管理StorageGRID

StorageGRID

NetApp
November 04, 2025

目錄

管理StorageGRID

管理StorageGRID 功能：總覽

請使用這些指示來設定及管理StorageGRID 一套功能完善的系統。

關於這些指示

設定及管理 StorageGRID 的主要工作可讓您：

- 使用 Grid Manager 來設定群組和使用者
- 建立租戶帳戶、以允許 S3 和 Swift 用戶端應用程式儲存和擷取物件
- 設定及管理 StorageGRID 網路
- 設定AutoSupport 功能
- 管理節點設定

開始之前

- 您大致瞭StorageGRID 解整個系統。
- 您對Linux命令Shell、網路及伺服器硬體設定與組態擁有相當詳細的知識。

開始使用 Grid Manager

網頁瀏覽器需求

您必須使用支援的網頁瀏覽器。

網頁瀏覽器	支援的最低版本
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

您應該將瀏覽器視窗設定為建議的寬度。

瀏覽器寬度	像素
最低	1024
最佳化	1280

登入Grid Manager

您可以在支援的網頁瀏覽器的位址列中輸入管理節點的完整網域名稱（FQDN）或IP位址、以存取Grid Manager登入頁面。

總覽

每StorageGRID 個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。您可以登入任何管理節點上的Grid Manager來管理StorageGRID 此系統。不過、管理節點並不完全相同：

- 在一個管理節點上所做的警示認可（舊系統）不會複製到其他管理節點。因此、針對警示所顯示的資訊在每個管理節點上可能看起來不一樣。
- 部分維護程序只能從主要管理節點執行。

連線至 **HA** 群組

如果管理節點包含在高可用度（HA）群組中、您可以使用HA群組的虛擬IP位址或對應至虛擬IP位址的完整網域名稱來連線。主要管理節點應選取為群組的主要介面、以便在存取Grid Manager時、在主要管理節點上存取、除非主要管理節點無法使用。請參閱 "管理高可用度群組"。

使用 **SSO**

登入步驟在以下情況下略有不同 "已設定單一登入（ SSO ）"。

在第一個管理節點上登入 **Grid Manager**

開始之前

- 您擁有登入認證資料。
- 您使用的是 "支援的網頁瀏覽器"。
- Cookie會在您的網頁瀏覽器中啟用。
- 您屬於至少有一個權限的使用者群組。
- 您擁有 Grid Manager 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。

  若要在 HTTPS 預設連接埠（ 443 ）以外的連接埠上存取 Grid Manager 、請在 URL 中加入連接埠編號：

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO 無法在受限的 Grid Manager 連接埠上使用。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. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。請參閱 "管理安全性憑證"。
4. 登入Grid Manager。

   顯示的登入畫面取決於是否已針對 StorageGRID 設定單一登入（ SSO ）。

未使用 **SSO**

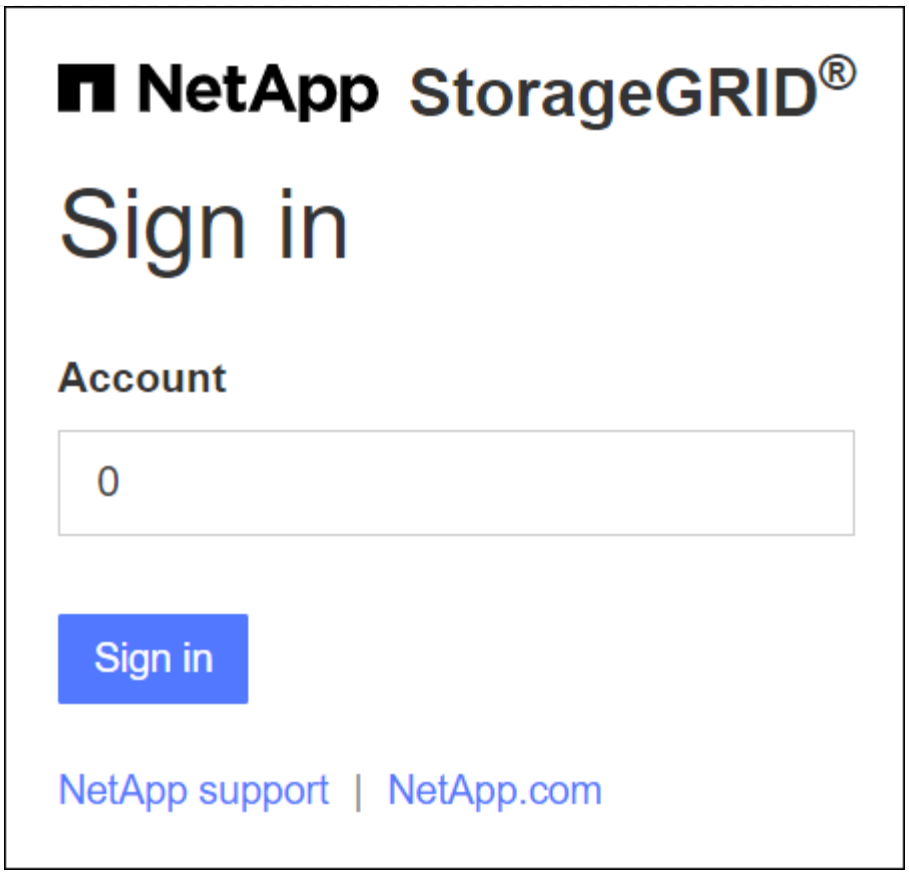
a. 輸入Grid Manager的使用者名稱和密碼。

b. 選擇*登入*。

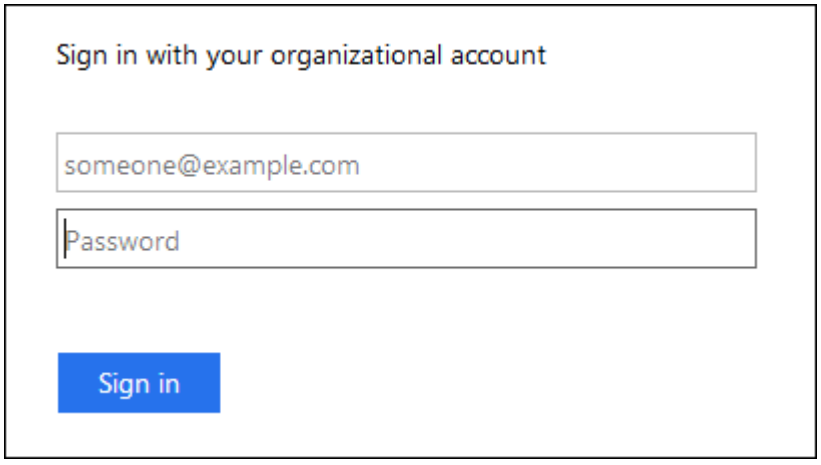
使用 **SSO**

- 如果 StorageGRID 正在使用 SSO 、而這是您第一次在此瀏覽器上存取 URL ：

  i. 選擇*登入*。您可以將 0 留在「帳戶」欄位中。



ii. 在組織的SSO登入頁面上輸入標準SSO認證。例如：

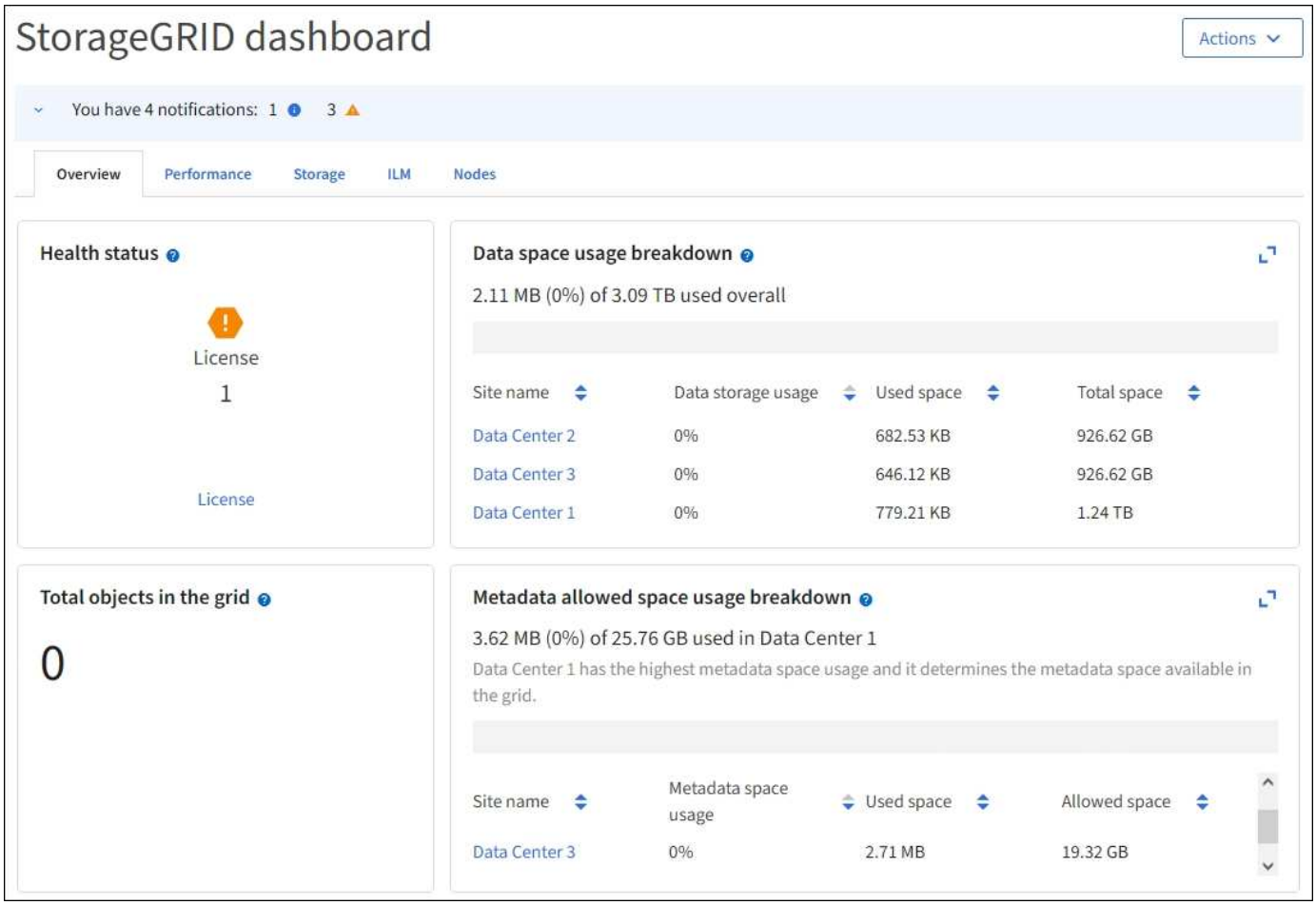


- 如果 StorageGRID 使用 SSO 、且您先前已存取 Grid Manager 或租戶帳戶：
  i. 輸入 * 0* （ Grid Manager 的帳戶 ID ）、或選擇 * Grid Manager* （如果它出現在最近帳戶清單中）。

ii. 選擇*登入*。

iii. 在組織的SSO登入頁面上、以標準SSO認證登入。

登入後、會出現 Grid Manager 首頁、其中包含儀表板。若要瞭解提供的資訊、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其他管理節點。

未使用 **SSO**

步驟

1. 在瀏覽器的位址列中、輸入其他管理節點的完整網域名稱或IP位址。視需要附上連接埠號碼。
2. 輸入Grid Manager的使用者名稱和密碼。
3. 選擇*登入*。

使用 **SSO**

如果 StorageGRID 正在使用 SSO 、而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

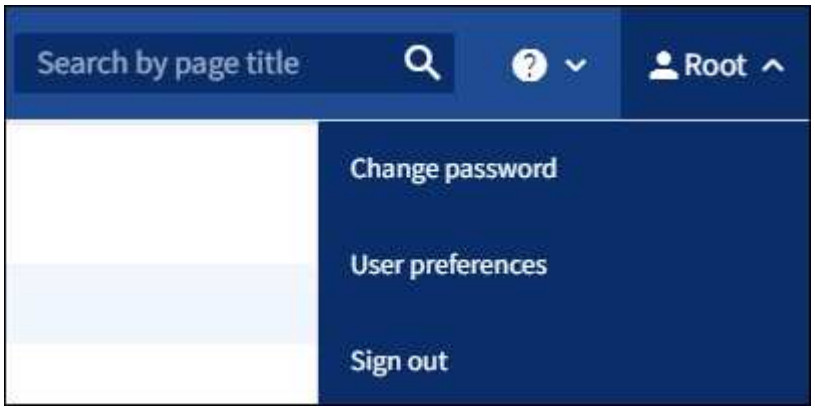
1. 在瀏覽器的網址列中、輸入其他管理節點的完整網域名稱或 IP 位址。
2. 如果您的 SSO 工作階段已過期、請再次輸入您的認證。

登出Grid Manager

完成 Grid Manager 的使用後、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Cookie設定、關閉瀏覽器可能不會將您登出系統。

步驟

1. 在右上角選取您的使用者名稱。



2. 選取 * 登出 * 。

選項	說明
SSO未在使用中	您已登出管理節點。 此時會顯示Grid Manager登入頁面。 *附註：*如果您登入一個以上的管理節點、則必須登出每個節點。
SSO已啟用	您已登出您正在存取的所有管理節點。 畫面上會顯示「這個登入頁面」StorageGRID 。網格管理器*在「*最近的帳戶」下拉式清單中列為預設值、*帳戶ID*欄位則顯示0。 • 注意： * 如果啟用 SSO 、而且您也已登入租戶管理程式、您也必須登入 "登出租戶帳戶" 至 "登出 SSO"。

變更您的密碼

如果您是Grid Manager的本機使用者、可以變更自己的密碼。

開始之前

您將使用登入Grid Manager "支援的網頁瀏覽器"。

關於這項工作

如果您以同盟使用者身分登入 StorageGRID 、或是啟用單一登入（ SSO ）、就無法在 Grid Manager 中變更密碼。而是必須變更外部身分識別來源的密碼、例如Active Directory或OpenLDAP。

步驟

1. 從Grid Manager標頭中、選取*您的名稱_*>*變更密碼*。
2. 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、且不得超過32個字元。密碼區分大小寫。

4. 重新輸入新密碼。
5. 選擇*保存*。

檢視**StorageGRID** 本授權資訊

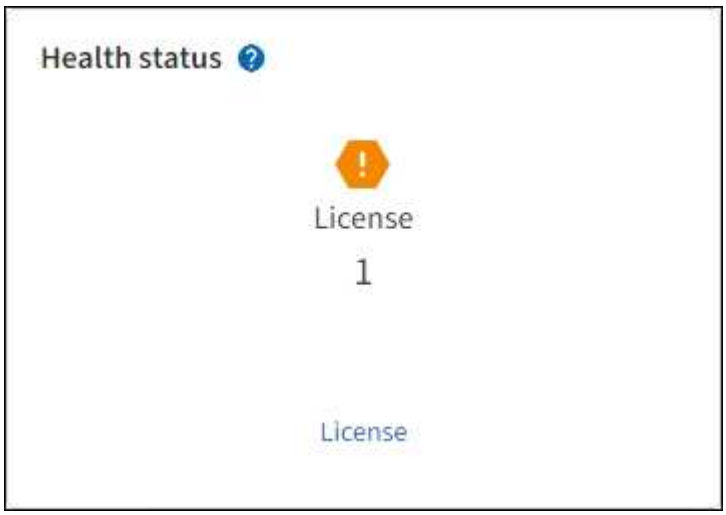
您可以視StorageGRID 需要檢視您的支援資訊、例如網格的最大儲存容量。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。

關於這項工作

如果此 StorageGRID 系統的軟體授權有問題、儀表板上的健全狀況狀態卡會包含授權狀態圖示和 * 授權 * 連結。此數字表示授權相關問題的數量。



步驟

1. 執行下列其中一項動作、即可存取「授權」頁面：
   - 選擇*維護*>*系統*>*授權*。
   - 從儀表板上的「健全狀況」狀態卡中、選取「授權狀態」圖示或「 * 授權 * 」連結。

     僅當授權發生問題時、才會顯示此連結。

2. 檢視目前授權的唯讀詳細資料：
   - 系統ID、這是此安裝的唯一識別號碼StorageGRID StorageGRID
   - 授權序號
   - 授權類型、 * 永久 * 或 * 訂閱 *

- 網格的授權儲存容量
- 支援的儲存容量
- 授權結束日期。* 不適用 * 代表永久授權。
- 支援結束日期

  此日期是從目前的使用許可檔案讀取，如果您在取得使用許可檔案之後延長或續約支援服務合約，則可能已過期。若要更新此值、請參閱 "更新StorageGRID 版本的授權資訊"。您也可以使用 Active IQ 檢視實際的合約結束日期。

- 授權文字檔的內容

更新StorageGRID 版本的授權資訊

您必須在StorageGRID 授權條款變更時、隨時更新您的不適用系統的授權資訊。例如、如果您為網格購買額外的儲存容量、則必須更新授權資訊。

開始之前

- 您有新的授權檔案可套用StorageGRID 到您的作業系統。
- 您有 "特定存取權限"。
- 您有資源配置通關密碼。

步驟

1. 選擇*維護*>*系統*>*授權*。
2. 在「更新授權」區段中、選取 * 瀏覽 * 。
3. 找到並選取新的授權檔案（`.txt`）。

   系統會驗證並顯示新的授權檔案。

4. 輸入資源配置通關密碼。
5. 選擇*保存*。

使用 API

使用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、或更快建立多個實體、例如使用者。

頂級資源

Grid Management API提供下列頂級資源：

- `/grid`：只有Grid Manager使用者才能存取、而且是根據已設定的群組權限而定。
- `/org`：只有屬於租戶帳戶的本機或聯盟LDAP群組的使用者才能存取。如需詳細資訊、請參閱 "使用租戶帳戶"。

- `/private`：只有Grid Manager使用者才能存取、而且是根據已設定的群組權限而定。私有API如有變更、恕不另行通知。私有端點也會忽略該要求的API版本。StorageGRID

發出**API**要求

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、可讓開發人員和非開發人員StorageGRID 利用API在Real-Time中執行作業。

Swagger使用者介面提供每個API作業的完整詳細資料和文件。

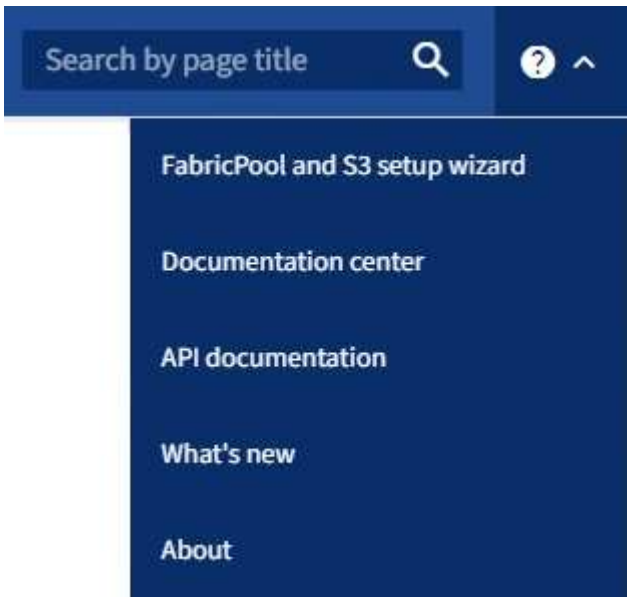
開始之前

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

> 您使用API文件網頁執行的任何API作業都是即時作業。請小心不要錯誤地建立、更新或刪除組態資料或其他資料。

步驟

1. 從 Grid Manager 標頭選取說明圖示、然後選取 * API 文件 * 。



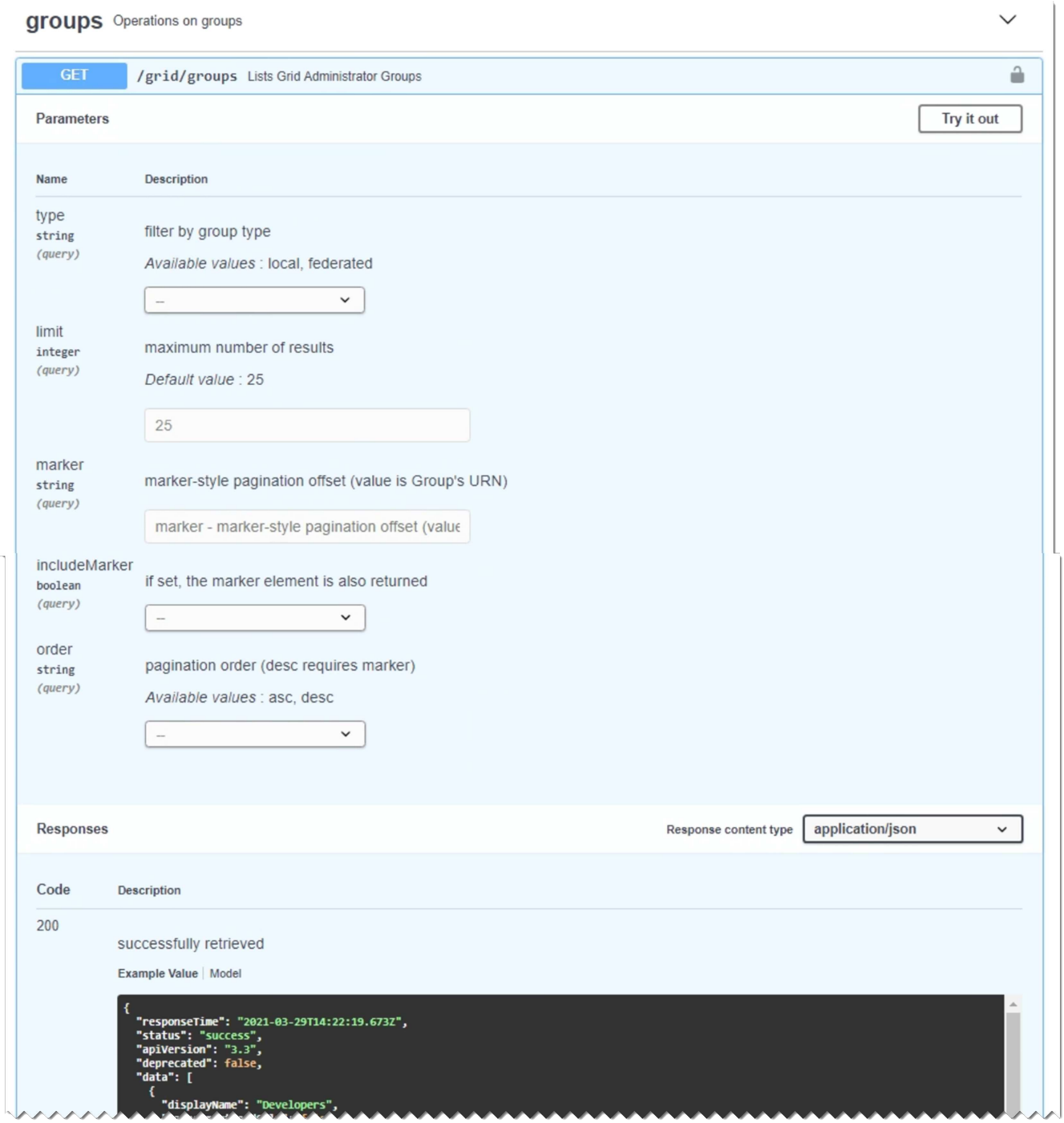
2. 若要使用私有API執行作業、請選取StorageGRID 「畫面管理API」頁面上的*前往私有API文件*。

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

3. 選取所需的作業。

   展開API作業時、您可以看到可用的HTTP動作、例如GET、PUT、update和DELETE。

4. 選取HTTP動作以查看申請詳細資料、包括端點URL、任何必要或選用參數的清單、申請本文的範例（視需要）、以及可能的回應。



5. 判斷要求是否需要其他參數、例如群組或使用者ID。然後取得這些值。您可能需要先發出不同的API要求、才能取得所需的資訊。
6. 判斷您是否需要修改範例要求本文。如果是、您可以選取*模型*來瞭解每個欄位的需求。
7. 選擇*試用*。
8. 提供任何必要的參數、或視需要修改申請本文。
9. 選擇*執行*。
10. 檢閱回應代碼以判斷要求是否成功。

Grid Management API會將可用的作業組織到下列各節中。

此清單僅包含公用API中可用的作業。

- * 帳戶 * ：管理儲存租戶帳戶的作業、包括建立新帳戶和擷取指定帳戶的儲存使用量。
- * 警示 * ：列出目前警示（舊版系統）的作業、並傳回網格健全狀況的相關資訊、包括目前警示和節點連線狀態摘要。
- * 警示記錄 * ：已解決警示的操作。
- * 警示接收者 * ：警示通知接收者的作業（電子郵件）。
- * 警示規則 * ：警示規則的作業。
- * 警示 / 靜音 * ：警示靜音作業。
- * 警示 * ：警示作業。
- * 稽核 * ：列出及更新稽核組態的作業。
- * 驗證 * ：執行使用者工作階段驗證的作業。

  Grid Management API支援承載權杖驗證方案。若要登入、您必須在驗證要求的Json實體中提供使用者名稱和密碼（也就是 `POST /api/v3/authorize`）。如果使用者已成功驗證、則會傳回安全性權杖。此權杖必須在後續API要求的標頭中提供（「授權：bear_tokon_」）。權杖將在 16 小時後過期。

  如果StorageGRID 啟用了單一登入功能、您必須執行不同的驗證步驟。請參閱「如果啟用單一登入、則驗證 API 。」

  如需改善驗證安全性的資訊、請參閱「防範跨網站要求偽造」。

- * 用戶端憑證 * ：設定用戶端憑證的作業，以便使用外部監控工具安全地存取 StorageGRID 。
- * 組態 * ：與 Grid Management API 產品版本和版本相關的作業。您可以列出該版本所支援的產品版本和Grid Management API主要版本、也可以停用已過時的API版本。
- * 停用功能 * ：檢視可能已停用功能的作業。
- * DNS 伺服器 * ：列出及變更已設定外部 DNS 伺服器的作業。
- * 磁碟機詳細資料 * ：特定儲存設備機型的磁碟機操作。
- * 端點網域名稱 * ：列出及變更 S3 端點網域名稱的作業。
- * 銷毀編碼 * ：銷毀編碼設定檔的操作。
- * 擴充 * ：擴充作業（程序層級）。
- * 擴充節點 * ：擴充作業（節點層級）。
- * 擴充站台 * ：擴充作業（站台層級）。
- * 網格網路 * ：列出及變更網格網路清單的作業。
- *GRID 密碼 * ：網格密碼管理作業。
- * 群組 * ：管理本機 Grid Administrator 群組及從外部 LDAP 伺服器擷取同盟 Grid Administrator 群組的作業。

- * 身分識別來源 * ：設定外部身分識別來源及手動同步同盟群組與使用者資訊的作業。
- * ILM * ：資訊生命週期管理（ ILM ）作業。
- * 進行中程序 * ：擷取目前進行中的維護程序。
- * 授權 * ：擷取及更新 StorageGRID 授權的作業。
- * 日誌 * ：收集和下載日誌文件的操作
- * 指標 * ： StorageGRID 指標上的作業、包括單一時間點的即時指標查詢、以及一段時間內的範圍指標查詢。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。

  包括的指標 *private* 其名稱僅供內部使用。這些指標可能會在StorageGRID 不另行通知的情況下於各個版本之間變更。

- * 節點詳細資料 * ：節點詳細資料的作業。
- * 節點健全狀況 * ：節點健全狀況狀態上的作業。
- * 節點儲存狀態 * ：節點儲存狀態上的作業。
- * ntp 伺服器 * ：列出或更新外部網路時間傳輸協定（ NTP ）伺服器的作業。
- * 物件 * ：物件和物件中繼資料的作業。
- * 恢復 * ：恢復過程的操作。
- * 恢復套件 * ：下載恢復套件的作業。
- * 區域 * ：檢視及建立區域的作業。
- *S3 物件鎖定 * ：在全域 S3 物件鎖定設定上的作業。
- * 伺服器憑證 * ：檢視及更新 Grid Manager 伺服器憑證的作業。
- **SNMP** ：目前 SNMP 組態的作業。
- * 儲存浮水印 * ：儲存節點浮水印。
- * 流量類別 * ：流量分類原則的作業。
- * 不受信任的用戶端網路 * ：在不受信任的用戶端網路組態上的作業。
- * 使用者 * ：檢視及管理 Grid Manager 使用者的作業。

Grid Management API版本管理

Grid Management API使用版本管理來支援不中斷營運的升級。

例如、此 Request URL 會指定 API 的版本 4 。

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

當進行與舊版不相容的變更時、 API 的主要版本會增加。當進行與舊版相容的變更時、會增加 API 的次要版本。相容的變更包括新增端點或新屬性。

下列範例說明如何根據所做的變更類型來提高API版本。

API變更類型	舊版本	新版本
與舊版相容	2.1.	2.2.
與舊版不相容	2.1.	3.0

第一次安裝 StorageGRID 軟體時、只會啟用最新版的 API 。不過、當您升級StorageGRID 至全新的功能版本的更新版時、您仍可繼續存取舊版的API、以取得至少一個StorageGRID 版本的更新功能。

您可以設定支援的版本。請參閱 Swagger API 文件的 * 組態 * 一節、以取得 "網格管理API" 以取得更多資訊。您應該在更新所有 API 用戶端以使用較新版本之後、停用舊版的支援。

過時的要求會以下列方式標示為已過時：

- 回應標頭為「deprecated：true」
- Json回應本文包含「deprecated」：true
- NMS.log中會新增已過時的警告。例如：

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

判斷目前版本支援哪些API版本

使用 `GET /versions` API 要求傳回支援的 API 主要版本清單。此要求位於 Swagger API 文件的 * 組態 * 區段。

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

指定要求的API版本

您可以使用路徑參數來指定API版本 (`/api/v4`）或標頭 (`Api-Version: 4`）。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
```

防範跨網站要求偽造（**CSRF**）

您StorageGRID 可以使用CSRF權杖來強化使用Cookie的驗證功能、協助防範跨網站要求偽造（CSRF）攻擊。Grid Manager與租戶管理程式會自動啟用此安全功能、其他API用戶端則可選擇是否在登入時啟用。

攻擊者若能觸發要求至不同網站（例如HTTP表單POST）、可能會導致使用登入使用者的Cookie發出特定要求。

利用CSRF權杖協助防範CSRF攻擊。StorageGRID啟用時、特定Cookie的內容必須符合特定標頭或特定POST本文參數的內容。

若要啟用此功能、請設定 `csrfToken` 參數至 `true` 驗證期間。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"
```

如果正確、則為A `GridCsrfToken` Cookie是以隨機值設定、用於登入Grid Manager和 `AccountCsrfToken` Cookie是以隨機值設定、用於登入租戶管理程式。

如果Cookie存在、則所有可修改系統狀態的要求（POST、PUT、PATCH、DELETE）都必須包含下列其中一項：

- 。 `X-Csrf-Token` 標頭、並將標頭值設為CSRF權杖Cookie的值。
- 對於接受格式編碼實體的端點：a `csrfToken` 表單編碼要求本文參數。

如需其他範例與詳細資料、請參閱線上API文件。

> 如果要求設定了 CSRF 權杖 Cookie 、也會針對任何要求 JSON 要求主體做為額外的防護措施、強制使用「 Content-Type ： application/json 」標頭來防範 CSRF 攻擊。

如果啟用單一登入、請使用**API**

如果啟用單一登入、請使用**API**（**Active Directory**）

如果您有 "已設定並啟用單一登入（SSO）" 而且您使用Active Directory做為SSO供應商、必須發出一系列API要求、才能取得適用於Grid Management API或租戶管理API的驗證權

杖。

如果啟用單一登入、請登入**API**

如果您使用Active Directory做為SSO身分識別供應商、則適用這些指示。

開始之前

- 您知道屬於StorageGRID 某個位向使用者群組的聯盟使用者的SSO使用者名稱和密碼。
- 如果您想要存取租戶管理API、就知道租戶帳戶ID。

關於這項工作

若要取得驗證權杖、您可以使用下列其中一個範例：

- 。 `storagegrid-ssoauth.py` Python指令碼、位於StorageGRID 安裝檔案目錄中 (`./rpms` 對於 Red Hat Enterprise Linux 、 `./debs` 適用於Ubuntu或DEBIAN,以及 `./vsphere` （適用於VMware）。
- Curl要求的工作流程範例。

  如果執行速度太慢、捲曲工作流程可能會逾時。您可能會看到以下錯誤： `A valid SubjectConfirmation was not found on this Response`。

  > 範例Curl工作流程無法防止其他使用者看到密碼。

如果您遇到 URL 編碼問題、可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python指令碼：前往步驟 2 。
   - 使用Curl要求。前往步驟3。
2. 如果您要使用 `storagegrid-ssoauth.py` 指令碼、將指令碼傳遞給Python解釋器、然後執行指令碼。

   出現提示時、請輸入下列引數的值：
   - SSO方法。輸入「ADFS」或「ADFS」。
   - SSO使用者名稱
   - 安裝了鏡面的網域StorageGRID
   - 解決這個StorageGRID 問題
   - 租戶帳戶ID（如果您要存取租戶管理API）。

```
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
```

輸出中提供了驗證權杖。StorageGRID您現在可以將權杖用於其他要求、類似於未使用SSO時使用API的方式。

3. 如果您要使用捲髮要求、請使用下列程序。

   a. 宣告登入所需的變數。

```
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做為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的驗證URL、請向發出POST要求 `/api/v3/authorize-saml`，並從回應中移除其他Json編碼。

   此範例顯示的已簽署驗證URL的POST要求 `TENANTACCOUNTID`。結果將傳送至 `python -m json.tool` 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URL編碼的已簽署URL、但不包含其他JSON-encoding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 `SAMLRequest` 從回應中取得以供後續命令使用。

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

d. 取得完整的URL、其中包含AD FS的用戶端要求ID。

其中一個選項是使用先前回應的URL來要求登入表單。

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

回應包括用戶端要求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要求ID。

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

f. 將您的認證資料傳送至先前回應的表單動作。

```
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會傳回302重新導向、並在標頭中顯示其他資訊。

> 如果您的SSO系統已啟用多因素驗證（MFA）、則表單POST也會包含第二個密碼或其他認證資料。

```
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. 儲存 `MSISAuth` 來自回應的Cookie。

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

h. 從驗證貼文傳送內含Cookie的Get要求至指定位置。

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

回應標頭會包含AD FS工作階段資訊、以供日後登出使用、而回應本文會在隱藏表單欄位中包含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 `SAMLResponse` 從隱藏欄位：

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

j. 使用儲存的 `SAMLResponse`、打造StorageGRID 一個不一樣的`/api/saml-response` 要求產生StorageGRID 驗證權杖。

適用於 `RelayState`、如果您要登入Grid Management API、請使用租戶帳戶ID或使用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
```

回應包括驗證權杖。

```
{
    "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另存為 `MYTOKEN`。

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

您現在可以使用 `MYTOKEN` 對於其他要求、類似於不使用SSO時使用API的方式。

如果啟用單一登入、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或租戶管理API。 如果您使用Active Directory做為SSO身分識別供應商、則適用這些指示

關於這項工作

如果需要、您可以登出組織的單一登出頁面、登出 StorageGRID API 。或者、您也可以觸發StorageGRID 來自下列項目的單一登出（SLO）：需要有效StorageGRID 的SESO承載權杖。

步驟

1. 若要產生已簽署的登出要求、請將「 Cookie 」「 SSO=true 」傳給 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
```

會傳回登出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. 傳送要求至登出URL以觸發SLO並重新導向StorageGRID 至還原。

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

會傳回302回應。重新導向位置不適用於純API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. 刪除StorageGRID 不記名權杖。

刪除StorageGRID 此不含SSO的不含支援權杖的方式相同。如果未提供「 Cookie 」「 SSO = True 」、則使用者會登出 StorageGRID 而不會影響 SSO 狀態。

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

答 `204 No Content` 回應表示使用者現在已登出。

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

如果啟用單一登入、請使用**API**（**Azure**）

如果您有 "已設定並啟用單一登入（SSO）" 您可以使用Azure做為SSO供應商、使用兩個範例指令碼來取得適用於Grid Management API或租戶管理API的驗證權杖。

如果啟用**Azure**單一登入、請登入**API**

如果您使用Azure做為SSO身分識別供應商、則適用這些指示

開始之前

- 您知道屬於StorageGRID 某個支援對象群組的聯盟使用者的SSO電子郵件地址和密碼。
- 如果您想要存取租戶管理API、就知道租戶帳戶ID。

關於這項工作

若要取得驗證權杖、您可以使用下列範例指令碼：

- 。 `storagegrid-ssoauth-azure.py` Python指令碼
- 。 `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 (`./rpms` 對於 Red Hat Enterprise Linux 、 `./debs` 適用於Ubuntu或DEBIAN,以及 `./vsphere` （適用於VMware）。

若要與 Azure 自行撰寫 API 整合、請參閱 `storagegrid-ssoauth-azure.py` 指令碼：Python指令碼會StorageGRID 直接提出兩項要求（先取得SAMLRequest、之後取得授權權杖）、也會呼叫Node.js指令碼與Azure互動、以執行SSO作業。

SSO作業可以使用一系列API要求執行、但這樣做並不直接。Puppeteer Node.js模組可用來掃描Azure SSO介面。

如果您遇到 URL 編碼問題、可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 安裝所需的相依性、如下所示：
   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. 將Python指令碼傳遞給Python解譯器以執行指令碼。

   然後Python指令碼會呼叫對應的Node.js指令碼、以執行Azure SSO互動。

3. 出現提示時、請輸入下列引數的值（或使用參數傳入）：
   - 用於登入Azure的SSO電子郵件地址
   - 解決這個StorageGRID 問題
   - 租戶帳戶ID（如果您要存取租戶管理API）
4. 出現提示時、請輸入密碼、並在需要時準備好提供MFA授權給Azure。

指令碼假設MFA是使用Microsoft驗證者完成。您可能需要修改指令碼、以支援其他形式的MFA （例如輸入在文字訊息中收到的程式碼）。

輸出中提供了驗證權杖。StorageGRID您現在可以將權杖用於其他要求、類似於未使用SSO時使用API的方式。

如果啟用單一登入、請使用**API**（**PingFedate**）

如果您有 "已設定並啟用單一登入（SSO）" 而且您使用PingFedate做為SSO供應商、必須發出一系列API要求、才能取得適用於Grid Management API或租戶管理API的驗證權杖。

如果啟用單一登入、請登入**API**

如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

開始之前

- 您知道屬於StorageGRID 某個位向使用者群組的聯盟使用者的SSO使用者名稱和密碼。
- 如果您想要存取租戶管理API、就知道租戶帳戶ID。

關於這項工作

若要取得驗證權杖、您可以使用下列其中一個範例：

- 。 `storagegrid-ssoauth.py` Python指令碼、位於StorageGRID 安裝檔案目錄中 (`./rpms` 對於 Red Hat Enterprise Linux 、 `./debs` 適用於Ubuntu或DEBIAN,以及 `./vsphere` （適用於VMware）。
- Curl要求的工作流程範例。

  如果執行速度太慢、捲曲工作流程可能會逾時。您可能會看到以下錯誤： `A valid SubjectConfirmation was not found on this Response`。

  範例Curl工作流程無法防止其他使用者看到密碼。

  如果您遇到 URL 編碼問題、可能會看到以下錯誤： `Unsupported SAML version`。

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python指令碼：前往步驟 2 。
   - 使用Curl要求。前往步驟3。
2. 如果您要使用 `storagegrid-ssoauth.py` 指令碼、將指令碼傳遞給Python解釋器、然後執行指令碼。

   出現提示時、請輸入下列引數的值：
   - SSO方法。您可以輸入「 pingfederate 」的任何變化（ PINGFEDESTATE 、 pingfederate 等）。
   - SSO使用者名稱
   - 安裝了鏡面的網域StorageGRID 。此欄位不適用於PingFedate。您可以將其保留空白或輸入任何值。

- 解決這個StorageGRID 問題
- 租戶帳戶ID（如果您要存取租戶管理API）。

```
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
```

輸出中提供了驗證權杖。StorageGRID您現在可以將權杖用於其他要求、類似於未使用SSO時使用API的方式。

3. 如果您要使用捲髮要求、請使用下列程序。

   a. 宣告登入所需的變數。

```
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做為 `TENANTACCOUNTID`。

   b. 若要接收已簽署的驗證URL、請向發出POST要求 `/api/v3/authorize-saml`，並從回應中移除其他Json編碼。

   此範例顯示TENANTACCOUNTID的簽署驗證URL的POST要求。結果會傳遞至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URL編碼的已簽署URL、但不包含其他JSON-encoding層。

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

c. 儲存 `SAMLRequest` 從回應中取得以供後續命令使用。

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

d. 匯出回應和Cookie、並回應回應回應：

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

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

e. 匯出「pf.adaperId」值、並回應回應回應：

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

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

f. 匯出「Ha」值（移除結尾斜槓/）、然後回應回應：

```
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. 傳送內含認證的Cookie：

```
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 `SAMLResponse` 從隱藏欄位：

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

j. 使用儲存的 `SAMLResponse`、打造StorageGRID 一個不一樣的`/api/saml-response` 要求產生StorageGRID 驗證權杖。

適用於 `RelayState`、如果您要登入Grid Management API、請使用租戶帳戶ID或使用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
```

回應包括驗證權杖。

```
{
    "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另存為 `MYTOKEN`。

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

您現在可以使用 `MYTOKEN` 對於其他要求、類似於不使用SSO時使用API的方式。

如果啟用單一登入、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或租戶管理API。 如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

關於這項工作

如果需要、您可以登出組織的單一登出頁面、登出 StorageGRID API 。或者、您也可以觸發StorageGRID 來自下列項目的單一登出（SLO）：需要有效StorageGRID 的SESO承載權杖。

步驟

1. 若要產生已簽署的登出要求、請將「 Cookie 」「 SSO=true 」傳給 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
```

會傳回登出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. 傳送要求至登出URL以觸發SLO並重新導向StorageGRID 至還原。

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

會傳回302回應。重新導向位置不適用於純API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. 刪除StorageGRID 不記名權杖。

刪除StorageGRID 此不含SSO的不含支援權杖的方式相同。如果未提供「 Cookie 」「 SSO = True 」、則使用者會登出 StorageGRID 而不會影響 SSO 狀態。

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

答 `204 No Content` 回應表示使用者現在已登出。

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

使用**API**停用功能

您可以使用Grid Management API來完全停用StorageGRID 作業系統中的某些功能。停用某項功能時、將無法指派權限給任何人、以執行與該功能相關的工作。

關於這項工作

停用的功能系統可讓您防止存取StorageGRID 某些功能。停用功能是防止擁有*根存取*權限的root使用者或屬於管理群組的使用者能夠使用該功能的唯一方法。

若要瞭解此功能的用途、請考慮下列案例：

公司*A*是一家服務供應商、*StorageGRID* 負責建立租戶帳戶、以租賃其所屬的一套系統的儲存容量。為了保護租戶物件的安全、*A*公司希望確保其員工在部署帳戶後、永遠無法存取任何租戶帳戶。

_公司A可以使用Grid Management API中的Deactivate Features系統來達成此目標。透過完全停用Grid Manager（UI和API）中的*變更租戶根密碼*功能、公司A可確保任何管理員使用者（包括root使用者和擁有*root access*權限的群組使用者）都無法變更任何租戶帳戶根使用者的密碼

步驟

1. 存取Grid Management API的Swagger文件。請參閱 "使用Grid Management API"。
2. 找出停用功能端點。
3. 若要停用某項功能、例如變更租戶根密碼、請將本文傳送至API、如下所示：

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

   申請完成時、變更租戶根密碼功能會停用。使用者介面中不再顯示 * 變更租戶根密碼 * 管理權限、嘗試變更租戶根密碼的任何 API 要求都會失敗、並顯示「 403 禁止」。

重新啟動停用的功能

根據預設、您可以使用Grid Management API重新啟動已停用的功能。不過、如果您想要防止停用的功能再次被重新啟動、您可以停用*啟用功能*功能本身。

> 無法重新啟用 * 作用功能 * 功能。如果您決定停用此功能、請注意、您將永遠喪失重新啟動任何其他停用功能的能力。您必須聯絡技術支援部門、才能恢復任何喪失的功能。

步驟

1. 存取Grid Management API的Swagger文件。
2. 找出停用功能端點。
3. 若要重新啟動所有功能、請將本文傳送至API、如下所示：

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

完成此要求後、所有功能（包括變更租戶根密碼功能）都會重新啟動。使用者介面現在會顯示*變更租戶根密碼*管理權限、如果使用者擁有*根存取*或*變更租戶根密碼*管理權限、則任何嘗試變更租戶根密碼的API要求都會成功。

> 上一個範例會重新啟動_all_停用的功能。如果停用其他應保持停用狀態的功能、您必須在PUT要求中明確指定這些功能。例如、若要重新啟動變更租戶根密碼功能並繼續停用警示認可功能、請傳送此PUT要求：
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

控制StorageGRID 對功能的存取

控制 StorageGRID 存取：總覽

您可以透過StorageGRID 建立或匯入群組和使用者、並指派權限給每個群組、來控制哪些人可以存取功能、以及使用者可以執行哪些工作。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

您可以透過從身分識別聯盟服務匯入群組和使用者、或設定本機群組和本機使用者、來判斷誰可以存取Grid Manager和Grid Management API。

使用 "身分識別聯盟" 進行設定 "群組" 和 "使用者" 更快、而且使用者可以使用熟悉的認證登入 StorageGRID 。如果您使用Active Directory、OpenLDAP或Oracle Directory Server、則可以設定身分識別聯盟。

> 如果您想要使用另一項LDAP v3服務、請聯絡技術支援部門。

您可以指派不同的工作來決定每個使用者可以執行哪些工作 "權限" 給每個群組。例如、您可能希望某個群組中的使用者能夠管理ILM規則、以及其他群組中的使用者執行維護工作。使用者必須屬於至少一個群組才能存取系統。

您也可以將群組設定為唯讀。唯讀群組中的使用者只能檢視設定和功能。他們無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何作業。

啟用單一登入

支援使用安全聲明標記語言2.0（SAML 2.0）標準的單一登入（SSO）StorageGRID 。您先請 "設定並啟用SSO"、所有使用者必須先由外部身分識別供應商驗證、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 。

變更資源配置複雜密碼

許多安裝與維護程序、以及下載StorageGRID 「還原套件」時、都需要使用資源配置密碼。也需要通關密碼才能下載適用於StorageGRID 整個系統的網格拓撲資訊和加密金鑰備份。您可以 "變更複雜密碼" 視需要而定。

變更節點主控台密碼

網格中的每個節點都有唯一的節點主控台密碼、您必須以「 admin 」的身分使用 SSH 登入節點、或是以 VM/實體主控台連線的根使用者登入。如有需要、您可以 "變更節點主控台密碼" 針對每個節點。

變更資源配置通關密碼

請使用此程序來變更StorageGRID 供應密碼。恢復、擴充和維護程序需要通關密碼。下載「恢復套件」備份時、也需要密碼、其中包括網格拓撲資訊、網格節點主控台密碼、StorageGRID 以及適用於該系統的加密金鑰。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您具有「維護」或「根」存取權限。
- 您有目前的資源配置通關密碼。

關於這項工作

許多安裝和維護程序以及的都需要資源配置通關密碼 "正在下載恢復套件"。中未列出資源配置通關密碼 `Passwords.txt` 檔案：請務必記錄資源配置通關密碼、並將密碼保存在安全的位置。

步驟

1. 選擇*組態*>*存取控制*網格密碼。
2. 在 * 變更資源配置密碼 * 下、選取 * 進行變更 *
3. 輸入您目前的資源配置通關密碼。
4. 輸入新的通關密碼。通關密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。
5. 將新的資源配置通關密碼儲存在安全的位置。安裝、擴充和維護程序都必須如此。
6. 重新輸入新的通關密碼、然後選取*「Save*（儲存*）」。

   資源配置通關密碼變更完成時、系統會顯示綠色的成功標語。

7. 選擇*恢復套件*。
8. 輸入新的資源配置密碼以下載新的恢復套件。

   變更資源配置通關密碼之後、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。

變更節點主控台密碼

網格中的每個節點都有唯一的節點主控台密碼、您必須登入節點。請使用這些步驟來變更網格中每個節點的每個唯一節點主控台密碼。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "維護或根存取權限"。
- 您有目前的資源配置通關密碼。

關於這項工作

使用節點主控台密碼、以「 admin 」身分使用 SSH 登入節點、或以 VM/ 實體主控台連線的 root 使用者身分登入。變更節點主控台密碼程序會為網格中的每個節點建立新密碼、並將密碼儲存在更新的中 `Passwords.txt` 恢復套件中的檔案。密碼會列在Passwords.txt檔案的「Password（密碼）」欄中。

SSH金鑰有個別的SSH存取密碼、用於節點之間的通訊。此程序不會變更 SSH 存取密碼。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*網格密碼*。
2. 在 * 變更節點主控台密碼 * 下、選取 * 進行變更 * 。

輸入資源配置通關密碼

步驟

1. 輸入您網格的資源配置密碼。
2. 選擇*繼續*。

下載目前的恢復套件

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. 選擇*下載恢復套件*。
2. 複製恢復套件檔案 (`.zip`）到兩個安全、安全且獨立的位置。

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。

3. 選擇*繼續*。
4. 當確認對話方塊出現時、如果您已準備好開始變更節點主控台密碼、請選取 * 是 * 。

   您無法在程序啟動後取消此程序。

變更節點主控台密碼

當節點主控台密碼程序啟動時、會產生新的還原套件、其中包含新密碼。然後、每個節點上的密碼都會更新。

步驟

1. 等待產生新的恢復套件、這可能需要幾分鐘的時間。
2. 選擇*下載新的恢復套件*。
3. 下載完成時：

   a. 開啟 `.zip` 檔案：

   b. 確認您可以存取內容、包括 `Passwords.txt` 檔案、其中包含新節點主控台密碼。

   c. 複製新的恢復套件檔案 (`.zip`）到兩個安全、安全且獨立的位置。

   請勿覆寫舊的恢復套件。

   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. 選取核取方塊、表示您已下載新的恢復套件並驗證內容。
5. 選取 * 變更節點主控台密碼 * 、並等待所有節點以新密碼更新。這可能需要幾分鐘的時間。

   如果變更所有節點的密碼、會出現綠色的成功橫幅。前往下一步。

   如果在更新程序期間發生錯誤、則會出現橫幅訊息、列出無法變更密碼的節點數量。系統會在任何無法變更密碼的節點上、自動重試此程序。如果程序結束時、部分節點仍未變更密碼、則會出現*重試*按鈕。

   如果一或多個節點的密碼更新失敗：

   a. 檢閱表中所列的錯誤訊息。

   b. 解決問題。

   c. 選擇*重試*。

   重試只會變更先前密碼變更嘗試期間失敗之節點上的節點主控台密碼。

6. 變更所有節點的節點主控台密碼後、請刪除 您下載的第一個恢復套件。
7. 您也可以選擇使用 * 恢復套件 * 連結來下載新恢復套件的其他複本。

使用身分識別聯盟

使用身分識別聯盟可更快設定群組和使用者、並讓使用者StorageGRID 使用熟悉的認證登入到這個功能。

設定**Grid Manager**的身分識別聯盟

如果您想要在其他系統（例如Active Directory、Azure Active Directory（Azure AD）、OpenLDAP或Oracle Directory Server）中管理系統管理群組和使用者、可以在Grid Manager中設定身分識別聯盟。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您使用Active Directory、Azure AD、OpenLDAP或Oracle Directory Server做為身分識別供應商。

  如果您想使用未列出的LDAP v3服務、請聯絡技術支援部門。

- 如果您打算使用OpenLDAP、則必須設定OpenLDAP伺服器。請參閱 設定OpenLDAP伺服器的準則。
- 如果您打算啟用單一登入（SSO）、則已檢閱 "單一登入的要求與考量"。
- 如果您打算使用傳輸層安全性（TLS）與LDAP伺服器進行通訊、則身分識別供應商使用的是TLS 1.2或1.3。請參閱 "用於傳出TLS連線的支援密碼"。

關於這項工作

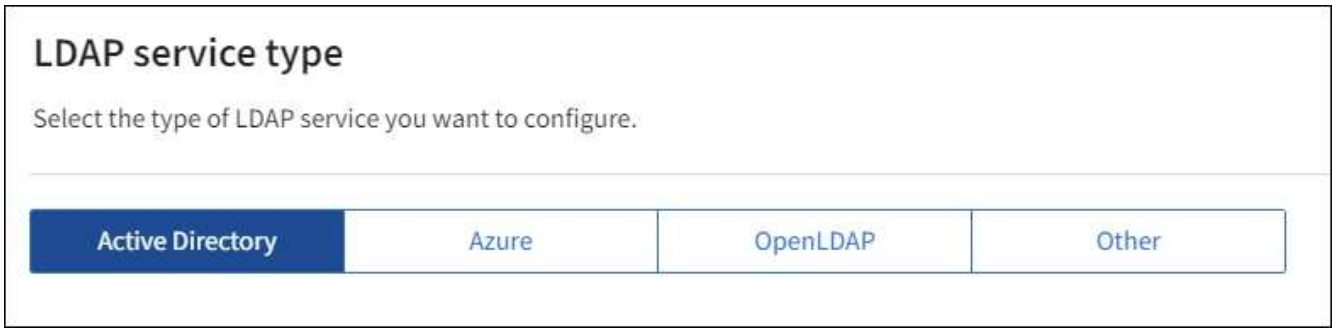
如果您想從其他系統（例如Active Directory、Azure AD、OpenLDAP或Oracle Directory Server）匯入群組、可以設定Grid Manager的身分識別來源。您可以匯入下列群組類型：

- 管理群組：管理群組中的使用者可以登入Grid Manager、並根據指派給群組的管理權限來執行工作。
- 不使用其本身身分識別來源的租戶使用者群組。租戶群組中的使用者可以登入租戶管理程式、並根據在租戶管理程式中指派給群組的權限來執行工作。請參閱 "建立租戶帳戶" 和 "使用租戶帳戶" 以取得詳細資料。

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服務類型區段中、選取您要設定的LDAP服務類型。



   選擇*其他*以設定使用Oracle Directory Server的LDAP伺服器值。

4. 如果選擇*其他*、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：含有LDAP使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName` 適用於Active Directory和 `uid` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `uid`。
   - *使用者UUID *：含有LDAP使用者永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定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、連字號會被忽略。

- 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 `sAMAccountName` 適用於Active Directory和 `cn` 適用於OpenLDAP。如果您要設定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。此屬性相當於 `objectGUID` 適用於Active Directory和 `entryUUID` 適用於OpenLDAP。如果您要設定Oracle Directory Server、請輸入 `nsuniqueid`。指定屬性的每個群組值必須是16位元組或字串格式的32位數十六進位數字、連字號會被忽略。

5. 對於所有LDAP服務類型、請在「設定LDAP伺服器」區段中輸入所需的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LDAP伺服器的連接埠。

     STARTTLS的預設連接埠為389、LDAPS的預設連接埠為636。不過、只要防火牆設定正確、您就可以使用任何連接埠。

   - 使用者名稱：將連線至LDAP伺服器之使用者的辨別名稱（DN）完整路徑。

     對於Active Directory、您也可以指定低層級的登入名稱或使用者主要名稱。

     指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

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

   - 密碼：與使用者名稱相關的密碼。

     如果您在未來變更密碼、您必須在此頁面上更新密碼。

   - 群組基礎**DN**：您要搜尋群組之LDAP子樹狀結構的辨別名稱（DN）完整路徑。在Active Directory範例（如下）中、識別名稱相對於基礎DN（DC=storagegRID、DC=example、DC=com）的所有群組均可做為聯盟群組使用。

     「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

   - 使用者基礎**DN**：您要搜尋使用者之LDAP子樹狀目錄的辨別名稱（DN）完整路徑。

     *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

   - * 連結使用者名稱格式 *（選用）：如果無法自動判斷模式、則應使用預設的使用者名稱模式StorageGRID 。

     建議提供*連結使用者名稱格式*、因為StorageGRID 如果無法連結服務帳戶、使用者可以登入。

輸入下列其中一種模式：

- * UserPrincipalName 模式（ Active Directory 和 Azure ） * ： `[USERNAME]@example.com`
- * 低階登入名稱模式（ Active Directory 和 Azure ） * ： `example\[USERNAME]`
- * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,DC=com`

請準確附上所寫的*（使用者名稱）*。

6. 在傳輸層安全性（TLS）區段中、選取安全性設定。
   - 使用**ARTTLS**：使用ARTTLS來保護與LDAP伺服器的通訊安全。這是Active Directory、OpenLDAP或其他的建議選項、但Azure不支援此選項。
   - 使用**LDAPS**：LDAPS（LDAP over SSL）選項使用TLS建立與LDAP伺服器的連線。您必須為Azure選取此選項。
   - 請勿使用**TLS**：StorageGRID 不保護介於整個系統與LDAP伺服器之間的網路流量。Azure不支援此選項。

   > ⓘ 如果Active Directory伺服器強制執行LDAP簽署、則不支援使用*「不使用TLS*」選項。您必須使用ARTTLS或LDAPS。

7. 如果您選取了ARTTLS或LDAPS、請選擇用來保護連線安全的憑證。
   - 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。
   - 使用自訂**CA**憑證：使用自訂安全性憑證。

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

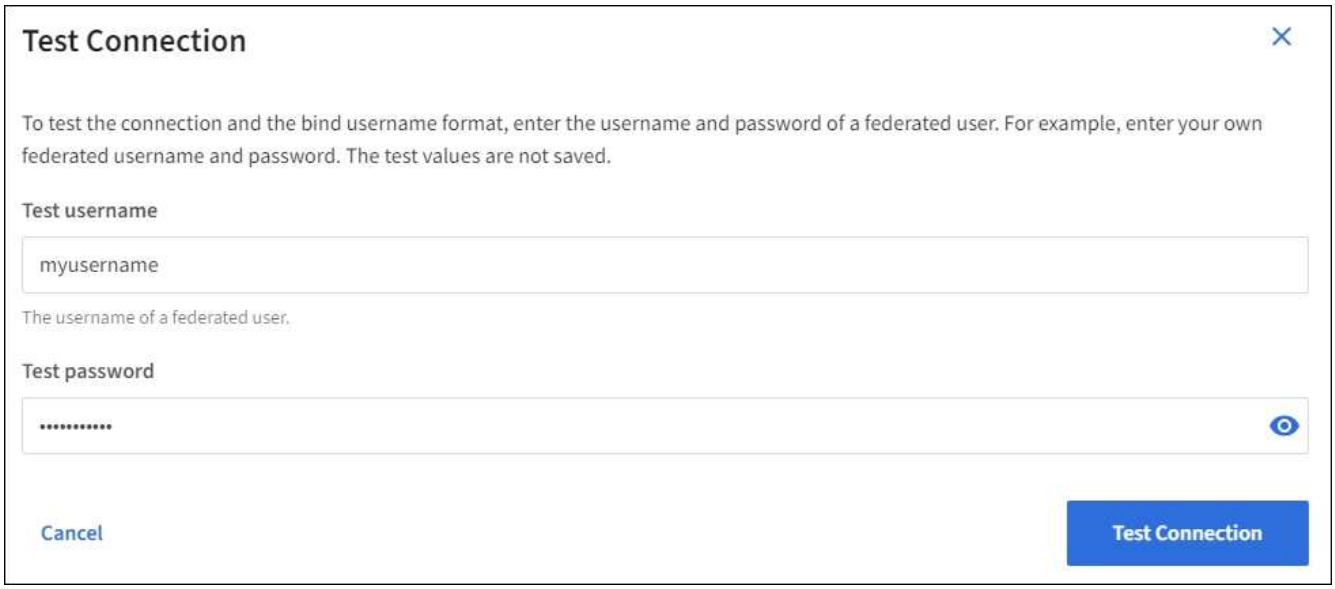
測試連線並儲存組態

輸入所有值之後、您必須先測試連線、才能儲存組態。如果您提供LDAP伺服器的連線設定和連結使用者名稱格式、則可透過此驗證。StorageGRID

步驟

1. 選擇*測試連線*。
2. 如果您未提供連結使用者名稱格式：
   - 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定無效、就會出現「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. 如果您提供連結使用者名稱格式、請輸入有效同盟使用者的使用者名稱和密碼。

   例如、輸入您自己的使用者名稱和密碼。請勿在使用者名稱中包含任何特殊字元、例如 @ 或 / 。



- 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（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、則會出現錯誤訊息。解決所有問題、然後再次測試連線。

強制與身分識別來源同步

此系統會定期同步來自身分識別來源的聯盟群組和使用者。StorageGRID如果您想要盡快啟用或限制使用者權限、可以強制啟動同步。

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

   如果同步處理來自身分識別來源的聯盟群組和使用者時發生問題、則會觸發*身分識別聯盟同步處理失敗*警示。

停用身分識別聯盟

您可以暫時或永久停用群組和使用者的身分識別聯盟。停用身分識別聯盟時StorageGRID 、不會在驗證和身分識別來源之間進行通訊。不過、您已設定的任何設定都會保留下來、讓您日後可以輕鬆重新啟用身分識別聯盟。

關於這項工作

在停用身分識別聯盟之前、您應注意下列事項：

- 聯盟使用者將無法登入。
- 目前已登入的聯盟使用者將在StorageGRID 其工作階段過期之前保留對此系統的存取權、但在工作階段過期後仍無法登入。
- 不會在不同步系統與身分識別來源之間進行同步、StorageGRID 也不會針對尚未同步的帳戶發出警示或警示。

- 如果將單點登錄 (SSO) 設置爲 **Enabled** 或 **Sandbox Mode** ，則禁用 **Enable identity Federation** （啓用身份聯合） * 複選框。「單一登入」頁面的**SSO**狀態必須為*停用、才能停用身分識別聯盟。請參閱 "停用單一登入"。

步驟

1. 前往「身分識別聯盟」頁面。
2. 取消勾選 * 啟用身分識別聯盟 * 核取方塊。

設定**OpenLDAP**伺服器的準則

如果您要使用OpenLDAP伺服器進行身分識別聯盟、則必須在OpenLDAP伺服器上設定特定設定。

> 對於非 ActiveDirectory 或 Azure 的身分識別來源、 StorageGRID 不會自動封鎖 S3 對外部停用使用者的存取。若要封鎖 S3 存取、請刪除使用者的任何 S3 金鑰、或將使用者從所有群組中移除。

memberOf和**refert**覆疊

應啟用memberof和refert覆疊。如需詳細資訊、請參閱中的反轉群組成員資格維護指示 "OpenLDAP文件：2.4版管理員指南"。

索引

您必須使用指定的索引關鍵字來設定下列OpenLDAP屬性：

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

此外、請確定使用者名稱說明中所述的欄位已建立索引、以獲得最佳效能。

請參閱中有關反轉群組成員資格維護的資訊 "OpenLDAP文件：2.4版管理員指南"。

管理管理群組

您可以建立管理群組、以管理一或多個管理使用者的安全性權限。使用者必須屬於某個群組、才能獲得StorageGRID 存取該系統的權限。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 如果您打算匯入聯盟群組、表示您已設定身分識別聯盟、而且聯盟群組已存在於設定的身分識別來源中。

建立管理群組

管理群組可讓您決定哪些使用者可以存取Grid Manager和Grid Management API中的哪些功能和作業。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*管理群組*。
2. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

- 如果您要指派權限給本機使用者、請建立本機群組。
- 建立聯盟群組、從身分識別來源匯入使用者。

本機群組

步驟

1. 選擇*本機群組*。
2. 輸入群組的顯示名稱、您可視需要稍後更新。例如「維護使用者」或「 ILM 管理員」。
3. 輸入群組的唯一名稱、您稍後無法更新。
4. 選擇*繼續*。

聯盟群組

步驟

1. 選取*聯盟群組*。
2. 輸入您要匯入的群組名稱、完全如同在設定的身分識別來源中所顯示的名稱。
   - 對於Active Directory和Azure、請使用sAMAccountName。
   - 若為OpenLDAP、請使用「CN"（通用名稱）」。
   - 對於另一個LDAP、請為LDAP伺服器使用適當的唯一名稱。
3. 選擇*繼續*。

管理群組權限

步驟

1. 若為*存取模式*、請選取群組中的使用者是否可以在Grid Manager和Grid Management API中變更設定及執行作業、或是只能檢視設定和功能。
   - 讀寫（預設）：使用者可以變更設定、並執行其管理權限所允許的作業。
   - 唯讀：使用者只能檢視設定和功能。他們無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何作業。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、且任何群組設定為*唯讀*、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 選取一或多個 "管理群組權限"。

您必須為每個群組指派至少一項權限、否則屬於該群組的使用者將無法登入StorageGRID 。

3. 如果您要建立本機群組、請選取*繼續*。如果您要建立聯盟群組、請選取*建立群組*和*完成*。

新增使用者（僅限本機群組）

步驟

1. 您也可以為此群組選取一或多個本機使用者。

   如果您尚未建立本機使用者、可以儲存群組而不新增使用者。您可以將此群組新增至「使用者」頁面上的使用者。請參閱 "管理使用者" 以取得詳細資料。

2. 選擇* Create group（創建組）和 Finish（完成）*。

檢視及編輯管理群組

您可以檢視現有群組的詳細資料、修改群組或複製群組。

- 若要檢視所有群組的基本資訊、請檢閱「群組」頁面上的表格。
- 若要檢視特定群組的所有詳細資料或編輯群組、請使用*「動作」*功能表或「詳細資料」頁面。

工作	「行動」功能表	詳細資料頁面
檢視群組詳細資料	a. 選取群組的核取方塊。 b. 選取*「動作*」>*「檢視群組詳細資料*」。	在表格中選取群組名稱。
編輯顯示名稱（僅限本機群組）	a. 選取群組的核取方塊。 b. 選擇*操作*>*編輯群組名稱*。 c. 輸入新名稱。 d. 選取*儲存變更*。	a. 選取群組名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選取*儲存變更*。
編輯存取模式或權限	a. 選取群組的核取方塊。 b. 選取*「動作*」>*「檢視群組詳細資料*」。 c. 或者、變更群組的存取模式。 d. 或者、選取或清除 "管理群組權限"。 e. 選取*儲存變更*。	a. 選取群組名稱以顯示詳細資料。 b. 或者、變更群組的存取模式。 c. 或者、選取或清除 "管理群組權限"。 d. 選取*儲存變更*。

複製群組

步驟

1. 選取群組的核取方塊。
2. 選取*「動作*」>*「重複群組*」。

3. 完成「複製群組」精靈。

刪除群組

當您想要從系統中移除群組時、可以刪除管理群組、並移除與群組相關的所有權限。刪除管理群組會移除群組中的任何使用者、但不會刪除使用者。

步驟

1. 在「群組」頁面中、選取您要移除的每個群組的核取方塊。
2. 選擇*操作*>*刪除群組*。
3. 選擇*刪除群組*。

管理群組權限

建立管理使用者群組時、您可以選取一或多個權限來控制對Grid Manager特定功能的存取。然後、您可以將每個使用者指派給一或多個這些管理群組、以決定使用者可以執行哪些工作。

您必須為每個群組指派至少一項權限、否則屬於該群組的使用者將無法登入Grid Manager或Grid Management API。

根據預設、任何屬於至少擁有一項權限之群組的使用者、都可以執行下列工作：

- 登入Grid Manager
- 檢視儀表板
- 檢視節點頁面
- 監控網格拓撲
- 檢視目前和已解決的警示
- 檢視目前和歷史警報（舊系統）
- 變更自己的密碼（僅限本機使用者）
- 檢視「組態與維護」頁面上提供的特定資訊

權限與存取模式之間的互動

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及執行作業、或是只能檢視相關的設定與功能。如果使用者屬於多個群組、且任何群組設定為*唯讀*、則使用者將擁有所有選取設定和功能的唯讀存取權。

下列各節將說明您在建立或編輯管理群組時可以指派的權限。任何未明確提及的功能都需要*根存取*權限。

root存取權

此權限可讓您存取所有網格管理功能。

認可警示（舊版）

此權限可讓您存取「Acknowledge and回應警示（舊系統）」。所有登入的使用者都可以檢視目前和歷史警報。

如果您希望使用者僅監控網格拓撲並認可警示、則應指派此權限。

變更租戶根密碼

此權限可讓您存取「租戶」頁面上的*變更root密碼*選項、讓您控制誰可以變更租戶本機root使用者的密碼。啟用S3金鑰匯入功能時、此權限也可用於移轉S3金鑰。沒有此權限的使用者無法看到 * 變更 root 密碼 * 選項。

若要授予「租戶」頁面的存取權（包含*變更root密碼*選項）、請同時指派*租戶帳戶*權限。

網格拓撲頁面組態

此權限可讓您存取「支援>*工具*>*網格拓撲*」頁面上的「組態」索引標籤。

ILM

此權限可讓您存取下列* ILM *功能表選項：

- 規則
- 原則
- 銷毀編碼
- 區域
- 儲存資源池

使用者必須擁有*其他網格組態*和*網格拓撲頁面組態*權限、才能管理儲存等級。

維護

使用者必須擁有維護權限、才能使用下列選項：

- 組態>*存取控制*：
  - 網格密碼
- 組態>*網路*：
  - S3 端點網域名稱
- 維護>*工作*：
  - 取消委任
  - 擴充
  - 物件存在檢查
  - 恢復
- 維護>*系統*：
  - 恢復套件

- 軟體更新
- 支援>*工具*：
  - 記錄

沒有維護權限的使用者可以檢視但無法編輯這些頁面：

- 維護>*網路*：
  - DNS伺服器
  - 網格網路
  - NTP 伺服器
- 維護>*系統*：
  - 授權
- 組態>*網路*：
  - S3 端點網域名稱
- 組態>*安全性*：
  - 憑證
- 組態>*監控*：
  - 稽核與syslog伺服器

管理警示

此權限可讓您存取管理警示的選項。使用者必須擁有此權限、才能管理靜音、警示通知及警示規則。

度量查詢

此權限可讓您存取：

- * 支援 * > * 工具 * > * 指標 * 頁面
- 使用 Grid Management API 的 * Metrics * 區段來自訂 Prometheus 指標查詢
- 包含計量的 Grid Manager 儀表板卡

物件中繼資料查詢

此權限可讓您存取「* ILM >*物件中繼資料查詢」頁面。

其他網格組態

此權限可讓您存取其他網格組態選項。

若要查看這些額外選項、使用者也必須具有* Grid拓撲頁面組態*權限。

- * ILM *：
  - 儲存等級

- 組態>*系統*：
  - 儲存選項
- 支援>*警示（舊版）*：
  - 自訂事件
  - 全域警示
  - 舊版電子郵件設定
- * 支援 * > * 其他 * ：
  - 連結成本

儲存應用裝置管理員

此權限提供：

- 透過 Grid Manager 存取儲存設備上的 E 系列 SANtricity 系統管理員。
- 可在支援這些作業的應用裝置的「管理磁碟機」索引標籤上執行疑難排解和維護工作。

租戶帳戶

此權限可讓您：

- 存取租戶頁面、您可以在其中建立、編輯及移除租戶帳戶
- 檢視現有的流量分類原則
- 檢視包含租戶詳細資料的 Grid Manager 儀表板卡

管理使用者

您可以檢視本機和聯盟使用者。您也可以建立本機使用者、並將其指派給本機管理群組、以決定這些使用者可以存取哪些Grid Manager功能。

開始之前

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

建立本機使用者

您可以建立一或多個本機使用者、並將每個使用者指派給一或多個本機群組。群組的權限可控制使用者可以存取的Grid Manager和Grid Management API功能。

您只能建立本機使用者。使用外部身分識別來源來管理同盟使用者和群組。

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。

如果啟用單一登入（ SSO ）、本機使用者將無法登入 StorageGRID 。

存取精靈

步驟

1. 選擇*組態*>*存取控制*>*管理使用者*。
2. 選取*建立使用者*。

輸入使用者認證資料

步驟

1. 輸入使用者的全名、唯一使用者名稱及密碼。
2. 或者、如果此使用者不應存取Grid Manager或Grid Management API、請選取* Yes*。
3. 選擇*繼續*。

指派給群組

步驟

1. 或者、將使用者指派給一或多個群組、以決定使用者的權限。

   如果您尚未建立群組、可以儲存使用者而不選取群組。您可以將此使用者新增至「群組」頁面上的群組。

   如果使用者屬於多個群組、則權限會累計。請參閱 "管理管理群組" 以取得詳細資料。

2. 選擇* Create user*（創建用戶*）並選擇* Finish（完成）*。

檢視及編輯本機使用者

您可以檢視現有本機和聯盟使用者的詳細資料。您可以修改本機使用者、以變更使用者的完整名稱、密碼或群組成員資格。您也可以暫時禁止使用者存取Grid Manager和Grid Management API。

您只能編輯本機使用者。使用外部身分識別來源來管理同盟使用者。

- 若要檢視所有本機和聯盟使用者的基本資訊、請檢閱「使用者」頁面上的表格。
- 若要檢視特定使用者的所有詳細資料、編輯本機使用者、或變更本機使用者的密碼、請使用* Actions（動作）*功能表或詳細資料頁面。

  使用者下次登出並重新登入Grid Manager時、即會套用任何編輯內容。

  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。

工作	「行動」功能表	詳細資料頁面
檢視使用者詳細資料	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料	在表格中選取使用者名稱。

工作	「行動」功能表	詳細資料頁面
編輯全名（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇* Actions > Edit full name*（操作>*編輯全名*）。 c. 輸入新名稱。 d. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選取*儲存變更*。
拒絕StorageGRID或允許存取	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取「存取」索引標籤。 d. 選取*是*以防止使用者登入Grid Manager或Grid Management API、或選取*否*以允許使用者登入。 e. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取「存取」索引標籤。 c. 選取*是*以防止使用者登入Grid Manager或Grid Management API、或選取*否*以允許使用者登入。 d. 選取*儲存變更*。
變更密碼（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取密碼索引標籤。 d. 輸入新密碼。 e. 選擇*變更密碼*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取密碼索引標籤。 c. 輸入新密碼。 d. 選擇*變更密碼*。
變更群組（僅限本機使用者）	a. 選取使用者的核取方塊。 b. 選擇*「Actions」（動作）>「View user details」（檢視使用者詳細資料 c. 選取群組索引標籤。 d. 或者、選取群組名稱後的連結、即可在新的瀏覽器索引標籤中檢視群組的詳細資料。 e. 選取*編輯群組*以選取不同的群組。 f. 選取*儲存變更*。	a. 選取使用者名稱以顯示詳細資料。 b. 選取群組索引標籤。 c. 或者、選取群組名稱後的連結、即可在新的瀏覽器索引標籤中檢視群組的詳細資料。 d. 選取*編輯群組*以選取不同的群組。 e. 選取*儲存變更*。

