稽核記錄

Active IQ Unified Manager 9.9

NetApp
December 15, 2023

目錄

稽核記錄

您可以使用稽核日誌來偵測稽核日誌是否已洩漏。使用者執行的所有活動都會受到監控、並記錄在稽核記錄中。稽核是針對Active IQ Unified Manager 所有使用者介面及公開API功能執行的、

您可以使用「稽核記錄：檔案檢視」來檢視Active IQ Unified Manager 及存取您的無法使用的所有稽核記錄檔。稽核記錄：檔案檢視中的檔案會根據建立日期列出。此檢視會顯示從安裝或升級到系統中現有的所有稽核記錄的資訊。每當您在Unified Manager中執行動作時、資訊都會更新、並可在記錄中使用。每個記錄檔的狀態都是使用「檔案完整性狀態」屬性擷取、該屬性會主動受到監控、以偵測記錄檔的竄改或刪除。稽核日誌可在系統中使用時、具有下列其中一種狀態：

州/省	說明
使用中	記錄目前所在的檔案。
正常	非作用中、已壓縮並儲存在系統中的檔案。
遭竄改	已遭手動編輯檔案之使用者破壞的檔案。
手冊刪除	已由授權使用者刪除的檔案。
指標移轉刪除	因為根據循環組態原則進行復原而刪除的檔案。
Unexpected刪除	因為不明原因而刪除的檔案。

「稽核記錄」頁面包含下列命令按鈕：

- 設定
- 刪除
- 下載

「刪除」按鈕可讓您刪除「稽核記錄」檢視中所列的任何稽核記錄。您可以刪除稽核記錄、並選擇性地提供刪除檔案的理由、以便日後判斷有效刪除。原因欄會列出原因、以及執行刪除作業的使用者名稱。

> 刪除記錄檔會導致從系統刪除檔案、但不會刪除資料庫表格中的項目。

您可以Active IQ Unified Manager 使用「稽核記錄」區段中的「下載」按鈕、從更新下載稽核記錄檔、然後匯出稽核記錄檔。標示為「正常」或「竄改」的檔案會以壓縮格式下載 `.gzip` 格式。

當產生完整AutoSupport 的支援套件組合時、支援套件會同時包含已歸檔和作用中的稽核記錄檔。但是當產生輕度支援套件時、它只會包含作用中的稽核記錄。不包含歸檔的稽核記錄。

設定稽核記錄

您可以使用「稽核記錄」區段中的「設定」按鈕來設定稽核記錄檔的循環原則、以及啟用稽核記錄的遠端記錄。

關於這項工作

您可以根據想要儲存在系統中的資料數量和頻率、設定* MAX檔案大小*和*稽核記錄保留天數*中的值。字段*總稽核日誌大小*中的值是系統中目前稽核日誌資料總數的大小。復原原則取決於*稽核記錄保留天數*、* MAX檔案大小*及*稽核記錄總大小*欄位中的值。當稽核日誌備份的大小達到*總稽核日誌大小*所設定的值時、會刪除先歸檔的檔案。這表示會刪除最舊的檔案。但檔案項目仍可在資料庫中使用、並標示為「滾存刪除」。「稽核記錄保留天數」值是保留稽核記錄檔的天數。超過此欄位中設定值的任何檔案都會被復原。

步驟

1. 按一下*稽核記錄*>**>*組態。
2. 在* MAX檔案大小*、*稽核記錄總大小*和*稽核記錄保留天數*中輸入值。

   如果您要啟用遠端記錄、則應選取*啟用遠端記錄*。

啟用遠端記錄稽核記錄

您可以選取「設定稽核記錄」對話方塊上的「*啟用遠端記錄」核取方塊、以啟用遠端稽核記錄。您可以使用此功能將稽核記錄傳輸到遠端Syslog伺服器。如此一來、您就能在空間有限時管理稽核記錄。

關於這項工作

遠端記錄稽核日誌可在Active IQ Unified Manager 監查伺服器上的稽核日誌檔遭到竄改時、提供防竄改備份。

步驟

1. 在「設定稽核記錄」對話方塊中、選取「啟用遠端記錄」核取方塊。

   顯示用於設定遠端記錄的其他欄位。

2. 輸入您要連線的遠端伺服器*主機名稱*和*連接埠*。
3. 在*伺服器CA憑證*欄位中、按一下*瀏覽*以選取目標伺服器的公開憑證。

   憑證應上傳至 `.pem` 格式。此憑證應從目標Syslog伺服器取得、且不應過期。憑證應包含所選的「主機名稱」、作為的一部分 `SubjectAltName` （SAN）屬性。

4. 輸入下列欄位的值：字元集、連線逾時、重新連線延遲。

   這些欄位的值應以毫秒為單位。

5. 在*格式*和*傳輸協定*欄位中選取所需的Syslog格式和TLS傳輸協定版本。

6. 如果目標Syslog伺服器需要憑證型驗證、請選取「啟用用戶端驗證」核取方塊。

   您必須先下載用戶端驗證憑證、然後將其上傳至Syslog伺服器、再儲存稽核記錄組態、否則連線將會失敗。視Syslog伺服器類型而定、您可能需要建立用戶端驗證憑證的雜湊。

   範例：SysLog NG需要使用命令建立憑證的<雜湊> `openssl x509 -noout -hash -in cert.pem`然後您應該以符號方式將用戶端驗證憑證連結至以<hash>.0命名的檔案。

7. 按一下「儲存」以設定與伺服器的連線、並啟用遠端記錄。

   您將被重新導向至「稽核記錄」頁面。