稽核SVM上的NAS事件
ONTAP 9

NetApp
February 12, 2026

目錄

稽核SVM上的NAS事件

瞭解如何針對 SMB 和 NFS 傳輸協定使用 ONTAP 來稽核檔案存取

您可以搭配ONTAP 使用適用於SMB和NFS傳輸協定的檔案存取稽核功能、例如使用FPolicy進行原生稽核和檔案原則管理。

在下列情況下、您應該設計及實作SMB與NFS檔案存取事件的稽核：

- 已設定基本的SMB和NFS傳輸協定檔案存取。
- 您想要使用下列其中一種方法來建立及維護稽核組態：
  - 原生ONTAP 的功能
  - 外部FPolicy伺服器

稽核SVM上的NAS事件

稽核NAS事件是一項安全性措施、可讓您追蹤及記錄儲存虛擬機器（SVM）上的特定SMB和NFS事件。這有助於您追蹤潛在的安全問題、並提供任何安全漏洞的證據。您也可以登錄及稽核Active Directory集中存取原則、以瞭解實作原則的結果。

SMB 活動

您可以稽核下列事件：

- SMB檔案與資料夾存取事件

  您可以稽核儲存在FlexVol 包含啟用稽核功能之SVM的物件上的SMB檔案和資料夾存取事件。

- SMB登入和登出事件

  您可以稽核SVM上SMB伺服器的SMB登入和登出事件。

- 集中存取原則執行事件

  您可以使用透過建議的集中存取原則套用的權限、來稽核SMB伺服器上物件的有效存取。透過集中存取原則的暫存進行稽核、可讓您在部署中央存取原則之前、先瞭解其影響。

  使用Active Directory GPO設定集中存取原則暫存稽核；不過、SVM稽核組態必須設定為稽核集中存取原則暫存事件。

  雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

NFS 事件

您可以利用NFSv4 ACL來稽核儲存在SVM上的物件、以稽核檔案和目錄事件。

稽核的運作方式

瞭解 ONTAP 的基本稽核概念

若要瞭解ONTAP 功能性稽核、您應該瞭解一些基本的稽核概念。

- 暫存檔案

  在合併與轉換之前、會儲存稽核記錄的個別節點上的中間二進位檔案。暫存檔案包含在暫存磁碟區中。

- 暫存磁碟區

  由支援儲存暫存檔案的功能所建立的專屬Volume ONTAP 。每個Aggregate有一個接移磁碟區。執行磁碟區由所有啟用稽核的儲存虛擬機器（SVM）共享、以儲存資料磁碟區在該特定集合體中的資料存取稽核記錄。每個SVM的稽核記錄都儲存在暫存磁碟區內的個別目錄中。

  叢集管理員可以檢視暫存磁碟區的相關資訊、但不允許執行其他大部分的Volume作業。只ONTAP 有能夠建立暫存磁碟區。自動為暫存磁碟區指派名稱。ONTAP所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID （例如： `MDV_aud_1d0131843d4811e296fc123478563412`）

- 系統磁碟區

  包含特殊中繼資料（例如檔案服務稽核記錄的中繼資料）的Some Volume。FlexVol管理SVM擁有整個叢集可見的系統磁碟區。接移磁碟區是一種系統磁碟區。

- 整合工作

  啟用稽核時建立的工作。這項在每個SVM上長期執行的工作、會將稽核記錄從SVM成員節點上的暫存檔案中移出。此工作會依照時間順序合併稽核記錄、然後將其轉換成稽核組態中指定的使用者可讀取事件記錄格式（無論是evtx或XML檔案格式）。轉換後的事件記錄會儲存在SVM稽核組態中指定的稽核事件記錄目錄中。

瞭解 ONTAP 稽核程序的功能

這個不一樣的稽核程序與Microsoft稽核程序不同。ONTAP在您設定稽核之前、您應該先瞭解ONTAP 不稽核程序的運作方式。

稽核記錄一開始會儲存在個別節點上的二進位暫存檔案中。如果在SVM上啟用稽核、則每個成員節點都會維護該SVM的暫存檔案。這些記錄會定期整合並轉換成使用者可讀取的事件記錄、這些記錄會儲存在SVM的稽核事件記錄目錄中。

在SVM上啟用稽核的程序

稽核只能在SVM上啟用。當儲存管理員在SVM上啟用稽核時、稽核子系統會檢查暫存磁碟區是否存在。每個包含SVM擁有之資料磁碟區的Aggregate都必須存在暫存Volume。稽核子系統會建立任何必要的暫存磁碟區（如果不存在）。

稽核子系統也會在啟用稽核之前完成其他必要工作：

- 稽核子系統會驗證記錄目錄路徑是否可用、而且不包含symlink。

  記錄目錄必須已存在於SVM命名空間內的路徑中。建議您建立新的Volume或qtree來保存稽核記錄檔。稽核子系統不會指派預設的記錄檔位置。如果稽核組態中指定的記錄目錄路徑不是有效路徑、則稽核組態建立會失敗 `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` 錯誤。

  如果目錄存在但包含symlink、則組態建立會失敗。

- 稽核會排程整合工作。

  排程此工作之後、就會啟用稽核。SVM稽核組態和記錄檔會在重新開機時持續存在、或者NFS或SMB伺服器會停止或重新啟動。

事件記錄整合

記錄整合是一項排程工作、會在停用稽核之前、定期執行。停用稽核時、整合工作會驗證是否已合併所有剩餘的記錄。

保證稽核

依預設、稽核是保證的。此功能可確保記錄所有可稽核的檔案存取事件（如設定的稽核原則ACL所指定）、即使節點無法使用亦然。ONTAP在將該作業的稽核記錄儲存至持續儲存設備上的暫存磁碟區之前、無法完成要求的檔案作業。如果稽核記錄無法提交至暫存檔案中的磁碟、無論是因為空間不足或其他問題、用戶端作業都會遭到拒絕。

> 系統管理員或具有權限層級存取權的帳戶使用者、可以使用NetApp Manageability SDK或REST API來略過檔案稽核記錄作業。您可以檢閱儲存在中的命令記錄檔、判斷是否已使用 NetApp Manageability SDK 或 REST API 執行任何檔案動作 `audit.log` 檔案：
>
> 如需命令歷程記錄稽核記錄的詳細資訊、請參閱中的「管理管理管理活動的稽核記錄」一節 "系統管理"。

