



控制防火牆 StorageGRID software

NetApp
July 23, 2026

目錄

控制防火牆	1
在外部防火牆控制 StorageGRID 存取	1
管理 StorageGRID 中的內部防火牆控制	1
特權位址清單和管理外部存取索引標籤	2
\${post_edited_translations.segment}	3
配置 StorageGRID 內部防火牆	4
\${post_edited_translations.segment}	4
\${post_edited_translations.segment}	5
管理外部存取	5
不受信任的用戶端網路	6

控制防火牆

在外部防火牆控制 **StorageGRID** 存取

`${post_edited_translations.segment}`

您可以透過在外部防火牆開啟或結案特定連接埠，控制對 StorageGRID Admin Nodes 上使用者介面和 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在防火牆處連線至 Grid Manager。

如果要設定 StorageGRID 內部防火牆，請參閱"[\\${post_edited_translations.segment}](#)"。

連接埠	說明	<code>\${post_edited_translations.segment}</code>
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 Grid Manager、Grid Management API、Tenant Manager 和 Tenant Management API。 <code>\${post_edited_translations.segment}</code>
8443	<code>\${post_edited_translations.segment}</code>	• <code>\${post_edited_translations.segment}</code> • Web 瀏覽器和管理 API 用戶端無法存取租戶管理器或租戶管理 API。 • <code>\${post_edited_translations.segment}</code>
9443	<code>\${post_edited_translations.segment}</code>	• Web 瀏覽器和管理 API 用戶端可以使用 HTTPS 存取租戶管理器和租戶管理 API。 • Web 瀏覽器和管理 API 用戶端無法存取 Grid Manager 或 Grid Management API。 • <code>\${post_edited_translations.segment}</code>



單一登入 (SSO) 在受限的 Grid Manager 或 Tenant Manager 連接埠上不可用。如果您希望使用者使用單一登入進行驗證，則必須使用預設的 HTTPS 連接埠 (443)。

相關資訊

- "[\\${post_edited_translations.segment}](#)"
- "[建立租戶帳戶](#)"
- "[\\${post_edited_translations.segment}](#)"

管理 **StorageGRID** 中的內部防火牆控制

StorageGRID 在每個節點上包含內部防火牆，透過控制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網路存取。您在防火牆控制頁面上所做的組態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您的網格所需的存取。

- 特權位址清單：使用此索引標籤允許對已結案連接埠進行選定的存取。您可以新增以 CIDR 表示法表示的 IP 位址或子網路，以存取使用「管理外部存取」索引標籤關閉的連接埠。
- 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。

此標籤上的設定置換「管理外部存取」標籤中的設定。

- 具有不受信任用戶端網路的節點，只接受在該節點上設定的負載平衡器端點連接埠上的連線（全域端點、節點介面及節點類型繫結端點）。
- 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_唯一開啟的連接埠_。
- `#{post_edited_translations.segment}`



在一個標籤頁中所做的設定可能會影響在另一個標籤頁中所做的存取變更。請務必檢查所有標籤頁中的設定，以確保您的網路運作符合預期。

若要設定內部防火牆控制，請參閱 "[設定防火牆控制](#)"。

如需更多關於外部防火牆與網路安全性的資訊，請參閱 "[#{post_edited_translations.segment}](#)"。

特權位址清單和管理外部存取索引標籤

「特權位址清單」標籤可讓您註冊一個或多個 IP 位址，這些位址將被授予對已關閉的網格連接埠的存取權限。「管理外部存取」標籤可讓您結案對選定外部連接埠或所有開啟的外部連接埠的外部存取（外部連接埠是指預設情況下非網格節點可存取的連接埠）。這兩個標籤通常可以結合使用，以自訂網格所需的精確網路存取權限。



特權 IP 位址預設情況下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工作

假設您要使用防禦主機（經過安全性強化之主機）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. `#{post_edited_translations.segment}`



在封鎖連接埠 443 和 8443 之前，請先新增特權 IP 位址。任何目前連線至被封鎖連接埠的使用者（包括您自己）都將失去對 Grid Manager 的存取權限，除非其 IP 位址已新增至特權位址清單中。

儲存您的組態後，除了 jump host 之外，您網格中 Admin 節點上的所有外部連接埠都將對所有主機進行區塊。接著，您可以使用 jump host，以更安全的方式在您的網格上執行維護工作。

