稽核的運作方式
ONTAP 9

NetApp
February 12, 2026

目錄

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。

版權資訊

商標資訊