設定安全性設定

StorageGRID 11.8

NetApp
May 10, 2024

目錄

設定安全性設定

管理 TLS 和 SSH 原則

TLS 和 SSH 原則決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性原則控制 TLS 和 SSH 如何加密移動中的資料。一般而言、請使用現代化相容性（預設）原則、除非您的系統需要符合一般準則、或您需要使用其他密碼。

某些 StorageGRID 服務尚未更新、無法在這些原則中使用密碼。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

選取安全性原則

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。

   「 *TLS 與 SSH 原則 * 」標籤會顯示可用的原則。目前作用中的原則會在原則方塊上以綠色核取記號表示。

2. 檢閱方塊以瞭解可用的原則。

原則	說明
現代化相容性（預設）	如果您需要增強式加密、而且沒有特殊要求、請使用預設原則。此原則與大多數 TLS 和 SSH 用戶端相容。
舊版相容性	如果您需要舊版用戶端的其他相容性選項、請使用此原則。此原則中的其他選項可能會使其比現代相容性原則更不安全。
一般準則	如果您需要通用準則認證、請使用此原則。

原則	說明
FIPS 嚴格	如果您需要通用準則認證、而且需要使用 NetApp 密碼編譯安全模組 3.0.8 來連接負載平衡器端點、租戶管理器和 Grid Manager 、請使用此原則。使用此原則可能會降低效能。 • 注意 * ：選取此原則之後、所有節點都必須是 "以不連續的方式重新開機" 啟動 NetApp 密碼編譯安全性模組。使用 * 維護 * > * 循環重新開機 * 來啟動和監控重新開機。
自訂	如果您需要套用自己的密碼、請建立自訂原則。

3. 若要查看每個原則的密碼、通訊協定和演算法的詳細資料、請選取 * 檢視詳細資料 * 。
4. 若要變更目前的原則、請選取 * 使用原則 * 。

   原則方塊上的 * 目前原則 * 旁會出現綠色核取記號。

建立自訂安全性原則

如果您需要套用自己的密碼、可以建立自訂原則。

步驟

1. 從最類似您要建立之自訂原則的原則方塊中、選取 * 檢視詳細資料 * 。
2. 選取 * 複製到剪貼簿 * 、然後選取 * 取消 * 。

3. 從 * 自訂原則 * 方塊中、選取 * 設定與使用 * 。
4. 貼上您複製的 JSON 、然後進行任何必要的變更。
5. 選取 * 使用原則 * 。

   「自訂原則」方塊的 * 目前原則 * 旁會出現綠色核取記號。

6. 您也可以選擇 * 編輯組態 * 來對新的自訂原則進行更多變更。

暫時恢復為預設的安全性原則

如果您設定了自訂安全性原則、如果設定的 TLS 原則與不相容、則可能無法登入 Grid Manager "已設定的伺服器憑證"。

您可以暫時還原為預設的安全性原則。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@_Admin_Node_IP_`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。
2. 執行下列命令：

   ```
   restore-default-cipher-configurations
   ```
3. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。
4. 請依照中的步驟進行 選取安全性原則 重新設定原則。

設定網路和物件安全性

您可以設定網路和物件安全性來加密儲存的物件、防止某些 S3 和 Swift 要求、或允許用戶端連線至儲存節點使用 HTTP 而非 HTTPS 。

儲存的物件加密

儲存的物件加密可在透過 S3 擷取時、加密所有物件資料。根據預設、儲存的物件不會加密、但您可以選擇使用 AES - 128 或 AES - 256 加密演算法來加密物件。啟用此設定時、所有新擷取的物件都會加密、但不會對現有的儲存物件進行任何變更。如果停用加密、目前加密的物件仍會保持加密狀態、但新擷取的物件不會加密。

