



## **TR-4626** : 負載平衡器

How to enable StorageGRID in your environment

NetApp  
July 05, 2024

# 目錄

|  |   |
|--|---|
| TR-4626：負載平衡器 .....                        | 1 |
| 將協力廠商負載平衡器搭配 StorageGRID 使用 .....          | 1 |
| 瞭解如何在 StorageGRID 中實作 HTTPS 的 SSL 憑證 ..... | 2 |
| 在 StorageGRID 中設定信任的協力廠商負載平衡器 .....        | 3 |
| 瞭解本機流量管理負載平衡器 .....                        | 3 |
| 瞭解 StorageGRID 組態的幾個使用案例 .....             | 6 |
| 驗證 StorageGRID 中的 SSL 連線 .....             | 9 |
| 瞭解 StorageGRID 的整體負載平衡需求 .....             | 9 |

# TR-4626：負載平衡器

## 將協力廠商負載平衡器搭配 StorageGRID 使用

瞭解協力廠商和全域負載平衡器在 StorageGRID 等物件儲存系統中的角色。

使用協力廠商負載平衡器實作 NetApp® StorageGRID® 的一般指南。

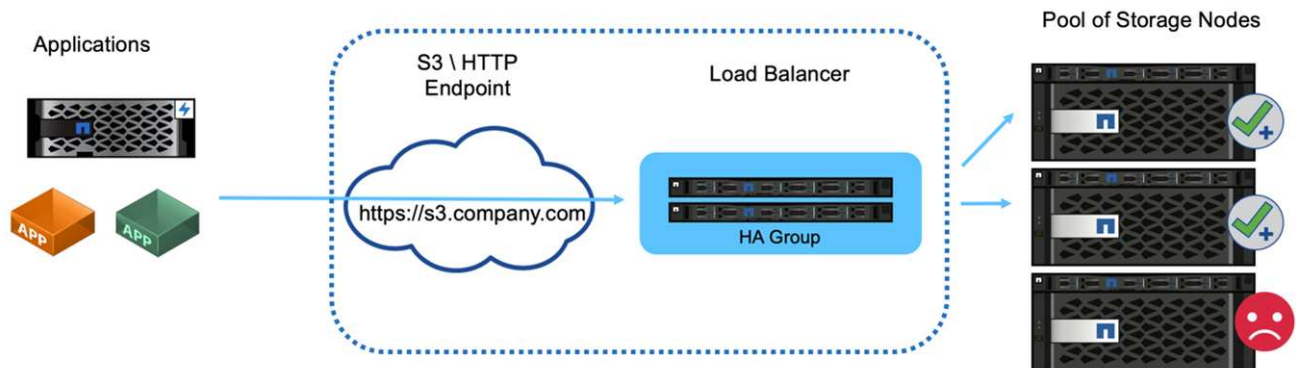
物件儲存是雲端儲存的同義詞、而且正如您所期望的、應用程式會透過 URL 利用雲端儲存位址來處理該儲存。在這個簡單的 URL 之後、StorageGRID 可以在單一站台或跨地理分佈式站台擴充容量、效能和耐用度。使這種簡易性成爲可能的元件是負載平衡器。

本文件旨在教導 StorageGRID 客戶有關負載平衡器選項的資訊、並提供第三方負載平衡器組態的一般指引。

### 負載平衡器基礎知識

負載平衡器是企業級物件儲存系統（例如 StorageGRID）的重要元件。StorageGRID 包含多個儲存節點、每個節點都可以呈現給定 StorageGRID 執行個體的整個簡易儲存服務（S3）名稱空間。負載平衡器可建立高可用度的端點、讓我們將 StorageGRID 節點放在後端。StorageGRID 在 S3 相容的物件儲存系統中是獨一無二的、因為它提供自己的負載平衡器、但也支援第三方或一般用途的負載平衡器、例如 F5、Citrix NetScaler、HA Proxy、NGINX 等等。

