已配置的本地用户，组和权限的信息。
- 还原到 ONTAP 的先前主要版本后， ONTAP 在身份验证和凭据创建期间不会使用本地用户和组。
- 不会从文件和文件夹 ACL 中删除本地用户和组。
- 如果文件访问请求取决于因向本地用户或组授予权限而授予的访问权限，则这些请求将被拒绝。

  要允许访问，您必须重新配置文件权限，以允许基于域对象而不是本地用户和组对象进行访问。

什么是本地权限

支持的权限列表

ONTAP 具有一组预定义的受支持权限。默认情况下，某些预定义的本地组已添加其中一些权限。此外，您还可以从预定义组添加或删除权限，或者创建新的本地用户或组，并向您

创建的组或现有域用户和组添加权限。

下表列出了 Storage Virtual Machine （ SVM ）上支持的权限，并列出了已分配权限的 BUILTIN 组：

权限名称	默认安全设置	Description
`SeTcbPrivilege`	无	作为操作系统的一部分
`SeBackupPrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	备份文件和目录，覆盖所有 ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	还原文件和目录，覆盖任何 ACL 会将任何有效的用户或组 SID 设置为文件所有者
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	获取文件或其他对象的所有权
`SeSecurityPrivilege`	`BUILTIN\Administrators`	管理审核 其中包括查看、转储和清除安全日志。
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`，`BUILTIN\Power Users`，`BUILTIN\Users`， `Everyone`	绕过遍历检查 具有此权限的用户无需具有遍历(x)权限即可遍历文件夹、符号链接或接合。

相关信息

- 分配本地权限
- 配置绕过遍历检查

分配权限

您可以直接为本地用户或域用户分配权限。或者，您也可以将用户分配给已分配权限与这些用户所需功能匹配的本地组。

- 您可以为创建的组分配一组权限。

  然后，将用户添加到具有所需权限的组。

- 您还可以将本地用户和域用户分配给默认权限与要授予这些用户的权限匹配的预定义组。

相关信息

- 向本地或域用户或组添加权限
- 从本地或域用户或组中删除权限
- 重置本地或域用户和组的权限

- 配置绕过遍历检查

使用 BUILTIN 组和本地管理员帐户的准则

使用 BUILTIN 组和本地管理员帐户时，应牢记一些特定准则。例如，您可以重命名本地管理员帐户，但不能删除此帐户。

- 管理员帐户可以重命名，但无法删除。
- 无法从 BUILTIN\Administrators 组中删除管理员帐户。
- BUILTIN 组可以重命名，但不能删除。

  重命名 BUILTIN 组后，可以使用已知名称创建另一个本地对象；但是，系统会为该对象分配一个新的 RID 。

- 没有本地来宾帐户。

相关信息

预定义的 BUILTIN 组和默认权限

本地用户密码的要求

默认情况下，本地用户密码必须满足复杂性要求。密码复杂度要求与 Microsoft Windows *local security policy* 中定义的要求类似。

密码必须满足以下条件：

- 长度必须至少为六个字符
- 不得包含用户帐户名称
- 必须包含以下四个类别中至少三个类别的字符：
  - 大写英文字符（A 到 Z）
  - 小写英文字符（a 到 z）
  - 基数为 10 位（0 到 9）
  - 特殊字符：

    ~@ # $ % { caret } & * _ - + = ` \ | () [ ] : ; " < > , .? /

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

更改本地用户帐户密码

预定义的 BUILTIN 组和默认权限

您可以将本地用户或域用户的成员资格分配给 ONTAP 提供的一组预定义的 BUILTIN 组。预定义的组已分配预定义的权限。

下表介绍了预定义的组：

预定义的 **BUILTIN** 组	默认权限
`BUILTIN\Administrators`第544次 首次创建时、本地 `Administrator` ID为500的帐户将自动成为此组的成员。Storage Virtual Machine (SVM)加入域后、 `domain\Domain Admins` 将组添加到组中。如果SVM离开域、则 `domain\Domain Admins` 组将从组中删除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`547 首次创建时，此组没有任何成员。此组的成员具有以下特征： • 可以创建和管理本地用户和组。 • 无法将自身或任何其他对象添加到中 `BUILTIN\Administrators` 组。	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`第551号 首次创建时，此组没有任何成员。如果出于备份目的打开文件或文件夹，则此组的成员可以覆盖对这些文件或文件夹的读写权限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`545 首次创建时、此组没有任何成员(除了隐含的 `Authenticated Users` 特殊组)。当SVM加入域时、 `domain\Domain Users` 已将组添加到此组。如果SVM离开域、则 `domain\Domain Users` 已从此组中删除组。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此组包括所有用户，包括来宾（但不包括匿名用户）。这是具有隐含成员资格的隐含组。	`SeChangeNotifyPrivilege`

