



稽核訊息總覽

StorageGRID 11.5

NetApp
April 11, 2024

目錄

稽核訊息總覽	1
稽核訊息流程與保留	1
變更稽核訊息層級	4
存取稽核記錄檔	6
稽核記錄檔輪替	6

稽核訊息總覽

這些指示包含StorageGRID 有關不稽核訊息和稽核記錄的結構和內容資訊。您可以使用此資訊來讀取及分析系統活動的稽核記錄。

這些指示適用於負責製作系統活動和使用報告的系統管理員、這些報告需要分析StorageGRID 整個系統的稽核訊息。

我們假設您已充分瞭解StorageGRID 到在這個系統內進行稽核活動的性質。若要使用文字記錄檔、您必須擁有管理節點上已設定之稽核共用的存取權。

相關資訊

["管理StorageGRID"](#)

稽核訊息流程與保留

所有StorageGRID 的支援服務都會在正常系統運作期間產生稽核訊息。您應該瞭解這些稽核訊息是如何在StorageGRID 整個過程中、透過整個系統移至 `audit.log` 檔案：

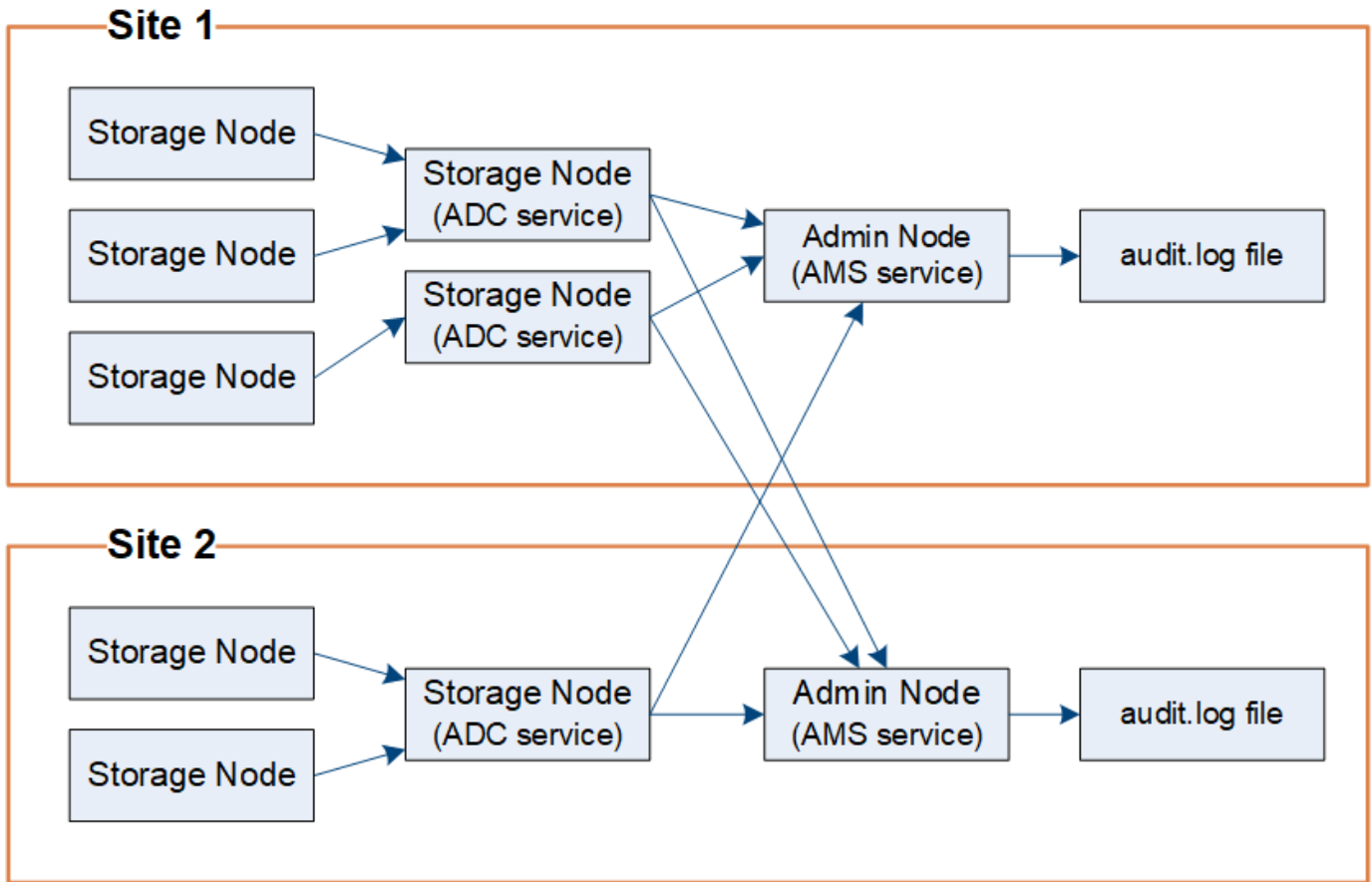
稽核訊息流程

稽核訊息由管理節點和具有管理網域控制器（ADC）服務的儲存節點處理。

如稽核訊息流程圖所示、每StorageGRID 個節點都會將稽核訊息傳送至資料中心站台的其中一個ADC服務。每個站台上安裝的前三個儲存節點會自動啟用「ADC」服務。

接著、每個ADC服務會做為中繼、並將其稽核訊息集合傳送到StorageGRID 整個系統的每個管理節點、讓每個管理節點都能完整記錄系統活動。

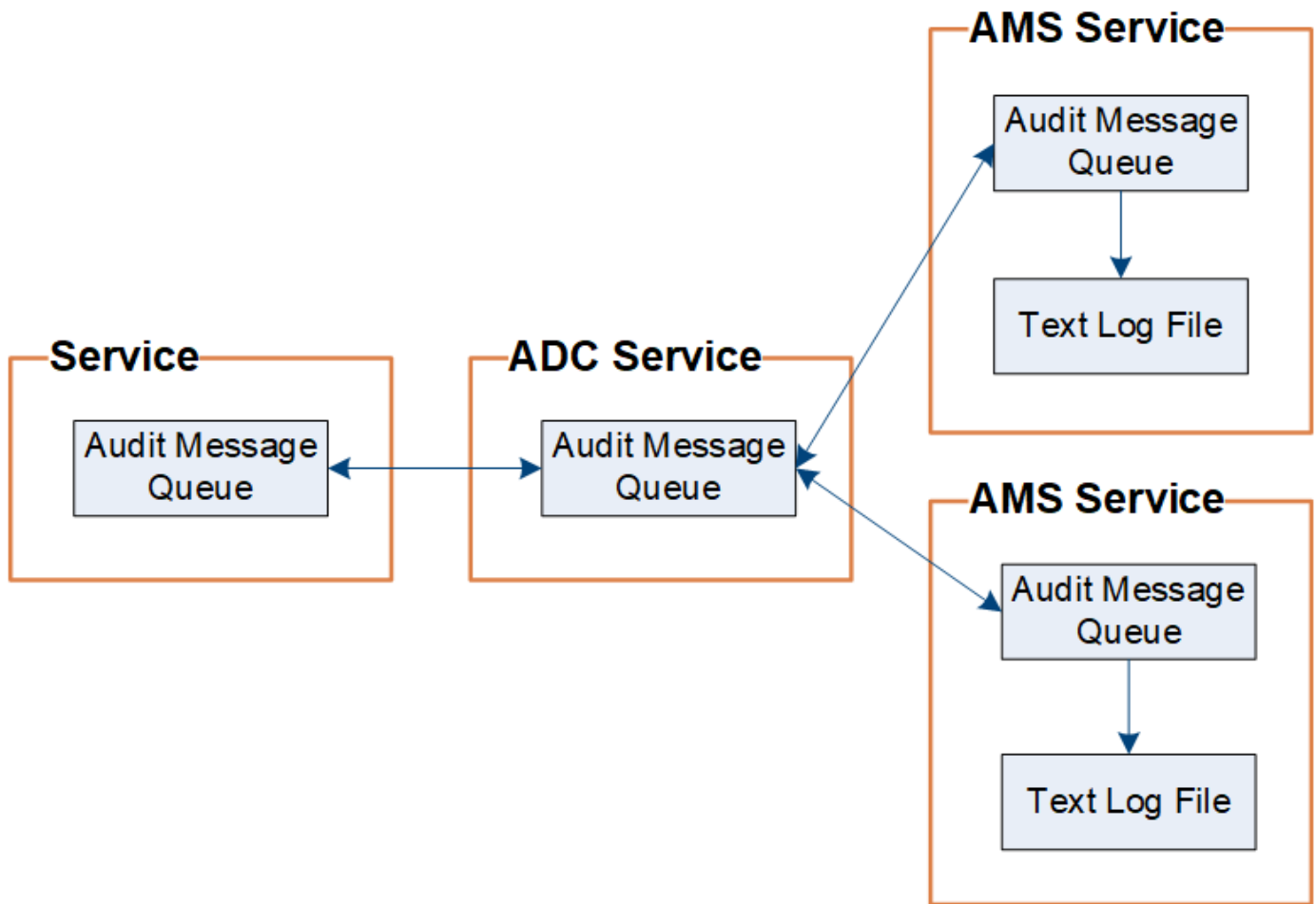
每個管理節點都會將稽核訊息儲存在文字記錄檔中、而作用中的記錄檔則會命名為 `audit.log`。