下圖使用範例 URL/ 完整網域名稱 (FQDN) 「s3.company.com」。負載平衡器會建立一個虛擬 IP（VIP）、透過 DNS 解析至 FQDN、然後將應用程式的任何要求導向至 StorageGRID 節點集區。負載平衡器會在每個節點上執行健全狀況檢查、只會建立與健全節點的連線。



圖中顯示 StorageGRID 提供的負載平衡器、但第三方負載平衡器的概念相同。應用程式會使用負載平衡器上的 VIP 建立 HTTP 工作階段、而流量會透過負載平衡器傳遞至儲存節點。根據預設、從應用程式到負載平衡器、從負載平衡器到儲存節點的所有流量都會透過 HTTPS 加密。HTTP 是受支援的選項。

### 本機和全域負載平衡器

負載平衡器有兩種類型：

- \* 本地交通經理（LTM）\*。在單一站台的節點集區上分散連線。
- \* 全球服務負載平衡器（GSLB）\*。跨多個站台分散連線、有效平衡 LTM 負載平衡器的負載。將 GSLB 視爲智慧型 DNS 伺服器。當用戶端要求 StorageGRID 端點 URL 時、GSLB 會根據可用度或其他因素（例如、哪個站台可爲應用程式提供較低的延遲）、將其解析為 LTM 的 VIP。雖然永遠需要 LTM、但根據

StorageGRID 站台數量和應用程式需求、GSLB 是選用的。

## StorageGRID 閘道節點負載平衡器與協力廠商負載平衡器的比較

相容於 S3 的物件儲存廠商、StorageGRID 獨家提供原生負載平衡器、可作為特定用途的應用裝置、VM 或容器使用。StorageGRID 提供的負載平衡器也稱為閘道節點。

對於尚未擁有負載平衡器（例如 F5、Citrix 等）的客戶、執行第三方負載平衡器可能非常複雜。StorageGRID 負載平衡器可大幅簡化負載平衡器作業。

Gateway Node 是企業級、高可用度和高效能負載平衡器。客戶可以選擇在同一個網格中實作閘道節點、協力廠商負載平衡器、甚至兩者。Gateway Node 是本機流量管理程式、而非 GSLB。

StorageGRID 負載平衡器具有下列優點：

- \* 簡易性 \*。資源集區的自動組態、健全狀況檢查、修補和維護、全都由 StorageGRID 管理。
- \* 效能 \*。StorageGRID 負載平衡器專用於 StorageGRID、因此您不會與其他應用程式競爭頻寬。
- \* 成本 \*。虛擬機器（VM）和容器版本均免費提供。
- \* 流量分類 \*。進階流量分類功能可讓 StorageGRID 特定的 QoS 規則與工作負載分析一起使用。
- \* 未來的 StorageGRID 特定功能 \*。StorageGRID 將繼續最佳化負載平衡器、並在即將推出的版本上新增創新功能。

如需部署 StorageGRID 閘道節點的詳細資訊，請參閱 ["本文檔StorageGRID"](#)。

## 何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID 文件中心 <https://docs.netapp.com/us-en/storagegrid-118/>
- NetApp StorageGRID 啟用 <https://docs.netapp.com/us-en/storagegrid-enable/>
- StorageGRID F5 負載平衡器設計考量 <https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/>
- Loadbalancer.org—Load 平衡 NetApp StorageGRID <https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/>
- Kemp —負載平衡 NetApp StorageGRID <https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID>

## 瞭解如何在 StorageGRID 中實作 HTTPS 的 SSL 憑證

瞭解在 StorageGRID 中實作 SSL 憑證的重要性和步驟。

如果您使用 HTTPS、則必須擁有安全通訊端層（SSL）憑證。SSL 通訊協定會識別用戶端和端點、並將它們驗證為信任的。SSL 也能加密流量。SSL 憑證必須由用戶端信任。若要達成此目的、SSL 憑證可以來自全球信任的憑證授權單位（CA）、例如 DigiCert、在基礎架構中執行的私有 CA、或是主機產生的自我簽署憑證。