相关信息

使用 BUILTIN 组和本地管理员帐户的准则

支持的权限列表

配置绕过遍历检查

启用或禁用本地用户和组功能

启用或禁用本地用户和组功能概述

在使用本地用户和组访问 NTFS 安全模式数据之前，必须启用本地用户和组功能。此外，如果要使用本地用户进行 SMB 身份验证，则必须启用本地用户身份验证功能。

默认情况下，本地用户和组功能以及本地用户身份验证处于启用状态。如果未启用它们，则必须先启用它们，然后才能配置和使用本地用户和组。您可以随时禁用本地用户和组功能。

除了显式禁用本地用户和组功能之外，如果集群中的任何节点还原到不支持本地用户和组功能的 ONTAP 版本，则 ONTAP 还会禁用此功能。只有当集群中的所有节点都运行支持本地用户和组功能的 ONTAP 版本时，才会启用此功能。

相关信息

修改本地用户帐户

修改本地组

向本地或域用户或组添加权限

启用或禁用本地用户和组

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用 SMB 访问的本地用户和组。默认情况下，本地用户和组功能处于启用状态。

关于此任务

您可以在配置 SMB 共享和 NTFS 文件权限时使用本地用户和组，也可以选择在创建 SMB 连接时使用本地用户进行身份验证。要使用本地用户进行身份验证，还必须启用本地用户和组身份验证选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

希望本地用户和组 ...	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户和组功能：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

相关信息

启用或禁用本地用户身份验证

启用或禁用本地用户帐户

启用或禁用本地用户身份验证

您可以为 Storage Virtual Machine （ SVM ）上的 SMB 访问启用或禁用本地用户身份验证。默认设置为允许本地用户身份验证，当 SVM 无法联系域控制器或您选择不使用域级别访问控制时，此功能非常有用。

开始之前

必须在 CIFS 服务器上启用本地用户和组功能。

关于此任务

您可以随时启用或禁用本地用户身份验证。如果要在创建 SMB 连接时使用本地用户进行身份验证，则还必须启用 CIFS 服务器的本地用户和组选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

本地身份验证的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`

本地身份验证的目标位置	输入命令 ...
已禁用	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户身份验证：

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

相关信息

本地用户身份验证的工作原理

启用或禁用本地用户和组

管理本地用户帐户

修改本地用户帐户

如果要更改现有用户的全名或问题描述，以及要启用或禁用用户帐户，则可以修改本地用户帐户。如果用户的名称受到影响或出于管理目的需要更改名称，您也可以重命名本地用户帐户。

如果您要 ...	输入命令 ...
修改本地用户的全名	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text` 如果全名包含空格、则必须使用双引号将其括起来。
修改本地用户的问题描述	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -description text` 如果问题描述包含空格、则必须使用双引号将其括起来。

如果您要 ...	输入命令 ...
启用或禁用本地用户帐户	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	重命名本地用户帐户

示例

以下示例将 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的本地用户 "`CIFS_SERVER\sue` " 重命名为 "`CIFS_SERVER\sue_new` "：

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

启用或禁用本地用户帐户

如果您希望用户能够通过 SMB 连接访问 Storage Virtual Machine （ SVM ）中包含的数据，则可以启用本地用户帐户。如果您不希望本地用户帐户通过 SMB 访问 SVM 数据，也可以禁用该用户帐户。

关于此任务

您可以通过修改用户帐户来启用本地用户。

步骤

1. 执行相应的操作：

如果您要 ...	输入命令 ...
启用用户帐户	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account -disabled false`
禁用用户帐户	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account -disabled true`

更改本地用户帐户密码

您可以更改本地用户的帐户密码。如果用户的密码受到影响或用户忘记了密码，则此功能非常有用。

步骤

1. 通过执行相应的操作更改密码： `vserver cifs users-and-groups local-user set-password -vserver *vserver_name* -user-name *user_name*`

示例

以下示例将为与 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 关联的本地用户 "`CIFS_SERVER\sue` " 设置密码：

