控制防火牆
StorageGRID software

NetApp
May 29, 2026

目錄

控制防火牆

控制外部防火牆的訪問

您可以在外部防火牆處開啟或關閉特定連接埠。

您可以透過開啟或關閉外部防火牆上的特定連接埠來控制對StorageGRID管理節點上的使用者介面和 API 的存取。例如，除了使用其他方法來控制系統存取之外，您可能還希望阻止租戶連接到防火牆處的網格管理器。

如果要設定StorageGRID內部防火牆，請參閱"配置內部防火牆"。

港口	描述	如果連接埠開放...
443	管理節點的預設 HTTPS 連接埠	Web 瀏覽器和管理 API 用戶端可以存取網格管理器、網格管理 API、租用戶管理器和租用戶管理 API。 *注意：*連接埠 443 也用於一些內部流量。
8443	管理節點上的網格管理器連接埠受限	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取網格管理器和網格管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取租用戶管理器或租用戶管理 API。 • 內部內容請求將被拒絕。
9443	管理節點上的限制租用戶管理器端口	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取租用戶管理器和租用戶管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取網格管理器或網格管理 API。 • 內部內容請求將被拒絕。

受限的網格管理器或租戶管理器連接埠上不提供單一登入 (SSO)。如果您希望使用者透過單一登入進行驗證，則必須使用預設 HTTPS 連接埠 (443)。

相關資訊

- "Sign in入網格管理器"
- "建立租用戶帳戶"
- "外部溝通"

管理內部防火牆控制

StorageGRID在每個節點上都包含一個內部防火牆，透過讓您能夠控制對節點的網路存取來增強網格的安全性。使用防火牆阻止除特定網格部署所需連接埠之外的所有連接埠的網路存取。您在防火牆控制頁面上所做的設定變更將部署到每個節點。

使用防火牆控制頁面上的三個標籤來自訂網格所需的存取權限。

- 特權位址清單：使用此標籤允許選擇存取已關閉的連接埠。您可以使用「管理外部存取」標籤以 CIDR 表示法新增可存取已關閉連接埠的 IP 位址或子網路。
- 管理外部存取：使用此選項卡關閉預設開啟的端口，或重新開啟先前關閉的端口。
- 不受信任的客戶端網路：使用此選項卡指定節點是否信任來自客戶端網路的入站流量。

  此標籤上的設定將覆蓋「管理外部存取」標籤中的設定。

  - 具有不受信任的客戶端網路的節點將僅接受該節點上配置的負載平衡器端點連接埠（全域、節點介面和節點類型綁定端點）上的連線。
  - 無論「管理外部網路」標籤上的設定為何，負載平衡器端點連接埠都是不受信任的用戶端網路上唯一開放的連接埠。
  - 當受信任時，管理外部存取標籤下開啟的所有連接埠以及用戶端網路上開啟的任何負載平衡器端點都是可存取的。

> ⓘ 您在一個選項卡上所做的設定可能會影響您在另一個選項卡上所做的存取變更。請務必檢查所有選項卡上的設置，以確保您的網路按照您預期的方式運作。

若要設定內部防火牆控制，請參閱"配置防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

特權地址清單和管理外部存取選項卡

特權位址清單標籤可讓您註冊一個或多個被授予存取已關閉的網格連接埠的 IP 位址。管理外部存取標籤可讓您關閉對選定外部連接埠或所有開啟的外部連接埠（外部連接埠是預設非網格節點可存取的連接埠）的外部存取。這兩個選項卡通常可以一起使用，以自訂您需要允許電網的精確網路存取。

> ⓘ 預設情況下，特權 IP 位址沒有內部網格連接埠存取權限。

範例 **1**：使用跳轉主機執行維護任務

假設您想使用跳轉主機（安全強化的主機）進行網路管理。您可以使用以下一般步驟：

1. 使用特權位址清單標籤新增跳轉主機的IP位址。
2. 使用“管理外部存取”標籤來阻止所有連接埠。

> ⚠ 在封鎖連接埠 443 和 8443 之前新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，網格中管理節點上的所有外部連接埠都將被阻止，跳轉主機除外。然後，您可以使用跳轉主機更安全地在電網上執行維護任務。

範例 **2**：鎖定敏感端口

假設您想要鎖定敏感連接埠和該連接埠上的服務（例如，連接埠 22 上的 SSH）。您可以使用以下一般步驟：

1. 使用特權位址清單標籤僅向需要存取該服務的主機授予存取權限。
2. 使用“管理外部存取”標籤來阻止所有連接埠。

> 在阻止存取指派給網格管理器和租用戶管理員的任何連接埠（預設連接埠為 443 和 8443）之前，請新增特權 IP 位址。任何目前連接到被封鎖連接埠的使用者（包括您）都將失去對網格管理器的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