使用全域信任的 CA 憑證是首選方法、因為不需要額外的用戶端端動作。憑證會載入負載平衡器或 StorageGRID、而用戶端則信任並連線至端點。

使用私有 CA 需要將根憑證和所有次級憑證新增至用戶端。信任私有 CA 憑證的程序可能會因用戶端作業系統和應用程式而異。例如、在 ONTAP for FabricPool 中、您必須將鏈中的每個憑證（根憑證、次級憑證、端點憑證）個別上傳至 ONTAP 叢集。

使用自我簽署的憑證需要用戶端信任提供的憑證、而不需要任何 CA 來驗證其真實性。有些應用程式可能不接受自我簽署的憑證、也無法忽略驗證。

SSL 憑證在用戶端負載平衡器 StorageGRID 路徑中的放置位置取決於您需要 SSL 終止的位置。您可以將負載平衡器設定為用戶端的終止端點、然後使用新的 SSL 憑證將負載平衡器重新加密或熱加密至 StorageGRID 連線。或者、您也可以通過流量、讓 StorageGRID 成為 SSL 終止端點。如果負載平衡器是 SSL 終止端點、則該憑證會安裝在負載平衡器上、其中包含 DNS 名稱 /URL 的主體名稱、以及任何其他將用戶端設定為透過負載平衡器連線至 StorageGRID 目標的 URL/DNS 名稱、包括任何萬用字元名稱。如果負載平衡器設定為通過、則必須在 StorageGRID 中安裝 SSL 憑證。同樣地、憑證必須包含 DNS 名稱 /URL 的主體名稱、以及任何其他設定用戶端透過負載平衡器連線至 StorageGRID 目標的 URL/DNS 名稱、包括任何萬用字元名稱。不需要在憑證中包含個別的儲存節點名稱、只有端點 URL 。

```
Subject DN: /C=US/postalCode=94089/ST=California/L=Sunnyvale/street=495 East Java Dr/O=NetApp, Inc./OU=IT1/OU=Unified Communication
s/CN=webscaledemo.netapp.com
Serial Number: 37:4C:6B:51:61:84:50:F8:7A:29:D9:83:24:12:36:2C
Issuer DN: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Organization Validation Secure Server CA
Issued On: 2019-05-23T00:00:00.000Z
Expires On: 2021-05-22T23:59:59.000Z
Alternative Names: DNS:webscaledemo.netapp.com
DNS:*.webscaledemo-rtp.netapp.com
DNS:*.webscaledemo.netapp.com
DNS:webscaledemo-rtp.netapp.com
SHA-1 Fingerprint: 60:91:44:E5:4F:7E:25:6B:B5:A0:19:87:D1:F2:8C:DD:AD:3A:88:CD
SHA-256 Fingerprint: FE:21:5D:BF:08:D9:5A:E5:09:CF:F6:3F:D3:5C:1E:9B:33:63:63:CA:25:2D:3F:39:0B:6A:B8:EC:08:BC:57:43
```

## 在 StorageGRID 中設定信任的協力廠商負載平衡器

瞭解如何在 StorageGRID 中設定信任的協力廠商負載平衡器。

如果您使用一或多個外部第 7 層負載平衡器、以及 S3 貯體或群組原則（以 IP 為基礎）、StorageGRID 必須判斷真正的傳送者 IP 位址。這是透過查看由負載平衡器插入要求的 X-Forwarded-for（XFF）標頭來達成的。由於直接傳送至儲存節點的要求很容易偽造 XFF 標頭、因此 StorageGRID 必須確認每個要求都是由信任的第 7 層負載平衡器路由。如果 StorageGRID 無法信任要求的來源、則會忽略 XFF 標頭。網格管理 API 可讓您設定信任的外部第 7 層負載平衡器清單。此全新 API 為私有 API、未來的 StorageGRID 版本可能會有所變更。如需最新資訊、請參閱知識庫文章 ["如何設定 StorageGRID 以搭配第三方第 7 層負載平衡器使用"](#)。