節點無法使用時的整合程序

如果包含屬於已啟用稽核之SVM的磁碟區的節點無法使用、則稽核整合工作的行為取決於節點的儲存容錯移轉（SFO）合作夥伴（或是雙節點叢集的HA合作夥伴）是否可用：

- 如果接移磁碟區可透過SFO合作夥伴取得、則會掃描上次從節點回報的接移磁碟區、並正常進行整合。
- 如果無法取得SFO合作夥伴、工作會建立部分記錄檔。

  當節點無法連線時、整合工作會整合該SVM其他可用節點的稽核記錄。為了識別尚未完成、工作會新增後置字元 `.partial` 合併的檔案名稱。

- 當無法使用的節點可用之後、該節點中的稽核記錄會與當時來自其他節點的稽核記錄合併。
- 所有稽核記錄都會保留下來。

事件記錄檔循環

稽核事件記錄檔會在達到設定的臨界值記錄大小或已設定的排程時進行旋轉。當事件記錄檔旋轉時、排程的整合工作會先將作用中的轉換檔重新命名為具有時間戳記的歸檔檔檔、然後建立新的作用中轉換事件記錄檔。

在**SVM**上停用稽核的程序

在SVM上停用稽核時、整合工作會最後觸發一次。所有未處理、記錄的稽核記錄都會以使用者可讀取的格式記錄。在SVM上停用稽核且可供檢視時、不會刪除儲存在事件記錄目錄中的現有事件記錄。

合併該SVM的所有現有暫存檔案之後、整合工作就會從排程中移除。停用SVM的稽核組態不會移除稽核組態。儲存管理員可以隨時重新啟用稽核。

稽核整合工作會在啟用稽核時建立、可監控整合工作、並在整合工作因錯誤而結束時重新建立。使用者無法刪除稽核整合工作。

ONTAP 稽核的必要條件

在儲存虛擬機器（SVM）上設定及啟用稽核之前、您必須瞭解特定的需求和考量。

- NFS 和 S3 稽核啟用 SVM 的合併限制取決於您的 ONTAP 版本：

版本ONTAP	最大值
9.8 及更早版本	50
9.9.1及更新版本	400

- 稽核不受限於SMB或NFS授權。

  即使叢集上未安裝SMB與NFS授權、您仍可設定及啟用稽核。

- NFS稽核支援安全性ACE（類型U）。
- 對於NFS稽核、模式位元與稽核ACE之間沒有對應關係。

  將ACL轉換為模式位元時、會跳過稽核ACE。將模式位元轉換為ACL時、不會產生稽核ACE。

- 稽核組態中指定的目錄必須存在。

  如果不存在、建立稽核組態的命令就會失敗。

- 稽核組態中指定的目錄必須符合下列需求：
  - 目錄不得包含符號連結。

    如果稽核組態中指定的目錄包含符號連結、建立稽核組態的命令就會失敗。

  - 您必須使用絕對路徑來指定目錄。

    您不應指定相對路徑、例如 `/vs1/../`。

- 稽核取決於暫存磁碟區中是否有可用空間。

您必須瞭解並制定計畫、確保集合體中含有稽核磁碟區的暫存磁碟區有足夠的空間。

- 稽核取決於磁碟區中是否有可用空間、其中包含儲存轉換事件記錄的目錄。

  您必須注意並制定計畫、確保用於儲存事件記錄的磁碟區有足夠的空間。您可以使用指定要保留在稽核目錄中的事件記錄數目 `-rotate-limit` 建立稽核組態時的參數、有助於確保磁碟區中有足夠的可用空間用於事件記錄。

- 雖然您可以在稽核組態中啟用集中存取原則接移、而不需在SMB伺服器上啟用動態存取控制、但必須啟用動態存取控制、才能產生集中存取原則接移事件。

  預設不會啟用動態存取控制。

啟用稽核時的**Aggregate space**考量

建立稽核組態並在叢集中至少一個儲存虛擬機器（SVM）上啟用稽核時、稽核子系統會在所有現有的集合體和所有建立的新集合體上建立暫存磁碟區。在叢集上啟用稽核時、您必須注意特定的Aggregate空間考量。

由於Aggregate中的空間不可用、所以暫存磁碟區建立可能會失敗。如果您建立稽核組態、而現有的Aggregate沒有足夠的空間來容納接移磁碟區、就可能發生這種情況。

在SVM上啟用稽核之前、您應該先確定現有集合體上有足夠的空間可用於暫存磁碟區。

限制 **ONTAP** 稽核記錄的暫存檔案大小

暫存檔案上的稽核記錄大小不得大於32 KB。

發生大型稽核記錄時

在下列其中一種情況下、在管理稽核期間可能會發生大量的稽核記錄：

- 新增或刪除具有大量使用者之群組的使用者。
- 新增或刪除檔案共用區上的檔案共用存取控制清單（ACL）、以供大量的檔案共用使用者使用。
- 其他案例。

停用管理稽核以避免此問題。若要這麼做、請修改稽核組態、並從稽核事件類型清單中移除下列項目：

- 檔案共用
- 使用者帳戶
- 安全性群組
- 授權原則變更

  移除之後、檔案服務稽核子系統不會稽核這些檔案。

稽核記錄過大的影響

- 如果稽核記錄的大小過大（超過32 KB）、則不會建立稽核記錄、稽核子系統會產生類似下列的事件管理系

統（EMS）訊息：

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

如果保證稽核、則檔案作業會因為無法建立稽核記錄而失敗。

- 如果稽核記錄的大小超過9、999個位元組、則會顯示與上述相同的EMS訊息。系統會建立部分稽核記錄、但缺少較大的金鑰值。
- 如果稽核記錄超過2、000個字元、則會顯示下列錯誤訊息、而非實際值：

```
The value of this field was too long to display.
```

瞭解 ONTAP 稽核事件記錄的支援格式

已轉換的稽核事件記錄檔支援的檔案格式為 EVTX 和 XML 檔案格式。

您可以在建立稽核組態時指定檔案格式的類型。根據預設、 ONTAP 會將二進位記錄轉換成 EVTX 檔案格式。

檢視及處理 ONTAP 稽核事件記錄

您可以使用稽核事件記錄來判斷是否有足夠的檔案安全性、以及是否有不當的檔案和資料夾存取嘗試。您可以檢視及處理儲存在中的稽核事件記錄 EVTX 或 XML 檔案格式。

- EVTX 檔案格式

  您可以開啟已轉換的 EVTX 使用 Microsoft 事件檢視器將事件記錄稽核為儲存的檔案。

  使用「事件檢視器」檢視事件記錄時、您可以使用兩種選項：

  - 一般檢視

    所有事件的通用資訊都會顯示在事件記錄中。在此版本ONTAP 的資訊不顯示事件記錄的事件特定資料。您可以使用詳細檢視來顯示特定事件的資料。

  - 詳細檢視

    提供友善的檢視和XML檢視。易記檢視和XML檢視會同時顯示所有事件通用的資訊、以及事件記錄的事件特定資料。

- XML 檔案格式

  您可以檢視及處理 XML 稽核支援的協力廠商應用程式上的事件記錄 XML 檔案格式。XML檢視工具可用於檢視稽核記錄、前提是您必須具備XML架構和XML欄位定義的相關資訊。如需XML架構和定義的詳細資訊、請參閱 "《稽核架構參考》ONTAP"。

