ONTAP 如何控制对文件的访问

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/nfs-admin/ontap-controls-access-files-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

ONTAP 如何控制对文件的访问 1
ONTAP 如何控制对文件的访问概述 1
基于身份验证的限制 1
基于文件的限制 1

ONTAP 如何控制对文件的访问

ONTAP 如何控制对文件的访问概述

ONTAP 会根据您指定的基于身份验证和基于文件的限制来控制对文件的访问。

当客户端连接到存储系统以访问文件时， ONTAP 必须执行两项任务：

- 身份验证

  ONTAP 必须通过使用可信源验证身份来对客户端进行身份验证。此外，客户端的身份验证类型是一种可用于确定客户端在配置导出策略时是否可以访问数据的方法（对于 CIFS 为可选）。

- Authorization

  ONTAP 必须通过将用户凭据与文件或目录上配置的权限进行比较并确定要提供的访问类型（如果有）来授权用户。

要正确管理文件访问控制， ONTAP 必须与 NIS ， LDAP 和 Active Directory 服务器等外部服务进行通信。要使用 CIFS 或 NFS 配置存储系统以进行文件访问，需要根据您在 ONTAP 中的环境设置相应的服务。

基于身份验证的限制

通过基于身份验证的限制，您可以指定哪些客户端计算机以及哪些用户可以连接到 Storage Virtual Machine （ SVM ）。

ONTAP 支持从 UNIX 和 Windows 服务器进行 Kerberos 身份验证。

基于文件的限制

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估三个安全级别后，访问权限由有效权限决定。

任何存储对象最多可包含三种类型的安全层：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

> 如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则不会看到存储级别访问防护安全性。即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别访问防护安全性。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

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。