



使用儲存層級存取保護來保護檔案存取安全 ONTAP 9

NetApp
March 11, 2024

目錄

使用儲存層級存取保護來保護檔案存取安全	1
使用儲存層級存取保護來保護檔案存取安全	1
使用儲存層級存取保護的使用案例	2
設定儲存層級存取保護的工作流程	2
設定儲存層級存取保護	4
有效的熔渣對照表	9
顯示儲存層級存取保護的相關資訊	9
移除儲存層級的存取保護	12

使用儲存層級存取保護來保護檔案存取安全

使用儲存層級存取保護來保護檔案存取安全

除了使用原生檔案層級來保護存取安全、以及匯出及共用安全性、您也可以設定儲存層級的存取保護、ONTAP 這是由流通量層級的第三層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取套用到儲存物件的存取。

僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

儲存層級存取保護行為

- 儲存層級的存取保護適用於儲存物件中的所有檔案或目錄。

由於某個Volume中的所有檔案或目錄都受限於儲存層級的存取保護設定、因此不需要透過傳播進行繼承。

- 您可以設定儲存層級的存取保護、使其僅套用至檔案、僅套用至目錄、或同時套用至磁碟區內的檔案和目錄。

- 檔案與目錄安全性

適用於儲存物件內的每個目錄和檔案。這是預設設定。

- 檔案安全性

適用於儲存物件內的每個檔案。套用此安全性不會影響目錄的存取或稽核。

- 目錄安全性

適用於儲存物件內的每個目錄。套用此安全性不會影響檔案的存取或稽核。

- 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。

- 如果您從NFS或SMB用戶端檢視檔案或目錄的安全性設定、就不會看到儲存層級的存取保護安全性。

它會套用至儲存物件層級、並儲存在用於判斷有效權限的中繼資料中。

- 即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的安全性。

它的設計僅供儲存管理員修改。

- 您可以將儲存層級的存取保護套用至NTFS或混合式安全型態的磁碟區。

- 只要包含該磁碟區的SVM已設定CIFS伺服器、您就可以將儲存層級的存取保護套用至具有UNIX安全樣式的磁碟區。

- 當磁碟區掛載於磁碟區交會路徑下、且該路徑上有儲存層級存取保護、則不會將其傳播至其下掛載的磁碟區。

- 儲存層級的存取保護安全性描述元會透過SnapMirror資料複寫和SVM複寫來複寫。
- 病毒掃描程式有特殊的分配。

即使儲存層級的存取保護拒絕存取物件、這些伺服器仍可享受特殊存取權限來篩選檔案和目錄。

- 如果因為儲存層級存取保護而拒絕存取、則不會傳送FPolicy通知。

存取檢查順序

檔案或目錄的存取權取決於匯出或共用權限、在磁碟區上設定的儲存層級存取保護權限、以及套用至檔案和/或目錄的原生檔案權限的組合效應。評估所有層級的安全性、以判斷檔案或目錄具有哪些有效權限。安全性存取檢查的執行順序如下：

1. SMB共用區或NFS匯出層級權限
2. 儲存層級存取保護
3. NTFS檔案/資料夾存取控制清單 (ACL)、NFSv4 ACL或UNIX模式位元

使用儲存層級存取保護的使用案例

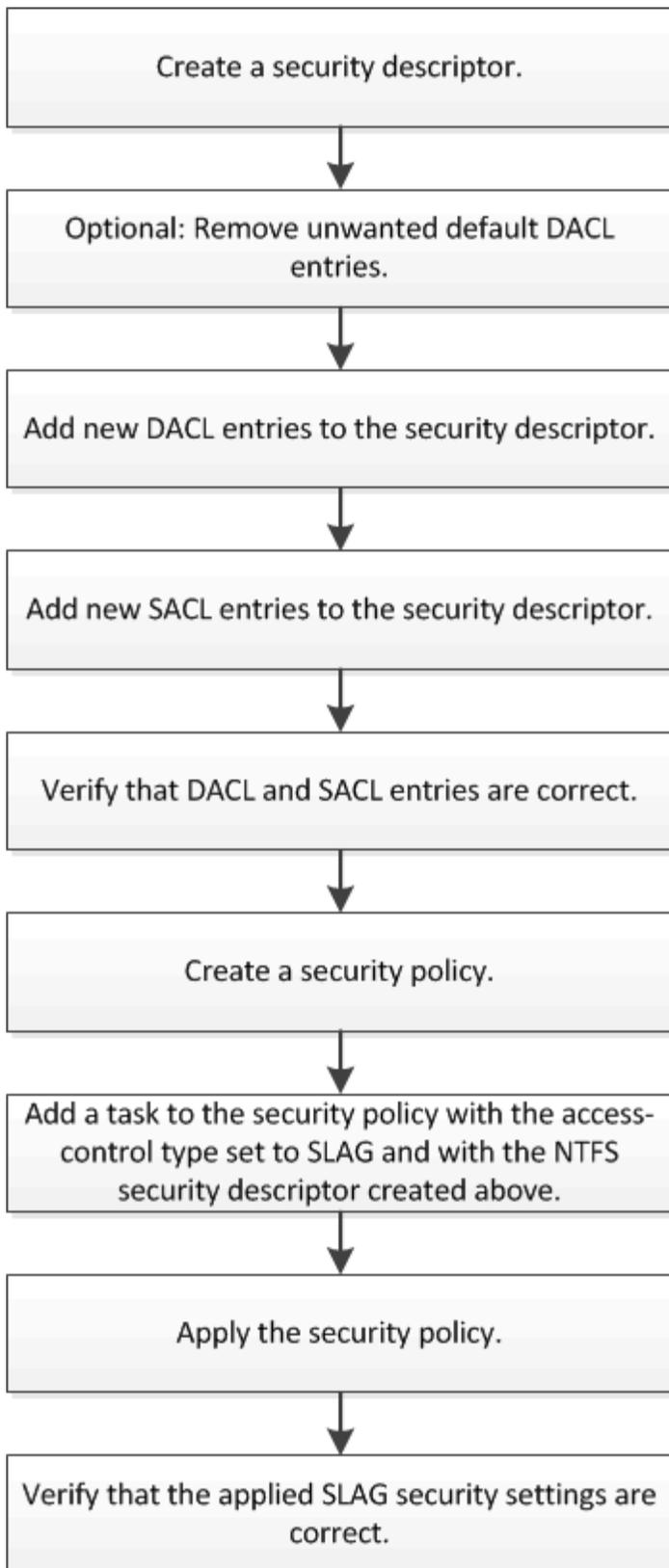
儲存層級的存取保護功能可在儲存層級提供額外的安全性、從用戶端看不到；因此、任何使用者或系統管理員都無法從其桌面撤銷。在某些使用案例中、在儲存層級控制存取的能力是有益的。