儲存配置後，連接埠 22 和 SSH 服務將可供特權位址清單上的主機使用。無論請求來自哪個接口，所有其他主機都將被拒絕存取該服務。

範例 **3**：停用對未使用的服務的訪問

在網路級別，您可以停用一些您不想使用的服務。例如，要阻止 HTTP S3 用戶端流量，您可以使用「管理外部存取」標籤上的切換按鈕來封鎖連接埠 18084。

不受信任的客戶端網路選項卡

如果您使用用戶端網絡，則可以透過僅在明確配置的端點上接受入站用戶端流量來協助保護StorageGRID免受惡意攻擊。

預設情況下，每個網格節點上的客戶端網路都是_受信任的_。也就是說，預設情況下， StorageGRID信任所有"可用的外部連接埠"。

您可以透過指定每個節點上的用戶端網路為_不受信任的_來減少對StorageGRID系統的惡意攻擊的威脅。如果節點的用戶端網路不受信任，則該節點僅接受明確配置為負載平衡器端點的連接埠上的入站連線。看"配置負載平衡器端點"和"配置防火牆控制"。

範例 **1**：網關節點僅接受 **HTTPS S3** 請求

假設您希望網關節點拒絕用戶端網路上除 HTTPS S3 請求之外的所有入站流量。您將執行以下常規步驟：

1. 從"負載平衡器端點"頁面上，在連接埠 443 上透過 HTTPS 為 S3 配置負載平衡器端點。
2. 從防火牆控制頁面中，選擇不受信任以指定網關節點上的用戶端網路不受信任。

儲存設定後，網關客戶端網路上的所有入站流量都將被丟棄，但連接埠 443 上的 HTTPS S3 請求和 ICMP 回顯（ping）請求除外。

範例 **2**：儲存節點發送 **S3** 平台服務請求

假設您想要啟用來自儲存節點的出站 S3 平台服務流量，但您想要阻止用戶端網路上到該儲存節點的任何入站連線。您將執行以下常規步驟：

- 從防火牆控制頁面的不受信任的用戶端網路標籤中，指示儲存節點上的用戶端網路不受信任。

儲存配置後，儲存節點不再接受客戶端網路上的任何傳入流量，但它繼續允許向配置的平台服務目標發出出站請求。

範例 **3**：將對網格管理器的存取限制在子網路內

假設您只想允許 Grid Manager 存取特定子網路。您將執行以下步驟：

1. 將管理節點的客戶端網路附加到子網路。
2. 使用不受信任的客戶端網路標籤將客戶端網路配置為不受信任。
3. 建立管理介面負載平衡器端點時，輸入連接埠並選擇該連接埠將存取的管理介面。
4. 對於不受信任的客戶端網絡，選擇「是」。
5. 使用「管理外部存取」標籤來封鎖所有外部連接埠（無論是否為該子網路外的主機設定了特權 IP 位址）。

儲存配置後，只有您指定的子網路上的主機才能存取網格管理器。所有其他主機均被封鎖。

配置內部防火牆

您可以設定StorageGRID防火牆來控制對StorageGRID節點上特定連接埠的網路存取。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你有"特定存取權限"。
- 您已查看了"管理防火牆控制"和"網路指南"。
- 如果您希望管理節點或網關節點僅在明確配置的端點上接受入站流量，則您已定義負載平衡器端點。

> 變更客戶端網路的配置時，如果尚未配置負載平衡器端點，則現有客戶端連線可能會失敗。

關於此任務

StorageGRID在每個節點上都包含一個內部防火牆，可讓您開啟或關閉網格節點上的某些連接埠。您可以使用防火牆控制標籤來開啟或關閉網格網路、管理網路和用戶端網路上預設開啟的連接埠。您也可以建立可以存取已關閉的網格連接埠的特權 IP 位址清單。如果您使用用戶端網絡，您可以指定節點是否信任來自客戶端網路的入站流量，並且可以設定客戶端網路上特定連接埠的存取。

將對網格外部 IP 位址開放的連接埠數量限制為僅絕對必要的端口，可增強網格的安全性。您使用三個防火牆控制標籤上的設定來確保僅開啟所需的連接埠。

有關使用防火牆控制的詳細資訊（包括範例），請參閱"管理防火牆控制"。

有關外部防火牆和網路安全的更多信息，請參閱"控制外部防火牆的訪問"。

存取防火牆控制

步驟

1. 選擇*設定* > 安全 > 防火牆控制。

   此頁面上的三個選項卡的描述如下"管理防火牆控制"。

2. 選擇任意選項卡來配置防火牆控制。

   您可以按任意順序使用這些選項卡。您在一個選項卡上設定的配置不會限制您在其他選項卡上可以執行的操作；但是，您在一個選項卡上所做的配置更改可能會更改在其他選項卡上配置的連接埠的行為。