複製使用者

您可以複製現有使用者、以建立具有相同權限的新使用者。

步驟

1. 選取使用者的核取方塊。

2. 選取*「動作*」>*「重複使用者*」。
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、將該使用者從系統中永久移除。

您無法刪除 root 使用者。

步驟

1. 在「使用者」頁面中、選取您要移除的每位使用者的核取方塊。
2. 選取*「動作*」>*「刪除使用者*」。
3. 選擇*刪除使用者*。

使用單一登入（**SSO**）

設定單一登入

啟用單一登入（SSO）時、如果使用者的認證是使用組織實作的SSO登入程序來授權、則只能存取Grid Manager、租戶管理程式、Grid Management API或租戶管理API。本機使用者無法登入 StorageGRID 。

單一登入的運作方式

支援使用安全聲明標記語言2.0（SAML 2.0）標準的單一登入（SSO）StorageGRID 。

在啟用單一登入（SSO）之前、請先檢閱StorageGRID 啟用SSO時、哪些地方會影響到「資訊登入」和「登出」程序。

啟用**SSO**時登入

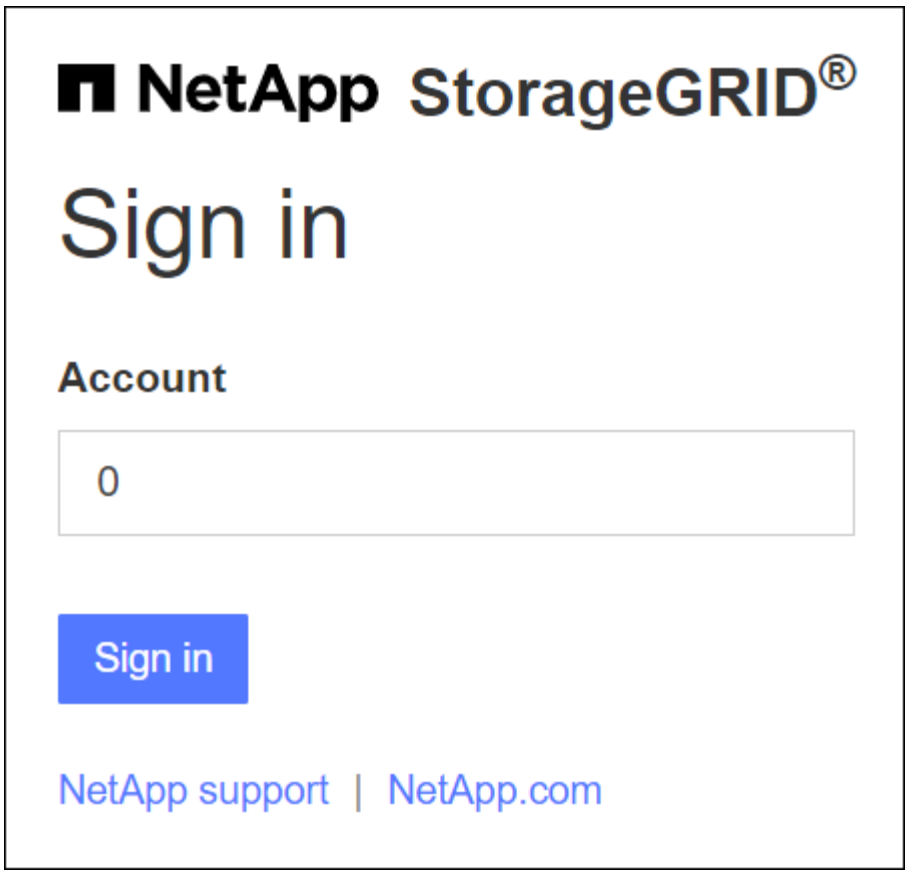
啟用SSO並登入StorageGRID 支援功能時、系統會將您重新導向至組織的SSO頁面、以驗證您的認證資料。

步驟

1. 在StorageGRID 網頁瀏覽器中輸入任何「靜態管理節點」的完整網域名稱或IP位址。

   畫面上會出現「簽署」頁面。StorageGRID

   - 如果這是您第一次存取此瀏覽器上的URL、系統會提示您輸入帳戶ID：

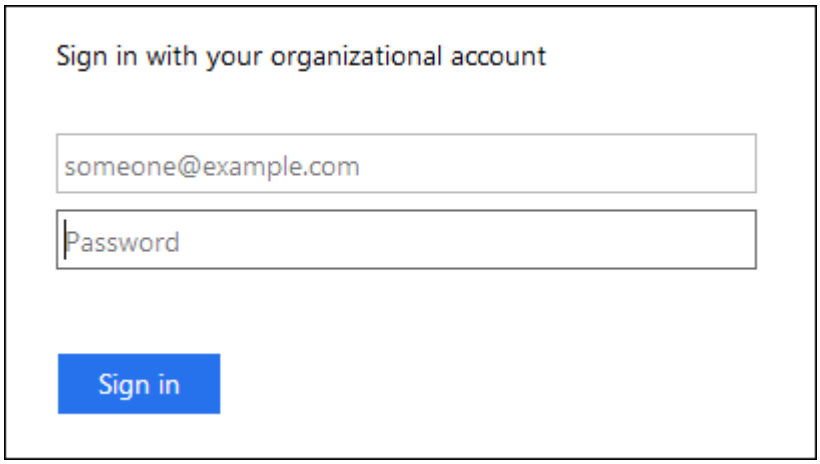


。如果您先前曾存取Grid Manager或Tenant Manager、系統會提示您選擇最近的帳戶或輸入帳戶ID：

輸入租戶帳戶的完整URL（即完整網域名稱或IP位址之後）時、不會顯示「協助登入」頁面StorageGRID `/?accountId=20-digit-account-id`）。而是會立即重新導向至組織的SSO登入頁面、您可以在其中登入 使用SSO認證登入。

2. 指出您要存取Grid Manager或租戶管理程式：
   - 若要存取Grid Manager、請將*帳戶ID*欄位保留空白、輸入* 0*作為帳戶ID、或選取* Grid Manager*（若出現在最近的帳戶清單中）。
   - 若要存取租戶管理程式、請輸入20位數的租戶帳戶ID、或是在最近的帳戶清單中、依名稱選取租戶。
3. 選擇*登入*

   可將您重新導向至組織的SSO登入頁面。StorageGRID例如：



4. [[signin_SSO]使用您的SSO認證登入。

   如果SSO認證資料正確：

   a. 身分識別供應商（IDP）提供驗證回應StorageGRID 功能以回應功能。
   b. 驗證驗證回應。StorageGRID
   c. 如果回應有效、且您屬於具有StorageGRID 下列存取權限的聯盟群組、您將會登入Grid Manager或租戶管理程式、視您選取的帳戶而定。

      如果無法存取服務帳戶、您仍可登入、只要您是擁有StorageGRID 存取權限之聯盟群組的現有使用者。

5. 您也可以存取其他管理節點、或是存取Grid Manager或租戶管理程式（如果您有足夠的權限）。

   您不需要重新輸入 SSO 認證。

啟用**SSO**時登出

啟用SSO以StorageGRID 利執行功能時、登出時會發生什麼事取決於您登入的項目、以及登出的位置。

步驟

1. 在使用者介面右上角找到 * 登出 * 連結。
2. 選取 * 登出 * 。

   畫面上會出現「簽署」頁面。StorageGRID「最近的帳戶」下拉式清單會更新為包含* Grid Manager*或租戶名稱、以便日後更快存取這些使用者介面。

如果您已登入...	您也可以登出...	您已登出...
一個或多個管理節點上的Grid Manager	任何管理節點上的Grid Manager	所有管理節點上的Grid Manager *附註：*如果您使用Azure進行SSO、可能需要幾分鐘的時間才能登出所有管理節點。
一或多個管理節點上的租戶管理程式	任何管理節點上的租戶管理程式	所有管理節點上的租戶管理程式
Grid Manager與租戶管理程式	網格管理程式	僅限Grid Manager。您也必須登出租戶管理程式、才能登出SSO。

下表摘要說明當您使用單一瀏覽器工作階段登出時會發生的情況。如果您在StorageGRID 多個瀏覽器工作階段之間登入到Sof、則必須分別登出所有瀏覽器工作階段。

單一登入的要求與考量

為 StorageGRID 系統啟用單一登入（ SSO ）之前、請先檢閱需求和考量事項。

身分識別供應商要求

支援下列SSO身分識別供應商（IDP）StorageGRID ：

- Active Directory Federation Service（AD FS）
- Azure Active Directory（Azure AD）
- PingFedate

您必須先為StorageGRID 您的支援系統設定身分識別聯盟、才能設定SSO身分識別供應商。您用於身分識別聯盟的LDAP服務類型會控制您可以實作的SSO類型。

已設定的**LDAP**服務類型	**SSO**身分識別供應商選項
Active Directory	• Active Directory • Azure • PingFedate
Azure	Azure

AD FS需求

您可以使用下列任何版本的AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS

- Windows Server 2016 AD FS

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

其他需求

- 傳輸層安全性（TLS）1.2或1.3
- Microsoft .NET Framework版本3.5.1或更新版本

Azure 的考量

如果您使用 Azure 做為 SSO 類型、且使用者的使用者主體名稱不使用 sAMAccountName 做為首碼、則當 StorageGRID 失去與 LDAP 伺服器的連線時、可能會發生登入問題。若要允許使用者登入、您必須還原與 LDAP 伺服器的連線。

伺服器憑證需求

根據預設、StorageGRID 在每個管理節點上使用管理介面憑證、以安全存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。當您設定依賴方信任（AD FS）、企業應用程式（Azure）或服務供應商連線（PingFedate）以供StorageGRID 進行時、您可以使用伺服器憑證做為StorageGRID 簽署憑證來執行Sfor Suse要求。

如果您還沒有 "已為管理介面設定自訂憑證"您現在應該這麼做。當您安裝自訂伺服器憑證時、它會用於所有管理節點、您可以在StorageGRID 所有依賴方信任、企業應用程式或SP連線中使用。

> 不建議在依賴方信任、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、而您要將其恢復、則會產生新的預設伺服器憑證。在登入還原的節點之前、您必須使用新的憑證來更新依賴方信任、企業應用程式或SP連線。

您可以登入節點的命令Shell並前往、以存取管理節點的伺服器憑證 `/var/local/mgmt-api` 目錄。自訂伺服器憑證即會命名 `custom-server.crt`。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）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。請參閱 "控制外部防火牆的存取"。

確認同盟使用者可以登入

啟用單一登入（SSO）之前、您必須確認至少有一位同盟使用者可以登入Grid Manager、並登入任何現有租戶帳戶的租戶管理程式。

開始之前

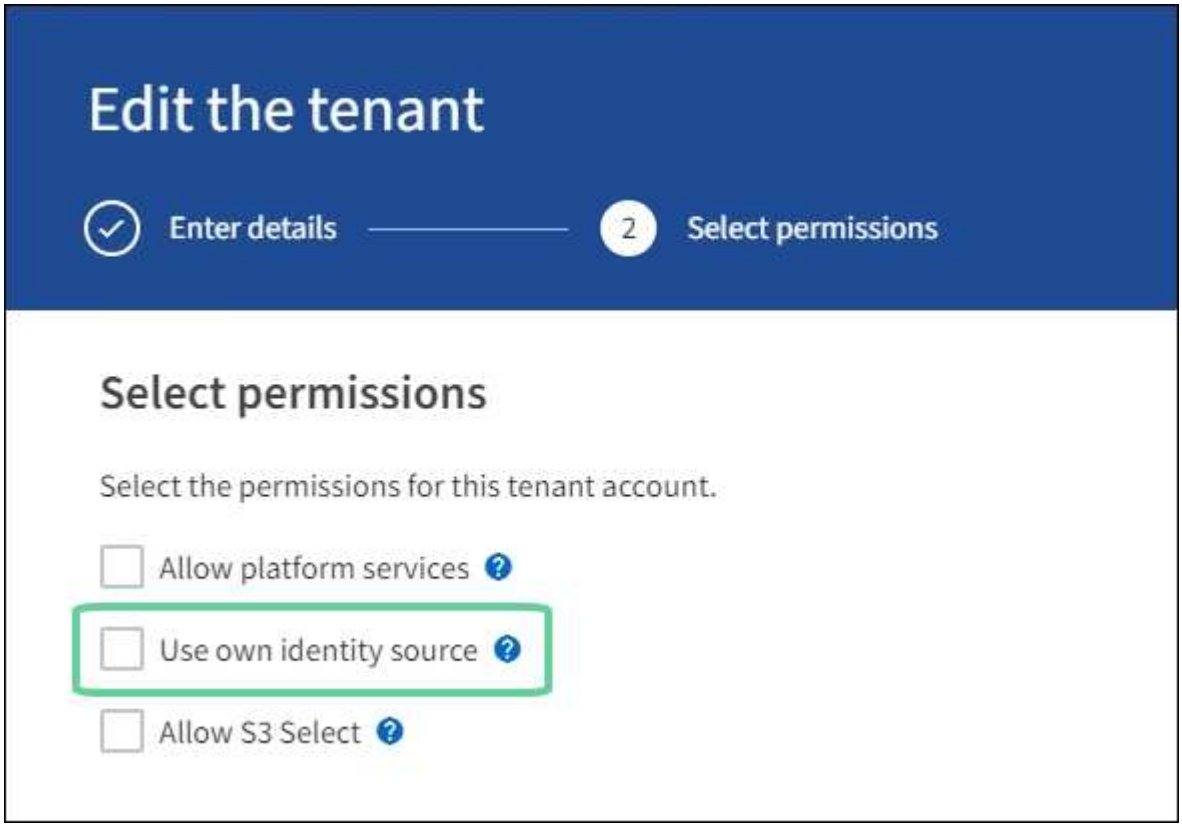
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已設定身分識別聯盟。

步驟

1. 如果有現有的租戶帳戶、請確認沒有租戶使用自己的身分識別來源。

> 啟用SSO時、在租戶管理程式中設定的身分識別來源會被在Grid Manager中設定的身分識別來源覆寫。屬於租戶身分識別來源的使用者將無法再登入、除非他們擁有Grid Manager身分識別來源的帳戶。

   a. 登入每個租戶帳戶的租戶管理程式。
   b. 選擇*存取管理*>*身分識別聯盟*。
   c. 確認未選取 * 啟用身分識別聯盟 * 核取方塊。
   d. 如果是、請確認不再需要此租戶帳戶使用的任何聯盟群組、清除核取方塊、然後選取 * 儲存 * 。
2. 確認聯盟使用者可以存取Grid Manager：
   a. 從Grid Manager中、選取*組態*>*存取控制*>*管理群組*。
   b. 請確定至少已從Active Directory身分識別來源匯入一個同盟群組、而且已將其指派為「根」存取權限。
   c. 登出。
   d. 確認您可以以聯盟群組中的使用者身分重新登入Grid Manager。
3. 如果有現有的租戶帳戶、請確認擁有root存取權限的聯盟使用者可以登入：
   a. 從Grid Manager中選取*租戶*。
   b. 選取租戶帳戶、然後選取*「Actions」（動作）>「Edit」（編輯）*。
   c. 在Enter details（輸入詳細資料）選項卡上、選取* Continue（繼續）*。
   d. 如果選中 * 使用自己的身份來源 * 複選框，則取消選中該複選框並選擇 * 保存 * 。



隨即顯示「租戶」頁面。

a. 選取租戶帳戶、選取*登入*、然後以本機root使用者身分登入租戶帳戶。
b. 在租戶管理程式中、選取*存取管理*>*群組*。
c. 請確定至少已指派Grid Manager中的一個聯盟群組給此租戶的根存取權限。
d. 登出。
e. 確認您可以以同盟群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求與考量"
- "管理管理群組"
- "使用租戶帳戶"

使用沙箱模式

您可以使用沙箱模式來設定及測試單一登入（SSO）、然後再為StorageGRID 所有的使用者啟用。啟用SSO之後、您可以在需要變更或重新測試組態時、隨時返回沙箱模式。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 您已為StorageGRID 您的整套系統設定身分識別聯盟。
- 若為身分識別聯盟* LDAP服務類型*、您會根據您打算使用的SSO身分識別供應商、選擇Active Directory或Azure。

已設定的**LDAP**服務類型	**SSO**身分識別供應商選項
Active Directory	• Active Directory • Azure • PingFedate
Azure	Azure

關於這項工作

啟用SSO且使用者嘗試登入管理節點時StorageGRID 、將驗證要求傳送給SSO身分識別供應商。接著、SSO身分識別供應商會將驗證回應傳回StorageGRID 至原地、指出驗證要求是否成功。對於成功的要求：

- Active Directory或PingFedate的回應包含使用者的通用唯一識別碼（UUID）。
- Azure的回應包括使用者主要名稱（UPN）。

若要讓StorageGRID 服務供應商（服務供應商）和SSO身分識別供應商能夠安全地溝通使用者驗證要求、您必須在StorageGRID 支援中心中設定某些設定。接下來、您必須使用SSO身分識別供應商的軟體、為每個管理節點建立信賴方信任（AD FS）、企業應用程式（Azure）或服務供應商（PingFedate）。最後、您必須返回StorageGRID 到支援SSO的功能。

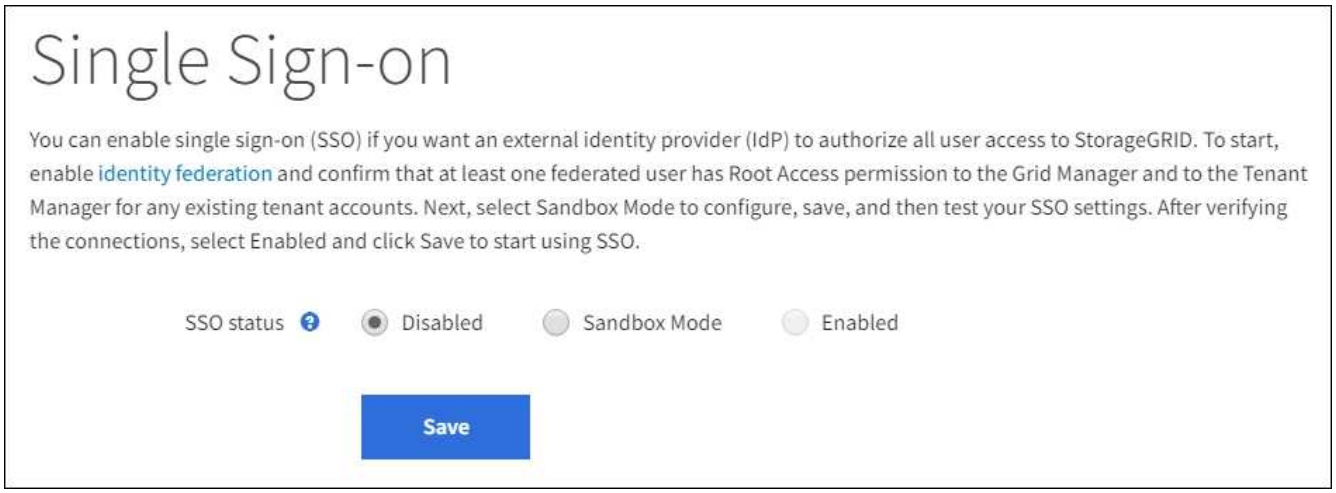
沙箱模式可讓您在啟用SSO之前、輕鬆執行此後端和後端組態、並測試所有設定。使用沙箱模式時、使用者無法使用 SSO 登入。

存取沙箱模式

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。

   此時將顯示「單一登入」頁面、並選取「停用」選項。



   如果 SSO 狀態選項未出現、請確認您已將身分識別提供者設定為同盟身分識別來源。請參閱"單一登入的要求與考量"。

2. 選擇* Sandbox Mode*。

   此時會出現「身分識別提供者」區段。

輸入身分識別供應商詳細資料

步驟

1. 從下拉式清單中選取* SSO類型*。
2. 根據您選取的SSO類型、填寫「身分識別提供者」區段中的欄位。

Active Directory

1. 輸入身分識別提供者的*聯盟服務名稱*、完全如同Active Directory Federation Service（AD FS）中所示。

   若要尋找Federation服務名稱、請前往Windows Server Manager。選擇*工具*>* AD FS管理*。從「動作」功能表中選取*「編輯Federation Service內容」*。Federation Service名稱會顯示在第二個欄位中。

2. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂CA憑證來保護連線安全。

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

   - 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

     如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

3. 在「依賴方」區段中、指定* StorageGRID 依賴方識別符號*以供參考。此值可控制AD FS中每個依賴方信任所使用的名稱。

   - 例如、如果您的網格只有一個管理節點、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會產生一個表格、根據節點的主機名稱、顯示系統中每個管理節點的依賴方識別碼。

   您必須為StorageGRID 您的系統中的每個管理節點建立信賴關係人信任關係。信任每個管理節點的依賴方、可確保使用者能夠安全地登入及登出任何管理節點。

4. 選擇*保存*。

   「儲存」按鈕上會出現綠色勾號幾秒鐘。

Azure

1. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂CA憑證來保護連線安全。

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

- 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

> 如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

2. 在「企業應用程式」區段中、指定*企業應用程式名稱* StorageGRID 以供參考。此值可控制Azure AD中每個企業應用程式所使用的名稱。

   - 例如、如果您的網格只有一個管理節點、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會產生一個表格、根據節點的主機名稱、顯示系統中每個管理節點的企業應用程式名稱。

> 您必須為StorageGRID 您的系統中的每個管理節點建立企業應用程式。為每個管理節點設定企業應用程式、可確保使用者安全地登入及登出任何管理節點。

3. 請依照中的步驟進行 "在Azure AD中建立企業應用程式" 為表格中所列的每個管理節點建立企業應用程式。
4. 從Azure AD複製每個企業應用程式的聯盟中繼資料URL。然後、將此URL貼到StorageGRID 相關的*聯盟中繼資料URL*欄位。
5. 複製並貼上所有管理節點的聯盟中繼資料URL之後、請選取*儲存*。

「儲存」按鈕上會出現綠色勾號幾秒鐘。

PingFedate

1. 指定當身分識別供應商傳送SSO組態資訊以回應StorageGRID 需求時、將使用哪些TLS憑證來保護連線安全。

   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂CA憑證來保護連線安全。

     如果選取此設定、請複製自訂憑證的文字、然後貼到「* CA認證*」文字方塊中。

   - 請勿使用**TLS**：請勿使用TLS憑證來保護連線安全。

> 如果您變更 CA 憑證、請立即變更 "在管理節點上重新啟動 mgmt-API 服務" 並測試 Grid Manager 是否成功登入 SSO 。

2. 在「服務供應商（SP）」區段中、指定* SP連線ID* StorageGRID 以供參考。此值可控制您在PingFedate中用於每個SP連線的名稱。

   - 例如、如果您的網格只有一個管理節點、而且您預期未來不會新增更多管理節點、請輸入 `SG` 或 `StorageGRID`。
   - 如果網格包含多個管理節點、請加入字串 `[HOSTNAME]` 在識別碼中。例如、 `SG-[HOSTNAME]`。這會根據節點的主機名稱、產生一個表格、顯示系統中每個管理節點的SP連線ID。

您必須為StorageGRID 您的系統中的每個管理節點建立SP連線。為每個管理節點建立SP連線、可確保使用者安全地登入及登出任何管理節點。

3. 在*聯盟中繼資料URL*欄位中、指定每個管理節點的聯盟中繼資料URL。

   請使用下列格式：

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

4. 選擇*保存*。

   「儲存」按鈕上會出現綠色勾號幾秒鐘。

設定依賴方信任、企業應用程式或**SP**連線

儲存組態時、會出現沙箱模式確認通知。本通知確認沙箱模式已啟用、並提供概觀指示。

根據需要、可將其保留在沙箱模式中。StorageGRID不過、在「單一登入」頁面上選取*沙箱模式*時、所有StorageGRID 的支援項目都會停用SSO功能。只有本機使用者才能登入。

請依照下列步驟設定信賴方信任（Active Directory）、完整企業應用程式（Azure）或設定SP連線（PingFedate）。

Active Directory

步驟

1. 移至Active Directory Federation Services（AD FS）。
2. 使用StorageGRID 「僅供單一登入」頁面上表所示的每個信賴方識別碼、建立一或多個可靠方的可靠信任。StorageGRID

   您必須為表格中顯示的每個管理節點建立一個信任關係。

   如需相關指示、請前往 "在AD FS中建立依賴方信任"。

Azure

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 下載並儲存該節點的SAML中繼資料。
3. 前往Azure Portal。
4. 請依照中的步驟進行 "在Azure AD中建立企業應用程式" 將每個管理節點的SAML中繼資料檔案上傳至對應的Azure企業應用程式。

PingFedate

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 下載並儲存該節點的SAML中繼資料。
3. 前往PingFedate。
4. "建立一個或多個StorageGRID 服務供應商（SP）連線以供使用"。使用每個管理節點的SP連線ID（如StorageGRID 「支援單一登入」頁面表格所示）、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**SSO**連線

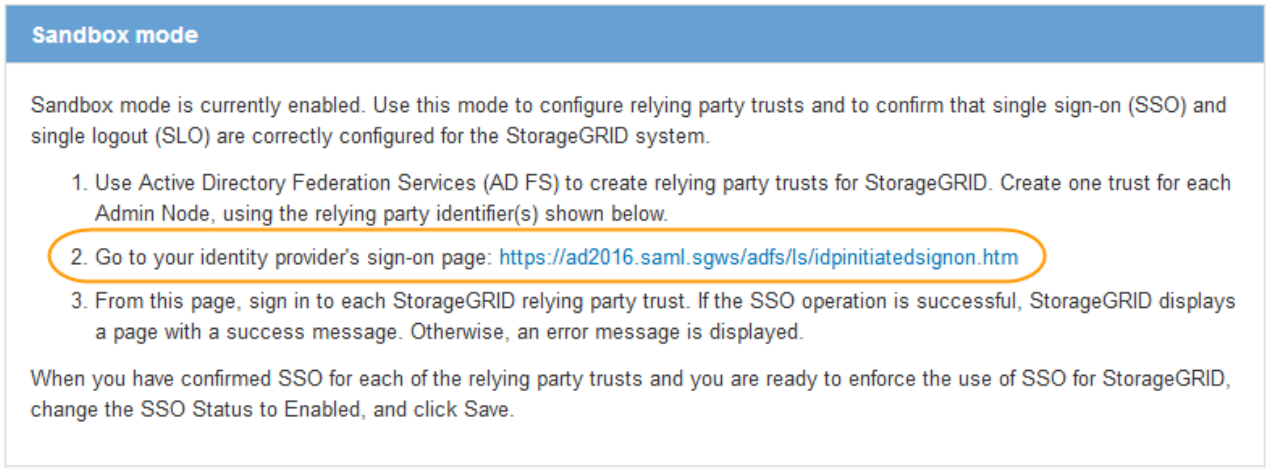
在您為整個StorageGRID 作業系統強制使用單一登入之前、您應確認已為每個管理節點正確設定單一登入和單一登出。

Active Directory

步驟

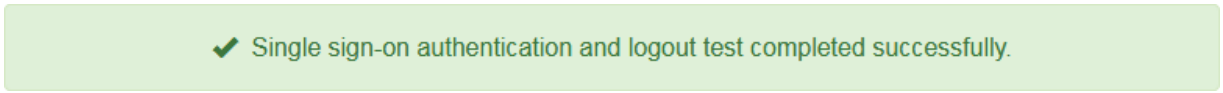
1. 從「功能表單一登入」頁面、找到沙箱模式訊息中的連結。StorageGRID

   此URL衍生自您在* Federation service name*欄位中輸入的值。



2. 選取連結、或複製URL並貼到瀏覽器、以存取身分識別供應商的登入頁面。
3. 若要確認您可以使用SSO登入StorageGRID 支援功能、請選取*登入下列其中一個站台*、選取您主要管理節點的依賴方識別碼、然後選取*登入*。

4. 輸入您的聯盟使用者名稱和密碼。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。



   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
5. 重複這些步驟、驗證網格中每個管理節點的SSO連線。

Azure

步驟

1. 前往Azure入口網站的「單一登入」頁面。
2. 選擇*測試此應用程式*。
3. 輸入同盟使用者的認證資料。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

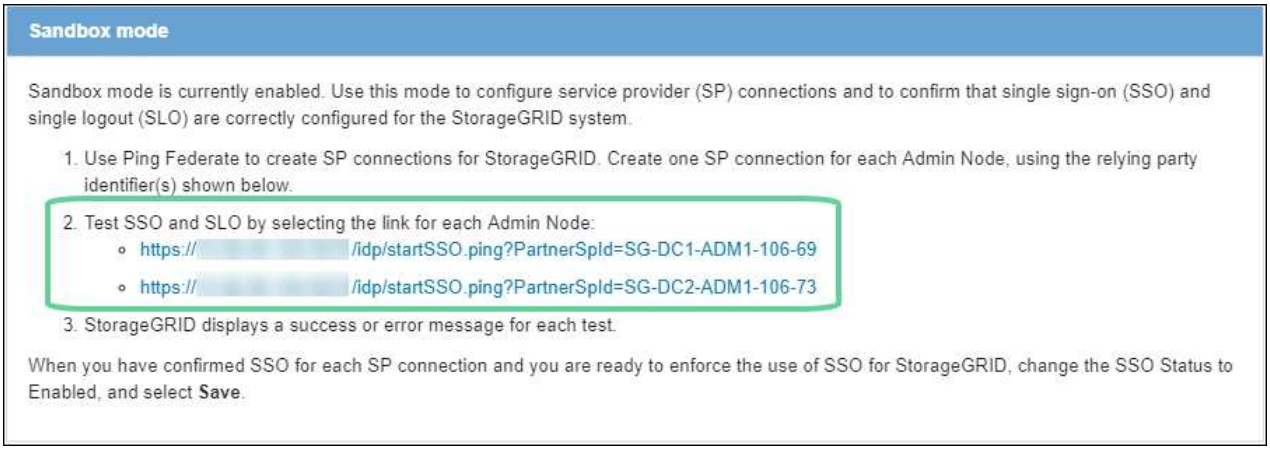
   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
4. 重複這些步驟、驗證網格中每個管理節點的SSO連線。

PingFedate

步驟

1. 從「功能表單一登入」頁面、選取沙箱模式訊息中的第一個連結。StorageGRID

   一次選取並測試一個連結。



2. 輸入同盟使用者的認證資料。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
3. 選取下一個連結、驗證網格中每個管理節點的SSO連線。

   如果您看到「頁面過期」訊息、請在瀏覽器中選取「上一步」按鈕、然後重新提交認證資料。

啟用單一登入

當您確認可以使用SSO登入每個管理節點時、您可以為整個StorageGRID 支援系統啟用SSO。

啟用SSO時、所有使用者都必須使用SSO存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。本機使用者無法再存取StorageGRID 此功能。

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。
2. 將SSO狀態變更為*已啟用*。
3. 選擇*保存*。
4. 檢閱警告訊息、然後選取*確定*。

   現在已啟用單一登入。

如果您使用Azure Portal、並StorageGRID 從用來存取Azure的同一部電腦存取驗證、請確定Azure Portal使用者也是授權StorageGRID 的使用者（已匯入StorageGRID 到「驗證」的聯盟群組中的使用者）。 或登出Azure Portal後再嘗試登入StorageGRID 。

在**AD FS**中建立依賴方信任

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關係人信任。您可以使用PowerShell命令、從StorageGRID 支援中心匯入SAML中繼資料、或手動輸入資料、來建立依賴方信任。

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* AD FS*作為SSO類型。
- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您知道系統中每個管理節點的完整網域名稱（或IP位址）和依賴方識別碼。您可以在StorageGRID 「管理員節點詳細資料」表的「單個登入」頁面上找到這些值。

  您必須為StorageGRID 您的系統中的每個管理節點建立信賴關係人信任關係。信任每個管理節點的依賴方、可確保使用者能夠安全地登入及登出任何管理節點。

- 您有在AD FS中建立信賴關係人信任關係的經驗、或是可以存取Microsoft AD FS文件。
- 您使用的是AD FS管理嵌入式管理單元、屬於「系統管理員」群組。
- 如果您是手動建立信賴關係人信任關係、則您擁有上傳至StorageGRID 該管理介面的自訂憑證、或者您知道如何從命令Shell登入管理節點。

關於這項工作

這些指示適用於Windows Server 2016 AD FS。如果您使用的是不同版本的AD FS、您會注意到程序上的細微差異。如有任何問題、請參閱Microsoft AD FS文件。

使用**Windows PowerShell**建立信賴廠商信任

您可以使用Windows PowerShell快速建立一或多個信賴關係人信任。

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命令提示字元中輸入下列命令：

   「Add-AdfsRelyingPartyTrust -Name「admin_Node_Identer」-Metadata URL "https://Admin_Node_FQDN/api/saml-metadata"

   - 適用於 `Admin_Node_Identifier`下、輸入管理節點的信賴方識別碼、完全如同「單一登入」頁面所示。例如、 `SG-DC1-ADM1`。
   - 適用於 `*Admin_Node_FQDN*`下、輸入相同管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

3. 從Windows Server Manager中、選取* Tools **>** AD FS Management *。

   隨即顯示AD FS管理工具。

4. 選取「* AD FS*>*信賴廠商信任*」。

   此時會出現信賴方信任清單。

5. 新增存取控制原則至新建立的信賴關係人信任：
   a. 找出您剛建立的信賴關係人。
   b. 在信任上按一下滑鼠右鍵、然後選取*編輯存取控制原則*。
   c. 選取存取控制原則。
   d. 選取*「Apply」（套用）、然後選取「OK」（確定）*
6. 新增請款核發政策至新建立的信賴方信託：
   a. 找出您剛建立的信賴關係人。
   b. 以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。
   c. 選取*新增規則*。
   d. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬性傳送為請款）、然後選取* Next*（下一步*）。
   e. 在「設定規則」頁面上、輸入此規則的顯示名稱。

      例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。

   f. 針對屬性存放區、選取* Active Directory *。
   g. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。
   h. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。
   i. 選擇*完成*、然後選擇*確定*。
7. 確認中繼資料已成功匯入。
   a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。
   b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

      如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

8. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。
9. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

透過匯入聯盟中繼資料來建立依賴方信任

您可以存取每個管理節點的SAML中繼資料、以匯入每個信賴方信任的值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。
2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方
3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。
4. 選取*匯入線上發佈的依賴方相關資料、或是本機網路上的相關資料*。
5. 在*聯盟中繼資料位址（主機名稱或URL）*中、輸入此管理節點的SAML中繼資料位置：

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

   適用於 `Admin_Node_FQDN`下、輸入相同管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

6. 完成「信賴方信任」精靈、儲存信賴方信任、然後關閉精靈。

   輸入顯示名稱時、請使用管理節點的信賴方識別碼、如同網格管理器的「單一登入」頁面上所顯示的一樣。例如、 `SG-DC1-ADM1`。

7. 新增報銷規則：
   a. 以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。
   b. 選擇*新增規則*：
   c. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬性傳送為請款）、然後選取* Next*（下一步*）。
   d. 在「設定規則」頁面上、輸入此規則的顯示名稱。

      例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。

   e. 針對屬性存放區、選取* Active Directory *。
   f. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。
   g. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。
   h. 選擇*完成*、然後選擇*確定*。
8. 確認中繼資料已成功匯入。
   a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。
   b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

      如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

9. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。
10. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

手動建立依賴方信任

如果您選擇不匯入依賴零件信任的資料、您可以手動輸入值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。
2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方
3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。
4. 選取*手動輸入依賴方的相關資料*、然後選取*下一步*。
5. 完成信賴廠商信任精靈：

   a. 輸入此管理節點的顯示名稱。

      為確保一致性、請使用管理節點的信賴方識別碼、如同網格管理器的「單一登入」頁面上所顯示的一樣。例如、 `SG-DC1-ADM1`。

   b. 跳過設定選用權杖加密憑證的步驟。

   c. 在「設定 URL 」頁面上、選取 * 啟用 SAML 2.0 WebSSO 傳輸協定的支援 * 核取方塊。

   d. 輸入管理節點的SAML服務端點URL：

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

      適用於 `*Admin_Node_FQDN*`下、輸入管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

   e. 在「設定識別碼」頁面上、指定相同管理節點的信賴方識別碼：

      `Admin_Node_Identifier`

      適用於 `Admin_Node_Identifier`下、輸入管理節點的信賴方識別碼、完全如同「單一登入」頁面所示。例如、 `SG-DC1-ADM1`。

   f. 檢閱設定、儲存信賴關係人信任、然後關閉精靈。

      此時會出現「編輯請款核發原則」對話方塊。

      如果對話方塊未出現、請以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。

6. 若要啟動「請款規則」精靈、請選取*「新增規則*」：

   a. 在Select Rule Template（選擇規則範本）頁面上、從清單中選取* Send LDAP Attributes*（將LDAP屬性傳送為請款）、然後選取* Next*（下一步*）。

   b. 在「設定規則」頁面上、輸入此規則的顯示名稱。

例如，* 對象 GUID 至名稱 ID* 或 * UPN 至名稱 ID* 。

c. 針對屬性存放區、選取* Active Directory *。

d. 在「對應」表格的 LDAP 屬性欄中、輸入 * objectGUID* 或選取 * 使用者主體名稱 * 。

e. 在「對應」表格的「傳出請款類型」欄中、從下拉式清單中選取*名稱ID*。

f. 選擇*完成*、然後選擇*確定*。

7. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。

8. 在「端點」索引標籤上、設定單一登出（SLO）的端點：

a. 選擇* Add SAML（添加SAML）*。

b. 選擇*端點類型*>* SAML登出*。

c. 選擇* Binding（綁定）* **Redirect**（重定向*）。

d. 在「信任的**URL**」欄位中、輸入此管理節點用於單一登出（SLO）的URL：

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

適用於 `*Admin_Node_FQDN*` 下、輸入管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）

a. 選擇*確定*。

9. 在*簽名*索引標籤上、指定此信賴憑證方信任的簽名證書：

a. 新增自訂憑證：

- 如果您有上傳至StorageGRID 該功能的自訂管理憑證、請選取該憑證。
- 如果您沒有自訂憑證、請登入管理節點、前往 `/var/local/mgmt-api` 管理節點的目錄、然後新增 `custom-server.crt` 憑證檔案：

  *附註：*使用管理節點的預設憑證 (`server.crt`）不建議使用。如果管理節點故障、當您恢復節點時、將會重新產生預設憑證、您將需要更新依賴方信任。

b. 選取*「Apply」（套用）、然後選取「OK」（確定）*。

依賴方屬性會儲存並關閉。

10. 重複這些步驟、為StorageGRID 您的整套系統中的所有管理節點設定依賴方信任。

11. 完成後、請返回StorageGRID 「還原」並測試所有信賴關係人的信任、以確認其設定正確。請參閱 "使用沙箱模式" 以取得相關指示。

在**Azure AD**中建立企業應用程式

您可以使用Azure AD為系統中的每個管理節點建立企業應用程式。

開始之前

- 您已開始設定StorageGRID 單一登入功能以供使用、並選擇* Azure *作為SSO類型。

- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您的系統中每個管理節點都有*企業應用程式名稱*。您可以從StorageGRID 「管理員節點」詳細資料表中複製這些值、該表位於「報價單一登入」頁面。

> 您必須為StorageGRID 您的系統中的每個管理節點建立企業應用程式。為每個管理節點設定企業應用程式、可確保使用者安全地登入及登出任何管理節點。

- 您有在Azure Active Directory中建立企業應用程式的經驗。
- 您有一個Azure帳戶、且有有效的訂閱。
- 您在Azure帳戶中有下列任一角色：Global Administrator、Cloud Application Administrator、Application Administrator或服務主體的擁有者。

存取**Azure AD**

步驟

1. 登入 "Azure Portal"。
2. 瀏覽至 "Azure Active Directory"。
3. 選取 "企業應用程式"。

建立企業應用程式並儲存**StorageGRID** 不可靠的**SSO**組態

若要在 StorageGRID 中儲存 Azure 的 SSO 組態、您必須使用 Azure 為每個管理節點建立企業應用程式。您將從Azure複製聯盟中繼資料URL、然後貼到StorageGRID 「支援單一登入」頁面上對應的*聯盟中繼資料URL*欄位。

步驟

1. 針對每個管理節點重複下列步驟。
   a. 在Azure Enterprise應用程式窗格中、選取*新增應用程式*。
   b. 選取*建立您自己的應用程式*。
   c. 如需名稱、請在StorageGRID 「Data Name（管理員節點）」詳細資料表中輸入您複製的*企業應用程式名稱*（英文）、位於「Data Flash（英文）」頁面上。
   d. 選擇*整合您在圖庫中找不到的任何其他應用程式（非圖庫）*選項按鈕。
   e. 選擇* Create （建立）。
   f. 選取* 2中的*入門*連結。設定單一登入*方塊、或選取左邊界的*單一登入*連結。
   g. 選取「* SAML *」方塊。
   h. 複製*應用程式聯盟中繼資料URL*、可在*步驟3 SAML簽署憑證*下找到。
   i. 前往StorageGRID 「僅供參考的單一登入」頁面、然後將URL貼到*聯盟中繼資料URL*欄位、此欄位對應您使用的*企業應用程式名稱*。
2. 在貼上每個管理節點的聯盟中繼資料URL、並對SSO組態進行所有其他必要變更之後、請在StorageGRID 「支援單一登入」頁面上選取「儲存」。

下載每個管理節點的**SAML**中繼資料

儲存SSO組態之後、您可以為StorageGRID 您的系統中的每個管理節點下載SAML中繼資料檔案。

步驟

1. 針對每個管理節點重複這些步驟。
   a. 從管理節點登入StorageGRID 到這個功能。
   b. 選擇*組態*>*存取控制*>*單一登入*。
   c. 選取按鈕、即可下載該管理節點的SAML中繼資料。
   d. 儲存您要上傳至Azure AD的檔案。

將**SAML**中繼資料上傳至每個企業應用程式

下載每StorageGRID 個「支援對象管理節點」的SAML中繼資料檔案之後、請在Azure AD中執行下列步驟：

步驟

1. 返回Azure Portal。
2. 針對每個企業應用程式重複這些步驟：

   您可能需要重新整理「企業應用程式」頁面、以查看先前新增至清單中的應用程式。

   a. 前往企業應用程式的「內容」頁面。
   b. 將*需要指派*設為*否*（除非您要個別設定指派）。
   c. 前往單一登入頁面。
   d. 完成SAML組態。
   e. 選取*上傳中繼資料檔案*按鈕、然後選取您為對應的管理節點下載的SAML中繼資料檔案。
   f. 載入檔案後、選取*「Save"（儲存）、然後選取「 X*」以關閉窗格。您將返回「使用SAML設定單一登入」頁面。
3. 請依照中的步驟進行 "使用沙箱模式" 測試每個應用程式。

在**PingFedate**中建立服務供應商（**SP**）連線

您可以使用PingFedate為系統中的每個管理節點建立服務供應商（SP）連線。為了加速程序、您將從StorageGRID S倚賴 者處匯入SAML中繼資料。

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* Ping federate*作為SSO類型。
- 在**Grid Manager**的「單一登入」頁面上選取「沙箱模式」。請參閱 "使用沙箱模式"。
- 您的系統中每個管理節點都有* SP連線ID*。您可以在StorageGRID 「管理員節點詳細資料」表的「單個登入」頁面上找到這些值。
- 您已下載系統中每個管理節點的* SAML中繼資料*。
- 您在PingFedate伺服器上建立SP連線的經驗豐富。

- 您擁有 "系統管理員參考指南" 適用於PingFedate伺服器。PingFedate文件提供詳細的逐步指示和說明。
- 您擁有 "管理員權限" 適用於PingFedate伺服器。

關於這項工作

以下說明概述如何將PingFedate Server版本10.3設定為StorageGRID SSO供應商以供支援。如果您使用的是另一個版本的PingFedate、您可能需要調整這些指示。請參閱PingFedate伺服器文件、以取得版本的詳細指示。

完整的**PingFedate**必備條件

在建立要用於StorageGRID 觀賞的SP連線之前、您必須先在PingFederate完成必要的工作。設定SP連線時、您將會使用這些必要條件的資訊。

建立資料儲存區**[data-store]**

如果您尚未建立資料存放區、請建立資料存放區、將PingFedate連線至AD FS LDAP伺服器。使用您使用的值 "設定身分識別聯盟" 在StorageGRID

- 類型：目錄（LDAP）
- * LDAP類型*：Active Directory
- 二進位屬性名稱：在LDAP二進位屬性索引標籤上輸入* objectGUID*、完全如圖所示。

建立密碼認證驗證器**[**密碼 驗證器**]**

如果您還沒有、請建立密碼認證驗證程式。

- 類型：LDAP使用者名稱密碼認證驗證程式
- 資料儲存區：選取您建立的資料儲存區。
- 搜尋基礎：輸入LDAP的資訊（例如：DC=SAML、DC=sgws）。
- 搜尋篩選器：SamAccountName=${userName}
- 範圍：子樹狀結構

建立**IDP**介面卡執行個體**[[**介 面卡執行個體**]**

如果您尚未建立IDP介面卡執行個體、請建立一個IDP介面卡執行個體。

步驟

1. 轉至*驗證*>*整合*>* IDP介面卡*。
2. 選擇* Create New Instance*（創建新實例*）。
3. 在類型索引標籤上、選取* HTML表單IDP介面卡*。
4. 在IDP介面卡索引標籤上、選取*新增一列至「認證驗證程式」*。
5. 選取 密碼認證驗證工具 您已建立。
6. 在Adapter Attributes*（適配器屬性）選項卡上，選擇* pseudonyation*的* username*屬性。
7. 選擇*保存*。

建立或匯入簽署憑證[[Signing認證證]

如果您尚未建立簽署憑證、請建立或匯入簽署憑證。

步驟

1. 請前往*安全*>*簽署與解密金鑰與憑證*。
2. 建立或匯入簽署憑證。

在PingFedate建立SP連線

當您在PingFedate建立SP連線時、會將從StorageGRID 支援管理節點的支援節點下載的SAML中繼資料匯入。中繼資料檔案包含許多您需要的特定值。

> 您必須為StorageGRID 您的支援系統中的每個管理節點建立SP連線、以便使用者安全地登入和登出任何節點。請依照下列指示建立第一個SP連線。然後前往 建立其他SP連線 建立所需的任何其他連線。

選擇SP連線類型

步驟

1. 請參訪*應用程式*>*整合*>* SP連線*。
2. 選取*建立連線*。
3. 選擇*不要使用範本進行此連線*。
4. 選擇*瀏覽器SSO設定檔*和* SAML 2.0*作為傳輸協定。

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. 從StorageGRID 「管理節點的「支援單一登入」頁面下載的SAML中繼資料檔案。
3. 檢閱中繼資料摘要和一般資訊索引標籤上提供的資訊。

   合作夥伴的實體ID和連線名稱均設定StorageGRID 為整套SP連線ID。（例如10.96105.200-DC1-ADM1-105-200）。基礎URL是StorageGRID 指「物件管理節點」的IP。

4. 選擇*下一步*。

設定IDP瀏覽器SSO

步驟

1. 從瀏覽器SSO索引標籤、選取*設定瀏覽器SSSSO *。
2. 在「SAML設定檔」索引標籤上、選取「* SP啟動的SSO*」、「* SP初始SLO*」、「* IDP啟動的SSO*」和「* IDP啟動的SLO*」選項。
3. 選擇*下一步*。
4. 在Assertion壽命索引標籤上、不做任何變更。

5. 在Assertion Creation（聲明創建）選項卡上，選擇* Configure Assertion creation （配置聲明創建）。
   a. 在「身分識別對應」索引標籤上、選取「標準」。
   b. 在「屬性合約」索引標籤上、使用* SAML Subject *做為「屬性合約」、以及匯入的未指定名稱格式。
6. 若要延長合約、請選取 * 刪除 * 以移除 `urn:oid`，不使用。

對應介面卡執行個體

步驟

1. 在驗證來源對應索引標籤上、選取*對應新介面卡執行個體*。
2. 在介面卡執行個體索引標籤上、選取 介面卡執行個體 您已建立。
3. 在「對應方法」索引標籤上、選取*從資料儲存區擷取其他屬性*。
4. 在「屬性來源與使用者查詢」索引標籤上、選取「新增屬性來源」。
5. 在「Data Store（資料儲存區）」索引標籤上、提供說明並選取 資料儲存區 您已新增。
6. 在LDAP目錄搜尋索引標籤上：
   - 輸入*基礎DN*、此DN應與StorageGRID 您在知識庫中輸入的LDAP伺服器值完全相符。
   - 在搜尋範圍中、選取* Subtree *。
   - 對於根物件類別、請搜尋並新增下列其中一個屬性： * 物件 GUID* 或 * userPrincipalName* 。
7. 在LDAP二進位屬性編碼類型索引標籤上、針對* objectGUID*屬性選取* Base64*。
8. 在LDAP Filter（LDAP篩選器）索引標籤上、輸入* sAMAccountName=${userName} *。
9. 在「屬性合約履行」標籤上、從「來源」下拉式清單中選取 * LDAP （屬性） * 、然後從「值」下拉式清單中選取 * objectGUID* 或 * userPrincipalName* 。
10. 檢閱並儲存屬性來源。
11. 在「故障儲存屬性來源」索引標籤上、選取*中止SSO交易*。
12. 檢閱摘要、然後選取*「完成」*。
13. 選擇*完成*。

設定傳輸協定設定

步驟

1. 在* SP Connection*>*瀏覽器SSSSO >*傳輸協定設定*索引標籤上、選取*設定傳輸協定設定。
2. 在 Assertion Consumer Service URL 標籤上、接受從 StorageGRID SAML 中繼資料（ * POST * for Binding and ）匯入的預設值 `/api/saml-response` 端點 URL ）。
3. 在「 SLO 服務 URL 」標籤上、接受從 StorageGRID SAML 中繼資料匯入的預設值（ * 重新導向 * 用於連結和 `/api/saml-logout` 端點 URL 。
4. 在允許的 SAML 繫結標籤上、清除 * 成品 * 和 * SOAP* 。只需要* POST 和*重新導向。
5. 在「簽章原則」索引標籤上、保留「 * 需要簽署驗證要求 * 」和「 * 永遠簽署聲明 * 」核取方塊的核取方塊。
6. 在加密原則索引標籤上、選取*無*。
7. 檢閱摘要並選取*完成*以儲存傳輸協定設定。

8. 檢閱摘要並選取*完成*以儲存瀏覽器SSO設定。

設定認證資料

步驟

1. 從SP連線索引標籤、選取*認證*。
2. 從「認證」標籤中、選取*「設定認證」*。
3. 選取 簽署憑證 您已建立或匯入。
4. 選擇*下一步*以前往*管理簽名驗證設定*。
   a. 在信任模式索引標籤上、選取*未鎖定*。
   b. 在「簽名驗證憑證」索引標籤上、檢閱從StorageGRID 「支援SAML」中繼資料匯入的簽署憑證資訊。
5. 檢閱摘要畫面、然後選取*「Save"（儲存）以儲存SP連線。

建立其他**SP**連線

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。您上傳每個複本的新中繼資料。

不同管理節點的SP連線使用相同的設定、但合作夥伴的實體ID、基礎URL、連線ID、連線名稱、簽名驗證、 和SLO回應URL。

步驟

1. 選擇* Action">* Copy*、為每個額外的管理節點建立初始SP連線的複本。
2. 輸入複本的「連線ID」和「連線名稱」、然後選取*「儲存*」。
3. 選擇對應至管理節點的中繼資料檔案：
   a. 選擇* Action">* Update with中繼資料*。
   b. 選擇*選擇「檔案」*並上傳中繼資料。
   c. 選擇*下一步*。
   d. 選擇*保存*。
4. 解決由於未使用屬性而導致的錯誤：
   a. 選取新連線。
   b. 選取*設定瀏覽器SSO >設定宣告建立>屬性合約*。
   c. 刪除* urn:OID*的項目。
   d. 選擇*保存*。

停用單一登入

如果您不想再使用此功能、可以停用單一登入（SSO）。您必須先停用單一登入、才能停用身分識別聯盟。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。

- 您有 "特定存取權限"。

步驟

1. 選擇*組態*>*存取控制*>*單一登入*。

   此時會出現「單一登入」頁面。

2. 選取*停用*選項。
3. 選擇*保存*。

   此時會出現一則警告訊息、指出本機使用者現在可以登入。

4. 選擇*確定*。

   下次登入StorageGRID 時StorageGRID 、會出現「畫面上顯示「資訊區登入」頁面、您必須輸入本機StorageGRID 或聯盟使用者的使用者名稱和密碼。

暫時停用並重新啟用單一管理節點的單一登入

如果單一登入（SSO）系統當機、您可能無法登入Grid Manager。在此情況下、您可以暫時停用及重新啟用單一管理節點的SSO。若要停用及重新啟用SSO、您必須存取節點的命令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。

關於這項工作

停用單一管理節點的SSO之後、您可以以本機根使用者的身分登入Grid Manager。若要保護StorageGRID 您的不穩定系統、您必須在登出時、使用節點的命令Shell在管理節點上重新啟用SSO。

> 停用單一管理節點的SSO並不會影響網格中任何其他管理節點的SSO設定。Grid Manager 中「單一登入」頁面上的「啟用 SSO 」核取方塊會保持選取狀態、除非您更新現有的 SSO 設定、否則所有的 SSO 設定都會保留。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。

2. 執行下列命令：`disable-saml`

   訊息表示該命令僅適用於此管理節點。

3. 確認您要停用SSO。

   訊息表示節點上的單一登入已停用。

4. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。

   現在會顯示Grid Manager登入頁面、因為SSO已停用。

5. 使用root使用者名稱和本機root使用者密碼登入。
6. 如果您因為需要修正SSO組態而暫時停用SSO：
   a. 選擇*組態*>*存取控制*>*單一登入*。
   b. 變更不正確或過時的SSO設定。
   c. 選擇*保存*。

      從「單一登入」頁面選取「儲存」、會自動重新啟用整個網格的SSO功能。

7. 如果您因為其他原因而需要存取Grid Manager而暫時停用SSO：
   a. 執行您需要執行的任何工作或工作。
   b. 選取 * 登出 * 、然後關閉 Grid Manager 。
   c. 在管理節點上重新啟用SSO。您可以執行下列任一步驟：

      - 執行下列命令： `enable-saml`

        訊息表示該命令僅適用於此管理節點。

      確認您要啟用SSO。

   訊息表示節點上已啟用單一登入。

   - 重新開機網格節點： `reboot`

8. 從網頁瀏覽器、從相同的管理節點存取Grid Manager。
9. 確認StorageGRID 畫面出現「畫面不顯示登入」頁面、且您必須輸入SSO認證、才能存取Grid Manager。

使用網格同盟

什麼是網格同盟？

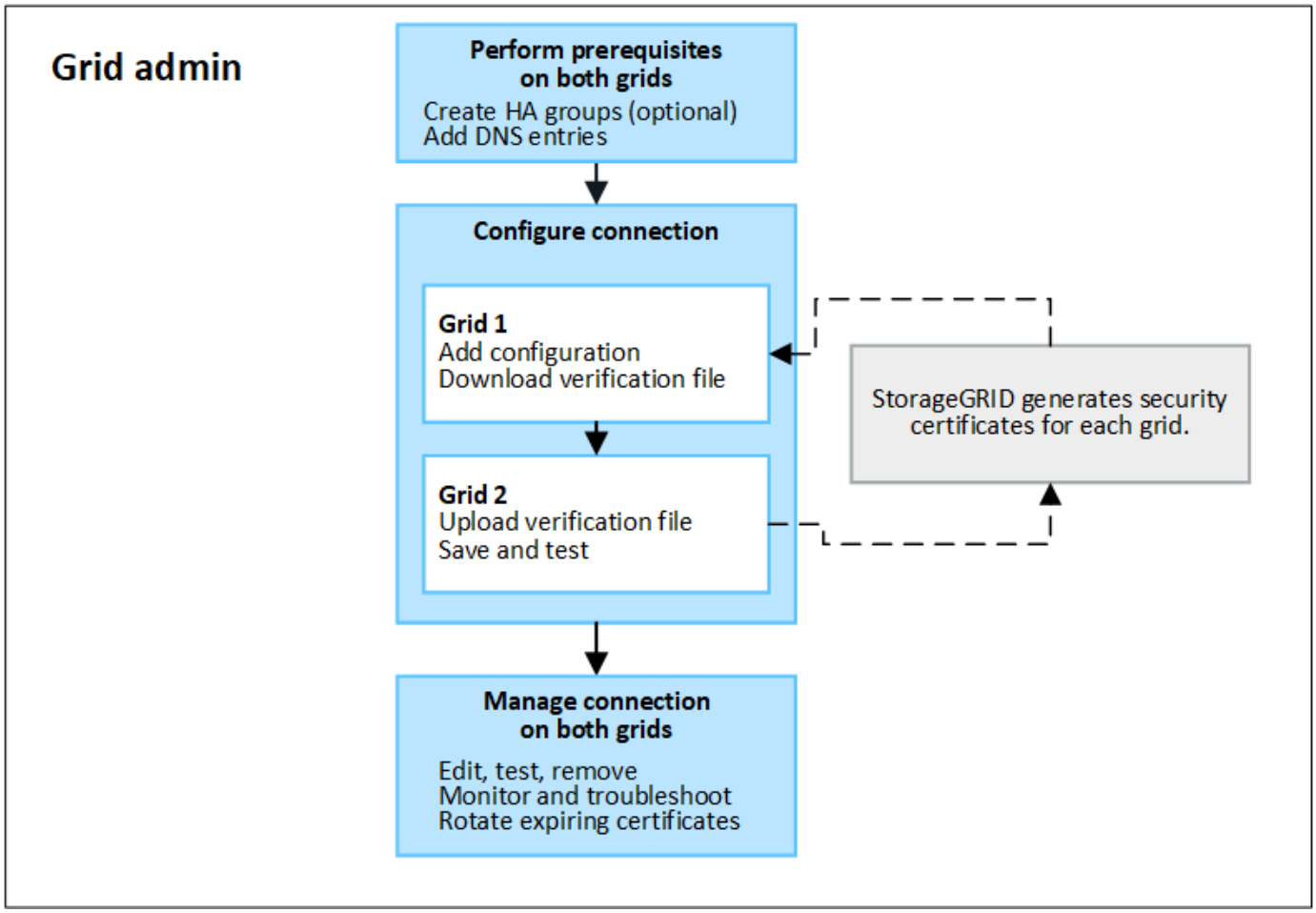
您可以使用網格同盟來複製租戶、並在兩個 StorageGRID 系統之間複寫其物件、以進行災難恢復。

什麼是網格同盟連線？

網格同盟連線是兩個 StorageGRID 系統中管理節點和閘道節點之間的雙向、信任和安全連線。

網格同盟的工作流程

工作流程圖摘要說明在兩個網格之間設定網格同盟連線的步驟。



網格同盟連線的考量與需求

- 用於網格同盟的兩個網格都必須執行 StorageGRID 11.7 或更新版本。
- 網格可以有一個或多個網格同盟連線到其他網格。每個網格同盟連線都與任何其他連線相互關聯。例如、如果 Grid 1 與 Grid 2 有一個連線、而與 Grid 3 有第二個連線、則 Grid 2 和 Grid 3 之間不會有任何隱含連線。
- 網格同盟連線是雙向的。建立連線後、您可以從任一網格監控及管理連線。
- 您必須至少存在一個網格同盟連線、才能使用 "帳戶複製" 或 "跨網格複寫"。

網路和 IP 位址需求

- 網格同盟連線可能發生在網格網路、管理網路或用戶端網路上。
- 網格同盟連線會將一個網格連接到另一個網格。每個網格的組態會在另一個網格上指定一個網格聯盟端點、該端點由管理節點、閘道節點或兩者組成。
- 最佳實務做法是連線 "高可用度（ HA ）群組" 每個網格上的 Gateway 和管理節點。使用 HA 群組有助於確

保當節點無法使用時、網格同盟連線將保持在線上狀態。如果任一 HA 群組中的作用中介面失敗、連線就可以使用備份介面。

- 不建議建立使用單一管理節點或閘道節點 IP 位址的網格同盟連線。如果節點無法使用、網格同盟連線也將無法使用。
- "跨網格複寫" 物件數量要求每個網格上的儲存節點能夠存取另一個網格上設定的管理節點和閘道節點。對於每個網格、請確認所有儲存節點都有高頻寬路由、以做為連線所使用的管理節點或閘道節點。

使用 **FQDN** 來平衡連線負載

對於正式作業環境、請使用完整網域名稱（ FQDN ）來識別連線中的每個網格。然後、建立適當的 DNS 項目、如下所示：

- Grid 1 的 FQDN 對應至 Grid 1 中 HA 群組的一或多個虛擬 IP （ VIP ）位址、或對應至 Grid 1 中一或多個 Admin 或 Gateway 節點的 IP 位址。
- Grid 2 的 FQDN 對應到 Grid 2 的一個或多個 VIP 位址、或是 Grid 2 中一個或多個 Admin 或 Gateway 節點的 IP 位址。

當您使用多個 DNS 項目時、使用連線的要求是負載平衡的、如下所示：

- 對應到多個 HA 群組 VIP 位址的 DNS 項目會在 HA 群組中的作用中節點之間進行負載平衡。
- 對應到多個管理節點或閘道節點 IP 位址的 DNS 項目會在對應節點之間進行負載平衡。

連接埠需求

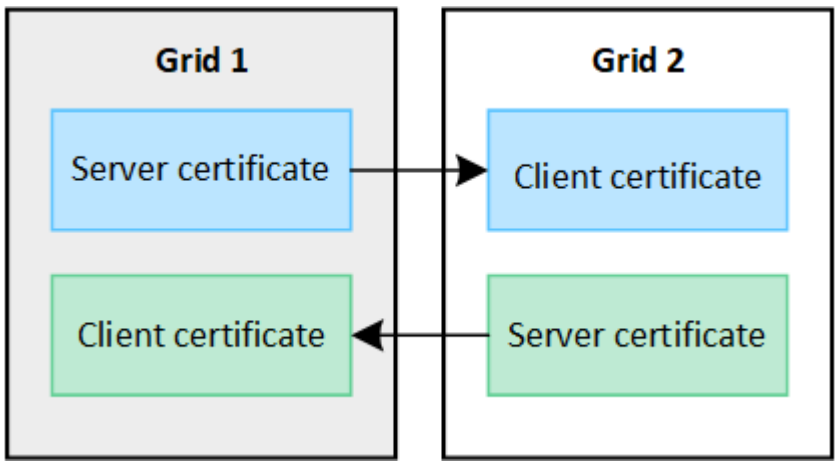
建立網格同盟連線時、您可以指定任何未使用的連接埠號碼、範圍從 23000 到 23999 。此連線中的兩個網格都會使用相同的連接埠。

您必須確保任一網格中的任何節點都不會使用此連接埠進行其他連線。

憑證需求

當您設定網格同盟連線時、 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 傳送至網格 2 的資訊
- 伺服器和用戶端憑證、用於驗證和加密從網格 2 傳送至網格 1 的資訊



依預設、憑證的有效期限為 730 天（ 2 年）。當這些憑證到期日即將到期時、 網格聯合憑證 * 過期警示會提醒

您旋轉憑證、您可以使用 Grid Manager 來進行。

如果連線任一端的憑證過期、連線就會停止運作。資料複寫將擱置、直到憑證更新為止。

深入瞭解

- "建立網格同盟連線"
- "管理網格同盟連線"
- "疑難排解網格同盟錯誤"

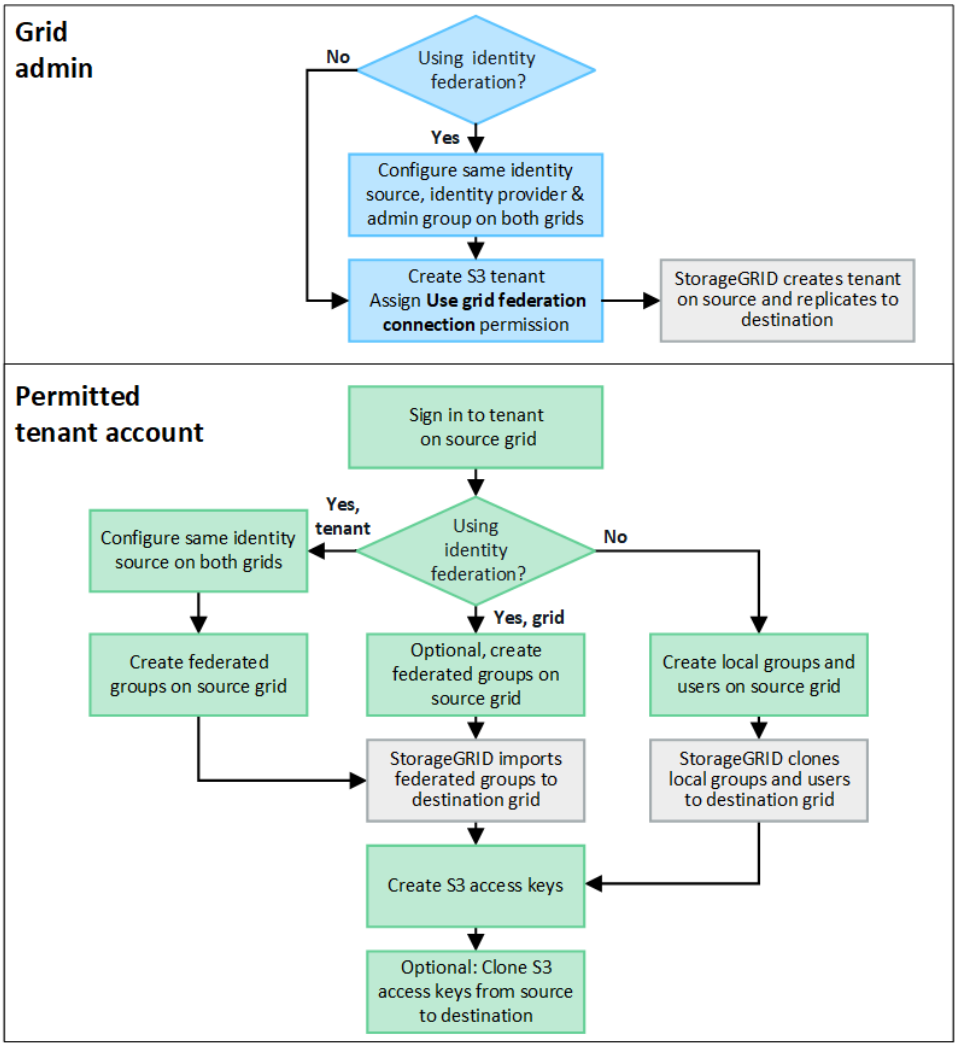
什麼是帳戶複製？

帳戶複製是自動複寫租戶帳戶、租戶群組、租戶使用者、以及選擇性的 中 StorageGRID 系統之間的 S3 存取金鑰 "網格同盟連線"。

需要複製帳戶 "跨網格複寫"。將帳戶資訊從來源 StorageGRID 系統複製到目的地 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區和物件。

帳戶複製工作流程

工作流程圖顯示網格管理員和允許的租戶設定帳戶複製所需執行的步驟。這些步驟會在之後執行 "已設定網格同盟連線"。



Grid 管理工作流程

網格管理員執行的步驟取決於中的 StorageGRID 系統 "網格同盟連線" 使用單一登入（ SSO ）或身分識別聯盟。

設定帳戶複製的 **SSO** （選用）

如果網格同盟連線中的任一 StorageGRID 系統使用 SSO 、則兩個網格都必須使用 SSO 。在建立網格同盟的租戶帳戶之前、租戶來源和目的地網格的網格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 "使用身分識別聯盟"。
2. 為兩個網格設定相同的 SSO 身分識別提供者（ IDP ）。請參閱 "設定單一登入"。
3. "建立相同的管理群組" 在兩個網格上匯入相同的同盟群組。

   當您建立租戶時、您將會選取此群組、以取得來源和目的地租戶帳戶的初始根存取權限。

   如果在您建立租戶之前、這兩個網格上都不存在這個管理群組、則租戶不會複寫到目的地。

設定帳戶複製的網格層級身分識別同盟（選用）

如果任一 StorageGRID 系統使用無 SSO 的身分識別聯盟、則兩個網格都必須使用身分識別聯盟。在建立網格同盟的租戶帳戶之前、租戶來源和目的地網格的網格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 "使用身分識別聯盟"。
2. 或者、如果同盟群組同時擁有來源和目的地租戶帳戶的初始根存取權限、 "建立相同的管理群組" 在兩個網格上匯入相同的同盟群組。

   如果您將「根」存取權限指派給兩個網格上都不存在的同盟群組、則租用戶不會複寫到目的地網格。

3. 如果您不想讓同盟群組擁有兩個帳戶的初始根目錄存取權限、請指定本機根目錄使用者的密碼。

建立允許的 **S3** 租戶帳戶

在選擇性設定 SSO 或身分識別聯盟之後、網格管理員會執行這些步驟、以判斷哪些租戶可以將儲存區物件複寫到其他 StorageGRID 系統。

步驟

1. 判斷您要做為租戶來源網格的網格、以進行帳戶複製作業。

   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. 在該網格上、建立新的 S3 租戶帳戶或編輯現有帳戶。
3. 指派 * 使用網格同盟連線 * 權限。
4. 如果租戶帳戶要管理自己的同盟使用者、請指派 * 使用自己的身分識別來源 * 權限。

   如果指派此權限、來源和目的地租戶帳戶必須先設定相同的身分識別來源、才能建立同盟群組。新增至來源租用戶的同盟群組無法複製到目的地租戶、除非兩個網格都使用相同的身分識別來源。

5. 選取特定的網格同盟連線。
6. 儲存新的或修改過的租戶。

   儲存具有 * 使用網格同盟連線 * 權限的新租用戶時、 StorageGRID 會自動在其他網格上建立該租用戶的複本、如下所示：

   - 兩個租戶帳戶都具有相同的帳戶 ID 、名稱、儲存配額和指派的權限。
   - 如果您選取同盟群組以擁有租用戶的根存取權限、則該群組會複製到目的地租戶。
   - 如果您選取本機使用者來擁有租用戶的根存取權限、則該使用者會複製到目的地租戶。不過、該使用者的密碼並未複製。

如需詳細資訊、請參閱 "管理網格同盟的允許租戶"。

允許的租戶帳戶工作流程

將具有 * 使用網格同盟連線 * 權限的租戶複寫到目的地網格之後、允許的租戶帳戶可以執行這些步驟來複製租戶群組、使用者和 S3 存取金鑰。

步驟

1. 登入租戶來源網格上的租戶帳戶。
2. 如果允許、請在來源和目的地租戶帳戶上設定識別聯盟。
3. 在來源租戶上建立群組和使用者。

   在來源租戶上建立新群組或使用者時、 StorageGRID 會自動將其複製到目的地租戶、但不會從目的地複製到來源。

4. 建立 S3 存取金鑰。
5. 或者、也可以將 S3 存取金鑰從來源租戶複製到目的地租戶。

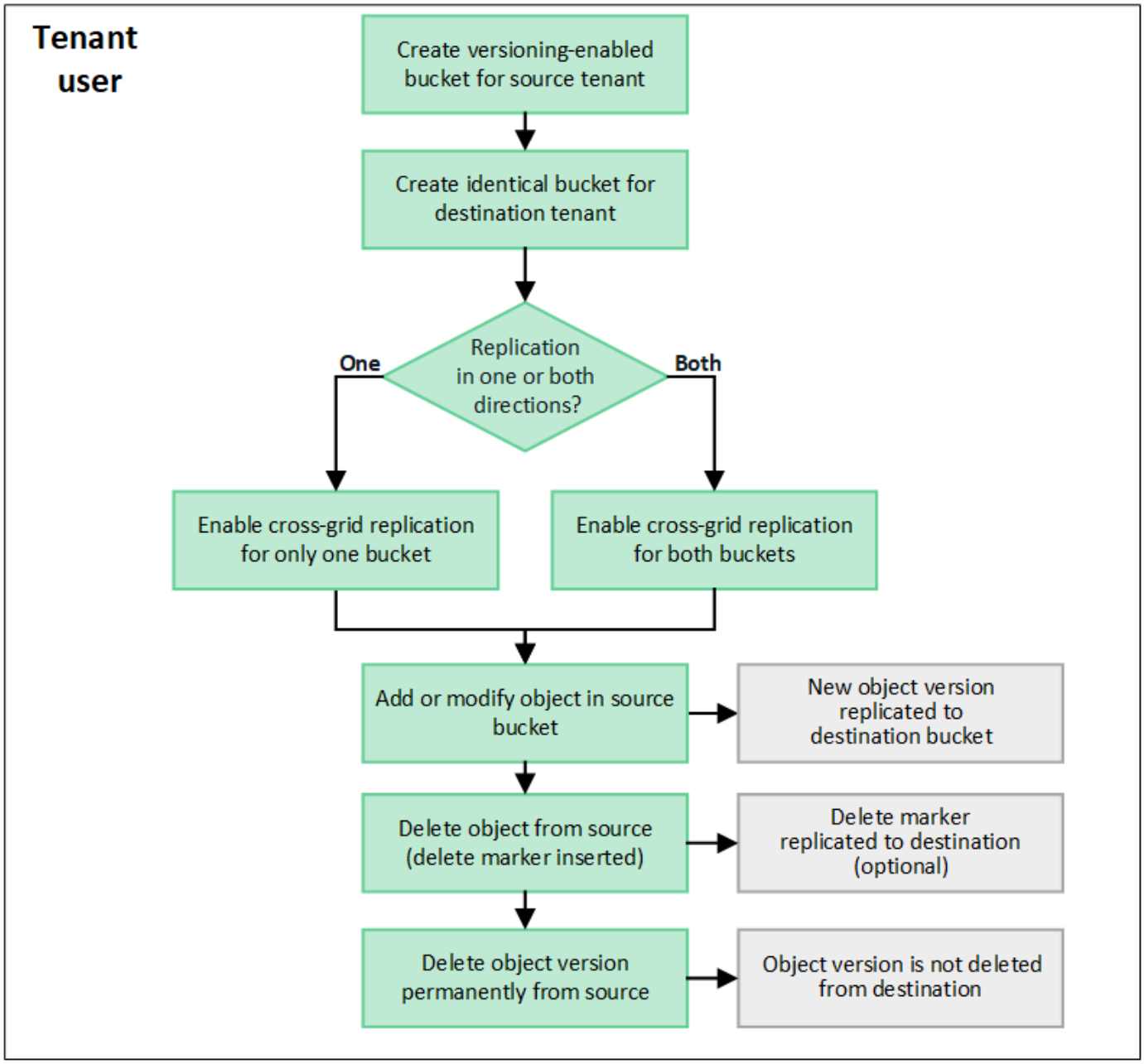
如需有關授權租戶帳戶工作流程的詳細資訊、以及如何複製群組、使用者和 S3 存取金鑰、請參閱 "複製租戶群組和使用者" 和 "使用 API 複製 S3 存取金鑰"。

