



如何使用本機使用者和群組 **ONTAP** ONTAP 9

NetApp
February 12, 2026

目錄

如何使用本機使用者和群組ONTAP	1
了解本機 ONTAP SMB 使用者和群組	1
建立本機 ONTAP SMB 使用者和本機群組的原因	1
了解本機 ONTAP SMB 使用者身份驗證	2
了解 ONTAP SMB 使用者存取權令牌	3
了解如何在包含本機群組的 ONTAP SMB SVM 上使用 SnapMirror	4
了解刪除 ONTAP SMB 伺服器對使用者和群組的影響	4
了解如何將 Microsoft 管理主控台與本機 ONTAP SMB 使用者和群組結合使用	4
了解如何恢復 ONTAP SMB 叢集	4

如何使用本機使用者和群組ONTAP

了解本機 ONTAP SMB 使用者和群組

您應該先知道哪些是本機使用者和群組、以及這些使用者和群組的一些基本資訊、然後再決定是否要在環境中設定及使用本機使用者和群組。

- 本機使用者

具有唯一安全性識別碼 (SID) 的使用者帳戶、只有在建立該帳戶的儲存虛擬機器 (SVM) 上才具有可見度。本機使用者帳戶具有一組屬性、包括使用者名稱和SID。本機使用者帳戶會使用NTLM驗證、在CIFS伺服器上進行本機驗證。

使用者帳戶有多種用途：

- 用於授予_使用者權限管理_權限給使用者。
- 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機群組

具有唯一SID的群組只能在建立該群組的SVM上看到。群組包含一組成員。成員可以是本機使用者、網域使用者、網域群組和網域機器帳戶。可以建立、修改或刪除群組。

群組有多種用途：

- 用於授予_使用者權限管理_權限給其成員。
- 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機網域

具有本機範圍的網域、受SVM限制。本機網域名稱為CIFS伺服器名稱。本機使用者和群組包含在本機網域內。

- 安全性識別碼 (SID)

SID是可識別Windows型安全性主體的可變長度數值。例如、一般的SID格式如下：s-1-5-21-3136354847-3130905135-2517279418-123456。

- * NTLM驗證*

一種Microsoft Windows安全性方法、用於驗證CIFS伺服器上的使用者。

- 叢集複寫資料庫 (RDB)

叢集中每個節點上都有執行個體的複寫資料庫。本機使用者和群組物件會儲存在RDB中。

建立本機 ONTAP SMB 使用者和本機群組的原因

在您的儲存虛擬機器 (SVM) 上建立本機使用者和本機群組的理由有好幾種。例如、如果

網域控制器 (DC) 無法使用、您可能想要使用本機群組來指派權限、或SMB伺服器位於工作群組中、您可以使用本機使用者帳戶來存取SMB伺服器。

您可以基於下列理由建立一或多個本機使用者帳戶：

- 您的SMB伺服器位於工作群組中、網域使用者無法使用。

工作群組組態需要本機使用者。

- 如果網域控制器無法使用、您希望能夠驗證並登入SMB伺服器。

本機使用者可以在網域控制器當機或網路問題使SMB伺服器無法連絡網域控制器時、使用NTLM驗證來驗證SMB伺服器。

- 您想要指派_使用者權限管理_權限給本機使用者。

_使用者權限管理_是SMB伺服器管理員控制使用者和群組在SVM上擁有哪些權限的能力。您可以將權限指派給使用者帳戶、或是將使用者設為具有這些權限的本機群組成員、藉此指派權限給使用者。

您可以基於下列理由建立一或多個本機群組：

- 您的SMB伺服器位於工作群組中、而且網域群組無法使用。

工作群組組態不需要本機群組、但這些群組對於管理本機工作群組使用者的存取權限非常有用。

- 您想要使用本機群組來控制檔案和資料夾資源的存取、以進行共用和檔案存取控制。
- 您想要使用自訂的_使用者權限管理_權限來建立本機群組。

某些內建使用者群組具有預先定義的權限。若要指派一組自訂的權限、您可以建立本機群組、並將必要的權限指派給該群組。然後您可以將本機使用者、網域使用者和網域群組新增至本機群組。

相關資訊

- [了解本地用戶身份驗證](#)
- [支援的權限清單](#)

了解本機 ONTAP SMB 使用者身份驗證

本機使用者必須先建立已驗證的工作階段、才能存取CIFS伺服器上的資料。

由於SMB是以工作階段為基礎、因此在第一次設定工作階段時、只要確定一次使用者身分即可。CIFS伺服器在驗證本機使用者時、會使用以NTLM為基礎的驗證。支援「位在位在位在位在位」的「位在位

在三種使用案例下使用本機驗證。ONTAP每個使用案例取決於使用者名稱的網域部分（使用網域\使用者格式）是否符合CIFS伺服器的本機網域名稱（CIFS伺服器名稱）：

