配置審計訊息和日誌目標

StorageGRID software

NetApp
May 29, 2026

目錄

配置審計訊息和日誌目標

使用外部系統日誌伺服器的注意事項

外部系統日誌伺服器是StorageGRID以外的伺服器，您可以使用它在單一位置收集系統稽核資訊。使用外部系統日誌伺服器可以減少管理節點上的網路流量並更有效地管理資訊。對於StorageGRID，出站 syslog 訊息包格式符合 RFC 3164。

您可以傳送到外部系統日誌伺服器的稽核資訊類型包括：

- 審計日誌包含系統正常運作期間產生的稽核訊息
- 與安全性相關的事件，例如登入和升級到 root
- 如果需要開啟支援案例來解決您遇到的問題，可能會要求應用程式日誌

何時使用外部系統日誌伺服器

如果您擁有大型網格、使用多種類型的 S3 應用程式或想要保留所有審計數據，則外部 syslog 伺服器特別有用。將審計資訊傳送到外部系統日誌伺服器使您能夠：

- 更有效率地收集和管理稽核訊息、應用程式日誌和安全事件等稽核資訊。
- 減少管理節點上的網路流量，因為稽核資訊直接從各個儲存節點傳輸到外部系統日誌伺服器，而無需透過管理節點。

> 當日誌傳送到外部系統日誌伺服器時，大於 8,192 位元組的單一日誌會在訊息末尾被截斷，以符合外部系統日誌伺服器實施中的常見限制。

> 為了在外部系統日誌伺服器發生故障時最大限度地提供完整資料復原的選項，最多可儲存 20 GB 的本機稽核記錄日誌(`localaudit.log`) 在每個節點上進行維護。

如何設定外部系統日誌伺服器

若要了解如何設定外部 syslog 伺服器，請參閱"設定審計訊息和外部系統日誌伺服器"。

如果您打算設定使用 TLS 或 RELP/TLS 協議，則必須擁有以下憑證：

- 伺服器 **CA** 證書：一個或多個可信任 CA 證書，用於驗證 PEM 編碼的外部系統日誌伺服器。如果省略，則將使用預設的 Grid CA 憑證。
- 用戶端憑證：用於以 PEM 編碼向外部系統日誌伺服器進行身份驗證的用戶端憑證。
- 客戶端私鑰：PEM 編碼的客戶端憑證的私鑰。

> 如果您使用客戶端證書，您還必須使用客戶端私鑰。如果您提供加密的私鑰，您還必須提供密碼。使用加密私鑰沒有顯著的安全優勢，因為必須儲存金鑰和密碼；如果可用，建議使用未加密的私鑰以簡化操作。

如何估計外部系統日誌伺服器的大小

通常，您的網格大小會根據所需的吞吐量進行調整，以每秒 S3 操作數或每秒位元組數來定義。例如，您可能要求網格每秒處理 1,000 個 S3 操作，或每秒 2,000 MB 的物件提取和檢索。您應該根據網格的資料要求來確定外部系統日誌伺服器的大小。

本節提供了一些啟發式公式，可協助您估計外部系統日誌伺服器需要處理的各種類型日誌訊息的速率和平均大小，以網格已知或期望的效能特徵（每秒 S3 操作）表示。

在估算公式中使用每秒 **S3** 次操作

如果您的網格大小是根據每秒位元組數表示的吞吐量來確定的，則必須將此大小轉換為每秒 S3 操作數才能使用估算公式。要轉換網格吞吐量，您必須先確定平均物件大小，您可以使用現有審計日誌和指標（如果有）中的信息，或者利用您對將使用StorageGRID 的應用程式的了解來確定。例如，如果您的網格大小可實現 2,000 MB/秒的吞吐量，且您的平均物件大小為 2 MB，那麼您的網格大小可實現每秒處理 1,000 個 S3 操作（2,000 MB/2 MB）。

> 以下部分中的外部系統日誌伺服器大小公式提供了常見情況的估計值（而不是最壞情況的估計）。根據您的配置和工作負載，您可能會看到比公式預測的更高或更低的系統日誌訊息速率或系統日誌資料量。這些公式僅供參考。

