管理稽核組態
ONTAP 9

NetApp
February 12, 2026

目錄

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。

版權資訊

商標資訊