使用事件檢視器檢視作用中稽核記錄的方式

如果稽核整合程序正在叢集上執行、則整合程序會將新記錄附加到啟用稽核的儲存虛擬機器（SVM）作用中稽核記錄檔。此作用中稽核記錄可透過Microsoft事件檢視器中的SMB共用區存取及開啟。

除了檢視現有的稽核記錄之外、「事件檢視器」還提供重新整理選項、可讓您重新整理主控台視窗中的內容。新附加的記錄是否可在事件檢視器中檢視、取決於是否在用來存取作用中稽核記錄的共用區上啟用oplocks。

共享區上的oplocks設定	行為
已啟用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業不會以合併程序附加的新事件來重新整理記錄。
已停用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業會以合併程序附加的新事件來重新整理記錄。

此資訊僅適用於 `EVTX` 事件記錄。 `XML` 事件記錄可以透過 SMB 瀏覽器或 NFS 、使用任何 XML 編輯器或檢視器來檢視。

可稽核的SMB事件

瞭解 ONTAP 可稽核以解讀結果的 SMB 事件

可稽核特定的SMB事件、包括特定檔案和資料夾存取事件、特定登入和登出事件、以及集中存取原則暫存事件。ONTAP瞭解哪些存取事件可以稽核、有助於解讀事件記錄的結果。

可以審核以下附加 SMB 事件：

事件ID（EVT/evtx）	活動	說明	類別
4670	物件權限已變更	物件存取：權限已變更。	檔案存取
4907	物件稽核設定已變更	物件存取：稽核設定已變更。	檔案存取
4913.	物件中心存取原則已變更	物件存取：CAP已變更。	檔案存取

下列SMB事件ONTAP 可在下列版本中透過下列功能進行稽核：

事件ID（EVT/evtx）	活動	說明	類別
540/4624	帳戶已成功登入	登入/登出：網路（SMB）登入。	登入與登出
598/4625	帳戶無法登入	登入/登出：不明的使用者名稱或錯誤的密碼。	登入與登出
530/4625	帳戶無法登入	登入/登出：帳戶登入時間限制。	登入與登出

531/4625	帳戶無法登入	登入/登出：帳戶目前已停用。	登入與登出
532/4625	帳戶無法登入	登入/登出：使用者帳戶已過期。	登入與登出
533/4625	帳戶無法登入	登入/登出：使用者無法登入此電腦。	登入與登出
534/4625	帳戶無法登入	登入/登出：使用者未在此授予登入類型。	登入與登出
535/4625	帳戶無法登入	登入/登出：使用者密碼已過期。	登入與登出
537-4625	帳戶無法登入	登入/登出：登入失敗的原因並非上述原因。	登入與登出
5310/4625	帳戶無法登入	登入/登出：帳戶已鎖定。	登入與登出
538/4634	帳戶已登出	登入/登出：本機或網路使用者登出。	登入與登出
560/ 4656	開啟物件/建立物件	物件存取：物件（檔案或目錄）開啟。	檔案存取
563/4659	開啟要刪除的物件	物件存取：要求物件（檔案或目錄）的控點、目的是刪除。	檔案存取
564/4660	刪除物件	物件存取：刪除物件（檔案或目錄）。當Windows用戶端嘗試刪除物件（檔案或目錄）時、會產生此事件。ONTAP	檔案存取
567/4663	讀取物件/寫入物件/取得物件屬性/設定物件屬性	物件存取：物件存取嘗試（讀取、寫入、取得屬性、設定屬性）。 附註： ONTAP 針對此活動、僅針對物件上的第一個SMB讀取和第一個SMB寫入作業（成功或失敗）進行不稽核。這可防止ONTAP 在單一用戶端開啟物件並對同一個物件執行多次連續的讀取或寫入作業時、造成過多的記錄項目。	檔案存取
NA/4664	硬式連結	物件存取：嘗試建立硬式連結。	檔案存取
NA/4818	建議的集中存取原則並未授予與目前集中存取原則相同的存取權限	物件存取：集中存取原則Staging。	檔案存取

NA/ NA Data ONTAP 不適用事件ID 9999	重新命名物件	物件存取：物件已重新命名。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取
NA/ NA Data ONTAP 不景事件ID 9998	取消連結物件	物件存取：物件未連結。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取

活動**4656**的其他相關資訊

。 `HandleID` 稽核中的標記 `XML` 事件包含所存取物件（檔案或目錄）的處理方式。。 `HandleID` evtx 4656 事件的標記包含不同的資訊、取決於開啟的事件是用於建立新物件或開啟現有物件：

- 如果開啟的事件是建立新物件（檔案或目錄）的開放式要求、則 `HandleID` 稽核 XML 事件中的標記顯示為空白 `HandleID` （例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

  。 `HandleID` 為空白、因為在實際物件建立之前和處理代碼存在之前、會先稽核開啟（用於建立新物件）的要求。相同物件的後續稽核事件在中具有適當的物件控點 `HandleID` 標記。

- 如果開啟的事件是開啟現有物件的開放式要求、則稽核事件會在中指派該物件的處理代碼 `HandleID` 標記（例如： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>` ）。

決定 **ONTAP** 稽核物件的完整路徑

列印在中的物件路徑 `<ObjectName>` 稽核記錄的標記包含磁碟區名稱（以括弧括住）、以及包含磁碟區根目錄的相對路徑。如果您想要判斷稽核物件的完整路徑（包括交會路徑）、您必須採取某些步驟。

步驟

1. 請查看、判斷哪些磁碟區名稱和受稽核物件的相對路徑 `<ObjectName>` 稽核事件中的標記。

   在此範例中、磁碟區名稱為「 data1 」、檔案的相對路徑為 `/dir1/file.txt` ：

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. 使用上一步驟所決定的磁碟區名稱、判斷包含稽核物件之磁碟區的交會路徑：

