使用動態存取控制（DAC）保護檔案存取

ONTAP 9

NetApp
February 12, 2026

目錄

使用動態存取控制（DAC）保護檔案存取

了解 ONTAP SMB 伺服器的 DAC 檔案存取安全性

您可以使用動態存取控制、並在Active Directory中建立集中存取原則、並透過套用的群組原則物件（GPO）將其套用至SVM上的檔案和資料夾、以確保存取安全。您可以將稽核設定為使用集中式存取原則暫存事件、以便在套用變更之前查看中央存取原則的影響。

CIFS認證新增功能

在動態存取控制之前、CIFS認證會包含安全主體（使用者）的身分識別和Windows群組成員資格。有了動態存取控制、憑證中還會新增三種類型的資訊：裝置身分識別、裝置宣告及使用者宣告：

- 裝置識別

  使用者身分識別資訊的類比、但使用者登入裝置的身分識別和群組成員資格除外。

- 裝置聲明

  關於裝置安全主體的說法。例如、裝置宣告可能是特定OU的成員。

- 使用者聲明

  關於使用者安全性主體的說法。例如、使用者聲稱其AD帳戶可能是特定OU的成員。

集中存取原則

檔案的集中存取原則可讓組織集中部署及管理授權原則、這些原則包括使用者群組、使用者宣告、裝置宣告及資源內容的條件式運算式。

例如、若要存取高商業影響資料、使用者必須是全職員工、而且只能從受管理裝置存取資料。集中存取原則是在Active Directory中定義、並透過GPO機制散佈到檔案伺服器。

使用進階稽核進行集中式存取原則登臺

中央存取原則可以是「年齡」、在這種情況下、會在檔案存取檢查期間以「假設」的方式進行評估。原則生效時會發生的結果、以及與目前設定的不同之處、會記錄為稽核事件。如此一來、系統管理員就能在實際執行原則之前、先使用稽核事件記錄來研究存取原則變更的影響。評估存取原則變更的影響之後、即可透過GPO將原則部署至所需的SVM。

相關資訊

- 了解受支援的 GPO
- 了解如何將群組原則物件套用至 SMB 伺服器
- 在伺服器上啟用或停用 GPO 支援
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊

- 顯示有關集中存取原則規則的資訊
- 配置中央存取策略以保護伺服器上的數據
- 顯示有關伺服器安全的信息
- "SMB與NFS稽核與安全性追蹤"

ONTAP SMB 伺服器支援的 DAC 功能

如果您想要在CIFS伺服器上使用動態存取控制（DAC）、您需要瞭解ONTAP 如何在Active Directory環境中支援動態存取控制功能。

支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、支援下列功能：ONTAP

功能	註解
宣告進入檔案系統	聲稱是簡單的名稱和值配對、說明使用者的一些真實情況。使用者認證包含宣告資訊、檔案上的安全性描述元可以執行包含宣告檢查的存取檢查。如此可讓系統管理員更精細地控制哪些人可以存取檔案。
檔案存取檢查的條件式運算式	修改檔案的安全性參數時、使用者可以將任意複雜的條件運算式新增至檔案的安全性描述元。條件運算式可以包含宣告檢查。
透過集中存取原則集中控制檔案存取	集中存取原則是一種儲存在Active Directory中的ACL、可標記為檔案。只有在磁碟上的安全性描述元和標記的集中存取原則都允許存取時、才會授予檔案存取權。這可讓系統管理員控制從中央位置（AD）存取檔案的權限、而不需要修改磁碟上的安全性描述元。
集中存取原則接移	藉由「老舊」變更中央存取原則、並在稽核報告中看到變更的影響、來增加在不影響實際檔案存取的情況下嘗試安全性變更的能力。
支援使用ONTAP CLI顯示有關中央存取原則安全性的資訊	延伸 `vserver security file-directory show` 顯示已套用集中存取原則的相關資訊。
包括集中存取原則的安全性追蹤	延伸 `vserver security trace` 命令系列可顯示包含已套用集中存取原則相關資訊的結果。

不支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、不支援下列功能：ONTAP

功能	註解
NTFS檔案系統物件的自動分類	這是ONTAP Windows檔案分類基礎架構的副檔名、不受支援。
進階稽核、不包括集中存取原則接移	進階稽核僅支援集中存取原則移位。

了解如何將 DAC 和中央存取原則與 ONTAP SMB 伺服器結合使用

使用動態存取控制（DAC）和集中存取原則來保護CIFS伺服器上的檔案和資料夾安全時、必須謹記某些考量事項。

如果原則規則套用至網域\系統管理員使用者、則NFS存取權限可能會被拒絕

在某些情況下、如果將集中存取原則安全性套用至root使用者嘗試存取的資料、則可能會拒絕NFS存取root。當集中存取原則包含套用至網域\系統管理員的規則、且根帳戶對應至網域\系統管理員帳戶時、就會發生此問題。

您應該將規則套用至具有管理權限的群組、例如網域\系統管理員群組、而非套用規則至網域\系統管理員使用者。如此一來、您就可以將root對應到網域\系統管理員帳戶、而不受root影響。

在Active Directory中找不到所套用的集中存取原則時、CIFS伺服器的BUILTIN\Administrator群組可存取資源

CIFS伺服器中包含的資源可能會套用集中存取原則、但如果CIFS伺服器使用集中存取原則的SID嘗試從Active Directory擷取資訊、則該SID與Active Directory中任何現有的集中存取原則SID都不相符。在此情況下、CIFS伺服器會套用該資源的本機預設還原原則。

