



稽核記錄 ONTAP 9

NetApp
February 12, 2026

目錄

稽核記錄	1
瞭解 ONTAP 稽核記錄實作	1
瞭解 ONTAP 稽核記錄的變更	2
顯示 ONTAP 稽核記錄內容	2
管理 ONTAP 稽核 Get 要求設定	3
啟用ONTAP跨叢集審核	4
啟用或停用跨叢集審計	4
啟用 GET 稽核的效果	5
管理 ONTAP 稽核記錄目的地	5

稽核記錄

瞭解 ONTAP 稽核記錄實作

審計日誌中記錄的管理活動包含在標準AutoSupport報告中，某些日誌記錄活動包含在EMS 訊息中。您也可以將稽核日誌轉送至指定的目標位置，並可使用ONTAP CLI 或 Web 瀏覽器顯示稽核日誌檔案。

從版本的《Sy9.11.1》開始ONTAP、您可以使用System Manager來顯示稽核記錄內容。

從 ONTAP 9.12.1 開始、ONTAP 會針對稽核記錄提供竄改警示。ONTAP 會執行每日背景工作、檢查 audit.log 檔案是否遭到竄改、如果發現任何已變更或竄改的記錄檔、則會傳送 EMS 警示。

從ONTAP 9.17.1 開始，以及從ONTAP 9.16.1 P4 和更高版本的 9.16.1 修補程式版本開始，["還可以記錄使用跨集群操作從對等集群發起的遠端管理活動"](#)。這些活動包括使用者驅動的和源自另一個叢集的內部操作。

ONTAP中記錄的管理活動

ONTAP記錄在叢集上執行的管理活動，例如發出了什麼請求、觸發請求的使用者、使用者的存取方式以及請求的時間。

管理活動可以是以下類型之一：

- **SET 請求：**
 - 這些請求通常適用於非顯示命令或操作。
 - 這些要求會在您執行時發出 `create`、`modify` 或 `delete` 例如命令。
 - 預設會記錄 SET 請求。
- **GET 請求：**
 - 這些請求檢索資訊並將其顯示在管理介面中。
 - 這些要求會在您執行時發出 `show` 例如命令。
 - 預設不會記錄 GET 請求，但您可以控制是否從ONTAP CLI 發送 GET 請求(`-cliget`)，來自ONTAP API (`-ontapiget`)，或透過ONTAP REST API (`-httpget`) 記錄在文件中。

審計日誌記錄和輪換

ONTAP記錄管理活動 `/mroot/etc/log/mlog/audit.log` 節點的檔案。CLI指令 (`clustershell`、`nodeshell` 和非互動式 `systemshell`) 以及 API 指令均記錄在此。互動式 `systemshell` 指令不記錄。稽核日誌包含時間戳，用於顯示叢集中所有節點是否同步。

◦ `audit.log` 檔案是由 AutoSupport 工具傳送給指定的收件者。您也可以將內容安全地轉送到您指定的外部目的地、例如Splunk或syslog伺服器。

◦ `audit.log` 檔案會每日旋轉。當檔案大小達到100 MB時、也會進行旋轉、並保留先前的48個複本（最多總共49個檔案）。稽核檔案執行每日旋轉時、不會產生任何EMS訊息。如果稽核檔案因為超過檔案大小限制而旋轉、則會產生EMS訊息。

啟用 GET 稽核時，請考慮設定日誌轉發，以避免因日誌快速輪替而導致資料遺失。有關更多信息，請參閱以下知識庫文章：["啟用稽核日誌轉發"](#)。

瞭解 ONTAP 稽核記錄的變更

從 ONTAP 9 開始 `command-history.log` 檔案取代為 `audit.log` 和 `mgwd.log` 檔案不再包含稽核資訊。如果您要升級 ONTAP 至 VMware 版、請檢閱任何參考舊版檔案及其內容的指令碼或工具。

升級至 ONTAP 9 之後、即為現有的 `command-history.log` 檔案會保留。它們會以新的方式旋轉（刪除）
`audit.log` 檔案會在中旋轉（建立）。

檢查的工具和指令碼 `command-history.log` 檔案可能會繼續運作、因為有的軟式連結 `command-history.log` 至 `audit.log` 在升級時建立。不過、檢查的工具和指令碼 `mgwd.log` 檔案將會失敗、因為該檔案不再包含稽核資訊。