範例 2：鎖定敏感連接埠

假設您想要鎖定敏感的連接埠以及該連接埠上的服務。您可以使用以下一般步驟：

1. 使用「特權位址清單」索引標籤，僅向需要存取該服務的主機授予存取權限。
2. `$_POST[post_edited_translations.segment]`



在封鎖任何用於存取 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。任何目前連線至已封鎖連接埠的使用者（包括您自己）都將失去對 Grid Manager 的存取權限，除非其 IP 位址已新增至特權位址清單中。

儲存組態之後，敏感的连接埠和該连接埠上的服務即可供特殊權限位址清單上的主機使用。無論要求來自哪個介面，所有其他主機都會被拒絕存取該服務。

範例 3：停用對未使用服務的存取

在網路層級上，您可以停用一些您不打算使用的服務。例如，若要封鎖 HTTP S3 用戶端流量，您可以使用「管理外部存取」標籤上的切換開關來封鎖連接埠 18084。

`$_POST[post_edited_translations.segment]`

如果您使用的是用戶端網路，可以透過僅在明確設定的端點上接受傳入用戶端流量，協助保護 StorageGRID 免受惡意攻擊。

預設情況下，每個網格節點上的用戶端網路都是受信任的。也就是說，預設情況下，StorageGRID 會信任所有“[可用外部連接埠](#)”上傳入每個網格節點的連線。

您可以透過將每個節點上的用戶端網路設定為「不受信任」來降低 StorageGRID 系統遭受惡意攻擊的風險。如果節點的用戶端網路不受信任，則該節點僅接受明確設定為負載平衡器端點的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](#)”。

`$_POST[post_edited_translations.segment]`

假設您希望閘道節點拒絕用戶端網路上除 HTTPS S3 請求之外的所有傳入流量。您可以執行以下一般步驟：

1. 從“[負載平衡器端點](#)”頁面，在連接埠 443 上設定 S3 over HTTPS 的負載平衡端點。
2. 在防火牆控制頁面中，選擇「不受信任」以指定閘道節點上的用戶端網路不受信任。

儲存組態後，閘道節點用戶端網路上的所有傳入流量將被捨棄，但連接埠 443 上的 HTTPS S3 請求和 ICMP 回顯（ping）請求除外。

`$_POST[post_edited_translations.segment]`

假設您想要從儲存節點啟用傳出 S3 平台服務流量，但希望阻止用戶端網路上到該儲存節點的任何傳入連線。您可以執行以下一般步驟：

- 在防火牆控制頁面的「不受信任的用戶端網路」索引標籤中，將儲存節點上的用戶端網路標記為不受信任。

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，但仍允許向已設定的平台服務目的地傳出請求。

範例 3：將對 Grid Manager 的存取限制在子網路內

假設您只想在特定子網路上允許 Grid Manager 存取。您需要執行以下步驟：

1. `${post_edited_translations.segment}`
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. 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. 針對「不受信任的用戶端網路」選取 **Yes**。
5. 使用「管理外部存取」標籤來鎖定所有外部連接埠（無論是否為該子網路以外的主機設定特權 IP 位址）。

在您儲存組態之後，只有您指定之子網路上的主機才能存取 Grid Manager。所有其他主機都會被區塊。

配置 StorageGRID 內部防火牆

`${post_edited_translations.segment}`

開始之前

- 您已使用 ["支援的網頁瀏覽器"](#) 登入 Grid Manager。
- 您有["特定存取權限"](#)。
- 您已查看 ["管理防火牆控制"](#) 和 ["\\${post_edited_translations.segment}"](#) 中的資訊。
- `${post_edited_translations.segment}`



變用戶端網路組態時，如果負載平衡器端點尚未設定，則現有用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，可讓您開啟或結案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，來開啟或結案網格網路、管理網路和用戶端網路上預設開啟的連接埠。您也可以建立一個特權 IP 位址清單，以存取已結案的網格連接埠。如果您使用的是用戶端網路，可以指定節點是否信任來自用戶端網路的傳入流量，並可以設定用戶端網路上特定連接埠的存取。