   在此範例中、磁碟區名稱為「 data1 」、而包含稽核物件之磁碟區的交會路徑為 `/data/data1` ：

   ```
   volume show -junction -volume data1
   ```

   ```
                                Junction                       Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. 附加在中找到的相對路徑、以決定稽核物件的完整路徑 `<ObjectName>` 標記為磁碟區的交會路徑。

   在此範例中、磁碟區的交會路徑為：

   `/data/data1/dir1/file.text`

瞭解 ONTAP 對符號連結和硬式連結的稽核

稽核symlink和硬式連結時、必須謹記某些考量事項。

稽核記錄包含所稽核物件的相關資訊、包括中所識別的已稽核物件路徑 `ObjectName` 標記。您應該瞭解 symlinks 和硬式連結的路徑如何記錄在中 `ObjectName` 標記。

symlinks

symlink是一個具有獨立inode的檔案、其中包含指向目的地物件（稱為目標）位置的指標。透過symlink存取物件時ONTAP 、流通會自動解譯symlink、並遵循實際規範的非規範傳輸協定路徑、前往磁碟區中的目標物件。

在下列範例輸出中、有兩個 symlink 、兩者都指向一個名為的檔案 `target.txt`。其中一個symlink是相對symlink、一個是絕對symlink。如果稽核其中任一符號連結、則為 `ObjectName` 稽核事件中的標記包含檔案路徑 `target.txt`：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

硬式連結

硬式連結是指將名稱與檔案系統上現有檔案相關聯的目錄項目。硬式連結指向原始檔案的inode位置。如同用什麼方式解譯symlinks、它會解譯硬式連結、並遵循實際規範路徑前往Volume中的目標物件。ONTAP ONTAP稽核硬式連結物件的存取時、稽核事件會在中記錄這條絕對規範路徑 `ObjectName` 標記而非硬連結路徑。

瞭解替代 NTFS 資料串流的 ONTAP 稽核

在使用NTFS替代資料流稽核檔案時、您必須謹記某些考量事項。

要稽核的物件位置會使用兩個標籤（即）記錄在事件記錄中 `ObjectName` 標記（路徑）和 `HandleID` 標記（控點）。若要正確識別正在記錄的串流要求、您必須知道ONTAP 這些欄位中有哪些資料流是NTFS替代資料串流的佐證記錄：

- evtxID：4656個事件（開啟並建立稽核事件）
  - 替代資料串流的路徑會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。

- evtxID：4663個事件（所有其他稽核事件、例如讀取、寫入、getattr等）
  - 基礎檔案的路徑、而非替代資料串流、會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。

範例

下列範例說明如何使用識別 evtx ID ： 4663 個事件以用於替代資料串流 `HandleID` 標記。即使是 `ObjectName` 在讀取稽核事件中記錄的標記（路徑）位於基礎檔案路徑 `HandleID` 標記可用於將事件識別為替代資料串流的稽核記錄。

串流檔案名稱採用格式 `base_file_name:stream_name`。在此範例中 `dir1` 目錄包含基礎檔案、具有下列路徑的替代資料串流：

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

下列事件範例中的輸出會如所示被刪減；輸出不會顯示事件的所有可用輸出標記。

對於 evtx ID 4656 （開放式稽核事件）、替代資料串流的稽核記錄輸出會在中記錄替代資料串流名稱 `ObjectName` 標記：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

對於 evtx ID 4663 （讀取稽核事件）、相同替代資料串流的稽核記錄輸出會在中記錄基礎檔案名稱 `ObjectName` 標記；不過、中的控點 `HandleID` 標記是替代資料串流的處理方式、可用於將此事件與替代資料串流建立關聯：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

瞭解 ONTAP 對 NFS 檔案和目錄存取事件的稽核

可以稽核某些NFS檔案和目錄存取事件。ONTAP瞭解哪些存取事件可稽核、有助於解讀轉換後的稽核事件記錄結果。

您可以稽核下列NFS檔案和目錄存取事件：

- 讀取
- 開啟
- 關閉
- readdir
- 寫入
- 設定
- 建立
- 連結
- OPENATTR
- 移除
- GetAttr
- 驗證
- n驗證
- 重新命名

若要可靠地稽核NFS重新命名事件、您應該在目錄上設定稽核ACE、而不要在檔案上設定、因為如果目錄權限足夠、就不會檢查檔案權限來執行重新命名作業。

規劃 ONTAP VM 上的稽核組態

在儲存虛擬機器（SVM）上設定稽核之前、您必須先瞭解可用的組態選項、並針對每個選項規劃您要設定的值。此資訊可協助您設定稽核組態、以滿足您的業務需求。

所有稽核組態都有一些通用的組態參數。

此外、您也可以使用某些參數來指定在旋轉合併和轉換的稽核記錄時使用哪些方法。您可以在設定稽核時指定下列三種方法之一：

- 根據記錄大小來旋轉記錄

  這是用來旋轉記錄的預設方法。

- 根據排程來旋轉記錄
- 根據記錄大小和排程來旋轉記錄（以先發生的事件為準）

至少應設定一種記錄輪調方法。

所有稽核組態的通用參數

建立稽核組態時、必須指定兩個必要參數。您也可以指定三個選用參數：

資訊類型	選項	必要	包括	您的價值
*SVM*名稱 要在其中建立稽核組態的SVM名稱。SVM必須已經存在。	`-vserver vserver_name`	是的	是的	
記錄目的地路徑 指定儲存已轉換稽核記錄的目錄、通常是專屬磁碟區或qtree。路徑必須已存在於SVM命名空間中。 路徑長度最多可達864個字元、且必須具有讀寫權限。 如果路徑無效、稽核組態命令就會失敗。 如果SVM是SVM災難恢復來源、則記錄目的地路徑無法位於根磁碟區上。這是因為根磁碟區內容並未複寫到災難恢復目的地。 您無法將FlexCache 無法使用的功能區當成記錄目的地ONTAP （例如、更新版本的更新版本）。	`-destination text`	是的	是的	

要稽核的事件類別_ 指定要稽核的事件類別。您可以稽核下列事件類別： • 檔案存取事件（SMB和NFSv4） • SMB登入和登出事件 • 集中存取原則執行事件 從 Windows 2012 Active Directory 網域開始、就可以使用中央存取原則的移位事件。 • 非同步刪除 • 檔案共用類別事件 • 稽核原則變更事件 • 本機使用者帳戶管理事件 • 安全性群組管理事件 • 授權原則變更事件 預設為稽核檔案存取和SMB登入及登出事件。 • 備註： * 您可以先指定 `cap-staging` 在事件類別中、 SVM 上必須存在 SMB 伺服器。雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。	`-events{file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`

否			記錄檔案輸出格式 決定稽核記錄的輸出格式。輸出格式可以是 ONTAP 專用格式 XML 或 Microsoft Windows EVTX 記錄格式。依預設、輸出格式為 EVTX。	-format {xml
evtx}	否			記錄檔案旋轉限制 決定要保留多少稽核記錄檔、然後再將最舊的記錄檔轉出。例如、如果您輸入的值 5，最後五個記錄檔會保留。 的值 0 表示保留所有記錄檔。預設值為 0 。

用於判斷何時旋轉稽核事件記錄的參數

根據記錄大小旋轉記錄

預設值是根據大小來旋轉稽核記錄。

- 預設記錄大小為100 MB
- 如果您要使用預設的記錄檔旋轉方法和預設的記錄檔大小、則不需要設定任何特定的記錄檔旋轉參數。

