設定安全性設定

StorageGRID software

NetApp
July 23, 2026

目錄

設定安全性設定

管理 StorageGRID 中的 TLS 和 SSH 原則

TLS 和 SSH 原則決定了使用哪些協定和密碼，以便與用戶端應用程式建立安全的 TLS 連線，以及與內部 StorageGRID 服務建立安全的 SSH 連線。

安全性原則控制 TLS 和 SSH 如何加密傳輸中的資料。通常情況下，請使用「現代相容性（預設）」原則，除非您的系統需要符合通用準則 (Common Criteria) 或需要使用其他加密演算法。

部分 StorageGRID 服務尚未更新，以使用這些原則中的加密演算法。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

選擇安全性原則

步驟

1. ${post_edited_translations.segment}

   An error occurred.

2. ${post_edited_translations.segment}

${post_edited_translations.segment}

如果您需要強式加密且沒有特殊需求，請使用預設原則。此原則與大多數 TLS 和 SSH 用戶端相容。

${post_edited_translations.segment}

如果您需要適用於較舊用戶端的額外相容性選項，請使用 Legacy 相容性原則。此原則中的額外選項可能會使其比 Modern 相容性原則更不安全。

${post_edited_translations.segment}

如果您需要獲得通用準則認證，請使用通用準則原則。

${post_edited_translations.segment}

如果您需要 Common Criteria 認證，且需要使用 NetApp Cryptographic Security Module （NCSM） 3.0.8 或 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組來進行連線至負載平衡器端點、Tenant Manager 和 Grid Manager 的外部用戶端連線，請使用 FIPS 嚴格原則。使用此原則可能會降低效能。

NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組用於以下操作：

- ${post_edited_translations.segment}
  - 以下服務之間的 TLS 連線：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api 、nginx、nginx-gw 和 cache-svc
  - 用戶端與 nginx-gw 服務（負載平衡器端點）之間的 TLS 連線
  - ${post_edited_translations.segment}
  - 物件內容加密（適用於 SSE-S3、SSE-C 和儲存物件加密設定）
  - SSH 連線

  如需詳細資訊，請參閱 NIST Cryptographic Algorithm Validation Program "憑證 #4838"。

- NetApp StorageGRID Kernel Crypto API 模組

  NetApp StorageGRID 核心加密 API 模組僅存在於 VM 和 StorageGRID 應用裝置平台上。

  - 熵收集
  - ${post_edited_translations.segment}

  如需詳細資訊，請參閱 NIST Cryptographic Algorithm Validation Program "證書編號 #A6242 至 #A6257" 與 "Entropy 憑證 #E223"。

注意：選取此原則後，"執行滾動重新開機"所有節點以啟動 NCSM。使用 維護 > 輪流重新開機 來啟動並監控重新開機。

自訂
${post_edited_translations.segment}

（選用）如果您的 StorageGRID 具有 FIPS 140 密碼編譯需求，請啟用 FIPS 模式功能以使用 NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組：

a. 將 `fipsMode`參數設定為 `true`。

b. 出現提示時，請"執行滾動重新開機"所有節點以啟動密碼編譯模組。使用 * 組織維護 * > * 輪流重新開機 * 來啟動和監控重新開機。

c. 選擇 **Support** > **Diagnostics** 以檢視作用中的 FIPS 模組版本。

3. 若要查看每項原則的密碼編譯、協定和演算法的詳細資訊，請選取 **View details**。
4. ${post_edited_translations.segment}

   在原則圖塊的「目前原則」旁邊會出現一個綠色對勾。

${post_edited_translations.segment}

如果您需要套用自己的密碼編譯，可以建立自訂原則。

步驟

1. 在與您要建立的自訂原則最相似的原則圖塊中，選擇 **View details**。
2. 選擇*複製到剪貼簿*，然後選擇*取消*。

3. ${post_edited_translations.segment}
4. 貼上您複製的 JSON，並進行必要的修改。
5. 選擇 **Use policy**。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}

暫時回復預設安全性原則

如果您設定了自訂安全性原則，且設定的 TLS 原則與 "${post_edited_translations.segment}" 不相容，您可能無法登入 Grid Manager。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. 執行下列命令：

   ```
   restore-default-cipher-configurations
   ```

3. 透過網頁瀏覽器，存取同一管理節點上的 Grid Manager。
4. 請依照選擇安全性原則中的步驟重新設定原則。

設定 StorageGRID 網路和物件安全

您可以設定網路和物件安全性，以加密儲存的物件、阻止某些 S3 請求，或允許用戶端連線至儲存節點時使用 HTTP 而非 HTTPS。

儲存物件加密

儲存物件加密可在透過 S3 匯入所有物件資料時對其進行加密。預設情況下，儲存物件不會加密，但您可以選擇使用 AES‐128 或 AES‐256 加密演算法對物件加密。啟用此設定後，所有新匯入的物件都會加密，但現有儲存物件不會有任何變更。如果停用加密，目前已加密的物件仍保持加密狀態，但新匯入的物件將不會加密。