審計日誌的估算公式

如果除了網格預計支援的每秒 S3 操作數之外，您沒有關於 S3 工作負載的任何信息，那麼您可以使用以下公式估算外部 syslog 伺服器需要處理的審計日誌量，假設您將審計級別保留為默認值（所有類別都設置為正常，存儲除外，設置為錯誤）：

```
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 個 S3 操作，那麼您的外部 syslog 伺服器的大小應支援每秒 2,000 個 syslog 訊息，並且應該能夠以每秒 1.6 MB 的速率接收（通常儲存）審計日誌資料。

如果您對自己的工作量了解更多，就可以做出更準確的估計。對於審計日誌，最重要的附加變數是 S3 操作中 PUT（相對於 GETS）的百分比，以及以下 S3 欄位的平均大小（以位元組為單位）（表中使用的 4 個字元的縮寫是審計日誌欄位名稱）：

程式碼	場地	描述
南卡羅來納大學	S3 租用戶帳戶名稱（請求發送者）	發送請求的使用者的租戶帳戶的名稱。對於匿名請求則為空。
SBAC	S3 租用戶帳戶名稱（儲存桶擁有者）	儲存桶擁有者的租用戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 儲存桶	S3 儲存桶名稱。

程式碼	場地	描述
S3KY	S3 鍵	S3 密鑰名稱，不包括儲存桶名稱。對 bucket 的操作不包含該欄位。

讓我們使用 P 來表示 S3 操作中 PUT 的百分比，其中 0 ≤ P ≤ 1（因此，對於 100% PUT 工作負載，P = 1，對於 100% GET 工作負載，P = 0）。

讓我們用 K 來表示 S3 帳戶名稱、S3 儲存桶和 S3 金鑰總和的平均大小。假設 S3 帳戶名稱始終為 my-s3-account（13 個位元組），儲存桶具有固定長度的名稱，如 /my/application/bucket-12345（28 個位元組），物件具有固定長度的鍵，如 5733a5d7-f069-41ef-894-13626ccfbc69-41ef-84-13626ccfbccfbc36c36c36c36c36c6cc3cc56cc56ccfbccfbc36c36cc36cc36cc3c）。那麼K的值為90（13+13+28+36）。

如果您可以確定 P 和 K 的值，則可以使用下列公式估算外部系統日誌伺服器需要處理的稽核日誌量，假設您將稽核等級保留為預設值（所有類別都設為正常，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 個 S3 操作，您的工作負載為 50% PUT，並且您的 S3 帳戶名稱、儲存桶名稱和物件名稱平均為 90 個位元組，那麼您的外部系統日誌伺服器的大小應支援每秒 1,500 個系統日誌訊息，並且應該能夠以每秒 1 MB 的審計速率接收資料速率。

非違約審計水準的估計公式

為審計日誌提供的公式假定使用預設審計等級設定（所有類別均設定為正常，但儲存除外，設定為錯誤）。沒有用於估計非預設審計層級設定的審計訊息的速率和平均大小的詳細公式。但是，可以使用下表對速率進行粗略估計；您可以使用審計日誌提供的平均大小公式，但請注意，這可能會導致高估，因為「額外」審計訊息平均小於預設審計訊息。

狀態	公式
複製：審計等級全部設定為“調試”或“正常”	審計日誌速率 = 8 x S3 操作率
擦除編碼：審計等級全部設定為“調試”或“正常”	使用與預設值相同的公式

安全事件的估計公式

安全事件與 S3 操作無關，通常只產生極少量的日誌和資料。由於這些原因，沒有提供估算公式。

應用日誌的估算公式

如果除了網格預計支援的每秒 S3 操作數之外，您沒有關於 S3 工作負載的任何信息，那麼您可以使用以下公式估算外部 syslog 伺服器需要處理的應用程式日誌量：

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

因此，例如，如果您的網格大小為每秒 1,000 個 S3 操作，那麼您的外部 syslog 伺服器的大小應該支援每秒 3,300 個應用程式日誌，並且能夠以每秒約 1.2 MB 的速率接收（和儲存）應用程式日誌資料。

如果您對自己的工作量了解更多，就可以做出更準確的估計。對於應用程式日誌，最重要的附加變數是資料保護策略（複製與擦除編碼）、PUT 的 S3 操作百分比（與 GET/其他相比）以及以下 S3 欄位的平均大小（以位元組為單位）（表中使用的 4 個字元的縮寫是審計日誌欄位名稱）：

程式碼	場地	描述
南卡羅來納大學	S3 租用戶帳戶名稱（請求發送者）	發送請求的使用者的租戶帳戶的名稱。對於匿名請求則為空。
SBAC	S3 租用戶帳戶名稱（儲存桶擁有者）	儲存桶擁有者的租用戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 儲存桶	S3 儲存桶名稱。
S3KY	S3 鍵	S3 密鑰名稱，不包括儲存桶名稱。對 bucket 的操作不包含該欄位。

尺寸估算範例

本節透過範例案例來說明如何使用具有以下資料保護方法的電網估算公式：

- 複製
- 擦除編碼

如果您使用複製來保護數據

令 P 表示 S3 操作中 PUT 的百分比，其中 0 ≤ P ≤ 1（因此，對於 100% PUT 工作負載，P = 1，對於 100% GET 工作負載，P = 0）。

設 K 表示 S3 帳號名稱、S3 儲存桶和 S3 金鑰總和的平均大小。假設 S3 帳戶名稱始終為 my-s3-account（13 個位元組），儲存桶具有固定長度的名稱，如 /my/application/bucket-12345（28 個位元組），物件具有固定長度的鍵，如 5733a5d7-f069-41ef-894-13626ccfbc69-41ef-84-13626ccfbccfbc36c36c36c36c36c6cc3cc56cc56ccfbccfbc36c36cc36cc36cc3c）。那麼 K 的值為 90（13+13+28+36）。

如果您可以確定 P 和 K 的值，您就可以使用下列公式估算外部 syslog 伺服器必須能夠處理的應用程式日誌量。

