設定稽核訊息和記錄目的地

StorageGRID 11.8

NetApp
May 10, 2024

目錄

設定稽核訊息和記錄目的地

使用外部 **Syslog** 伺服器的考量事項

外部syslog伺服器是StorageGRID 指不屬於功能區的伺服器、可用來在單一位置收集系統稽核資訊。使用外部 Syslog 伺服器可減少管理節點上的網路流量、並更有效率地管理資訊。對於 StorageGRID 、輸出系統記錄訊息封包格式符合 RFC 3164 。

您可以傳送至外部syslog伺服器的稽核資訊類型包括：

- 稽核日誌包含正常系統作業期間所產生的稽核訊息
- 安全性相關事件、例如登入和升級至root
- 如果需要開啟支援案例來疑難排解您遇到的問題、可能會要求的應用程式記錄

何時使用外部 **Syslog** 伺服器

如果您有大型網格、使用多種 S3 應用程式、或想要保留所有稽核資料、外部 Syslog 伺服器就特別有用。將稽核資訊傳送至外部syslog伺服器、可讓您：

- 更有效率地收集和管理稽核資訊、例如稽核訊息、應用程式記錄和安全事件。
- 減少管理節點上的網路流量、因為稽核資訊會直接從各種儲存節點傳輸到外部 Syslog 伺服器、而無需透過管理節點。

> 當記錄傳送至外部 Syslog 伺服器時、訊息結尾處會截斷大於 8 、 192 位元組的單一記錄、以符合外部 Syslog 伺服器實作的一般限制。

> 為了在外部 Syslog 伺服器發生故障時最大化完整資料恢復選項、最多可有 20 GB 的稽核記錄本機記錄 (`localaudit.log`) 會在每個節點上進行維護。

如何設定外部 **Syslog** 伺服器

若要瞭解如何設定外部 Syslog 伺服器、請參閱 "設定稽核訊息和外部 Syslog 伺服器"。

如果您打算設定使用 TLS 或 RELP/TLS 通訊協定、則必須擁有下列憑證：

- * 伺服器 CA 憑證 * ：一或多個信任的 CA 憑證、用於驗證以 PEM 編碼的外部 Syslog 伺服器。如果省略、則會使用預設的Grid CA憑證。
- * 用戶端憑證 * ：用戶端憑證、用於以 PEM 編碼驗證外部 Syslog 伺服器。
- * 用戶端私密金鑰 * ：用戶端憑證的私密金鑰、採用 PEM 編碼。

> 如果您使用用戶端憑證、也必須使用用戶端私密金鑰。如果您提供加密的私密金鑰、也必須提供密碼。使用加密的私密金鑰並無顯著的安全效益、因為必須儲存金鑰和通關密碼；建議使用未加密的私密金鑰（若有）、以簡化操作。

如何預估外部**syslog**伺服器的大小

一般而言、網格的大小可達到所需的處理量、定義為每秒S3作業量或每秒位元組數。例如、您可能需要網格處理每秒1、000次S3作業、或每秒2、000 MB的物件擷取和擷取作業。您應該根據網格的資料需求來調整外部syslog伺服器的大小。

本節提供一些啟發式公式、可協助您預估外部syslog伺服器需要處理的各種類型的記錄訊息速率和平均大小、以網格的已知或所需效能特性表示（每秒S3作業數）。

在預估公式中使用**S3**作業/秒

如果網格的處理量大小是以每秒位元組數表示、您必須將此規模轉換為每秒S3作業、才能使用估計公式。若要轉換網格處理量、您必須先判斷平均物件大小、以便使用現有稽核記錄和指標（如果有）中的資訊、或是運用您對StorageGRID 使用物件的應用程式所擁有的知識。例如、如果您的網格大小達到每秒2、000 MB的處理量、而且平均物件大小為2 MB、那麼您的網格大小就能處理每秒1、000次S3作業（2、000 MB / 2 MB）。

> ⓘ 下列各節中的外部syslog伺服器規模調整公式提供一般案例預估（而非最糟案例預估）。視組態和工作負載而定、系統記錄訊息或系統記錄資料量的速率可能高於或低於公式所預測的速率。公式只能用作準則。

稽核記錄的估計公式

如果您沒有S3工作負載的相關資訊、而非預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的稽核記錄數量： 假設您將「稽核層級」設為預設值（所有類別均設為「正常」、但「儲存設備」設為「錯誤」除外）：