此功能的一般使用案例包括下列案例：

- 透過稽核及控制所有使用者在儲存層級的存取、來保護智慧財產
- 金融服務公司（包括銀行和交易集團）的儲存設備
- 為個別部門提供具有獨立檔案儲存設備的政府服務
- 大學保護所有學生檔案

設定儲存層級存取保護的工作流程

設定儲存層級存取保護（slag）的工作流程使用相同ONTAP的CLI命令來設定NTFS檔案權限和稽核原則。您可以在指定的儲存虛擬機器（SVM）磁碟區上設定slag、而非在指定的目標上設定檔案和目錄存取。



相關資訊

[設定儲存層級存取保護](#)

設定儲存層級存取保護

在Volume或qtree上設定儲存層級存取保護時、您需要遵循許多步驟。儲存層級的存取保護可提供在儲存層級設定的存取安全性層級。它提供的安全性適用於從所有NAS傳輸協定到套用它的儲存物件的所有存取。

步驟

1. 使用建立安全性描述元 `vserver security file-directory ntfs create` 命令。

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1

NTFS Security      Owner Name
Descriptor Name
-----
sd1                -
```

安全性描述元會以下列四個預設DACL存取控制項目 (ACE) 建立：

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
                  Type        Rights
-----
BUILTIN\Administrators
                  allow      full-control  this-folder, sub-folders,
files
BUILTIN\Users
                  allow      full-control  this-folder, sub-folders,
files
CREATOR OWNER
                  allow      full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
                  allow      full-control  this-folder, sub-folders,
files
```

如果您不想在設定儲存層級存取保護時使用預設項目、可以在建立及新增自己的ACE至安全性描述元之前將其移除。

2. 從安全性描述元中移除任何您不想設定儲存層級存取保護安全性的預設DACL ACE：
 - a. 使用移除任何不想要的 DACL ACE `vserver security file-directory ntfs dacl remove` 命令。

在此範例中、安全性描述元中會移除三個預設的DACL ACE：BUILTIN\Administrator、BUILTIN\Users 和Creator Owners。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. 請使用確認您不想用於儲存層級存取保護安全性的 DACL ACE 已從安全性描述元中移除 vserver security file-directory ntfs dacl show 命令。

在此範例中、命令的輸出會驗證安全性描述元中是否已移除三個預設的DACL ACE、只留下NT AUTHORITY\SYSTEM預設的DACL ACE項目：

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
                  Type        Rights
-----
NT AUTHORITY\SYSTEM
                  allow      full-control  this-folder, sub-folders,
files
```

3. 使用將一或多個 DACL 項目新增至安全性描述元 vserver security file-directory ntfs dacl add 命令。

在此範例中、安全性描述元中會新增兩個DACL ACE：

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. 使用將一或多個 SACL 項目新增至安全性描述元 vserver security file-directory ntfs sacl add 命令。

在此範例中、兩個 SACLACE 會新增至安全性描述元：

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. 使用確認 DACL 和 SACL ACE 已正確設定 `vserver security file-directory ntfs dacl show` 和 `vserver security file-directory ntfs sacl show` 命令。

在此範例中、下列命令會顯示安全性描述元「shd1」的DACL項目資訊：

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
Type              Rights
-----
EXAMPLE\Domain Users
                  allow      read        this-folder, sub-folders,
files
EXAMPLE\engineering
                  allow      full-control this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
                  allow      full-control this-folder, sub-folders,
files
```

