



稽核記錄

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目錄

稽核記錄	1
設定稽核記錄	2
啟用遠端記錄稽核記錄	2

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 及存取您的整個過程中的所有稽核記錄檔。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。

稽核記錄檔會定期歸檔、並儲存至資料庫以供參考。在歸檔之前、稽核記錄會經過數位簽署、以維持安全性和完整性。

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。

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>*設定*」。
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。

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。



- 連線逾時 * 值可能會影響組態。如果組態回應所需的時間比定義的值長、可能會因為連線錯誤而導致組態失敗。若要建立成功的連線、請增加 * 連線逾時 * 值、然後再試一次組態。

版權資訊

Copyright © 2023 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。