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

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	`vserver security file-directory show -vserver vserver_name -path path`

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::> vserver security file-directory show -vserver 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::> vserver security file-directory show -vserver 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
```