- 網域部分相符

在要求存取資料時提供本機使用者認證的使用者、會在CIFS伺服器本機驗證。

- 網域部分不符

嘗試在CIFS伺服器所屬網域中的網域控制器上使用NTLM驗證。ONTAP如果驗證成功、登入即告完成。如果驗證失敗、接下來的情況取決於驗證失敗的原因。

例如、如果使用者存在於Active Directory中、但密碼無效或過期、ONTAP 則無法嘗試在CIFS伺服器上使用對應的本機使用者帳戶。而是驗證失敗。有些情況ONTAP 下、即使有CIFS伺服器上的對應本機帳戶存在、也會使用該帳戶進行驗證、即使這些NetBios網域名稱不相符。例如、如果存在相符的網域帳戶、但該帳戶已停用、ONTAP 則會使用CIFS伺服器上對應的本機帳戶進行驗證。

- 未指定網域部分

以本機使用者身分先嘗試驗證。ONTAP如果本機使用者驗證失敗、ONTAP 則由CIFS伺服器所屬網域中的網域控制器來驗證使用者。

成功完成本機或網域使用者驗證後ONTAP、將會建構完整的使用者存取權杖、並將本機群組成員資格和權限納入考量。

如需本機使用者的NTLM驗證詳細資訊、請參閱Microsoft Windows文件。

相關資訊

[在伺服器上啟用或停用本機使用者身份驗證](#)

了解 ONTAP SMB 使用者存取權令牌

當使用者對應共用時、會建立已驗證的SMB工作階段、並建構使用者存取權杖、其中包含使用者、使用者群組成員資格和累積權限、以及對應的UNIX使用者的相關資訊。

除非停用此功能、否則本機使用者和群組資訊也會新增至使用者存取權杖。存取權杖的建構方式取決於登入是針對本機使用者還是Active Directory網域使用者：

- 本機使用者登入

雖然本機使用者可以是不同本機群組的成員、但本機群組不能是其他本機群組的成員。本機使用者存取權杖是由指派給特定本機使用者所屬群組的所有權限聯合所組成。

- 網域使用者登入

當網域使用者登入時ONTAP、即可取得使用者存取權杖、其中包含使用者所屬之所有網域群組的使用者ID和SID。使用網域使用者存取權杖的聯合、搭配使用者網域群組的本機成員資格（若有）所提供的存取權杖、以及指派給網域使用者或其任何網域群組成員資格的任何直接權限。ONTAP

對於本機和網域使用者登入、也會針對使用者存取權杖設定主要群組RID。預設 RID 為 Domain Users（RID 513）。您無法變更預設值。

Windows對UNIX和UNIX對Windows名稱對應程序、對本機和網域帳戶都遵循相同的規則。



從UNIX使用者到本機帳戶並無暗示的自動對應。如果需要、則必須使用現有的名稱對應命令來指定明確的對應規則。

了解如何在包含本機群組的 ONTAP SMB SVM 上使用 SnapMirror

在包含本機群組的SVM所擁有的磁碟區上設定SnapMirror時、您應該瞭解相關準則。

您無法使用應用到SnapMirror複寫到另一個SVM之檔案、目錄或共用的ACE中的本機群組。如果您使用SnapMirror功能在另一個SVM上建立磁碟區的DR鏡像、而該磁碟區有一個用於本機群組的ACE、則該ACE在鏡射上無效。如果將資料複寫到不同的SVM、資料就會有效地跨入不同的本機網域。授予本機使用者和群組的權限僅在最初建立的SVM範圍內有效。

了解刪除 ONTAP SMB 伺服器對使用者和群組的影響

預設的本機使用者和群組集是在建立CIFS伺服器時建立、並與託管CIFS伺服器的儲存虛擬機器（SVM）建立關聯。SVM管理員可以隨時建立本機使用者和群組。刪除CIFS伺服器時、您必須瞭解本機使用者和群組的情況。

本機使用者和群組與SVM相關聯、因此在刪除CIFS伺服器時、不會因為安全考量而刪除它們。雖然在刪除CIFS伺服器時不會刪除本機使用者和群組、但它們會隱藏起來。在SVM上重新建立CIFS伺服器之前、您無法檢視或管理本機使用者和群組。



CIFS伺服器管理狀態不會影響本機使用者或群組的可見度。

了解如何將 Microsoft 管理主控台與本機 ONTAP SMB 使用者和群組結合使用

您可以從Microsoft管理主控台檢視本機使用者和群組的相關資訊。有了這個版本ONTAP的功能、您就無法從Microsoft管理主控台為本機使用者和群組執行其他管理工作。

了解如何恢復 ONTAP SMB 叢集

如果您計畫將叢集還原至ONTAP 不支援本機使用者和群組的支援版本、以及本機使用者和群組用於管理檔案存取或使用者權限、則必須注意某些考量。

- 基於安全考量、當ONTAP 將設定的本機使用者、群組和權限資訊還原至不支援本機使用者和群組功能的版本時、不會刪除這些資訊。
- 還原至ONTAP 舊版的主要版本時ONTAP 、在驗證和認證建立期間、不使用本地使用者和群組。
- 本機使用者和群組不會從檔案和資料夾ACL中移除。
- 由於授予本機使用者或群組權限、因此會拒絕視存取權限而定的檔案存取要求。

若要允許存取、您必須重新設定檔案權限、以根據網域物件而非本機使用者和群組物件來允許存取。

版權資訊

Copyright © 2026 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 保留隨時變更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。