稽核訊息保留

使用複製與刪除程序、確保不會遺失任何稽核訊息、然後再寫入稽核記錄。StorageGRID

當節點產生或轉送稽核訊息時、該訊息會儲存在網格節點系統磁碟的稽核訊息佇列中。訊息複本一律會保留在稽核訊息佇列中、直到訊息寫入管理節點的稽核記錄檔為止 /var/local/audit/export 目錄。這有助於避免在傳輸期間遺失稽核訊息。



稽核訊息佇列可能因為網路連線問題或稽核容量不足而暫時增加。隨著佇列增加、它們會佔用每個節點的更多可用空間 `/var/local/` 目錄。如果問題持續發生、而且節點的稽核訊息目錄太滿、則個別節點會優先處理其待處理項目、並暫時無法接收新訊息。

具體而言、您可能會看到下列行為：

- 如果是 `/var/local/audit/export` 管理節點所使用的目錄已滿、管理節點將被標記為無法用於新的稽核訊息、直到目錄不再滿為止。S3和Swift用戶端要求不受影響。當稽核儲存庫無法連線時、會觸發XAMS（無法連線的稽核儲存庫）警示。
- 如果是 `/var/local/` 儲存節點與ADC服務搭配使用的目錄已滿92%、節點將被標記為無法稽核訊息、直到目錄只滿87%為止。S3和Swift用戶端對其他節點的要求不受影響。當稽核中繼無法連線時、會觸發NRLY（可用的稽核中繼）警示。



如果沒有可用的儲存節點搭配ADC服務、儲存節點會將稽核訊息儲存在本機。

- 如果是 `/var/local/` 儲存節點使用的目錄已滿85%、節點將開始拒絕S3和Swift用戶端要求 503 Service Unavailable。

下列類型的問題可能導致稽核訊息佇列變得非常龐大：

- 管理節點或儲存節點與ADC服務的中斷。如果其中一個系統節點當機、其餘節點可能會變成回溯記錄。
- 超過系統稽核容量的持續活動率。

- `/var/local/` 由於與稽核訊息無關的原因、導致某個ADC儲存節點上的空間變滿。發生這種情況時、節點會停止接受新的稽核訊息、並優先處理其目前的待處理項目、這可能會導致其他節點發生待處理。

大型稽核佇列警示和稽核訊息佇列 (AMQS) 警示

為了協助您監控一段時間內稽核訊息佇列的大小、當儲存節點佇列或管理節點佇列中的訊息數目達到特定臨界值時、就會觸發*大型稽核佇列*警示和舊版AMQS警示。

如果觸發*大型稽核佇列*警示或舊版AMQS警示、請先檢查系統負載、如果最近發生大量交易、警示和警示應會隨著時間而解除、並可予以忽略。

如果警示或警示持續存在並增加嚴重性、請檢視佇列大小的圖表。如果數在數小時或數天內持續增加、則稽核負載可能超過系統的稽核容量。將用戶端寫入和用戶端讀取的稽核層級變更為「錯誤」或「關閉」、以降低用戶端作業率或減少記錄的稽核訊息數。請參閱[變更稽核訊息層級](#)。」

重複的訊息

如果發生網路或節點故障、StorageGRID 那麼這個系統會採取保守的方法。因此、稽核記錄中可能會出現重複的訊息。

變更稽核訊息層級

您可以調整稽核層級、以增加或減少稽核記錄中每個稽核訊息類別的稽核訊息數量。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有特定的存取權限。

關於這項工作

稽核日誌中記錄的稽核訊息會根據「組態>*監控*>*稽核*」頁面上的設定進行篩選。

您可以針對下列每個訊息類別設定不同的稽核層級：

- 系統：此層級預設為正常。
- * Storage *：此層級預設為「錯誤」。
- 管理：依預設、此層級設為正常。
- 用戶端讀取：此層級預設為「正常」。
- 用戶端寫入：此層級預設為正常。