什麼是跨網格複寫？

跨網格複寫是在兩個 StorageGRID 系統中所選的 S3 貯體之間自動複寫物件、這些系統是在中連接的 "網格同盟連線"。 "帳戶複製" 為跨網格複寫所需。

跨網格複寫的工作流程

工作流程圖摘要說明在兩個網格上的儲存格之間設定跨網格複寫的步驟。



跨網格複寫的需求

如果租戶帳戶具有 * 使用網格同盟連線 * 權限、則可使用一或多個 "網格同盟連線"、擁有「根目錄」存取權限的租戶使用者、可以在每個網格上對應的租戶帳戶中建立相同的貯體。這些貯體：

- 必須具有相同的名稱、但可以有不同的區域
- 必須啟用版本設定
- 必須停用 S3 物件鎖定
- 必須為空白

建立兩個貯體之後、即可針對任一或兩個貯體設定跨網格複寫。

深入瞭解

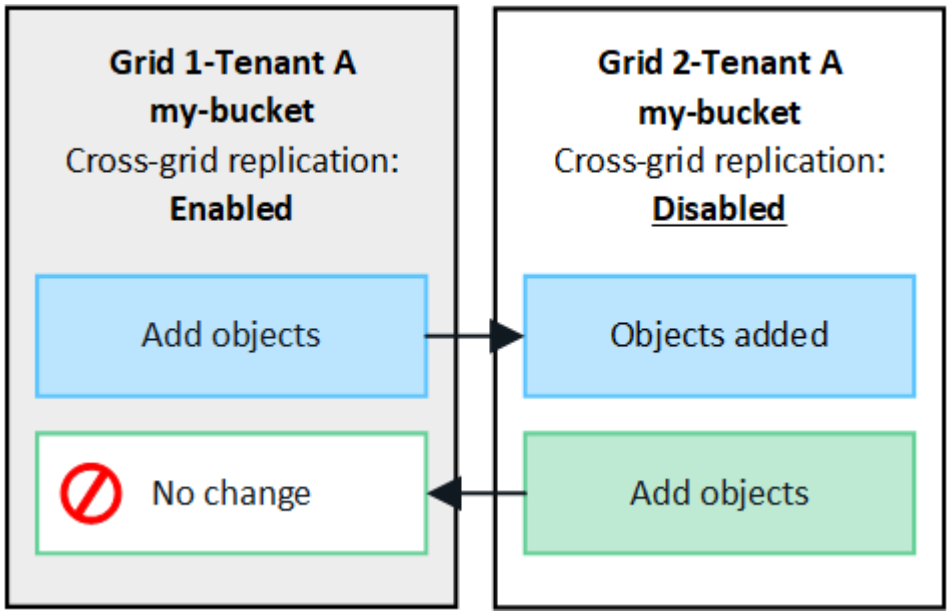
"管理跨網格複寫"

跨網格複寫的運作方式

跨網格複寫可設定為單向或雙向進行。

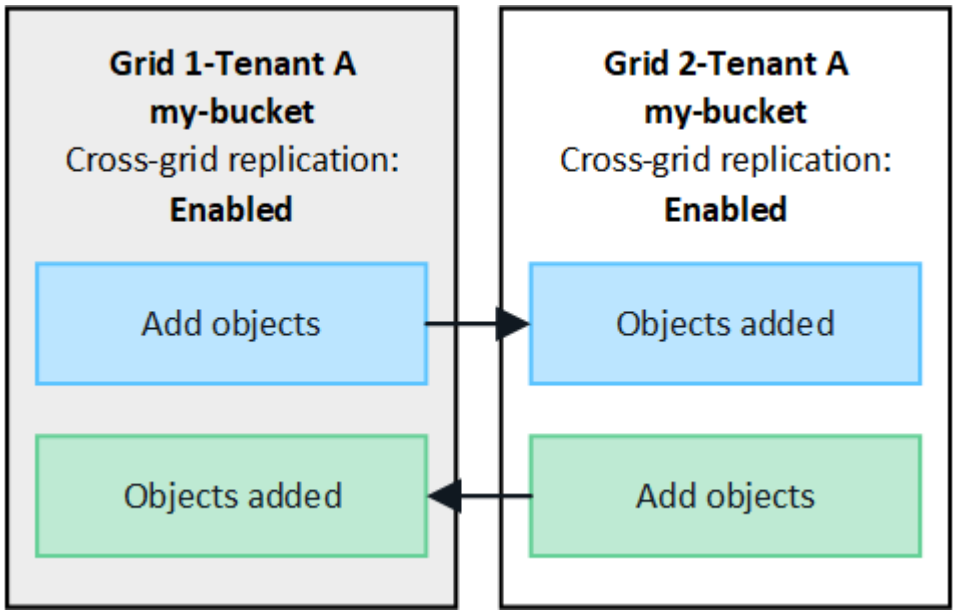
單向複寫

如果您只在一個網格上為某個儲存格啟用跨網格複寫、則新增至該儲存格（來源儲存格）的物件會複寫至另一個網格（目的地儲存格）上的對應儲存格。然而、新增至目的地儲存區的物件不會複寫回來源。在圖中、已啟用跨網格複寫 `my-bucket` 從網格 1 到網格 2 、但在其他方向並未啟用。



雙向複寫

如果您在兩個網格上為相同的儲存格啟用跨網格複寫、則新增至任一儲存格的物件都會複寫至其他網格。在圖中、已啟用跨網格複寫 `my-bucket` 兩個方向。



擷取物件時會發生什麼情況？

當 S3 用戶端將物件新增至已啟用跨網格複寫的貯體時、會發生下列情況：

1. StorageGRID 會自動將物件從來源貯體複製到目的地貯體。執行此背景複寫作業的時間取決於多項因素、包括擱置中的其他複寫作業數。

   S3 用戶端可發出 GetObject 或 HeadObject 要求、以驗證物件的複寫狀態。回應包括 StorageGRID 專屬的 `x-ntap-sg-cgr-replication-status` 回應標頭會有下列其中一個值： S3 用戶端可發出 GetObject 或 HeadObject 要求、以驗證物件的複寫狀態。回應包括 StorageGRID 專屬的 `x-ntap-sg-cgr-replication-status` 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	• * 成功 * ：所有網格連線的複寫都成功。 • * 擱置 * ：物件尚未複寫至至少一個網格連線。 • * 失敗 * ：複寫並未擱置任何網格連線、至少有一個失敗且永久失敗。使用者必須解決此錯誤。
目的地	• 複本 * ：物件已從來源網格複寫。

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

2. StorageGRID 使用每個網格的主動式 ILM 原則來管理物件、就像管理任何其他物件一樣。例如、 Grid 1 上的 Object A 可能會儲存為兩個複寫複本、並永久保留、而複寫至 Grid 2 的 Object A 則可能會使用 2+1 銷毀編碼來儲存、並在三年後刪除。

刪除物件時會發生什麼情況？

如所述 "刪除資料流程"， StorageGRID 可以基於下列任何原因刪除物件：

- S3 用戶端發出刪除要求。
- 租戶管理員使用者選取 "刪除貯體中的物件" 從貯體移除所有物件的選項。
- 貯體具有生命週期組態、已過期。
- ILM 規則中的物件最後一個時間週期結束、而且沒有指定其他放置位置。

當 StorageGRID 因貯體作業中的刪除物件、貯體生命週期到期或 ILM 放置到期而刪除物件時、複寫的物件永遠不會從網格同盟連線中的其他網格中刪除。不過、 S3 用戶端刪除所新增至來源貯體的刪除標記、可選擇性地複寫至目的地貯體。

若要瞭解 S3 用戶端從已啟用跨網格複寫的儲存區刪除物件時會發生什麼情況、請檢閱 S3 用戶端如何從已啟用版本設定的儲存區刪除物件、如下所示：

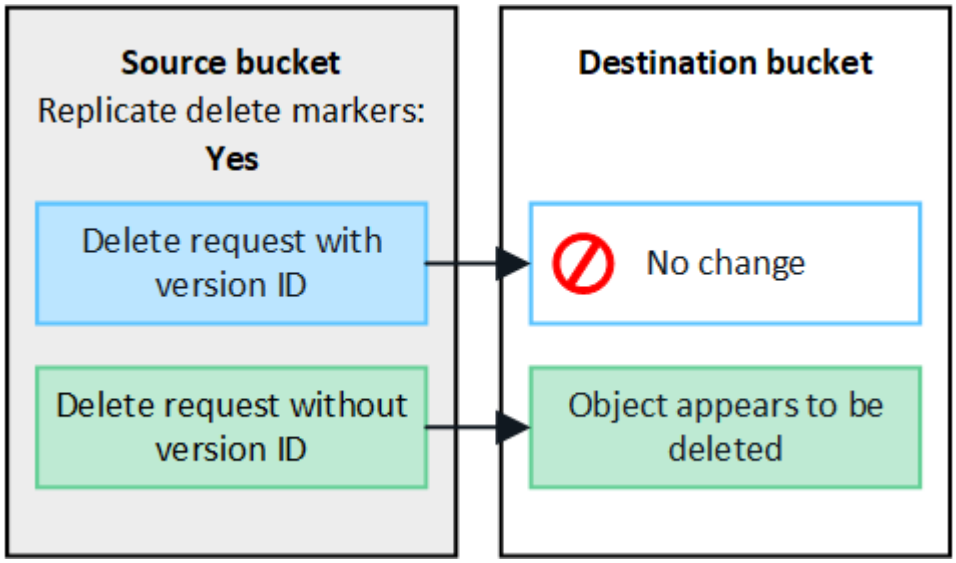
- 如果 S3 用戶端發出包含版本 ID 的刪除要求、該版本的物件將會永久移除。貯體中不會新增刪除標記。
- 如果 S3 用戶端發出不含版本 ID 的刪除要求、 StorageGRID 不會刪除任何物件版本。而是將刪除標記新增至貯體。刪除標記會使 StorageGRID 如同物件被刪除一樣：
  - 沒有版本 ID 的 GetObject 要求將會失敗 `404 No Object Found`

- 具有有效版本 ID 的 GetObject 要求將會成功、並傳回要求的物件版本。

當 S3 用戶端從已啟用跨網格複寫的貯體中刪除物件時、 StorageGRID 會決定是否將刪除要求複寫到目的地、如下所示：

- 如果刪除要求包含版本 ID 、則該物件版本會從來源網格中永久移除。不過、 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。
- 如果刪除要求不包含版本 ID 、則 StorageGRID 可根據為貯體設定跨網格複寫的方式、選擇性地複寫刪除標記：
  - 如果您選擇複寫刪除標記（預設）、則會將刪除標記新增至來源貯體、並複寫至目的地貯體。實際上、這兩個網格上的物件似乎都會被刪除。
  - 如果您選擇不複寫刪除標記、則會將刪除標記新增至來源貯體、但不會複寫至目的地貯體。實際上、在來源網格上刪除的物件不會在目的地網格上刪除。

在圖中、 * 複寫刪除標記 * 在下列情況下設為 * 是 * "已啟用跨網格複寫"。刪除包含版本 ID 之來源貯體的要求、將不會刪除目的地貯體中的物件。刪除不包含版本 ID 的來源貯體要求、將會顯示為刪除目的地貯體中的物件。



如果您想要在網格之間保持物件刪除同步、請建立對應的 "S3 生命週期組態" 適用於兩個網格上的貯體。

加密物件的複寫方式

當您使用跨網格複寫在網格之間複寫物件時、可以加密個別物件、使用預設的儲存格加密、或設定全網格加密。您可以在為貯體啟用跨網格複寫之前或之後、新增、修改或移除預設的貯體或全網格加密設定。

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 （伺服器端加密搭配 StorageGRID 託管金鑰）。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 （伺服器端加密搭配客戶提供的金鑰）。擷取作業將會失敗。

若要使用儲存庫的預設加密、請使用 PuttBucketEncryption 要求並設定 `SSEAlgorithm` 參數至 `AES256`。貯體層級加密適用於任何未經擷取的物件 `x-amz-server-side-encryption` 要求標頭：請參閱 "在貯體上作業"。

若要使用網格層級加密、請將 * 儲存的物件加密 * 選項設定為 * AES-256* 。網格層級加密適用於任何未在儲存區層級加密或未在擷取時未加密的物件 `x-amz-server-side-encryption` 要求標頭：請參閱 "設定網路和物件選項"。

> SSE 不支援 AES-128 。如果使用 **AES-128** 選項為來源網格啟用 * 儲存的物件加密 * 選項、則 AES-128 演算法的使用將不會傳播到複寫的物件。相反地、複寫的物件會使用目的地的預設儲存格或網格層級加密設定（如果有）。

在決定如何加密來源物件時、 StorageGRID 會套用下列規則：

1. 使用 `x-amz-server-side-encryption` 擷取標頭（如果有）。
2. 如果沒有擷取標頭、請使用儲存區預設加密設定（如果已設定）。
3. 如果未設定貯體設定、請使用網格範圍加密設定（如果已設定）。
4. 如果沒有網格範圍的設定、請勿加密來源物件。

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

1. 除非來源物件使用 AES-128 加密、否則請使用與來源物件相同的加密。
2. 如果來源物件未加密或使用 AES-128 、請使用目的地儲存區的預設加密設定（如果已設定）。
3. 如果目的地貯體沒有加密設定、請使用目的地的全網格加密設定（如果已設定）。
4. 如果沒有網格範圍的設定、請勿加密目的地物件。

不支援 **PutObjectTagged** 和 **DeleteObjectTagging**

已啟用跨網格複寫的貯體中的物件不支援 PutObjectTagged 和 DeleteObjectTagged 要求。

如果 S3 用戶端發出推送對象標記或刪除對象標記要求、 `501 Not Implemented` 會傳回。訊息是 `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`。

分割物件的複寫方式

來源網格的最大區段大小適用於複寫到目的地網格的物件。將物件複寫到其他網格時、來源網格的 * 最大區段大小 * 設定（ * 組態 * > * 系統 * > * 儲存選項 * ）將會同時用於兩個網格。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則為 50 MB 。如果您在來源網格上擷取 2 GB 物件、該物件會儲存為兩個 1 GB 區段。即使網格的最大區段大小為 50 MB 、也會將其複寫到目的地網格、做為兩個 1 GB 區段。

比較跨網格複寫和 **CloudMirror** 複寫

開始使用網格同盟時、請檢閱兩者的相似點和差異 "跨網格複寫" 和 "CloudMirror複寫服務StorageGRID"。

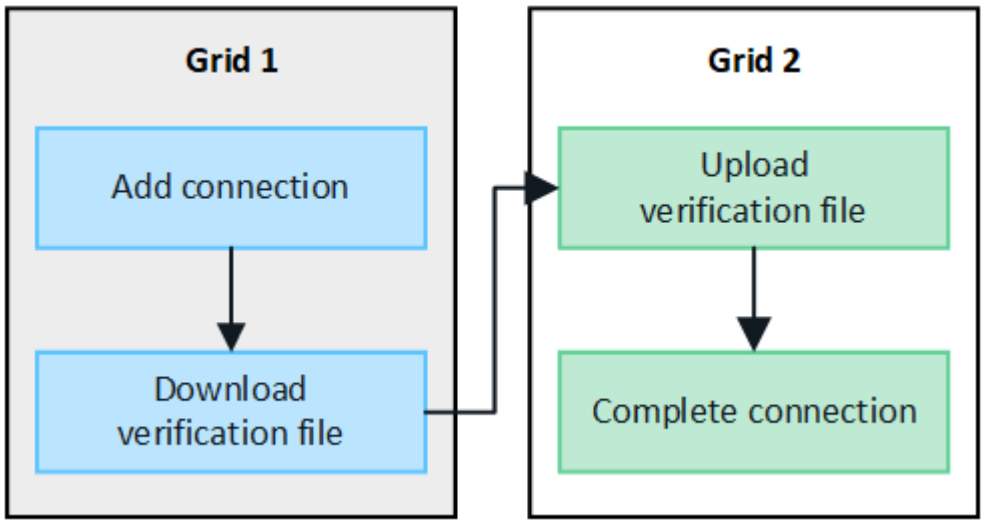
	跨網格複寫	**CloudMirror**複寫服務
主要目的為何？	一個 StorageGRID 系統可做為災難恢復系統。貯體中的物件可在網格之間以一個或兩個方向複寫。	可讓租戶自動將物件從 StorageGRID （來源）的貯體複寫到外部 S3 貯體（目的地）。 CloudMirror複寫可在獨立的S3基礎架構中建立物件的獨立複本。這份不受影響的複本並未作為備份、但通常會在雲端中進一步處理。
如何設定？	1. 設定兩個網格之間的網格同盟連線。 2. 新增自動複製到其他網格的租戶帳戶。 3. 新增新的租戶群組和使用者、這些群組和使用者也會被複製。 4. 在每個網格上建立對應的儲存格、並可在一個或兩個方向進行跨網格複寫。	1. 租戶使用者使用租戶管理程式或S3 API定義CloudMirror端點（IP位址、認證等）來設定CloudMirror複寫。 2. 該租戶帳戶擁有的任何貯體都可以設定為指向 CloudMirror 端點。
誰負責設定？	• 網格管理員會設定連線和租戶。 • 租戶使用者可設定群組、使用者、金鑰和貯體。	一般而言、租戶使用者。
目的地為何？	網格聯合連線中其他 StorageGRID 系統上對應且相同的 S3 儲存貯體。	• 任何相容的 S3 基礎架構（包括 Amazon S3 ）。 • Google Cloud Platform（GCP）
是否需要物件版本設定？	是的、來源和目的地貯體都必須啟用物件版本設定。	否、 CloudMirror 複寫支援來源和目的地上的任何未版本控制和版本控制的貯體組合。
什麼原因會將物件移至目的地？	物件新增至已啟用跨網格複寫的儲存區時、會自動複寫。	將物件新增至已設定 CloudMirror 端點的儲存區時、物件會自動複寫。除非經過修改、否則不會複寫在使用 CloudMirror 端點設定儲存區之前存在於來源儲存區中的物件。
物件如何複寫？	跨網格複寫會建立版本控制的物件、並將版本 ID 從來源貯體複寫到目的地貯體。如此一來、就能在兩個網格上維護版本順序。	CloudMirror 複寫不需要啟用版本控制的儲存區、因此 CloudMirror 只能維護網站內金鑰的訂購。對於不同站台的物件要求、我們無法保證會維持訂購。
如果物件無法複寫該怎麼辦？	物件會排入佇列進行複寫、但受中繼資料儲存限制規範。	物件會排入佇列進行複寫、但必須遵守平台服務限制（請參閱 "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、當物件複寫到其他網格時、也會複寫其系統中繼資料。兩個網格上的中繼資料將相同。	否、當物件複寫到外部儲存區時、系統中繼資料會更新。中繼資料會因位置而異、視擷取時間和 S3 基礎架構的行為而定。

	跨網格複寫	**CloudMirror**複寫服務
如何擷取物件？	應用程式可向任一網格上的儲存格提出要求、以擷取或讀取物件。	應用程式可以向 StorageGRID 或 S3 目的地提出要求、以擷取或讀取物件。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。不需要使用此功能。StorageGRID
如果刪除物件會發生什麼情況？	• 包含版本 ID 的刪除要求絕不會複寫到目的地網格。 • 刪除不包含版本 ID 的要求、將刪除標記新增至來源貯體、可選擇性地複寫至目的地網格。 • 如果只針對一個方向設定跨網格複寫、則可刪除目的地儲存區中的物件、而不會影響來源。	結果會因來源和目的地儲存區的版本設定狀態而異（不需要相同）： • 如果兩個儲存區都已版本化、則刪除要求會在兩個位置新增刪除標記。 • 如果只有來源貯體已版本化、則刪除要求會將刪除標記新增至來源、但不會新增至目的地。 • 如果兩個貯體都沒有版本化、則刪除要求會從來源中刪除物件、而非從目的地刪除物件。 同樣地、也可以刪除目的地儲存區中的物件、而不會影響來源。

建立網格同盟連線

如果您想要複製租戶詳細資料並複寫物件資料、可以在兩個 StorageGRID 系統之間建立網格同盟連線。

如圖所示、建立網格同盟連線包括兩個網格上的步驟。您可以在一個網格上新增連線、然後在另一個網格上完成連線。您可以從任一網格開始。



開始之前

- 您已檢閱 "考量與要求" 用於設定網格同盟連線。

- 如果您打算為每個網格使用完整網域名稱（ FQDN ）、而非 IP 或 VIP 位址、則您知道要使用哪些名稱、而且已確認每個網格的 DNS 伺服器都有適當的項目。
- 您使用的是 "支援的網頁瀏覽器"。
- 您擁有兩個網格的「根」存取權限和資源配置複雜密碼。

新增連線

在兩個 StorageGRID 系統中的任一系統上執行這些步驟。

步驟

1. 從任一網格上的主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取 * 新增連線 * 。
4. 輸入連線的詳細資料。

欄位	說明
連線名稱	可協助您辨識此連線的唯一名稱、例如「 Grid 1-Grid 2 」。
此網格的 FQDN 或 IP	下列其中一項： • 您目前登入之網格的 FQDN • 此網格上 HA 群組的 VIP 位址 • 此網格上管理節點或閘道節點的 IP 位址。IP 可以位於目的地網格所能到達的任何網路上。
連接埠	您要用於此連線的連接埠。您可以輸入任何未使用的連接埠號碼、範圍從 23000 到 23999 。 此連線中的兩個網格都會使用相同的連接埠。您必須確保任一網格中的任何節點都不會使用此連接埠進行其他連線。
此網格的憑證有效天數	您希望此連線網格的安全性憑證有效的天數。預設值為 730 天（ 2 年）、但您可以輸入 1 至 762 天的任何值。 當您儲存連線時、 StorageGRID 會自動為每個網格產生用戶端和伺服器憑證。
此網格的資源配置複雜密碼	您已登入之網格的資源配置複雜密碼。

欄位	說明
其他網格的 FQDN 或 IP	下列其中一項： • 您要連線的網格 FQDN • 其他網格上 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。IP 可以位於來源網格所能到達的任何網路上。

5. 選取 * 儲存並繼續 * 。
6. 對於「下載驗證檔案」步驟、請選取 * 下載驗證檔案 * 。

   在其他網格上完成連線後、您就無法再從任一網格下載驗證檔案。

7. 找到下載的檔案 (*connection-name*.grid-federation）、並將其儲存至安全的位置。

   此檔案包含機密（遮罩為 *）和其他敏感的詳細資料、必須安全地儲存及傳輸。

8. 選取 * 關閉 * 以返回「 Grid Federation 」頁面。
9. 確認已顯示新連線、且其 * 連線狀態 * 為 * 正在等待連線 * 。
10. 提供 *connection-name*.grid-federation 將檔案傳送至其他網格的網格管理員。

完整連線

在您要連線的 StorageGRID 系統（另一個網格）上執行這些步驟。

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取 * 上傳驗證檔案 * 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）。

   畫面會顯示連線的詳細資料。

5. 您也可以為此網格輸入不同的安全性憑證有效天數。* 憑證有效天數 * 項目預設為您在第一個網格上輸入的值、但每個網格可以使用不同的到期日。

   一般而言、在連線的兩端、使用相同天數的憑證。

   如果連線任一端的憑證過期、連線將會停止運作、而且在更新憑證之前、複製作業將會擱置。

6. 輸入您目前登入網格的資源配置密碼。
7. 選取 * 儲存並測試 * 。

會產生憑證並測試連線。如果連線有效、就會出現成功訊息、而且新連線會列在「 Grid Federation 」（網格聯盟）頁面上。* 連線狀態 * 將為 * 已連線 * 。

如果出現錯誤訊息、請解決任何問題。請參閱 "疑難排解網格同盟錯誤"。

8. 移至第一個網格上的「網格聯盟」頁面、然後重新整理瀏覽器。確認 * 連線狀態 * 現在為 * 連線 * 。
9. 建立連線後、安全地刪除驗證檔案的所有複本。

   如果您編輯此連線、將會建立新的驗證檔案。原始檔案無法重複使用。

完成後

- 檢閱的考量事項 "管理允許的租戶"。
- "建立一個或多個新的租戶帳戶"、指派 * 使用網格聯盟連線 * 權限、然後選取新的連線。
- "管理連線" 視需要而定。您可以編輯連線值、測試連線、旋轉連線憑證或移除連線。
- "監控連線" 作為正常 StorageGRID 監控活動的一部分。
- "疑難排解連線問題"包括解決與帳戶複製和跨網格複寫有關的任何警示和錯誤。

管理網格同盟連線

管理 StorageGRID 系統之間的網格同盟連線、包括編輯連線詳細資料、旋轉憑證、移除租戶權限、以及移除未使用的連線。

開始之前

- 您可以使用登入任一網格上的 Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限" 對於您登入的網格。

[[edit_grid_fed_connection] 編輯網格同盟連線

您可以登入連線中任一網格上的主要管理節點、以編輯網格同盟連線。變更第一個網格之後、您必須下載新的驗證檔案並上傳至其他網格。

編輯連線時、帳戶複製或跨網格複寫要求會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、但在上傳至第二個網格、儲存及測試之前、不會使用。

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. 選取 * 節點 * 、並確認系統中的所有其他管理節點都已上線。

   編輯網格同盟連線時、 StorageGRID 會嘗試在第一個網格上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至所有管理節點、當您選取 * 儲存並測試 * 時、會出現警告訊息。

3. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。

4. 使用 Grid Federation 頁面上的 * Actions* 功能表或特定連線的詳細資料頁面、編輯連線詳細資料。請參閱 "建立網格同盟連線" 輸入內容。

   「行動」功能表

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

   詳細資料頁面

   a. 選取連線名稱以顯示其詳細資料。
   b. 選擇*編輯*。
   c. 輸入新資訊。

5. 輸入您登入網格的資源配置密碼。
6. 選取 * 儲存並繼續 * 。

   新值會儲存、但在您將新驗證檔案上傳至其他網格之前、這些值不會套用至連線。

7. 選擇 * 下載驗證檔案 * 。

   若要稍後下載此檔案、請前往連線的詳細資料頁面。

8. 找到下載的檔案 (*connection-name*.grid-federation) 、並將其儲存至安全的位置。

   驗證檔案包含機密資料、必須安全地儲存及傳輸。

9. 選取 * 關閉 * 以返回「 Grid Federation 」頁面。
10. 確認 * 連線狀態 * 為 * 擱置編輯 * 。

    如果開始編輯連線時連線狀態不是 * 已連線 * 、則不會變更為 * 擱置編輯 * 。

11. 提供 *connection-name*.grid-federation 將檔案傳送至其他網格的網格管理員。

完成連線編輯

將驗證檔案上傳至其他網格、即可完成連線編輯。

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取 * 上傳驗證檔案 * 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。
5. 輸入您目前登入網格的資源配置密碼。

6. 選取 * 儲存並測試 * 。

   如果可以使用編輯的值建立連線、就會出現成功訊息。否則會出現錯誤訊息。檢閱訊息並解決任何問題。

7. 關閉精靈以返回「 Grid Federation 」頁面。
8. 確認 * 連線狀態 * 為 * 已連線 * 。
9. 移至第一個網格上的「網格聯盟」頁面、然後重新整理瀏覽器。確認 * 連線狀態 * 現在為 * 連線 * 。
10. 建立連線後、安全地刪除驗證檔案的所有複本。

[[test_grid_fed_connection] 測試網格同盟連線

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 使用 Grid Federation 頁面上的 * Actions* 功能表或特定連線的詳細資料頁面來測試連線。

   「行動」功能表

   a. 選取連線的選項按鈕。
   b. 選取 * 動作 * > * 測試 * 。

   詳細資料頁面

   a. 選取連線名稱以顯示其詳細資料。
   b. 選擇*測試連線*。

4. 檢閱連線狀態：

連線狀態	說明
連線	兩個網格都已連線並正常通訊。
錯誤	連線處於錯誤狀態。例如、憑證已過期或組態值不再有效。
擱置編輯	您已編輯此網格上的連線、但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其他網格。
正在等待連線	您已在此網格上設定連線、但其他網格上的連線尚未完成。從這個網格下載驗證檔案、並將其上傳至其他網格。
不明	連線處於未知狀態、可能是因為網路問題或離線節點。

5. 如果連線狀態為 * 錯誤 * 、請解決任何問題。然後再次選擇 * 測試連線 * 以確認問題已解決。

旋轉連線憑證

每個網格同盟連線都會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接近到期日時、* 網格聯合憑證過期 * 警示會提醒您旋轉憑證。

如果連線任一端的憑證過期、連線將會停止運作、而且在更新憑證之前、複製作業將會擱置。

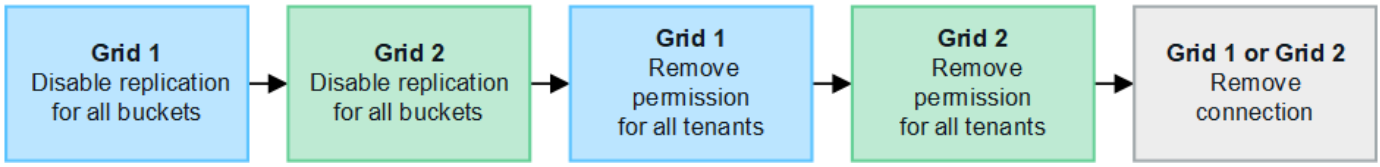
步驟

1. 從任一網格上的主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 從「 Grid Federation 」（網格聯盟）頁面的任一索引標籤中、選取連線名稱以顯示其詳細資料。
4. 選取*憑證*索引標籤。
5. 選取 * 「旋轉憑證」 * 。
6. 指定新憑證的有效天數。
7. 輸入您登入網格的資源配置密碼。
8. 選取 * 「旋轉憑證」 * 。
9. 視需要在連線的其他網格上重複這些步驟。

   一般而言、在連線的兩端、使用相同天數的憑證。

[[remove_grid 饋送 _connection]] 移除網格同盟連線

您可以從連線中的任一網格移除網格同盟連線。如圖所示、您必須在兩個網格上執行必要步驟、以確認任一網格上的任何租戶都未使用連線。



移除連線之前、請注意下列事項：

- 移除連線並不會刪除已在方格之間複製的任何項目。例如、當租戶權限移除時、不會從任一網格中刪除兩個網格上的租戶使用者、群組和物件。如果要刪除這些項目、您必須手動從兩個方格中刪除它們。
- 當您移除連線時、任何擱置複寫的物件（擷取但尚未複寫到其他網格）都會永久失敗。

停用所有租戶貯體的複寫

步驟

1. 從任一網格開始、從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取連線名稱以顯示其詳細資料。
4. 在 * 允許的租戶 * 標籤上、判斷是否有任何租戶正在使用連線。
5. 如果列出任何租戶、請指示所有租戶 "停用跨網格複寫" 適用於連線中兩個網格上的所有貯體。

如果任何租戶貯體已啟用跨網格複寫、則無法移除 * 使用網格同盟連線 * 權限。每個租戶帳戶都必須停用其在兩個網格上的貯體跨網格複寫。

移除每個租戶的權限

停用所有租戶貯體的跨網格複寫之後、請移除兩個網格上所有租戶的 * 使用網格同盟權限 * 。

步驟

1. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
2. 選取連線名稱以顯示其詳細資料。
3. 對於「 * 允許租戶 * 」索引標籤上的每個租戶、請移除每個租戶的 * 使用網格同盟連線 * 權限。請參閱 "管理允許的租戶"。
4. 對其他網格上的允許租戶重複這些步驟。

移除連線

步驟

1. 當任一網格上沒有租戶正在使用連線時、請選取 * 移除 * 。
2. 檢閱確認訊息、然後選取 * 移除 * 。
   - 如果可以移除連線、就會顯示成功訊息。網格同盟連線現在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。您可以執行下列其中一項：
     - 解決錯誤（建議）。請參閱 "疑難排解網格同盟錯誤"。
     - 強制移除連線。請參閱下一節。

[[force-remove_grid 饋送 _connection]] 強制移除網格同盟連線

如有必要、您可以強制移除狀態為 * 已連線 * 的連線。

強制移除只會從本機網格刪除連線。若要完全移除連線、請在兩個網格上執行相同步驟。

步驟

1. 在確認對話方塊中、選取 * 強制移除 * 。

   隨即顯示成功訊息。無法再使用此網格同盟連線。不過、租戶貯體可能仍啟用跨網格複寫、而且可能已在連線的網格之間複寫某些物件複本。

2. 從連線中的其他網格、從主要管理節點登入 Grid Manager 。
3. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
4. 選取連線名稱以顯示其詳細資料。
5. 選取 * 移除 * 和 * 是 * 。
6. 選取 * 強制移除 * 可移除此網格的連線。

管理 **Grid Federation** 的允許租戶

您可以允許 S3 租戶帳戶在兩個 StorageGRID 系統之間使用網格同盟連線。當租戶可以使用連線時、必須採取特殊步驟來編輯租戶詳細資料、或永久移除租戶使用連線的權限。

開始之前

- 您可以使用登入任一網格上的 Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限" 對於您登入的網格。
- 您有 "已建立網格同盟連線" 在兩個網格之間。
- 您已檢閱的工作流程 "帳戶複製" 和 "跨網格複寫"。
- 視需要、您已針對連線中的兩個網格設定單一登入（ SSO ）或識別聯盟。請參閱 "什麼是帳戶複製"。

建立允許的租戶

如果您想要允許新的或現有的租戶帳戶使用網格同盟連線來進行帳戶複製和跨網格複寫、請遵循的一般指示 "建立新的 S3 租戶" 或 "編輯租戶帳戶" 並注意下列事項：

- 您可以從連線中的任一網格建立租用戶。建立租戶的網格是 _ 租戶的來源網格 _ 。
- 連線狀態必須為 * 已連線 * 。
- 建立或編輯租戶以啟用 * 使用網格同盟連線 * 權限、然後儲存在第一個網格上時、會自動將相同的租戶複寫到另一個網格。複寫租戶的網格是 _ 租戶的目的地網格 _ 。
- 兩個網格上的租戶將擁有相同的 20 位數帳戶 ID 、名稱、說明、配額和權限。您也可以選擇使用 * 說明 * 欄位來協助識別來源租戶和目的地租戶。例如、對於在 Grid 1 上建立的租戶、此描述也會顯示給複製到 Grid 2 的租戶：「此租戶是在 Grid 1 上建立的。」
- 基於安全考量、本機根使用者的密碼不會複製到目的地網格。

> 在本機根使用者登入目的地網格上複寫的租用戶之前、該網格的網格管理員必須先登入 "變更本機 root 使用者的密碼"。

- 新的或編輯過的租用戶在兩個網格上都可用之後、租戶使用者就可以執行這些作業：
  - 從租戶的來源網格建立群組和本機使用者、這些群組和使用者會自動複製到租戶的目的地網格。請參閱 "複製租戶群組和使用者"。
  - 建立新的 S3 存取金鑰、可選擇性地複製到租戶的目的地網格。請參閱 "使用 API 複製 S3 存取金鑰"。
  - 在連線的兩個網格上建立相同的儲存格、並在單一方向或雙向啟用跨網格複寫。請參閱 "管理跨網格複寫"。

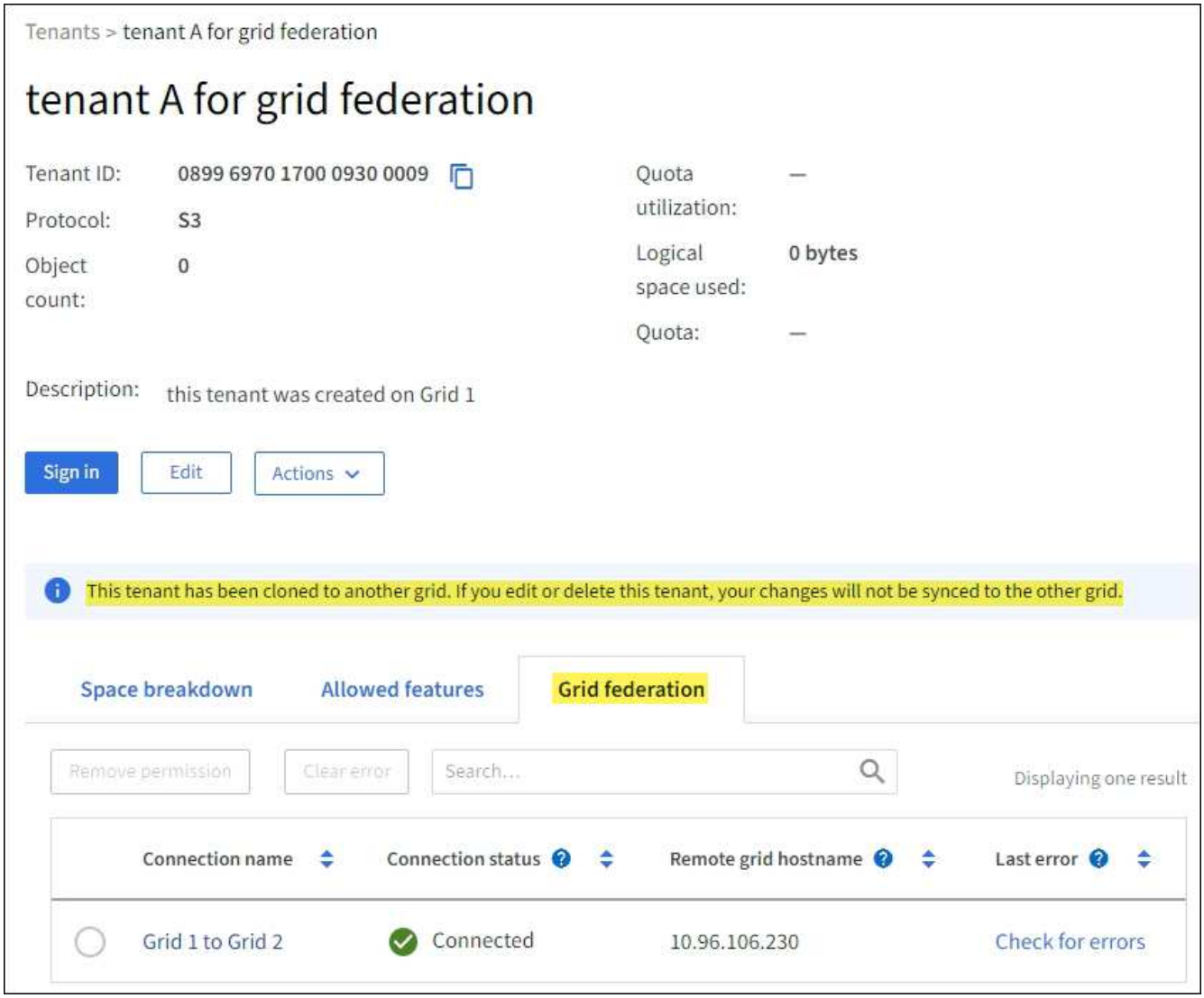
檢視允許的租戶

您可以查看允許使用網格同盟連線之租用戶的詳細資料。

步驟

1. 選取*租戶*。
2. 從「租戶」頁面中、選取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（也就是說、如果租戶是在此網格上建立的）、就會出現橫幅、提醒您租戶已複製到另一個網格。如果您編輯或刪除此租用戶、您的變更將不會同步至其他網格。



3. （可選）選擇 *Grid Federation （網格聯盟） * 選項卡 "監控網格同盟連線"。

編輯允許的租戶

如果您需要編輯具有 * 使用網格同盟連線 * 權限的租用戶、請遵循的一般指示 "編輯租戶帳戶" 並注意下列事項：

- 如果租戶具有 * 使用網格同盟連線 * 權限、您可以從連線中的任一網格編輯租戶詳細資料。不過、您所做的任何變更都不會複製到其他網格。如果您想要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、您無法清除 * 使用網格同盟連線 * 權限。
- 編輯租戶時、您無法選取不同的網格同盟連線。

刪除允許的租戶

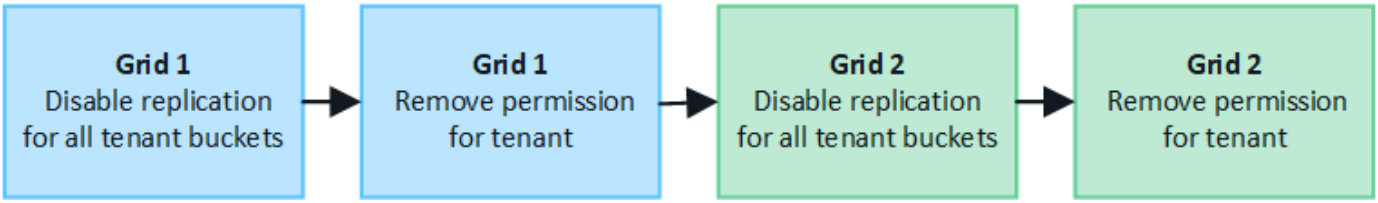
如果您需要移除具有 * 使用網格同盟連線 * 權限的租用戶、請遵循的一般指示 "刪除租戶帳戶" 並注意下列事項：

- 在您移除來源網格上的原始租戶之前、您必須先移除來源網格上帳戶的所有貯體。
- 在您移除目的地網格上的複製租戶之前、您必須先移除目的地網格上帳戶的所有貯體。
- 如果您移除原始或複製的租用戶、則該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、則任何複製到目的地網格的租戶群組、使用者或金鑰都不會受到影響。您可以刪除複製的租戶、或是讓它管理自己的群組、使用者、存取金鑰和貯體。
- 如果您要移除目的地網格上的複製租用戶、如果將新群組或使用者新增至原始租用戶、就會發生複製錯誤。

  若要避免這些錯誤、請先移除租戶使用網格同盟連線的權限、再從此網格刪除租戶。

[[remove-grid 聯合連線權限 **]]** 移除使用網格同盟連線權限

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。



移除租戶使用網格同盟連線的權限之前、請注意下列事項：

- 如果任何租戶的貯體已啟用跨網格複寫、則無法移除 * 使用網格同盟連線 * 權限。租戶帳戶必須先停用所有貯體的跨網格複寫。
- 移除「 * 使用網格同盟連線 * 」權限、並不會刪除任何已在網格之間複寫的項目。例如、任何存在於兩個網格上的租戶使用者、群組和物件、都不會在移除租戶權限時從任一網格中刪除。如果要刪除這些項目、您必須手動從兩個方格中刪除它們。
- 如果您想要以相同的網格同盟連線重新啟用此權限、請先刪除目的地網格上的此租用戶、否則重新啟用此權限將會導致錯誤。

重新啟用「 * 使用網格同盟連線 * 」權限、可讓本機網格成為來源網格、並觸發複製至所選網格同盟連線所指定的遠端網格。如果遠端網格上已存在租戶帳戶、複製將會導致衝突錯誤。

開始之前

- 您使用的是 "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限" 適用於兩個網格。

停用租戶貯體的複寫

第一步是停用所有租戶貯體的跨網格複寫。

步驟

1. 從任一網格開始、從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取連線名稱以顯示其詳細資料。
4. 在 * 允許的租戶 * 索引標籤上、判斷租戶是否正在使用連線。

5. 如果列出租戶、請指示他們 "停用跨網格複寫" 適用於連線中兩個網格上的所有貯體。

> 如果任何租戶貯體已啟用跨網格複寫、則無法移除 * 使用網格同盟連線 * 權限。租戶必須在兩個網格上停用其儲存格的跨網格複寫。

移除租戶權限

停用租戶貯體的跨網格複寫之後、您可以移除租戶使用網格同盟連線的權限。

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 從「 Grid Federation 」頁面或「租戶」頁面移除權限。

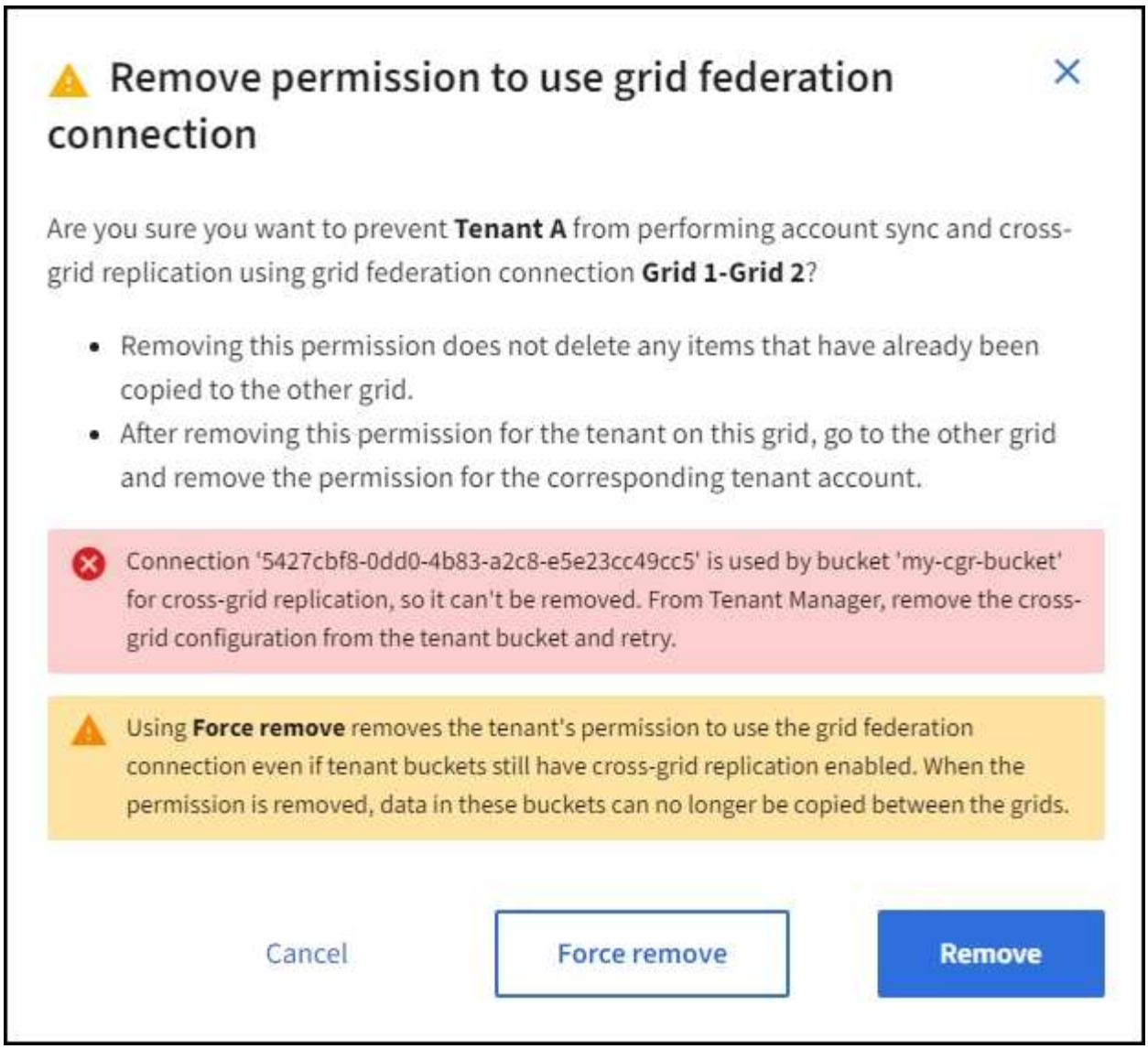
網格同盟頁面

a. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
b. 選取連線名稱以顯示其詳細資料頁面。
c. 在 * 允許的租戶 * 標籤上、選取租戶的選項按鈕。
d. 選取 * 移除權限 * 。

租戶頁面

a. 選取*租戶*。
b. 選取租戶名稱以顯示詳細資料頁面。
c. 在 * 網格聯盟 * 索引標籤上、選取連線的選項按鈕。
d. 選取 * 移除權限 * 。

3. 檢閱確認對話方塊中的警告、然後選取 * 移除 * 。
   - 如果權限可以移除、您會返回詳細資料頁面、並顯示成功訊息。此租用戶無法再使用網格同盟連線。
   - 如果一或多個租戶貯體仍啟用跨網格複寫、則會顯示錯誤。



您可以執行下列其中一項：

- （建議。） 登入租戶管理程式、並停用每個租戶桶的複寫功能。請參閱 "管理跨網格複寫"。然後重複步驟以移除 * 使用網格連線 * 權限。
- 強制移除權限。請參閱下一節。

4. 移至其他網格並重複這些步驟、以移除其他網格上相同租用戶的權限。

強制移除權限

如有必要、您可以強制移除租戶使用網格同盟連線的權限、即使租戶區已啟用跨網格複寫。

在強制移除租戶權限之前、請注意的一般考量事項 移除權限 以及以下額外考量：

- 如果您強制移除 * 使用網格同盟連線 * 權限、任何擱置複寫至其他網格（擷取但尚未複寫）的物件都會繼續複寫。若要防止這些處理中物件到達目的地貯體、您也必須移除其他網格上的租戶權限。
- 移除「 * 使用網格同盟連線 * 」權限之後、任何擷取到來源貯體的物件、將永遠不會複寫到目的地貯體。

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 選擇 * 組態 * > * 系統 * > * 網格聯盟 * 。
3. 選取連線名稱以顯示其詳細資料頁面。
4. 在 * 允許的租戶 * 標籤上、選取租戶的選項按鈕。
5. 選取 * 移除權限 * 。
6. 檢閱確認對話方塊中的警告、然後選取 * 強制移除 * 。

   隨即顯示成功訊息。此租用戶無法再使用網格同盟連線。

7. 視需要移至其他網格、然後重複這些步驟、強制移除其他網格上相同租戶帳戶的權限。例如、您應該在其他網格上重複這些步驟、以防止處理中的物件到達目的地儲存格。

疑難排解網格同盟錯誤

您可能需要疑難排解與網格同盟連線、帳戶複製和跨網格複寫相關的警示和錯誤。

[[grid-Federation 錯誤]] Grid 聯盟連線警示和錯誤

您可能會收到網格同盟連線的警示或錯誤。

在進行任何變更以解決連線問題之後、請測試連線、以確保連線狀態回到 * 已連線 * 。如需相關指示、請參閱 "管理網格同盟連線"。

Grid Federation 連線失敗警示

問題

觸發 * Grid Federation 連線失敗 * 警示。

詳細資料

此警示表示網格之間的網格同盟連線無法運作。

建議採取的行動

1. 檢閱網格同盟頁面上兩個網格的設定。確認所有值都正確無誤。請參閱 "管理網格同盟連線"。
2. 檢閱用於連線的憑證。請確定沒有過期網格同盟憑證的警示、而且每個憑證的詳細資料都是有效的。請參閱中的旋轉連線憑證指示 "管理網格同盟連線"。
3. 確認兩個網格中的所有管理節點和閘道節點均為線上且可供使用。解決可能影響這些節點的任何警示、然後再試一次。
4. 如果您為本機或遠端網格提供完整網域名稱（ FQDN ）、請確認 DNS 伺服器已連線且可供使用。請參閱 "什麼是網格同盟？" 適用於網路、 IP 位址和 DNS 需求。

Grid Federation 憑證警示過期

問題

觸發了 * 網格聯合憑證過期 * 警示。

詳細資料

此警示表示一或多個網格同盟憑證即將過期。

建議採取的行動

請參閱中的旋轉連線憑證指示 "管理網格同盟連線"。

編輯網格同盟連線時發生錯誤

問題

編輯網格同盟連線時、當您選取 * 儲存並測試 * 時、會看到下列警告訊息：「無法在一或多個節點上建立候選組態檔案。」

詳細資料

編輯網格同盟連線時、 StorageGRID 會嘗試在第一個網格上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至所有管理節點、例如管理節點離線、就會出現警告訊息。

建議採取的行動

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

帳戶複製錯誤

無法登入複製的租戶帳戶

問題

您無法登入複製的租戶帳戶。租戶管理程式登入頁面上的錯誤訊息是「您的此帳戶認證無效。請再試一次。 "

詳細資料

基於安全理由、當租戶帳戶從租戶的來源網格複製到租戶的目的地網格時、您為租戶的本機根使用者設定的密碼不會複製。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複製到目的地網格。

建議採取的行動

根使用者必須先由網格管理員登入租戶的目的地網格、才能登入租戶的目的地網格 "變更本機 root 使用者的密碼" 在目的地網格上。

複製的本機使用者必須先在目的地網格上新增使用者密碼、才能登入租戶的目的地網格。如需相關指示、請參閱 "管理本機使用者" 請參閱租戶管理程式的使用說明。

未建立複本的租戶

問題

在建立具有「 * 使用網格同盟連線 * 」權限的新租用戶之後、您會看到訊息「租戶建立時不含複製項目」。

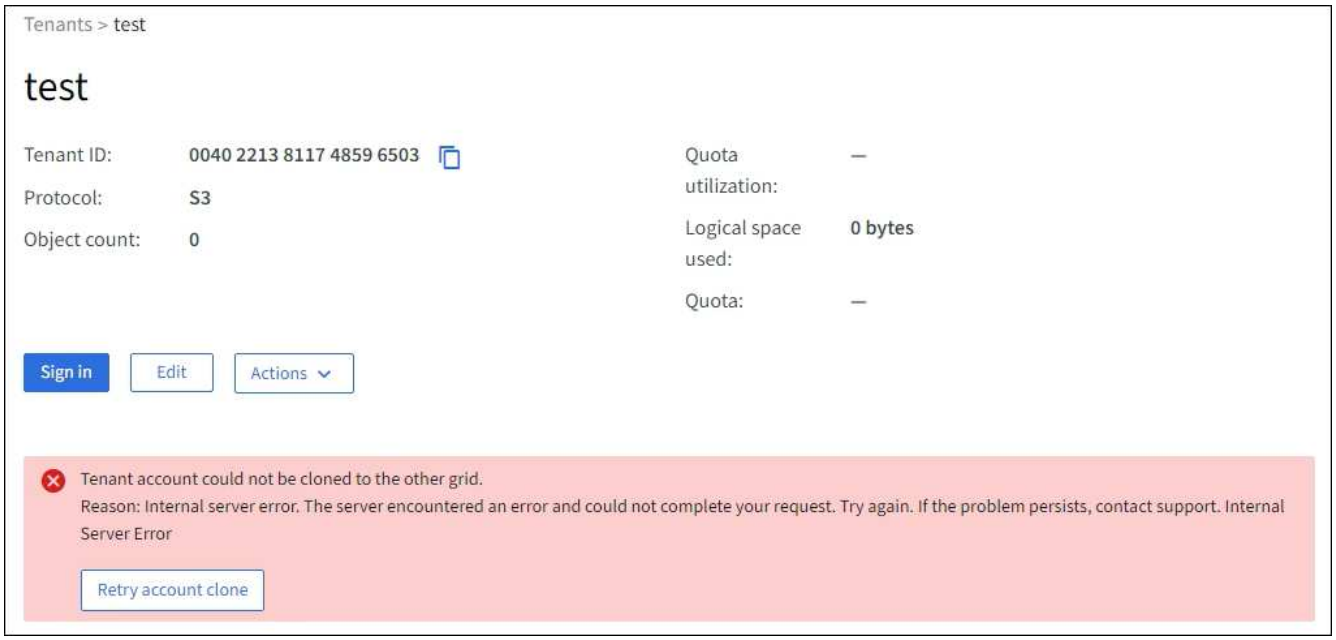
詳細資料

如果連線狀態的更新延遲、可能導致不良連線被列為 * 連線 * 、就會發生此問題。

建議採取的行動

1. 檢閱錯誤訊息中列出的原因、並解決可能導致連線無法正常運作的任何網路或其他問題。請參閱 Grid Federation 連線警示和錯誤。

2. 請依照指示在中測試網格同盟連線 "管理網格同盟連線" 確認問題已解決。
3. 從租戶的來源網格中、選取 * 租戶 * 。
4. 找出無法複製的租戶帳戶。
5. 選取租戶名稱以顯示詳細資料頁面。
6. 選擇 * 重試帳戶複製 * 。



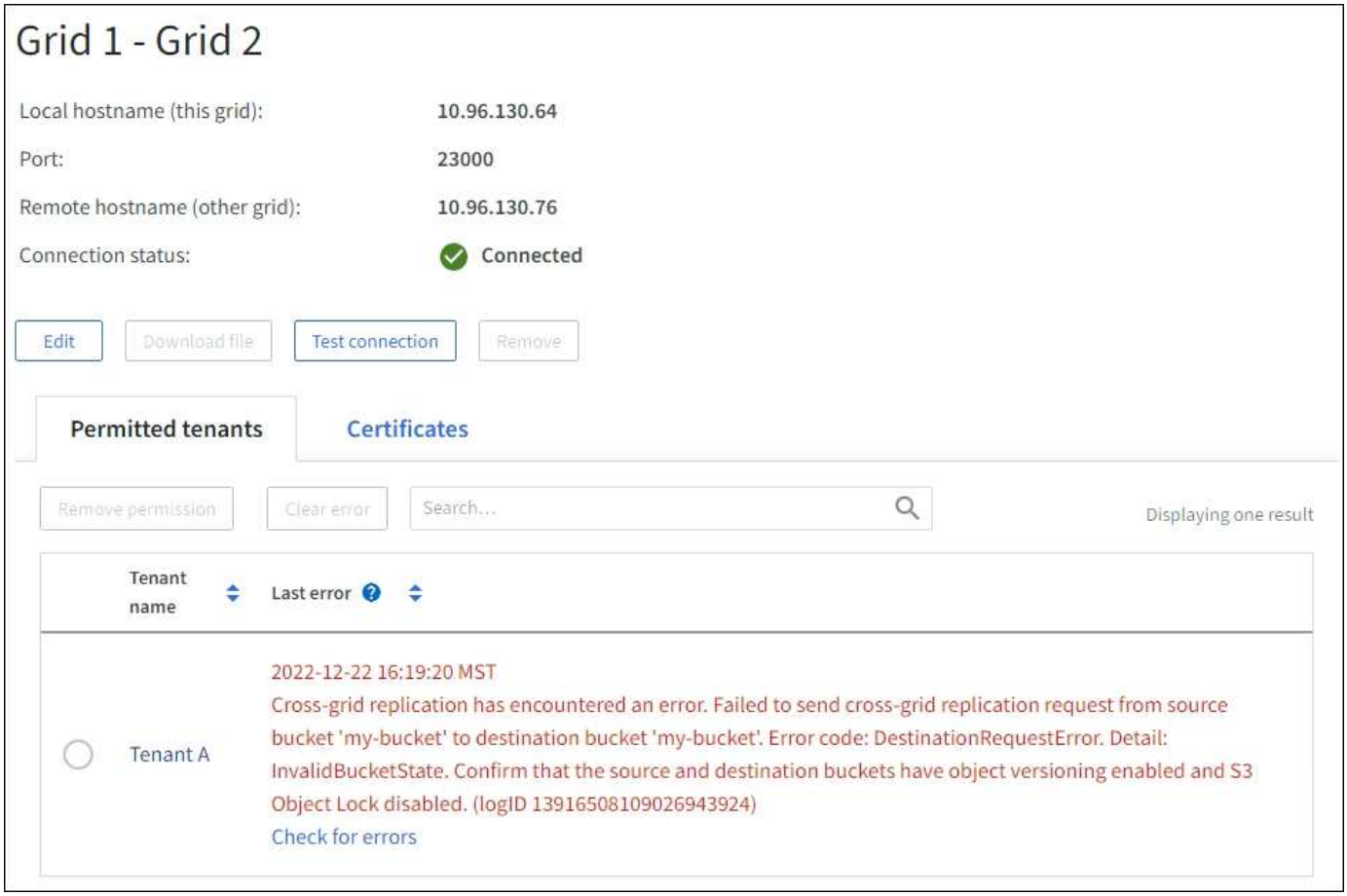
如果錯誤已解決、則租戶帳戶現在將會複製到其他網格。

跨網格複寫警示和錯誤

顯示連線或租戶的最後一個錯誤

問題

何時 "檢視網格同盟連線" （或是當 "管理允許的租戶" 對於連線）、您會在連線詳細資料頁面的 * 最後一個錯誤 * 欄中看到錯誤。例如：



詳細資料

對於每個網格同盟連線、 * 最後一個錯誤 * 欄會顯示租戶資料複寫到其他網格時發生的最新錯誤（如果有）。此欄只會顯示最後發生的跨網格複寫錯誤、不會顯示先前可能發生的錯誤。 此欄可能會因為下列其中一個原因而發生錯誤：

- 找不到來源物件版本。
- 找不到來源貯體。
- 目的地貯體已刪除。
- 目的地貯體是由不同的帳戶重新建立。
- 目的地貯體已暫停版本設定。
- 目的地貯體是由相同的帳戶重新建立、但現在已取消版本管理。

建議採取的行動

如果在 * 最後一個錯誤 * 欄中出現錯誤訊息、請遵循下列步驟：

1. 檢閱訊息文字。
2. 執行任何建議的動作。例如、如果目的地貯體上的版本設定已暫停進行跨網格複寫、請重新啟用該貯體的版本設定。
3. 從表格中選取連線或租戶帳戶。
4. 選取 * 清除錯誤 * 。

5. 選擇 * 是 * 以清除訊息並更新系統狀態。
6. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

   若要確保清除錯誤訊息、請在訊息中的時間戳記之後至少等待 5 分鐘、然後再擷取新物件。

   清除錯誤之後、如果物件被擷取到另一個儲存格中、而且發生錯誤、就可能會出現新的 * 最後一個錯誤 * 。

7. 若要判斷是否有任何物件因儲存區錯誤而無法複寫、請參閱 "識別並重試失敗的複寫作業"。

跨網格複寫永久故障警示

問題

觸發 * 跨網格複寫永久失敗 * 警示。

詳細資料

此警示表示租戶物件無法在兩個網格上的貯體之間複寫、原因是需要使用者介入才能解決。此警示通常是由來源或目的地貯體變更所造成。

建議採取的行動

1. 登入觸發警示的網格。
2. 移至 * 組態 * > * 系統 * > * 網格聯盟 * 、然後找出警示中列出的連線名稱。
3. 在「允許的租戶」標籤上、查看 * 最後一個錯誤 * 欄、以判斷哪些租戶帳戶有錯誤。
4. 若要深入瞭解故障、請參閱中的指示 "監控網格同盟連線" 檢閱跨網格複寫計量。
5. 對於每個受影響的租戶帳戶：
   a. 請參閱中的指示 "監控租戶活動" 確認租戶未超過目的地網格上的配額、以進行跨網格複寫。
   b. 視需要增加目標網格上的租戶配額、以允許儲存新物件。
6. 對於每個受影響的租戶、請在兩個網格上登入租戶管理器、以便比較貯體清單。
7. 針對已啟用跨網格複寫的每個貯體、請確認下列事項：
   - 另一個網格上有相同租戶的對應貯體（必須使用正確名稱）。
   - 兩個儲存格都已啟用物件版本設定（任一格線上都無法暫停版本設定）。
   - 兩個貯體都停用 S3 物件鎖定。
   - 兩個貯體都不處於 * 刪除物件：唯讀 * 狀態。
8. 若要確認問題已解決、請參閱中的指示 "監控網格同盟連線" 若要檢閱跨網格複寫計量、或執行下列步驟：
   a. 返回「 Grid Federation 」頁面。
   b. 選取受影響的租戶、然後在 * 上次錯誤 * 欄中選取 * 清除錯誤 * 。
   c. 選擇 * 是 * 以清除訊息並更新系統狀態。
   d. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

若要確保清除錯誤訊息、請在訊息中的時間戳記之後至少等待 5 分鐘、然後再擷取新物件。

警示解決後、可能需要一天的時間才能清除。

a. 前往 "識別並重試失敗的複寫作業" 識別無法複寫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

觸發 * 跨網格複寫資源 Unavailable * 警示。

詳細資料

此警示表示跨網格複寫要求因資源無法使用而擱置中。例如、可能發生網路錯誤。

建議採取的行動

1. 監控警示、查看問題是否自行解決。
2. 如果問題持續發生、請判斷網格是否有相同連線的 * 網格同盟連線失敗 * 警示、或是某個節點的 * 無法與節點 * 通訊警示。當您解決這些警示時、可能會解決此警示。
3. 若要深入瞭解故障、請參閱中的指示 "監控網格同盟連線" 檢閱跨網格複寫計量。
4. 如果您無法解決警示、請聯絡技術支援部門。

問題解決後、跨網格複寫將會正常進行。

識別並重試失敗的複寫作業

解決 *Cross-Grid 複寫永久性失敗 * 警示之後、您應該判斷是否有任何物件或刪除標記無法複寫到其他網格。接著您可以重新擷取這些物件、或使用 Grid Management API 來重試複寫。

「 *Cross-Grid 複寫永久失敗 * 」警示表示租戶物件無法在兩個網格上的貯體之間複寫、原因是需要使用者介入才能解決。此警示通常是由來源或目的地貯體變更所造成。如需詳細資訊、請參閱 "疑難排解網格同盟錯誤"。

判斷是否有任何物件無法複寫

若要判斷是否有任何物件或刪除標記尚未複寫到其他網格、您可以搜尋稽核記錄 "CGRR （跨網格複寫要求）" 訊息。當 StorageGRID 無法將物件、多個零件物件或刪除標記複寫至目的地儲存區時、此訊息會新增至記錄檔。

您可以使用 "稽核說明工具" 將結果轉換成更容易讀取的格式。

開始之前

- 您擁有root存取權限。
- 您擁有 `Passwords.txt` 檔案：
- 您知道主要管理節點的 IP 位址。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。

2. 在 audit.log 中搜尋 CGRR 訊息、並使用稽核說明工具來格式化結果。

   例如、此命令會在過去 30 分鐘內為所有 CGRR 訊息提供 Greps 、並使用稽核說明工具。

   ```
   # 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。在範例中、所有跨網格複寫要求都會傳回一般錯誤、因為物件無法複寫。前三個錯誤是用於「複寫物件」作業、最後三個錯誤是用於「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
```

每個項目都包含下列資訊：

欄位	說明
CGRR 跨網格複寫要求	要求的名稱
租戶	租戶的帳戶 ID
連線	網格同盟連線的 ID
營運	嘗試的複寫作業類型： • Replicate 物件 • 複寫刪除標記 • 複寫多個部分物件
鏟斗	貯體名稱
物件	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、則錯誤為「一般錯誤」。

重試失敗的複製

產生物件清單並刪除未複寫至目的地儲存區的標記、並解決基礎問題之後、您可以使用下列兩種方法重試複寫：

- 將每個物件重新擷取至來源貯體。
- 如所述、使用 Grid Management 私有 API 。

步驟

1. 從 Grid Manager 頂端選取說明圖示、然後選取 * API 文件 * 。
2. 選取 * 前往私有 API 文件 * 。

> ⓘ 標示為「私有」的 StorageGRID API 端點如有變更、恕不另行通知。私有端點也會忽略該要求的API版本。StorageGRID

3. 在 **Cross-GRID** 複寫 **- advanci** 區段中、選取下列端點：

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

4. 選擇*試用*。
5. 在 * 本文 * 文字方塊中、將 * 版本 ID* 的範例項目取代為 audit.log 的版本 ID 、該版本 ID 對應於失敗的跨網格複寫要求。

   請務必保留字串周圍的雙引號。

6. 選擇*執行*。
7. 確認伺服器回應碼為 **204** 、表示物件或刪除標記已標記為待定、以便跨網格複寫至其他網格。

   擱置表示已將跨網格複寫要求新增至內部佇列以進行處理。

監控複寫重試次數

您應該監控複寫重試作業、以確保其完成。

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久的時間。

您可以使用下列兩種方式來監控重試作業：

- 使用 S3 "標題物件" 或 "GetObject" 申請。回應包括 StorageGRID 專屬 `x-ntap-sg-cgr-replication-status` 回應標頭會有下列其中一個值：

網格	複寫狀態
來源	• * 成功 * ：複寫成功。 • * 擱置 * ：物件尚未複寫。 • * 失敗 * ：複寫失敗且持續失敗。使用者必須解決此錯誤。
目的地	• 複本 * ：物件已從來源網格複寫。

- 如所述、使用 Grid Management 私有 API 。

步驟

1. 在私有 API 文件的 * 跨網格複寫進階 * 區段中、選取下列端點：

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

2. 選擇*試用*。
3. 在「參數」區段中、輸入您在中使用的版本 ID `cross-grid-replication-retry-failed` 申請。
4. 選擇*執行*。
5. 確認伺服器回應碼為 **200** 。
6. 檢閱複寫狀態、這將是下列其中一項：
   - * 擱置 * ：物件尚未複寫。
   - * 已完成 * ：複寫成功。
   - * 失敗 * ：複寫失敗且永久失敗。使用者必須解決此錯誤。

管理安全性

管理安全性：總覽

您可以從Grid Manager設定各種安全性設定、以協助保護StorageGRID 您的作業系統。

管理加密

StorageGRID 提供數種加密資料的選項。您應該 "檢閱可用的加密方法" 判斷哪些符合您的資料保護需求。

管理憑證

您可以 "設定及管理伺服器憑證" 用於 HTTP 連線或用於驗證伺服器用戶端或使用者身分識別的用戶端憑證。

設定金鑰管理伺服器

使用 "金鑰管理伺服器" 即使從資料中心移除應用裝置、也能保護 StorageGRID 資料。應用裝置磁碟區加密後、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。

> 若要使用加密金鑰管理、您必須在安裝期間、在將應用裝置新增至網格之前、為每個應用裝置啟用*節點加密*設定。

管理**Proxy**設定

如果您使用的是 S3 平台服務或雲端儲存集區、則可以設定 "儲存 Proxy 伺服器" 儲存節點與外部 S3 端點之間的連接。如果您使用 HTTPS 或 HTTP 傳送 AutoSupport 套件、則可以設定 "管理 Proxy 伺服器" 管理節點與技術支援之間的關係。

控制防火牆

若要增強系統的安全性、您可以開啟或關閉的特定連接埠、以控制對 StorageGRID 管理節點的存取 "外部防火牆"。您也可以透過設定每個節點的網路存取控制 "內部防火牆"。您可以防止存取所有連接埠、但部署所需的連接埠除外。

檢閱**StorageGRID** 功能加密方法

StorageGRID 提供數種加密資料的選項。您應該檢閱可用的方法、以判斷哪些方法符合您的資料保護需求。

下表提供StorageGRID 有關支援的加密方法的高階摘要。

加密選項	運作方式	適用於
Grid Manager中的金鑰管理伺服器（KMS）	您 "設定金鑰管理伺服器" 適用於 StorageGRID 網站和 "啟用應用裝置的節點加密"。然後、應用裝置節點會連線至KMS、以要求金鑰加密金鑰（KEK）。此金鑰會加密及解密每個Volume上的資料加密金鑰（DEK）。	安裝期間啟用*節點加密*的應用裝置節點。應用裝置上的所有資料都能受到保護、避免資料中心的實體遺失或移除。 • 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。

加密選項	運作方式	適用於
StorageGRID 應用裝置安裝程式中的磁碟機加密頁面	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複雜密碼。當您設定磁碟機密碼時、除非任何人知道密碼短語、否則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、請移至 * 設定硬體 * > * 磁碟機加密 * 、設定適用於節點中所有 StorageGRID 管理的自我加密磁碟機的磁碟機密碼。	包含自我加密磁碟機的應用裝置。安全磁碟機上的所有資料都能受到保護、避免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。如果您的儲存設備具有自我加密磁碟機和 SANtricity 控制器、則可以在 SANtricity 中啟用磁碟機安全性。
在《支援資料保護系統》中提升安全性SANtricity	如果您的 StorageGRID 應用裝置已啟用磁碟機安全功能、您可以使用來 "系統管理程式SANtricity"建立及管理安全金鑰。存取受保護磁碟機上的資料需要金鑰。	具有全磁碟加密（ FDE ）磁碟機或自我加密磁碟機的儲存設備。安全磁碟機上的所有資料都能受到保護、避免實體遺失或從資料中心移除。無法與某些儲存設備或任何服務應用裝置搭配使用。
儲存的物件加密	您可以啟用 "儲存的物件加密" Grid Manager 中的選項。啟用時、在貯體層級或物件層級未加密的任何新物件、都會在擷取期間加密。	新擷取的S3和Swift物件資料。 現有儲存的物件不會加密。物件中繼資料和其他敏感資料不會加密。
S3儲存區加密	您發出 PuttBucketEncryption 要求、以啟用貯體的加密。在物件層級未加密的任何新物件、都會在擷取期間加密。	僅限新擷取的S3物件資料。 必須為儲存區指定加密。現有的貯體物件不會加密。物件中繼資料和其他敏感資料不會加密。 "在貯體上作業"
S3物件伺服器端加密（SSe）	您發出S3要求來儲存物件並納入 `x-amz-server-side-encryption` 要求標頭：	僅限新擷取的S3物件資料。 必須為物件指定加密。物件中繼資料和其他敏感資料不會加密。 可管理金鑰。StorageGRID "使用伺服器端加密"

加密選項	運作方式	適用於
S3物件伺服器端加密、使用客戶提供的金鑰（SSE-C）	您發出S3要求以儲存物件、並包含三個要求標頭。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	僅限新擷取的S3物件資料。 必須為物件指定加密。物件中繼資料和其他敏感資料不會加密。 金鑰是在StorageGRID 非功能性的範圍內管理。 "使用伺服器端加密"
外部Volume或資料存放區加密	如果StorageGRID 您的部署平台支援、您可以使用不屬於支援的加密方法來加密整個磁碟區或資料存放區。	所有物件資料、中繼資料和系統組態資料、假設每個磁碟區或資料存放區都已加密。 外部加密方法可更嚴密地控制加密演算法和金鑰。可與其他列出的方法結合使用。
物件加密不StorageGRID 包括在內	您可以在StorageGRID 物件資料和中繼資料被擷取到StorageGRID 資料之前、使用非功能性的加密方法來加密物件資料和中繼資料。	僅限物件資料和中繼資料（系統組態資料未加密）。 外部加密方法可更嚴密地控制加密演算法和金鑰。可與其他列出的方法結合使用。 "Amazon Simple Storage Service - 開發人員指南：使用用戶端加密來保護資料"

使用多種加密方法

視您的需求而定、您一次可以使用多種加密方法。例如：

- 您可以使用 KMS 來保護應用裝置節點、也可以使用 SANtricity 系統管理員中的磁碟機安全功能、在同一個應用裝置中的自我加密磁碟機上「雙重加密」資料。
- 您可以使用 KMS 來保護應用裝置節點上的資料、也可以使用儲存的物件加密選項來加密擷取的所有物件。

如果只有一小部分物件需要加密、請考慮改為在儲存區或個別物件層級控制加密。啟用多層加密會增加效能成本。

管理憑證

管理安全性憑證：總覽

安全證書是小型資料檔案、用於在StorageGRID 各個元件之間、StorageGRID 以及在各個

元件與外部系統之間建立安全且值得信賴的連線。

使用兩種類型的安全性憑證：StorageGRID

- 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、驗證伺服器的用戶端身分、並提供安全的資料通訊路徑。伺服器和用戶端各有一份憑證複本。
- *用戶端憑證*驗證伺服器的用戶端或使用者身分、提供比僅密碼更安全的驗證。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、伺服器會以含有公開金鑰的伺服器憑證回應。用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端會使用相同的公開金鑰啟動與伺服器的工作階段。