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒2、000個syslog訊息、而且應能以每秒1.6 MB的速率接收（及儲存）稽核記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。在稽核記錄中、最重要的其他變數是S3作業所佔的百分比（相對於（表中使用的4個字元縮寫為稽核記錄欄位名稱）、以及下列S3欄位的平均大小（以位元組為單位）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 貯體	S3儲存區名稱。
S3KY	S3 金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

讓我們使用P來表示S3作業所佔的百分比、其中0≤P≤1（因此、對於100%負載工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓我們使用 K 來代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以使用下列公式預估外部syslog伺服器需要處理的稽核記錄數量、前提是您將稽核層級設為預設值（所有類別均設為「正常」、儲存除外、 設定為「錯誤」）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則您的工作負載為50%、您的S3帳戶名稱、儲存區名稱、 而且物件名稱平均為90位元組、外部syslog伺服器的大小應可支援每秒1、500則syslog訊息、而且應能以每秒約1 MB的速率接收（及儲存）稽核記錄資料。

非預設稽核層級的估計公式

提供給稽核記錄的公式會假設使用預設的稽核層級設定（所有類別均設定為「正常」、但儲存區設為「錯誤」除外）。對於非預設稽核層級設定、無法使用估算稽核訊息速率和平均大小的詳細公式。不過、下表可用於粗略估計費率； 您可以使用提供給稽核記錄的平均大小公式、但請注意、這可能會導致預估過度、因為「額外」稽核訊息平均比預設稽核訊息小。

條件	公式
複寫：稽核層級全部設為「偵錯」或「正常」	稽核記錄速率 = 8 x S3 作業率
銷毀編碼：稽核層級全部設為「除錯」或「正常」	使用與預設設定相同的公式

安全性事件的估計公式

安全事件與 S3 作業無關、通常會產生可忽略的記錄和資料量。因此、我們不會提供任何預估公式。

應用程式記錄的估計公式

如果您沒有S3工作負載的相關資訊、而不是預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的應用程式記錄數量：

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒3、300個應用程式記錄、並能以每秒1.2 MB的速率接收（及儲存）應用程式記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。對於應用程式記錄、最重要的其他變數是資料保護策略（複寫與銷毀編碼）、所放置S3作業的百分比（與獲得/其他）、以及下列S3欄位的平均大小（以位元組為單位）（表中使用的4個字元縮寫為稽核記錄欄位名稱）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 貯體	S3儲存區名稱。
S3KY	S3 金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

規模估算範例

本節說明如何使用下列資料保護方法來使用網格的估計公式範例：

- 複寫
- 銷毀編碼

如果您使用複寫來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓 K 代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、工作負載為50%、S3帳戶名稱、儲存區名稱及物件名稱平均為90個位元組、則外部syslog伺服器的大小應可支援每秒1800個應用程式記錄、 並以每秒0.5 MB的速率接收（通常是儲存）應用程式資料。

如果您使用銷毀編碼來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓 K 代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

舉例來說、如果您的網格大小為每秒 1 、 000 次 S3 作業、則您的工作負載為 50% 、而您的 S3 帳戶名稱、貯體名稱、 物件名稱平均 90 個位元組、外部 Syslog 伺服器的大小應可支援每秒 2 、 250 個應用程式記錄檔、而且應能以每秒 0.6 MB 的速度接收（通常是儲存）應用程式資料。

設定稽核訊息和外部 **Syslog** 伺服器

您可以設定許多與稽核訊息相關的設定。您可以調整記錄的稽核訊息數量、定義您要包含在用戶端讀寫稽核訊息中的任何 HTTP 要求標頭、設定外部 Syslog 伺服器、以及指定要傳送稽核記錄、安全性事件記錄和 StorageGRID 軟體記錄的位置。

