管理 StorageGRID

StorageGRID software

NetApp
July 23, 2026

目錄

管理 StorageGRID 1
管理 StorageGRID 1
關於這些說明 1
開始之前 1
開始使用 Grid Manager 1
StorageGRID 的 Web 瀏覽器需求 1
登入 StorageGRID Grid Manager 2
登出 StorageGRID Grid Manager 3
更改 StorageGRID Grid Manager 密碼 4
檢視 StorageGRID 授權資訊 5
${post_edited_translations.segment} 6
使用 API 6
控制對 StorageGRID 的存取 27
${post_edited_translations.segment} 27
更改 StorageGRID 佈建通關密碼 28
在 StorageGRID 中變更節點主控台密碼 29
變更 StorageGRID 管理節點的 SSH 存取密碼 31
在 StorageGRID 中使用身分識別聯盟 32
管理 StorageGRID 中的管理員群組 37
StorageGRID 中的管理員群組權限 40
在 StorageGRID 中管理使用者 43
使用單一登入 (SSO) 46
使用網格聯邦 68
了解 StorageGRID 網格聯邦 68
瞭解 StorageGRID 中的帳戶複製 71
瞭解 StorageGRID 中的跨網格複寫 73
比較 StorageGRID 中的跨網格複寫和 CloudMirror 複寫 79
建立 StorageGRID 網格聯合連線 81
管理 StorageGRID 網格聯合連線 84
管理 StorageGRID 網格聯盟的允許租戶 88
排查 StorageGRID 中的網格聯合錯誤 94
識別並重試失敗的 StorageGRID 複寫作業 99
${post_edited_translations.segment} 102
在 StorageGRID 中管理安全性 102
檢閱 StorageGRID 加密方法 103
管理憑證 106
設定安全性設定 133
${post_edited_translations.segment} 139
${post_edited_translations.segment} 156

控制防火牆 157
管理租戶 163
StorageGRID 中的租戶帳戶 163
建立 StorageGRID 租用戶帳戶 164
編輯 StorageGRID 租用戶帳戶 169
變更 StorageGRID 租戶本機 root 使用者的密碼 170
刪除 StorageGRID 租用戶帳戶 171
${post_edited_translations.segment} 172
在 StorageGRID 中為租戶帳戶管理 S3 Select 180
設定用戶端連線 181
設定 S3 用戶端連線至 StorageGRID 181
StorageGRID 中 S3 用戶端的安全性 184
使用 S3 設定精靈 185
管理 HA 群組 194
管理負載平衡 203
在 StorageGRID 中設定 S3 端點網域名稱 216
StorageGRID 客戶端連線的 IP 位址和連接埠 217
管理網路和連線 219
配置 StorageGRID 網路設定 219
StorageGRID 網路指南 219
在 StorageGRID 中檢視 IP 位址 221
在 StorageGRID 中設定 VLAN 介面 222
為管理介面啟用 StorageGRID CORS 226
管理流量分類原則 226
StorageGRID 中支援的用於出站 TLS 連線的加密套件 233
StorageGRID 中活動、閒置和並行 HTTP 連線的優勢 233
在 StorageGRID 中管理連結成本 235
使用 AutoSupport 237
了解 AutoSupport 在 StorageGRID 中的應用 237
在 StorageGRID 中設定 AutoSupport 240
手動觸發 StorageGRID 中的 AutoSupport 套件 244
StorageGRID AutoSupport 套件故障排除 244
透過 StorageGRID 傳送 E 系列 AutoSupport 套件 245
管理儲存節點 250
使用儲存設備選項 250
在 StorageGRID 中管理物件中繼資料儲存 253
在 StorageGRID 中增加 Metadata Reserved Space 設定 259
壓縮 StorageGRID 中儲存的物件 261
在 StorageGRID 中管理已滿的 Storage Nodes 261
管理管理節點 262
在 StorageGRID 中使用多個管理節點 262

識別 StorageGRID 中的主要管理節點 263

管理 StorageGRID

管理 StorageGRID

請依照以下說明設定和管理 StorageGRID 系統。

關於這些說明

設定和管理 StorageGRID 的主要任務包括：

- 使用 Grid Manager 設定群組和使用者
- 建立租戶帳戶，以允許 S3 用戶端應用程式儲存和擷取物件
- 設定與管理 StorageGRID 網路
- 設定 AutoSupport
- ${post_edited_translations.segment}

開始之前

- 您對 StorageGRID 系統有基本的了解。
- ${post_edited_translations.segment}

開始使用 Grid Manager

StorageGRID 的 Web 瀏覽器需求

${post_edited_translations.segment}

${post_edited_translations.segment}	最低支援版本
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

將瀏覽器視窗寬度設定為建議值。

瀏覽器寬度	像素
${post_edited_translations.segment}	1024
最佳	1280

登入 StorageGRID Grid Manager

您可以透過在支援的 Web 瀏覽器的網址列中輸入管理節點的完整網域名稱 (FQDN) 或 IP 位址來存取 Grid Manager 登入頁面。

每個 StorageGRID 系統包含一個主要管理節點和任意數量的非主要管理節點。您可以在任何管理節點上登入 Grid Manager 來管理 StorageGRID 系統。但是，某些維護程序只能從主要管理節點執行。

連線至 HA 群組

如果高可用度（ HA ）群組中包含管理節點，您可以使用 HA 群組的虛擬 IP 位址或對應至虛擬 IP 位址的完整網域進行連線。應選擇主要管理節點作為群組的主要介面，以便在您存取 Grid Manager 時，除非主要管理節點無法使用，否則您是在主要管理節點上存取它。請參閱 "管理高可用度群組"。

使用 SSO

如果 "已設定單一登入 (SSO)。"，登入步驟會略有不同。

${post_edited_translations.segment}

開始之前

- 您已擁有登入憑證。
- 您正在使用一個"支援的網頁瀏覽器"。
- 您的瀏覽器已啟用 Cookie。
- 您所屬的使用者群組至少擁有一項權限。
- 您已取得網格管理員的 URL：

  `https://FQDN_or_Admin_Node_IP/`

  您可以使用完整網域名稱、管理節點的 IP 位址或管理節點 HA 群組的虛擬 IP 位址。

  若要透過 HTTPS 預設連接埠 （443） 以外的連接埠存取 Grid Manager，請在 URL 中包含連接埠號碼：

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO 功能在受限的 Grid Manager 連接埠上無法使用。您必須使用連接埠 443。

步驟

1. 啟動支援的網頁瀏覽器。
2. 在瀏覽器的網址列中，輸入 Grid Manager 的 URL。
3. 如果出現安全性警報，請使用瀏覽器的安裝精靈安裝憑證。參見"管理安全性證書"。
4. 登入網格管理器。

   ${post_edited_translations.segment}

${post_edited_translations.segment}

a. 請輸入您的 Grid Manager 使用者名稱和密碼。

b. 選擇 **Sign In**。

使用 **SSO**

- 如果 StorageGRID 使用 SSO，並且這是您首次在此瀏覽器上存取該 URL：

  i. 選擇 **Sign in**。帳戶欄位可以保留 0。

  ii. 在貴組織的 SSO 登入頁面上輸入您的標準 SSO 憑證。

  ${post_edited_translations.segment}

  A. 輸入 **0**（Grid Manager 的帳戶 ID），或者如果 **Grid Manager** 出現在最近的帳戶清單中，則選取 **Grid Manager**。

  B. ${post_edited_translations.segment}

  C. 使用您的標準 SSO 憑證登入您組織的 SSO 登入頁面。

當您登入時，系統會顯示 Grid Manager 的首頁，其中包含儀表板。若要瞭解所提供的資訊，請參閱 "檢視及管理儀表板"。

登入另一個管理節點

請依照下列步驟登入另一個管理節點。

${post_edited_translations.segment}

步驟

1. 在瀏覽器網址列中，輸入另一個管理節點的完整網域名稱或 IP 位址。視需要加入連接埠號碼。
2. 請輸入您的 Grid Manager 使用者名稱和密碼。
3. 選擇 **Sign In**。

使用 **SSO**

如果 StorageGRID 使用 SSO，且您已登入一個管理節點，則無需再次登入即可存取其他管理節點。

步驟

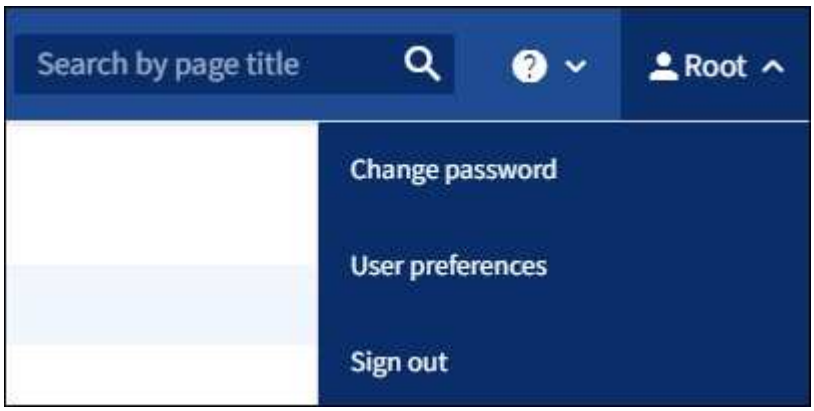
1. 在瀏覽器網址列中輸入另一個管理節點的完整網域名稱或 IP 位址。
2. ${post_edited_translations.segment}

登出 **StorageGRID Grid Manager**

使用完 Grid Manager 後，您必須登出，以確保未經授權的使用者無法存取 StorageGRID 系統。根據瀏覽器的 Cookie 設定，關閉瀏覽器可能無法使您登出系統。

步驟

1. 請在右上角選擇您的使用者名稱。



2. 選擇「登出」。

選項	說明
單一登入未使用	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}
已啟用單一登入	您已從所有正在存取的管理節點登出。此時將顯示 StorageGRID 登入頁面。**Grid Manager** 在 **Recent Accounts** 下拉式清單中列為預設值，且 **Account ID** 欄位顯示為 0。 *注意：*如果已啟用 SSO 且您也已登入租戶管理器，則您也必須"登出租戶帳戶"至"登出 SSO"。

更改 **StorageGRID Grid Manager** 密碼

如果您是 Grid Manager 的本機使用者，您可以自行變更密碼。

開始之前

您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

如果您以聯合使用者登入 StorageGRID，或啟用了單一登入 （SSO），則無法在 Grid Manager 中變更密碼。您必須在外部身分識別來源（例如 Active Directory 或 OpenLDAP）中變更密碼。

步驟

1. 從 Grid Manager 標題中，選擇 您的姓名 > 變更密碼。
2. 請輸入您目前的密碼。
3. 輸入新密碼。

   您的密碼必須包含至少 8 個字元，且不超過 32 個字元。密碼區分大小寫。

4. 請重新輸入新密碼。
5. 選取 **Save** 。

檢視 **StorageGRID** 授權資訊

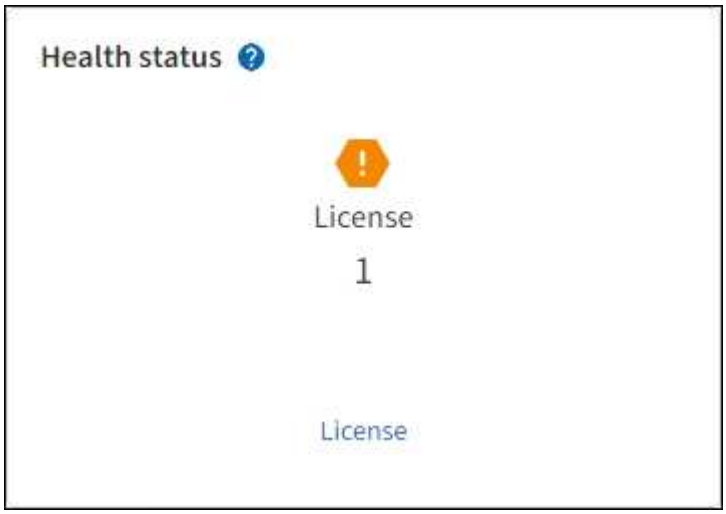
${post_edited_translations.segment}

開始之前

您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

如果此 StorageGRID 系統的軟體授權發生問題，儀表板上的「健全狀況」狀態卡會包含「授權」狀態圖示和 **License** 連結。該數字表示與授權相關的問題數量。



步驟

1. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 從儀表板的「健全狀況」卡中，選擇「授權狀態」圖示或「授權」連結。

     ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 授權序號
   - ${post_edited_translations.segment}
   - 網格的授權儲存容量
   - ${post_edited_translations.segment}
   - 授權結束日期。永久授權會顯示 **N/A**。
   - ${post_edited_translations.segment}

     此日期是從目前的授權檔案中讀取，如果您在取得授權檔案後延長或續約支援服務合約，則此日期可能

會過期。若要更新此值，請參閱 "${post_edited_translations.segment}"。您也可以使用 Active IQ 檢視實際的合約結束日期。

- ${post_edited_translations.segment}

${post_edited_translations.segment}

如果您的授權條款發生變更，您必須更新 StorageGRID 系統的授權資訊。例如，如果您為網格購買了額外儲存容量，則必須更新授權資訊。

開始之前

- 您有一個新的授權檔案需要套用到您的 StorageGRID 系統。
- 您有"特定存取權限"。
- 您擁有佈建密碼。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 找到並選取新的授權檔案(`.txt`）。

   新的授權檔案已驗證並顯示。

4. 請輸入佈建密碼。
5. 選取 **Save** 。

使用 **API**

使用 **StorageGRID Grid Management API**

您可以使用 Grid Management REST API 而非 Grid Manager 使用者介面來執行系統管理工作。例如，您可能想要使用 API 來自動化作業，或更快速地建立多個實體（例如使用者）。

${post_edited_translations.segment}

${post_edited_translations.segment}

- `/grid`: 存取僅限於 Grid Manager 使用者，並根據設定的群組權限而定。
- `/org`：存取權限僅限於屬於租戶帳戶的本機或聯合 LDAP 群組的使用者。如需詳細資訊，請參閱 "使用租戶帳戶"。
- `/private`：存取權限僅限於 Grid Manager 使用者，並以設定的群組權限為基礎。私有 API 可能隨時變更，恕不另行通知。StorageGRID 私有端點也會忽略請求中的 API 版本。

發出 **API** 請求

Grid Management API 使用 Swagger 開放原始碼 API 平台。Swagger 提供直覺式使用者介面，讓開發人員和非開發人員都能使用該 API 在 StorageGRID 中執行即時操作。

${post_edited_translations.segment}

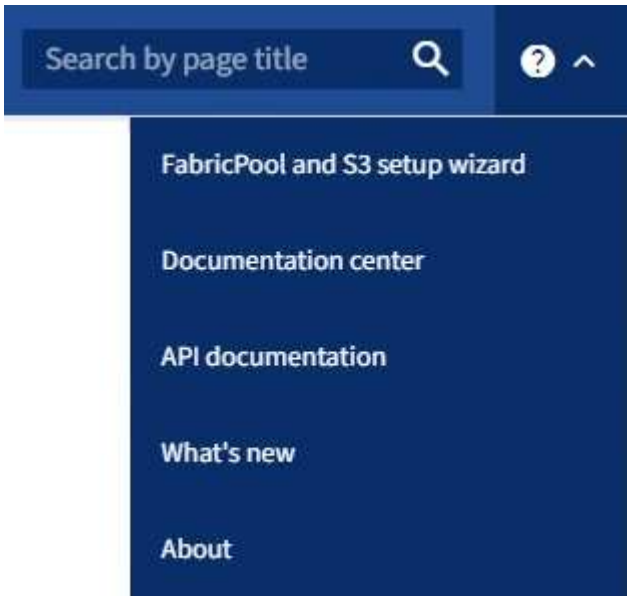
開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

> 您透過 API 文件網頁執行的任何 API 操作都是即時操作。請務必小心，避免誤建立、更新或刪除組態資料或其他資料。

步驟

1. ${post_edited_translations.segment}



neoplasms_and_cancer_types_1000_1000.jpg (1000×1000)

Neoplasms and cancer types are broad categories of abnormal cell growth. Neoplasms, commonly known as tumors, can be benign (non-cancerous) or malignant (cancerous). Cancer, on the other hand, refers specifically to malignant neoplasms that have the potential to invade or spread to other parts of the body.

There are over 100 different types of cancer, which are typically classified by the type of cell or organ in which they originate. Some of the most common types of cancer include:

1. Carcinoma: This is the most common type of cancer, originating in the epithelial cells that line the inside and outside of organs. Examples include breast, lung, prostate, and colon cancers.
2. Sarcoma: This type of cancer originates in supportive and connective tissues, such as bones, tendons, cartilage, muscle, and fat.
3. Leukemia: This is a cancer of the blood-forming tissues, including the bone marrow and lymphatic system. It leads to the overproduction of abnormal white blood cells.
4. Lymphoma: This cancer originates in the lymphatic system, which is part of the body's immune system. It affects lymphocytes, a type of white blood cell.
5. Myeloma: This cancer starts in the plasma cells of the bone marrow, which are responsible for producing antibodies.
6. Central Nervous System Cancers: These cancers originate in the brain and spinal cord.

Understanding the different types of neoplasms and cancers is crucial for accurate diagnosis, treatment planning, and prognosis. Treatment options vary widely depending on the type and stage of the cancer, and may include surgery, chemotherapy, radiation therapy, immunotherapy, and targeted therapy.

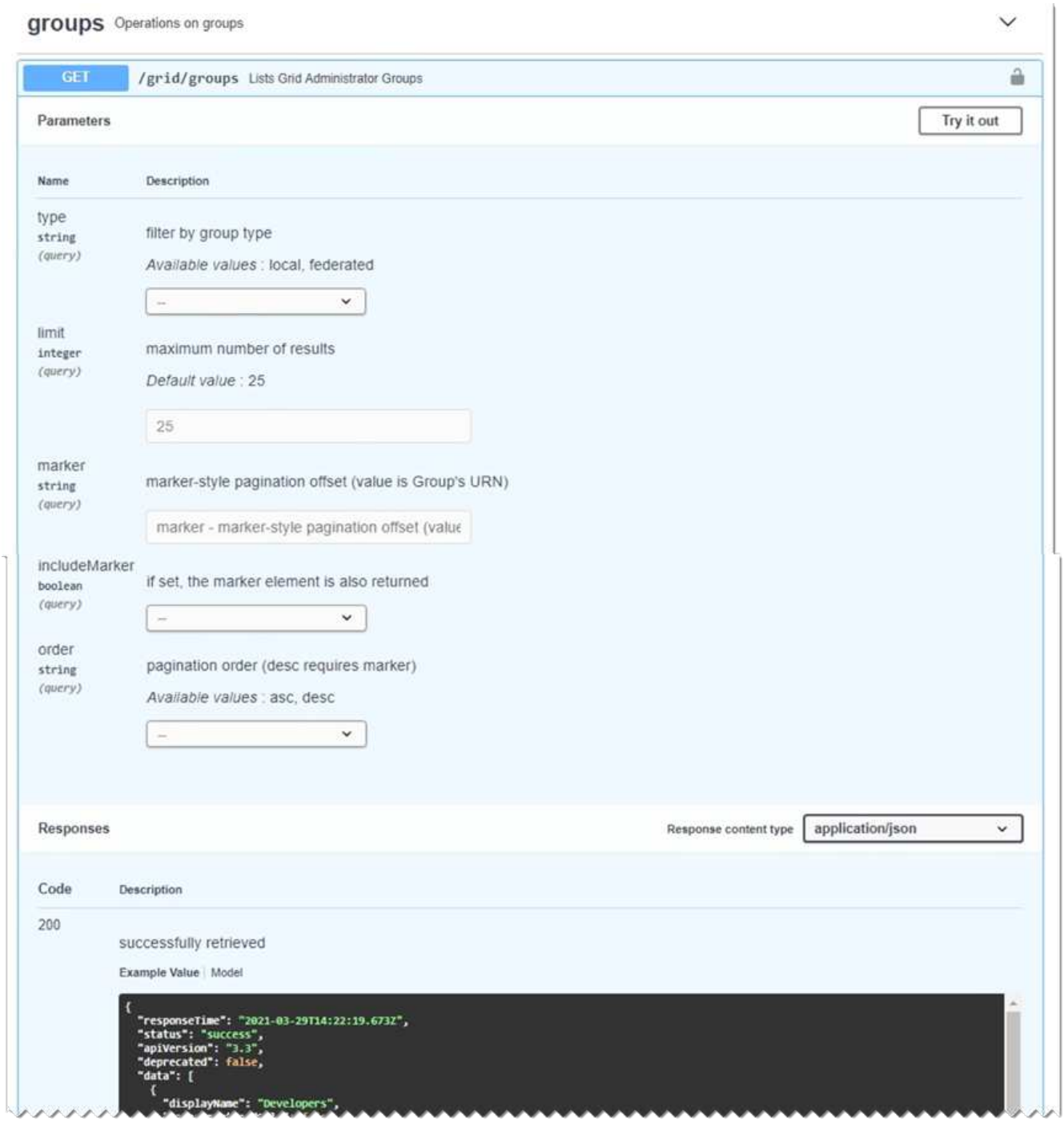
1. ${post_edited_translations.segment}

   私有 API 如有變更，恕不另行通知。StorageGRID 私有端點也會忽略要求的 API 版本。

2. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}



4. 確定請求是否需要其他參數，例如群組 ID 或使用者 ID。然後，取得這些值。您可能需要先發出另一個 API 請求，才能獲得所需資訊。
5. 確定是否需要修改範例要求本文。如果需要，您可以選取 **Model** 來瞭解每個欄位的需求。
6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}
8. 選擇 **Execute**。
9. ${post_edited_translations.segment}

StorageGRID 中的 **Grid Management API** 操作

網格管理 API 將可用作業組織成以下幾個部分。

此清單僅包含公用 API 中可用的操作。

- 帳戶：管理儲存設備租戶帳戶的作業，包括建立新帳戶及擷取指定帳戶的儲存設備使用情況。
- **alert-history**：對已解決警報的操作。
- **alert-receivers**：對警報通知接收器（電子郵件）的操作。
- **alert-rules**：對警報規則的操作。
- **alert-silences**：對警報靜默的操作。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **auth**：執行使用者工作階段驗證的操作。

  Grid Management API 支援 Bearer Token 驗證機制。若要登入，您必須在驗證要求的 JSON 本文中提供使用者名稱與密碼（也就是 `POST /api/v3/authorize`）。如果使用者成功通過驗證，系統將會傳回安全性權杖。必須在後續 API 要求的標頭中提供此權杖（"Authorization: Bearer *token*"）。此權杖將在 16 小時後逾期。

  如果 StorageGRID 系統啟用了單一登入，則必須執行不同的驗證步驟。請參閱「如果啟用了單一登入，如何對 API 進行驗證」。

  ${post_edited_translations.segment}

- **client-certificates**：設定用戶端憑證的操作，以便使用外部監控工具安全地存取 StorageGRID。
- **config**：與產品版本及網格管理 API 版本相關的作業。您可以列出產品版本以及該版本支援的網格管理 API 主要版本，也可以停用已過時的 API 版本。
- **deactivated-features**：檢視可能已停用的功能的操作。
- **dns-servers**：列出並變更已設定的外部 DNS 伺服器的操作。
- **drive-details**：針對特定儲存應用裝置型號的磁碟機操作。
- **endpoint-domain-names**：列出並變更 S3 端點網域名稱的操作。
- **erasure-coding**：對糾刪碼設定檔進行操作。
- ${post_edited_translations.segment}

- **expansion-nodes**：擴展操作（節點層級）。
- **expansion-sites**：擴充作業（站台層級）。
- **grid-networks**: 列出並變更網格網路清單的操作。
- **grid-passwords**：網格密碼管理操作。
- ${post_edited_translations.segment}
- **identity-source**：設定外部身分來源並手動同步聯合群組和使用者資訊的操作。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **metrics**：針對 StorageGRID 計量執行的作業，包括單一時間點的即時計量查詢，以及一段時間範圍內的範圍計量查詢。Grid Management API 使用 Prometheus 系統監控工具作為後端資料來源。如需建構 Prometheus 查詢的相關資訊，請參閱 Prometheus 網站。

> 名稱中包含 *private* 的計量僅供內部使用。這些計量可能會在不同的 StorageGRID 版本之間變更，恕不另行通知。

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **ntp-servers**：列出或更新外部網路時間協定 (NTP) 伺服器的作業。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **recovery-package**：下載恢復套件的操作。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **untrusted-client-network**: 對不受信任的用戶端網路組態執行操作。
- ${post_edited_translations.segment}

StorageGRID 中的 **Grid Management API** 版本控制

網格管理 API 使用版本控制來支援無中斷升級。

例如，此請求 URL 指定了 API 的版本 4。

`https://hostname_or_ip_address/api/v4/authorize`

當 API 進行了與舊版本不相容的變更時，主版本號碼會提升。當 API 進行了與舊版本相容的變更時，次版本號碼會提升。相容的變更包括新增新的端點或屬性。

以下範例說明如何根據所做的變更類型來提升 API 版本。

API 變更類型	舊版	新版本
與舊版本相容	2.1	2.2
與舊版本不相容	2.1	3.0

首次安裝 StorageGRID 軟體時，僅啟用最新版本的 API。但是，升級到 StorageGRID 的新功能版本後，您至少可以在一個 StorageGRID 功能版本內繼續存取舊版的 API。

> 您可以設定支援的版本。如需詳細資訊，請參閱 "網格管理 API" 的 Swagger API 文件的 **config** 部分。將所有 API 用戶端更新至新版本後，您應停用對舊版本的支援。

過時的請求會透過以下方式標記為已棄用：

- 回應標頭為「Deprecated: true」
- JSON 回應正文包含「deprecated」：true
- nms.log 中新增了一條已棄用的警告訊息。例如：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

確定目前版本支援哪些 **API** 版本

使用 `GET /versions` API 請求傳回受支援的 API 主要版本清單。此請求位於 Swagger API 文件的 **config** 部分。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

為請求指定 **API** 版本

您可以使用路徑參數 (`/api/v4`）或標頭 (`Api-Version: 4`）指定 API 版本。如果您同時提供這兩個值，則標頭值會覆寫路徑值。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

防止 **StorageGRID** 中的跨站請求偽造（**CSRF**）攻擊

您可以使用 CSRF 令牌來增強基於 Cookie 的驗證，從而協助 StorageGRID 防範跨站請求偽造 （CSRF） 攻擊。Grid Manager 和 Tenant Manager 會自動啟用此安全性功能；其他 API 用戶端可以在登入時選擇是否啟用此功能。

${post_edited_translations.segment}

StorageGRID 透過使用 CSRF 令牌來協助防範 CSRF 攻擊。啟用此功能後，特定 Cookie 的內容必須與特定標頭或特定 POST 請求體參數的內容相符。

若要啟用此功能，請在驗證期間將 `csrfToken`參數設定為 `true`。預設值為 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

設為 true 時，系統會為登入 Grid Manager 的作業設定具有隨機值的 `GridCsrfToken` Cookie，並為登入 Tenant Manager 的作業設定具有隨機值的 `AccountCsrfToken` Cookie。

${post_edited_translations.segment}

- 此 `X-Csrf-Token`標頭，且標頭的值設定為 CSRF token Cookie 的值。
- 對於接受表單編碼主體的端點：A `csrfToken` 表單編碼的要求主體參數。

${post_edited_translations.segment}

${post_edited_translations.segment}

如果啟用了單一登入，請使用 **API**。

如果您擁有"${post_edited_translations.segment}"並使用 Active Directory 作為 SSO 供應商，則必須發出一系列 API 請求，以取得對 Grid Management API 或 Tenant Management API 有效的驗證權杖。

如果啟用了單一登入，請登入 **API**。

如果您使用 Active Directory 作為 SSO 身分識別供應商，則適用這些說明。

開始之前

- 您知道屬於 StorageGRID 使用者群組的聯合使用者的 SSO 使用者名稱和密碼。
- 如果您想存取租戶管理 API，您需要知道租戶帳戶 ID。

關於此任務

若要取得驗證令牌，您可以使用下列範例之一：

- The `storagegrid-ssoauth.py` Python 指令碼位於 StorageGRID 安裝檔案目錄中，(`./rpms`適用於 RHEL， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`適用於 VMware）。
- curl 請求的工作流程範例。

  如果您執行 curl 工作流程的速度太慢，該工作流程可能會逾時。您可能會看到錯誤： `A valid SubjectConfirmation was not found on this Response`。

  ${post_edited_translations.segment}

如果遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 請選擇以下其中一種方法來取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2。
   - 使用 curl 請求。前往步驟 3。
2. 如果您想使用該 `storagegrid-ssoauth.py`指令碼，請將指令碼傳遞給 Python 解譯器並執行該指令碼。

   ${post_edited_translations.segment}

   - 單一登入 (SSO) 方法。輸入 ADFS 或 adfs。
   - SSO 使用者名稱
   - StorageGRID 安裝所在的網域
   - ${post_edited_translations.segment}
   - 如果您想存取租戶管理 API，則需要租戶帳戶 ID。

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

3. 如果要使用 curl 請求，請依照下列步驟操作。

   a. 聲明登入所需的變數。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   若要存取 Grid Management API，請使用 0 作為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的驗證 URL，請向 `/api/v3/authorize-saml` 發出 POST 要求，並從回應中移除額外的 JSON 編碼。

   此範例展示了針對已簽名驗證 URL 的 POST 請求 `TENANTACCOUNTID`。結果將傳遞給 `python -m json.tool`以移除 JSON 編碼。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   此範例的回應包含一個經過 URL 編碼的簽章 URL，但不包含額外的 JSON 編碼階層。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 儲存回應中的 `SAMLRequest`，以便在後續命令中使用。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. 從 AD FS 取得包含用戶端請求 ID 的完整 URL。

一種方法是使用先前回應中的 URL 請求登入表單。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

回應包含用戶端請求 ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 從回應中儲存用戶端請求 ID。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. ${post_edited_translations.segment}

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 傳回 302 重新導向，並在標頭中包含額外資訊。

> 如果您的 SSO 系統啟用了多因素驗證 （MFA），則表單提交中還將包含第二個密碼或其他憑證。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 從回應中儲存 `MSISAuth` Cookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 使用驗證 POST 請求中的 Cookie 向指定位置發送 GET 請求。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

回應標頭將包含 AD FS 工作階段資訊，以供稍後登出使用，回應本文包含隱藏表單欄位中的 SAMLResponse。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 儲存隱藏欄位中的 `SAMLResponse` 值：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已儲存的 `SAMLResponse`，向 StorageGRID 發出 `/api/saml-response` 請求以產生 StorageGRID 驗證權杖。

對於 `RelayState`，請使用租戶帳戶 ID，或者如果您想要登入 Grid Management API，請使用 0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

回應包含驗證令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 將回應中的驗證權杖儲存為 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

現在您可以使用 `MYTOKEN` 來處理其他請求，就像未使用 SSO 時使用 API 一樣。

如果啟用了單一登入，請登出 **API**。

如果已啟用單一登入 （SSO），則必須發出一系列 API 請求才能從 Grid Management API 或 Tenant Management API 登出。如果您使用 Active Directory 作為 SSO 身分識別供應商，則這些說明適用。

關於此任務

如有需要，您可以透過組織的單一登出頁面登出，從而退出 StorageGRID API。或者，您也可以從 StorageGRID 觸發單一登出 （SLO），這需要有效的 StorageGRID 持有者權杖。

步驟

1. 若要產生已簽署的登出請求，請將 `Cookie "sso=true"` 傳遞給 SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

傳回一個登出 URL：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存登出 URL。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. ${post_edited_translations.segment}

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 回應。重新導向位置不適用於僅透過 API 進行的登出。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. ${post_edited_translations.segment}

刪除 StorageGRID bearer token 的運作方式與沒有 SSO 時相同。如果未提供 `Cookie "sso=true"，使用者將從 StorageGRID 登出，而不影響 SSO 狀態。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 回應表示使用者現在已登出。

```
HTTP/1.1 204 No Content
```

如果啟用了單一登入（**Entra ID**），請使用 **StorageGRID API**

如果您有 "${post_edited_translations.segment}" 且使用 Entra ID 作為 SSO 供應商，您可以使用兩個範例指令碼來取得適用於 Grid Management API 或 Tenant Management API 的有效驗證權杖。

如果已啟用 **Entra ID** 單一登入，請登入 **API**。

如果您使用 Entra ID 作為 SSO 身分供應商，則適用以下說明。

開始之前

- 您知道屬於 StorageGRID 使用者群組的聯合使用者的 SSO 電子郵件地址和密碼。
- 如果您想存取租戶管理 API，您需要知道租戶帳戶 ID。

關於此任務

若要取得驗證權杖，可以使用下列範例指令碼：

- The `storagegrid-ssoauth-azure.py` Python 指令碼
- The `storagegrid-ssoauth-azure.js` Node.js 指令碼

這兩個指令碼都位於 StorageGRID 安裝檔案目錄中（RHEL 為 (`./rpms`，Ubuntu 或 Debian 為 `./debs`，VMware 則為 `./vsphere`）。

若要撰寫您自己與 Entra ID 的 API 整合，請參閱 `storagegrid-ssoauth-azure.py`指令碼。這個 Python 指令碼直接向 StorageGRID 發出兩個請求（第一個請求用於取得 SAMLRequest，第二個請求用於取得授權權杖），同時也呼叫 Node.js 指令碼與 Entra ID 互動以執行 SSO 操作。

SSO 作業可以使用一系列 API 要求來執行，但這樣做並不簡單。Puppeteer Node.js 模組可用於抓取 Entra ID SSO 介面。

如果遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 依下列步驟安裝所需的相依性：
   a. 安裝 Node.js（請參閱 "https://nodejs.org/en/download/"）。
   b. 安裝所需的 Node.js 模組（puppeteer 和 jsdom）：

      ```
      npm install -g <module>
      ```

2. ${post_edited_translations.segment}

   然後，Python 指令碼將呼叫對應的 Node.js 指令碼來執行 Entra ID SSO 互動。

3. 出現提示時，請輸入以下參數的值（或使用參數傳遞它們）：
   - 用於登入 Entra ID 的 SSO 電子郵件地址
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
4. 出現提示時，輸入密碼，並準備好在 Entra ID 要求時提供 MFA 授權。

該指令碼假定使用 Microsoft Authenticator 進行多因素驗證 （MFA）。您可能需要修改指令碼以支援其他形式的 MFA （例如輸入透過簡訊收到的驗證碼）。

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

如果啟用單一登入，請使用 **StorageGRID API**（**PingFederate**）

如果您擁有"${post_edited_translations.segment}"並使用 PingFederate 作為 SSO 供應商，則必須發出一系列 API 請求，以取得對 Grid Management API 或 Tenant Management API 有效的驗證權杖。

如果啟用了單一登入，請登入 **API**。

如果您使用 PingFederate 作為 SSO 身分供應商，則適用以下說明。

開始之前

- 您知道屬於 StorageGRID 使用者群組的聯合使用者的 SSO 使用者名稱和密碼。
- 如果您想存取租戶管理 API，您需要知道租戶帳戶 ID。

關於此任務

若要取得驗證令牌，您可以使用下列範例之一：

- The `storagegrid-ssoauth.py` Python 指令碼位於 StorageGRID 安裝檔案目錄中，(`./rpms`適用於 RHEL， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`適用於 VMware）。
- curl 請求的工作流程範例。

  如果您執行 curl 工作流程的速度太慢，該工作流程可能會逾時。您可能會看到錯誤： `A valid SubjectConfirmation was not found on this Response`。

  ${post_edited_translations.segment}

  如果遇到 URL 編碼問題，您可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 請選擇以下其中一種方法來取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2。
   - 使用 curl 請求。前往步驟 3。
2. 如果您想使用該 `storagegrid-ssoauth.py`指令碼，請將指令碼傳遞給 Python 解譯器並執行該指令碼。

   ${post_edited_translations.segment}

   - SSO 方法。您可以輸入 "pingfederate" 的任何變體（PINGFEDERATE、pingfederate 等）。
   - SSO 使用者名稱
   - 安裝 StorageGRID 的網域。此欄位不用於 PingFederate。您可以將其保留空白，或輸入任何值。

- ${post_edited_translations.segment}
- 如果您想存取租戶管理 API，則需要租戶帳戶 ID。

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 授權權杖已在輸出中提供。現在，您可以像未使用 SSO 時使用 API 一樣，使用此權杖發出其他請求。

3. 如果要使用 curl 請求，請依照下列步驟操作。

   a. 聲明登入所需的變數。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

   若要存取 Grid Management API，請使用 0 作為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的驗證 URL，請向 `/api/v3/authorize-saml` 發出 POST 要求，並從回應中移除額外的 JSON 編碼。

   此範例顯示針對 TENANTACCOUNTID 的已簽署驗證 URL 的 POST 要求。結果將傳遞至 python -m json.tool 以移除 JSON 編碼。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   此範例的回應包含一個經過 URL 編碼的簽章 URL，但不包含額外的 JSON 編碼階層。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 儲存回應中的 `SAMLRequest`，以便在後續命令中使用。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 匯出回應和 Cookie，並輸出回應：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 匯出「pf.adapterId」值，並輸出回應：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. ${post_edited_translations.segment}

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 匯出「行動」值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 傳送 Cookie 及憑證：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 儲存隱藏欄位中的 `SAMLResponse` 值：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已儲存的 `SAMLResponse`，向 StorageGRID 發出 `/api/saml-response` 請求以產生 StorageGRID 驗證權杖。

對於 `RelayState`，請使用租戶帳戶 ID，或者如果您想要登入 Grid Management API，請使用 0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

回應包含驗證令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 將回應中的驗證權杖儲存為 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

現在您可以使用 `MYTOKEN` 來處理其他請求，就像未使用 SSO 時使用 API 一樣。

如果啟用了單一登入，請登出 **API**。

如果已啟用單一登入 （SSO），您必須發出一系列 API 要求，以登出 Grid Management API 或 Tenant Management API。如果您使用 PingFederate 作為 SSO 身分識別供應商，則適用這些說明

關於此任務

如有需要，您可以透過組織的單一登出頁面登出，從而退出 StorageGRID API。或者，您也可以從 StorageGRID 觸發單一登出 （SLO），這需要有效的 StorageGRID 持有者權杖。

步驟

1. 若要產生已簽署的登出請求，請將 `Cookie "sso=true"` 傳遞給 SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

傳回一個登出 URL：

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 儲存登出 URL。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. ${post_edited_translations.segment}

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 回應。重新導向位置不適用於僅透過 API 進行的登出。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. ${post_edited_translations.segment}

刪除 StorageGRID bearer token 的運作方式與沒有 SSO 時相同。如果未提供 `Cookie "sso=true"，使用者將從 StorageGRID 登出，而不影響 SSO 狀態。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 回應表示使用者現在已登出。

```
HTTP/1.1 204 No Content
```

使用 **API** 停用 **StorageGRID** 功能

您可以使用 Grid Management API 完全停用 StorageGRID 系統中的特定功能。停用功能後，即無法指派任何人執行與該功能相關工作的權限。

關於此任務

「已停用功能」系統可讓您封鎖對 StorageGRID 系統中某些功能的存取。停用功能是阻止 root 使用者或屬於具有 **Root access** 權限之管理員群組的使用者使用該功能的唯一方法。

為了理解此功能的用途，請考慮以下場景：

A 公司是一家服務供應商，透過建立租戶帳戶的方式出租其 StorageGRID 系統的儲存容量。為了保護租戶物件的安全性，A 公司希望確保其員工在帳戶部署後永遠無法存取任何租戶帳戶。

公司 A 可以透過使用 Grid Management API 中的「停用功能」系統來達成此目標。透過在 Grid Manager （包括使用者介面和 API）中完全停用「變更租戶 root 密碼」功能，公司 A 可確保管理員使用者（包括 root 使用者和屬於具有「Root 存取權」權限之群組的使用者）無法變更任何租戶帳戶的 root 使用者密碼。

步驟

1. 存取網格管理 API 的 Swagger 文件。參見"${post_edited_translations.segment}"。
2. 找到「停用功能」端點。
3. 若要停用某項功能（例如「變更租戶 root 使用者密碼」），請向 API 傳送如下的請求本文：

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   當要求完成時，「變更租戶 root 密碼」功能即會停用。變更租戶 **root** 密碼 管理權限將不再出現在使用者介面中，且任何嘗試變更租戶 root 密碼的 API 要求都將失敗，並出現 "403 Forbidden"。

${post_edited_translations.segment}

預設情況下，您可以使用 Grid Management API 重新啟用已停用的功能。但是，如果您希望防止已停用的功能被重新啟用，則可以停用 **activateFeatures** 功能本身。

> **activateFeatures** 功能無法重新啟動。如果您決定停用此功能，請注意，您將永久失去重新啟用任何其他已停用功能的能力。您必須聯絡技術支援以還原任何遺失的功能。

步驟

1. ${post_edited_translations.segment}
2. 找到「停用功能」端點。
3. ${post_edited_translations.segment}

```
{ "grid": null }
```

當此要求完成時，所有功能（包括變更租戶根目錄密碼功能）都會重新啟用。「變更租戶根目錄密碼」管理權限現在會顯示在使用者介面中，且任何嘗試變更租戶根目錄密碼的 API 要求都將成功，前提是使用者具有「**root** 存取權」或「變更租戶根目錄密碼」管理權限。

前面的範例會重新啟用所有已停用的功能。如果還有其他已停用但應保持停用狀態的功能，則必須在 PUT 請求中明確指定它們。例如，若要重新啟用「變更租戶根目錄密碼」功能並繼續停用 storageAdmin 管理權限，請傳送下列 PUT 要求：+ `{ "grid": {"storageAdmin": true} }`

控制對 StorageGRID 的存取

${post_edited_translations.segment}

您可以建立或匯入使用者群組，並為每個使用者群組指派權限，從而控制誰可以存取 StorageGRID 以及使用者可以執行哪些任務。您也可以選擇啟用單一登入 （SSO） 、建立用戶端憑證以及變更網格密碼。

控制對 **Grid Manager** 的存取

${post_edited_translations.segment}

使用 "${post_edited_translations.segment}" 可加快設定 "${post_edited_translations.segment}" 與 "使用者" 的速度，並允許使用者使用熟悉的認證資訊登入 StorageGRID。如果您使用 Active Directory、OpenLDAP 或 Oracle Directory Server，則可以設定身分識別聯盟。

${post_edited_translations.segment}

您可透過將不同的 "權限" 指派給每個群組，來決定每個使用者可以執行的工作。例如，您可能希望某個群組中的使用者能夠管理 ILM 規則，而另一個群組中的使用者則能執行維護工作。使用者必須至少屬於一個群組才能存取系統。

您可以選擇將某個群組設定為唯讀。唯讀群組中的使用者只能檢視設定和功能。無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何操作。

啟用單一登入

StorageGRID 系統支援使用 Security Assertion Markup Language 2.0 (SAML 2.0) 標準的單一登入 (SSO)。在您 "設定並啟用 SSO" 之後，所有使用者都必須先通過外部身分識別供應商的驗證，才能存取 Grid Manager 、Tenant Manager、Grid Management API 或 Tenant Management API。本地使用者無法登入 StorageGRID。

${post_edited_translations.segment}

許多安裝和維護程序，以及下載 StorageGRID 恢復套件，都需要資源配置複雜密碼。下載 StorageGRID 系統的網格拓撲資訊和加密金鑰備份也需要此複雜密碼。您可以視需要 "更改密碼短語"。

${post_edited_translations.segment}

網格中的每個節點都有一個節點主控台密碼，您需要使用 SSH 以「admin」身分登入節點，或在虛擬機器/實體主控台連線上以 root 使用者身分登入。如有需要，您可以"變更節點主控台密碼"對每個節點執行此操作。

更改 StorageGRID 佈建通關密碼

使用此步驟變更 StorageGRID 佈建密碼。恢復、擴充和維護程序需要此密碼。下載包含網格拓撲資訊、網格節點主控台密碼和 StorageGRID 系統加密金鑰的恢復套件備份也需要此密碼。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有維護或 root 存取權限。
- 您擁有目前的設定密碼。

關於此任務

許多安裝和維護程序都需要佈建密碼，以及 "下載恢復套件"。佈建密碼未列在 `Passwords.txt` 檔案中。請務必記錄佈建密碼，並將其保存在安全的位置。

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。
2. 在 **Change provisioning passphrase** 下，選擇 **Make a change**
3. 請輸入您目前的佈建複雜密碼。
4. 請輸入新的密碼片語。密碼片語長度必須至少為 8 個字元，最多為 32 個字元。密碼片語區分大小寫。

   請將佈建密碼儲存在安全的位置。安裝、擴充和維護程序都需要用到它。

5. 重新輸入新的密碼短語，然後選擇 **Save**。

   配置密碼變更完成後，系統會顯示綠色成功橫幅。

6. 選擇 **Recovery Package**。
7. 輸入新的佈建密碼，以下載新的恢復套件。

   變更佈建密碼後，您必須立即下載新的恢復套件。恢復套件檔案可讓您在發生故障時還原系統。

在 StorageGRID 中變更節點主控台密碼

網格中的每個節點都有一個節點主控台密碼，用於登入節點。預設情況下，每個節點的密碼都是唯一的。您可以將每個節點的密碼變更為新的唯一密碼，也可以將所有節點的密碼變更為全域密碼。這些密碼儲存在恢復套件中。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

您可以使用節點主控台密碼透過 SSH 以「admin」身分登入節點，或透過虛擬機器/實體主控台連線以 root 使用者身分登入。您可以使用下列選項之一變更節點主控台密碼：

- 自動為每個節點套用隨機密碼
- ${post_edited_translations.segment}
- 為一個或多個節點指定並套用唯一密碼

密碼儲存在恢復套件中更新的 `Passwords.txt` 檔案中。密碼列在檔案的 Password 欄位中。

> 用於節點之間通訊的 SSH 金鑰 "${post_edited_translations.segment}" 與節點主控台密碼是分隔的。此程序不會變更 SSH 存取密碼。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。
2. ${post_edited_translations.segment}

下載目前恢復套件

在變更節點主控台密碼之前，請先下載目前的恢復套件。如果任何節點的密碼變更程序失敗，您可以使用此檔案中的密碼。

步驟

1. 請輸入網格的佈建密碼。
2. ${post_edited_translations.segment}
3. 將恢復套件檔案 (`.zip`) 複製到兩個安全且分隔的地點。

> 恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 選擇 **Continue** 。

提供新密碼

1. 選擇您要使用的密碼變更方式。
   - 自動：StorageGRID 會自動為所有節點指派一個新的隨機主控台密碼。
   - 自訂：您提供主控台密碼。

自動

1. 選擇 **Continue** 。

自訂

1. 請選擇以下選項之一：
   - 全域主控台密碼：對所有節點套用相同的主控台密碼。
   - 唯一控制台密碼：在一個或多個節點上套用不同的密碼。
2. 如果您選取了 **Global console password**，請輸入您要用於所有節點的密碼。
3. 如果您選取了 **Unique console passwords**，請為一個或多個節點輸入唯一密碼。
4. 選擇 **Continue** 。

${post_edited_translations.segment}

1. 當出現確認對話方塊時，如果您已準備好讓 StorageGRID 開始變更節點主控台密碼，請選擇 **Yes**。

   此程序一旦開始便無法取消。

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. 開啟 `.zip` 檔案。
4. 確認您可以存取內容，包括 `Passwords.txt`檔案，其中包含新節點主控台密碼。
5. 將新的恢復套件檔案 (`.zip`) 複製到兩個安全、安全且分隔的位置。

   ${post_edited_translations.segment}

   您必須保護恢復檔案的安全，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

6. 選取此核取方塊，表示您已下載新的恢復套件並驗證其內容。
7. 選擇 **Continue** 。

   StorageGRID 更新每個節點的密碼。

   如果在更新過程中出現錯誤，進度條會顯示密碼變更失敗的節點數量。系統會自動對所有密碼變更失敗的節點重試更新過程。如果程序結束時仍有部分節點的密碼未變更，則會顯示 **Retry** 按鈕。

8. ${post_edited_translations.segment}

a. ${post_edited_translations.segment}

b. 解決問題。

c. 選擇 **Retry**。

重試只會變更先前密碼變更嘗試失敗的節點上的節點主控台密碼。

9. 當進度條顯示沒有剩餘更新時，選擇 **Finish**。

10. 在所有節點的節點主控台密碼變更完畢後，請刪除 您下載的第一個恢復套件。

變更 StorageGRID 管理節點的 SSH 存取密碼

變更管理節點的 SSH 存取密碼也會更新網格中每個節點的唯一內部 SSH 金鑰集。主要管理節點使用這些 SSH 金鑰，透過安全的無密碼驗證來存取節點。

使用 SSH 金鑰以 `admin`身分登入節點，或以 root 使用者身分登入虛擬機器或實體控制台連線。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"維護或 Root 存取權限"。
- 您擁有目前的設定密碼。

關於此任務

Admin 節點的新存取密碼以及每個節點的新內部金鑰，都儲存在恢復套件中的 `Passwords.txt` 檔案中。這些金鑰列在該檔案的 Password 欄中。

用於節點間通訊的 SSH 金鑰有個別的 SSH 存取密碼。此程序不會變更這些密碼。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Grid passwords**。

2. 在「Change SSH keys」下，選擇「Make a change」。

下載目前恢復套件

在變更 SSH 存取金鑰之前，請先下載目前的恢復套件。如果任何節點的金鑰變更程序失敗，您可以使用此檔案中的金鑰。

步驟

1. 請輸入網格的佈建密碼。

2. ${post_edited_translations.segment}

3. 將恢復套件檔案 (`.zip`) 複製到兩個安全且分隔的地點。

恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 選擇 **Continue** 。
5. ${post_edited_translations.segment}

   此程序一旦開始便無法取消。

變更 **SSH** 存取金鑰

當變更 SSH 存取金鑰的程序開始時，會產生一個包含新金鑰的新恢復套件。然後，每個節點上的金鑰都會更新。

步驟

1. ${post_edited_translations.segment}
2. 當「下載新的恢復套件」按鈕啟用時，選取*下載新的恢復套件*，並將新的恢復套件檔案 (`.zip`) 儲存至兩個安全且分隔的位置。
3. 下載完成後：

   a. 開啟 `.zip` 檔案。

   b. 確認您可以存取內容，包括 `Passwords.txt`檔案，其中包含新的 SSH 存取金鑰。

   c. 將新的恢復套件檔案 (`.zip`) 複製到兩個安全、安全且分隔的位置。

      ${post_edited_translations.segment}

   恢復套件檔案必須受到保護，因為它包含可用於從 StorageGRID 系統取得資料的加密金鑰和密碼。

4. 等待每個節點上的金鑰更新，這可能需要幾分鐘。

   如果所有節點的金鑰都已更改，則會顯示綠色成功橫幅。

   如果在更新過程中出現錯誤，系統會顯示橫幅訊息，列出金鑰變更失敗的節點數量。系統會自動對所有金鑰變更失敗的節點重試更新過程。如果重試後仍有部分節點的金鑰未變更，則會顯示 **Retry** 按鈕。

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. 解決問題。

   c. 選擇 **Retry**。

      重試只會變更先前金鑰變更嘗試失敗的節點上的 SSH 存取金鑰。

5. 在變更所有節點的 SSH 存取金鑰之後，請刪除 您下載的第一個恢復套件。
6. ${post_edited_translations.segment}

在 **StorageGRID** 中使用身分識別聯盟

${post_edited_translations.segment}

為 Grid Manager 設定身分識別聯盟

如果您希望在其他系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）中管理管理員群組和使用者，可以在 Grid Manager 中設定身分識別聯盟。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您已"特定存取權限"。
- 您使用的是 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作為身分供應商。

> ⓘ 如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用 OpenLDAP，則必須設定 OpenLDAP 伺服器。請參閱OpenLDAP 伺服器設定指南。
- 如果您打算啟用單一登入 （SSO），您已經查看了"${post_edited_translations.segment}"。
- 如果您打算使用傳輸層安全性協定 (TLS) 與 LDAP 伺服器進行通訊，則身分識別供應商將使用 TLS 1.2 或 1.3。請參閱"支援的傳出 TLS 連線加密套件"。

關於此任務

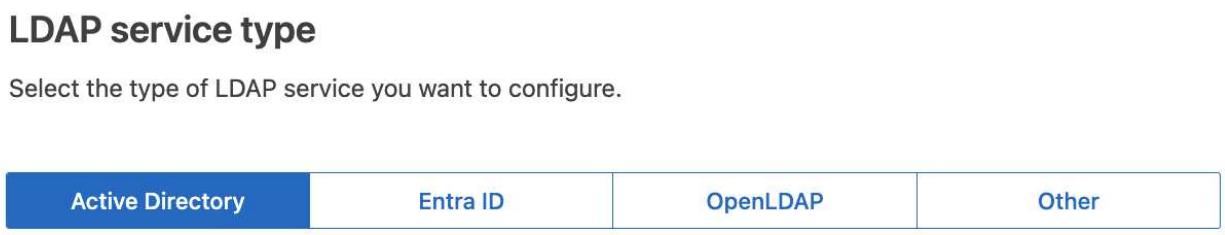
如果您想要從其他系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）匯入群組，可以為 Grid Manager 設定身分識別來源。您可以匯入以下類型的群組：

- 管理群組。管理群組中的使用者可以根據指派給該群組的管理權限，登入 Grid Manager 並執行工作。
- 租戶使用者群組適用於不使用自有身分來源的租戶。租戶群組中的使用者可以登入 Tenant Manager 並執行任務，具體任務取決於 Tenant Manager 中指派給該群組的權限。如需詳細資訊、請參閱 "建立租戶帳戶" 和 "使用租戶帳戶"。

輸入組態

步驟

1. 選擇 組態 > 存取控制 > 身分識別聯盟。
2. 選取 啟用身分識別聯盟。
3. 在 LDAP 服務類型部分，選擇要設定的 LDAP 服務類型。



選擇「其他」以設定使用 Oracle Directory Server 的 LDAP 伺服器的值。

4. 如果您選擇了 **Other**，請填寫 LDAP 屬性區段中的欄位。否則，請前往下一步。

- 使用者唯一名稱：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性等效於 Active Directory 的 `sAMAccountName`和 `OpenLDAP` 的 `uid`。如果您正在設定 Oracle Directory Server，請輸入 `uid`。
- 使用者 **UUID**：包含 LDAP 使用者永久唯一識別碼的屬性名稱。此屬性相當於 Active Directory 的 `objectGUID` 和 OpenLDAP 的 `entryUUID`。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。指定屬性的每個使用者值必須是 16 位元組或字串格式的 32 位數十六進位數字，其中會忽略連字號。
- 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性名稱。此屬性相當於 Active Directory 的 `sAMAccountName` 和 OpenLDAP 的 `cn`。如果您正在設定 Oracle Directory Server，請輸入 `cn`。
- 群組 **UUID**：包含 LDAP 群組永久唯一識別碼的屬性名稱。此屬性等效於 Active Directory 的 `objectGUID`和 `OpenLDAP` 的 `entryUUID`。如果您正在設定 Oracle Directory Server，請輸入 `nsuniqueid`。每個群組的指定屬性值必須為 32 位元十六進位數，格式可以是 16 個位元組或字串，其中連字元將被忽略。

5. 對於所有 LDAP 服務類型，請在「設定 LDAP 伺服器」部分輸入所需的 LDAP 伺服器和網路連線資訊。
   - 主機名稱：LDAP 伺服器的完整網域名稱（FQDN）或 IP 位址。
   - 連接埠：用於連接到 LDAP 伺服器的連接埠。

     STARTTLS 的預設 port 為 389，而 LDAPS 的預設 port 為 636。不過，只要您的防火牆設定正確，您可以使用任何 port。

   - 使用者名稱：將連接到 LDAP 伺服器的使用者辨別名稱 (DN) 完整路徑。

     對於 Active Directory，您也可以指定下級登入名稱或使用者主體名稱。

     ${post_edited_translations.segment}

     - `sAMAccountName` 或 `uid`
     - `objectGUID`、 `entryUUID` 或 `nsuniqueid`
     - `cn`
     - `memberOf` 或 `isMemberOf`
     - **Active Directory**： `objectSid`、 `primaryGroupID`、 `userAccountControl` 和 `userPrincipalName`
     - **Entra ID**: `accountEnabled` 與 `userPrincipalName`

   - ${post_edited_translations.segment}

     如果將來更改密碼，您必須在此頁面上更新密碼。

   - 群組基本 **DN**：您要搜尋群組之 LDAP 子樹狀結構的辨識名稱 （DN） 完整路徑。在 Active Directory 範例 （如下） 中，其辨識名稱相對於基本 DN （DC=storagegrid,DC=example,DC=com） 的所有群組，都可以用作同盟群組。

     ${post_edited_translations.segment}

   - 使用者基本 **DN**：要搜尋使用者的 LDAP 子樹的專有名稱 (DN) 的完整路徑。

${post_edited_translations.segment}

- **Bind username format**（選用）：如果無法自動判斷模式，StorageGRID 應使用的預設使用者名稱模式。

  建議提供 **Bind username format**，因為如果 StorageGRID 無法與服務帳戶連結，可允許使用者登入。

  請輸入以下模式之一：

  - **UserPrincipalName** 模式（**AD** 與 **Entra ID**）：`[USERNAME]@example.com`
  - **Down-level logon name pattern** （**AD** 和 **Entra ID**）：`example\[USERNAME]`
  - 辨別名稱模式：`CN=[USERNAME],CN=Users,DC=example,DC=com`

    ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
   - 使用 **STARTTLS**：使用 STARTTLS 來保護與 LDAP 伺服器的通訊。對於 Active Directory、OpenLDAP 或其他 LDAP 伺服器，這是建議選項，但此選項不支援 Microsoft Entra ID。
   - 使用 **LDAPS**：LDAPS （LDAP over SSL） 選項會使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Microsoft Entra ID 選擇此選項。
   - 請勿使用 **TLS**：StorageGRID 系統與 LDAP 伺服器之間的網路流量將不受保護。此選項不支援 Microsoft Entra ID。

     如果您的 Active Directory 伺服器強制執行 LDAP 簽名，則不支援使用「不使用 **TLS**」選項。您必須使用 STARTTLS 或 LDAPS。

7. ${post_edited_translations.segment}
   - 使用作業系統 **CA** 憑證：使用作業系統上安裝的預設 Grid CA 憑證來保護連線安全。
   - **Use custom CA certificate**：使用自訂安全性憑證。

     ${post_edited_translations.segment}

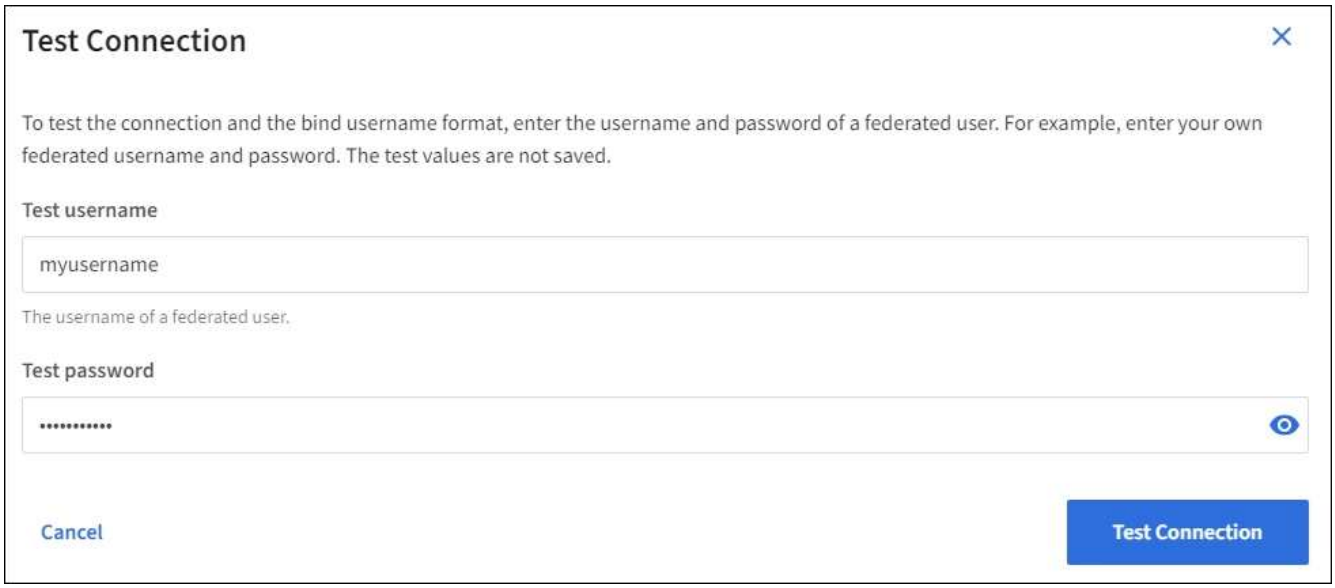
${post_edited_translations.segment}

輸入所有值後，必須先測試連線才能儲存組態。StorageGRID 會驗證 LDAP 伺服器的連線設定以及連結使用者名稱格式（如果您已提供）。

步驟

1. 選擇 **Test connection**。
2. ${post_edited_translations.segment}
   - 如果連線設定有效，則會顯示「測試連線成功」訊息。選擇*儲存*以儲存組態。
   - 如果連線設定無效，則會顯示「無法建立測試連線」訊息。選擇*關閉*。然後，解決所有問題並再次測試連線。
3. 如果您提供了連結使用者名稱格式，請輸入有效聯合使用者的使用者名稱和密碼。

   例如，請輸入您自己的使用者名稱和密碼。使用者名稱中請勿包含任何特殊字元，例如 @ 或 /。



- 如果連線設定有效，則會顯示「測試連線成功」訊息。選擇*儲存*以儲存組態。
- 如果連線設定、連結使用者名稱格式或測試使用者名稱和密碼無效，則會顯示錯誤訊息。請解決所有問題並再次測試連線。

強制與身分來源同步

StorageGRID 系統會定期從識別來源同步聯盟群組與使用者。如果您想儘快啟用或限制使用者權限，可以強制開始同步。

步驟

1. 前往身分聯盟頁面。
2. ${post_edited_translations.segment}

   同步程序可能需要一些時間，視您的環境而定。

   ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以暫時或永久停用群組和使用者的身分聯合。停用身分聯合後，StorageGRID 與身分來源之間將不再通訊。但是，您已設定的所有設定都將保留，以便您日後可以輕鬆重新啟用身分聯合。

關於此任務

在停用身分聯合之前，您應該注意以下事項：

- 已加入聯盟的用戶將無法登入。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 如果單一登入 （SSO） 狀態為 已啟用 或 沙箱模式，則 啟用身分識別同盟 核取方塊會停用。您必須先將單一登入頁面上的 SSO 狀態設為 已停用，才能停用身分識別同盟。請參閱 "${post_edited_translations.segment}"。

步驟

1. 前往身分聯盟頁面。
2. ${post_edited_translations.segment}

OpenLDAP 伺服器設定指南

${post_edited_translations.segment}

> 對於非 Active Directory 或 Microsoft Entra ID 的身分識別來源，StorageGRID 不會自動封鎖在外部被停用之使用者的 S3 存取。若要封鎖 S3 存取，請刪除該使用者的任何 S3 金鑰，或將該使用者從所有群組中移除。

${post_edited_translations.segment}

應啟用 memberof 與 refint 重疊。如需詳細資訊，請參閱 "OpenLDAP 文件：版本 2.4 管理員指南" 中的反向群組成員資格維護說明。

${post_edited_translations.segment}

${post_edited_translations.segment}

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

${post_edited_translations.segment}

請參閱 "OpenLDAP 文件：版本 2.4 管理員指南" 中關於反向群組成員資格維護的資訊。

管理 **StorageGRID** 中的管理員群組

您可以建立管理員群組來管理一個或多個管理員使用者的安全性權限。使用者必須屬於某個群組，才能獲得對 StorageGRID 系統的存取權限。

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"。
- 如果您打算匯入聯合群組，則您已設定身分聯合，且該聯合群組已存在於已設定的身分來源中。

建立管理員群組

管理員群組可讓您決定哪些使用者可以存取 Grid Manager 和 Grid Management API 中的哪些功能和操作。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以建立本機群組或匯入聯合群組。

- 如果要為本機使用者指派權限，請建立本機群組。
- 建立聯合群組，從身分來源匯入使用者。

本地群組

步驟

1. 選擇*本機群組*。
2. 請輸入該群組的顯示名稱，您可以稍後視需要更新。例如，「Maintenance Users」或「ILM Administrators」。
3. 請為群組輸入唯一名稱，此名稱之後將無法更新。
4. 選擇 **Continue** 。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 請輸入要匯入的群組名稱，務必與已設定的身分識別來源中顯示的名稱完全一致。
   - 對於 Active Directory 和 Microsoft Entra ID，請使用 sAMAccountName。
   - 對於 OpenLDAP，請使用 CN （Common Name）。
   - 對於另一個 LDAP，請使用 LDAP 伺服器的對應唯一名稱。
3. 選擇 **Continue** 。

${post_edited_translations.segment}

步驟

1. 對於*存取模式*，選擇群組中的使用者是否可以變更 Grid Manager 和 Grid Management API 中的設定並執行操作，或者他們是否只能檢視設定和功能。
   - ${post_edited_translations.segment}
   - 唯讀：使用者只能檢視設定和功能。無法對 Grid Manager 或 Grid Management API 進行任何變更或執行任何操作。本機唯讀使用者可以變更自己的密碼。

   如果使用者屬於多個群組，且其中任何一個群組設定為*唯讀*，則該使用者對所有選定的設定和功能將具有唯讀存取權限。

2. 選取一或多個 "管理員群組權限"。

   ${post_edited_translations.segment}

3. 如果要建立本機群組，請選擇「繼續」。如果要建立聯合群組，請選擇「建立群組」和「完成」。

新增使用者（僅限本地群組）

步驟

1. ${post_edited_translations.segment}

   如果您尚未建立本機使用者，則可以在不新增使用者的情況下儲存該群組。您可以在「使用者」頁面上將此群組新增至使用者。如需詳細資訊、請參閱 "管理使用者"。

2. ${post_edited_translations.segment}

檢視和編輯管理員群組

您可以檢視現有群組的詳細資訊、修改群組或複製群組。

- 若要檢視所有群組的基本資訊，請審查「群組」頁面上的表格。
- 若要檢視特定群組的所有詳細資訊或編輯群組，請使用 **Actions** 功能表或詳細資料頁面。

任務	操作選單	詳細資料頁面
檢視群組詳細資料	a. ${post_edited_translations.segment} b. 選取 **Actions** > **View group details**。	從表格中選擇群組名稱。
編輯顯示名稱（僅限本機群組）	a. ${post_edited_translations.segment} b. 選擇 **Actions** > **Edit group name**。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。	a. 選擇群組名稱以顯示詳細資訊。 b. 選擇編輯圖示 。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。
編輯存取模式或權限	a. ${post_edited_translations.segment} b. 選取 **Actions** > **View group details**。 c. ${post_edited_translations.segment} d. （可選）選擇或清除 "管理員群組權限"。 e. 選擇 **Save changes** 。	a. 選擇群組名稱以顯示詳細資訊。 b. ${post_edited_translations.segment} c. （可選）選擇或清除 "管理員群組權限"。 d. 選擇 **Save changes** 。

複製群組

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

刪除群組

當您想要從系統中移除管理群組，並移除與該群組相關聯的所有權限時，可以刪除管理群組。刪除管理群組會將所有使用者從該群組中移除，但不會刪除這些使用者。

步驟

1. 在「群組」頁面中，選取要移除的每個群組的核取方塊。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

StorageGRID 中的管理員群組權限

建立管理使用者群組時，您可以選取一或多個權限，以控制對 Grid Manager 特定功能的存取。接著，您可以將每個使用者指派給一或多個此類管理群組，以決定該使用者可以執行的工作。

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 檢視儀表板
- 檢視節點頁面
- 檢視目前及已解決的警示
- 變更自己的密碼（僅限本機使用者）
- ${post_edited_translations.segment}

${post_edited_translations.segment}

對於所有權限，群組的 存取模式 設定會決定使用者是否可以變更設定並執行作業，或者他們是否只能檢視相關的設定和功能。如果使用者屬於多個群組，且有任何群組設定為 唯讀，則該使用者將對所有選取的設定和功能具有唯讀存取權限。

