控制防火牆
StorageGRID 11.8

NetApp
May 10, 2024

目錄

控制防火牆

控制外部防火牆的存取

您可以在外部防火牆開啟或關閉特定連接埠。

您可以StorageGRID 在外部防火牆開啟或關閉特定連接埠、以控制對使用者介面和API的存取。例如、除了使用其他方法來控制系統存取之外、您可能還想要防止租戶連線到防火牆的Grid Manager。

如果您想要設定 StorageGRID 內部防火牆、請參閱 "設定內部防火牆"。

連接埠	說明	如果連接埠已開啟...
443..	管理節點的預設HTTPS連接埠	Web瀏覽器和管理API用戶端可存取Grid Manager、Grid Management API、租戶管理程式和租戶管理API。 *附註：*連接埠443也用於部分內部流量。
8443	管理節點上的受限網格管理器連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取Grid Manager和Grid Management API。 • Web 瀏覽器和管理 API 用戶端無法存取租戶管理員或租戶管理 API 。 • 系統將拒絕內部內容的要求。
9443.	管理節點上的受限租戶管理程式連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取租戶管理程式和租戶管理API。 • Web 瀏覽器和管理 API 用戶端無法存取 Grid Manager 或 Grid Management API 。 • 系統將拒絕內部內容的要求。

單一登入（SSO）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。

相關資訊

- "登入Grid Manager"
- "建立租戶帳戶"
- "外部通訊"

管理內部防火牆控制

StorageGRID 在每個節點上都包含內部防火牆、可讓您控制對節點的網路存取、藉此增強網格的安全性。使用防火牆可防止網路存取所有連接埠、但您的特定網格部署所需的連接埠除外。您在「防火牆控制」頁面上所做的組態變更會部署到每個節點。

使用「防火牆控制」頁面上的三個索引標籤、自訂您網格所需的存取權限。

- * 貴賓位址清單 * ：使用此索引標籤可允許選取的存取已關閉的連接埠。您可以使用「管理外部存取」索引標籤、以 CIDR 表示法新增 IP 位址或子網路、以存取關閉的連接埠。
- * 管理外部存取 * ：使用此索引標籤關閉預設開啟的連接埠、或重新開啟先前關閉的連接埠。
- * 不受信任的用戶端網路 * ：使用此索引標籤指定節點是否信任來自用戶端網路的傳入流量。

  此索引標籤上的設定會覆寫「管理外部存取」索引標籤中的設定。

  - 具有不受信任用戶端網路的節點只會接受在該節點上設定的負載平衡器端點連接埠（全域、節點介面和節點類型繫結端點）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 _ 都是不受信任用戶端網路上唯一開放的連接埠 _ 。
  - 當信任時、所有在「管理外部存取」索引標籤下開啟的連接埠、以及在「用戶端網路」上開啟的任何負載平衡器端點都可以存取。

> 您在一個索引標籤上所做的設定可能會影響您在其他索引標籤上所做的存取變更。請務必檢查所有索引標籤上的設定、以確保您的網路運作方式符合預期。

若要設定內部防火牆控制、請參閱 "設定防火牆控制項"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

權限位址清單和管理外部存取索引標籤

「貴賓位址清單」標籤可讓您登錄一或多個 IP 位址、以存取已關閉的網格連接埠。「管理外部存取」索引標籤可讓您關閉外部存取、以存取選取的外部連接埠或所有開啟的外部連接埠（外部連接埠為非網格節點預設可存取的連接埠）。這兩個索引標籤通常可以一起使用、以自訂您需要的確切網路存取、以供網格使用。

> 預設情況下、特權 IP 位址沒有內部網格連接埠存取。

範例 **1** ：使用跳躍主機來執行維護工作

假設您想要使用跨接主機（安全強化的主機）進行網路管理。您可以使用下列一般步驟：

1. 使用「貴賓位址清單」標籤新增跳躍主機的 IP 位址。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

> 在封鎖連接埠 443 和 8443 之前、請先新增權限 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存組態之後、除了跳躍主機之外、所有主機都會封鎖網格中管理節點上的所有外部連接埠。然後、您可以使用跳躍主機更安全地在網格上執行維護工作。

範例 **2** ：限制存取 **Grid Manager** 和 **Tenant Manager**

假設基於安全考量、您想要限制對 Grid Manager 和 Tenant Manager （預設連接埠）的存取。您可以使用下列一般步驟：

1. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 443 。
2. 使用「管理外部存取」索引標籤上的切換開關、即可存取連接埠 8443 。
3. 使用「管理外部存取」索引標籤上的切換開關、即可存取連接埠 9443 。

儲存組態後、主機將無法存取連接埠 443 、但仍可透過連接埠 8443 存取 Grid Manager 、並透過連接埠 9443 存取 Tenant Manager 。

> 連接埠 443 、 8443 和 9443 是 Grid Manager 和 Tenant Manager 的預設連接埠。您可以切換任何連接埠、以限制對特定 Grid Manager 或 Tenant Manager 的存取。