稽核訊息和記錄會記錄系統活動和安全事件、是監控和疑難排解的重要工具。所有StorageGRID 的節點都會產生稽核訊息和記錄、以追蹤系統活動和事件。

您也可以設定外部 Syslog 伺服器、以遠端儲存稽核資訊。使用外部伺服器可將稽核訊息記錄的效能影響降至最低、而不會降低稽核資料的完整性。如果您有大型網格、使用多種 S3 應用程式、或想要保留所有稽核資料、外部 Syslog 伺服器就特別有用。請參閱 "外部syslog伺服器的考量" 以取得詳細資料。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "維護或根存取權限"。
- 如果您計畫設定外部 Syslog 伺服器、您已檢閱 "使用外部 Syslog 伺服器的考量事項" 並確保伺服器有足夠的容量來接收及儲存記錄檔。
- 如果您打算使用 TLS 或 RELP/TLS 通訊協定來設定外部 Syslog 伺服器、則您擁有所需的伺服器 CA 和用戶端憑證、以及用戶端私密金鑰。

變更稽核訊息層級

您可以在稽核日誌中針對下列每個類別的訊息設定不同的稽核層級：

稽核類別	預設設定	更多資訊
系統	正常	"系統稽核訊息"
儲存設備	錯誤	"物件儲存稽核訊息"
管理	正常	"管理稽核訊息"
用戶端讀取	正常	"用戶端讀取稽核訊息"

稽核類別	預設設定	更多資訊
用戶端寫入	正常	"用戶端寫入稽核訊息"
ILM	正常	"ILM 稽核訊息"
跨網格複寫	錯誤	"CGRR ：跨網格複寫要求"

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。如果您最初使用舊版 StorageGRID 、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*>*稽核與系統記錄伺服器*。
2. 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。

如果您不需要 S3 應用程式的用戶端讀取作業詳細記錄、請選擇性地將「 * 用戶端讀取 * 」設定變更為「 * 錯誤 * 」、以減少稽核記錄中記錄的稽核訊息數。

3. 選擇*保存*。

綠色橫幅表示您的組態已儲存。

定義 HTTP 要求標頭

您可以選擇性地定義要包含在用戶端讀寫稽核訊息中的任何 HTTP 要求標頭。這些傳輸協定標頭僅適用於 S3 和 Swift 要求。

步驟

1. 在「 * 稽核通訊協定標頭 * 」區段中、定義您要包含在用戶端讀寫稽核訊息中的 HTTP 要求標頭。

使用星號（*）做為萬用字元、以符合零個或多個字元。使用轉義順序（*）來符合文字星號。

2. 如有需要、請選取*新增其他標頭*以建立其他標頭。

   在要求中找到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。

3. 選擇*保存*

   綠色橫幅表示您的組態已儲存。

[[use-external -syslog-server]] 使用外部 Syslog 伺服器

您可以選擇性地設定外部 Syslog 伺服器、將稽核記錄、應用程式記錄和安全性事件記錄儲存到網格外的位置。

如果您不想使用外部 Syslog 伺服器、請跳過此步驟並前往 選取稽核資訊目的地。

如果此程序中可用的組態選項不夠靈活、無法滿足您的需求、則可使用套用其他組態選項 `audit-destinations` 端點、位於的私有 API 區段 "網格管理API"。例如、如果您想要將不同的 Syslog 伺服器用於不同的節點群組、可以使用 API 。

輸入系統記錄資訊

存取「設定外部系統記錄伺服器」精靈、並提供 StorageGRID 存取外部系統記錄伺服器所需的資訊。

步驟

1. 從「稽核與系統記錄伺服器」頁面、選取*「設定外部系統記錄伺服器*」。或者、如果您先前已設定外部 Syslog 伺服器、請選取 * 編輯外部 Syslog 伺服器 * 。

   此時將顯示 Configure external Syslog server （配置外部系統日誌服務器）

2. 在嚮導的 * 輸入系統日誌 info* 步驟中，在 * 主機 * 字段中輸入外部系統日誌服務器的有效完全限定域名或 IPv4 或 IPv6 地址。
3. 輸入外部syslog伺服器上的目的地連接埠（必須是介於1和6555之間的整數）。預設連接埠為 514 。
4. 選取用於傳送稽核資訊至外部syslog伺服器的傳輸協定。

   建議使用 **TLS** 或 **RELP/TLS** 。您必須上傳伺服器憑證、才能使用上述任一選項。使用憑證有助於保護網格與外部syslog伺服器之間的連線。如需詳細資訊、請參閱 "管理安全性憑證"。