「儲存的物件加密」設定僅適用於未透過貯體層級或物件層級加密進行加密的 S3 物件。

如需 StorageGRID 加密方法的詳細資訊、請參閱 "檢閱StorageGRID 功能加密方法"。

防止用戶端修改

防止用戶端修改是全系統的設定。當選擇 * 防止用戶端修改 * 選項時、會拒絕下列要求。

S3 REST API

- 刪除 Bucket 要求
- 任何修改現有物件資料、使用者定義中繼資料或S3物件標記的要求

Swift REST API

- 刪除Container要求
- 要求修改任何現有物件。例如、下列作業會遭拒：「放置覆寫」、「刪除」、「中繼資料更新」等。

啟用 HTTP 以進行儲存節點連線

根據預設、用戶端應用程式會使用 HTTPS 網路傳輸協定來直接連線至儲存節點。您可以選擇性地為這些連線啟用HTTP、例如在測試非正式作業網格時。

只有當 S3 和 Swift 用戶端需要直接與儲存節點建立 HTTP 連線時、才可使用 HTTP 進行儲存節點連線。您不需要將此選項用於僅使用 HTTPS 連線的用戶端或連線至負載平衡器服務的用戶端（因為您可以 "設定每個負載平衡器端點" 使用 HTTP 或 HTTPS ）。

請參閱 "摘要：用於用戶端連線的IP位址和連接埠" 瞭解使用 HTTP 或 HTTPS 連線至儲存節點時、 S3 和 Swift 用戶端使用的連接埠。

選取選項

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有root存取權限。

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選取 * 網路和物件 * 索引標籤。
3. 對於儲存的物件加密、如果您不想加密儲存的物件、請使用 * 無 * （預設）設定、或選取 * AES-128* 或 * AES-256* 來加密儲存的物件。
4. 如果您想要防止 S3 和 Swift 用戶端提出特定要求、請選擇性地選取 * 防止用戶端修改 * 。

   如果您變更此設定、則需要約一分鐘的時間才能套用新設定。系統會快取設定的值、以利效能與擴充。

5. 如果用戶端直接連線至儲存節點、且您想使用 HTTP 連線、則可選擇 * 啟用儲存節點連線的 HTTP * 。

   啟用正式作業網格的HTTP時請務必小心、因為要求會以未加密的方式傳送。

6. 選擇*保存*。

變更介面安全性設定

介面安全性設定可讓您控制使用者是否在超過指定時間的非作用中狀態下登出、以及是否在 API 錯誤回應中包含堆疊追蹤。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。

- 您有 "root 存取權限"。

關於這項工作

「 * 安全性設定 * 」頁面包含 * 瀏覽器閒置逾時 * 和 * 管理 API 堆疊追蹤 * 設定。

瀏覽器閒置逾時

指出使用者的瀏覽器在登出之前可以停用多久。預設值為15分鐘。

瀏覽器閒置逾時也由下列項目控制：

- 另有一個不可設定StorageGRID 的獨立式計時功能、可用於系統安全性。每個使用者的驗證權杖會在使用者登入後 16 小時過期。當使用者的驗證過期時、該使用者會自動登出、即使瀏覽器閒置逾時已停用、或瀏覽器逾時的值尚未達到。若要續約權杖、使用者必須重新登入。
- 假設 StorageGRID 已啟用單一登入（ SSO ）、則身分識別提供者的逾時設定。

  如果啟用 SSO 且使用者的瀏覽器逾時、使用者必須重新輸入其 SSO 認證、才能再次存取 StorageGRID 。請參閱 "設定單一登入"。

管理 **API** 堆疊追蹤

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、但您可能想要在測試環境中啟用此功能。一般而言、您應該在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選擇 * 介面 * 標籤。
3. 若要變更瀏覽器閒置逾時的設定：
   a. 展開折疊。
   b. 若要變更逾時期間、請指定介於 60 秒到 7 天之間的值。預設逾時為 15 分鐘。
   c. 若要停用此功能、請取消選取核取方塊。
   d. 選擇*保存*。

      新設定不會影響目前登入的使用者。使用者必須重新登入或重新整理瀏覽器、新的逾時設定才會生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開折疊。
   b. 選取此核取方塊可在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

      ! 在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。
   c. 選擇*保存*。