如果您最初使用StorageGRID 版本10.3或更新版本安裝了這些預設值、則適用這些預設值。如果您已從StorageGRID 舊版的更新版本進行升級、則所有類別的預設值都會設為「正常」。



在升級期間、稽核層級的組態將無法立即生效。

步驟

1. 選擇*組態*>*監控*>*稽核*。

Audit

Audit Levels

System	<input type="text" value="Normal"/>
Storage	<input type="text" value="Error"/>
Management	<input type="text" value="Normal"/>
Client Reads	<input type="text" value="Normal"/>
Client Writes	<input type="text" value="Normal"/>

Audit Protocol Headers

Header Name 1	<input type="text" value="X-Forwarded-For"/>	✕
Header Name 2	<input type="text" value="x-amz-*"/>	+ ✕

Save

- 針對每個稽核訊息類別、從下拉式清單中選取稽核層級：

稽核層級	說明
關	不會記錄任何類別的稽核訊息。
錯誤	僅記錄錯誤訊息、稽核結果代碼「不成功」(SUCS)的訊息。
正常	記錄標準交易訊息：此類別的說明中所列訊息。
偵錯	已過時。此層級的行為與正常稽核層級相同。

針對任何特定層級所包含的訊息、包括將記錄在較高層級的訊息。例如、「正常」層級包含所有的錯誤訊息。

- 在「稽核傳輸協定標頭」下、輸入要包含在「用戶端讀取」和「用戶端寫入」稽核訊息中的HTTP要求標頭名稱。使用星號(*)做為萬用字元、或使用轉義序列(*)做為文字星號。按一下加號以建立標題名稱欄位清單。



稽核傳輸協定標頭僅適用於S3和Swift要求。

在要求中找到這類HTTP標頭時、這些標頭會包含在稽核訊息的「HTRH」欄位中。



僅當*用戶端讀取*或*用戶端寫入*的稽核層級不是*關閉*時、才會記錄稽核傳輸協定要求標頭。

4. 按一下「*儲存*」。

相關資訊

["系統稽核訊息"](#)

["物件儲存稽核訊息"](#)

["管理稽核訊息"](#)

["用戶端讀取稽核訊息"](#)

["管理StorageGRID"](#)

存取稽核記錄檔

稽核共用包含作用中的 `audit.log` 檔案及任何壓縮的稽核記錄檔。若要輕鬆存取稽核記錄、您可以設定用戶端存取NFS和CIFS的稽核共用（已過時）。您也可以直接從管理節點的命令列存取稽核記錄檔。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有 `Passwords.txt` 檔案：
- 您必須知道管理節點的IP位址。

步驟

1. 登入管理節點：
 - a. 輸入下列命令：`ssh admin@primary_Admin_Node_IP`
 - b. 輸入中所列的密碼 `Passwords.txt` 檔案：
2. 移至包含稽核記錄檔的目錄：

```
cd /var/local/audit/export
```

3. 視需要檢視目前或已儲存的稽核記錄檔。

相關資訊

["管理StorageGRID"](#)

稽核記錄檔輪替

稽核記錄檔會儲存至管理節點的 `/var/local/audit/export` 目錄。作用中的稽核記錄檔會命名為 `audit.log`。

一天一次、活動 `audit.log` 檔案已儲存、且是新的 `audit.log` 檔案已啟動。儲存檔案的名稱會以格式指出儲存時間 `yyyy-mm-dd.txt`。如果在一天內建立多個稽核記錄、則檔案名稱會使用檔案儲存的日期、加上數字、格式如下 `yyyy-mm-dd.txt.n`。例如、`2018-04-15.txt` 和 `2018-04-15.txt.1` 是2018年4月15日建立並儲存的第一個和第二個記錄檔。

一天後、儲存的檔案會以壓縮格式重新命名 `yyyy-mm-dd.txt.gz`，保留原始日期。隨著時間推移、這會導致分配給管理節點上稽核記錄的儲存空間使用量。指令碼會監控稽核記錄空間使用量、並視需要刪除記錄檔、以釋出中的空間 `/var/local/audit/export` 目錄。稽核日誌會根據建立日期刪除、而最舊的則會先刪除。您可以在下列檔案中監控指令碼的動作：`/var/local/log/manage-audit.log`。

此範例顯示使用中的 `audit.log` 檔案、前一天的檔案 (`2018-04-15.txt`)、以及前一天的壓縮檔案 (`2018-04-14.txt.gz`)。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

版權資訊

Copyright © 2024 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。