- 如果您想要根據記錄檔大小來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-schedule-minute` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

如果您不想使用預設記錄大小、可以設定 `-rotate-size` 指定自訂記錄大小的參數：

資訊類型	選項	必要	包括	您的價值
記錄檔案大小限制 決定稽核記錄檔大小限制。	`-rotate-size {integer[kb`	MB	GB	TB

根據排程旋轉記錄

如果您選擇根據排程來旋轉稽核記錄、您可以使用任何組合的時間型旋轉參數來排程記錄輪調。

- 如果您使用時間型旋轉、則會使用 `-rotate-schedule-minute` 參數為必填。
- 所有其他的時間型旋轉參數都是選用的。
- 旋轉排程是使用所有與時間相關的值來計算。

  例如、如果您只指定 `-rotate-schedule-minute` 參數時、稽核記錄檔會根據一週中所有天所指定的分鐘數、在一年中所有月份的所有小時內進行旋轉。

- 如果只指定一或兩個時間型旋轉參數（例如、 `-rotate-schedule-month` 和 `-rotate-schedule -minutes`）、記錄檔會根據您在一週的所有天、所有時間、但僅在指定的月份內所指定的分鐘值來旋轉。

  例如、您可以指定稽核日誌在一月、三月和八月的所有週一、週三和週六上午10：30進行輪調

- 如果您同時指定兩者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`的問題。

  例如、如果您指定 `-rotate-schedule-dayofweek` 星期五和 `-rotate-schedule-day` 截至 13 日、稽核記錄將會在每週五和指定月份的第 13 天、而不只是在每週五的第 13 天輪調。

- 如果您想要根據排程來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-size` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-size -`

您可以使用下列可用稽核參數清單、來決定要使用哪些值來設定稽核事件記錄輪調的排程：

資訊類型	選項	必要	包括	您的價值
記錄輪調排程：月 決定每月循環稽核記錄的排程。 有效值為 `January` 透過 `December`和 `all`。例如、您可以指定稽核日誌在1月、3月和8月期間輪調。	`-rotate-schedule-month chron_month`	否		

記錄輪調排程：週中日 決定每日（一週中的某天）排程以循環稽核記錄。 有效值為 `Sunday` 透過 `Saturday`和 `all`。例如、您可以指定稽核日誌在週二和週五、或一週中的所有日子循環顯示。	`-rotate-schedule -dayofweek chron_dayofweek`	否		
記錄輪調排程：天 決定每月的日期排程、以循環稽核記錄。 有效值範圍從 `1` 透過 `31`。例如、您可以指定稽核日誌在每月的第10天和第20天、或每月的所有天進行旋轉。	`-rotate-schedule-day chron_dayofmonth`	否		
_記錄輪調排程：hour _ 決定每小時循環稽核記錄的排程。 有效值範圍從 `0` （午夜）至 `23` （下午 11 ： 00 ）。指定 `all` 每小時輪換稽核記錄。例如、您可以指定稽核日誌的旋轉時間為6（上午6點）和18（下午6點）。	`-rotate-schedule-hour chron_hour`	否		
記錄輪調排程：分 決定稽核日誌的分鐘排程。 有效值範圍從 `0` 至 `59`。例如、您可以指定稽核日誌在30分鐘內旋轉。	`-rotate-schedule-minute chron_minute`	是、如果設定排程型記錄輪調、則為否		

根據記錄大小和排程來旋轉記錄

您可以選擇根據記錄大小和排程來旋轉記錄檔、方法是同時設定 `-rotate-size` 參數和時間型旋轉參數。例如：IF `-rotate-size` 設為 10 MB 、且 `-rotate-schedule-minute` 設為 15 、當記錄檔大小達到 10 MB 或每小時 15 分鐘（以先發生的事件為準）時、記錄檔會旋轉。

在SVM上建立檔案和目錄稽核組態

在 ONTAP VM 上建立檔案和目錄稽核組態

在儲存虛擬機器（SVM）上建立檔案和目錄稽核組態、包括瞭解可用的組態選項、規劃組態、然後設定和啟用組態。然後您可以顯示稽核組態的相關資訊、以確認所產生的組態為所需的組態。

在開始稽核檔案和目錄事件之前、您必須先在儲存虛擬機器（SVM）上建立稽核組態。

開始之前

如果您打算建立稽核組態以進行集中存取原則暫存、則SVM上必須有SMB伺服器。

- 雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。

  動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

- 如果命令中某個欄位的引數無效、例如欄位的輸入無效、項目重複、以及項目不存在、則命令會在稽核階段之前失敗。

  此類失敗不會產生稽核記錄。

關於這項工作

如果SVM是SVM災難恢復來源、則目的地路徑無法位於根磁碟區上。

步驟

1. 使用規劃工作表中的資訊、建立稽核組態、根據記錄大小或排程來旋轉稽核記錄：

如果您想要以下列方式來旋轉稽核記錄…	輸入…
記錄檔大小	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
排程	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

範例

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/audit_log` 目錄。記錄檔大小限制為 `200 MB`。當記錄大小達到200 MB時、就會進行旋轉：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/cifs_event_logs` 目錄。記錄檔大小限制為 `100 MB` （預設值）、且記錄輪調限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

下列範例建立稽核組態、以稽核檔案作業、CIFS登入和登出事件、以及使用時間型輪調的集中存取原則暫存事件。記錄格式為 `EVTX` （預設）。稽核記錄會每月於下午12：30循環一次一週中的所有天。日誌輪轉限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

相關資訊

- "在SVM上啟用稽核"
- "驗證稽核組態"

在設定稽核組態之後，啟用 ONTAP SVM 的稽核

完成稽核組態的設定之後、您必須在儲存虛擬機器（SVM）上啟用稽核。

開始之前

SVM稽核組態必須已經存在。

關於這項工作

當SVM災難恢復ID捨棄組態第一次啟動（完成SnapMirror初始化之後）且SVM具有稽核組態時ONTAP 、無法自動停用稽核組態。在唯讀SVM上停用稽核、以防止執行磁碟區填滿。只有在SnapMirror關係中斷且SVM為讀寫時、才能啟用稽核。

步驟

1. 在SVM上啟用稽核：

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

相關資訊

- "建立稽核組態"
- "驗證稽核組態"

驗證 ONTAP 稽核組態

完成稽核組態之後、您應該確認稽核設定正確且已啟用。

步驟

1. 驗證稽核組態：

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   下列命令會以清單形式顯示儲存虛擬機器（SVM）VS1的所有稽核組態資訊：

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 200MB
       Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
   ```