以下各節說明建立或編輯管理員群組時可以指派的權限。任何未明確提及的功能都需要 **Root access** 權限。

Root 存取

${post_edited_translations.segment}

${post_edited_translations.segment}

此權限可讓您存取 Tenants 頁面上的 **Change root password** 選項，從而控制哪些使用者可以變更租戶本機 root 使用者的密碼。啟用 S3 金鑰匯入功能時，此權限也用於移轉 S3 金鑰。沒有此權限的使用者將無法看到 **Change root password** 選項。

若要授予包含「變更 root 密碼」選項的「租戶」頁面的存取權限，也需要指派「租戶帳戶」權限。

ILM

${post_edited_translations.segment}

- 規則
- ${post_edited_translations.segment}
- 原則標籤
- 儲存池
- ${post_edited_translations.segment}
- 地區
- 物件中繼資料查詢

${post_edited_translations.segment}

${post_edited_translations.segment}

使用者必須擁有維護權限才能使用這些選項：

- 組態 > 存取控制：
  - 網格密碼
- 組態 > 網路：
  - ${post_edited_translations.segment}
- ${post_edited_translations.segment}
  - 取消委任
  - 擴充
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
- 維護 > 系統：
  - 恢復套件
  - 軟體更新
- 支援 > 工具：
  - ${post_edited_translations.segment}

沒有維護權限的使用者可以檢視這些頁面，但不能編輯：

- ${post_edited_translations.segment}
  - DNS 伺服器
  - Grid 網路
  - NTP 伺服器
- 維護 > 系統：

    - 授權
- 組態 > 網路：
    - ${post_edited_translations.segment}
- 組態 > 安全性：
    - 憑證
- 組態 > 監控：
    - 稽核與 syslog 伺服器

管理警報

此權限提供存取管理警示的選項。使用者必須擁有此權限才能管理靜默、警示通知和警示規則。

計量查詢

此權限允許存取：

- 支援 > 工具 > 計量 頁面
- ${post_edited_translations.segment}
- 包含計量的網格管理器儀表板卡片

物件中繼資料查詢

此權限提供對 **ILM** > 物件中繼資料查詢 頁面的存取。

${post_edited_translations.segment}

此權限允許存取以下額外的網格組態選項：

- ${post_edited_translations.segment}
    - ${post_edited_translations.segment}
- 組態 > 系統：
- ${post_edited_translations.segment}
    - 連結成本

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

租戶帳戶

此權限賦予您以下能力：

- 存取「租戶」頁面，您可以在此建立、編輯和移除租戶帳戶。

- ${post_edited_translations.segment}
- 檢視包含租戶詳細資訊的 Grid Manager 儀表板卡片

在 StorageGRID 中管理使用者

您可以檢視本機使用者和聯合使用者。您也可以建立本機使用者並將其指派至本機管理員群組，以決定這些使用者可以存取哪些 Grid Manager 功能。

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"。

建立本機使用者

您可以建立一個或多個本機使用者，並將每個使用者指派到一個或多個本機群組。群組的權限控制使用者可以存取哪些 Grid Manager 和 Grid Management API 功能。

您只能建立本機使用者。若要管理聯合使用者和群組，請使用外部身分來源。

Grid Manager 包含一個名為「root」的預先定義本機使用者。您無法移除 root 使用者。

> 如果啟用了單一登入 （SSO），則本機使用者無法登入 StorageGRID。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Admin users**。
2. 選取 **Create user**。

請輸入使用者憑證

步驟

1. 請輸入使用者的全名、唯一的使用者名稱和密碼。
2. 如果此使用者不應擁有 Grid Manager 或 Grid Management API 的存取權，可選擇選取「是」。
3. 選擇 **Continue** 。

分配到各個群組

步驟

1. （可選）將使用者指派到一個或多個群組，以決定使用者的權限。

   如果您尚未建立群組，則可以在不選擇群組的情況下儲存使用者。您可以在「群組」頁面上將此使用者新增至群組。

   如果使用者屬於多個使用者群組，則權限會累積。詳情請參閱"${post_edited_translations.segment}"。

2. 選擇 **Create user** ，然後選擇 **Finish** 。

檢視及編輯本機使用者

您可以檢視現有本機使用者和聯合使用者的詳細資訊。您可以修改本機使用者，例如變更使用者的全名、密碼或群組成員資格。您也可以暫時阻止使用者存取 Grid Manager 和 Grid Management API。

您只能編輯本機使用者。若要管理聯合使用者，請使用外部身分來源。

- 若要檢視所有本機和聯合使用者的基本資訊，請審查「使用者」頁面上的表格。
- 若要檢視特定使用者的所有詳細資訊、編輯本機使用者或變更本機使用者的密碼，請使用 **Actions** 功能表或詳細資料頁面。

  任何編輯都會在使用者下次登出並重新登入 Grid Manager 時生效。

  本機使用者可以使用 Grid Manager 橫幅中的「變更密碼」選項來變更自己的密碼。

任務	操作選單	詳細資料頁面
檢視使用者詳細資料	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。	從表格中選擇使用者的姓名。
編輯全名（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **Edit full name**。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇編輯圖示 。 c. 請輸入新名稱。 d. 選擇 **Save changes** 。
拒絕或允許 StorageGRID 存取	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選取「存取」索引標籤。 d. 選擇「是」可阻止使用者登入 Grid Manager 或 Grid Management API，選擇「否」可允許使用者登入。 e. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選取「存取」索引標籤。 c. 選擇「是」可阻止使用者登入 Grid Manager 或 Grid Management API，選擇「否」可允許使用者登入。 d. 選擇 **Save changes** 。
變更密碼（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選擇「密碼」標籤。 d. 請輸入新密碼。 e. 選擇 **Change password**。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇「密碼」標籤。 c. 請輸入新密碼。 d. 選擇 **Change password**。

任務	操作選單	詳細資料頁面
變更群組（僅限本機使用者）	a. 選取該使用者的核取方塊。 b. 選擇 **Actions** > **View user details**。 c. 選擇「群組」索引標籤。 d. （可選）選取群組名稱後的連結，即可在新瀏覽器標籤頁中檢視該群組的詳細資訊。 e. 選擇 **Edit groups** 以選擇不同的群組。 f. 選擇 **Save changes** 。	a. 選擇使用者名稱以顯示詳細資訊。 b. 選擇「群組」索引標籤。 c. （可選）選取群組名稱後的連結，即可在新瀏覽器標籤頁中檢視該群組的詳細資訊。 d. 選擇 **Edit groups** 以選擇不同的群組。 e. 選擇 **Save changes** 。

匯入同盟使用者

您可以將一個或多個聯合使用者（最多 100 個使用者）直接匯入到「使用者」頁面。

步驟

1. 選擇 **Configuration** > **Access control** > **Admin users**。
2. 選取 **Import federated users**。
3. 輸入一個或多個聯合使用者的 UUID 或使用者名稱。

   對於多個條目，請將每個 UUID 或使用者名稱新增至新的一行。

4. 選取 **Import**。

   如果一個或多個使用者的匯入作業失敗，請執行下列步驟：

   a. 展開 **Users not imported** ，然後選擇 **Copy users** 。

   b. 選擇 **Previous** ，然後將複製的使用者貼上到 **Import federated users** 對話方塊中，重新嘗試匯入。

   關閉*匯入聯合使用者*對話方塊後，成功匯入的使用者的聯合使用者資訊將顯示在「使用者」頁面上。

複製使用者

您可以複製現有使用者，建立具有相同權限的新使用者。

步驟

1. 選取該使用者的核取方塊。
2. 選擇 **Actions** > **Duplicate user**。
3. 完成複製使用者精靈。

刪除使用者

您可以刪除本機使用者，將其從系統中永久移除。

您無法刪除 root 使用者。

步驟

1. 在「使用者」頁面中，選取要移除的每個使用者的核取方塊。
2. 選擇*動作* > 刪除使用者。
3. 選取*刪除使用者*。

使用單一登入 (SSO)

了解 StorageGRID 單一登入

啟用單一登入 （SSO） 後，使用者只有在透過貴組織實作的 SSO 登入流程驗證其憑證後，才能存取 Grid Manager、Tenant Manager、Grid Management API 或 Tenant Management API。本機使用者無法登入 StorageGRID。

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在網頁瀏覽器中輸入任何 StorageGRID 管理節點的完整網域名稱或 IP 位址。

   StorageGRID 登入頁面隨即出現。

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

   當您輸入租戶帳戶的完整 URL （即完整網域或 IP 位址，後跟 `/?accountId=20-digit-account-id`）時，不會顯示 StorageGRID 登入頁面。相反地，您會立即被重新導向至您組織的 SSO 登入頁面，您可以在該頁面 使用您的 SSO 憑證登入。

2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 若要存取 Tenant Manager，請輸入 20 位數的租戶帳戶 ID，或如果租戶出現在最近的帳戶清單中，請按名稱選擇租戶。
3. 選擇 **Sign in**

   StorageGRID 會將您重新導向至您組織的 SSO 登入頁面。例如：

4. 使用您的 SSO 憑證登入。

   如果您的 SSO 憑證正確：

a. ${post_edited_translations.segment}
b. StorageGRID 驗證驗證回應。
c. ${post_edited_translations.segment}

${post_edited_translations.segment}

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

啟用 **SSO** 後登出

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 選擇「登出」。

StorageGRID 登入頁面隨即顯示。最近使用的帳戶 下拉式功能表已更新，包含 **Grid Manager** 或租戶名稱，以便您日後能更快速地存取這些使用者介面。

此表摘要說明如果您使用的是單一瀏覽器工作階段，在登出時會發生什麼事。如果您在多個瀏覽器工作階段中登入 StorageGRID，則必須個別登出所有的瀏覽器工作階段。

如果您已登入.....	然後您登出.....	您已登出.....
Grid Manager 位於一個或多個管理節點上	任何管理節點上的 Grid Manager	所有管理節點上的 Grid Manager *注意：*如果您使用 Entra ID 進行 SSO，則可能需要幾分鐘才能從所有管理節點登出。
${post_edited_translations.segment}	${post_edited_translations.segment}	所有管理節點上的租戶管理器
${post_edited_translations.segment}	Grid Manager	僅限 Grid Manager。您也必須從 Tenant Manager 登出才能登出單一登入 （SSO）。

StorageGRID 單一登入的要求和注意事項

在為 StorageGRID 系統啟用單一登入 （SSO） 之前，請審查相關要求和注意事項。

${post_edited_translations.segment}

StorageGRID 支援以下 SSO 身分供應商 (IdP)：

- Active Directory Federation Service （AD FS）

- ${post_edited_translations.segment}
- PingFederate

您必須先為您的 StorageGRID 系統設定身分識別同盟，然後才能設定 SSO 身分識別供應商。您用於身分識別同盟的 LDAP 服務類型會控制您可以實作的 SSO 類型。

${post_edited_translations.segment}	**${post_edited_translations.segment}**
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

${post_edited_translations.segment}

您可以使用以下任何版本的 AD FS：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Windows Server 2016 應該使用 "KB3201845 更新"或更高版本。

其他要求

- 傳輸層安全協定 (TLS) 1.2 或 1.3
- Microsoft .NET Framework，版本 3.5.1 或更高版本

Entra ID 的相關注意事項

如果您使用 Entra ID 作為 SSO 類型，且使用者的使用者主體名稱未使用 sAMAccountName 作為前綴，則當 StorageGRID 與 LDAP 伺服器斷開連線時，可能會出現登入問題。若要允許使用者登入，您必須還原與 LDAP 伺服器的連線。

伺服器憑證要求

預設情況下，StorageGRID 會在每個管理節點上使用管理介面憑證來保護對 Grid Manager、Tenant Manager、Grid Management API 和 Tenant Management API 的存取。當您為 StorageGRID 設定信賴方信任（AD FS）、企業應用程式（Entra ID）或服務供應商連線（PingFederate）時，您將使用伺服器憑證作為 StorageGRID 請求的簽署憑證。

如果您尚未"已為管理介面設定自訂憑證"，請立即執行。安裝自訂伺服器憑證後，該憑證將用於所有管理節點，您可以將其用於所有 StorageGRID 信賴方信任、企業應用程式或 SP 連線。

不建議在信賴方信任、企業應用程式或 SP 連線中使用管理節點的預設伺服器憑證。如果節點發生故障並恢復後，系統會產生一個新的預設伺服器憑證。在登入已復原的節點之前，您必須使用新憑證更新信賴方信任、企業應用程式或 SP 連線。

您可以透過登入該節點的命令 shell 並前往 `/var/local/mgmt-api` 目錄，來存取 Admin Node 的伺服器憑證。自訂伺服器憑證的名稱為 `custom-server.crt`。該節點的預設伺服器憑證名稱為 `server.crt`。

連接埠需求

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)。請參閱"${post_edited_translations.segment}"。

確認聯合使用者可以登入 **StorageGRID**

${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"。
- ${post_edited_translations.segment}

步驟

1. 如果存在租戶帳戶，請確認沒有租戶使用自己的身分來源。

   啟用單一登入 （SSO） 後，租戶管理員中設定的身分來源將會被 Grid Manager 中設定的身分來源覆寫。除非擁有 Grid Manager 身分來源的帳戶，否則屬於租戶身分來源的使用者將無法再登入。

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   a. 從 Grid Manager 中，選擇 **Configuration** > **Access control** > **Admin groups**。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. 確認您可以以聯合群組使用者的身分重新登入 Grid Manager。

3. ${post_edited_translations.segment}
   a. 從 Grid Manager 中選擇 租戶。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. 從 Tenant Manager 中選擇 **Access Management** > **Groups**。
   g. ${post_edited_translations.segment}

h. ${post_edited_translations.segment}

i. 請確認您可以以聯合群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求和注意事項"
- "${post_edited_translations.segment}"
- "使用租戶帳戶"

在 **StorageGRID** 中設定 **SSO**

您可以依照 「Configure SSO」 精靈的指示並進入沙箱模式，在為所有 StorageGRID 使用者啟用單一登入 （SSO） 之前進行設定與測試。啟用 SSO 之後，您可以在需要變更或重新測試組態時返回沙箱模式。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 您已為 StorageGRID 系統設定身分識別聯盟。
- 對於身分識別聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分識別供應商選擇 Active Directory 或 Entra ID。

${post_edited_translations.segment}	**${post_edited_translations.segment}**
Active Directory Federation Service （AD FS）	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

關於此任務

啟用 SSO 後，當使用者嘗試登入管理節點時，StorageGRID 會向 SSO 身分供應商傳送驗證請求。SSO 身分供應商隨後會向 StorageGRID 傳送驗證回應，指示驗證要求是否成功。對於成功的請求：

- 來自 Active Directory 或 PingFederate 的回應包含使用者的通用唯一識別碼 (UUID)。
- Entra ID 的回應包含使用者主體名稱 (UPN)。

為了讓 StorageGRID （服務供應商）和 SSO 身分供應商能夠安全地就使用者身分驗證請求進行通訊，您需要完成以下任務：

1. 在 StorageGRID 中設定組態。
2. 使用 SSO 身分識別供應商的軟體，為每個管理節點建立信任憑證者關係（AD FS）、企業應用程式（Entra ID）或服務供應商（PingFederate）。
3. 返回 StorageGRID 以啟用 SSO。

沙盒模式便於進行此來回組態，並在啟用單一登入 (SSO) 之前測試所有設定。使用沙盒模式時，使用者無法使用 SSO 登入。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on**。「單一登入」頁面隨即出現。

   如果「設定 SSO 設定」按鈕處於停用狀態，請確認您已將身分識別供應商設定為聯合身分識別來源。請參閱 "單一登入的要求和注意事項"。

2. 選取 **Configure SSO settings**。「提供身分供應商詳細資料」頁面隨即出現。

提供身分識別供應商詳細資訊

步驟

1. 從下拉清單中選取 **SSO** 類型。
2. ${post_edited_translations.segment}

   若要尋找同盟服務名稱，請前往 Windows Server Manager。選取 **Tools** > **AD FS Management**。從 Action 功能表中，選取 **Edit Federation Service Properties**。同盟服務名稱會顯示在第二個欄位中。

3. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

   - ${post_edited_translations.segment}

     如果變更 CA 憑證，請立即 "${post_edited_translations.segment}" 並測試是否能成功單一登入 Grid Manager。

4. 選擇 繼續。隨即顯示「提供信任憑證者識別碼」頁面。

${post_edited_translations.segment}

1. 根據您選擇的 SSO 類型，填寫「提供信賴方識別碼」頁面上的欄位。

Active Directory

a. 為 StorageGRID 指定*信賴方識別碼*。此值控制您在 AD FS 中為每個信賴方信任所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示網格中每個管理節點的信賴方識別碼。

   > 您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

Entra ID

a. 在「企業應用程式」區段中，指定 StorageGRID 的 企業應用程式名稱。此值控制您在 Entra ID 中為每個企業應用程式使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點對應的企業應用程式名稱。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

b. 請按照 "在 Entra ID 中建立企業應用程式" 中的步驟，為表格中列出的每個管理節點建立企業應用程式。

c. 從 Entra ID 複製每個企業應用程式的同盟中繼資料 URL。然後，將此 URL 貼到 StorageGRID 中對應的*同盟中繼資料 URL* 欄位中。

d. 複製並貼上所有管理節點的聯盟中繼資料 URL 後，選取 儲存並進入沙盒模式。

PingFederate

a. 在「服務供應商 （SP）」部分，為 StorageGRID 指定 **SP** 連線 **ID**。此值控制您在 PingFederate 中每個 SP 連線所使用的名稱。

   - 例如，如果您的網格只有一個 Admin 節點，且您預計未來不會增加更多 Admin 節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示系統中每個管理節點的 SP 連線 ID。

   > 您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線。為每個管理節點建立 SP 連線可確保使用者可以安全地登入和登出任何管理節點。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. ${post_edited_translations.segment}

設定信賴方信任、企業應用程式或 **SP** 連線

儲存組態並進入沙盒模式後，您可以完成並測試所選 SSO 類型的組態。

StorageGRID 可依需求保持在沙盒模式下。但是，只有同盟使用者和本機使用者才能登入。

Active Directory

步驟

1. 前往 Active Directory Federation Services （AD FS）。
2. 使用「設定 SSO」頁面上表格中顯示的每個信賴方識別碼，為 StorageGRID 建立一個或多個信賴方信任。

   ${post_edited_translations.segment}

   如需說明，請前往 "${post_edited_translations.segment}"。

Entra ID

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. ${post_edited_translations.segment}
4. 請依照 "在 Entra ID 中建立企業應用程式" 中的步驟，將每個管理節點的 SAML 中繼資料檔案上傳至其對應的 Entra ID 企業應用程式。

PingFederate

步驟

1. ${post_edited_translations.segment}
2. 然後，對網格中的任何其他管理節點重複這些步驟：
   a. 登入節點。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 下載並儲存該節點的 SAML 中繼資料。
3. 前往 PingFederate。
4. "為 StorageGRID 建立一個或多個服務供應商 （SP） 連線"。使用每個管理節點的 SP 連線 ID （顯示在「設定 SSO」頁面上的表格中）以及您為該管理節點下載的 SAML 中繼資料。

   您必須為表中所示的每個管理節點建立一個 SP 連線。

測試組態

在對整個 StorageGRID 系統強制使用單一登入之前，請確認每個管理節點的單一登入和單一登出都已正確設定。

Active Directory

步驟

1. 在「設定 SSO」頁面上，找到精靈的「測試組態」步驟中的連結。

   URL 源自於您在「聯合服務名稱」欄位中輸入的值。

2. 選擇連結，或將 URL 複製並貼上到瀏覽器中，即可存取您的身分提供者的登入頁面。
3. 若要確認您可以使用 SSO 登入 StorageGRID，請選取 * 登入下列其中一個網站 *，選取您主要管理節點的信賴方識別碼，然後選取 * 登入 *。
4. 請輸入您的聯合使用者名稱和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
5. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

Entra ID

步驟

1. 前往 Azure 入口網站中的單一登入頁面。
2. 選擇 **Test this application**。
3. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
4. 重複這些步驟，以驗證網格中每個管理節點的 SSO 連線。

PingFederate

步驟

1. 在「設定 SSO」頁面中，選取「沙盒模式」訊息中的第一個連結。

   一次選擇並測試一個連結。

2. 請輸入聯合使用者的憑證。
   - 如果 SSO 登入和登出操作成功，則會顯示成功訊息。
   - 如果 SSO 作業未成功，則會出現錯誤訊息。請修正此問題，清除瀏覽器的 Cookie，然後重試。
3. ${post_edited_translations.segment}

   如果看到「頁面已過期」訊息，請選擇瀏覽器中的「後退」按鈕，然後重新提交您的憑證。

啟用單一登入

${post_edited_translations.segment}

當啟用 SSO 時，所有使用者都必須使用 SSO 來存取 Grid Manager、Tenant Manager、Grid Management API 及 Tenant Management API。本機使用者無法再存取 StorageGRID。

步驟

1. 在設定 SSO 精靈的測試組態步驟中，選取 啟用 **SSO**。
2. 查看警告訊息，然後選擇 **Enable SSO**。

   現在已啟用單一登入。單一登入頁面隨即出現，且現在包含您剛才設定的 SSO 詳細資料。

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

如果您正在使用 Azure Portal，且您從用於存取 Entra ID 的相同電腦存取 StorageGRID，請確保 Azure Portal 使用者也是授權的 StorageGRID 使用者（已匯入至 StorageGRID 的聯合群組中的使用者），或在嘗試登入 StorageGRID 之前登出 Azure Portal。

在 **AD FS** 中為 **StorageGRID** 建立信賴方信任

您必須使用 Active Directory Federation Services （AD FS） 為系統中的每個管理節點建立信賴方信任。您可以使用 PowerShell 命令建立信賴方信任、從 StorageGRID 匯入 SAML 中繼資料，或手動輸入資料。

開始之前

- 您已為 StorageGRID 設定單一登入，並選取 **AD FS** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您知道系統中每個 Admin 節點的完整網域名稱（或 IP 位址）和信任憑證者識別碼。您可以在 StorageGRID 設定單一登入頁面的 Admin 節點詳細資料表中找到這些值。

  您必須為 StorageGRID 系統中的每個管理節點建立信賴憑證者信任。為每個管理節點建立信賴憑證者信任，可確保使用者能夠安全地登入和登出任何管理節點。

- ${post_edited_translations.segment}
- 您正在使用 AD FS Management 嵌入式管理單元，且您屬於 Administrators 群組。
- ${post_edited_translations.segment}

關於此任務

這些說明適用於 Windows Server 2016 AD FS。如果您使用的是不同版本的 AD FS，您會注意到程序中的些微差異。如果您有任何疑問，請參閱 Microsoft AD FS 文件。

使用 **Windows PowerShell** 建立信賴憑證者信任

您可以使用 Windows PowerShell 快速建立一個或多個信賴方信任。

步驟

1. 從 Windows 開始功能表中，以滑鼠右鍵選取 PowerShell 圖示，然後選取*以系統管理員身分執行*。

2. 在 PowerShell 命令提示字元下，輸入以下命令：

   `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` United States (US) - Company name: NetApp - Source text: `Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"` - The source text only contains an image placeholder tag. - According to the instructions, I must keep all `` tags exactly as they appear in the source text and return only the correct translation.

Output: `Add-AdfsRelyingPartyTrust -Name "*Admin_Node_Identifer*" -MetadataURL "https://*Admin_Node_FQDN*/api/saml-metadata"`_

+ 對於 ***`Admin_Node_Identifier`***，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， **`SG-DC1-ADM1`**。 針對 *`Admin_Node_FQDN`*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

1. ${post_edited_translations.segment}

   AD FS 管理工具出現。

2. ${post_edited_translations.segment}

   信賴方信任清單隨即出現。

3. 為新建立的信賴方信任新增存取控制原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇存取控制原則。
   d. ${post_edited_translations.segment}
4. 為新建立的信賴方信任新增宣告發行原則：
   a. 找到您剛建立的信賴方信任。
   b. ${post_edited_translations.segment}
   c. 選擇 新增規則。
   d. ${post_edited_translations.segment}
   e. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   f. ${post_edited_translations.segment}
   g. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   h. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   i. 選擇 **Finish**，然後選擇 **OK**。
5. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

6. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
7. 完成後，返回 StorageGRID 並"測試所有信賴憑證者信任"確認其組態是否正確。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇「匯入有關依賴方的線上或區域網路上發佈的資料」。
5. 在「聯合中繼資料位址（主機名稱或 URL）」中，輸入此管理節點的 SAML 中繼資料的位置：

`https://Admin_Node_FQDN/api/saml-metadata`

針對 *Admin_Node_FQDN*，請輸入相同 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

6. ${post_edited_translations.segment}

輸入顯示名稱時，請使用管理節點的信賴方識別碼，該識別碼必須與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

7. 新增聲明規則：
   a. ${post_edited_translations.segment}
   b. 選擇 新增規則：
   c. ${post_edited_translations.segment}
   d. 在「設定規則」頁面上，輸入該規則的顯示名稱。

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。
   g. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。
   h. 選擇 **Finish**，然後選擇 **OK**。
8. 確認中繼資料已成功匯入。
   a. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。
   b. 確認「端點」、「識別碼」和「簽名」標籤上的欄位已填寫。

如果缺少中繼資料，請確認 Federation 中繼資料地址是否正確，或手動輸入值。

9. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。
10. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

手動建立信賴方信任

如果您選擇不匯入依賴方信託的資料，您可以手動輸入這些值。

步驟

1. 在 Windows Server 管理員中，選取 工具，然後選取 **AD FS Management**。
2. 在「操作」下，選擇 **Add Relying Party Trust**。
3. 在歡迎頁面上，選擇 **Claims aware**，然後選擇 **Start**。
4. 選擇 **Enter data about the relying party manually**，然後選擇 **Next**。
5. 完成信賴方信任嚮導：

   a. ${post_edited_translations.segment}

      為保持一致性，請使用管理節點的信賴方識別碼，該識別碼應與 Grid Manager 單一登入頁面上顯示的識別碼完全一致。例如， `SG-DC1-ADM1`。

   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. 輸入管理節點的 SAML 服務端點 URL：

      `https://Admin_Node_FQDN/api/saml-response`

      針對 *`Admin_Node_FQDN`*，請輸入 Admin Node 的完整網域。（如有需要，您也可以改用該節點的 IP 位址。然而，如果您在此處輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴憑證者信任。）

   e. ${post_edited_translations.segment}

      `*Admin_Node_Identifier*`_

      對於 *`Admin_Node_Identifier`*，請輸入管理節點的信賴方識別碼，其內容必須與單一登入頁面上顯示的內容完全一致。例如， `SG-DC1-ADM1`。

   f. 檢查設定，儲存信賴方信任，然後結束精靈。

      「編輯宣告簽發原則」對話方塊隨即出現。

      ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 在「設定規則」頁面上，輸入該規則的顯示名稱。

${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. 在映射表的 LDAP 屬性欄中，鍵入 **objectGUID** 或選擇 **User-Principal-Name**。

e. 在對應表的「傳出宣告類型」欄位中，從下拉清單中選擇「名稱 ID」。

f. 選擇 **Finish**，然後選擇 **OK**。

7. 以滑鼠右鍵按一下信賴方信任，以開啟其屬性。

8. ${post_edited_translations.segment}

a. 選擇 新增 **SAML**。

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

d. ${post_edited_translations.segment}

```
https://Admin_Node_FQDN/api/saml-logout
```

對於 *Admin_Node_FQDN*，請輸入管理節點的完整網域名稱。（如有必要，您也可以使用節點的 IP 位址。但是，如果您在此輸入 IP 位址，請注意，如果該 IP 位址發生變更，您必須更新或重新建立此信賴方信任。）

a. 選擇 **OK** 。

9. 在「簽署」標籤上，指定此信賴方信任的簽署憑證：

a. 新增自訂憑證：

- 如果您有已上傳至 StorageGRID 的自訂管理憑證，請選擇該憑證。
- 如果沒有自訂憑證，請登入管理節點，前往管理節點的 `/var/local/mgmt-api`目錄，然後新增 `custom-server.crt`憑證檔案。

> 不建議使用管理節點的預設憑證 (`server.crt`。如果管理節點發生故障，恢復節點後將重新產生預設憑證，屆時您需要更新信賴方信任關係。

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

10. 重複這些步驟，為 StorageGRID 系統中的所有管理節點設定信賴方信任。

11. 完成後，請返回 StorageGRID 並"測試所有信賴憑證者信任"以確認其已正確設定。

在 **Entra ID** 中為 **StorageGRID** 建立企業應用程式

您可以使用 Entra ID 為系統中的每個管理節點建立一個企業應用程式。

開始之前

- 您已開始為 StorageGRID 設定單一登入，並選擇了 **Entra ID** 作為 SSO 類型。
- 您在 Grid Manager 中有 "進入沙盒模式"。

- 您擁有系統中每個管理節點的 企業應用程式名稱。您可以從「設定 SSO」頁面上的管理節點詳細資料表格中複製這些值。

> 您必須為 StorageGRID 系統中的每個管理節點建立一個企業應用程式。為每個管理節點配備企業應用程式可確保使用者可以安全地登入和登出任何管理節點。

- 您擁有使用 Entra ID 建立企業應用程式的經驗。
- ${post_edited_translations.segment}
- 您在 Entra ID 帳戶中擁有以下角色之一：Global Administrator、Cloud Application Administrator、Application Administrator 或服務主體的擁有者。

存取 **Entra ID**

步驟

1. 登入 "${post_edited_translations.segment}"。
2. 導航至 "Entra ID"。
3. 選擇 "企業應用程式"。

${post_edited_translations.segment}

若要在 StorageGRID 中儲存 Entra ID 的單一登入組態，您必須使用 Entra ID 為每個管理節點建立一個企業應用程式。您將從 Entra ID 複製同盟中繼資料 URL，並將其貼到「設定單一登入」頁面上對應的 同盟中繼資料 **URL** 欄位中。

步驟

1. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 選擇 **Create your own application**。
   c. 對於名稱，請輸入您從「設定 SSO」頁面上的「管理節點詳細資料」表中複製的*企業應用程式名稱*。
   d. 保持選取「整合您在資源庫中找不到的任何其他應用程式（非資源庫）」選項按鈕。
   e. 選擇 **Create** 。
   f. 在「2. 設定單一登入」方塊中選擇「開始使用」連結，或在左側邊欄中選擇「單一登入」連結。
   g. 選取 **SAML** 核取方塊。
   h. 複製 **App Federation Metadata Url**，您可以在 **Step 3 SAML Signing Certificate** 下找到它。
   i. 前往「設定 SSO」頁面，並將 URL 貼到與您使用的「企業應用程式名稱」對應的「同盟中繼資料 URL」欄位中。
2. 為每個管理節點貼上同盟中繼資料 URL 並對 SSO 組態進行所有其他必要的變更後，在「設定 SSO」頁面上選擇「儲存」。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 從管理節點登入 StorageGRID。
   b. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   c. 選擇按鈕以下載該管理節點的 SAML 中繼資料。
   d. 儲存檔案，然後將其上傳到 Entra ID。

將 **SAML** 中繼資料上傳到每個企業應用程式

為每個 StorageGRID 管理節點下載 SAML 中繼資料檔案後，在 Entra ID 中執行下列步驟：

步驟

1. ${post_edited_translations.segment}
2. 對每個企業應用程式重複這些步驟：

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}
   b. 將 **Assignment required** 設為 **No** （除非您想單獨設定指派）。
   c. 前往單一登入頁面。
   d. ${post_edited_translations.segment}
   e. 選擇「上傳中繼資料檔案」按鈕，然後選擇您為對應的管理節點下載的 SAML 中繼資料檔案。
   f. 檔案載入完成後，選擇 **Save**，然後選擇 **X** 以關閉窗格。您將返回「使用 SAML 設定單一登入」頁面。
3. "${post_edited_translations.segment}"。

在 **PingFederate** 中為 **StorageGRID** 建立服務提供者連線

您需要使用 PingFederate 為系統中的每個管理節點建立一個服務供應商 （SP） 連線。為了加快此過程，您將從 StorageGRID 匯入 SAML 中繼資料。

開始之前

- ${post_edited_translations.segment}
- 您在 Grid Manager 中有 "進入沙盒模式"。
- 您擁有系統中每個管理節點的 **SP** 連線 **ID**。您可以在「設定 SSO」頁面的管理節點詳細資料表中找到這些值。
- 您已下載系統中每個管理節點的 **SAML** 中繼資料。
- 您有在 PingFederate Server 中建立 SP 連線的經驗。
- 您已取得 "管理員參考指南" PingFederate 伺服器端所需的檔案。PingFederate 文件中提供了詳細的逐步說明和解釋。
- 您已取得 "管理員權限" PingFederate 伺服器端所需的檔案。

關於此任務

這些說明摘要介紹如何將 PingFederate Server 10.3 版設定為 StorageGRID 的 SSO 供應商。如果您使用的是

其他版本的 PingFederate，您可能需要調整這些說明。有關您版本的詳細說明，請參閱 PingFederate Server 文件。

完成 **PingFederate** 中的先決條件

在您可以建立將用於 StorageGRID 的 SP 連線之前，您必須先在 PingFederate 中完成先決條件工作。當您設定 SP 連線時，將會使用來自這些先決條件的資訊。

建立資料儲存區

如果您尚未執行此操作，請建立資料儲存區以將 PingFederate 連線至 AD FS LDAP 伺服器。請使用您在 StorageGRID 中 "${post_edited_translations.segment}" 時所使用的值。

- 類型：目錄（LDAP）
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

建立密碼認證資料驗證器

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 搜尋篩選條件：sAMAccountName=${username}
- ${post_edited_translations.segment}

建立 **IdP** 介面卡執行個體

如果還沒有建立 IdP 介面卡執行個體，請建立一個。

步驟

1. 前往 **Authentication** > **Integration** > **IdP Adapters**。
2. 選擇 **Create New Instance**。
3. 在「類型」標籤上，選擇「HTML Form IdP Adapter」。
4. 在 IdP Adapter 標籤上，選擇「在『Credential Validators』新增一行」。
5. 選取您建立的 ${post_edited_translations.segment}。
6. 在「介面卡屬性」標籤上，為「**Pseudonym**」選擇「**username**」屬性。
7. 選取 **Save** 。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 前往 **Security** > **Signing & Decryption Keys & Certificates**。

2. 建立或匯入簽署憑證。

在 **PingFederate** 中建立 **SP** 連線

在 PingFederate 中建立 SP 連線時，您需要匯入從 StorageGRID 下載的管理節點 SAML 中繼資料。該中繼資料檔案包含您需要的許多特定值。

> 您必須為 StorageGRID 系統中的每個管理節點建立一個 SP 連線，以便使用者可以安全地登入和登出任何節點。請依照以下說明建立第一個 SP 連線。然後，前往 <<${post_edited_translations.segment}>> 建立您所需的任何其他連線。

選擇 **SP** 連線類型

步驟

1. 前往 **Applications** > **Integration** > **SP Connections**。
2. 選擇 **Create Connection**。
3. 選擇 **Do not use a template for this connection**。
4. ${post_edited_translations.segment}

匯入 **SP** 中繼資料

步驟

1. 在「匯入中繼資料」索引標籤上，選取 檔案。
2. 選擇您從管理節點的「設定 SSO」頁面下載的 SAML 中繼資料檔案。
3. ${post_edited_translations.segment}

   合作夥伴實體 ID 和連線名稱設定為 StorageGRID SP 連線 ID。（例如，10.96.105.200-DC1-ADM1-105-200）。基本 URL 是 StorageGRID 管理節點的 IP 位址。

4. 選擇 **Next** 。

${post_edited_translations.segment}

步驟

1. 在「瀏覽器 SSO」標籤中，選擇「設定瀏覽器 SSO」。
2. ${post_edited_translations.segment}
3. 選擇 **Next** 。
4. ${post_edited_translations.segment}
5. 在「斷言建立」標籤上，選取「設定斷言建立」。
   a. 在「身分映射」標籤上，選取 **Standard**。
   b. ${post_edited_translations.segment}
6. 如需延長合約，請選擇 **Delete** 以移除 `urn:oid`（未使用）。

對應介面卡執行個體

步驟

1. 在「驗證來源對應」標籤上，選擇 **Map New Adapter Instance**。
2. 在「介面卡執行個體」標籤上，選擇您建立的介面卡執行個體。
3. 在「映射方法」標籤上，選取*從資料儲存區擷取其他屬性*。
4. 在「屬性來源和使用者尋找」標籤上，選擇 **Add Attribute Source**。
5. 在「資料儲存區」標籤上，提供執行摘要並選擇您新增的 資料儲存區 。
6. 在 LDAP 目錄搜尋標籤上：
   - 輸入 **Base DN**，該值應與您在 StorageGRID 中為 LDAP 伺服器輸入的值完全相符。
   - 在搜尋範圍中，選擇 **Subtree**。
   - 對於根物件類別，搜尋並新增下列屬性之一：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二進位屬性編碼類型標籤上，為 **objectGUID** 屬性選擇 **Base64**。
8. 在 LDAP 篩選器標籤上，輸入 **sAMAccountName=${username}**。
9. 在「屬性合約履行」標籤上，從「來源」下拉清單中選擇 **LDAP** （屬性），然後從「值」下拉清單中選擇 **objectGUID** 或 **userPrincipalName**。
10. 審查並儲存屬性來源。
11. 在「Failsave 屬性來源」標籤上，選取 中止 **SSO** 交易。
12. 審查摘要並選擇 **Done**。
13. 選擇 **Done**。

設定通訊協定設定

步驟

1. 在「**SP Connection**」>「**Browser SSO**」>「**Protocol Settings**」標籤上，選擇「**Configure Protocol Settings**」。
2. 在「Assertion Consumer Service URL」索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **POST**，Endpoint URL 為 `/api/saml-response`）。
3. 在 SLO 服務 URL 索引標籤上，接受預設值，這些預設值是從 StorageGRID SAML 中繼資料匯入的（Binding 為 **REDIRECT**， `/api/saml-logout`為端點 URL）。
4. 在「允許的 SAML 綁定」標籤中，清除 **ARTIFACT** 和 **SOAP**。只需 **POST** 和 **REDIRECT**。
5. 在「簽署原則」標籤上，保持選取「要求對驗證要求進行簽署」和「始終簽署判斷提示」核取方塊。
6. 在「加密原則」索引標籤上，選取 **None**。
7. 審查摘要並選取 **Done** 以儲存通訊協定設定。
8. 審查摘要並選擇「完成」以儲存瀏覽器 SSO 設定。

設定認證資料

步驟

1. 在 SP Connection 標籤中，選擇「憑證」。

2. ${post_edited_translations.segment}
3. 選擇您建立或匯入的 簽署憑證。
4. ${post_edited_translations.segment}
    a. 在「信任模型」標籤上，選擇 **Unanchored**。
    b. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以複製第一個 SP 連線，為網格中的每個管理節點建立所需的 SP 連線。每個複本都需要上傳新的中繼資料。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. 選擇 **Choose File** 並上傳中繼資料。
    c. 選擇 **Next** 。
    d. 選取 **Save** 。
4. ${post_edited_translations.segment}
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. ${post_edited_translations.segment}
    d. 選取 **Save** 。

停用 **StorageGRID** 中的 **SSO**

如果您不再需要此功能，可以停用單一登入 （SSO）。您必須先停用單一登入，然後才能停用身分識別聯盟。

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"。

步驟

1. 選擇 **Configuration** > **Access control** > **Single sign-on**。

    單一登入頁面隨即出現。

2. 選擇 停用單一登入。

3. ${post_edited_translations.segment}

   螢幕上出現警告訊息，指出本機使用者現在可以登入。

${post_edited_translations.segment}

暫時停用並重新啟用 **StorageGRID** 管理節點的 **SSO**

如果單一登入 （SSO） 系統故障，您可能無法登入 Grid Manager。在這種情況下，您可以暫時停用並重新啟用一個 Admin Node 的 SSO。若要停用並重新啟用 SSO，您必須存取該節點的命令 shell。

開始之前

- 您有"特定存取權限"。
- 您擁有 `Passwords.txt` 檔案。
- 您知道本機 root 使用者的密碼。

關於此任務

在您停用一個管理節點的 SSO 之後，您可以本機 root 使用者身分登入 Grid Manager。為了確保您的 StorageGRID 系統是安全的，您必須在登出後立即使用該節點的命令 shell 重新啟用管理節點上的 SSO。

> 停用單一 Admin Node 的 SSO 並不會影響網格中任何其他 Admin Node 的 SSO 設定。Grid Manager 中「單一登入」頁面上的「啟用 **SSO**」核取方塊仍會保持選取狀態，且所有現有的 SSO 設定都會保留，除非您對其進行更新。

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. 執行下列命令：`disable-saml`

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

4. 透過網頁瀏覽器，存取同一管理節點上的 Grid Manager。

   由於 SSO 已停用，現在將顯示 Grid Manager 登入頁面。

5. ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
   a. 選擇 **Configuration** > **Access control** > **Single sign-on**。
   b. ${post_edited_translations.segment}
   c. 選取 **Save** 。

      ${post_edited_translations.segment}

7. 如果您因為需要存取 Grid Manager 而暫時停用了 SSO：
   a. 執行您需要執行的任何工作。
   b. ${post_edited_translations.segment}
   c. 在 Admin 節點上重新啟用 SSO。您可以執行下列任一步驟：

      - 執行下列命令： `enable-saml`

        ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - 重啟網格節點： `reboot`
8. 透過網頁瀏覽器，從同一個管理節點存取 Grid Manager。
9. 確認 StorageGRID 登入頁面出現，且您必須輸入 SSO 憑證才能存取 Grid Manager。

使用網格聯邦

了解 **StorageGRID** 網格聯邦

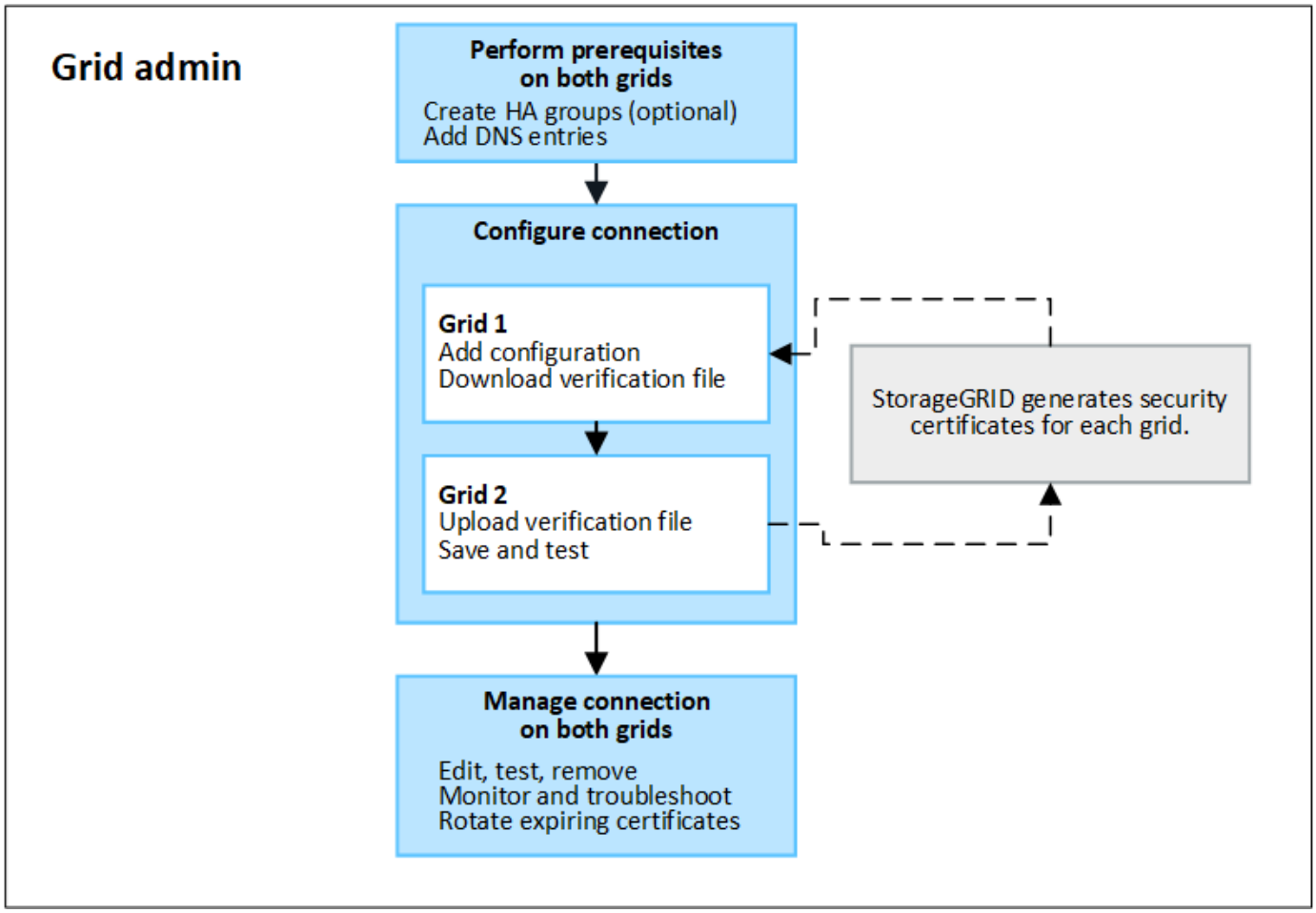
您可以使用網格聯合來 Clone 租戶，並在兩個 StorageGRID 系統之間複寫其物件，以實現災難恢復。

什麼是網格聯盟連線？

網格聯盟連線是兩個 StorageGRID 系統中 Admin 節點和 Gateway 節點之間的雙向、可信任且安全的連線。

網格聯盟工作流程

工作流程圖總結了在兩個網格之間設定網格聯邦連線的步驟。



網格聯邦連線的考量事項和需求

- 用於網格聯合的網格必須執行 StorageGRID 版本，這些版本必須完全相同，或彼此之間最多只有一個主要版本差異。

  有關版本要求的詳細資訊，請參閱 "版本資訊"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。

- 一個網格可以與其他網格建立一個或多個網格聯邦連接。每個網格聯邦連接都是獨立的，與其他連接互不影響。例如，如果 Grid 1 與 Grid 2 有一個連接，又與 Grid 3 有一個連接，那麼 Grid 2 和 Grid 3 之間並不存在隱含的連接。
- 網格聯盟連線是雙向的。連線建立後，您可以從任一網格監控和管理該連線。
- 必須至少存在一個網格同盟連線，才能使用 "帳戶 Clone" 或 "${post_edited_translations.segment}"。

網路和 **IP** 位址需求

- 網格聯盟連線可在網格網路、管理網路或用戶端網路上進行。
- 網格同盟連線可將一個網格連線至另一個網格。每個網格的組態都會指定另一個網格上的網格同盟端點，該端點由 Admin 節點、Gateway 節點或兩者組成。
- 最佳實務做法是連線每個網格上 Gateway 和 Admin 節點的 "高可用度 （HA） 群組"。使用 HA 群組有助於確保在節點變得無法使用時，網格同盟連線仍保持線上狀態。如果任一 HA 群組中的作用中介面故障，連線可以使用備份介面。

- 不建議建立使用單一 Admin 節點或 Gateway 節點 IP 位址的網格同盟連線。如果該節點變得無法使用，網格同盟連線也將變得無法使用。
- "跨網格複寫" 物件需要每個網格上的 Storage 節點能夠存取另一個網格上已設定的 Admin 和 Gateway 節點。對於每個網格，請確認所有 Storage 節點皆有高頻寬路由至用於連線的 Admin 節點或 Gateway 節點。

${post_edited_translations.segment}

在正式作業環境中，請使用完整網域名稱 (FQDN) 來識別連線中的每個網格。然後，如下建立對應的 DNS 項目：

- Grid 1 的 FQDN 會對應到 Grid 1 中 HA 群組的一個或多個虛擬 IP （VIP） 位址，或對應到 Grid 1 中一個或多個管理節點或閘道節點的 IP 位址。
- Grid 2 的 FQDN 會對應到 Grid 2 的一個或多個 VIP 位址，或對應到 Grid 2 中的一個或多個管理節點或閘道節點的 IP 位址。

${post_edited_translations.segment}

- 對應到多個 HA 群組 VIP 位址的 DNS 項目會在 HA 群組的作用中節點之間進行負載平衡。
- 對應至多個管理節點或閘道節點 IP 位址的 DNS 條目，會在對應的節點之間進行負載平衡。

連接埠需求

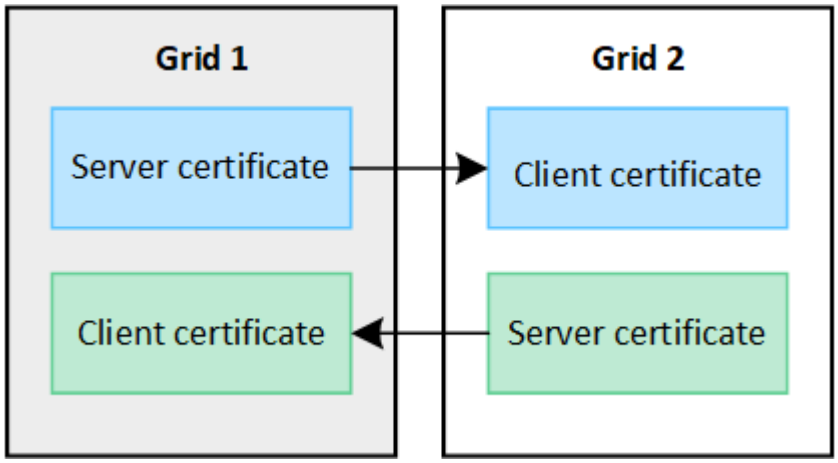
建立網格聯合連線時，您可以指定 23000 到 23999 之間的任何未使用的連接埠號碼。此連線中的兩個網格將使用相同的連接埠。

您必須確保兩個網格中的任何節點都沒有使用此連接埠進行其他連線。

憑證需求

設定網格聯合連線時，StorageGRID 會自動產生四個 SSL 憑證：

- 伺服器和用戶端憑證，用於驗證和加密從網格 1 傳送到網格 2 的資訊
- 伺服器和用戶端憑證用於驗證和加密從網格 2 傳送到網格 1 的資訊。



預設情況下，憑證有效期為 730 天（2 年）。當這些憑證接近到期日時，網格聯盟憑證到期 警示會提醒您輪換憑證，您可以使用 Grid Manager 執行此操作。

如果連接兩端的憑證過期，連線將停止運作。資料複寫將處於暫停狀態，直到憑證更新為止。

深入瞭解

- "建立網格聯盟連線"
- "管理網格同盟連線"
- "排除網格同盟錯誤"

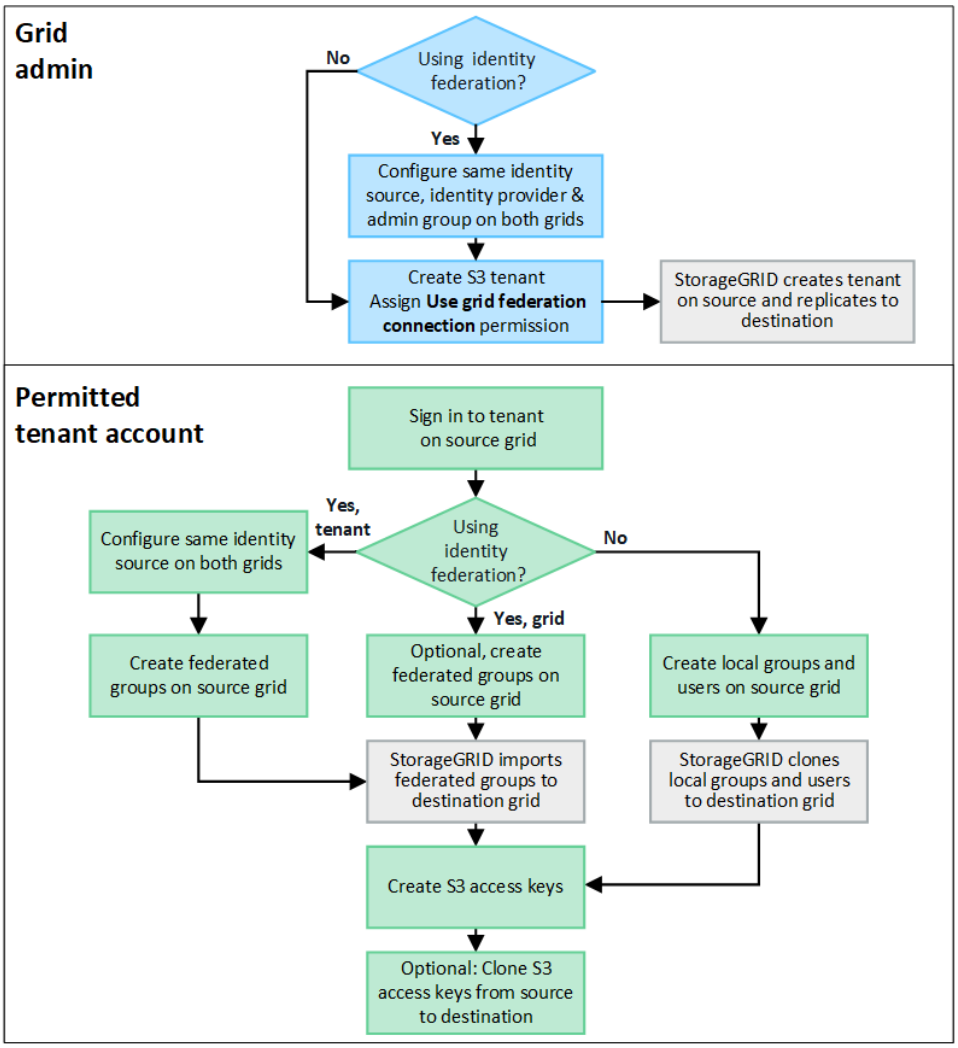
瞭解 StorageGRID 中的帳戶複製

帳戶 Clone 是指在 "網格聯盟連線" 中的 StorageGRID 系統之間自動複寫租戶帳戶、租戶群組、租戶使用者，以及 （選擇性） S3 存取金鑰。

需要為 "${post_edited_translations.segment}" 進行帳戶 Clone。將帳戶資訊從來源 StorageGRID 系統 Clone 至目的地 StorageGRID 系統，可確保租戶使用者和群組能夠存取任一網格上的對應儲存桶和物件。

帳戶 Clone 工作流程

工作流程圖顯示了網格系統管理員和允許的租戶設定帳戶 Clone 所將執行的步驟。這些步驟是在 "網格聯盟連線已設定" 之後執行。



${post_edited_translations.segment}

網格管理員執行的步驟取決於 "網格聯盟連線" 中的 StorageGRID 系統是否使用單一登入 （SSO） 或身分聯合。

${post_edited_translations.segment}

如果網格聯合連接中的任何一個 StorageGRID 系統使用 SSO，則兩個網格都必須使用 SSO。在為網格聯合建立租戶帳戶之前，租戶來源和目的地網格的網格系統管理員必須執行下列步驟。

步驟

1. 為兩個網格設定相同的身分識別來源。請參閱"${post_edited_translations.segment}"。
2. 為兩個網格設定相同的 SSO 身分識別供應商 (IdP)。請參閱"設定單一登入"。
3. "建立相同的管理員群組"在兩個網格上匯入相同的聯合群組。

   ${post_edited_translations.segment}

   ${post_edited_translations.segment}

為帳戶 **Clone** 設定網格層級身分識別聯盟（選用）

如果任一 StorageGRID 系統使用未啟用 SSO 的身分識別同盟，則兩個網格都必須使用身分識別同盟。在為網格同盟建立租戶帳戶之前，租戶來源和目的地網格的網格系統管理員必須執行這些步驟。

步驟

1. 為兩個網格設定相同的身分識別來源。請參閱"${post_edited_translations.segment}"。
2. 如果聯合群組對來源和目的地租戶帳戶都具有初始 Root 存取權限，則可以透過在兩個網格上匯入同一個聯合群組來"建立相同的管理員群組"實現此權限。

   如果將 Root 存取權限指派給兩個網格上都不存在的聯合群組，租戶不會複寫到目的地網格。

3. ${post_edited_translations.segment}

建立允許的 **S3** 租戶帳戶

在選擇性設定 SSO 或身分聯合之後，網格管理員執行下列步驟，以確定哪些租戶可以將儲存桶物件複寫到其他 StorageGRID 系統。

步驟

1. 決定要將哪個網格作為租戶帳戶 Clone 操作的來源網格。

   最初建立租戶的網格稱為租戶的_來源網格_。複寫租戶的網格稱為租戶的_目的地網格_。

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 如果租戶帳戶將管理自己的聯合使用者，則指派「使用自己的身分來源」權限。

   如果指派了此權限，則來源和目的地租戶帳戶必須先設定相同的身分來源，然後才能建立聯合群組。除非兩個網格使用相同的身分來源，否則新增至來源租戶的聯合群組無法 Clone 到目的地租戶。

5. 選擇特定的網格聯邦連線。
6. ${post_edited_translations.segment}

   當儲存具有「使用網格聯合連線」權限的新租戶時，StorageGRID 會自動在另一個網格上建立該租戶的複本，如下所示：

   - 兩個租戶帳戶具有相同的帳戶 ID、名稱、儲存設備配額和已指派的權限。
   - 如果您選擇了一個聯合群組，使其對租戶具有 Root 存取權限，則該群組將 Clone 至目的地租戶。
   - 如果您選擇某個本機使用者擁有租戶的 Root 存取權限，則該使用者將被 Clone 到目的地租戶。但是，該使用者的密碼不會被 Clone。

如需詳細資訊，請參閱 "管理網格聯邦的授權租戶"。

允許的租戶帳戶工作流程

將具有「使用網格聯合連線」權限的租戶複寫到目的地網格後，允許的租戶帳戶可以執行下列步驟來 Clone 租戶群組、使用者和 S3 存取金鑰。

步驟

1. 在租戶的來源網格上登入租戶帳戶。
2. 如果允許，請在來源租戶帳戶和目的地租戶帳戶上設定身分識別聯合。
3. ${post_edited_translations.segment}

   當在來源租戶上建立新群組或使用者時，StorageGRID 會自動將其 Clone 到目的地租戶，但不會從目的地 Clone 回來源。

4. 建立 S3 存取金鑰。
5. （可選）將來源租戶的 S3 存取金鑰 Clone 到目的地租戶。

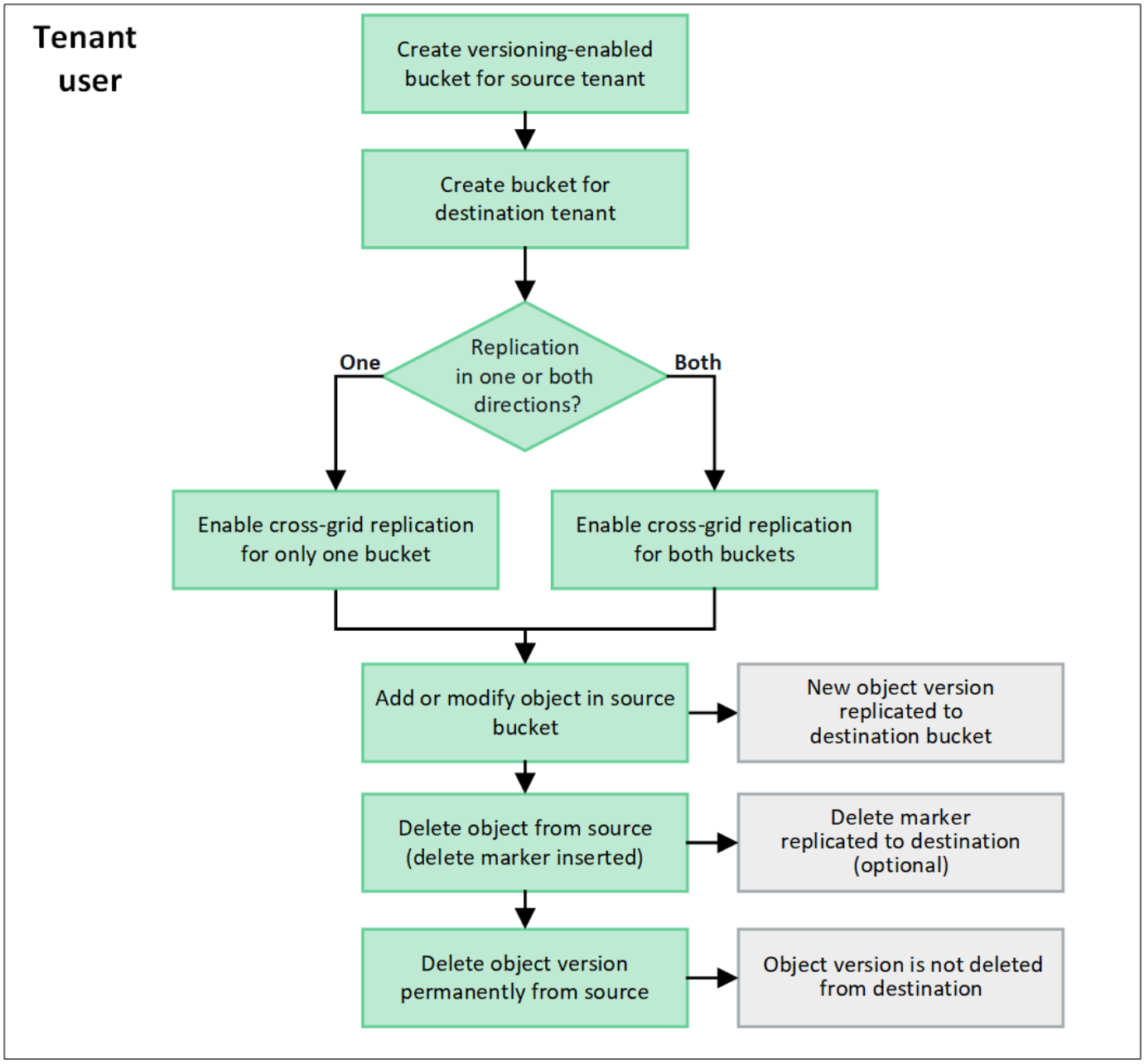
有關允許的租戶帳戶工作流程的詳細資訊，以及如何 Clone 群組、使用者和 S3 存取金鑰，請參閱 "Clone 租戶群組和使用者" 和 "使用 API Clone S3 存取金鑰"。

瞭解 StorageGRID 中的跨網格複寫

跨網格複寫是指在兩個以 "網格聯盟連線" 方式連接的 StorageGRID 系統中，在選定的 S3 儲存桶之間自動複寫物件。"帳戶 Clone" 是跨網格複寫的必要條件。

${post_edited_translations.segment}

${post_edited_translations.segment}



${post_edited_translations.segment}

如果租戶帳戶擁有*使用網格聯合連線*權限，可使用一或多個 "網格同盟連線"，則具有 Root 存取權限的租戶使用者可以在每個網格的對應租戶帳戶中建立儲存桶。這些儲存桶：

- 可以擁有彼此不同的名稱
- 可以有不同的區域
- 必須啟用版本控制
- ${post_edited_translations.segment}

建立完兩個儲存桶後，可以為其中一個或兩個儲存桶設定跨網格複寫。

深入瞭解

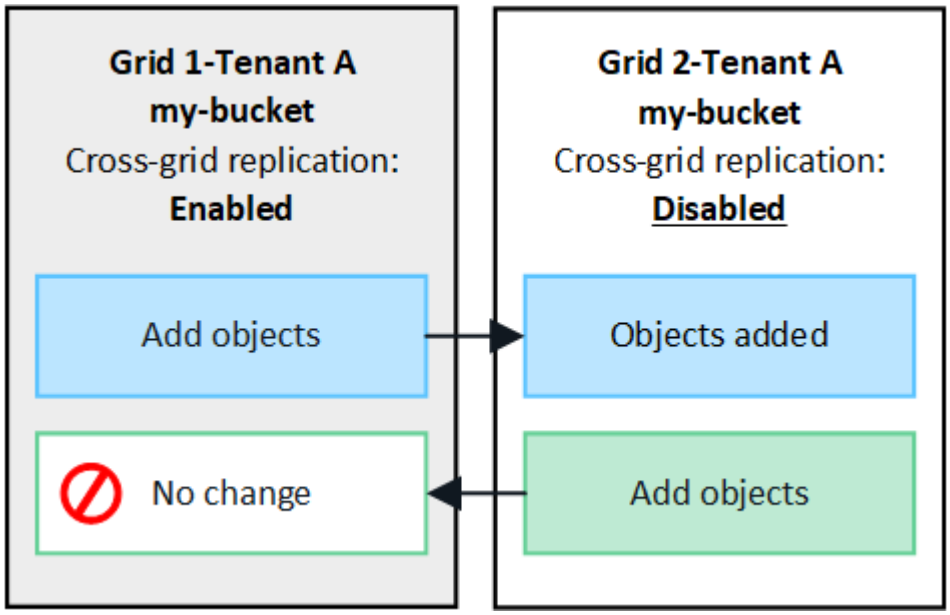
"管理跨網格複寫"

${post_edited_translations.segment}

您可以設定跨網格複寫以單向或雙向進行。

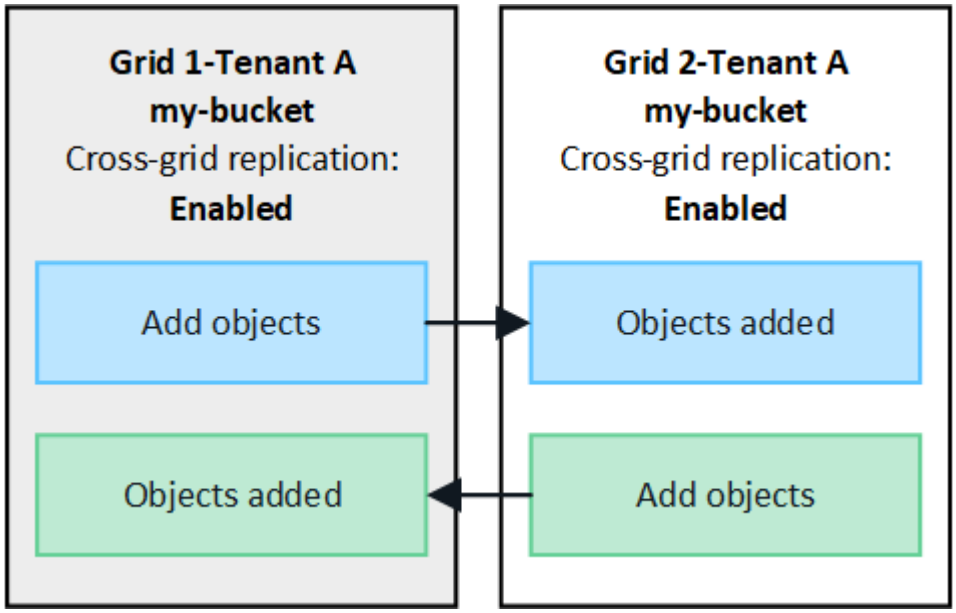
單向複寫

如果僅在一個網格上為某個儲存桶啟用跨網格複寫，則新增至該儲存桶（來源儲存桶）的物件會複寫到另一個網格上的對應儲存桶（目的地儲存桶）。但是，新增至目的地儲存桶的物件不會複寫回來源。如圖所示，已啟用從 Grid 1 到 Grid 2 的跨網格複寫 `my-bucket`，但未啟用反向複寫。



雙向複寫

如果您在兩個網格上為同一個貯體啟用跨網格複寫，則新增至任一貯體的物件都會複寫到另一個網格。在圖中，已針對雙向啟用跨網格複寫 `my-bucket`。



${post_edited_translations.segment}

當 S3 用戶端為已啟用跨網格複寫的儲存桶新增物件時，會發生下列情況：

1. StorageGRID 自動將物件從來源儲存桶複寫至目的地儲存桶。執行此背景複寫作業所需的時間取決於多種因素，包括待處理的其他複寫作業數量。

   S3 用戶端可以透過發出 GetObject 或 HeadObject 要求，來驗證物件的複寫狀態。回應中包含 StorageGRID 專用的 `x-ntap-sg-cgr-replication-status` 回應標頭，其值為下列其中之一：

${post_edited_translations.segment}	**${post_edited_translations.segment}**
來源	• 已完成：所有網格連線的複寫均已成功。 • **PENDING**：該物件尚未複寫至至少一個網格連線。 • **FAILURE**：所有網格連線的複寫作業均未擱置，且至少有一個連線發生永久故障。使用者必須解決此錯誤。
目的地	${post_edited_translations.segment}