   所有的傳輸協定選項都需要外部syslog伺服器的支援和組態。您必須選擇與外部syslog伺服器相容的選項。

   可靠的事件記錄傳輸協定（RELP）可延伸系統記錄傳輸協定的功能、以提供可靠的事件訊息傳輸。如果您的外部syslog伺服器必須重新啟動、使用RELP有助於防止稽核資訊遺失。

5. 選擇*繼續*。
6. [[attach 憑證]] 如果您選取 **TLS** 或 **RELP/TLS** 、請上傳伺服器 CA 憑證、用戶端憑證和用戶端私密金鑰。

a. 選取*瀏覽*以取得您要使用的憑證或金鑰。
b. 選取憑證或金鑰檔案。
c. 選取*「Open*（開啟*）」上傳檔案。

憑證或金鑰檔名稱旁會出現綠色勾號、通知您已成功上傳。

7. 選擇*繼續*。

管理系統記錄內容

您可以選取要傳送至外部 Syslog 伺服器的資訊。

步驟

1. 針對精靈的 * 管理系統記錄內容 * 步驟、選取您要傳送至外部系統記錄伺服器的每種稽核資訊類型。
   - * 傳送稽核記錄 * ：傳送 StorageGRID 事件和系統活動
   - * 傳送安全性事件 * ：傳送安全性事件，例如未獲授權的使用者嘗試登入或使用者以 root 身分登入
   - * 傳送應用程式記錄 * ：傳送有助於疑難排解的記錄檔、包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` （僅限管理節點）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   如需 StorageGRID 軟體記錄的相關資訊、請參閱 "軟體記錄StorageGRID"。

2. 使用下拉式功能表為您要傳送的每個稽核資訊類別選取嚴重性和醫事機構（訊息類型）。

   設定嚴重性和設施值可協助您以可自訂的方式來彙總記錄、以便更輕鬆地進行分析。

   a. 對於 * 嚴重性 * 、請選取 * Passthrough * 、或選取介於 0 和 7 之間的嚴重性值。

      如果您選取值、所選的值將套用至此類型的所有訊息。如果您以固定值覆寫嚴重性、則會遺失關於不同嚴重性的資訊。

嚴重性	說明
Passthrough	傳送至外部 Syslog 的每則訊息、其嚴重性值與本機登入節點時相同： • 對於稽核記錄、嚴重性為「資訊」。 • 對於安全事件、嚴重性值是由節點上的 Linux 發佈所產生。 • 對於應用程式記錄、「資訊」和「通知」之間的嚴重性會因問題而異。例如、新增 NTP 伺服器並設定 HA 群組會提供「 info 」的值、而刻意停止 SSM 或 RSM 服務則會提供「 notice 」的值。
0%	緊急：系統無法使用
1.	警示：必須立即採取行動
2.	關鍵：關鍵條件
3.	錯誤：錯誤情況
4.	警告：警告條件
5.	注意：正常但重要的情況
6.	資訊：資訊訊息
7.	偵錯：偵錯層級的訊息

b. 對於 * 設施 * 、請選取 * Passthrough * 、或選取介於 0 和 23 之間的設施值。

如果您選取一個值、它會套用至所有此類型的訊息。如果您以固定值覆寫醫事機構、則會遺失有關不同醫事機構的資訊。

設施	說明
Passthrough	傳送至外部 Syslog 的每則訊息、其設施值與本機登入節點時相同： • 對於稽核記錄、傳送至外部 Syslog 伺服器的設施為「 local7 」。 • 對於安全事件、設施值是由節點上的 Linux 套裝作業系統所產生。 • 對於應用程式記錄、傳送至外部 Syslog 伺服器的應用程式記錄具有下列設施值： ◦ `bycast.log`：用戶或守護程序 ◦ `bycast-err.log`：用戶、守護程序、 local3 或 local4 ◦ `jaeger.log`： local2. ◦ `nms.log`： local3. ◦ `prometheus.log`： local4. ◦ `raft.log`： local5. ◦ `hagroups.log`： local6.
0%	KERN（核心訊息）
1.	使用者（使用者層級訊息）
2.	郵件
3.	精靈（系統精靈）
4.	驗證（安全性/授權訊息）
5.	系統記錄（系統記錄所產生的訊息）
6.	LPR（線路印表機子系統）
7.	新聞（網路新聞子系統）
8.	uucp
9.	cron（時鐘精靈）
10.	安全性（安全性/授權訊息）
11.	FTP
12.	NTP

設施	說明
13.	記錄稽核（記錄稽核）
14.	記錄警示（記錄警示）
15.	時鐘（時鐘精靈）
16.	local0
17.	local1.
18.	local2.
19	local3.
20.	本地4
21.	本地5.
22	本地化 6.
23	本地化7.