相關資訊

- "建立稽核組態"
- "在SVM上啟用稽核"

設定檔案和資料夾稽核原則

啟用 ONTAP SVM 上的稽核組態，並設定檔案和資料夾稽核原則

在檔案和資料夾存取事件上實作稽核是兩步驟的程序。首先、您必須在儲存虛擬機器（SVM）上建立並啟用稽核組態。其次、您必須在要監控的檔案和資料夾上設定稽核原則。您可以設定稽核原則、以監控成功和失敗的存取嘗試。

您可以設定SMB和NFS稽核原則。SMB與NFS稽核原則具有不同的組態需求與稽核功能。

如果已設定適當的稽核原則、ONTAP 僅當SMB或NFS伺服器正在執行時、才會監控稽核原則中指定的SMB和NFS存取事件。

在 **NTFS** 安全性樣式的檔案和目錄上設定 **ONTAP** 稽核原則

在稽核檔案和目錄作業之前、您必須先在要收集稽核資訊的檔案和目錄上設定稽核原則。這是設定及啟用稽核組態的附加功能。您可以使用Windows安全性索引標籤或ONTAP 使用CLI來設定NTFS稽核原則。

使用**Windows**安全性索引標籤設定**NTFS**稽核原則

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、在檔案和目錄上設定NTFS稽核原則。這是在Windows用戶端上設定資料稽核原則時所使用的相同方法、讓您能夠使用慣用的GUI介面。

開始之前

稽核必須在儲存虛擬機器（SVM）上設定、其中包含您要套用系統存取控制清單（SACL）的資料。

關於這項工作

若要設定NTFS稽核原則、請將項目新增至與NTFS安全性描述元相關聯的NTFS SACL。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。安全性描述元可包含用於套用檔案和資料夾存取權限的判別存取控制清單（DACL）、用於檔案和資料夾稽核的SACL、或同時套用SACL和DACL。

若要使用Windows安全性索引標籤設定NTFS稽核原則、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. 填寫*對應網路磁碟機*方塊：
   a. 選取*磁碟機*字母。
   b. 在「資料夾」方塊中、輸入包含共用區的SMB伺服器名稱、其中包含您要稽核的資料及共用區名稱。

      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。

      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`。

   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. 選取您要啟用稽核存取的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄、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. 執行所需的動作：

如果你想…	請執行下列動作

設定新使用者或群組的稽核	a. 按一下「 * 新增 * 」。 b. 在「輸入要選取的物件名稱」方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。
移除使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 按一下「確定」。 d. 跳過此程序的其餘部分。
變更使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要變更的使用者或群組。 b. 按一下 * 編輯 * 。 c. 按一下「確定」。

如果您要在使用者或群組上設定稽核、或是變更現有使用者或群組的稽核、就會開啟「<object>的稽核項目」方塊。

9. 在「套用至」方塊中、選取您要套用此稽核項目的方式。

   您可以選擇下列其中一項：

   - 此資料夾、子資料夾及檔案
   - 此資料夾及子資料夾
   - 僅此資料夾
   - 此資料夾與檔案
   - 僅限子資料夾與檔案
   - 僅子資料夾
   - * 僅檔案 * 如果您要在單一檔案上設定稽核、則「 * 套用至 * 」方塊不會啟用。「套用至」方塊設定預設為*僅此物件*。

   由於稽核需要SVM資源、因此請僅選取提供稽核事件的最低層級、以符合您的安全需求。

10. 在「存取」方塊中、選取您要稽核的項目、以及是否要稽核成功的事件、失敗事件或兩者。
    - 若要稽核成功的事件、請選取「成功」方塊。
    - 若要稽核失敗事件、請選取「失敗」方塊。

      只選取您需要監控的動作、以符合安全性需求。如需這些可稽核事件的詳細資訊、請參閱Windows文件。您可以稽核下列事件：

    - 完全控制

- 周遊資料夾/執行檔案
- 列出資料夾/讀取資料
- 讀取屬性
- 讀取延伸屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入延伸屬性
- 刪除子資料夾與檔案
- 刪除
- 讀取權限
- 變更權限
- 取得所有權

11. 如果不希望稽核設定傳播到原始容器的後續檔案和資料夾、請選取「僅將這些稽核項目套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「 * 套用 * 」。
13. 完成新增、移除或編輯稽核項目之後、請按一下*確定*。

    「<object>的稽核項目」方塊隨即關閉。

14. 在「稽核」方塊中、選取此資料夾的繼承設定。

    只選取提供稽核事件的最低層級、以符合您的安全需求。您可以選擇下列其中一項：

    - 選取[包含來自此物件父物件的可繼承稽核項目]方塊。
    - 選取「使用此物件的可繼承稽核項目來取代所有子系上所有現有的可繼承稽核項目」方塊。
    - 選取兩個方塊。
    - 請選取兩個方塊。 如果您要在單一檔案上設定SACL，則[稽核]方塊中不會出現[以這個物件的可繼承稽核項目取代所有子系上所有現有的可繼承稽核項目]方塊。
15. 按一下「確定」。

    稽核方塊隨即關閉。

使用**ONTAP CLI**設定**NTFS**稽核原則

您可以使用ONTAP CLI在檔案和資料夾上設定稽核原則。這可讓您設定NTFS稽核原則、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以使用設定 NTFS 稽核原則 `vserver security file-directory` 命令系列。

您只能使用CLI設定NTFS SACL。此支援的不支援NFSv4 SACL系列。ONTAP深入瞭解如何使用這些命令來設定 NTFS SACL "指令參考資料ONTAP"，並將其新增至中的檔案和資料夾。

設定 **UNIX** 安全性樣式檔案和目錄的 **ONTAP** 稽核

您可以將稽核ACE新增至NFSv4.x ACL、以設定UNIX安全樣式檔案和目錄的稽核。這可讓您監控特定NFS檔案和目錄存取事件、以確保安全。

關於這項工作

對於NFSv4.x、可自由判斷的ACE和系統的ACE都儲存在相同的ACL中。它們不會儲存在個別的DACL和SACL中。因此、在將稽核ACE新增至現有ACL時、您必須謹慎小心、以免覆寫及遺失現有ACL。將稽核ACE新增至現有ACL的順序並不重要。

步驟

1. 使用擷取檔案或目錄的現有 ACL `nfs4_getfacl` 或等效命令。

   如"指令參考資料ONTAP"需有關操作 ACL 的詳細資訊，請參閱。

2. 附加所需的稽核ACE。
3. 使用將更新的 ACL 套用至檔案或目錄 `nfs4_setfacl` 或等效命令。

顯示套用至檔案和目錄的稽核原則相關資訊

存取 **Windows** 安全性索引標籤，即可檢視 **ONTAP** 稽核原則資訊

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。

顯示 **ONTAP FlexVol** 磁碟區上 **NTFS** 稽核原則的相關資訊

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
```

使用萬用字元顯示 **ONTAP** 檔案安全性和稽核原則的相關資訊

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
```