   StorageGRID 不支援 `x-amz-replication-status` 標頭。

2. StorageGRID 使用每個網格的作用中 ILM 原則來管理物件，就像管理任何其他物件一樣。例如，網格 1 上的物件 A 可能儲存為兩個複寫複本並永久保留，而複寫到網格 2 的物件 A 複本可能使用 2+1 銷毀編碼儲存，並在三年後刪除。

${post_edited_translations.segment}

如前所述"刪除資料流"，StorageGRID 可以基於以下任何原因刪除物件：

- S3 用戶端發出刪除請求。
- Tenant Manager 使用者選取 "刪除儲存桶中的物件" 選項，以從儲存貯體中移除所有物件。
- 此儲存桶具有生命週期組態，會過期。
- ${post_edited_translations.segment}

當 StorageGRID 因為「刪除貯體中的物件」作業、貯體生命週期過期或 ILM 放置位置過期而刪除物件時，絕不會從網格同盟連線中的另一個網格刪除複寫的物件。不過，S3 用戶端刪除作業新增至來源貯體的刪除標記，可以選擇性地複寫到目的地貯體。

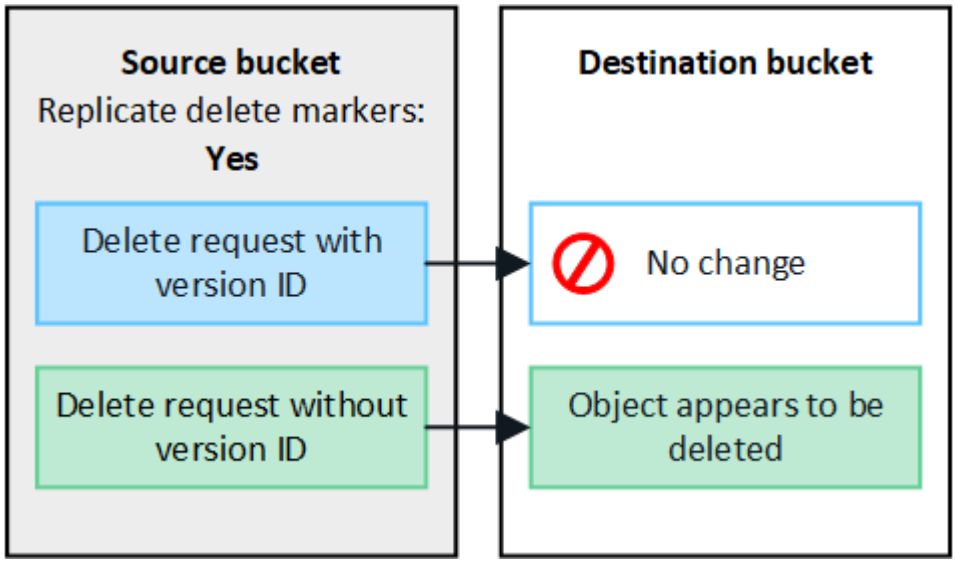
${post_edited_translations.segment}

- 如果 S3 用戶端發出包含版本 ID 的刪除要求，該版本的物件將會被永久移除。系統不會將刪除標記新增至儲存貯體。
- 如果 S3 用戶端發出不包含版本 ID 的刪除要求，StorageGRID 就不會刪除任何物件版本。相反地，它會在貯體中新增一個刪除標記。刪除標記會使 StorageGRID 表現得像是該物件已被刪除一樣：
  - 不含版本 ID 的 GetObject 請求會失敗，並顯示 `404 No Object Found`
  - 具有有效版本 ID 的 GetObject 要求會成功，並傳回要求的物件版本。

${post_edited_translations.segment}

- 如果刪除要求包含版本 ID，該物件版本將會從來源網格中永久移除。然而，StorageGRID 不會複寫包含版本 ID 的刪除要求，因此不會從目的地刪除相同的物件版本。
- ${post_edited_translations.segment}
  - 如果選擇複寫刪除標記（預設），則會在來源儲存桶中新增刪除標記，並將其複寫到目的地桶。實際上，該物件在兩個網格中都顯示為已刪除。
  - 如果您選擇不複寫刪除標記，則刪除標記會新增至來源儲存桶，但不會複寫到目的地儲存桶。實際上，在來源網格中刪除的物件不會在目的地網格中刪除。

在圖中，當 "已啟用跨網格複寫" 時，複寫刪除標記 被設定為 是。包含版本 ID 的來源儲存貯體刪除要求，不會刪除目的地儲存貯體中的物件。不包含版本 ID 的來源儲存貯體刪除要求，似乎會刪除目的地儲存貯體中的物件。



如果您想在網格之間保持物件刪除同步，請為兩個網格上的儲存貯體建立對應的 "S3 生命週期組態"。

加密物件如何複寫

當您使用跨網格複寫在網格之間複寫物件時，您可以加密個別物件、使用預設貯體加密，或設定整個網格的加密。您可以在為貯體啟用跨網格複寫之前或之後，新增、修改或移除預設貯體或整個網格的加密設定。

若要加密個別物件，您可以在將物件新增至來源貯體時，使用 SSE （使用 StorageGRID 管理的金鑰進行伺服器端加密）。請使用 `x-amz-server-side-encryption` 要求標頭，並指定 `AES256`。請參閱 "使用伺服器端加密"。

跨網格複寫不支援使用 SSE-C（使用客戶提供的金鑰進行伺服器端加密）。擷取操作將會失敗。

若要對儲存貯體使用預設加密，請使用 PutBucketEncryption 請求並將 `SSEAlgorithm`參數設為 `AES256`。儲存貯體層級加密適用於任何未包含 `x-amz-server-side-encryption`請求標頭的擷取物件。請參閱"儲存貯體上的作業"。

若要使用網格層級加密，請將 **Stored object encryption** 選項設定為 **AES-256**。網格層級加密適用於任何未在儲存貯體層級加密，或是在沒有 `x-amz-server-side-encryption` 要求標頭的情況下擷取的物件。請參閱 "

設定網路和物件選項"。

> SSE 不支援 AES-128。如果來源網格使用 **AES-128** 選項啟用了 儲存物件加密 選項，則 AES-128 演算法的使用不會傳播到複寫物件。相反，複寫物件將使用目的地預設的儲存桶或網格層級加密設定（如果可用）。

StorageGRID 在決定如何加密來源物件時，會套用下列規則：

1. 使用 `x-amz-server-side-encryption`擷取標頭（如果存在）。
2. 如果不存在擷取標頭，則使用儲存桶的預設加密設定（如果已設定）。
3. 如果未設定儲存桶設定，則使用網格範圍的加密設定（如果已設定）。
4. 如果沒有全網格設定，則不加密來源物件。

在決定如何加密複寫物件時，StorageGRID 會依照下列順序套用這些規則：

1. 使用與來源物件相同的加密，除非該物件使用 AES-128 加密。
2. 如果來源物件未加密或使用 AES-128，則使用目的地儲存桶的預設加密設定（如果已設定）。
3. 如果目的地儲存桶沒有加密設定，則使用目的地的網格範圍加密設定（如果已設定）。
4. ${post_edited_translations.segment}

使用 **S3** 物件鎖定進行跨網格複寫

在下列情況下，您可以設定已啟用 S3 物件鎖定的 StorageGRID 儲存區之間的跨網格複寫。

當來源儲存桶上的 **S3 Object Lock** 為……	目的地桶上的 **S3** 物件鎖定是……
已啟用	已啟用
已停用	已啟用

當來源儲存桶上的 S3 物件鎖定啟用時：

- 這些物件在目的地按以下順序設定了保留設定並進行鎖定：
  a. 來源物件的保留標頭值：

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. 來源儲存桶的預設保留（如果已設定）。
  c. 目的地儲存桶的預設保留（如果已設定）。

  目的地儲存桶的預設保留不會置換從來源物件複製的保留設定。
- 上傳物件時，您可以使用 `x-amz-object-lock-legal-hold`設定目的地物件的合法持有狀態。
- 如果目的地租戶或儲存桶不支援來源物件的 S3 物件鎖定設定，則會發生錯誤。請參閱"跨網格複寫警報和錯

誤。"

當來源儲存桶上的 S3 物件鎖定停用時：

- 您可以設定目的地貯體的預設保留，將 S3 物件鎖定保留設定套用至目的地物件。
- 目的地物件無法設定合法持有狀態。

PutObjectTagging 和 DeleteObjectTagging 不受支援

PutObjectTagging 和 DeleteObjectTagging 要求不支援已啟用跨網格複寫的儲存桶中的物件。

如果 S3 用戶端發出 PutObjectTagging 或 DeleteObjectTagging 請求，則會傳回 `501 Not Implemented`。訊息為 `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`。

PutObjectRetention 和 PutObjectLegalHold 不受支援

PutObjectRetention 和 PutObjectLegalHold 要求對於已啟用跨網格複寫的儲存桶中的物件，尚未完全支援。

如果 S3 用戶端發出 PutObjectRetention 或 PutObjectLegalHold 要求，則來源物件的設定會被修改，但變更不會套用到目的地。

分割物件如何複寫

來源網格的最大區段大小適用於複製到目的地網格的物件。當物件複製到另一個網格時，來源網格的「最大區段大小」設定（位於「組態」>「系統」>「儲存選項」）將套用於兩個網格。例如，假設來源網格的最大區段大小為 1 GB，而目的地網格的最大區段大小為 50 MB。如果您在來源網格上擷取 2 GB 的物件，則該物件將儲存為兩個 1 GB 的區段。即使目的地網格的最大區段大小為 50 MB，該物件也會以兩個 1 GB 的區段形式複製到目的地網格。

比較 StorageGRID 中的跨網格複寫和 CloudMirror 複寫

當您開始使用網格同盟時，請審查 "${post_edited_translations.segment}" 與 "StorageGRID CloudMirror 複寫服務" 之間的相似之處與差異。

您無法在透過跨網格複寫所複寫的儲存桶上使用 CloudMirror，反之亦然。

	跨網格複寫	**CloudMirror** 複寫服務
${post_edited_translations.segment}	一個 StorageGRID 系統可作為災難恢復系統。儲存貯體中的物件可以在網格之間進行單向或雙向複寫。	允許租戶自動將物件從 StorageGRID 中的儲存桶（來源）複寫到外部 S3 儲存桶（目的地）。 CloudMirror 複寫會在獨立的 S3 基礎架構中建立物件的獨立複本。此獨立複本不作為備份使用，但通常會在雲端中進行進一步處理。

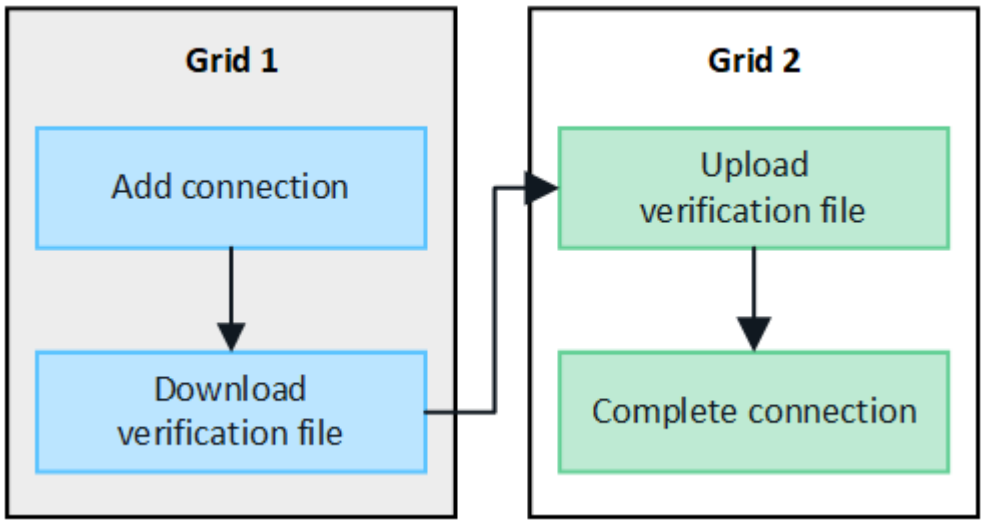
	跨網格複寫	**CloudMirror** 複寫服務
它是如何設定的？	1. ${post_edited_translations.segment} 2. ${post_edited_translations.segment} 3. ${post_edited_translations.segment} 4. ${post_edited_translations.segment}	1. 租戶使用者透過使用 Tenant Manager 或 S3 API 定義 CloudMirror 端點（IP 位址、認證資訊等）來設定 CloudMirror 複寫。 2. 該租戶帳戶所擁有的任何儲存貯器皆可設定為指向 CloudMirror 端點。
誰負責設定？	• ${post_edited_translations.segment} • ${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	在網格聯合連線中的另一個 StorageGRID 系統上，存在一個對應且相同的 S3 儲存桶。	• ${post_edited_translations.segment} • Google Cloud Platform (GCP)
是否需要物件版本控制？	${post_edited_translations.segment}	否， CloudMirror 複寫支援在來源和目的地兩端未啟用版本控制與已啟用版本控制之儲存貯體的任何組合。
是什麼原因導致物件移動至目的地？	${post_edited_translations.segment}	當物件新增至已設定 CloudMirror 端點的儲存桶時，系統會自動複寫這些物件。在儲存桶設定 CloudMirror 端點之前已存在於來源儲存桶中的物件，除非經過修改，否則不會被複寫。
物件如何複寫？	跨網格複寫會建立版本化物件，並將來源儲存桶中的版本 ID 複寫到目的地儲存桶。這樣可以確保兩個網格之間的版本順序保持一致。	CloudMirror 複寫不需要啟用版本控制的貯體，因此 CloudMirror 只能維護站台內金鑰的順序。無法保證對不同站台之物件的請求會維持順序。
如果物件無法複寫怎麼辦？	該物件已排入複寫佇列，受中繼資料儲存限制。	該物件已排入複寫佇列，受平台服務限制約束（請參閱"關於使用平台服務的建議"）。
物件的系統中繼資料是否已複寫？	是的，當物件複寫到另一個網格時，其系統中繼資料也會一併複寫。兩個網格上的中繼資料將完全相同。	不，當物件複寫到外部儲存桶時，其系統中繼資料會更新。中繼資料會因位置而異，取決於擷取時間和獨立 S3 基礎架構的行為。
如何擷取物件？	應用程式可以透過向任一網格上的儲存桶發出請求來擷取或讀取物件。	應用程式可以透過向 StorageGRID 或 S3 目的地發出請求來擷取或讀取物件。例如，假設您使用 CloudMirror 複寫將物件鏡射到合作夥伴組織。合作夥伴可以使用自己的應用程式直接從 S3 目的地讀取或更新物件。不需要使用 StorageGRID。

	跨網格複寫	CloudMirror 複寫服務
${post_edited_translations.segment}	• 包含版本 ID 的刪除請求永遠不會複寫到目的地網格。 • ${post_edited_translations.segment} • ${post_edited_translations.segment}	結果會因來源和目的地儲存桶的版本狀態而異（兩者不必相同）： • ${post_edited_translations.segment} • 如果只有來源儲存桶已啟用版本控制，刪除請求將會在來源中新增刪除標記，但不會新增至目的地。 • 如果兩個儲存桶都沒有版本控制，則刪除請求將從來源中刪除物件，但不會從目的地中刪除物件。 同樣，可以刪除目的地儲存貯體中的物件，而不會影響來源。

建立 StorageGRID 網格聯合連線

如果要 Clone 租戶詳細資料並複寫物件資料，可以在兩個 StorageGRID 系統之間建立網格聯合連線。

如圖所示，建立網格聯邦連接需要在兩個網格上分別執行步驟。您需要在一個網格上新增連接，然後在另一個網格上完成連接。您可以從任一網格開始操作。



開始之前

- 您已檢閱設定網格聯合連線的"${post_edited_translations.segment}"。
- 如果您打算為每個網格使用完整網域名稱 (FQDN) 而不是 IP 或 VIP 位址，您就知道要使用哪些名稱，並且您已確認每個網格的 DNS 伺服器都有適當的項目。
- 您正在使用一個"支援的網頁瀏覽器"。
- ${post_edited_translations.segment}

新增連線

在兩個 StorageGRID 系統中的任一個上執行這些步驟。

步驟

1. 從任一網格上的主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選擇 **Add connection**。
4. ${post_edited_translations.segment}

欄位	說明
連線名稱	一個獨特的名稱，幫助您識別此連線，例如「Grid 1-Grid 2」。
${post_edited_translations.segment}	${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment} • 此網格上管理節點或閘道節點的 IP 位址。該 IP 可以位於目的地網格可到達的任何網路上。
連接埠	您要用於此連線的連接埠。您可以輸入 23000 到 23999 之間的任何未使用連接埠號碼。 此連線中的兩個網格都將使用相同的連接埠。您必須確保任一網格中的任何節點都不會將此連接埠用於其他連線。
${post_edited_translations.segment}	此連接中該網格的安全性憑證有效天數。預設值為 730 天（2 年），但您可以輸入 1 到 762 天之間的任何值。 ${post_edited_translations.segment}
${post_edited_translations.segment}	您目前登入的網格的佈建密碼。
另一個網格的 FQDN 或 IP 位址	${post_edited_translations.segment} • ${post_edited_translations.segment} • 另一個網格上 HA 群組的 VIP 位址 • 另一個網格上管理節點或閘道節點的 IP 位址。此 IP 可以位於來源網格可連達的任何網路上。

5. 選擇 **Save and continue**。
6. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

7. 找出下載的檔案 (*connection-name*.grid-federation)，並將其儲存到安全的位置。

   此檔案包含機密（遮罩為 *）與其他敏感詳細資訊，且必須安全地儲存與傳輸。

8. 選擇 **Close** 以返回 Grid federation 頁面。
9. ${post_edited_translations.segment}
10. 將 `*connection-name*.grid-federation`檔案提供給另一個網格的網格管理員。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 從主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選擇 **Upload verification file** 以存取上傳頁面。
4. 選取 上傳驗證檔案。然後，瀏覽並選取從第一個網格下載的檔案 (*connection-name*.grid-federation) 。

   ${post_edited_translations.segment}

5. 您也可以為該網格的安全性憑證輸入不同的有效天數。*憑證有效天數*項目預設為您在第一個網格中輸入的值，但每個網格可以使用不同的到期日。

   一般來說，連接兩端的憑證有效期限應相同。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}

   憑證已產生，且連線已測試。如果連線有效，則會顯示成功訊息，且新連線將列在網格聯盟頁面上。連線狀態 將顯示為 已連線。

   如果出現錯誤訊息，請解決任何問題。參見"排除網格同盟錯誤"。

8. 前往第一個網格上的網格同盟頁面，然後重新整理瀏覽器。確認「連線狀態」目前為「已連線」。
9. ${post_edited_translations.segment}

   如果您編輯此連線，系統將建立一個新的驗證檔案。原始檔案將無法重複使用。

完成後

- 檢視以下方面的考量事項"${post_edited_translations.segment}"。
- "建立一個或多個新的租戶帳戶"，指派 使用網格同盟連線 權限，並選取新的連線。
- "管理連線"（視需要）。您可以編輯連線值、測試連線、輪換連線憑證或移除連線。
- "監控連線"作為您日常 StorageGRID 監控活動的一部分。

- "排查連線故障"，包括解決與帳戶 Clone 和跨網格複寫相關的任何警報和錯誤。

管理 StorageGRID 網格聯合連線

管理 StorageGRID 系統之間的網格聯合連線包括編輯連線詳細資料、輪替憑證、移除租戶權限和移除未使用的連線。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入任一網格上的 Grid Manager。
- 您擁有"${post_edited_translations.segment}"您目前登入的網格的權限。

編輯網格同盟連線

您可以透過登入連線中任一網格的主要管理節點來編輯網格聯盟連線。在對第一個網格進行變更後，您必須下載新的驗證檔案並將其上傳到另一個網格。

> 在編輯連線期間，帳戶 Clone 或跨網格複寫請求將繼續使用現有的連線設定。您對第一個網格所做的任何編輯都會儲存在本機，但只有在上傳到第二個網格、儲存並測試後才會生效。

開始編輯連線

步驟

1. 從任一網格上的主要管理節點登入 Grid Manager。
2. 選擇 **Nodes** ，並確認系統中所有其他管理節點已線上。

> 編輯網格聯合連線時，StorageGRID 會嘗試在第一個網格的所有管理節點上儲存一個「候選組態」檔案。如果該檔案無法儲存到所有管理節點，則在選擇 **Save and test** 時會顯示警告訊息。

3. 選擇 **Configuration** > **System** > **Grid federation**。
4. 使用網格聯盟頁面上的 **Actions** 功能表或特定連線的詳細資訊頁面編輯連線詳細資訊。請參閱 "建立網格聯盟連線" 以了解需要輸入的內容。

操作選單

a. 選取連線的選項按鈕。
b. 選取 **Actions** > **Edit**。
c. 輸入新資訊。

詳細資料頁面

a. ${post_edited_translations.segment}
b. ${post_edited_translations.segment}
c. 輸入新資訊。

5. 請輸入您目前登入的網格佈建密碼。

6. 選擇 **Save and continue**。

   新值已儲存，但只有在您將新的驗證檔案上傳到另一個網格後，這些新值才會套用到連線中。

7. 選擇 **Download verification file**。

   ${post_edited_translations.segment}

8. 找出下載的檔案 (*connection-name*.grid-federation)，並將其儲存到安全的位置。

   驗證檔案包含機密資訊，必須安全地儲存和傳輸。

9. 選擇 **Close** 以返回 Grid federation 頁面。
10. 確認*連線狀態*為*待編輯*。

    如果在開始編輯連線時連線狀態不是 **Connected**，則不會變成 **Pending edit**。

11. 將 `*connection-name*.grid-federation`檔案提供給另一個網格的網格管理員。

完成連線編輯

在另一個網格上傳驗證檔案，完成連線編輯。

步驟

1. 從主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選擇 **Upload verification file** 以存取上傳頁面。
4. 選擇 **Upload verification file**。然後，瀏覽並選擇從第一個網格下載的檔案。
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

   如果使用修改後的值可以建立連線，則會顯示成功訊息。否則，會顯示錯誤訊息。請查看訊息並解決任何問題。

7. 關閉精靈以返回網格聯盟頁面。
8. 確認*連線狀態*為*已連線*。
9. 前往第一個網格上的網格同盟頁面，然後重新整理瀏覽器。確認「連線狀態」目前為「已連線」。
10. ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 從主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 使用網格同盟頁面上的 **Actions** 功能表或特定連線的詳細資訊頁面測試連線。

操作選單

a. 選取連線的選項按鈕。

b. 選擇 **Actions** > **Test**。

詳細資料頁面

a. ${post_edited_translations.segment}

b. 選擇 **Test connection**。

4. 查看連線狀態：

連線狀態	說明
已連接	兩個網格均已連接並正常通訊。
錯誤	連線處於錯誤狀態。例如，憑證已過期或組態值已失效。
待編輯	您已編輯此網格上的連線，但該連線仍在使用現有的組態。若要完成編輯，請將新的驗證檔案上傳至另一個網格。
${post_edited_translations.segment}	您已在此網格上設定連線，但另一個網格上的連線尚未完成。請從此網格下載驗證檔案，並將其上傳至另一個網格。
未知	${post_edited_translations.segment}

5. 如果連線狀態為 **Error**，請解決任何問題。然後，再次選取 **Test connection** 以確認問題已解決。

輪替連線憑證

每個網格聯盟連線都使用四個自動產生的 SSL 憑證來保護連線安全。當每個網格的兩個憑證即將到期時、網格聯盟憑證到期 警示會提醒您輪換憑證。

${post_edited_translations.segment}

步驟

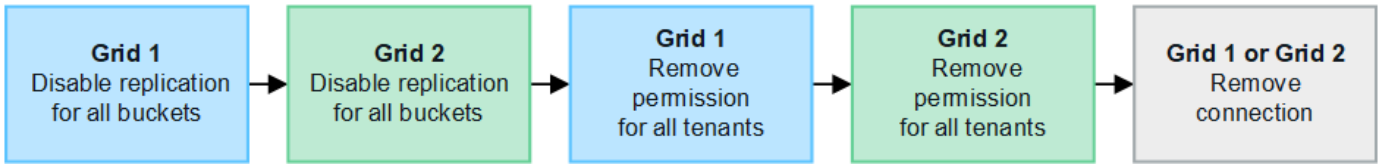
1. 從任一網格上的主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. ${post_edited_translations.segment}
4. 選取 **Certificates** 索引標籤。
5. 選取 **Rotate certificates**。
6. 請指定新憑證的有效天數。
7. 請輸入您目前登入的網格佈建密碼。
8. 選取 **Rotate certificates**。

9. ${post_edited_translations.segment}

   一般來說，連接兩端的憑證有效期限應相同。

移除網格同盟連線

您可以從連線中的任一網格移除網格聯合連線。如圖所示，您必須在兩個網格上執行先決條件步驟，以確認該連線未被任一網格上的任何租戶使用。



${post_edited_translations.segment}

- 移除連接不會刪除網格之間已複製的任何項目。例如，當租戶的權限被移除時，兩個網格中都存在的租戶使用者、群組和物件不會從任何一個網格中刪除。如果您想要刪除這些項目，則必須手動從兩個網格中刪除它們。
- 移除連線時，任何正在等待複寫的物件（已攝取但尚未複寫到另一個網格）的複寫都會永久失敗。

停用所有租戶儲存桶的複寫

步驟

1. ${post_edited_translations.segment}
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選取連線名稱以顯示其詳細資訊。
4. ${post_edited_translations.segment}
5. 如果列出了任何租戶，請指示所有租戶"停用跨網格複寫"在連線的兩個網格上為其所有儲存桶進行操作。

> 如果任何租戶儲存桶啟用了跨網格複寫，則無法移除「使用網格聯合連線」權限。每個租戶帳戶都必須在兩個網格上為其儲存桶停用跨網格複寫。

移除每個租戶的權限

在所有租戶儲存桶中停用跨網格複寫後，從兩個網格上的所有租戶中移除 **Use grid federation permission** 。

步驟

1. 選擇 **Configuration** > **System** > **Grid federation**。
2. 選取連線名稱以顯示其詳細資訊。
3. 在「允許的租戶」索引標籤中，移除每個租戶的「使用網格聯合連線」權限。請參閱"${post_edited_translations.segment}"。
4. 對另一個網格上的允許租戶重複這些步驟。

移除連線

步驟

1. 當兩個網格上都沒有租戶使用該連線時，選取 **Remove**。
2. 查看確認訊息，然後選擇 移除。
   - 如果連線可以移除，則會顯示成功訊息。網格同盟連線現已從兩個網格中移除。
   - 如果無法移除連線（例如，連線仍在使用中或發生連線錯誤），則會顯示錯誤訊息。您可以執行下列操作之一：
     - 解決此錯誤（建議）。參見"排除網格同盟錯誤"。
     - 強制移除連線。請參閱下一節。

強制移除網格同盟連線

如有必要，您可以強制移除狀態不是「已連線」的連線。

強制移除只會從本機網格中刪除連線。若要徹底移除連線，請在兩個網格上執行相同的步驟。

步驟

1. 在確認對話方塊中，選取 * 強制移除 *。

   顯示成功訊息。此網格聯合連線將不再可用。但是，租戶儲存區可能仍已啟用跨網格複寫，且某些物件複本可能已在連線中的網格之間複寫。

2. 從連線中的另一個網格，從主要管理節點登入 Grid Manager。
3. 選擇 **Configuration** > **System** > **Grid federation**。
4. 選取連線名稱以顯示其詳細資訊。
5. 選擇 **Remove** 和 **Yes**。
6. 選擇 **Force remove** 以從此網格中移除連線。

管理 StorageGRID 網格聯盟的允許租戶

您可以允許 S3 租戶帳戶使用兩個 StorageGRID 系統之間的網格聯合連線。如果允許租戶使用連線，則需要執行特殊步驟才能編輯租戶詳細資料或永久移除租戶使用該連線的權限。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入任一網格上的 Grid Manager。
- 您擁有"${post_edited_translations.segment}"您目前登入的網格的權限。
- 您位於"建立網格聯盟連線"兩個網格之間。
- 您已檢閱 "帳戶 Clone" 與 "${post_edited_translations.segment}" 的工作流程。
- 根據需求，您已為連線中的兩個網格設定單一登入（SSO）或身分識別同盟。請參閱 "什麼是帳戶 Clone"。

建立允許的租戶

如果您希望允許新的或現有的租戶帳戶使用網格聯合連線進行帳戶 Clone 和跨網格複寫，請按照一般說明 "${post_edited_translations.segment}" 或 "${post_edited_translations.segment}"，並注意以下事項：

- 您可以從連線中的任一網格建立租戶。建立租戶的網格稱為該租戶的來源網格。
- 連線狀態必須為「已連線」。
- 當在第一個網格中建立或編輯租戶以啟用 **Use grid federation connection** 權限並儲存後，相同的租戶會自動複寫到另一個網格。租戶複寫至的網格即為該租戶的_目的地網格_。
- 兩個網格上的租戶將具有相同的 20 位數帳戶 ID、名稱、執行摘要、配額和權限。您也可以選擇使用「執行摘要」欄位來協助識別哪個是來源租戶，哪一個是目的地租戶。例如，在網格 1 上建立的租戶的執行摘要也會顯示在複製到網格 2 的租戶中："此租戶是在網格 1 上建立的。"
- 基於安全性考量，本機 root 使用者的密碼不會複製到目的地網格。

  在本機 root 使用者可以登入目的地網格上的複寫租戶之前，該網格的網格系統管理員必須 "更改本機 root 使用者的密碼"。

- 在新租戶或編輯後的租戶同時出現在兩個網格中之後，租戶使用者可以執行以下操作：
  - 從租戶的來源網格建立群組和本地使用者，這些群組和使用者會自動 Clone 到租戶的目的地網格。請參閱 "Clone 租戶群組和使用者"。
  - 建立新的 S3 存取金鑰，其可選擇性地 Clone 到租戶的目的地網格。請參閱 "使用 API Clone S3 存取金鑰"。
  - 在連線中的兩個網格上建立相同的儲存貯體，並啟用單向或雙向的跨網格複寫。請參閱 "管理跨網格複寫"。

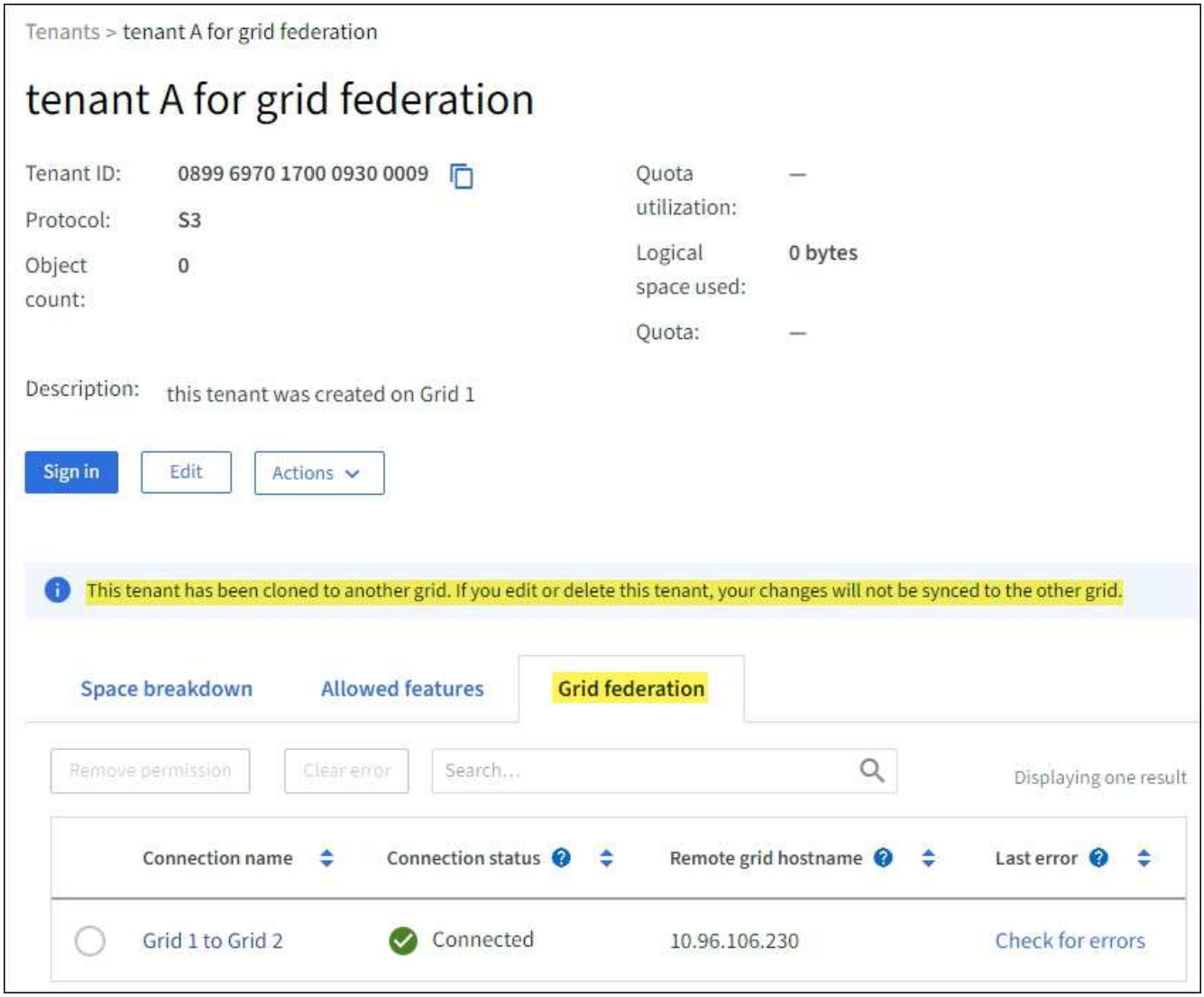
檢視獲准租戶

${post_edited_translations.segment}

步驟

1. 選擇*租戶*。
2. 在「租戶」頁面中，選擇租戶名稱以檢視租戶詳細資料頁面。

   如果這是租戶的來源網格（即，如果租戶是在此網格上建立的），則會顯示橫幅，提醒您該租戶已 Clone 到另一個網格。如果您編輯或刪除此租戶，您的變更將不會同步到另一個網格。



3. （可選）選擇 **Grid federation** 索引標籤以 "${post_edited_translations.segment}"。

編輯已獲許可的租戶

如果您需要編輯具有 使用網格同盟連線 權限的租戶，請遵循 "${post_edited_translations.segment}" 的一般說明，並注意以下事項：

- 如果租戶具有 **Use grid federation connection** 權限，您可以從連線中的任一網格編輯租戶詳細資料。然而，您所做的任何變更將不會複製到另一個網格。如果您想在網格之間保持租戶詳細資料同步，則必須在兩個網格上進行相同的編輯。
- 編輯租戶時，無法清除「使用網格聯合連線」權限。
- ${post_edited_translations.segment}

刪除已獲許可的租戶

如果您需要移除擁有「使用網格聯合連線」權限的租戶，請按照一般說明操作 "${post_edited_translations.segment}"，並附註以下事項：

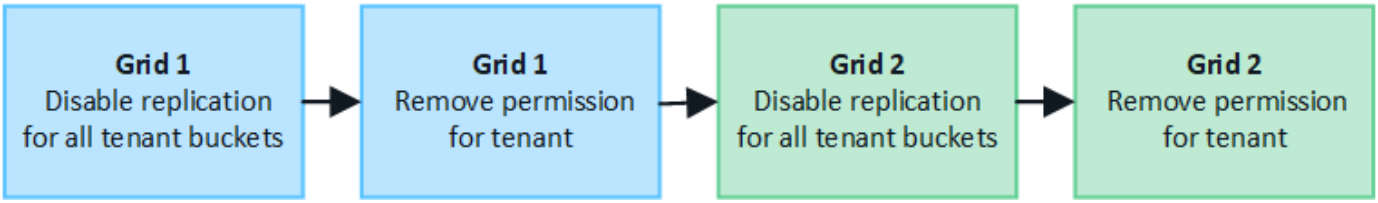
- 在移除來源網格上的原始租戶之前，必須先移除來源網格上該帳戶的所有儲存桶。

- 在目的地網格上移除 Clone 租戶之前，必須先移除目的地網格上該帳戶的所有儲存桶。
- 如果移除原始租戶或 Clone 租戶，則帳戶將無法再用於跨網格複寫。
- 如果您要移除來源網格上的原始租戶，則複製到目的地網格的任何租戶群組、使用者或金鑰將不受影響。您可以刪除複製的租戶，或允許其管理自己的群組、使用者、存取金鑰和貯體。
- ${post_edited_translations.segment}

  為避免這些錯誤，請在從該網格中刪除租戶之前，移除租戶使用網格同盟連線的權限。

${post_edited_translations.segment}

若要防止租戶使用網格同盟連線，您必須移除「使用網格同盟連線」權限。



在移除租戶使用網格聯合連線的權限之前，請注意以下事項：

- 如果租戶的任何儲存桶已啟用跨網格複寫，則無法移除 **Use grid federation connection** 權限。租戶帳戶必須先為其所有儲存桶停用跨網格複寫。
- 移除「使用網格同盟連線」權限不會刪除已在網格之間複寫的任何項目。例如，當移除租戶的權限時，存在於兩個網格上的任何租戶使用者、群組和物件都不會從任何一個網格中刪除。如果您想要刪除這些項目，您必須手動從兩個網格中將其刪除。
- ${post_edited_translations.segment}

> 重新啟用「使用網格同盟連線」權限後，本機網格將成為來源網格，並觸發 Clone 至所選網格同盟連線指定的遠端網格。如果租戶帳戶已存在於遠端網格中，則 Clone 將導致衝突錯誤。

開始之前

- 您正在使用一個"支援的網頁瀏覽器"。
- 您已擁有兩個網格的 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選取連線名稱以顯示其詳細資訊。
4. 在「允許的租戶」標籤上，確定租戶是否正在使用該連線。
5. 如果列出了該租戶，請指示他們針對連線中兩個網格上的所有貯體"停用跨網格複寫"。

如果任何租戶儲存桶已啟用跨網格複寫，則無法移除「使用網格聯合連線」權限。租戶必須在兩個網格上停用其儲存桶的跨網格複寫。

移除租戶權限

停用租戶儲存桶的跨網格複寫後，您可以移除租戶使用網格聯合連線的權限。

步驟

1. 從主要管理節點登入 Grid Manager。
2. ${post_edited_translations.segment}

${post_edited_translations.segment}

a. 選擇 **Configuration** > **System** > **Grid federation**。

b. 選取連線名稱以顯示其詳細資訊頁面。

c. 在「允許的租戶」索引標籤上，選取租戶的選項按鈕。

d. 選擇 移除權限。

租戶頁面

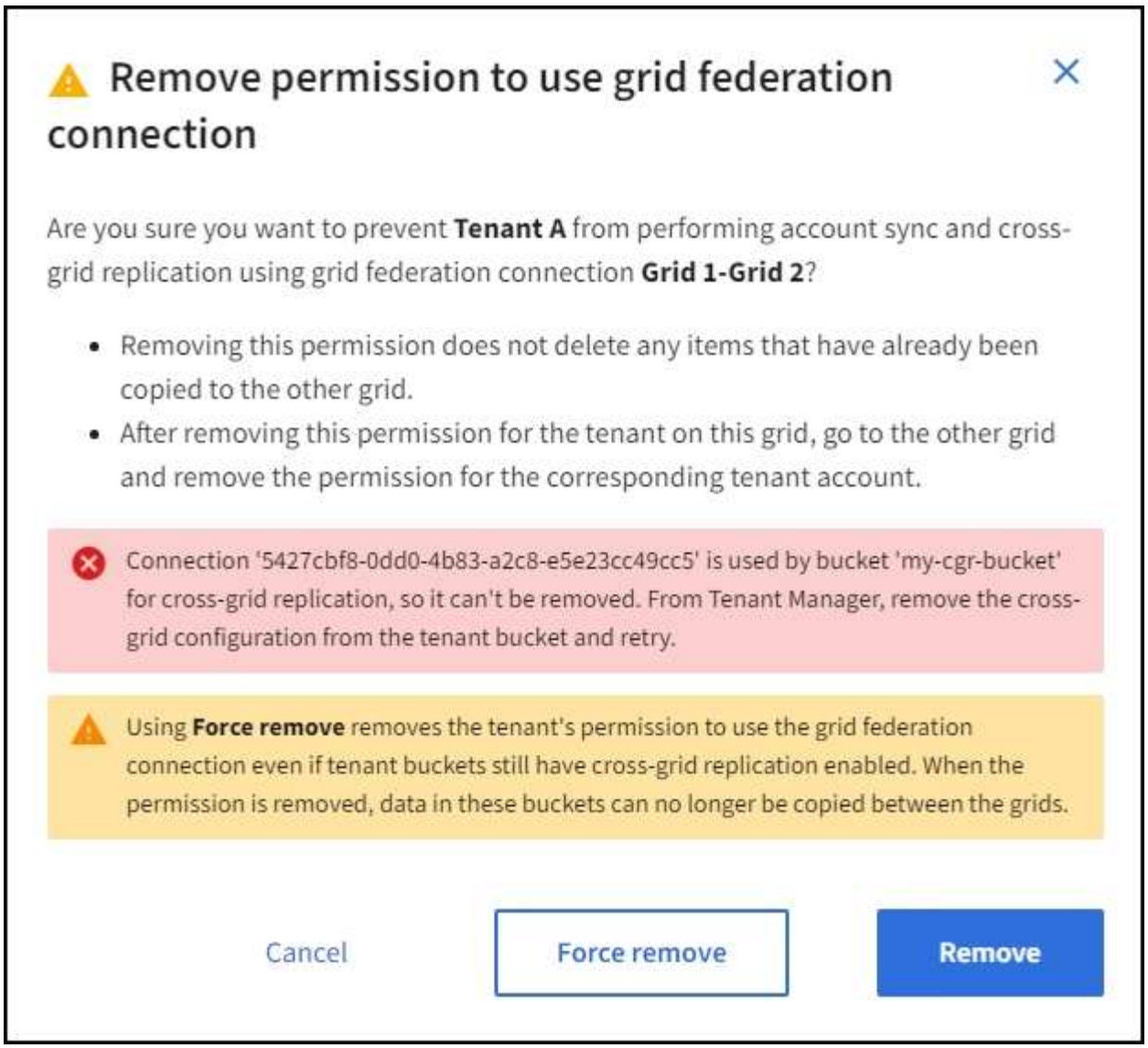
a. 選擇*租戶*。

b. 選取租戶名稱以顯示詳細資訊頁面。

c. 在「網格聯盟」索引標籤上，選取連線的選項按鈕。

d. 選擇 移除權限。

3. 查看確認對話方塊中的警告，然後選擇 移除。
   - 如果可以移除該權限，您將返回詳細資訊頁面並顯示成功訊息。此租戶將無法再使用網格聯合連線。
   - ${post_edited_translations.segment}



${post_edited_translations.segment}

- （建議。）登入 Tenant Manager，停用每個租戶儲存桶的複寫。請參閱 "管理跨網格複寫"。然後，重複上述步驟以移除 **Use grid connection** 權限。
- 強制移除權限。請參閱下一節。

4. ${post_edited_translations.segment}

強制移除權限

${post_edited_translations.segment}

在強制移除租戶的權限之前，請注意 移除權限 的一般注意事項，以及以下其他注意事項：

- 如果您強制移除 **Use grid federation connection**（使用網格同盟連線）權限，則任何擱置複寫至另一個網格的物件（已擷取但尚未複寫）將會繼續進行複寫。若要防止這些處理中的物件到達目的地 bucket，您也必須在另一個網格上移除該租戶的權限。
- 移除*使用網格聯合連線*權限後，任何擷取至來源儲存區的物件都不會複寫至目的地儲存區。

步驟

1. 從主要管理節點登入 Grid Manager。
2. 選擇 **Configuration** > **System** > **Grid federation**。
3. 選取連線名稱以顯示其詳細資訊頁面。
4. 在「允許的租戶」索引標籤上，選取租戶的選項按鈕。
5. 選擇 移除權限。
6. ${post_edited_translations.segment}

   系統會顯示成功訊息。此租戶將無法再使用網格同盟連線。

7. 視需要前往另一個網格，並重複這些步驟，以強制移除另一個網格上相同租戶帳戶的權限。例如，您應該在另一個網格上重複這些步驟，以防止處理中的物件到達目的地貯體。

排查 StorageGRID 中的網格聯合錯誤

您可能需要疑難排解與網格聯合連線、帳戶 Clone 和跨網格複寫相關的警示和錯誤。

網格同盟連線警示與錯誤

您的網格聯盟連線可能會收到警報或發生錯誤。

在對連線問題進行任何變更後，請測試連線以確保連線狀態恢復為 **Connected**。如需相關指示，請參閱"管理網格同盟連線"。

${post_edited_translations.segment}

問題

已觸發「網格聯盟連線故障」警報。

詳細資料

此警報表示網格之間的網格同盟連線出現故障。

建議採取的措施

1. 檢查兩個網格的「網格聯合」頁面上的設定。確認所有數值均正確。參見"管理網格同盟連線"。
2. 檢閱用於連線的憑證。確保沒有過期的網格聯盟憑證警示，且每個憑證的詳細資訊均有效。請參閱 "管理網格同盟連線" 中有關輪換連線憑證的說明。
3. 確認兩個網格中的所有管理節點和 Gateway 節點均已線上並可用。解決可能影響這些節點的任何警報，然後重試。
4. 如果您為本機或遠端網格提供了完整網域名稱 （FQDN），請確認 DNS 伺服器為線上且可用。請參閱 "什麼是網格聯邦？" 以了解連網、IP 位址和 DNS 需求。

網格聯盟憑證到期警示

問題

${post_edited_translations.segment}

詳細資料

此警報表示一個或多個網格聯盟憑證即將過期。

建議採取的措施

請參閱 "管理網格同盟連線" 中輪換連線憑證的說明。

編輯網格同盟連線時發生錯誤

問題

${post_edited_translations.segment}

詳細資料

編輯網格聯合連線時，StorageGRID 會嘗試在第一個網格的所有管理節點上儲存「候選組態」檔案。如果無法將此檔案儲存到所有管理節點（例如，由於某個管理節點離線），則會顯示警告訊息。

建議採取的措施

1. 在用於編輯連線的網格中，選取 **Nodes**。
2. 確認該網格的所有管理節點均已線上。
3. 如果任何節點離線，請將其重新上線，然後再次嘗試編輯連線。

帳戶 **Clone** 錯誤

無法登入 **Clone** 的租戶帳戶

問題

您無法登入 Clone 的租戶帳戶。Tenant Manager 登入頁面上的錯誤訊息為「您此帳戶的認證資訊無效。請重試。」

詳細資料

基於安全性考量，將租戶帳戶從租戶的來源網格 Clone 到租戶的目的地網格時，您為租戶本機 root 使用者設定的密碼不會被 Clone。同樣地，當租戶在其來源網格上建立本機使用者時，本機使用者密碼不會被 Clone 到目的地網格。

建議採取的措施

在 root 使用者能夠登入租戶的目的地網格之前，網格系統管理員必須先在目的地網格上 "更改本機 root 使用者的密碼"。

在 Clone 的本機使用者能夠登入租戶的目的地網格之前，Clone 租戶的 root 使用者必須為目的地網格上的該使用者新增密碼。如需相關指示，請參閱 Tenant Manager 使用說明中的"管理使用者"。

建立租戶時未使用 **Clone**

問題

${post_edited_translations.segment}

詳細資料

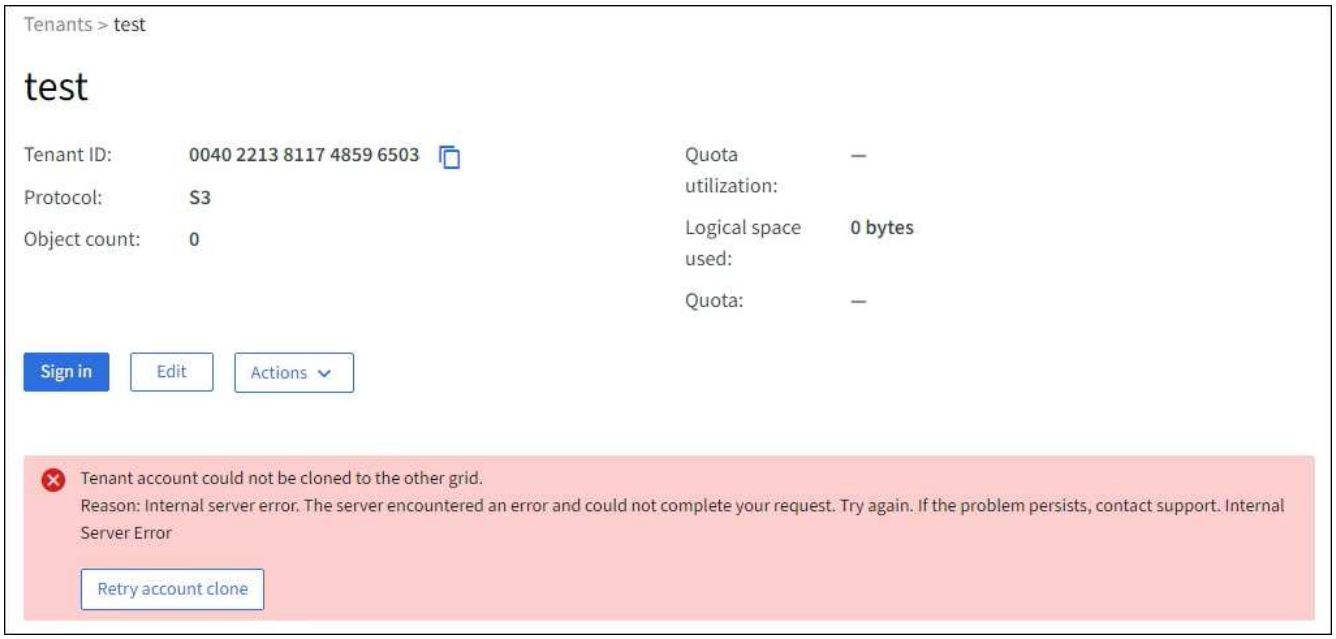
如果連線狀態的更新延遲，則可能會出現此問題，這可能會導致不正常的連線被列為 **Connected**。

建議採取的措施

1. 查看錯誤訊息中列出的原因，並解決可能導致連線失敗的任何連網或其他問題。參見網格聯盟連接警報和錯

誤。

2. 按照說明測試 "管理網格同盟連線" 中的網格聯盟連線，以確認問題已解決。
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. 選擇租戶名稱以顯示詳細資訊頁面。
6. 選擇 **Retry account clone**。



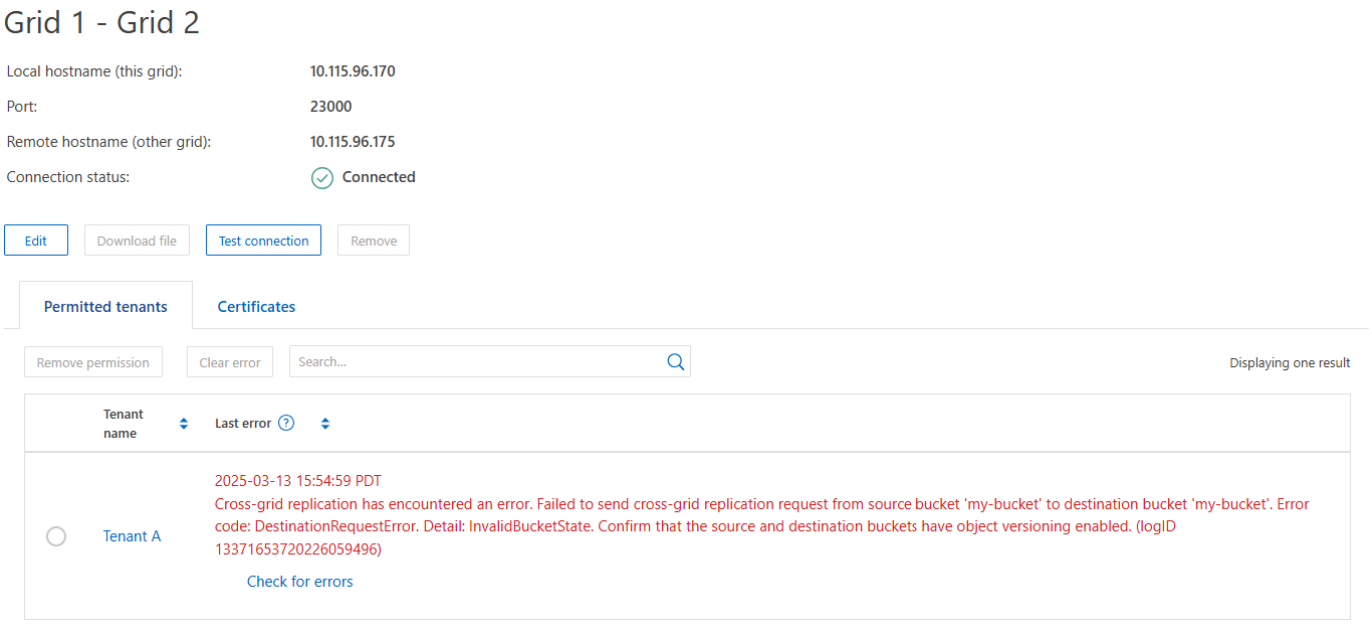
如果錯誤已解決，租用戶帳戶現在將複製到另一個網格。

跨網格複寫警報和錯誤

連線或租戶的最後顯示錯誤

問題

當 "檢視網格聯盟連線" 時（或當 "管理獲準租戶" 為某個連線時），您會在連線詳細資料頁面的「上次錯誤」欄中發現錯誤。例如：



詳細資料

對於每個網格聯合連接，「上次錯誤」欄顯示租戶資料複寫到其他網格時發生的最新錯誤（如有）。此欄僅顯示上次跨網格複寫錯誤；之前可能發生的錯誤不會顯示。此欄中的錯誤可能由以下原因之一引起：

- 未找到來源物件版本。
- 找不到來源儲存桶。
- 目的地儲存桶已刪除。
- 目的地儲存桶已由其他帳戶重新建立。
- 目的地儲存桶已暫停版本控制。
- 目的地儲存桶由相同帳戶重新建立，但現在未進行版本控制。
- 來源物件的 S3 物件鎖定設定與目的地網格的租戶層級保留設定不符。
- 來源物件具有 S3 Object Lock 設定，且目的地儲存桶已停用 S3 Object Lock。

建議採取的措施

如果「上次錯誤」欄位中出現錯誤訊息，請依照下列步驟操作：

1. 審查訊息內容。
2. 執行任何建議的操作。例如，如果跨網格複寫的目的地儲存桶的版本控制已暫停，請重新啟用該儲存桶的版本控制。
3. 從表格中選擇連線或租戶帳戶。
4. 選擇 **Clear error**。
5. 選擇 **Yes** 以清除訊息並更新系統狀態。
6. 等待 5-6 分鐘，然後將新物件擷取至儲存桶。確認錯誤訊息不再出現。

> 為確保錯誤訊息已清除，請在訊息中的時間戳記之後至少等待 5 分鐘，再擷取新物件。

清除錯誤後，如果將物件擷取到另一個也存在錯誤的儲存桶中，則可能會出現新的 **Last error**。

7. 若要確定是否有任何物件因儲存桶錯誤而未能複寫，請參閱"識別並重試失敗的複寫操作"。

跨網格複寫永久故障警報

問題

觸發了「跨網格複寫永久故障」警報。

詳細資料

此警報表示，由於需要使用者介入才能解決的原因，租戶物件無法在兩個網格的儲存桶之間進行複寫。此警報通常是由來源或目的地儲存桶的變更所引起的。

建議採取的措施

1. 登入觸發警報的網格。
2. 前往 組態 > 系統 > 網格聯盟，找到警示中列出的連線名稱。
3. 在「允許的租戶」索引標籤上，查看「上次錯誤」欄，以確定哪些租戶帳戶有問題。
4. 要深入瞭解此故障，請參閱"監控網格聯盟連線"中審查跨網格複寫計量的說明。
5. 對於每個受影響的租戶帳戶：
   a. 請參閱 "${post_edited_translations.segment}" 中的說明，以確認租戶未超過目的地網格上用於跨網格複寫的配額。
   b. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}
7. 對於每個啟用了跨網格複寫的儲存桶，請確認以下內容：
   - 在另一個網格中，同一租戶有一個對應的儲存桶（必須使用確切的名稱）。
   - 兩個儲存桶都已啟用物件版本控制（兩個網格上的版本控制均無法暫停）。
   - 兩個儲存桶均未處於「刪除物件：唯讀」狀態。
8. 若要確認問題已解決，請參閱 "監控網格聯盟連線" 中的說明以審查跨網格複寫計量，或執行以下步驟：
   a. 返回網格聯盟頁面。
   b. 選取受影響的租戶，然後在 **Last error** 欄中選取 **Clear Error**。
   c. 選擇 **Yes** 以清除訊息並更新系統狀態。
   d. 等待 5-6 分鐘，然後將新物件擷取至儲存桶。確認錯誤訊息不再出現。

      為確保錯誤訊息已清除，請在訊息中的時間戳記之後至少等待 5 分鐘，再擷取新物件。

   警報解決後，可能需要一天才能清除。

   a. 前往 "識別並重試失敗的複寫操作" 識別未能複製到其他網格的任何物件或刪除標記，並視需要重試複寫。

跨網格複寫資源無法使用警示

問題

已觸發「跨網格複寫資源無法使用」警報。

詳細資料

此警示表示跨網格複寫要求因資源無法使用而處於擱置狀態。例如，可能發生網路錯誤。

建議採取的措施

1. ${post_edited_translations.segment}
2. 如果問題仍然存在，請確定任一網格是否針對相同連線發出 **Grid federation connection failure** 警報，或針對某個節點發出 **Unable to communicate with node** 警報。解決這些警報後，此警報可能也會解決。
3. 要深入瞭解此故障，請參閱"監控網格聯盟連線"中審查跨網格複寫計量的說明。
4. 如果無法解決警報問題，請聯絡技術支援。

問題解決後，跨網格複寫將照常進行。

識別並重試失敗的 StorageGRID 複寫作業

解決「跨網格複寫永久故障」警報後，您應該確定是否有任何物件或刪除標記未能複寫到另一個網格。然後，您可以重新擷取這些物件，或使用 Grid Management API 重試複寫。

「跨網格複寫永久故障」警報表示租戶物件無法在兩個網格的儲存桶之間進行複寫，原因需要使用者介入才能解決。此警報通常是由來源或目的地儲存桶的變更所引起。如需詳細資訊，請參閱 "排除網格同盟錯誤"。

確定是否有任何物件複製失敗

若要確定是否有任何物件或刪除標記未複寫到其他網格，您可以搜尋稽核日誌中的"${post_edited_translations.segment}"訊息。當 StorageGRID 無法將物件、多部分物件或刪除標記複寫到目的地儲存桶時，此訊息會新增至日誌中。

您可以使用 "audit-explain 工具" 將結果轉換為更易讀的格式。

開始之前

- 您擁有根目錄存取權限。
- 您擁有 `Passwords.txt` 檔案。
- ${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   此命令的結果將類似於此範例，其中包含六個 CGRR 訊息的項目。在此範例中，所有跨網格複寫要求都傳回一般錯誤，因為無法複寫該物件。前三個錯誤代表「複寫物件」作業，後三個錯誤則代表「複寫刪除標記」作業。

   ```
   CGRR Cross-Grid Replication Request tenant:50736445269627437748
   connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
   object" bucket:bucket123 object:"audit-0"
   version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
   error
   CGRR Cross-Grid Replication Request tenant:50736445269627437748
   connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
   object" bucket:bucket123 object:"audit-3"
   version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
   error
   CGRR Cross-Grid Replication Request tenant:50736445269627437748
   connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
   delete marker" bucket:bucket123 object:"audit-1"
   version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
   error
   CGRR Cross-Grid Replication Request tenant:50736445269627437748
   connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
   delete marker" bucket:bucket123 object:"audit-5"
   version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
   error
   ```

   每筆記錄包含以下資訊：

欄位	說明
${post_edited_translations.segment}	請求的名稱
租戶	${post_edited_translations.segment}
連線	${post_edited_translations.segment}

欄位	說明
作業	嘗試執行的複寫操作類型： • 複寫物件 • ${post_edited_translations.segment} • ${post_edited_translations.segment}
儲存貯體	儲存桶名稱
${post_edited_translations.segment}	物件名稱
版本	物件的版本 ID
錯誤	錯誤類型。如果跨網格複寫失敗，錯誤為 "General error"。

重試失敗的複寫

產生未複寫到目的地儲存桶的物件和刪除標記清單並解決根本問題後，您可以透過以下兩種方式之一重試複寫：

- 將每個物件重新匯入來源儲存桶。
- 依照指示使用 Grid Management 私有 API。

步驟

1. ${post_edited_translations.segment}
2. 選擇「前往私有 API 文件」。

   標記為「Private」的 StorageGRID API 端點如有變更，恕不另行通知。StorageGRID 私有端點也會忽略請求的 API 版本。

3. 在 **cross-grid-replication-advanced** 部分，選擇以下端點：

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. ${post_edited_translations.segment}
5. 在 **body** 文字方塊中，將 **versionID** 的範例條目替換為 audit.log 中與失敗的跨網格複寫請求對應的版本 ID。

   請務必保留字串周圍的雙引號。

6. 選擇 **Execute**。
7. ${post_edited_translations.segment}

   待處理狀態表示跨網格複寫請求已新增至內部佇列中進行處理。

${post_edited_translations.segment}

${post_edited_translations.segment}

將物件或刪除標記複寫到另一個網格可能需要幾個小時或更長時間。

您可以透過以下兩種方式之一監控重試操作：

- 使用 S3 "HeadObject" 或 "GetObject" 要求。回應包含 StorageGRID 專屬的 `x-ntap-sg-cgr-replication-status`回應標頭，其將具有下列其中一個值：

${post_edited_translations.segment}	**${post_edited_translations.segment}**
來源	• **COMPLETED**: 複寫成功。 • **PENDING**：該物件尚未複寫。 • 失敗：複寫發生永久性故障。使用者必須解決此錯誤。
目的地	${post_edited_translations.segment}

- 依照指示使用 Grid Management 私有 API。

步驟

1. ${post_edited_translations.segment}

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. ${post_edited_translations.segment}
3. 在「參數」部分，輸入您在 `cross-grid-replication-retry-failed`請求中使用的版本 ID。
4. 選擇 **Execute**。
5. 確認伺服器回應代碼為 **200**。
6. ${post_edited_translations.segment}
   - **PENDING**：該物件尚未複寫。
   - **COMPLETED**: 複寫成功。
   - **FAILED**：複寫發生永久性故障。使用者必須解決此錯誤。

${post_edited_translations.segment}

在 **StorageGRID** 中管理安全性

您可以透過 Grid Manager 設定各種安全性設定，以協助保護您的 StorageGRID 系統。

管理加密

StorageGRID 提供數種加密資料的選項。您應該 "審查可用的加密方法"，以確定哪些選項符合您的資料保護需

求。

管理憑證

您可以"${post_edited_translations.segment}"用於 HTTP 連線或用於向伺服器驗證用戶端或使用者身分的用戶端憑證。

${post_edited_translations.segment}

使用 "${post_edited_translations.segment}" 可讓您保護 StorageGRID 資料，即使應用裝置已從資料中心移除也是如此。在應用裝置磁碟區加密之後，除非節點可以與 KMS 進行通訊，否則您將無法存取應用裝置上的任何資料。

${post_edited_translations.segment}

${post_edited_translations.segment}

如果您使用 S3 平台服務或雲端儲存池，則可以在儲存節點與外部 S3 端點之間設定 "${post_edited_translations.segment}"。如果您使用 HTTPS 或 HTTP 傳送 AutoSupport 套件，則可以在管理節點與技術支援之間設定 "${post_edited_translations.segment}"。

控制防火牆

為了增強系統的安全性，您可以透過在 "${post_edited_translations.segment}" 開啟或關閉特定連接埠來控制對 StorageGRID 管理節點的存取。您也可以透過設定每個節點的 "${post_edited_translations.segment}" 來控制其網路存取。您可以封鎖部署所需連接埠以外的所有連接埠存取。

檢閱 **StorageGRID** 加密方法

StorageGRID 提供數種加密資料的選項。您應該審查可用的方法，以確定哪些方法符合您的資料保護需求。

此表提供 StorageGRID 中可用加密方法的高階摘要。

${post_edited_translations.segment}	運作方式	適用於
${post_edited_translations.segment}	您"設定金鑰管理伺服器"造訪 StorageGRID 網站 "為該應用裝置啟用節點加密"。然後，應用裝置節點會連線到 KMS 以要求金鑰加密金鑰 （KEK）。此金鑰用於加密和解密每個 Volume 上的資料加密金鑰（DEK）。	在安裝期間啟用了 **Node Encryption** 的應用裝置節點。應用裝置上的所有資料都受到保護，以防止實體遺失或自資料中心移除。 注意：使用 KMS 管理加密金鑰僅支援儲存節點和服務應用裝置。

${post_edited_translations.segment}	運作方式	適用於
${post_edited_translations.segment}	如果應用裝置包含支援硬體加密的磁碟機，您可以在安裝期間設定磁碟機密碼。設定磁碟機密碼後，除非知道該密碼，否則任何人都無法從已從系統移除的磁碟機中恢復有效資料。開始安裝之前，請前往 **Configure Hardware** > **Drive Encryption**，設定適用於節點中所有由 StorageGRID 管理的自我加密磁碟機的磁碟機密碼。	配備自加密磁碟機的應用裝置。安全磁碟機上的所有資料均可防止實體遺失或從資料中心移除。 磁碟機加密不適用於 SANtricity 管理的磁碟機。如果您擁有配備自加密磁碟機和 SANtricity 控制器的儲存應用裝置，則可以在 SANtricity 中啟用磁碟機安全性。
${post_edited_translations.segment}	如果您的 StorageGRID 應用裝置已啟用 Drive Security 功能，您可以使用 "SANtricity System Manager"來建立和管理安全性金鑰。需要此金鑰才能存取受保護磁碟機上的資料。	具有 Full Disk Encryption (FDE) 磁碟機或自我加密磁碟機的儲存應用裝置。安全磁碟機上的所有資料均受到保護，可防止實體遺失或從資料中心移除。無法與某些儲存應用裝置或任何服務應用裝置搭配使用。
儲存物件加密	您可以在 Grid Manager 中啟用 "儲存物件加密" 選項。啟用後，任何未在儲存桶層級或物件層級加密的新物件都會在擷取期間加密。	${post_edited_translations.segment} 已儲存的物件未加密。物件中繼資料和其他敏感資料未加密。
S3 bucket 加密	您發出 PutBucketEncryption 要求，以啟用 Bucket 的加密。任何未在物件層級進行加密的新物件，都會在擷取期間進行加密。	${post_edited_translations.segment} 必須為儲存桶指定加密方式。儲存桶中已有的物件不會加密。物件中繼資料和其他敏感資料不會加密。 "儲存貯體上的作業"
S3 物件伺服器端加密 （SSE）	您發出 S3 請求來儲存物件，並包含 `x-amz-server-side-encryption`請求標頭。	${post_edited_translations.segment} 必須為物件指定加密方式。物件中繼資料和其他敏感資料不會加密。 StorageGRID 負責管理金鑰。 "使用伺服器端加密"

${post_edited_translations.segment}	運作方式	適用於
使用客戶提供的金鑰進行 S3 物件伺服器端加密 （SSE-C）	${post_edited_translations.segment} • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	${post_edited_translations.segment} 必須為物件指定加密方式。物件中繼資料和其他敏感資料不會加密。 ${post_edited_translations.segment} "使用伺服器端加密"
外部 Volume 或資料存放區加密	如果您的部署平台支援，您可以使用 StorageGRID 以外的加密方法來加密整個 Volume 或資料存放區。	所有物件資料、中繼資料和系統組態資料，假設每個 Volume 或資料儲存都已加密。 外部加密方法可對加密演算法和金鑰提供更嚴格的控制。可與列出的其他方法結合使用。
${post_edited_translations.segment}	您可以使用 StorageGRID 外部的加密方法來加密物件資料和中繼資料，然後再將其擷取至 StorageGRID。	${post_edited_translations.segment} 外部加密方法可對加密演算法和金鑰提供更嚴格的控制。可與列出的其他方法結合使用。 "Amazon Simple Storage Service - 使用者指南：使用用戶端側加密保護資料"