```
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
```

因此，例如，如果您的網格大小為每秒 1,000 個 S3 操作，您的工作負載為 50% PUT，並且您的 S3 帳戶名稱、儲存桶名稱和物件名稱平均為 90 位元組，那麼您的外部 syslog 伺服器的大小應支援每秒 1800 個應用程式，並且將資料以儲存速率 0.55 的 MB（5.5 應用程式）。

如果您使用擦除編碼來保護數據

令 P 表示 S3 操作中 PUT 的百分比，其中 0 ≤ P ≤ 1（因此，對於 100% PUT 工作負載，P = 1，對於 100% GET 工作負載，P = 0）。

設 K 表示 S3 帳號名稱、S3 儲存桶和 S3 金鑰總和的平均大小。假設 S3 帳戶名稱始終為 my-s3-account（13 個位元組），儲存桶具有固定長度的名稱，如 /my/application/bucket-12345（28 個位元組），物件具有固定長度的鍵，如 5733a5d7-f069-41ef-894-13626ccfbc69-41ef-84-13626ccfbccfbc36c36c36c36c36c6cc3cc56cc56ccfbccfbc36c36cc36cc36cc3c）。那麼 K 的值為 90（13+13+28+36）。

如果您可以確定 P 和 K 的值，您就可以使用下列公式估算外部 syslog 伺服器必須能夠處理的應用程式日誌量。