範例 **3** ：鎖定敏感連接埠

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 ）。您可以使用下列一般步驟：

1. 使用「貴賓」位址清單標籤、僅授予需要存取服務的主機存取權。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

> 在您封鎖存取任何指派給存取 Grid Manager 和 Tenant Manager 的連接埠（預設連接埠為 443 和 8443 ）之前、請先新增特權 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存組態後、連接埠 22 和 SSH 服務將可用於權限位址清單上的主機。無論要求來自哪個介面、所有其他主機都將無法存取服務。

範例 **4** ：停用對未使用服務的存取

在網路層級、您可以停用一些不想使用的服務。例如、如果您不提供 Swift 存取、請執行下列一般步驟：

1. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 18083 。
2. 使用「管理外部存取」索引標籤上的切換開關來封鎖連接埠 18085 。

儲存組態後、儲存節點不再允許 Swift 連線、但仍允許存取未封鎖連接埠上的其他服務。

不受信任的用戶端網路索引標籤

如果您使用的是用戶端網路、StorageGRID 只有在明確設定的端點上接受傳入用戶端流量、才能保護不受惡意攻擊的安全。

依預設、每個網格節點上的用戶端網路為_truste_。也就是說、根據預設、 StorageGRID 會信任所有網格節點的傳入連線 "可用的外部連接埠"。

您可以StorageGRID 指定每個節點上的用戶端網路為_不受信任_、藉此減少對您的作業系統進行惡意攻擊的威脅。如果節點的用戶端網路不受信任、則節點只接受明確設定為負載平衡器端點之連接埠上的傳入連線。請參閱 "設定負載平衡器端點" 和 "設定防火牆控制項"。

範例**1**：閘道節點僅接受**HTTPS S3**要求

假設您希望閘道節點拒絕用戶端網路上除HTTPS S3要求以外的所有傳入流量。您可以執行下列一般步驟：

1. 從 "負載平衡器端點" 頁面中、在連接埠 443 上、透過 HTTPS 為 S3 設定負載平衡器端點。
2. 在「防火牆控制」頁面中、選取「不受信任」、以指定「閘道節點」上的「用戶端網路」不可信任。

儲存組態之後、除了連接埠443上的HTTPS S3要求和ICMP回應（ping）要求之外、閘道節點用戶端網路上的所有傳入流量都會捨棄。

範例**2**：儲存節點傳送**S3**平台服務要求

假設您想要從儲存節點啟用輸出 S3 平台服務流量、但想要防止任何傳入連線到用戶端網路上的該儲存節點。您可以執行以下一般步驟：

- 從「防火牆控制」頁面的「不受信任的用戶端網路」索引標籤、指出儲存節點上的用戶端網路不受信任。

儲存組態後、儲存節點將不再接受用戶端網路上的任何傳入流量、但仍會繼續允許傳出要求至設定的平台服務目的地。

範例 **3** ：將網格管理程式的存取限制在子網路上

假設您只想在特定子網路上允許 Grid Manager 存取。您可以執行下列步驟：

1. 將管理節點的用戶端網路連接至子網路。
2. 使用不受信任的用戶端網路索引標籤、將用戶端網路設定為不受信任。
3. 當您建立管理介面負載平衡器端點時、請輸入連接埠、然後選取連接埠將存取的管理介面。
4. 對於不受信任的用戶端網路、請選取 * 是 * 。
5. 使用管理外部存取索引標籤來封鎖所有外部連接埠（無論是否為該子網路以外的主機設定了權限 IP 位址）。

儲存組態之後、只有指定子網路上的主機才能存取 Grid Manager 。所有其他主機都會遭到封鎖。

設定內部防火牆

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

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱中的資訊 "管理防火牆控制" 和 "網路準則"。
- 如果您希望管理節點或閘道節點僅接受明確設定的端點上的傳入流量、則表示您已定義負載平衡器端點。

> 變更用戶端網路的組態時、如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

關於這項工作

StorageGRID 在每個節點上都有內部防火牆、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」索引標籤來開啟或關閉預設在 Grid Network 、 Admin Network 和 Client Network 上開啟的連接埠。您也可以建立權限 IP 位址清單、以存取已關閉的網格連接埠。如果您使用的是用戶端網路、您可以指定節點是否

信任來自用戶端網路的傳入流量、也可以設定用戶端網路上特定連接埠的存取。

將開放給網格外部 IP 位址的連接埠數量限制為只有絕對必要的連接埠數量、可增強網格的安全性。您可以使用三個防火牆控制索引標籤上的每個設定、確保只開啟所需的連接埠。

如需使用防火牆控制項的詳細資訊、包括範例、請參閱 "管理防火牆控制"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

存取防火牆控制

步驟

1. 選擇 * 組態 * > * 安全性 * > * 防火牆控制 * 。

   此頁面上的三個索引標籤如所述 "管理防火牆控制"。

2. 選取任何索引標籤以設定防火牆控制項。

   您可以依任何順序使用這些索引標籤。您在一個索引標籤上設定的組態不會限制您可以在其他索引標籤上執行的動作；不過、您在一個索引標籤上所做的組態變更可能會變更在其他索引標籤上設定的連接埠行為。