## 瞭解本機流量管理負載平衡器

探索本機流量管理負載平衡器的指引、並判斷最佳組態。

以下是第三方負載平衡器組態的一般指南。請與負載平衡器管理員合作、為您的環境決定最佳組態。

### 建立儲存節點資源群組

將 StorageGRID 儲存節點群組至資源集區或服務群組（術語可能與特定負載平衡器不同）。StorageGRID 儲存節點在下列連接埠上呈現 S3 API：

- S3 HTTPS : 18082
- S3 HTTP : 18084

大多數客戶選擇透過標準 HTTPS 和 HTTP 連接埠（443 和 80）、在虛擬伺服器上呈現 API。



每個 StorageGRID 站台都需要預設的三個儲存節點、其中兩個節點必須正常運作。

## 健全狀況檢查

協力廠商負載平衡器需要一種方法來判斷每個節點的健全狀況及其接收流量的資格。NetApp 建議使用 HTTP OPTIONS 方法來執行健全狀況檢查。負載平衡器會向每個個別的儲存節點發出 HTTP OPTIONS 要求、並預期會有 200 狀態回應。

如果有任何儲存節點未提供回應、則 200 該節點將無法服務儲存要求。您的應用程式和業務需求應決定這些檢查的逾時時間、以及負載平衡器所採取的行動。

例如、如果資料中心 1 的四個儲存節點中有三個關閉、您可能會將所有流量導向資料中心 2。

建議的輪詢間隔是每秒一次、在三次失敗檢查之後、將節點標示為離線。

### S3 健全狀況檢查範例

在以下範例中，我們會傳送 OPTIONS 並檢查 200 OK。我們使用的 OPTIONS 原因是 Amazon S3）不支援未經授權的要求。

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
* Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

## 檔案或內容型健全狀況檢查

一般而言、NetApp 不建議使用檔案型健全狀況檢查。例如、通常會在具有唯讀原則的貯體中建立小型檔案—healthcheck.htm。然後負載平衡器會擷取並評估此檔案。此方法有幾個缺點：

- \* 視單一帳戶而定。\*如果擁有該檔案的帳戶已停用、則健全狀況檢查會失敗、而且不會處理任何儲存要求。
- \* 資料保護規則。\*預設的資料保護方案是兩個複本的方法。在此案例中、如果裝載健全狀況檢查檔案的兩個儲存節點無法使用、健全狀況檢查會失敗、而且儲存要求不會傳送至健全的儲存節點、使網格離線。
- \* 稽核記錄檔位。\*負載平衡器每 X 分鐘從每個儲存節點擷取一次檔案、建立許多稽核記錄項目。
- \* 資源密集。\*每隔幾秒從每個節點擷取一次健全狀況檢查檔案、就會消耗網格和網路資源。

如果需要內容型健全狀況檢查、請使用專屬租戶搭配專用 S3 儲存區。

## 工作階段持續性

工作階段持續性（或黏性）是指允許指定 HTTP 工作階段持續的時間。依預設、儲存節點會在 10 分鐘後捨棄工作階段。較長的持續性可能會導致更好的效能、因為應用程式不需要為每個動作重新建立工作階段、但保持開啟這些工作階段會消耗資源。如果您確定工作負載會受惠、則可以減少第三方負載平衡器上的工作階段持續性。

## 虛擬代管型定址

虛擬託管樣式現在是 AWS S3 的預設方法、雖然 StorageGRID 和許多應用程式仍支援路徑樣式、但實作虛擬託管式支援是最佳做法。虛擬託管式要求的主機名稱中包含貯體。

若要支援虛擬代管樣式、請執行下列動作：

- 支援萬用字元 DNS 查詢：\*.s3.company.com
- 使用具有主體替代名稱的 SSL 憑證來支援萬用字元：\*.s3.company.com 有些客戶已表示對萬用字元憑證的使用有安全顧慮。StorageGRID 持續支援路徑樣式存取、FabricPool 等重要應用程式也同樣支援路徑樣式存取。也就是說、某些 S3 API 呼叫在沒有虛擬主機支援的情況下失敗或行為不當。