使用多種加密方法

根據您的需求，您可以同時使用多種加密方法。例如：

- ${post_edited_translations.segment}
- 您可以使用 KMS 來保護應用裝置節點上的資料，也可以使用儲存物件加密選項在擷取物件時對其加密。

如果只有一小部分物件需要加密，請考慮在儲存桶或單一物件層級控制加密。啟用多層加密會產生額外的效能開銷。

相關資訊

"${post_edited_translations.segment}"

管理憑證

管理 **StorageGRID** 中的安全性憑證

安全性憑證是小型資料檔案，用於在 StorageGRID 元件之間以及 StorageGRID 元件與外部系統之間建立安全且可信任的連線。

StorageGRID 使用兩種類型的安全性憑證：

- 使用 HTTPS 連線時需要*伺服器憑證*。伺服器憑證用於在用戶端和伺服器之間建立安全連線，驗證伺服器對其用戶端的身分識別，並為資料傳輸提供安全的通訊路徑。伺服器和用戶端各自擁有一份憑證複本。
- *用戶端憑證*用於向伺服器驗證用戶端或使用者身份，提供比單獨使用密碼更安全的驗證。用戶端憑證不會加密資料。

當用戶端使用 HTTPS 連線至伺服器時，伺服器會以包含公開金鑰的伺服器憑證進行回應。用戶端會將伺服器簽署與其憑證複本上的簽署進行比較。如果簽署相符，用戶端會使用相同的公開金鑰與伺服器建立工作階段。

StorageGRID 在某些連線中擔任伺服器（例如負載平衡器端點），或在其他連線中擔任用戶端（例如 CloudMirror 複寫服務）。

預設網格 **CA** 憑證

StorageGRID 具有內建的憑證授權單位 （CA），可在系統安裝期間產生內部 Grid CA 憑證。預設會使用 Grid CA 憑證來保護內部 StorageGRID 流量的安全。外部憑證授權單位 （CA） 可以核發完全符合您組織資訊安全性原則的自訂憑證。

在非正式作業環境中，請使用 Grid CA 憑證。若是正式作業環境，請使用由外部憑證授權單位簽署的自訂憑證。支援不使用憑證的非安全連線，但不建議使用。

- ${post_edited_translations.segment}
- 所有自訂憑證都必須符合 "${post_edited_translations.segment}"。
- ${post_edited_translations.segment}

> StorageGRID 亦包含在所有網格上均相同的作業系統 CA 憑證。在正式作業環境中，請確保指定由外部憑證授權單位簽署的自訂憑證，以取代作業系統 CA 憑證。

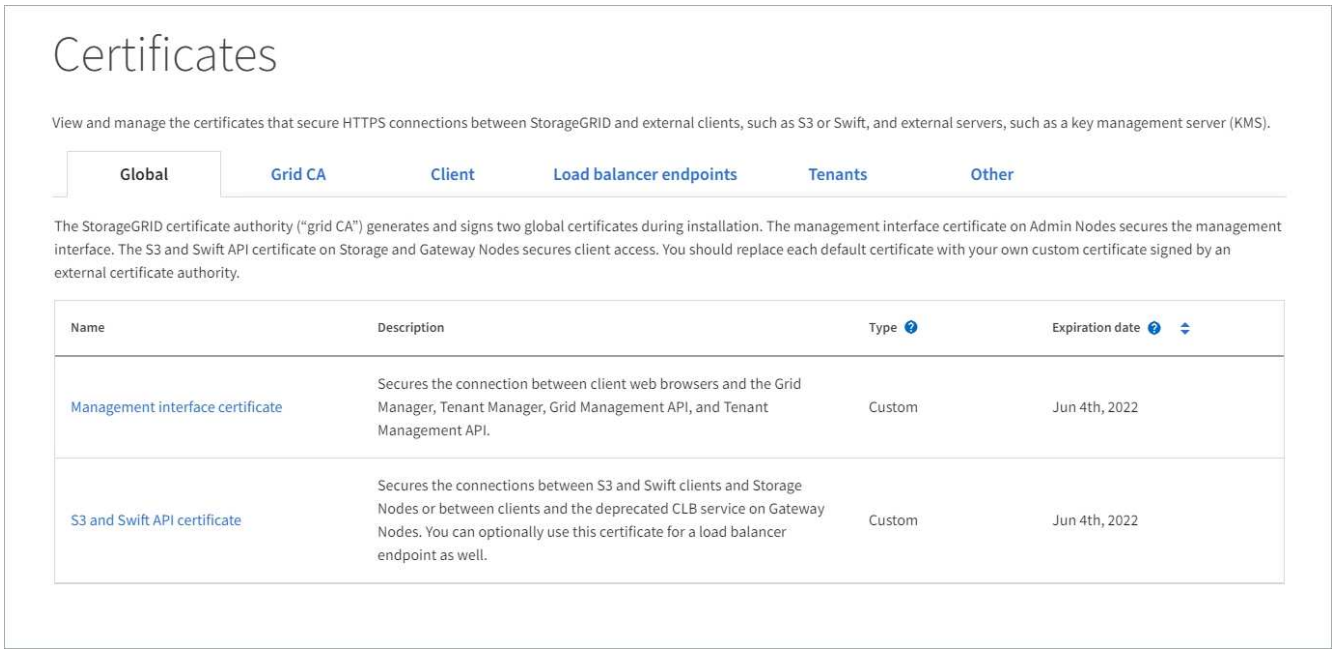
伺服器與用戶端憑證類型的變體是以多種方式實作。在您設定系統之前，您應該先準備好特定 StorageGRID 組態所需的所有憑證。

存取安全性憑證

您可以在單一位置存取所有 StorageGRID 憑證的資訊，以及每個憑證組態工作流程的連結。

步驟

1. ${post_edited_translations.segment}



—

2. 在「憑證」頁面上選取索引標籤，即可檢視每個憑證類別的資訊並存取憑證設定。如果您擁有 "${post_edited_translations.segment}"，則可以存取索引標籤。

   - 全域：保護來自 Web 瀏覽器和外部 API 用戶端的 StorageGRID 存取。
   - **Grid CA**：保護 StorageGRID 內部流量。
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - 租戶：保護與身分識別聯合伺服器的連線，或從平台服務端點到 S3 儲存資源的連線。
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

全球

全域憑證可保護 Web 瀏覽器和外部 S3 API 用戶端對 StorageGRID 的存取安全性。StorageGRID 憑證授權單位會在安裝期間初始產生兩個全域憑證。正式作業環境的最佳實務做法是使用由外部憑證授權單位簽署的自訂憑證。

- [管理介面憑證]: 保護用戶端網頁瀏覽器至 StorageGRID 管理介面的連線。
- <<${post_edited_translations.segment}>>：保護用戶端 API 與儲存節點、管理節點和閘道節點之間的連線，S3 用戶端應用程式使用這些連線來上傳和下載物件資料。

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 說明
- 類型：自訂或預設。+ 為了提高網格安全性，您應該始終使用自訂憑證。
- ${post_edited_translations.segment}

您可以：

- 為了提高網格安全性，請將預設憑證替換為由外部憑證授權單位簽署的自訂憑證：
  - "${post_edited_translations.segment}" 用於 Grid Manager 和 Tenant Manager 連線。
  - "替換 S3 API 憑證"用於儲存節點和負載平衡器端點（選用）連線。
- "還原預設管理介面憑證"。
- "${post_edited_translations.segment}"。
- "${post_edited_translations.segment}"。
- 複製或下載 "管理介面憑證" 或 "${post_edited_translations.segment}"。

網格 **CA**

由 StorageGRID 憑證授權單位在安裝 StorageGRID 期間產生的 ${post_edited_translations.segment}，可保護所有內部 StorageGRID 流量。

${post_edited_translations.segment}

您可以 "${post_edited_translations.segment}"，但無法變更它。

用戶端

${post_edited_translations.segment}由外部憑證授權單位產生，可保護外部監控工具與 StorageGRID Prometheus 資料庫之間連線的安全。

憑證表中每個已設定的用戶端憑證各有一列記錄，並指示該憑證是否可用於 Prometheus 資料庫存取，以及憑證的到期日期。

您可以：

- "上傳或產生新的用戶端憑證。"
- 選取憑證名稱以顯示憑證詳細資料，您可以在其中執行以下操作：

- "變更用戶端憑證名稱。"
- "${post_edited_translations.segment}"
- "上傳並替換用戶端憑證。"
- "複製或下載用戶端憑證。"
- "${post_edited_translations.segment}"

◦ 選擇 **Actions** 可快速"編輯"、"${post_edited_translations.segment}"或"移除"用戶端憑證。您最多可以選擇 10 個用戶端憑證，並使用 **Actions** > **Remove** 一次移除它們。

負載平衡器端點

${post_edited_translations.segment} 保護 S3 用戶端與 Gateway Nodes 和 Admin Nodes 上的 StorageGRID 負載平衡器服務之間的連線安全。

負載平衡器端點表格中，每個已設定的負載平衡器端點各有一列，並指示該端點使用的是全域 S3 API 憑證還是自訂負載平衡器端點憑證。每個憑證的到期日期也會顯示於表格中。

${post_edited_translations.segment}

您可以：

◦ "${post_edited_translations.segment}"，包括其憑證詳細資料。

◦ "為 FabricPool 指定負載平衡器端點憑證。"

◦ "${post_edited_translations.segment}"而不是產生新的負載平衡器端點憑證。

${post_edited_translations.segment}

租戶可以使用 ${post_edited_translations.segment} 或 平台服務端點憑證 來保護其與 StorageGRID 的連線安全。

${post_edited_translations.segment}

您可以：

◦ "選擇租戶名稱以登入 Tenant Manager。"

◦ "選擇租戶名稱以檢視租戶身分識別聯盟詳細資訊"

◦ "選擇租戶名稱以檢視租戶平台服務詳細資料"

◦ "在建立端點期間指定平台服務端點憑證"

其他

StorageGRID 使用其他安全性憑證來實現特定用途。這些憑證依其功能名稱列出。其他安全性憑證包括：

◦ 雲端儲存池憑證

◦ 電子郵件警示通知憑證

◦ 外部 syslog 伺服器憑證

◦ 網格同盟連線憑證

- 身分聯合憑證
- 金鑰管理伺服器 (KMS) 憑證
- <<${post_edited_translations.segment},單一登入憑證>>

資訊顯示函數使用的憑證類型及其伺服器和用戶端憑證到期日期（如適用）。選擇函數名稱會開啟瀏覽器索引標籤，您可以在其中檢視和編輯憑證詳細資訊。

> 只有擁有 "${post_edited_translations.segment}"，才能檢視和存取其他憑證的資訊。

您可以：

- "為 S3、C2S S3 或 Azure 指定雲端儲存池憑證"
- "指定用於警示電子郵件通知的憑證"
- "為外部 syslog 伺服器使用憑證"
- "輪換網格聯盟連線憑證"
- "檢視並編輯身分識別同盟憑證"
- "上傳金鑰管理伺服器（KMS）伺服器和用戶端憑證"
- "手動為信賴方信任指定 SSO 憑證"

安全性憑證詳細資料

以下將介紹每種類型的安全性證書，並附上實作說明的連結。

管理介面憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證用戶端 Web 瀏覽器與 StorageGRID 管理介面之間的連線，讓使用者無需收到安全性警告即可存取 Grid Manager 和 Tenant Manager。 此憑證也可驗證 Grid Management API 和 Tenant Management API 的連線。 您可以使用安裝期間建立的預設憑證，也可以上傳自訂憑證。	**Configuration** > **Security** > **Certificates**，選擇 **Global** 索引標籤，然後選擇 **Management interface certificate**	"設定管理介面憑證"

${post_edited_translations.segment}

憑證類型	說明	導航位置	詳細資料
伺服器	驗證與儲存節點和負載平衡器端點（選用）的安全 S3 用戶端連線。	**Configuration** > **Security** > **Certificates**，選擇 **Global** 索引標籤，然後選擇 **S3 API certificate**	"設定 S3 API 憑證"

${post_edited_translations.segment}

請參閱 預設網格 CA 憑證執行摘要。

管理員用戶端憑證

憑證類型	說明	導航位置	詳細資料
用戶端	安裝在每個用戶端上，允許 StorageGRID 對外部用戶端存取進行驗證。 • 允許授權的外部用戶端存取 StorageGRID Prometheus 資料庫。 • 允許使用外部工具對 StorageGRID 進行安全的監控。	**Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤	"設定用戶端憑證"

負載平衡器端點憑證

憑證類型	說明	導航位置	詳細資料
伺服器	用於驗證 S3 用戶端與 Gateway Nodes 和 Admin Nodes 上的 StorageGRID Load Balancer 服務之間的連線。您可以在設定負載平衡器端點時上傳或產生負載平衡器憑證。用戶端應用程式在連線至 StorageGRID 以儲存和擷取物件資料時，會使用此負載平衡器憑證。 您也可以使用自訂版本的全域 <<${post_edited_translations.segment}>> 憑證來驗證與負載平衡器服務的連線。如果使用全域憑證來驗證負載平衡器連線，則無需為每個負載平衡器端點上傳或產生個別的憑證。 *注意：*用於負載平衡器驗證的憑證是 StorageGRID 正常運作期間最常用的憑證。	設定 > 網路 > 負載平衡器端點	• "設定負載平衡器端點" • "為 FabricPool 建立負載平衡器端點"

雲端儲存池端點憑證

憑證類型	說明	導航位置	詳細資料
伺服器	用於驗證從 StorageGRID 雲端儲存池到外部儲存設備位置（例如 S3 Glacier 或 Microsoft Azure Blob 儲存設備）的連線。每種雲端供應商類型都需要不同的憑證。	**ILM** > 儲存池	"建立雲端儲存池"

電子郵件警示通知憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證 SMTP 電子郵件伺服器與 StorageGRID 之間的連線，用於警示通知。 • 如果與 SMTP 伺服器的通訊需要傳輸層安全性協定 (TLS)，則必須指定電子郵件伺服器 CA 憑證。 • 僅當 SMTP 郵件伺服器需要用戶端憑證進行驗證時，才指定用戶端憑證。	提醒 > 郵件設定	"設定電子郵件通知以接收提醒"

外部 **syslog** 伺服器憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證外部 syslog 伺服器與 StorageGRID 中記錄事件的本機系統日誌伺服器之間的 TLS 或 RELP/TLS 連線。 *注意：*與外部 syslog 伺服器建立 TCP、RELP/TCP 和 UDP 連線時，不需要外部 syslog 伺服器憑證。	設定 > 監控 > 稽核與 **syslog** 伺服器	"使用外部 syslog 伺服器"

網格同盟連線憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證並加密目前 StorageGRID 系統與網格同盟連線中另一個網格之間所傳送的資訊。	設定 > 系統 > 網格同盟	• "建立網格聯盟連線" • "輪換連線憑證"

身分聯合憑證

憑證類型	說明	導航位置	詳細資料
伺服器	驗證 StorageGRID 與外部身分供應商（例如 Active Directory、OpenLDAP 或 Oracle Directory Server）之間的連線。用於身分聯合，允許由外部系統管理管理員群組和使用者。	設定 > 存取控制 > 身分識別同盟	"${post_edited_translations.segment}"

金鑰管理伺服器 **(KMS)** 憑證

憑證類型	說明	導航位置	詳細資料
伺服器和用戶端	驗證 StorageGRID 與外部金鑰管理伺服器 (KMS) 之間的連線，該伺服器為 StorageGRID 應用裝置節點提供加密金鑰。	設定 > 安全性 > 金鑰管理伺服器	"新增金鑰管理伺服器（KMS）"

平台服務端點憑證

憑證類型	說明	導航位置	詳細資料
伺服器	對 StorageGRID 平台服務與 S3 儲存設備資源之間的連線進行驗證。	${post_edited_translations.segment}	"${post_edited_translations.segment}" "${post_edited_translations.segment}"

${post_edited_translations.segment}

憑證類型	說明	導航位置	詳細資料
伺服器	驗證用於單一登入 （SSO） 請求的身分識別聯合服務（例如 Active Directory Federation Services （ADFS））與 StorageGRID 之間的連線。	${post_edited_translations.segment}	"設定單一登入"

證書範例

範例 **1**：負載平衡器服務

${post_edited_translations.segment}

1. 您可以在 StorageGRID 中設定負載平衡器端點並上傳或產生伺服器憑證。
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. 用戶端會比較伺服器簽署與其憑證複本上的簽署。如果簽署符合，用戶端會使用相同的公開金鑰啟動工作階段。
6. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

1. 使用外部金鑰管理伺服器軟體，您可以將 StorageGRID 設定為 KMS 用戶端，並取得 CA 簽署的伺服器憑證、公用用戶端憑證和用戶端憑證的私密金鑰。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. KMS 伺服器驗證憑證簽署，並決定信任 StorageGRID。
5. ${post_edited_translations.segment}

StorageGRID 中支援的伺服器憑證類型

StorageGRID 系統支援使用 RSA 或 ECDSA（橢圓曲線數位簽章演算法）加密的自訂憑證。

安全性原則的加密演算法類型必須與伺服器憑證類型相符。例如，RSA 加密演算法需要 RSA 憑證，而 ECDSA 加密演算法需要 ECDSA 憑證。請參閱 "管理安全性證書"。如果您設定了與伺服器憑證不相容的自訂安全性原則，您可以 "暫時回復預設安全性原則"。

如需更多關於 StorageGRID 如何保護用戶端連線安全的資訊，請參閱 "${post_edited_translations.segment}"。

在 **StorageGRID** 中設定管理介面憑證

您可以將預設的管理介面憑證取代為單一自訂憑證，以允許使用者存取 Grid Manager 和 Tenant Manager，而不會遇到安全性警告。您也可以回復為預設的管理介面憑證，或產生新的憑證。

關於此任務

預設情況下，每個管理節點都會獲得一個由網格 CA 簽署的憑證。這些由 CA 簽署的憑證可以替換為單一通用的自訂管理介面憑證及其對應的私鑰。

由於所有管理節點都使用單一自訂管理介面憑證，因此如果用戶端在連線至 Grid Manager 和 Tenant Manager 時需要驗證主機名稱，則必須將該憑證指定為萬用字元憑證或多網域憑證。請定義自訂憑證，使其與網格中的所有管理節點相符。

您需要在伺服器上完成組態，並且根據您使用的根憑證授權單位 (CA)，使用者可能還需要在他們將用於存取 Grid Manager 和 Tenant Manager 的 Web 瀏覽器中安裝 Grid CA 憑證。

為確保伺服器憑證失效不會中斷運作，當伺服器憑證即將過期時，系統會觸發「管理介面的伺服器憑證過期」警示。如有需要，您可以透過選取 **Configuration** > **Security** > **Certificates**，然後在 Global 索引標籤上查看管理介面憑證的到期日期，來檢視目前憑證的到期時間。

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 你${post_edited_translations.segment}。

${post_edited_translations.segment}

若要新增自訂管理介面憑證，您可以提供自己的憑證，也可以使用 Grid Manager 產生憑證。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 選擇 **Use custom certificate**。
4. 上傳或產生憑證。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇 **Upload certificate**。

b. 上傳所需的伺服器憑證檔案：

   - ${post_edited_translations.segment}
   - 憑證私鑰：自訂伺服器憑證私鑰檔案 (`.key`)

     EC 私鑰必須至少 224 位元。RSA 私鑰必須至少 2048 位元。

   - **CA** 套裝組合：包含來自每個中介發行憑證授權單位（CA）憑證的單一選用檔案。此檔案應包含每個 PEM 編碼的 CA 憑證檔案，並依憑證鏈順序串接。

c. 展開 憑證詳細資料 以檢視您上傳之每個憑證的中繼資料。如果您上傳了選用的 CA 套裝組合，每個憑證都會顯示在各自的索引標籤上。

   - ${post_edited_translations.segment}

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

   - 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」以複製憑證內容並貼上到其他位置。

d. 選擇 **Save**。+ 自訂管理介面憑證將用於所有後續與 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的新連線。

產生證書

產生伺服器憑證檔案。

正式作業環境的最佳實務做法是使用由外部憑證授權單位簽署的自訂管理介面憑證。

a. 選擇 **Generate certificate**。

b. 請提供憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用 * 做為萬用字元來代表多個網域名稱。
IP	憑證中要包含的一個或多個 IP 位址。
${post_edited_translations.segment}	X.509 憑證擁有者的主旨或可分辨名稱 (DN)。 如果此欄位中未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主旨通用名稱 (CN)。

欄位	說明
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 ${post_edited_translations.segment}

c. 選擇 **Generate** 。

d. ${post_edited_translations.segment}

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

e. 選擇 **Save**。+ 自訂管理介面憑證將用於所有後續與 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的新連線。

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

6. 新增自訂管理介面憑證後，「管理介面憑證」頁面會顯示目前使用中憑證的詳細憑證資訊。+ 您可以根據需要下載或複製憑證 PEM。

還原預設管理介面憑證

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   當您還原預設管理介面憑證時，您設定的自訂伺服器憑證檔案將會被刪除，且無法從系統中復原。預設管理介面憑證會用於所有後續的新用戶端連線。

4. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

開始之前

- 您有"特定存取權限"。
- 您擁有 `Passwords.txt` 檔案。

關於此任務

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. 請輸入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。
3. ${post_edited_translations.segment}

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 對於 `--domains`，請使用萬用字元來代表所有管理節點的完整網域名稱。例如，`*.ui.storagegrid.example.com` 使用 * 萬用字元來代表 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 設定 `--type`為 `management`以設定管理介面憑證，此憑證由 Grid Manager 和 Tenant Manager 使用。
   - 預設情況下，產生的憑證有效期為一年（365 天），必須在過期前重新產生。您可以使用 `--days` 參數來置換預設的有效期。

     > ⓘ 憑證的有效期自執行 `make-certificate` 時開始。您必須確保管理用戶端與 StorageGRID 同步至相同的時間來源；否則，用戶端可能會拒絕該憑證。

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
     ```

     輸出結果包含管理 API 用戶端所需的公開憑證。
4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}
5. 登出命令 shell。 `$ exit`
6. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

7. 設定您的管理用戶端以使用您複製的公開憑證。請包含 BEGIN 和 END 標記。

${post_edited_translations.segment}

您可以儲存或複製管理介面憑證的內容以供其他地方使用。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

下載憑證檔案或 **CA** 套裝組合

下載憑證或 CA 套裝組合 `.pem`檔案。如果您使用的是選用的 CA 套裝組合，則套裝組合中的每個憑證都會顯示在各自的子索引標籤中。

a. 選擇「下載憑證」或「下載 CA 套裝組合」。

如果您正在下載 CA 套裝組合，則 CA 套裝組合二級標籤中的所有憑證將下載為單一檔案。

b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 套裝組合 **PEM**

複製憑證文字以貼到其他地方。如果您使用的是選用 CA 套裝組合，套裝組合中的每個憑證都會顯示在各自的子索引標籤上。

a. 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」。

如果您要複製 CA 套裝組合，則 CA 套裝組合次要標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。

c. 將文字檔案以副檔名 `.pem`儲存。

例如： `storagegrid_certificate.pem`

在 **StorageGRID** 中設定 **S3 API** 憑證

您可以替換或還原用於 S3 用戶端連線至儲存節點或負載平衡器端點的伺服器憑證。替換後的自訂伺服器憑證專屬於您的組織。

此版本的文件網站已移除 Swift 相關細節。請參閱 "${post_edited_translations.segment}"。

關於此任務

預設情況下，每個 Storage Node 都會獲發由網格 CA 簽署的 X.509 伺服器憑證。這些 CA 簽署的憑證可以替換為單一常用的自訂伺服器憑證和對應的私密金鑰。

所有 Storage Nodes 均使用單一自訂伺服器憑證，因此，如果用戶端在連線至儲存設備端點時需要驗證主機名稱，則必須將該憑證指定為萬用字元憑證或多網域憑證。請定義自訂憑證，使其與網格中的所有 Storage Nodes 相符。

在伺服器上完成組態後，您可能還需要在用於存取系統的 S3 API 用戶端中安裝 Grid CA 憑證，具體取決於您使用的根憑證授權單位 (CA)。

> 為確保伺服器憑證失效不會中斷運行，當根目錄伺服器憑證即將過期時，系統會觸發「S3 API 全域伺服器憑證即將過期」警報。如有需要，您可以透過選取「組態」>「安全性」>「憑證」，然後在「全域」標籤上查看 S3 API 憑證的到期日期，來檢視目前憑證的到期時間。

您可以上傳或產生自訂 S3 API 憑證。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 選擇 **Use custom certificate**。
4. 上傳或產生憑證。

上傳證書

上傳所需的伺服器憑證檔案。

a. 選擇 **Upload certificate**。

b. 上傳所需的伺服器憑證檔案：

   - ${post_edited_translations.segment}
   - 憑證私鑰：自訂伺服器憑證私鑰檔案 (`.key`)

     EC 私鑰必須至少 224 位元。RSA 私鑰必須至少 2048 位元。

   - **CA** 套裝組合：包含來自每個中介發行憑證授權單位憑證的單一選用檔案。此檔案應包含每個 PEM 編碼的 CA 憑證檔案，並依憑證鏈順序串聯。

c. 選取憑證詳細資料，以顯示已上傳之每個自訂 S3 API 憑證的中繼資料與 PEM。如果您上傳了選用的 CA 套裝組合，每個憑證都會顯示在各自的索引標籤上。

   - ${post_edited_translations.segment}

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

     例如： `storagegrid_certificate.pem`

   - 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」以複製憑證內容並貼上到其他位置。

d. 選取 **Save** 。

   自訂伺服器憑證用於後續新的 S3 用戶端連線。

產生證書

產生伺服器憑證檔案。

a. 選擇 **Generate certificate**。

b. 請提供憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用 * 做為萬用字元來代表多個網域名稱。
IP	憑證中要包含的一個或多個 IP 位址。
${post_edited_translations.segment}	X.509 憑證擁有者的主旨或可分辨名稱 (DN)。 如果此欄位中未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主旨通用名稱 (CN)。

欄位	說明
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 ${post_edited_translations.segment}

c. 選擇 **Generate** 。

d. ${post_edited_translations.segment}

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

e. 選取 **Save** 。

自訂伺服器憑證用於後續新的 S3 用戶端連線。

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 新增自訂 S3 API 憑證後，S3 API 憑證頁面會顯示目前使用中自訂 S3 API 憑證的詳細憑證資訊。+ 您可以根據需要下載或複製憑證 PEM。

${post_edited_translations.segment}

您可以回復使用預設的 S3 API 憑證來建立 S3 用戶端與儲存節點的連線。但是，您不能將預設的 S3 API 憑證用於負載平衡器端點。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   當您還原全域 S3 API 憑證的預設版本時，您設定的自訂伺服器憑證檔案將會被刪除，且無法從系統中復原。預設的 S3 API 憑證將用於後續與儲存節點的新 S3 用戶端連線。

4. ${post_edited_translations.segment}

如果您擁有根目錄存取權限，並且使用了自訂 S3 API 憑證來連接負載平衡器端點，則會顯示負載平衡器端點清單，這些端點將無法再使用預設 S3 API 憑證存取。請前往 "設定負載平衡器端點" 編輯或移除受影響的端點。

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以儲存或複製 S3 API 憑證內容以供其他地方使用。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

下載憑證檔案或 **CA** 套裝組合

下載憑證或 CA 套裝組合 `.pem`檔案。如果您使用的是選用的 CA 套裝組合，則套裝組合中的每個憑證都會顯示在各自的子索引標籤中。

a. 選擇「下載憑證」或「下載 CA 套裝組合」。

   如果您正在下載 CA 套裝組合，則 CA 套裝組合二級標籤中的所有憑證將下載為單一檔案。

b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

複製憑證或 **CA** 套裝組合 **PEM**

複製憑證文字以貼到其他地方。如果您使用的是選用 CA 套裝組合，套裝組合中的每個憑證都會顯示在各自的子索引標籤上。

a. 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」。

   如果您要複製 CA 套裝組合，則 CA 套裝組合次要標籤中的所有憑證都會一起複製。

b. 將複製的憑證貼到文字編輯器中。

c. 將文字檔案以副檔名 `.pem`儲存。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用 S3 REST API"
- "設定 S3 端點網域名稱"

複製 **StorageGRID Grid CA** 憑證

StorageGRID 使用內部憑證授權單位 (CA) 來保護內部流量。即使您上傳了自己的憑證，此憑證也不會變更。

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"。

關於此任務

如果已設定自訂伺服器憑證，用戶端應用程式應使用該自訂伺服器憑證驗證伺服器。它們不應從 StorageGRID 系統複製 CA 憑證。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Grid CA** 索引標籤。
2. 在「憑證 PEM」區段中，下載或複製憑證。

   下載憑證檔案

   下載憑證 `.pem`檔案。

   a. 選取 **Download certificate**。
   b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

      例如： `storagegrid_certificate.pem`

   複製憑證 **PEM**

   複製證書文字並貼上到其他位置。

   a. 選擇 **Copy certificate PEM**。
   b. 將複製的憑證貼到文字編輯器中。
   c. 將文字檔案以副檔名 `.pem`儲存。

      例如： `storagegrid_certificate.pem`

為 **FabricPool** 設定 **StorageGRID** 憑證

對於執行嚴格主機名稱驗證且不支援停用嚴格主機名稱驗證的 S3 用戶端（例如使用 FabricPool 的 ONTAP 用戶端），您可以在設定負載平衡器端點時產生或上傳伺服器憑證。

開始之前

- 您有"特定存取權限"。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

當您建立負載平衡器端點時，可以產生自我簽署的伺服器憑證，或上傳由已知憑證授權單位（CA）簽署的憑證。在生產環境中，您應該使用由已知 CA 簽署的憑證。由 CA 簽署的憑證可以不中斷地進行輪替。它們也更為安全，因為能針對中間人攻擊提供更好的保護。

以下步驟為使用 FabricPool 的 S3 用戶端提供一般性指導原則。如需更詳細的資訊和程序，請參閱 "設定 StorageGRID 以供 FabricPool 使用"。

步驟

1. 選擇性地設定高可用度（HA）群組以供 FabricPool 使用。
2. 建立供 FabricPool 使用的 S3 負載平衡器端點。

   建立 HTTPS 負載平衡器端點時，系統會提示您上傳伺服器憑證、憑證私密金鑰和選用的 CA 套裝組合。

3. 將 StorageGRID 作為雲端層附加至 ONTAP。

   請指定負載平衡器端點連接埠以及您上傳的 CA 憑證中所使用的完整網域名稱。然後，請提供 CA 憑證。

   如果 StorageGRID 憑證是由中間 CA 核發的，則必須提供該中間 CA 憑證。如果 StorageGRID 憑證是由根 CA 直接核發的，則必須提供該根 CA 憑證。

在 **StorageGRID** 中設定用戶端憑證

用戶端憑證可讓授權的外部用戶端存取 StorageGRID Prometheus 資料庫，為外部工具監控 StorageGRID 提供安全的方式。

如果您需要使用外部監控工具存取 StorageGRID，則必須使用 Grid Manager 上傳或產生用戶端憑證，並將憑證資訊複製到外部工具。

參見 "管理安全性證書" 和 "設定自訂伺服器憑證"。

為確保伺服器憑證失效不會中斷執行，當伺服器憑證即將過期時，系統會觸發*憑證頁面上設定的用戶端憑證過期*警報。如有需要，您可以透過選擇 **Configuration** > **Security** > **Certificates**，然後在 Client 標籤上查看用戶端憑證的過期日期，來檢視目前憑證的到期時間。

如果您使用金鑰管理伺服器 (KMS) 來保護特殊設定的應用裝置節點上的資料，請參閱有關 "上傳 KMS 用戶端憑證" 的具體資訊。

開始之前

- 您擁有根目錄存取權限。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 設定用戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 如果您已設定 StorageGRID 管理介面憑證，則您擁有用於設定管理介面憑證的 CA、用戶端憑證和私密金鑰。
  - 若要上傳您自己的憑證，憑證的私密金鑰必須存放在您的本機電腦上。

- 私鑰必須在建立時儲存或記錄。如果您沒有原始私鑰，則必須建立新的私鑰。

- 編輯用戶端憑證：
  - 您擁有管理節點的 IP 位址或網域名稱。
  - 若要上傳您自己的憑證或新憑證，私密金鑰、用戶端憑證和 CA （如果使用）都位於您的本機電腦上。

新增用戶端證書

若要新增用戶端憑證，請使用下列其中一個程序：

- [管理介面憑證已設定]
- CA 核發的用戶端證書
- 從 Grid Manager 產生的憑證

管理介面憑證已設定

如果已使用客戶提供的 CA、用戶端憑證和私密金鑰設定了管理介面憑證，請使用此程序新增用戶端憑證。

步驟

1. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選擇 **Add** 。
3. 請輸入憑證名稱。
4. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
5. 選擇 **Continue** 。
6. 在「附加憑證」步驟中，上傳管理介面憑證。
   a. 選擇 **Upload certificate**。
   b. 選擇 **Browse** ，然後選擇管理介面憑證檔案(`.pem`) 。
      - 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。
      - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

      新證書會顯示在「用戶端」標籤上。
7. 設定外部監控工具，例如 Grafana。

CA 核發的用戶端證書

如果未設定管理介面憑證，且您計劃為 Prometheus 新增使用 CA 頒發的用戶端憑證和私密金鑰的用戶端憑證，請使用此程序新增系統管理員用戶端憑證。

步驟

1. 執行以下步驟"設定管理介面憑證"。
2. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。

3. 選擇 **Add** 。
4. 請輸入憑證名稱。
5. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
6. 選擇 **Continue** 。
7. 在「附加憑證」步驟中，上傳用戶端憑證、私鑰和 CA 套裝組合檔案：
   a. 選擇 **Upload certificate**。
   b. 選擇 **Browse** ，然後選擇用戶端憑證、私鑰和 CA 套裝組合檔案(`.pem`) 。
      - 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。
      - 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
   c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

      新證書會顯示在「用戶端」標籤上。
8. 設定外部監控工具，例如 Grafana。

從 **Grid Manager** 產生的憑證

如果未設定管理介面憑證，且您計劃為 Prometheus 新增用戶端憑證（此憑證使用 Grid Manager 中的產生憑證功能），請使用此程序新增系統管理員用戶端憑證。

步驟

1. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選擇 **Add** 。
3. 請輸入憑證名稱。
4. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
5. 選擇 **Continue** 。
6. 在「附加憑證」步驟中，選取「產生憑證」。
7. 請提供憑證資訊：
   - 主旨（可選）：憑證擁有者的 X.509 主旨或可分辨名稱 (DN)。
   - 有效天數：產生的憑證自產生時起有效的天數。
   - 新增金鑰用途擴充：如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。

     這些擴充定義了憑證中包含的金鑰的用途。

     除非您在使用包含這些擴充功能的憑證時，舊版用戶端發生連線問題，否則請保持選取此核取方塊。
8. 選擇 **Generate** 。
9. 選擇 用戶端憑證詳細資料 以顯示憑證中繼資料和憑證 PEM。

關閉對話方塊後，您將無法檢視憑證私鑰。請將金鑰複製或下載到安全位置。

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy private key** 以複製憑證私鑰，以便貼上到其他位置。
- 選擇 **Download private key** 將私密金鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

10. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

    新證書會顯示在「用戶端」標籤上。

11. 在 Grid Manager 中，選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Global** 索引標籤。
12. 選擇 **Management Interface certificate**。
13. 選擇 **Use custom certificate**。
14. 從用戶端憑證詳細資料步驟上傳 certificate.pem 和 private_key.pem 檔案。無需上傳 CA 套裝組合。
    a. 選擇 **Upload certificate**，然後選擇 **Continue**。
    b. 上傳每個憑證檔案 (`.pem`) 。
    c. 選擇 **Save** 以將憑證儲存至 Grid Manager 中。

       新證書將顯示在管理介面證書頁面上。

15. 設定外部監控工具，例如 Grafana。

設定外部監控工具

步驟

1. 請在外部監控工具（例如 Grafana）上設定以下設定。
    a. 名稱：請輸入連線的名稱。

       StorageGRID 不需要此資訊，但您必須提供名稱才能測試連線。

    b. **URL**：輸入管理節點的網域名稱或 IP 位址。請指定 HTTPS 和連接埠 9091。

       例如： `https://admin-node.example.com:9091`

    c. 啟用 **TLS Client Auth** 和 **With CA Cert**。
    d. 在 TLS/SSL 驗證詳細資訊下，複製並貼上：+
       - 管理介面 CA 憑證到 **CA Cert**

- 用戶端憑證至 **Client Cert**
- **Client Key** 的私鑰

e. **ServerName**：請輸入管理節點的網域名稱。

ServerName 必須與管理介面憑證中顯示的網域名稱一致。

2. 儲存並測試從 StorageGRID 或本機檔案複製的憑證和私密金鑰。

現在您可以使用外部監控工具存取 StorageGRID 中的 Prometheus 計量。

有關計量的資訊，請參閱 "監控 StorageGRID 的說明"。

編輯用戶端憑證

您可以編輯系統管理員用戶端憑證以變更其名稱、啟用或停用 Prometheus 存取，或在目前憑證過期時上傳新憑證。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。

憑證到期日和 Prometheus 存取權限列於表中。如果憑證即將到期或已過期，表中將顯示一則訊息，並觸發警示。

2. 選擇要編輯的憑證。
3. 選擇*編輯*，然後選擇*編輯名稱和權限*。
4. 請輸入憑證名稱。
5. 若要使用外部監控工具存取 Prometheus 計量，請選擇 * 允許 prometheus*。
6. 選擇 **Continue** 以將憑證儲存在 Grid Manager 中。

更新後的憑證顯示在「用戶端」索引標籤上。

附加新用戶端證書

當現有憑證過期時，您可以上傳新憑證。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。

憑證到期日和 Prometheus 存取權限列於表中。如果憑證即將到期或已過期，表中將顯示一則訊息，並觸發警示。

2. 選擇要編輯的憑證。
3. 選擇 **Edit**，然後選擇編輯選項。

上傳證書

複製證書文字並貼上到其他位置。

a. 選擇 **Upload certificate**，然後選擇 **Continue**。

b. 上傳用戶端憑證名稱(`.pem`）。

選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

c. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

更新後的憑證顯示在「用戶端」索引標籤上。

產生證書

產生憑證文字，以便貼到其他位置。

a. 選擇 **Generate certificate**。

b. 請提供憑證資訊：

- 主旨（可選）：憑證擁有者的 X.509 主旨或可分辨名稱 (DN)。
- 有效天數：產生的憑證自產生時起有效的天數。
- 新增金鑰用途擴充：如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。

  這些擴充定義了憑證中包含的金鑰的用途。

  除非您在使用包含這些擴充功能的憑證時，舊版用戶端發生連線問題，否則請保持選取此核取方塊。

c. 選擇 **Generate** 。

d. 選擇「用戶端憑證詳細資料」以顯示憑證中繼資料和憑證 PEM。

  關閉對話方塊後，您將無法檢視憑證私鑰。請將金鑰複製或下載到安全位置。

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。
- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy private key** 以複製憑證私鑰，以便貼上到其他位置。
- 選擇 **Download private key** 將私密金鑰儲存為檔案。

  指定私鑰檔案名稱和下載位置。

e. 選擇 **Create** 以將憑證儲存在 Grid Manager 中。

新證書會顯示在「用戶端」標籤上。

下載或複製用戶端憑證

您可以下載或複製用戶端憑證以供其他地方使用。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選取要複製或下載的憑證。
3. 下載或複製憑證。

下載憑證檔案

下載憑證 `.pem`檔案。

a. 選取 **Download certificate**。
b. 指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

複製憑證

複製證書文字並貼上到其他位置。

a. 選擇 **Copy certificate PEM**。
b. 將複製的憑證貼到文字編輯器中。
c. 將文字檔案以副檔名 `.pem`儲存。

例如： `storagegrid_certificate.pem`

移除用戶端憑證

如果您不再需要系統管理員用戶端憑證，可以將其移除。

步驟

1. 選擇 **Configuration** > **Security** > **Certificates**，然後選擇 **Client** 索引標籤。
2. 選取要移除的憑證。

3. 選取 **Delete** ，然後確認。

若要移除最多 10 個憑證，請在「用戶端」索引標籤上選擇要移除的每個憑證，然後選擇 **Actions** > **Delete**。

憑證移除後，使用該憑證的用戶端必須指定新的用戶端憑證，才能存取 StorageGRID Prometheus 資料庫。

設定安全性設定

管理 **StorageGRID** 中的 **TLS** 和 **SSH** 原則

TLS 和 SSH 原則決定了使用哪些協定和密碼，以便與用戶端應用程式建立安全的 TLS 連線，以及與內部 StorageGRID 服務建立安全的 SSH 連線。

安全性原則控制 TLS 和 SSH 如何加密傳輸中的資料。通常情況下，請使用「現代相容性（預設）」原則，除非您的系統需要符合通用準則 (Common Criteria) 或需要使用其他加密演算法。

部分 StorageGRID 服務尚未更新，以使用這些原則中的加密演算法。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

選擇安全性原則

步驟

1. ${post_edited_translations.segment}

   An error occurred.

2. ${post_edited_translations.segment}

${post_edited_translations.segment}

如果您需要強式加密且沒有特殊需求，請使用預設原則。此原則與大多數 TLS 和 SSH 用戶端相容。

${post_edited_translations.segment}

如果您需要適用於較舊用戶端的額外相容性選項，請使用 Legacy 相容性原則。此原則中的額外選項可能會使其比 Modern 相容性原則更不安全。

${post_edited_translations.segment}

如果您需要獲得通用準則認證，請使用通用準則原則。

${post_edited_translations.segment}

如果您需要 Common Criteria 認證，且需要使用 NetApp Cryptographic Security Module （NCSM） 3.0.8 或 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組來進行連線至負載平衡器端點、Tenant Manager 和 Grid Manager 的外部用戶端連線，請使用 FIPS 嚴格原則。使用此原則可能會降低效能。

NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組用於以下操作：

- ${post_edited_translations.segment}
  - 以下服務之間的 TLS 連線：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api 、nginx、nginx-gw 和 cache-svc
  - 用戶端與 nginx-gw 服務（負載平衡器端點）之間的 TLS 連線
  - ${post_edited_translations.segment}
  - 物件內容加密（適用於 SSE-S3、SSE-C 和儲存物件加密設定）
  - SSH 連線

  如需詳細資訊，請參閱 NIST Cryptographic Algorithm Validation Program "憑證 #4838"。

- NetApp StorageGRID Kernel Crypto API 模組

  NetApp StorageGRID 核心加密 API 模組僅存在於 VM 和 StorageGRID 應用裝置平台上。

  - 熵收集
  - ${post_edited_translations.segment}

  如需詳細資訊，請參閱 NIST Cryptographic Algorithm Validation Program "證書編號 #A6242 至 #A6257" 與 "Entropy 憑證 #E223"。

注意：選取此原則後，"執行滾動重新開機"所有節點以啟動 NCSM。使用 維護 > 輪流重新開機 來啟動並監控重新開機。

自訂
${post_edited_translations.segment}

（選用）如果您的 StorageGRID 具有 FIPS 140 密碼編譯需求，請啟用 FIPS 模式功能以使用 NCSM 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模組：

a. 將 `fipsMode`參數設定為 `true`。

b. 出現提示時，請"執行滾動重新開機"所有節點以啟動密碼編譯模組。使用 * 組織維護 * > * 輪流重新開機 * 來啟動和監控重新開機。

c. 選擇 **Support** > **Diagnostics** 以檢視作用中的 FIPS 模組版本。

3. 若要查看每項原則的密碼編譯、協定和演算法的詳細資訊，請選取 **View details**。
4. ${post_edited_translations.segment}

   在原則圖塊的「目前原則」旁邊會出現一個綠色對勾。

${post_edited_translations.segment}

如果您需要套用自己的密碼編譯，可以建立自訂原則。

步驟

1. 在與您要建立的自訂原則最相似的原則圖塊中，選擇 **View details**。
2. 選擇*複製到剪貼簿*，然後選擇*取消*。

3. ${post_edited_translations.segment}
4. 貼上您複製的 JSON，並進行必要的修改。
5. 選擇 **Use policy**。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}

暫時回復預設安全性原則

如果您設定了自訂安全性原則，且設定的 TLS 原則與 "${post_edited_translations.segment}" 不相容，您可能無法登入 Grid Manager。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
   a. 輸入以下命令： `ssh admin@Admin_Node_IP`
   b. 請輸入 `Passwords.txt`檔案中列出的密碼。
   c. 輸入以下命令以切換至根目錄： `su -`
   d. 請輸入 `Passwords.txt`檔案中列出的密碼。

      當您以根目錄身分登入時，提示符號會從 `$`變為 `#`。

2. 執行下列命令：

   ```
   restore-default-cipher-configurations
   ```

3. 透過網頁瀏覽器，存取同一管理節點上的 Grid Manager。
4. 請依照選擇安全性原則中的步驟重新設定原則。

設定 **StorageGRID** 網路和物件安全

您可以設定網路和物件安全性，以加密儲存的物件、阻止某些 S3 請求，或允許用戶端連線至儲存節點時使用 HTTP 而非 HTTPS。

儲存物件加密

儲存物件加密可在透過 S3 匯入所有物件資料時對其進行加密。預設情況下，儲存物件不會加密，但您可以選擇使用 AES‐128 或 AES‐256 加密演算法對物件加密。啟用此設定後，所有新匯入的物件都會加密，但現有儲存物件不會有任何變更。如果停用加密，目前已加密的物件仍保持加密狀態，但新匯入的物件將不會加密。

儲存物件加密設定僅適用於尚未透過儲存桶層級或物件層級加密進行加密的 S3 物件。

有關 StorageGRID 加密方法的更多詳細資訊，請參閱"檢閱 StorageGRID 加密方法"。

防止用戶端修改

「防止用戶端修改」是一項全系統設定。選取「防止用戶端修改」選項後，以下請求將被拒絕。

S3 REST API

- DeleteBucket 請求
- 任何修改現有物件資料、使用者定義中繼資料或 S3 物件標記的請求

為儲存節點連線啟用 **HTTP**

預設情況下，用戶端應用程式使用 HTTPS 網路傳輸協定與儲存節點建立任何直接連線。您可以選擇為這些連線啟用 HTTP，例如，在測試非生產網格時。

只有當 S3 用戶端需要直接與儲存節點建立 HTTP 連線時，才使用 HTTP 進行儲存節點連線。對於僅使用 HTTPS 連線的用戶端或連線到負載平衡器服務的用戶端，則無需使用此選項（因為可以"設定每個負載平衡器端點"使用 HTTP 或 HTTPS）。

請參閱 "摘要：用戶端連線的 IP 位址和連接埠" 以了解 S3 用戶端在使用 HTTP 或 HTTPS 連線至儲存節點時所使用的連接埠。

選擇選項

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有根目錄存取權限。

步驟

1. ${post_edited_translations.segment}
2. 選擇「網路和物件」索引標籤。
3. 對於儲存物件加密，如果您不希望對儲存物件進行加密，請使用 **None**（預設）設定；或選擇 **AES-128** 或 **AES-256** 來加密儲存物件。
4. 如果您想防止 S3 用戶端發出特定請求，可以選擇性地選取 **Prevent client modification**。

   更改此設定後，新設定大約需要一分鐘才能生效。已設定的值會被快取，以提高效能和擴充性。

5. 如果用戶端直接連線至儲存節點，且您想要使用 HTTP 連線，請選擇性地選取 **Enable HTTP for Storage Node connections**。

   在生產網格中啟用 HTTP 時要格外小心，因為請求將以未加密的方式傳送。

6. 選取 **Save** 。

更改 **StorageGRID** 介面安全性設定

${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"${post_edited_translations.segment}"。

關於此任務

${post_edited_translations.segment}

${post_edited_translations.segment}

指示使用者瀏覽器在登出前可以保持非活動狀態的時間長度。預設值為 15 分鐘。

瀏覽器閒置逾時時間也受以下因素控制：

- 一個獨立、不可設定的 StorageGRID 定時器，其包含在系統安全性中。每位使用者登入 16 小時後，其驗證權杖便會過期。當使用者的驗證過期時，該使用者會自動登出，即使已停用瀏覽器閒置逾時或尚未達到瀏覽器逾時值也是如此。若要更新權杖，使用者必須重新登入。
- ${post_edited_translations.segment}

如果啟用了 SSO 且使用者的瀏覽器逾時，則使用者必須重新輸入其 SSO 憑證才能再次存取 StorageGRID。請參閱"單一登入 (SSO) 的工作原理"。

${post_edited_translations.segment}

控制是否在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

此選項預設為停用狀態，但您可能需要在測試環境中啟用此功能。通常，在生產環境中應停用 stack trace，以避免在發生 API 錯誤時洩露內部軟體細節。

步驟

1. ${post_edited_translations.segment}
2. 選取*介面*索引標籤。
3. ${post_edited_translations.segment}
   a. 展開折疊面板。
   b. 若要變更逾時時間，請指定 60 秒到 7 天之間的值。預設逾時時間為 15 分鐘。
   c. 若要停用此功能，請取消選取該複選框。
   d. 選取 **Save** 。

   新設定不會影響目前已登入的使用者。使用者必須重新登入或重新整理瀏覽器，新的逾時設定才能生效。
4. 若要變更 Management API stack trace 的設定：
   a. 展開折疊面板。
   b. 勾選此核取方塊，即可在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

      ${post_edited_translations.segment}
   c. 選取 **Save** 。

管理 **StorageGRID** 中的外部 **SSH** 存取

透過封鎖或允許外部存取來管理傳入網格流量的 SSH 存取。管理 SSH 外部存取不會影響網格中節點之間的流量。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

關於此任務

為了增強系統安全性，預設會封鎖外部 SSH 存取。如果您需要執行需要傳入 SSH 存取的工作（例如疑難排解），請暫時允許外部存取。完成工作後，請封鎖外部存取。

步驟

1. ${post_edited_translations.segment}
2. 選取 **Block SSH** 索引標籤。

3. 使用「封鎖傳入 SSH 存取」選項來管理外部 SSH 存取：
   a. 選取此核取方塊可封鎖存取（預設）。
   b. 取消選取核取方塊以允許存取。

> 需要服務筆記型電腦與所有其他網格節點之間在連接埠 22 上的存取權限。完成維護工作時，請移除連接埠 22 的存取權限。

4. 選取 **Save** 。

${post_edited_translations.segment}

瞭解 **StorageGRID** 中的金鑰管理伺服器

${post_edited_translations.segment}

StorageGRID 僅支援特定的金鑰管理伺服器。如需支援的產品與版本清單，請使用 "NetApp 互作業性矩陣工具（IMT）"。

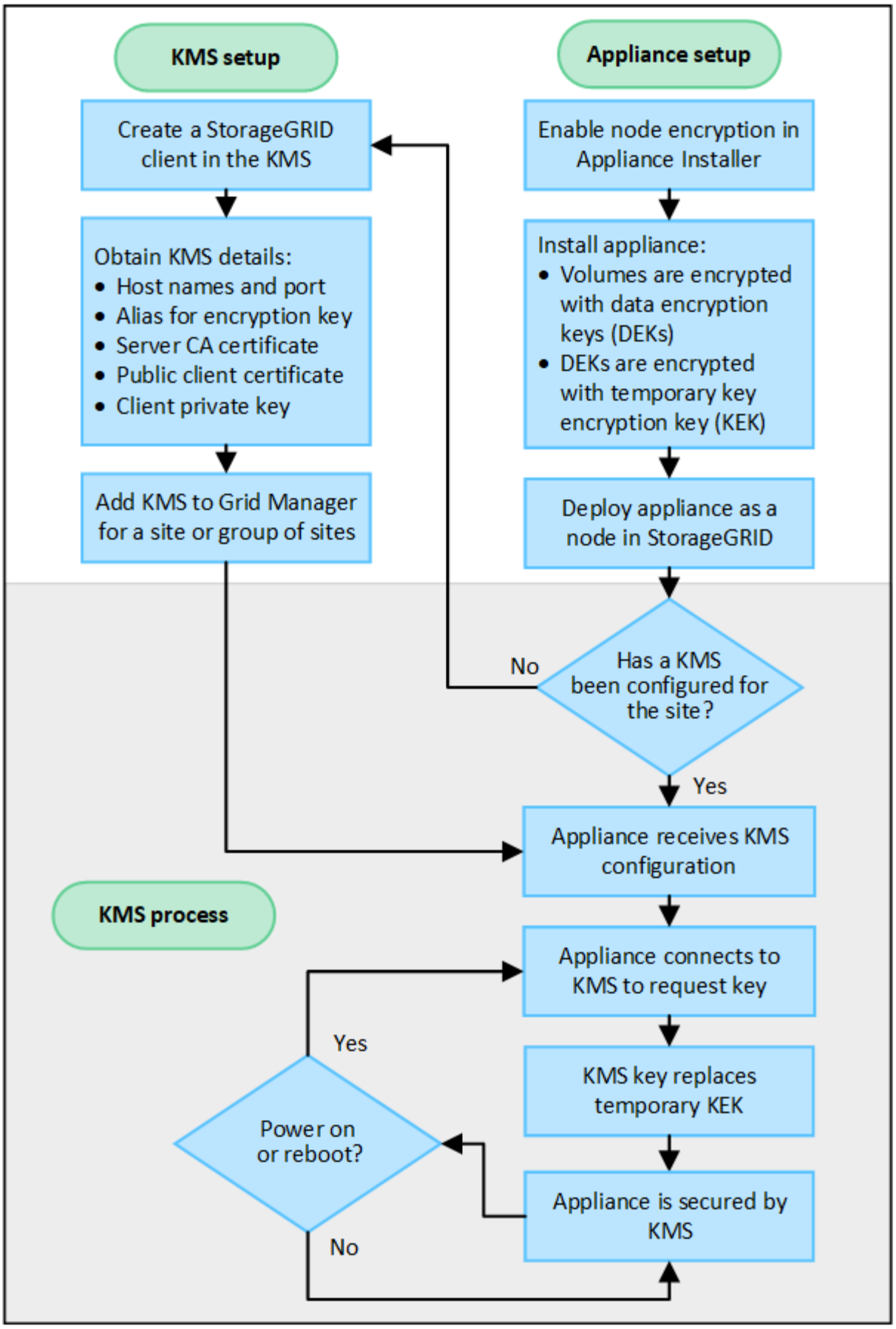
您可以使用一或多個金鑰管理伺服器，為安裝期間啟用 **Node Encryption**（節點加密）設定的任何 StorageGRID 應用裝置節點管理節點加密金鑰。將金鑰管理伺服器與這些應用裝置節點搭配使用，即使應用裝置從資料中心移出，也能保護您的資料。在應用裝置磁碟區加密之後，除非節點可以與 KMS 通訊，否則您無法存取應用裝置上的任何資料。

> StorageGRID 不會建立或管理用於加密和解密應用裝置節點的外部金鑰。如果您計劃使用外部金鑰管理伺服器來保護 StorageGRID 資料，您必須瞭解如何設定該伺服器，且必須瞭解如何管理加密金鑰。執行金鑰管理工作已超出這些說明的範圍。如果您需要協助，請參閱金鑰管理伺服器的說明文件或聯絡技術支援。

StorageGRID 金鑰管理伺服器和應用裝置組態

在使用金鑰管理伺服器 (KMS) 保護應用裝置節點上的 StorageGRID 資料之前，您必須完成兩個組態任務：設定一個或多個 KMS 伺服器，並為應用裝置節點啟用節點加密。完成這兩項組態任務後，金鑰管理程序將自動進行。

此流程圖顯示使用 KMS 保護應用裝置節點上 StorageGRID 資料的高階步驟。



流程圖顯示 KMS 設定和應用裝置設定並行進行；但是，您可以根據需求，在為新應用裝置節點啟用節點加密之

前或之後設定金鑰管理伺服器。

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟	請參閱
存取 KMS 軟體，並在每個 KMS 或 KMS 叢集中新增 StorageGRID 用戶端。	"在 KMS 中將 StorageGRID 設定為用戶端"
取得 KMS 上 StorageGRID 用戶端所需的資訊。	"在 KMS 中將 StorageGRID 設定為用戶端"
將 KMS 新增至 Grid Manager，將其指派給單一網站或預設網站群組，上傳所需的憑證，然後儲存 KMS 組態。	"${post_edited_translations.segment}"

設定應用裝置

設定用於 KMS 的應用裝置節點包括以下高階步驟。

1. 在應用裝置安裝的硬體組態階段，使用 StorageGRID Appliance Installer 為應用裝置啟用 節點加密 設定。

   將應用裝置新增至網格後，您無法啟用「節點加密」設定；對於未啟用節點加密的應用裝置，您也無法使用外部金鑰管理。

2. 執行 StorageGRID Appliance Installer。安裝過程中，將為每個應用裝置 Volume 指派一個隨機資料加密金鑰 （DEK），如下所示：
   - DEK 用於加密每個 Volume 上的資料。這些金鑰是使用應用裝置作業系統中的 Linux Unified Key Setup （LUKS） 磁碟加密產生的，且無法變更。
   - 每個 DEK 都由一個主金鑰加密金鑰 （KEK） 加密。初始 KEK 是一個臨時金鑰，用於加密 DEK，直到應用裝置能夠連接到 KMS。
3. 將應用裝置節點新增至 StorageGRID。

如需詳細資訊，請參閱 "啟用節點加密"。

金鑰管理加密過程（自動進行）

金鑰管理加密包括以下自動執行的高階步驟。

1. 當您將啟用了節點加密的應用裝置安裝到網格中時，StorageGRID 會決定包含新節點的站台是否存在 KMS 組態。
   - 如果網站已設定 KMS，應用裝置將接收 KMS 組態。
   - 如果網站尚未設定 KMS，應用裝置上的資料將繼續由臨時 KEK 加密，直到您為網站設定 KMS 並且應用裝置收到 KMS 組態為止。
2. 該應用裝置使用 KMS 組態連接到 KMS 並請求加密金鑰。
3. KMS 向應用裝置發送加密金鑰。KMS 發送的新金鑰取代了臨時 KEK，現在用於加密和解密應用裝置磁碟區

的 DEK。

> 在加密應用裝置節點連接到已設定的 KMS 之前存在的任何資料都會使用臨時金鑰進行加密。但是，在臨時金鑰被 KMS 加密金鑰取代之前，不應認為應用裝置磁碟區已受到保護而免於從資料中心移除。

4. 如果應用裝置通電或重新開機，它會重新連接到 KMS 以請求金鑰。金鑰儲存在揮發性記憶體容量中，無法在斷電或重新開機後保留。

StorageGRID 金鑰管理伺服器需求和注意事項

${post_edited_translations.segment}

支援哪個版本的 **KMIP**？

${post_edited_translations.segment}

"${post_edited_translations.segment}"

${post_edited_translations.segment}

網路防火牆設定必須允許每個應用裝置節點透過用於金鑰管理互作業協定 （KMIP） 通訊的連接埠進行通訊。

${post_edited_translations.segment}

${post_edited_translations.segment}

應用裝置節點與已設定的 KMS 之間的通訊使用安全的 TLS 連線。StorageGRID 在與 KMS 或 KMS 叢集建立 KMIP 連線時，可根據 KMS 支援的協定以及"${post_edited_translations.segment}"您所使用的協定，支援 TLS 1.2 或 TLS 1.3 協定。

StorageGRID 在建立連線時會與 KMS 協商協定和密碼（TLS 1.2）或密碼套件（TLS 1.3）。若要查看可用的協定版本和密碼/密碼套件，請審查網格的使用中 TLS 和 SSH 原則的 `tlsOutbound`部分（組態 > 安全性 安全性設定）。

${post_edited_translations.segment}

您可以使用金鑰管理伺服器 (KMS) 來管理網格中任何已啟用 **Node Encryption** 設定的 StorageGRID 應用裝置的加密金鑰。此設定只能在應用裝置安裝的硬體組態階段使用 StorageGRID Appliance Installer 啟用。

> ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

- 以虛擬機器 (VM) 形式部署的節點
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

對於全新安裝，通常應在建立租用戶之前，先在 Grid Manager 中設定一個或多個金鑰管理伺服器。此順序可確保在將任何物件資料儲存到節點之前，節點已受到保護。

${post_edited_translations.segment}

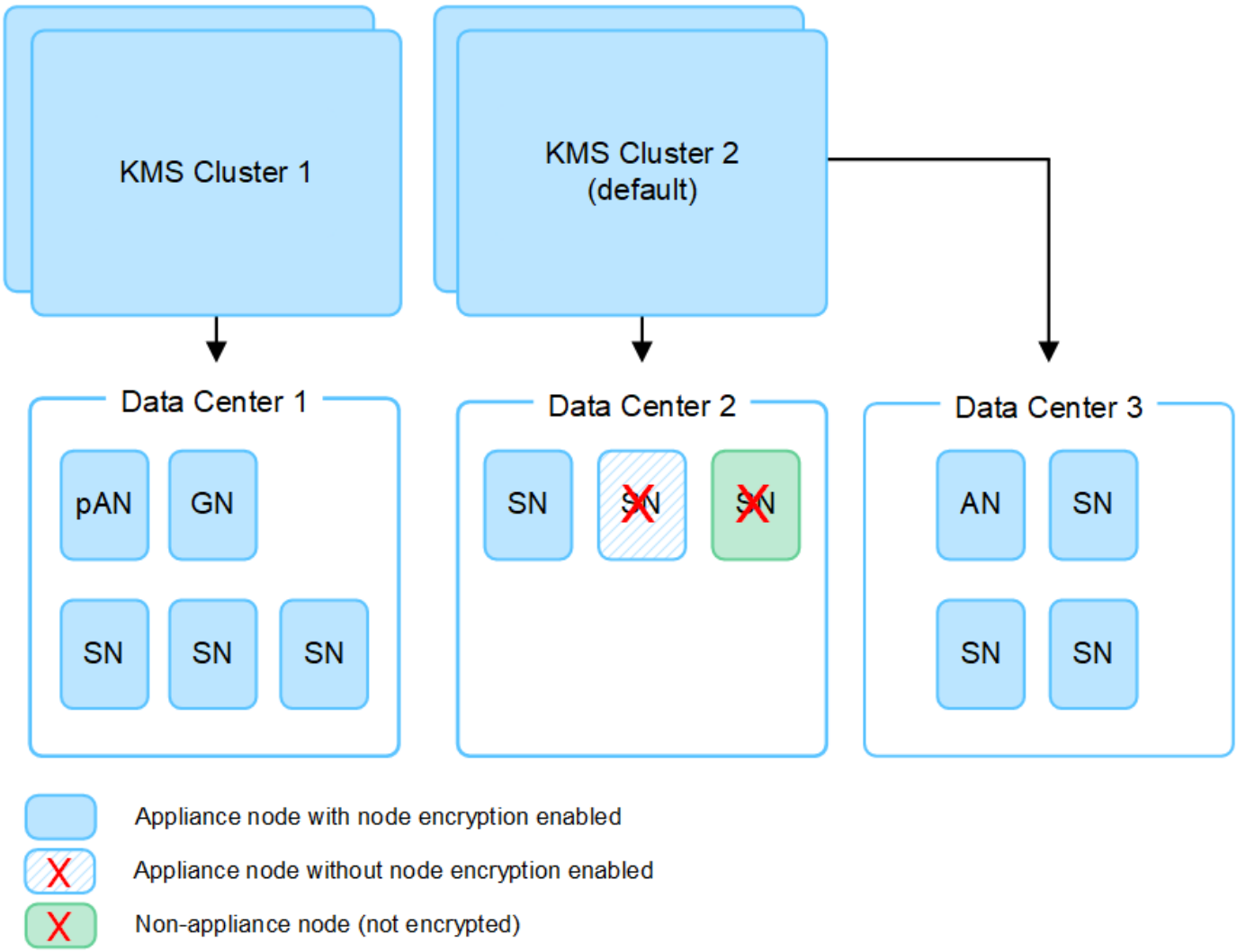
${post_edited_translations.segment}

您可以設定一個或多個外部金鑰管理伺服器，為 StorageGRID 系統中的應用裝置節點提供加密金鑰。每個 KMS 為單一站台或站台群組內的 StorageGRID 應用裝置節點提供單一加密金鑰。

StorageGRID 支援使用 KMS 叢集。每個 KMS 叢集包含多個複製的金鑰管理伺服器，這些伺服器共用組態設定和加密金鑰。建議使用 KMS 叢集進行金鑰管理，因為它能提高高可用度組態的故障轉移能力。

例如，假設您的 StorageGRID 系統有三個資料中心站台。您可以設定一個 KMS 叢集，為資料中心 1 的所有應用裝置節點提供金鑰，並設定第二個 KMS 叢集，為所有其他站台的所有應用裝置節點提供金鑰。當您新增第二個 KMS 叢集時，可以為資料中心 2 和資料中心 3 設定預設 KMS。

請注意，KMS 不能用於非應用裝置節點，也不能用於安裝期間未啟用 **Node Encryption** 設定的任何應用裝置節點。



金鑰輪替時會發生什麼事？

作為一項安全性最佳實務做法，您應該定期"輪換加密金鑰"每個已設定的 KMS。

新加密金鑰版本可用時：

- 金鑰會自動分發到與 KMS 關聯的一個或多個站台上的加密應用裝置節點。分發應在金鑰輪換後一小時內完成。
- 如果加密應用裝置節點在發佈新金鑰版本時處於離線狀態，該節點將在重新開機後立即收到新金鑰。
- 如果因任何原因而無法使用新的金鑰版本來加密應用裝置磁碟區，則會針對該應用裝置節點觸發 **KMS** 加密金鑰輪替失敗 警示。您可能需要聯絡技術支援以協助解決此警示。

應用裝置節點加密後可以重複使用嗎？

如果您需要將加密的應用裝置安裝到另一個 StorageGRID 系統中，您必須先將該網格節點退役，以便將物件資料移至另一個節點。然後，您可以使用 StorageGRID 應用裝置安裝程式來"${post_edited_translations.segment}"。清除 KMS 組態會停用 節點加密 設定，並移除應用裝置節點與 StorageGRID 站台之 KMS 組態之間的關聯。

${post_edited_translations.segment}

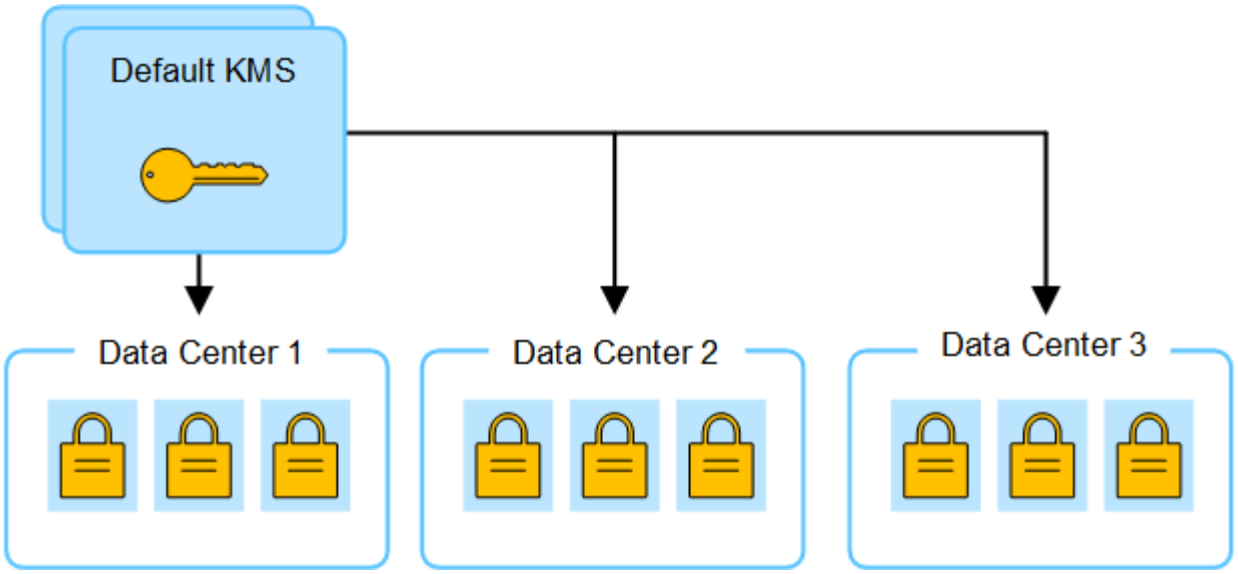
變更 **StorageGRID** 站台的 **KMS** 時的注意事項

每個金鑰管理伺服器 （KMS） 或 KMS 叢集都會向單一站台或一組站台的所有應用裝置節點提供加密金鑰。如果您需要變更站台所使用的 KMS，您可能需要將加密金鑰從一個 KMS 複製到另一個 KMS。

