



使用檔案權限來保護檔案存取安全 ONTAP 9

NetApp
November 27, 2024

目錄

使用檔案權限來保護檔案存取安全	1
使用Windows安全性索引標籤設定進階NTFS檔案權限	1
使用ONTAP CLI設定NTFS檔案權限	3
UNIX檔案權限如何在透過SMB存取檔案時提供存取控制	4

使用檔案權限來保護檔案存取安全

使用Windows安全性索引標籤設定進階NTFS檔案權限

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、設定檔案和資料夾的標準NTFS檔案權限。

開始之前

執行此工作的系統管理員必須擁有足夠的NTFS權限、才能變更所選物件的權限。

關於這項工作

在Windows主機上設定NTFS檔案權限的方法是將項目新增至NTFS安全性描述元相關聯的NTFS判別存取控制清單 (DACL)。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。

2. 完成*對應網路磁碟機*對話方塊：

a. 選取*磁碟機*字母。

b. 在「資料夾」方塊中、輸入CIFS伺服器名稱、其中包含您要套用權限的資料及共用名稱。

如果您的 CIFS 伺服器名稱為「CIFS 伺服器」、且您的共用名稱為「shahre1」、則應輸入
\\CIFS_SERVER\share1。



您可以指定CIFS伺服器的資料介面IP位址、而非CIFS伺服器名稱。

c. 單擊*完成*。

您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要設定NTFS檔案權限的檔案或目錄。

4. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。

5. 選取*安全性*索引標籤。

「安全性」標籤會顯示已設定NTFS權限的使用者和群組清單。「權限」方塊會針對每個選取的使用者或群組、顯示有效的「允許」和「拒絕」權限清單。

6. 按一下*進階*。

「Windows內容」視窗會顯示指派給使用者和群組之現有檔案權限的相關資訊。

7. 按一下*變更權限*。

「權限」視窗隨即開啟。

8. 執行所需的動作：

如果您想要...	請執行下列動作...
設定新使用者或群組的進階NTFS權限	a. 按一下「* 新增 *」。 b. 在*輸入要選取的物件名稱*方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。
變更使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要變更其進階權限的使用者或群組。 b. 按一下 * 編輯 * 。
移除使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 跳至步驟13。

如果您要在新使用者或群組上新增進階NTFS權限、或是變更現有使用者或群組的NTFS進階權限、就會開啟「<Object>的權限項目」方塊。

9. 在「套用至」方塊中、選取您要套用此NTFS檔案權限項目的方式。

如果您要在單一檔案上設定NTFS檔案權限、則「套用至」方塊不會作用。「套用至」設定預設為*僅此物件*。

10. 在「權限」方塊中、針對您要在此物件上設定的進階權限、選取「允許」或「拒絕」方塊。

- 若要允許指定的存取權、請選取*允許*方塊。
- 若要不允許指定的存取、請選取* Deny (拒絕) *方塊。您可以設定下列進階權限的權限：
- 完全控制

如果您選擇此進階權限、則會自動選擇所有其他進階權限（允許或拒絕權限）。

- 周遊資料夾/執行檔案
- 列出資料夾/讀取資料
- 讀取屬性
- 讀取延伸屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入延伸屬性
- 刪除子資料夾與檔案
- 刪除

- 讀取權限
- 變更權限
- 取得所有權



如果任何進階權限方塊無法選取、這是因為權限是從父物件繼承而來。

11. 如果您希望此物件的子資料夾和檔案繼承這些權限、請選取「僅將這些權限套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「確定」。
13. 完成新增、移除或編輯NTFS權限之後、請指定此物件的繼承設定：

- 選取「包含此物件父項的可繼承權限」方塊。

這是預設值。

- 選取「使用此物件的可繼承權限來取代所有子物件權限」方塊。

如果您要在單一檔案上設定NTFS檔案權限、則此設定不會出現在「權限」方塊中。



選取此設定時請務必謹慎。此設定會移除所有子物件上的所有現有權限、並以此物件的權限設定取代這些權限。您可能不小心移除不想移除的權限。在混合式安全型磁碟區或qtree中設定權限時尤其重要。如果子物件具有UNIX有效的安全樣式、將NTFS權限傳播到這些子物件會ONTAP 導致將這些物件從UNIX安全樣式變更為NTFS安全樣式、而這些子物件上的所有UNIX權限都會以NTFS權限取代。

- 選取兩個方塊。
- 請選取兩個方塊。

14. 按一下「確定」以關閉「權限」方塊。
15. 按一下「確定」以關閉「進階安全性設定<Object>」方塊。

如需如何設定進階NTFS權限的詳細資訊、請參閱Windows文件。

相關資訊

[使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性](#)

[在NTFS安全型磁碟區上顯示檔案安全性的相關資訊](#)

[在混合式安全型磁碟區上顯示檔案安全性的相關資訊](#)

[顯示UNIX安全型磁碟區上的檔案安全資訊](#)

使用ONTAP CLI設定NTFS檔案權限

您可以使用ONTAP CLI在檔案和目錄上設定NTFS檔案權限。這可讓您設定NTFS檔案權限、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以將項目新增至與NTFS安全性描述元相關聯的NTFS判別存取控制清單 (DACL) 、以設定NTFS檔案權限。然後將安全性描述元套用至NTFS檔案和目錄。

您只能使用命令列設定NTFS檔案權限。您無法使用CLI來設定NFSv4 ACL。

步驟

1. 建立NTFS安全性描述元。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. 將DACL新增至NTFS安全性描述元。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. 建立檔案/目錄安全性原則。

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

UNIX檔案權限如何在透過SMB存取檔案時提供存取控制

一個包含以下三種類型的安全型態之一：NTFS、UNIX或混合式。FlexVol無論安全風格為何、您都可以透過SMB存取資料、不過需要適當的UNIX檔案權限、才能以UNIX有效的安全性存取資料。

當透過SMB存取資料時、在判斷使用者是否有權執行要求的動作時、會使用數種存取控制：

- 匯出權限

設定SMB存取的匯出權限為選用項目。

- 共用權限
- 檔案權限

下列類型的檔案權限可能會套用至使用者想要執行動作的資料：

- NTFS
- UNIX NFSv4 ACL
- UNIX模式位元

對於已設定NFSv4 ACL或UNIX模式位元的資料、會使用UNIX樣式權限來決定資料的檔案存取權限。SVM管理員需要設定適當的檔案權限、以確保使用者擁有執行所需動作的權限。



混合式安全型磁碟區中的資料可能具有NTFS或UNIX有效的安全風格。如果資料具有UNIX有效的安全樣式、則在決定資料的檔案存取權限時、會使用NFSv4權限或UNIX模式位元。

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。