充當某些連線（例如負載平衡器端點）的伺服器、或作為其他連線（例如CloudMirror複寫服務）的用戶端。StorageGRID

預設**Grid CA**憑證

包含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。StorageGRID根據預設、Grid CA憑證用於保護內部StorageGRID 的不穩定流量。外部憑證授權單位（CA）可核發完全符合組織資訊安全原則的自訂憑證。雖然您可以將Grid CA憑證用於非正式作業環境、但正式作業環境的最佳做法是使用外部憑證授權單位所簽署的自訂憑證。也支援不含憑證的不安全連線、但不建議這麼做。

- 自訂 CA 憑證不會移除內部憑證；不過，自訂憑證應該是指定用於驗證伺服器連線的憑證。
- 所有自訂憑證都必須符合 "伺服器憑證的系統強化準則"。
- 支援將CA的憑證整合至單一檔案（稱為CA憑證套件）StorageGRID 。

> 此外、還包括所有網格上相同的作業系統CA憑證。StorageGRID在正式作業環境中、請務必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。

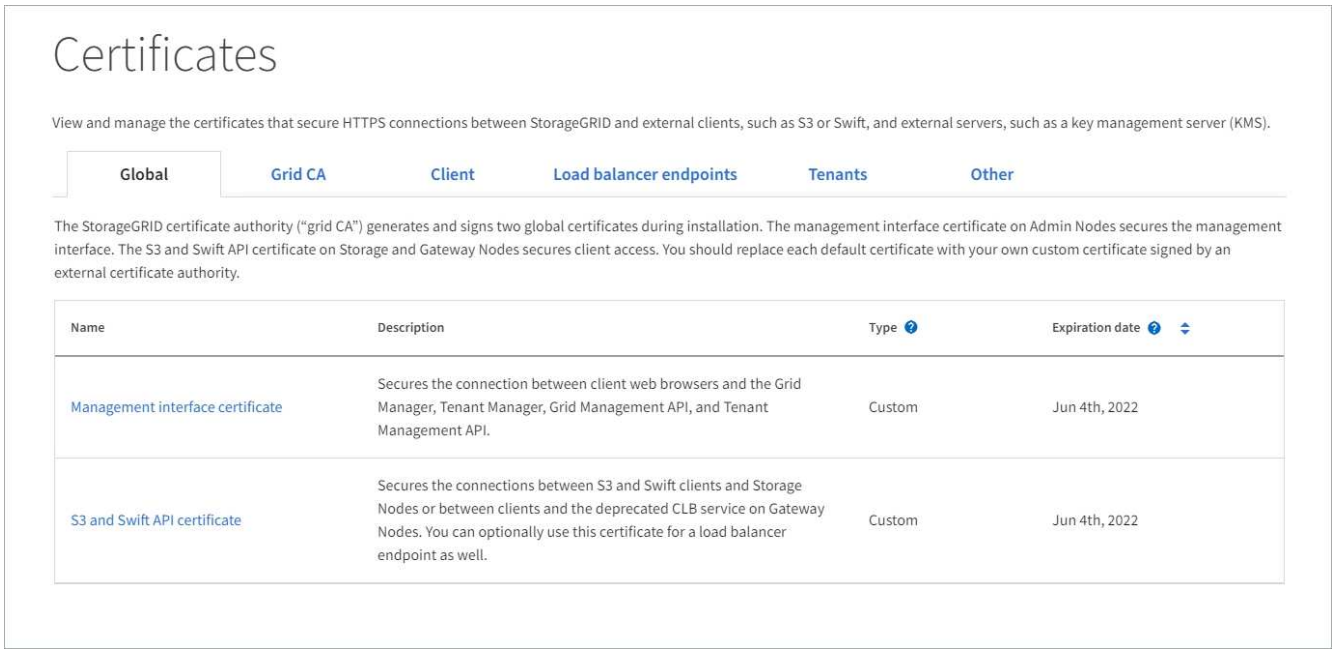
伺服器和用戶端憑證類型的變種會以多種方式實作。在設定系統之前、您應該StorageGRID 準備好特定的支援功能組態所需的所有憑證。

存取安全性憑證

您可以在StorageGRID 單一位置存取所有的資訊、以及每個憑證的組態工作流程連結。

步驟

1. 從 Grid Manager 中、選取 * 組態 * > * 安全性 * > * 憑證 * 。



2. 選取「憑證」頁面上的索引標籤、以取得每個憑證類別的相關資訊、並存取憑證設定。如果您有、可以存取索引標籤 "適當的權限"。

   - 全球：保護StorageGRID 從網頁瀏覽器和外部API用戶端進行的不受限存取。
   - * Grid CA*：保護內部StorageGRID 的不安全流量。
   - 用戶端：保護外部用戶端與StorageGRID 《The S動estetheus資料庫》之間的連線。
   - 負載平衡器端點：保護S3和Swift用戶端與StorageGRID 「平衡負載平衡器」之間的連線。
   - 租戶：保護連線至身分識別聯盟伺服器、或從平台服務端點到S3儲存資源的安全。
   - 其他：保護StorageGRID 需要特定憑證的不實連線。

每個索引標籤都會在下方說明、並提供其他憑證詳細資料的連結。

全域

全域認證可從StorageGRID 網頁瀏覽器、外部S3和Swift API用戶端安全地進行不受限的存取。安裝期間、由版本資訊驗證機構產生兩個全域憑證StorageGRID 。正式作業環境的最佳實務做法是使用外部憑證授權單位簽署的自訂憑證。

- [管理介面認證]：保護用戶端網路瀏覽器與StorageGRID 功能完善的管理介面的連線。
- S3和Swift API認證：保護用戶端API連線至儲存節點、管理節點和閘道節點的安全、S3和Swift用戶端應用程式可用來上傳和下載物件資料。

安裝的全域憑證相關資訊包括：

- 名稱：憑證名稱、含管理憑證的連結。
- 說明
- 類型：自訂或預設。+ 您應該一律使用自訂憑證來改善網格安全性。
- 到期日：如果使用預設憑證、則不會顯示到期日。

您可以：

- 使用外部憑證授權單位簽署的自訂憑證來取代預設憑證、以改善網格安全性：
  - "取代預設StorageGRID產生的管理介面憑證" 用於Grid Manager和Tenant Manager連線。
  - "更換S3和Swift API認證" 用於儲存節點和負載平衡器端點（選用）連線。
- "還原預設的管理介面憑證。"
- "還原預設的S3和Swift API憑證。"
- "使用指令碼來產生新的自我簽署管理介面憑證。"
- 複製或下載 "管理介面認證" 或 "S3和Swift API認證"。

網格**CA**

。 Grid CA憑證由安裝過程中的驗證機關所產生、StorageGRID 可保護所有內部的資訊流量。StorageGRID StorageGRID

憑證資訊包括憑證到期日和憑證內容。

您可以 "複製或下載 Grid CA 憑證"但您無法加以變更。

用戶端

用戶端憑證由外部憑證授權單位所產生、可確保外部監控工具與StorageGRID VMware資料庫之間的連線安全無虞。

憑證表格中有一列用於每個已設定的用戶端憑證、並指出該憑證是否可用於Prometheus資料庫存取、以及憑證到期日。

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：

- "變更用戶端憑證名稱。"
- "設定Prometheus存取權限。"
- "上傳並取代用戶端憑證。"
- "複製或下載用戶端憑證。"
- "移除用戶端憑證。"

- 選取*「動作」即可快速執行 "編輯"、 "附加"或 "移除" 用戶端憑證。您最多可以選取**10**個用戶端憑證、並使用「動作*」>「移除」一次移除這些憑證。

負載平衡器端點

負載平衡器端點憑證 保護 S3 和 Swift 用戶端之間的連線、以及閘道節點和管理節點上的 StorageGRID 負載平衡器服務。

負載平衡器端點表針對每個已設定的負載平衡器端點都有一列、可指出端點是使用全域S3和Swift API憑證、還是使用自訂負載平衡器端點憑證。也會顯示每個憑證的到期日。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

您可以：

- "檢視負載平衡器端點"，包括其憑證詳細資料。
- "指定要FabricPool 使用的負載平衡器端點憑證。"
- "使用全域S3和Swift API認證" 而非產生新的負載平衡器端點憑證。

租戶

租戶可以使用 身分識別聯盟伺服器憑證 或 平台服務端點憑證 使用StorageGRID NetApp保護連線安全。

租戶表格會針對每個租戶顯示一列、並指出每個租戶是否有權使用自己的身分識別來源或平台服務。

您可以：

- "選取要登入租戶管理程式的租戶名稱"
- "選取租戶名稱以檢視租戶身分識別聯盟詳細資料"
- "選取租戶名稱以檢視租戶平台服務詳細資料"
- "在端點建立期間指定平台服務端點憑證"

其他

針對特定用途使用其他安全性憑證。StorageGRID這些憑證會依其功能名稱列出。其他安全性憑證包括：

- 雲端儲存資源池認證
- 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
- 身分識別聯盟憑證

- 金鑰管理伺服器（KMS）憑證
- 單一登入憑證

資訊指出功能使用的憑證類型、以及適用的伺服器和用戶端憑證到期日。選取功能名稱會開啟瀏覽器索引標籤、您可以在其中檢視及編輯憑證詳細資料。

您只能檢視和存取其他憑證的資訊（如果您有）"適當的權限"。

您可以：

- "指定S3、C2S S3或Azure的雲端儲存池憑證"
- "指定警示電子郵件通知的憑證"
- "使用外部 Syslog 伺服器的憑證"
- "旋轉網格同盟連線憑證"
- "檢視及編輯身分識別聯盟憑證"
- "上傳金鑰管理伺服器（KMS）伺服器和用戶端憑證"
- "手動指定依賴方信任的 SSO 憑證"

安全性憑證詳細資料

每種安全性憑證類型如下所述、並提供實作指示的連結。

管理介面認證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證用戶端網頁瀏覽器與StorageGRID RealSet管理介面之間的連線、讓使用者能夠存取Grid Manager和Tenant Manager、而不會出現安全性警告。 此憑證也會驗證Grid Management API和租戶管理API連線。 您可以使用安裝期間建立的預設憑證、或是上傳自訂憑證。	組態>*安全性*>*憑證*、選取*全域*索引標籤、然後選取*管理介面憑證*	"設定管理介面憑證"

S3和Swift API認證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證安全的 S3 或 Swift 用戶端連線至儲存節點和負載平衡器端點（選用）。	組態>*安全性*>*憑證*、選取*全域*索引標籤、然後選取* S3和Swift API憑證*	"設定S3和Swift API憑證"

Grid CA憑證

請參閱 預設Grid CA憑證說明。

系統管理員用戶端憑證

憑證類型	說明	導覽位置	詳細資料
用戶端	安裝在每個用戶端上、StorageGRID 讓功能驗證外部用戶端存取。 • 允許授權的外部用戶端存取StorageGRID《The WilsPrometheus資料庫》。 • 允許StorageGRID 使用外部工具安全監控功能。	組態>*安全性*>*憑證*、然後選取*用戶端*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	導覽位置	詳細資料
伺服器	驗證S3或Swift用戶端之間的連線、StorageGRID 以及閘道節點和管理節點上的「RealsLoad Balancer」服務。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StorageGRID 至物件資料時、會使用負載平衡器憑證來儲存及擷取物件資料。 您也可以使用全域的自訂版本 S3和Swift API認證 用於驗證負載平衡器服務連線的憑證。如果使用全域憑證來驗證負載平衡器連線、您就不需要為每個負載平衡器端點上傳或產生個別的憑證。 *附註：*用於負載平衡器驗證的憑證、是正常StorageGRID 執行過程中最常使用的憑證。	組態>*網路*>*負載平衡器端點*	• "設定負載平衡器端點" • "建立FabricPool 負載平衡器端點以供使用"

雲端儲存資源池端點憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證StorageGRID 從Ss3 Glacier或Microsoft Azure Blob儲存設備等外部儲存位置的連接。每種雲端供應商類型都需要不同的憑證。	• ILM >*儲存資源池	"建立雲端儲存資源池"

電子郵件警示通知憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證用於StorageGRID 警示通知的SMTP電子郵件伺服器與功能鏈之間的連線。 • 如果與SMTP伺服器的通訊需要傳輸層安全性（TLS）、您必須指定電子郵件伺服器CA憑證。 • 只有在SMTP電子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。	警示>*電子郵件設定*	"設定警示的電子郵件通知"

外部**syslog**伺服器憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證外部syslog伺服器之間的TLS或RELP/TLS連線、該伺服器會將事件記錄StorageGRID 在整個過程中。 *附註：*不需要外部系統記錄伺服器憑證、就能連接到外部系統記錄伺服器的TCP、RELP/TCP及udp連線。	• 組態 * > * 監控 * > * 稽核與系統記錄伺服器 *	"使用外部syslog伺服器"

[[grid-Federation 認證 **]] Grid** 聯盟連線憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證並加密目前StorageGRID 系統與網格同盟連線中其他網格之間傳送的資訊。	• 組態 * > * 系統 * > * 網格聯盟 *	• "建立網格同盟連線" • "旋轉連線憑證"

身分識別聯盟憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證StorageGRID Reality與外部身分識別供應商（例如Active Directory、OpenLDAP或Oracle Directory Server）之間的連線。用於身分識別聯盟、可讓管理員群組和使用者由外部系統管理。	組態>*存取控制*>*身分識別聯盟*	"使用身分識別聯盟"

金鑰管理伺服器（**KMS**）憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證StorageGRID 支援功能與外部金鑰管理伺服器（KMS）之間的連線、此伺服器可為StorageGRID 應用裝置節點提供加密金鑰。	組態>*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	導覽位置	詳細資料
伺服器	驗證StorageGRID 從SReals功能 平台服務到S3儲存資源的連線。	租戶管理程式>*儲存設備（S3）>*平台服務端點	"建立平台服務端點" "編輯平台服務端點"

單一登入（**SSO**）憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證身分識別聯盟服務（例如Active Directory Federation Services（AD FS））和StorageGRID 用來處理單一登入（SSO）要求的支援服務之間的連線。	組態>*存取控制*>*單一登入*	"設定單一登入"

憑證範例

範例**1**：負載平衡器服務

在此範例中StorageGRID 、用作伺服器的是功能。

1. 您可以設定負載平衡器端點、並在StorageGRID 中上傳或產生伺服器憑證。

2. 您可以設定S3或Swift用戶端連線至負載平衡器端點、然後將相同的憑證上傳至用戶端。
3. 當用戶端想要儲存或擷取資料時、會使用HTTPS連線至負載平衡器端點。
4. 以伺服器憑證做出回應、其中包含公開金鑰、並以私密金鑰為基礎提供簽名。StorageGRID
5. 用戶端會將伺服器簽章與憑證複本上的簽章進行比較、藉此驗證此憑證。如果簽名相符、用戶端就會使用相同的公開金鑰來啟動工作階段。
6. 用戶端會將物件資料傳送StorageGRID 至物件資料。

範例**2**：外部金鑰管理伺服器（**KMS**）

在此範例中StorageGRID 、由客戶扮演的角色就是

1. 使用外部金鑰管理伺服器軟體、您可以將StorageGRID 效能設定為KMS用戶端、並取得CA簽署的伺服器憑證、公用用戶端憑證及用戶端憑證的私密金鑰。
2. 您可以使用Grid Manager設定KMS伺服器、並上傳伺服器和用戶端憑證及用戶端私密金鑰。
3. 當某個節點需要加密金鑰時、它會向KMS伺服器提出要求、要求其中包含來自憑證的資料、以及以私密金鑰為基礎的簽名。StorageGRID
4. KMS伺服器會驗證憑證簽章、並決定其是否值得信賴StorageGRID 。
5. KMS伺服器會使用已驗證的連線來回應。

設定伺服器憑證

支援的伺服器憑證類型

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

安全性原則的加密類型必須符合伺服器憑證類型。例如、 RSA 加密器需要 RSA 憑證、而 ECDSA 加密器則需要 ECDSA 憑證。請參閱 "管理安全性憑證"。如果您設定的自訂安全性原則與伺服器憑證不相容、您可以 "暫時恢復為預設的安全性原則"。

如需 StorageGRID 如何保護用戶端連線的詳細資訊、請參閱 "S3 和 Swift 用戶端的安全性"。

設定管理介面憑證

您可以使用單一自訂憑證來取代預設的管理介面憑證、讓使用者能夠存取Grid Manager和租戶管理程式、而不會遇到安全性警告。您也可以還原為預設的管理介面憑證、或是產生新的憑證。

關於這項工作

根據預設、每個管理節點都會核發由網格CA簽署的憑證。這些CA簽署的憑證可由單一通用的自訂管理介面憑證和對應的私密金鑰取代。

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、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有管理節點。

您需要在伺服器上完成組態、視您使用的根憑證授權單位（CA）而定、使用者可能也需要在網頁瀏覽器中安裝Grid CA憑證、以便存取Grid Manager和租戶管理程式。

為了確保作業不會因伺服器憑證故障而中斷、當此伺服器憑證即將過期時、就會觸發 * 管理介面伺服器憑證過期 * 警示。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「全域」索引標籤上查看管理介面憑證的到期日。

如果您使用網域名稱而非IP位址來存取Grid Manager或Tenant Manager、則瀏覽器會顯示憑證錯誤、且在發生下列任一情況時、不會出現跳過的選項：

- 您的自訂管理介面憑證將過期。
- 您 從自訂管理介面憑證還原為預設伺服器憑證。

新增自訂管理介面認證

若要新增自訂管理介面認證、您可以提供自己的認證、或使用Grid Manager產生認證。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生憑證。

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC 私密金鑰必須大於 224 位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位（CA）的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 展開*憑證詳細資料*、即可查看您上傳之每個憑證的中繼資料。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇*保存*。+ 自訂管理介面憑證用於所有後續的 Grid Manager 、 Tenant Manager 、 Grid Manager API 或 Tenant Manager API 連線。

產生憑證

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*產生憑證*。

b. 指定憑證資訊：

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*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。

欄位	說明
有效天數	憑證建立後過期的天數。
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取 * 憑證詳細資料 * 以查看所產生憑證的中繼資料。

- 選取*下載憑證*以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。+ 自訂管理介面憑證用於所有後續的 Grid Manager 、 Tenant Manager 、 Grid Manager API 或 Tenant Manager API 連線。

5. 重新整理頁面以確保網頁瀏覽器已更新。

> 上傳或產生新的憑證後、請允許清除任何相關的憑證過期警示一天。

6. 新增自訂管理介面憑證之後、「管理介面憑證」頁面會顯示使用中憑證的詳細憑證資訊。+ 您可以視需要下載或複製憑證 PEM 。

還原預設的管理介面憑證

您可以恢復使用Grid Manager和Tenant Manager連線的預設管理介面憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選擇*使用預設憑證*。

   當您還原預設的管理介面憑證時、您設定的自訂伺服器憑證檔案會被刪除、而且無法從系統中還原。預設的管理介面憑證會用於所有後續的新用戶端連線。

4. 重新整理頁面以確保網頁瀏覽器已更新。

使用指令碼來產生新的自我簽署管理介面憑證

如果需要嚴格的主機名稱驗證、您可以使用指令碼來產生管理介面憑證。

開始之前

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

關於這項工作

正式作業環境的最佳實務做法是使用外部憑證授權單位所簽署的憑證。

步驟

1. 取得每個管理節點的完整網域名稱（FQDN）。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

   當您以root登入時、提示會從變更 `$` 至 `#`。
3. 使用StorageGRID 新的自我簽署憑證來設定功能。

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

   - 適用於 `--domains`、使用萬用字元代表所有管理節點的完整網域名稱。例如、 `*.ui.storagegrid.example.com` 使用*萬用字元表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 至 `management` 設定 Grid Manager 和 Tenant Manager 使用的管理介面憑證。
   - 根據預設、產生的憑證有效期間為一年（365天）、必須在到期前重新建立。您可以使用 `--days` 用於置換預設有效期間的引數。

     > 憑證的有效期間始於何時 `make-certificate` 執行。您必須確保管理用戶端與StorageGRID 其他來源同步、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
     ```

     產生的輸出包含管理API用戶端所需的公開憑證。
4. 選取並複製憑證。

   在您的選擇中加入開始標記和結束標記。

5. 登出命令Shell。 `$ exit`
6. 確認已設定憑證：
   a. 存取Grid Manager。
   b. 選擇*組態*>*安全性*>*憑證*
   c. 在* Global*索引標籤上、選取*管理介面認證*。
7. 設定管理用戶端使用您複製的公用憑證。包括開始和結束標記。

下載或複製管理介面憑證

您可以儲存或複製管理介面憑證內容、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選取「伺服器」或「* CA套裝組合*」索引標籤、然後下載或複製憑證。

下載憑證檔案或**CA**套裝組合

下載憑證或 CA 套件 `.pem` 檔案：如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*下載憑證*或*下載CA套裝組合*。

   如果您要下載CA套件、CA套件次要索引標籤中的所有憑證都會以單一檔案下載。

b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或**CA**套裝組合**PEE**

複製憑證文字以貼到其他位置。如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

   如果您要複製CA套件組合、CA套件中的所有憑證都會一起複製二線索引標籤。

b. 將複製的憑證貼到文字編輯器中。
c. 以副檔名儲存文字檔 `.pem`。

   例如： `storagegrid_certificate.pem`

您可以取代或還原用於 S3 或 Swift 用戶端連線至儲存節點或負載平衡器端點的伺服器憑證。置換的自訂伺服器憑證是您組織專屬的。

關於這項工作

根據預設、每個儲存節點都會核發由網格CA簽署的X．509伺服器憑證。這些CA簽署的憑證可由單一通用的自訂伺服器憑證和對應的私密金鑰取代。

所有儲存節點都使用單一自訂伺服器憑證、因此如果用戶端在連線至儲存端點時需要驗證主機名稱、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有儲存節點。

在伺服器上完成組態之後、您可能還需要在S3或Swift API用戶端中安裝Grid CA憑證、以便根據所使用的根憑證授權單位（CA）來存取系統。

> 為了確保作業不會因伺服器憑證故障而中斷、當根伺服器憑證即將過期時、會觸發 S3 和 Swift API* 的 * 全域伺服器憑證過期。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「全域」索引標籤上查看S3和Swift API憑證的到期日。

您可以上傳或產生自訂的S3和Swift API認證。

新增自訂S3和Swift API認證

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選擇*使用自訂憑證*。
4. 上傳或產生憑證。

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（PEM編碼）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC 私密金鑰必須大於 224 位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 選取憑證詳細資料、以顯示上傳之每個自訂S3和Swift API憑證的中繼資料和PEM。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇*保存*。

   自訂伺服器憑證用於後續的S3和Swift用戶端連線。

產生憑證

產生伺服器憑證檔案。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

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*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。
有效天數	憑證建立後過期的天數。

欄位	說明
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*「憑證詳細資料」*以顯示所產生之自訂S3和Swift API憑證的中繼資料和PEM。

- 選取*下載憑證*以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。

自訂伺服器憑證用於後續的S3和Swift用戶端連線。

5. 選取索引標籤以顯示預設StorageGRID 的還原伺服器憑證的中繼資料、已上傳的CA簽署憑證、或是已產生的自訂憑證。

   上傳或產生新的憑證後、請允許清除任何相關的憑證過期警示一天。

6. 重新整理頁面以確保網頁瀏覽器已更新。

7. 新增自訂S3和Swift API憑證之後、S3和Swift API憑證頁面會顯示使用中自訂S3和Swift API憑證的詳細憑證資訊。+ 您可以視需要下載或複製憑證 PEM 。

還原預設的**S3**和**Swift API**憑證

您可以將 S3 和 Swift 用戶端連線的預設 S3 和 Swift API 憑證還原成儲存節點。不過、您無法將預設的 S3 和 Swift API 憑證用於負載平衡器端點。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選擇*使用預設憑證*。

   當您還原全域 S3 和 Swift API 憑證的預設版本時、您所設定的自訂伺服器憑證檔案會遭到刪除、而且無法從系統中還原。預設的 S3 和 Swift API 憑證將用於後續新的 S3 和 Swift 用戶端連線至儲存節點。

4. 選取*確定*以確認警告並還原預設的S3和Swift API憑證。

如果您具有根存取權限、而且自訂S3和Swift API憑證已用於負載平衡器端點連線、則會顯示負載平衡器端點清單、無法再使用預設S3和Swift API憑證存取。前往 "設定負載平衡器端點" 可編輯或刪除受影響的端點。

5. 重新整理頁面以確保網頁瀏覽器已更新。

下載或複製**S3**和**Swift API**認證

您可以儲存或複製S3和Swift API憑證內容、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*。
2. 在* Global*索引標籤上、選取* S3和Swift API認證*。
3. 選取「伺服器」或「* CA套裝組合*」索引標籤、然後下載或複製憑證。

下載憑證檔案或**CA**套裝組合

下載憑證或 CA 套件 `.pem` 檔案：如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*下載憑證*或*下載CA套裝組合*。

   如果您要下載CA套件、CA套件次要索引標籤中的所有憑證都會以單一檔案下載。

b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或**CA**套裝組合**PEE**

複製憑證文字以貼到其他位置。如果您使用選用的CA套件組合、套件中的每個憑證都會顯示在其各自的子索引標籤上。

a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

   如果您要複製CA套件組合、CA套件中的所有憑證都會一起複製二線索引標籤。

b. 將複製的憑證貼到文字編輯器中。

c. 以副檔名儲存文字檔 `.pem`。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用S3 REST API"
- "使用Swift REST API"
- "設定 S3 端點網域名稱"

複製Grid CA憑證

使用內部憑證授權單位（CA）來保護內部流量。StorageGRID如果您上傳自己的憑證、此憑證不會變更。

開始之前

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

關於這項工作

如果已設定自訂伺服器憑證、用戶端應用程式應使用自訂伺服器憑證來驗證伺服器。他們不應該從StorageGRID這個系統複製CA憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選取*網格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. 選擇*下載憑證*。
   b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製憑證PE

   複製憑證文字以貼到其他位置。

   a. 選擇*複製憑證PEP*。
   b. 將複製的憑證貼到文字編輯器中。
   c. 以副檔名儲存文字檔 `.pem`。

      例如： `storagegrid_certificate.pem`

設定StorageGRID 適用FabricPool 的驗證

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"。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。

關於這項工作

建立負載平衡器端點時、您可以產生自我簽署的伺服器憑證、或是上傳由已知憑證授權單位（CA）簽署的憑證。在正式作業環境中、您應該使用由已知CA簽署的憑證。由CA簽署的憑證可在不中斷營運的情況下循環。它們也更安全、因為它們能更有效地防範攔截式攻擊。

下列步驟為使用FabricPool 支援功能的S3用戶端提供一般準則。如需詳細資訊和程序、請參閱 "設定StorageGRID 適用於FabricPool 靜態的"。

步驟

1. 或者、設定高可用度（HA）群組FabricPool 以供使用。
2. 建立S3負載平衡器端點FabricPool 以供使用。

   當您建立HTTPS負載平衡器端點時、系統會提示您上傳伺服器憑證、憑證私密金鑰及選用的CA套件組合。

3. 在StorageGRID 整個過程中附加作雲端層的功能。ONTAP

   指定負載平衡器端點連接埠、以及您上傳的CA憑證所使用的完整網域名稱。然後提供CA憑證。

   如果中介CA核發StorageGRID 了此資訊證書、您必須提供中繼CA憑證。如果StorageGRID 此驗證是由根CA直接發出、您必須提供根CA憑證。

設定用戶端憑證

用戶端憑證可讓獲授權的外部用戶端存取StorageGRID 《The》《The VMware資料庫》、為外部工具提供安全的監控StorageGRID 方式。

如果您需要StorageGRID 使用外部監控工具存取功能、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。

請參閱 "管理安全性憑證" 和 "設定自訂伺服器憑證"。

為了確保作業不會因伺服器憑證故障而中斷、當此伺服器憑證即將過期時、會觸發「憑證頁面 * 」警示上設定的 * 用戶端憑證到期日。如有需要、您可以選取*組態*>*安全性*>*憑證*來檢視目前憑證的到期日、並在「用戶端」索引標籤上查看用戶端憑證的到期日。

如果您使用金鑰管理伺服器（KMS）來保護特殊設定應用裝置節點上的資料、請參閱相關的特定資訊 "上傳KMS用戶端憑證"。

開始之前

- 您擁有root存取權限。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 若要設定用戶端憑證：
  - 您擁有管理節點的IP位址或網域名稱。
  - 如果您已設定StorageGRID 完整套管理介面認證、則會使用CA、用戶端認證和私密金鑰來設定管理介面認證。
  - 若要上傳您自己的憑證、您可以在本機電腦上取得該憑證的私密金鑰。

- 私密金鑰必須在建立時已儲存或記錄。如果您沒有原始的私密金鑰、則必須建立新的私密金鑰。

- 若要編輯用戶端憑證：
  - 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的憑證、您的本機電腦上可以使用私密金鑰、用戶端憑證和CA（如果使用）。

新增用戶端憑證

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發行的用戶端憑證
- 從Grid Manager產生憑證

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來設定管理介面憑證、請使用此程序來新增用戶端憑證。

步驟

1. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。
2. 選取*「Add*」。
3. 輸入憑證名稱。
4. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
5. 選擇*繼續*。
6. 對於 * 附加憑證 * 步驟、請上傳管理介面憑證。
   a. 選擇*上傳憑證*。
   b. 選取 * 瀏覽 * 並選取管理介面憑證檔案 (`.pem`) 。
      - 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。
      - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

      新的憑證會顯示在「用戶端」索引標籤上。
7. 設定外部監控工具例如 Grafana 。

CA發行的用戶端憑證

如果未設定管理介面憑證、且您計畫新增使用CA發行用戶端憑證和私密金鑰的Prometheus用戶端憑證、請使用此程序來新增管理員用戶端憑證。

步驟

1. 執行步驟至 "設定管理介面憑證"。
2. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。

3. 選取*「Add*」。
4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*。
7. 對於 * 附加憑證 * 步驟、請上傳用戶端憑證、私密金鑰和 CA 套裝組合檔案：
   a. 選擇*上傳憑證*。
   b. 選取 * 瀏覽 * 並選取用戶端憑證、私密金鑰和 CA 套件檔案 (`.pem`) 。
      - 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。
      - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

      新的憑證會顯示在「用戶端」索引標籤上。
8. 設定外部監控工具例如 Grafana 。

從**Grid Manager**產生憑證

如果管理介面憑證尚未設定、且您計畫在Grid Manager中新增使用產生憑證功能的Prometheus用戶端憑證、請使用此程序來新增管理員用戶端憑證。

步驟

1. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*用戶端*索引標籤。
2. 選取*「Add*」。
3. 輸入憑證名稱。
4. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
5. 選擇*繼續*。
6. 對於 * 附加憑證 * 步驟、請選取 * 產生憑證 * 。
7. 指定憑證資訊：
   - * 主旨 *（選用）：憑證擁有者的 X.509 主體或辨別名稱（ DN ）。
   - * 有效天數 * ：產生的憑證自產生之日起有效的天數。
   - * 新增金鑰使用方式延伸 * ：如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸功能會新增至產生的憑證。

     這些延伸定義了憑證中所含金鑰的用途。

     除非您在憑證包含這些副檔名時、遇到舊版用戶端的連線問題、否則請保留此核取方塊。
8. 選取*產生*。
9. [Client_cert詳細資料]選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
- 選取*下載憑證*以儲存憑證檔案。

  指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製私密金鑰*以複製憑證私密金鑰、以便貼到其他位置。
- 選取*下載私密金鑰*將私密金鑰儲存為檔案。

  指定私密金鑰檔案名稱和下載位置。

10. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

    新的憑證會顯示在「用戶端」索引標籤上。

11. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*全域*索引標籤。
12. 選擇*管理介面認證*。
13. 選擇*使用自訂憑證*。
14. 從上傳認證.pem和Private金鑰.pem檔案 用戶端憑證詳細資料 步驟。不需要上傳CA套裝組合。
    a. 選擇*上傳認證*、然後選擇*繼續*。
    b. 上傳每個憑證檔案 (`.pem`) 。
    c. 選取*「儲存*」、將憑證儲存在Grid Manager中。

       新的憑證會出現在管理介面憑證頁面上。

15. 設定外部監控工具例如 Grafana 。

設定外部監控工具

步驟

1. 在外部監控工具（例如Grafana）上設定下列設定。
   a. 名稱：輸入連線名稱。

      不需要此資訊、但您必須提供名稱來測試連線。StorageGRID

   b. * URL*：輸入管理節點的網域名稱或IP位址。指定HTTPS和連接埠9091。

      例如： `https://admin-node.example.com:9091`

   c. 啟用* TLS用戶端驗證*和* CA認證*。
   d. 在「TLS/SSL驗證詳細資料」下、複製並貼上：+
      - 管理介面CA憑證至「**CA認證」

- 用戶端認證至*用戶端認證
- 用於**用戶端金鑰*的私密金鑰

e. 伺服器名稱：輸入管理節點的網域名稱。

伺服器名稱必須符合管理介面憑證中顯示的網域名稱。

2. 儲存並測試您從StorageGRID 餐廳或本機檔案複製的憑證和私密金鑰。

您現在可以StorageGRID 使用外部監控工具、從功能表上存取Prometheus指標。

如需度量的相關資訊、請參閱 "監控StorageGRID 功能說明"。

編輯用戶端憑證

您可以編輯系統管理員用戶端憑證來變更其名稱、啟用或停用Prometheus存取、或是在目前憑證過期時上傳新的憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。

下表列出憑證到期日和Prometheus存取權限。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

2. 選取您要編輯的憑證。
3. 選取*編輯*、然後選取*編輯名稱和權限*
4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*以在Grid Manager中儲存憑證。

更新的憑證會顯示在「用戶端」索引標籤上。

附加新的用戶端憑證

您可以在目前的憑證過期時上傳新的憑證。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。

下表列出憑證到期日和Prometheus存取權限。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

2. 選取您要編輯的憑證。
3. 選取*編輯*、然後選取編輯選項。

上傳憑證

複製憑證文字以貼到其他位置。

a. 選擇*上傳認證*、然後選擇*繼續*。

b. 上傳用戶端憑證名稱 (`.pem`) 。

   選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   - 選取*下載憑證*以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

c. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

   更新的憑證會顯示在「用戶端」索引標籤上。

產生憑證

產生要貼到其他位置的憑證文字。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

   - * 主旨 * （選用）：憑證擁有者的 X.509 主體或辨別名稱（ DN ）。
   - * 有效天數 * ：產生的憑證自產生之日起有效的天數。
   - * 新增金鑰使用方式延伸 * ：如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸功能會新增至產生的憑證。

     這些延伸定義了憑證中所含金鑰的用途。

     除非您在憑證包含這些副檔名時、遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。
   - 選取*下載憑證*以儲存憑證檔案。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

- 選取*複製私密金鑰*以複製憑證私密金鑰、以便貼到其他位置。
- 選取*下載私密金鑰*將私密金鑰儲存為檔案。

  指定私密金鑰檔案名稱和下載位置。

e. 選取*「Create」（建立）*以在Grid Manager中儲存憑證。

新的憑證會顯示在「用戶端」索引標籤上。

下載或複製用戶端憑證

您可以下載或複製用戶端憑證、以便在其他地方使用。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。
2. 選取您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. 選擇*下載憑證*。

b. 指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

複製憑證

複製憑證文字以貼到其他位置。

a. 選擇*複製憑證PEP*。

b. 將複製的憑證貼到文字編輯器中。

c. 以副檔名儲存文字檔 `.pem`。

例如： `storagegrid_certificate.pem`

移除用戶端憑證

如果不再需要系統管理員用戶端憑證、您可以將其移除。

步驟

1. 選擇*組態*>*安全性*>*憑證*、然後選擇*用戶端*索引標籤。

2. 選取您要移除的憑證。
3. 選擇*刪除*、然後確認。

若要移除最多10個憑證、請在「用戶端」索引標籤上選取要移除的每個憑證、然後選取*「動作」>「刪除」*。

移除憑證後、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 《The動ePrometheus資料庫》。

設定安全性設定

管理 **TLS** 和 **SSH** 原則

TLS 和 SSH 原則決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性原則控制 TLS 和 SSH 如何加密移動中的資料。一般而言、請使用現代化相容性（預設）原則、除非您的系統需要符合一般準則、或您需要使用其他密碼。

某些 StorageGRID 服務尚未更新、無法在這些原則中使用密碼。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

選取安全性原則

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。

   「 *TLS 與 SSH 原則 * 」標籤會顯示可用的原則。目前作用中的原則會在原則方塊上以綠色核取記號表示。

2. 檢閱方塊以瞭解可用的原則。

原則	說明
現代化相容性（預設）	如果您需要增強式加密、而且沒有特殊要求、請使用預設原則。此原則與大多數 TLS 和 SSH 用戶端相容。

原則	說明
舊版相容性	如果您需要舊版用戶端的其他相容性選項、請使用此原則。此原則中的其他選項可能會使其比現代相容性原則更不安全。
一般準則	如果您需要通用準則認證、請使用此原則。
FIPS 嚴格	如果您需要通用準則認證、而且需要使用 NetApp 密碼編譯安全模組 3.0.8 來連接負載平衡器端點、租戶管理器和 Grid Manager 、請使用此原則。使用此原則可能會降低效能。 • 注意 * ：選取此原則之後、所有節點都必須是 "以不連續的方式重新開機" 啟動 NetApp 密碼編譯安全性模組。使用 * 維護 * > * 循環重新開機 * 來啟動和監控重新開機。
自訂	如果您需要套用自己的密碼、請建立自訂原則。

3. 若要查看每個原則的密碼、通訊協定和演算法的詳細資料、請選取 * 檢視詳細資料 * 。
4. 若要變更目前的原則、請選取 * 使用原則 * 。

   原則方塊上的 * 目前原則 * 旁會出現綠色核取記號。

建立自訂安全性原則

如果您需要套用自己的密碼、可以建立自訂原則。

步驟

1. 從最類似您要建立之自訂原則的原則方塊中、選取 * 檢視詳細資料 * 。
2. 選取 * 複製到剪貼簿 * 、然後選取 * 取消 * 。

3. 從 * 自訂原則 * 方塊中、選取 * 設定與使用 * 。
4. 貼上您複製的 JSON 、然後進行任何必要的變更。

5. 選取 * 使用原則 * 。

   「自訂原則」方塊的 * 目前原則 * 旁會出現綠色核取記號。

6. 您也可以選擇 * 編輯組態 * 來對新的自訂原則進行更多變更。

暫時恢復為預設的安全性原則

如果您設定了自訂安全性原則、如果設定的 TLS 原則與不相容、則可能無法登入 Grid Manager "已設定的伺服器憑證"。

您可以暫時還原為預設的安全性原則。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。

2. 執行下列命令：

   ```
   restore-default-cipher-configurations
   ```

3. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。
4. 請依照中的步驟進行 選取安全性原則 重新設定原則。

設定網路和物件安全性

您可以設定網路和物件安全性來加密儲存的物件、防止某些 S3 和 Swift 要求、或允許用戶端連線至儲存節點使用 HTTP 而非 HTTPS 。

儲存的物件加密

儲存的物件加密可在透過 S3 擷取時、加密所有物件資料。根據預設、儲存的物件不會加密、但您可以選擇使用 AES - 128 或 AES - 256 加密演算法來加密物件。啟用此設定時、所有新擷取的物件都會加密、但不會對現有的儲存物件進行任何變更。如果停用加密、目前加密的物件仍會保持加密狀態、但新擷取的物件不會加密。

「儲存的物件加密」設定僅適用於未透過貯體層級或物件層級加密進行加密的 S3 物件。

如需 StorageGRID 加密方法的詳細資訊、請參閱 "檢閱StorageGRID 功能加密方法"。

防止用戶端修改

防止用戶端修改是全系統的設定。當選擇 * 防止用戶端修改 * 選項時、會拒絕下列要求。

S3 REST API

- 刪除 Bucket 要求
- 任何修改現有物件資料、使用者定義中繼資料或S3物件標記的要求

Swift REST API

- 刪除Container要求
- 要求修改任何現有物件。例如、下列作業會遭拒：「放置覆寫」、「刪除」、「中繼資料更新」等。

啟用 **HTTP** 以進行儲存節點連線

根據預設、用戶端應用程式會使用 HTTPS 網路傳輸協定來直接連線至儲存節點。您可以選擇性地為這些連線啟用HTTP、例如在測試非正式作業網格時。

只有當 S3 和 Swift 用戶端需要直接與儲存節點建立 HTTP 連線時、才可使用 HTTP 進行儲存節點連線。您不需要將此選項用於僅使用 HTTPS 連線的用戶端或連線至負載平衡器服務的用戶端（因為您可以 "設定每個負載平衡器端點" 使用 HTTP 或 HTTPS ）。

請參閱 "摘要：用於用戶端連線的IP位址和連接埠" 瞭解使用 HTTP 或 HTTPS 連線至儲存節點時、 S3 和 Swift 用戶端使用的連接埠。

選取選項

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有root存取權限。

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選取 * 網路和物件 * 索引標籤。
3. 對於儲存的物件加密、如果您不想加密儲存的物件、請使用 * 無 * （預設）設定、或選取 * AES-128* 或 * AES-256* 來加密儲存的物件。
4. 如果您想要防止 S3 和 Swift 用戶端提出特定要求、請選擇性地選取 * 防止用戶端修改 * 。

   如果您變更此設定、則需要約一分鐘的時間才能套用新設定。系統會快取設定的值、以利效能與擴充。

5. 如果用戶端直接連線至儲存節點、且您想使用 HTTP 連線、則可選擇 * 啟用儲存節點連線的 HTTP * 。

   啟用正式作業網格的HTTP時請務必小心、因為要求會以未加密的方式傳送。

6. 選擇*保存*。

變更介面安全性設定

介面安全性設定可讓您控制使用者是否在超過指定時間的非作用中狀態下登出、以及是否

在 API 錯誤回應中包含堆疊追蹤。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "root 存取權限"。

關於這項工作

「 * 安全性設定 * 」頁面包含 * 瀏覽器閒置逾時 * 和 * 管理 API 堆疊追蹤 * 設定。

瀏覽器閒置逾時

指出使用者的瀏覽器在登出之前可以停用多久。預設值為15分鐘。

瀏覽器閒置逾時也由下列項目控制：

- 另有一個不可設定StorageGRID 的獨立式計時功能、可用於系統安全性。每個使用者的驗證權杖會在使用者登入後 16 小時過期。當使用者的驗證過期時、該使用者會自動登出、即使瀏覽器閒置逾時已停用、或瀏覽器逾時的值尚未達到。若要續約權杖、使用者必須重新登入。
- 假設 StorageGRID 已啟用單一登入（ SSO ）、則身分識別提供者的逾時設定。

  如果啟用 SSO 且使用者的瀏覽器逾時、使用者必須重新輸入其 SSO 認證、才能再次存取 StorageGRID 。請參閱 "設定單一登入"。

管理 **API** 堆疊追蹤

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、但您可能想要在測試環境中啟用此功能。一般而言、您應該在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。

步驟

1. 選擇 * 組態 * > * 安全性 * > * 安全性設定 * 。
2. 選擇 * 介面 * 標籤。
3. 若要變更瀏覽器閒置逾時的設定：
   a. 展開折疊。
   b. 若要變更逾時期間、請指定介於 60 秒到 7 天之間的值。預設逾時為 15 分鐘。
   c. 若要停用此功能、請取消選取核取方塊。
   d. 選擇*保存*。

      新設定不會影響目前登入的使用者。使用者必須重新登入或重新整理瀏覽器、新的逾時設定才會生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開折疊。
   b. 選取此核取方塊可在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

      在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。

c. 選擇*保存*。

設定金鑰管理伺服器

設定金鑰管理伺服器：總覽

您可以設定一或多個外部金鑰管理伺服器（KMS）、以保護特殊設定的應用裝置節點上的資料。

StorageGRID 僅支援特定的金鑰管理伺服器。如需受支援產品和版本的清單、請使用 "NetApp互通性對照表工具IMT （不含）"。

什麼是金鑰管理伺服器（**KMS**）？

金鑰管理伺服器（KMS）是一種外部的第三方系統StorageGRID 、可透過StorageGRID 金鑰管理互通性傳輸協定（KMIP）、為相關聯的站台上的應用裝置節點提供加密金鑰。

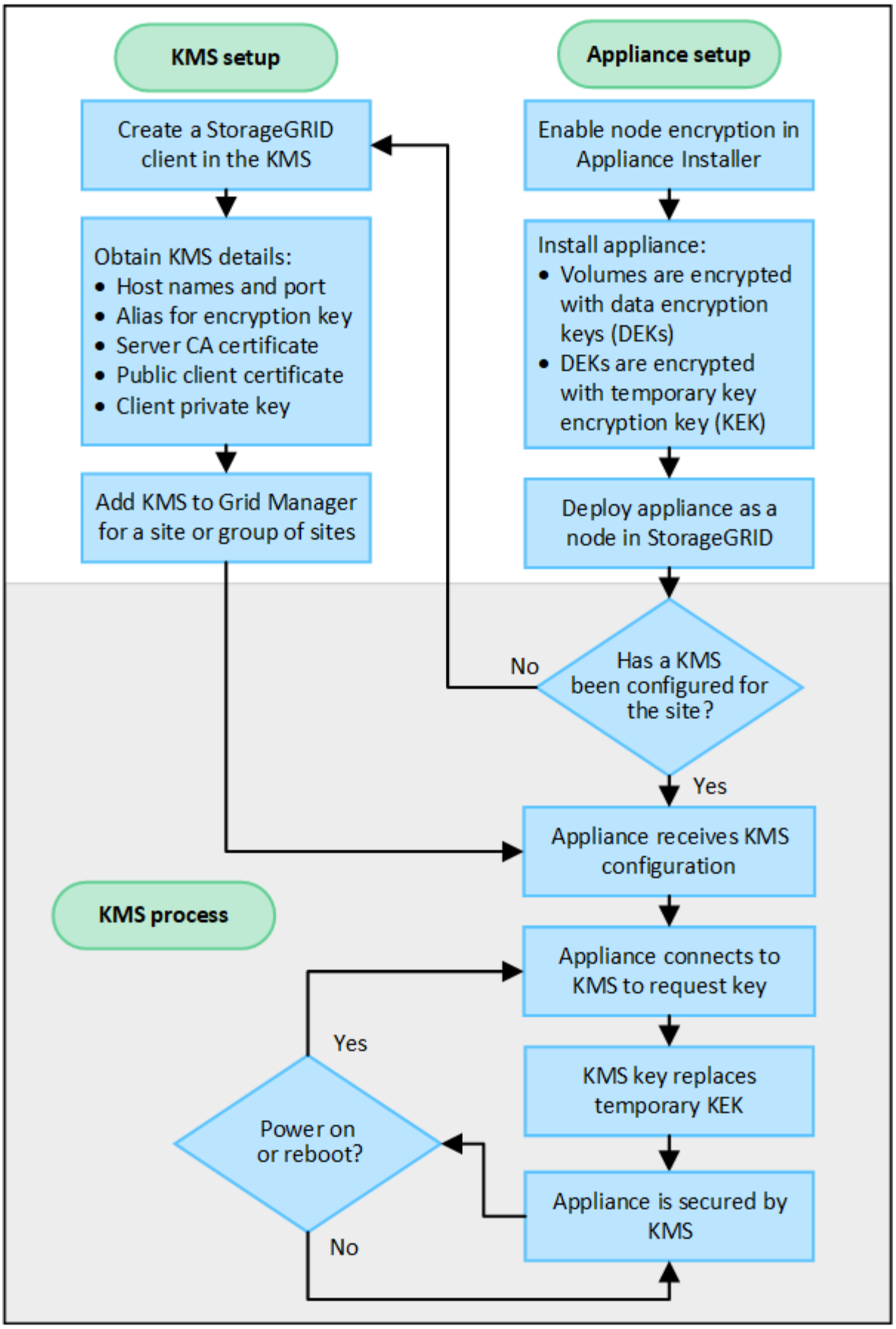
您可以使用一或多個金鑰管理伺服器、來管理StorageGRID 安裝期間啟用*節點加密*設定的任何節點的節點加密金鑰。即使從資料中心移除應用裝置、將關鍵管理伺服器與這些應用裝置節點搭配使用、也能保護資料。應用裝置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

不建立或管理用於加密和解密應用裝置節點的外部金鑰。StorageGRID如果您打算使用外部金鑰管理伺服器來保護StorageGRID 這些資料、您必須瞭解如何設定該伺服器、而且必須瞭解如何管理加密金鑰。執行關鍵管理工作的範圍超出這些指示的範圍。如果您需要協助、請參閱金鑰管理伺服器的文件、或聯絡技術支援部門。

KMS與應用裝置組態總覽

在使用金鑰管理伺服器（KMS）來保護StorageGRID 應用裝置節點上的各項資料之前、您必須先完成兩項組態工作：設定一或多個KMS伺服器、以及為應用裝置節點啟用節點加密。完成這兩項組態工作之後、就會自動執行金鑰管理程序。

流程圖顯示使用KMS保護StorageGRID 應用裝置節點上的資訊安全的高階步驟。



流程圖會顯示KMS設定與應用裝置設定並行執行、不過您可以根據需求、在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。

設定金鑰管理伺服器（KMS）

設定金鑰管理伺服器包括下列高層級步驟。

步驟	請參閱
存取KMS軟體、並在StorageGRID 每個KMS或KMS叢集上新增一個用戶端以供使用。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
在StorageGRID KMS取得有關該客戶端的必要資訊。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
將KMS新增至Grid Manager、指派給單一站台或預設站台群組、上傳必要的憑證、並儲存KMS組態。	"新增金鑰管理伺服器（KMS）"

設定產品

設定KMS使用的應用裝置節點包括下列高層級步驟。

1. 在設備安裝的硬體組態階段、請使用StorageGRID 「支援服務」功能的「應用程式安裝程式」來啟用應用裝置的「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、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

2. 執行StorageGRID 《程式安裝程式：在安裝期間、會將隨機資料加密金鑰（DEek）指派給每個應用裝置磁碟區、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 統一金鑰設定（ LUKS ）磁碟加密來產生、無法變更。
   - 每個個別的「DEK」都是使用主要金鑰加密金鑰（KEK）進行加密。初始KEK是加密DEK的暫用金鑰、直到應用裝置連線至KMS為止。
3. 將應用裝置節點新增StorageGRID 至

請參閱 "啟用節點加密" 以取得詳細資料。

金鑰管理加密程序（自動執行）

金鑰管理加密包括下列自動執行的高層級步驟。

1. 當您在網格中安裝已啟用節點加密的應用裝置時StorageGRID 、即可判斷包含新節點的站台是否存在KMS組態。
   - 如果站台已設定KMS、則裝置會接收KMS組態。
   - 如果尚未為站台設定KMS、則在您為站台設定KMS、且裝置收到KMS組態之前、應用裝置上的資料會繼續由暫用KEK加密。
2. 應用裝置使用KMS組態連線至KMS、並要求加密金鑰。

3. KMS會傳送加密金鑰給應用裝置。來自KMS的新金鑰取代了暫用KEK、現在用於加密和解密應用裝置磁碟區的DEK。

> 加密應用裝置節點連線至設定的KMS之前存在的任何資料、都會以暫用金鑰加密。不過、除非KMS加密金鑰取代暫用金鑰、否則應用裝置磁碟區不應被視為受到保護、以免從資料中心移除。

4. 如果裝置電源已開啟或重新開機、則會重新連線至KMS以要求金鑰。儲存在揮發性記憶體中的金鑰、無法在停電或重新開機的情況下繼續運作。

使用金鑰管理伺服器的考量與要求

在設定外部金鑰管理伺服器（KMS）之前、您必須先瞭解考量事項與需求。

支援哪個版本的 **KMIP** ？

支援KMIP 1.4版。StorageGRID

"關鍵管理互通性傳輸協定規格1.4版"

網路考量因素為何？

網路防火牆設定必須允許每個應用裝置節點透過金鑰管理互通性傳輸協定（KMIP）通訊所使用的連接埠進行通訊。預設KMIP連接埠為5696。

您必須確保使用節點加密的每個應用裝置節點、都能透過網路存取您為站台設定的KMS或KMS叢集。

支援哪些 **TLS** 版本？

應用裝置節點與設定的KMS之間的通訊使用安全的TLS連線。StorageGRID 可根據 KMS 支援的內容和支援的內容、在 KMIP 連線至 KMS 或 KMS 叢集時、支援 TLS 1.2 或 TLS 1.3 傳輸協定 "TLS 和 SSH 原則" 您正在使用。

StorageGRID 在建立連線時、會與 KMS 交涉通訊協定和密碼（ TLS 1.2 ）或密碼套件（ TLS 1.3 ）。若要查看有哪些可用的通訊協定版本和加密程式 / 加密套件、請參閱 `tlsOutbound` 網格作用中 TLS 和 SSH 原則的一節（ * 組態 * > * 安全性 * * 安全性設定 * ）。

支援哪些應用裝置？

您可以使用金鑰管理伺服器（KMS）來管理StorageGRID 網格中任何啟用「節點加密」設定的項目之加密金鑰。此設定只能在安裝應用StorageGRID 程式的硬體組態階段、使用《支援環境》安裝程式來啟用。

> 將應用裝置新增至網格後、您無法啟用節點加密、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

您可以使用已設定的 KMS for StorageGRID 應用裝置和應用裝置節點。

您無法將已設定的 KMS 用於軟體型（非應用裝置）節點、包括下列項目：

- 部署為虛擬機器（VM）的節點
- 部署在Linux主機上Container引擎內的節點

部署在這些其他平台上的節點、可以在StorageGRID 資料存放區或磁碟層級使用非功能加密。

何時應該設定金鑰管理伺服器？

對於新安裝、您通常應該先在Grid Manager中設定一或多個金鑰管理伺服器、然後再建立租戶。此順序可確保節點在儲存任何物件資料之前受到保護。

您可以在安裝應用裝置節點之前或之後、在Grid Manager中設定金鑰管理伺服器。

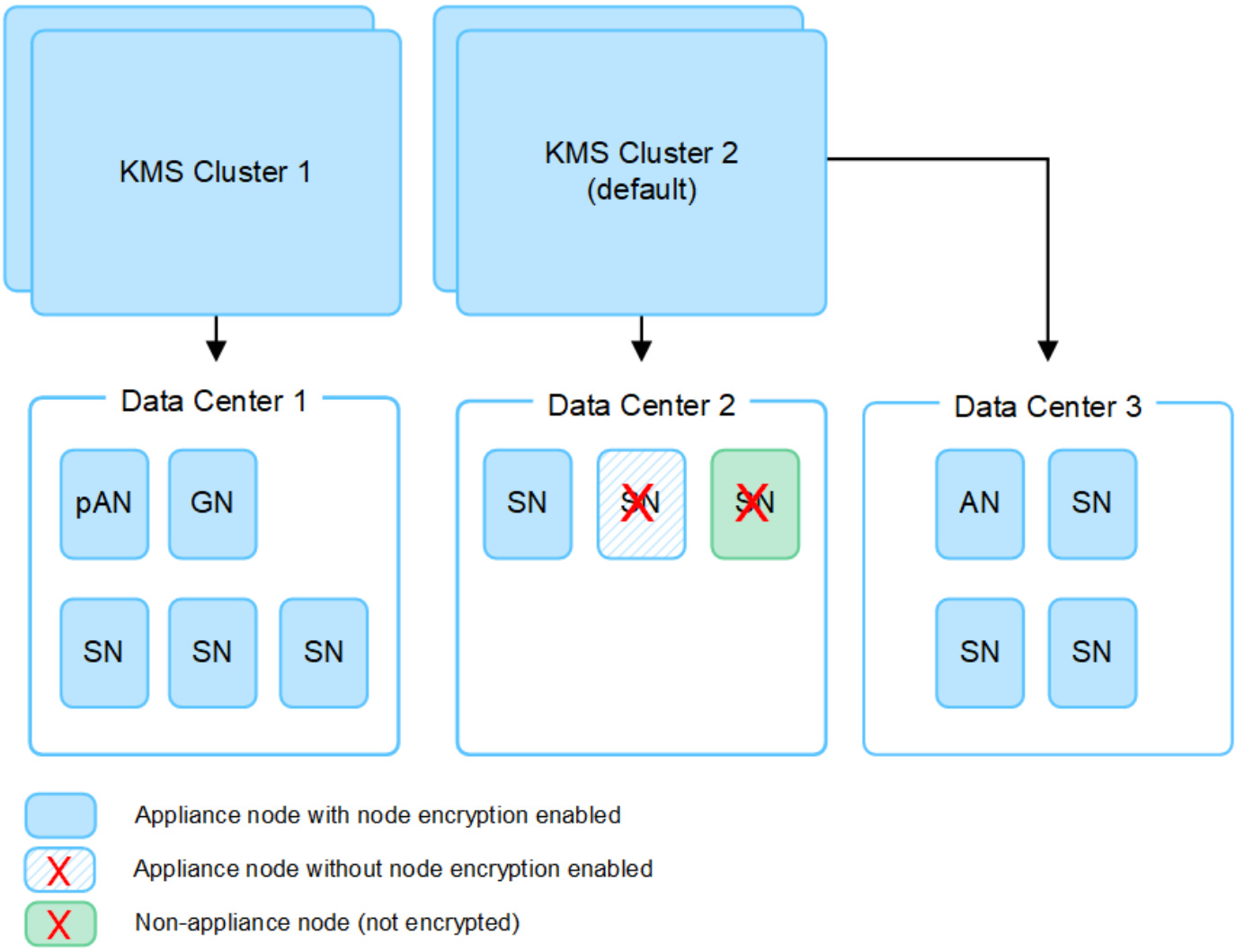
我需要多少個關鍵管理伺服器？

您可以設定一或多個外部金鑰管理伺服器、為StorageGRID 您的作業系統中的應用裝置節點提供加密金鑰。每個KMS都會在StorageGRID 單一站台或一組站台上、提供單一的加密金鑰給各個不完整的應用裝置節點。

支援使用KMS叢集。StorageGRID每個KMS叢集都包含多個複寫的金鑰管理伺服器、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、因為它能改善高可用度組態的容錯移轉功能。

舉例來說、假設StorageGRID 您的一套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。新增第二個KMS叢集時、您可以為資料中心2和資料中心3設定預設KMS。

請注意、您無法將 KMS 用於非應用裝置節點、或用於安裝期間未啟用 * 節點加密 * 設定的任何應用裝置節點。



當金鑰旋轉時會發生什麼事？

最佳安全實務做法是定期進行 "旋轉加密金鑰" 由每個設定的 KMS 使用。

當新的金鑰版本可用時：

- 它會自動發佈至站台或與KMS相關之站台的加密應用裝置節點。發佈應在鑰匙轉動後一個小時內完成。
- 如果在發佈新金鑰版本時、加密的應用裝置節點已離線、節點會在重新開機時立即收到新金鑰。
- 如果由於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、則會針對應用裝置節點觸發 * KMS 加密金鑰旋轉失敗 * 警示。您可能需要聯絡技術支援部門、以協助解決此警示。

我可以在設備節點加密後重複使用嗎？

如果您需要將加密的應用裝置安裝到另一個StorageGRID 版本、則必須先取消委任網格節點、才能將物件資料移到另一個節點。然後、您可以使用 StorageGRID 應用裝置安裝程式來執行 "清除 KMS 組態"。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 本網站KMS組態之間的關聯。

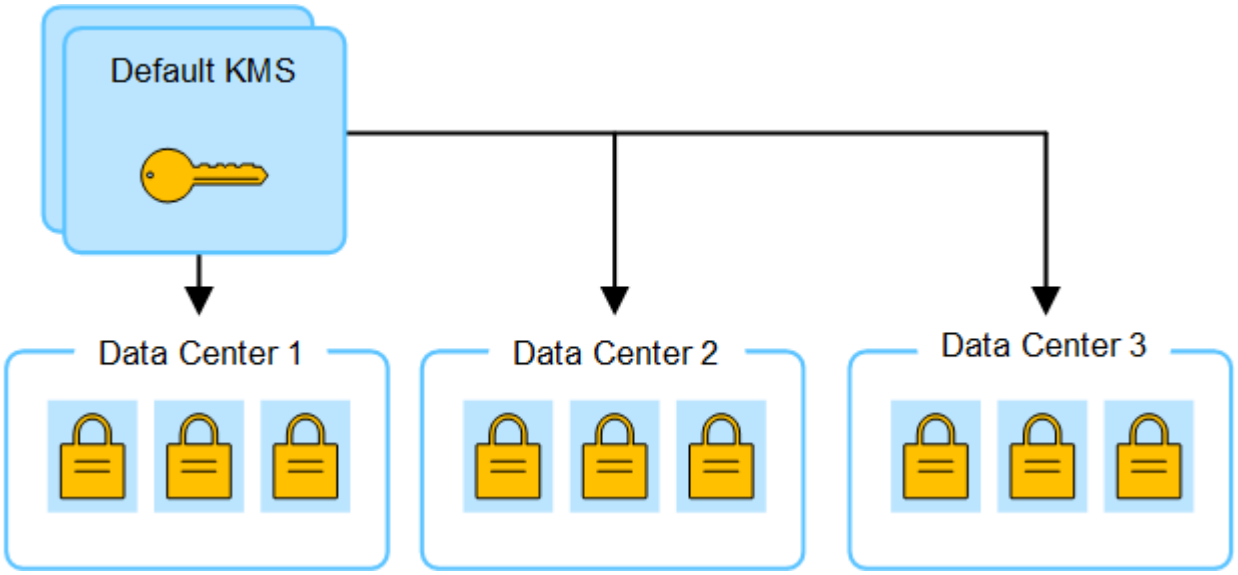
由於無法存取KMS加密金鑰、因此無法再存取設備上的任何資料、而且會永久鎖定。

每個金鑰管理伺服器（KMS）或KMS叢集都會為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使用的KMS、可能需要將加密金鑰從一個KMS複製到另一個KMS。

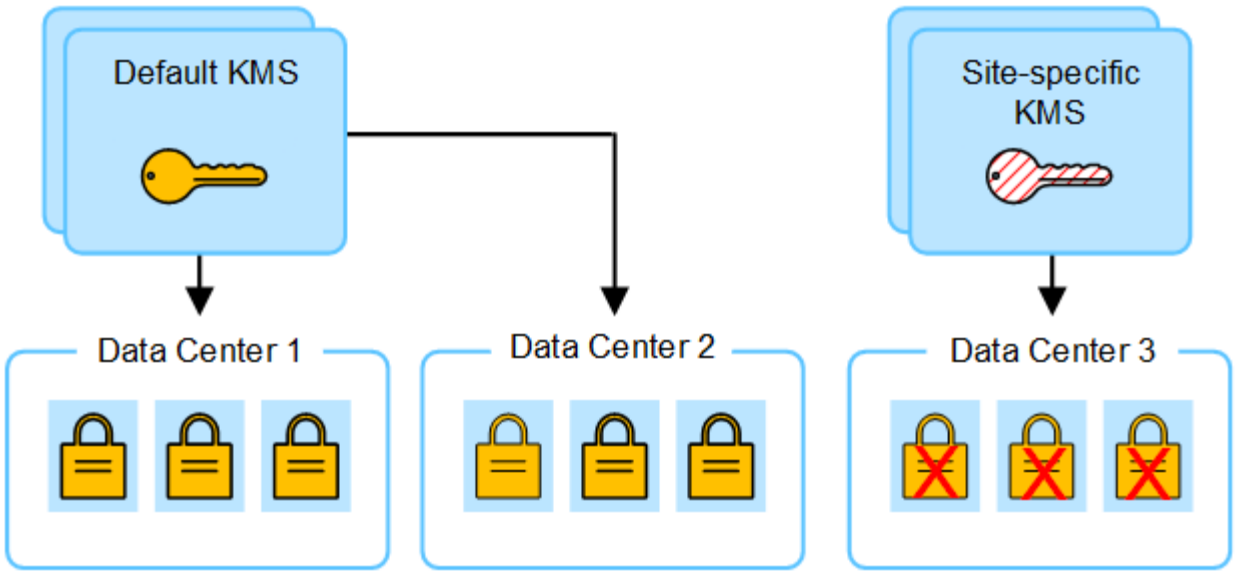
如果您變更站台使用的KMS、則必須確保該站台先前加密的應用裝置節點可以使用儲存在新KMS上的金鑰來解密。在某些情況下、您可能需要將目前版本的加密金鑰從原始KMS複製到新的KMS。您必須確保KMS擁有正確的金鑰、以便在站台上解密加密的應用裝置節點。

例如：

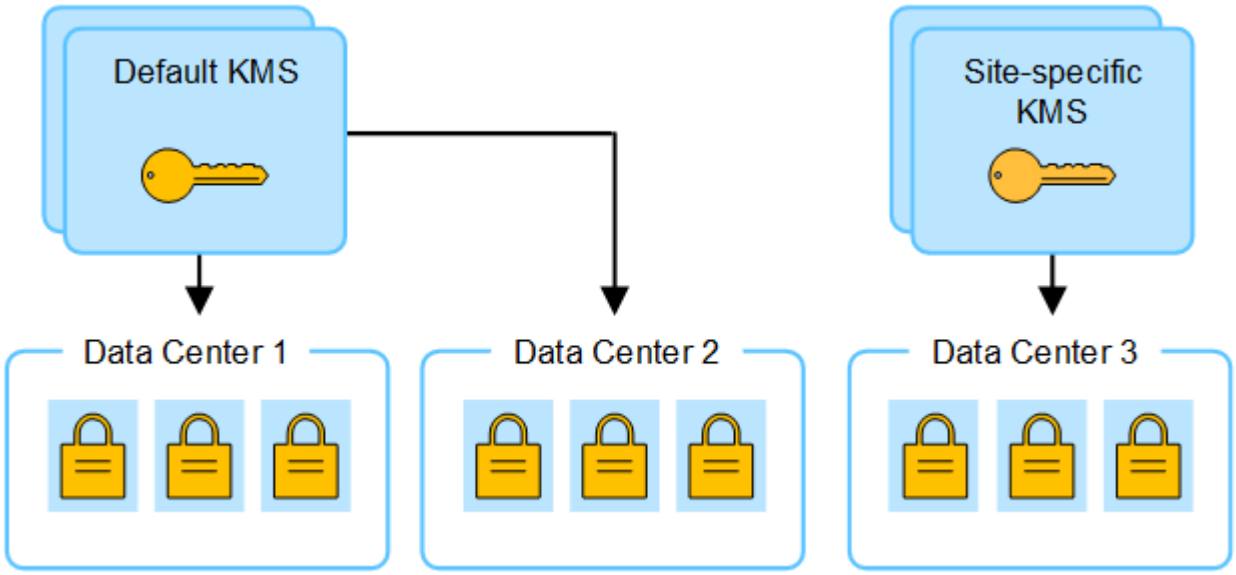
1. 您一開始會設定預設 KMS 、以套用至所有沒有專屬 KMS 的網站。
2. 儲存KMS時、所有啟用「節點加密」設定的應用裝置節點都會連線至KMS、並要求加密金鑰。此金鑰用於加密所有站台的應用裝置節點。此相同金鑰也必須用於解密這些應用裝置。



3. 您決定為單一站台新增站台專屬的KMS（圖中的資料中心3）。不過、由於應用裝置節點已加密、因此當您嘗試儲存站台特定KMS的組態時、就會發生驗證錯誤。發生此錯誤的原因是站台特定的KMS沒有正確的金鑰來解密該站台的節點。



4. 若要解決此問題、請將目前版本的加密金鑰從預設KMS複製到新的KMS。（技術上、您可以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。） 站台專屬的KMS現在擁有正確的金鑰、可在Data Center 3解密應用裝置節點、以便儲存在StorageGRID 原地。



變更站台使用**KMS**的使用案例

下表摘要列出變更站台KMS的最常見案例所需步驟。

變更站台**KMS**的使用案例	必要步驟
您有一或多個站台專屬的KMS項目、您想要使用其中一個做為預設KMS。	編輯站台專屬的KMS。在*管理金鑰*欄位中、選取*不受其他KMS管理的站台（預設KMS）*。網站專屬KMS現在將做為預設KMS使用。它將套用至任何沒有專屬 KMS 的網站。 "編輯金鑰管理伺服器（KMS）"

變更站台**KMS**的使用案例	必要步驟
您有預設的KMS、而且您在擴充中新增了一個網站。您不想在新網站上使用預設的 KMS 。	1. 如果新站台的應用裝置節點已在預設KMS中加密、請使用KMS軟體將目前版本的加密金鑰從預設KMS複製到新的KMS。 2. 使用Grid Manager新增KMS並選取網站。 "新增金鑰管理伺服器（KMS）"
您想讓站台的KMS使用不同的伺服器。	1. 如果站台上的應用裝置節點已由現有的KMS加密、請使用KMS軟體將目前版本的加密金鑰從現有的KMS複製到新的KMS。 2. 使用Grid Manager編輯現有的KMS組態、然後輸入新的主機名稱或IP位址。 "新增金鑰管理伺服器（KMS）"

在**StorageGRID KMS**中設定以用戶端身份執行的功能

您必須先為StorageGRID 每個外部金鑰管理伺服器或KMS叢集設定用作用戶端的功能、才能將KMS新增StorageGRID 至原地。

這些指示適用於 Thales CipherTrust Manager 和 Hashicorp Vault 。如需受支援產品和版本的清單、請使用 "NetApp互通性對照表工具IMT （不含）"。

步驟

1. 在KMS軟體中、為StorageGRID 您打算使用的每個KMS或KMS叢集建立一個完善的用戶端。

   每個KMS都會在StorageGRID 單一站台或一組站台上、管理一個用於「不完整」應用裝置節點的加密金鑰。

2. [[create-key-with -kms-product]] 使用下列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 AES 加密金鑰。

     加密金鑰必須為 2 、 048 位元以上、而且必須可匯出。

   - 讓 StorageGRID 建立金鑰。測試並儲存之後、系統會提示您 "正在上傳用戶端憑證"。

3. 記錄每個KMS或KMS叢集的下列資訊。

   當您將 KMS 新增至 StorageGRID 時、需要以下資訊：

   - 每個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、請取得由憑證授權單位（CA）簽署的伺服器憑證、或是包含每個以憑證鏈順序串聯的、以PEE編碼之CA憑證檔案的憑證套件。

   伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

- 憑證必須使用隱私增強型郵件（ PEF ） Base - 64 編碼的 X ・ 509 格式。
- 每個伺服器憑證中的「Subject Alternative Name（SAN）（主體替代名稱（SAN））」欄位必須包含StorageGRID 完整網域名稱（FQDN）或要連線的IP位址。

> 在StorageGRID 進行KMS設定時、您必須在*主機名稱*欄位中輸入相同的FQDN或IP位址。

- 伺服器憑證必須符合KMS KMIP介面所使用的憑證、後者通常使用連接埠5696。

5. 取得由StorageGRID 外部KMS核發的公有用戶端憑證、以及用戶端憑證的私密金鑰。

   用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

新增金鑰管理伺服器（**KMS**）

您可以使用StorageGRID 「驗鑰管理伺服器」精靈來新增每個KMS或KMS叢集。

開始之前

- 您已檢閱 "使用金鑰管理伺服器的考量與要求"。
- 您有 "設定StorageGRID 成KMS中的用戶端"，而且您擁有每個KMS或KMS叢集所需的資訊。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

關於這項工作

如有可能、請先設定任何站台專屬的金鑰管理伺服器、再設定適用於其他KMS未管理之所有站台的預設KMS。如果您先建立預設KMS、則網格中的所有節點加密應用裝置都會以預設KMS加密。如果您想要稍後建立站台專屬的KMS、必須先將目前版本的加密金鑰從預設的KMS複製到新的KMS。請參閱 "變更網站KMS的考量事項" 以取得詳細資料。

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、您會提供 KMS 或 KMS 叢集的詳細資料。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現金鑰管理伺服器頁面、並選取組態詳細資料索引標籤。

2. 選擇* Create （建立）。

   隨即顯示新增金鑰管理伺服器精靈的步驟 1 （ KMS 詳細資料）。

3. 針對您StorageGRID 在該KMS中設定的KMS和整套用戶端、輸入下列資訊。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於1到64個字元之間。

欄位	說明
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。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、系統會提示您讓 StorageGRID 建立金鑰。
管理的金鑰	將與此KMS相關聯的網站。StorageGRID如有可能、您應該先設定任何站台專屬的金鑰管理伺服器、再設定適用於其他KMS未管理之所有站台的預設KMS。 • 如果此KMS將管理特定站台應用裝置節點的加密金鑰、請選取站台。 • 選取 * 不受其他 KMS 管理的網站（預設 KMS ） * 來設定預設 KMS 、以套用至任何沒有專用 KMS 的網站、以及您在後續擴充中新增的任何網站。 *附註：*如果您選取先前已由預設KMS加密的網站、但未將目前版本的原始加密金鑰提供給新的KMS、則儲存KMS組態時會發生驗證錯誤。
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即KMIP標準連接埠。
主機名稱	KMS的完整網域名稱或IP位址。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

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、您可以上傳 KMS 的伺服器憑證（或憑證套件）。伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

步驟

1. 從 * 步驟 2 （上傳伺服器憑證） * 中、瀏覽至儲存伺服器憑證或憑證套件的位置。
2. 上傳憑證檔案。

   隨即顯示伺服器憑證中繼資料。

   如果您上傳了憑證套件組合、每個憑證的中繼資料都會顯示在其各自的索引標籤上。

3. 選擇*繼續*。

步驟 **3** ：上傳用戶端憑證

在新增金鑰管理伺服器精靈的步驟 3 （上傳用戶端憑證）中、您可以上傳用戶端憑證和用戶端憑證私密金鑰。用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

步驟

1. 從 * 步驟 3 （上傳用戶端憑證） * 、瀏覽至用戶端憑證的位置。
2. 上傳用戶端憑證檔案。

   此時會出現用戶端憑證中繼資料。
3. 瀏覽至用戶端憑證的私密金鑰位置。
4. 上傳私密金鑰檔案。
5. 選擇 * 測試並儲存 * 。

   如果金鑰不存在、系統會提示您建立 StorageGRID 。

   測試金鑰管理伺服器與應用裝置節點之間的連線。如果所有連線都有效、且KMS上找到正確的金鑰、新的金鑰管理伺服器就會新增至金鑰管理伺服器頁面的表格。

   新增KMS之後、「金鑰管理伺服器」頁面上的憑證狀態會立即顯示為「未知」。可能需要StorageGRID 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. 如果您選取 * 測試並儲存 * 時出現錯誤訊息、請檢閱訊息詳細資料、然後選取 * 確定 * 。

   例如、如果連線測試失敗、您可能會收到「無法處理的實體」錯誤。
7. 如果您需要儲存目前的組態而不測試外部連線、請選取 * 強制儲存 * 。

   選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。
8. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

   系統會儲存KMS組態、但不會測試與KMS的連線。

管理 **KMS**

管理金鑰管理伺服器（ KMS ）包括檢視或編輯詳細資料、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

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "必要的存取權限"。

檢視 **KMS** 詳細資料

您可以檢視 StorageGRID 系統中每個金鑰管理伺服器（ KMS ）的相關資訊、包括金鑰詳細資料、以及伺服器和用戶端憑證的目前狀態。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面、並顯示下列資訊：