特殊權限位址清單

您可以使用「貴賓」位址清單標籤、將預設關閉或由「管理外部存取」標籤上的設定關閉的連接埠、授予主機存取權。

預設情況下、特權 IP 位址和子網路沒有內部網格存取。此外、即使在「管理外部存取」索引標籤中遭到封鎖、仍可存取負載平衡器端點和在「貴賓」位址清單索引標籤中開啟的其他連接埠。

「貴賓」位址清單標籤上的設定無法覆寫「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在「貴賓位址清單」標籤上、輸入您要授予封閉連接埠存取權的位址或 IP 子網路。
2. 您也可以選擇 * 以 CIDR 表示法新增其他 IP 位址或子網路 * 來新增其他的特殊權限用戶端。

   將盡可能少的位址新增至權限清單。

3. （可選）選擇 * 允許特權 IP 地址訪問 StorageGRID 內部端口 * 。請參閱 "內部連接埠StorageGRID"。

   此選項會移除內部服務的某些保護。如果可能、請將其停用。

4. 選擇*保存*。

管理外部存取

在「管理外部存取」索引標籤中關閉連接埠時、除非您將 IP 位址新增至特殊權限位址清單、否則任何非網格 IP 位址都無法存取連接埠。您只能關閉預設開啟的連接埠、而且只能開啟已關閉的連接埠。

「管理外部存取」索引標籤上的設定無法覆寫「不受信任的用戶端網路」索引標籤上的設定。例如、如果節點不受信任、則即使在「管理外部存取」索引標籤上開啟連接埠 SSH/22 、用戶端網路上的連接埠 SSH/22 也會遭到封鎖。「不受信任的用戶端網路」標籤上的設定會覆寫用戶端網路上的關閉連接埠（例如 443 、 8443 、 9443 ）。

步驟

1. 選取 * 管理外部存取 * 。 索引標籤會顯示一個表格、其中包含網格中節點的所有外部連接埠（預設為非網格節點可存取的連接埠）。
2. 使用下列選項設定您要開啟和關閉的連接埠：
   - 使用每個連接埠旁的切換開關來開啟或關閉選取的連接埠。
   - 選取 * 開啟所有顯示的連接埠 * 以開啟表格中列出的所有連接埠。
   - 選取 * 關閉所有顯示的連接埠 * 以關閉表格中列出的所有連接埠。

   如果您關閉 Grid Manager 連接埠 443 或 8443 、除非已將目前連線至封鎖連接埠的任何使用者（包括您）的 IP 位址新增至「貴賓」位址清單、否則他們將無法存取 Grid Manager 。

   使用表格右側的捲軸、確定您已檢視所有可用的連接埠。使用搜尋欄位、輸入連接埠編號、以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，如果您輸入 **2** ，則會顯示字串 "2" 做為其名稱一部分的所有連接埠。

3. 選擇*保存*

不受信任的用戶端網路

如果節點的用戶端網路不受信任、則節點只接受設定為負載平衡器端點的連接埠上的傳入流量、以及您在此索引標籤上選取的其他連接埠（選擇性）。您也可以使用此索引標籤來指定擴充中新增節點的預設設定。

如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

您在 * 不受信任的用戶端網路 * 標籤上所做的組態變更會覆寫 * 管理外部存取 * 標籤上的設定。

步驟

1. 選取 * 不受信任的用戶端網路 * 。
2. 在 Set New Node Default （設定新節點預設值）區段中、指定在擴充程序中將新節點新增至網格時的預設設定值。
   - * Trusted * （預設值）：當節點新增至擴充時、其 Client Network 會受到信任。
   - 不受信任：在擴充中新增節點時、其用戶端網路不受信任。

     視需要、您可以返回此索引標籤、變更特定新節點的設定。

     此設定不會影響StorageGRID 到您的不完善系統中現有的節點。

3. 使用下列選項來選取節點、這些節點只能在明確設定的負載平衡器端點或其他選取的連接埠上允許用戶端連

線：

- 選取 * 不信任顯示的節點 * 、將表格中顯示的所有節點新增至「不受信任的用戶端網路」清單。
- 選取 * 信任顯示的節點 * 、將表格中顯示的所有節點從「不受信任的用戶端網路」清單中移除。
- 使用每個節點旁的切換、將所選節點的 Client Network 設為 Trusted 或 Trusted 。

例如、您可以選取 * 在顯示的節點上不信任 * 、將所有節點新增至「不信任的用戶端網路」清單、然後使用個別節點旁的切換、將該單一節點新增至「信任的用戶端網路」清單。

使用表格右側的捲軸、確定您已檢視所有可用的節點。使用搜尋欄位輸入節點名稱、即可尋找任何節點的設定。您可以輸入部分名稱。例如、如果您輸入 * GW* 、則會顯示字串 "Gw" 做為其名稱一部分的所有節點。

4. 選擇*保存*。

新的防火牆設定會立即套用及強制執行。如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。