```
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
```

因此，例如，如果您的網格大小為每秒 1,000 個 S3 操作，您的工作負載為 50% PUT，並且您的 S3 帳戶名稱、存儲桶名稱和對象名稱平均為 90 字節，那麼您的外部 syslog 伺服器的大小應支援每秒 2,250 個應用程式記錄日誌，並且應該能夠以 MB 0.66）應用程式的記錄.6.66）。

設定審計訊息和外部系統日誌伺服器

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；定義任何要包含在用戶端讀取和寫入稽核訊息中的 HTTP 請求標頭；設定外部系統日誌伺服器；並指定稽核日誌、安全事件日誌和StorageGRID軟體日誌的傳送位置。

稽核訊息和日誌記錄系統活動和安全事件，是監控和故障排除的重要工具。所有StorageGRID節點都會產生稽核訊息和日誌來追蹤系統活動和事件。

或者，您可以設定外部系統日誌伺服器來遠端保存稽核資訊。使用外部伺服器可以最大限度地減少稽核訊息記錄對效能的影響，而不會降低稽核資料的完整性。如果您擁有大型網格、使用多種類型的 S3 應用程式或想要保留所有審計數據，則外部 syslog 伺服器特別有用。看"設定審計訊息和外部系統日誌伺服器"了解詳情。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"維護或 Root 存取權限"。
- 如果您打算設定外部系統日誌伺服器，您已查看"使用外部系統日誌伺服器的注意事項"並確保伺服器有足夠的容量來接收和儲存日誌檔案。
- 如果您打算使用 TLS 或 RELP/TLS 協定設定外部 syslog 伺服器，則您需要具備所需的伺服器 CA 和用戶端憑證以及用戶端私鑰。

更改審計訊息級別

您可以為審計日誌中的以下每個類別的訊息設定不同的審計等級：

審計類別	預設設定	更多資訊
系統	普通的	"系統審計訊息"
儲存	錯誤	"物件儲存審計訊息"
管理	普通的	"管理審計訊息"
客戶端讀取	普通的	"客戶端讀取審計訊息"
客戶寫道	普通的	"客戶端寫入審計訊息"
工業光魔	普通的	"ILM 審計訊息"
跨網格複製	錯誤	"CGRR：跨網格複製請求"

如果您最初使用 10.3 或更高版本安裝StorageGRID ，則這些預設值適用。如果您最初使用的是早期版本的StorageGRID，則所有類別的預設設定都為「正常」。

升級期間，審計等級配置不會立即生效。

步驟

1. 選擇 設定 > 監控 > 稽核和系統日誌伺服器。
2. 對於每個審計訊息類別，從下拉清單中選擇一個審計層級：

審計級別	描述
離開	未記錄該類別的任何審計訊息。
錯誤	僅記錄錯誤訊息－結果代碼不為「成功」（SUCS）的稽核訊息。
普通的	記錄標準事務訊息－這些類別的說明中所列的訊息。
偵錯	已棄用。此級別的行為與正常審計級別相同。

任何特定層級所包含的訊息都包括在更高層級記錄的訊息。例如，正常等級包括所有錯誤訊息。

如果您不需要 S3 應用程式的用戶端讀取操作的詳細記錄，則可以選擇將 用戶端讀取 設定變更為 錯誤 以減少稽核日誌中記錄的稽核訊息數量。

3. 選擇*儲存*。

   綠色橫幅表示您的配置已儲存。

定義 HTTP 請求標頭

您可以選擇定義要包含在客戶端讀寫審計訊息中的任何 HTTP 請求標頭。這些協定標頭僅適用於 S3 請求。

步驟

1. 在*審計協定標頭*部分中，定義您想要包含在客戶端讀寫審計訊息中的 HTTP 請求標頭。

   使用星號 (*) 作為通配符來匹配零個或多個字元。使用轉義序列 (*) 來匹配文字星號。

2. 如果需要，請選擇「新增另一個標題」來建立其他標題。

   當在請求中發現 HTTP 標頭時，它們會包含在欄位 HTRH 下的稽核訊息中。

   僅當 客戶端讀取 或 客戶端寫入 的審計級別不是 關閉 時，才會記錄審計協議請求標頭。

3. 選擇“儲存”

   綠色橫幅表示您的配置已儲存。

使用外部 syslog 伺服器

您可以選擇設定外部系統日誌伺服器，將稽核日誌、應用程式日誌和安全性事件日誌儲存到網格外部的位置。

如果您不想使用外部系統日誌伺服器，請跳過此步驟並轉到選擇審計資訊目的地。

如果此過程中可用的配置選項不夠靈活，無法滿足您的要求，則可以使用 `audit-destinations`端點，位於"電網管理API"。例如，如果您想要對不同的節點群組使用不同的 syslog 伺服器，則可以使用 API。

輸入系統日誌訊息

存取設定外部系統日誌伺服器精靈並提供StorageGRID存取外部系統日誌伺服器所需的資訊。

步驟

1. 從稽核和系統日誌伺服器頁面中，選擇*設定外部系統日誌伺服器*。或者，如果您之前設定了外部系統日誌伺服器，請選擇*編輯外部系統日誌伺服器*。