此外、由於下列項目不被視為有用、導致不必要的記錄活動、因此在更新版本的版本中、不再包含稽核記錄：
ONTAP

- 內部命令由 ONTAP 執行（也就是、其中 `username=root`）
- 命令別名（與指向的命令分開）

從 ONTAP 功能支援的第 9 部分開始、您可以使用 TCP 和 TLS 傳輸協定、將稽核記錄安全地傳輸到外部目的地。

顯示 ONTAP 稽核記錄內容

您可以顯示叢集的內容 `/mroot/etc/log/mlog/audit.log` 使用 ONTAP CLI、系統管理員或網頁瀏覽器來建立檔案。

叢集的記錄檔項目包括：

時間

記錄項目時間戳記。

應用程式

用於連線至叢集的應用程式。可能值的範例包括 `internal`、`console`、`ssh http ontapi`、`snmp`、`rsh telnet` 和 `service-processor`。

使用者

遠端使用者的使用者名稱。

州/省

稽核要求的目前狀態，可以是 `success`、`pending` 或 `error`。

訊息

可選欄位、其中可能包含錯誤或命令狀態的其他資訊。

工作階段 ID

接收要求的工作階段 ID。每個 SSH、S 階段、作業、都會指派一個工作階段 ID、而每個 HTTP、ONTAPI 或 SNMP、_REQUER_ 都會指派一個唯一的工作階段 ID。

儲存 VM

使用者連線的SVM。

範圍

顯示 svm 當要求位於資料儲存 VM 上時、否則會顯示 cluster。

命令ID

在CLI工作階段中收到的每個命令的ID。這可讓您建立要求與回應的關聯。ZAPI、HTTP和SNMP要求沒有命令ID。

您可以從ONTAP「系統ONTAP 管理員」的「系統管理程式」中、從「系統瀏覽器」、以「版本9.11.1」開頭、從「版本資訊」CLI顯示叢集的記錄項目。

系統管理員

- 若要顯示詳細目錄、請選取*事件與工作>稽核記錄*。+ 每一欄都有篩選、排序、搜尋、顯示和庫存類別的控制項。詳細目錄可下載為Excel活頁簿。
- 若要設定篩選條件、請按一下右上方的 * 篩選 * 按鈕、然後選取所需的欄位。+ 您也可以按一下工作階段 ID 連結、檢視在發生故障的工作階段中執行的所有命令。

CLI

若要顯示從叢集中多個節點合併的稽核項目，請輸入：

```
security audit log show <[parameters]>
```

您可以使用 `security audit log show` 命令來顯示個別節點的稽核項目，或是從叢集中的多個節點合併。您也可以使用 Web 瀏覽器，在單一節點上顯示目錄內容 `/mroot/etc/log/mlog`。如["指令參考資料ONTAP"](#)需詳細 `security audit log show` 資訊，請參閱。

網頁瀏覽器


您可以使用 Web 瀏覽器，在單一節點上顯示目錄內容 `/mroot/etc/log/mlog`。"瞭解如何使用網頁瀏覽器存取節點的記錄檔，核心傾印和 MIB 檔案"。

管理 ONTAP 稽核 Get 要求設定

雖然預設會記錄設定要求、但不會記錄取得要求。不過、您可以控制是否從 ONTAP HTML 傳送 GET 要求 (`-httpget`)、ONTAP CLI (`-cliget`) 或 ONTAP API (`-ontapiget`) 會記錄在檔案中。

您可以從ONTAP「系統ONTAP 管理程式」修改稽核記錄設定、從「系統管理程式」開始修改從「版本9.11.1」開始的記錄。

系統管理員

1. 選擇*事件與工作>稽核記錄*。
2. 按一下  右上角的、然後選擇要新增或移除的要求。

CLI

- 若要指定從 ONTAP CLI 或 API 取得要求應記錄在稽核記錄檔（audit.log 檔案）中、除了預設的 Set 要求外、請輸入：

```
security audit modify [-cliget {on|off}][--httpget {on|off}][--ontapiget {on|off}]
```
- 若要顯示目前的設定、請輸入：

```
security audit show
```

如"[指令參考資料ONTAP](#)"需詳細 `security audit show` 資訊，請參閱。

啟用ONTAP跨叢集審核

從ONTAP 9.17.1 以及ONTAP 9.16.1 P4 和更高版本的 9.16.1 修補程式版本開始，您可以在ONTAP中啟用跨叢集稽核功能，以記錄從對等叢集發起的操作。這種遠端審計功能在多個ONTAP叢集互動的環境中尤其有用，可以提供遠端操作的可追溯性和責任追究。

