使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/smb-admin/create-ntfs-security-descriptor-file-task.html on April 20, 2024. Always check docs.netapp.com for the latest.

目錄

使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性 1
建立NTFS安全性描述元 1
將 NTFS DACL 存取控制項目新增至 NTFS 安全性描述元 1
建立安全性原則 2
新增工作至安全性原則 3
套用安全性原則 5
監控安全性原則工作 5
驗證套用的檔案安全性 6

使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性

建立NTFS安全性描述元

建立NTFS安全性描述元（檔案安全性原則）是設定NTFS存取控制清單（ACL）並套用至儲存虛擬機器（SVM）內的檔案和資料夾的第一步。您可以將安全性描述元與原則工作中的檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

將 NTFS DACL 存取控制項目新增至 NTFS 安全性描述元

將DACL（判別存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是設定及套用NTFS ACL至檔案或資料夾的第二步驟。每個項目都會識別允許或拒絕存取的物件、並定義物件可以或無法對ACE中定義的檔案或資料夾執行的操作。

關於這項工作

您可以將一或多個 ACE 新增至安全性描述元的 DACL 。

如果安全性描述元包含具有現有 ACE 的 DACL 、則命令會將新的 ACE 新增至 DACL 。如果安全性描述元不包含DACL、則命令會建立DACL並新增新的ACE。

您可以選擇自訂 DACL 項目、方法是指定要允許或拒絕中指定之帳戶的權限 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

> 如果您未指定 DACL 項目的權限、則預設會將權限設定為 `Full Control`。

您可以指定如何套用繼承、以選擇性地自訂DACL項目。

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 將 DACL 項目新增至安全性描述元：`vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   `vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny -account domain\joe -rights full-control -apply-to this-folder -vserver vs1`

2. 驗證 DACL 項目是否正確：`vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   `vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                    Vserver: vs1
          Security Descriptor Name: sd1
                     Allow or Deny: deny
               Account Name or SID: DOMAIN\joe
                     Access Rights: full-control
            Advanced Access Rights: -
                          Apply To: this-folder
                     Access Rights: full-control
```

建立安全性原則

為SVM建立檔案安全性原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個SVM建立關聯（包含NTFS安全型磁碟區或混合式安全型磁碟區）。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

新增工作至安全性原則

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。

- 原則可以包含一或多個工作。

  即使原則可以包含多項工作、您也無法將原則設定為同時包含檔案目錄和儲存層級的存取保護工作。原則必須包含所有儲存層級的存取保護工作或所有檔案目錄工作。

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

將工作新增至安全性原則時、您必須指定下列四個必要參數：

- SVM名稱
- 原則名稱
- 路徑
- 與路徑相關聯的安全性描述元

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式
- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 將具有相關安全性描述元的工作新增至安全性原則： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

套用安全性原則

將檔案安全性原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後步驟。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

> 套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則：`vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

監控安全性原則工作

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                  Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

驗證套用的檔案安全性

您可以驗證檔案安全性設定、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的設定。

關於這項工作

您必須提供SVM名稱、其中包含資料、以及您要驗證安全性設定之檔案和資料夾的路徑。您可以使用選用的 `-expand-mask` 顯示安全性設定詳細資訊的參數。

步驟

1. 顯示檔案和資料夾安全性設定： `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
         Vserver: vs1
               File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
```

```
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
                             .... .... .... .... .... ...1 .... .... =
```

```
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
Write Owner
                            .... .... .... .0.. .... .... .... .... =
Write DAC
                            .... .... .... ..0. .... .... .... .... =
Read Control
                            .... .... .... ...0 .... .... .... .... =
Delete
                            .... .... .... .... .... ...0 .... .... =
Write Attributes
                            .... .... .... .... .... .... 0... .... =
Read Attributes
                            .... .... .... .... .... .... .0.. .... =
Delete Child
                            .... .... .... .... .... .... ..0. .... =
```

```
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

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。