   - 組態詳細資料索引標籤會列出所有已設定的金鑰管理伺服器。
   - 加密節點索引標籤會列出已啟用節點加密的任何節點。

2. 若要檢視特定 KMS 的詳細資料並在該 KMS 上執行作業、請選取 KMS 的名稱。KMS 的詳細資料頁面會列出下列資訊：

欄位	說明
管理的金鑰	與KMS相關的站台。StorageGRID 此欄位會顯示特定StorageGRID 的站台名稱、或*不由其他KMS管理的站台名稱（預設KMS）。*
主機名稱	KMS的完整網域名稱或IP位址。 如果有兩個金鑰管理伺服器的叢集、則會列出兩個伺服器的完整網域名稱或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的完整網域名稱或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`。 若要檢視叢集中的所有主機名稱、請選取 KMS 、然後選取 * 編輯 * 或 * 動作 * > * 編輯 * 。

3. 選取 KMS 詳細資料頁面上的索引標籤、即可檢視下列資訊：

索引標籤	欄位	說明
關鍵詳細資料	金鑰名稱	KMS中的核心用戶端別名StorageGRID 。
金鑰UID	金鑰最新版本的唯一識別碼。	上次修改時間
金鑰最新版本的日期與時間。	伺服器憑證	中繼資料

索引標籤	欄位	說明
憑證的中繼資料、例如序號、到期日和時間、以及憑證 PEM 。	憑證 PEM	憑證的 PEM （隱私強化郵件）檔案內容。
用戶端憑證	中繼資料	憑證的中繼資料、例如序號、到期日和時間、以及憑證 PEM 。

4. 根據組織安全實務做法的要求、選擇 * 旋轉機碼 * 、或使用 KMS 軟體來建立新版本的金鑰。

當金鑰旋轉成功時、會更新金鑰 UID 和上次修改的欄位。

如果您使用 KMS 軟體來旋轉加密金鑰、請將其從上次使用的金鑰版本旋轉至相同金鑰的新版本。請勿旋轉至完全不同的金鑰。

切勿嘗試變更KMS的金鑰名稱（別名）來旋轉金鑰。若要從KMS存取先前使用過的所有金鑰版本（以及未來的任何金鑰版本）、必須使用相同的金鑰別名。StorageGRID如果您變更設定KMS的金鑰別名、StorageGRID 則可能無法解密您的資料。

管理憑證

立即解決任何伺服器或用戶端憑證問題。如有可能、請在憑證過期之前更換憑證。

您必須盡快解決任何憑證問題、才能維持資料存取。

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. 如果任何 KMS 的憑證過期時間都是未知的、請等待 30 分鐘、然後重新整理您的網頁瀏覽器。
4. 如果 " 憑證到期 " 欄顯示憑證已過期或即將過期 , 請選取 KMS 前往 KMS 詳細資料頁面。
   a. 選取 * 伺服器憑證 * 、並驗證「到期日」欄位的值。
   b. 若要取代憑證、請選取 * 編輯憑證 * 來上傳新的憑證。
   c. 重複這些子步驟、然後選取 * 用戶端憑證 * 、而非伺服器憑證。
5. 當觸發 *KMS CA 憑證過期 * 、 *KMS 用戶端憑證過期 * 和 *KMS 伺服器憑證過期 * 警示時、請記下每個警示的說明、然後執行建議的動作。

StorageGRID 可能需要 30 分鐘才能取得憑證過期的更新。重新整理網頁瀏覽器以查看目前的值。

檢視加密節點

您可以在StorageGRID 啟用「節點加密」設定的支援功能系統中、檢視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*。

   此時會出現「金鑰管理伺服器」頁面。「組態詳細資料」索引標籤會顯示任何已設定的金鑰管理伺服器。

2. 從頁面頂端、選取 * 加密節點 * 索引標籤。

   加密節點索引標籤會列出 StorageGRID 系統中已啟用 * 節點加密 * 設定的應用裝置節點。

3. 檢閱表格中每個應用裝置節點的資訊。

欄位	說明
節點名稱	應用裝置節點的名稱。
節點類型	節點類型：儲存設備、管理或閘道。
網站	安裝節點的站台名稱。StorageGRID
KMS 名稱	用於節點的KMS描述性名稱。 如果沒有列出 KMS 、請選取組態詳細資料索引標籤以新增 KMS 。 "新增金鑰管理伺服器（KMS）"
金鑰UID	加密金鑰的唯一ID、用於加密及解密應用裝置節點上的資料。若要檢視整個金鑰 UID 、請選取文字。 破折號（-）表示金鑰唯一碼未知、可能是因為應用裝置節點與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。如果節點已連線、時間戳記每30分鐘更新一次。變更KMS組態之後、連線狀態可能需要幾分鐘的時間才能更新。 • 附註： * 重新整理您的網路瀏覽器、以查看新值。

4. 如果「狀態」欄指出KMS問題、請立即解決問題。

   在一般KMS作業期間、狀態將*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（管理性關閉或未知）。

   其他狀態訊息則對應StorageGRID 於名稱相同的Ses姓名：

   ◦ 無法載入kms組態

   ◦ KMS連線錯誤

   ◦ 找不到kms加密金鑰名稱

   ◦ KMS加密金鑰旋轉失敗

   ◦ KMS金鑰無法解密應用裝置磁碟區

。未設定公里

執行這些警示的建議動作。

您必須立即解決任何問題、確保資料受到完整保護。

編輯 KMS

您可能需要編輯金鑰管理伺服器的組態、例如、如果憑證即將過期。

開始之前

- 如果您打算更新選取的KMS網站、則表示您已檢閱 "變更網站KMS的考量事項"。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要編輯的 KMS 、然後選取 * 動作 * > * 編輯 * 。

   您也可以在表格中選取 KMS 名稱、然後在 KMS 詳細資料頁面上選取 * 編輯 * 來編輯 KMS 。

3. 您也可以在「編輯金鑰管理伺服器」精靈的 * 步驟 1 （ KMS 詳細資料） * 中更新詳細資料。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於1到64個字元之間。
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。必須介於 1 到 255 個字元之間。 在極少數情況下、您只需要編輯金鑰名稱即可。例如、如果在KMS中重新命名別名、或是先前金鑰的所有版本都已複製到新別名的版本歷程記錄、則必須編輯金鑰名稱。
管理的金鑰	如果您正在編輯網站專屬的 KMS 、但尚未有預設的 KMS 、請選擇性地選取 * 「不是由其他 KMS 管理的網站」（預設 KMS ） * 。此選項會將網站專屬的 KMS 轉換成預設的 KMS 、適用於所有沒有專屬 KMS 的網站、以及新增至擴充中的任何網站。 • 注意： * 如果您正在編輯網站專屬的 KMS 、則無法選取其他網站。如果您正在編輯預設 KMS 、則無法選取特定網站。
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即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。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

   此時將顯示 Edit a Key Management Server （編輯金鑰管理伺服器）精靈的步驟 2 （上傳伺服器憑證）。
6. 如果您需要更換伺服器憑證、請選取*瀏覽*並上傳新檔案。
7. 選擇*繼續*。

   此時將顯示 Edit a Key Management Server （編輯金鑰管理伺服器）精靈的步驟 3 （上傳用戶端憑證）。
8. 如果您需要更換用戶端憑證和用戶端憑證私密金鑰、請選取*瀏覽*並上傳新檔案。
9. 選擇 * 測試並儲存 * 。

   測試金鑰管理伺服器與受影響站台上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的表格。
10. 如果出現錯誤訊息、請檢閱訊息詳細資料、然後選取*確定*。

    例如、如果您為此KMS選取的站台已由其他KMS管理、或連線測試失敗、您可能會收到「無法處理的實體」錯誤。
11. 如果您需要在解決連線錯誤之前儲存目前的組態、請選取 * 強制儲存 * 。

    選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。

    系統會儲存KMS組態。
12. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

    KMS 組態已儲存、但 KMS 的連線未經過測試。

移除金鑰管理伺服器（**KMS**）

在某些情況下、您可能會想要移除金鑰管理伺服器。例如、如果您已停用站台、可能會想要移除站台專屬的KMS。

開始之前

- 您已檢閱 "使用金鑰管理伺服器的考量與要求"。

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

關於這項工作

在下列情況下、您可以移除KMS：

- 如果站台已停用、或站台中沒有啟用節點加密的應用裝置節點、您可以移除站台專屬的KMS。
- 如果每個已啟用節點加密功能的應用裝置節點已存在站台專屬KMS、您可以移除預設KMS。

步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要移除的 KMS 、然後選取 * 動作 * > * 移除 * 。

   您也可以選取表格中的 KMS 名稱、然後從 KMS 詳細資料頁面中選取 * 移除 * 來移除 KMS 。

3. 請確認下列各項正確無誤：
   - 您正在移除網站專屬 KMS 、此網站沒有啟用節點加密的應用裝置節點。
   - 您正在移除預設的 KMS 、但每個具有節點加密的站台都已存在特定站台的 KMS 。
4. 選擇*是*。

   KMS組態隨即移除。

管理Proxy設定

設定儲存 Proxy

如果您使用的是平台服務或雲端儲存資源池、可以在儲存節點和外部S3端點之間設定不透明的Proxy。例如、您可能需要不透明的Proxy、才能將平台服務訊息傳送至外部端點、例如網際網路上的端點。

設定的儲存 Proxy 設定不適用於 Kafka 平台服務端點。

開始之前

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

關於這項工作

您可以設定單一儲存 Proxy 的設定。

步驟

1. 選擇*組態*>*安全性*>* Proxy設定*。
2. 在 * 儲存 * 標籤上、選取 * 啟用儲存代理 * 核取方塊。

3. 選取儲存 Proxy 的傳輸協定。
4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 或者、輸入用來連線至Proxy伺服器的連接埠。

   將此欄位保留空白以使用通訊協定的預設連接埠： HTTP 為 80 、 SOCKS5 為 1080 。

6. 選擇*保存*。

   儲存儲存 Proxy 之後、即可設定並測試平台服務或雲端儲存池的新端點。

   Proxy變更可能需要10分鐘才能生效。

7. 檢查Proxy伺服器的設定、確保StorageGRID 不會封鎖來自下列項目的平台服務相關訊息。
8. 如果您需要停用儲存 Proxy 、請清除核取方塊、然後選取 * 儲存 * 。

設定管理 **Proxy** 設定

如果您使用 HTTP 或 HTTPS 傳送 AutoSupport 套件、則可以在管理節點和技術支援（ AutoSupport ）之間設定不透明的 Proxy 伺服器。

如需 AutoSupport 的詳細資訊、請參閱 "設定AutoSupport 功能"。

開始之前

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

關於這項工作

您可以設定單一管理 Proxy 的設定。

步驟

1. 選擇*組態*>*安全性*>* Proxy設定*。

   此時會顯示 Proxy 設定頁面。依預設、會在索引標籤功能表中選取儲存設備。

2. 選擇 * 管理 * 標籤。
3. 選中 **Enable Admin Proxy** 複選框。
4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 輸入用來連線至Proxy伺服器的連接埠。
6. 您也可以輸入 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、請將這些欄位保留空白。

7. 選取下列其中一項：

   ◦ 如果您想要保護與管理 Proxy 的連線、請選取 * 驗證 Proxy 憑證 * 。上傳 CA 套件以驗證管理 Proxy 伺服器所提供 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、如果驗證了 Proxy 憑證、將無法運作。

上傳 CA 套件後、便會顯示其中繼資料。

。如果您不想在與管理 Proxy 伺服器通訊時驗證憑證、請選取 * 不要驗證 Proxy 憑證 * 。

8. 選擇*保存*。

儲存管理 Proxy 之後、系統會設定管理節點與技術支援之間的 Proxy 伺服器。

Proxy變更可能需要10分鐘才能生效。

9. 如果您需要停用管理 Proxy 、請清除 * 啟用管理 Proxy * 核取方塊、然後選取 * 儲存 * 。

控制防火牆

控制外部防火牆的存取

您可以在外部防火牆開啟或關閉特定連接埠。

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

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

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

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

相關資訊

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

管理內部防火牆控制

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

使用「防火牆控制」頁面上的三個索引標籤、自訂您網格所需的存取權限。

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

  此索引標籤上的設定會覆寫「管理外部存取」索引標籤中的設定。

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

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

若要設定內部防火牆控制、請參閱 "設定防火牆控制項"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

權限位址清單和管理外部存取索引標籤

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

預設情況下、特權 IP 位址沒有內部網格連接埠存取。

範例 **1** ：使用跳躍主機來執行維護工作

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

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

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

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

範例 **2**：鎖定敏感端口

假設您想要鎖定敏感連接埠和該連接埠上的服務（例如、連接埠 22 上的 SSH ）。您可以使用下列一般步驟：

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

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

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

範例 **3**：停用對未使用的服務的訪問

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

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

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

不受信任的用戶端網路索引標籤

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

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

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

範例**1**：閘道節點僅接受**HTTPS S3**要求

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

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

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

範例**2**：儲存節點傳送**S3**平台服務要求

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

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

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

範例 **3** ：將網格管理程式的存取限制在子網路上

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

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

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

設定內部防火牆

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

開始之前

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

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

關於這項工作

StorageGRID 在每個節點上都有內部防火牆、可讓您開啟或關閉網格節點上的某些連接埠。您可以使用「防火牆控制」索引標籤來開啟或關閉預設在 Grid Network 、 Admin Network 和 Client Network 上開啟的連接埠。您也可以建立權限 IP 位址清單、以存取已關閉的網格連接埠。如果您使用的是用戶端網路、您可以指定節點是否信任來自用戶端網路的傳入流量、也可以設定用戶端網路上特定連接埠的存取。

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

如需使用防火牆控制項的詳細資訊、包括範例、請參閱 "管理防火牆控制"。

如需外部防火牆和網路安全性的詳細資訊、請參閱 "控制外部防火牆的存取"。

存取防火牆控制

步驟

1. 選擇 * 組態 * > * 安全性 * > * 防火牆控制 * 。

   此頁面上的三個索引標籤如所述 "管理防火牆控制"。

2. 選取任何索引標籤以設定防火牆控制項。

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

特殊權限位址清單

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

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

「貴賓」位址清單標籤上的設定無法覆寫「不受信任的用戶端網路」標籤上的設定。

步驟

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

   將盡可能少的位址新增至權限清單。

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

   此選項會移除內部服務的某些保護。如果可能、請將其停用。

4. 選擇*保存*。

管理外部存取

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

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

步驟

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

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

   使用表格右側的捲軸、確定您已檢視所有可用的連接埠。使用搜尋欄位、輸入連接埠編號、以尋找任何外部連接埠的設定。您可以輸入部分連接埠號碼。例如，如果您輸入 **2** ，則會顯示字串 "2" 做為其名稱一部分的所有連接埠。

3. 選擇*保存*

不受信任的用戶端網路

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

如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

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

步驟

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

   視需要、您可以返回此索引標籤、變更特定新節點的設定。

   此設定不會影響StorageGRID 到您的不完善系統中現有的節點。

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

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

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

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

4. 選擇*保存*。

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

管理租戶

管理租戶：總覽

身為網格管理員、您可以建立和管理 S3 和 Swift 用戶端用來儲存和擷取物件的租戶帳戶。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

什麼是租戶帳戶？

租戶帳戶可讓您使用簡易儲存服務（S3）REST API或Swift REST API、在StorageGRID 一個無法恢復的系統中儲存及擷取物件。

每個租戶帳戶都有同盟或本機群組、使用者、 S3 貯體或 Swift 容器和物件。

租戶帳戶可用來分隔不同實體所儲存的物件。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：*如果您是在StorageGRID 企業應用程式中管理一套功能完善的系統、您可能會想要將網格的物件儲存區由組織中的不同部門加以隔離。在此案例中、您可以為行銷部門、客戶支援部門、人力資源部門等建立租戶帳戶。

  如果您使用 S3 用戶端傳輸協定、則可以使用 S3 儲存區和儲存區原則來分隔企業各部門之間的物件。您不需要使用租戶帳戶。請參閱實作說明 "S3 貯體和貯體原則" 以取得更多資訊。

- *服務供應商使用案例：*如果您以StorageGRID 服務供應商的身份管理一個支援系統、則可以將網格的物件儲存區、由將儲存設備租賃至網格的不同實體來分隔。在這種情況下、您會為公司A、公司B、公司C等建立租戶帳戶。

如需詳細資訊、請參閱 "使用租戶帳戶"。

如何建立租戶帳戶？

建立租戶帳戶時、請指定下列資訊：

- 基本資訊、包括租戶名稱、用戶端類型（ S3 或 Swift ）和選用的儲存配額。
- 租戶帳戶的權限、例如租戶帳戶是否可以使用 S3 平台服務、設定自己的身分識別來源、使用 S3 Select 或使用網格同盟連線。
- 租戶的初始根存取權、取決於 StorageGRID 系統是使用本機群組和使用者、身分識別聯盟或單一登入（ SSO ）。

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物件鎖定時、所有S3租戶帳戶都能建立及管理相容的儲存區。

租戶管理程式的用途為何？

建立租戶帳戶之後、租戶使用者可以登入租戶管理員、以執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）
- 管理群組和使用者
- 使用網格同盟進行帳戶複製和跨網格複寫
- 管理S3存取金鑰
- 建立及管理 S3 儲存區
- 使用 S3 平台服務
- 使用S3 Select
- 監控儲存使用量

> 雖然 S3 租戶使用者可以使用 Tenant Manager 來建立和管理 S3 存取金鑰和貯體、但他們必須使用 S3 用戶端應用程式來擷取和管理物件。請參閱 "使用S3 REST API" 以取得詳細資料。

> Swift使用者必須擁有root存取權限、才能存取租戶管理程式。不過、「根」存取權限不允許使用者驗證Swift REST API、以建立容器和擷取物件。使用者必須具有Swift Administrator權限、才能驗證到Swift REST API。

建立租戶帳戶

您必須建立至少一個租戶帳戶、以控制StorageGRID 對您的作業系統儲存設備的存取。

建立租戶帳戶的步驟會因是否而異 "身分識別聯盟" 和 "單一登入" 已設定、以及您用來建立租戶帳戶的Grid Manager帳戶是否屬於具有root存取權限的管理群組。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權或 Tenant 帳戶權限"。
- 如果租戶帳戶將使用為Grid Manager設定的身分識別來源、而您想要將租戶帳戶的根存取權限授予聯盟群組、則表示您已將該聯盟群組匯入Grid Manager。您不需要指派任何 Grid Manager 權限給此管理群組。請參閱 "管理管理群組"。
- 如果您想要允許 S3 租戶複製帳戶資料、並使用網格聯盟連線將貯體物件複寫到其他網格：

- 您有 "已設定網格同盟連線"。
- 連線狀態為 * 已連線 * 。
- 您擁有root存取權限。
- 您已檢閱的考量事項 "管理 Grid Federation 的允許租戶"。
- 如果租戶帳戶將使用為 Grid Manager 設定的身分識別來源、則您已將相同的聯盟群組匯入兩個網格上的 Grid Manager 。

  當您建立租戶時、您將會選取此群組、以取得來源和目的地租戶帳戶的初始根存取權限。

如果在您建立租戶之前、這兩個網格上都不存在這個管理群組、則租戶不會複寫到目的地。

存取精靈

步驟

1. 選取*租戶*。
2. 選擇* Create （建立）。

輸入詳細資料

步驟

1. 輸入租戶的詳細資料。

欄位	說明
名稱	租戶帳戶的名稱。租戶名稱不一定是唯一的。建立租戶帳戶時、它會收到唯一的 20 位數帳戶 ID 。
說明（選用）	協助識別租戶的說明。 如果您要建立將使用網格同盟連線的租用戶、請選擇性使用此欄位來協助識別來源租戶和目的地租戶。例如、對於在 Grid 1 上建立的租戶、此描述也會顯示給複製到 Grid 2 的租戶：「此租戶是在 Grid 1 上建立的。」
用戶端類型	此租戶將使用的用戶端傳輸協定類型、可以是 * S2* 或 * Swift * 。 • 附註 * ： Swift 用戶端應用程式的支援已過時、將於未來版本中移除。
儲存配額（選用）	如果您想要此租用戶擁有儲存配額、則需要配額和單位的數值。

2. 選擇*繼續*。

[[admin-租 戶選取權限 **]]** 選取權限

步驟

1. 或者、選取您想要此租用戶擁有的任何權限。

其中有些權限有額外的需求。如需詳細資料、請選取每個權限的說明圖示。

權限	如果選取 ...
允許平台服務	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"。
使用自己的身分識別來源	租戶可以為同盟群組和使用者設定及管理自己的身分識別來源。如果您有、此選項會停用 "已設定 SSO" 適用於您的 StorageGRID 系統。
允許 S3 Select	租戶可以發出 S3 SelectObjectContent API 要求、以篩選及擷取物件資料。請參閱 "管理用戶帳戶的S3 Select"。 • 重要 * ： SelectObjectContent 要求可降低所有 S3 用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。
使用網格同盟連線	租戶可以使用網格同盟連線。 選取此選項： • 使此租用戶和新增至帳戶的所有租戶群組和使用者、從這個網格（ _ 來源網格 _ ）複製到所選連線（ _ 目的地網格 _ ）的其他網格。 • 允許此租戶在每個網格上對應的儲存格之間設定跨網格複寫。 請參閱 "管理 Grid Federation 的允許租戶"。

2. 如果您選取 * 使用網格同盟連線 * 、請選取其中一個可用的網格同盟連線。

3. 選擇*繼續*。

定義 root 存取權並建立租戶

步驟

1. 根據您的 StorageGRID 系統是使用身分識別聯盟、單一登入（ SSO ）或兩者、定義租戶帳戶的根存取權。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。

選項	請這麼做
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

2. 選取*建立租戶*。

   成功訊息隨即出現、新的租戶會列在租戶頁面上。若要瞭解如何檢視租戶詳細資料及監控租戶活動、請參閱 "監控租戶活動"。

3. 如果您為租用戶選取 * 使用網格同盟連線 * 權限：

   a. 確認已將相同的租戶複寫到連線中的其他網格。兩個網格上的租戶將擁有相同的 20 位數帳戶 ID 、名稱、說明、配額和權限。

      如果您看到錯誤訊息「 Tenant Created without a clone 」、請參閱中的指示 "疑難排解網格同盟錯誤"。

   b. 如果您在定義 root 存取權限時提供本機 root 使用者密碼、 "變更本機 root 使用者的密碼" 適用於複寫的租戶。

      在變更密碼之前、本機根使用者無法在目的地網格上登入租戶管理程式。

登入租戶（選用）

視需要、您可以立即登入新租戶以完成組態、或是稍後登入租戶。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 "控制外部防火牆的存取"。

立即登入

如果您使用...	執行此動作...
連接埠 443 和您為本機 root 使用者設定密碼	1. 選取 * 以 root 登入 * 。 當您登入時、會出現連結以設定貯體、身分識別聯盟、群組和使用者。 2. 選取連結以設定租戶帳戶。 每個連結都會在租戶管理程式中開啟對應的頁面。若要完成頁面、請參閱 "租戶帳戶使用說明"。
連接埠 443 並未設定本機根使用者的密碼	選取 * 登入 * 、然後在根存取聯盟群組中輸入使用者的認證。

如果您使用...	執行此動作...
受限連接埠	1. 選擇 * 完成 * 2. 請在「租戶」表格中選取 * 限制 * 、以深入瞭解如何存取此租戶帳戶。 租戶管理程式的URL格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 是管理節點的完整網域名稱或IP位址 ◦ *port* 為租戶專用連接埠 ◦ *20-digit-account-id* 是租戶的唯一帳戶ID

稍後登入

如果您使用...	請執行下列其中一項...
連接埠 443	• 從Grid Manager中選取*租戶*、然後選取租戶名稱右側的*登入*。 • 在網頁瀏覽器中輸入租戶的URL： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 是管理節點的完整網域名稱或IP位址 ◦ *20-digit-account-id* 是租戶的唯一帳戶ID
受限連接埠	• 從Grid Manager中選取*租戶*、然後選取*受限*。 • 在網頁瀏覽器中輸入租戶的URL： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* 是管理節點的完整網域名稱或IP位址 ◦ *port* 為租戶專用的受限連接埠 ◦ *20-digit-account-id* 是租戶的唯一帳戶ID

設定租戶

依照中的指示操作 "使用租戶帳戶" 若要管理租戶群組和使用者、 S3 存取金鑰、工作區、平台服務、以及帳戶複製和跨網格複寫。

編輯租戶帳戶

您可以編輯租戶帳戶、以變更顯示名稱、儲存配額或租戶權限。

如果租戶具有 * 使用網格同盟連線 * 權限、您可以從連線中的任一網格編輯租戶詳細資料。不過、您在連線中的某個網格上所做的任何變更、都不會複製到另一個網格。如果您想要讓租戶詳細資料在網格之間保持完全同步、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

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權或 Tenant 帳戶權限"。

步驟

1. 選取*租戶*。

2. 找出您要編輯的租戶帳戶。

   使用搜尋方塊、依名稱或租戶 ID 搜尋租戶。

3. 選取租戶。您可以執行下列其中一項：
   - 選取租戶的核取方塊、然後選取 * 動作 * > * 編輯 * 。
   - 選取租戶名稱以顯示詳細資料頁面、然後選取 * 編輯 * 。
4. 您也可以變更這些欄位的值：
   - 名稱
   - 說明
   - 儲存配額
5. 選擇*繼續*。
6. 選取或清除租戶帳戶的權限。
   - 如果您停用已在使用的租戶*平台服務*、則他們針對S3儲存區所設定的服務將停止運作。不會傳送錯誤訊息給租戶。例如、如果租戶已設定S3儲存區的CloudMirror複寫、他們仍可將物件儲存在儲存區中、但

這些物件的複本將不再建立在已設定為端點的外部S3儲存區中。請參閱 "管理S3租戶帳戶的平台服務"。

- 變更 * 使用自己的身分識別來源 * 的設定、以判斷租戶帳戶是使用自己的身分識別來源、還是使用為 Grid Manager 設定的身分識別來源。

  如果 * 使用自己的身分識別來源 * ：

  - 已停用並選取、租戶已啟用自己的身分識別來源。租戶必須先停用其身分識別來源、才能使用為Grid Manager設定的身分識別來源。
  - 已停用且未選取、 StorageGRID 系統會啟用 SSO 。租戶必須使用為Grid Manager設定的身分識別來源。

- 視需要選取或清除 * 允許 S3 選取 * 權限。請參閱 "管理用戶帳戶的S3 Select"。
- 若要移除 * 使用網格同盟連線 * 權限：

  i. 前往租戶的詳細資料頁面。

  ii. 選取 * Grid Federation * 標籤。

  iii. 選取 * 移除權限 * 。

- 若要新增 * 使用網格同盟連線 * 權限：

  i. 選中 * 使用網格聯合連接 * 複選框。

  ii. 或者、選取 * 複製現有的本機使用者和群組 * 、將其複製到遠端網格。如果需要、您可以停止正在進行的複製、或是在完成最後一次複製作業之後、如果無法複製某些本機使用者或群組、請重試複製。

變更租戶本機**root**使用者的密碼

如果root使用者被鎖定在帳戶之外、您可能需要變更租戶本機root使用者的密碼。

開始之前

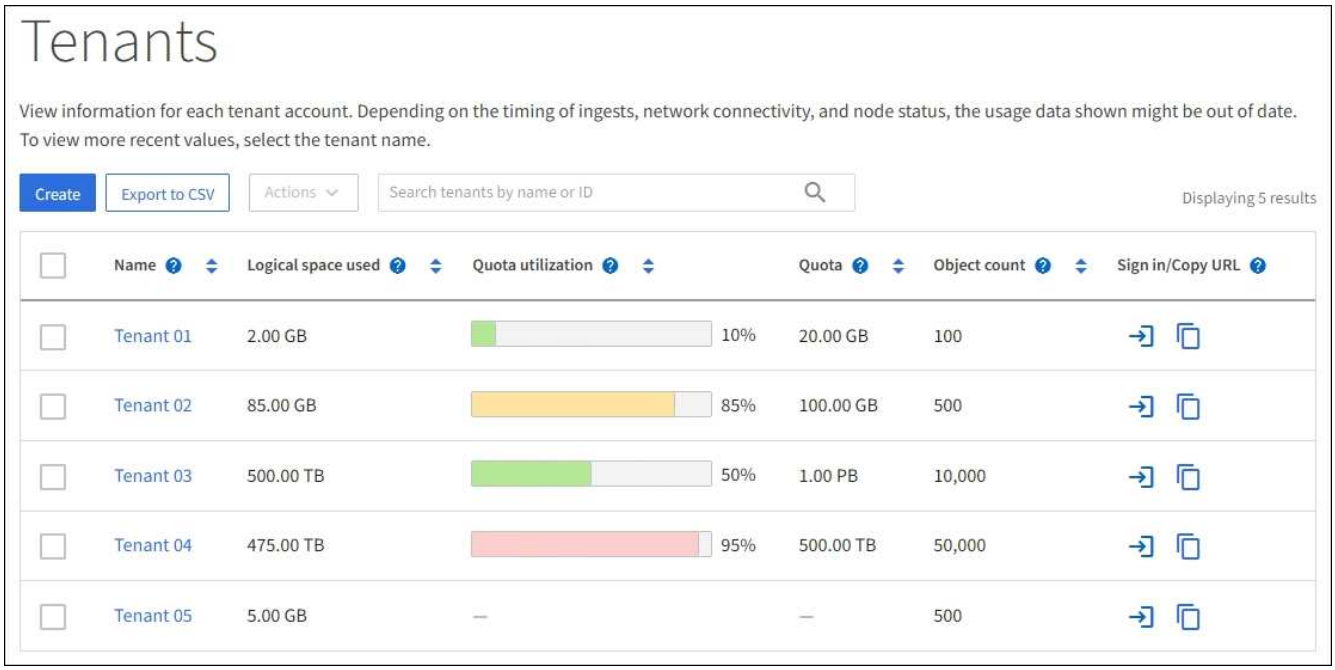
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。

關於這項工作

如果您的 StorageGRID 系統已啟用單一登入（ SSO ）、則本機根使用者無法登入租戶帳戶。若要執行root使用者工作、使用者必須屬於擁有租戶根存取權限的聯盟群組。

步驟

1. 選取*租戶*。



2. 選取租戶帳戶。您可以執行下列其中一項：
   - 選取租戶的核取方塊、然後選取 * 動作 * > * 變更 root 密碼 * 。
   - 選取租戶名稱以顯示詳細資料頁面、然後選取 * 動作 * > * 變更 root 密碼 * 。
3. 輸入租戶帳戶的新密碼。
4. 選擇*保存*。

刪除租戶帳戶

若要永久移除租戶對系統的存取權、您可以刪除租戶帳戶。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已移除與租戶帳戶相關的所有貯體（ S3 ）、容器（ Swift ）和物件。
- 如果租戶獲准使用網格同盟連線、您已檢閱的考量事項 "刪除具有使用網格同盟連線權限的租用戶"。

步驟

1. 選取*租戶*。
2. 找出您要刪除的租戶帳戶。

   使用搜尋方塊、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 * 動作 * > * 刪除 * 。
4. 若要刪除單一租戶、請執行下列其中一項：
   - 選取核取方塊、然後選取 * 動作 * > * 刪除 * 。
   - 選取租戶名稱以顯示詳細資料頁面、然後選取 * 動作 * > * 刪除 * 。

5. 選擇*是*。

管理平台服務

管理租戶平台服務：總覽

如果您為S3租戶帳戶啟用平台服務、則必須設定網格、讓租戶能夠存取使用這些服務所需的外部資源。

什麼是平台服務？

平台服務包括CloudMirror複寫、事件通知及搜尋整合服務。

CloudMirror複寫

StorageGRID CloudMirror 複寫服務用於將特定物件從 StorageGRID 儲存庫鏡射到指定的外部目的地。

例如、您可以使用CloudMirror複寫將特定的客戶記錄鏡射到Amazon S3、然後利用AWS服務對資料執行分析。

CloudMirror 複寫與跨網格複寫功能有一些重要的相似之處和差異。若要深入瞭解、請參閱 "比較跨網格複寫和 CloudMirror 複寫"。

如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。

通知

每個貯體事件通知可用於傳送有關物件上執行之特定動作的通知至指定的外部 Kafka 叢集或 Amazon Simple Notification Service 。

例如、您可以設定要傳送警示給系統管理員、以通知新增至儲存區的每個物件、其中物件代表與重大系統事件相關的記錄檔。

雖然事件通知可在已啟用S3物件鎖定的儲存區上設定、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

搜尋整合服務

搜尋整合服務用於將 S3 物件中繼資料傳送至指定的彈性搜尋索引、以便使用外部服務搜尋或分析中繼資料。

例如、您可以設定儲存區、將S3物件中繼資料傳送至遠端Elasticsearch服務。然後您可以使用Elasticsearch來執行跨儲存區的搜尋、並對物件中繼資料中的模式進行精密分析。

雖然可在啟用S3物件鎖定的儲存區上設定Elasticsearch整合、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

平台服務可讓租戶將外部儲存資源、通知服務、以及搜尋或分析服務與資料一起使用。由於平台服務的目標位置通常是StorageGRID 不適用於您的非執行部署、因此您必須決定是否允許租戶使用這些服務。如果您這麼做、則必須在建立或編輯租戶帳戶時啟用平台服務的使用。您也必須設定網路、讓租戶產生的平台服務訊息能夠到達目的地。

在使用平台服務之前、請注意下列建議：

- 如果StorageGRID 在支援版本管理和CloudMirror複寫功能的情況下、在整個系統中的S3儲存區中、您也應該為目的地端點啟用S3儲存區版本管理功能。這可讓CloudMirror複寫在端點上產生類似的物件版本。
- 您不應使用超過100個主動租戶、而S3要求需要CloudMirror複寫、通知和搜尋整合。擁有超過100個作用中租戶可能會導致S3用戶端效能變慢。
- 對於無法完成的端點的要求、將會排入最多 50 、 000 個要求的佇列。此限制在作用中租戶之間平均分攤。新租戶可暫時超逾這 50 萬個限額，以免新增租戶受到不公平的懲罰。

相關資訊

- "管理平台服務"
- "設定儲存Proxy設定"
- "監控 StorageGRID"

平台服務的網路和連接埠

如果您允許S3租戶使用平台服務、則必須設定網格的網路連線、以確保平台服務訊息可傳送至目的地。

您可以在建立或更新租戶帳戶時、為S3租戶帳戶啟用平台服務。如果已啟用平台服務、租戶可以建立端點、做為CloudMirror複寫、事件通知或從S3儲存區搜尋整合訊息的目的地。這些平台服務訊息會從執行ADC服務的儲存節點傳送至目的地端點。

例如、租戶可能會設定下列類型的目的地端點：

- 本機代管的彈性搜尋叢集
- 支援接收 Amazon Simple Notification Service 訊息的本機應用程式
- 本地託管的 Kafka 叢集
- 本地託管的S3儲存區位於StorageGRID 相同或其他的例子
- 外部端點、例如Amazon Web Services上的端點。

若要確保平台服務訊息能夠傳送、您必須設定含有「ADC儲存節點」的網路。您必須確保下列連接埠可用於傳送平台服務訊息至目的地端點。

根據預設、平台服務訊息會在下列連接埠上傳送：

- **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StorageGRID 將某個支援區部署做為CloudMirror複寫的目的地、則複寫訊息可能會在80或443以外的連接埠接收。確保StorageGRID 端點中已指定目的地支援的S3連接埠。

如果您使用不透明的Proxy伺服器、也必須使用 "設定儲存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。

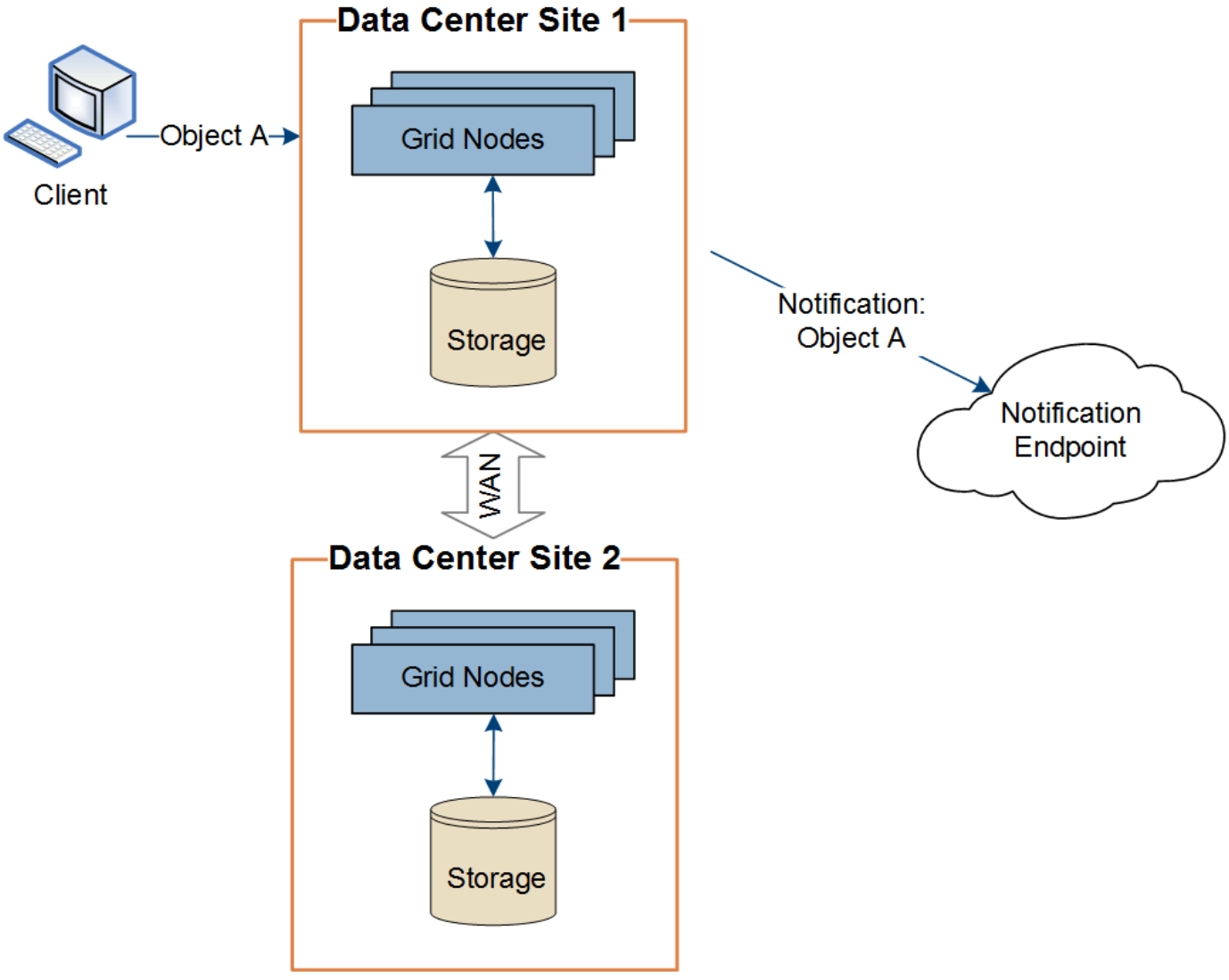
相關資訊

- "使用租戶帳戶"

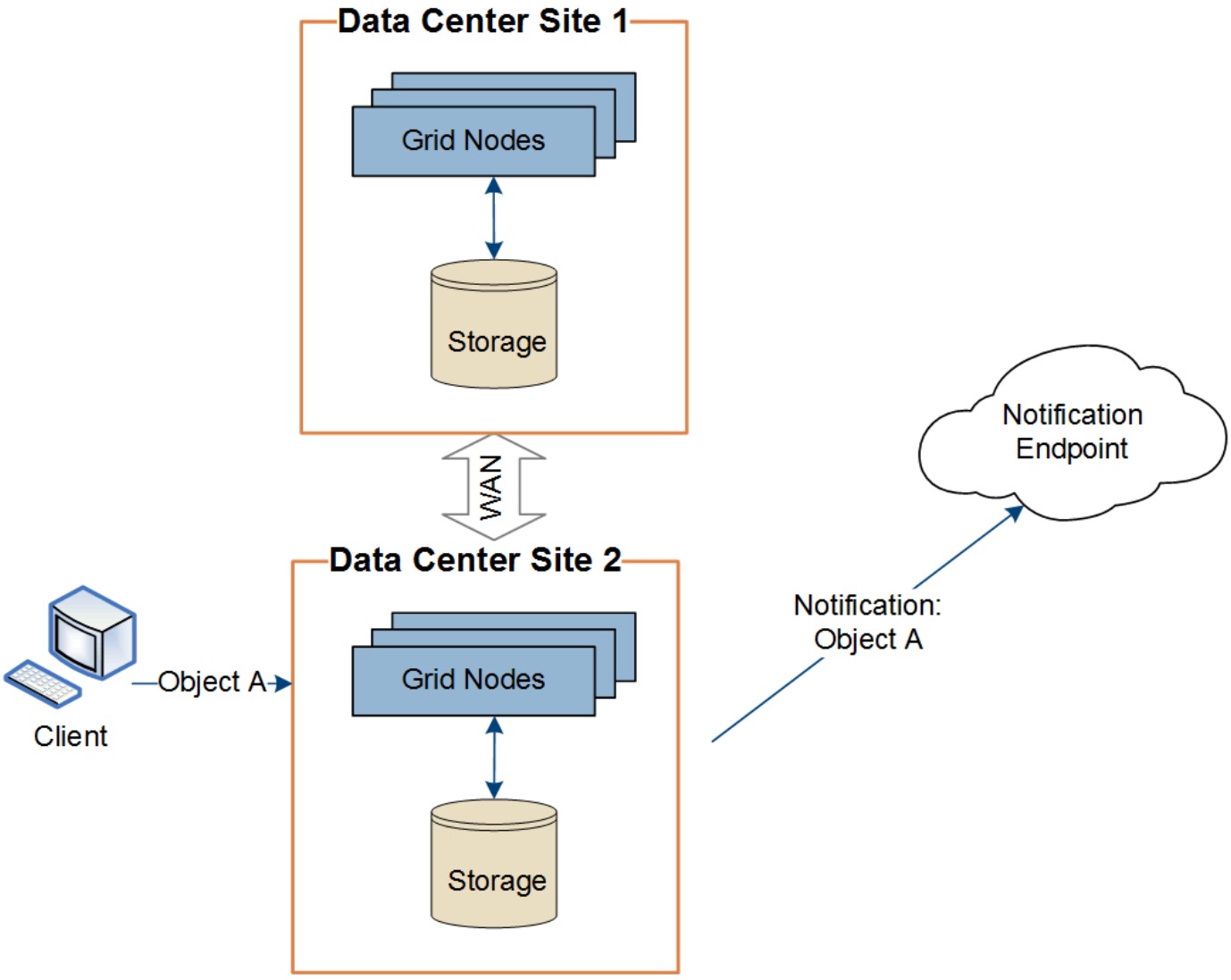
每個站台提供平台服務訊息

所有平台服務作業都是以每個站台為基礎來執行。

也就是、如果租戶使用用戶端連線至資料中心站台1的閘道節點、在物件上執行S3 API建立作業、則會觸發該動作的通知、並從資料中心站台1傳送。



如果用戶端隨後在資料中心站台2的相同物件上執行S3 API刪除作業、則會觸發有關刪除動作的通知、並從資料中心站台2傳送。



請確定每個站台的網路設定都能讓平台服務訊息傳送到目的地。

疑難排解平台服務

平台服務中使用的端點是由租戶使用者在租戶管理程式中建立和維護、但是、如果租戶在設定或使用平台服務時遇到問題、您可能可以使用Grid Manager來協助解決問題。

新端點的問題

租戶必須先使用租戶管理程式建立一或多個端點、才能使用平台服務。每個端點代表一個平台服務的外部目的地、例如 StorageGRID S3 儲存庫、 Amazon Web Services 儲存庫、 Amazon Simple Notification Service 主題、 Kafka 主題、或本地或 AWS 上託管的 ElasticSearch 叢集。每個端點都包括外部資源的位置、以及存取該資源所需的認證資料。

當租戶建立端點時StorageGRID 、此驗證系統會驗證端點是否存在、以及是否可以使用指定的認證來達到端點。端點的連線會從每個站台的一個節點驗證。

如果端點驗證失敗、會出現錯誤訊息、說明端點驗證失敗的原因。租戶使用者應解決此問題、然後再次嘗試建立端點。

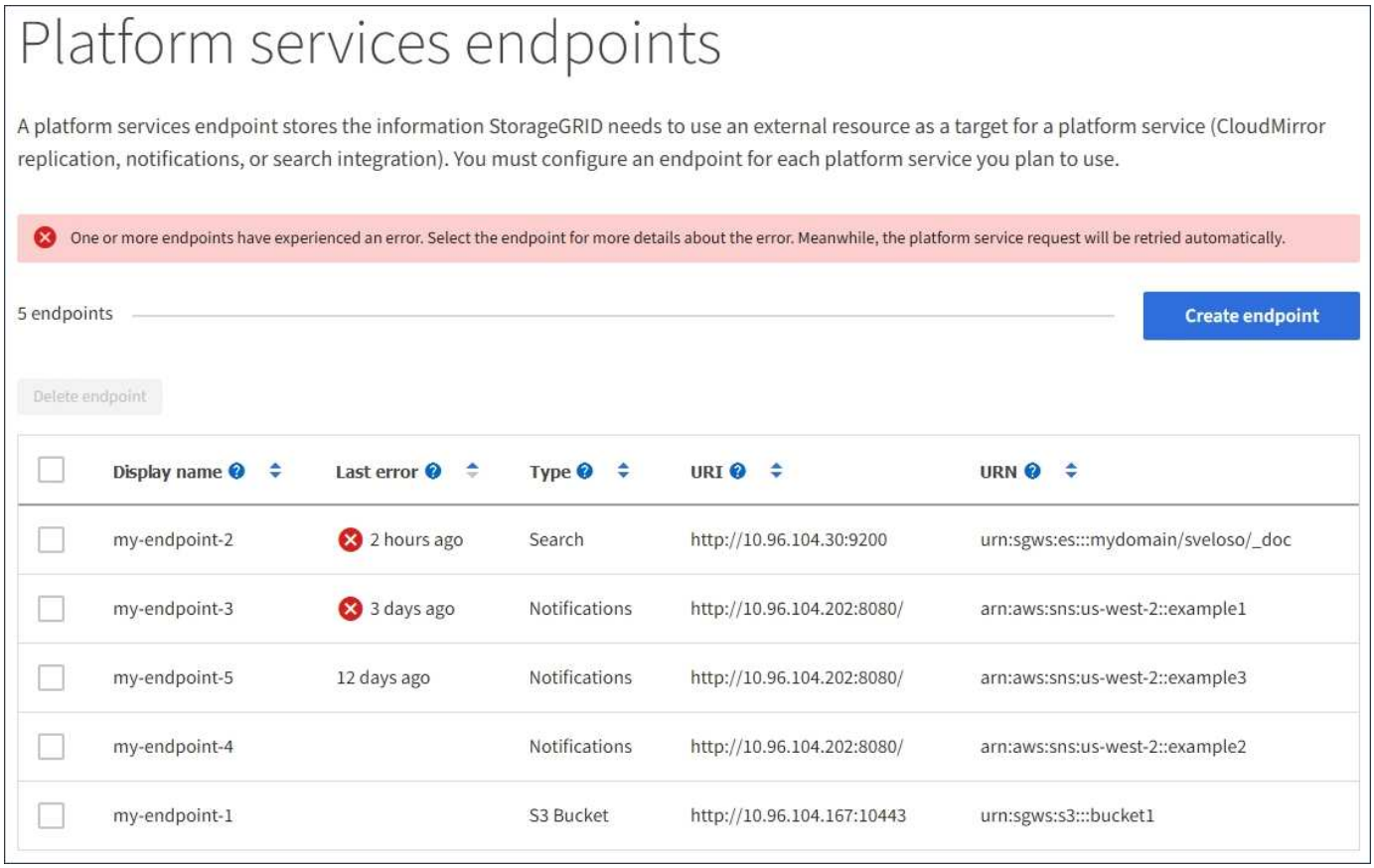
如果未啟用租戶帳戶的平台服務、端點建立將會失敗。

現有端點的問題

如果 StorageGRID 嘗試連線至現有端點時發生錯誤、租戶管理程式的儀表板上會顯示訊息。

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.

租戶使用者可前往「端點」頁面、檢閱每個端點的最新錯誤訊息、並判斷錯誤發生時間多久前。「最後一個錯誤」欄會顯示每個端點的最新錯誤訊息、並指出錯誤發生時間已多久。包括的錯誤 過去7天內出現圖示。



*最後一個錯誤*欄中的某些錯誤訊息可能會在括弧中包含一個記錄ID。網格管理員或技術支援人員可以使用此ID、在bytcast記錄中找到更多有關錯誤的詳細資訊。

與**Proxy**伺服器相關的問題

如果您已設定 "儲存代理伺服器" 在儲存節點與平台服務端點之間、如果您的 Proxy 服務不允許來自 StorageGRID 的訊息、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、確保平台服務相關訊息不會遭到封鎖。

確定是否發生錯誤

如果過去 7 天內發生任何端點錯誤、租戶管理程式中的儀表板會顯示警示訊息。您可以前往「端點」頁面、查看更多錯誤的詳細資料。

用戶端作業失敗

某些平台服務問題可能會導致S3儲存區上的用戶端作業失敗。例如、如果內部複寫狀態機器（RSM）服務停止、或是有太多平台服務訊息排入佇列等待傳送、S3用戶端作業就會失敗。

若要檢查服務狀態：

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「站台_>*儲存節點_*>* SUS*>*服務*」。

可恢復和不可恢復的端點錯誤

建立端點之後、平台服務要求可能會因為各種原因而發生錯誤。使用者介入可恢復部分錯誤。例如、可能會發生可恢復的錯誤、原因如下：

- 使用者的認證資料已刪除或過期。
- 目的地庫位不存在。
- 無法傳送通知。

如果遇到可恢復的錯誤、平台服務要求將會重試、直到成功為止。StorageGRID

其他錯誤無法恢復。例如、如果刪除端點、就會發生無法恢復的錯誤。

如果遇到不可恢復的端點錯誤、則會在Grid Manager中觸發Total Event（SMT）舊版警示。StorageGRID若要檢視「事件總數」老舊警示：

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇*站台_*>*節點_*>* SUS*>*事件*。
3. 檢視表格頂端的「上次事件」。

   中也會列出事件訊息 `/var/local/log/bycast-err.log`。

4. 請遵循SMTT警示內容中提供的指引來修正問題。
5. 選取*組態*索引標籤以重設事件計數。
6. 通知租戶其平台服務訊息尚未傳送的物件。
7. 指示租戶透過更新物件的中繼資料或標記、重新觸發失敗的複寫或通知。

   租戶可以重新提交現有的值、以避免進行不必要的變更。

無法傳送平台服務訊息

如果目的地遇到問題、導致無法接受平台服務訊息、用戶端在儲存庫上的操作就會成功、但平台服務訊息卻無法傳送。例如、如果目的地上的認證資料已更新、StorageGRID 導致無法再驗證目的地服務、就可能發生此錯誤。

如果由於不可恢復的錯誤而無法傳送平台服務訊息、則會在 Grid Manager 中觸發 Total Events （ SMTT ）舊版警示。

平台服務要求的效能變慢

如果傳送要求的速度超過目的地端點接收要求的速度、則支援使用此軟體來限制傳入S3的貯體要求。StorageGRID節流只會在有待傳送至目的地端點的要求待處理項目時發生。

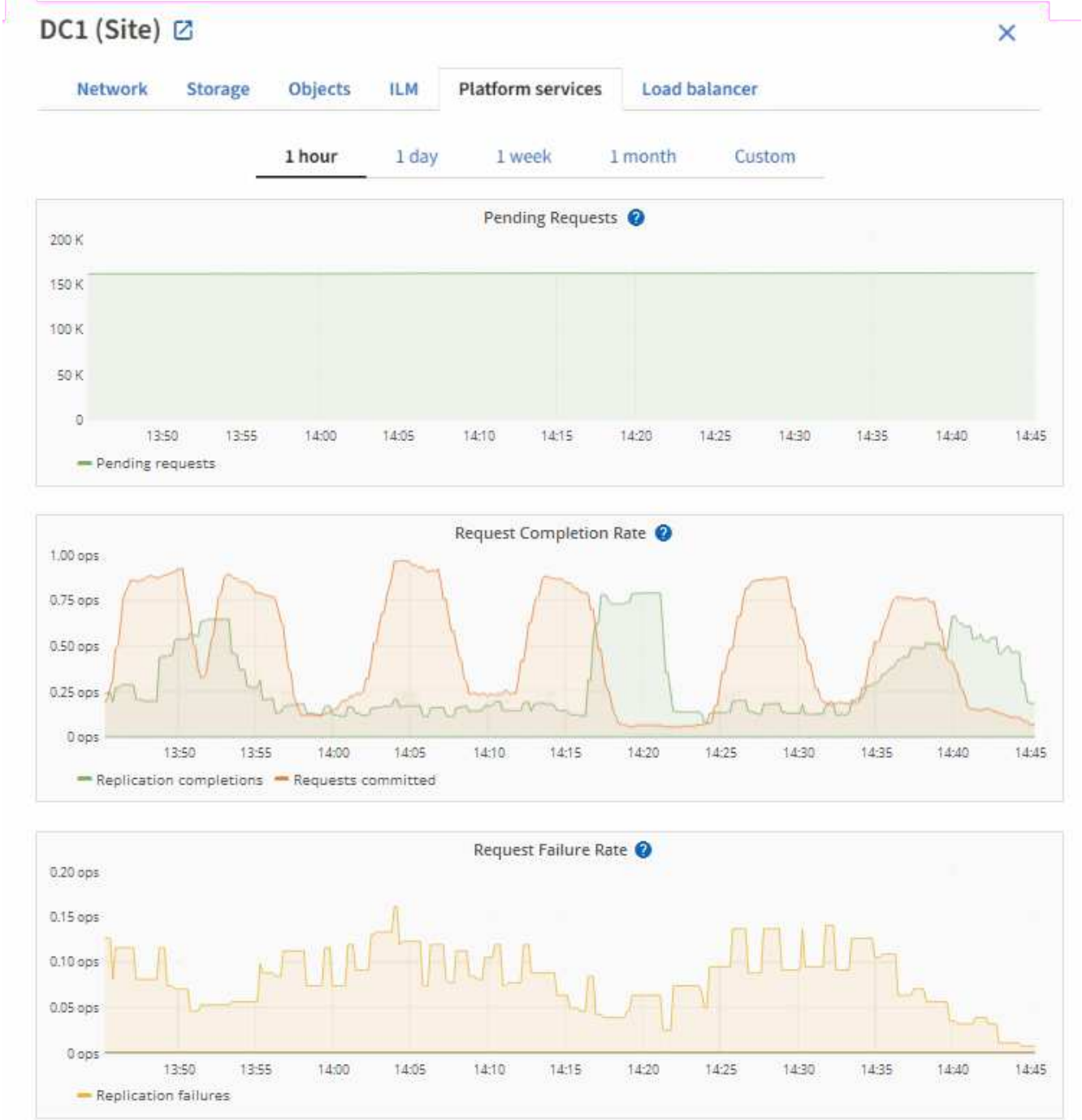
唯一的可見效果是傳入S3要求執行時間較長。如果您開始偵測到效能大幅降低、應該降低擷取速度、或是使用容量較大的端點。如果要求的待處理項目持續增加、用戶端S3作業（例如PUT要求）最終將會失敗。

CloudMirror要求較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資料傳輸。

平台服務要求失敗

若要檢視平台服務的要求失敗率：

1. 選擇*節點*。
2. 選擇「站台_>*平台服務*」。
3. 檢視「要求錯誤率」圖表。



平台服務無法使用警示

*平台服務無法使用*警示表示站台無法執行平台服務作業、因為有太少的儲存節點正在執行或可用、因此無法在站台上執行平台服務作業。

此RSM服務可確保平台服務要求會傳送至各自的端點。

若要解決此警示、請判斷站台上的哪些儲存節點包含了RSM服務。（同時包含ADC服務的儲存節點上會有此RSM服務。） 然後、請確保大部分的儲存節點都在執行中且可供使用。

如果站台上有多個包含RSM服務的儲存節點故障、您就會遺失該站台的任何擱置中平台服務要求。

平台服務端點的其他疑難排解指南

如需其他資訊、請參閱 使用租戶帳戶 › 疑難排解平台服務端點。

相關資訊

- "疑難排解 StorageGRID 系統"

管理用戶帳戶的S3 Select

您可以允許某些S3租戶使用S3 Select針對個別物件發出SelectObjectContent要求。

S3 Select提供一種有效率的方法來搜尋大量資料、而不需要部署資料庫和相關資源來啟用搜尋。它也能降低擷取資料的成本與延遲。

什麼是S3 Select？

S3 Select可讓S3用戶端使用SelectObjectContent要求來篩選及擷取物件所需的資料。S3 Select的支援功能包括S3 Select命令與功能的子集。StorageGRID

使用S3 Select的考量與要求

網格管理需求

網格管理員必須授予租戶 S3 Select 權限。選取*「允許S3選取*時機」 "建立租戶" 或 "編輯租戶"。

物件格式需求

您要查詢的物件必須採用下列其中一種格式：

- * CSV* 。可依原樣使用、也可壓縮至 GZIP 或 bzip2 歸檔。
- * 硬地板 * 。硬地板物件的其他需求：
  - S3 Select 僅支援使用 GZIP 或 Snappy 進行柱式壓縮。S3 Select 不支援 Parquet 物件的全物件壓縮。
  - S3 Select 不支援硬地板輸出。您必須將輸出格式指定為 CSV 或 JSON 。
  - 最大未壓縮列群組大小為 512 MB 。
  - 您必須使用物件架構中指定的資料類型。
  - 您無法使用時間間隔、 JSON 、清單、時間或 UUID 邏輯類型。

端點需求

必須將SelectObjectContent要求傳送至 "負載平衡器端點StorageGRID"。

端點使用的管理節點和閘道節點必須是下列其中一項：

- 服務應用裝置節點
- VMware 型軟體節點
- 執行核心且啟用 cgroup v2 的裸機節點

一般考量

查詢無法直接傳送至儲存節點。

SelectObjectContent要求可降低所有S3用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。

請參閱 "使用S3 Select的說明"。

以檢視 "Grafana圖表" 對於S3 Select作業、請在Grid Manager中選取* support*>* Tools*>* Metrics *。

設定用戶端連線

設定 **S3** 和 **Swift** 用戶端連線：總覽

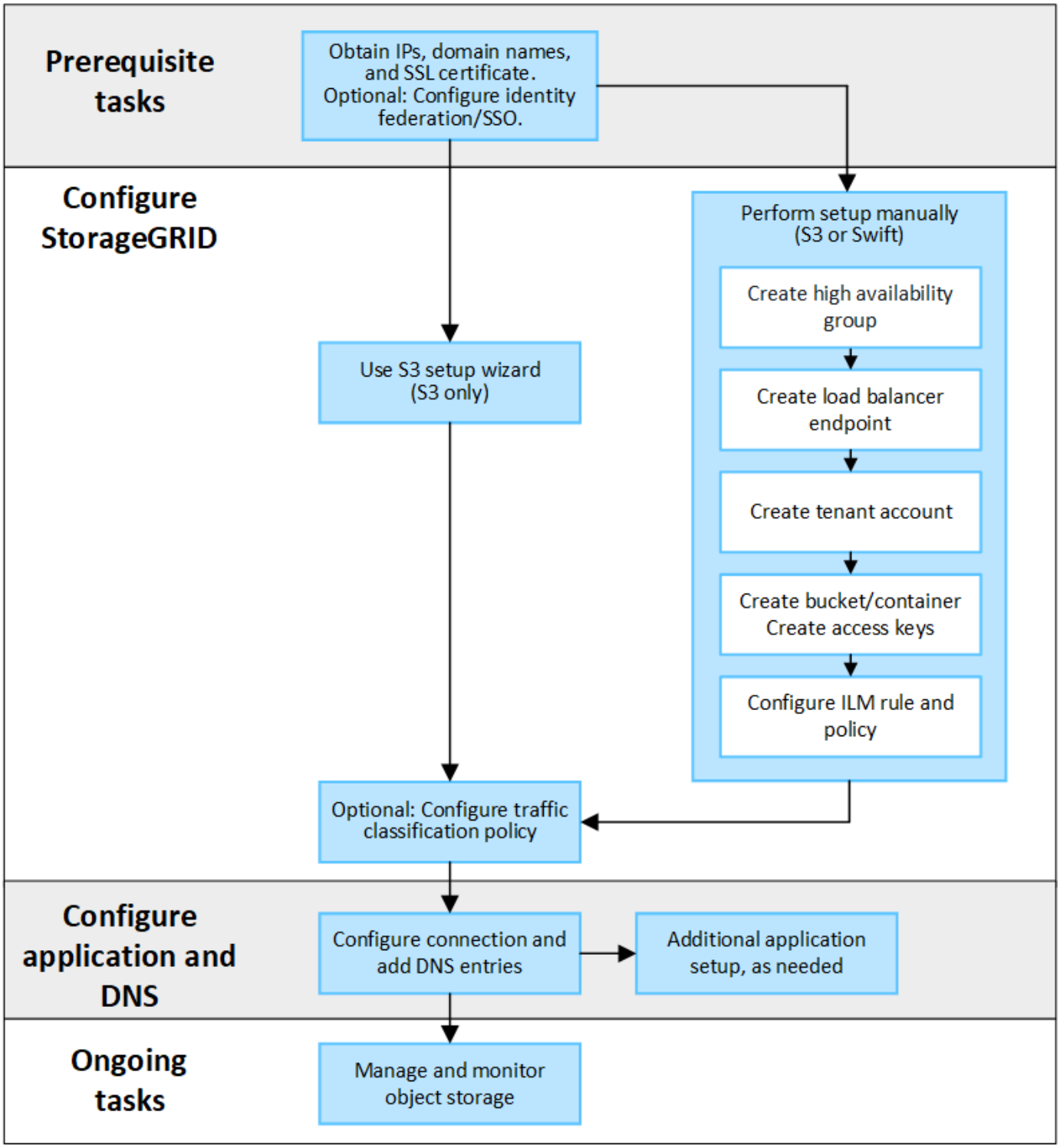
身為網格管理員、您可以管理組態選項、以控制 S3 和 Swift 用戶端應用程式如何連線至 StorageGRID 系統、以儲存和擷取資料。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

組態工作流程

如工作流程圖所示、將 StorageGRID 連接至任何 S3 或 Swift 應用程式有四個主要步驟：

1. 根據用戶端應用程式與 StorageGRID 的連線方式、在 StorageGRID 中執行必要工作。
2. 使用 StorageGRID 取得應用程式連線至網格所需的值。您可以使用 S3 設定精靈、或手動設定每個 StorageGRID 實體。
3. 使用 S3 或 Swift 應用程式完成 StorageGRID 連線。建立 DNS 項目、將 IP 位址與您打算使用的任何網域名稱建立關聯。
4. 在應用程式和 StorageGRID 中執行持續的工作、以隨時間而管理和監控物件儲存。



將 **StorageGRID** 附加至用戶端應用程式所需的資訊

在您將 StorageGRID 附加到 S3 或 Swift 用戶端應用程式之前、您必須先在 StorageGRID 中執行組態步驟、並取得特定值。

我需要什麼價值？

下表顯示您必須在 StorageGRID 中設定的值、以及 S3 或 Swift 應用程式和 DNS 伺服器使用這些值的位置。

價值	其中已設定值	使用值的位置
虛擬 IP （ VIP ）位址	StorageGRID > HA 群組	DNS 項目
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
伺服器名稱（ FQDN ）	StorageGRID > 負載平衡器端點	• 用戶端應用程式 • DNS 項目
S3 存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租戶與貯體	用戶端應用程式
貯體 / 容器名稱	StorageGRID > 租戶與貯體	用戶端應用程式

如何取得這些價值？

視您的需求而定、您可以執行下列任一動作來取得所需資訊：

- * 使用 "S3 設定精靈"*。S3 安裝精靈可協助您快速設定 StorageGRID 中的必要值、並輸出一個或兩個檔案、供您在設定 S3 應用程式時使用。精靈會引導您完成必要步驟、並協助確保您的設定符合 StorageGRID 最佳實務做法。

  如果您正在設定 S3 應用程式、建議您使用 S3 安裝精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 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、並輸出可在 ONTAP 中設定 FabricPool 雲端層時使用的檔案。

  如果您計畫將 StorageGRID 作為 FabricPool 雲端層的物件儲存系統、建議您使用 FabricPool 設定精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 手動設定項目 * 。如果您要連線至 Swift 應用程式（或是連線至 S3 應用程式、而不想使用 S3 安裝精靈）、您可以手動執行組態來取得所需的值。請遵循下列步驟：

  a. 設定您要用於 S3 或 Swift 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 或 Swift 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 或 Swift 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、然後為每個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. 在租戶帳戶內建立一或多個 S3 貯體或 Swift 容器。如需 S3 的詳細資訊、請參閱 "建立S3儲存區"。若要使用 Swift 、請使用 "提交容器要求"。

  f. 若要為屬於新租戶或貯體 / 容器的物件新增特定放置指示、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原則"。

S3 或 Swift 用戶端的安全性

StorageGRID 租戶帳戶使用 S3 或 Swift 用戶端應用程式、將物件資料儲存至 StorageGRID 。您應該檢閱為用戶端應用程式實作的安全性措施。

摘要

下表摘要說明如何為 S3 和 Swift REST API 實作安全性：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X．509伺服器憑證
用戶端驗證	**S3** S3 帳戶（存取金鑰 ID 和秘密存取金鑰） **Swift** Swift 帳戶（使用者名稱和密碼）
用戶端授權	**S3** 貯體擁有權及所有適用的存取控制原則 **Swift** 系統管理員角色存取

StorageGRID 如何為用戶端應用程式提供安全性

S3 和 Swift 用戶端應用程式可以連線至 Gateway 節點或管理節點上的負載平衡器服務、或直接連線至 Storage Node 。

- 連線至負載平衡器服務的用戶端可以根據您的方式使用 HTTPS 或 HTTP "設定負載平衡器端點"。

  HTTPS 提供安全的 TLS 加密通訊、建議使用。您必須將安全性憑證附加至端點。

  HTTP 提供較不安全的未加密通訊、只能用於非正式作業或測試網格。

- 連線至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 提供較不安全、未加密的通訊、但可選擇性使用 "已啟用" 適用於非正式作業或測試網格。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與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StorageGRID 給才能執行REST API作業。請參閱 "驗證要求" 和 "支援

的Swift API端點"。

安全性憑證與用戶端應用程式

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線到負載平衡器服務時、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 &#8212 ；網格管理員上傳的自訂伺服器憑證、或是網格管理員在設定端點時在 StorageGRID 中產生的憑證。

  請參閱 "負載平衡考量"。

- 當用戶端應用程式直接連線至儲存節點時、它們會使用安裝 StorageGRID 系統（由系統憑證授權單位簽署）時為儲存節點產生的系統產生的伺服器憑證、 或是由網格管理員提供給網格的單一自訂伺服器憑證。請參閱 "新增自訂 S3 或 Swift API 憑證"。

用戶端應設定為信任已簽署其用於建立TLS連線之任何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 系統支援一組加密套件、用戶端應用程式可在建立 TLS 工作階段時使用這些套件。要配置加密算法，請轉至 * 配置 * > * 安全性 * > * 安全性設置 * ，然後選擇 *TLS 和 SSH 策略 * 。

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

> 不再支援SSLv3和TLS 1.1（或更早版本）。

使用 **S3** 設定精靈

使用 **S3** 設定精靈：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 安裝精靈會引導您完成每個步驟、設定 StorageGRID 以搭配 S3 應用程式使用。在完成精靈的過程中、您可以下載檔案、以便在 S3 應用程式中輸入值。使用精靈可更快速地設定您的系統、並確保您的設定符合 StorageGRID 最佳實務做法。

如果您有 "root 存取權限"、您可以在開始使用 StorageGRID Grid Manager 時完成 S3 設定精靈、也可以隨時存取並完成精靈。視您的需求而定、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

使用精靈之前、請確認您已完成這些先決條件。

取得 **IP** 位址並設定 **VLAN** 介面

如果您要設定高可用度（ HA ）群組、就會知道 S3 應用程式將連線到哪些節點、以及將使用哪個 StorageGRID 網路。您也知道要輸入哪些子網路 CIDR 、閘道 IP 位址和虛擬 IP （ VIP ）位址值。

如果您打算使用虛擬 LAN 來分隔 S3 應用程式的流量、則表示您已經設定了 VLAN 介面。請參閱 "設定VLAN介面"。

設定身分識別聯盟和 **SSO**

如果您計畫在 StorageGRID 系統上使用身分識別聯盟或單一登入（ SSO ）、則表示您已啟用這些功能。您也知道 S3 應用程式將使用哪個同盟群組的租戶帳戶擁有 root 存取權。請參閱 "使用身分識別聯盟" 和 "設定單一登入"。

取得及設定網域名稱

您知道 StorageGRID 要使用哪個完整網域名稱（ FQDN ）。網域名稱伺服器（ DNS ）項目會將此 FQDN 對應到您使用精靈建立的 HA 群組的虛擬 IP （ VIP ）位址。

如果您計畫使用 S3 虛擬託管式要求、您應該要有 "已設定 S3 端點網域名稱"。建議使用虛擬託管式要求。

檢閱負載平衡器和安全性憑證需求

如果您計畫使用 StorageGRID 負載平衡器、您已檢閱負載平衡的一般考量事項。您擁有要上傳的憑證或產生憑證所需的值。

如果您打算使用外部（第三方）負載平衡器端點、則該負載平衡器具有完整網域名稱（ FQDN ）、連接埠和憑證。

設定任何網格同盟連線

如果您想要允許 S3 租戶複製帳戶資料、並使用網格同盟連線將貯體物件複寫到其他網格、請在啟動精靈之前確認下列事項：

- 您有 "已設定網格同盟連線"。
- 連線狀態為 * 已連線 * 。
- 您擁有root存取權限。

存取並完成 **S3** 設定精靈

您可以使用 S3 設定精靈來設定 StorageGRID 、以便搭配 S3 應用程式使用。安裝精靈提供應用程式存取 StorageGRID 儲存區和儲存物件所需的值。

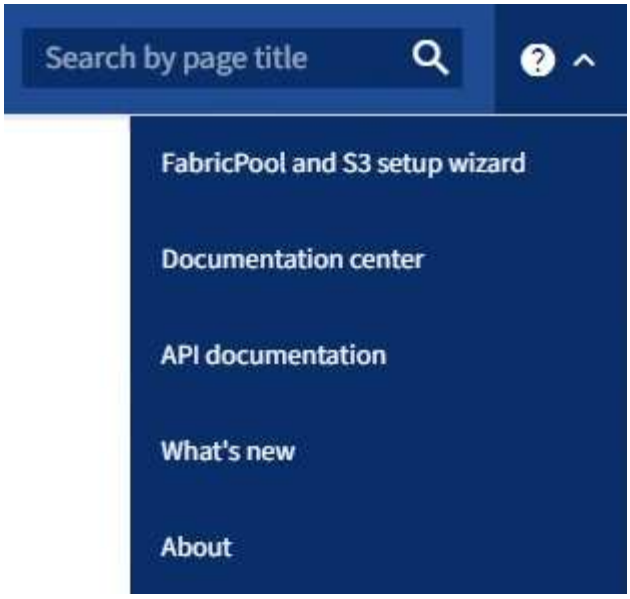
開始之前

- 您擁有 "root 存取權限"。
- 您已檢閱 "考量與要求" 以使用精靈。

存取精靈

步驟

1. 使用登入Grid Manager "支援的網頁瀏覽器"。
2. 如果儀表板上出現 * FabricPool 和 S3 設定精靈 * 橫幅、請選取橫幅中的連結。如果橫幅不再出現、請從 Grid Manager 的標題列中選取說明圖示、然後選取 * FabricPool 和 S3 設定精靈 * 。



3. 在 FabricPool and S3 安裝精靈頁面的 S3 應用程式區段中、選取 * 立即設定 * 。

步驟 **6** 之 **1** ：設定 **HA** 群組

HA 群組是每個節點包含 StorageGRID 負載平衡器服務的集合。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用 HA 群組來協助保持 S3 資料連線可用。如果 HA 群組中的作用中介面發生故障、備份介面就能管理工作負載、對 S3 作業幾乎沒有影響。

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、則不需要建立 HA 群組。選取 * 略過此步驟 * 並前往 步驟 2 、共 6 步：設定負載平衡器端點。
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。

建立**HA**群組

a. 若要建立新的 HA 群組、請選取 * 建立 HA 群組 * 。

b. 如需 * 輸入詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
HA 群組名稱	此 HA 群組的唯一顯示名稱。
說明（選用）	此 HA 群組的描述。

c. 在 * 新增介面 * 步驟中、選取您要在此 HA 群組中使用的節點介面。

使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。

您可以選取一或多個節點、但每個節點只能選取一個介面。

d. 對於「介面優先順序」步驟、請判斷此 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。主介面是作用中介面、除非發生故障。

如果 HA 群組包含多個介面、且作用中介面故障、則虛擬 IP （ VIP ）位址會依照優先順序移至第一個備份介面。如果該介面故障、VIP位址會移至下一個備份介面、依此類推。解決故障時、 VIP 位址會移回可用的最高優先順序介面。

e. 在 * 輸入 IP 位址 * 步驟中、請填寫下列欄位。

欄位	說明
子網路 CIDR	以 CIDR 表示法和 #8212 表示的 VIP 子網路位址； IPv4 位址後面接著斜線和子網路長度（ 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（選用）	如果用於存取 StorageGRID 的 S3 IP 位址與 StorageGRID VIP 位址不在同一子網路上、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	為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內。 至少一個位址必須是 IPv4 。您也可以指定其他的IPv6位址。

f. 選取 * 建立 HA 群組 * 、然後選取 * 完成 * 以返回 S3 設定精靈。

g. 選取 * 繼續 * 以移至負載平衡器步驟。

使用現有 **HA** 群組

a. 若要使用現有的 HA 群組、請從 * 選取 HA 群組 * 中選取 HA 群組名稱。

b. 選取 * 繼續 * 以移至負載平衡器步驟。

步驟 **2** 、共 **6** 步：設定負載平衡器端點

StorageGRID 使用負載平衡器從用戶端應用程式管理工作負載。負載平衡可將多個儲存節點的速度和連線容量最大化。

您可以使用 StorageGRID 負載平衡器服務（存在於所有閘道和管理節點上）、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。