在此範例中、下列命令會顯示安全性描述元「shd1」的SACL項目相關資訊：

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
Type              Rights
-----
EXAMPLE\Domain Users
                  failure    read        this-folder, sub-folders,
files
EXAMPLE\engineering
                  success    full-control this-folder, sub-folders,
files
```

6. 使用建立安全性原則 `vserver security file-directory policy create` 命令。

以下範例建立名為「policy1」的原則：

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

7. 使用確認原則已正確設定 `vserver security file-directory policy show` 命令。

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

```
Vserver          Policy Name
-----          -
vs1              policy1
```

8. 使用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` 命令 `-access-control` 參數設為 `slag`。

即使原則可以包含多個儲存層級的存取保護工作、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。

在此範例中、工作會新增至名為「policy1」的原則、該原則會指派給安全性描述元「shD1」。它會指派給 `/datavol1` 存取控制類型設為「lag」的路徑。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
propagate -ntfs-sd sd1
```

9. 使用確認工作已正確設定 `vserver security file-directory policy task show` 命令。

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
Vserver: vs1
Policy: policy1

  Index  File/Folder  Access          Security  NTFS      NTFS
Security
          Path          Control          Type      Mode      Descriptor
Name
-----
1        /datavol1    slag            ntfs     propagate sd1
```

10. 使用套用儲存層級存取保護安全性原則 `vserver security file-directory apply` 命令。

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

已排程要套用安全性原則的工作。

11. 使用驗證套用的儲存層級存取保護安全性設定是否正確 `vserver security file-directory show` 命令。

在此範例中、命令的輸出顯示儲存層級存取保護安全性已套用至 NTFS 磁碟區 `/datavol1`。即使預設

的DACL允許「所有人」完全控制、儲存層級的存取保護安全性仍會限制（及稽核）存取儲存層級存取保護設定中定義的群組。

```
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:0x8004
    Owner: BUILTIN\Administrators
    Group: BUILTIN\Administrators
    DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    ALLOW-Everyone-0x10000000-OI|CI|IO

    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
```

相關資訊

[使用CLI在SVM上管理NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護](#)

[設定儲存層級存取保護的工作流程](#)

[顯示儲存層級存取保護的相關資訊](#)

[移除儲存層級存取保護](#)

有效的熔渣對照表

您可以在磁碟區或qtree或兩者上設定slag。根據slog對照表、您可以定義哪些Volume或qtree是適用的slog組態、以符合表格中所列的各種情境。

	在美國的主動轉向系統中使用大量的	Snapshot複本中的Volume slag	在美國的美國美國美國戰地服務團 (AFS) 中使用qtree	Snapshot複本中的qtree lavg
存取檔案系統 (AFs) 中的Volume存取	是的	否	不適用	不適用
Snapshot複本中的Volume存取	是的	否	不適用	不適用
在主動轉向服務器中存取qtree (當qtree中有slog時)	否	否	是的	否
在主動轉向服務器中存取qtree (當qtree中不存在slog時)	是的	否	否	否
Snapshot複本中的qtree存取 (當qtree AFS中不存在slog時)	否	否	是的	否
Snapshot複本中的qtree存取 (當qtree AFS中不存在slog時)	是的	否	否	否

顯示儲存層級存取保護的相關資訊

儲存層級的存取保護是套用在磁碟區或qtree上的第三層安全保護。無法使用Windows內容視窗檢視儲存層級的存取保護設定。您必須使用ONTAP VMware CLI來檢視儲存層級存取保護安全性的相關資訊、以使用來驗證組態或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器 (SVM) 的名稱、以及要顯示其儲存層級存取保護安全性資訊的磁碟區或qtree路徑。

您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 顯示儲存層級的存取保護安全設定、並提供所需的詳細資料：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
更詳細的資料	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

範例

以下範例顯示 NTFS 安全性樣式磁碟區的儲存層級存取保護安全性資訊及路徑 /datavol1 在 SVM VS1 中：

```
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:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
              ALLOW-Everyone-0x1f01ff
              ALLOW-Everyone-0x10000000-OI|CI|IO

    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
```

以下範例顯示儲存層級存取保護在路徑上的混合式安全樣式磁碟區相關資訊 /datavol5 在 SVM VS1 中。此磁碟區的最上層具有UNIX有效的安全性。Volume具有儲存層級的存取保護安全性。

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

        Vserver: vs1
        File Path: /datavol5
File Inode Number: 3374
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
        ACLs: 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

```

移除儲存層級的存取保護

如果您不想再在儲存層級設定存取安全性、可以移除磁碟區或qtree上的儲存層級存取保護。移除儲存層級的存取保護不會修改或移除一般NTFS檔案和目錄安全性。

步驟

1. 使用確認磁碟區或 qtree 已設定儲存層級存取保護 `vserver security file-directory show` 命令。

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
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:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. 使用移除儲存層級存取保護 `vserver security file-directory remove-slag` 命令。

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. 使用確認儲存層級存取保護已從 Volume 或 `qtree` 移除 `vserver security file-directory show` 命令。

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
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:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs
    AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
    ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
    ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

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。