



ONTAP 如何處理 NFS 用戶端驗證

ONTAP 9

NetApp
April 24, 2024

目錄

ONTAP 如何處理 NFS 用戶端驗證	1
如何處理NFS用戶端驗證總覽ONTAP	1
如何使用名稱服務ONTAP	1
如何使用此功能、從NFS用戶端授予SMB檔案存取權限ONTAP	1
NFS認證快取的運作方式	2

ONTAP 如何處理 NFS 用戶端驗證

如何處理NFS用戶端驗證總覽ONTAP

NFS用戶端必須經過適當驗證、才能存取SVM上的資料。利用您所設定的名稱服務來檢查UNIX認證、藉此驗證用戶端。ONTAP

當NFS用戶端連線至SVM時、ONTAP 根據SVM的名稱服務組態、透過檢查不同的名稱服務來取得使用者的UNIX認證。可檢查本機UNIX帳戶、NIS網域及LDAP網域的認證資料。ONTAP至少必須設定其中一項、ONTAP 才能讓支援中心成功驗證使用者。您可以指定多個名稱服務及ONTAP 其搜尋順序。

在純NFS環境中使用UNIX Volume安全性樣式、此組態足以驗證並為從NFS用戶端連線的使用者提供適當的檔案存取。

如果您使用混合、NTFS或統一磁碟區安全樣式、ONTAP 則必須為UNIX使用者取得SMB使用者名稱、才能使用Windows網域控制器進行驗證。這可能是因為使用本機UNIX帳戶或LDAP網域來對應個別使用者、或改用預設的SMB使用者。您可以指定ONTAP 名稱服務以何種順序搜尋、或指定預設的SMB使用者。

如何使用名稱服務ONTAP

使用名稱服務取得使用者和用戶端的相關資訊。ONTAP使用此資訊驗證使用者存取或管理儲存系統上的資料、並在混合式環境中對應使用者認證資料。ONTAP

當您設定儲存系統時、必須指定ONTAP 要使用哪些名稱服務來取得使用者認證以進行驗證。支援下列名稱服務：
ONTAP

- 本機使用者（檔案）
- 外部NIS網域（NIS）
- 外部 LDAP 網域（LDAP）

您可以使用 `vserver services name-service ns-switch` 命令系列可將 SVM 設定為使用來源來搜尋網路資訊、以及搜尋這些資訊的順序。這些命令可提供的等效功能 `/etc/nsswitch.conf` UNIX 系統上的檔案。

當NFS用戶端連線至SVM時、ONTAP 此功能會檢查指定的名稱服務、以取得使用者的UNIX認證資料。如果名稱服務設定正確、ONTAP 而且能夠取得UNIX認證資料、ONTAP 則無法成功驗證使用者。

在混合式安全型態的環境中ONTAP、可能必須對應使用者認證資料。您必須針對環境適當設定名稱服務、以便ONTAP 讓支援功能能夠正確對應使用者認證資料。

此外、還會使用名稱服務來驗證SVM系統管理員帳戶。ONTAP在設定或修改名稱服務交換器時、您必須謹記此點、以免意外停用SVM系統管理員帳戶的驗證。如需SVM管理使用者的詳細資訊、請參閱 ["系統管理員驗證與RBAC"](#)。

如何使用此功能、從NFS用戶端授予SMB檔案存取權限ONTAP

使用Windows NT檔案系統（NTFS）安全性語意、判斷UNIX使用者是否能在NFS用戶端上存取具有NTFS權限的檔案。ONTAP

為達成此目的、可將使用者的UNIX使用者ID (UID) 轉換成SMB認證、然後使用SMB認證來驗證使用者是否擁有檔案的存取權限。ONTAPSMB認證包含主要安全性識別碼 (SID)、通常是使用者的Windows使用者名稱、以及對應於使用者所屬Windows群組的一或多個群組SID。

將UNIX UID轉換為SMB認證所需的時間ONTAP 可從數十毫秒轉換為數百毫秒、因為此程序涉及連絡網域控制器。此功能可將UID對應至SMB認證、並在認證快取中輸入對應、以縮短轉換所造成的驗證時間。ONTAP

NFS認證快取的運作方式

當NFS使用者要求存取儲存系統上的NFS匯出時、ONTAP 必須從外部名稱伺服器或從本機檔案擷取使用者認證資料、才能驗證使用者。然後將這些認證資料儲存在內部認證快取中、以供日後參考。ONTAP瞭解NFS認證快取的運作方式、可讓您處理潛在的效能和存取問題。

如果沒有認證快取、ONTAP 每當NFS使用者要求存取時、就必須查詢名稱服務。在許多使用者存取的忙碌儲存系統上、這很快就會導致嚴重的效能問題、造成不必要的延遲、甚至使NFS用戶端存取遭到拒絕。

利用認證快取功能、ONTAP 當NFS用戶端傳送另一個要求時、將會擷取使用者認證資料、然後儲存預先決定的時間量、以便快速輕鬆地存取。此方法具有下列優點：

- 它可處理較少的外部名稱伺服器（例如NIS或LDAP）要求、進而減輕儲存系統的負載。
- 它能減少傳送要求給外部名稱伺服器的次數、進而減輕其負載。
- 它可免除從外部來源取得認證的等待時間、以便驗證使用者、進而加速使用者存取。

支援將正面和負面的認證資料儲存在認證快取中。ONTAP正向認證表示使用者已通過驗證並獲得存取權。負面認證表示使用者未通過驗證、因此被拒絕存取。

根據預設、ONTAP 將正向認證資料儲存24小時；也就是ONTAP 在初始驗證使用者之後、將快取認證資料用於該使用者24小時內的任何存取要求。如果使用者在24小時後要求存取、週期就會開始：ONTAP 由下列項目開始：循環捨棄快取的認證資料、並從適當的名稱服務來源再次取得認證資料。如果在過去24小時內、名稱伺服器上的認證有所變更、ONTAP 則會快取更新的認證資料、以供未來24小時使用。

根據預設、ONTAP 功能不正常的情況下、將負面認證資料儲存兩小時；也就是ONTAP 在一開始拒絕使用者存取之後、該使用者在兩小時內仍拒絕任何存取要求。如果使用者在2小時後要求存取、則週期將從下列項目開始：ONTAP 再次從適當的名稱服務來源取得認證。如果在過去兩小時內、名稱伺服器上的認證資料有所變更、ONTAP 則會快取更新的認證資料、以供未來兩小時使用。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。