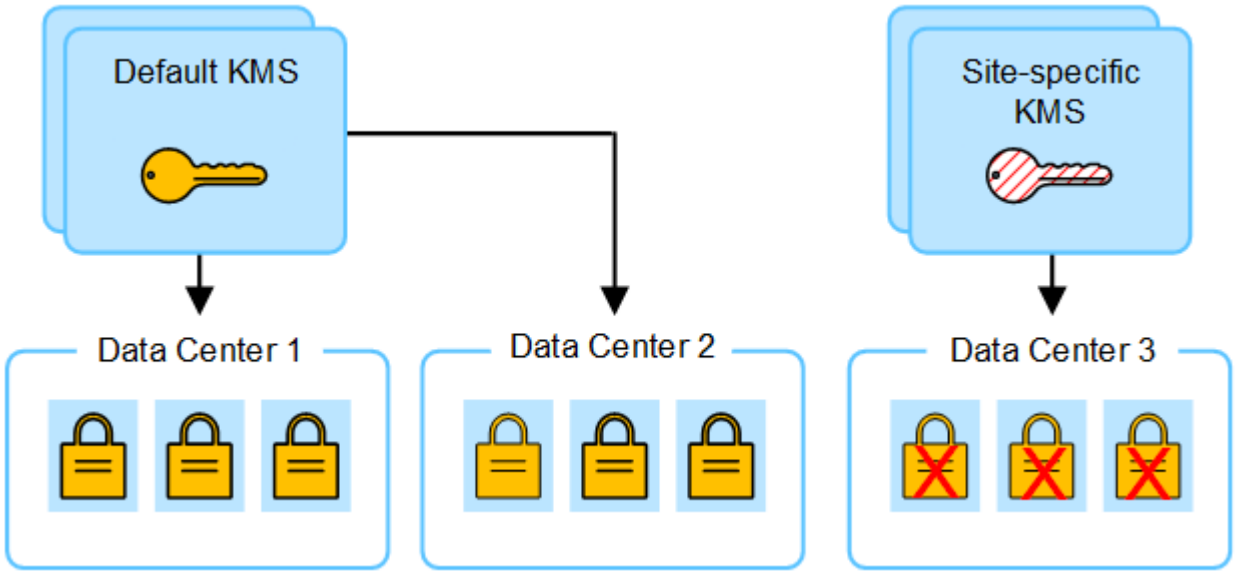
如果變更網站使用的金鑰管理系統 (KMS)，則必須確保可以使用儲存在新 KMS 上的金鑰解密該網站上先前加密的應用裝置節點。在某些情況下，您可能需要將目前版本的加密金鑰從原始 KMS 複製到新的 KMS。您必須確保 KMS 擁有正確的金鑰，以便解密該網站上加密的應用裝置節點。

例如：

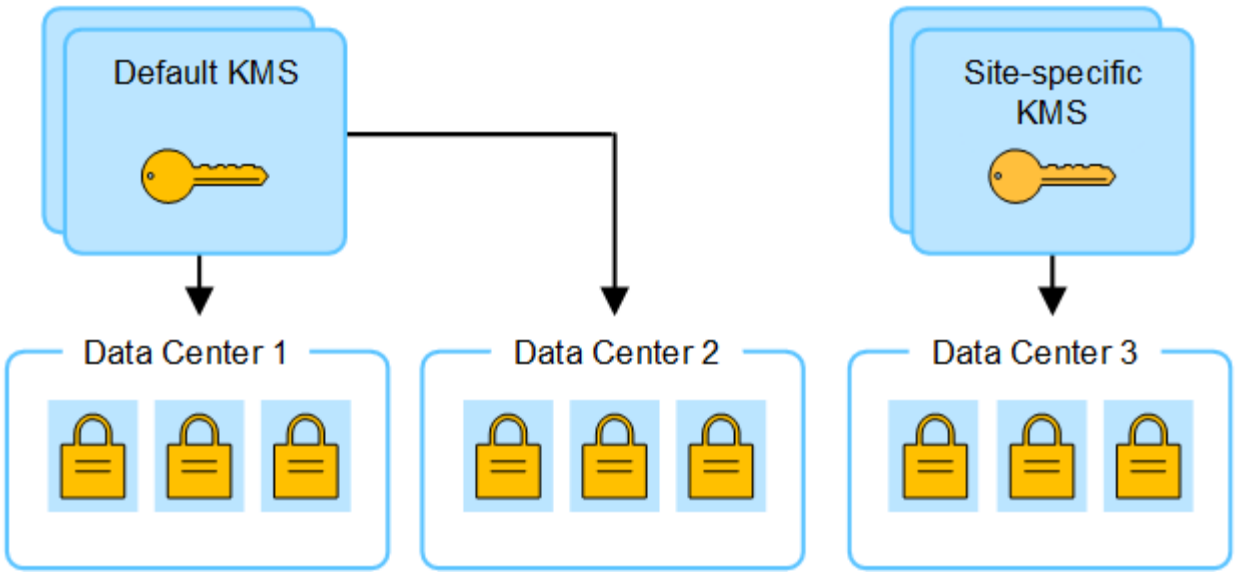
1. 首先，您設定一個預設的 KMS，該 KMS 適用於所有沒有專用 KMS 的站台。
2. 儲存 KMS 後，所有啟用了「節點加密」設定的應用裝置節點都會連接到 KMS 並要求加密金鑰。此金鑰用於加密所有站台上的應用裝置節點。解密這些應用裝置也必須使用此金鑰。



3. 您決定為某個站台（圖中的 Data Center 3）新增一個站台特定的 KMS。但是，由於應用裝置節點已加密，因此在嘗試儲存站台特定 KMS 的組態時會發生驗證錯誤。出現此錯誤的原因是站台特定 KMS 沒有解密該站台節點的正確金鑰。



4. 若要解決此問題，您可以將目前的加密金鑰版本從預設 KMS 複製到新的 KMS。（技術上而言，您是將原始金鑰複製到具有相同別名的新金鑰。原始金鑰會成為新金鑰的先前版本。）特定站台的 KMS 現在具有正確的金鑰來解密 Data Center 3 的應用裝置節點，因此可以將其儲存在 StorageGRID 中。



變更網站所使用 **KMS** 的使用案例

${post_edited_translations.segment}

變更站台 **KMS** 的使用案例	**${post_edited_translations.segment}**
${post_edited_translations.segment}	編輯站台專屬的 KMS。在 **Manages keys for** 欄位中，選取 **Sites not managed by another KMS (default KMS)**。站台專屬的 KMS 現在將作為預設 KMS 使用。它將套用至任何沒有專用 KMS 的站台。 "${post_edited_translations.segment}"
您擁有預設的 KMS ，且您在擴充中新增了新的站台。您不想對新站台使用預設的 KMS 。	1. ${post_edited_translations.segment} 2. ${post_edited_translations.segment} "${post_edited_translations.segment}"
您希望網站的 KMS 使用不同的伺服器。	1. 如果網站上的應用裝置節點已由現有 KMS 加密，請使用 KMS 軟體將目前版本的加密金鑰從現有 KMS 複製到新的 KMS。 2. 使用 Grid Manager，編輯現有的 KMS 組態，並輸入新的主機名稱或 IP 位址。 "${post_edited_translations.segment}"

在 **KMS** 中將 **StorageGRID** 設定為用戶端

在將 KMS 新增至 StorageGRID 之前，必須將 StorageGRID 設定為每個外部金鑰管理伺服器或 KMS 叢集的用戶端。

這些說明適用於 Thales CipherTrust Manager 和 Hashicorp Vault。有關支援的產品和版本清單，請使用 "NetApp 互作業性矩陣工具（IMT）"。

步驟

1. 從 KMS 軟體中，為計畫使用的每個 KMS 或 KMS 叢集建立一個 StorageGRID 用戶端。

   每個 KMS 管理單一站台或一組站台中 StorageGRID 應用裝置節點的單一加密金鑰。

2. 使用以下兩種方法之一建立金鑰：

   - 使用 KMS 產品的金鑰管理頁面。為每個 KMS 或 KMS 叢集建立一個 AES 加密金鑰。

     加密金鑰必須至少為 2,048 位元，且必須是可匯出的。

   - 讓 StorageGRID 建立金鑰。在 "上傳用戶端憑證" 之後測試並儲存時，系統會提示您。

3. 記錄每個 KMS 或 KMS 叢集的以下資訊。

   將 KMS 新增至 StorageGRID 時，您需要以下資訊：

   - 每台伺服器的主機名稱或 IP 位址。
   - KMS 使用的 KMIP 連接埠。
   - KMS 中加密金鑰的金鑰別名。

4. 對於每個 KMS 或 KMS 叢集，取得由憑證授權單位 （CA） 簽署的伺服器憑證，或取得包含每個 PEM 編碼的 CA 憑證檔案（按憑證鏈順序串連）的憑證套裝組合。

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     > 在 StorageGRID 中設定 KMS 時，必須在 主機名稱 欄位中輸入相同的 FQDN 或 IP 位址。

   - 伺服器憑證必須與 KMS 的 KMIP 介面使用的憑證相符，該介面通常使用連接埠 5696。

5. ${post_edited_translations.segment}

   用戶端憑證允許 StorageGRID 向 KMS 進行驗證。

在 **StorageGRID** 中新增金鑰管理伺服器

您可以使用 StorageGRID 金鑰管理伺服器精靈來新增每個 KMS 或 KMS 叢集。

開始之前

- 您已審閱 "${post_edited_translations.segment}"。
- 您已"在 KMS 中將 StorageGRID 設定為用戶端"，且擁有每個 KMS 或 KMS 叢集所需的資訊。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

關於此任務

如果可能，請在設定適用於所有未由其他 KMS 管理的站台的預設 KMS 之前，先設定任何站台專屬的金鑰管理

伺服器。如果您先建立預設 KMS，則網格中所有節點加密的應用裝置都將由預設 KMS 加密。如果您稍後想要建立站台專屬的 KMS，則必須先將目前版本的加密金鑰從預設 KMS 複製到新的 KMS。如需詳細資訊，請參閱 "更改網站 KMS 的注意事項"。

步驟 1：KMS 詳細資料

在「新增金鑰管理伺服器」精靈的步驟 1（KMS 詳細資料）中，您可以提供有關 KMS 或 KMS 叢集的詳細資訊。

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。

   金鑰管理伺服器頁面隨即顯示，並已選取「組態詳細資料」索引標籤。

2. 選擇 **Create** 。

   「新增金鑰管理伺服器」精靈的步驟 1（KMS 詳細資料）隨即出現。

3. 請輸入您在 KMS 中設定的 KMS 和 StorageGRID 用戶端的以下資訊。

欄位	說明
KMS 名稱	用於協助您識別此 KMS 的描述性名稱。長度必須介於 1 到 64 個字元之間。
金鑰名稱	KMS 中 StorageGRID 用戶端的確切金鑰別名。長度必須介於 1 到 255 個字元之間。 注意：如果您尚未使用 KMS 產品建立金鑰，系統將提示您讓 StorageGRID 建立金鑰。
${post_edited_translations.segment}	將與此 KMS 關聯的 StorageGRID 站台。如果可能，您應在設定適用於所有未由其他 KMS 管理之站台的預設 KMS 之前，先設定任何特定站台的金鑰管理伺服器。 • 如果此 KMS 將管理特定網站上應用裝置節點的加密金鑰，請選擇該網站。 • 選擇「未由其他 KMS 管理的網站（預設 KMS）」以設定預設 KMS，該預設 KMS 將套用於任何沒有專用 KMS 的網站以及您在後續擴充中新增的任何網站。 注意： 如果您選擇了先前由預設 KMS 加密的站台，但未向新 KMS 提供原始加密金鑰的目前版本，則在儲存 KMS 組態時將發生驗證錯誤。
連接埠	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設值為 5696，這是 KMIP 標準連接埠。

欄位	說明
主機名稱	KMS 的完整網域名稱或 IP 位址。 • 附註：* 伺服器憑證的主體替代名稱 （SAN） 欄位必須包含您在此處輸入的 FQDN 或 IP 位址。否則， StorageGRID 將無法連線至 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在設定 KMS 叢集，請選擇 新增另一個主機名稱 為叢集中的每個伺服器新增主機名稱。
5. 選擇 **Continue** 。

步驟 **2**：上傳伺服器憑證

在「新增金鑰管理伺服器」精靈的步驟 2（上傳伺服器憑證）中，您需要上傳 KMS 的伺服器憑證（或憑證套裝組合）。伺服器憑證允許外部 KMS 向 StorageGRID 進行驗證。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   伺服器憑證中繼資料隨即顯示。

   如果您上傳了憑證套裝組合，則每個憑證的中繼資料將顯示在各自的標籤頁中。

3. 選擇 **Continue** 。

${post_edited_translations.segment}

在「新增金鑰管理伺服器」精靈的步驟 3 （ 上傳用戶端憑證 ） 中，您要上傳用戶端憑證和用戶端憑證私有金鑰。用戶端憑證可讓 StorageGRID 向 KMS 進行自我驗證。

步驟

1. ${post_edited_translations.segment}
2. 上傳用戶端憑證檔案。

   用戶端憑證中繼資料隨即顯示。

3. 瀏覽至用戶端憑證私密金鑰所在的位置。
4. 上傳私鑰檔案。
5. 選擇 **Test and save**。

   如果金鑰不存在，系統會提示您讓 StorageGRID 建立一個金鑰。

   金鑰管理伺服器與應用裝置節點之間的連線已完成測試。如果所有連線均有效，並且在 KMS 中找到正確的加密金鑰，則新的金鑰管理伺服器將新增至「金鑰管理伺服器」頁面上的表格中。

新增 KMS 後，金鑰管理伺服器頁面上的憑證狀態會立即顯示為「未知」。StorageGRID 可能需要長達 30 分鐘才能取得每個憑證的實際狀態。您必須重新整理網頁瀏覽器才能查看目前狀態。

6. 如果在選取 **Test and save** 時出現錯誤訊息，請審查訊息詳細資料，然後選取 **OK**。

   例如，如果連線測試失敗，您可能會收到 422：Unprocessable Entity 錯誤。

7. 如果您需要在不測試外部連線的情況下儲存目前組態，請選擇「強制儲存」。

   選擇「強制儲存」會儲存 KMS 組態，但不會測試每個應用裝置到該 KMS 的外部連線。如果組態有問題，您可能無法重新開機受影響網站上已啟用節點加密的應用裝置節點。在問題解決之前，您可能無法存取您的資料。

8. 審查確認警告，如果您確定要強制儲存組態，請選擇「確定」。

   KMS 組態已儲存，但與 KMS 的連線尚未測試。

在 **StorageGRID** 中管理金鑰管理伺服器

管理金鑰管理伺服器 (KMS) 包括檢視或編輯詳細資訊、管理憑證、檢視加密節點，以及在不再需要時移除 KMS。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"所需存取權限"。

檢視 **KMS** 詳細資料

${post_edited_translations.segment}

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - 「加密節點」標籤列出所有已啟用節點加密的節點。

2. 若要檢視特定 KMS 的詳細資料並對該 KMS 執行作業，請選取該 KMS 的名稱。該 KMS 的詳細資料頁面會列出下列資訊：

欄位	說明
${post_edited_translations.segment}	${post_edited_translations.segment} ${post_edited_translations.segment}

欄位	說明
主機名稱	${post_edited_translations.segment} 如果存在由兩個金鑰管理伺服器組成的叢集，則會列出這兩個伺服器的完整網域或 IP 位址。如果叢集中有兩個以上的金鑰管理伺服器，則會列出第一個 KMS 的完整網域或 IP 位址，以及叢集中其他金鑰管理伺服器的數量。 例如： `10.10.10.10 and 10.10.10.11` 或 `10.10.10.10 and 2 others`。 ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

標籤頁	欄位	說明
${post_edited_translations.segment}	金鑰名稱	${post_edited_translations.segment}
${post_edited_translations.segment}	最新版本金鑰的唯一識別碼。	${post_edited_translations.segment}
金鑰最新版本的日期和時間。	伺服器憑證	${post_edited_translations.segment}
憑證的中繼資料，例如序號、到期日期和時間，以及憑證 PEM。	憑證 PEM	憑證的 PEM （隱私增強郵件）檔案的內容。
用戶端憑證	${post_edited_translations.segment}	憑證的中繼資料，例如序號、到期日期和時間，以及憑證 PEM。

4. 根據貴組織的安全性實務需要，選擇 **Rotate key** 或使用 KMS 軟體建立新版本的金鑰。

金鑰輪換成功後，金鑰 UID 和上次修改時間欄位將會更新。

如果您使用 KMS 軟體輪換加密金鑰，請將其從上次使用的金鑰版本輪換為相同金鑰的新版本。請勿輪換為完全不同的金鑰。

切勿嘗試透過變更 KMS 的金鑰名稱（別名）來輪替金鑰。StorageGRID 需要能使用相同的金鑰別名從 KMS 存取所有先前使用的金鑰版本（以及任何未來的金鑰版本）。如果您變更已設定 KMS 的金鑰別名，StorageGRID 可能會無法解密您的資料。

管理憑證

及時解決任何伺服器或用戶端憑證問題。如果可能，請在憑證過期前更換。

${post_edited_translations.segment}

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。
2. 在表格中，查看每個 KMS 的憑證到期值。
3. ${post_edited_translations.segment}
4. 如果「憑證到期」欄位顯示憑證已過期或即將過期，請選擇 KMS 以前往 KMS 詳細資料頁面。
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. 重複這些子步驟，並選擇「用戶端憑證」而不是「伺服器憑證」。
5. ${post_edited_translations.segment}

   StorageGRID 可能需要長達 30 分鐘才能更新憑證到期資訊。請重新整理網頁瀏覽器以查看目前值。

${post_edited_translations.segment}

${post_edited_translations.segment}

您可以檢視 StorageGRID 系統中已啟用 節點加密 設定的應用裝置節點的相關資訊。

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。

   此時將顯示「金鑰管理伺服器」頁面。「組態詳細資料」標籤顯示所有已設定的金鑰管理伺服器。

2. 從頁面頂部選擇*加密節點*索引標籤。

   「加密節點」標籤列出了 StorageGRID 系統中啟用了「節點加密」設定的應用裝置節點。

3. 審查表格中每個應用裝置節點的資訊。

欄	說明
節點名稱	應用裝置節點的名稱。
節點類型	節點類型：儲存、管理或閘道。
地點	節點所在的 StorageGRID 站點名稱。
KMS 名稱	用於節點的 KMS 描述性名稱。 如果沒有列出 KMS，請選擇「組態詳細資料」標籤新增 KMS。 "${post_edited_translations.segment}"

欄	說明
${post_edited_translations.segment}	用於加密和解密應用裝置節點上資料的加密金鑰的唯一 ID。若要檢視完整的金鑰 UID，請選擇該文字。 短橫線 (--) 表示金鑰 UID 未知，可能是由於應用裝置節點和 KMS 之間的連線問題。
狀態	KMS 與應用裝置節點之間的連線狀態。如果節點已連接，時間戳記每 30 分鐘更新一次。KMS 組態變更後，連線狀態可能需要幾分鐘才能更新。 ${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   在 KMS 正常運作期間，狀態將顯示為「已連線至 KMS」。如果節點與網格中斷連線，則會顯示節點連線狀態（管理性故障或未知）。

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - KMS 金鑰無法解密應用裝置 Volume
   - KMS 未設定

   ${post_edited_translations.segment}

   ${post_edited_translations.segment}

編輯 **KMS**

例如，如果憑證即將過期，您可能需要編輯金鑰管理伺服器的組態。

開始之前

- 如果您計劃更新為 KMS 選擇的站台，您已審查過"${post_edited_translations.segment}"。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。

   金鑰管理伺服器頁面隨即出現，並顯示所有已設定的金鑰管理伺服器。

2. 選擇要編輯的 KMS，然後選擇 **Actions** > **Edit**。

   您也可以透過在表格中選擇 KMS 名稱，然後在 KMS 詳細資料頁面上選擇「編輯」來編輯 KMS。

3. （可選）在「編輯金鑰管理伺服器」精靈的「步驟 1 （KMS 詳細資料）」中更新詳細資訊。

欄位	說明
KMS 名稱	用於協助您識別此 KMS 的描述性名稱。長度必須介於 1 到 64 個字元之間。
金鑰名稱	KMS 中 StorageGRID 用戶端的確切金鑰別名。長度必須介於 1 到 255 個字元之間。 只有在極少數情況下才需要編輯金鑰名稱。例如，如果 KMS 中的別名被重新命名，或者先前金鑰的所有版本都已複製到新別名的版本歷史記錄中，則必須編輯金鑰名稱。
${post_edited_translations.segment}	如果您正在編輯網站特定的 KMS，且尚未設定預設 KMS，您可以選擇「未由其他 KMS 管理的網站（預設 KMS）」選項。此選項會將網站特定的 KMS 轉換為預設 KMS，該預設 KMS 將套用於所有沒有專用 KMS 的網站以及在擴充功能中新增的任何網站。 附註： 如果您正在編輯特定站台的 KMS，則無法選取其他站台。如果您正在編輯預設 KMS，則無法選取特定站台。
連接埠	KMS 伺服器用於金鑰管理互通協定 (KMIP) 通訊的連接埠。預設值為 5696，這是 KMIP 標準連接埠。
主機名稱	KMS 的完整網域名稱或 IP 位址。 • 附註：* 伺服器憑證的主體替代名稱 （SAN） 欄位必須包含您在此處輸入的 FQDN 或 IP 位址。否則， StorageGRID 將無法連線至 KMS 或 KMS 叢集中的所有伺服器。

4. 如果您正在設定 KMS 叢集，請選擇 新增另一個主機名稱 為叢集中的每個伺服器新增主機名稱。
5. 選擇 **Continue** 。

   編輯金鑰管理伺服器精靈的第 2 步（上傳伺服器憑證）出現。

6. ${post_edited_translations.segment}
7. 選擇 **Continue** 。

   編輯金鑰管理伺服器精靈的步驟 3（上傳用戶端憑證）出現。

8. 如果需要替換用戶端憑證和用戶端憑證私鑰，請選擇 **Browse** 並上傳新檔案。
9. 選擇 **Test and save**。

   系統會測試金鑰管理伺服器與受影響站台的所有節點加密應用裝置節點之間的連線。如果所有節點連線均有效，且在 KMS 上找到正確的金鑰，則金鑰管理伺服器會新增至「金鑰管理伺服器」頁面上的表格中。

10. 如果出現錯誤訊息，請審查訊息詳細資料，然後選擇 **OK**。

    例如，如果您為此 KMS 選擇的網站已由另一個 KMS 管理，或連線測試失敗，則可能會收到 422:

Unprocessable Entity 錯誤。

11. 如果在解決連線錯誤之前需要儲存目前組態，請選擇「強制儲存」。

> 選擇「強制儲存」會儲存 KMS 組態，但不會測試每個應用裝置到該 KMS 的外部連線。如果組態有問題，您可能無法重新開機受影響網站上已啟用節點加密的應用裝置節點。在問題解決之前，您可能無法存取您的資料。

KMS 組態已儲存。

12. 審查確認警告，如果您確定要強制儲存組態，請選擇「確定」。

${post_edited_translations.segment}

${post_edited_translations.segment}

在某些情況下，您可能需要移除金鑰管理伺服器。例如，如果您已停用某個站台，則可能需要移除該站台特定的 KMS。

開始之前

- 您已審閱 "${post_edited_translations.segment}"。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

關於此任務

在以下情況下，您可以移除 KMS：

- ${post_edited_translations.segment}
- 如果每個站台都已存在特定於站台的 KMS，且每個站台都有啟用了節點加密的應用裝置節點，則可以移除預設 KMS。

步驟

1. 選擇 組態 > 安全性 > 金鑰管理伺服器。

金鑰管理伺服器頁面隨即出現，並顯示所有已設定的金鑰管理伺服器。

2. 選擇要移除的 KMS，然後選擇 **Actions** > **Remove**。

${post_edited_translations.segment}

3. ${post_edited_translations.segment}
   - 您正在移除一個網站特定的 KMS，該網站沒有啟用節點加密的應用裝置節點。
   - ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

KMS 組態已移除。

${post_edited_translations.segment}

配置 **StorageGRID** 儲存代理

如果您使用平台服務或雲端儲存池，則可以在儲存節點和外部 S3 端點之間設定非透明 Proxy。例如，您可能需要非透明 Proxy 來允許平台服務訊息傳送到外部端點，例如網際網路上的端點。

${post_edited_translations.segment}

開始之前

- 您有"特定存取權限"。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

您可以設定單一儲存設備 Proxy 的設定。

步驟

1. 選取 **Configuration** > **Security** > **Proxy settings**。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 輸入 Proxy 伺服器的主機名稱或 IP 位址。
5. （可選）輸入用於連線至 Proxy 伺服器的連接埠。

   ${post_edited_translations.segment}

6. 選取 **Save** 。

   儲存設備 Proxy 儲存後，即可設定和測試平台服務或雲端儲存池的新端點。

   Proxy 變更最多可能需要 10 分鐘才能生效。

7. 檢查 Proxy 伺服器的設定，確保來自 StorageGRID 的平台服務相關訊息不會被封鎖。
8. 如果需要停用儲存設備 Proxy，請清除核取方塊，然後選擇 儲存。

在 **StorageGRID** 中設定管理 **Proxy** 設定

如果您使用 HTTP 或 HTTPS 傳送 AutoSupport 套件，則可以在管理節點與技術支援之間設定非透明 Proxy 伺服器（AutoSupport）。

如需更多關於 AutoSupport 的資訊，請參閱 "設定 AutoSupport"。

開始之前

- 您有"特定存取權限"。
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

關於此任務

您可以為單一管理 Proxy 設定組態。

步驟

1. 選取 **Configuration** > **Security** > **Proxy settings**。

   此時會顯示「Proxy 設定」頁面。預設情況下，索引標籤選單中會選取「儲存」。

2. 選擇 **Admin** 索引標籤。
3. 選取 **Enable Admin Proxy** 核取方塊。
4. 輸入 Proxy 伺服器的主機名稱或 IP 位址。
5. 輸入用於連線至 Proxy 伺服器的連接埠。
6. （可選）輸入 Proxy 伺服器的使用者名稱和密碼。

   如果您的 Proxy 伺服器不需要使用者名稱或密碼，請將這些欄位留空。

7. 請選擇以下選項之一：

   - 如果要保護與管理 Proxy 的連線安全，請選擇「驗證 Proxy 憑證」。上傳 CA 憑證套裝組合以驗證管理 Proxy 伺服器提供的 SSL 憑證的真實性。

     AutoSupport on Demand、E 系列 AutoSupport through StorageGRID，以及 StorageGRID 升級頁面上的更新路徑判斷，在驗證 Proxy 憑證時將無法運作。

     上傳 CA 套裝組合後，其中繼資料就會顯示出來。

   - 如果您不想在與管理 Proxy 伺服器通訊時驗證憑證，請選擇「不驗證 **Proxy** 憑證」。

8. 選取 **Save** 。

   儲存管理 Proxy 後，即可設定管理節點與技術支援之間的 Proxy 伺服器。

   Proxy 變更最多可能需要 10 分鐘才能生效。

9. 如果需要停用管理員 Proxy，請清除「啟用管理員 Proxy」核取方塊，然後選取「儲存」。

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	**${post_edited_translations.segment}**
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。 ${post_edited_translations.segment}
8443	${post_edited_translations.segment}	• ${post_edited_translations.segment} • 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。 • ${post_edited_translations.segment}
9443	${post_edited_translations.segment}	• 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。 • ${post_edited_translations.segment}

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_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，敏感的連接埠和該連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_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_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_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。

${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}

> 變更用戶端網路組態時，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。

限制對網格外部 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格存取。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。

管理租戶

StorageGRID 中的租戶帳戶

租戶帳戶可讓您使用 Simple Storage Service （S3） REST API 在 StorageGRID 系統中儲存和擷取物件。

此版本的說明文件網站已移除 Swift 詳細資訊。請參閱 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

每個租戶帳戶都有聯合群組或本機群組、使用者、S3 儲存桶和物件。

租戶帳戶可用於依不同實體隔離儲存的物件。例如，多個租戶帳戶可用於下列任一使用案例：

- 企業使用案例： 如果您在企業應用程式中管理 StorageGRID 系統，您可能需要根據組織中的不同部門對網格的物件儲存進行隔離。在這種情況下，您可以為行銷部、客戶支援部、人力資源部等建立租戶帳戶。

如果您使用 S3 用戶端協定，可以使用 S3 儲存貯體和儲存貯體原則來隔離企業中各部門之間的物件。您不需要使用租戶帳戶。如需詳細資訊，請參閱實作 "S3 儲存桶和儲存桶原則" 的說明。

- 服務供應商使用案例： 如果您以服務供應商形式管理 StorageGRID 系統，您可以根據租用網格儲存設備的不同實體對網格的物件儲存進行隔離。在這種情況下，您需要為 A 公司、B 公司、C 公司等建立租戶帳戶。

如需詳細資訊，請參閱 "使用租戶帳戶"。

${post_edited_translations.segment}

使用 Grid 管理程式建立租戶帳戶。建立租戶帳戶時，您需要指定以下資訊：

- 基本資訊包括租戶名稱、用戶端類型（S3）和選用的儲存設備配額。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

此外，如果 S3 租戶帳戶需要符合法規要求，您可以為 StorageGRID 系統啟用 S3 物件鎖定設定。啟用 S3 物件鎖定後，所有 S3 租戶帳戶都可以建立和管理符合法規的儲存桶。

Tenant Manager 是用來做什麼的？

建立租戶帳戶後，租戶使用者可以登入 Tenant Manager 執行下列工作：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 使用網格聯合進行帳戶 Clone 和跨網格複寫
- ${post_edited_translations.segment}
- 建立和管理 S3 儲存桶
- ${post_edited_translations.segment}
- 使用 S3 Select
- 監控儲存設備使用情況

雖然 S3 租戶用戶可以使用 Tenant Manager 建立和管理 S3 存取金鑰和儲存桶，但他們必須使用 S3 用戶端應用程式來擷取和管理物件。如需詳細資訊，請參閱 "使用 S3 REST API"。

建立 **StorageGRID** 租用戶帳戶

${post_edited_translations.segment}

建立租戶帳戶的步驟取決於是否已設定 "${post_edited_translations.segment}" 與 "${post_edited_translations.segment}"，以及您用來建立租戶帳戶的 Grid Manager 帳戶是否屬於具有 root 存取權權限的管理群組。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

- 您擁有 "${post_edited_translations.segment}"。
- 如果租戶帳戶將使用為 Grid Manager 設定的識別來源，且您想要將租戶帳戶的 root 存取權權限授予同盟群組，則您已將該同盟群組匯入 Grid Manager。您不需要為此管理群組指派任何 Grid Manager 權限。請參閱 "${post_edited_translations.segment}"。
- 如果您希望允許 S3 租戶使用網格聯合連線將帳戶資料 Clone 並複寫儲存桶物件到另一個網格：
  - 您有"已設定網格同盟連線"。
  - 連線狀態為*已連線*。
  - 您擁有根目錄存取權限。
  - 您已審查 "${post_edited_translations.segment}" 的考量事項。
  - ${post_edited_translations.segment}

    ${post_edited_translations.segment}

    ${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 選擇*租戶*。
2. 選擇 **Create** 。

${post_edited_translations.segment}

步驟

1. 輸入租戶的詳細資料。

欄位	說明
Name	租戶帳戶的名稱。租戶名稱不需要是唯一的。建立租戶帳戶時，它會收到一個唯一的 20 位數帳戶 ID。
${post_edited_translations.segment}	${post_edited_translations.segment} 如果您要建立的租戶將使用網格聯合連線，您可以選擇使用此欄位來協助識別哪個是來源租戶，哪一個是目的地租戶。例如，在 Grid 1 上建立的租戶的以下執行摘要也會顯示在複寫到 Grid 2 的租戶中：「此租戶是在 Grid 1 上建立的。」
用戶端類型	必須是*S3*。
${post_edited_translations.segment}	${post_edited_translations.segment}

2. 選擇 **Continue** 。

選擇權限

步驟

1. （可選）選擇您希望此租戶擁有的基本權限。

   其中部分權限有其他額外需求。如需詳細資訊，請選取每個權限的說明圖示。

權限	**${post_edited_translations.segment}**
${post_edited_translations.segment}	租戶可以使用 S3 平台服務，例如 CloudMirror。請參閱 "管理 S3 租戶帳戶的平台服務"。
${post_edited_translations.segment}	租戶可以為同盟群組與使用者設定及管理自己的身分識別來源。如果您已為您的 StorageGRID 系統 "${post_edited_translations.segment}" ，則會停用此選項。
${post_edited_translations.segment}	租戶可以發出 S3 SelectObjectContent API 要求，以篩選並擷取物件資料。請參閱 "${post_edited_translations.segment}"。 重要提示：SelectObjectContent 請求可能會降低所有 S3 用戶端和租戶的負載平衡器效能。請僅在必要時啟用此功能，且僅對受信任的租戶啟用。

2. ${post_edited_translations.segment}

權限	**${post_edited_translations.segment}**
${post_edited_translations.segment}	${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment} 請參閱 "管理網格聯盟的允許租戶"。
S3 物件鎖定	${post_edited_translations.segment} • 設定最大保留期間 定義新增至此儲存桶的物件應保留多長時間，從物件被擷取時開始計算。 • *允許法規遵循模式*可防止使用者在保留期間覆寫或刪除受保護的物件版本。

3. 選擇 **Continue** 。

定義 **root** 存取權並建立租戶

步驟

1. ${post_edited_translations.segment}

選項	**${post_edited_translations.segment}**
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	a. 選取現有的聯合群組，使其擁有租戶的 root 存取權。 b. （可選）指定以本機 root 使用者身分登入租戶時要使用的密碼。
${post_edited_translations.segment}	選取現有的聯合群組，以取得租戶的 root 存取權限。本機使用者無法登入。

2. 選擇 **Create tenant**。

   系統將顯示成功訊息，新租戶將列在「租戶」頁面上。若要了解如何檢視租戶詳細資訊和監控租戶活動，請參閱"${post_edited_translations.segment}"。

   ${post_edited_translations.segment}

3. 如果您為租戶選擇了「使用網格聯合連線」權限：

   a. 確認已將完全相同的租戶複寫到連線中的另一個網格。兩個網格上的租戶將具有相同的 20 位數帳戶 ID、名稱、執行摘要、配額和權限。

      如果您看到「Tenant created without a clone」錯誤訊息，請參閱 "排除網格同盟錯誤" 中的說明。

   b. 如果您在定義 root 存取權時提供了本機 root 使用者密碼，"更改本機 root 使用者的密碼"適用於複製的租戶。

      ${post_edited_translations.segment}

登入租戶（選用）

根據需要，您可以立即登入新租戶以完成組態，也可以稍後登入租戶。登入步驟取決於您是使用預設連接埠 (443) 還是受限連接埠登入 Grid Manager。請參閱 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

如果您正在使用.....	**${post_edited_translations.segment}**
${post_edited_translations.segment}	1. 選擇 **Sign in as root**。 ${post_edited_translations.segment} 2. ${post_edited_translations.segment} 每個連結都會在 Tenant Manager 中開啟對應的頁面。若要完成此頁面，請參閱 "租戶帳戶使用說明"。

如果您正在使用.....	**${post_edited_translations.segment}**
連接埠 443，但您沒有為本機 root 使用者設定密碼。	選擇 **Sign in**，然後輸入 root 存取權聯合群組中使用者的憑證。
${post_edited_translations.segment}	1. 選擇 **Finish** 2. 在租戶表中選擇「受限」，以深入瞭解如何存取此租戶帳戶。 租戶管理員的 URL 格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 是 Admin Node 的完整網域名稱或 IP 位址 ◦ *port* 是僅限租戶使用的連接埠 ◦ *20-digit-account-id* 是租戶的唯一帳戶 ID

稍後登入

如果您正在使用.....	**${post_edited_translations.segment}**
${post_edited_translations.segment}	• ${post_edited_translations.segment} • ${post_edited_translations.segment} `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 是 Admin Node 的完整網域名稱或 IP 位址 ◦ *20-digit-account-id* 是租戶的唯一帳戶 ID
${post_edited_translations.segment}	• 從 Grid Manager 中選擇 * 租戶 *，然後選擇 * 受限 *。 • ${post_edited_translations.segment} `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* 是 Admin Node 的完整網域名稱或 IP 位址 ◦ *port* 是僅限租戶的受限連接埠 ◦ *20-digit-account-id* 是租戶的唯一帳戶 ID

${post_edited_translations.segment}

請遵循 "使用租戶帳戶" 中的說明來管理租戶群組與使用者、S3 存取金鑰、儲存貯體、平台服務，以及帳戶 Clone 與跨網格複寫。

編輯 StorageGRID 租用戶帳戶

您可以編輯租戶帳戶以變更顯示名稱、儲存設備配額或租戶權限。

如果租戶擁有「使用網格聯合連線」權限，則可以從連線中的任一網格編輯租戶詳細資料。但是，您在連線中的一個網格上所做的任何變更都不會複製到另一個網格。如果您希望保持網格之間的租戶詳細資料完全同步，請在兩個網格上進行相同的編輯。請參閱 "管理網格同盟連線的允許租戶"。

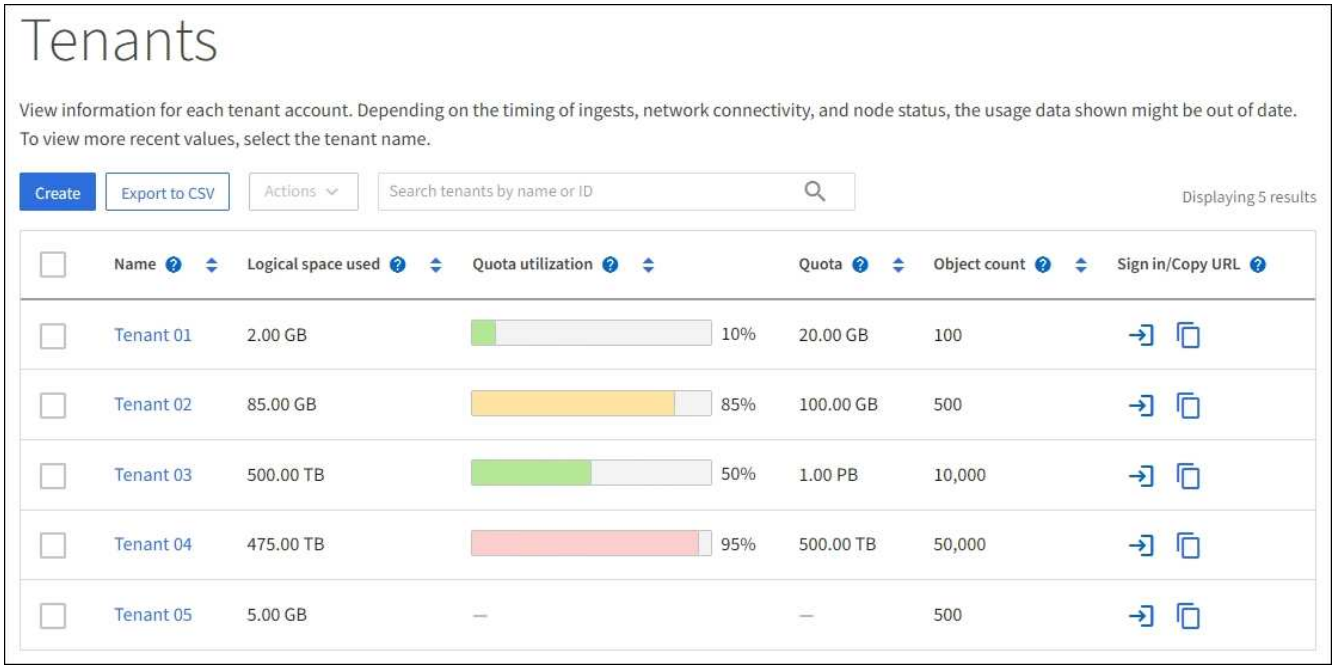
開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

步驟

1. 選擇*租戶*。



2. 尋找要編輯的租戶帳戶。

   使用搜尋框依名稱或租戶 ID 搜尋租戶。

3. 選擇租戶。您可以執行下列任一操作：
   - 選取租戶的核取方塊，然後選取 **Actions** > **Edit**。
   - 選擇租戶名稱以顯示詳細資訊頁面，然後選擇 **Edit**。
4. （可選）變更以下欄位的值：
   - 名稱
   - 說明

- 儲存配額

5. 選擇 **Continue** 。
6. 選擇或清除租戶帳戶的權限。
   - 如果您為正在使用平台服務的租戶停用這些服務，他們為其 S3 儲存桶所設定的服務將停止運作。系統不會向租戶發送任何錯誤訊息。例如，如果租戶已為某個 S3 儲存桶設定 CloudMirror 複寫，他們仍然可以在該儲存桶中儲存物件，但這些物件的複本將不再建立至他們設定為端點的外部 S3 儲存桶中。請參閱 "管理 S3 租戶帳戶的平台服務"。
   - 變更 **Use own identity source** 的設定，以確定租戶帳戶是使用自己的身分來源，還是為 Grid Manager 所設定的身分來源。

     如果*使用自有身分來源*為：

     - 已停用並選取，表示租戶已啟用其自身的身分來源。租戶必須先停用自身的身分來源，才能使用為 Grid Manager 設定的身分來源。
     - 已停用且未選取，StorageGRID 系統已啟用 SSO。租戶必須使用為 Grid Manager 設定的身分識別來源。
   - 根據需要選擇或清除「允許 S3 Select」權限。請參閱"${post_edited_translations.segment}"。
   - ${post_edited_translations.segment}
     i. 選擇 **Grid federation** 索引標籤。
     ii. 選擇 移除權限。
   - 新增「使用網格聯合連線」權限：
     i. 選擇 **Grid federation** 索引標籤。
     ii. 勾選 **Use grid federation connection** 核取方塊。
     iii. 您也可以選擇 **Clone existing local users and groups** 將其 Clone 到遠端網格。如果需要，您可以停止正在進行的 Clone 操作，或者在上次 Clone 操作完成後，如果某些本機使用者或群組 Clone 失敗，您可以重試 Clone。
   - 設定最長保留期間或啟用法規遵循模式：

     必須先在網格上啟用 S3 物件鎖定，才能使用這些設定。

     i. 選擇 **S3 Object Lock** 索引標籤。
     ii. 對於「設定最長保留期間」，請輸入一個值，然後從下拉式選單中選擇時間段。
     iii. 若要啟用「允許法規遵循模式」，請選取該核取方塊。

變更 StorageGRID 租戶本機 root 使用者的密碼

如果租戶的本機 root 使用者被鎖定而無法存取帳戶，您可能需要變更該 root 使用者的密碼。

開始之前

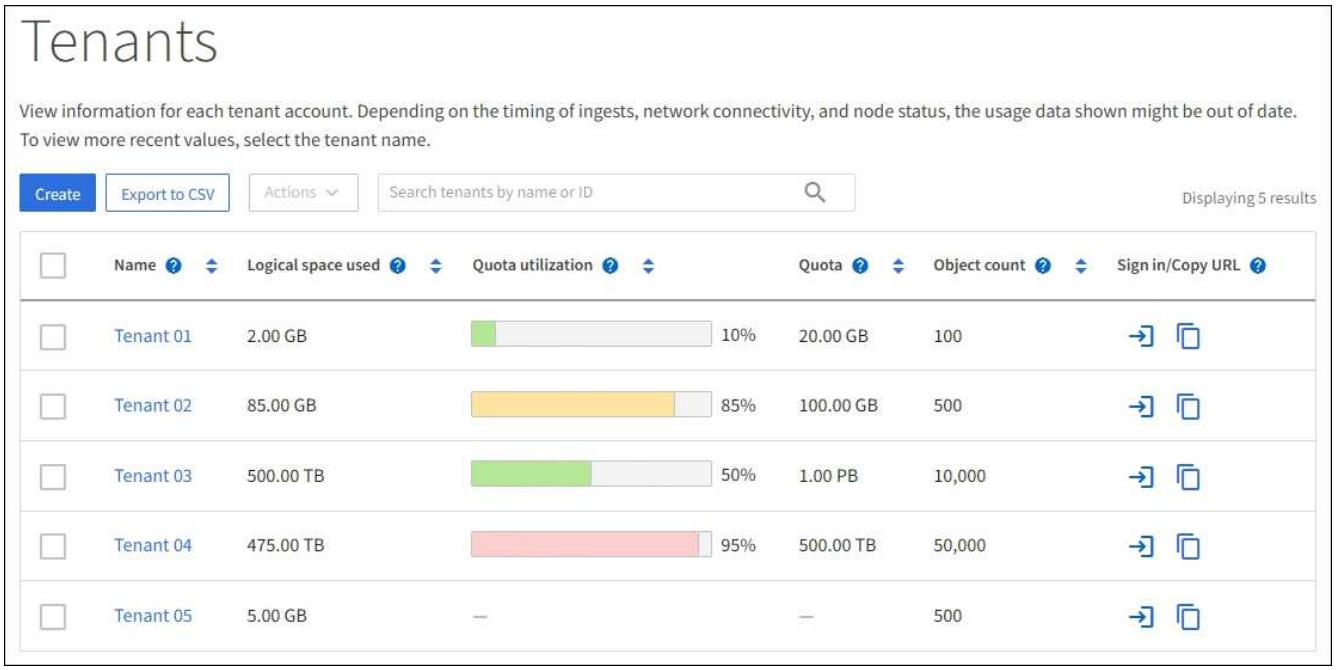
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"特定存取權限"。

關於此任務

如果您的 StorageGRID 系統啟用了單一登入 （SSO），則本機 root 使用者無法登入租戶帳戶。若要執行 root 使用者任務，使用者必須屬於具有租戶根目錄存取權限的聯合群組。

步驟

1. 選擇*租戶*。



2. 選擇租戶帳戶。您可以執行下列任一操作：
   - 選取租戶的核取方塊，然後選取 **Actions** > **Change root password**。
   - 選取租戶名稱以顯示詳細資料頁面，然後選取 **Actions** > **Change root password**。
3. 請輸入租戶帳戶的新密碼。
4. 選取 **Save** 。

刪除 StorageGRID 租用戶帳戶

如果您想要永久移除租戶對系統的存取，則可以刪除租戶帳戶。

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"。
- 您已移除與租戶帳戶相關聯的所有 S3 儲存桶和物件。
- 如果允許租戶使用網格同盟連線，您已審查 "刪除具有「使用網格聯合連線」權限的租戶" 的考量事項。

步驟

1. 選擇*租戶*。
2. 尋找要刪除的租戶帳戶。

使用搜尋框依名稱或租戶 ID 搜尋租戶。

3. 若要刪除多個租戶，請選取核取方塊，然後選取 **Actions** > **Delete**。
4. 若要刪除單一租戶，請執行下列任一操作：
   - 選取核取方塊，然後選取 **Actions** > **Delete**。
   - 選擇租戶名稱以顯示詳細資料頁面，然後選擇 **Actions** > **Delete**。
5. ${post_edited_translations.segment}

${post_edited_translations.segment}

了解 **StorageGRID** 平台服務

平台服務包括 CloudMirror 複寫、事件通知和搜尋整合服務。

如果為 S3 租戶帳戶啟用平台服務，則必須設定網格，以便租戶可以存取使用這些服務所需的外部資源。

平台服務不支援 "分支桶"。

CloudMirror 複寫

StorageGRID CloudMirror 複寫服務用於將 StorageGRID 儲存桶中的特定物件鏡射到指定的外部目的地。

例如，您可以使用 CloudMirror 複寫將特定客戶記錄鏡射到 Amazon S3，然後運用 AWS 服務對您的資料執行分析。

CloudMirror 複寫與跨網格複寫功能有一些重要的相似之處和不同之處。若要深入瞭解，請參閱 "比較跨網格複寫和 CloudMirror 複寫"。

CloudMirror 如果來源儲存桶已啟用 S3 Object Lock，則不支援複寫。

通知

${post_edited_translations.segment}

例如，您可以設定警示，以便在每個物件新增至儲存桶時向系統管理員傳送警示，其中物件代表與關鍵系統事件相關聯的日誌檔案。

${post_edited_translations.segment}

搜尋整合服務

搜尋整合服務用於將 S3 物件中繼資料傳送到指定的 Elasticsearch 索引，以便可以使用外部服務搜尋或分析中繼資料。

例如，您可以設定您的儲存貯體，將 S3 物件中繼資料傳送到遠端 Elasticsearch 服務。然後，您可以使用 Elasticsearch 跨儲存貯體進行搜尋，並對物件中繼資料中呈現的模式進行複雜的分析。

雖然可以在啟用 S3 物件鎖定的儲存桶上設定 Elasticsearch 整合，但物件的 S3 物件鎖定中繼資料（包括保留至日期和法律保留狀態）將不會包含在通知訊息中。

平台服務使租戶能夠利用外部儲存資源、通知服務以及搜尋或分析服務來處理其資料。由於平台服務的目標位置通常位於 StorageGRID 部署外部，因此您必須決定是否允許租戶使用這些服務。如果允許，則必須在建立或編輯租戶帳戶時啟用平台服務。您還必須設定網路，以確保租戶產生的平台服務訊息能夠到達其目的地。

關於使用平台服務的建議

在使用平台服務之前、請注意下列建議：

- 如果 StorageGRID 系統中的 S3 儲存桶同時啟用了版本控制和 CloudMirror 複寫，則也應為目的地端點啟用 S3 儲存桶版本控制。這樣可以確保 CloudMirror 複寫在端點上產生相似的物件版本。
- 對於需要 CloudMirror 複寫、通知和搜尋整合的 S3 請求，不應使用超過 100 個活躍租戶。超過 100 個活躍租戶可能會導致 S3 用戶端效能下降。
- 無法完成的端點請求將排入佇列，最多可排入 500,000 個請求。此限制由所有作用中租戶平均共享。新租戶可暫時超過此 500,000 的限制，以避免新建立的租戶受到不公平的懲罰。

相關資訊

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "監控 StorageGRID"

StorageGRID 平台服務的網路和連接埠

如果允許 S3 租戶使用平台服務，則必須設定網格的連網，以確保平台服務訊息能夠傳遞到其目的地。

建立或更新 S3 租戶帳戶時，您可以啟用該租戶帳戶的平台服務。啟用平台服務後，租戶可以建立端點，作為其 S3 儲存桶中 CloudMirror 複寫、事件通知或搜尋整合訊息的目的地。這些平台服務訊息由執行 ADC 服務的儲存節點傳送至目的地端點。

例如，租戶可以設定以下類型的目的地端點：

- 本地託管的 Elasticsearch 叢集
- 支援接收 Amazon Simple Notification Service 訊息的本機應用程式
- 本機託管的 Kafka 叢集
- 支援 HTTP POST 通知請求的外部或本機託管 webhook 端點。

  此端點可以託管在各種 Web 伺服器、框架或資料處理工具（例如 Fluentd）上。

- 位於相同或其他 StorageGRID 執行個體上的本機託管 S3 儲存桶
- 外部終端節點，例如 Amazon Web Services 上的終端節點。

為確保平台服務訊息能夠送達，您必須設定包含 ADC 儲存節點的網路。您必須確保可以使用下列連接埠將平台服務訊息傳送到目的地端點。

預設情況下，平台服務訊息會透過以下連接埠發送：

- **80**：適用於以 http 開頭的端點 URI（大多數端點）

- **443**：適用於以 https 開頭的端點 URI（大多數端點）
- **9092**：適用於以 http 或 https 開頭的端點 URI（僅限 Kafka 端點）

租戶在建立或編輯端點時可以指定不同的連接埠。

> 如果將 StorageGRID 部署用作 CloudMirror 複寫的目的地，則複寫訊息可能會在 80 或 443 以外的連接埠上接收。請確保在端點中指定目的地 StorageGRID 部署用於 S3 的連接埠。

如果您使用非透明 Proxy 伺服器，則也必須"設定儲存設備 Proxy 設定"允許將訊息傳送至外部端點（例如網際網路上的端點）。

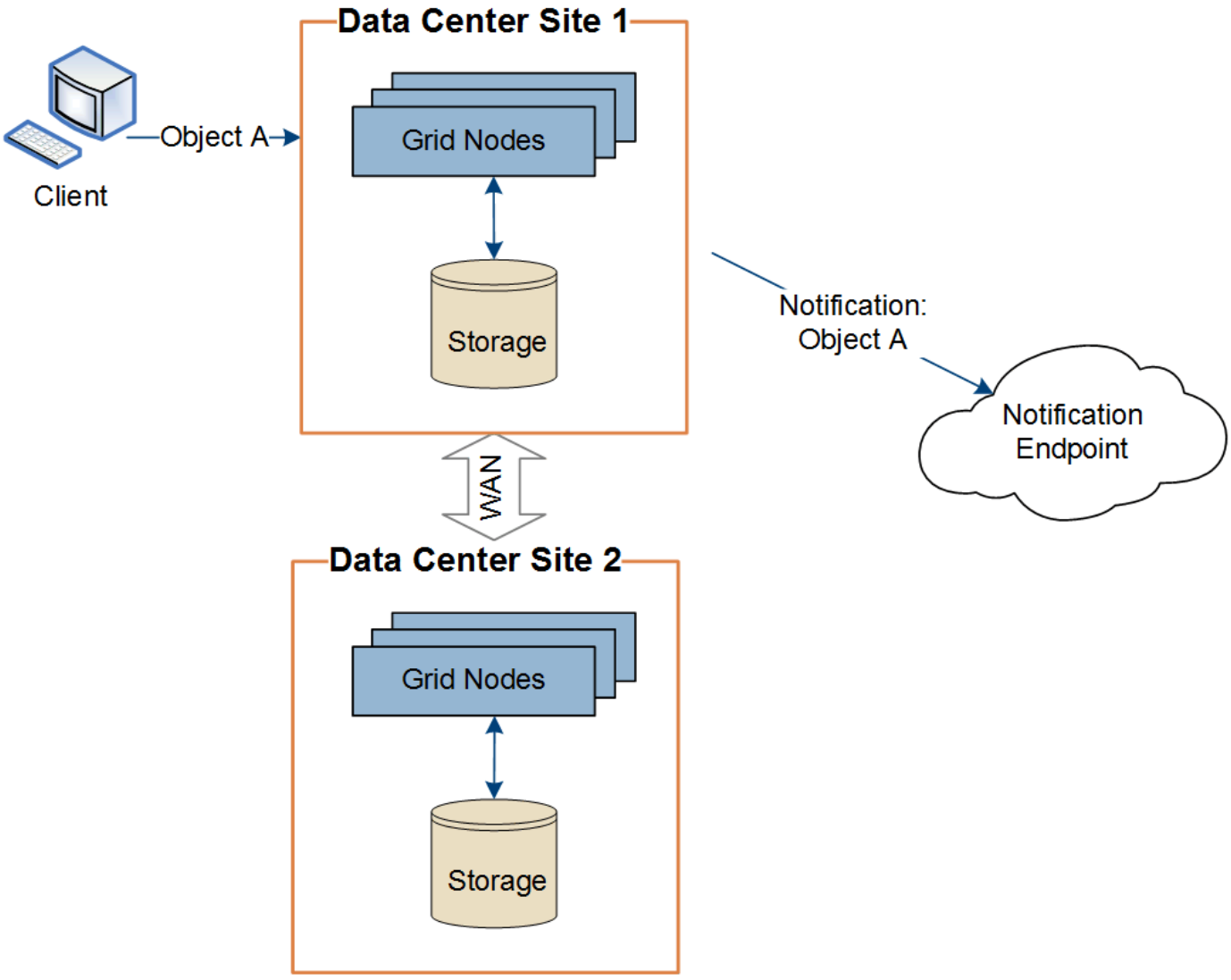
相關資訊

"使用租戶帳戶"

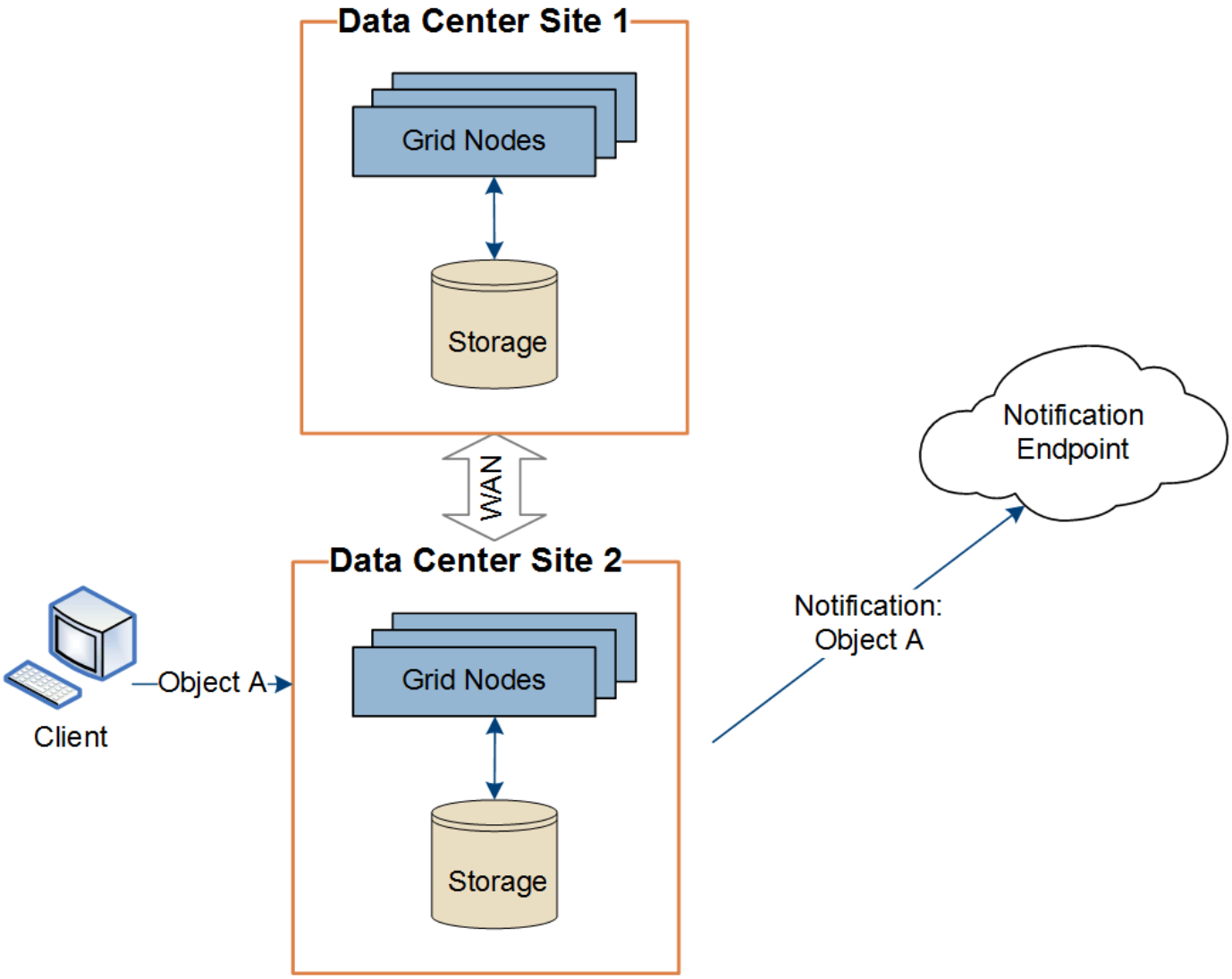
按站點交付 **StorageGRID** 平台服務訊息

所有平台服務作業均以每個站台為基礎執行。

也就是說，如果租戶使用用戶端透過連接到資料中心站點 1 的 Gateway Node 對物件執行 S3 API 建立操作，則會觸發該行動的通知，並從資料中心站點 1 發送該通知。



如果用戶端隨後從資料中心站點 2 對相同物件執行 S3 API 刪除操作，則會觸發有關刪除行動的通知，並從資料中心站點 2 發送該通知。



確保每個站台的連網設定正確，以便平台服務訊息能夠傳遞到目的地。

疑難排解 **StorageGRID** 平台服務

平台服務中使用的端點由租用戶使用者在 Tenant Manager 中建立和維護。但是，如果租用戶在設定或使用平台服務時遇到問題，您可以嘗試使用 Grid Manager 來協助解決問題。

${post_edited_translations.segment}

租戶必須先使用租戶管理器建立一個或多個終端節點，才能使用平台服務。每個終端節點代表一個平台服務的外部目的地，例如 StorageGRID S3 儲存桶、Amazon Web Services 儲存桶、Amazon Simple Notification Service 主題、Kafka 主題或託管在本機或 AWS 上的 Elasticsearch 叢集。每個終端節點都包含外部資源的位置以及存取該資源所需的憑證。

當租戶建立端點時，StorageGRID 系統會驗證該端點是否存在，以及是否可以使用指定的認證資訊進行連線。至端點的連線會從每個站台的一個節點進行驗證。

如果端點驗證失敗，系統會出現錯誤訊息說明端點驗證失敗的原因。租戶使用者應解決該問題，然後嘗試重新建立端點。

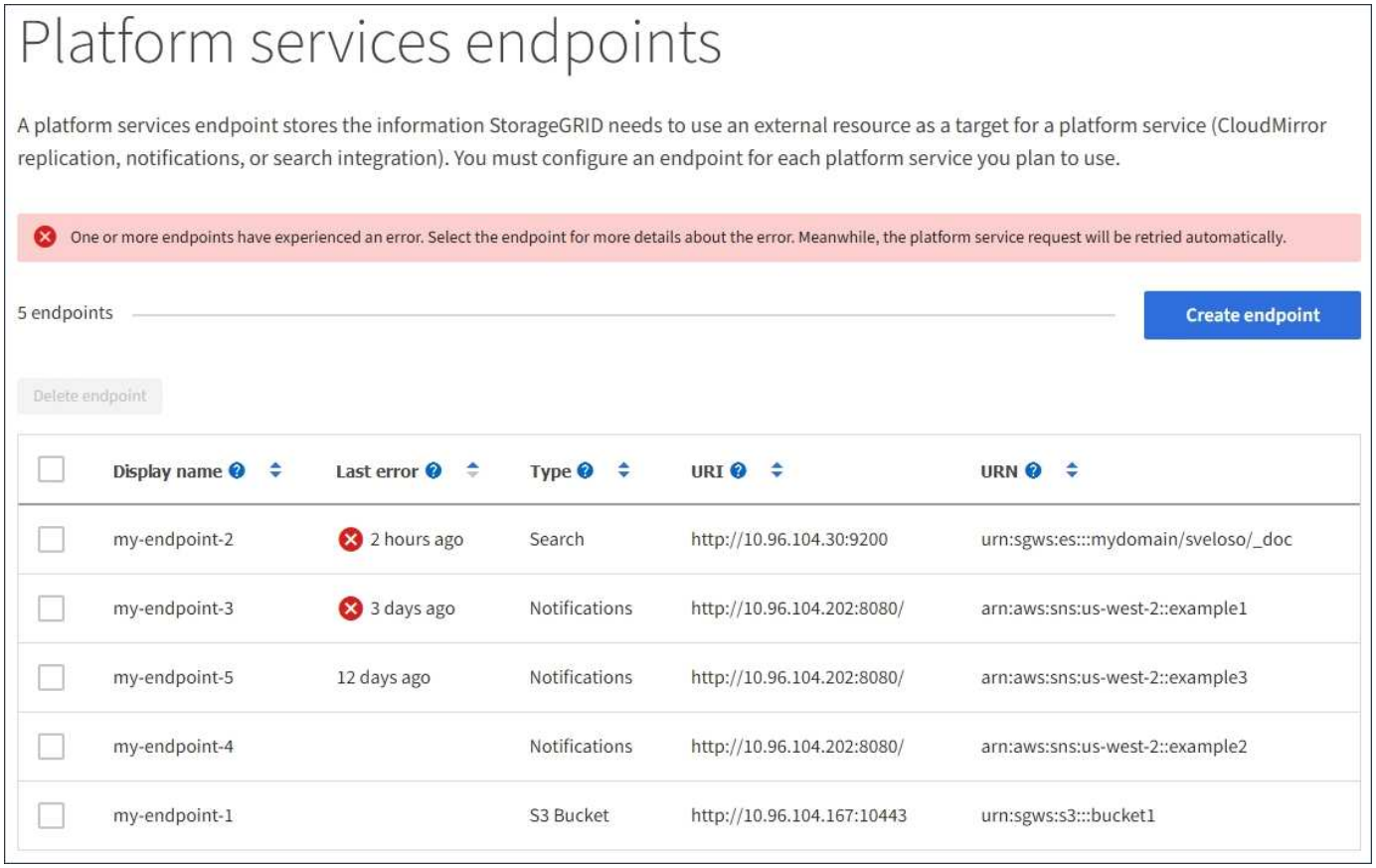
${post_edited_translations.segment}

現有端點存在問題

如果 StorageGRID 嘗試連線到現有端點時發生錯誤，則會在 Tenant Manager 的儀表板上顯示一則訊息。

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

租用戶使用者可以前往「端點」頁面，查看每個端點的最新錯誤訊息，並確認錯誤發生的時間。「上次錯誤」欄位顯示每個端點的最新錯誤訊息，並指示錯誤發生的時間。包含 ⊗ 圖示的錯誤表示過去 7 天內發生的錯誤。



「上次錯誤」欄位中的某些錯誤訊息可能包含括號內的日誌 ID。網格系統管理員或技術支援可以使用此 ID 在 bycast.log 中找到有關該錯誤的更多詳細資訊。

與 **Proxy** 伺服器相關的問題

如果您已在儲存節點和平台服務端點之間設定了 "${post_edited_translations.segment}"，則當您的 Proxy 服務不允許來自 StorageGRID 的訊息時，可能會發生錯誤。若要解決這些問題，請檢查 Proxy 伺服器的設定，確保與平台服務相關的訊息未被封鎖。

確定是否發生錯誤

如果過去 7 天內發生任何端點錯誤，Tenant Manager 中的儀表板會顯示警示訊息。您可以前往端點頁面，檢視

有關該錯誤的更多詳細資料。

${post_edited_translations.segment}

某些平台服務問題可能會導致用戶端對 S3 儲存桶的操作失敗。例如，如果內部複製狀態機 (RSM) 服務停止運行，或待發送的平台服務訊息佇列過長，則 S3 用戶端操作將會失敗。

查看服務狀態：

1. 選擇 節點 > ***site*** > ***Storage Node*** > 概覽。
2. 檢查「警報」表中是否有活躍警報。
3. 解決任何作用中的警示。視需要聯絡技術支援。

可恢復和不可恢復的端點錯誤

建立端點之後，可能會因為各種原因而發生平台服務要求錯誤。某些錯誤可在使用者介入後恢復。例如，可能會因為下列原因而發生可恢復的錯誤：

- 使用者的憑證已刪除或已過期。
- ${post_edited_translations.segment}
- 通知無法送達。

${post_edited_translations.segment}

其他類型的錯誤則無法恢復。例如，以下原因可能導致無法復原的錯誤：

- ${post_edited_translations.segment}
- webhook 端點目的地對通知請求的回應出現 `400 Bad Request`錯誤。

如果 StorageGRID 遇到無法復原的端點錯誤：

- 在 Grid Manager 中，請前往 **Support** > **Tools** > **Metrics** > **Grafana** > **Platform Services Overview** 以檢視錯誤詳細資料。
- 在租戶管理員中，前往 **STORAGE (S3)** > **Platform Services Endpoints** 以檢視錯誤詳細資料。
- 檢查 `/var/local/log/bycast-err.log`是否有相關錯誤。具有 ADC 服務的儲存節點包含此日誌檔。

${post_edited_translations.segment}

如果目的地遇到無法接收平台服務訊息的問題，則用戶端對儲存桶的操作會成功，但平台服務訊息無法送達。例如，如果目的地上的憑證更新，導致 StorageGRID 無法再向目的地服務進行驗證，則可能會發生此錯誤。