如需此工作的詳細資訊、請參閱 "負載平衡考量"。

若要使用 StorageGRID 負載平衡器服務、請選取 * StorageGRID 負載平衡器 * 索引標籤、然後建立或選取您要使用的負載平衡器端點。若要使用外部負載平衡器、請選取 * 外部負載平衡器 * 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. 若要建立負載平衡器端點、請選取 * 建立端點 * 。
2. 如需 * 輸入端點詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
名稱	端點的描述性名稱。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為您建立的第一個端點為 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 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。 • 注意： * 不允許其他網格服務使用的連接埠。請參閱 "網路連接埠參考"。
用戶端類型	必須是 *S3 * 。
網路傳輸協定	選擇* HTTPS *。 • 注意 * ：支援與 StorageGRID 通訊、但不建議使用 TLS 加密。

3. 對於 *Select 綁定模式 * 步驟，請指定綁定模式。繫結模式可控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

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 來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
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。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
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	根據您選取的節點類型、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. 對於租戶存取步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

5. 對於 * 附加憑證 * 步驟、請選取下列其中一項：

欄位	說明
上傳憑證（建議）	使用此選項可上傳 CA 簽署的伺服器憑證、憑證私密金鑰及選用的 CA 套件組合。
產生憑證	使用此選項可產生自我簽署的憑證。請參閱 "設定負載平衡器端點" 以取得詳細的輸入內容。
使用 StorageGRID S3 和 Swift 憑證	只有在您已上傳或產生 StorageGRID 通用憑證的自訂版本時、才可使用此選項。請參閱 "設定S3和Swift API憑證" 以取得詳細資料。

6. 選擇 * 完成 * 返回 S3 設定精靈。
7. 選擇 * 繼續 * 以前往租戶和貯體步驟。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

使用現有負載平衡器端點

步驟

1. 若要使用現有的端點、請從 * 選取負載平衡器端點 * 中選取其名稱。
2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

使用外部負載平衡器

步驟

1. 若要使用外部負載平衡器、請填寫下列欄位。

欄位	說明
FQDN	外部負載平衡器的完整網域名稱（ FQDN ）。
連接埠	S3 應用程式用來連線到外部負載平衡器的連接埠編號。

欄位	說明
憑證	複製外部負載平衡器的伺服器憑證、然後貼到此欄位。

2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

步驟 **3** 、共 **6** 步：建立租戶和貯體

租戶是可以使用 S3 應用程式在 StorageGRID 中儲存及擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、貯體、物件和一組特定功能。您必須先建立租戶、然後才能建立 S3 應用程式用來儲存物件的貯體。

貯體是用來儲存租戶物件和物件中繼資料的容器。雖然有些租戶可能有許多貯體、但精靈可協助您以最快且最簡單的方式建立租戶和貯體。您可以稍後使用租戶管理器來新增任何您需要的額外貯體。

您可以為此 S3 應用程式建立新的租戶、以便使用。或者、您也可以為新租戶建立貯體。最後、您可以允許精靈為租戶的根使用者建立 S3 存取金鑰。

如需此工作的詳細資訊、請參閱 "建立租戶帳戶" 和 "建立S3儲存區"。

步驟

1. 選取*建立租戶*。
2. 如需輸入詳細資料步驟、請輸入下列資訊。

欄位	說明
名稱	租戶帳戶的名稱。租戶名稱不一定是唯一的。建立租戶帳戶時、會收到唯一的數字帳戶ID。
說明（選用）	協助識別租戶的說明。
用戶端類型	此租戶將使用的用戶端傳輸協定類型。對於 S3 設定精靈、會選取 **S2** 、且欄位會停用。
儲存配額（選用）	如果您想要此租用戶擁有儲存配額、則需要配額和單位的數值。

3. 選擇*繼續*。
4. 或者、選取您想要此租用戶擁有的任何權限。

其中有些權限有額外的需求。如需詳細資料、請選取每個權限的說明圖示。

權限	如果選取 ...
允許平台服務	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"。

權限	如果選取 ...
使用自己的身分識別來源	租戶可以為同盟群組和使用者設定及管理自己的身分識別來源。如果您有、此選項會停用 "已設定 SSO" 適用於您的 StorageGRID 系統。
允許 S3 Select	租戶可以發出 S3 SelectObjectContent API 要求、以篩選及擷取物件資料。請參閱 "管理用戶帳戶的S3 Select"。 • 重要 * ： SelectObjectContent 要求可降低所有 S3 用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。
使用網格同盟連線	租戶可以使用網格同盟連線。 選取此選項： • 使此租用戶和新增至帳戶的所有租戶群組和使用者、從這個網格（ _ 來源網格 _ ）複製到所選連線（ _ 目的地網格 _ ）的其他網格。 • 允許此租戶在每個網格上對應的儲存格之間設定跨網格複寫。 請參閱 "管理 Grid Federation 的允許租戶"。

5. 如果您選取 * 使用網格同盟連線 * 、請選取其中一個可用的網格同盟連線。
6. 根據您的 StorageGRID 系統是否使用、定義租戶帳戶的根存取權 "身分識別聯盟"、 "單一登入（ SSO ）"或兩者。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

7. 如果您希望精靈為 root 使用者建立存取金鑰 ID 和秘密存取金鑰、請選取 * 自動建立 root 使用者 S3 存取金鑰 * 。

如果租戶的唯一使用者是 root 使用者、請選取此選項。如果其他使用者將使用此租戶、請使用 Tenant Manager 來設定金鑰和權限。

8. 選擇*繼續*。
9. 針對「建立貯體」步驟、您可以選擇性地為租戶物件建立貯體。否則、請選取 * 建立不含貯體的租戶 * 以移至 下載資料步驟。

如果已啟用網格的 S3 物件鎖定功能、則在此步驟建立的儲存格並未啟用 S3 物件鎖定功能。如果您需要為此 S3 應用程式使用 S3 物件鎖定貯體、請選取 * 建立不含 Bucket 的租戶 * 。然後、使用 Tenant Manager "建立貯體" 而是。

a. 輸入 S3 應用程式將使用的儲存區名稱。例如、 `S3-bucket`。

   您無法在建立貯體之後變更貯體名稱。

b. 為此貯體選取 * 區域 * 。

   使用預設區域 (`us-east-1`）除非您預期未來會使用 ILM 來根據貯體的區域篩選物件。

c. 如果您要儲存此貯體中每個物件的每個版本、請選取 * 啟用物件版本管理 * 。

d. 選取 * 建立租戶和貯體 * 、然後前往下載資料步驟。

步驟 **4** 、共 **6** 步：下載資料

在下載資料步驟中、您可以下載一或兩個檔案、以儲存您剛設定的詳細資料。

步驟

1. 如果您選取 * 自動建立 root 使用者 S3 存取金鑰 * 、請執行下列其中一項或兩項操作：
   - 選取 * 下載存取金鑰 * 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。
   - 選取複製圖示（）將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。
2. 選擇 * 下載組態值 * 下載 `.txt` 包含負載平衡器端點、租戶、貯體和根使用者設定的檔案。
3. 將此資訊儲存至安全的位置。

   在複製兩個存取金鑰之前、請勿關閉此頁面。關閉此頁面後、金鑰將無法使用。請務必將此資訊儲存在安全的位置、因為此資訊可用於從 StorageGRID 系統取得資料。

4. 如果出現提示、請選取核取方塊、確認您已下載或複製金鑰。
5. 選取 * 繼續 * 以移至 ILM 規則和原則步驟。

第 **5** 步、共 **6** 步：審查 **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 原則會為所有物件建立兩個複寫複本。此原則會生效、直到您至少啟動一個新原則為止。

步驟

1. 檢閱頁面上提供的資訊。
2. 如果您要新增屬於新租戶或貯體之物件的特定指示、請建立新規則和新原則。請參閱 "建立ILM規則" 和 "ILM 原則：概觀"。
3. 請選擇 * 我已檢閱這些步驟、並瞭解我需要做什麼 * 。
4. 選取核取方塊、表示您瞭解接下來該怎麼做。
5. 選擇 * 繼續 * 前往 * 摘要 * 。

步驟 **6** 之 **6** ：檢視摘要

步驟

1. 檢閱摘要。
2. 請記下後續步驟中的詳細資料、其中說明在連線到 S3 用戶端之前可能需要的其他組態。例如、選取 * 以 root 身分登入 * 會將您帶到租戶管理員、您可以在其中新增租戶使用者、建立其他貯體、以及更新貯體設定。
3. 選擇*完成*。
4. 使用您從 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

管理高可用度（**HA**）群組：總覽

您可以將多個管理節點和閘道節點的網路介面分組為高可用度（HA）群組。如果HA群組中的作用中介面故障、備份介面就能管理工作負載。

什麼是**HA**群組？

您可以使用高可用度（HA）群組、為S3和Swift用戶端提供高可用度的資料連線、或提供高可用度的Grid Manager和Tenant Manager連線。

每個HA群組均可存取所選節點上的共享服務。

- 包含閘道節點、管理節點或兩者的HA群組、可為S3和Swift用戶端提供高可用度的資料連線。
- 僅包含管理節點的HA群組可提供高可用度的網格管理程式和租戶管理程式連線。
- 只包含服務應用裝置和 VMware 型軟體節點的 HA 群組、可為提供高可用度的連線 "使用S3 Select的S3租戶"。 使用S3 Select時建議使用HA群組、但不需要。

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取網路介面。您可以使用Grid Network（eth0）介面、用戶端網路（eth2）介面、VLAN介面、或是新增至節點的存取介面。

   如果 HA 群組具有 DHCP 指派的 IP 位址、則無法將介面新增至 HA 群組。

2. 您可以指定一個介面做為主要介面。主介面是作用中介面、除非發生故障。
3. 您可以決定任何備份介面的優先順序。
4. 您可以為群組指派一到10個虛擬IP（VIP）位址。用戶端應用程式可以使用這些VIP位址來連線StorageGRID至

如需相關指示、請參閱 "設定高可用度群組"。

什麼是作用中介面？

正常運作期間、HA群組的所有VIP位址都會新增至主要介面、這是優先順序中的第一個介面。只要主介面仍可用、當用戶端連線至群組的任何VIP位址時、就會使用該介面。也就是說、在正常作業期間、主要介面是群組的「作用中」介面。

同樣地、在正常作業期間、 HA 群組的任何低優先順序介面都會做為「備份」介面。除非主要（目前使用中）介面無法使用、否則不會使用這些備份介面。

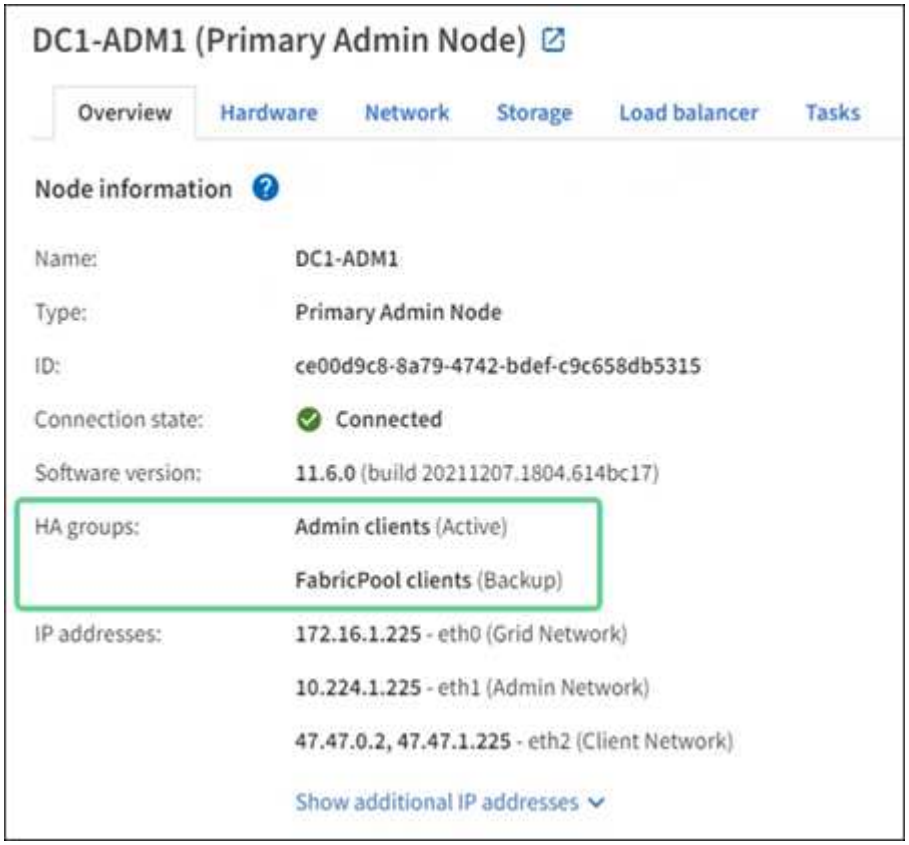
檢視節點的目前**HA**群組狀態

若要查看節點是否指派給HA群組並判斷其目前狀態、請選取* nodes **>***節點_。

如果「總覽」索引標籤包含* HA群組*的項目、則該節點會指派給列出的HA群組。群組名稱後面的值是HA群組中節點的目前狀態：

- * Active*：HA群組目前裝載於此節點上。
- 備份：HA群組目前未使用此節點、這是備份介面。
- * 停止 * ：由於已手動停止高可用度（ keepalive ）服務、因此無法在此節點上裝載 HA 群組。
- * 故障 * ：由於下列一項或多項原因、因此無法在此節點上裝載 HA 群組：
  - 負載平衡器（Ngine-GW）服務未在節點上執行。
  - 節點的eth0或VIP介面關閉。
  - 節點當機。

在此範例中、主要管理節點已新增至兩個HA群組。此節點目前是管理用戶端群組的作用中介面、FabricPool 也是適用於「支援客戶」群組的備份介面。



當作用中介面故障時會發生什麼事？

目前裝載VIP位址的介面是作用中介面。如果HA群組包含多個介面、且作用中介面故障、VIP位址會依照優先順序移至第一個可用的備份介面。如果該介面故障、VIP位址會移至下一個可用的備份介面、依此類推。

容錯移轉可因下列任一原因觸發：

- 介面設定所在的節點會停機。
- 介面設定所在的節點至少失去與所有其他節點的連線2分鐘。
- 作用中介面關閉。
- 負載平衡器服務會停止。
- 高可用度服務停止。

> 主控作用中介面的節點外部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。

容錯移轉程序通常只需幾秒鐘、而且速度足夠快、用戶端應用程式只會遇到些微影響、而且可以仰賴正常的重試行為來繼續作業。

當故障得以解決且優先順序較高的介面再次可用時、VIP位址會自動移至可用的最高優先順序介面。

如何使用**HA**群組？

您可以使用高可用度（HA）群組、為StorageGRID 物件資料和管理用途提供高可用度的連接至物件資料。

- HA群組可提供高可用度的管理連線至Grid Manager或Tenant Manager。
- HA群組可為S3和Swift用戶端提供高可用度的資料連線。
- 僅包含一個介面的HA群組可讓您提供多個VIP位址、並明確設定IPv6位址。

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、請從提供所需服務的節點類型新增介面。

- 管理節點：包括負載平衡器服務、並可存取Grid Manager或租戶管理程式。
- * 閘道節點 * ：包括負載平衡器服務。

HA群組的用途	將此類型的節點新增至**HA**群組
存取Grid Manager	• 主管理節點（主） • 非主要管理節點 *附註：*主要管理節點必須是主要介面。部分維護程序只能從主要管理節點執行。
僅限租戶管理程式存取	• 主要或非主要管理節點
S3或Swift用戶端存取-負載平衡器服務	• 管理節點 • 閘道節點

HA群組的用途	將此類型的節點新增至HA群組
的S3用戶端存取 "S3 Select"	• 服務應用裝置 • VMware軟體節點 附註：使用S3 Select時建議使用HA群組、但不需要。

搭配Grid Manager或Tenant Manager使用HA群組的限制

如果Grid Manager或Tenant Manager服務失敗、HA群組容錯移轉就不會觸發。

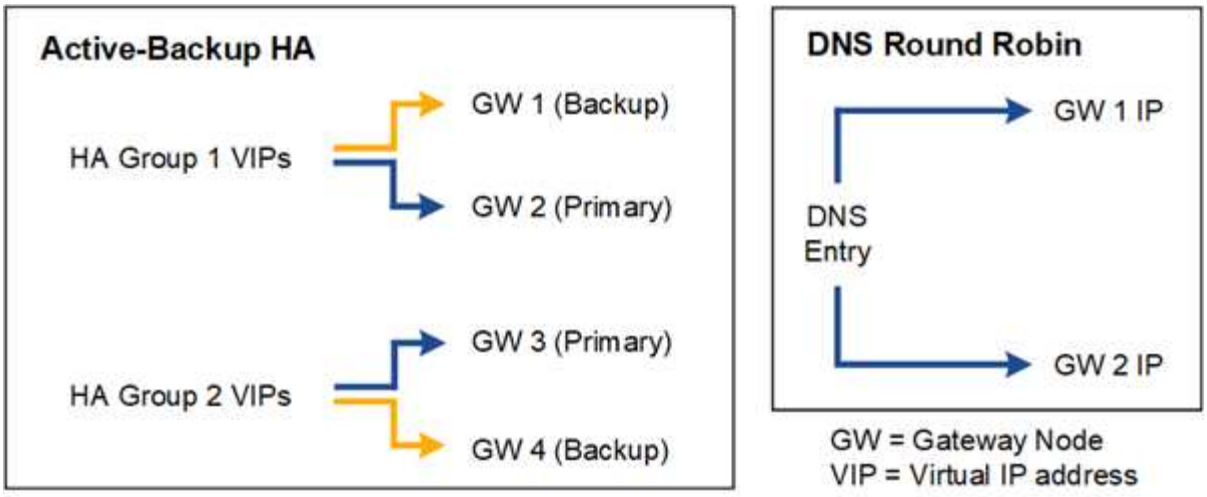
如果您在容錯移轉發生時登入Grid Manager或租戶管理程式、系統將會登出、您必須再次登入才能繼續執行工作。

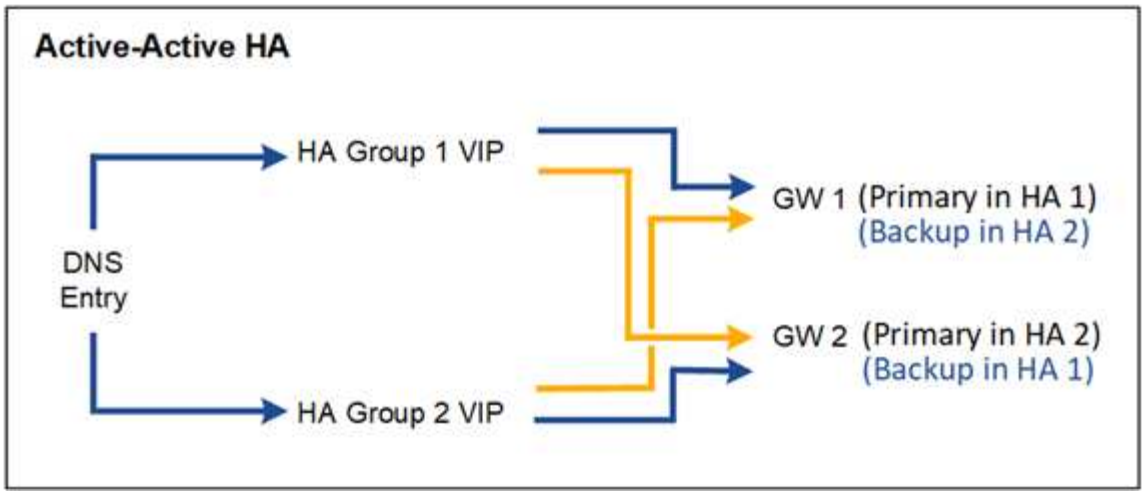
當主要管理節點無法使用時、無法執行某些維護程序。容錯移轉期間、您可以使用Grid Manager監控StorageGRID 您的作業系統。

HA群組的組態選項

下圖提供不同的HA群組設定方式範例。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。





下表摘要說明各HA組態的優點、如圖所示。

組態	優勢	缺點
主動備份HA	• 由不需依賴外部資源的不受依賴的功能執行管理StorageGRID 。 • 快速容錯移轉：	• HA群組中只有一個節點處於作用中狀態。每個HA群組至少有一個節點處於閒置狀態。
DNS循環配置資源	• 增加Aggregate處理量。 • 無閒置主機。	• 慢速容錯移轉、可能取決於用戶端行為。 • 需要在StorageGRID 不屬於此功能的情況下組態硬體。 • 需要客戶實作的健全狀況檢查。
主動式HA	• 流量分散於多個HA群組。 • 高Aggregate處理量、可隨HA群組數量而擴充。 • 快速容錯移轉：	• 更複雜的設定。 • 需要在StorageGRID 不屬於此功能的情況下組態硬體。 • 需要客戶實作的健全狀況檢查。

設定高可用度群組

您可以設定高可用度（HA）群組、以提供對管理節點或閘道節點上服務的高可用度存取。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 如果您打算在HA群組中使用VLAN介面、則表示您已建立VLAN介面。請參閱 "設定VLAN介面"。
- 如果您打算針對HA群組中的節點使用存取介面、則已建立介面：
  - * Red Hat Enterprise Linux （安裝節點之前） * ： "建立節點組態檔"
  - * Ubuntu或DEBIAN*（安裝節點之前）*： "建立節點組態檔"
  - * Linux（安裝節點之後）*： "Linux：新增主幹或存取介面至節點"
  - * VMware（安裝節點之後）*： "VMware：新增主幹或存取介面至節點"

建立高可用度群組

當您建立高可用度群組時、請選取一或多個介面、然後依優先順序加以組織。然後、您將一個或多個VIP位址指派給群組。

介面必須是要納入HA群組的閘道節點或管理節點。HA群組只能將一個介面用於任何指定節點、但同一個節點的其他介面可用於其他HA群組。

存取精靈

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。
2. 選擇* Create （建立）。

輸入**HA**群組的詳細資料

步驟

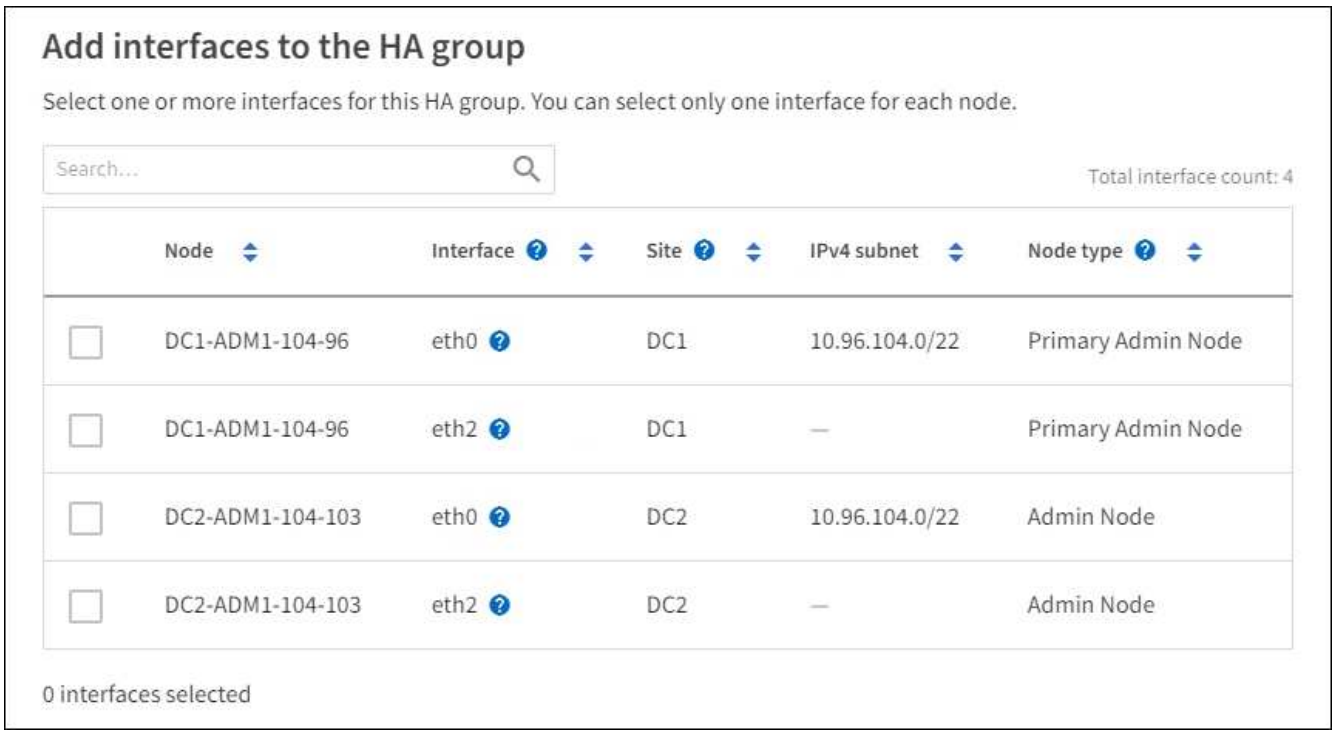
1. 為HA群組提供唯一名稱。
2. （可選）輸入HA群組的說明。
3. 選擇*繼續*。

新增介面至**HA**群組

步驟

1. 選取一或多個介面以新增至此HA群組。

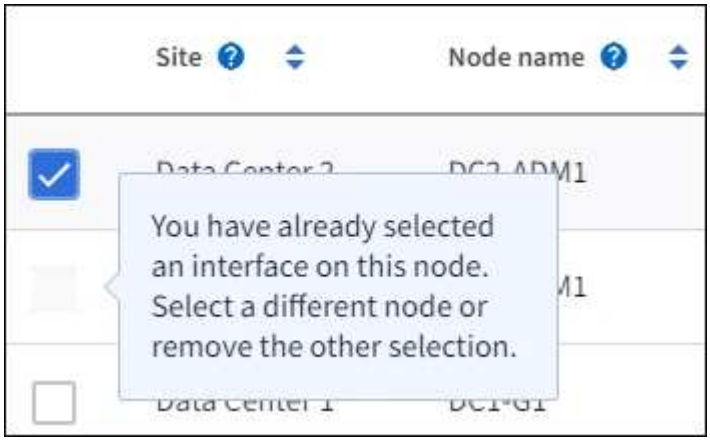
   使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。



建立VLAN介面之後、請等待5分鐘、讓新介面出現在表格中。

選擇介面的準則

- 您必須選取至少一個介面。
- 您只能為節點選取一個介面。
- 如果HA群組用於管理節點服務的HA保護（包括Grid Manager和Tenant Manager）、請選取「僅管理節點上的介面」。
- 如果HA群組用於HA保護S3或Swift用戶端流量、請選取管理節點、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、則會顯示資訊注意事項。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、備份管理節點也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、則其核取方塊會停用。工具提示提供更多資訊。



- 如果介面的子網路值或閘道與其他選取的介面衝突、則無法選取介面。

。如果設定的介面沒有靜態 IP 位址、則無法選取該介面。

2. 選擇*繼續*。

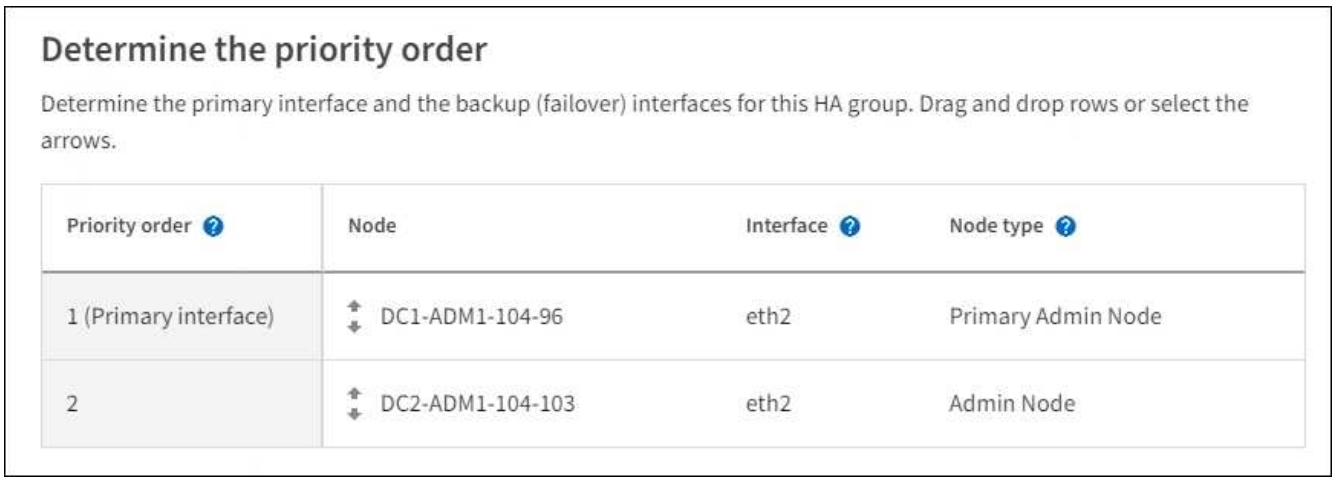
決定優先順序

如果 HA 群組包含多個介面、您可以判斷哪個是主要介面、哪些是備份（容錯移轉）介面。 如果主要介面故障、 VIP 位址會移至可用的最高優先順序介面。如果該介面故障、VIP位址會移至下一個可用的最高優先順序介面、依此類推。

步驟

1. 在 * 優先順序 * 欄中拖曳列、以決定主要介面和任何備份介面。

   清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。



   如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行。

2. 選擇*繼續*。

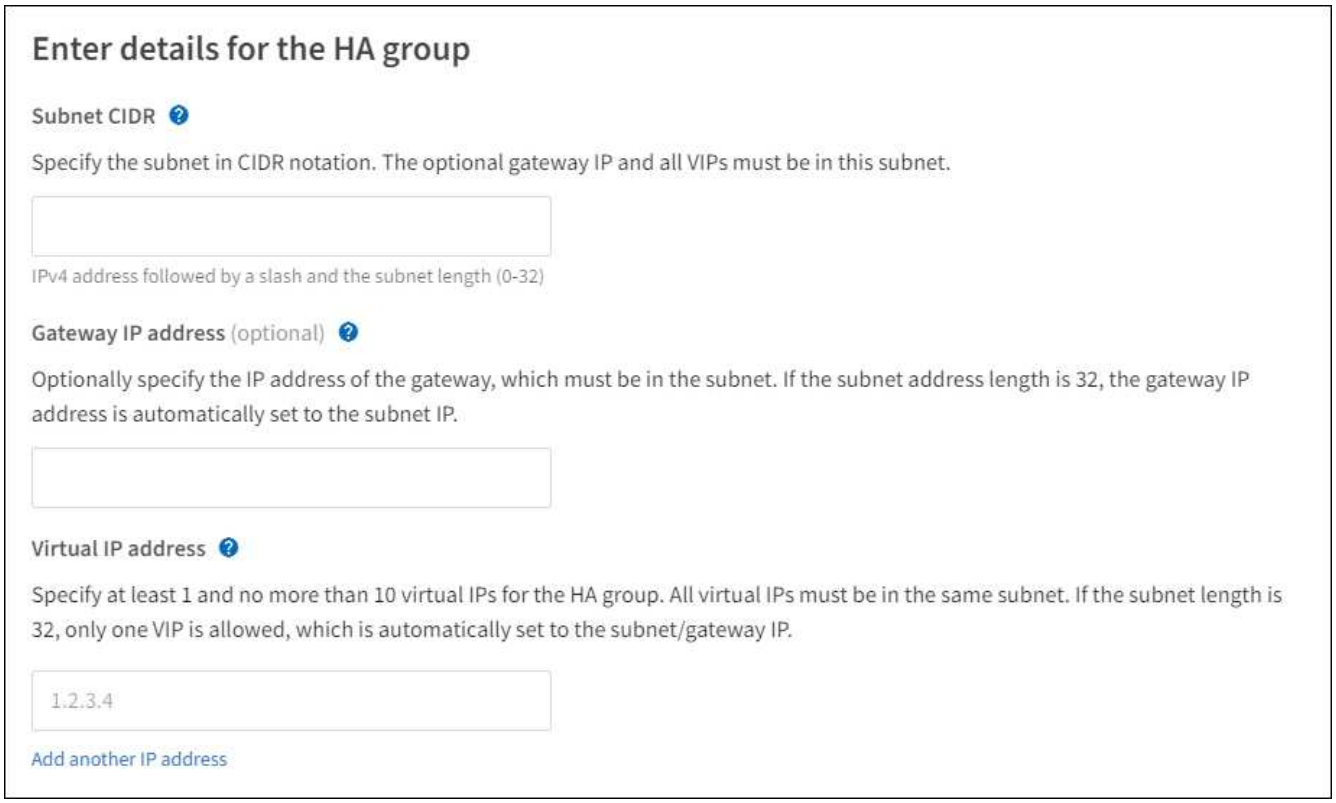
輸入**IP**位址

步驟

1. 在*子網路CID*欄位中、以CIDR表示法指定VIP子網路、即一種IPV4位址、後面接著一條斜槓和子網路長度（0-32）。

   網路位址不得設定任何主機位元。例如、 `192.16.0.0/22`。

   如果您使用32位元前置碼、VIP網路位址也會做為閘道位址和VIP位址。



2. 或者、如果任何S3、Swift、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、請輸入*閘道IP位址*。閘道位址必須位於VIP子網路內。

   用戶端和管理使用者將使用此閘道來存取虛擬IP位址。

3. 為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內、而且所有位址都會同時在作用中介面上作用。

   您必須至少提供一個IPV4位址。您也可以指定其他的IPv6位址。

4. 選擇* Create HA group（建立HA群組）、然後選取 Finish（完成）*。

   HA群組隨即建立、您現在可以使用已設定的虛擬IP位址。

後續步驟

如果您要使用此HA群組進行負載平衡、請建立負載平衡器端點、以判斷連接埠和網路傳輸協定、並附加任何必要的憑證。請參閱 "設定負載平衡器端點"。

編輯高可用度群組

您可以編輯高可用度（HA）群組、以變更其名稱和說明、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、如果您想要在站台或節點取消委任程序中移除與所選介面相關聯的節點、則可能需要編輯HA群組。

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。

「高可用度群組」頁面會顯示所有現有的HA群組。

2. 選取您要編輯之 HA 群組的核取方塊。
3. 根據您要更新的內容、執行下列其中一項：
   - 選取*「動作*」>*「編輯虛擬IP位址*」以新增或移除VIP位址。
   - 選取*「動作*」>*「編輯HA群組*」以更新群組的名稱或說明、新增或移除介面、變更優先順序、或新增或移除VIP位址。
4. 如果您選取*編輯虛擬IP位址*：
   a. 更新HA群組的虛擬IP位址。
   b. 選擇*保存*。
   c. 選擇*完成*。
5. 如果您選取*編輯HA群組*：
   a. 或者、請更新群組的名稱或說明。
   b. 或者、選取或清除核取方塊以新增或移除介面。

      如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行

   c. 您也可以拖曳資料列來變更此 HA 群組的主要介面和任何備份介面的優先順序。
   d. 或者、更新虛擬IP位址。
   e. 選取*「Save（儲存）」、然後選取「Finish（完成）」*。

移除高可用度群組

您可以一次移除一或多個高可用度（HA）群組。

如果 HA 群組繫結至負載平衡器端點、則無法移除該群組。若要刪除 HA 群組、您必須將其從任何使用它的負載平衡器端點中移除。

若要避免用戶端中斷、請先更新任何受影響的S3或Swift用戶端應用程式、再移除HA群組。更新每個用戶端以使用其他IP位址進行連線、例如、不同HA群組的虛擬IP位址、或是安裝期間為介面設定的IP位址。

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。
2. 檢閱您要移除之每個 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. 移至 * 組態 * > * 網路 * > * 負載平衡器端點 * 。
   b. 選取端點的核取方塊。
   c. 選取*「動作*」>*「編輯端點繫結模式*」。
   d. 更新繫結模式以移除 HA 群組。
   e. 選取*儲存變更*。
3. 如果未列出負載平衡器端點、請選取您要移除的每個 HA 群組的核取方塊。

4. 選取 * 動作 * > * 移除 HA 群組 * 。
5. 檢閱訊息並選擇*刪除HA群組*以確認您的選擇。

   您選取的所有HA群組都會移除。「高可用度群組」頁面上會出現綠色的成功橫幅。

管理負載平衡

負載平衡考量

您可以使用負載平衡來處理來自 S3 和 Swift 用戶端的擷取和擷取工作負載。

什麼是負載平衡？

當用戶端應用程式從 StorageGRID 系統儲存或擷取資料時、 StorageGRID 會使用負載平衡器來管理擷取和擷取工作負載。負載平衡可在多個儲存節點之間分配工作負載、以最大化速度和連線容量。

此功能可在所有管理節點和所有閘道節點上安裝支援程式、並提供第7層負載平衡功能。StorageGRID它會對用戶端要求執行傳輸層安全性（TLS）終止、檢查要求、並建立新的安全連線至儲存節點。

將用戶端流量轉送至儲存節點時、每個節點上的負載平衡器服務都會獨立運作。透過加權程序、負載平衡器服務會將更多要求路由傳送至CPU可用度較高的儲存節點。

> 雖然推薦使用「VMware負載平衡器」服務、但StorageGRID 您可能想要改為整合協力廠商負載平衡器。如需相關資訊、請聯絡您的NetApp客戶代表或參閱 "TR-4626：StorageGRID 不包括第三方和全域負載平衡器"。

我需要多少個負載平衡節點？

一般最佳實務做法StorageGRID 是、您的一套系統應該在負載平衡器服務中包含兩個或多個節點。例如、站台可能包含兩個閘道節點、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、請確定每個負載平衡節點都有足夠的網路、硬體或虛擬化基礎架構。

什麼是負載平衡器端點？

負載平衡器端點會定義傳入和傳出用戶端應用程式要求用來存取包含負載平衡器服務之節點的連接埠和網路傳輸協定（ HTTPS 或 HTTP ）。端點也會定義用戶端類型（ S3 或 Swift ）、繫結模式、以及選擇性的允許或封鎖租戶清單。

若要建立負載平衡器端點、請選取 * 組態 * > * 網路 * > * 負載平衡器端點 * 、或完成 FabricPool 和 S3 設定精靈。如需相關指示：

- "設定負載平衡器端點"
- "使用 S3 設定精靈"
- "使用 FabricPool 設定精靈"

連接埠的考量事項

對於您建立的第一個端點、負載平衡器端點的連接埠預設為 10433 、但您可以指定介於 1 到 65535 之間的任何未使用的外部連接埠。如果您使用連接埠 80 或 443 、端點將僅使用 Gateway 節點上的負載平衡器服務。這些

連接埠保留在管理節點上。如果您對多個端點使用相同的連接埠、則必須為每個端點指定不同的繫結模式。

不允許其他網格服務使用的連接埠。請參閱 "網路連接埠參考"。

網路傳輸協定的考量事項

在大多數情況下、用戶端應用程式與 StorageGRID 之間的連線應該使用傳輸層安全性（ TLS ）加密。支援但不建議連線至無 TLS 加密的 StorageGRID 、尤其是在正式作業環境中。當您選取 StorageGRID 負載平衡器端點的網路傳輸協定時、應該選取 **HTTPS** 。

負載平衡器端點憑證的考量事項

如果選擇 **HTTPS** 作爲負載平衡器端點的網絡協議，則必須提供安全證書。建立負載平衡器端點時、您可以使用以下三個選項中的任何一個：

- * 上傳簽署的憑證（建議） * 。此憑證可由公開信任或私有憑證授權單位（ CA ）簽署。最佳做法是使用公開信任的 CA 伺服器憑證來保護連線安全。與產生的憑證不同、 CA 簽署的憑證可以不中斷地旋轉、有助於避免過期問題。

  您必須先取得下列檔案、才能建立負載平衡器端點：

  - 自訂伺服器憑證檔案。
  - 自訂伺服器憑證私密金鑰檔案。
  - 或者、每個中繼發行憑證授權單位的憑證 CA 套裝組合。
- * 產生自我簽署的憑證 * 。
- * 使用全球 StorageGRID S3 和 Swift 認證 * 。您必須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和Swift API憑證"。

