ONTAP 如何使用本地用户和组

ONTAP 9

NetApp
September 12, 2024

目录

ONTAP 如何使用本地用户和组 . . . 1
本地用户和组概念 . . . 1
创建本地用户和本地组的原因 . . . 1
本地用户身份验证的工作原理 . . . 2
如何构建用户访问令牌 . . . 3
在包含本地组的 SVM 上使用 SnapMirror 的准则 . . . 4
删除 CIFS 服务器时本地用户和组会发生什么情况 . . . 4
如何对本地用户和组使用 Microsoft 管理控制台 . . . 4
还原准则 . . . 4

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。