查看相關警報。

平台服務請求效能下降

如果請求發送速率超過目的地端點接收速率，StorageGRID 軟體可能會限制對某個儲存桶的 S3 請求速率。只有當有大量請求積壓等待發送到目的地端點時，才會發生限速。

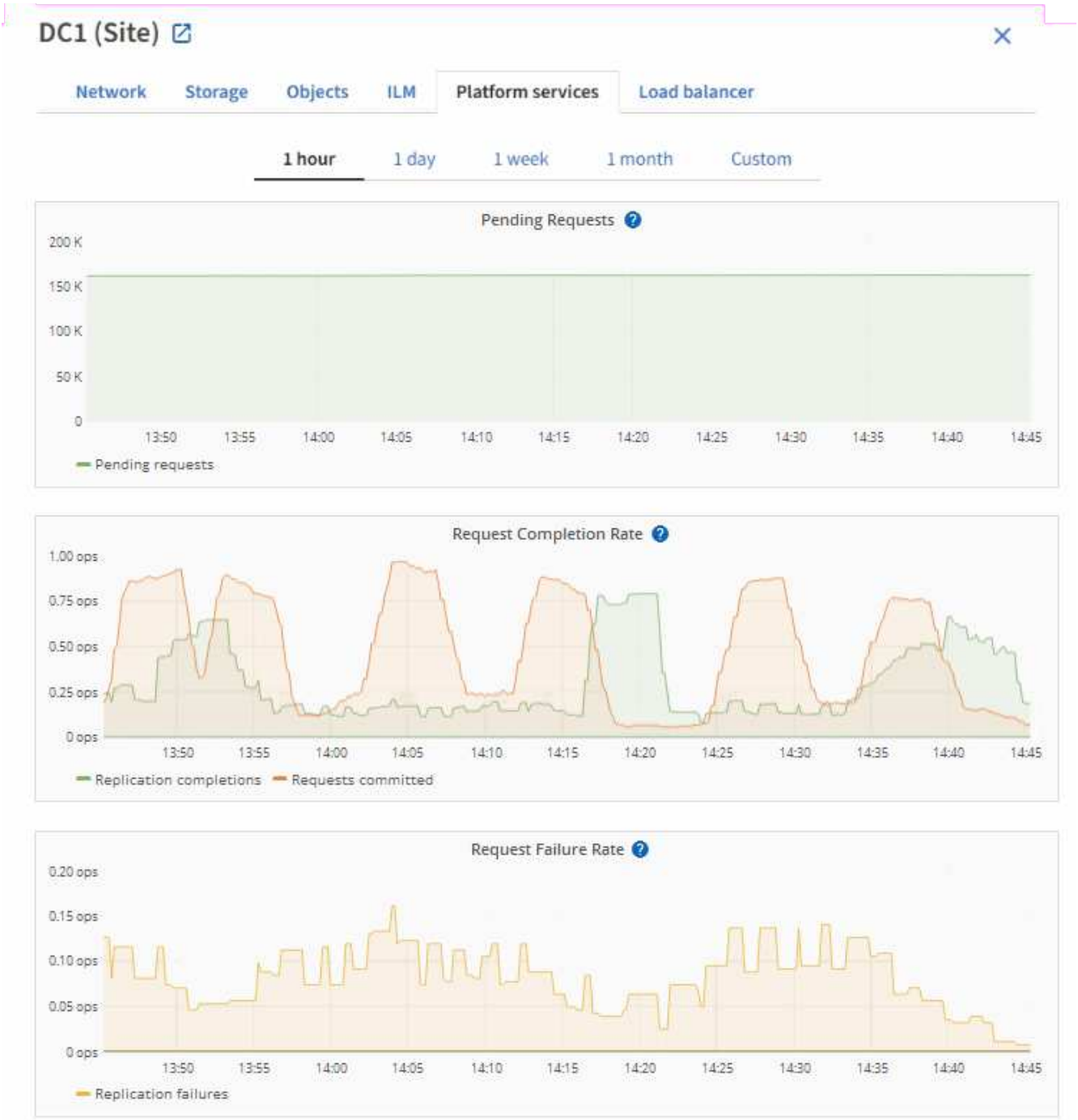
唯一可見的影響是傳入的 S3 請求執行時間會延長。如果效能明顯下降，則應降低擷取速率或使用容量更大的端點。如果請求積壓持續成長，用戶端的 S3 操作（例如 PUT 請求）最終會失敗。

CloudMirror 要求更容易受到目的地端點效能的影響，因為這些要求通常比搜尋整合或事件通知要求涉及更多的資料傳輸。

平台服務請求失敗

檢視平台服務的請求故障率：

1. 選取 **Nodes** 。
2. 選擇 ***site*** > 平台服務。
3. 檢視請求錯誤率圖表。



${post_edited_translations.segment}

*平台服務無法使用*警示表示由於執行或可用的含 RSM 服務的儲存節點太少，因此無法在站台上執行任何平台服務操作。

RSM 服務確保平台服務請求傳送至各自的端點。

若要解決此警示，請確定站台中哪些儲存節點包含 RSM 服務。（RSM 服務存在於也包含 ADC 服務的儲存節點上。）然後，確保這些儲存節點中的簡單多數正在運作且可用。

${post_edited_translations.segment}

平台服務端點的其他疑難排解指南

更多資訊請參閱"${post_edited_translations.segment}"。

相關資訊

"${post_edited_translations.segment}"

在 StorageGRID 中為租戶帳戶管理 S3 Select

您可以允許特定的 S3 租戶使用 S3 Select 對個別物件發出 SelectObjectContent 要求。

S3 Select 提供了一種有效率的方法來搜尋大量資料，而無需部署資料庫及相關資源來啟用搜尋。它還能降低擷取資料的成本與延遲。

什麼是 S3 Select？

S3 Select 允許 S3 用戶端使用 SelectObjectContent 要求，以僅篩選和擷取物件中所需的資料。S3 Select 的 StorageGRID 實作包含 S3 Select 命令和功能的子集。

使用 S3 Select 的注意事項和要求

網格管理要求

網格系統管理員必須授予租戶 S3 Select 能力。選取 **Allow S3 Select**，當 "${post_edited_translations.segment}" 或 "編輯租戶" 時。

物件格式要求

${post_edited_translations.segment}

- **CSV**。可直接使用，也可壓縮成 GZIP 或 BZIP2 壓縮包。
- **Parquet**。Parquet 物件的其他需求：
  - S3 Select 僅支援使用 GZIP 或 Snappy 的欄式壓縮。S3 Select 不支援 Parquet 物件的整個物件壓縮。
  - S3 Select 不支援 Parquet 輸出。您必須將輸出格式指定為 CSV 或 JSON。
  - 未壓縮資料列群組的最大大小為 512 MB。
  - 必須使用物件架構中指定的資料類型。

- 您不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 邏輯類型。

端點要求

SelectObjectContent 請求必須傳送至 "StorageGRID 負載平衡器端點"。

端點使用的管理節點和 Gateway 節點必須是下列節點之一：

- ${post_edited_translations.segment}
- 基於 VMware 的軟體節點
- 裸機節點執行已啟用 cgroup v2 的核心

一般性考慮

${post_edited_translations.segment}

> SelectObjectContent 請求可能會降低所有 S3 用戶端和所有租戶的負載平衡器效能。僅在需要時且僅針對信任的租戶啟用此功能。

請參閱 "S3 Select 使用說明"。

若要檢視"Grafana 圖表" S3 Select 操作隨時間的變化情況，請在 Grid Manager 中選擇 **Support** > **Tools** > **Metrics**。

設定用戶端連線

設定 **S3** 用戶端連線至 **StorageGRID**

身為網格系統管理員，您可管理控制 S3 用戶端應用程式如何連線至 StorageGRID 系統以儲存和擷取資料的組態選項。

> 此版本的文件網站已移除 Swift 相關細節。請參閱 "StorageGRID 11.8：設定 S3 和 Swift 用戶端連線"。

組態工作

1. 根據用戶端應用程式連線至 StorageGRID 的方式，在 StorageGRID 中執行必要的先決條件工作。

所需任務

您必須獲得：

- IP 位址
- 網域名稱
- SSL 憑證

選用任務

（可選）設定：

- 身分聯合
- 單一登入（SSO）

1. 使用 StorageGRID 取得應用程式連接到網格所需的值。您可以使用 S3 設定精靈，也可以手動設定每個 StorageGRID 實體。+

使用 **S3** 設定精靈

請依照 S3 設定精靈中的步驟操作。

手動設定

1. 建立高可用度群組
2. 建立負載平衡器端點
3. 建立租戶帳戶
4. 建立儲存桶和存取金鑰
5. 設定 ILM 規則和原則

1. 使用 S3 應用程式完成與 StorageGRID 的連線。建立 DNS 項目，將 IP 位址與您計劃使用的任何網域名稱建立關聯。

   根據需要，執行其他應用程式設定。

2. 在應用程式和 StorageGRID 中執行後續任務，以管理和監控物件儲存隨時間的變化。

將 **StorageGRID** 連接至用戶端應用程式所需的資訊

在將 StorageGRID 連接到 S3 用戶端應用程式之前，必須在 StorageGRID 中執行組態步驟並取得某些值。

我需要哪些數值？

下表顯示您必須在 StorageGRID 中設定的值，以及 S3 應用程式和 DNS 伺服器使用這些值的位置。

價值	**${post_edited_translations.segment}**	**${post_edited_translations.segment}**
虛擬 IP（VIP）位址	${post_edited_translations.segment}	${post_edited_translations.segment}
連接埠	StorageGRID > 負載平衡器端點	用戶端應用程式
SSL 憑證	StorageGRID > 負載平衡器端點	用戶端應用程式
${post_edited_translations.segment}	StorageGRID > 負載平衡器端點	• 用戶端應用程式 • ${post_edited_translations.segment}
S3 存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租戶與儲存桶	用戶端應用程式
儲存桶/Container 名稱	StorageGRID > 租戶與儲存桶	用戶端應用程式

${post_edited_translations.segment}

${post_edited_translations.segment}

- 請使用 **"S3 設定精靈"**。S3 設定精靈可協助您快速設定 StorageGRID 中的所需值，並輸出一個或兩個檔案，供您在設定 S3 應用程式時使用。此精靈會引導您完成所需步驟，並確保您的設定符合 StorageGRID 最佳實務做法。

  如果您正在設定 S3 應用程式，建議使用 S3 設定精靈，除非您知道自己有特殊要求或您的實作需要進行大量自訂。

- 使用 **"FabricPool 設定精靈"**。與 S3 設定精靈類似，FabricPool 設定精靈可協助您快速設定所需的值，並輸出一個檔案，供您在 ONTAP 中設定 FabricPool 雲端分層時使用。

  如果您打算使用 StorageGRID 作為 FabricPool 雲端分層的物件儲存系統，建議使用 FabricPool 設定精靈，除非您知道自己有特殊需求或您的實作需要進行大量自訂。

- 手動設定項目。如果您要連線至 S3 應用程式，且不想使用 S3 設定精靈，則可以透過手動執行組態來取得所需的值。請依照以下步驟操作：

  a. 設定要用於 S3 應用程式的高可用度 （HA） 群組。請參閱"設定高可用度群組"。

  b. 建立 S3 應用程式將使用的負載平衡器端點。請參閱"設定負載平衡器端點"。

  c. 建立 S3 應用程式將使用的租戶帳戶。請參閱 "建立租戶帳戶"。

  d. 對於 S3 租戶，請登入租戶帳戶，並為每個將存取應用程式的使用者產生存取金鑰 ID 和秘密存取金鑰。請參閱"建立您自己的存取金鑰"。

  e. 在租戶帳戶中建立一或多個 S3 儲存貯體。關於 S3，請參閱 "建立 S3 儲存桶"。

  f. 若要為屬於新租戶或儲存桶/Container 的物件新增特定的放置指令，請建立新的 ILM 規則並啟動新的

ILM 原則以使用該規則。請參閱 "建立 ILM 規則" 和 "建立 ILM 策略"。

StorageGRID 中 S3 用戶端的安全性

StorageGRID 租戶帳戶使用 S3 用戶端應用程式將物件資料儲存至 StorageGRID。您應該審查為用戶端應用程式實作的安全性措施。

總結

以下列表總結了 S3 REST API 的安全性實作方式：

${post_edited_translations.segment}
${post_edited_translations.segment}

${post_edited_translations.segment}
由系統 CA 簽署的 X.509 伺服器憑證或系統管理員提供的自訂伺服器憑證

用戶端驗證
S3 帳戶存取金鑰 ID 和秘密存取金鑰

${post_edited_translations.segment}
儲存桶所有權和所有適用的存取控制原則

${post_edited_translations.segment}

${post_edited_translations.segment}

- 連接到負載平衡器服務的用戶端可以使用 HTTPS 或 HTTP，具體取決於您如何"設定負載平衡器端點"。

  HTTPS 提供安全的 TLS 加密通訊，建議使用。您必須為端點附加安全性憑證。

  HTTP 提供的是安全性較低、未加密的通訊，因此只應在非生產或測試網格中使用。

- 連接到儲存節點的用戶端也可以使用 HTTPS 或 HTTP。

  HTTPS 是預設值，建議使用。

  HTTP 提供較低安全性的未加密通訊，但對於非生產或測試網格，可選擇性地"已啟用"啟用。

- StorageGRID 與用戶端之間的通訊使用 TLS 加密。
- 無論負載平衡器端點設定為接受 HTTP 連線或 HTTPS 連線，負載平衡器服務與網格內儲存節點之間的通訊都會加密。
- 用戶端必須提供 "HTTP 驗證標頭" 給 StorageGRID，才能執行 REST API 操作。

安全性憑證和用戶端應用程式

在所有情況下，用戶端應用程式都可以使用網格系統管理員上傳的自訂伺服器憑證或 StorageGRID 系統產生的憑證建立 TLS 連線：

- 當用戶端應用程式連接到負載平衡器服務時，它們會使用為負載平衡器端點設定的憑證。每個負載平衡器端

點都有自己的憑證—可以是網格系統管理員上傳的自訂伺服器憑證，也可以是網格系統管理員在 StorageGRID 中設定端點時產生的憑證。

請參閱 "負載平衡的考慮因素"。

- 當用戶端應用程式直接連線至儲存節點時，它們可以使用在安裝 StorageGRID 系統時為儲存節點產生的系統產生伺服器憑證（由系統憑證授權單位簽署），或使用網格系統管理員為網格提供的單一自訂伺服器憑證。請參閱"新增自訂 S3 API 證書"。

應將用戶端設定為信任簽署其用於建立 TLS 連線之憑證的憑證授權單位。

TLS 程式庫支援的雜湊和加密演算法

StorageGRID 系統支援一組密碼套件，用戶端應用程式在建立 TLS 工作階段時可以使用這些密碼套件。若要設定密碼，請前往 設定 > 安全性 > 安全性設定，然後選取 **TLS** 和 **SSH** 原則。

支援的 TLS 版本

StorageGRID 支援 TLS 1.2 和 TLS 1.3。

SSLv3 和 TLS 1.1（或更早版本）已不再支援。

使用 S3 設定精靈

StorageGRID S3 設定精靈的考量與需求

您可以使用 S3 設定精靈將 StorageGRID 設定為 S3 應用程式的物件儲存系統。

何時使用 S3 設定精靈

S3 設定精靈將引導您完成設定 StorageGRID 以搭配 S3 應用程式使用的每個步驟。在完成精靈的過程中，您需要下載一些檔案，以便在 S3 應用程式中輸入相應的值。使用此精靈可以更快速地設定您的系統，並確保您的設定符合 StorageGRID 最佳實務。

如果您擁有 "${post_edited_translations.segment}"，則可以在開始使用 StorageGRID Grid Manager 時完成 S3 設定精靈，或者您也可以稍後隨時存取並完成該精靈。根據您的需求，您也可以手動設定部分或全部必要項目，然後使用精靈來組合 S3 應用程式所需的值。

使用精靈之前

在使用精靈之前，請確認您已完成以下先決條件。

取得 **IP** 位址並設定 **VLAN** 介面

如果您將設定高可用度（HA）群組，您會知道 S3 應用程式將連線到哪些節點，以及將使用哪個 StorageGRID 網路。您也知道要為子網路 CIDR、閘道 IP 位址和虛擬 IP（VIP）位址輸入哪些值。

如果您計劃使用虛擬區域網路來隔離來自 S3 應用程式的流量，則您已設定 VLAN 介面。請參閱 "設定 VLAN 介面"。

設定身分識別聯盟和單一登入

如果您打算為 StorageGRID 系統使用身分聯合或單一登入 （SSO），則已啟用這些功能。您也知道哪個聯

合群組應擁有 S3 應用程式將使用的租戶帳戶的 root 存取權。請參閱 "${post_edited_translations.segment}" 和 "設定單一登入"。

${post_edited_translations.segment}

您知道要將哪個完整網域（FQDN）用於 StorageGRID。網域名稱伺服器（DNS）項目會將此 FQDN 對應至您使用精靈建立之 HA 群組的虛擬 IP（VIP）位址。

如果您打算使用 S3 虛擬託管式請求，則應該"${post_edited_translations.segment}"。建議使用虛擬託管式請求。

${post_edited_translations.segment}

如果您計劃使用 StorageGRID 負載平衡器，您已檢閱負載平衡的一般考量事項。您已擁有要上傳的憑證，或是產生憑證所需的值。

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

- 您有"已設定網格同盟連線"。
- 連線狀態為*已連線*。
- 您擁有根目錄存取權限。

在 **StorageGRID** 中存取並完成 **S3** 設定精靈

您可以使用 S3 設定精靈來設定 StorageGRID，以搭配 S3 應用程式使用。設定精靈會提供應用程式存取 StorageGRID 儲存貯體和儲存物件所需的值。

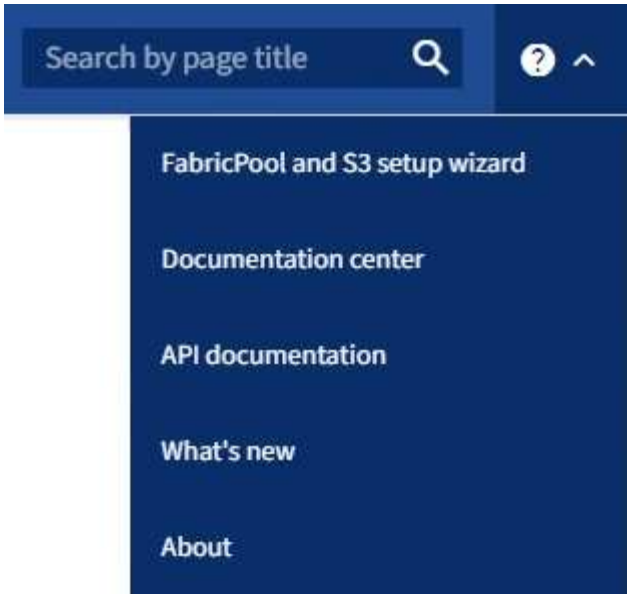
開始之前

- 您有"${post_edited_translations.segment}"。
- 您已審閱使用精靈的 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

步驟

1. 使用 "支援的網頁瀏覽器" 登入 Grid Manager。
2. 如果儀表板上出現「* FabricPool 和 S3 設定精靈*」橫幅，請選擇橫幅中的連結。如果橫幅不再顯示，請從 Grid Manager 的標題列中選擇說明圖示，然後選擇「* FabricPool 和 S3 設定精靈*」。



3. 在 FabricPool 和 S3 設定精靈頁面的 S3 應用程式部分中，選擇「立即設定」。

步驟 **1** （共 **6** 步）：設定 **HA** 群組

HA 群組是由多個節點組成的集合，每個節點包含 StorageGRID 負載平衡器服務。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用高可用性 （HA） 群組來幫助維持 S3 資料連線的可用性。如果 HA 群組中的作用中介面發生故障，備份介面可以管理工作負載，對 S3 作業的影響微乎其微。

如需此工作的詳細資訊，請參閱 "管理高可用度群組"。

步驟

1. 如果您打算使用外部負載平衡器，則無需建立 HA 群組。選取 **Skip this step** 並前往 <<${post_edited_translations.segment}>>。
2. 若要使用 StorageGRID 負載平衡器，您可以建立新的 HA 群組或使用現有的 HA 群組。

${post_edited_translations.segment}

a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

欄位	說明
HA 組名	${post_edited_translations.segment}
${post_edited_translations.segment}	此 HA 群組的執行摘要。

c. 在「新增介面」步驟中，選擇要在此 HA 群組中使用的節點介面。

${post_edited_translations.segment}

您可以選擇一個或多個節點，但每個節點只能選擇一個介面。

d. 在「排列介面優先順序」步驟中，確定此 HA 群組的主要介面和任何備份介面。

拖曳列以變更*優先順序*欄中的值。

清單中的第一個介面是主要介面。除非發生故障，否則主要介面為作用中介面。

如果高可用性 (HA) 群組包含多個介面，且目前活動介面發生故障，則虛擬 IP (VIP) 位址會依優先順序轉移到第一個備份介面。如果該介面也發生故障，則 VIP 位址會轉移到下一個備份介面，依此類推。故障解決後，VIP 位址會回到優先順序最高的可用介面。

e. 在「輸入 IP 位址」步驟中，請填寫以下欄位。

欄位	說明
子網路 CIDR	VIP 子網路的位址（CIDR 表示法）— IPv4 位址後接斜線和子網路長度（0-32）。 網路位址不得設定任何主機位元。例如 `192.16.0.0/22`。
閘道 IP 位址（可選）	如果用於存取 StorageGRID 的 S3 IP 位址與 StorageGRID VIP 位址不在同一子網路中，請輸入 StorageGRID VIP 本機閘道 IP 位址。本機閘道 IP 位址必須位於 VIP 子網路內。
虛擬 IP 位址	請為 HA 群組中的作用中介面輸入至少一個且不超過十個 IP 位址。所有 IP 位址都必須在 VIP 子網路內。 至少有一個位址必須是 IPv4。您可以選擇性指定其他 IPv4 和 IPv6 位址。

f. ${post_edited_translations.segment}

g. ${post_edited_translations.segment}

${post_edited_translations.segment}

a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

StorageGRID 使用負載平衡器來管理來自用戶端應用程式的工作負載。負載平衡能最大化跨多個 Storage 節點的速度與連線容量。

您可以使用所有 Gateway 和 Admin 節點上的 StorageGRID 負載平衡器服務，也可以連線至外部（第三方）負載平衡器。建議使用 StorageGRID 負載平衡器。

有關此工作的詳細資訊，請參閱"負載平衡的考慮因素"。

若要使用 StorageGRID 負載平衡服務，請選取 **StorageGRID load balancer** 索引標籤，然後建立或選取您要使用的負載平衡端點。若要使用外部負載平衡器，請選取 **External load balancer** 索引標籤，並提供您已設定之系統的詳細資料。

建立端點

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

欄位	說明
Name	端點的描述性名稱。
連接埠	用於負載平衡的 StorageGRID 連接埠。對於您建立的第一個端點，此欄位預設值為 10433，但您可以輸入任何未使用的外部連接埠。如果您輸入 80 或 443，則該端點僅在閘道節點上設定，因為這些連接埠在管理節點上已保留。 *附註：*不允許使用其他網格服務所使用的連接埠。請參閱 "StorageGRID 內部連接埠"。
用戶端類型	必須是*S3*。
網路傳輸協定	選擇 **HTTPS** 。 ${post_edited_translations.segment}

3. 在「選擇綁定模式」步驟中，指定綁定模式。綁定模式控制如何存取端點，是使用任意 IP 位址，還是使用特定的 IP 位址和網路介面。

模式	說明
全域（預設）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （VIP） 位址或對應的 FQDN 存取端點。 除非您需要限制此端點的存取能力，否則請使用 全域 設定（預設值）。
HA 群組的虛擬 IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）才能存取此端點。 具有此綁定模式的端點都可以使用相同的連接埠號，只要您為端點選擇的 HA 群組不重疊即可。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN）來存取此端點。
節點類型	根據您選擇的節點類型，用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）或任何閘道節點的 IP 位址（或對應的 FQDN）來存取此端點。

4. ${post_edited_translations.segment}

欄位	說明
允許所有租戶（預設）	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	選定的租戶帳戶無法使用此端點存取其儲存桶。所有其他租戶均可使用此端點。

5. 在「附加憑證」步驟中，請選擇下列選項之一：

欄位	說明
上傳憑證（建議）	${post_edited_translations.segment}
產生證書	使用此選項可產生自簽名憑證。請參閱 "設定負載平衡器端點" 以取得輸入內容的詳細資訊。
使用 StorageGRID S3 憑證	僅當您已上傳或產生自訂版本的 StorageGRID 全域憑證時才使用此選項。如需詳細資訊，請參閱 "設定 S3 API 憑證"。

6. 選擇 **Finish** 以返回 S3 設定精靈。
7. 選擇 **Continue** 以前往租戶和儲存桶步驟。

${post_edited_translations.segment}

使用現有的負載平衡器端點

步驟

1. 若要使用現有端點，請從「選擇負載平衡器端點」中選擇其名稱。
2. 選擇 **Continue** 以前往租戶和儲存桶步驟。

使用外部負載平衡器

步驟

1. 若要使用外部負載平衡器，請填寫以下欄位。

欄位	說明
FQDN	${post_edited_translations.segment}
連接埠	S3 應用程式將用於連線至外部負載平衡器的連接埠號碼。
證書	${post_edited_translations.segment}

2. 選擇 **Continue** 以前往租戶和儲存桶步驟。

步驟 **3**（共 **6** 步）：建立租戶和儲存桶

租戶是指可以使用 S3 應用程式在 StorageGRID 中儲存和擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、儲存桶、物件和一組特定的權限。

儲存桶是用於儲存租戶物件及其物件中繼資料的 Container。雖然租戶可以擁有多個儲存桶，但精靈可以幫助您以最快捷、最簡單的方式建立租戶和儲存桶。如果您之後需要新增儲存桶或設定選項，可以使用 Tenant Manager。

如需此工作的詳細資訊，請參閱 "建立租戶帳戶" 與 "建立 S3 儲存桶"。

步驟

1. ${post_edited_translations.segment}

   租戶名稱不需要是唯一的。建立租戶帳戶時，它會收到一個唯一的數值帳戶 ID。

2. 根據您的 StorageGRID 系統是否使用 "${post_edited_translations.segment}"、"單一登入 (SSO)"或兩者，為租戶帳戶定義 root 存取權。

選項	**${post_edited_translations.segment}**
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	a. 選擇現有的同盟群組，使其對租戶具有 "${post_edited_translations.segment}"。 b. （可選）指定以本機 root 使用者身分登入租戶時要使用的密碼。
${post_edited_translations.segment}	選取現有的聯合群組，以便為租戶提供 "${post_edited_translations.segment}"。本機使用者無法登入。

3. ${post_edited_translations.segment}

   如果租戶的唯一使用者是 root 使用者，請選擇此選項。如果其他使用者也將使用此租戶，"${post_edited_translations.segment}"以設定金鑰和權限。

4. ${post_edited_translations.segment}

   如果已為此網格啟用 S3 Object Lock ，則在此步驟中建立的貯存庫不會啟用 S3 Object Lock 。如果您需要為此 S3 應用程式使用 S3 Object Lock 貯存庫，請勿選取立即建立貯存庫。相反地，請稍後使用 Tenant Manager 來 "${post_edited_translations.segment}"。

   a. 輸入 S3 應用程式將使用的儲存桶名稱。例如， `s3-bucket`。

      建立儲存桶後無法變更儲存桶名稱。

   b. 選擇此儲存桶的*區域*。

      除非您預計未來會使用 ILM 根據 Bucket 的地區來篩選物件，否則請使用預設地區 (`us-east-1`) 。

5. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 如果您選擇了*自動建立 root 使用者 S3 存取金鑰*，請執行下列一項或兩項操作：
   - 選擇 **Download access keys** 以下載 `.csv`包含租戶帳戶名稱、存取金鑰 ID 和秘密存取金鑰的檔案。
   - 選擇複製圖示（）將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。
2. 選擇 **Download configuration values** 以下載 `.txt`包含負載平衡器端點、租戶、儲存桶和 root 使用者設定的檔案。
3. 請將此資訊儲存到安全的位置。

> 在您製作這兩個存取金鑰的複本之前，請勿結案此頁面。結案此頁面後，將無法再取得這些金鑰。請務必將此資訊儲存在安全的的位置，因為它可用於從您的 StorageGRID 系統取得資料。

4. 如果出現提示，請選取核取方塊以確認您已下載或複製金鑰。
5. 選擇 **Continue** 以進入 ILM 規則和原則步驟。

步驟 **5**（共 **6** 步）：檢視 **S3** 的 **ILM** 規則和 **ILM** 原則

資訊生命週期管理 （ILM） 規則可控制 StorageGRID 系統中所有物件的放置、持續時間和擷取行為。StorageGRID 隨附的 ILM 原則會建立所有物件的兩個複寫複本。此原則會一直有效，直到您啟動至少一個新原則為止。

步驟

1. ${post_edited_translations.segment}
2. 如果您想要為屬於新租戶或儲存桶的物件新增特定指令，請建立新規則和新原則。請參閱 "建立 ILM 規則" 和 "${post_edited_translations.segment}"。
3. 選擇「我已閱讀這些步驟並了解我需要做什麼」。
4. 選取此複選框，表示您明白下一步該怎麼做。
5. 選擇 **Continue** 前往 **Summary**。

${post_edited_translations.segment}

步驟

1. 檢閱摘要。
2. 請記下後續步驟中的詳細資訊，其中說明了在連線至 S3 用戶端之前可能需要的額外組態。例如，選取 **Sign in as root** 會帶您前往 Tenant Manager，您可以在該處新增租戶使用者、建立額外的儲存貯體，以及更新儲存貯體設定。
3. 選擇 **Finish** 。
4. 使用從 StorageGRID 下載的檔案或手動取得的值來設定應用程式。

管理 HA 群組

了解 StorageGRID 高可用性群組

高可用度 （HA） 群組為 S3 用戶端提供高可用度的資料連線，並為 Grid Manager 和 Tenant Manager 提供高可用度的連線。

您可以將多個管理節點和閘道節點的網路介面分組到一個高可用度 （HA） 群組中。如果 HA 群組中的作用中介面發生故障，備份介面可以管理工作負載。

每個 HA 群組提供對所選節點上共享服務的存取。

- 包含 Gateway Node、Admin Node 或兩者的 HA 群組為 S3 用戶端提供高可用度的資料連線。
- 僅包含管理節點的 HA 群組可為 Grid Manager 和 Tenant Manager 提供高可用度的連線。
- 僅包含服務設備和基於 VMware 的軟體節點的 HA 群組可以為"使用 S3 Select 的 S3 租用戶"提供高可用度的連線。建議在使用 S3 Select 時使用 HA 群組，但並非必要。

如何建立 HA 群組？

1. 您可以為一個或多個管理節點或閘道節點選擇網路介面。您可以使用 Grid Network （eth0） 介面、Client Network （eth2） 介面、VLAN 介面或您已新增至節點的存取介面。

   ${post_edited_translations.segment}

2. 您可以將一個介面指定為主要介面。除非發生故障，否則主要介面為作用中介面。
3. ${post_edited_translations.segment}
4. 您可以為該群組指派 1 到 10 個虛擬 IP （VIP） 位址。用戶端應用程式可以使用這些 VIP 位址中的任何一個連線至 StorageGRID。

如需相關指示，請參閱 "設定高可用度群組"。

目前啟動的介面是什麼？

正常運作期間，HA 群組的所有 VIP 位址都會加入主介面（優先順序最高的介面）。只要主介面可用，用戶端連接到該群組的任何 VIP 位址時都會使用該介面。也就是說，在正常運作期間，主介面是該群組的「作用中」介面。

同樣地，在正常運作期間，HA 群組中任何優先順序較低的介面都會充當「備份」介面。除非主要（目前作用中）介面變得無法使用，否則不會使用這些備份介面。

${post_edited_translations.segment}

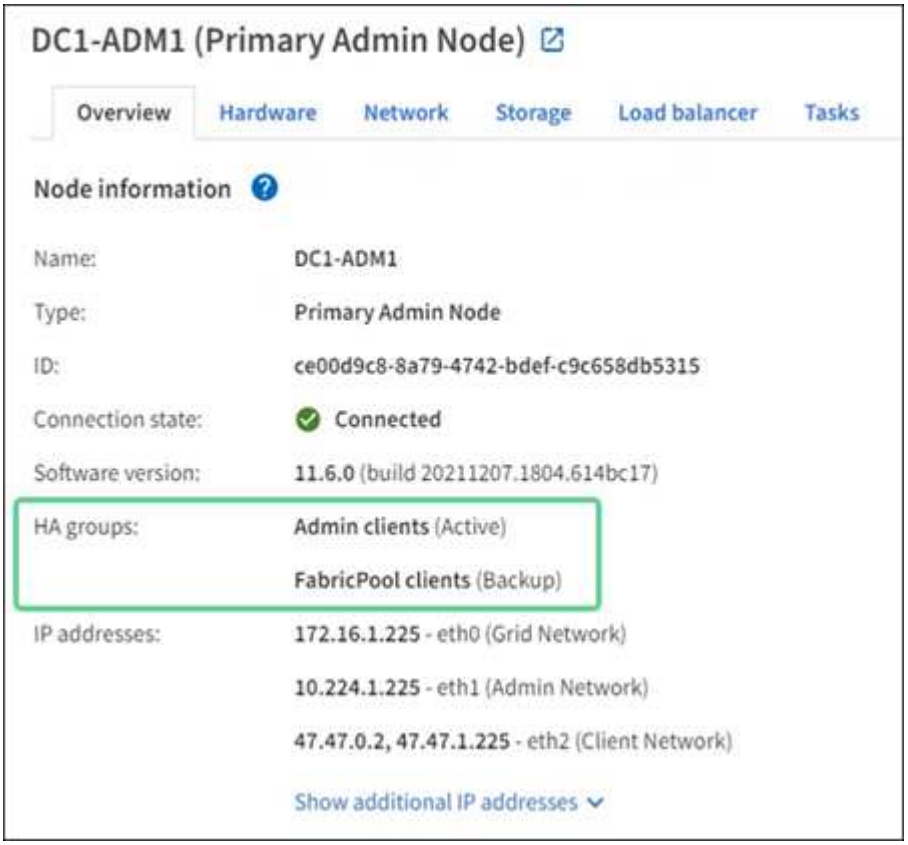
${post_edited_translations.segment}

如果「概覽」標籤包含「HA 群組」條目，則表示該節點已指派到所列的 HA 群組。群組名稱後面的值表示該節點在 HA 群組中的目前狀態：

- **Active**：HA 群組目前託管在此節點上。
- 備份：HA 群組目前未使用此節點；這是一個備份介面。

- 已停止：由於高可用度（keepalived）服務已手動停止，因此無法在此節點上託管 HA 群組。
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - 節點已關閉。

在本例中，主管理節點已新增至兩個高可用度 （HA） 群組。該節點目前是 Admin clients 群組的作用中介面，也是 FabricPool clients 群組的備份介面。



${post_edited_translations.segment}

目前裝載 VIP 位址的介面即為作用中介面。如果 HA 群組包含多個介面，且作用中介面發生故障，則 VIP 位址會依優先順序移至第一個可用的備份介面。如果該介面發生故障，則 VIP 位址會移至下一個可用的備份介面，依此類推。

${post_edited_translations.segment}

- 設定該介面的節點發生故障。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 高可用度服務停止運作。

裝載作用中介面的節點外部若發生網路故障，可能不會觸發容錯移轉。同樣地，Grid Manager 或 Tenant Manager 的服務也不會觸發容錯移轉。

${post_edited_translations.segment}

${post_edited_translations.segment}

StorageGRID HA 群組如何提供高可用性

${post_edited_translations.segment}

- HA 群組可以為 Grid Manager 或 Tenant Manager 提供高可用度的管理連線。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

只有當群組中包含的所有節點都提供相同的服務時，HA 群組才能提供高可用度。建立 HA 群組時，請從提供您所需服務的節點類型中新增介面。

- 管理節點：包含負載平衡器服務，並啟用對 Grid Manager 或 Tenant Manager 的存取。
- ${post_edited_translations.segment}

${post_edited_translations.segment}	**${post_edited_translations.segment}**
存取 Grid Manager	• ${post_edited_translations.segment} • 非主要管理節點 附註： 主 Admin 節點必須是主介面。某些維護程序只能從主 Admin 節點執行。
僅限存取 Tenant Manager	• ${post_edited_translations.segment}
S3 用戶端存取——負載平衡器服務	• 管理節點 • 閘道節點
適用於 "${post_edited_translations.segment}" 的 S3 用戶端存取	• 服務應用裝置 • ${post_edited_translations.segment} 注意：使用 S3 Select 時建議使用 HA 群組，但並非必須。

${post_edited_translations.segment}

如果 Grid Manager 或 Tenant Manager 服務發生故障，則不會觸發 HA 群組故障轉移。

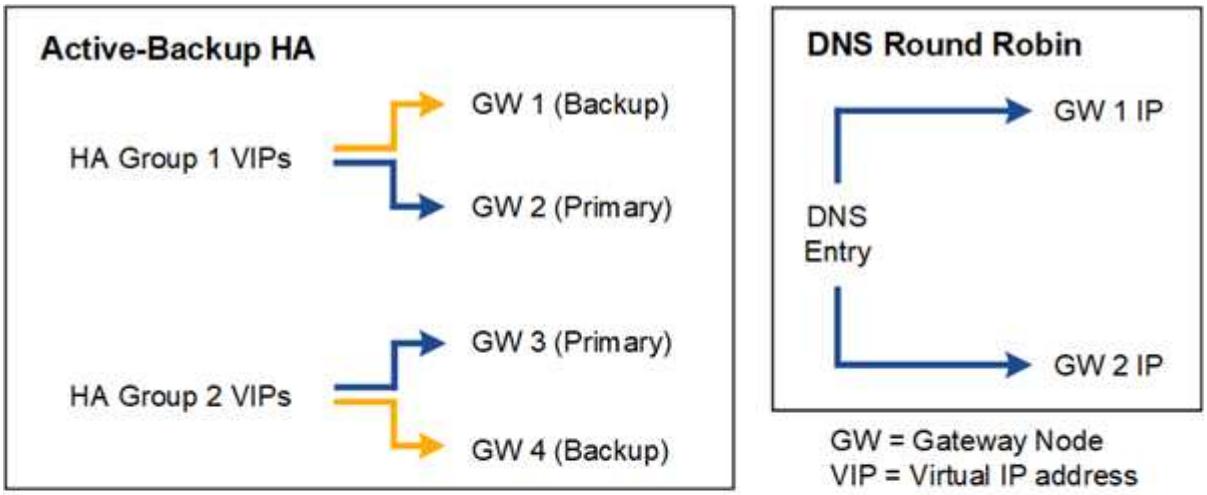
${post_edited_translations.segment}

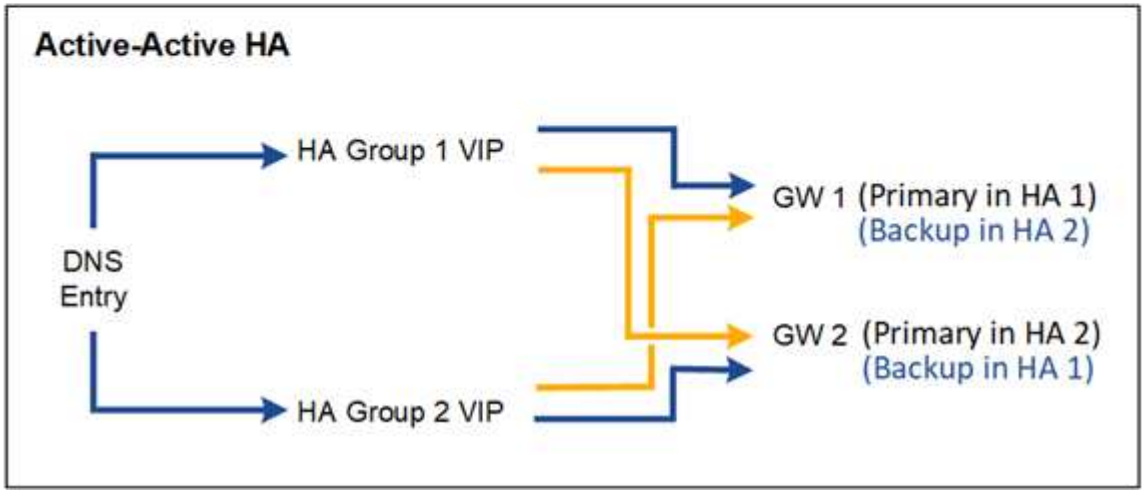
當主要管理節點無法使用時，無法執行某些維護程序。在容錯移轉期間，您可以使用 Grid Manager 來監控您的 StorageGRID 系統。

StorageGRID 高可用性群組的設定選項

以下圖表提供了配置高可用性（ HA ）群組的不同方法範例。每個選項都有優點和缺點。

在圖中，藍色表示 HA 群組中的主要介面，黃色表示 HA 群組中的備份介面。





表格總結了圖中所示的每種 HA 組態的優點。

組態	優勢	缺點
Active-Backup HA	• 由 StorageGRID 管理，無任何外部相依性。 • 快速故障轉移。	• HA 群組中只有一個節點處於作用中狀態。每個 HA 群組中至少有一個節點處於閒置狀態。
DNS 循環配置	• 提高彙總處理量。 • 沒有閒置主機。	• 故障轉移速度較慢，可能取決於用戶端行為。 • 需要在 StorageGRID 之外設定硬體。 • 需要客戶實施資訊健檢。

組態	優勢	缺點
主動-主動 HA	• 流量分佈在多個 HA 群組。 • 彙總處理量高，可隨 HA 群組的數量而擴充。 • 快速故障轉移。	• 設定起來更複雜。 • 需要在 StorageGRID 之外設定硬體。 • 需要客戶實施資訊健檢。

在 **StorageGRID** 中設定高可用性群組

${post_edited_translations.segment}

StorageGRID 系統最多可以有 255 個 HA 群組。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 如果您計劃在 HA 群組中使用 VLAN 介面，您已建立該 VLAN 介面。請參閱 "設定 VLAN 介面"。
- 如果您打算為 HA 群組中的節點使用存取介面，則您已建立了該介面：
  - **Linux** （安裝節點之前）："建立節點組態檔"
  - **Linux** （安裝節點後）："${post_edited_translations.segment}"
  - **VMware**（節點安裝完成後）："${post_edited_translations.segment}"

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。如需支援版本的清單，請參閱 "NetApp 互作業性矩陣工具（IMT）"。

建立高可用度群組

當您建立高可用度群組時，您會選取一或多個介面，並依優先順序進行組織。然後，您會將一或多個 VIP 位址指派給該群組。

若要將介面納入高可用度（HA）群組，此介面必須屬於閘道節點或管理節點。一個 HA 群組對於任何指定節點只能使用一個介面；但是，同一節點的其他介面可以用於其他 HA 群組。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Network** > **High availability groups**。
2. 選擇 **Create** 。

輸入 **HA** 群組的詳細資料

步驟

1. 請為 HA 群組提供唯一名稱。
2. （可選）輸入 HA 群組的執行摘要。

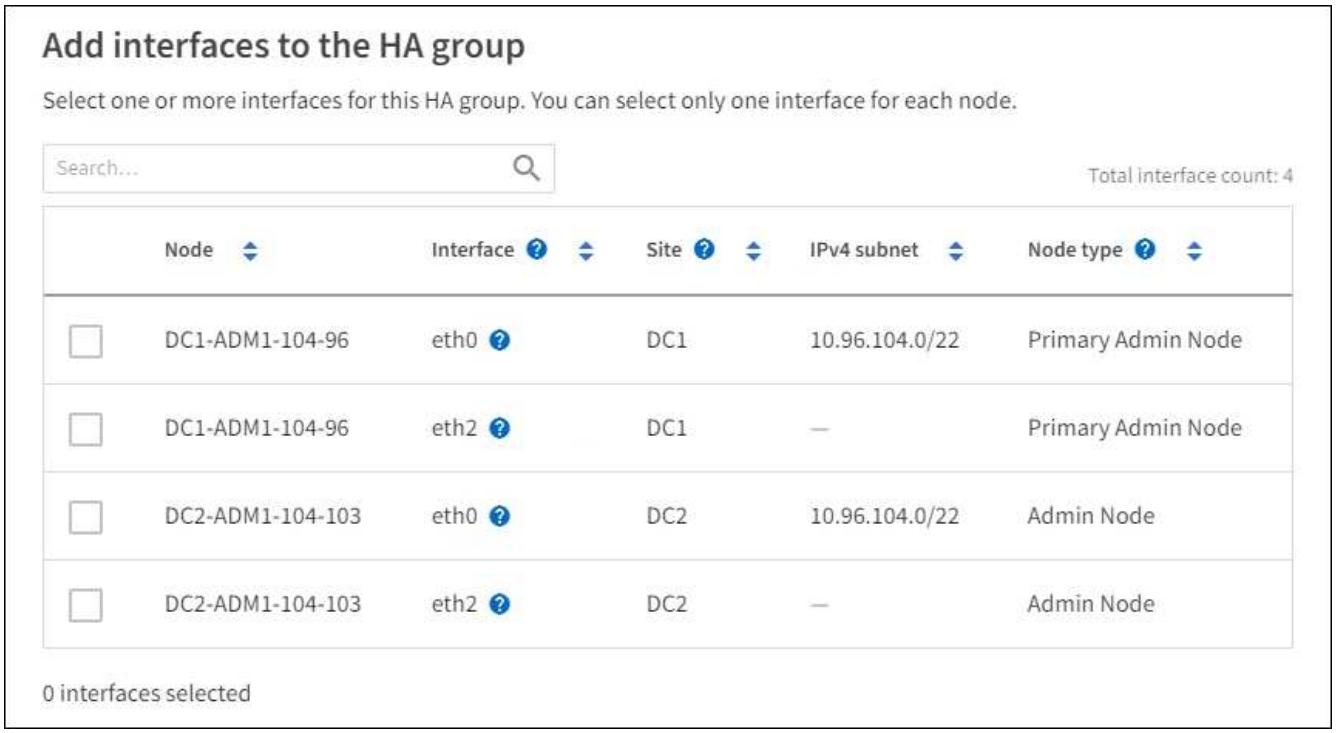
3. 選擇 **Continue** 。

將介面新增至 **HA** 群組

步驟

1. ${post_edited_translations.segment}

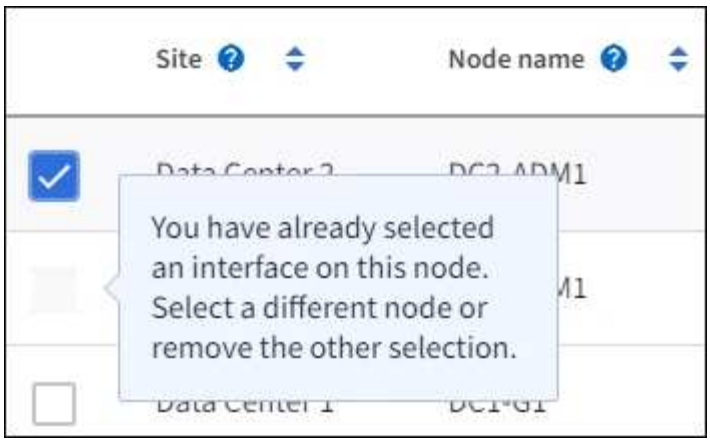
   ${post_edited_translations.segment}



   ${post_edited_translations.segment}

   介面選擇指南

   - ${post_edited_translations.segment}
   - 一個節點只能選擇一個介面。
   - ${post_edited_translations.segment}
   - 如果 HA 群組用於 S3 用戶端流量的 HA 保護，請選擇管理節點、閘道節點或兩者上的介面。
   - 如果您在不同類型的節點上選取介面，則會出現提示附註。系統會提醒您，如果發生容錯移轉，先前作用中節點所提供的服務可能無法在新作用中的節點上使用。例如，備份閘道節點無法提供管理節點服務的 HA 保護。同樣地，備份管理節點無法執行主要管理節點所能提供的所有維護程序。
   - 如果您無法選取介面，其核取方塊會被停用。工具提示會提供更多資訊。



- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

2. 選擇 **Continue** 。

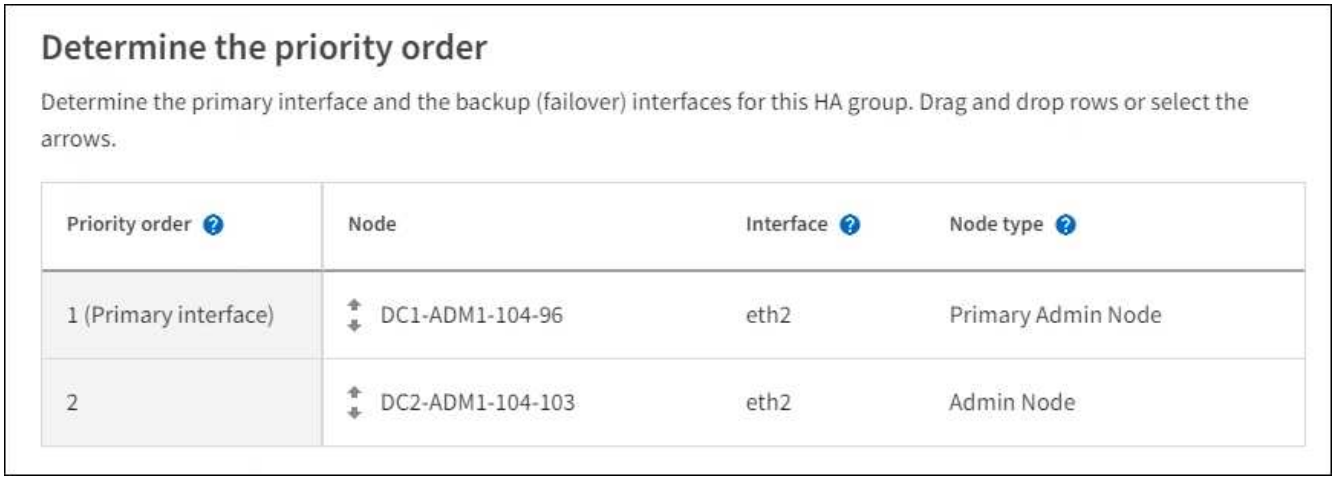
${post_edited_translations.segment}

如果 HA 群組包含多個介面，您可以決定哪個是主要介面，哪些是備份（容錯移轉）介面。如果主要介面發生故障，VIP 位址會移至可用度最高的優先順序介面。如果該介面發生故障，VIP 位址會移至下一個可用度最高的優先順序介面，依此類推。

步驟

1. ${post_edited_translations.segment}

   清單中的第一個介面是主要介面。除非發生故障，否則主要介面為作用中介面。



> 如果 HA 群組提供對 Grid Manager 的存取，則必須在主要管理節點上選擇一個介面作為主要介面。某些維護程序只能從主要管理節點執行。

2. 選擇 **Continue** 。

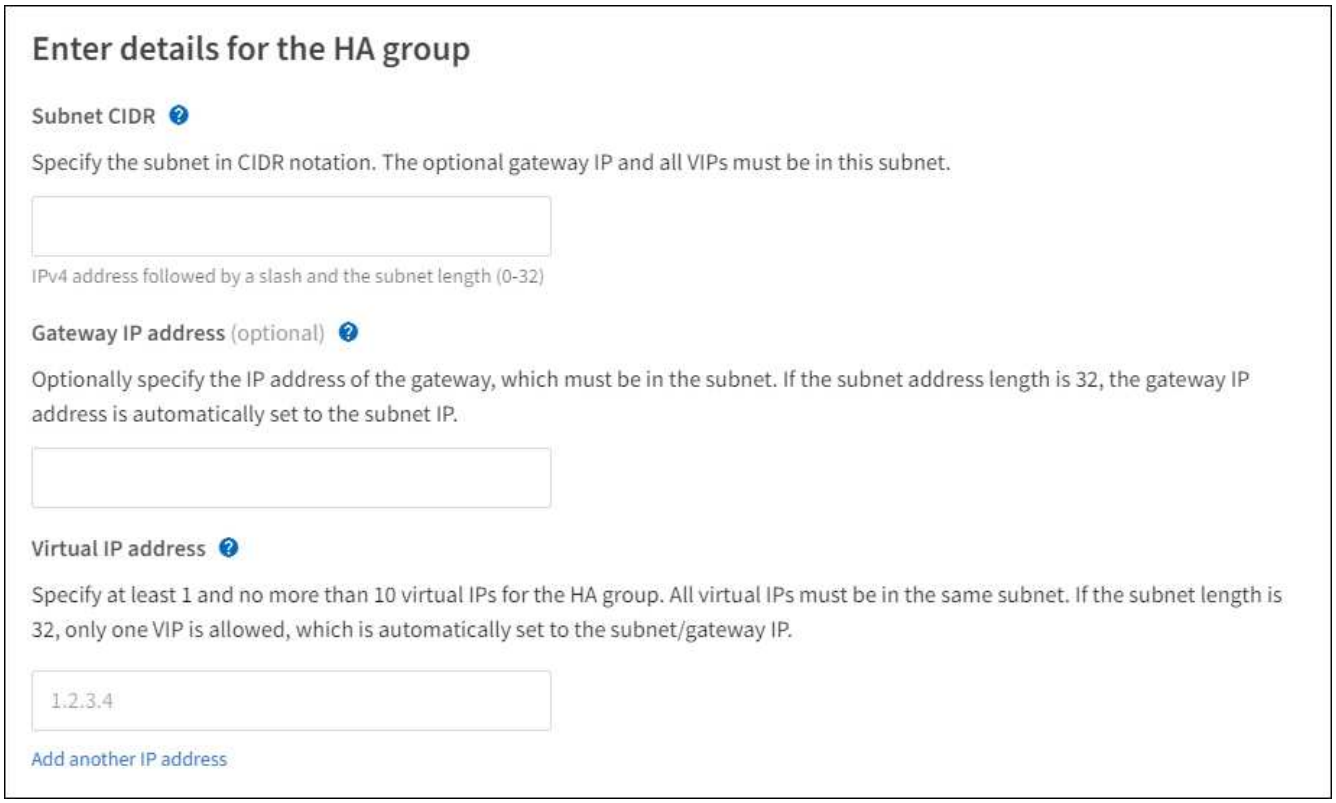
${post_edited_translations.segment}

步驟

1. 在 子網路 **CIDR** 欄位中，以 CIDR 表示法指定 VIP 子網路——IPv4 位址後面接著一個斜槓和子網路長度（0-32）。

   網路位址不得設定任何主機位元。例如 `192.16.0.0/22`。

   如果使用 32 位元前綴，則 VIP 網路位址也可用作閘道位址和 VIP 位址。



2. 如果任何 S3 管理用戶端或租戶用戶端將從不同的子網路存取這些 VIP 位址，則可選擇輸入*閘道 IP 位址*。閘道位址必須位於 VIP 子網路內。

   用戶端和管理員用戶將使用此閘道存取虛擬 IP 位址。

3. 輸入至少一個且不超過十個 VIP 位址，供 HA 群組中的作用中介面使用。所有 VIP 位址都必須在 VIP 子網路內，且所有位址都將同時在作用中介面上處於作用中狀態。

   您必須提供至少一個 IPv4 位址。您也可以選擇指定其他 IPv4 和 IPv6 位址。

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

後續步驟

如果您將使用此 HA 群組進行負載平衡，請建立負載平衡器端點以決定連接埠與網路傳輸協定，並附加任何必要的憑證。請參閱 "設定負載平衡器端點"。

${post_edited_translations.segment}

您可以編輯高可用度 (HA) 群組，以變更其名稱和執行摘要、新增或移除介面、變更優先順序，或新增或更新虛擬 IP 位址。

例如，如果您想要在網站或節點退役過程中移除與選定介面關聯的節點，則可能需要編輯 HA 群組。

步驟

1. 選擇 **Configuration** > **Network** > **High availability groups**。

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   - 選擇 **Actions** > **Edit virtual IP address** 以新增或移除 VIP 位址。
   - ${post_edited_translations.segment}
4. 如果您選擇了「編輯虛擬 IP 位址」：
   a. 更新 HA 群組的虛擬 IP 位址。
   b. 選取 **Save** 。
   c. 選擇 **Finish** 。
5. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. （可選）選取或取消選取核取方塊以新增或移除介面。

      如果 HA 群組提供對 Grid Manager 的存取，則必須在主要管理節點上選取一個介面作為主要介面。某些維護程序只能從主要管理節點執行。

   c. ${post_edited_translations.segment}
   d. （可選）更新虛擬 IP 位址。
   e. 選擇*儲存*，然後選擇*完成*。

${post_edited_translations.segment}

您可以一次移除一個或多個高可用度（HA）群組。

如果 HA 群組已繫結至負載平衡端點，則無法將其移除。若要刪除 HA 群組，您必須將其從任何使用該群組的負載平衡端點中移除。

為防止用戶端服務中斷，請在移除 HA 群組之前更新所有受影響的 S3 用戶端應用程式。更新每個用戶端，使其使用另一個 IP 位址連線，例如，使用不同 HA 群組的虛擬 IP 位址，或使用安裝期間為介面設定的 IP 位址。

步驟

1. 選擇 **Configuration** > **Network** > **High availability groups**。
2. 檢視您要移除之每個 HA 群組的 負載平衡器端點 欄。如果列出任何負載平衡器端點：
   a. 前往 組態 > 網路 > 負載平衡器端點。

b. 選取端點的核取方塊。

c. ${post_edited_translations.segment}

d. 更新綁定模式以移除 HA 群組。

e. 選擇 **Save changes** 。

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

您選擇的所有高可用度群組均已移除。高可用度群組頁面上將顯示綠色成功橫幅。

管理負載平衡

了解 **StorageGRID** 負載平衡

${post_edited_translations.segment}

${post_edited_translations.segment}

當用戶端應用程式從 StorageGRID 系統儲存或擷取資料時，StorageGRID 使用負載平衡器來管理擷取和擷取工作負載。負載平衡透過將工作負載分配到多個儲存節點，以最大化速度和連線容量。

StorageGRID 負載平衡器服務安裝在所有管理節點和所有閘道節點上，提供第 7 層負載平衡。它執行用戶端請求的傳輸層安全性 (TLS) 終止，檢查請求，並與儲存節點建立新的安全連線。

每個節點上的負載平衡服務在將用戶端流量轉送到儲存節點時獨立運作。負載平衡服務透過加權過程，將更多請求路由到 CPU 可用度更高的儲存節點。

儘管 StorageGRID 負載平衡器服務是建議的負載平衡機制，但您也可以選擇整合第三方負載平衡器。有關資訊，請聯繫您的 NetApp 客戶代表或參閱 "將第三方負載平衡器與 StorageGRID 結合使用"。

${post_edited_translations.segment}

作為通用最佳實務做法，StorageGRID 系統中的每個站台都應包含兩個或多個執行負載平衡服務的節點。例如，一個站台可以包含兩個閘道節點，或同時包含一個管理節點和一個閘道節點。無論您使用的是服務應用裝置、裸機節點或虛擬機器 （VM） 型節點，請確保每個負載平衡節點都擁有足夠的連網、硬體或虛擬化基礎架構。

${post_edited_translations.segment}

負載平衡器端點定義了傳入與傳出的用戶端應用程式要求用來存取包含 Load Balancer 服務之節點的連接埠與網路傳輸協定（HTTPS 或 HTTP）。此端點還定義了用戶端類型（S3）、繫結模式，以及選用的允許或封鎖租戶清單。

若要建立負載平衡器端點，可以使用 Grid Manager，也可以完成 S3 設定和 FabricPool 精靈：

- "設定負載平衡器端點"
- "使用 S3 設定精靈"
- "使用 FabricPool 設定精靈"

${post_edited_translations.segment}

當工作負載僅處理部分資料並多次存取物件時，快取可顯著提升效能。此外，快取還允許在無需完整部署網格的情況下遠端存取物件儲存。負載平衡器快取僅適用於閘道節點。

${post_edited_translations.segment}

- 僅對可快取的工作負載啟用快取。如果工作負載存取未快取資料的頻率高於存取已快取資料的頻率，則其效能會低於未使用快取的情況。在某些情況下，高覆蓋率和高驅逐率的工作負載也可能超出硬碟寫入壽命的保證範圍。
- 考慮新增額外的端點或節點來快取適合快取的個別工作負載。
- 對可快取的和不可快取的工作負載使用不同的端點。這種分離可確保快取機制得到正確套用，且不會干擾不可快取的資料處理。
- 透過將潛在可快取的工作負載導向啟用快取的端點來評估其潛力。監控並驗證快取命中率，以確定該工作負載是否適合快取。此評估有助於最佳化效能並確保有效利用快取資源。
- "${post_edited_translations.segment}" 以確定現有的工作負載是否適合進行快取。在指定的時間段內，確定 GET 要求中針對唯一物件的百分比。若要適合進行快取，此值應低於 50%。

適合使用快取的工作負載範例

- ${post_edited_translations.segment}
- 高效能運算（HPC）
- AI/ML 訓練
- ${post_edited_translations.segment}
- 媒體資產管理
- 影片製作

- 可以快取多個物件版本。
- ${post_edited_translations.segment}

不適合使用快取的工作負載範例

- FabricPool
- 備份應用程式
- 儲存分層

如果快取中要提供的任何內容需要靜態加密， "啟用節點或磁碟機加密"在快取節點上。

不會被快取的物件和請求類型

- 此 `response-content-encoding`查詢參數
- 該 `partNumber` 查詢參數
- 條件標頭
  - `If-Match`

- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

- 使用以下任一方式進行靜態加密的請求：
  - SSE（使用 StorageGRID 管理的金鑰進行伺服器端加密）
  - SSE-C（使用客戶提供的金鑰進行伺服器端加密）
  - 儲存物件加密

任何未快取的請求都會轉送到上游 LDR，就如同快取未啟用一樣。

相關資訊

- "${post_edited_translations.segment}"
- 如需負載平衡器快取的詳細資訊，請聯絡技術支援。

${post_edited_translations.segment}

負載平衡器端點的連接埠在您建立第一個端點時預設為 10433，但您可以指定 1 到 65535 之間的任何未使用外部連接埠。如果您使用連接埠 80 或 443，端點將僅在閘道節點上使用負載平衡器服務。這些連接埠在管理節點上已保留。如果您將相同的連接埠用於多個端點，則必須為每個端點指定不同的繫結模式。

不允許使用其他網格服務使用的連接埠。參見"StorageGRID 內部連接埠"。

網路傳輸協定的注意事項

大多數情況下，用戶端應用程式與 StorageGRID 之間的連線應使用傳輸層安全性協定 （TLS） 加密。雖然支援不使用 TLS 加密連接到 StorageGRID，但不建議這樣做，尤其是在生產環境中。為 StorageGRID 負載平衡器端點選擇網路傳輸協定時，應選擇 **HTTPS**。

負載平衡器端點憑證的注意事項

如果您選擇 **HTTPS** 作為負載平衡器端點的網路傳輸協定，則必須提供安全性憑證。建立負載平衡器端點時，您可以使用以下三種選項中的任何一種：

- 上傳已簽署的憑證（建議使用）。此憑證可由公開信任或私有的憑證授權單位（CA）簽署。使用公開信任的 CA 伺服器憑證來保護連線安全性是最佳實務做法。與產生的憑證相比，由 CA 簽署的憑證可以不中斷地進行輪替，這有助於避免過期問題。

  ${post_edited_translations.segment}

  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - （可選）包含每個中間頒發憑證授權單位之憑證的 CA 套裝組合。
- ${post_edited_translations.segment}
- 使用全域 **StorageGRID S3** 憑證。您必須先上傳或產生此憑證的自訂版本，才能為負載平衡器端點選取該憑證。請參閱 "設定 S3 API 憑證"。

我需要哪些數值？

要建立證書，您必須知道 S3 用戶端應用程式將用於存取端點的所有網域名稱和 IP 位址。

憑證的 **Subject DN**（Distinguished Name）條目必須包含用戶端應用程式將用於 StorageGRID 的完整網域名稱。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

根據需要，憑證可以使用萬用字元來表示執行負載平衡器服務的所有管理節點和閘道節點的完整網域名稱。例如，`*.storagegrid.example.com`使用 * 萬用字元來表示 `adm1.storagegrid.example.com`和 `gn1.storagegrid.example.com`。

如果您計劃使用 S3 虛擬主機樣式要求，則憑證還必須為您設定的每個 "S3 端點網域名稱" 包含一個「替代名稱」項目，包括任何萬用字元名稱。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果您在網域名稱中使用萬用字元，請審查 "伺服器憑證強化準則"。

您也必須為安全性憑證中的每個名稱定義一個 DNS 項目。

如何管理即將過期的憑證？

${post_edited_translations.segment}

${post_edited_translations.segment}

- 仔細監控任何警告憑證即將到期的警示，例如「負載平衡器端點憑證即將到期」和「S3 API 全域伺服器憑證即將到期」警示。
- 請務必保持 StorageGRID 與 S3 應用程式的憑證版本同步。如果您取代或更新用於負載平衡器端點的憑證，則必須取代或更新 S3 應用程式所使用的同等憑證。
- 使用公開簽署的 CA 憑證。如果使用由 CA 簽署的憑證，則可以無中斷地更換即將到期的憑證。
- ${post_edited_translations.segment}

結合模式的考量因素

綁定模式可讓您控制哪些 IP 位址可用於存取負載平衡器端點。如果端點使用綁定模式，則用戶端應用程式只能使用允許的 IP 位址或其對應的完整網域名稱 （FQDN） 存取該端點。使用任何其他 IP 位址或 FQDN 的用戶端應用程式都無法存取該端點。

您可以指定以下任一種綁定模式：

- **Global** （預設）：用戶端應用程式可以使用任何 Gateway 節點或 Admin 節點的 IP 位址、任何網路上的任何 HA 群組的虛擬 IP （VIP） 位址或對應的 FQDN 來存取端點。除非您需要限制端點的存取能力，否則請使用此設定。

- **HA** 群組的虛擬 **IP** 位址。用戶端應用程式必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）。
- 節點介面。用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN）。
- 節點類型。根據您選取的節點類型，用戶端必須使用任何 Admin Node 的 IP 位址（或對應的 FQDN），或是任何 Gateway Node 的 IP 位址（或對應的 FQDN）。

租戶存取的考慮因素

租戶存取是一項選用的安全性功能，可讓您控制哪些 StorageGRID 租戶帳戶可以使用負載平衡器端點來存取其 bucket。您可以允許所有租戶存取端點（預設），也可以針對每個端點指定允許或封鎖的租戶清單。

您可以使用此功能在租戶及其端點之間提供更好的安全性隔離。例如，您可以使用此功能來確保某個租戶擁有的極機密或高度機密資料完全無法被其他租戶存取。

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
   - **Public** 端點：使用連接埠 10443，允許所有租戶存取。
   - *絕密*端點：使用連接埠 10444，僅允許 *絕密*租戶存取。所有其他租戶均無法存取此端點。
2. 它 `top-secret.pdf`位於屬於 **Top secret** 租戶的儲存桶中。

若要存取 `top-secret.pdf`，**Top secret** 租戶中的使用者可以向 `\https://w.x.y.z:10444/top-secret.pdf`發出 GET 要求。因為此租戶允許使用 10444 端點，所以使用者可以存取該物件。然而，如果屬於任何其他租戶的使用者向相同的 URL 發出相同的要求，他們會立即收到「拒絕存取」訊息。即使認證和簽署有效，存取仍會被拒絕。

CPU 可用度

每個管理節點和閘道節點上的負載平衡器服務在將 S3 流量轉送到儲存節點時獨立運作。負載平衡器服務透過加權機制，將更多請求路由到 CPU 可用度更高的儲存節點。節點 CPU 負載資訊每隔幾分鐘更新一次，但權重更新頻率可能更高。所有儲存節點都會被指派一個最小基準權重值，即使某個節點報告的使用率達到 100% 或未能報告其使用率。

在某些情況下，有關 CPU 可用度的資訊僅限於負載平衡器服務所在的站點。

配置 **StorageGRID** 負載平衡器端點

負載平衡器端點決定了 S3 用戶端連線至 Gateway 節點和管理節點上的 StorageGRID 負載平衡器時可使用的連接埠和網路傳輸協定。您也可以使用端點存取 Grid Manager 、Tenant Manager 或兩者。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 您已審閱 "負載平衡的考量因素"。