   出現設定外部系統日誌伺服器精靈。

2. 對於精靈的 輸入系統日誌資訊 步驟，在 主機 欄位中輸入外部系統日誌伺服器的有效完全限定網域名稱或 IPv4 或 IPv6 位址。
3. 輸入外部系統日誌伺服器上的目標連接埠（必須是 1 到 65535 之間的整數）。預設連接埠為 514。
4. 選擇用於將審計資訊傳送到外部系統日誌伺服器的協定。

建議使用 **TLS** 或 **RELP/TLS**。您必須上傳伺服器憑證才能使用這兩個選項之一。使用憑證有助於保護網格和外部系統日誌伺服器之間的連線。有關更多信息，請參閱"管理安全證書" 。

所有協定選項都需要外部系統日誌伺服器的支援和配置。您必須選擇與外部系統日誌伺服器相容的選項。

> 可靠事件日誌協定 (RELP) 擴展了 syslog 協定的功能，以提供可靠的事件訊息傳遞。如果您的外部系統日誌伺服器必須重新啟動，使用 RELP 可以協助防止稽核資訊遺失。

5. 選擇*繼續*。
6. 如果您選擇了 **TLS** 或 **RELP/TLS**，請上傳伺服器 CA 憑證、用戶端憑證和用戶端私鑰。
   a. 選擇「瀏覽」以尋找您想要使用的憑證或金鑰。
   b. 選擇憑證或密鑰檔。
   c. 選擇*開啟*上傳檔案。

      憑證或金鑰檔案名稱旁邊會出現一個綠色勾號，通知您已成功上傳。
7. 選擇*繼續*。

管理系統日誌內容

您可以選擇要傳送到外部系統日誌伺服器的資訊。

步驟

1. 對於精靈的*管理系統日誌內容*步驟，選擇要傳送到外部系統日誌伺服器的每種類型的稽核資訊。
   - 發送審計日誌：發送StorageGRID事件和系統活動
   - 傳送安全事件：傳送安全事件，例如未經授權的使用者嘗試登入或使用者以 root 身分登入時
   - 發送應用程式日誌: 發送"StorageGRID軟體日誌文件"對於故障排除很有用，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`（僅限管理節點）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - 傳送存取日誌：將外部請求的 HTTP 存取日誌傳送到網格管理器、租用戶管理器、配置的負載平衡器端點以及來自遠端系統的網格聯合請求。
2. 使用下拉式選單選擇要傳送的每類審計資訊的嚴重性和設施（訊息類型）。

   設定嚴重性和設施值可以幫助您以可自訂的方式聚合日誌，以便於分析。

   a. 對於*嚴重性*，選擇*通過*，或選擇 0 到 7 之間的嚴重性值。

      如果您選擇一個值，則所選值將套用於此類型的所有訊息。如果使用固定值覆蓋嚴重性，則有關不同嚴

重性的資訊將會遺失。

嚴重程度	描述
直通	發送到外部系統日誌的每個訊息都具有與本地記錄到節點時相同的嚴重性值： • 對於審計日誌，嚴重性為「資訊」。 • 對於安全事件，嚴重性值由節點上的 Linux 發行版產生。 • 對於應用程式日誌，嚴重性在「資訊」和「通知」之間變化，具體取決於問題是什麼。例如，新增 NTP 伺服器並設定 HA 群組會給予「info」的值，而故意停止 SSM 或 RSM 服務會給予「notice」的值。 • 對於訪問日誌，嚴重性為「資訊」。
0	緊急情況：系統無法使用
1	警報：必須立即採取行動
2	危急：危急情況
3	錯誤：錯誤狀況
4	警告：警告條件
5	注意：正常但重要的情況
6	訊息：訊息訊息
7	調試：調試級別訊息

b. 對於 **Facilty**，選擇 **Passthrough**，或選擇 0 到 23 之間的設施值。

如果您選擇一個值，它將套用於此類型的所有訊息。如果使用固定值覆蓋設施，則有關不同設施的資訊將會遺失。

設施	描述
直通	發送到外部系統日誌的每個訊息都具有與本地記錄到節點時相同的設施值： • 對於稽核日誌，傳送到外部系統日誌伺服器的設備是「local7」。 • 對於安全事件，設施值由節點上的 Linux 發行版產生。 • 對於應用程式日誌，發送到外部 syslog 伺服器的應用程式日誌具有以下設施值： ◦ `bycast.log`：使用者或守護程式 ◦ `bycast-err.log`：使用者、守護程式、local3 或 local4 ◦ `jaeger.log`：本地2 ◦ `nms.log`：本地3 ◦ `prometheus.log`：本地4 ◦ `raft.log`：本地5 ◦ `hagroups.log`：本地6 • 對於存取日誌，傳送到外部系統日誌伺服器的設備是「local0」。
0	kern（內核訊息）
1	用戶（用戶級訊息）
2	郵件
3	守護程式（系統守護程式）
4	auth（安全/授權訊息）
5	syslog（由 syslogd 內部產生的訊息）
