



顯示套用至檔案和目錄的稽核原則相關資訊 ONTAP 9

NetApp
April 24, 2024

目錄

顯示套用至檔案和目錄的稽核原則相關資訊	1
使用Windows安全性索引標籤顯示稽核原則的相關資訊	1
使用FlexVol CLI在整個過程中顯示有關NTFS稽核原則的資訊	2
顯示檔案安全性與稽核原則相關資訊的方法	4

顯示套用至檔案和目錄的稽核原則相關資訊

使用Windows安全性索引標籤顯示稽核原則的相關資訊

您可以使用「Windows內容」視窗中的「安全性」索引標籤、顯示已套用至檔案和目錄的稽核原則相關資訊。這種方法與存放在Windows伺服器上的資料相同、可讓客戶使用慣用的GUI介面。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

若要顯示已套用至NTFS檔案和資料夾的SACL相關資訊、請在Windows主機上完成下列步驟。

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、輸入儲存虛擬機器（SVM）的IP位址或SMB伺服器名稱、其中包含要稽核的資料及共用名稱。

如果您的 SMB 伺服器名稱為「ShMB_Server」、而您的共用名稱為「shahre1」、則您應該輸入 \\SMB_SERVER\share1。



您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 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. 選取您要顯示稽核資訊的檔案或目錄。
4. 在檔案或目錄上按一下滑鼠右鍵、然後選取*內容*。
5. 選取*安全性*索引標籤。
6. 按一下*進階*。
7. 選取*稽核*索引標籤。
8. 按一下 * 繼續 *。

稽核方塊隨即開啟。「稽核項目」方塊會顯示套用SACL的使用者和群組摘要。

9. 在「稽核項目」方塊中、選取您要顯示其SACL項目的使用者或群組。
10. 按一下 * 編輯 *。

隨即開啟<object>的稽核項目方塊。

11. 在「存取」方塊中、檢視套用至所選物件的目前SACL。
12. 按一下*取消*以關閉*稽核項目*方塊。
13. 單擊*取消*關閉*稽核*方塊。

使用FlexVol CLI在整個過程中顯示有關NTFS稽核原則的資訊

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用這些資訊來驗證安全性組態或疑難排解稽核問題。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（如果已針對指定的檔案或目錄路徑設定動態存取控制）。
- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	<code>vserver security file-directory show -vserver vserver_name -path path</code>

詳細清單

```
vserver security file-directory show -vserver  
vserver_name -path path -expand-mask true
```

範例

下列範例顯示路徑的稽核原則資訊 /corp 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp  
      Vserver: vs1  
      File Path: /corp  
      File Inode Number: 357  
      Security Style: ntfs  
      Effective Style: ntfs  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
      Unix User Id: 0  
      Unix Group Id: 0  
      Unix Mode Bits: 777  
      Unix Mode Bits in Text: rwxrwxrwx  
      ACLs: NTFS Security Descriptor  
      Control:0x8014  
      Owner:DOMAIN\Administrator  
      Group:BUILTIN\Administrators  
      SACL - ACEs  
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA  
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA  
      DACL - ACEs  
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI  
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI  
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI  
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 /datavol1 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

```

cluster::> vsriver security file-directory show -vsriver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

顯示檔案安全性與稽核原則相關資訊的方法

您可以使用萬用字元 (*) 來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽

核原則相關資訊。

萬用字元 (*) 可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。

如果您想要顯示名為「*」的特定檔案或目錄資訊、則必須在雙引號 (「」) 內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 /1/ SVM VS1 ：

```
cluster::> vsserver security file-directory show -vsserver vs1 -path /1/*
```

```

        Vserver: vs1
        File Path: /1/1
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8514
              Owner: BUILTIN\Administrators
              Group: BUILTIN\Administrators
              DACL - ACEs
              ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

        Vserver: vs1
        File Path: /1/1/abc
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8404
              Owner: BUILTIN\Administrators
              Group: BUILTIN\Administrators
              DACL - ACEs
              ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「*」的檔案資訊 /vol1/a SVM VS1 的路徑會以雙引號 (") 括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
            Unix User Id: 1002  
            Unix Group Id: 65533  
            Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
            Control:0x8014  
            SACL - ACEs  
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
            DACL - ACEs  
                ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                ALLOW-OWNER@-0x1f01ff-FI|DI  
                ALLOW-GROUP@-0x1200a9-IG
```


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。