- 如果您先前重新對應了打算用於負載平衡器端點的連接埠，您有 "移除連接埠重映射"。
- 您已建立任何計劃使用的高可用度（HA）群組。建議使用 HA 群組，但並非必要。請參閱 "管理高可用度群組"。
- 如果負載平衡器端點將由 "S3 Select 的 S3 租戶" 使用，則不得使用任何裸機節點的 IP 位址或 FQDN。用於 S3 Select 的負載平衡器端點僅允許使用服務應用裝置和微軟 VMware 基礎的軟體節點。
- 您已設定任何計劃使用的 VLAN 介面。請參閱 "設定 VLAN 介面"。
- ${post_edited_translations.segment}

  ${post_edited_translations.segment}

  - 要上傳憑證，您需要伺服器憑證、憑證私密金鑰，以及（可選）CA 套裝組合。
  - 若要產生憑證，您需要 S3 用戶端用來存取端點的所有網域名稱和 IP 位址。您也必須知道主旨（辨識名稱）。
  - 如果您想使用 StorageGRID S3 API 憑證（該憑證也可用於直接連線至儲存節點），您已將預設憑證取代為由外部憑證授權單位簽署的自訂憑證。請參閱"設定 S3 API 憑證"。

${post_edited_translations.segment}

每個 S3 用戶端負載平衡器端點都指定一個連接埠、用戶端類型（S3）和網路傳輸協定（HTTP 或 HTTPS）。管理介面負載平衡器端點指定一個連接埠、介面類型和非信任用戶端網路。

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. 若要為 S3 用戶端建立端點，請選擇「S3 用戶端」標籤。
3. ${post_edited_translations.segment}
4. 選擇 **Create** 。

輸入端點詳細資料

步驟

1. ${post_edited_translations.segment}

${post_edited_translations.segment}

欄位	說明
Name	端點的描述性名稱，將顯示在負載平衡器端點頁面的表格中。
連接埠	您要用於負載平衡的 StorageGRID 連接埠。對於您建立的第一個端點，此欄位預設為 10433，但您可以輸入 1 到 65535 之間任何未使用的外部連接埠。 如果輸入 **80** 或 **8443**，則端點僅在 Gateway 節點上設定，除非您已釋放連接埠 8443。然後，您可以將連接埠 8443 用作 S3 端點，該連接埠將同時在 Gateway 節點和 Admin 節點上設定。
用戶端類型	必須是*S3*。
網路傳輸協定	用戶端連接到此端點時將使用的網路傳輸協定。 • 選擇 **HTTPS** 以進行安全的 TLS 加密通訊（建議使用）。您必須先附加安全性憑證，才能儲存端點。 • 選擇 **HTTP** 表示較不安全的未加密通訊。僅在非生產網格中使用 HTTP。
${post_edited_translations.segment}	啟用或停用此負載平衡器端點的 "${post_edited_translations.segment}"。 如果快取發生問題，請參閱 "${post_edited_translations.segment}"。

管理介面

欄位	說明
Name	端點的描述性名稱，將顯示在負載平衡器端點頁面的表格中。
連接埠	${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment} • ${post_edited_translations.segment} 注意：您可以使用這些預設連接埠或其他可用連接埠。
介面類型	${post_edited_translations.segment}
不受信任的用戶端網路	如果此端點應可供不受信任的用戶端網路存取，請選取 是。否則，請選取 否。 選擇「是」後，該連接埠將在所有不受信任的用戶端網路上開啟。 注意：只有在建立負載平衡器端點時，才能設定連接埠對不受信任的用戶端網路開啟或關閉。

1. 選擇 **Continue** 。

選擇綁定模式

步驟

1. ${post_edited_translations.segment}

   某些綁定模式可用於用戶端端點或管理介面端點。此處列出兩種端點類型的所有模式。

模式	說明
全域（用戶端端點的預設值）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （VIP） 位址或對應的 FQDN 存取端點。 除非需要限制此端點的存取能力，否則請使用*全域*設定。
HA 群組的虛擬 IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN）才能存取此端點。 具有此綁定模式的端點都可以使用相同的連接埠號，只要您為端點選擇的 HA 群組不重疊即可。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN）來存取此端點。
節點類型（僅限用戶端端點）	根據您選擇的節點類型，用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）或任何閘道節點的 IP 位址（或對應的 FQDN）來存取此端點。
${post_edited_translations.segment}	用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN）來存取此端點。

   如果多個端點使用同一個連接埠，StorageGRID 將按以下優先順序決定使用哪個端點：**HA** 群組的虛擬 **IP** > 節點介面 > 節點類型 > 全域。

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}

   如果您要建立管理介面端點，請選擇僅與管理節點關聯的 VIP。

3. ${post_edited_translations.segment}
4. 如果您選擇了*節點類型*，請選擇「管理節點」（包括主要管理節點和任何非主要管理節點）或「閘道節點」。

控制租戶存取

> 只有當管理介面端點具有 租戶管理器的介面類型 時，該端點才能控制租戶存取。

步驟

1. 在「租戶存取」步驟中，請選擇下列選項之一：

欄位	說明
允許所有租戶（預設）	${post_edited_translations.segment} 如果您尚未建立任何租戶帳戶，則必須選擇此選項。新增租戶帳戶後，您可以編輯負載平衡器端點以允許或封鎖特定帳戶。
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	選定的租戶帳戶無法使用此端點存取其儲存桶。所有其他租戶均可使用此端點。

2. 如果您要建立的是 **HTTP** 端點，則無需附加憑證。選取 **Create** 以新增負載平衡器端點。然後，前往 完成後。否則，請選取 **Continue** 以附加憑證。

附上證書

步驟

1. 如果您要建立 **HTTPS** 端點，請選擇要附加到端點的安全性憑證類型。

   ${post_edited_translations.segment}

   - 上傳憑證。如果您有自訂憑證需要上傳，請選擇此選項。
   - 產生證書。如果您擁有產生自訂憑證所需的值，請選擇此選項。
   - 使用 **StorageGRID S3** 憑證。如果您想使用全域 S3 API 憑證，請選擇此選項，該憑證也可用於直接連線至儲存節點。

     除非您已將網格 CA 簽署的預設 S3 API 憑證，替換為外部憑證授權單位簽署的自訂憑證，否則您無法選擇此選項。請參閱 "設定 S3 API 憑證"。

   - 使用管理介面憑證。如果您想要使用全域管理介面憑證，請選取此選項，此憑證也可用於直接連線至 Admin Nodes。
2. 如果您未使用 StorageGRID S3 憑證，請上傳或產生該憑證。

上傳證書

a. 選擇 **Upload certificate**。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：PEM 編碼的自訂伺服器憑證檔案。
   - 憑證私鑰：自訂伺服器憑證私鑰檔案 (`.key`)

     EC 私鑰必須至少 224 位元。RSA 私鑰必須至少 2048 位元。

   - **CA** 套裝組合：包含來自每個中介發行憑證授權單位（CA）憑證的單一選用檔案。此檔案應包含每個 PEM 編碼的 CA 憑證檔案，並依憑證鏈順序串接。

c. 展開 憑證詳細資料 以檢視您上傳之每個憑證的中繼資料。如果您上傳了選用的 CA 套裝組合，每個憑證都會顯示在各自的索引標籤上。

   - ${post_edited_translations.segment}

     指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

   例如： `storagegrid_certificate.pem`

   - 選擇「複製憑證 PEM」或「複製 CA 套裝組合 PEM」以複製憑證內容並貼上到其他位置。

d. 選取 **Create**。+ 負載平衡器端點已建立。自訂憑證將用於 S3 用戶端或管理介面與端點之間後續的所有新連線。

產生證書

a. 選擇 **Generate certificate**。

b. 請提供憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用 * 做為萬用字元來代表多個網域名稱。
IP	憑證中要包含的一個或多個 IP 位址。
${post_edited_translations.segment}	X.509 憑證擁有者的主旨或可分辨名稱 (DN)。 如果此欄位中未輸入任何值，則產生的憑證將使用第一個網域名稱或 IP 位址作為主旨通用名稱 (CN)。
${post_edited_translations.segment}	${post_edited_translations.segment}

欄位	說明
${post_edited_translations.segment}	如果選取（預設且建議），則會將金鑰用途和擴充金鑰用途擴充功能新增至產生的憑證。 這些擴充定義了憑證中包含的金鑰的用途。 ${post_edited_translations.segment}

c. 選擇 **Generate** 。

d. ${post_edited_translations.segment}

- 選取 **Download certificate** 以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名 `.pem`儲存檔案。

例如： `storagegrid_certificate.pem`

- 選擇 **Copy certificate PEM** 以複製憑證內容並貼到其他位置。

e. 選擇 **Create** 。

負載平衡器端點已建立。自訂憑證將用於 S3 用戶端或管理介面與此端點之間的所有後續新連線。

完成後

步驟

1. ${post_edited_translations.segment}

   您在 DNS 記錄中輸入的 IP 位址取決於您是否使用負載平衡節點的 HA 群組：

   - 如果您設定了 HA 群組，用戶端將連線到該 HA 群組的虛擬 IP 位址。
   - 如果您不使用 HA 群組，用戶端將使用閘道節點或管理節點的 IP 位址連線至 StorageGRID 負載平衡器服務。

     您還必須確保 DNS 記錄參照所有必要的端點網域名稱，包括任何萬用字元名稱。

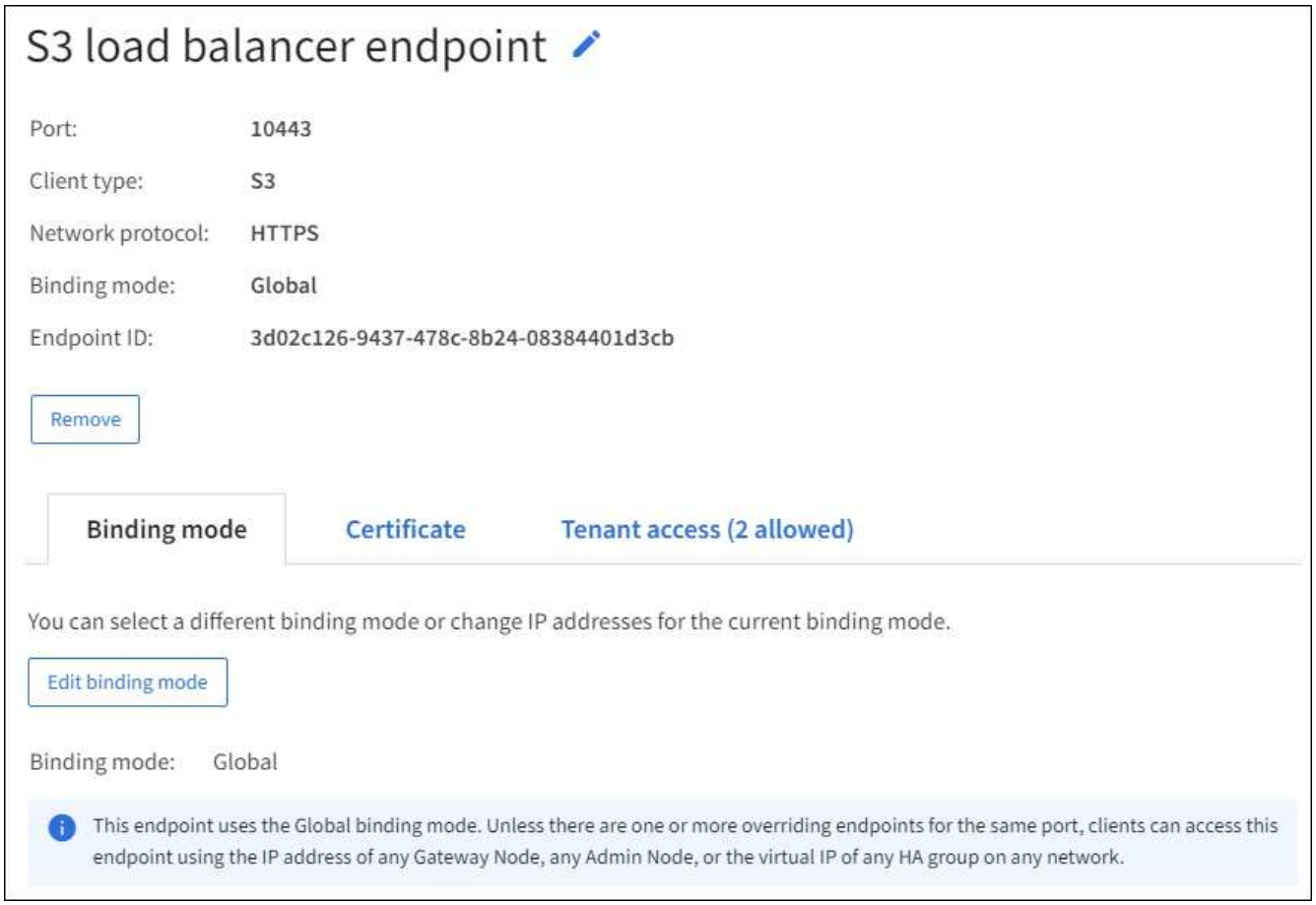
2. 向 S3 用戶端提供連接到端點所需的資訊：
   - 連接埠號
   - 完整網域名稱或 IP 位址
   - 任何所需的憑證詳細資料

檢視並編輯負載平衡器端點

您可以檢視現有負載平衡器端點的詳細資訊，包括安全端點的憑證中繼資料。您也可以變更端點的某些設定。

- ${post_edited_translations.segment}

- 若要檢視特定端點的所有詳細資訊（包括憑證中繼資料），請在表格中選擇該端點的名稱。顯示的資訊會根據端點類型及其組態方式而有所不同。



- ${post_edited_translations.segment}

如果在編輯管理介面端點的連接埠時失去對 Grid Manager 的存取，請更新 URL 和連接埠以重新取得存取權限。

${post_edited_translations.segment}

任務	操作選單	詳細資料頁面
編輯端點名稱	a. 選取端點的核取方塊。 b. 選擇 **Actions** > **Edit endpoint name**。 c. 請輸入新名稱。 d. 選取 **Save** 。	a. 選擇端點名稱以顯示詳細資訊。 b. 選擇編輯圖示 。 c. 請輸入新名稱。 d. 選取 **Save** 。

任務	操作選單	詳細資料頁面
編輯端點埠	a. 選取端點的核取方塊。 b. 選擇 **Actions** > **Edit endpoint port** c. 請輸入有效的連接埠號碼。 d. 選取 **Save** 。	*n/a*
${post_edited_translations.segment}	a. 選取端點的核取方塊。 b. ${post_edited_translations.segment} c. 視需要更新繫結模式。 d. 選擇 **Save changes** 。	a. 選擇端點名稱以顯示詳細資訊。 b. 選取 **Edit binding mode**。 c. 視需要更新繫結模式。 d. 選擇 **Save changes** 。
編輯端點憑證	a. 選取端點的核取方塊。 b. 選擇 **Actions** > **Edit endpoint certificate**。 c. ${post_edited_translations.segment} d. 選擇 **Save changes** 。	a. 選擇端點名稱以顯示詳細資訊。 b. ${post_edited_translations.segment} c. 選擇 **Edit certificate**。 d. ${post_edited_translations.segment} e. 選擇 **Save changes** 。
${post_edited_translations.segment}	a. 選取端點的核取方塊。 b. 選擇 **Actions** > **Edit tenant access**。 c. 選擇不同的存取選項，從清單中選擇或移除租戶，或兩者都執行。 d. 選擇 **Save changes** 。	a. 選擇端點名稱以顯示詳細資訊。 b. ${post_edited_translations.segment} c. 選擇 **Edit tenant access**。 d. 選擇不同的存取選項，從清單中選擇或移除租戶，或兩者都執行。 e. 選擇 **Save changes** 。

移除負載平衡器端點

您可以使用「動作」功能表移除一個或多個端點，也可以從詳細資料頁面移除單一端點。

為避免用戶端服務中斷，請在移除負載平衡器端點之前更新所有受影響的 S3 用戶端應用程式。請將每個用戶端更新為使用分配給另一個負載平衡器端點的連接埠進行連線。同時，請務必更新所有必需的憑證資訊。

如果在移除管理介面端點時失去對 Grid Manager 的存取，請更新 URL。

- 若要移除一個或多個端點：
  a. 在負載平衡器頁面中，選取要移除的每個端點的核取方塊。
  b. 選擇 **Actions** > **Remove**。
  c. 選擇 **OK** 。

- 從詳細資料頁面移除一個端點：
  a. 在負載平衡器頁面中，選擇端點名稱。
  b. 在詳細資料頁面選擇 移除。
  c. 選擇 **OK** 。

在 StorageGRID 中設定 S3 端點網域名稱

${post_edited_translations.segment}

不支援使用 IP 位址作為端點網域名稱。未來的版本將禁止這種組態。

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"。
- 您已確認網格升級工作並未進行中。

網格升級進行期間，請勿對網域名稱組態進行任何變更。

關於此任務

若要讓用戶端能夠使用 S3 端點網域名稱，您必須執行下列所有操作：

- ${post_edited_translations.segment}
- 確保"用戶端用於與 StorageGRID 建立 HTTPS 連線的憑證"已對用戶端要求的所有網域名稱進行簽署。

  例如，如果端點是 `s3.company.com`，則必須確保用於 HTTPS 連線的憑證包含 `s3.company.com`端點和端點的萬用字元主體替代名稱 （SAN）： `*.s3.company.com`。

- 設定用戶端所使用的 DNS 伺服器。請加入用戶端用來建立連線之 IP 位址的 DNS 記錄，並確保這些記錄參照所有必要的 S3 端點網域名稱，包括任何萬用字元名稱。

用戶端可以透過閘道節點、管理節點或儲存節點的 IP 位址連接到 StorageGRID，也可以透過連接到高可用度群組的虛擬 IP 位址來連接。您應該了解用戶端應用程式如何連接到網格，以便在 DNS 記錄中包含正確的 IP 位址。

使用 HTTPS 連線（建議）存取網格的用戶端可以使用下列任一憑證：

- 連接到負載平衡器端點的用戶端可以使用該端點的自訂憑證。每個負載平衡器端點都可以設定為識別不同的 S3 端點網域名稱。
- 連接到負載平衡器端點或直接連接到儲存節點的用戶端可以自訂全域 S3 API 憑證，以包含所有必要的 S3 端點網域名稱。

如果您不新增 S3 端點網域名稱且清單為空，則會停用對 S3 虛擬託管式請求的支援。

新增 **S3** 端點網域名稱

步驟

1. 選擇 **Configuration** > **Network** > **S3 endpoint domain names**。
2. 在 **Domain name 1** 欄位中輸入網域名稱。選取 **Add another domain name** 以新增更多網域名稱。
3. 選取 **Save** 。
4. 確保用戶端使用的伺服器憑證與所需的 S3 端點網域名稱相符。
   - 如果用戶端連接到使用自身憑證的負載平衡器端點，"${post_edited_translations.segment}"。
   - 如果用戶端連接到使用全域 S3 API 憑證的負載平衡器端點或直接連接到儲存節點，"${post_edited_translations.segment}"。
5. ${post_edited_translations.segment}

結果

現在，當用戶端使用端點 *bucket.s3.company.com* 時，DNS 伺服器會解析為正確的端點，且憑證會如預期驗證端點。

${post_edited_translations.segment}

如果變更 S3 應用程式使用的名稱，虛擬託管式請求將會失敗。

步驟

1. 選擇 **Configuration** > **Network** > **S3 endpoint domain names**。
2. ${post_edited_translations.segment}
3. 選取 **Save** 。
4. 選取 **Yes** 以確認您的變更。

刪除 **S3** 端點網域名稱

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Network** > **S3 endpoint domain names**。
2. 選擇網域名稱旁邊的刪除圖示 ✕。
3. ${post_edited_translations.segment}

相關資訊

- "使用 S3 REST API"
- "${post_edited_translations.segment}"
- "設定高可用度群組"

StorageGRID 客戶端連線的 IP 位址和連接埠

為了儲存或擷取物件，S3 用戶端應用程式連接到負載平衡器服務（該服務包含在所有管理節點和閘道節點上），或連接到本機發佈路由器 （LDR） 服務（該服務包含在所有儲存節

點上）。

用戶端應用程式可以使用網格節點的 IP 位址以及該節點上服務的連接埠號碼來連線至 StorageGRID。（選填）您可以建立負載平衡節點的高可用度（HA）群組，以提供使用虛擬 IP（VIP）位址的高可用度連線。如果您想要使用完整網域（FQDN）代替 IP 或 VIP 位址來連線至 StorageGRID，您可以設定 DNS 項目。

此表總結了用戶端連接到 StorageGRID 的不同方式，以及每種連線類型所使用的 IP 位址和連接埠。如果您已建立負載平衡器端點和高可用度 （HA） 群組，請參閱 <<${post_edited_translations.segment}>> 以在 Grid Manager 中找到這些值。

${post_edited_translations.segment}	**${post_edited_translations.segment}**	**IP** 位址	連接埠
${post_edited_translations.segment}	負載平衡器	${post_edited_translations.segment}	指派給負載平衡器端點的連接埠
${post_edited_translations.segment}	負載平衡器	管理節點的 IP 位址	指派給負載平衡器端點的連接埠
閘道節點	負載平衡器	閘道節點的 IP 位址	指派給負載平衡器端點的連接埠
儲存節點	LDR	儲存節點的 IP 位址	預設 S3 連接埠： • HTTPS：18082 • HTTP: 18084

${post_edited_translations.segment}

若要將用戶端應用程式連接到 HA 閘道節點群組的負載平衡器端點，請使用如下所示結構的 URL：

`https://VIP-of-HA-group:LB-endpoint-port`

${post_edited_translations.segment}

`https://192.0.2.5:10443`

${post_edited_translations.segment}

1. 使用 "支援的網頁瀏覽器" 登入 Grid Manager。
2. 尋找網格節點的 IP 位址：
   a. 選取 **Nodes** 。
   b. ${post_edited_translations.segment}
   c. 選擇 **Overview** 標籤。
   d. ${post_edited_translations.segment}
   e. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

- **eth0:** 網格網路
- ${post_edited_translations.segment}
- **eth2:** 用戶端網路（選購）

> ${post_edited_translations.segment}

3. 尋找高可用度群組的虛擬 IP 位址：
   a. 選擇 **Configuration** > **Network** > **High availability groups**。
   b. 在表格中，記下 HA 群組的虛擬 IP 位址。
4. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. 記下您要使用的端點的連接埠號碼。

> 如果連接埠號碼為 80 或 443，則端點僅在 Gateway 節點上設定，因為這些連接埠在 Admin 節點上已保留。所有其他連接埠皆在 Gateway 節點和 Admin 節點上設定。

   c. 從表格中選取端點名稱。
   d. 確認 **Client type**（S3）與將使用該端點的用戶端應用程式相符。

管理網路和連線

配置 StorageGRID 網路設定

您可以透過 Grid Manager 設定各種網路設定，以調校 StorageGRID 系統的運作。

設定 VLAN 介面

您可以"建立虛擬區域網路 (VLAN) 介面"隔離和劃分流量，以提高安全性、靈活度和效能。每個 VLAN 介面都與管理節點和閘道節點上的一個或多個父介面關聯。您可以在高可用度群組和負載平衡器端點中使用 VLAN 介面，以便依應用程式或租戶隔離用戶端或管理流量。

流量分類原則

您可以使用 "流量分類原則" 來識別和處理不同類型的網路流量，包括與特定儲存桶、租戶、用戶端子網路或負載平衡器端點相關的流量。這些原則有助於限制流量和監控。

StorageGRID 網路指南

${post_edited_translations.segment}

請參閱 "${post_edited_translations.segment}" 以了解如何連接 S3 用戶端。

預設 StorageGRID 網路

${post_edited_translations.segment}

如需網路拓撲的詳細資訊，請參閱 "${post_edited_translations.segment}"。

Grid 網路

必要。網格網路用於所有內部 StorageGRID 流量。它提供網格中所有節點之間跨所有站台和子網路的連線能力。

${post_edited_translations.segment}

選用。Admin Network 通常用於系統管理和維護。它也可以用於用戶端傳輸協定存取。Admin Network 通常是私有網路，不需要在站台之間進行路由。

用戶端網路

選用。用戶端網路是一個開放式網路，通常用於提供 S3 用戶端應用程式的存取，以便隔離並保護網格網路。用戶端網路可以與透過本機閘道可連線的任何子網路通訊。

準則

- 每個 StorageGRID 節點都需要一個專用的網路介面、IP 位址、子網路遮罩和閘道，才能連接到它所分配的每個網路。
- ${post_edited_translations.segment}
- 每個網路、每個網格節點僅支援單一閘道，且該閘道必須與節點位於相同的子網路。如有需要，您可以在閘道中實作更複雜的路由。
- ${post_edited_translations.segment}

網路	**${post_edited_translations.segment}**
${post_edited_translations.segment}	eth0
${post_edited_translations.segment}	eth1
${post_edited_translations.segment}	eth2

- 如果節點已連線至 StorageGRID 應用裝置，則每個網路都會使用特定的連接埠。如需詳細資訊，請參閱您應用裝置的安裝說明。
- 預設路由是針對每個節點自動產生的。如果已啟用 eth2，則 0.0.0.0/0 會使用 eth2 上的用戶端網路。如果未啟用 eth2，則 0.0.0.0/0 會使用 eth0 上的網格網路。
- 只有當網格節點加入網格後，用戶端網路才能開始運作。
- ${post_edited_translations.segment}

選用介面

您可以選擇性地向節點新增額外的介面。例如，您可以向管理節點或閘道節點新增一個中繼介面，以便使用"VLAN 介面"隔離屬於不同應用程式或租戶的流量。或者，您可以新增一個存取介面以在"${post_edited_translations.segment}"中使用。

若要新增主幹或存取介面，請參閱以下內容：

- **VMware**（節點安裝完成後）：${post_edited_translations.segment}"
  - **Linux**（安裝節點之前）：建立節點組態檔"
  - **Linux**（安裝節點後）：${post_edited_translations.segment}"

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。如需支援版本的清單，請參閱 NetApp 互作業性矩陣工具（IMT）"。

在 **StorageGRID** 中檢視 **IP** 位址

您可以檢視 StorageGRID 系統中每個網格節點的 IP 位址。然後，您可以使用此 IP 位址在命令列登入網格節點，並執行各種維護程序。

開始之前

您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。

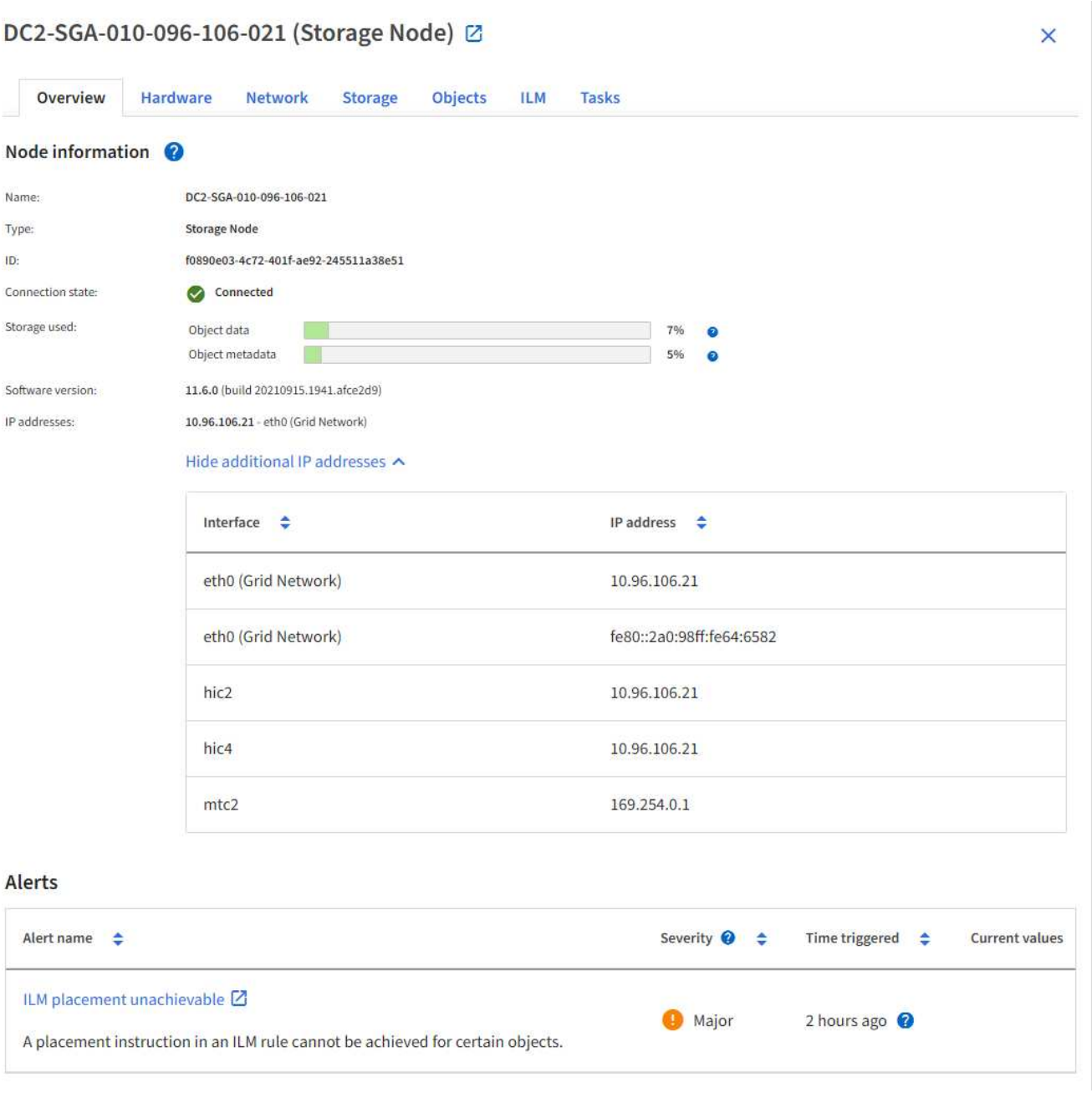
關於此任務

如需變更 IP 位址的相關資訊，請參閱 "${post_edited_translations.segment}"。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   此網格節點的 IP 位址列於下表中。



在 StorageGRID 中設定 VLAN 介面

在管理節點和閘道節點上建立虛擬區域網路 （VLAN） 介面，並將其用於 HA 群組和負載平衡器端點，以隔離和劃分流量，從而提高安全性、靈活度和效能。HA 群組中選定的節點可以使用 VLAN 介面共享最多 10 個虛擬 IP 位址，這樣，如果某個節點發生故障，則另一個節點可以接管進出這些虛擬 IP 位址的流量。

VLAN 介面注意事項

- 您可以透過輸入 VLAN ID 並選擇一個或多個節點上的父介面來建立 VLAN 介面。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

- 對於每個 VLAN 介面，您只能為指定的節點選取一個父介面。例如，您無法在同一個閘道節點上，將網格網路介面和用戶端網路介面同時用作同一個 VLAN 的父介面。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 如果需要新增主幹介面，詳情請參閱以下內容：
  - **VMware**（節點安裝完成後）："${post_edited_translations.segment}"
  - **Linux** （安裝節點之前）："建立節點組態檔"
  - **Linux** （安裝節點後）："${post_edited_translations.segment}"

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。如需支援版本的清單，請參閱 "NetApp 互作業性矩陣工具（IMT）"。

建立 **VLAN** 介面

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 網路中已設定主幹介面，並將其連接至 VM 或 Linux 節點。您知道該主幹介面的名稱。
- 您知道您正在設定的 VLAN 的 ID。

關於此任務

您的網路管理員可能已設定一個或多個中繼介面以及一個或多個 VLAN，用於隔離屬於不同應用程式或租用戶的用戶端或管理流量。每個 VLAN 都由一個數字 ID 或標籤來識別。例如，您的網路可能使用 VLAN 100 用於 FabricPool 流量，而使用 VLAN 200 用於歸檔應用程式。

您可以使用 Grid Manager 建立 VLAN 介面，允許用戶端存取特定 VLAN 上的 StorageGRID。建立 VLAN 介面時，您需要指定 VLAN ID，並在一個或多個節點上選擇父（幹線）介面。

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **Network** > **VLAN interfaces**。
2. 選擇 **Create** 。

輸入 **VLAN** 介面的詳細資訊

步驟

1. 指定網路中 VLAN 的 ID。您可以輸入 1 到 4094 之間的任意值。

   VLAN ID 不需要唯一。例如，您可以在一個站點使用 VLAN ID 200 來傳輸管理流量，並在另一個站點使用相同的 VLAN ID 來傳輸用戶端流量。您可以在每個站點建立具有不同父介面集的分隔 VLAN 介面。但是，具有相同 ID 的兩個 VLAN 介面不能共享同一節點上的相同介面。如果您指定的 ID 已被使用，則會顯示一則訊息。

2. （可選）輸入 VLAN 介面的簡短執行摘要。

3. 選擇 **Continue** 。

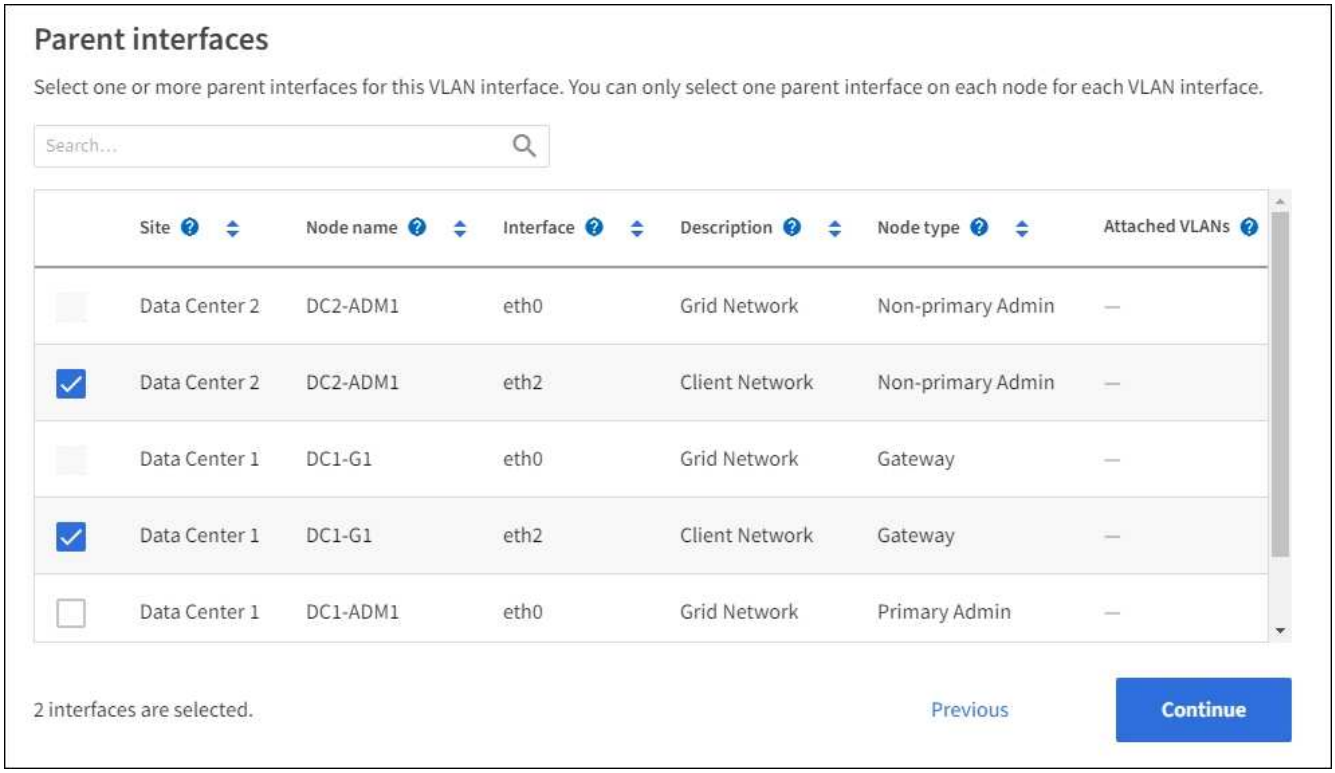
選擇父介面

此表列出網格中每個站台所有管理節點和閘道節點的可用介面。管理網路 （eth1） 介面不能用作父介面，因此不會顯示。

步驟

1. 選擇一個或多個父介面以將此 VLAN 附加到這些父介面。

   例如，您可能想要將 VLAN 附加到閘道節點和管理節點的用戶端網路 （eth2） 介面。



2. 選擇 **Continue** 。

確認設定

步驟

1. 檢查組態並進行必要的變更。
   - 如果需要變更 VLAN ID 或執行摘要，請選擇頁面頂端的 **Enter VLAN details**。
   - 如果需要變更父介面，請選擇頁面頂部的「Choose parent interfaces」或選擇「Previous」。
   - 如果需要刪除父級介面，請選擇垃圾桶圖示。
2. 選取 **Save** 。
3. 最多等待 5 分鐘，新介面才會出現在高可用度群組頁面上，並列在節點的*網路介面*表中（節點 > 父介面節點 > 網路）。

編輯 **VLAN** 介面

編輯 VLAN 介面時，您可以進行以下類型的變更：

- 更改 VLAN ID 或執行摘要。
- 新增或移除父介面。

例如，如果您計劃退役關聯的節點，則可能需要從 VLAN 介面中移除父介面。

請注意下列事項：

- 如果 VLAN 介面用於 HA 群組，則無法變更 VLAN ID。
- 如果父介面在 HA 群組中使用，則無法移除該父介面。

  例如，假設 VLAN 200 連接到節點 A 和 B 的父介面。如果 HA 群組將 VLAN 200 介面用於節點 A，將 eth2 介面用於節點 B，則可以移除節點 B 未使用的父介面，但不能移除節點 A 已使用的父介面。

步驟

1. 選擇 **Configuration** > **Network** > **VLAN interfaces**。
2. 選取要編輯的 VLAN 介面對應的核取方塊。然後，選取 **Actions** > **Edit**。
3. （可選）更新 VLAN ID 或執行摘要。然後選擇 * 繼續 *。

   如果 VLAN 用於 HA 群組，則無法更新 VLAN ID。

4. （可選）選取或取消選取核取方塊以新增父介面或移除未使用的介面。然後，選取 **Continue**。
5. 檢查組態並進行必要的變更。
6. 選取 **Save** 。

移除 **VLAN** 介面

您可以移除一個或多個 VLAN 介面。

如果 VLAN 介面目前正在高可用性 （HA） 群組中使用，則無法移除。必須先將 VLAN 介面從 HA 群組中移除，才能移除。

為避免用戶端流量中斷，請考慮執行下列其中一項操作：

- 在移除此 VLAN 介面之前，請先將新的 VLAN 介面新增至 HA 群組。
- 建立一個不使用此 VLAN 介面的新 HA 群組。
- 如果要移除的 VLAN 介面目前是作用中介面，請編輯 HA 群組。將要移除的 VLAN 介面移至優先權清單的底部。等待新的主要介面建立通訊後，再從 HA 群組中移除舊介面。最後，刪除該節點上的 VLAN 介面。

步驟

1. 選擇 **Configuration** > **Network** > **VLAN interfaces**。
2. 選取要移除的每個 VLAN 介面對應的核取方塊。然後，選取 **Actions** > **Delete**。
3. 選取 **Yes** 以確認您的選擇。

您選擇的所有 VLAN 介面均已移除。VLAN 介面頁面上將顯示綠色成功橫幅。

為管理介面啟用 StorageGRID CORS

身為網格系統管理員，如果您希望可以使用管理 API 從另一個網域存取 StorageGRID 中的資料，則可以為 StorageGRID 的管理 API 請求啟用跨來源資源共用 （CORS）。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- "${post_edited_translations.segment}" 提供對所有 CORS 組態請求的存取。

關於此任務

CORS 是一種安全性機制，允許一個網域中的用戶端 Web 應用程式存取另一個網域中的資源。例如，假設您想要在網域 `\http://www.example.com`中為 StorageGRID 建立監控儀表板。透過在 StorageGRID 中為 `\http://www.example.com`和「Grid Manager」啟用 CORS，StorageGRID 網域可回應來自 `\http://www.example.com`的 Grid Management API 請求。

Management API (mgmt-api) 請求，包含 `application/json`或 `multipart/formdata`對 `Content-Type`的請求，均支援 CORS。

步驟

1. 在 Grid Manager 中，前往 組態 > 網路 > 管理介面 **CORS** 設定。
2. 選擇 **Grid Manager**、**Tenant Manager** 或同時選擇這兩個選項。
   - ${post_edited_translations.segment}
   - **Tenant Manager**：為跨網域租戶管理 API 請求啟用 CORS。
3. 在 **Domains** 欄位中輸入另一個網域的 URL。

   如果要為 StorageGRID 中的多個網域啟用 CORS，請選擇「新增另一個網域」。
4. 選取 **Save** 。

相關資訊

"為儲存桶和物件設定 StorageGRID CORS"

管理流量分類原則

StorageGRID 中的流量分類原則

流量分類原則可讓您識別和監控不同類型的網路流量。這些原則有助於限制和監控流量，從而提升您的服務品質 (QoS)。

流量分類原則會套用至 Gateway Nodes 和 Admin Nodes 上 StorageGRID Load Balancer 服務的端點。若要建立流量分類原則，您必須已建立負載平衡器端點。

${post_edited_translations.segment}

每項流量分類原則都包含一條或多條符合規則，用於識別與以下一個或多個實體相關的網路流量：

- 儲存貯格
- 子網路
- ${post_edited_translations.segment}
- 負載平衡器端點

StorageGRID 會根據規則的目標監控符合該原則中任何規則的流量。任何符合原則中任何規則的流量都會由該原則處理。反之，您也可以設定規則來符合除特定實體之外的所有流量。

流量限制

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

限制值是按負載平衡器強制執行的。如果流量同時分佈在多個負載平衡器上，則總最大速率是您指定的速率限制的倍數。

> 您可以建立原則來限制 Aggregate 頻寬或限制每次要求頻寬。然而，StorageGRID 無法同時限制這兩種頻寬類型。Aggregate 頻寬限制可能會對未受限制的流量造成額外的輕微效能影響。

對於 Aggregate 或單次請求頻寬限制，請求將按照您設定的速率進行入站或出站。StorageGRID 只能強制執行一種速度，因此將依比對器類型強制執行最特定的原則比對項目。請求所消耗的頻寬不會計入其他包含 Aggregate 頻寬限制原則的較不具體的比對原則。對於所有其他類型的限制，用戶端請求將延遲 250 毫秒，且對於超過任何比對原則限制的請求，將收到 503 Slow Down 回應。

${post_edited_translations.segment}

使用具有服務等級協定 **(SLA)** 的流量分類原則

您可以結合容量限制和資料保護使用流量分類原則，以強制執行服務等級協定 （SLA），該協定對容量、資料保護和效能提供具體規定。

以下範例展示了服務等級協定 （SLA） 的三個層級。您可以建立流量分類原則，以達成每個 SLA 分層的效能目標。

服務等級層	容量	資料保護	允許的最大效能	成本
金級	允許 1 PB 儲存設備	3 複本 ILM 規則	25 K 次請求/秒 5 GB/秒（40 Gbps ）頻寬	每月$$$

服務等級層	容量	資料保護	允許的最大效能	成本
銀	允許 250 TB 儲存設備	2 複本 ILM 規則	每秒 10 K 次請求 1.25 GB/sec （10 Gbps）頻寬	每月 $$
銅級	允許 100 TB 儲存設備	2 複本 ILM 規則	5 K 次請求/秒 1 GB/秒（8 Gbps）頻寬	每月 $

建立 **StorageGRID** 流量分類原則

您可以建立流量分類原則來監控網路流量，並可選擇以儲存桶、儲存桶正規表示式、CIDR、負載平衡器端點或租戶限制網路流量。此外，您還可以根據頻寬、並行請求數或請求速率設定原則限制。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

步驟

1. 選擇 組態 > 網路 > 流量分類。
2. 選擇 **Create** 。
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

4. 選取 **Add rule** 並指定以下詳細資料，以針對該原則建立一或多個比對規則。您建立的任何原則都應至少包含一個比對規則。選取 **Continue**。

欄位	說明
類型	選擇符合規則適用的流量類型。流量類型包括儲存貯體、儲存貯體規則運算式、CIDR、負載平衡器端點和租戶。

欄位	說明
${post_edited_translations.segment}	請輸入與所選類型相符的值。 • ${post_edited_translations.segment} • ${post_edited_translations.segment} 此正規表示式未設定錨點。使用 ^ 錨點來匹配儲存桶名稱的開頭，使用 $ 錨點來匹配名稱的結尾。正規表示式匹配支援 PCRE （Perl 相容正規表示式）語法的子集。 • ${post_edited_translations.segment} • 負載平衡器端點：選取端點名稱。這些是您在 "設定負載平衡器端點" 上定義的負載平衡器端點。 • 租戶：租戶比對使用存取金鑰 ID。如果請求不包含存取金鑰 ID （例如，匿名存取），則使用所存取儲存桶的所有權來確定租戶。
反向匹配	如果您想要比對除與剛才定義的「類型」和「比對值」一致的流量_以外_的所有網路流量，請選取 反向比對 核取方塊。否則，請保持清除該核取方塊。 ${post_edited_translations.segment} 對於包含多個匹配器（其中至少一個是反向匹配器）的原則，請注意不要建立匹配所有請求的原則。

5. （可選）選擇 **Add a limit**，然後選擇以下詳細資訊，以新增一個或多個限制來控制規則匹配的網路流量。

   ${post_edited_translations.segment}

欄位	說明
類型	您想要套用至符合規則之網路流量的限制類型。例如，您可以限制頻寬或要求速率。 注意：您可以建立原則來限制 Aggregate 頻寬或限制單次請求頻寬。但是，StorageGRID 無法同時限制這兩種頻寬。當使用 Aggregate 頻寬時，單次請求頻寬將無法使用。反之，當使用單次請求頻寬時，Aggregate 頻寬將無法使用。Aggregate 頻寬限制可能會對未受限流量造成輕微的額外效能影響。 對於頻寬限制，StorageGRID 會套用與所設定的限制類型最相符的原則。例如，如果您設定了僅限制單向流量的原則，那麼反向流量將不受限制，即使有符合其他具有頻寬限制之原則的流量也是如此。StorageGRID 會依下列順序實現頻寬限制的「最佳」配對： • 精確的 IP 位址（/32 遮罩） • 確切的儲存桶名稱 • Bucket 正規表示式 • ${post_edited_translations.segment} • 端點 • 非精確 CIDR 匹配（非 /32） • 反向匹配
適用於	此限制是否適用於用戶端讀取請求（GET 或 HEAD）或寫入請求（PUT、POST 或 DELETE）。
價值	根據您選擇的單位，限制網路流量的數值。例如，輸入 10 並選擇 MiB/s，以防止此規則比對的網路流量超過 10 MiB/s。 注意：視單位設定而定，可用的單位將是二進位（例如 GiB）或十進位（例如 GB）。若要變更單位設定，請選取 Grid Manager 右上角的使用者下拉式功能表，然後選取 **User Preferences**。
單元	${post_edited_translations.segment}

${post_edited_translations.segment}

6. 選擇 **Continue** 。
7. 讀取並審查流量分類原則。使用 上一步 按鈕返回並根據需要進行變更。當您對原則感到滿意時，選取 儲存並繼續。

   ${post_edited_translations.segment}

完成後

"${post_edited_translations.segment}"以驗證原則是否正在執行您預期的流量限制。

編輯 **StorageGRID** 流量分類原則

您可以編輯流量分類原則，變更其名稱或執行摘要，或建立、編輯或刪除該原則的任何規則或限制。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

步驟

1. 選擇 組態 > 網路 > 流量分類。

   「流量分類原則」頁面隨即出現，現有原則以表格形式列出。

2. 使用「動作」功能表或詳細資料頁面編輯原則。請參閱 "建立流量分類原則" 以了解輸入內容。

   操作選單

   a. 選取該原則的核取方塊。

   b. 選取 **Actions** > **Edit**。

   詳細資料頁面

   a. 選擇原則名稱。

   b. 選擇原則名稱旁的「編輯」按鈕。

3. 在「輸入原則名稱」步驟中，您可以選擇編輯原則名稱或執行摘要，然後選取*繼續*。
4. 在「新增符合規則」步驟中，您可以選擇新增規則或編輯現有規則的「類型」和「符合值」，然後選擇「繼續」。
5. 在「設定限制」步驟中，您可以選擇新增、編輯或刪除限制，然後選取 **Continue**。
6. 審查更新後的原則，然後選擇「儲存並繼續」。

   您對原則所做的變更已儲存，網路流量現在將根據流量分類原則進行處理。您可以檢視流量圖表，並驗證原則是否正在執行您預期的流量限制。

刪除 **StorageGRID** 流量分類原則

如果您不再需要某個流量分類原則，可以將其刪除。請務必刪除正確的原則，因為原則一旦刪除將無法復原。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

步驟

1. 選擇 組態 > 網路 > 流量分類。

${post_edited_translations.segment}

2. 使用「動作」功能表或詳細資料頁面刪除原則。

   操作選單

   a. 選取該原則的核取方塊。
   b. 選擇 **Actions** > **Remove**。

   原則詳細資料頁面

   a. 選擇原則名稱。
   b. ${post_edited_translations.segment}

3. 選擇「是」以確認您要刪除該原則。

   原則已刪除。

在 StorageGRID 中檢視網路流量指標

您可以透過檢視流量分類原則頁面上的圖表來監控網路流量。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有 "${post_edited_translations.segment}"。

關於此任務

對於任何現有的網路流量分類原則，您可以檢視負載平衡器服務的計量，以確定該原則是否成功限制整個網路的網路流量。圖表中的資料可以協助您確定是否需要調整原則。

${post_edited_translations.segment}

步驟

1. 選擇 組態 > 網路 > 流量分類。

   ${post_edited_translations.segment}

2. 選擇要檢視計量的流量分類原則名稱。
3. 選擇*計量*索引標籤。

   隨即顯示網路流量分類原則圖表。圖表僅會顯示符合所選原則之網路流量的計量。

   頁面上包含以下圖表。

   - 要求速率：此圖表提供所有負載平衡器處理且符合此原則的頻寬量。接收的資料包含所有要求的要求標頭，以及具有主體資料之回應的主體資料大小。傳送的資料包含所有要求的回應標頭，以及在回應中包含主體資料之要求的回應主體資料大小。

請求完成後，此圖表僅顯示頻寬使用量。對於速度較慢或物件較大的請求，實際瞬時頻寬可能與此圖表中顯示的值有所不同。

- 錯誤回應率：此圖表顯示符合此原則的請求向用戶端傳回錯誤（HTTP 狀態碼 >= 400）的大致速率。
- ${post_edited_translations.segment}
- 原則頻寬使用量：此圖表提供所有負載平衡器處理的符合此原則的頻寬使用量。接收資料包括所有要求的要求標頭，以及含有本文資料的回應之本文資料大小。傳送資料包括所有要求的回應標頭，以及回應中含有本文資料的要求之回應本文資料大小。

4. ${post_edited_translations.segment}
5. 在「計量」標題下方選擇 **Grafana dashboard**，即可檢視原則的所有圖表。除了「計量」標籤中的四個圖表外，您還可以檢視另外兩個圖表：
   - 按物件大小劃分的寫入請求速率：符合此原則的 PUT/POST/DELETE 請求的速率。在單一儲存格上定位可顯示每秒速率。懸停檢視中顯示的速率會截斷為整數計數，當儲存桶中存在非零請求時，速率可能報告 0。
   - 以物件大小劃分的讀取請求速率：符合此原則的 GET/HEAD 請求的速率。懸停在單一儲存格上顯示每秒速率。懸停檢視中顯示的速率會截斷為整數計數，當儲存桶中存在非零請求時，速率可能報告 0。
6. ${post_edited_translations.segment}
   a. 選擇 **Support** > **Tools** > **Metrics**。
   b. 從 **Grafana** 部分選擇 **Traffic Classification Policy**。
   c. 請從頁面左上角的選單中選擇原則。
   d. ${post_edited_translations.segment}

   流量分類原則是透過其 ID 進行識別。原則 ID 會列在「流量分類原則」頁面上。
7. 分析圖表，確定原則限制流量的頻率，以及是否需要調整原則。

StorageGRID 中支援的用於出站 TLS 連線的加密套件

${post_edited_translations.segment}

支援的 **TLS** 版本

StorageGRID 支援 TLS 1.2 和 TLS 1.3，用於連線至用於身分識別聯盟和雲端儲存集區的外部系統。

為了確保與各種外部系統的相容性，已選取支援與外部系統搭配使用的 TLS 加密套件。該清單比支援與 S3 用戶端應用程式搭配使用的加密套件清單更長。若要設定加密套件，請前往 組態 > 安全性 > 安全性設定，然後選取 **TLS and SSH policies**。

TLS 組態選項（例如協定版本、密碼組合、金鑰交換演算法和 MAC 演算法）在 StorageGRID 中無法設定。如果您對這些設定有特定需求，請聯絡您的 NetApp 帳戶代表。

StorageGRID 中活動、閒置和並行 HTTP 連線的優勢

HTTP 連線的設定方式會影響 StorageGRID 系統的效能。組態方式會根據 HTTP 連線是處於作用中狀態、閒置還是存在多個並行連線而有所不同。

您可以識別以下幾種 HTTP 連線類型的效能優勢：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

當用戶端應用程式處於閒置時，請保持 HTTP 連線開啟，以便後續交易處理。閒置的 HTTP 連線最多保持開啟狀態 10 分鐘。StorageGRID 可能會自動關閉開啟且閒置超過 10 分鐘的 HTTP 連線。

開放且閒置的 HTTP 連線具有以下優點：

- 縮短從 StorageGRID 系統確定需要執行 HTTP 交易到 StorageGRID 系統能夠執行該交易之間的延遲。

  ${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

透過平衡慢啟動優勢和資源分配，決定保持閒置連線開啟多久。

${post_edited_translations.segment}

對於直接連線至儲存節點的連線，即使 HTTP 連線持續執行交易，也應將作用中 HTTP 連線的持續時間限制在最多 10 分鐘。

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}

  隨著時間推移，隨著負載平衡需求發生變化，HTTP 連線可能不再是最佳選擇。當用戶端應用程式為每筆交易建立分隔的 HTTP 連線時，系統會執行最佳的負載平衡，但此方法會抵消與持續連線相關的寶貴效益。

- ${post_edited_translations.segment}
- 允許啟動維護程序。

  ${post_edited_translations.segment}

對於用戶端與負載平衡器服務的連線，限制開啟連線的持續時間有助於某些維護程序及時啟動。如果不限制用戶端連線的持續時間，則可能需要幾分鐘才能自動終止作用中的連線。

並發 **HTTP** 連線的優勢

您應該保持多個連至 StorageGRID 系統的 TCP/IP 連線開啟，以允許平行處理，這能提高效能。平行連線的最佳數量取決於多種因素。

並行 HTTP 連線具有以下優點：

- 降低延遲

  交易可以立即開始，無需等待其他交易完成。

- 處理量提高

  ${post_edited_translations.segment}

用戶端應用程式應建立多個 HTTP 連線。當用戶端應用程式需要執行交易時，它可以選擇並立即使用任何目前未處理交易的已建立連線。

每個 StorageGRID 系統的拓撲對於並行交易和連線的峰值處理量各有不同。峰值處理量取決於運算、連網、儲存資源、WAN 連結，以及 StorageGRID 系統支援的伺服器、服務和應用程式的數量。

StorageGRID 系統通常支援多個用戶端應用程式。在確定最大並行連線數時，請記住這一點。如果用戶端應用程式由多個軟體實體組成，且每個實體都與 StorageGRID 系統建立連線，則需要將所有實體的連線數加總。在下列情況下，您可能需要調整最大並行連線數：

- StorageGRID 系統的拓撲會影響系統能夠支援的最大並行交易數和連線數。
- 透過頻寬有限的網路與 StorageGRID 系統互動的用戶端應用程式，可能需要降低並行程度，以確保個別交易在合理的時間內完成。
- 當許多用戶端應用程式共享 StorageGRID 系統時，您可能需要降低並發度，以避免超出系統限制。

將 **HTTP** 連線資源池分離，用於讀取和寫入操作

您可以為讀取和寫入操作使用分隔的 HTTP 連線池，並控制每個操作所使用的資源池大小。獨立的 HTTP 連線池可讓您更好地控制交易並達到負載平衡。

用戶端應用程式可以建立以擷取為主（讀取）或以儲存為主（寫入）的負載。透過為讀取和寫入交易分別設定獨立的 HTTP 連線資源池，您可以調整每個資源池指派給讀取或寫入交易的資源比例。

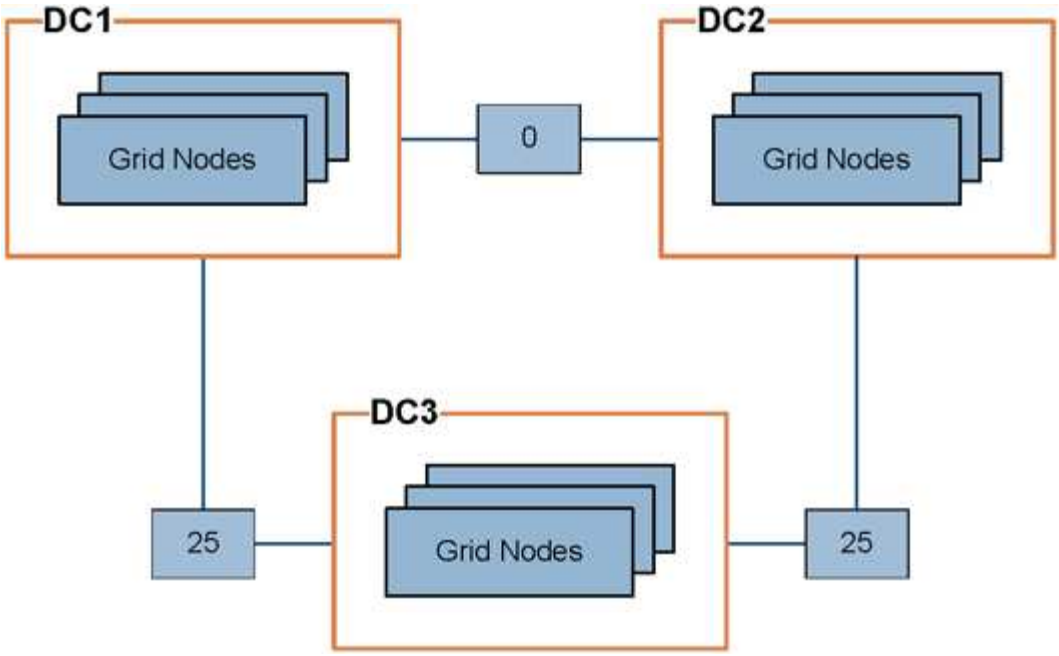
在 StorageGRID 中管理連結成本

當存在兩個或多個資料中心站台時，連結成本可讓您優先選擇哪個資料中心站台提供所要求的服務。您可以調整連結成本以反映站台間的延遲。

什麼是連結成本？

- 連結成本用於決定優先使用哪個物件複本來完成物件檢索。
- 連結成本由 Grid Management API 和 Tenant Management API 使用，以決定要使用哪些內部 StorageGRID 服務。
- 連結成本由管理節點和閘道節點上的負載平衡服務用於導向用戶端連線。請參閱 "負載平衡的考慮因素"。

此圖顯示一個由三個站台組成的網格，站台之間已設定連結成本：



- 管理節點和閘道節點上的 Load Balancer 服務會將用戶端連線平均分配至相同資料中心站台的所有儲存節點，以及連結成本為 0 的任何資料中心站台。

  在本例中，資料中心站點 1 （DC1） 的 Gateway Node 將用戶端連線平均分配給 DC1 的 Storage Node 和 DC2 的 Storage Node。DC3 的 Gateway Node 僅將用戶端連線傳送到 DC3 的 Storage Node。

- 當擷取存在多個複本的物件時，StorageGRID 會從連結成本最低的資料中心擷取複本。

  例如，如果 DC2 上的用戶端應用程式擷取同時儲存在 DC1 和 DC3 上的物件，則會從 DC1 擷取該物件，因為從 DC1 到 DC2 的連結成本為 0，低於從 DC3 到 DC2 的連結成本 （25） 。

連結成本是任意的相對數值，沒有具體的計量單位。例如，連結成本為 50 的連結使用優先順序低於連結成本為 25 的連結。下表列出了常用的連結成本。

連結	連結成本	附註
在實體資料中心站點之間	25（預設值）	透過 WAN 連結連接的資料中心。
${post_edited_translations.segment}	0	${post_edited_translations.segment}

更新連結成本

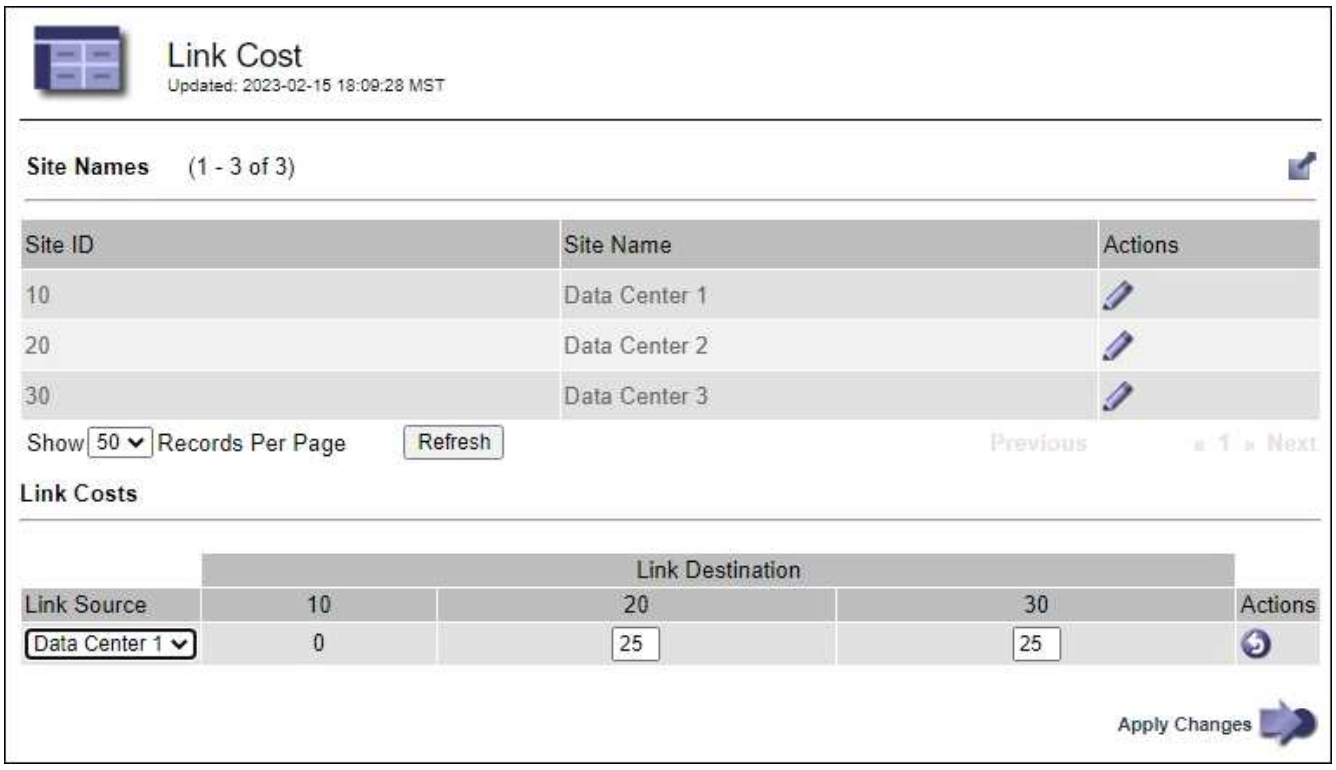
您可以更新資料中心站台之間的連結成本，以反映站台之間的延遲。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有 "其他網格組態權限"。

步驟

1. 選擇 **Support** > **Other** > **Link cost**。



2. 在「連結來源」下選擇一個站台，然後在「連結目的地」下輸入 0 到 100 之間的成本值。

   如果來源和目的地相同，則無法變更連結成本。

   若要取消變更，請選擇 **Revert**。

3. ${post_edited_translations.segment}

使用 AutoSupport

了解 AutoSupport 在 StorageGRID 中的應用

AutoSupport 功能可讓 StorageGRID 傳送健全狀況和狀態套件給 NetApp 技術支援。

使用 AutoSupport 有助於更快解決問題。技術支援可以監控您系統的儲存容量需求，並協助確定您是否需要新增節點或站台。（可選）AutoSupport 可以將套件傳送至一個額外的目的地。

StorageGRID 有兩種類型的 AutoSupport：

- **StorageGRID AutoSupport** 回報 StorageGRID 軟體問題。首次安裝 StorageGRID 時預設啟用。如有需要，您可以 "變更預設 AutoSupport 組態"。

> 如果 StorageGRID AutoSupport 未啟用，網格管理器儀表板上會顯示一則訊息。該訊息包含指向 AutoSupport 組態頁面的連結。如果您結案該訊息，即使 AutoSupport 仍處於停用狀態，在清除瀏覽器快取之前，該訊息也不會再次出現。

- 應用裝置硬體 **AutoSupport** 報告 StorageGRID 應用裝置問題。您必須 "設定每台應用裝置上的硬體 AutoSupport"。

什麼是 **Active IQ**？

Active IQ 是一款雲端型數位顧問，利用預測分析和 NetApp 安裝基礎的社群智慧。其持續的風險評估、預測警示、指導性建議和自動化操作可協助您在問題發生之前就加以預防，進而改善系統健全狀況並提高系統可用度。

如果您想在 NetApp 支援網站上使用 Active IQ 儀表板和功能，則必須啟用 AutoSupport。

"${post_edited_translations.segment}"

AutoSupport 套件中包含的資訊

一個 AutoSupport 套件包含下列檔案與詳細資料。

檔案名稱	欄位	說明
AUTOSUPPORT-HISTORY.XML	AutoSupport 序號 + 此 AutoSupport 的目的地 + 傳送狀態 + 傳送嘗試次數 + AutoSupport 主題 + 傳送 URI + 上次錯誤 + AutoSupport PUT 檔案名稱 + 產生時間 + AutoSupport 壓縮大小 + AutoSupport 解壓縮大小 + 總收集時間（毫秒）	AutoSupport 歷史檔案。
${post_edited_translations.segment}	節點 + 聯絡技術支援的協定 + HTTP/HTTPS 的技術支援 URL + 技術支援地址 + AutoSupport OnDemand 狀態 + AutoSupport OnDemand 伺服器 URL + AutoSupport OnDemand 輪詢間隔	AutoSupport 狀態檔案。提供所用協定、技術支援 URL 和地址、輪詢間隔以及 OnDemand AutoSupport 是否啟用或停用等詳細資訊。
BUCKETS.XML	${post_edited_translations.segment}	提供 Bucket 層級的組態詳細資料與統計資料。Bucket 組態的範例包括平台服務、法規遵循和 Bucket 一致性。
${post_edited_translations.segment}	${post_edited_translations.segment}	整個網格的組態資訊檔案。包含關於網格憑證、中繼資料保留空間、整個網格的組態設定（法規遵循、S3 Object Lock、物件壓縮、警示、syslog 及 ILM 組態）、糾刪碼設定檔詳細資料、DNS 名稱以及 "${post_edited_translations.segment}" 的資訊。
GRID-SPEC.XML	網格規格，原始 XML	用於設定和部署 StorageGRID。包含網格規格、NTP 伺服器 IP、DNS 伺服器 IP、網路拓撲和節點硬體設定檔。