## SSL 終止

第三方負載平衡器上的 SSL 終止有安全效益。如果負載平衡器遭到入侵、網格就會被分割。

支援的組態有三種：

- \* SSL 傳遞。\*SSL 憑證會以自訂伺服器憑證形式安裝在 StorageGRID 上。
- \* SSL 終止與重新加密（建議使用）\*如果您已經在負載平衡器上執行 SSL 憑證管理、而不是在 StorageGRID 上安裝 SSL 憑證、這可能會很有幫助。此組態提供額外的安全性優點、可將攻擊面限制在負載平衡器上。
- \* 使用 HTTP 終止 SSL。\*在此組態中、SSL 會在第三方負載平衡器上終止、而負載平衡器與 StorageGRID 之間的通訊則不會加密、以利用 SSL 卸載（在現代處理器中內嵌 SSL 程式庫、這是有限的效益）。

## 傳遞組態

如果您偏好設定負載平衡器以進行傳遞、則必須在 StorageGRID 上安裝憑證。前往功能表：組態 [ 伺服器憑證 > 物件儲存 API 服務端點伺服器憑證 ]。



## 來源用戶端 IP 可見度

StorageGRID 11.4 引進了信任的第三方負載平衡器概念。若要將用戶端應用程式 IP 轉寄至 StorageGRID、您必須設定此功能。如需詳細資訊、請參閱 "如何設定 StorageGRID 以搭配第三方第 7 層負載平衡器使用。"

若要啟用 XFF 標頭來檢視用戶端應用程式的 IP、請遵循下列步驟：

### 步驟

1. 在稽核記錄中記錄用戶端 IP。
2. 使用 `aws:SourceIp` S3 儲存區或群組原則。

### 負載平衡策略

大多數負載平衡解決方案都提供多種負載平衡策略。以下是常見策略：

- \* 循環 \* 通用配戴、但節點數極少、大型傳輸會阻塞單一節點。
- \* 最少連線。 \* 非常適合小型和混合式物件工作負載、因此所有節點的連線分配均相同。

隨著可選擇的儲存節點數量增加、演算法的選擇變得不那麼重要。

### 資料路徑

所有資料都會流經本機流量管理器負載平衡器。StorageGRID 不支援直接伺服器路由 (DSR)。

### 驗證連線的發佈

若要驗證您的方法是否在儲存節點之間平均分配負載、請檢查指定站台中每個節點上建立的工作階段：

- \* UI 方法。 \* 前往功能表：Support[ 指標 > S3 概觀 > LDR HTTP 工作階段 ]
- \* 指標 API \* 使用 `storagegrid_http_sessions_incoming_currently_established`

## 瞭解 StorageGRID 組態的幾個使用案例

探索客戶與 NetApp IT 實作的 StorageGRID 組態使用案例。

下列範例說明 StorageGRID 客戶實作的組態、包括 NetApp IT。

### F5 BIG-IP 本機流量管理程式狀態檢查監控 S3 貯體

若要設定 F5 BIG-IP 本機流量管理程式健全狀況檢查監控器、請依照下列步驟進行：

### 步驟

1. 建立新的監視器。
  - a. 在 Type (類型) 字段中，輸入 HTTPS。
  - b. 視需要設定時間間隔和逾時。
  - c. 在「傳送字串」欄位中、輸入 `OPTIONS / HTTP/1.1\r\n\r\n\r\n` 為回車；BIG-IP 軟體的不同版本需要零、一或兩組 `\r\n` 順序。如需更多資訊、請參閱 <https://support.f5.com/csp/article/K10655>。



- d. 在接收字串欄位中、輸入：HTTP/1.1 200 OK。

Local Traffic » Monitors » New Monitor...