6	lpr（行式印表機子系統）
7	新聞（網路新聞子系統）
8	UUCP
9	cron（時鐘守護程式）
10	安全（安全/授權訊息）
11	FTP

設施	描述
12	NTP
13	logaudit（日誌稽核）
14	logalert（日誌警報）
15	時鐘（時鐘守護程式）
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. 選擇*繼續*。

發送測試訊息

在開始使用外部系統日誌伺服器之前，您應該要求網格中的所有節點向外部系統日誌伺服器發送測試訊息。在承諾將資料傳送到外部系統日誌伺服器之前，您應該使用這些測試訊息來幫助您驗證整個日誌收集基礎架構。

在確認外部系統日誌伺服器從網格中的每個節點收到測試訊息並且該訊息按預期處理之前，請勿使用外部系統日誌伺服器設定。

步驟

1. 如果您不想發送測試訊息，因為您確定您的外部系統日誌伺服器配置正確並且可以從網格中的所有節點接收審計訊息，請選擇*跳過並完成*。

   綠色橫幅表示配置已儲存。

2. 否則，選擇*發送測試訊息*（建議）。

   測試結果會持續顯示在頁面上，直到您停止測試。在測試進行過程中，您的稽核訊息將繼續傳送到您先前配置的目的地。

3. 如果您在 syslog 伺服器設定期間或執行時收到任何錯誤，請修正它們並再次選擇*傳送測試訊息*。

   看"排除外部系統日誌伺服器故障"幫助您解決任何錯誤。

4. 等到看到綠色橫幅，表示所有節點都已通過測試。
5. 檢查您的系統日誌伺服器以確定測試訊息是否按預期接收和處理。

   如果您使用 UDP，請檢查整個日誌收集基礎架構。UDP 協定不像其他協定那樣允許嚴格的錯誤檢測。

6. 選擇*停止並完成*。

   您將返回*審計和系統日誌伺服器*頁面。綠色橫幅表示系統日誌伺服器配置已儲存。

   直到您選擇包含外部系統日誌伺服器的目標時， StorageGRID稽核資訊才會傳送至外部系統日誌伺服器。

選擇審計資訊目的地

您可以指定稽核日誌、安全事件日誌和"StorageGRID軟體日誌"已發送。

StorageGRID預設為本機節點稽核目標，並將稽核資訊儲存在 `/var/local/log/localaudit.log`。

使用時 `/var/local/log/localaudit.log`，網格管理器和租用戶管理器稽核日誌條目可能會被傳送到儲存節點。您可以使用下列方法來尋找哪個節點具有最新條目 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`命令。

某些目標僅在您設定了外部系統日誌伺服器後才可用。

步驟

1. 在審計和系統日誌伺服器頁面上，選擇審計資訊的目標。

   *僅本機節點*和*外部系統日誌伺服器*通常提供更好的效能。

選項	描述
僅限本地節點（預設）	稽核訊息、安全事件日誌和應用程式日誌不會傳送到管理節點。相反，它們僅保存在生成它們的節點（“本地節點”）上。每個本地節點產生的審計資訊儲存在 `/var/local/log/localaudit.log`。 注意： StorageGRID會定期刪除本機日誌以釋放空間。當節點的日誌檔案達到 1 GB 時，將儲存現有檔案並啟動新的日誌檔案。日誌的輪換限制為 21 個檔案。當建立第 22 個版本的日誌檔案時，最舊的日誌檔案將被刪除。每個節點平均儲存約 20 GB 的日誌資料。

選項	描述
管理節點/本地節點	審計訊息被傳送到管理節點上的稽核日誌，安全事件日誌和應用程式日誌儲存在產生它們的節點上。審計資訊儲存在以下文件中： • 管理節點（主節點和非主節點）：`/var/local/audit/export/audit.log` • 所有節點：`/var/local/log/localaudit.log`文件通常為空或缺失。它可能包含次要訊息，例如某些訊息的附加副本。
外部系統日誌伺服器	審計資訊被傳送到外部系統日誌伺服器並保存在本地節點上（`/var/local/log/localaudit.log`）。傳送的訊息類型取決於您如何設定外部系統日誌伺服器。僅當您設定了外部系統日誌伺服器後，此選項才會啟用。
管理節點和外部系統日誌伺服器	審計訊息被傳送到審計日誌（`/var/local/audit/export/audit.log`），並將稽核資訊傳送至外部系統日誌伺服器並保存在本機節點上（`/var/local/log/localaudit.log`）。傳送的訊息類型取決於您如何設定外部系統日誌伺服器。僅當您設定了外部系統日誌伺服器後，此選項才會啟用。

2. 選擇*儲存*。

   出現警告訊息。

3. 選擇「確定」確認您要變更審計資訊的目的地。

   綠色橫幅表示審計配置已儲存。

   新日誌將發送至您選擇的目的地。現有日誌仍保留在其目前位置。

版權資訊

商標資訊