檔案名稱	欄位	說明
${post_edited_translations.segment}	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	網格工作（維護程序）狀態檔案。提供網格作用中、已終止、已完成、失敗及擱置中工作的詳細資料。
${post_edited_translations.segment}	${post_edited_translations.segment}	網格資訊。
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	ILM 計量資訊檔案。包含每個節點的 ILM 評估率和網格範圍的計量。
ILM.XML	ILM 原始 XML	ILM 作用中原則檔案。包含作用中 ILM 原則的詳細資料，例如儲存資源池 ID、擷取行為、篩選器、規則與執行摘要。
LOG.TGZ	*n/a*	可下載的日誌檔。包含 `bycast-err.log`和 `servermanager.log`來自每個節點的資訊。
${post_edited_translations.segment}	收集順序 + 此資料的 AutoSupport 內容檔名 + 此資料項目的執行摘要 + 收集的位元組數 + 收集花費的時間 + 此資料項目的狀態 + 錯誤的執行摘要 + 此資料的 AutoSupport 內容類型	包含 AutoSupport 中繼資料和所有 AutoSupport 檔案的簡短執行摘要。
NMS-ENTITIES.XML	屬性索引 + 實體 OID + 節點 ID + 設備型號 ID + 設備型號版本 + 實體名稱	"NMS 樹" 中的群組與服務實體。提供網格拓撲詳細資料。可根據該節點上執行的服務來確定節點。
${post_edited_translations.segment}	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	物件狀態，包括背景掃描狀態、作用中傳輸、傳輸率、總傳輸次數、刪除速率、損壞的片段、遺失的物件、缺少的物件、嘗試修理次數、掃描速率、估計掃描週期和修理完成狀態。
SERVER-STATUS.XML	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	伺服器組態。包含每個節點的以下詳細資料：平台類型、作業系統、已安裝的記憶體容量、可用記憶體容量、儲存設備連線能力、儲存應用裝置機箱序號、儲存控制器故障磁碟機數量、運算控制器機箱溫度、運算硬體、運算控制器序號、電源供應、磁碟機大小和磁碟機類型。

檔案名稱	欄位	說明
SERVICE-STATUS.XML	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	服務節點資訊檔案。包含已指派表空間、可用表空間、資料庫 Reaper 計量、區段修理持續時間、修理作業持續時間、自動作業重新啟動和自動作業終止等詳細資訊。
STORAGE-GRADES.XML	儲存等級 ID + 儲存等級名稱 + 儲存節點 ID + 儲存節點路徑	每個儲存節點的儲存等級定義檔案。
SUMMARY-ATTRIBUTES.XML	${post_edited_translations.segment}	匯總 StorageGRID 使用資訊的進階系統狀態資料。提供諸如網格名稱、站點名稱、每個網格和每個站點的儲存節點數、授權類型、授權容量和使用情況、軟體支援條款以及 S3 作業詳情等詳細資訊。
${post_edited_translations.segment}	名稱 + 嚴重性 + 節點名稱 + 警示狀態 + 站台名稱 + 警示觸發時間 + 警示解決時間 + 規則 ID + 節點 ID + 站台 ID + 已靜默 + 其他附註 + 其他標籤	目前系統警示表示 StorageGRID 系統中的潛在問題。
USERAGENTS.XML	${post_edited_translations.segment}	基於應用程式使用者代理程式的統計資料。例如，每個使用者代理程式的 PUT/GET/DELETE/HEAD 操作次數以及每次操作的總位元組大小。
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport 標頭資料。

在 **StorageGRID** 中設定 **AutoSupport**

預設情況下，首次安裝 StorageGRID 時會啟用 StorageGRID AutoSupport 功能。但是，您必須在每個應用裝置上設定硬體 AutoSupport。如有需要，您可以變更 AutoSupport 組態。

如果要變更 StorageGRID AutoSupport 的組態，請僅在主要管理節點上進行變更。您必須設定硬體 AutoSupport在每個應用裝置上進行變更。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。
- 如果您使用 HTTPS 傳送 AutoSupport 套件，則您已向主要管理節點提供傳出網際網路存取，可以直接提供

，也可以透過 "使用 Proxy 伺服器"（不需要傳入連線）。

- 如果在 StorageGRID AutoSupport 頁面上選擇了 HTTP，則必須"設定 Proxy 伺服器"以 HTTPS 方式轉送 AutoSupport 封包。NetApp 的 AutoSupport 伺服器將拒絕使用 HTTP 傳送的封包。
- 如果您使用 SMTP 作為 AutoSupport 套件的傳輸協定，則需要設定 SMTP 郵件伺服器。

關於此任務

您可以使用以下任何選項組合，將 AutoSupport 套件傳送至技術支援：

- 每週：每週自動傳送一次 AutoSupport 套件。預設設定：已啟用。
- 事件觸發：每小時或發生重大系統事件時，自動傳送 AutoSupport 套件。預設設定：啟用。
- 隨需：允許技術支援人員要求您的 StorageGRID 系統自動傳送 AutoSupport 套件，這在他們積極處理問題時非常有用（需要 HTTPS AutoSupport 傳輸協定）。預設設定：停用。
- 使用者觸發：隨時手動傳送 AutoSupport 套件。
- 日誌收集："手動收集日誌檔案和系統資料，並傳送 AutoSupport 套件"。

指定 **AutoSupport** 套件的傳輸協定

您可以使用下列任何一種協定來傳送 AutoSupport 套件：

- **HTTPS**：這是新安裝的預設設定，也是建議設定。此協定使用 443 連接埠。如果您想要 啟用 AutoSupport 隨需功能，則必須使用 HTTPS。
- **HTTP**：如果您選擇 HTTP，則必須設定 Proxy 伺服器，以將 AutoSupport 封包轉送為 HTTPS。NetApp 的 AutoSupport 伺服器會拒絕使用 HTTP 傳送的封包。此協定使用 80 連接埠。
- **SMTP**：如果您希望以電子郵件傳送 AutoSupport 套件，請使用此選項。

您設定的協定用於傳送所有類型的 AutoSupport 套件。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 選擇您要用於傳送 AutoSupport 套件的協定。
3. 如果您選擇了 **HTTPS**，請選擇是否使用 NetApp 支援憑證（TLS 憑證）來保護與技術支援伺服器的連線。
   - 驗證憑證 （預設）：確保 AutoSupport 封包的傳輸是安全的。NetApp 支援憑證已隨 StorageGRID 軟體一起安裝。
   - 不驗證憑證：僅當您有正當理由不使用憑證驗證時才選擇此選項，例如憑證出現臨時問題時。
4. 選擇 **Save**。所有每週、使用者觸發和事件觸發的套件都將使用所選協定傳送。

停用每週 **AutoSupport**

預設情況下，StorageGRID 系統已設定為每週向技術支援傳送一次 AutoSupport 套件。

若要確定每週 AutoSupport 套件的傳送時間，請前往「**AutoSupport** > 結果」索引標籤。在「每週 **AutoSupport**」區段中，查看「下次排程時間」的值。

您可以隨時停用每週 AutoSupport 套件的自動傳送功能。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 取消選取「啟用每週 AutoSupport」核取方塊。
3. 選取 **Save** 。

停用事件觸發的 **AutoSupport**

StorageGRID 系統預設設定為每小時向技術支援傳送一個 AutoSupport 套件。

您可以隨時停用事件觸發的 AutoSupport。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 取消選取「啟用事件觸發 AutoSupport」核取方塊。
3. 選取 **Save** 。

啟用 **AutoSupport on Demand**

AutoSupport on Demand 可協助解決技術支援正積極處理的問題。

預設會停用 AutoSupport on Demand。啟用此功能可允許技術支援要求您的 StorageGRID 系統自動傳送 AutoSupport 套件。技術支援也可以設定 AutoSupport on Demand 查詢的輪詢時間間隔。

技術支援無法啟用或停用 AutoSupport on Demand。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. ${post_edited_translations.segment}
3. 選取 啟用每週 **AutoSupport** 核取方塊。
4. 選取 啟用隨選 **AutoSupport** 核取方塊。
5. 選取 **Save** 。

   AutoSupport on Demand 已啟用，且技術支援可以向 StorageGRID 傳送 AutoSupport on Demand 要求。

${post_edited_translations.segment}

預設情況下，StorageGRID 會聯絡 NetApp 以確定是否有適用於您系統的軟體更新。如果有可用的 StorageGRID Hotfix 或新版本，新版本將會顯示在 StorageGRID 升級頁面上。

您可以根據需要選擇停用軟體更新檢查。例如，如果您的系統無法存取 WAN，則應停用此檢查以避免下載錯誤。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. ${post_edited_translations.segment}
3. 選取 **Save** 。

新增額外的 **AutoSupport** 目的地

當您啟用 AutoSupport 時，健康狀況與狀態套件將會傳送給技術支援。您可以為所有 AutoSupport 套件指定一個額外的目的地。

若要驗證或變更用於傳送 AutoSupport 套件的協定，請參閱說明以 指定 AutoSupport 套件的協定。

您無法使用 SMTP 協定傳送 AutoSupport 套件至額外的目的地。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 選取 啟用額外 **AutoSupport** 目的地。
3. 請具體說明以下內容：

主機名稱

其他 AutoSupport 目的地伺服器的伺服器主機名稱或 IP 位址。

您只能輸入一個附加目的地。

連接埠

用於連線至其他 AutoSupport 目的地伺服器的連接埠。預設為 HTTP 的連接埠 80 或 HTTPS 的連接埠 443。

憑證驗證

是否使用 TLS 憑證來保護與附加目的地的連線安全。

- 選取 **Verify certificate** 以使用憑證驗證。
- 選取「不驗證憑證」，即可在不進行憑證驗證的情況下傳送 AutoSupport 套件。

  只有當您有正當理由不使用憑證驗證時才選擇此選項，例如憑證出現臨時問題時。

4. 如果您選擇了*驗證憑證*，請執行以下操作：
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}
5. 選取 **Save** 。

所有未來的每週、事件觸發及使用者觸發的 AutoSupport 封包都將傳送到此額外目的地。

為應用裝置設定 **AutoSupport**

應用裝置的 AutoSupport 會報告 StorageGRID 硬體問題，而 StorageGRID AutoSupport 則會報告 StorageGRID 軟體問題，但有一個例外：對於 SGF6112，StorageGRID AutoSupport 會同時報告硬體和軟體問題。您必須在除 SGF6112 以外的每個應用裝置上設定 AutoSupport，SGF6112 不需要額外的設定。服務應用裝置和儲存應用裝置的 AutoSupport 實作方式有所不同。

您可以使用 SANtricity 為每個儲存應用裝置啟用 AutoSupport。您可以在初始應用裝置設定期間，或在安裝應用裝置之後設定 SANtricity AutoSupport：

- 針對 SG6000 和 SG5700 應用裝置， "在 SANtricity System Manager 中設定 AutoSupport"

如果您在 "SANtricity System Manager" 中設定透過 Proxy 傳送 AutoSupport，則來自 E 系列應用裝置的 AutoSupport 套件可以包含在 StorageGRID AutoSupport 中。

StorageGRID AutoSupport 不會報告硬體問題，例如 DIMM 或主機介面卡 （HIC） 故障。但是，某些元件故障可能會觸發"硬體警報"。對於具有基板管理控制器 （BMC） 的 StorageGRID 應用裝置，您可以設定電子郵件和 SNMP 陷阱來報告硬體故障：

- "設定 BMC 警報的電子郵件通知"
- "設定 BMC 的 SNMP 設定"

相關資訊

"NetApp 支援"

手動觸發 **StorageGRID** 中的 **AutoSupport** 套件

為了協助技術支援人員疑難排解 StorageGRID 系統的問題，您可以手動觸發傳送 AutoSupport 套件。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您擁有 Root 存取或其他網格組態權限。

步驟

1. 選擇 **Support** > **Tools** > **AutoSupport**。
2. 在 動作 索引標籤上，選取 傳送使用者觸發的 **AutoSupport**。

   StorageGRID 嘗試傳送 AutoSupport 套件至 NetApp 支援網站。如果嘗試成功，則會更新「結果」索引標籤上的「最新結果」和「上次成功時間」值。如果發生問題，「最新結果」值會更新為「失敗」，且 StorageGRID 不會再次嘗試傳送 AutoSupport 套件。

3. 1 分鐘後，重新整理瀏覽器中的 AutoSupport 網頁，以存取最新結果。

此外，您也可以"${post_edited_translations.segment}"將它們傳送到 NetApp 支援網站。

StorageGRID AutoSupport 套件故障排除

如果嘗試傳送 AutoSupport 套件失敗，StorageGRID 系統會根據 AutoSupport 套件的類型採取不同的動作。您可以透過選取 支援 > 工具 > **AutoSupport** > 結果，來檢查 AutoSupport 套件的狀態。

當 AutoSupport 套件傳送失敗時，「Failed」會出現在 **AutoSupport** 頁面的 **Results** 索引標籤上。

如果您已設定 Proxy 伺服器將 AutoSupport 封包轉寄至 NetApp，您應該 "請確認 Proxy 伺服器組態設定是否正確"。

每週 **AutoSupport** 套件故障

如果每週的 AutoSupport 套件傳送失敗，StorageGRID 系統將採取下列動作：

1. 將「最新結果」屬性更新為「正在重試」。
2. 嘗試在一小時內每四分鐘重新傳送 AutoSupport 封包一次，共 15 次。
3. 發送失敗一小時後，將「最新結果」屬性更新為「失敗」。
4. 在下一個排定的時間嘗試再次傳送 AutoSupport 封包。
5. 如果因為 NMS 服務無法使用而導致套件傳送失敗，或在七天內傳送套件，則維持正常 AutoSupport 排程。
6. 當 NMS 服務再次可用時，如果套件已有七天或更長時間未傳送，則立即傳送 AutoSupport 套件。

使用者觸發或事件觸發的 **AutoSupport** 套件故障

如果使用者觸發或事件觸發的 AutoSupport 套件傳送失敗，StorageGRID 系統會採取以下動作：

1. 如果已知錯誤，則顯示錯誤訊息。例如，如果使用者選擇 SMTP 協定但未提供正確的電子郵件組態設定，則會顯示以下錯誤： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不會再嘗試傳送套件。
3. 將錯誤記錄在 `nms.log` 中。

如果發生故障且選取的通訊協定為 SMTP，請驗證 StorageGRID 系統的電子郵件伺服器是否已正確設定，以及您的電子郵件伺服器是否正在執行（支援 > 警報（舊版） > 舊版電子郵件設定）。AutoSupport 頁面上可能會出現以下錯誤訊息： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

瞭解如何"${post_edited_translations.segment}"。

修復 **AutoSupport** 套件故障

如果發生故障且選取的協定為 SMTP，請驗證 StorageGRID 系統的電子郵件伺服器是否已正確設定，以及您的電子郵件伺服器是否正在執行。以下錯誤訊息可能會顯示在 AutoSupport 頁面上： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

透過 **StorageGRID** 傳送 **E** 系列 **AutoSupport** 套件

您可以透過 StorageGRID 管理節點而非儲存應用裝置管理連接埠，將 E 系列 SANtricity System Manager AutoSupport 套件傳送至技術支援。

如需更多關於搭配 E 系列應用裝置使用 AutoSupport 的資訊，請參閱 "E 系列硬體 AutoSupport"。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入網格管理員。
- 您有"儲存應用裝置系統管理員或 Root 存取權限"。
- 您已設定 SANtricity AutoSupport：
  - 針對 SG6000 和 SG5700 應用裝置， "在 SANtricity System Manager 中設定 AutoSupport"

> 若要使用 Grid Manager 存取 SANtricity System Manager，您必須擁有 SANtricity 韌體 8.70 或更高版本。

關於此任務

E 系列 AutoSupport 套件包含儲存硬體的詳細資訊，比 StorageGRID 系統所傳送的其他 AutoSupport 套件更為具體。

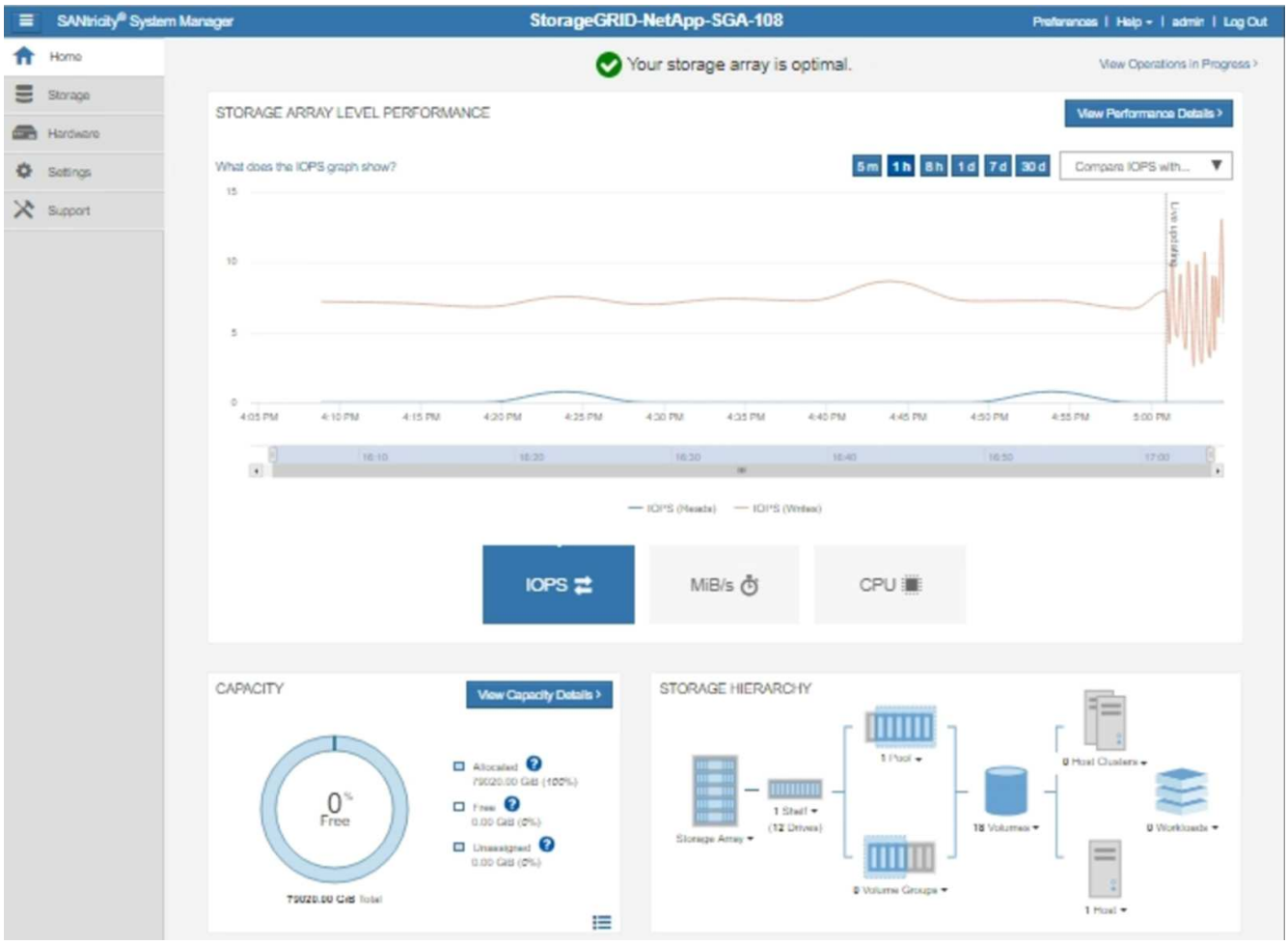
您可以在 SANtricity System Manager 中設定特殊的 Proxy 伺服器位址，以便透過 StorageGRID 管理節點傳輸 AutoSupport 套件，而無需使用應用裝置的管理連接埠。以這種方式傳輸的 AutoSupport 套件由 "慣用寄件者管理節點" 傳送，並使用已在 Grid Manager 中設定的任何 "管理員 Proxy 設定"。

> 此程序僅適用於為 E 系列 AutoSupport 套件設定 StorageGRID Proxy 伺服器。如需 E 系列 AutoSupport 組態的詳細資訊，請參閱 "NetApp E 系列和 SANtricity 文件"。

步驟

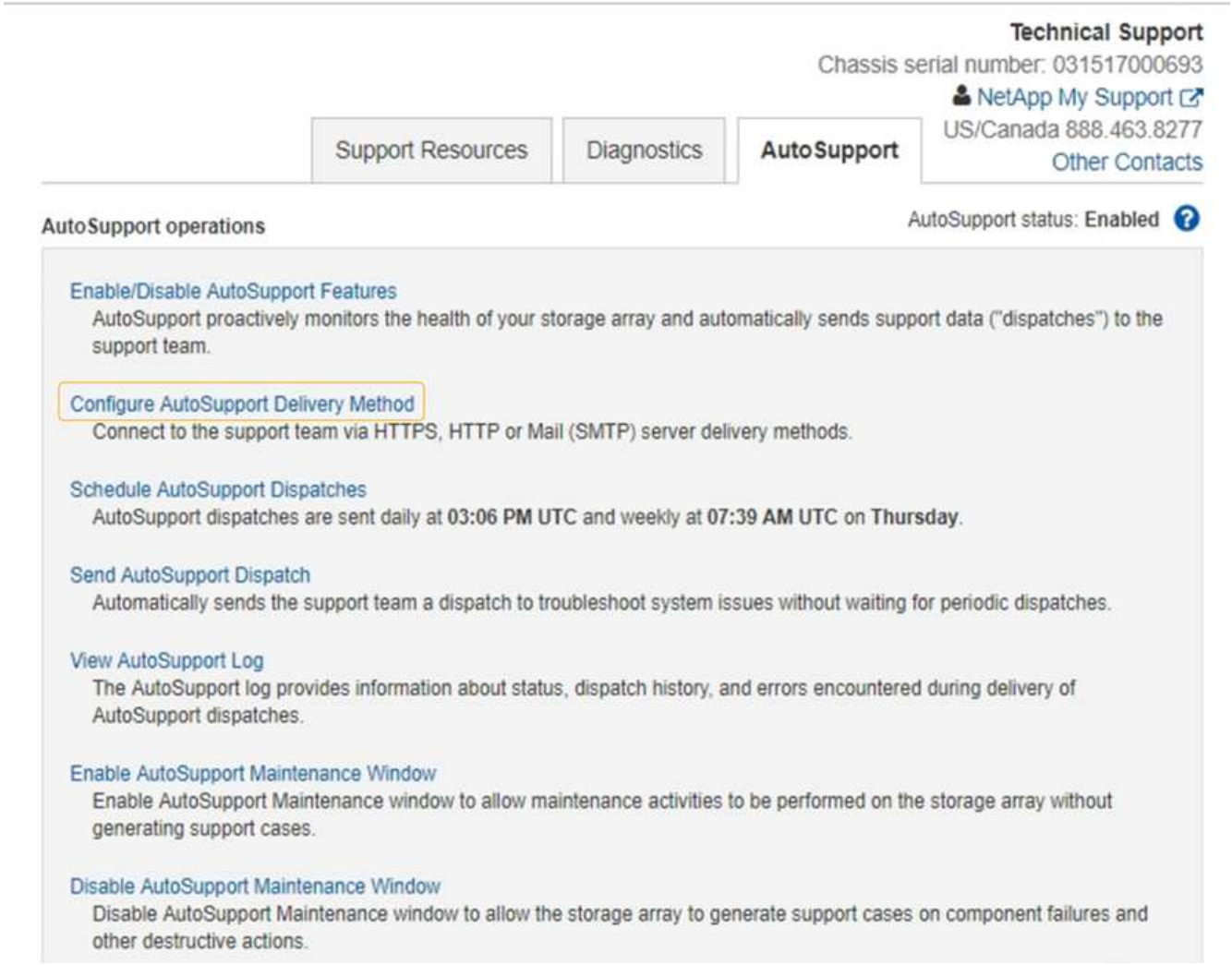
1. 在 Grid Manager 中，選擇 **Nodes** 。
2. 從左側的節點清單中，選擇要設定的儲存應用裝置節點。
3. 選擇 **SANtricity System Manager**。

   SANtricity System Manager 首頁隨即出現。



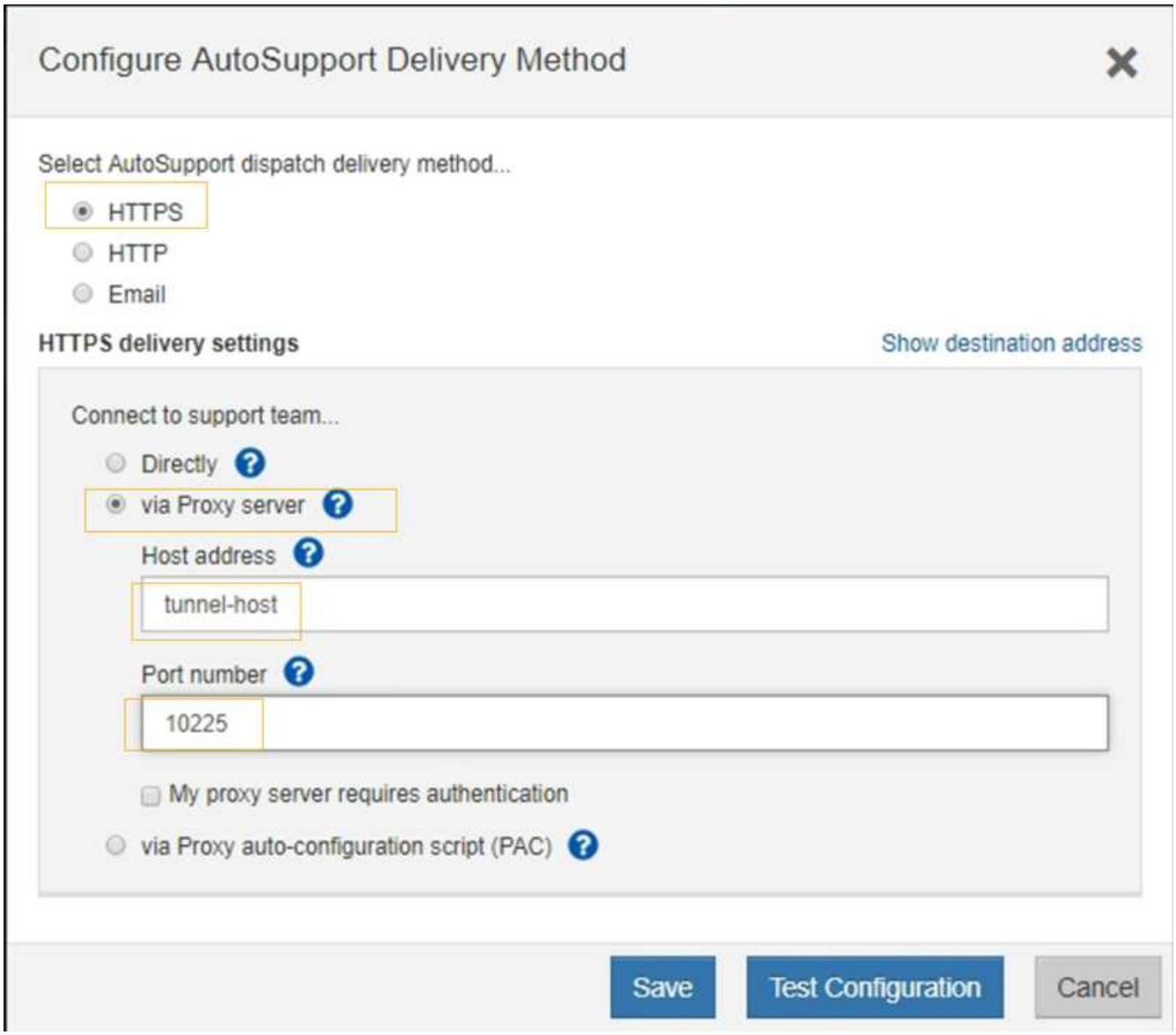
4. 選擇 支援 > 支援中心 > **AutoSupport**。

   AutoSupport 操作頁面隨即出現。



5. 選擇 **Configure AutoSupport Delivery Method** 。

   顯示「設定 AutoSupport 傳送方式」頁面。



6. 選擇*HTTPS*作為傳輸方式。

   用於啟用 HTTPS 的憑證已預先安裝。

7. ${post_edited_translations.segment}
8. 輸入 `tunnel-host`作為 **Host address**。

   `tunnel-host` 是使用管理節點傳送 E 系列 AutoSupport 套件的特殊位址。

9. 輸入 `10225` 作為 **Port number**。

   `10225` 是 StorageGRID Proxy 伺服器上的連接埠號碼，用於接收來自應用裝置中 E 系列控制器的 AutoSupport 套件。

10. 選擇 **Test Configuration** 來測試您的 AutoSupport Proxy 伺服器的路由和組態。

    如果正確，綠色橫幅中會顯示一則訊息：「您的 AutoSupport 組態已驗證。」

如果測試失敗，則會在紅色橫幅中顯示錯誤訊息。請檢查您的 StorageGRID DNS 設定和連網，確保 "慣用寄件者管理節點" 可以連線至 NetApp 支援網站，然後再試一次。

11. 選取 **Save** 。

組態已儲存，並顯示確認訊息：「AutoSupport 傳送方式已設定完成。」

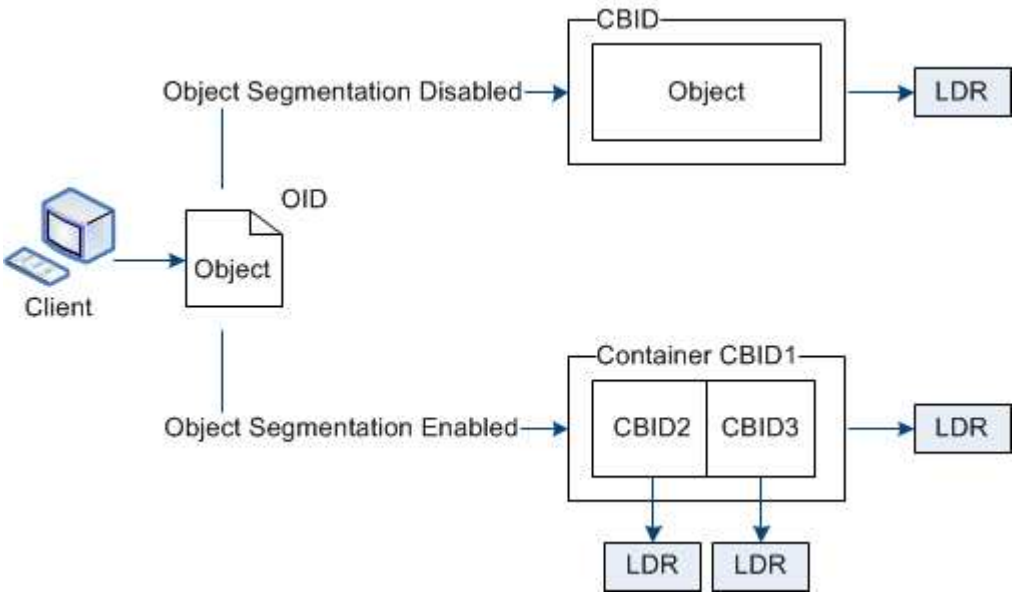
管理儲存節點

使用儲存設備選項

了解 **StorageGRID** 中的物件分割

物件分割是指將一個物件分割成一組較小且固定大小的物件，以針對大型物件最佳化儲存設備與資源使用率的程序。S3 multi-part upload 也會建立分割的物件，其中每個部分皆由一個物件代表。

當物件擷取至 StorageGRID 系統時，LDR 服務會將物件分割成多個區段，並建立一個區段 Container，該 Container 會將所有區段的標頭資訊列為內容。



${post_edited_translations.segment}

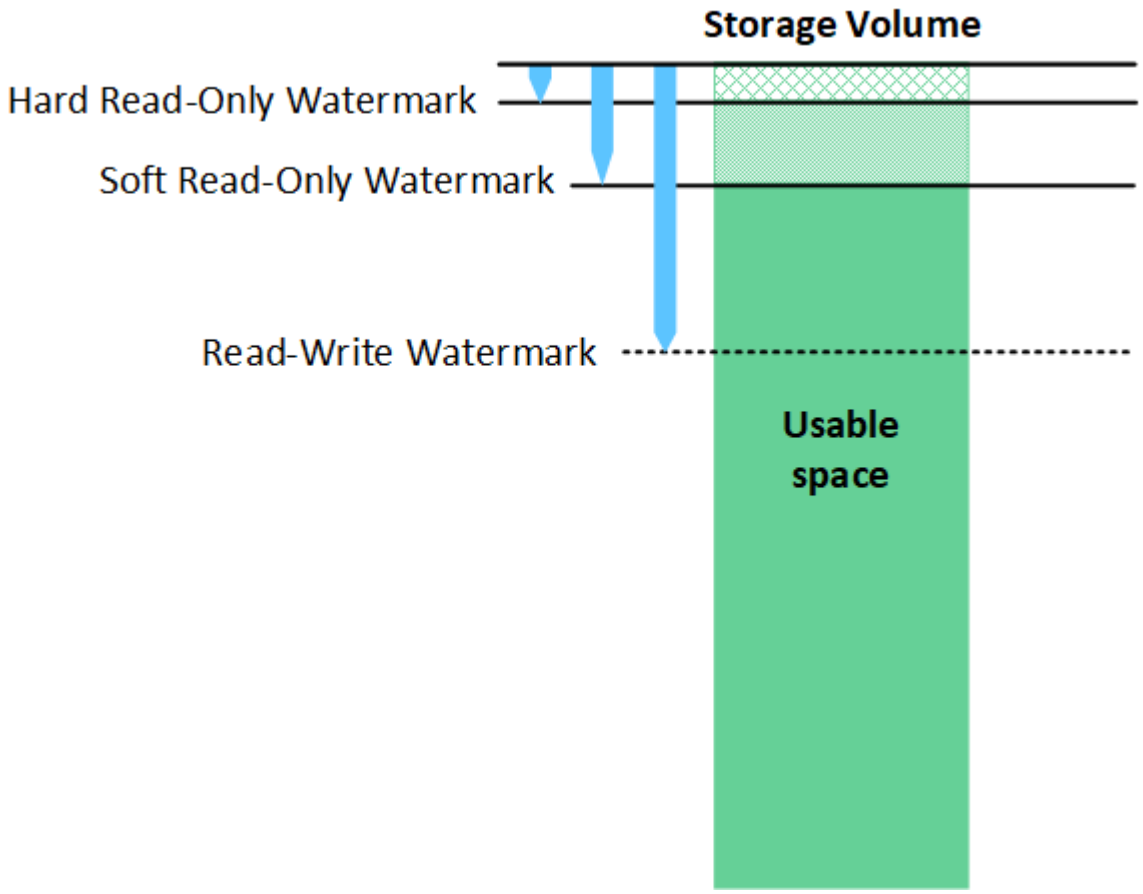
Container 和區段不一定儲存在同一個儲存節點上。Container 和區段可以儲存在 ILM 規則指定的儲存資源池中的任何儲存節點上。

每個區段都由 StorageGRID 系統獨立處理，並計入「Managed Objects」和「Stored Objects」等屬性的數量。例如，如果儲存至 StorageGRID 系統的物件被分割為兩個區段，則在擷取完成後，「Managed Objects」的值會增加三個，如下所示：

```
segment container + segment 1 + segment 2 = three stored objects
```

了解 **StorageGRID** 中的儲存磁碟區浮水印

${post_edited_translations.segment}



儲存 Volume 水印僅適用於複製和銷除編碼物件資料所使用的空間。若要了解 Volume 0 上為物件中繼資料保留的空間，請前往 "管理物件中繼資料儲存設備"。

${post_edited_translations.segment}

${post_edited_translations.segment}

如果儲存節點中每個 Volume 的可用空間少於該 Volume 的軟唯讀浮水印，則該儲存節點將進入唯讀模式。唯讀模式表示此儲存節點向 StorageGRID 系統的其他部分通告唯讀服務，但會處理所有待處理的寫入要求。

例如，假設儲存節點中的每個 Volume 都有一個 10 GB 的軟唯讀浮水印。一旦每個 Volume 的可用空間少於 10 GB，儲存節點就會轉換至軟唯讀模式。

什麼是硬性唯讀水位標記？

*儲存設備 Volume 硬唯讀浮水印*是下一個浮水印，用於指示節點的物件資料可用空間即將滿。

如果某個 Volume 上的可用空間小於該 Volume 的硬性唯讀水位線，則對該 Volume 的寫入作業將會失敗。但是，其他 Volume 的寫入作業可以繼續進行，直到這些 Volume 上的可用空間小於其硬性唯讀水位線為止。

例如，假設儲存節點中的每個 Volume 都有一個 5 GB 的強制唯讀浮水印。一旦每個 Volume 的可用空間少於 5 GB，儲存節點就不再接受任何寫入要求。

硬性唯讀浮水印的值總是小於軟性唯讀浮水印的值。

什麼是讀寫浮水印？

*儲存設備 Volume 讀寫浮水印*僅適用於已轉換為唯讀模式的 Storage Node。它決定節點何時可以再次變為讀寫狀態。當 Storage Node 中任何一個儲存設備 Volume 上的可用空間大於該 Volume 的讀寫浮水印時，節點會自動轉換回讀寫狀態。

例如，假設儲存節點已轉換為唯讀模式。同時假設每個 Volume 的讀寫浮水印為 30 GB。一旦任何 Volume 的可用空間增加到 30 GB，該節點將再次變為讀寫模式。

${post_edited_translations.segment}

檢視儲存設備 **Volume** 浮水印

您可以檢視目前的水位線設定與系統最佳化的值。如果未使用最佳化的水位線，您可以判定是否可以或應該調整設定。

開始之前

- ${post_edited_translations.segment}
- 您已使用 "支援的網頁瀏覽器" 登入 Grid Manager。
- 您有"${post_edited_translations.segment}"。

檢視目前浮水印設定

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     這是預設設置，也是推薦設定。請勿更新這些值。您也可以選擇檢視最佳化的儲存設備浮水印。

   - 如果未選取「使用最佳化的值」複選框，則會使用自訂（非最佳化）浮水印。不建議使用自訂浮水印設定。請依照相關說明"${post_edited_translations.segment}"確定是否可以或應調整這些設定。

     指定自訂浮水印設定時，必須輸入大於 0 的值。

檢視最佳化的儲存設備浮水印

StorageGRID 使用兩個 Prometheus 計量來顯示其為儲存 Volume 軟唯讀浮水印計算的最佳化值。您可以檢視網格中每個儲存節點的最小和最大最佳化值。

1. 選擇 **Support** > **Tools** > **Metrics**。
2. 在 Prometheus 部分，選擇連結以存取 Prometheus 使用者介面。
3. 若要查看建議的最小軟唯讀浮水印，請輸入以下 Prometheus 指標，然後選擇「執行」：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

最後一列顯示每個儲存節點上所有儲存 Volume 的軟唯讀浮水印最小最佳化值。如果此值大於儲存 Volume 軟唯讀浮水印的自訂設定，則會針對該儲存節點觸發 **Low read-only watermark override** 警示。

4. 若要查看建議的最大軟唯讀浮水印，請輸入以下 Prometheus 指標，然後選擇「執行」：

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後一欄顯示每個儲存節點上所有儲存 Volume 的軟唯讀水位線最大最佳化值。

在 **StorageGRID** 中管理物件中繼資料儲存

StorageGRID 系統的物件中繼資料容量控制著此系統可儲存的最大物件數量。為確保您的 StorageGRID 系統有足夠的空間來儲存新物件，您必須了解 StorageGRID 將物件中繼資料儲存在哪裡以及如何儲存。

${post_edited_translations.segment}

物件中繼資料是指描述物件的任何資訊。StorageGRID 使用物件中繼資料來追蹤網格中所有物件的位置，並管理每個物件隨時間的生命週期。

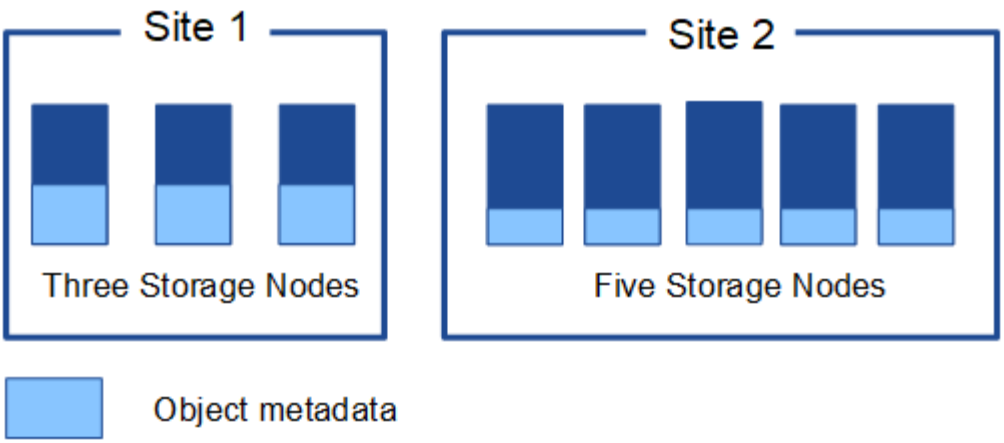
對於 StorageGRID 中的物件，物件中繼資料包括以下類型的資訊：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 對於銷毀編碼物件複本，每個片段的目前儲存設備位置。
- ${post_edited_translations.segment}
- 對於分段物件和多部分物件，分段識別碼和資料大小。

物件中繼資料是如何儲存的？

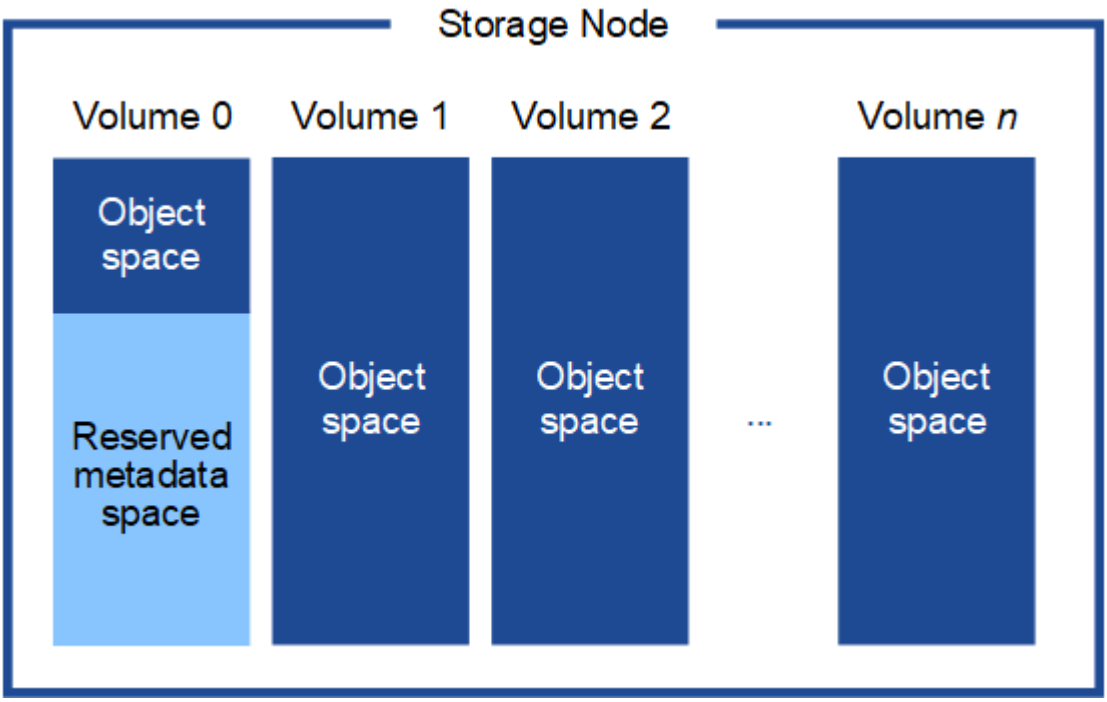
StorageGRID 將物件中繼資料維護在 Cassandra 資料庫中，該資料庫獨立於物件資料儲存。為了提供備援並保護物件中繼資料免於遺失，StorageGRID 在每個站點為系統中所有物件儲存三份中繼資料複本。

此圖表示兩個站台的儲存節點。每個站台擁有相同數量的物件中繼資料，且每個站台的中繼資料會分散至該站台的所有儲存節點。



物件中繼資料儲存在哪裡？

${post_edited_translations.segment}



如圖所示，StorageGRID 在每個儲存節點的儲存設備 Volume 0 上保留空間，用於存放物件中繼資料。它利用保留空間來儲存物件中繼資料並執行必要的資料庫操作。儲存設備 Volume 0 以及儲存節點中所有其他儲存設備磁碟區上的剩餘空間，則專門用於存放物件資料（複本和銷除編碼片段）。

特定儲存節點上為物件中繼資料預留的空間大小取決於以下幾個因素。

中繼資料保留空間設定

「中繼資料保留空間」是一個系統層級的設定，代表在每個儲存節點的 Volume 0 上為中繼資料保留的空間大小。如表所示，此設定的預設值是基於：

- 您最初安裝 StorageGRID 時所使用的軟體版本。
- 每個儲存節點上的記憶體容量。

用於初始 **StorageGRID** 安裝的版本	儲存節點上的記憶體容量	**${post_edited_translations.segment}**
11.5 至 12.0	網格中每個儲存節點的容量為 128 GB 或更多	${post_edited_translations.segment}
	${post_edited_translations.segment}	3 TB（3,000 GB）
11.1 至 11.4	任何一個站台的每個儲存節點上，容量至少為 128 GB	4 TB（4,000 GB）
	${post_edited_translations.segment}	3 TB（3,000 GB）
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 選擇 **Configuration** > **System** > **Storage settings**。
2. 在「儲存設定」頁面上，展開「中繼資料保留空間」區段。

對於 StorageGRID 11.8 或更高版本，中繼資料保留空間值必須至少為 100 GB，且不得超過 1 PB。

對於每個儲存節點具有 128 GB 或更多 RAM 的新 StorageGRID 11.6 或更高版本安裝，預設設定為 8,000 GB（8 TB）。

中繼資料實際保留空間

與系統範圍的「Metadata reserved space」設定相比，物件中繼資料的「實際保留空間」是針對每個 Storage Node 決定的。對於任何指定的 Storage Node，中繼資料的實際保留空間取決於該節點的 Volume 0 大小以及系統範圍的「Metadata reserved space」設定。

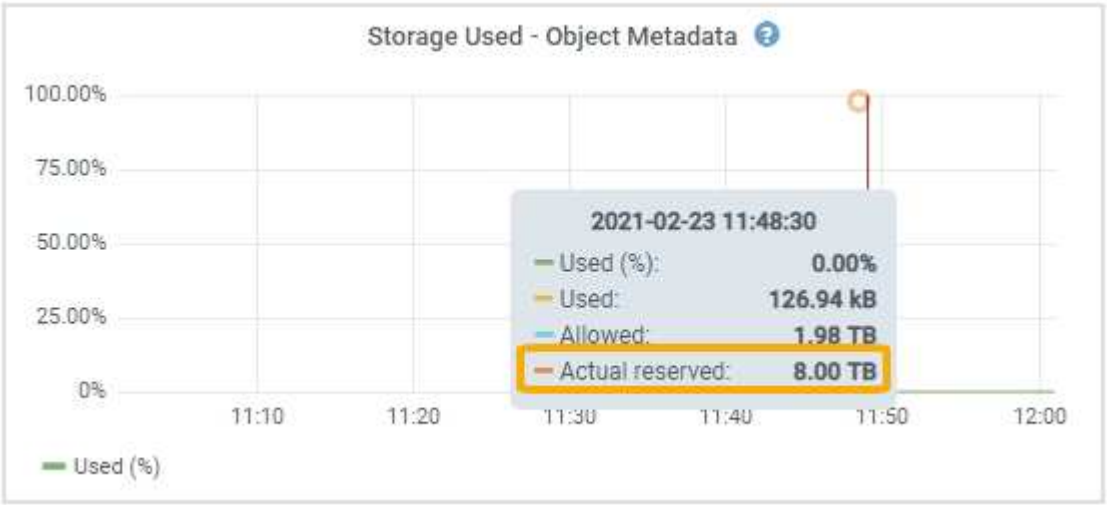
${post_edited_translations.segment}	中繼資料實際保留空間
${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment} • ${post_edited_translations.segment} • 中繼資料保留空間設定 ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}



在快照中，* 實際保留 * 值為 8 TB。此快照適用於新安裝 StorageGRID 11.6 中的大型儲存設備節點。由於此儲存設備節點的系統範圍中繼資料保留空間設定小於 Volume 0，因此此節點的實際保留空間等於中繼資料保留空間設定。

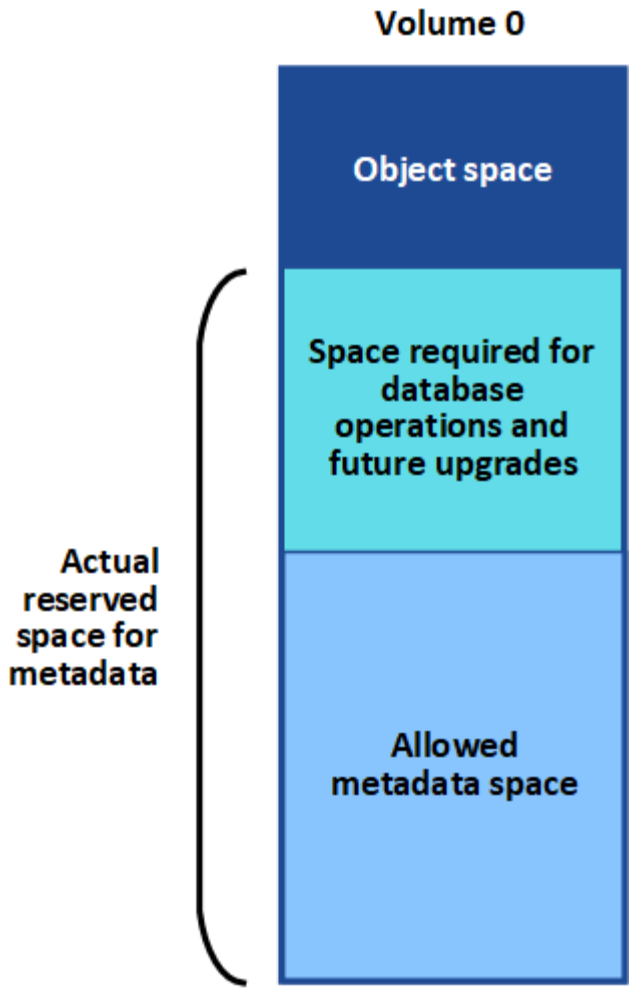
${post_edited_translations.segment}

假設您使用 11.7 或更新版本安裝新的 StorageGRID 系統。在此範例中，假設每個儲存節點（Storage Node）具有超過 128 GB 的 RAM，且儲存節點 1（SN1）的 Volume 0 為 6 TB。根據這些數值：

- 系統範圍的 **Metadata reserved space** 設定為 8 TB。（如果每個 Storage Node 具有超過 128 GB RAM，則這是全新安裝 StorageGRID 11.6 或更高版本的預設值。）
- SN1 的中繼資料實際保留空間為 6 TB。（由於 Volume 0 小於 中繼資料保留空間 設定，因此會保留整個 Volume。）

允許的中繼資料空間

每個 Storage Node 實際用於中繼資料的保留空間，會再細分為可用於物件中繼資料的空間（即 允許的中繼資料空間），以及基本資料庫作業（例如資料精簡與修理）和未來硬體與軟體升級所需的空間。允許的中繼資料空間決定了整體的物件容量。



下表顯示 StorageGRID 如何根據節點的記憶體容量和中繼資料的實際保留空間，計算不同儲存節點的*允許的中繼資料空間*。

		儲存節點上的記憶體容量	
	${post_edited_translations.segment}	>= 128 GB	中繼資料的實際保留空間
⇐ 4 TB	實際保留空間的 60% 用於中繼資料，最大可達 1.32 TB	實際保留空間的 60% 用於中繼資料，最大可達 1.98 TB	4 TB

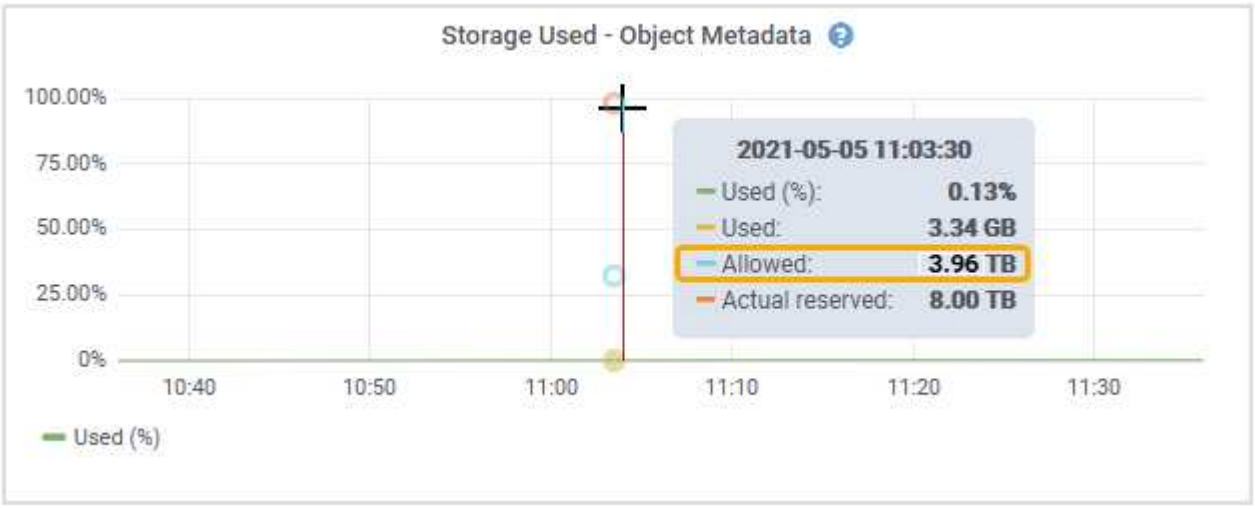
${post_edited_translations.segment}

${post_edited_translations.segment}

步驟

1. 從 Grid Manager 中選擇 **Nodes** 。
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. 將遊標停留在「儲存設備使用情況 - 物件中繼資料」圖表上，找到 **Allowed** 值。



${post_edited_translations.segment}

${post_edited_translations.segment}

`storagegrid_storage_utilization_metadata_allowed_bytes`

${post_edited_translations.segment}

假設您使用 11.6 版本安裝 StorageGRID 系統。在此範例中，假設每個 Storage Node 的記憶體容量都大於 128 GB，且 Storage Node 1 （SN1） 的 Volume 0 為 6 TB。根據這些值：

- 系統範圍的 中繼資料保留空間 設定為 8 TB。（這是 StorageGRID 11.6 或更高版本的預設值，此時每個 Storage 節點具有超過 128 GB RAM。）
- SN1 的中繼資料實際保留空間為 6 TB。（由於 Volume 0 小於 中繼資料保留空間 設定，因此會保留整個 Volume。）
- 根據中繼資料允許空間表中所示的計算，SN1 上中繼資料的允許空間為 3 TB：（中繼資料的實際保留空間 − 1 TB）× 60%，最大可達 3.96 TB。

不同大小的儲存節點如何影響物件容量

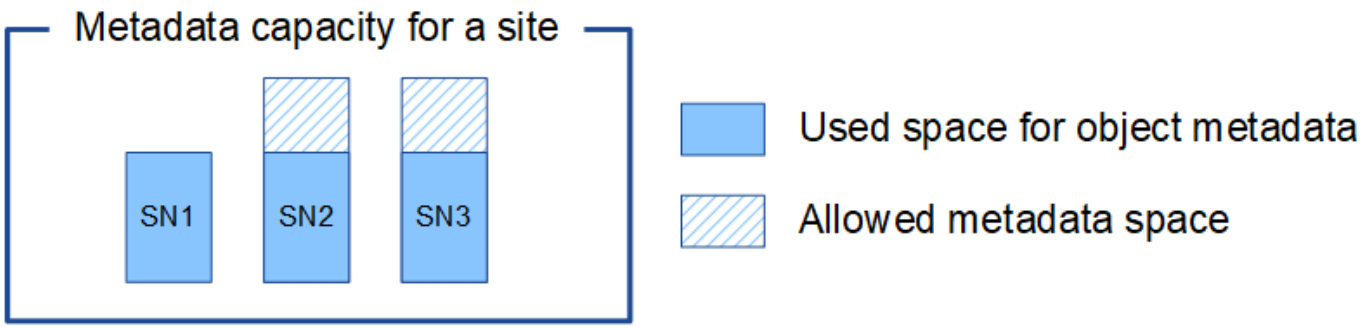
如上所述，StorageGRID 將物件中繼資料均勻分佈到每個站台的各個儲存節點上。因此，如果一個站台包含大小不同的儲存節點，則該站台中最小的節點決定了該站台的中繼資料容量。

${post_edited_translations.segment}

- 您有一個單站台網格，其中包含三個不同大小的儲存節點。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

儲存節點	**Volume 0** 的大小	實際保留的中繼資料空間	允許的中繼資料空間
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

由於物件中繼資料均勻分佈在站台內的各個 Storage Node 上，因此本例中每個節點只能容納 1.32 TB 的中繼資料。SN2 和 SN3 額外允許的 0.66 TB 中繼資料空間無法使用。



${post_edited_translations.segment}

由於物件中繼資料容量控制著最大物件數量，因此當一個節點的中繼資料容量耗盡時，網格實際上就滿了。

相關資訊

- 若要了解如何監控每個 Storage 節點的物件中繼資料容量，請參閱 "${post_edited_translations.segment}" 的說明。
- 若要增加系統的物件中繼資料容量，"${post_edited_translations.segment}"請新增儲存節點。

在 **StorageGRID** 中增加 **Metadata Reserved Space** 設定

${post_edited_translations.segment}

您需要準備的項目

- 您已使用 "支援的網頁瀏覽器" 登入網格管理員。
- 您擁有 "根存取權限或其他網格組態權限"。

關於此任務

${post_edited_translations.segment}

只有當以下兩個條件都成立時，才能增加系統範圍的中繼資料保留空間設定值：

- 系統中任何站台的儲存節點均具有 128 GB 或更多 RAM。
- 系統中任何站台的儲存節點在儲存設備 Volume 0 上都有足夠的可用空間。

請注意，如果增加此設定，所有儲存節點的儲存 Volume 0 上可用於物件儲存的空間將同時減少。因此，根據您預期的物件中繼資料需求，您可能需要將中繼資料保留空間設定為小於 8 TB 的值。

一般來說，使用較大的值比使用較小的值更好。如果「中繼資料保留空間」設定過大，您可以稍後將其減少。相反，如果您稍後增加該值，系統可能需要移動物件資料以釋放空間。

有關中繼資料保留空間設定如何影響特定儲存節點上物件中繼資料儲存的允許空間的詳細說明，請參閱"管理物件中繼資料儲存設備"。

步驟

1. 確定目前的中繼資料保留空間設定。
   a. 選擇 **Configuration** > **System** > **Storage settings**。
   b. 請記下*中繼資料保留空間*的值。
2. 請確保每個儲存節點的儲存設備 Volume 0 上有足夠的可用空間來增加此值。
   a. 選取 **Nodes** 。
   b. 選擇網格中的第一個儲存節點。
   c. 選擇「儲存設備」標籤。
   d. 在「Volume」部分，找到 **/var/local/rangedb/0** 項目。
   e. 確認「可用」值等於或大於您要使用的新值與目前中繼資料保留空間值之間的差異。

      例如，如果中繼資料保留空間設定目前為 4 TB，且您想要將其增加到 6 TB，則可用值必須為 2 TB 或更大。

   f. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點沒有足夠的可用空間，則無法增加中繼資料保留空間值。請勿繼續執行此程序。
      - 如果每個儲存節點在 Volume 0 上都有足夠的可用空間，請繼續執行下一步。
3. 請確保每個儲存節點至少有 128 GB 的 RAM。
   a. 選取 **Nodes** 。
   b. 選擇網格中的第一個儲存節點。
   c. 選擇 **Hardware** 索引標籤。
   d. 將滑鼠懸停在記憶體容量使用圖上。確保 **Total Memory** 至少為 128 GB。
   e. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點的可用總記憶體容量不足，則無法增加中繼資料保留空間值。請勿繼續執行此程序。
      - 如果每個儲存節點至少有 128 GB 的總記憶體容量，則進入下一步。
4. 更新中繼資料保留空間設定。
   a. 選擇 **Configuration** > **System** > **Storage settings**。
   b. 選擇 **Metadata Reserved Space**。
   c. 請輸入新值。

      例如，要輸入 8 TB（這是支援的最大值），請輸入 **8000000000000**（8 後面跟著 12 個零）。

d. 選取 **Save** 。

壓縮 StorageGRID 中儲存的物件

${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"。

關於此任務

預設情況下，物件壓縮處於停用狀態。如果啟用壓縮，StorageGRID 會在儲存每個物件時嘗試使用無損壓縮對其進行壓縮。

更改此設定後，新設定大約需要一分鐘才能生效。已設定的值會被快取，以提高效能和擴充性。

啟用物件壓縮之前，請注意以下事項：

- ${post_edited_translations.segment}
- 將物件儲存至 StorageGRID 的應用程式，可能會在儲存物件之前先將其壓縮。如果用戶端應用程式在將物件儲存至 StorageGRID 之前已經將其壓縮，則選取此選項將無法進一步縮減物件的大小。
- 如果您將 NetApp FabricPool 與 StorageGRID 搭配使用，請勿選取 壓縮儲存的物件。
- 如果選取了 **Compress stored objects**，S3 用戶端應用程式應避免執行指定傳回位元組範圍的 GetObject 作業。這些「範圍讀取」作業效率不彰，因為 StorageGRID 必須有效地解壓縮物件才能存取要求的位元組。從極大型物件要求小範圍位元組的 GetObject 作業效率特別低；例如，從 50 GB 的壓縮物件中讀取 10 MB 的範圍是沒有效率的。

  如果從壓縮物件讀取範圍，用戶端請求可能會逾時。

  如果需要壓縮物件，且用戶端應用程式必須使用範圍讀取，請增加應用程式的讀取逾時時間。

步驟

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 選取 **Save** 。

在 StorageGRID 中管理已滿的 Storage Nodes

當 Storage Node 達到容量上限時，您必須透過新增儲存設備來擴充 StorageGRID 系統。有三個可用選項：新增儲存磁碟區、新增儲存擴充櫃，以及新增 Storage Node。

${post_edited_translations.segment}

每個 Storage Node 均支援最大數量的儲存磁碟區。定義的最大值視平台而異。如果 Storage Node 包含的儲存磁碟區數量少於最大數量，您可以新增磁碟區以增加其容量。請參閱 "擴充 StorageGRID 系統" 的說明。

${post_edited_translations.segment}

部分 StorageGRID 應用裝置儲存節點（例如 SG6060 或 SG6160）支援額外儲存容量架。如果您擁有的 StorageGRID 應用裝置具有擴充功能，但尚未擴充至最大容量，則可以新增儲存設備架來增加容量。請參閱相關說明 "擴充 StorageGRID 系統"。

${post_edited_translations.segment}

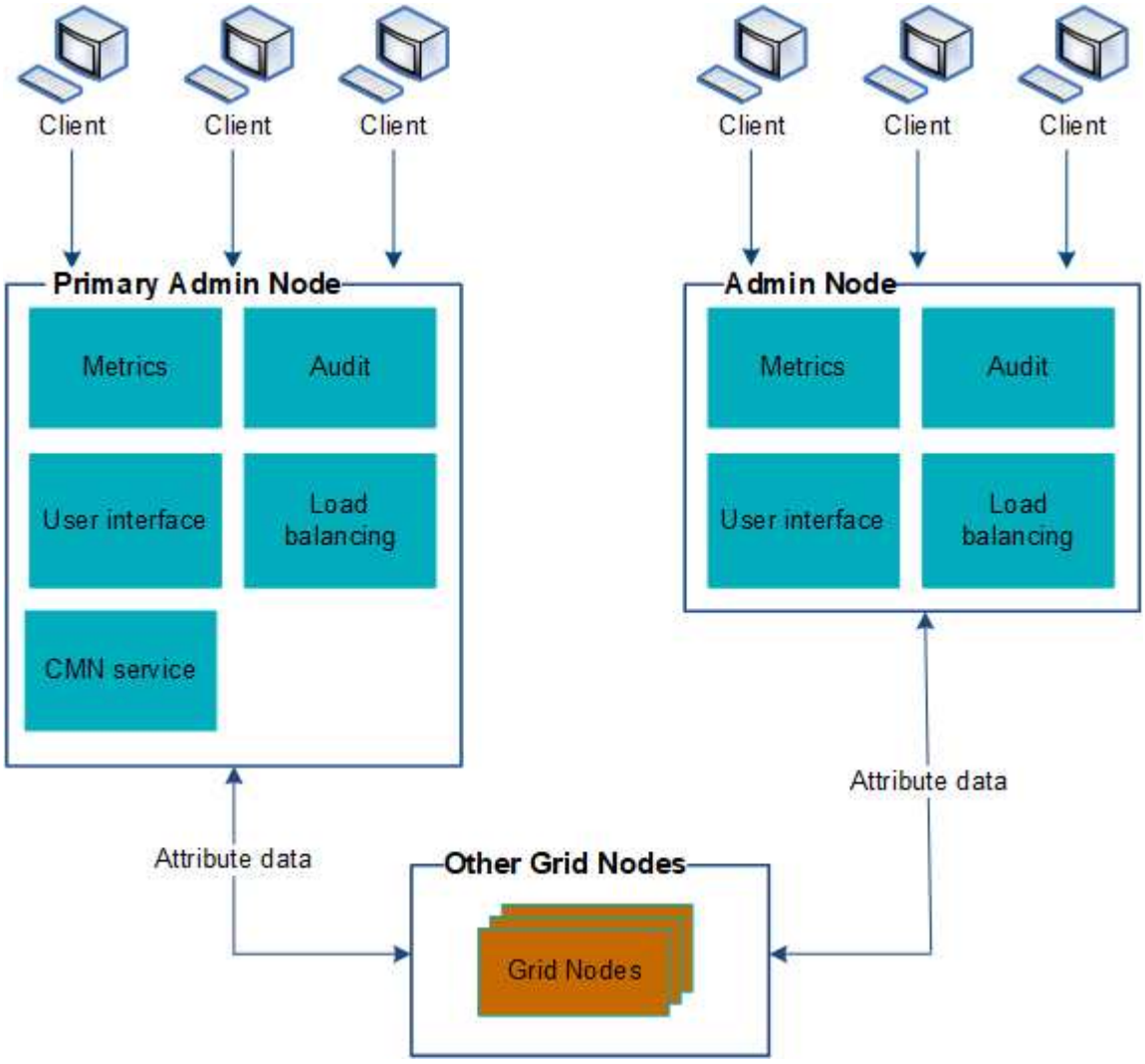
您可以透過新增儲存節點來增加儲存容量。新增儲存設備時，必須仔細考慮目前作用中的 ILM 規則和容量需求。請參閱相關說明 "擴充 StorageGRID 系統"。

管理管理節點

在 **StorageGRID** 中使用多個管理節點

${post_edited_translations.segment}

如果 Admin Node 變得無法使用，屬性處理仍會繼續，警示仍會觸發，且電子郵件通知和 AutoSupport 套件仍會傳送。然而，除了通知和 AutoSupport 套件之外，擁有多個 Admin Node 並不提供容錯移轉保護。



${post_edited_translations.segment}

- Web 用戶端可以重新連線到任何其他可用的管理節點。
- 如果系統管理員已設定管理節點的高可用度群組，則 Web 用戶端可以繼續使用 HA 群組的虛擬 IP 位址存取 Grid Manager 或 Tenant Manager。請參閱"管理高可用度群組"。

> 使用 HA 群組時，如果作用中的管理節點發生故障，存取將會中斷。HA 群組的虛擬 IP 位址容錯移轉至群組內的另一個管理節點後，使用者必須重新登入。

某些維護任務只能透過主管理節點執行。如果主管理節點發生故障，必須先恢復，StorageGRID 系統才能完全恢復正常運作。

識別 StorageGRID 中的主要管理節點

主管理節點比非主管理節點提供更多功能。例如，某些維護程序必須使用主管理節點執行。

有關管理節點的詳細資訊，請參閱 "什麼是管理節點"。

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"。

步驟

1. 選取 **Nodes** 。
2. ${post_edited_translations.segment}

   在搜尋結果中，識別「類型」欄位中顯示「Primary Admin Node」的節點。應該會列出一個主要管理節點。