可稽核的CLI變更事件

瞭解可稽核的 ONTAP CLI 變更事件

可稽核某些CLI變更事件、包括特定SMB共用事件、特定稽核原則事件、特定本機安全性群組事件、本機使用者群組事件、以及授權原則事件。ONTAP瞭解哪些變更事件可稽核、有助於解讀事件記錄的結果。

您可以手動旋轉稽核記錄、啟用或停用稽核、顯示稽核變更事件的相關資訊、修改稽核變更事件、以及刪除稽核變更事件、藉此管理儲存虛擬機器（SVM）稽核CLI變更事件。

身為系統管理員、如果您執行任何命令來變更SMB共用區、本機使用者群組、本機安全性群組、授權原則及稽核原則事件的相關組態、 產生記錄並稽核相應的事件：

稽核類別	活動	事件ID	執行此命令…
主機稽核	原則變更	[4719]稽核組態已變更	`vserver audit disable
enable	modify`	檔案共用	已新增[5142]網路共用

`vserver cifs share create`	[5143]網路共用區已修改	`vserver cifs share modify` `vserver cifs share create`	modify
delete` `vserver cifs share add	remove`	[5144]網路共用區已刪除	`vserver cifs share delete`
稽核	使用者帳戶	[4720]本機使用者已建立	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722]本機使用者已啟用	`vserver cifs users-and-groups local-user create	modify`	[4724]本機使用者密碼重設
`vserver cifs users-and-groups local-user set-password`	[4725]本機使用者已停用	`vserver cifs users-and-groups local-user create	modify`
[4726]本機使用者已刪除	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738]本機使用者變更	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781]本機使用者重新命名	`vserver cifs users-and-groups local-user rename`	安全性群組	[4731]已建立本機安全性群組
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734]本機安全性群組已刪除	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735]本機安全性群組已修改
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732]使用者已新增至本機群組	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`

[4733]使用者已從本機群組中移除	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	授權原則變更	[4704]已指派使用者權限
`vserver cifs users-and-groups privilege add-privilege`	[4705]使用者權限已移除	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

相關資訊

- "Vserver"

管理檔案共用 ONTAP 事件

為儲存虛擬機器（SVM）設定檔案共用事件並啟用稽核時、就會產生稽核事件。使用修改SMB 網路共用時、會產生檔案共用事件 `vserver cifs share` 相關命令。

新增、修改或刪除SVM的SMB網路共用時、會產生事件ID為5142、5143和5144的檔案共用事件。SMB 網路共用組態是使用修改的 `cifs share access control create|modify|delete` 命令。

下列範例顯示建立名為「稽核目的地」的共用物件時、會產生ID為5143的檔案共用事件：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

管理稽核原則變更 ONTAP 事件

當為儲存虛擬機器（SVM）設定稽核原則變更事件並啟用稽核時、就會產生稽核事件。使用修改稽核原則時、會產生稽核原則變更事件 `vserver audit` 相關命令。

每當停用、啟用或修改稽核原則時、就會產生事件ID 4719的稽核原則變更事件、並有助於識別使用者嘗試停用稽核以涵蓋追蹤的時間。此設定預設為設定、需要診斷權限才能停用。

下列範例顯示稽核原則變更事件、並在停用稽核時產生ID 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

管理使用者帳戶 **ONTAP** 事件

當儲存虛擬機器（SVM）的使用者帳戶事件設定為啟用稽核時、就會產生稽核事件。

事件ID為4720、4722、4724、4725、4726、 當本機SMB或NFS使用者從系統建立或刪除、本機使用者帳戶啟用、停用或修改、以及本機SMB使用者密碼重設或變更時、就會產生4738和4781。使用修改使用者帳戶時、會產生使用者帳戶事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令。

下列範例顯示建立本機SMB使用者時產生ID 4720的使用者帳戶事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

下列範例顯示在先前範例中建立的本機SMB使用者重新命名時、產生ID為4781的使用者帳戶事件：

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

管理安全性群組 ONTAP 事件

當儲存虛擬機器（SVM）的安全性群組事件設定為啟用稽核時、就會產生稽核事件。

從系統建立或刪除本機SMB或NFS群組、並從群組新增或移除本機使用者時、會產生事件ID為4731、4732、4733、4734和4735的安全性群組事件。當使用修改使用者帳戶時、就會產生安全性群組事件 `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令。

下列範例顯示建立本機UNIX安全性群組時、產生ID 4731的安全性群組事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

管理授權原則變更 ONTAP 事件

當儲存虛擬機器（SVM）的授權原則變更事件設定為啟用稽核時、就會產生稽核事件。

每當SMB使用者和SMB群組的授權權限被授予或撤銷時、就會產生事件ID為4704和4705的授權原則變更事件。當使用指派或撤銷授權權限時、就會產生授權原則變更事件 `vserver cifs users-and-groups privilege` 相關命令。

下列範例顯示指派SMB使用者群組授權權限時、產生ID 4704的授權原則事件：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

管理稽核組態

手動旋轉稽核事件記錄檔，以檢視特定的 ONTAP SVM 事件記錄

您必須先將記錄轉換成使用者可讀取的格式、才能檢視稽核事件記錄。如果您想要先檢視特定儲存虛擬機器（SVM）的事件記錄、再ONTAP 由SVM自動旋轉記錄、您可以手動旋轉SVM上的稽核事件記錄。

步驟

1. 使用旋轉稽核事件記錄 `vserver audit rotate-log` 命令。

   ```
   vserver audit rotate-log -vserver vs1
   ```

   稽核事件記錄會以稽核組態指定的格式儲存在 SVM 稽核事件記錄目錄中 (`XML` 或 `EVTX`）、並可使用適當的應用程式來檢視。

啟用或停用 ONTAP SVM 上的稽核

您可以在儲存虛擬機器（SVM）上啟用或停用稽核。您可能想要停用稽核功能、暫時停止檔案和目錄稽核。您可以隨時啟用稽核（如果存在稽核組態）。

開始之前

在SVM上啟用稽核之前、SVM的稽核組態必須已經存在。

"建立稽核組態"

關於這項工作

停用稽核不會刪除稽核組態。

步驟

1. 執行適當的命令：

如果您想要稽核...	輸入命令...
已啟用	`vserver audit enable -vserver vserver_name`
已停用	`vserver audit disable -vserver vserver_name`