**General Properties**

|                |                   |
|----------------|-------------------|
| Name           | https_storagegrid |
| Description    |                   |
| Type           | HTTPS             |
| Parent Monitor | https             |

Configuration: Basic

|                        |   |
|------------------------|---|
| Interval               | 5 seconds   |
| Timeout                | 16 seconds  |
| Send String            | OPTIONS / HTTP/1.1\r\n\r\n                                    |
| Receive String         | HTTP/1.1 200 OK   |
| Receive Disable String |   |
| Cipher List            | DEFAULT+SHA.+3DES.+kEDH                                       |
| User Name              |   |
| Password               |   |
| Reverse                | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Transparent            | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Alias Address          | * All Addresses   |
| Alias Service Port     | * All Ports   |
| Adaptive               | <input type="checkbox"/> Enabled                              |

2. 在 " 建立集區 " 中，針對所需的每個連接埠建立一個集區。
- a. 指派您在上一個步驟中建立的健全狀況監視器。
  - b. 選取負載平衡方法。
  - c. 選取服務連接埠：18082（S3）。
  - d. 新增節點。

## Citrix NetScaler

Citrix NetScaler 會為儲存端點建立虛擬伺服器、並將 StorageGRID 儲存節點稱為應用程式伺服器、然後將其分組至服務。

使用 HTTPS-ECV 健全狀況檢查監視器建立自訂監視器、以使用選項要求和接收來執行建議的健全狀況檢查 200。HTTP-ECV 是以傳送字串設定、並驗證接收字串。

有關詳細信息，請參閱 Citrix 文檔 "[HTTP-ECV 健全狀況檢查監視器的組態範例](#)"，。

The screenshot shows the Citrix NetScaler configuration interface for a monitor. At the top, there is a 'Monitors' section with buttons for 'Add Binding', 'Edit Binding', 'Unbind', and 'Edit Monitor'. Below this is a table with columns for 'Monitor Name', 'Weight', and 'State'. The table contains one entry: 'STORAGE-GRID-TCP-ECV-MON' with a weight of '1' and a state of '✓'. Below the table is the 'Configure Monitor' section. The 'Name' field is 'STORAGE-GRID-TCP-ECV-MON' and the 'Type' is 'TCP-ECV'. Under 'Basic Parameters', the 'Interval' is set to '5' seconds and the 'Response Timeout' is '2' seconds. The 'Send String' field contains 'OPTIONS / HTTP/1.1/VV/VV' and the 'Receive String' field contains 'HTTP/1.1 200 OK'. There is a checked 'Secure' checkbox and an 'SSL Profile' dropdown menu with 'Add' and 'Edit' buttons.

## Loadbalancer.org

Loadbalancer.org 已經與 StorageGRID 進行了自己的整合測試，並提供了廣泛的組態指南：[https://pdfs.loadbalancer.org/NetApp\\_StorageGRID\\_Deployment\\_Guide.pdf](https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf)。

## Kemp

Kemp 已與 StorageGRID 進行了自己的整合測試、並提供廣泛的組態指南：<https://kemptechnologies.com/solutions/netapp/>。

## HAProxy

將 HAProxy 設定為使用選項要求、並檢查 haproxy.cfg 中健全狀況檢查的 200 狀態回應。您可以將前端的繫結連接埠變更為其他連接埠、例如 443。

以下是 HAProxy 上 SSL 終止的範例：

```

frontend s3
    bind *:443 crt /etc/ssl/server.pem ssl
    default_backend s3-serve
rs
backend s3-servers
    balance leastconn
    option httpchk
    http-check expect status 200
    server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
    server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
    server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000

```

以下是 SSL 傳遞的範例：

```

frontend s3
    mode tcp
    bind *:443
    default_backend s3-servers
backend s3-servers
    balance leastconn
    option httpchk
    http-check expect status 200
    server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
    server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
    server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000