特權地址列表

您可以使用「特權位址清單」標籤授予主機對預設關閉或透過「管理外部存取」標籤上的設定關閉的連接埠的存取權。

預設情況下，特權 IP 位址和子網路沒有內部網格存取權限。此外，即使在「管理外部存取」標籤中被阻止，也可以存取在「特權位址清單」標籤中開啟的負載平衡器端點和其他連接埠。

「特權位址清單」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在特權位址清單標籤上，輸入要授予對封閉連接埠的存取權限的位址或 IP 子網路。
2. 或者，選擇*以 CIDR 表示法新增另一個 IP 位址或子網路*來新增其他特權用戶端。

   將盡可能少的地址添加到特權清單中。

3. 或者，選擇*允許特權 IP 位址存取StorageGRID內部連接埠*。看"StorageGRID內部連接埠" 。

   此選項刪除了一些內部服務的保護。如果可能的話，將其保持禁用狀態。

4. 選擇*儲存*。

管理外部訪問

當在「管理外部存取」標籤中關閉某個端口時，任何非網格 IP 位址都無法存取該端口，除非您將該 IP 位址新增至特權位址清單。您只能關閉預設開啟的端口，並且只能打開您已關閉的端口。

「管理外部存取」標籤上的設定不能覆蓋「不受信任的用戶端網路」標籤上的設定。例如，如果某個節點不受信任，則即使在「管理外部存取」標籤上開啟了連接埠 SSH/22，該連接埠也會在用戶端網路上被封鎖。不受信任的客戶端網路標籤上的設定將覆蓋客戶端網路上的已關閉連接埠（例如 443、8443、9443）。

步驟

1. 選擇*管理外部存取*。此標籤顯示一個表，其中包含網格中節點的所有外部連接埠（預設非網格節點可存取的連接埠）。
2. 使用以下選項配置要開啟和關閉的連接埠：

   - 使用每個連接埠旁邊的開關來開啟或關閉選定的連接埠。
   - 選擇*開啟所有顯示的連接埠*以開啟表中列出的所有連接埠。
   - 選擇*關閉所有顯示的連接埠*以關閉表中列出的所有連接埠。

     如果您關閉 Grid Manager 連接埠 443 或 8443，則目前連接到封鎖連接埠的任何使用者（包括您）都會失去對 Grid Manager 的存取權限，除非他們的 IP 位址已新增至特權位址清單中。

使用表格右側的捲軸確保您已查看所有可用連接埠。使用搜尋欄位輸入連接埠號碼來尋找任何外部連接埠的設定。您可以輸入部分連接埠號碼。例如，如果輸入 **2**，則會顯示名稱中包含字串「2」的所有連接埠。

3. 選擇“儲存”

不受信任的客戶端網絡

如果節點的用戶端網路不受信任，則該節點僅接受配置為負載平衡器端點的連接埠上的入站流量，以及（可選）您在此標籤上選擇的其他連接埠。您也可以使用此標籤指定擴充功能中新增的新節點的預設值。

如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。

您在「不受信任的用戶端網路」標籤上所做的設定變更將覆蓋「管理外部存取」標籤上的設定。

步驟

1. 選擇*不受信任的客戶端網路*。
2. 在「設定新節點預設值」部分中，指定在擴充過程中將新節點新增至網格時的預設設定。
   - 受信任（預設）：當在擴充功能中新增節點時，其客戶端網路是受信任的。
   - 不受信任：當在擴展中添加節點時，其客戶端網路不受信任。

   根據需要，您可以返回此選項卡來更改特定新節點的設定。

   此設定不會影響StorageGRID系統中的現有節點。

3. 使用下列選項來選擇應僅允許在明確配置的負載平衡器端點或其他選定連接埠上進行用戶端連線的節點：
   - 選擇*不信任顯示的節點*將表中顯示的所有節點新增至不受信任的客戶端網路清單。
   - 選擇「信任顯示的節點」以從不受信任的客戶端網路清單中刪除表中顯示的所有節點。
   - 使用每個節點旁邊的切換按鈕將所選節點的客戶端網路設定為受信任或不受信任。

   例如，您可以選擇*不信任顯示的節點*將所有節點新增至不受信任的用戶端網路清單中，然後使用單一節點旁的切換按鈕將該單一節點新增至受信任的用戶端網路清單。

   使用表格右側的捲軸確保您已查看所有可用節點。使用搜尋欄位輸入節點名稱來尋找任何節點的設定。您可以輸入部分名稱。例如，如果輸入 **GW**，則會顯示名稱中包含字串「GW」的所有節點。

4. 選擇*儲存*。

   新的防火牆設定將立即套用並強制執行。如果尚未配置負載平衡器端點，現有客戶端連線可能會失敗。