2. 確認稽核處於所需狀態：

   `vserver audit show -vserver vserver_name`

範例

下列範例可啟用SVM VS1的稽核：

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

下列範例停用SVM VS1的稽核：

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

顯示 ONTAP 稽核組態的相關資訊

您可以顯示稽核組態的相關資訊。這些資訊可協助您判斷每個SVM的組態是否符合您的需求。顯示的資訊也可讓您驗證是否已啟用稽核組態。

關於這項工作

您可以在所有SVM上顯示稽核組態的詳細資訊、也可以指定選用參數來自訂輸出中顯示的資訊。如果您未指定任何選用參數、則會顯示下列項目：

- 稽核組態套用至的SVM名稱
- 稽核狀態、可以是 `true` 或 `false`

  如果稽核狀態為 `true`，已啟用稽核。如果稽核狀態為 `false`，稽核已停用。

- 要稽核的事件類別
- 稽核記錄格式
- 稽核子系統儲存合併及轉換稽核記錄的目標目錄

步驟

1. 使用顯示稽核組態的相關資訊 `vserver audit show` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver audit show`資訊，請參閱。

範例

下列範例顯示所有SVM稽核組態的摘要：

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

下列範例以清單形式顯示所有SVM的所有稽核組態資訊：

```
cluster1::> vserver audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

用於修改稽核組態的 **ONTAP** 命令

如果您想要變更稽核設定、可以隨時修改目前的組態、包括修改記錄路徑目的地和記錄格式、修改要稽核的事件類別、如何自動儲存記錄檔、以及指定要儲存的記錄檔數目上限。

如果您想要...	使用此命令...
修改記錄目的地路徑	`vserver audit modify` 使用 `-destination` 參數
修改要稽核的事件類別	`vserver audit modify` 使用 `-events` 參數 若要稽核集中存取原則暫存事件、必須在儲存虛擬機器（SVM）上啟用動態存取控制（DAC）SMB伺服器選項。
修改記錄格式	`vserver audit modify` 使用 `-format` 參數

根據內部記錄檔大小啟用自動儲存	`vserver audit modify` 使用 `-rotate-size` 參數
根據時間間隔啟用自動儲存	`vserver audit modify` 使用 `-rotate -schedule-month`、`-rotate-schedule -dayofweek`、`-rotate-schedule-day`、`-rotate-schedule-hour`和 `-rotate-schedule-minute` 參數
指定儲存的記錄檔數目上限	`vserver audit modify` 使用 `-rotate-limit` 參數

刪除 ONTAP SVM 上的稽核組態

如果您不想再稽核儲存虛擬機器（SVM）上的檔案和目錄事件、也不想在SVM上維護稽核組態、可以刪除稽核組態。

步驟

1. 停用稽核組態：

   ```
   vserver audit disable -vserver vserver_name

   vserver audit disable -vserver vs1
   ```

2. 刪除稽核組態：

   ```
   vserver audit delete -vserver vserver_name

   vserver audit delete -vserver vs1
   ```

瞭解還原稽核 ONTAP 叢集的影響

如果您打算還原叢集、ONTAP 當叢集中有啟用稽核的儲存虛擬機器（SVM）時、您應該注意下列還原程序。您必須先採取特定行動、才能恢復。

還原ONTAP 至不支援SMB登入和登出事件稽核、以及集中存取原則執行事件的版本

支援SMB登入和登出事件的稽核、以及集中存取原則執行事件、從叢集Data ONTAP 式的版本資訊8.3開始。如果您要回復ONTAP 到不支援這些事件類型的版本、而且您有監控這些事件類型的稽核組態、則必須在還原之前變更這些啟用稽核的SVM的稽核組態。您必須修改組態、以便只稽核檔案作業事件。

疑難排解 ONTAP 稽核和暫存磁碟區空間問題

當暫存磁碟區或包含稽核事件記錄的磁碟區空間不足時、可能會發生問題。如果空間不足、就無法建立新的稽核記錄、這會使用戶端無法存取資料、而且存取要求也會失敗。您應該知道如何疑難排解及解決這些磁碟區空間問題。

疑難排解與事件記錄磁碟區相關的空間問題

如果包含事件記錄檔的磁碟區空間不足、稽核將無法將記錄轉換成記錄檔。這會導致用戶端存取失敗。您必須知道如何疑難排解與事件記錄磁碟區相關的空間問題。

- 儲存虛擬機器（ SVM ）和叢集管理員可以顯示有關 Volume 和 Aggregate 使用率和組態的資訊、藉此判斷是否有足夠的磁碟區空間。
- 如果包含事件記錄的磁碟區空間不足、SVM和叢集管理員可以移除部分事件記錄檔、或是增加磁碟區的大小、來解決空間問題。

> ⓘ 如果包含事件記錄磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有叢集管理員可以增加集合體的大小。

- 事件記錄檔的目的地路徑可透過修改稽核組態、變更為另一個磁碟區上的目錄。

> ⓘ 在下列情況下、資料存取遭拒：
>
> - 目的地目錄即會刪除。
> - 主控目的地目錄的磁碟區上的檔案限制達到其最大層級。

深入瞭解：

- "如何檢視磁碟區的相關資訊、以及增加磁碟區大小"。
- "如何檢視有關集合體與管理集合體的資訊"。

疑難排解與接移磁碟區相關的空間問題

如果任何包含儲存虛擬機器（SVM）暫存檔案的磁碟區空間不足、稽核將無法將記錄寫入暫存檔案。這會導致用戶端存取失敗。若要疑難排解此問題、您必須顯示磁碟區使用量的相關資訊、以判斷SVM中使用的任何暫存磁碟區是否已滿。

如果包含合併事件記錄檔的磁碟區有足夠空間、但由於空間不足、仍有用戶端存取失敗、則暫存磁碟區可能空間不足。SVM管理員必須聯絡您、以判斷內含SVM暫存檔案的暫存磁碟區是否空間不足。如果因暫存磁碟區空間不足而無法產生稽核事件、則稽核子系統會產生EMS事件。畫面會顯示下列訊息： `No space left on device`。只有您可以檢視暫存磁碟區的相關資訊、SVM管理員無法檢視。

所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID 。以下範例顯示管理SVM上的四個系統磁碟區、這些磁碟區是在為叢集中的資料SVM建立檔案服務稽核組態時自動建立的：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

如果暫存磁碟區空間不足、您可以增加磁碟區的大小來解決空間問題。

如果包含暫存磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有您可以增加Aggregate的大小、SVM管理員才能增加。

如果一個或多個集合體的可用空間小於 2GB （在 ONTAP 9.14.1 及更早版本中）或 5GB （從 ONTAP 9.15.1 開始）、則 SVM 稽核建立會失敗。當SVM稽核建立失敗時、所建立的暫存磁碟區會被刪除。