



管理稽核組態

ONTAP 9

NetApp
February 12, 2026

目錄

管理稽核組態	1
手動旋轉稽核事件記錄檔，以檢視特定的 ONTAP SVM 事件記錄	1
啟用或停用 ONTAP SVM 上的稽核	1
顯示 ONTAP 稽核組態的相關資訊	2
用於修改稽核組態的 ONTAP 命令	4
刪除 ONTAP SVM 上的稽核組態	4
瞭解還原稽核 ONTAP 叢集的影響	5
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	5

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 EVT) 、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	<code>vserver audit enable -vserver vserver_name</code>
已停用	<code>vserver audit disable -vserver vserver_name</code>

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	<code>vserver audit modify 使用 -destination 參數</code>
修改要稽核的事件類別	<code>vserver audit modify 使用 -events 參數</code>  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	<code>vserver audit modify 使用 -format 參數</code>
根據內部記錄檔大小啟用自動儲存	<code>vserver audit modify 使用 -rotate-size 參數</code>
根據時間間隔啟用自動儲存	<code>vserver audit modify 使用 -rotate -schedule-month、-rotate-schedule-dayofweek、-rotate-schedule-day、-rotate-schedule-hour 和 -rotate-schedule-minute 參數</code>
指定儲存的記錄檔數目上限	<code>vserver audit modify 使用 -rotate-limit 參數</code>

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

Copyright © 2026 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。