配置安全設定

StorageGRID software

NetApp
May 29, 2026

目錄

配置安全設定

管理 TLS 和 SSH 策略

TLS 和 SSH 原則決定使用哪些協定和密碼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。

安全性策略控制 TLS 和 SSH 如何加密傳輸中的資料。一般來說，使用現代相容性（預設）策略，除非您的系統需要符合通用標準或您需要使用其他密碼。

某些StorageGRID服務尚未更新以使用這些原則中的密碼。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

選擇安全策略

步驟

1. 選擇*配置* > 安全 > 安全設定。

   *TLS 和 SSH 策略*標籤顯示可用的策略。目前有效的策略在策略圖塊上以綠色複選標記表示。

2. 查看圖塊以了解可用的策略。

政策	描述
現代相容性（預設）	如果您需要強加密並且除非您有特殊要求，請使用預設策略。此策略與大多數 TLS 和 SSH 用戶端相容。
舊版相容性	如果您需要為舊客戶端提供額外的相容性選項，請使用此原則。此策略中的附加選項可能會使其安全性低於現代相容性策略。
通用標準	如果您需要通用標準認證，請使用此政策。

政策	描述
FIPS 嚴格	如果您需要通用標準認證並且需要使用NetApp加密安全模組 3.0.8 將外部用戶端連接到負載平衡器端點、租用戶管理器和網格管理器，請使用此原則。使用此策略可能會降低效能。 注意：選擇此策略後，所有節點都必須"以滾動方式重啟"啟動NetApp加密安全模組。使用*維護* > *滾動重新啟動*來啟動和監控重新啟動。
風俗	如果您需要套用自己的密碼，請建立自訂原則。

3. 要查看有關每個策略的密碼、協定和演算法的詳細信息，請選擇*查看詳細資訊*。
4. 若要變更目前策略，請選擇*使用策略*。

   政策圖塊上的「目前政策」旁邊會出現一個綠色複選標記。

建立自訂安全性策略

如果您需要套用自己的密碼，您可以建立自訂原則。

步驟

1. 從與您要建立的自訂策略最相似的策略的圖塊中，選擇「查看詳細資訊」。
2. 選擇*複製到剪貼簿*，然後選擇*取消*。

3. 從*自訂策略*圖塊中，選擇*配置和使用*。
4. 貼上您複製的 JSON 並進行所需的更改。
5. 選擇*使用策略*。

   自訂策略圖塊上的「目前策略」旁邊會出現一個綠色複選標記。

6. 或者，選擇「編輯配置」對新的自訂策略進行更多變更。

暫時恢復預設安全策略

如果您設定了自訂安全性策略，且設定的 TLS 策略與"設定伺服器憑證"。

您可以暫時恢復預設安全性策略。

步驟

1. 登入管理節點：
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 輸入 `Passwords.txt`文件。
   c. 輸入以下命令切換到root： `su -`
   d. 輸入 `Passwords.txt`文件。

      當您以 root 身分登入時，提示字元將從 `$`到 `#`。

2. 運行以下命令：

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

3. 從 Web 瀏覽器存取相同管理節點上的網格管理器。
4. 請依照以下步驟操作選擇安全策略重新配置策略。

設定網路和物件安全

您可以設定網路和物件安全性來加密儲存的對象，阻止某些 S3 請求，或允許用戶端連接到儲存節點使用 HTTP 而不是 HTTPS。

儲存物件加密

儲存物件加密可以對透過 S3 提取的所有物件資料進行加密。預設情況下，儲存的物件未加密，但您可以選擇使用 AES-128 或 AES-256 加密演算法來加密物件。啟用該設定後，所有新攝取的物件都會被加密，但現有儲存的物件不會發生任何變更。如果停用加密，目前加密的物件仍保持加密，但新攝取的物件不會被加密。

儲存物件加密設定僅適用於尚未透過儲存桶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信息，請參閱"查看StorageGRID加密方法"。

防止客戶端修改

防止客戶端修改是一個系統範圍的設定。當選擇“防止客戶端修改”選項時，以下請求將被拒絕。

S3 REST API

- DeleteBucket 請求
- 任何修改現有物件的資料、使用者定義的元資料或 S3 物件標記的請求

為儲存節點連線啟用 HTTP

預設情況下，客戶端應用程式使用 HTTPS 網路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，您不需要使用此選項（因為您可以"配置每個負載平衡器端點"使用 HTTP 或 HTTPS)。

看"摘要：客戶端連接的 IP 位址和連接埠"了解 S3 用戶端使用 HTTP 或 HTTPS 連接到儲存節點時使用哪些連接埠。

選擇選項

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您擁有 Root 存取權限。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“網路和物件”標籤。
3. 對於儲存對象加密，如果您不想加密儲存對象，請使用 **None**（預設）設置，或選擇 **AES-128** 或 **AES-256** 來加密儲存對象。
4. 如果您想阻止 S3 用戶端發出特定請求，可以選擇「阻止客戶端修改」。

   如果您更改此設置，則大約需要一分鐘才能應用新設置。配置的值被緩存，以提高效能和擴展性。

5. 如果用戶端直接連接到儲存節點並且您想要使用 HTTP 連接，則可以選擇*為儲存節點連接啟用 HTTP*。

   為生產網格啟用 HTTP 時要小心，因為請求將以未加密的形式傳送。

6. 選擇*儲存*。

更改介面安全設定

透過介面安全性設置，您可以控制當使用者處於非活動狀態的時間超過指定時間時是否將其註銷，以及是否在 API 錯誤回應中包含堆疊追蹤。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"Root存取權限"。

關於此任務

*安全設定*頁麵包括*瀏覽器不活動逾時*和*管理 API 堆疊追蹤*設定。

瀏覽器不活動逾時

指示使用者登出之前瀏覽器可以處於非活動狀態的時間。預設值為 15 分鐘。

瀏覽器不活動逾時也受以下因素控制：

- 一個單獨的、不可設定的StorageGRID計時器，用於系統安全。每個使用者的身份驗證令牌在使用者登入 16 小時後過期。當使用者的身份驗證過期時，該使用者將自動登出，即使瀏覽器不活動逾時已停用或尚未達到瀏覽器逾時值。若要更新令牌，使用者必須重新登入。
- 身分提供者的逾時設置，假設為StorageGRID啟用了單一登入 (SSO)。

  如果啟用了 SSO 並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 。看"配置單一登入" 。

管理 **API** 堆疊追蹤

控制是否在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

預設此選項是停用的，但您可能希望為測試環境啟用此功能。一般來說，您應該在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇“介面”選項卡。
3. 若要更改瀏覽器不活動逾時設定：
   a. 展開手風琴。
   b. 若要變更逾時期限，請指定 60 秒到 7 天之間的值。預設超時時間為 15 分鐘。
   c. 若要停用此功能，請取消選取該複選框。
   d. 選擇*儲存*。

      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刷新瀏覽器才能使新的逾時設定生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開手風琴。
   b. 選取該複選框以在網格管理器和租用戶管理器 API 錯誤回應中傳回堆疊追蹤。

      在生產環境中停用堆疊追蹤，以避免在發生 API 錯誤時洩露內部軟體詳細資訊。

   c. 選擇*儲存*。

版權資訊

商標資訊