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

显示有关本地用户的信息

您可以通过摘要形式显示所有本地用户的列表。如果要确定为特定用户配置了哪些帐户设置，则可以显示该用户的详细帐户信息以及多个用户的帐户信息。此信息可帮助您确定是否需要修改用户的设置，以及对身份验证或文件访问问题进行故障排除。

关于此任务

不会显示有关用户密码的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示有关 Storage Virtual Machine （ SVM ）上所有用户的信息	`vserver cifs users-and-groups local-user show -vserver *vserver_name*`
显示用户的详细帐户信息	`vserver cifs users-and-groups local-user show -instance -vserver *vserver_name* -user-name *user_name*`

运行命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地用户的信息：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

显示有关本地用户的组成员资格的信息

您可以显示有关本地用户所属的本地组的信息。您可以使用此信息来确定用户对文件和文件夹应具有的访问权限。此信息有助于确定用户应拥有哪些文件和文件夹访问权限，或者解决文件访问问题。

关于此任务

您可以自定义命令，使其仅显示要查看的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示指定本地用户的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
显示此本地用户所属本地组的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
显示与指定 Storage Virtual Machine （ SVM ）关联的本地用户的用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
显示指定 SVM 上所有本地用户的详细信息	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

示例

以下示例显示 SVM vs1 上所有本地用户的成员资格信息；用户 "`CIFS_SERVER\Administrator` " 是 "`BUILTIN\Administrators` " 组的成员， "`CIFS_SERVER\sue` " 是 "`CIFS_SERVER\G1` " 组的成员：

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

删除本地用户帐户

如果不再需要本地用户帐户对 CIFS 服务器进行本地 SMB 身份验证或确定对 SVM 中数据的访问权限，则可以从 Storage Virtual Machine （SVM）中删除这些帐户。

关于此任务

删除本地用户时，请记住以下几点：

- 文件系统未更改。

  不会调整引用此用户的文件和目录上的 Windows 安全描述符。

- 所有对本地用户的引用都将从成员资格和权限数据库中删除。
- 无法删除众所周知的标准用户，例如管理员。

步骤

1. 确定要删除的本地用户帐户的名称： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. 删除本地用户： `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. 验证是否已删除此用户帐户： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地用户 "`CIFS_SERVER\sue` "：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

管理本地组

修改本地组

您可以通过更改现有本地组的问题描述或重命名组来修改现有本地组。

如果您要 ...	使用命令 ...
修改本地组问题描述	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` 如果问题描述包含空格、则必须使用双引号将其括起来。
重命名本地组	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

示例

以下示例将本地组 "`CIFS_SERVER\engineering` " 重命名为 "`CIFS_SERVER\engineering_new` "：

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

以下示例修改本地组 "`CIFS_SERVER\engineering` " 的问题描述：

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

显示有关本地组的信息

您可以显示在集群或指定 Storage Virtual Machine （ SVM ）上配置的所有本地组的列表。在对 SVM 上所含数据的文件访问问题或 SVM 上的用户权限（特权）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

所需信息	输入命令 ...
集群上的所有本地组	`vserver cifs users-and-groups local-group show`
SVM 上的所有本地组	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地组的信息：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

管理本地组成员资格

您可以通过添加和删除本地或域用户，或者添加和删除域组来管理本地组成员资格。如果您希望根据放置在组上的访问控制来控制对数据的访问，或者您希望用户拥有与该组关联的权限，则此功能非常有用。

关于此任务

向本地组添加成员的准则：

- 您不能将用户添加到特殊的 _Everyone 组。
- 本地组必须存在，然后才能向其中添加用户。
- 用户必须存在，然后才能将其添加到本地组。
- 您不能将本地组添加到其他本地组。
- 要将域用户或组添加到本地组， Data ONTAP 必须能够将此名称解析为 SID 。

从本地组中删除成员的准则：

- 您不能从特殊的 _Everyone _ 组中删除成员。
- 要从中删除成员的组必须存在。
- ONTAP 必须能够将要从组中删除的成员的名称解析为相应的 SID 。

步骤

1. 添加或删除组中的成员。

如果您要 ...	然后使用命令 ...
将成员添加到组	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要添加到指定本地组的本地用户，域用户或域组的逗号分隔列表。
从组中删除成员	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要从指定本地组中删除的本地用户，域用户或域组的逗号分隔列表。

以下示例将本地用户 `SMB_SERVER\sue` 和域组`AD_DOM\DOM_eng` 添加到 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下示例将从 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中删除本地用户 `SMB_SERVER\sue` 和 `SMB_SERVER\James`：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