本機預設還原原則可讓CIFS伺服器的BUILTIN\Administrator群組存取該資源。

為 ONTAP SMB 伺服器啟用或停用 DAC

預設會停用可讓您使用動態存取控制（DAC）來保護CIFS伺服器上物件的選項。如果您想要在CIFS伺服器上使用動態存取控制、則必須啟用此選項。如果您稍後決定不想使用動態存取控制來保護儲存在CIFS伺服器上的物件、可以停用此選項。

您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定動態存取控制的資訊。

"Microsoft TechNet：動態存取控制案例總覽"

關於這項工作

啟用動態存取控制後、檔案系統就能包含具有動態存取控制相關項目的ACL。如果停用動態存取控制、則會忽略目前的動態存取控制項目、不允許新的項目。

此選項僅適用於進階權限層級。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您想要動態存取控制...	輸入命令...
已啟用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
已停用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 返回系統管理員權限等級： `set -privilege admin`

相關資訊

配置中央存取策略以保護伺服器上的數據

當 ONTAP SMB 伺服器上停用 DAC 時，管理包含 DAC ACE 的 ACL

如果您的資源已將ACL套用至動態存取控制ACE、而且您在儲存虛擬機器（SVM）上停用了動態存取控制、則必須先移除動態存取控制ACE、才能管理該資源上的非動態存取控制ACE。

關於這項工作

停用動態存取控制之後、除非您移除現有的動態存取控制ACE、否則無法移除現有的非動態存取控制ACE或新增非動態存取控制ACE。

您可以使用一般用來管理ACL的工具來執行這些步驟。

步驟

1. 判斷要將哪些動態存取控制ACE套用至資源。
2. 從資源移除動態存取控制ACE。
3. 視需要從資源中新增或移除非動態存取控制ACE。

設定中央存取策略以保護 ONTAP SMB 伺服器上的數據

您必須採取幾個步驟、才能使用集中存取原則來保護CIFS伺服器上的資料存取安全、包括在CIFS伺服器上啟用動態存取控制（DAC）、在Active Directory中設定集中存取原則、將集中存取原則套用至含GPO的Active Directory容器、 並在CIFS伺服器上啟用GPO。

開始之前

- Active Directory必須設定為使用集中存取原則。
- 您必須對Active Directory網域控制器擁有足夠的存取權限、才能建立集中存取原則、以及建立GPO並套用至包含CIFS伺服器的容器。

- 您必須對儲存虛擬機器（SVM）擁有足夠的管理存取權限、才能執行必要的命令。

關於這項工作

集中存取原則會定義並套用至Active Directory上的群組原則物件（GPO）。您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定集中存取原則的資訊。

"Microsoft TechNet：集中存取原則案例"

步驟

1. 如果 SVM 尚未使用啟用動態存取控制、請在 SVM 上啟用動態存取控制 `vserver cifs options modify` 命令。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 如果尚未使用啟用群組原則物件（ GPO ）、請在 CIFS 伺服器上啟用這些物件 `vserver cifs group-policy modify` 命令。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. 在Active Directory上建立集中存取規則和集中存取原則。
4. 建立群組原則物件（GPO）、在Active Directory上部署集中存取原則。
5. 將GPO套用至CIFS伺服器電腦帳戶所在的容器。
6. 使用手動更新套用至 CIFS 伺服器的 GPO `vserver cifs group-policy update` 命令。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. 使用確認 GPO 中央存取原則已套用至 CIFS 伺服器上的資源 `vserver cifs group-policy show-applied` 命令。

   下列範例顯示預設網域原則有兩個套用至CIFS伺服器的集中存取原則：

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
   ```

```
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
```

```
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

相關資訊

- 了解如何將群組原則物件套用至 SMB 伺服器
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊
- 啟用或停用伺服器的 DAC

顯示有關 ONTAP SMB 伺服器的 DAC 安全性的信息

您可以顯示NTFS磁碟區上的動態存取控制（DAC）安全性資訊、以及在混合式安全型磁碟區上具有NTFS有效安全性的資料。這包括有關條件式ACE、資源ACE和集中存取原則ACE的資訊。您可以使用結果來驗證安全性組態、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、以及您要顯示其檔案或資料夾安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
其中輸出會顯示群組和使用者的SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
關於將十六進位位元遮罩轉譯為文字格式之檔案和目錄的檔案和目錄安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

範例

下列範例顯示有關路徑的動態存取控制安全性資訊 `/vol1` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

相關資訊

- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊

ONTAP SMB 伺服器上 DAC 的復原註意事項

您應該瞭解還原ONTAP 至不支援動態存取控制（DAC）的版本時會發生什麼事、以及還原之前和之後必須執行的動作。

如果您想要將叢集還原成ONTAP 不支援動態存取控制的版本、且已在一或多個儲存虛擬機器（SVM）上啟用動態存取控制、則必須先執行下列動作、才能還原：

- 您必須停用叢集上所有已啟用動態存取控制的SVM。
- 您必須修改包含的叢集上的任何稽核組態 `cap-staging` 僅使用的事件類型 `file-op` 事件類型。

您必須瞭解動態存取控制ACE的檔案和資料夾、並採取行動：

- 如果叢集還原、則不會移除現有的動態存取控制ACE；不過、檔案存取檢查會忽略這些ACE。
- 由於還原後會忽略動態存取控制ACE、因此使用動態存取控制ACE的檔案存取權會有所變更。

  這可能會允許使用者存取先前無法存取的檔案、或無法存取先前可能存取的檔案。

- 您應該將非動態存取控制ACE套用至受影響的檔案、以還原其先前的安全層級。

  這可以在還原之前或還原完成後立即完成。

由於還原後會忽略動態存取控制ACE、因此在將非動態存取控制ACE套用至受影響的檔案時、不需要將其移除。不過、如果需要、您可以手動移除。

版權資訊

商標資訊