我需要什麼價值？

若要建立憑證、您必須知道 S3 或 Swift 用戶端應用程式用來存取端點的所有網域名稱和 IP 位址。

憑證的 * 主體 DN* （辨別名稱）項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
```

必要時、憑證可以使用萬用字元來代表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*萬用字元表示 `adm1.storagegrid.example.com` 和 `gn1.storagegrid.example.com`。

如果您打算使用 S3 虛擬託管式要求、則該憑證也必須為每個要求提供 * 替代名稱 * 項目 "S3 端點網域名稱" 您已設定、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、請參閱 "伺服器憑證的強化準則"。

您也必須為安全性憑證中的每個名稱定義 DNS 項目。

如何管理過期的憑證？

如果用於保護 S3 應用程式與 StorageGRID 之間連線的憑證過期、應用程式可能會暫時失去對 StorageGRID 的存取權。

若要避免憑證過期問題、請遵循下列最佳實務做法：

- 請仔細監控任何警告即將到期的憑證、例如 * 負載平衡器端點憑證到期 * 、以及 * S3 和 Swift API* 警示的通用伺服器憑證到期日。
- 請務必讓 StorageGRID 和 S3 應用程式的憑證版本保持同步。如果您更換或更新用於負載平衡器端點的憑證、則必須更換或更新 S3 應用程式所使用的同等憑證。
- 使用公開簽署的 CA 憑證。如果您使用由 CA 簽署的憑證、您可以不中斷地更換即將過期的憑證。
- 如果您已產生自我簽署的 StorageGRID 憑證、且該憑證即將過期、則必須在現有憑證過期之前、手動在 StorageGRID 和 S3 應用程式中置換憑證。

綁定模式的注意事項

繫結模式可讓您控制哪些 IP 位址可用於存取負載平衡器端點。如果端點使用繫結模式、則用戶端應用程式只有在使用允許的 IP 位址或其對應的完整網域名稱（ FQDN ）時、才能存取端點。使用任何其他 IP 位址或 FQDN 的用戶端應用程式無法存取端點。

您可以指定下列任何一種繫結模式：

- * 通用 *（預設）：用戶端應用程式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 來存取端點。除非您需要限制端點的存取、否則請使用此設定。
- * HA 群組的虛擬 IP * 。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 ）。

租戶存取的考量事項

租戶存取是一項選擇性的安全功能、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他們的貯體。您可以允許所有租戶存取端點（預設）、也可以指定每個端點的允許或封鎖租戶清單。

您可以使用此功能、在租戶與其端點之間提供更好的安全隔離。例如、您可以使用此功能來確保某個租戶擁有的最高機密或高度機密資料、不會被其他租戶完全存取。

為了進行存取控制、如果在要求中未提供存取金鑰（例如匿名存取）、則租戶會根據用戶端要求中使用的存取金鑰來決定租戶。

租戶存取範例

若要瞭解此安全功能的運作方式、請考慮下列範例：

1. 您已建立兩個負載平衡器端點、如下所示：
   - * 公有 * 端點：使用連接埠 10443 並允許存取所有租戶。
   - *Top secret * 端點：使用連接埠 10444 、僅允許存取 *Top secret * 租戶。所有其他租戶都會被封鎖、無法存取此端點。
2. 。 `top-secret.pdf` 位於 *Top Secret * 租戶擁有的貯體內。

存取 `top-secret.pdf`、 * 上秘密 * 租戶中的使用者可以向發出 GET 要求 `https://w.x.y.z:10444/top-secret.pdf`。由於此租戶可以使用 10444 端點、因此使用者可以存取物件。不過、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、他們就會收到立即存取遭拒訊息。即使認證和簽章有效、存取仍會遭到拒絕。

CPU可用度

將S3或Swift流量轉送至儲存節點時、每個管理節點和閘道節點上的負載平衡器服務都會獨立運作。透過加權程序、負載平衡器服務會將更多要求路由傳送至CPU可用度較高的儲存節點。節點CPU負載資訊會每隔幾分鐘更新一次、但加權可能會更頻繁地更新。所有儲存節點都會被指派最低的基本權重值、即使節點回報100%使用率或無法報告使用率亦然。

在某些情況下、CPU可用度的相關資訊僅限於負載平衡器服務所在的站台。

設定負載平衡器端點

負載平衡器端點決定連接StorageGRID 至閘道和管理節點上的S3和Swift用戶端可使用的連接埠和網路傳輸協定。您也可以使用端點來存取 Grid Manager 、 Tenant Manager 或兩者。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 您已檢閱 "負載平衡考量"。
- 如果您先前已重新對應要用於負載平衡器端點的連接埠、您就擁有了 "已移除連接埠重新對應"。
- 您已建立任何打算使用的高可用度（HA）群組。建議使用HA群組、但不需要。請參閱 "管理高可用度群組"。
- 如果將使用負載平衡器端點 "S3租戶選擇"、不得使用任何裸機節點的IP位址或FQDN。S3 Select 所使用的負載平衡器端點僅允許使用服務應用裝置和 VMware 型軟體節點。
- 您已設定任何打算使用的VLAN介面。請參閱 "設定VLAN介面"。
- 如果您要建立HTTPS端點（建議）、您就有伺服器憑證的資訊。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

- 若要上傳憑證、您需要伺服器憑證、憑證私密金鑰、以及選擇性的CA套裝組合。
- 若要產生憑證、您需要S3或Swift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（辨別名稱）。
- 如果您想要使用StorageGRID Sfor S3和Swift API認證（也可用於直接連線至儲存節點）、則您已使用由外部憑證授權單位簽署的自訂認證來取代預設認證。請參閱 "設定S3和Swift API憑證"。

建立負載平衡器端點

每個 S3 或 Swift 用戶端負載平衡器端點都會指定連接埠、用戶端類型（ S3 或 Swift ）、以及網路傳輸協定（ HTTP 或 HTTPS ）。管理介面負載平衡器端點會指定連接埠、介面類型和不受信任的用戶端網路。

存取精靈

步驟

1. 選擇*組態*>*網路*>*負載平衡器端點*。
2. 若要為 S3 或 Swift 用戶端建立端點、請選取 *S3 或 Swift 用戶端 * 標籤。
3. 若要建立端點以存取 Grid Manager 、 Tenant Manager 或兩者、請選取 * 管理介面 * 索引標籤。
4. 選擇* Create （建立）。

輸入端點詳細資料

步驟

1. 選取適當的指示、以輸入您要建立的端點類型的詳細資料。

S3 或 **Swift** 用戶端

欄位	說明
名稱	端點的描述性名稱、會出現在「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選用功能。StorageGRID此欄位預設為 10433 、表示您建立的第一個端點、但您可以輸入 1 到 65535 之間的任何未使用的外部連接埠。 如果您輸入 **80** 或 **8443** ，則端點僅在網關節點上配置，除非您已釋放端口 8443 。然後、您可以使用連接埠 8443 做為 S3 端點、而且連接埠將同時在 Gateway 和 Admin Node 上設定。
用戶端類型	將使用此端點的用戶端應用程式類型：* S3 或 Swift *。
網路傳輸協定	用戶端連線至此端點時所使用的網路傳輸協定。 • 選擇* HTTPS *進行安全的TLS加密通訊（建議）。您必須先附加安全性憑證、才能儲存端點。 • 選擇「* HTTP *」以獲得較不安全且未加密的通訊。僅將HTTP用於非正式作業網格。

管理介面

欄位	說明
名稱	端點的描述性名稱、會出現在「負載平衡器端點」頁面的表格中。
連接埠	您要用來存取 Grid Manager 、 Tenant Manager 或兩者的 StorageGRID 連接埠。 • 網格管理器： **8443** • 租戶經理： **9443** • Grid Manager 和 Tenant Manager ： **443** • 注意 * ：您可以使用這些預設連接埠或其他可用的連接埠。
介面類型	選取您要使用此端點存取的 StorageGRID 介面選項按鈕。
不受信任的用戶端網路	如果不受信任的用戶端網路應該可以存取此端點、請選取 * 是 * 。否則、請選取 * 否 * 。 當您選取 * 是 * 時、連接埠會在所有不受信任的用戶端網路上開啟。 • 注意 * ：當您建立負載平衡器端點時、您只能將連接埠設定為開放或關閉給不受信任的用戶端網路。

1. 選擇*繼續*。

選取繫結模式

步驟

1. 選取端點的繫結模式、以控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

   有些繫結模式適用於用戶端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 來存取端點。 除非您需要限制此端點的存取、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。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
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（僅限用戶端端端點）	根據您選取的節點類型、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。
所有管理節點（管理介面端點的預設值）	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。

   如果多個端點使用相同的連接埠、 StorageGRID 會使用此優先順序來決定要使用的端點： * HA 群組的虛擬 IP * > * 節點介面 * > * 節點類型 * > * 全域 * 。

   如果您要建立管理介面端點、則只允許使用管理節點。

2. 如果您選取* HA群組的虛擬IP *、請選取一或多個HA群組。

   如果您要建立管理介面端點、請選取僅與管理節點相關聯的 VIP 。

3. 如果您選取*節點介面*、請針對您要與此端點建立關聯的每個管理節點或閘道節點、選取一或多個節點介面。
4. 如果您選取 * 節點類型 * 、請選取管理節點（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

管理介面端點只有在端點具有時、才能控制租戶存取 租戶管理器的介面類型。

步驟

1. 對於 * 租戶存取 * 步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。 如果您尚未建立任何租戶帳戶、則必須選取此選項。新增租戶帳戶之後、您可以編輯負載平衡器端點、以允許或封鎖特定帳戶。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

2. 如果您要建立 **HTTP** 端點、則不需要附加憑證。選取*「Create」（建立）*以新增負載平衡器端點。然後前往 完成後。否則、請選取*繼續*以附加憑證。

附加憑證

步驟

1. 如果您要建立* HTTPS *端點、請選取要附加到端點的安全性憑證類型。

   憑證可保護S3和Swift用戶端與管理節點或閘道節點上的負載平衡器服務之間的連線。

   - 上傳認證。如果您有要上傳的自訂憑證、請選取此選項。
   - 產生憑證。如果您有產生自訂憑證所需的值、請選取此選項。
   - 使用**StorageGRID SS3**和**Swift**認證。如果您想要使用全域S3和Swift API憑證、也可以直接用於儲存節點的連線、請選取此選項。

     除非您已使用外部憑證授權單位簽署的自訂憑證取代由網格 CA 簽署的預設 S3 和 Swift API 憑證、否則無法選取此選項。請參閱 "設定S3和Swift API憑證"。

   - * 使用管理介面憑證 * 。如果您想要使用通用管理介面憑證、也可用於直接連線至管理節點、請選取此選項。

2. 如果您沒有使用 StorageGRID S3 和 Swift 憑證、請上傳或產生憑證。

上傳憑證

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（以PEM編碼）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC 私密金鑰必須大於 224 位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位（CA）的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 展開*憑證詳細資料*、即可查看您上傳之每個憑證的中繼資料。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇* Create （建立）。+ 隨即建立負載平衡器端點。自訂憑證用於 S3 和 Swift 用戶端之間的所有後續新連線、或是管理介面和端點之間的所有新連線。

產生憑證

a. 選擇*產生憑證*。

b. 指定憑證資訊：

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*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。
有效天數	憑證建立後過期的天數。

欄位	說明
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取 * 憑證詳細資料 * 以查看所產生憑證的中繼資料。

   ▪ 選取*下載憑證*以儲存憑證檔案。

   指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   ▪ 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇* Create （建立）。

   隨即建立負載平衡器端點。自訂憑證用於 S3 與 Swift 用戶端之間的所有後續新連線、或是管理介面與此端點之間的所有新連線。

完成後

步驟

1. 如果您使用 DNS 、請確定 DNS 包含一筆記錄、將 StorageGRID 完整網域名稱（ FQDN ）與用戶端用來建立連線的每個 IP 位址建立關聯。

   您在DNS記錄中輸入的IP位址取決於您是否使用HA負載平衡節點群組：

   ◦ 如果您已設定 HA 群組、用戶端將會連線至該 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。

   您也必須確保DNS記錄會參考所有必要的端點網域名稱、包括任何萬用字元名稱。

2. 提供S3和Swift用戶端連線至端點所需的資訊：

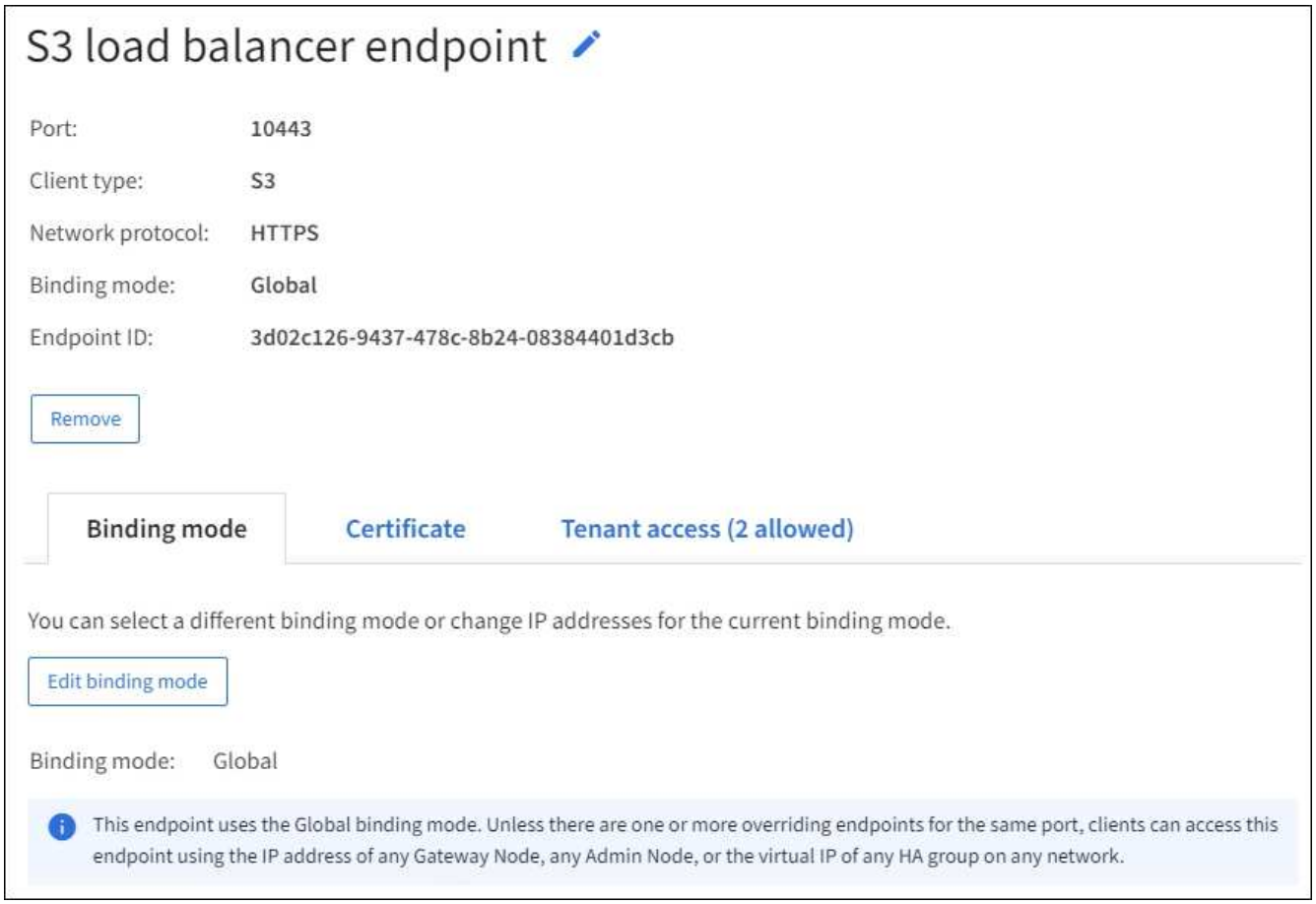
   ◦ 連接埠號碼

   ◦ 完整網域名稱或IP位址

   ◦ 任何必要的憑證詳細資料

您可以檢視現有負載平衡器端點的詳細資料、包括安全端點的憑證中繼資料。您可以變更端點的特定設定。

- 若要檢視所有負載平衡器端點的基本資訊、請檢閱「負載平衡器端點」頁面上的表格。
- 若要檢視特定端點的所有詳細資料、包括憑證中繼資料、請在表格中選取端點的名稱。顯示的資訊會因端點類型及其設定方式而異。



- 若要編輯端點、請使用負載平衡器端點頁面上的 * 動作 * 功能表。

如果您在編輯管理介面端點的連接埠時、無法存取 Grid Manager 、請更新 URL 和連接埠以重新取得存取權。

編輯端點之後、您可能需要等待15分鐘、才能將變更套用至所有節點。

工作	「行動」功能表	詳細資料頁面
編輯端點名稱	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點名稱*」。 c. 輸入新名稱。 d. 選擇*保存*。	a. 選取端點名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選擇*保存*。

工作	「行動」功能表	詳細資料頁面
編輯端點連接埠	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯端點連接埠 * c. 輸入有效的連接埠號碼。 d. 選擇*保存*。	*n*
編輯端點繫結模式	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點繫結模式*」。 c. 視需要更新連結模式。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇*編輯綁定模式*。 c. 視需要更新連結模式。 d. 選取*儲存變更*。
編輯端點憑證	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點憑證*」。 c. 視需要上傳或產生新的自訂憑證、或開始使用全域S3和Swift憑證。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇*認證*標籤。 c. 選取*編輯憑證*。 d. 視需要上傳或產生新的自訂憑證、或開始使用全域S3和Swift憑證。 e. 選取*儲存變更*。
編輯租戶存取	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯租戶存取 * 。 c. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇 * 租戶存取 * 標籤。 c. 選取 * 編輯租戶存取 * 。 d. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 e. 選取*儲存變更*。

移除負載平衡器端點

您可以使用* Actions（動作）*功能表移除一或多個端點、也可以從詳細資料頁面移除單一端點。

若要避免用戶端中斷、請先更新任何受影響的S3或Swift用戶端應用程式、再移除負載平衡器端點。使用指派給另一個負載平衡器端點的連接埠、更新每個用戶端以進行連線。請務必同時更新任何必要的憑證資訊。

如果您在移除管理介面端點時失去對 Grid Manager 的存取權、請更新 URL 。

- 若要移除一或多個端點：
  a. 在「負載平衡器」頁面中、選取您要移除的每個端點的核取方塊。
  b. 選擇*「Actions」（動作）>「Remove*」（移除

c. 選擇*確定*。

- 若要從詳細資料頁面移除一個端點：
  a. 從「負載平衡器」頁面。選取端點名稱。
  b. 在詳細資料頁面上選取*移除*。
  c. 選擇*確定*。

設定 S3 端點網域名稱

若要支援 S3 虛擬代管型要求、您必須使用 Grid Manager 來設定 S3 用戶端所連線的 S3 端點網域名稱清單。

不支援將 IP 位址用於端點網域名稱。未來的版本將會阻止此組態。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已確認網格升級尚未進行。

網格升級進行中時、請勿變更網域名稱組態。

關於這項工作

若要讓用戶端使用S3端點網域名稱、您必須執行下列所有動作：

- 使用Grid Manager將S3端點網域名稱新增StorageGRID 至整個系統。
- 請確定 "用戶端用於 StorageGRID HTTPS 連線的憑證" 針對用戶端所需的所有網域名稱進行簽署。

  例如、如果端點是 `s3.company.com`、您必須確保用於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`。

- 設定用戶端使用的DNS伺服器。為用戶端用來建立連線的 IP 位址加入 DNS 記錄、並確保記錄會參照所有必要的 S3 端點網域名稱、包括任何萬用字元名稱。

用戶端可以StorageGRID 使用閘道節點、管理節點或儲存節點的IP位址、或是連線至高可用度群組的虛擬IP位址、來連線至功能區。您應該瞭解用戶端應用程式如何連線至網格、以便在DNS記錄中包含正確的IP位址。

使用HTTPS連線（建議）到網格的用戶端可使用下列任一憑證：

- 連線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設定為辨識不同的 S3 端點網域名稱。
- 連線至負載平衡器端點或直接連線至儲存節點的用戶端可以自訂全域 S3 和 Swift API 憑證、以包含所有必要的 S3 端點網域名稱。

如果您沒有新增 S3 端點網域名稱、而且清單是空的、則會停用 S3 虛擬託管樣式要求的支援。

新增 **S3** 端點網域名稱

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 在 * 網域名稱 1* 欄位中輸入網域名稱。選取 * 新增其他網域名稱 * 以新增更多網域名稱。
3. 選擇*保存*。
4. 確定用戶端使用的伺服器憑證符合所需的 S3 端點網域名稱。
   - 如果用戶端連線到使用其本身憑證的負載平衡器端點、 "更新與端點相關的憑證"。
   - 如果用戶端連線到使用全域 S3 和 Swift API 憑證的負載平衡器端點、或直接連線到儲存節點、 "更新全域 S3 和 Swift API 憑證"。
5. 新增必要的DNS記錄、以確保端點網域名稱要求能夠解析。

結果

現在、當用戶端使用端點時 *bucket.s3.company.com*、DNS伺服器會解析為正確的端點、而且憑證會依照預期驗證端點。

重新命名 **S3** 端點網域名稱

如果您變更 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 選取您要編輯的網域名稱欄位、然後進行必要的變更。
3. 選擇*保存*。
4. 選擇 * 是 * 以確認您的變更。

刪除 **S3** 端點網域名稱

如果您移除 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 選取刪除圖示 ✕ 在網域名稱旁。
3. 選擇 * 是 * 以確認刪除。

相關資訊

- "使用S3 REST API"
- "檢視IP位址"
- "設定高可用度群組"

摘要：用於用戶端連線的**IP**位址和連接埠

若要儲存或擷取物件、 S3 和 Swift 用戶端應用程式會連線到負載平衡器服務（包含在所有

管理節點和閘道節點上）、或是連接到所有儲存節點上的本機分配路由器（ LDR ）服務。

用戶端應用程式可以使用網格節點的 IP 位址和該節點上服務的連接埠號碼、來連線至 StorageGRID 。您也可以建立高可用度（ HA ）負載平衡節點群組、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名稱（ FQDN ）而非 IP 或 VIP 位址連線至 StorageGRID 、您可以設定 DNS 項目。

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如果您已經建立負載平衡器端點和高可用度（ HA ）群組、請參閱 何處可以找到 IP 位址 在 Grid Manager 中找出這些值。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA 群組	負載平衡器	HA群組的虛擬IP位址	指派給負載平衡器端點的連接埠
管理節點	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 預設Swift連接埠： • HTTPS ： 18083 • HTTP ： 18085

URL 範例

若要將用戶端應用程式連線至 HA 群組的閘道節點負載平衡器端點、請使用如下所示的 URL 結構：

`https://VIP-of-HA-group:LB-endpoint-port`

例如、如果 HA 群組的虛擬 IP 位址為 192.0.2.5 、而負載平衡器端點的連接埠號碼為 10443 、則應用程式可以使用下列 URL 連線至 StorageGRID ：

`https://192.0.2.5:10443`

何處可以找到 **IP** 位址

1. 使用登入Grid Manager "支援的網頁瀏覽器"。
2. 若要尋找網格節點的IP位址：
   a. 選擇*節點*。

b. 選取您要連線的管理節點、閘道節點或儲存節點。

c. 選擇* Overview（概述）*選項卡。

d. 在「節點資訊」區段中、記下節點的IP位址。

e. 選取*顯示更多*以檢視IPv6位址和介面對應。

您可以從用戶端應用程式建立連線至清單中的任何IP位址：

- * eth0：* Grid Network
- * eth1：*管理網路（選用）
- * eth2：*用戶端網路（選用）

> 如果您正在檢視管理節點或閘道節點、且該節點是高可用度群組中的作用中節點、則HA群組的虛擬IP位址會顯示在eth2上。

3. 若要尋找高可用度群組的虛擬IP位址：

a. 選擇*組態*>*網路*>*高可用度群組*。

b. 在表中、記下HA群組的虛擬IP位址。

4. 若要尋找負載平衡器端點的連接埠號碼：

a. 選擇*組態*>*網路*>*負載平衡器端點*。

b. 記下您要使用的端點連接埠編號。

> 如果連接埠號碼為 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。所有其他連接埠都在閘道節點和管理節點上設定。

c. 從表格中選取端點名稱。

d. 確認 * 用戶端類型 * （ S3 或 Swift ）符合將使用端點的用戶端應用程式。

管理網路和連線

設定網路設定：總覽

您可以從Grid Manager設定各種網路設定、以微調StorageGRID 您的系統運作。

設定**VLAN**介面

您可以 "建立虛擬 LAN （ VLAN ）介面" 隔離及分割流量、以確保安全性、靈活度及效能。每個VLAN介面都會與管理節點和閘道節點上的一個或多個父介面相關聯。您可以使用HA群組和負載平衡器端點中的VLAN介面、依應用程式或租戶來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" 識別及處理不同類型的網路流量、包括與特定貯體、租戶、用戶端子網路或負載平衡器端點相關的流量。這些原則可協助限制流量及監控。

關於鏈路的準則StorageGRID

您可以使用Grid Manager來設定及管理StorageGRID 各種不一致的網路和連線。

請參閱 "設定S3和Swift用戶端連線" 以瞭解如何連接S3或Swift用戶端。

預設StorageGRID 的網路

根據預設StorageGRID 、每個網格節點支援三個網路介面、可讓您針對每個個別網格節點設定網路、以符合安全性和存取需求。

如需網路拓撲的詳細資訊、請參閱 "網路準則"。

網格網路

必要。Grid Network用於所有內部StorageGRID 的資訊流量。它可在網格中的所有節點之間、跨所有站台和子網路提供連線功能。

管理網路

選用。管理網路通常用於系統管理和維護。也可用於用戶端傳輸協定存取。管理網路通常是私有網路、不需要在站台之間進行路由傳送。

用戶端網路

選用。用戶端網路是一種開放式網路、通常用於提供S3和Swift用戶端應用程式的存取、因此網格網路可以隔離並加以保護。用戶端網路可透過本機閘道與任何可連線的子網路進行通訊。

準則

- 每個 StorageGRID 節點都需要專屬的網路介面、 IP 位址、子網路遮罩、以及指派給它的每個網路的閘道。
- 網格節點在網路上不能有多個介面。
- 每個網路支援單一閘道、每個網格節點、而且必須與節點位於相同的子網路上。您可以視需要在閘道中實作更複雜的路由。
- 在每個節點上、每個網路都會對應至特定的網路介面。

網路	介面名稱
網格	eth0
管理（選用）	eth1.
用戶端（選用）	道德 2

- 如果節點連接StorageGRID 到某個ENetApp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、請參閱應用裝置的安裝說明。
- 系統會自動針對每個節點產生預設路由。如果啟用eth2、則0.00.0.0/0會使用eth2上的用戶端網路。如果未啟用eth2、則0.00.0.0/0會在eth0上使用Grid Network。

- 在網格節點加入網格之前、用戶端網路不會運作
- 管理網路可在網格節點部署期間進行設定、以便在網格完全安裝之前、能夠存取安裝使用者介面。

選用介面

或者、您也可以將額外的介面新增至節點。例如、您可能想要將主幹介面新增至管理節點或閘道節點、以便使用 "VLAN 介面" 可分隔屬於不同應用程式或租戶的流量。或者、您可能想要新增存取介面、以便在中使用 "高可用度（HA）群組"。

若要新增主幹或存取介面、請參閱下列內容：

- * VMware（安裝節點之後）*： "VMware：新增主幹或存取介面至節點"
  - * Red Hat Enterprise Linux （安裝節點之前） * ： "建立節點組態檔"
  - * Ubuntu或DEBIAN*（安裝節點之前）*： "建立節點組態檔"
  - * RHEL 、 Ubuntu 或 Debian （安裝節點之後） * ： "Linux：新增主幹或存取介面至節點"

檢視**IP**位址

您可以檢視StorageGRID 您的系統的各個網格節點的IP位址。然後、您可以使用此 IP 位址登入命令列的網格節點、並執行各種維護程序。

開始之前

您將使用登入Grid Manager "支援的網頁瀏覽器"。

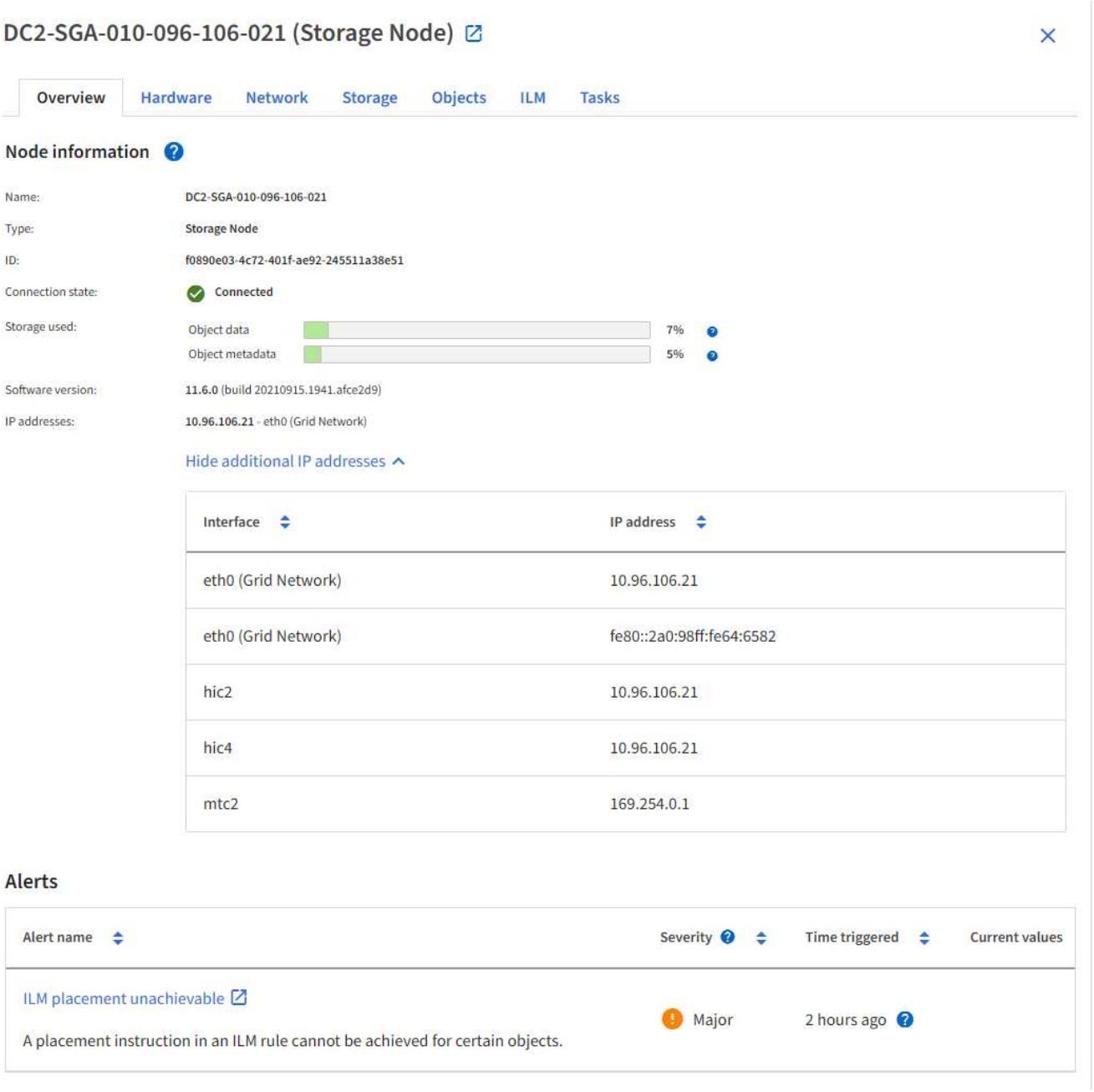
關於這項工作

如需變更 IP 位址的相關資訊、請參閱 "設定IP位址"。

步驟

1. 選擇*節點*>*網格節點*>*總覽*。
2. 選取IP位址標題右側的*顯示更多*。

   該網格節點的IP位址會列在表格中。



設定VLAN介面

您可以在管理節點和閘道節點上建立虛擬LAN（VLAN）介面、並在HA群組和負載平衡器端點中使用這些介面來隔離和分割流量、以確保安全性、靈活度和效能。

VLAN介面考量

- 您可以輸入VLAN ID、然後在一個或多個節點上選擇父介面、藉此建立VLAN介面。
- 父介面必須設定為交換器的主幹介面。
- 父介面可以是Grid Network（eth0）、Client Network（eth2）、或VM或裸機主機的其他主幹介面（例如、ens256）。
- 對於每個VLAN介面、您只能為指定節點選取一個父介面。例如、您無法在同一個 VLAN 的父介面上、同時

使用 Grid Network 介面和 Client Network 介面。

- 如果VLAN介面適用於管理節點流量、包括與Grid Manager和租戶管理程式相關的流量、請選取「僅管理節點」上的介面。
- 如果VLAN介面適用於S3或Swift用戶端流量、請選取管理節點或閘道節點上的介面。
- 如果您需要新增主幹介面、請參閱下列詳細資料：
  - * VMware（安裝節點之後）*： "VMware：新增主幹或存取介面至節點"
  - * RHEL （安裝節點之前） * ： "建立節點組態檔"
  - * Ubuntu或DEBIAN*（安裝節點之前）*： "建立節點組態檔"
  - * RHEL 、 Ubuntu 或 Debian （安裝節點之後） * ： "Linux：新增主幹或存取介面至節點"

建立**VLAN**介面

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 已在網路中設定主幹介面、並附加至VM或Linux節點。您知道主幹介面的名稱。
- 您知道正在設定的VLAN ID。

關於這項工作

您的網路管理員可能已設定一或多個主幹介面和一或多個VLAN、以隔離屬於不同應用程式或租戶的用戶端或管理流量。每個VLAN都會以數字ID或標記來識別。例如、您的網路可能會使用VLAN 100作為FabricPool 不二次流量傳輸、而使用VLAN 200作為歸檔應用程式。

您可以使用Grid Manager建立VLAN介面、讓用戶端能夠在StorageGRID 特定VLAN上存取功能。當您建立VLAN介面時、請指定VLAN ID並選取一或多個節點上的父（主幹）介面。

存取精靈

步驟

1. 選擇*組態*>*網路*>* VLAN介面*。
2. 選擇* Create （建立）。

輸入**VLAN**介面的詳細資料

步驟

1. 指定網路中VLAN的ID。您可以輸入介於1和4094之間的任何值。

   VLAN ID 不一定是唯一的。例如、您可以使用VLAN ID 200來管理某個站台的流量、使用相同的VLAN ID來處理另一個站台的用戶端流量。您可以在每個站台建立具有不同父介面的獨立VLAN介面組。不過、兩個 ID 相同的 VLAN 介面無法在節點上共用相同的介面。 如果您指定已使用的ID、則會出現訊息。

2. （可選）輸入VLAN介面的簡短說明。
3. 選擇*繼續*。

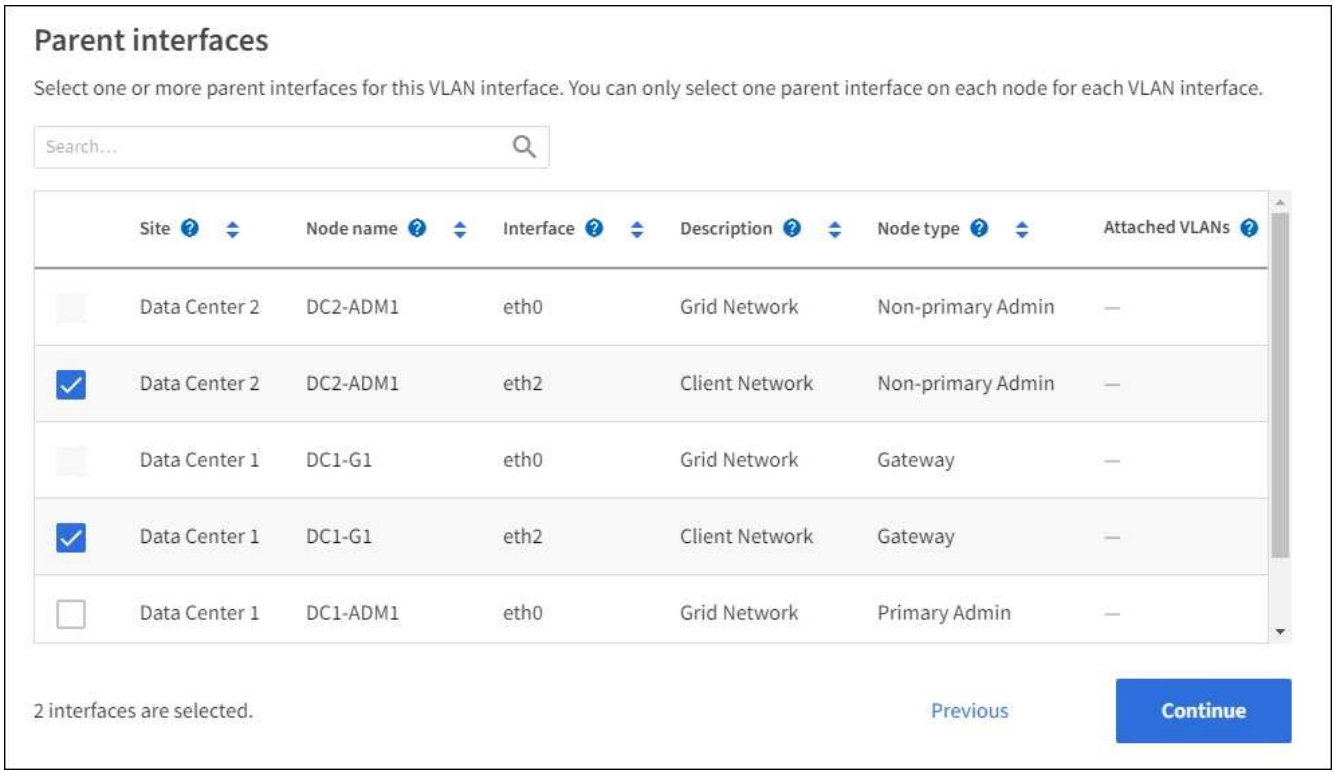
選擇父介面

下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 ）介面無法用作父介面、也無法顯示。

步驟

1. 選取一個或多個父介面來附加此VLAN。

   例如、您可能想要將VLAN附加至閘道節點和管理節點的用戶端網路（eth2）介面。



2. 選擇*繼續*。

確認設定

步驟

1. 檢閱組態並進行任何變更。
   - 如果您需要變更VLAN ID或說明、請選取頁面頂端的*輸入VLAN詳細資料*。
   - 如果您需要變更父介面、請選取頁面頂端的*選擇父介面*、或選取*上一個*。
   - 如果您需要移除父介面、請選取垃圾桶 。
2. 選擇*保存*。
3. 等待5分鐘、讓新介面在「高可用度群組」頁面上顯示為選項、並在節點的*網路介面*表格中列出（節點>*父介面節點_*>*網路*）。

編輯**VLAN**介面

編輯VLAN介面時、您可以進行下列類型的變更：

- 變更VLAN ID或說明。
- 新增或移除父介面。

例如、如果您打算取消委任關聯節點、可能會想要從VLAN介面移除父介面。

請注意下列事項：

- 如果在HA群組中使用VLAN介面、則無法變更VLAN ID。
- 如果父介面用於HA群組、則無法移除該父介面。

  例如、假設VLAN 200連接到節點A和B上的父介面如果 HA 群組將 VLAN 200 介面用於節點 A 、並將 eth2 介面用於節點 B 、您可以移除節點 B 未使用的父介面、但無法移除節點 A 使用的父介面

步驟

1. 選擇*組態*>*網路*>* VLAN介面*。
2. 選取您要編輯的 VLAN 介面核取方塊。然後選取*「動作*」>*「編輯*」。
3. 或者、請更新VLAN ID或說明。然後選擇*繼續*。

   如果在HA群組中使用VLAN、則無法更新VLAN ID。

4. 您也可以選取或清除核取方塊、以新增父介面或移除未使用的介面。然後選擇*繼續*。
5. 檢閱組態並進行任何變更。
6. 選擇*保存*。

移除**VLAN**介面

您可以移除一或多個VLAN介面。

如果VLAN介面目前用於HA群組、則無法移除。您必須先從HA群組移除VLAN介面、才能將其移除。

若要避免用戶端流量中斷、請考慮執行下列其中一項：

- 移除此VLAN介面之前、請先將新的VLAN介面新增至HA群組。
- 建立不使用此VLAN介面的新HA群組。
- 如果您要移除的VLAN介面目前是作用中介面、請編輯HA群組。將您要移除的VLAN介面移至優先順序清單的底部。等到新的主要介面建立通訊之後、再從HA群組移除舊介面。最後、刪除該節點上的VLAN介面。

步驟

1. 選擇*組態*>*網路*>* VLAN介面*。
2. 選取您要移除之每個 VLAN 介面的核取方塊。然後選取*「動作*」>*「刪除*」。
3. 選擇*是*以確認您的選擇。

   您選取的所有VLAN介面都會移除。VLAN介面頁面上會出現綠色的成功橫幅。

管理流量分類原則

管理流量分類原則：總覽

為了強化服務品質（QoS）產品、您可以建立流量分類原則、以識別及監控不同類型的網路流量。這些原則可協助限制流量及監控。

流量分類原則會套用至StorageGRID 閘道節點和管理節點的「動態負載平衡器」服務上的端點。若要建立流量分類原則、您必須已經建立負載平衡器端點。

符合的規則

每個流量分類原則都包含一或多個相符的規則、用以識別與下列一或多個實體相關的網路流量：

- 桶
- 子網路
- 租戶
- 負載平衡器端點

此功能可根據規則的目標、監控符合原則中任何規則的流量。StorageGRID符合原則任何規則的任何流量都會由該原則處理。相反地、您可以設定規則以符合指定實體以外的所有流量。

流量限制

您也可以選擇將下列限制類型新增至原則：

- Aggregate 頻寬
- 每個要求的頻寬
- 並行要求
- 要求率

限制值是以每個負載平衡器為基礎強制執行。如果流量同時分散於多個負載平衡器、則總最大傳輸率是您指定的速率限制的倍數。

> 您可以建立原則來限制Aggregate頻寬或限制每個要求的頻寬。不過、 StorageGRID 無法同時限制這兩種頻寬類型。Aggregate頻寬限制可能會對不受限制的流量造成額外的次要效能影響。

針對Aggregate或每個要求頻寬限制、要求會以您設定的速率傳入或傳出。由於支援的速度只能達到一種、因此根據matcher類型、最符合的原則就是強制執行的速度。StorageGRID此要求所使用的頻寬、並不會與其他包含 Aggregate 頻寬限制原則的較不明確的相符原則相較。對於所有其他限制類型、用戶端要求會延遲250毫秒、並針對超過任何相符原則限制的要求、收到503個慢速回應。

在Grid Manager中、您可以檢視交通路況圖表、並驗證原則是否強制實施您預期的流量限制。

將流量分類原則與**SLA**搭配使用

您可以將流量分類原則與容量限制和資料保護搭配使用、以強制執行服務層級協議（SLA）、以提供容量、資料保護和效能的詳細資訊。

以下範例顯示SLA的三層。您可以建立流量分類原則、以達成每個SLA層級的效能目標。

服務層級	容量	資料保護	允許的最大效能	成本
金級	允許1 PB儲存容量	3複製ILM規則	每秒25 K個要求 每秒5 GB（40 Gbps）頻寬	每月$$
銀級	允許 250 TB 儲存容量	2 複製 ILM 規則	每秒 10 萬次申請 1.25 GB/秒（10 Gbps）頻寬	每月$
銅級	允許 100 TB 儲存容量	2 複製 ILM 規則	每秒 5 K 個要求 每秒 1 Gb （ 8 Gbps ）頻寬	每月$

建立流量分類原則

如果您想要監控流量分類原則、並選擇性地根據貯體、貯體 regex 、 CIDR 、負載平衡器端點或租戶來限制網路流量、則可以建立流量分類原則。您也可以根據頻寬、並行要求數或要求率、來設定原則限制。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 您已建立任何想要比對的負載平衡器端點。
- 您已建立任何想要比對的租戶。

步驟

1. 選擇*組態*>*網路*>*流量分類*。
2. 選擇* Create （建立）。
3. 輸入原則的名稱和說明（選用）、然後選取 * 繼續 * 。

   例如、請說明此流量分類原則的適用範圍及限制。

4. 選取 * 新增規則 * 並指定下列詳細資料、以建立原則的一或多個相符規則。您建立的任何原則都應該至少有一個相符的規則。選擇*繼續*。

欄位	說明
類型	選取符合規則所套用的流量類型。流量類型包括貯體、貯體 regex 、 CIDR 、負載平衡器端點和租戶。

欄位	說明
符合值	輸入符合所選類型的值。 • 貯體：輸入一個或多個貯體名稱。 • 貯體 regex ：輸入一個或多個用於與一組貯體名稱相符的規則運算式。 規則運算式未鎖定。使用 ^ 錨點來比對貯體名稱的開頭、並使用 $ 錨點來比對名稱的結尾。規則運算式比對支援 PCRE （ Perl 相容規則運算式）語法子集。 • CIDR ：以 CIDR 表示法輸入一個或多個符合所需子網路的 IPv4 子網路。 • 負載平衡器端點：選取端點名稱。這些是您在上定義的負載平衡器端點 "設定負載平衡器端點"。 • 租戶：租戶比對使用存取金鑰 ID 。如果要求不包含存取金鑰 ID （例如匿名存取）、則會使用存取的貯體所有權來決定租戶。
反轉比對	如果您想要比對所有網路流量（除了 _ 流量與剛定義的類型和比對值一致）、請選取 * 反轉比對 * 核取方塊。否則、請保留核取方塊的核取方塊。 例如、如果您想要將此原則套用至負載平衡器端點以外的所有端點、請指定要排除的負載平衡器端點、然後選取 * 逆向比對 * 。 對於包含多個資料處理者的原則、其中至少有一個是反向資料處理者、請注意不要建立符合所有要求的原則。

5. 您也可以選擇 * 新增限制 * 、然後選取下列詳細資料、以新增一或多個限制、以控制與規則相符的網路流量。

> StorageGRID 會收集指標、即使您沒有新增任何限制、也能瞭解流量趨勢。

欄位	說明
類型	您要套用至規則所對應網路流量的限制類型。例如、您可以限制頻寬或要求率。 • 注意 * ：您可以建立原則來限制彙總頻寬或限制每個要求的頻寬。不過、StorageGRID 無法同時限制這兩種頻寬類型。當使用 Aggregate 頻寬時、無法使用每個要求的頻寬。相反地、當每個要求的頻寬正在使用中時、就無法使用集合頻寬。Aggregate頻寬限制可能會對不受限制的流量造成額外的次要效能影響。 在頻寬限制方面StorageGRID 、餐廳會套用最符合限制類型的原則。例如、如果您的原則只限制一個方向的流量、則相反方向的流量將不受限制、即使有流量符合具有頻寬限制的其他原則。StorageGRID 以下列順序實作頻寬限制的「最佳」比對： • 確切IP位址（/32遮罩） • 確切的儲存區名稱 • 鏟斗回收系統 • 租戶 • 端點 • 非精確的CIDR相符項目（非/32） • 反比對
適用於	此限制是否適用於用戶端讀取要求（ GET 或 HEAD ）或寫入要求（ PUT 、 POST 或 DELETE ）。
價值	根據您選擇的單位、網路流量將受限於的值。例如、輸入 10 並選取 MIB/s 、以防止符合此規則的網路流量超過 10 MIB/s • 附註 * ：視單位設定而定、可用的單位為二進位（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清單、然後選取 * 使用者偏好設定 * 。
單位	描述您輸入值的單位。

例如、如果您想為 SLA 層建立 40 Gb/s 頻寬限制、請建立兩個集合頻寬限制： Get/head 為 40 Gb/s 、以及將 /post/delete 設為 40 Gb/s

6. 選擇*繼續*。
7. 閱讀並檢閱流量分類原則。使用 * 上一頁 * 按鈕返回並視需要進行變更。當您對原則感到滿意時、請選取 * 儲存並繼續 * 。

   S3 和 Swift 用戶端流量現在會根據流量分類原則來處理。

完成後

"檢視網路流量指標" 驗證原則是否強制執行您預期的流量限制。

編輯流量分類原則

您可以編輯流量分類原則來變更其名稱或說明、或建立、編輯或刪除原則的任何規則或限制。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

步驟

1. 選擇*組態*>*網路*>*流量分類*。

   此時會出現「流量分類原則」頁面、並在表格中列出現有的原則。

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" 輸入內容。

   「行動」功能表

   a. 選取原則的核取方塊。

   b. 選取 * 動作 * > * 編輯 * 。

   詳細資料頁面

   a. 選取原則名稱。

   b. 選取原則名稱旁邊的 * 編輯 * 按鈕。

3. 對於 Enter policy name （輸入策略名稱）步驟，可選擇編輯策略名稱或說明，然後選擇 **Continue** 。
4. 對於 Add matched rules （添加匹配規則）步驟，可選擇添加規則或編輯現有規則的 **Type** 和 **Match Value** ，然後選擇 **Continue** 。
5. 對於設定限制步驟、您可以選擇性地新增、編輯或刪除限制、然後選取 * 繼續 * 。
6. 檢閱更新的原則、然後選取 * 儲存並繼續 * 。

   您對原則所做的變更將會儲存、而且網路流量現在會根據流量分類原則來處理。您可以檢視交通路況圖表、並驗證原則是否強制執行預期的流量限制。

刪除流量分類原則

如果您不再需要流量分類原則、可以刪除該原則。請務必刪除正確的原則、因為刪除時無法擷取原則。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

步驟

1. 選擇*組態*>*網路*>*流量分類*。

此時會出現「流量分類原則」頁面、並在表格中列出現有的原則。

2. 使用「動作」功能表或「詳細資料」頁面刪除原則。

「行動」功能表

a. 選取原則的核取方塊。

b. 選擇*「Actions」（動作）>「Remove*」（移除

原則詳細資料頁面

a. 選取原則名稱。

b. 選取原則名稱旁邊的 * 移除 * 按鈕。

3. 選取 * 是 * 以確認您要刪除原則。

原則即會刪除。

檢視網路流量指標

您可以從「流量分類原則」頁面檢視可用的圖表、以監控網路流量。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權或 Tenant 帳戶權限"。

關於這項工作

對於任何現有的流量分類原則、您可以檢視負載平衡器服務的計量、以判斷原則是否成功限制網路中的流量。圖表中的資料可協助您判斷是否需要調整原則。

即使流量分類原則未設定任何限制、也會收集指標、圖表也會提供實用資訊、協助您瞭解流量趨勢。

步驟

1. 選擇*組態*>*網路*>*流量分類*。

此時會顯示「流量分類原則」頁面、並在表格中列出現有的原則。

2. 選取您要檢視其度量的流量分類原則名稱。
3. 選取 * 指標 * 索引標籤。

此時會出現流量分類原則圖表。這些圖表只會顯示符合所選原則之流量的度量。

頁面中包含下列圖表。

- 要求速率：此圖表提供所有負載平衡器所處理之此原則的頻寬量。收到的資料包括所有要求的要求標頭、以及包含實體資料的回應的實體資料大小。「已傳送」包含所有要求的回應標頭、以及回應中包含實體資料之要求的回應實體資料大小。

當要求完成時、此圖表只會顯示頻寬使用量。對於慢速或大型物件要求、實際的即時頻寬可能與此圖表中報告的值不同。

- 錯誤回應率：此圖表提供與此原則相符的要求將錯誤（ HTTP 狀態代碼 >=400 ）傳回用戶端的大約速率。
- 平均要求持續時間（非錯誤）：此圖表提供符合此原則之成功要求的平均持續時間。
- 原則頻寬使用量：此圖表提供所有負載平衡器所處理之符合此原則的頻寬量。收到的資料包括所有要求的要求標頭、以及包含實體資料的回應的實體資料大小。「已傳送」包含所有要求的回應標頭、以及回應中包含實體資料之要求的回應實體資料大小。

4. 將游標放在折線圖上、即可在圖表的特定部分上看到值的快顯視窗。
5. 選取 Metrics 標題下方的 * Grafana Dashboard * 、即可檢視原則的所有圖形。除了 * 指標 * 索引標籤中的四個圖形之外、您還可以檢視另外兩個圖形：
   - 依物件大小寫入要求率：符合此原則的放置 / 張貼 / 刪除要求的速率。個別儲存格上的定位會顯示每秒的速率。懸停檢視中顯示的速率會被截斷為整數數、當貯體中有非零要求時、可能會報告 0 。
   - 依物件大小讀取要求率：符合此原則的 GET / HEAD 要求率。個別儲存格上的定位會顯示每秒的速率。懸停檢視中顯示的速率會被截斷為整數數、當貯體中有非零要求時、可能會報告 0 。
6. 或者、也可以從*支援*功能表存取圖表。
   a. 選取*支援*>*工具*>*指標*。
   b. 從 **Grafana** 區段中選取 * 交通分類政策 * 。
   c. 從頁面左上角的功能表中選取原則。
   d. 將游標放在圖形上方、即可看到快顯視窗、其中顯示樣本的日期和時間、彙總至計數的物件大小、以及該期間內每秒的要求數。

      流量分類原則會以其ID來識別。原則 ID 會列在「流量分類原則」頁面上。
7. 分析圖表、判斷原則限制流量的頻率、以及是否需要調整原則。

用於傳出**TLS**連線的支援密碼

支援一組有限的加密套件、以便傳輸層安全（TLS）連線至用於身分識別聯盟和雲端儲存資源池的外部系統。StorageGRID

支援的**TLS**版本

支援TLS 1.2和TLS 1.3、可連線至用於身分識別聯盟和雲端儲存資源池的外部系統。StorageGRID

已選取支援搭配外部系統使用的TLS加密器、以確保與各種外部系統相容。此清單大於S3或Swift用戶端應用程式所支援的密碼清單。要配置加密算法，請轉至 * 配置 * > * 安全性 * > * 安全性設置 * ，然後選擇 *TLS 和 SSH 策略 * 。

StorageGRID 中無法設定 TLS 組態選項、例如傳輸協定版本、加密算法、金鑰交換演算法和 MAC 演算法。如果您有關於這些設定的特定要求、請聯絡您的NetApp客戶代表。

作用中、閒置及並行**HTTP**連線的優點

如何設定HTTP連線、可能會影響StorageGRID 到整個系統的效能。組態會因HTTP連線為作用中或閒置狀態、或是您同時有多個連線而有所不同。

您可以找出下列類型HTTP連線的效能優勢：

- 閒置HTTP連線
- 作用中HTTP連線
- 並行HTTP連線

保持閒置**HTTP**連線開啟的優點

即使用戶端應用程式閒置、您仍應保持HTTP連線開啟、以允許用戶端應用程式透過開放式連線執行後續交易。根據系統測量與整合體驗、您應將閒置的HTTP連線保持開啟狀態最長10分鐘。可能會自動關閉持續開啟和閒置超過10分鐘的HTTP連線。StorageGRID

開放式和閒置的HTTP連線提供下列優點：

- 縮短延遲時間、從StorageGRID 由整個過程中、由整個過程中的資訊系統判斷它必須執行HTTP交易到StorageGRID 整個系統能夠執行交易的時間

  縮短延遲是主要優勢、尤其是在建立TCP/IP和TLS連線所需的時間內。

- 使用先前執行的傳輸來初始化TCP/IP慢速啟動演算法、藉此提高資料傳輸率
- 即時通知多種故障情況、可中斷用戶端應用程式與StorageGRID 該系統之間的連線

判斷閒置連線開啟的時間長度、是在與現有連線相關的慢速啟動優點與內部系統資源連線的理想分配之間取得平衡。

作用中**HTTP**連線的優點

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、您仍應將作用中 HTTP 連線的持續時間限制為最多 10 分鐘。

判斷連線應保持開啟的最長時間、是在連線持續性的優點與連線至內部系統資源的理想分配之間取得平衡。

對於用戶端連線至儲存節點、限制作用中的 HTTP 連線有下列優點：

- 在StorageGRID 整個支援過程中實現最佳負載平衡。

  隨著時間推移、隨著負載平衡需求的變更、HTTP連線可能不再是最佳狀態。當用戶端應用程式為每筆交易建立獨立的HTTP連線時、系統會執行最佳負載平衡、但這會使持續連線所帶來的更多寶貴成果喪失價值。

- 允許用戶端應用程式將HTTP交易導向具有可用空間的LDR服務。
- 可啟動維護程序。

  部分維護程序只會在所有進行中的HTTP連線完成後才會開始。

對於連接到負載平衡器服務的用戶端連線、限制開放連線的持續時間、有助於讓部分維護程序立即啟動。如果用

戶端連線的持續時間不受限制、則自動終止作用中連線可能需要幾分鐘的時間。

並行**HTTP**連線的優點

您應該StorageGRID 將多個TCP/IP連線保持開放狀態、以允許平行處理、進而提升效能。最佳的平行連線數量取決於各種因素。

並行HTTP連線提供下列優點：

- 縮短延遲時間

  交易可以立即開始、而非等待其他交易完成。

- 提高處理量

  此系統可執行平行交易、並提高集合交易處理量。StorageGRID

用戶端應用程式應建立多個HTTP連線。當用戶端應用程式必須執行交易時、它可以選取並立即使用任何目前未處理交易的已建立連線。

在StorageGRID 效能開始降級之前、每個支援系統的拓撲在並行交易和連線方面都有不同的尖峰處理量。尖峰處理量取決於運算資源、網路資源、儲存資源和WAN連結等因素。此外、伺服器和服務的數量、StorageGRID 以及支援哪些應用程式、也是因素。

支援多種用戶端應用程式的系統。StorageGRID當您決定用戶端應用程式所使用的並行連線數目上限時、請謹記這一點。如果用戶端應用程式包含多個軟體實體、每個實體都會建立StorageGRID 與該系統的連線、您應該新增整個實體之間的所有連線。在下列情況下、您可能必須調整並行連線的最大數量：

- 此系統的拓撲會影響系統可支援的並行交易和連線數量上限。StorageGRID
- 在StorageGRID 頻寬有限的網路上與該系統互動的用戶端應用程式、可能必須降低並行度、以確保在合理的時間內完成個別交易。
- 當許多用戶端應用程式共用StorageGRID 該系統時、您可能必須減少並行處理的程度、以避免超出系統限制。

分隔**HTTP**連線集區以進行讀取和寫入作業

您可以使用不同的HTTP連線集區進行讀取和寫入作業、並控制每個集區的使用量。獨立的HTTP連線集區可讓您更有效地控制交易並平衡負載。

用戶端應用程式可建立擷取主導（讀取）或儲存主導（寫入）的負載。有了個別的HTTP連線集區、即可針對讀寫交易調整每個集區的專屬容量、以處理讀寫交易。

管理連結成本

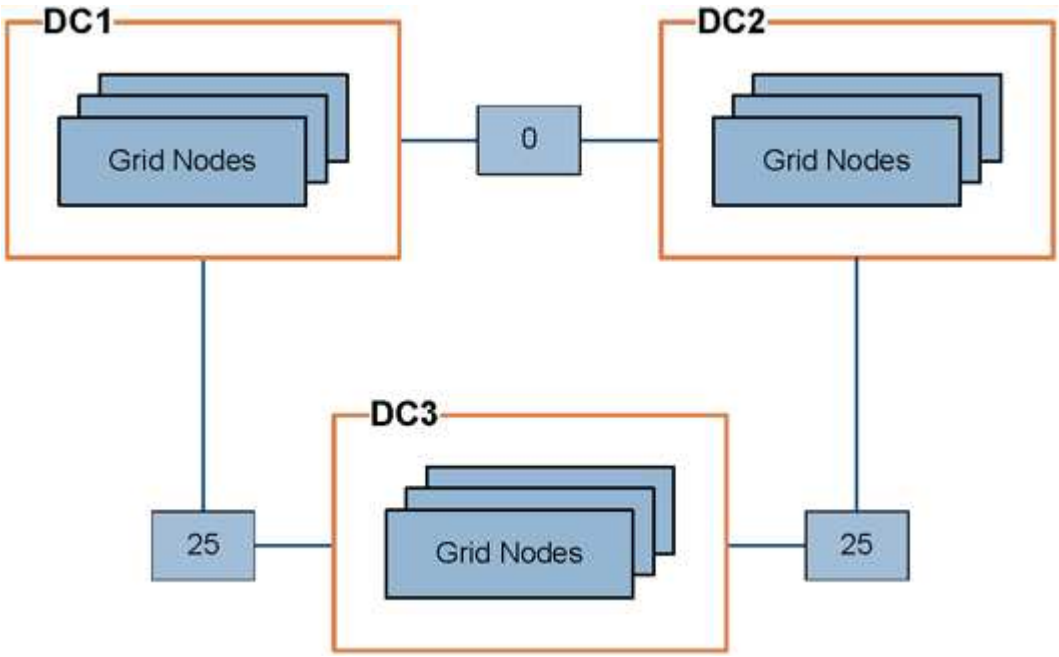
連結成本可讓您在有兩個以上的資料中心站台存在時、排定哪個資料中心站台提供所要求的服務的優先順序。您可以調整連結成本、以反映站台之間的延遲。

什麼是連結成本？

- 連結成本用於排定要使用哪個物件複本來完成物件擷取的優先順序。

- Grid Management API和租戶管理API會使用連結成本來判斷要StorageGRID 使用哪些內部的哪些服務。
- 管理節點和閘道節點上的負載平衡器服務會使用連結成本來導向用戶端連線。請參閱 "負載平衡考量"。

此圖顯示三個站台網格、其中設定站台之間的連結成本：



- 管理節點和閘道節點上的負載平衡器服務會將用戶端連線平均分散到同一個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。

  在此範例中、資料中心站台1（DC1）的閘道節點會將用戶端連線平均分配給DC1的儲存節點、以及DC2的儲存節點。DC3的閘道節點只會將用戶端連線傳送至DC3的儲存節點。

- 當擷取以多個複寫複本形式存在的物件時、StorageGRID 會在連結成本最低的資料中心擷取複本。

  在範例中、如果 DC2 的用戶端應用程式擷取同時儲存在 DC1 和 DC3 的物件、則會從 DC1 擷取該物件、因為 DC1 到 DC2 的連結成本為 0 、低於 DC3 到 DC2 的連結成本（ 25 ）。

連結成本是任意的相對數字、沒有特定的計量單位。例如、連結成本50的優先使用成本低於連結成本25。下表顯示常用的連結成本。

連結	連結成本	附註
在實體資料中心站台之間	25（預設）	透過WAN連結連線的資料中心。
在同一個實體位置的邏輯資料中心站台之間	0%	邏輯資料中心位於同一實體建築物或園區內、由LAN連接。

更新連結成本

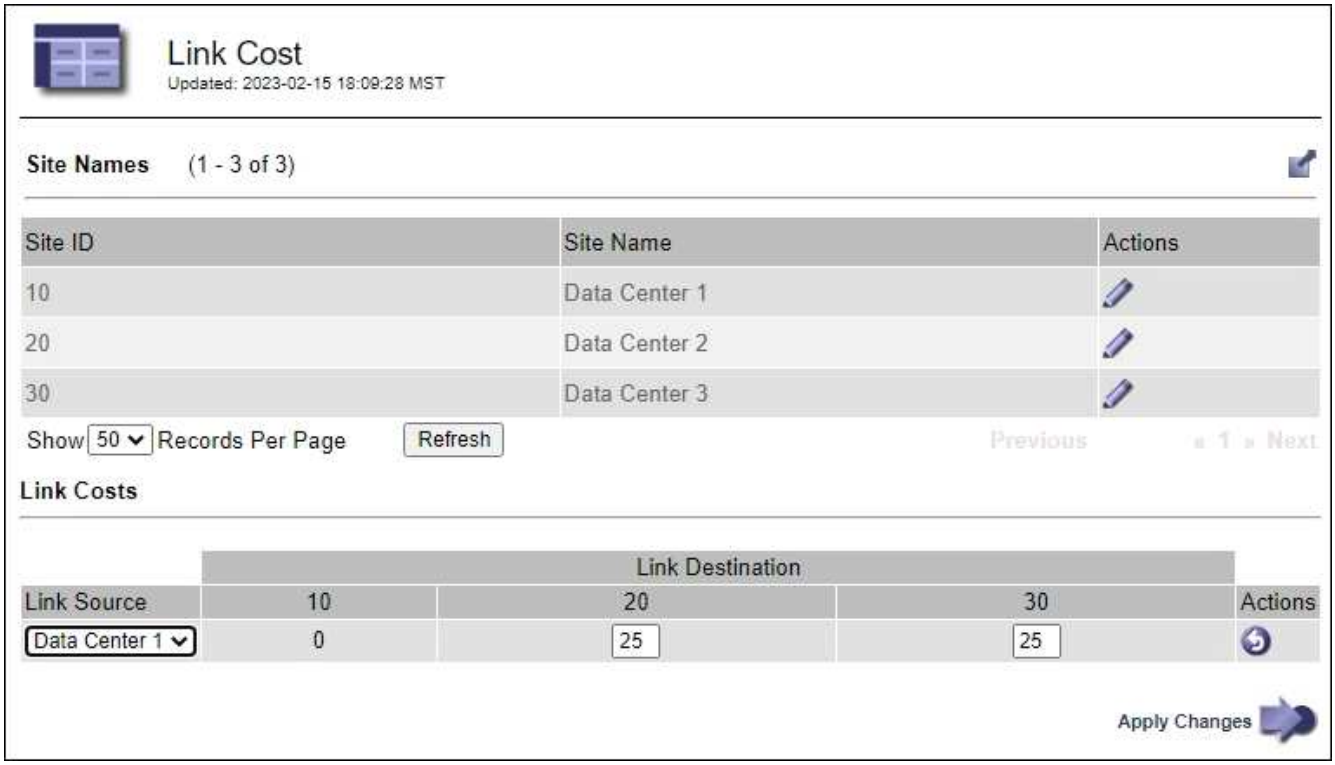
您可以更新資料中心站台之間的連結成本、以反映站台之間的延遲。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "Grid 拓撲頁面組態權限"。

步驟

1. 選擇 * 支援 * > * 其他 * > * 連結成本 * 。



2. 在「連結來源」下選取站台、然後在「連結目的地」下輸入介於0和100之間的成本值。

   如果來源與目的地相同、則無法變更連結成本。

   若要取消變更、請選取 回復。

3. 選取*套用變更*。

使用AutoSupport

使用 **AutoSupport** ：概述

AutoSupport 功能可讓 StorageGRID 將健全狀況和狀態套件傳送至 NetApp 技術支援。

使用 AutoSupport 可以大幅加速問題的判斷與解決。技術支援也能監控系統的儲存需求、協助您判斷是否需要新增節點或站台。您也可以設定 AutoSupport 套件、將其傳送至其他目的地。

StorageGRID 有兩種類型的 AutoSupport ：

StorageGRID AutoSupport

回報 StorageGRID 軟體問題。在您第一次安裝 StorageGRID 時、預設為啟用。您可以 "變更預設的 AutoSupport 組態" 如有需要。

如果未啟用 StorageGRID AutoSupport 、則會在 Grid Manager 儀表板上顯示訊息。此訊息包含AutoSupport 指向「資訊功能」組態頁面的連結。如果您關閉訊息、它將不會再次出現、直到您的瀏覽器快取被清除為止、即使AutoSupport 停用的是停用的。

應用裝置硬體 **AutoSupport**

回報 StorageGRID 應用裝置問題。您必須 "在每個應用裝置上設定硬體 AutoSupport"。

什麼是**Active IQ** 功能？

NetApp是雲端型數位顧問、運用NetApp安裝基礎上的預測分析和社群智慧。Active IQ其持續風險評估、預測性警示、說明性指引及自動化行動、可協助您在問題發生之前預防問題發生、進而改善系統健全狀況並提高系統可用度。

如果您想要在 NetApp 支援網站 上使用 Active IQ 儀表板和功能、您必須啟用 AutoSupport 。

"Active IQ Digital Advisor 數位顧問文件"

AutoSupport 套件中包含的資訊

AutoSupport 套件包含下列 XML 檔案和詳細資料。

檔案名稱	欄位	說明
AutoSupport 歷史記錄 .xml	AutoSupport 序號 此 AutoSupport + 的目的地 觸發事件 交付狀態 交付嘗試 AutoSupport 主旨 傳遞 URI 上次錯誤 AutoSupport Put Filename 世代時代 AutoSupport 壓縮大小 AutoSupport 解壓縮大小 總收集時間（毫秒）	AutoSupport 歷程檔案。
AutoSupport .xml	節點 聯絡支援 + 的通訊協定 支援 HTTP/HTTPS + 的 URL 支援地址 AutoSupport 隨選狀態 AutoSupport 隨需伺服器 URL AutoSupport 隨需輪詢間隔	AutoSupport 狀態檔案。提供使用的通訊協定、技術支援 URL 和位址、輪詢間隔、以及啟用或停用的隨選 AutoSupport 等詳細資料。

檔案名稱	欄位	說明
buckets 。 xml	貯體 ID 帳戶 ID 建置版本 位置限制組態 法規遵循已啟用 法規遵循組態 啟用 S3 物件鎖定 S3 物件鎖定組態 一致性組態 CORS 已啟用 CORS 組態 上次存取時間已啟用 原則已啟用 原則組態 通知已啟用 通知組態 Cloud Mirror 已啟用 Cloud Mirror 組態 啟用搜尋 搜尋組態 Swift 讀取 ACL 已啟用 Swift 讀取 ACL 組態 Swift Write ACL 已啟用 Swift Write ACL 組態 已啟用貯體標記 貯體標記組態 版本設定	提供貯體層級的組態詳細資料和統計資料。貯體組態範例包括平台服務、法規遵循及貯體一致性。
GRID 組態 .xml	屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	全網格組態資訊檔案。包含網格憑證、中繼資料保留空間、網格範圍組態設定（符合性、S3 物件鎖定、物件壓縮、警示、系統記錄、和 ILM 組態）、銷毀編碼設定檔詳細資料、DNS 名稱、 "NMS 名稱"等等。
GRE-SPEC.xml	網格規格、原始 XML	用於設定及部署 StorageGRID 。包含網格規格、 NTP 伺服器 IP 、 DNS 伺服器 IP 、網路拓撲和節點的硬體設定檔。
GRID 工作 .xml	節點 服務路徑 屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	網格工作（維護程序）狀態檔案。提供網格作用中、終止、完成、失敗及擱置工作的詳細資料。

檔案名稱	欄位	說明
GRB.JSON	Grid + Revision + 軟體版本 + 說明 + 授權 + 密碼 + DNS + NTP + 站台 + 節點	網格資訊。
ILM 組態 .xml	屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	ILM 組態的屬性清單。
ILM-STATUS.xml	節點 服務途徑 屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	ILM 計量資訊檔案。包含每個節點的 ILM 評估率、以及全網格的計量。
ILM 。 xml	ILM 原始 XML	ILM 作用中原則檔案。包含使用中 ILM 原則的詳細資料、例如儲存池 ID 、擷取行為、篩選器、規則和說明。也包含預設 ILM 原則的 XML 。
log.Tgz	*n*	可下載的記錄檔。包含 `bycast-err.log` 和 `servermanager.log` 從每個節點。
Manifest.xml	採樣訂單 此資料的 AutoSupport 內容檔名 此資料項目的說明 收集的位元組數 收集時間 此資料項目的狀態 錯誤說明 此資料的 AutoSupport 內容類型	包含 AutoSupport 中繼資料及所有 AutoSupport XML 檔案的簡短說明。
NMS-Entitys.xml	屬性索引 實體 OID 節點 ID 裝置型號 ID 裝置機型版本 實體名稱	中的群組和服務實體 "NMS 樹狀結構"。提供網格拓撲詳細資料。節點可根據節點上執行的服務來決定。

檔案名稱	欄位	說明
objectS-status.xml	節點 服務途徑 屬性 ID 屬性名稱 價值 索引 表 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、傳輸總數、刪除率、 毀損的片段、遺失的物件、遺失的物件、嘗試的修復、掃描速率、 預估掃描期間、維修完成狀態等。
Server-status.xml	節點 服務途徑 屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	伺服器組態和事件檔案。包含每個節點的下列詳細資料：平台類型、作業系統、安裝的記憶體、可用記憶體、儲存連線、 儲存應用裝置機箱序號、儲存控制器磁碟機數失敗、運算控制器機箱溫度、運算硬體、運算控制器序號、電源供應器、磁碟機大小、磁碟機類型等。
service-status.xml	節點 服務途徑 屬性 ID 屬性名稱 價值 索引 表 ID 表格名稱	服務節點資訊檔案。包含詳細資料、例如分配的表格空間、可用表格空間、資料庫的 Reaper 指標、區段修復持續時間、修復工作持續時間、自動重新啟動工作、自動終止工作、 還有更多。
儲存等級 .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。
摘要屬性 .xml	群組 OID 群組路徑 摘要屬性 ID 摘要屬性名稱 價值 索引 表 ID 表格名稱	彙總 StorageGRID 使用資訊的高階系統狀態資料。提供詳細資料、例如網格名稱、網站名稱、每個網格和每個網站的儲存節點數量、授權類型、授權容量和使用量、軟體支援條款、以及 S3 和 Swift 作業的詳細資料。

檔案名稱	欄位	說明
system-arms.xml	節點 服務途徑 嚴重性 警用屬性 屬性名稱 狀態 價值 觸發時間 認可時間	系統層級警示（已過時）和狀態資料、用於指出異常活動或潛在問題。
system-alerts.xml	姓名 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 靜音 其他註釋 其他標籤	指出 StorageGRID 系統中潛在問題的目前系統警示。
USERAGENTS.xml	使用者代理程式 天數 HTTP 要求總數 擷取的總位元組數 擷取的總位元組數 提交要求 取得要求 刪除要求 主管要求 貼文要求 選項要求 平均要求時間（毫秒） 平均投入要求時間（毫秒） 平均取得要求時間（毫秒） 平均刪除要求時間（毫秒） 平均頭部要求時間（毫秒） 平均要求後時間（毫秒） 平均選項要求時間（毫秒）	以應用程式使用者代理程式為基礎的統計資料。例如、每個使用者代理程式的放置 / 取得 / 刪除 / 顯示頭作業數、以及每項作業的總位元組大小。
X-header-data	X-NetApp-asup-Generated on X-NetApp-asup-hostname+ X-NetApp-asup-OS 版本 X-NetApp-asup-Serial-num+ X-NetApp-asup-Subject X-NetApp-asup-system-id X-NetApp-asup-mode-name	AutoSupport 標頭資料。

設定AutoSupport 功能

根據預設、 StorageGRID AutoSupport 功能會在您第一次安裝 StorageGRID 時啟用。不過、您必須在每個應用裝置上設定硬體 AutoSupport 。您可以視需要變更 AutoSupport 組態。

如果您要變更 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。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 如果您要使用 HTTPS 傳送 AutoSupport 套件、您已直接或提供主要管理節點的輸出網際網路存取 "使用 Proxy 伺服器" （不需要輸入連線）。
- 如果在 StorageGRID AutoSupport 頁面上選取 HTTP 、表示您已設定 Proxy 伺服器、將 AutoSupport 套件轉送為 HTTPS 。NetApp 的 AutoSupport 伺服器將拒絕使用 HTTP 傳送的套件。

  "瞭解如何設定管理 Proxy 設定"。
- 如果您將使用 SMTP 做為 AutoSupport 套件的傳輸協定、則表示您已設定 SMTP 郵件伺服器。相同的郵件伺服器組態用於警示電子郵件通知（舊系統）。

關於這項工作

您可以使用下列任一選項組合、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：已啟用。
- * 隨選 * ：允許技術支援人員要求您的 StorageGRID 系統自動傳送 AutoSupport 套件、這在他們主動處理問題時很有用（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。

[[specify － protocol-for － autosupport － packages]] 指定 **AutoSupport** 軟件包的協議

您可以使用下列任一種通訊協定來傳送 AutoSupport 套件：

- * HTTPS *：這是新安裝的預設及建議設定。此通訊協定使用連接埠 443 。如果您想要 啟用 AutoSupport on Demand 功能，您必須使用 HTTPS 。
- **HTTP** ：如果您選取 HTTP 、則必須設定 Proxy 伺服器、才能將 AutoSupport 套件轉送為 HTTPS 。NetApp 的 AutoSupport 伺服器拒絕使用 HTTP 傳送的套件。此通訊協定使用連接埠 80 。
- **SMTP** ：如果您想要以電子郵件傳送 AutoSupport 套件、請使用此選項。如果您使用 SMTP 做為 AutoSupport 套件的傳輸協定、則必須在「舊版電子郵件設定」頁面（ * 支援 * > * 警示（舊版） * > * 舊版電子郵件設定 * ）上設定 SMTP 郵件伺服器。

您設定的傳輸協定用於傳送所有類型的 AutoSupport 封裝。

步驟

1. 選擇 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。

2. 選取您要用來傳送 AutoSupport 套件的傳輸協定。
3. 如果您選取 **HTTPS** 、請選取是否要使用 NetApp 支援憑證（ TLS 憑證）來保護連線至技術支援伺服器的安全。
   - * 驗證憑證 *（預設）：確保 AutoSupport 套件的傳輸安全無虞。NetApp支援證書已隨StorageGRID 支援軟體一起安裝。
   - 不驗證憑證：只有在有充分理由不使用憑證驗證時（例如憑證暫時有問題時）、才選取此選項。
4. 選擇*保存*。所有每週、使用者觸發和事件觸發的套件都會使用選取的傳輸協定來傳送。

停用每週 **AutoSupport**

根據預設、 StorageGRID 系統會設定為每週傳送一次 AutoSupport 套件給技術支援。

若要判斷每週 AutoSupport 套件的傳送時間、請前往 * AutoSupport * > * 結果 * 標籤。在 * 每週 AutoSupport * 區段中、查看 * 下一個排程時間 * 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 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。
2. 清除 * 啟用每週 AutoSupport * 核取方塊。
3. 選擇*保存*。

停用事件觸發的 **AutoSupport**

根據預設、 StorageGRID 系統會設定為每小時傳送一次 AutoSupport 套件給技術支援。

您可以隨時停用事件觸發的 AutoSupport 。

步驟

1. 選擇 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。
2. 清除 * 啟用事件觸發的 AutoSupport * 核取方塊。
3. 選擇*保存*。

啟用**AutoSupport** 隨需功能

根據需求提供支援、協助您解決技術支援部門正在積極處理的問題。AutoSupport

根據預設、AutoSupport 會停用隨需功能。啟用此功能可讓技術支援部門要求您的 StorageGRID 系統自動傳送 AutoSupport 套件。技術支援部門也可以設定AutoSupport 「根據需求進行查詢」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 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。
2. 選取* HTTPS *作為傳輸協定。
3. 選中 *Enable Weekly AutoSupport （每週啓用） * 複選框。

4. 選中 **Enable AutoSupport on Demand** 複選框。
5. 選擇*保存*。

   支援隨需提供支援、技術支援人員可將「根據需求提出的要求」傳送至AutoSupport AutoSupport StorageGRID

停用軟體更新檢查

根據預設、StorageGRID 此功能會聯絡NetApp以判斷您的系統是否有可用的軟體更新。如果StorageGRID 有可用的更新版本或更新版本、則StorageGRID 更新版本會顯示在「更新版」頁面上。

視需要、您可以選擇停用軟體更新檢查。例如、如果您的系統沒有WAN存取、您應該停用檢查、以避免下載錯誤。

步驟

1. 選擇 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。
2. 清除 * 檢查軟體更新 * 核取方塊。
3. 選擇*保存*。

新增**AutoSupport** 其他的目的地

啟用 AutoSupport 時、 heath 和 status 套件會傳送至技術支援。您可以為所有 AutoSupport 套件指定一個額外目的地。

若要驗證或變更用於傳送 AutoSupport 套件的傳輸協定、請參閱的指示 指定 AutoSupport 套件的通訊協定。

> ⓘ 您無法使用 SMTP 傳輸協定將 AutoSupport 套件傳送至其他目的地。

步驟

1. 選擇 * 支援 * > * 工具 * > * AutoSupport * > * 設定 * 。
2. 選取 * 啟用其他 AutoSupport 目的地 * 。
3. 指定下列項目：

   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。

   > ⓘ 您只能輸入一個額外的目的地。

   連接埠
   : 用於連接至其他 AutoSupport 目的地伺服器的連接埠。預設為 HTTP 連接埠 80 或 HTTPS 連接埠 443 。

   憑證驗證
   : 是否使用 TLS 憑證來保護連線至其他目的地的安全。

     ◦ 選取 * 驗證憑證 * 以使用憑證驗證。

◦ 選取 * 不驗證憑證 * 、即可在沒有憑證驗證的情況下傳送 AutoSupport 套件。

只有當您有充分理由不使用憑證驗證時（例如憑證暫時有問題時）、才選取此選項。

4. 如果您選取 * 驗證憑證 * 、請執行下列步驟：
   a. 瀏覽至 CA 憑證的位置。
   b. 上傳 CA 憑證檔案。

      CA 憑證中繼資料即會出現。

5. 選擇*保存*。

所有未來的每週、事件觸發及使用者觸發 AutoSupport 套件都會傳送至其他目的地。

[[autosup-for -ariance]] 設定應用裝置的 **AutoSupport**

AutoSupport for Appliance 回報 StorageGRID 硬體問題、而 StorageGRID AutoSupport 回報 StorageGRID 軟體問題、但有一個例外：對於 SGF6112 、 StorageGRID AutoSupport 同時報告硬體和軟體問題。您必須在每個應用裝置上設定 AutoSupport 、 SGF6112 除外、因為 SGF6112 不需要額外的組態。AutoSupport 在服務應用裝置和儲存設備上的實作方式有所不同。

您可以使用 SANtricity 為每個儲存設備啟用 AutoSupport 。您可以在初始應用裝置設定期間或安裝應用裝置之後、設定 SANtricity AutoSupport ：

- 對於 SG6000 和 SG5700 應用裝置、 "在 SANtricity 系統管理員中設定 AutoSupport"

如果您在中設定透過 Proxy 進行 AutoSupport 傳輸、則 E 系列應用裝置的 AutoSupport 套件可包含在 StorageGRID AutoSupport 中 "系統管理程式SANtricity"。

StorageGRID AutoSupport 不會回報硬體問題、例如 DIMM 或主機介面卡（ HIC ）故障。不過、可能會觸發某些元件故障 "硬體警示"。對於配備主機板管理控制器（ BMC ）的 StorageGRID 應用裝置、您可以設定電子郵件和 SNMP 設陷來回報硬體故障：

- "設定 BMC 警示的電子郵件通知"
- "設定 BMC 的 SNMP 設定"

相關資訊

"NetApp支援"

手動觸發 **AutoSupport** 套件

為了協助技術支援人員疑難排解 StorageGRID 系統的問題、您可以手動觸發要傳送的 AutoSupport 套件。

開始之前

- 您必須使用登入Grid Manager "支援的網頁瀏覽器"。
- 您必須具有「根目錄」存取權或其他網格組態權限。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 在 * 動作 * 索引標籤上、選取 * 傳送使用者觸發的 AutoSupport * 。

   StorageGRID 會嘗試將 AutoSupport 套件傳送至 NetApp 支援網站 。如果嘗試成功、「結果」索引標籤上的*最近結果*和*上次成功時間*值將會更新。如果發生問題、 * 最近的結果 * 值會更新為「失敗」、而 StorageGRID 不會再次嘗試傳送 AutoSupport 套件。

   傳送使用者觸發的 AutoSupport 套件後、請在 1 分鐘後重新整理瀏覽器中的 AutoSupport 頁面、以存取最新的結果。

疑難排解 **AutoSupport** 套件

如果嘗試傳送 AutoSupport 套件失敗、 StorageGRID 系統會根據 AutoSupport 套件類型採取不同的動作。您可以選擇 * 支援 * > * 工具 * > * AutoSupport * > * 結果 * 來檢查 AutoSupport 套件的狀態。

當 AutoSupport 套件無法傳送時、「失敗」會出現在 * AutoSupport * 頁面的 * 結果 * 索引標籤上。

如果您將 Proxy 伺服器設定為將 AutoSupport 套件轉送至 NetApp 、則應該如此 "確認 Proxy 伺服器組態設定正確無誤"。

每週 **AutoSupport** 套件故障

如果每週 AutoSupport 套件無法傳送、 StorageGRID 系統會採取下列動作：

1. 將最新的結果屬性更新為「Retrying（重新執行）」。
2. 每四分鐘嘗試重新傳送 AutoSupport 套件 15 次、持續一小時。
3. 傳送失敗一小時後、將最近的「結果」屬性更新為「失敗」。
4. 嘗試在下一次排程時間再次傳送 AutoSupport 套件。
5. 如果套件因為 NMS 服務無法使用而失敗、且套件在七天內傳送、則會維持正常的 AutoSupport 排程。
6. 當 NMS 服務再次可用時、如果一個套件尚未傳送超過七天、就會立即傳送 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 套件無法傳送、 StorageGRID 系統會採取下列動作：

1. 如果已知錯誤、則顯示錯誤訊息。例如、如果使用者選取的是未提供正確電子郵件組態設定的SMTP傳輸協定、則會顯示下列錯誤： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不會再次嘗試傳送套件。
3. 在中記錄錯誤 `nms.log`。

如果發生故障且選擇了使用SMTP*、請確認StorageGRID 已正確設定支援系統的電子郵件伺服器、且您的電子郵件伺服器正在執行（支援>*警示（舊版）>>舊版電子郵件設定*）。下列錯誤訊息可能會出現在AutoSupport

「介紹」頁面上： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

瞭解操作方法 "設定電子郵件伺服器設定"。

修正 **AutoSupport** 套件故障

如果發生故障且選擇了使用SMTP,請確認StorageGRID 該系統的電子郵件伺服器已正確設定,而且您的電子郵件伺服器正在執行中。下列錯誤訊息可能會出現在AutoSupport 「介紹」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、而非儲存設備管理連接埠、將 E 系列 SANtricity 系統管理員 AutoSupport 套件傳送給技術支援。

請參閱 "E 系列硬體 AutoSupport" 如需搭配 E 系列應用裝置使用 AutoSupport 的詳細資訊、請參閱。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "儲存設備管理員或根存取權限"。
- 您已設定 SANtricity AutoSupport ：
  - 對於 SG6000 和 SG5700 應用裝置、 "在 SANtricity 系統管理員中設定 AutoSupport"

> 您必須擁有SANtricity 更新版本的韌體8.70才能SANtricity 使用Grid Manager存取《系統管理程式》。

關於這項工作

E 系列 AutoSupport 套件包含儲存硬體的詳細資料、比 StorageGRID 系統傳送的其他 AutoSupport 套件更為具體。

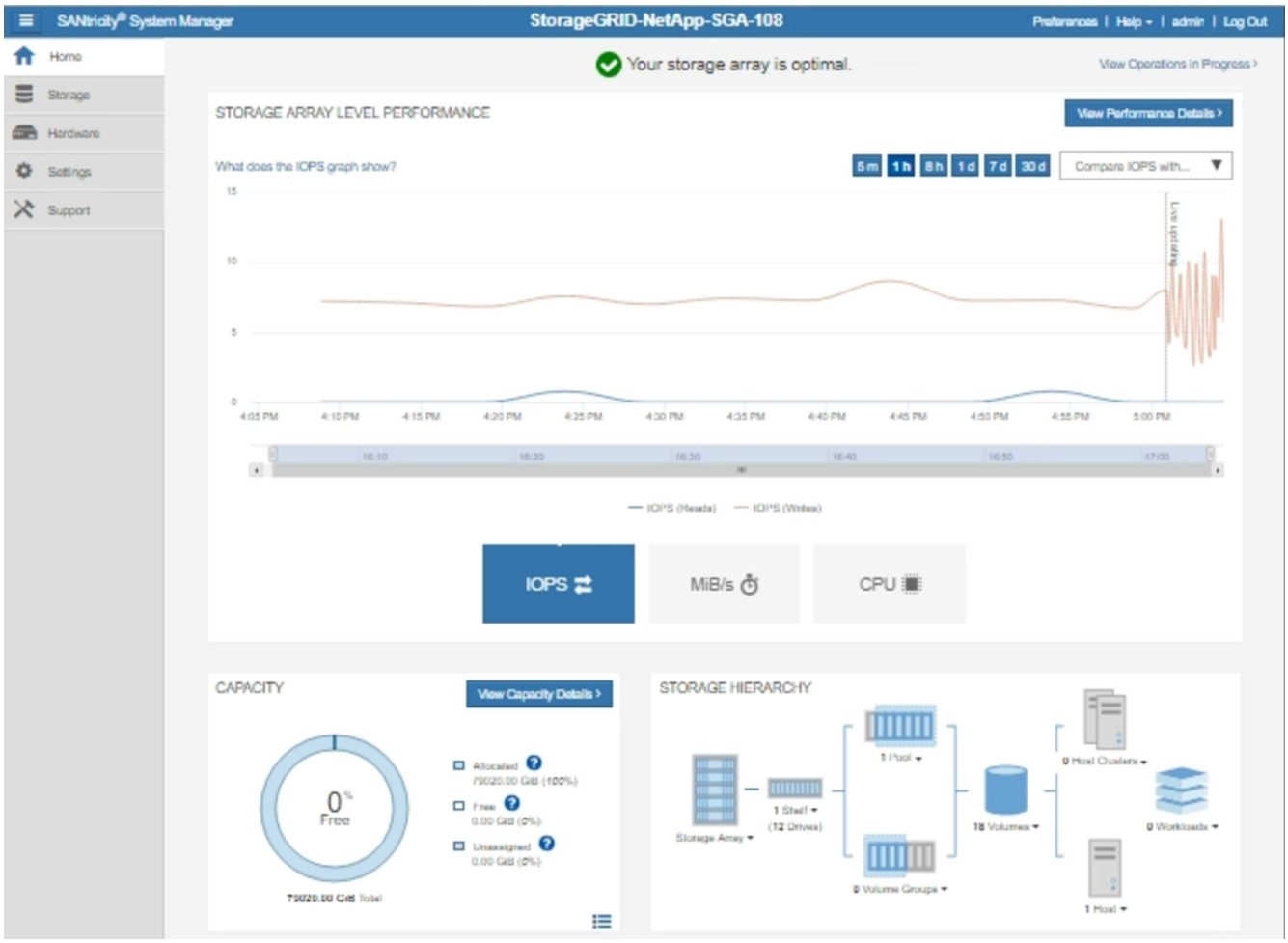
您可以在 SANtricity 系統管理員中設定特殊的 Proxy 伺服器位址、以便透過 StorageGRID 管理節點傳輸 AutoSupport 套件、而無需使用應用裝置的管理連接埠。以這種方式傳輸的 AutoSupport 套件會由傳送 "偏好的寄件者管理節點"、而且他們使用任何 "管理 Proxy 設定" 已在 Grid Manager 中設定的。

> 此程序僅適用於設定 E 系列 AutoSupport 套件的 StorageGRID Proxy 伺服器。如需E系列AutoSupport 的進一步資訊、請參閱 "NetApp E系列與SANtricity VMware文檔"。

步驟

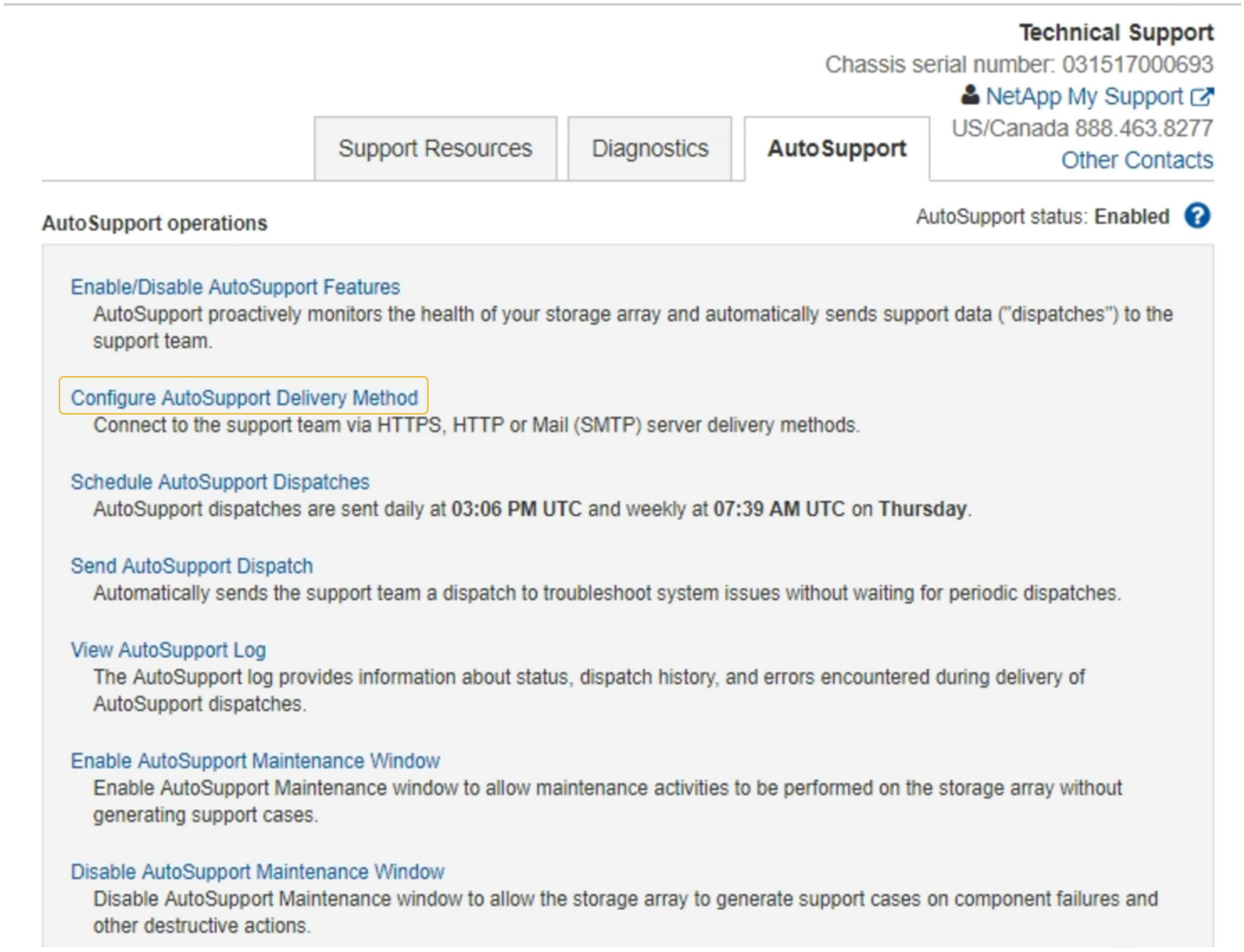
1. 在Grid Manager中、選取* nodes *。
2. 從左側節點清單中、選取您要設定的儲存應用裝置節點。
3. 選擇* SANtricity 《系統管理程式》*。

   出現「系統管理程式」首頁。SANtricity



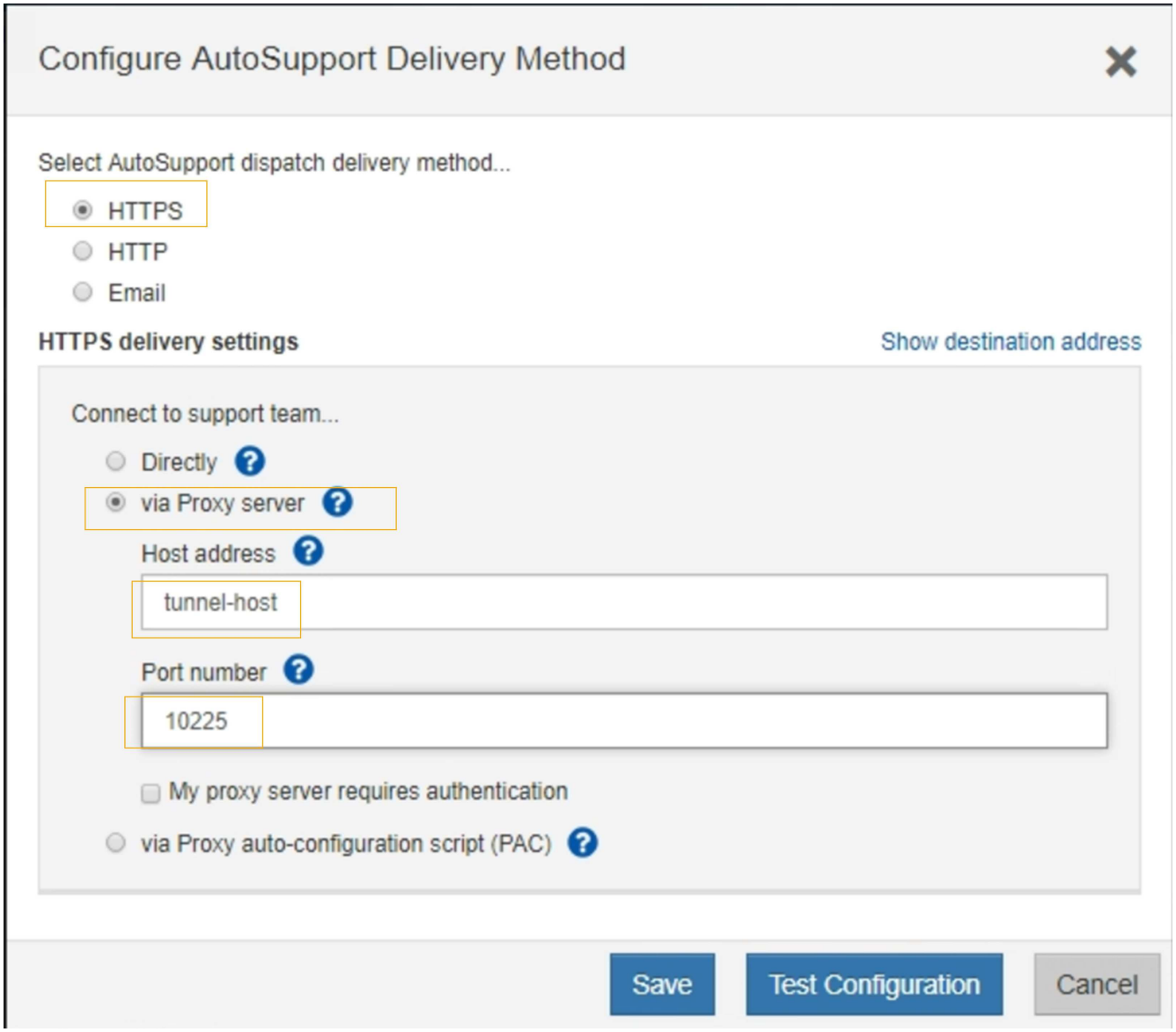
4. 選擇*支援*>*支援中心*>* AutoSupport 支援*。

   畫面上會出現「介紹操作」頁面。AutoSupport



5. 選擇*設定AutoSupport 「供應方法」*。

   此時會出現「設定AutoSupport 供應方法」頁面。



6. 選擇* HTTPS *作為交付方法。

   已預先安裝啟用 HTTPS 的憑證。

7. 選擇*透過Proxy伺服器*。
8. 輸入 `tunnel-host` 主機位址。

   `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` 連接埠號碼。

   `10225` 是 StorageGRID Proxy 伺服器上的連接埠編號、可從應用裝置的 E 系列控制器接收 AutoSupport 套件。

10. 選擇*測試組態*來測試AutoSupport 您的Proxy伺服器的路由和組態。

    如果正確、綠色橫幅中會出現訊息：「您的 AutoSupport 組態已通過驗證。」

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 設定和網路、確定 "偏好的寄件者管理節點" 可以連線至 NetApp 支援網站 、然後再試一次。

11. 選擇*保存*。

    隨即儲存組態、並顯示確認訊息：「 AutoSupport 傳遞方法已設定。」

管理儲存節點

管理儲存節點：總覽

儲存節點提供磁碟儲存容量與服務。管理儲存節點需要：

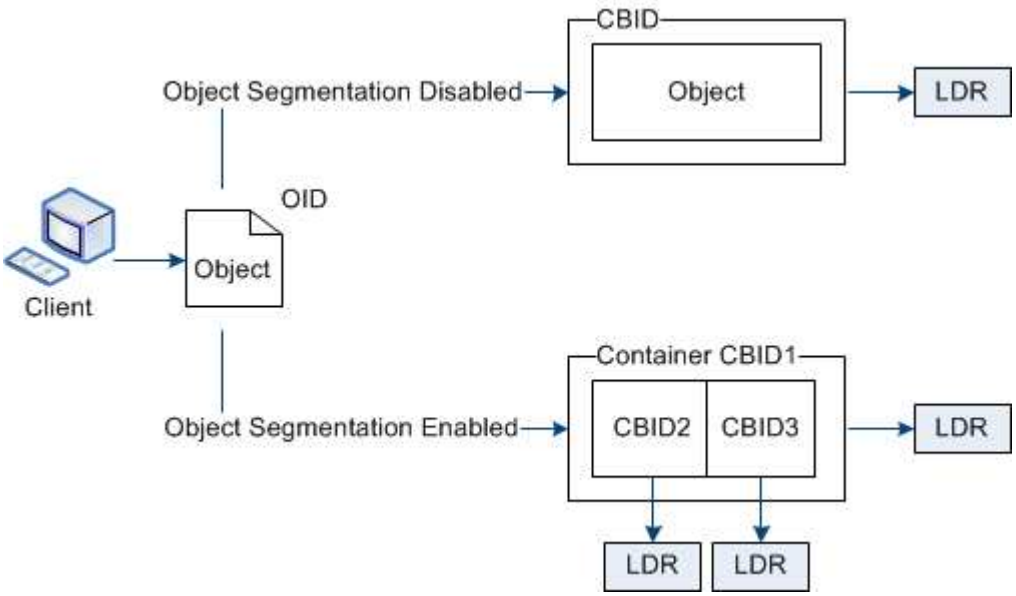
- 管理儲存選項
- 瞭解什麼是儲存Volume浮點、以及當儲存節點變成唯讀時、如何使用浮水印覆寫來控制
- 監控及管理用於物件中繼資料的空間
- 設定儲存物件的全域設定
- 套用儲存節點組態設定
- 管理完整儲存節點

使用儲存選項

什麼是物件區隔？

物件分割是將物件分割成一組較小的固定大小物件、以最佳化大型物件的儲存和資源使用量的程序。S3多重部分上傳也會建立分段物件、並有代表每個部分的物件。

將物件擷取至StorageGRID 物件系統時、LdR服務會將物件分割成區段、並建立區段容器、將所有區段的標頭資訊列為內容。



在擷取區段容器時、LMR服務會從區段組合原始物件、並將物件傳回用戶端。

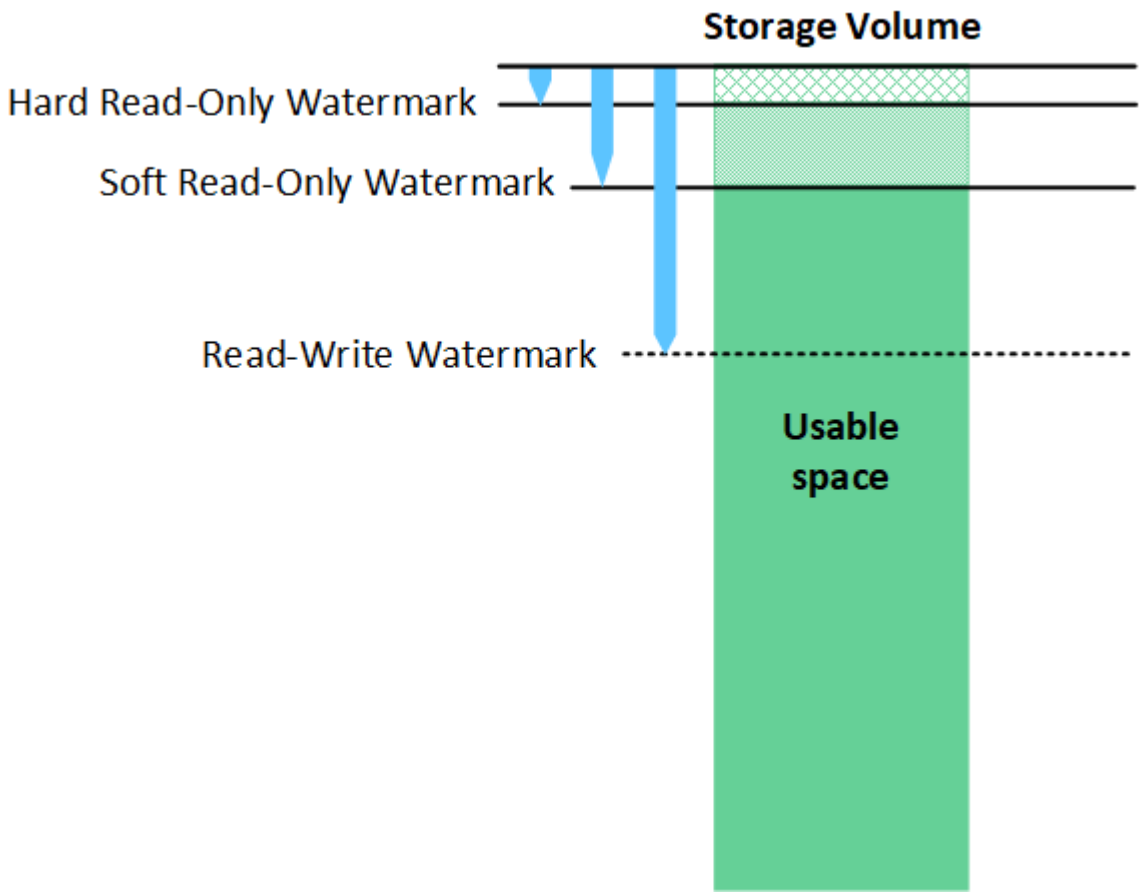
容器和區段不一定儲存在同一個儲存節點上。容器和區段可儲存在ILM規則中指定之儲存資源池內的任何儲存節點上。

每個區段均由StorageGRID 整個系統獨立處理、並有助於計算託管物件和儲存物件等屬性的數量。例如、如果將儲存在StorageGRID 物件叢集系統中的物件分割成兩個區段、則在擷取完成後、「Managed物件」的值會增加三倍、如下所示：