3. 選擇*繼續*。

傳送測試訊息

開始使用外部syslog伺服器之前、您應該要求網格中的所有節點都將測試訊息傳送至外部syslog伺服器。您應該使用這些測試訊息來協助驗證整個記錄收集基礎架構、然後再將資料傳送至外部syslog伺服器。

請勿使用外部 Syslog 伺服器組態、除非您確認外部 Syslog 伺服器收到來自網格中每個節點的測試訊息、且訊息已如預期般處理。

步驟

1. 如果您不想傳送測試訊息、因為您確定已正確設定外部 Syslog 伺服器、而且可以從網格中的所有節點接收稽核資訊、請選取 * 略過並完成 * 。

   綠色橫幅表示已儲存組態。

2. 否則、請選取 * 傳送測試訊息 * （建議）。

   測試結果會持續顯示在頁面上、直到您停止測試為止。測試進行中時、您的稽核訊息會繼續傳送至先前設定的目的地。

3. 如果您收到任何錯誤、請更正錯誤、然後再次選取*傳送測試訊息*。

請參閱 "排除外部syslog伺服器的故障" 協助您解決任何錯誤。

4. 請等到看到綠色橫幅、表示所有節點都已通過測試。
5. 請檢查您的syslog伺服器、確定是否收到測試訊息、並按照預期處理。

> 如果您使用的是udp、請檢查整個記錄收集基礎架構。UDP 傳輸協定不允許像其他傳輸協定一樣嚴格地偵測錯誤 通訊協定。

6. 選擇*停止並結束*。

   您將返回到* Audit和syslog server*頁面。綠色橫幅表示系統記錄伺服器組態已儲存。

> 除非您選取包含外部 Syslog 伺服器的目的地、否則 StorageGRID 稽核資訊不會傳送至外部 Syslog 伺服器。

選取稽核資訊目的地

您可以指定稽核記錄檔、安全性事件記錄檔和的位置 "軟體記錄StorageGRID" 已傳送。

> 某些目的地只有在您已設定外部 Syslog 伺服器時才可使用。

步驟

1. 在「稽核與系統記錄伺服器」頁面上、選取稽核資訊的目的地。

> * 僅限本機節點 * 和 * 外部系統記錄伺服器 * 通常可提供更好的效能。

選項	說明
僅限本機節點	稽核訊息、安全性事件記錄和應用程式記錄不會傳送至管理節點。而是僅儲存在產生這些節點的節點上（「本機節點」）。在每個本機節點上產生的稽核資訊都儲存在中 `/var/local/log/localaudit.log` • 注意 * ： StorageGRID 會定期移除輪替中的本機記錄檔、以釋放空間。當節點的記錄檔達到1 GB時、會儲存現有檔案、並啟動新的記錄檔。記錄檔的旋轉限制為21個檔案。建立22版記錄檔時、會刪除最舊的記錄檔。每個節點平均儲存約20 GB的記錄資料。
管理節點 / 本機節點	稽核訊息會傳送至稽核記錄 (`/var/local/log/audit.log`）在管理節點上、安全事件記錄和應用程式記錄會儲存在產生它們的節點上。
外部syslog伺服器	稽核資訊會傳送至外部 Syslog 伺服器、並儲存在本機節點上。傳送的資訊類型取決於您設定外部syslog伺服器的方式。只有在設定外部syslog伺服器之後、才會啟用此選項。

選項	說明
管理節點和外部syslog伺服器	稽核訊息會傳送至稽核記錄 (`/var/local/log/audit.log`）並將稽核資訊傳送至外部 Syslog 伺服器、並儲存在本機節點上。傳送的資訊類型取決於您設定外部syslog伺服器的方式。只有在設定外部syslog伺服器之後、才會啟用此選項。

2. 選擇*保存*。

   出現警告訊息。

3. 選取 * 確定 * 以確認您要變更稽核資訊的目的地。

   綠色橫幅表示稽核組態已儲存。

   新記錄會傳送至您選取的目的地。現有記錄仍會保留在目前位置。