跨集群審計可以區分用戶發起的 GET（讀取）或 SET（建立/修改/刪除）操作。預設情況下，目標群集僅會審計使用者發起的 SET 操作。任何讀取資料的請求，例如 GET 或 show CLI 中的命令，無論請求是否跨集群，預設都不會受到審核。

開始之前

- 你必須有 `advanced` 等級權限
- 此叢集必須與另一個叢集對等，且兩個叢集都必須執行ONTAP 9.16.1 P4 或更高版本。



在部分節點（而非所有節點）升級到ONTAP 9.16.1 P4 或更高版本的環境中，稽核日誌記錄僅在執行升級版本的節點上進行。建議將所有節點升級到受支援的版本，以確保一致的審計行為。

啟用或停用跨叢集審計

步驟

1. 透過設定 cluster-peer 參數 `on` 或者 `off`：

```
security audit modify -cluster-peer {on|off}
```

2. 透過檢查目前審核狀態來確認叢集對等設定是啟用還是停用：

```
security audit show
```

回覆:

```
Audit Setting State
-----
      CLI GET: off
      HTTP GET: off
      ONTAPI GET: off
Cluster Peer: on
```

啟用 GET 稽核的效果

從ONTAP 9.17.1 開始，如果您 **"啟用 CLI、HTTP、ONTAPI GET 審計"**在對等叢集上，您也可以啟用對跨叢集使用者發起的 GET 請求的審核。在早期ONTAP版本中，GET 審核僅適用於本機叢集上的請求。在ONTAP 9.17.1 中，如果您使用 `cluster-peer`` 選項設定為 ``on``，本地集群和跨集群請求都將被審核。

管理 ONTAP 稽核記錄目的地

您最多可將稽核記錄轉送至10個目的地。例如、您可以將記錄轉送至Splunk或syslog伺服器、以供監控、分析或備份之用。

關於這項工作

若要設定轉送、您必須提供syslog或Splunk主機的IP位址、其連接埠號碼、傳輸傳輸傳輸傳輸協定、以及用於轉送記錄的syslog工具。 **"深入瞭解syslog工具"**。

您可以使用 ``-protocol`` 參數選取下列其中一個傳輸值：

未加密的udp

無安全性的使用者資料包傳輸協定（預設）

TCP未加密

傳輸控制傳輸協定、無安全性

TCP加密

傳輸層安全性（ TLS ） + 的傳輸控制傳輸協定 選取 TCP 加密傳輸協定時、可使用 * 驗證伺服器 * 選項。

預設連接埠為 514 （用於 UDP ） 、 6514 （用於 TCP ） 、但您可以指定任何符合網路需求的連接埠。

您可以使用 ``-message-format`` 命令選取下列其中一種訊息格式：

舊版 NetApp

RFC-3164 Syslog 格式的變化（格式： <PRIVAL> TAIMP 主機名稱： MSG ）




RFC-5424

根據 RFC-5424 格式的系統記錄格式（格式： <PRIVAL> 資料處理時間戳主機名稱： MSG ）

您可以從ONTAP 「系統ONTAP 管理程式」從「功能性CLI」轉寄稽核記錄、從「功能性功能」開始、從「功能

性功能」開始。

系統管理員

- 若要顯示稽核記錄目的地、請選取*叢集>設定*。+*通知管理方塊*會顯示記錄目的地的計數。按一下  以顯示詳細資料。
- 若要新增、修改或删除稽核記錄目的地、請選取*事件與工作>稽核記錄*、然後按一下畫面右上角的*管理稽核目的地*。+ 按一下  Add、或按一下  *主機位址*欄、以編輯或删除項目。

CLI

1. 針對您要轉送稽核記錄的每個目的地、指定目的地IP位址或主機名稱及任何安全性選項。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

- 如果是 cluster log-forwarding create 命令無法 ping 目的主機以驗證連線、命令失敗並顯示錯誤。雖然不建議使用、但請使用 -force 使用命令的參數會略過連線驗證。
 - 當您設定時 -verify-server 參數至 true，記錄轉送目的地的身分識別是透過驗證其憑證來驗證。您可以將值設為 true 僅當您選取時 tcp-encrypted 中的值 -protocol 欄位。
2. 使用驗證目的地記錄是否正確 cluster log-forwarding show 命令。

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	6514	tcp-encrypted	true	user

2 entries were displayed.

相關資訊

- ["叢集記錄轉送顯示"](#)
- ["建立叢集記錄轉送"](#)

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。