限制對網格外 IP 位址開啟的連接埠數量，僅開放絕對必要的連接埠，可增強網格的安全性。您可以使用三個防火牆控制標籤上的設定，確保僅開啟所需的連接埠。

如需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"](#)。

如需更多關於外部防火牆與網路安全性的資訊，請參閱 ["\\${post_edited_translations.segment}"](#)。

`${post_edited_translations.segment}`

步驟

1. `${post_edited_translations.segment}`

此頁面上的三個索引標籤說明於 ["管理防火牆控制"](#)。

2. `${post_edited_translations.segment}`

您可以依任何順序使用這些索引標籤。您在某個索引標籤上設定的組態不會限制您在其他索引標籤上所能執行的操作；然而，您在某個索引標籤上進行的組態變更可能會改變在其他索引標籤上設定的連接埠行為。

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

特權 IP 位址和子網路預設沒有內部網絡存取。此外，即使在「管理外部存取」索引標籤中被封鎖，在「特權位址清單」索引標籤中開啟的負載平衡器端點和其他連接埠仍可存取。



`${post_edited_translations.segment}`

步驟

1. 在 Privileged address list 索引標籤上，輸入您要授予結案連接埠存取權限的位址或 IP 子網路。
2. `${post_edited_translations.segment}`



盡量少將地址加入特權清單。

3. (可選) 選取「允許特權 IP 位址存取 StorageGRID 內部連接埠」。請參閱["StorageGRID 內部連接埠"](#)。



此選項會移除內部服務的部分保護。如果可能，請保持停用。

4. 選取 **Save**。

管理外部存取

在「管理外部存取」標籤中關閉連接埠後，除非您將 IP 位址新增至特權位址清單，否則任何非網格 IP 位址都無法存取該連接埠。您只能關閉預設開啟的連接埠，也只能開啟您已關閉的連接埠。



「管理外部存取」標籤中的設定無法置換「不受信任的用戶端網路」標籤中的設定。例如，如果某個節點不受信任，即使在「管理外部存取」標籤中連接埠 SSH/22 已開啟，則該連接埠在用戶端網路上也會被封鎖。「不受信任的用戶端網路」標籤中的設定置換用戶端網路上已關閉的連接埠（例如 443、8443、9443）。

步驟

1. 選擇 **Manage external access**。此標籤顯示一個表格，其中包含網格中節點的所有外部連接埠（預設非網格節點可以存取的連接埠）。
2. `${post_edited_translations.segment}`
 - 使用每個連接埠旁邊的切換按鈕開啟或關閉所選連接埠。
 - 選擇 **Open all displayed ports** 以開啟表格中列出的所有連接埠。
 - 選擇 **Close all displayed ports** 以結案表格中列出的所有連接埠。



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



使用表格右側的捲動軸，以確保您已檢視所有可用的埠。輸入埠號，即可使用搜尋欄位來尋找任何外部埠的設定。您可以輸入部分埠號。例如，如果您輸入 **2**，則會顯示名稱中包含字串「2」的所有埠。

3. 選擇 **Save**

不受信任的用戶端網路

如果節點的用戶端網路不受信任，則該節點僅接受設定為負載平衡器端點的連接埠上的傳入流量，以及（可選）您在此索引標籤中選擇的其他連接埠。您也可以使用此索引標籤為擴充中新增的節點指定預設設定。



`${post_edited_translations.segment}`

在「不受信任的用戶端網路」標籤上所做的組態變更會置換「管理外部存取」標籤上的設定。

步驟

1. `${post_edited_translations.segment}`
2. `${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
 - 不受信任：在擴充中新增節點時，其用戶端網路不受信任。

如有需要，您可以返回此標籤以變更特定新節點的設定。



此設定不會影響 StorageGRID 系統中的現有節點。

3. 使用下列選項選擇僅允許用戶端連線至明確設定的負載平衡器端點或其他選定連接埠的節點：

- 選擇「對顯示的節點取消信任」可將表中顯示的所有節點新增至「不受信任的用戶端網路」清單。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

例如，您可以選擇「對顯示的節點取消信任」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」清單中。



使用表格右側的捲軸，以確保您已檢視所有可用的節點。輸入節點名稱，即可使用搜尋欄位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**，則會顯示名稱中包含字串 "GW" 的所有節點。

4. 選取 **Save**。

新的防火牆設定會立即套用並強制執行。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 © 2026 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。