



# 設定安全樣式 ONTAP 9

NetApp  
April 24, 2024

# 目錄

- 設定安全樣式 ..... 1
  - 安全樣式如何影響資料存取 ..... 1
  - 在SVM根磁碟區上設定安全樣式 ..... 3
  - 在FlexVol 功能區上設定安全樣式 ..... 4
  - 在qtree上設定安全性樣式 ..... 4

# 設定安全樣式

## 安全樣式如何影響資料存取

### 安全樣式及其影響為何

共有四種不同的安全型態：UNIX、NTFS、混合式及統一化。每種安全樣式對資料權限的處理方式都有不同的影響。您必須瞭解不同的影響、以確保為您的目的選擇適當的安全型態。

請務必瞭解、安全樣式並未決定哪些用戶端類型可以或無法存取資料。安全樣式只會決定ONTAP 用來控制資料存取的權限類型、以及哪些用戶端類型可以修改這些權限。

例如、如果某個磁碟區使用UNIX安全型態、則SMB用戶端仍可存取資料（前提是他們必須正確驗證及授權）、因為ONTAP 此為多重傳輸協定的本質。不過ONTAP 、VMware使用UNIX權限、只有UNIX用戶端可以使用原生工具進行修改。

安全風格	可以修改權限的用戶端	用戶端可以使用的權限	打造出有效的安全風格	可存取檔案的用戶端
UNIX	NFS	NFSv3模式位元 NFSv4.x ACL	UNIX	NFS與SMB
NTFS	中小企業	NTFS ACL	NTFS	
混合	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.ACL		
		NTFS ACL	NTFS	
統一化（僅適用於Infinite Volume、ONTAP 9.4 及更早版本。）	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

支援UNIX、NTFS和混合式安全型態的支援。FlexVol當安全性樣式混合或統一化時、有效權限取決於上次修改權限的用戶端類型、因為使用者是個別設定安全性樣式。如果上次修改權限的用戶端是NFSv3用戶端、則權限為UNIX NFSv3模式位元。如果最後一個用戶端是NFSv4用戶端、則權限為NFSv4 ACL。如果最後一個用戶端是SMB用戶端、則權限為Windows NTFS ACL。

統一化的安全風格僅適用於無限個Volume、ONTAP 而不再支援於更新版本的版本。如需詳細資訊、請參閱 [介紹Volume管理總覽FlexGroup](#)。

從 ONTAP 9.2 開始 `show-effective-permissions` 的參數 `vserver security file-directory` 命令可讓您在指定的檔案或資料夾路徑上顯示授予 Windows 或 UNIX 使用者的有效權限。此外、選用參數 `-share -name` 可讓您顯示有效共用權限。



最初設定部分預設檔案權限。ONTAP根據預設、UNIX、混合式及統一化安全樣式磁碟區中所有資料的有效安全樣式為UNIX、有效權限類型為UNIX模式位元（0755、除非另有說明）、直到用戶端依照預設安全性樣式所允許的方式進行設定為止。根據預設、NTFS安全型磁碟區中所有資料的有效安全樣式為NTFS、並具有ACL、可讓所有人完全掌控。

## 設定安全樣式的位置與時機

安全樣式可在FlexVol 支援樹狀結構（根或資料磁碟區）和qtree上設定。安全樣式可在建立時手動設定、自動繼承或稍後變更。

### 決定要在**SVM**上使用哪種安全型態

為了協助您決定要在磁碟區上使用哪種安全樣式、您應該考慮兩個因素。主要因素是管理檔案系統的系統管理員類型。次要因素是存取磁碟區上資料的使用者或服務類型。

在Volume上設定安全樣式時、您應該考慮環境的需求、以確保您選擇最佳的安全樣式、並避免管理權限時發生問題。下列考量事項可協助您決定：

安全風格	選擇是否...
UNIX	<ul style="list-style-type: none"><li>• 檔案系統由UNIX管理員管理。</li><li>• 大多數使用者是NFS用戶端。</li><li>• 存取資料的應用程式會使用UNIX使用者做為服務帳戶。</li></ul>
NTFS	<ul style="list-style-type: none"><li>• 檔案系統由Windows管理員管理。</li><li>• 大多數使用者是 SMB 用戶端。</li><li>• 存取資料的應用程式會使用Windows使用者做為服務帳戶。</li></ul>
混合	<ul style="list-style-type: none"><li>• 檔案系統由UNIX和Windows系統管理員管理、使用者同時由NFS和SMB用戶端組成。</li></ul>

### 安全樣式繼承的運作方式

如果您在建立新FlexVol 的流通量或qtree時未指定安全樣式、它會以不同的方式繼承其安全風格。

安全樣式會以下列方式繼承：

- 此功能會繼承包含SVM的根磁碟區安全樣式。FlexVol
- qtree會繼承其包含FlexVol 的不穩定區的安全樣式。
- 檔案或目錄會繼承其包含FlexVol 的不穩定磁碟區或qtree的安全樣式。

### 如何保留**UNIX**權限**ONTAP**

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

## 使用Windows安全性索引標籤管理UNIX權限

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。

## 在SVM根磁碟區上設定安全樣式

您可以設定儲存虛擬機器（SVM）根磁碟區安全樣式、以決定SVM根磁碟區上資料所使用的權限類型。

### 步驟

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 定義安全樣式的參數。

根 Volume 安全樣式的可能選項為 `unix`、`ntfs` 或 `mixed`。

2. 顯示並驗證組態、包括您所建立SVM的根磁碟區安全樣式：

```
vserver show -vserver vserver_name
```

## 在FlexVol 功能區上設定安全樣式

您可以設定FlexVol 「靜態Volume」安全樣式、以判斷FlexVol 儲存虛擬機器（SVM）的各個版本上的資料所使用的權限類型。

### 步驟

1. 執行下列其中一項動作：

如果FlexVol 是這個問題...	使用命令...
尚不存在	<code>volume create</code> 並包含 <code>-security-style</code> 指定安全樣式的參數。
已存在	<code>volume modify</code> 並包含 <code>-security-style</code> 指定安全樣式的參數。

FlexVol Volume 安全樣式的可能選項為 `unix`、`ntfs` 或 `mixed`。

如果您在建立FlexVol 一個穩定區時未指定安全樣式、則此磁碟區會繼承根磁碟區的安全樣式。

如需更多關於的資訊、請參閱 `volume create` 或 `volume modify` 命令、請參閱 ["邏輯儲存管理"](#)。

2. 若要顯示組態、包括FlexVol 您所建立的穩定功能、請輸入下列命令：

```
volume show -volume volume_name -instance
```

## 在qtree上設定安全性樣式

您可以設定qtree Volume安全樣式、以決定用於qtree上資料的權限類型。

### 步驟

1. 執行下列其中一項動作：

如果qtree ...	使用命令...
尚未存在	<code>volume qtree create</code> 並包含 <code>-security-style</code> 指定安全樣式的參數。
已存在	<code>volume qtree modify</code> 並包含 <code>-security-style</code> 指定安全樣式的參數。

qtree 安全樣式的可能選項為 `unix`、`ntfs` 或 `mixed`。

如果在建立 qtree 時未指定安全樣式、則預設的安全樣式為 `mixed`。

如需更多關於的資訊、請參閱 `volume qtree create` 或 `volume qtree modify` 命令、請參閱 ["邏輯儲存管理"](#)。

2. 若要顯示組態、包括您建立的 qtree 安全樣式、請輸入下列命令：`volume qtree show -qtree`

*qtree\_name* -instance

## 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。