



控制防火牆

StorageGRID 11.7

NetApp
April 12, 2024

目錄

控制防火牆	1
控制外部防火牆的存取	1
管理內部防火牆控制	1
設定內部防火牆	4

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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。

此索引標籤也提供選項、可指定設定不受信任用戶端網路時要開啟的其他連接埠。這些連接埠可讓您存取 Grid Manager、Tenant Manager 或兩者。

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。
- 在「不受信任的用戶端網路」標籤下開啟的其他連接埠會在所有不受信任的用戶端網路上開啟、即使沒有設定負載平衡器端點也一樣。
- 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和所選的其他連接埠 _ 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、以存取已關閉的網路連接埠。「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 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。

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、只能在明確設定的端點或您在此索引標籤上選取的其他連接埠上接受傳入用戶端流量、以協助保護 StorageGRID 免受惡意攻擊。

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的連接埠傳入連線、以及使用「[防火牆控制](#)」頁面上的「不受信任的用戶端網路」索引標籤指定的任何其他連接埠。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. 在索引標籤的 * 「在不受信任的用戶端網路上開啟的其他連接埠」區段中、新增連接埠 443 或 8443 。
4. 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 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。
- 使用每個連接埠旁邊的切換、將所選節點的用戶端網路設為信任或不信任。

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. 您也可以選擇在不受信任的用戶端網路上開啟的任何其他連接埠。這些連接埠可讓您存取 Grid Manager 、Tenant Manager 或兩者。

例如、您可能想要使用此選項、以確保可在用戶端網路上存取 Grid Manager 進行維護。



這些附加連接埠會在用戶端網路上開啟、無論它們是否在「管理外部存取」標籤中關閉。

5. 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。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。