相关信息

显示有关本地组成员的信息

显示有关本地组成员的信息

您可以显示在集群或指定 Storage Virtual Machine （ SVM ）上配置的本地组的所有成员的列表。在对文件访问问题或用户权限（权限）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
集群上所有本地组的成员	`vserver cifs users-and-groups local-group show-members`
SVM 上所有本地组的成员	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

示例

以下示例显示了有关 SVM vs1 上所有本地组的成员的信息：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

删除本地组

如果不再需要本地组来确定与该 SVM 关联的数据的访问权限，或者不再需要将 SVM 用户权限（特权）分配给组成员，则可以从 Storage Virtual Machine （ SVM ）中删除该本地组。

关于此任务

删除本地组时，请记住以下几点：

- 文件系统未更改。

不会调整引用此组的文件和目录上的 Windows 安全描述符。

- 如果该组不存在，则会返回错误。
- 不能删除特殊的 _Everyone 组。
- 无法删除 *BUILTIN\Administrators _ _BUILTIN\Users* 等内置组。

步骤

1. 通过显示SVM上的本地组列表来确定要删除的本地组的名称： `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 删除本地组： `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 验证是否已删除此组： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地组 "`CIFS_SERVER\sales` "：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

更新本地数据库中的域用户和组名称

您可以将域用户和组添加到 CIFS 服务器的本地组。这些域对象会注册到集群上的本地数

据库中。如果重命名域对象，则必须手动更新本地数据库。

关于此任务

您必须指定要更新域名的 Storage Virtual Machine （ SVM ）的名称。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行相应的操作：

要更新域用户和组以及 ...	使用此命令 ...
显示成功更新和无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*
显示已成功更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only false`
仅显示无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only true`
禁止有关更新的所有状态信息	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress -all-output true`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将更新与 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 关联的域用户和组的名称。对于上次更新，需要更新一组依赖名称：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

管理本地权限

向本地或域用户或组添加权限

您可以通过添加权限来管理本地或域用户或组的用户权限。添加的权限将覆盖分配给其中任何对象的默认权限。这样可以自定义用户或组的权限，从而增强安全性。

开始之前

要添加权限的本地或域用户或组必须已存在。

关于此任务

向对象添加权限将覆盖该用户或组的默认权限。添加权限不会删除先前添加的权限。

在向本地或域用户或组添加权限时，必须牢记以下几点：

- 您可以添加一个或多个权限。
- 在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 向本地或域用户或组添加一个或多个权限： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 验证所需权限是否已应用于对象： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下示例将特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege` 添加到 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上的用户 "`CIFS_SERVER\sue` " 中：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

从本地或域用户或组中删除权限

您可以通过删除权限来管理本地或域用户或组的用户权限。这样可以自定义用户和组的最大权限，从而增强安全性。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从本地或域用户或组删除权限时，必须牢记以下几点：

- 您可以删除一个或多个权限。
- 从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 从本地或域用户或组中删除一个或多个权限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 验证是否已从对象中删除所需权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将从 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的用户 "`cifs_server\sue` " 中删除特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege`：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

重置本地或域用户和组的权限

您可以重置本地或域用户和组的权限。如果您已修改本地或域用户或组的权限，并且不再需要或需要这些修改，则此功能将非常有用。

关于此任务

重置本地或域用户或组的权限会删除该对象的任何权限条目。

步骤

1. 重置本地或域用户或组的权限： `vserver cifs users-and-groups privilege reset-privilege -vserver *vserver_name* -user-or-group-name *name*`
2. 验证是否已对此对象重置权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将重置 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上用户 "`CIFS_SERVER\sue` " 的权限。默认情况下，普通用户没有与其帐户关联的权限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

以下示例将重置组 "`BUILTIN\Administrators` " 的权限，从而有效地删除权限条目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

显示有关权限覆盖的信息

您可以显示有关分配给域或本地用户帐户或组的自定义权限的信息。此信息有助于确定是否应用了所需的用户权限。

步骤

1. 执行以下操作之一：

要显示的信息	输入此命令 ...
Storage Virtual Machine （SVM）上所有域和本地用户及组的自定义权限	`vserver cifs users-and-groups privilege show -vserver vserver_name`
SVM 上特定域或本地用户和组的自定义权限	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下命令显示与 SVM vs1 的本地或域用户和组明确关联的所有权限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```