```

如需 StorageGRID 組態的完整範例、請參閱 ["HAProxy 組態範例"](#) GitHub 上的。

## 驗證 StorageGRID 中的 SSL 連線

瞭解如何在 StorageGRID 中驗證 SSL 連線。

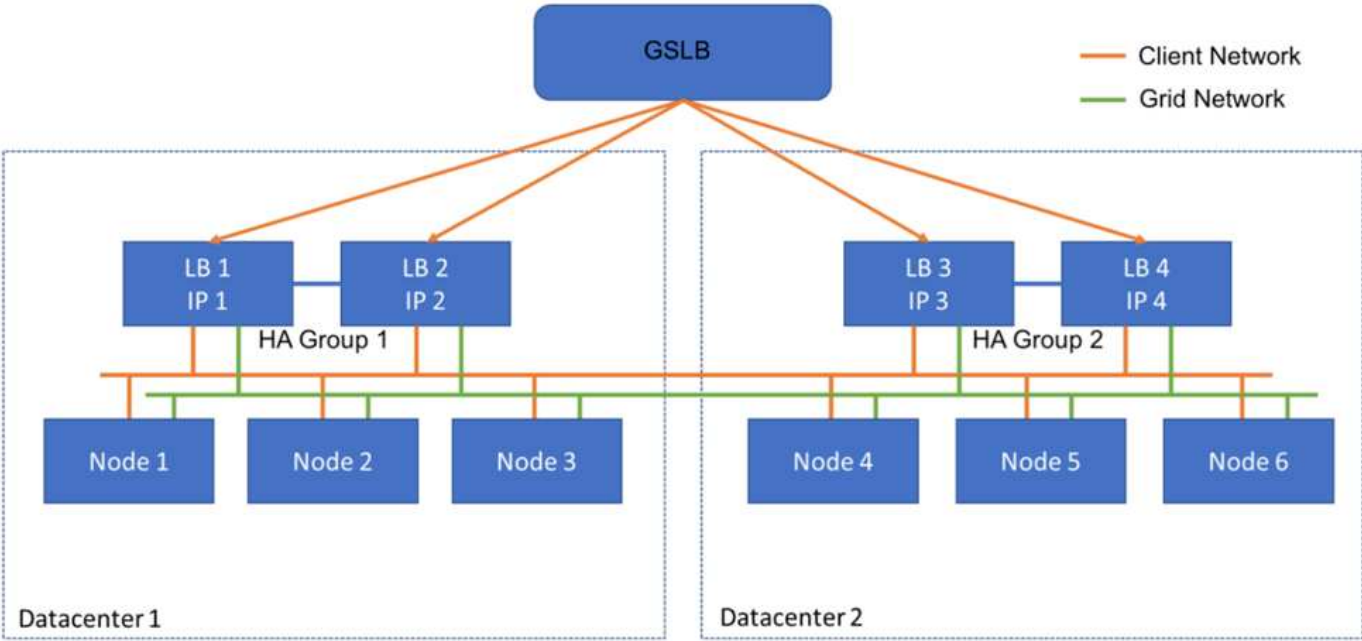
設定負載平衡器之後、您應該使用 Openssl 和 AWS CLI 等工具來驗證連線。其他應用程式（例如 S3 瀏覽器）可能會忽略 SSL 組態錯誤。

## 瞭解 StorageGRID 的整體負載平衡需求

探索 StorageGRID 中的整體負載平衡設計考量與需求。

全域負載平衡需要與 DNS 整合、才能在多個 StorageGRID 站台之間提供智慧型路由。此功能不在 StorageGRID 網域範圍內、必須由第三方解決方案提供、例如先前討論的負載平衡器產品和 / 或 DNS 流量控制解決方案、例如 Infoblox。這種頂層負載平衡可提供智慧型路由至命名空間中最近的目的地站台、以及中斷偵測和重新導向至命名空間中的下一個站台。典型的 GSLB 實作是由含有站台本機負載平衡器之站台集區的頂層 GSLB 所組成。站台負載平衡器包含本機站台儲存節點的集區。這可以包括用於 GSLB 功能的協力廠商負載平

衡器與提供站台本機負載平衡的 StorageGRID、或是協力廠商的組合、或是先前討論過的許多協力廠商都能同時提供 GSLB 和 站台本機負載平衡。



## 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。