稽核記錄
ONTAP 9

NetApp
September 12, 2024

目錄

稽核記錄

如何執行稽核記錄ONTAP

稽核日誌中記錄的管理活動會包含在標準AutoSupport 版的功能表報告中、而EMS訊息中也會包含某些記錄活動。您也可以將稽核記錄轉送到指定的目的地、並使用CLI或Web瀏覽器來顯示稽核記錄檔。

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。

系統會記錄叢集上執行的管理活動、例如發出的要求、觸發要求的使用者、使用者的存取方法、以及要求的時間。ONTAP

管理活動可以是下列其中一種類型：

- 設定要求、通常適用於非顯示命令或作業：
  - 這些要求會在您執行時發出 `create`、 `modify`或 `delete` 例如命令。
  - 預設會記錄設定要求。
- 取得要求、以擷取資訊並顯示在管理介面中：
  - 這些要求會在您執行時發出 `show` 例如命令。
  - 依預設不會記錄 GET 要求、但您可以控制是否從 ONTAP CLI 傳送 GET 要求 (`-cliget`）、來自 ONTAP API (`-ontapiget`）、或來自 REST API (`-httpget`）會記錄在檔案中。

ONTAP 會在中記錄管理活動 `/mroot/etc/log/mlog/audit.log` 節點的檔案。這裏記錄了三個Shell中用於CLI命令的命令（即clusterShell、nodesell和非交互式系統Shell（不記錄交互式系統Shell命令）以及API命令。稽核記錄包含時間戳記、可顯示叢集中的所有節點是否都同步時間。

。 `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。

變更以稽核ONTAP 記錄功能。9.

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。可能的值範例如下 `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、可能是 `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` 用於顯示個別節點的稽核項目、或是從叢集中的多個節點合併的命令。您也可以顯示的內容 `/mroot/etc/log/mlog` 使用 Web 瀏覽器在單一節點上建立目錄。 如需詳細資料、請參閱手冊頁。

網頁瀏覽器

您可以顯示的內容 `/mroot/etc/log/mlog` 使用 Web 瀏覽器在單一節點上建立目錄。 "瞭解如何使用網頁瀏覽器存取節點的記錄檔、核心傾印檔和MIBA檔案"。

管理稽核取得要求設定

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
  ```

如需詳細資料、請參閱手冊頁。

管理稽核記錄目的地

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。

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、修改或刪除稽核記錄目的地、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、以編輯或刪除項目。

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 514 -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

                                                    Verify Syslog
Destination Host           Port   Protocol         Server Facility
-------------------------- ------ --------         ------ --------
192.168.123.96             514    udp-unencrypted false  user
192.168.123.98             514    tcp-encrypted   true   user
2 entries were displayed.
```

如需詳細資料、請參閱手冊頁。