儲存物件加密設定僅適用於尚未透過儲存桶層級或物件層級加密進行加密的 S3 物件。

有關 StorageGRID 加密方法的更多詳細資訊，請參閱"檢閱 StorageGRID 加密方法"。

防止用戶端修改

「防止用戶端修改」是一項全系統設定。選取「防止用戶端修改」選項後，以下請求將被拒絕。

S3 REST API

- DeleteBucket 請求
- 任何修改現有物件資料、使用者定義中繼資料或 S3 物件標記的請求

為儲存節點連線啟用 HTTP

預設情況下，用戶端應用程式使用 HTTPS 網路傳輸協定與儲存節點建立任何直接連線。您可以選擇為這些連線啟用 HTTP，例如，在測試非生產網格時。

只有當 S3 用戶端需要直接與儲存節點建立 HTTP 連線時，才使用 HTTP 進行儲存節點連線。對於僅使用 HTTPS 連線的用戶端或連線到負載平衡器服務的用戶端，則無需使用此選項（因為可以"設定每個負載平衡器端

點"使用 HTTP 或 HTTPS）。

請參閱 "摘要：用戶端連線的 IP 位址和連接埠" 以了解 S3 用戶端在使用 HTTP 或 HTTPS 連線至儲存節點時所使用的連接埠。

選擇選項

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有根目錄存取權限。

步驟

1. ${post_edited_translations.segment}
2. 選擇「網路和物件」索引標籤。
3. 對於儲存物件加密，如果您不希望對儲存物件進行加密，請使用 **None**（預設）設定；或選擇 **AES-128** 或 **AES-256** 來加密儲存物件。
4. 如果您想防止 S3 用戶端發出特定請求，可以選擇性地選取 **Prevent client modification**。

   更改此設定後，新設定大約需要一分鐘才能生效。已設定的值會被快取，以提高效能和擴充性。

5. 如果用戶端直接連線至儲存節點，且您想要使用 HTTP 連線，請選擇性地選取 **Enable HTTP for Storage Node connections**。

   在生產網格中啟用 HTTP 時要格外小心，因為請求將以未加密的方式傳送。

6. 選取 **Save** 。

更改 StorageGRID 介面安全性設定

${post_edited_translations.segment}

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

關於此任務

${post_edited_translations.segment}

${post_edited_translations.segment}

指示使用者瀏覽器在登出前可以保持非活動狀態的時間長度。預設值為 15 分鐘。

瀏覽器閒置逾時時間也受以下因素控制：

- 一個獨立、不可設定的 StorageGRID 定時器，其包含在系統安全性中。每位使用者登入 16 小時後，其驗證權杖便會過期。當使用者的驗證過期時，該使用者會自動登出，即使已停用瀏覽器閒置逾時或尚未達到瀏覽器逾時值也是如此。若要更新權杖，使用者必須重新登入。

- ${post_edited_translations.segment}

  如果啟用了 SSO 且使用者的瀏覽器逾時，則使用者必須重新輸入其 SSO 憑證才能再次存取 StorageGRID。請參閱"單一登入 (SSO) 的工作原理"。

${post_edited_translations.segment}

控制是否在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

此選項預設為停用狀態，但您可能需要在測試環境中啟用此功能。通常，在生產環境中應停用 stack trace，以避免在發生 API 錯誤時洩露內部軟體細節。

步驟

1. ${post_edited_translations.segment}
2. 選取*介面*索引標籤。
3. ${post_edited_translations.segment}
   a. 展開折疊面板。
   b. 若要變更逾時時間，請指定 60 秒到 7 天之間的值。預設逾時時間為 15 分鐘。
   c. 若要停用此功能，請取消選取該複選框。
   d. 選取 **Save** 。

      新設定不會影響目前已登入的使用者。使用者必須重新登入或重新整理瀏覽器，新的逾時設定才能生效。

4. 若要變更 Management API stack trace 的設定：
   a. 展開折疊面板。
   b. 勾選此核取方塊，即可在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

      ${post_edited_translations.segment}

   c. 選取 **Save** 。

管理 StorageGRID 中的外部 SSH 存取

透過封鎖或允許外部存取來管理傳入網格流量的 SSH 存取。管理 SSH 外部存取不會影響網格中節點之間的流量。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

關於此任務

為了增強系統安全性，預設會封鎖外部 SSH 存取。如果您需要執行需要傳入 SSH 存取的工作（例如疑難排解），請暫時允許外部存取。完成工作後，請封鎖外部存取。

步驟

1. ${post_edited_translations.segment}
2. 選取 **Block SSH** 索引標籤。
3. 使用「封鎖傳入 SSH 存取」選項來管理外部 SSH 存取：
   a. 選取此核取方塊可封鎖存取（預設）。
   b. 取消選取核取方塊以允許存取。

   需要服務筆記型電腦與所有其他網格節點之間在連接埠 22 上的存取權限。完成維護工作時，請移除連接埠 22 的存取權限。

4. 選取 **Save** 。