



ONTAP如何处理**NFS**客户端身份验证

ONTAP 9

NetApp
April 24, 2024

目录

- ONTAP如何处理NFS客户端身份验证 1
 - ONTAP 如何处理 NFS 客户端身份验证概述 1
 - ONTAP 如何使用名称服务 1
 - ONTAP 如何从 NFS 客户端授予 SMB 文件访问权限..... 1
 - NFS 凭据缓存的工作原理..... 2

ONTAP如何处理NFS客户端身份验证

ONTAP 如何处理 NFS 客户端身份验证概述

NFS 客户端必须经过适当的身份验证，才能访问 SVM 上的数据。ONTAP 会根据您配置的名称服务检查客户端的 UNIX 凭据，从而对客户端进行身份验证。

当 NFS 客户端连接到 SVM 时，ONTAP 会根据 SVM 的名称服务配置检查不同的名称服务来获取用户的 UNIX 凭据。ONTAP 可以检查本地 UNIX 帐户，NIS 域和 LDAP 域的凭据。必须至少配置其中一个，ONTAP 才能成功对用户进行身份验证。您可以指定多个名称服务以及 ONTAP 搜索这些服务的顺序。

在采用 UNIX 卷安全模式的纯 NFS 环境中，此配置足以对从 NFS 客户端连接的用户进行身份验证并提供正确的文件访问权限。

如果您使用的是混合、NTFS或统一卷安全模式、则ONTAP必须获取UNIX用户的SMB用户名、以便通过Windows域控制器进行身份验证。这可以通过使用本地UNIX帐户或LDAP域映射单个用户来实现、也可以改用默认SMB用户来实现。您可以指定ONTAP搜索哪些名称服务的顺序、也可以指定默认SMB用户。

ONTAP 如何使用名称服务

ONTAP 使用名称服务获取有关用户和客户端的信息。ONTAP 使用此信息对访问存储系统上的数据或管理存储系统的用户进行身份验证，并在混合环境中映射用户凭据。

配置存储系统时，必须指定希望 ONTAP 用于获取用户凭据进行身份验证的名称服务。ONTAP 支持以下名称服务：

- 本地用户（文件）
- 外部 NIS 域（NIS）
- 外部 LDAP 域（LDAP）

您可以使用 `vserver services name-service ns-switch` 命令系列、用于为SVM配置源以搜索网络信息以及搜索顺序。这些命令提供与等效的功能 `/etc/nsswitch.conf` 文件。

当 NFS 客户端连接到 SVM 时，ONTAP 会检查指定的名称服务以获取用户的 UNIX 凭据。如果名称服务配置正确，并且 ONTAP 可以获取 UNIX 凭据，则 ONTAP 将成功对用户进行身份验证。

在具有混合安全模式的环境中，ONTAP 可能必须映射用户凭据。您必须为您的环境正确配置名称服务，以使 ONTAP 能够正确映射用户凭据。

ONTAP 还使用名称服务对 SVM 管理员帐户进行身份验证。在配置或修改名称服务切换时，必须牢记这一点，以免意外禁用 SVM 管理员帐户的身份验证。有关SVM管理用户的详细信息、请参见 ["管理员身份验证和RBAC"](#)。

ONTAP 如何从 NFS 客户端授予 SMB 文件访问权限

ONTAP 使用 Windows NT 文件系统（NTFS）安全语义来确定 NFS 客户端上的 UNIX 用户是否有权访问具有 NTFS 权限的文件。

为此，ONTAP 会将用户的 UNIX 用户 ID（UID）转换为 SMB 凭据，然后使用 SMB 凭据验证用户是否有权访问此文件。SMB 凭据由一个主安全标识符（SID）（通常是用户的 Windows 用户名）以及一个或多个与用户所属 Windows 组对应的组 SID 组成。

ONTAP 将 UNIX UID 转换为 SMB 凭据所需的时间可能从数十毫秒到数百毫秒不等，因为此过程涉及到与域控制器联系。ONTAP 会将 UID 映射到 SMB 凭据，并在凭据缓存中输入映射，以缩短转换所导致的验证时间。

NFS 凭据缓存的工作原理

当 NFS 用户请求访问存储系统上的 NFS 导出时，ONTAP 必须从外部名称服务器或本地文件检索用户凭据以对用户进行身份验证。然后，ONTAP 会将这些凭据存储在内部凭据缓存中，以供日后参考。了解 NFS 凭据缓存的工作原理有助于您处理潜在的性能和访问问题。

如果没有凭据缓存，ONTAP 将必须在 NFS 用户每次请求访问时查询名称服务。在许多用户访问的繁忙存储系统上，这可能会快速导致严重的性能问题，从而导致不必要的延迟，甚至拒绝 NFS 客户端访问。

通过凭据缓存，ONTAP 会检索用户凭据，然后将其存储一段预定的时间，以便在 NFS 客户端发送另一个请求时快速轻松地进行访问。此方法具有以下优势：

- 它可以减少对外部名称服务器（例如 NIS 或 LDAP）的请求，从而减轻存储系统的负载。
- 它可以减少向外部名称服务器发送的请求，从而减轻这些服务器的负载。
- 它可以在用户进行身份验证之前，消除从外部源获取凭据的等待时间，从而加快用户访问速度。

ONTAP 会将肯定和否定凭据存储在凭据缓存中。肯定凭据表示用户已通过身份验证并获得访问权限。否定凭据表示用户未通过身份验证，并被拒绝访问。

默认情况下，ONTAP 会将肯定凭据存储 24 小时；也就是说，在对用户进行初始身份验证后，ONTAP 会对该用户 24 小时内的任何访问请求使用缓存的凭据。如果用户在 24 小时后请求访问，则此周期将重新开始：ONTAP 丢弃缓存的凭据，并从相应的名称服务源再次获取凭据。如果名称服务器上的凭据在过去 24 小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来 24 小时使用。

默认情况下，ONTAP 会将否定凭据存储两个小时；也就是说，在最初拒绝用户访问后，ONTAP 会继续拒绝该用户的任何访问请求两个小时。如果用户在 2 小时后请求访问，则循环将重新开始：ONTAP 再次从相应的名称服务源获取凭据。如果名称服务器上的凭据在过去两小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来两小时使用。

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。