```
segment container + segment 1 + segment 2 = three stored objects
```

什麼是儲存**Volume**浮水印？

利用三個儲存磁碟區浮點、確保儲存節點在極低空間執行之前、安全地轉換為唯讀狀態、並允許已轉換為唯讀狀態的儲存節點再次變成讀寫狀態。StorageGRID



儲存Volume浮點僅適用於複寫和銷毀編碼物件資料所使用的空間。若要瞭解保留給Volume 0上物件中繼資料的空間、請前往 "管理物件中繼資料儲存"。

什麼是軟式唯讀浮標？

「儲存磁碟區軟式唯讀浮點」是第一個浮點、表示儲存節點的物件資料可用空間已滿。

如果儲存節點中的每個磁碟區的可用空間少於該磁碟區的軟式唯讀浮點、則儲存節點會轉換成_read-only模式_。唯讀模式表示儲存節點會將唯讀服務廣告給StorageGRID 其他的作業系統、但會滿足所有擱置中的寫入要求。

例如、假設儲存節點中的每個磁碟區都有10 GB的軟式唯讀浮點。只要每個磁碟區的可用空間少於10 GB、儲存節點就會轉換成軟式唯讀模式。

什麼是硬式唯讀浮標？

「儲存**Volume**硬式唯讀浮點」是下一個浮點、表示節點的物件資料可用空間已滿。

如果磁碟區上的可用空間小於該磁碟區的硬式唯讀浮點、則寫入磁碟區的作業將會失敗。不過、寫入其他磁碟區的作業仍可繼續、直到這些磁碟區上的可用空間低於硬式唯讀浮標為止。

例如、假設儲存節點中的每個磁碟區都有5 GB的硬式唯讀浮點。只要每個磁碟區的可用空間少於5 GB、儲存節點就不再接受任何寫入要求。

硬式唯讀浮點永遠小於軟式唯讀浮點。

什麼是讀寫浮點？

「儲存磁碟區讀寫浮點」僅適用於轉換為唯讀模式的儲存節點。它決定何時可以再次讀寫節點。當儲存節點中任何一個儲存磁碟區的可用空間大於該磁碟區的讀寫浮點時、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。此外、假設每個磁碟區的讀寫浮點為30 GB。只要任何磁碟區的可用空間增加到30 GB、節點就會再次變成讀寫。

「讀寫浮點」永遠大於「軟式唯讀浮點」和「硬式唯讀浮點」。

檢視儲存**Volume**浮點

您可以檢視目前的浮水印設定和系統最佳化的值。如果未使用最佳化的浮水印、您可以判斷是否可以或應該調整設定。

開始之前

- 您已完成 StorageGRID 11.6 或更新版本的升級。
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。

檢視目前的浮水印設定

您可以在Grid Manager中檢視目前的儲存浮水印設定。

步驟

1. 選擇 * 支援 * > * 其他 * > * 儲存浮水印 * 。
2. 在「儲存浮水印」頁面上、查看「使用最佳化值」核取方塊。
   - 如果選取此核取方塊、則會根據儲存節點的大小和磁碟區的相對容量、針對每個儲存節點上的每個儲存磁碟區最佳化所有三個浮水印。

     這是預設和建議的設定。請勿更新這些值。您也可以選擇 檢視最佳化的儲存浮水印。
   - 如果取消選取 [使用最佳化值] 核取方塊，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。請使用的說明 "疑難排解低唯讀浮水印會覆寫警示" 以判斷您是否可以調整或應該調整設定。

指定自訂浮水印設定時、您必須輸入大於 0 的值。

[[view-優 化的儲存浮水印 **]]** 檢視最佳化的儲存浮水印

使用兩個Prometheus指標來顯示其針對*儲存Volume軟式唯讀浮點*所計算的最佳化值。StorageGRID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. 選取*支援*>*工具*>*指標*。
2. 在Prometheus區段中、選取連結以存取Prometheus使用者介面。
3. 若要查看建議的最小軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*執行*：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後一欄顯示每個儲存節點上所有儲存磁碟區的軟式唯讀浮點的最小最佳化值。如果此值大於*儲存磁碟區軟式唯讀浮點*的自訂設定、則會針對儲存節點觸發*低唯讀浮點置換*警示。

4. 若要查看建議的最大軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*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磁碟區的軟式唯讀浮點的最大最佳化值。

管理物件中繼資料儲存

物件中繼資料容量StorageGRID 的功能可控制可儲存在該系統上的物件數量上限。為了確保StorageGRID 您的系統有足夠空間儲存新物件、您必須瞭解StorageGRID 哪些地方及如何儲存物件中繼資料。

什麼是物件中繼資料？

物件中繼資料是指描述物件的任何資訊。利用物件中繼資料來追蹤整個網格中所有物件的位置、並長期管理每個物件的生命週期。StorageGRID

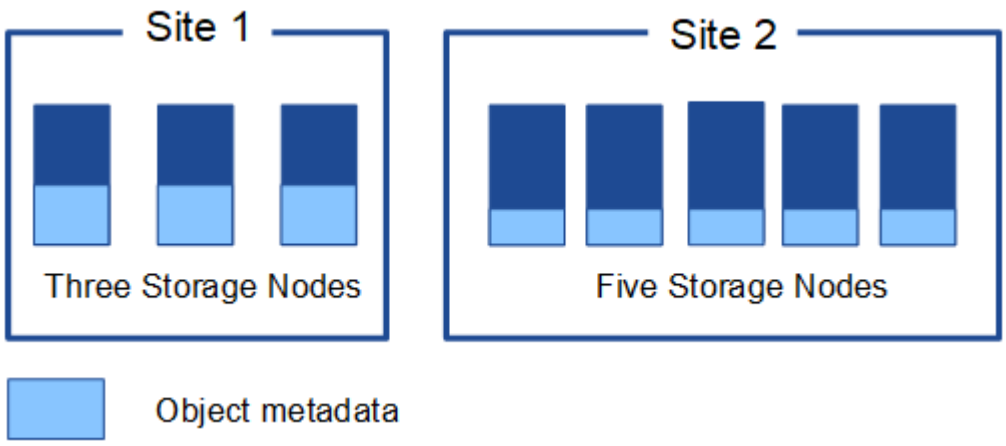
對於物件的物件、物件中繼資料包含下列類型的資訊：StorageGRID

- 系統中繼資料、包括每個物件的唯一ID（UUID）、物件名稱、S3儲存區或Swift容器的名稱、租戶帳戶名稱或ID、物件的邏輯大小、物件第一次建立的日期和時間、 以及物件上次修改的日期和時間。
- 任何與物件相關聯的自訂使用者中繼資料金鑰值配對。
- 對於S3物件、任何與物件相關聯的物件標記金鑰值配對。
- 對於複寫的物件複本、每個複本的目前儲存位置。
- 對於以銷毀編碼的物件複本、每個片段的目前儲存位置。
- 對於Cloud Storage Pool中的物件複本、物件的位置、包括外部儲存區名稱和物件的唯一識別碼。
- 對於分段物件和多部分物件、區段識別碼和資料大小。

物件中繼資料如何儲存？

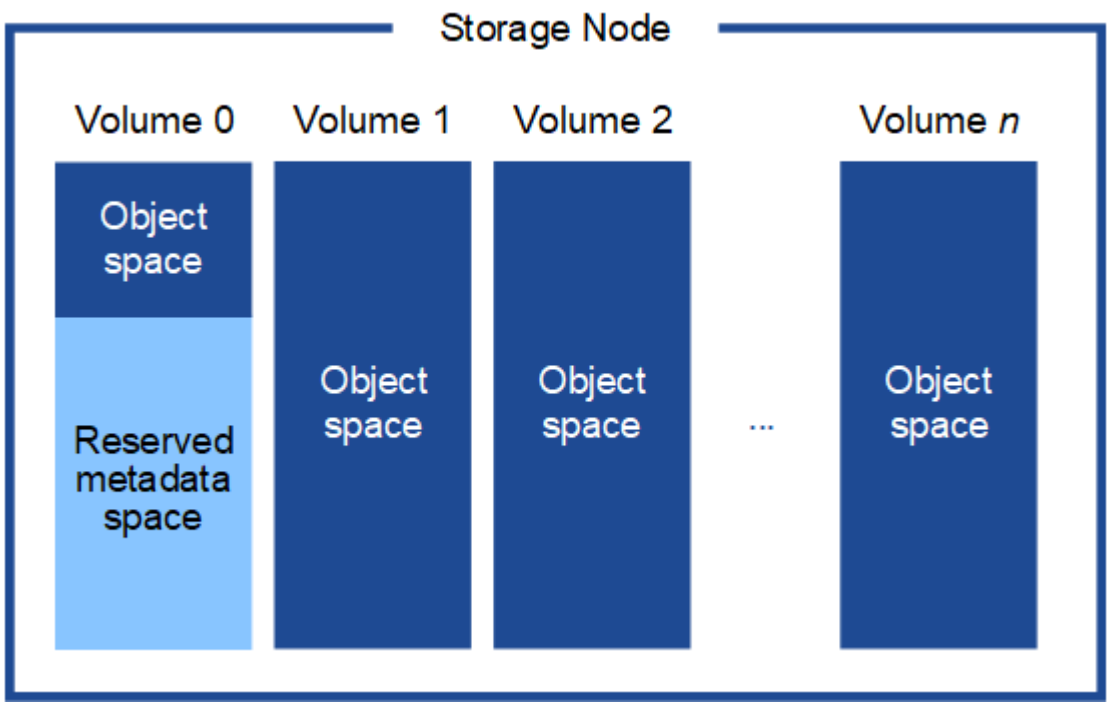
此功能可在Cassandra資料庫中維護物件中繼資料、並獨立儲存物件資料。StorageGRID為了提供備援並保護物件中繼資料免於遺失、StorageGRID 我們在每個站台儲存系統中所有物件的三份中繼資料複本。

此圖代表兩個站台的儲存節點。每個站台都有相同數量的物件中繼資料、而且每個站台的中繼資料會在該站台的所有儲存節點之間細分。



物件中繼資料儲存在何處？

此圖代表單一儲存節點的儲存磁碟區。



如圖所示StorageGRID 、在每個儲存節點的儲存磁碟區0上、利用此功能保留空間來儲存物件中繼資料。它會使用保留空間來儲存物件中繼資料、並執行必要的資料庫作業。儲存磁碟區0和儲存節點中所有其他儲存磁碟區的剩餘空間、僅用於物件資料（複寫複本和銷毀編碼片段）。

在特定儲存節點上、保留給物件中繼資料的空間量取決於以下說明的幾個因素。

中繼資料保留空間設定

_中繼 資料保留空間 _ 是系統範圍的設定、代表將保留給每個儲存節點的磁碟區 0 上中繼資料的空間量。如表所示、此設定的預設值是根據：

- 您剛開始安裝StorageGRID 時使用的軟體版本。
- 每個儲存節點上的RAM容量。

用於初始**StorageGRID** 安裝的版本	儲存節點上的**RAM**容量	預設中繼資料保留空間設定
11.5 至 11.8	在網格中的每個儲存節點上提供128 GB以上的容量	8 TB（8、000 GB）
	在網格中的任何儲存節點上小於128 GB	3 TB（3、000 GB）
11.1 至 11.4	在任一站台的每個儲存節點上提供128 GB以上的容量	4 TB（4、000 GB）
	每個站台上的任何儲存節點均小於128 GB	3 TB（3、000 GB）
11.0 或更早版本	任何金額	2 TB（2、000 GB）

檢視中繼資料保留空間設定

請依照下列步驟檢視 StorageGRID 系統的中繼資料保留空間設定。

步驟

1. 選擇 * 組態 * > * 系統 * > * 儲存設定 * 。
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 。

新 StorageGRID 11.6 或更高版本安裝的預設設定、其中每個儲存節點的 128 GB 或更多 RAM 為 8 、 000 GB （ 8 TB ）。

中繼資料的實際保留空間

與系統範圍的中繼資料保留空間設定不同、物件中繼資料的實際保留空間 _ 是針對每個儲存節點所決定。對於任何指定的儲存節點、中繼資料的實際保留空間取決於節點的 Volume 0 大小和系統範圍的中繼資料保留空間設定。

節點的**Volume 0**大小	中繼資料的實際保留空間
低於 500 GB （非正式作業用途）	10%的Volume 0

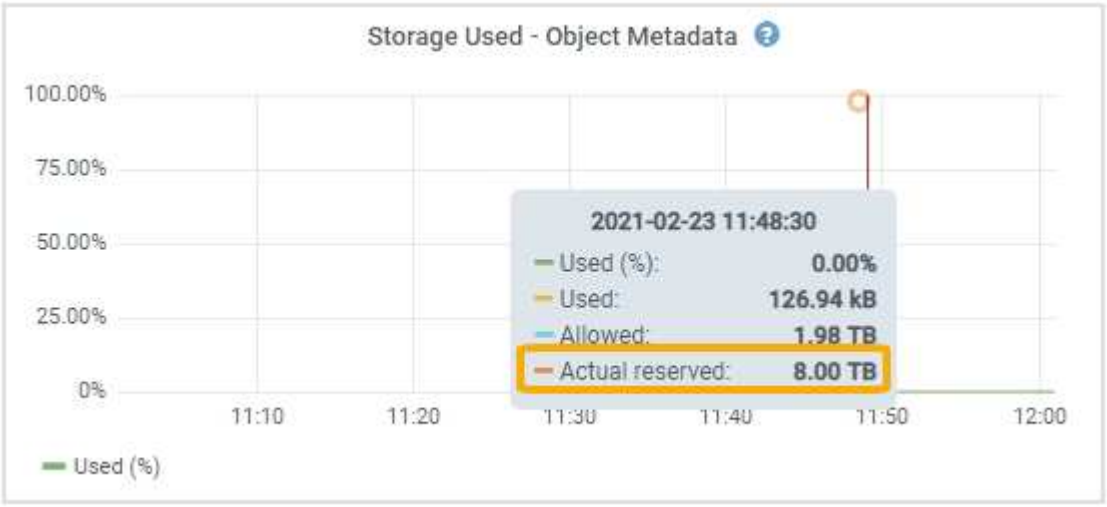
節點的**Volume 0**大小	中繼資料的實際保留空間
500 GB 以上 或 純中繼資料儲存節點	這些值越小： • Volume 0 • 中繼資料保留空間設定 • 附註 * ：僅中繼資料儲存節點只需要一個 rangedb 。

檢視中繼資料的實際保留空間

請依照下列步驟、檢視特定儲存節點上的中繼資料實際保留空間。

步驟

1. 從Grid Manager中選擇* nodes > Storage Node_*。
2. 選擇* Storage*（儲存設備）選項卡。
3. 將游標放在「已使用的儲存空間 - 物件中繼資料」圖表上、然後找出 * 實際保留 * 值。



在快照中、*實際保留*值為8 TB。此螢幕快照適用於全新StorageGRID 安裝的大規模儲存節點。由於系統範圍的中繼資料保留空間設定小於此儲存節點的 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。

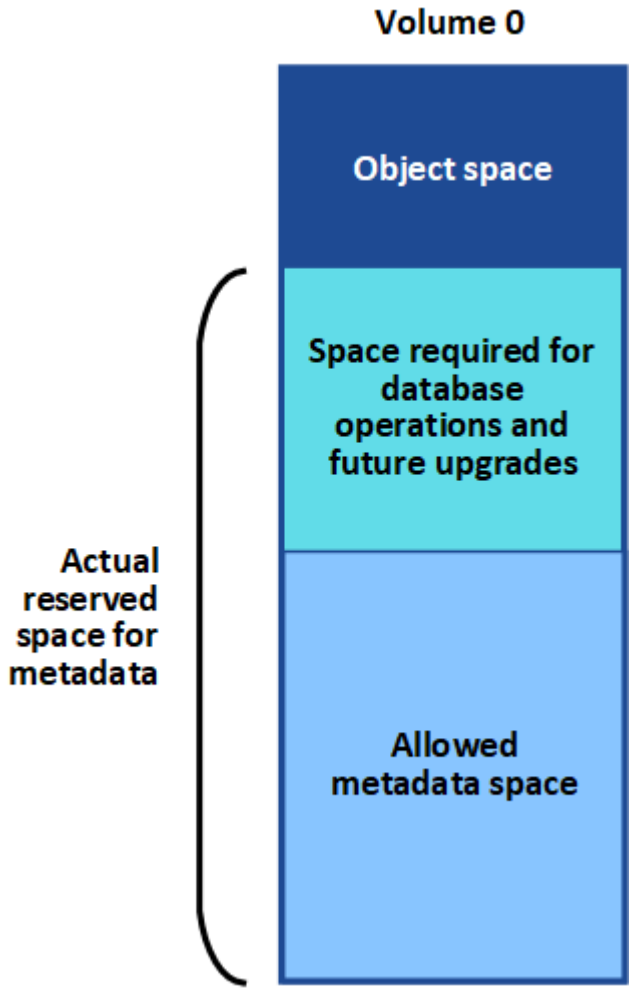
實際保留的中繼資料空間範例

假設您使用 11.7 版或更新版本來安裝新的 StorageGRID 系統。在此範例中、假設每個儲存節點的RAM超過128 GB、而儲存節點1（SN1）的Volume 0為6 TB。根據這些值：

- 系統範圍 * 中繼資料保留空間 * 設定為 8 TB 。（如果每個儲存節點的 RAM 超過 128 GB 、則這是新 StorageGRID 11.6 或更高版本安裝的預設值。）
- 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

每個儲存節點的中繼資料實際保留空間、都會細分為物件中繼資料可用空間（*allowed*中繼資料空間）、以及必要資料庫作業（例如壓縮與修復）和未來硬體與軟體升級所需的空間。允許的中繼資料空間可控制整體物件容量。



下表顯示StorageGRID 根據節點的記憶體容量和中繼資料的實際保留空間、如何針對不同的儲存節點計算*允許的中繼資料空間*。

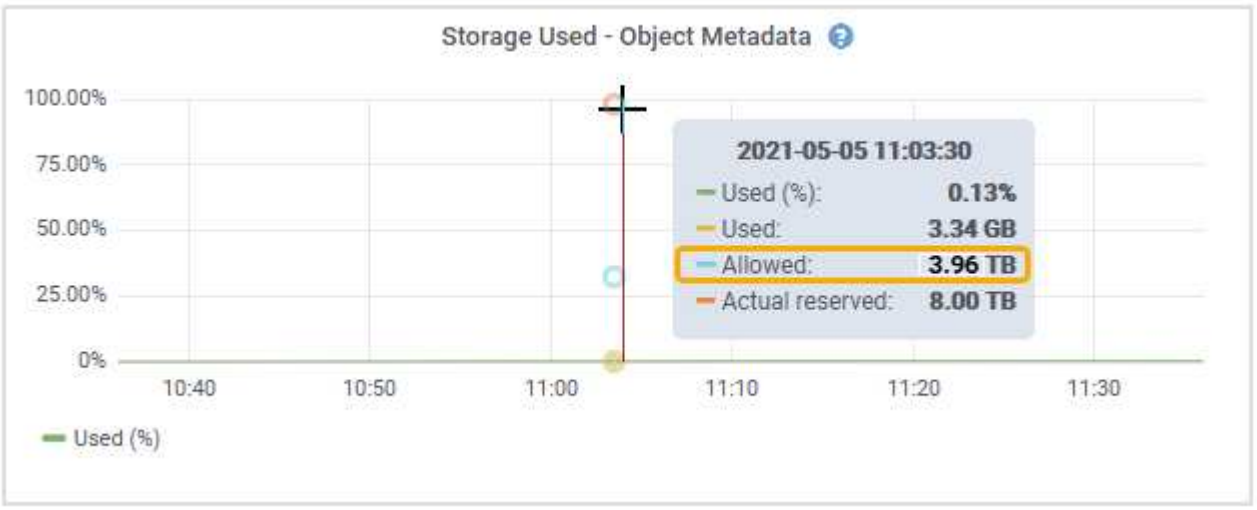
		*儲存節點*上的記憶體容量	
	&lt ； 128 GB	>= 128 GB	中繼資料的實際保留空間
&lt ； = 4 TB	實際保留空間的60%用於中繼資料、最高1.32 TB	實際保留的中繼資料空間的 60% 、最高可達 1.98 TB	4 TB

檢視允許的中繼資料空間

請遵循下列步驟、檢視儲存節點允許的中繼資料空間。

步驟

1. 從Grid Manager中選取* nodes *。
2. 選取儲存節點。
3. 選擇* Storage*（儲存設備）選項卡。
4. 將游標放在「已使用的儲存空間 - 物件中繼資料」圖表上、然後找出 * 允許 * 值。



在螢幕擷取畫面中、*允許*值為3.96 TB、這是實際保留用於中繼資料空間大於4 TB之儲存節點的最大值。

*允許*值對應於此Prometheus指標：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允許的中繼資料空間範例

假設您使用StorageGRID 11.6%版來安裝一個作業系統。在此範例中、假設每個儲存節點的RAM超過128 GB、而儲存節點1（SN1）的Volume 0為6 TB。根據這些值：

- 系統範圍 * 中繼資料保留空間 * 設定為 8 TB 。（當每個儲存節點的 RAM 超過 128 GB 時、這是 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 。）
- 根據中所示的計算結果、SN1上中繼資料的允許空間為3 TB 允許用於中繼資料空間的表格：（中繼資料的實際保留空間：1 TB）x 60%、最高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 、功能不均可在每個站台的儲存節點之間平均散佈物件中繼資料。因此、如果站台包含大小不同的儲存節點、站台上最小的節點就會決定站台的中繼資料容量。

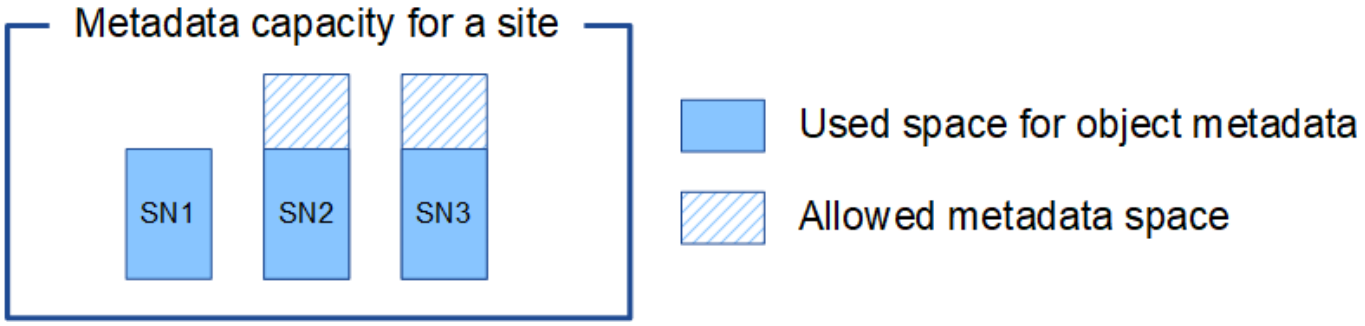
請考慮下列範例：

- 您的單一站台網格包含三個不同大小的儲存節點。

- * 中繼資料保留空間 * 設定為 4 TB 。
- 儲存節點具有下列實際保留中繼資料空間和允許的中繼資料空間值。

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

由於物件中繼資料會平均分散於站台的儲存節點、因此本範例中的每個節點只能容納1.32 TB的中繼資料。無法使用額外的 0.66 TB 的 SN2 和 SN3 中繼資料空間。



同樣地、StorageGRID 由於每StorageGRID 個站台的所有物件中繼資料都是由每個站台的StorageGRID 物件中繼資料容量所決定、因此整個作業系統的中繼資料容量取決於最小站台的物件中繼資料容量。

此外、由於物件中繼資料容量可控制最大物件數、因此當某個節點的中繼資料容量不足時、網格實際上已滿。

相關資訊

- 若要瞭解如何監控每個儲存節點的物件中繼資料容量、請參閱的指示 "監控 StorageGRID"。
- 若要增加系統的物件中繼資料容量、 "展開網格" 新增儲存節點。

增加中繼資料保留空間設定

如果您的儲存節點符合 RAM 和可用空間的特定需求、您可能可以增加中繼資料保留空間系統設定。

您需要的產品

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限或 Grid 拓撲頁面組態和其他 Grid 組態權限"。

關於這項工作

您可以手動將全系統的中繼資料保留空間設定增加至 8 TB 。

只有當這兩個陳述均為真時、您才能增加全系統中繼資料保留空間設定的值：

- 系統中任何站台的儲存節點都有128 GB以上的RAM。
- 系統中任何站台的儲存節點、在儲存Volume 0上都有足夠的可用空間。

請注意、如果您增加此設定、您將會同時減少所有儲存節點之儲存Volume 0上的物件儲存可用空間。因此、您可能偏好根據預期的物件中繼資料需求、將中繼資料保留空間設為小於8 TB的值。

> 一般而言、最好使用較高的值、而非較低的值。如果「中繼資料保留空間」設定太大、您可以稍後再加以減少。相反地、如果您稍後增加值、系統可能需要移動物件資料以釋放空間。

如需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空間的詳細說明、請參閱 "管理物件中繼資料儲存"。

步驟

1. 判斷目前的中繼資料保留空間設定。
   a. 選擇*組態*>*系統*>*儲存選項*。
   b. 在「Storage Watermarks（儲存浮點）」區段中、記下*中繼資料保留空間*的值。
2. 確保每個儲存節點的儲存Volume 0上有足夠的可用空間來增加此值。
   a. 選擇*節點*。
   b. 選取網格中的第一個儲存節點。
   c. 選取「Storage（儲存）」索引標籤。
   d. 在Volumes（磁碟區）區段中、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、而您想要將其增加至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上有足夠的可用空間、請前往下一步。
3. 確保每個儲存節點上至少有128 GB的RAM。
   a. 選擇*節點*。
   b. 選取網格中的第一個儲存節點。
   c. 選取*硬體*索引標籤。
   d. 將游標暫留在「記憶體使用量」圖表上。確保*總記憶體*至少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沒有足夠的可用總記憶體、則無法增加中繼資料保留空間值。請勿繼續執行此程序。
      - 如果每個儲存節點的總記憶體容量至少為128 GB、請執行下一步。
4. 更新中繼資料保留空間設定。

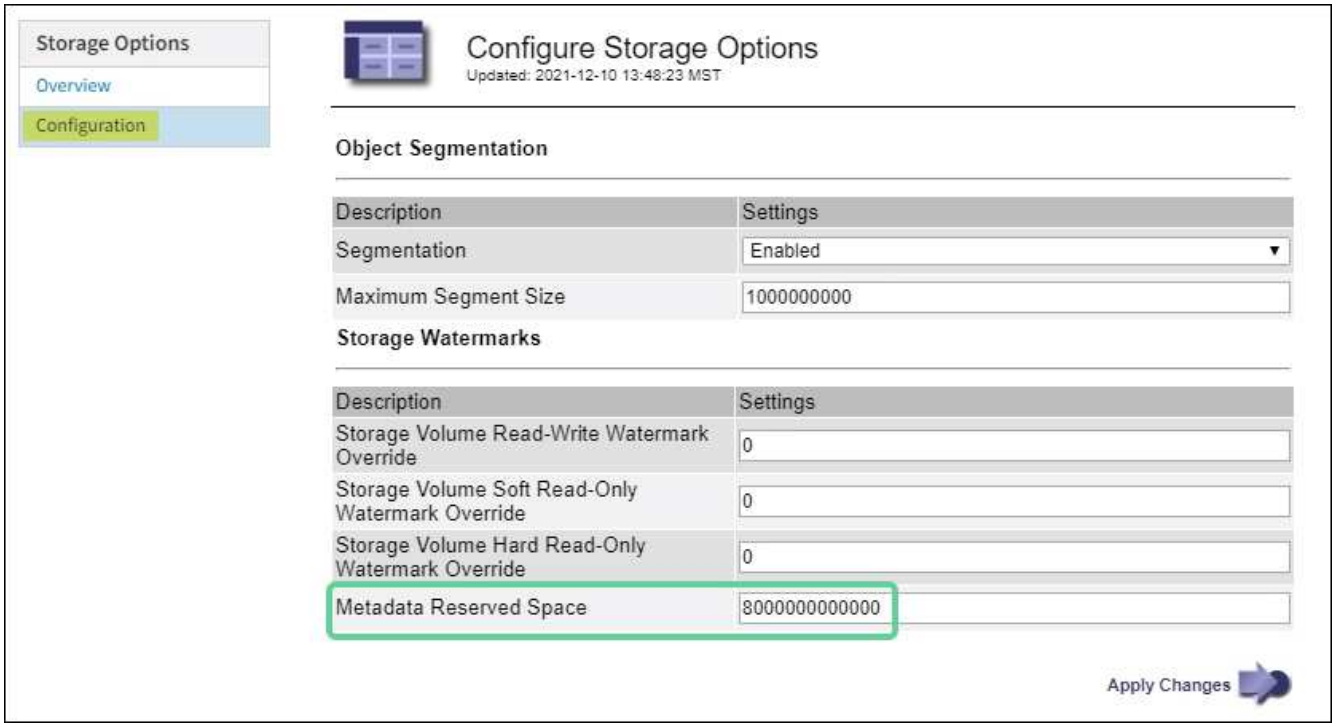
a. 選擇*組態*>*系統*>*儲存選項*。

b. 選取「組態」索引標籤。

c. 在「Storage Watermarks（儲存浮點）」區段中、選取*中繼資料保留空間*。

d. 輸入新值。

例如、若要輸入最大支援值8 TB、請輸入* 80000000000000000*（8、接著12個零）



a. 選取*套用變更*。

壓縮儲存的物件

您可以啟用物件壓縮、以減少儲存在 StorageGRID 中的物件大小、讓物件消耗的儲存空間更少。

開始之前

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

關於這項工作

根據預設、物件壓縮會停用。如果您啟用壓縮、 StorageGRID 會在儲存每個物件時、使用無損壓縮來嘗試壓縮每個物件。

如果您變更此設定、則需要約一分鐘的時間才能套用新設定。系統會快取設定的值、以利效能與擴充。

啟用物件壓縮之前、請注意下列事項：

- 除非您知道儲存的資料是可壓縮的、否則不應選取 * 壓縮儲存的物件 * 。
- 將物件儲存StorageGRID 至物件的應用程式可能會先壓縮物件、然後再儲存物件。如果用戶端應用程式在將物件儲存至 StorageGRID 之前已壓縮物件、選取此選項將不會進一步縮小物件的大小。
- 如果您使用 NetApp FabricPool 搭配 StorageGRID 、請勿選取 * 壓縮儲存的物件 * 。
- 如果選取 * 壓縮儲存的物件 * 、 S3 和 Swift 用戶端應用程式應避免執行指定位元組範圍的 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以存取要求的位元組。從非常大的物件要求少量位元組的 GetObject 作業尤其缺乏效率、例如從 50 GB 壓縮物件讀取 10 MB 範圍是效率不彰的。

  如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

  如果您需要壓縮物件、而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。

步驟

1. 選擇 * 組態 * > * 系統 * > * 儲存設定 * > * 物件壓縮 * 。
2. 選中 **Compress Stored objects** 複選框。
3. 選擇*保存*。

儲存節點組態設定

每個儲存節點都使用數個組態設定和計數器。您可能需要檢視目前的設定或重設計數器來清除警示（舊系統）。

除非文件中有特別指示、否則在修改任何儲存節點組態設定之前、您應諮詢技術支援部門。您可以視需要重設事件計數器、以清除舊有的警示。

請依照下列步驟存取儲存節點的組態設定和計數器。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選取「站台_>*儲存節點_*」。
3. 展開儲存節點、然後選取服務或元件。
4. 選取*組態*索引標籤。

下表摘要說明儲存節點組態設定。

LdR

屬性名稱	程式碼	說明
HTTP 狀態	HSTE	S3 、 Swift 和其他內部 StorageGRID 流量的 HTTP 目前狀態： • 離線：不允許任何作業、任何嘗試開啟HTTP工作階段至LMR服務的用戶端應用程式都會收到錯誤訊息。作用中工作階段會正常關閉。 • 線上：運作正常
自動啟動HTTP	HTAS	• 如果選取此選項、系統重新啟動時的狀態取決於* LdR*>* Storage*元件的狀態。如果* LdR*>* Storage*元件在重新啟動時為唯讀、則HTTP介面也是唯讀的。如果「* LdR*>* Storage*元件」為「線上」、則HTTP也會顯示為「線上」。否則、HTTP介面會維持在離線狀態。 • 如果未選取、HTTP介面會保持離線狀態、直到明確啟用為止。

LDR >資料儲存區

屬性名稱	程式碼	說明
重設遺失物件數	RCOR	重設此服務上遺失物件數的計數器。

LMR >儲存設備

屬性名稱	程式碼	說明
Storage State（儲存狀態）-所需的	SSD	使用者可設定的儲存元件所需狀態設定。LDR服務會讀取此值、並嘗試符合此屬性所指示的狀態。此值會在重新啟動後持續顯示。 例如、您可以使用此設定強制儲存成為唯讀、即使有足夠的可用儲存空間也沒問題。這對疑難排解很有用。 屬性可以使用下列其中一個值： • 離線：當所需的狀態為離線時、LMR服務會使* LdR*>* Storage*元件離線。 • 唯讀：當所需狀態為唯讀時、 LDR 服務會將儲存狀態移至唯讀、並停止接受新內容。不過、 LDR 服務仍會繼續接受 S3 或 ILM 導向的清除和刪除要求。請注意、在開啟的工作階段關閉之前、內容可能會繼續儲存至儲存節點一段短時間。 • 線上：正常系統作業期間、請將價值留在線上。儲存狀態（即儲存元件的目前狀態）將由服務根據LMR服務的條件（例如可用的物件儲存空間量）動態設定。如果空間不足、元件會變成唯讀。
健全狀況檢查逾時	SHCT	健全狀況檢查測試必須完成的時間限制（以秒為單位）、儲存磁碟區才會被視為健全狀況。只有在「支援」指示時才變更此值。

LMR >驗證

屬性名稱	程式碼	說明
重設遺失的物件數	VMI	重設偵測到的遺失物件數（Ois）。僅在物件存在檢查完成後才使用。遺失的複寫物件資料會由StorageGRID 整個系統自動還原。
驗證率	VPRI	設定背景驗證的執行速度。請參閱設定背景驗證率的相關資訊。
重設毀損的物件數	Vccr	重設計數器、以找出在背景驗證期間找到的毀損複寫物件資料。此選項可用於清除偵測到的毀損物件（OCOR）警示條件。

屬性名稱	程式碼	說明
刪除隔離的物件	OQRT	從隔離目錄中刪除毀損的物件、將隔離物件的計數重設為零、然後清除「已偵測到隔離物件（OQRT）」警示。此選項會在作業系統自動還原毀損的物件之後使用StorageGRID 。 如果觸發「遺失物件」警示、技術支援人員可能會想要存取隔離的物件。在某些情況下、隔離的物件可能有助於資料還原或偵錯造成毀損物件複本的基礎問題。

LDR >銷毀編碼

屬性名稱	程式碼	說明
重設寫入失敗計數	RSRWF-..	重設計數器、將銷毀編碼物件資料的寫入失敗寫入儲存節點。
重設讀取失敗計數	RSRF	重設計數器、以瞭解從儲存節點刪除編碼物件資料的讀取失敗情形。
重設刪除失敗計數	RSDF	重設計數器、以刪除儲存節點中以銷毀編碼的物件資料失敗。
重設偵測到毀損的複本計數	RSCC	重設計數器、以取得儲存節點上銷毀編碼物件資料的毀損複本數量。
重設偵測到的毀損片段計數	RCD	重設儲存節點上的銷毀編碼物件資料毀損的片段計數器。
重設偵測到的遺失片段計數	RSMD..	重設儲存節點上的銷毀編碼物件資料遺失片段計數器。僅在物件存在檢查完成後才使用。

LMR >複寫

屬性名稱	程式碼	說明
重設傳入複寫失敗計數	RICR	重設傳入複寫失敗的計數器。這可用來清除RIRF（傳入複寫-失敗）警示。
重設傳出複寫失敗計數	ROCR	重設傳出複寫失敗的計數器。這可用來清除RORF（傳出複製-失敗）警示。

屬性名稱	程式碼	說明
停用傳入複寫	DSIR	選取以停用傳入複寫、作為維護或測試程序的一部分。在正常操作期間保持未核取狀態。 停用傳入複寫時、可從儲存節點擷取物件、以複製到 StorageGRID 系統中的其他位置、但無法從其他位置將物件複製到此儲存節點： LDR 服務為唯讀。
停用輸出複寫	DSOR	選取以停用傳出複寫（包括HTTP擷取內容要求）、作為維護或測試程序的一部分。在正常操作期間保持未核取狀態。 停用輸出複寫時、物件可以複製到此儲存節點、但無法從儲存節點擷取物件、以複製到 StorageGRID 系統的其他位置。LDR服務為純寫入。

管理完整儲存節點

當儲存節點達到容量時、您必須StorageGRID 透過新增的儲存設備來擴充此功能。有三種選項可供選擇：新增儲存磁碟區、新增儲存擴充櫃、以及新增儲存節點。

新增儲存磁碟區

每個儲存節點都支援最大數量的儲存磁碟區。所定義的最大值會因平台而異。如果儲存節點包含的儲存磁碟區數量少於最大儲存磁碟區數量、您可以新增磁碟區來增加其容量。請參閱的說明 "擴充StorageGRID 功能"。

新增儲存擴充櫃

某些 StorageGRID 應用裝置儲存節點（例如 SG6060 或 SG6160 ）可支援額外的儲存櫃。如果StorageGRID 您擁有擴充功能尚未擴充至最大容量的不完整產品、您可以新增儲存櫃來增加容量。請參閱的說明 "擴充StorageGRID 功能"。

新增儲存節點

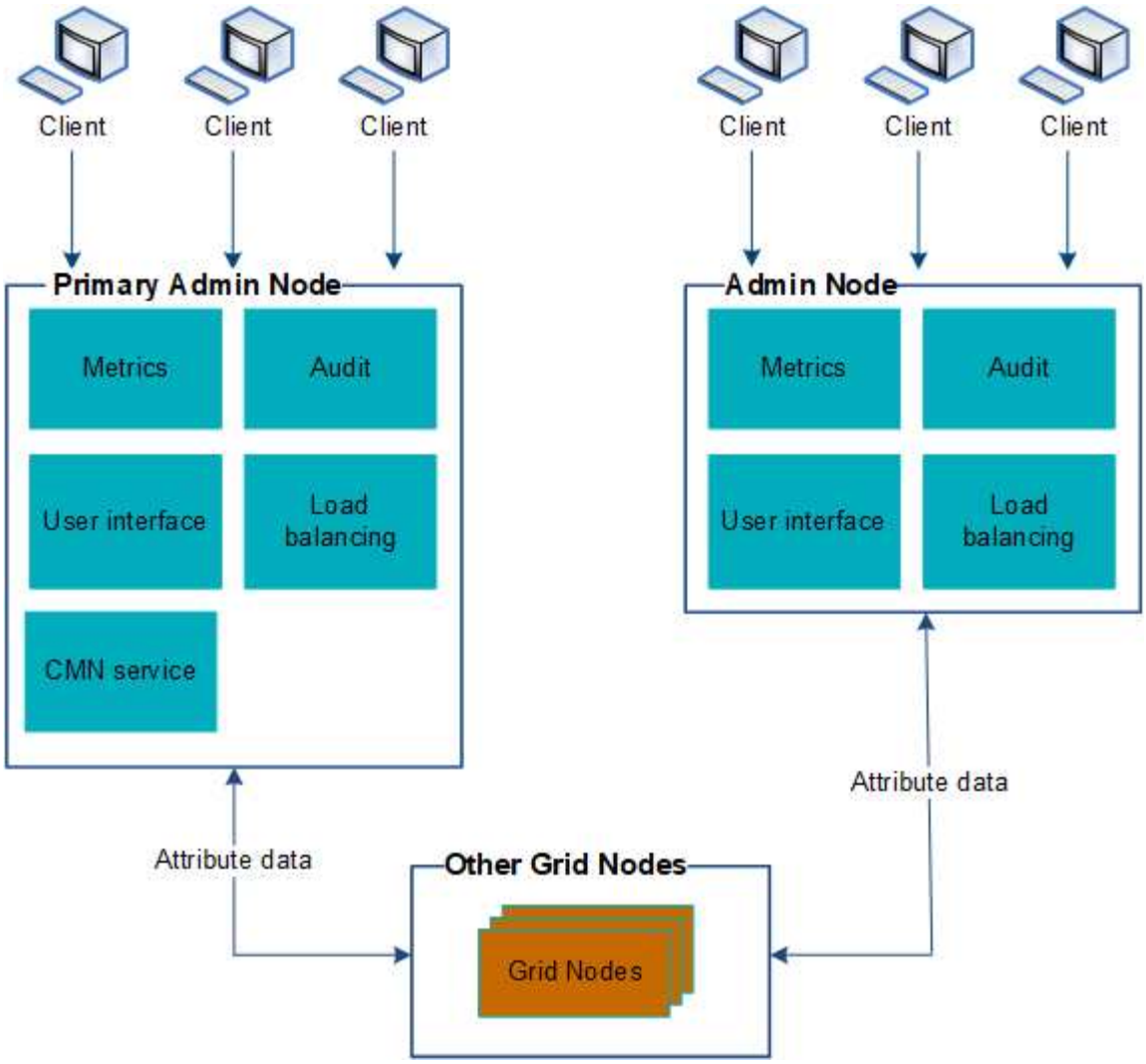
您可以新增儲存節點來增加儲存容量。新增儲存設備時、必須仔細考量目前使用中的ILM規則和容量需求。請參閱的說明 "擴充StorageGRID 功能"。

管理管理節點

使用多個管理節點

包含多個管理節點的支援系統可讓您持續監控及設定您的支援系統、即使其中一個管理節點故障亦然。StorageGRID StorageGRID

如果管理節點無法使用、屬性處理會繼續、警示和警示（舊版系統）仍會觸發、電子郵件通知和 AutoSupport 套件仍會傳送。不過、擁有多個管理節點並不提供容錯移轉保護、只有通知和 AutoSupport 套件除外。特別是、從一個管理節點發出的警示認可不會複製到其他管理節點。



如果管理節點故障、有兩個選項可以繼續檢視及設定StorageGRID 功能不全的系統：

- Web用戶端可重新連線至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、則網路用戶端可使用HA群組的虛擬IP位址、繼續存取Grid Manager或租戶管理程式。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故障、存取就會中斷。使用者必須在HA群組的虛擬IP位址容錯移轉至群組中的另一個管理節點之後、再次登入。

部分維護工作只能使用主要管理節點來執行。如果主要管理節點故障、則必須先將其恢復、才能StorageGRID使該系統再次完全正常運作。

識別主要管理節點

主管理節點裝載CMN服務。部分維護程序只能使用主要管理節點執行。

開始之前

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

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選取*站台_*>*管理節點*、然後選取 ➕ 可展開拓撲樹狀結構並顯示此管理節點上託管的服務。

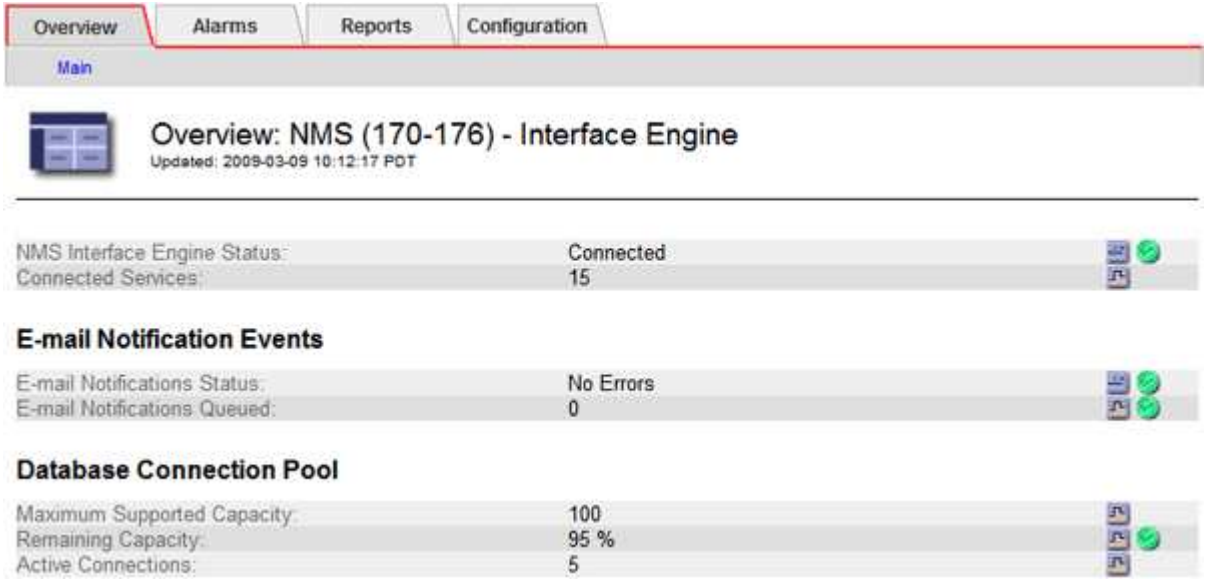
   主管理節點裝載CMN服務。

3. 如果此管理節點未裝載CMN服務、請檢查其他管理節點。

檢視通知狀態和佇列

管理節點上的網路管理系統（NMS）服務會將通知傳送至郵件伺服器。您可以在「介面引擎」頁面上檢視NMS服務的目前狀態及其通知佇列的大小。

若要存取「介面引擎」頁面、請選取*支援*>*工具*>*網格拓撲*。最後、選取*站台_*>*管理節點_*>* NMS*>*介面引擎*。



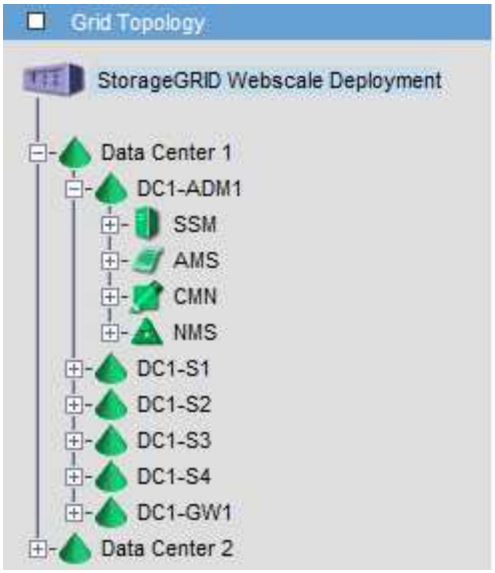
通知會透過電子郵件通知佇列處理、並依觸發順序逐一傳送至郵件伺服器。如果發生問題（例如、網路連線錯誤）、且郵件伺服器在嘗試傳送通知時無法使用、則會繼續嘗試將通知重新傳送至郵件伺服器60秒。如果通知在60秒後未傳送至郵件伺服器、則通知會從通知佇列中捨棄、並嘗試傳送佇列中的下一個通知。

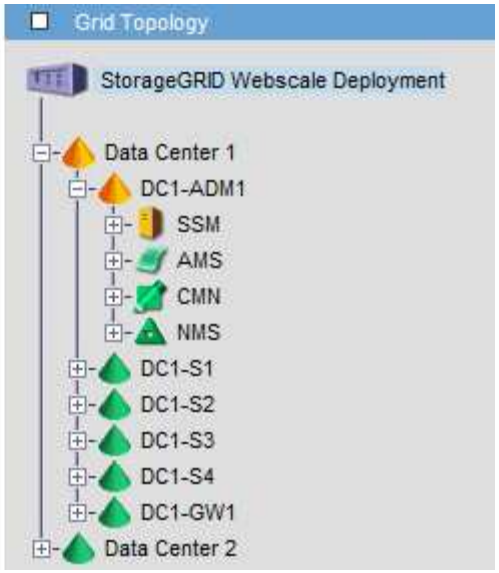
由於通知可從通知佇列中捨棄而不傳送、因此可能在未傳送通知的情況下觸發警示。如果在未傳送通知的情況下、從佇列中斷通知、則會觸發分鐘（電子郵件通知狀態）次要警報。

管理節點如何顯示已確認的警示（舊系統）

當您在一個管理節點上確認警示時、確認的警示不會複製到任何其他管理節點。由於確認不會複製到其他管理節點、因此每個管理節點的 Grid 拓撲樹狀結構看起來可能不同。

這種差異在連接Web用戶端時很有用。Web用戶端可以根據StorageGRID 管理員的需求、擁有不同的視野來檢視整個系統。





請注意、通知會從發生確認的管理節點傳送。

設定稽核用戶端存取

設定 **NFS** 的稽核用戶端存取

管理節點透過稽核管理系統（AMS）服務、將所有稽核的系統事件記錄到可透過稽核共用區取得的記錄檔中、稽核共用區會在安裝時新增至每個管理節點。稽核共用會自動啟用為唯讀共用。

NFS 支援已過時、將於未來版本中移除。

若要存取稽核記錄、您可以設定用戶端存取來稽核 NFS 的共用。或者、您也可以 "使用外部 Syslog 伺服器"。

此系統使用正面的認可、在稽核訊息寫入記錄檔之前、防止其遺失。StorageGRID在AMS服務或中繼稽核轉送服務已認可其控制權之前、訊息會一直排入服務佇列。如需詳細資訊、請參閱 "檢閱稽核記錄"。

開始之前

- 您擁有 `Passwords.txt` 具有 root / admin 密碼的檔案。
- 您擁有 `Configuration.txt` 檔案（可在恢復套件中取得）。
- 稽核用戶端使用NFS版本3（NFSv3）。

關於這項工作

針對StorageGRID 您要從中擷取稽核訊息的各個執行此程序、以利執行此程序。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`

d. 輸入中所列的密碼 `Passwords.txt` 檔案：

當您以root登入時、提示會從變更 `$` 至 `#`。

2. 確認所有服務的狀態均為「執行中」或「已驗證」。輸入： `storagegrid-status`

如果任何服務未列示為「執行中」或「已驗證」、請先解決問題再繼續。

3. 返回命令列。按* Ctrl-+ C*。
4. 啟動NFS組態公用程式。輸入： `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients              | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config  |
| enable-disable-share  | remove-ip-from-share | refresh-config   |
|                       |                      | help             |
|                       |                      | exit             |
----------------------------------------------------------------------
```

5. 新增稽核用戶端： `add-audit-share`
   a. 出現提示時、輸入稽核共用區的稽核用戶端IP位址或IP位址範圍： `client_IP_address`
   b. 出現提示時、請按* Enter *。
6. 如果允許多個稽核用戶端存取稽核共用區、請新增其他使用者的IP位址： `add-ip-to-share`
   a. 輸入稽核共用的數量： *`audit_share_number`*
   b. 出現提示時、輸入稽核共用區的稽核用戶端IP位址或IP位址範圍： *`client_IP_address`*
   c. 出現提示時、請按* Enter *。

   隨即顯示NFS組態公用程式。

   d. 針對每個具有稽核共用存取權的其他稽核用戶端重複這些子步驟。
7. 或者、請驗證您的組態。
   a. 輸入下列項目： `validate-config`

   系統會檢查並顯示這些服務。

   b. 出現提示時、請按* Enter *。

   隨即顯示NFS組態公用程式。

   c. 關閉NFS組態公用程式： `exit`
8. 判斷您是否必須在其他站台啟用稽核共用。
   ◦ 如果StorageGRID 這個部署是單一站台、請前往下一步。

- 如果StorageGRID 此功能包括其他站台的管理節點、請視需要啟用這些稽核共用：
  i. 遠端登入站台的管理節點：
    A. 輸入下列命令： `ssh admin@grid_node_IP`
    B. 輸入中所列的密碼 `Passwords.txt` 檔案：
    C. 輸入下列命令以切換至root： `su -`
    D. 輸入中所列的密碼 `Passwords.txt` 檔案：
  ii. 重複這些步驟、為每個額外的管理節點設定稽核共用。
  iii. 關閉遠端安全Shell登入遠端管理節點。輸入： `exit`

9. 登出命令Shell： `exit`

NFS稽核用戶端會根據其IP位址授予稽核共用的存取權。將稽核共用區的IP位址新增至共用區、將稽核共用區的存取權限授予新的NFS稽核用戶端、或移除現有的稽核用戶端IP位址、以移除該用戶端。

將**NFS**稽核用戶端新增至稽核共用區

NFS稽核用戶端會根據其IP位址授予稽核共用的存取權。將稽核共用的IP位址新增至稽核共用區、將稽核共用區的存取權限授予新的NFS稽核用戶端。

NFS 支援已過時、將於未來版本中移除。

開始之前

- 您擁有 `Passwords.txt` 具有 root / admin 帳戶密碼的檔案。
- 您有 `Configuration.txt` 檔案（可在恢復套件中取得）。
- 稽核用戶端使用NFS版本3（NFSv3）。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

   當您以root登入時、提示會從變更 `$` 至 `#`。

2. 啟動NFS組態公用程式： `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. 輸入： `add-ip-to-share`

   隨即顯示在管理節點上啟用的NFS稽核共用清單。稽核共用列示如下： `/var/local/log`

4. 輸入稽核共用的數量： *`audit_share_number`*
5. 出現提示時、輸入稽核共用區的稽核用戶端IP位址或IP位址範圍： *`client_IP_address`*

   稽核用戶端隨即新增至稽核共用區。

6. 出現提示時、請按* Enter *。

   隨即顯示NFS組態公用程式。

7. 針對應新增至稽核共用的每個稽核用戶端重複這些步驟。
8. 或者、請確認您的組態： `validate-config`

   系統會檢查並顯示這些服務。

   a. 出現提示時、請按* Enter *。

      隨即顯示NFS組態公用程式。

9. 關閉NFS組態公用程式： `exit`
10. 如果StorageGRID 這個部署是單一站台、請前往下一步。

    否則StorageGRID 、如果無法執行的部署包括其他站台的管理節點、則可視需要啟用這些稽核共用：

    a. 遠端登入站台的管理節點：

       i. 輸入下列命令： `ssh admin@grid_node_IP`

       ii. 輸入中所列的密碼 `Passwords.txt` 檔案：

       iii. 輸入下列命令以切換至root： `su -`

       iv. 輸入中所列的密碼 `Passwords.txt` 檔案：

    b. 重複這些步驟、為每個管理節點設定稽核共用。

    c. 關閉遠端安全Shell登入遠端管理節點： `exit`

11. 登出命令Shell： `exit`

驗證NFS稽核整合

設定稽核共用區並新增NFS稽核用戶端之後、您可以掛載稽核用戶端共用區、並驗證這些檔案是否可從稽核共用區取得。

NFS 支援已過時、將於未來版本中移除。

步驟

1. 使用主控AMS服務之管理節點的用戶端IP位址、驗證連線能力（或用戶端系統的變體）。輸入： `ping IP_address`

   確認伺服器回應、表示連線能力。

2. 使用適用於用戶端作業系統的命令掛載稽核唯讀共用。Linux 命令範例為（一行輸入）：

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit`

   使用管理節點的IP位址來裝載AMS服務、以及稽核系統的預先定義共用名稱。掛載點可以是用戶端選取的任何名稱（例如、 `myAudit` 上一個命令中）。

3. 確認檔案可從稽核共用區取得。輸入： `ls myAudit /*`

   其中 `myAudit` 是稽核共用的掛載點。至少應列出一個記錄檔。

從稽核共用區移除NFS稽核用戶端

NFS稽核用戶端會根據其IP位址授予稽核共用的存取權。您可以移除現有的稽核用戶端IP位址、以移除該用戶端。

開始之前

- 您擁有 `Passwords.txt` 具有 root / admin 帳戶密碼的檔案。
- 您擁有 `Configuration.txt` 檔案（可在恢復套件中取得）。

關於這項工作

您無法移除上次允許存取稽核共用的 IP 位址。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入中所列的密碼 `Passwords.txt` 檔案：
   c. 輸入下列命令以切換至root： `su -`
   d. 輸入中所列的密碼 `Passwords.txt` 檔案：

      當您以root登入時、提示會從變更 `$` 至 `#`。

2. 啟動NFS組態公用程式： `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

3. 從稽核共用區移除IP位址： `remove-ip-from-share`

   隨即顯示伺服器上設定的稽核共用編號清單。稽核共用列示如下： `/var/local/log`

4. 輸入與稽核共用區相對應的編號： *`audit_share_number`*

   隨即顯示允許存取稽核共用區的IP位址編號清單。

5. 輸入對應於您要移除之IP位址的號碼。

   稽核共用區將會更新、且不再允許任何具有此IP位址的稽核用戶端進行存取。

6. 出現提示時、請按* Enter *。

   隨即顯示NFS組態公用程式。

7. 關閉NFS組態公用程式： `exit`
8. 如果StorageGRID 您的不支援部署是多個資料中心站台部署、而其他站台則有額外的管理節點、請視需要停用這些稽核共用：
   a. 遠端登入每個站台的管理節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入中所列的密碼 `Passwords.txt` 檔案：
      iii. 輸入下列命令以切換至root： `su -`
      iv. 輸入中所列的密碼 `Passwords.txt` 檔案：
   b. 重複這些步驟、為每個額外的管理節點設定稽核共用。
   c. 關閉遠端安全Shell登入遠端管理節點： `exit`
9. 登出命令Shell： `exit`

變更**NFS**稽核用戶端的**IP**位址

如果您需要變更NFS稽核用戶端的IP位址、請完成下列步驟。

步驟

1. 將新的IP位址新增至現有的NFS稽核共用區。

2. 移除原始IP位址。

相關資訊

- "將NFS稽核用戶端新增至稽核共用區"
- "從稽核共用區移除NFS稽核用戶端"

管理歸檔節點

透過**S3 API**歸檔至雲端

您可以將歸檔節點設定為直接連線至Amazon Web Services（AWS）或任何其他可StorageGRID 透過S3 API連接至BIOS系統的系統。

> 對歸檔節點的支援已過時、將於未來版本中移除。透過S3 API將物件從歸檔節點移至外部歸檔儲存系統、已由ILM Cloud Storage Pool取代、提供更多功能。
>
> Cloud Tiering - Simple Storage Service （ S3 ）選項也已過時。如果您目前正在使用具有此選項的歸檔節點、 "將物件移轉至雲端儲存池" 而是。
>
> 此外、您應該從 StorageGRID 11.7 或更早版本的主動式 ILM 原則中移除歸檔節點。移除儲存在保存節點上的物件資料、可簡化未來的升級作業。請參閱 "使用ILM規則和ILM原則"。

設定**S3 API**的連線設定

如果您使用S3介面連線至歸檔節點、則必須設定S3 API的連線設定。在設定這些設定之前、由於無法與外部歸檔儲存系統通訊、因此ARC服務會維持在主要警示狀態。

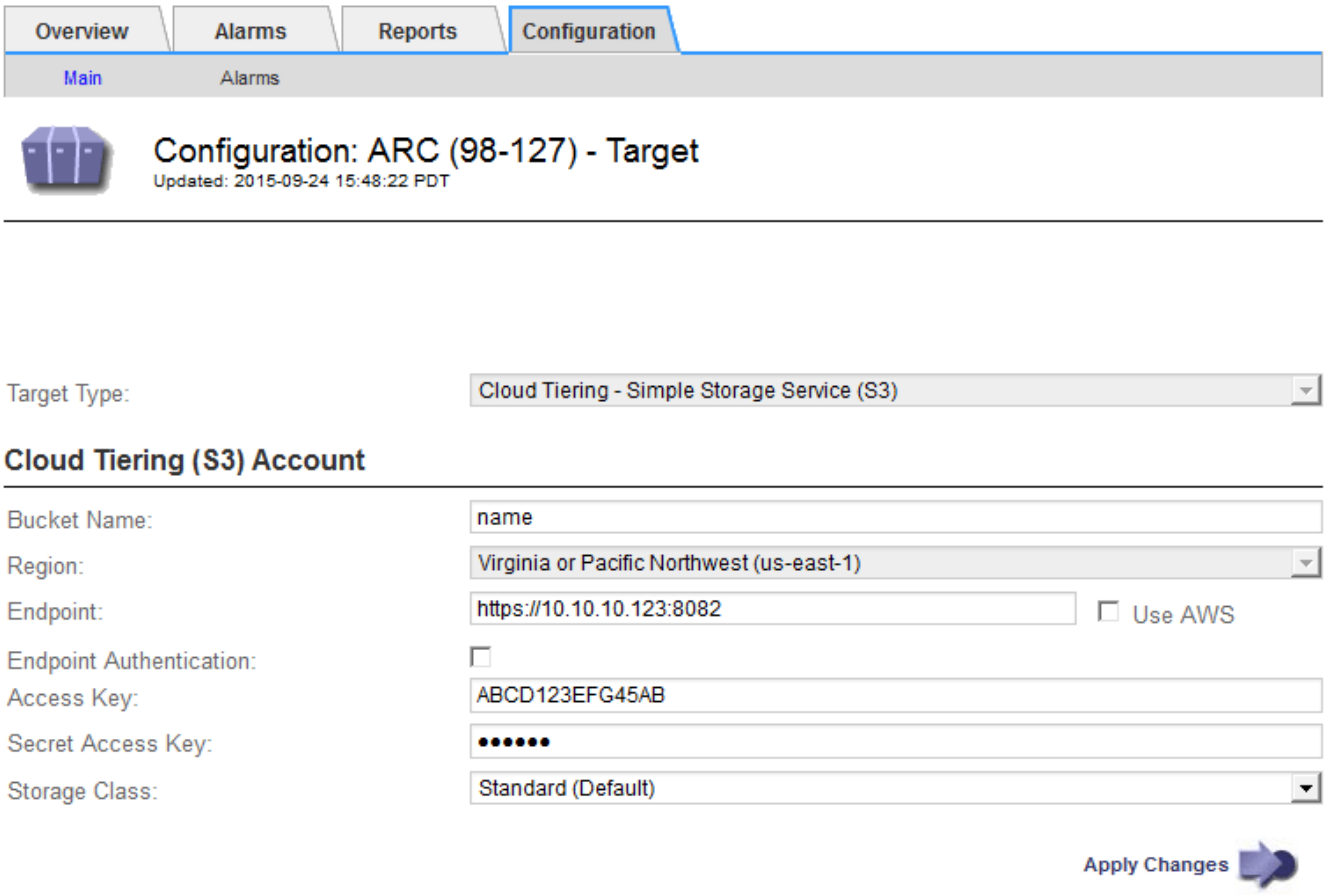
> 對歸檔節點的支援已過時、將於未來版本中移除。透過S3 API將物件從歸檔節點移至外部歸檔儲存系統、已由ILM Cloud Storage Pool取代、提供更多功能。
>
> Cloud Tiering - Simple Storage Service （ S3 ）選項也已過時。如果您目前正在使用具有此選項的歸檔節點、 "將物件移轉至雲端儲存池" 而是。
>
> 此外、您應該從 StorageGRID 11.7 或更早版本的主動式 ILM 原則中移除歸檔節點。移除儲存在保存節點上的物件資料、可簡化未來的升級作業。請參閱 "使用ILM規則和ILM原則"。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已在目標歸檔儲存系統上建立儲存貯體：
  - 此儲存庫專用於單一歸檔節點。其他歸檔節點或其他應用程式無法使用此功能。
  - 此庫位會針對您所在的位置選擇適當的區域。
  - 此儲存區應設定為暫停版本管理。
- 「物件區隔」已啟用、且「最大區段大小」小於或等於4.5 GiB（4、831838、208位元組）。如果使用S3做為外部歸檔儲存系統、超過此值的S3 API要求將會失敗。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇*歸檔節點*>* ARC/>*目標*。
3. 選擇*組態*>*主要*。



4. 從目標類型下拉式清單中選取*雲端分層-簡易儲存服務（S3）*。

   除非您選取目標類型、否則組態設定將無法使用。

5. 設定雲端分層（S3）帳戶、以便歸檔節點透過該帳戶連線至目標外部S3相容的歸檔儲存系統。

   此頁面上的大部分欄位都是不言自明的。以下說明您可能需要指引的欄位。

   - 地區：僅在選擇*使用AWS*時可用。您選取的區域必須符合儲存區的區域。
   - 端點*和*使用**AWS**：對於Amazon Web Services（AWS）、請選取*使用AWS*。*端點*會根據「庫位名稱」和「區域」屬性、自動填入端點URL。例如：

     ```
     https://bucket.region.amazonaws.com
     ```

     對於非AWS目標、請輸入裝載儲存區之系統的URL、包括連接埠號碼。例如：

```
https://system.com:1080
```

   - 端點驗證：預設為啟用。如果外部歸檔儲存系統的網路受到信任、您可以清除核取方塊、以停用目標外

部歸檔儲存系統的端點 SSL 憑證和主機名稱驗證。如果 StorageGRID 系統的另一個執行個體是目標歸檔儲存裝置、且系統已設定為公開簽署的憑證、您可以保持核取方塊的選取狀態。

- 儲存類別：選取*標準（預設）作為一般儲存設備。僅針對可輕鬆重新建立的物件、選取*減少備援。*減少備援*可降低儲存成本、降低可靠性。如果目標歸檔儲存系統是StorageGRID 另一個支援此功能的執行個體、則*儲存類別*會控制在目標系統上擷取時、物件的臨時複本數量、如果在目標系統上擷取物件時使用雙重提交。

6. 選取*套用變更*。

   指定的組態設定會經過驗證、並套用至StorageGRID 您的系統。套用設定之後、就無法變更目標。

修改**S3 API**的連線設定

將歸檔節點設定為透過S3 API連線至外部歸檔儲存系統之後、您可以在連線變更時修改部分設定。

開始之前

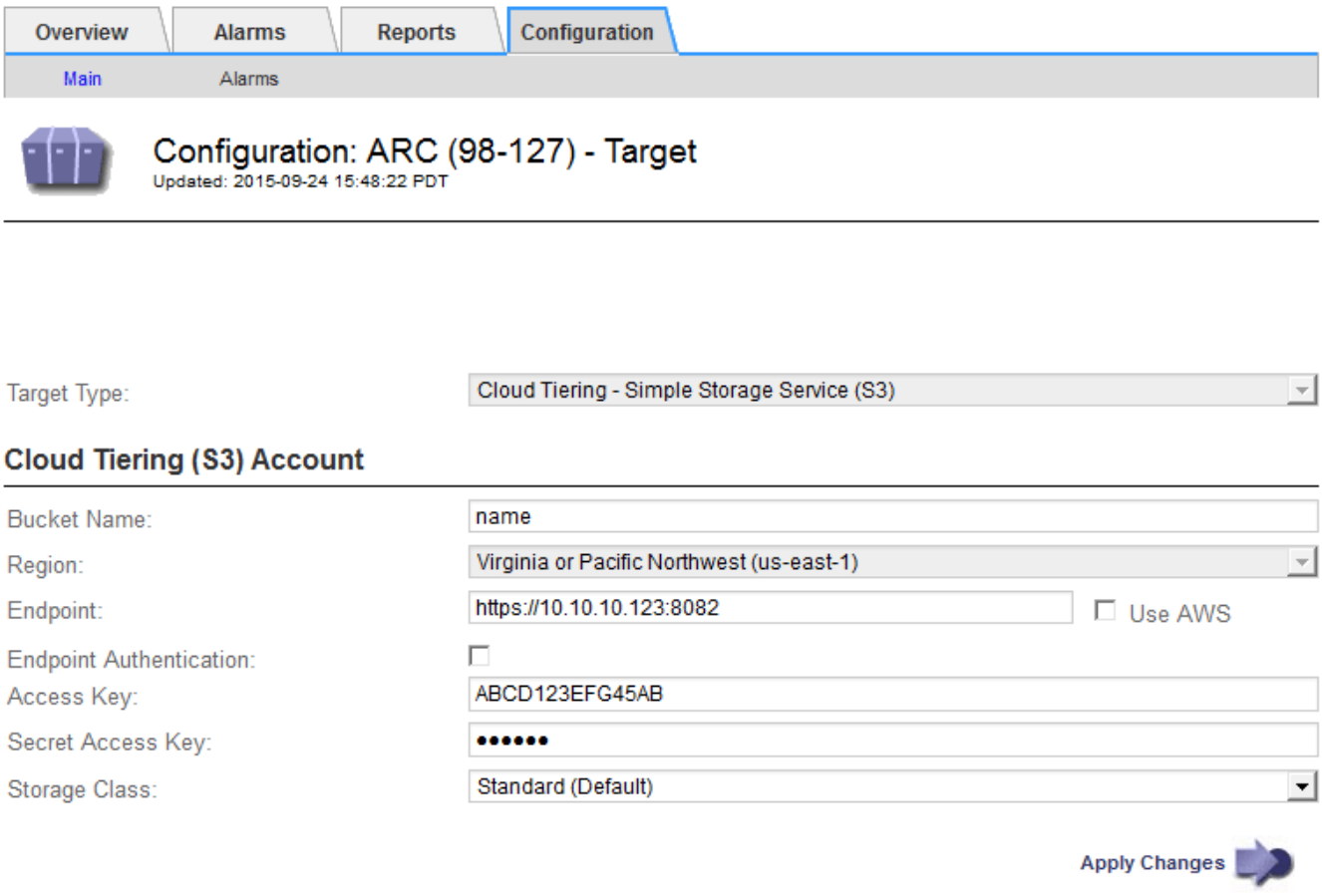
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。

關於這項工作

如果您變更Cloud Tiering（S3）帳戶、則必須確保使用者存取認證具有儲存區的讀取/寫入存取權、包括歸檔節點先前擷取至儲存區的所有物件。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*目標*」。
3. 選擇*組態*>*主要*。



4. 視需要修改帳戶資訊。

   如果您變更儲存類別、新的物件資料會與新的儲存類別一起儲存。擷取時、現有物件會繼續儲存在儲存類別集的下方。

   貯體名稱、區域和端點、使用 AWS 值、無法變更。

5. 選取*套用變更*。

修改雲端分層服務狀態

您可以變更Cloud Tiering Service的狀態、藉此控制歸檔節點讀取和寫入至透過S3 API連線的目標外部歸檔儲存系統的能力。

開始之前

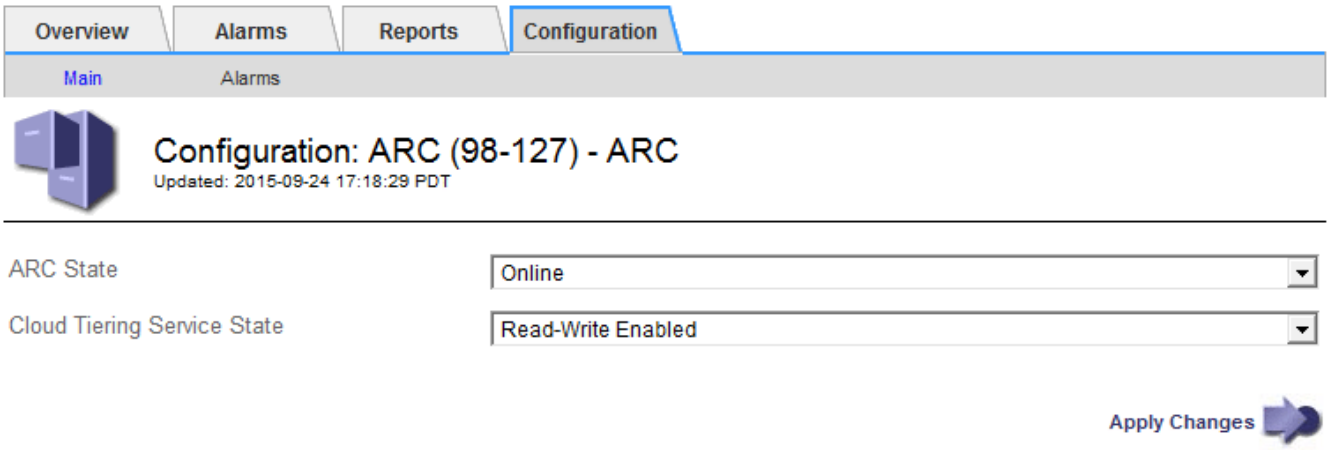
- 您必須使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 必須設定歸檔節點。

關於這項工作

您可以將雲端分層服務狀態變更為*已停用讀寫*、有效地使歸檔節點離線。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*」。
3. 選擇*組態*>*主要*。



4. 選取*雲端分層服務狀態*。
5. 選取*套用變更*。

重設**S3 API**連線的儲存失敗計數

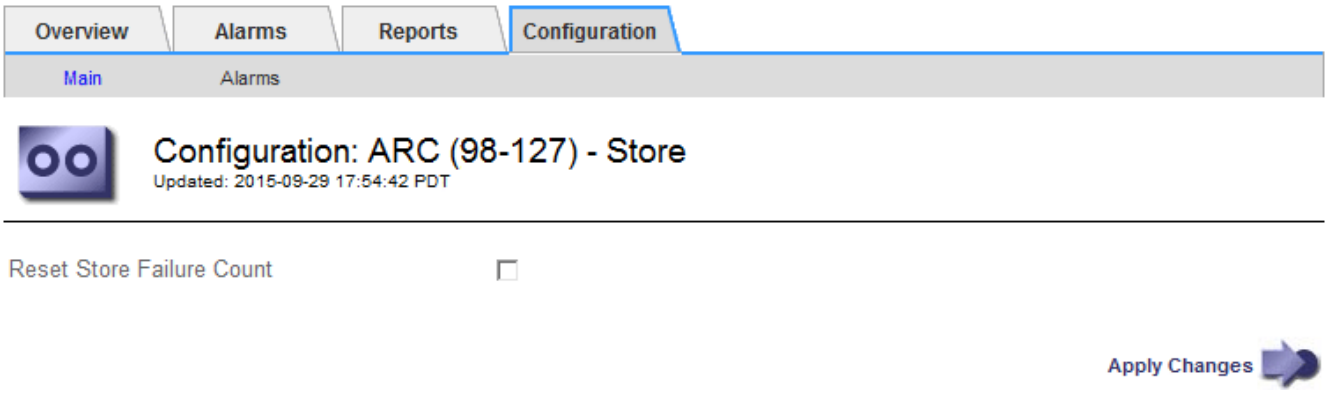
如果您的歸檔節點透過S3 API連線至歸檔儲存系統、您可以重設儲存失敗計數、以清除ARVf（儲存故障）警示。

開始之前

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

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*儲存*」。
3. 選擇*組態*>*主要*。



4. 選取*重設儲存失敗計數*。

5. 選取*套用變更*。

   Store Failures屬性會重設為零。

將物件從雲端分層- **S3**移轉至雲端儲存資源池

如果您目前正在使用 * 雲端分層 - 簡易儲存服務（ S3 ） * 功能、將物件資料分層至 S3 儲存區、則應改將物件移轉至雲端儲存池。Cloud Storage Pool提供可擴充的方法、可充分利用StorageGRID 您的整個系統中的所有儲存節點。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已將物件儲存在S3儲存區中、並已設定用於雲端分層。

> 在移轉物件資料之前、請聯絡您的NetApp客戶代表、以瞭解及管理任何相關成本。

關於這項工作

從ILM觀點來看、雲端儲存資源池類似於儲存資源池。然而、雖然儲存資源池由StorageGRID 儲存節點或位於VMware系統內的歸檔節點組成、但雲端儲存資源池則是由外部S3儲存區所組成。

在將物件從Cloud Tiering（S3）移轉至Cloud Storage Pool之前、您必須先建立S3儲存區、然後再StorageGRID 在其中建立Cloud Storage Pool。然後、您可以建立新的ILM原則、並以複製的ILM規則取代用來將物件儲存在雲端分層儲存區的ILM規則、該規則會將相同的物件儲存在雲端儲存資源池中。

> 當物件儲存在雲端儲存池中時、這些物件的複本也無法儲存在 StorageGRID 中。如果您目前用於雲端分層的ILM規則已設定為同時將物件儲存在多個位置、請考慮是否仍要執行此選擇性移轉、因為您將會失去該功能。如果您繼續進行此移轉、則必須建立新規則、而非複製現有規則。

步驟

1. 建立雲端儲存資源池。

   使用適用於雲端儲存資源池的新S3儲存區、確保只包含由雲端儲存資源池管理的資料。

2. 在主動式 ILM 原則中找出任何導致物件儲存在 Cloud Tiering 儲存區的 ILM 規則。
3. 複製這些規則。
4. 在複製的規則中、將放置位置變更為新的Cloud Storage Pool。
5. 儲存複製的規則。
6. 建立使用新規則的新原則。
7. 模擬並啟動新原則。

   當新原則啟動且進行ILM評估時、物件會從設定為雲端分層的S3儲存區移至為雲端儲存資源池設定的S3儲存區。網格上的可用空間不受影響。物件移至雲端儲存資源池之後、就會從雲端分層儲存區中移除。

相關資訊

"使用ILM管理物件"

透過**TSM**中介軟體歸檔至磁帶

您可以將歸檔節點設定為目標Tivoli Storage Manager（TSM）伺服器、該伺服器提供邏輯介面、可將物件資料儲存及擷取至隨機或連續存取儲存設備、包括磁帶庫。

歸檔節點的ARC服務可做為TSM伺服器的用戶端、使用Tivoli Storage Manager作為中介軟體、與歸檔儲存系統進行通訊。

> 對歸檔節點的支援已過時、將於未來版本中移除。透過S3 API將物件從歸檔節點移至外部歸檔儲存系統、已由ILM Cloud Storage Pool取代、提供更多功能。
>
> Cloud Tiering - Simple Storage Service （ S3 ）選項也已過時。如果您目前正在使用具有此選項的歸檔節點、 "將物件移轉至雲端儲存池" 而是。
>
> 此外、您應該從 StorageGRID 11.7 或更早版本的主動式 ILM 原則中移除歸檔節點。移除儲存在保存節點上的物件資料、可簡化未來的升級作業。請參閱 "使用ILM規則和ILM原則"。

TSM管理類別

由TSM中介軟體定義的管理類別、概述了TSMS廳 的備份與歸檔作業如何運作、並可用來指定TSM伺服器所套用內容的規則。此類規則獨立於StorageGRID 此等系統的ILM原則運作、且必須符合StorageGRID 此等系統的要求、即物件必須永久儲存、且永遠可供歸檔節點擷取。在歸檔節點將物件資料傳送至TSM伺服器之後、會套用TSM生命週期和保留規則、同時將物件資料儲存至由TSM伺服器管理的磁帶。

TSM管理類別是由TSM伺服器在歸檔節點將物件傳送至TSM伺服器之後、用來套用資料位置或保留的規則。例如、識別為資料庫備份的物件（可以較新資料覆寫的暫用內容）、處理方式可能與應用程式資料不同（必須無限期保留的固定內容）。

設定與**TSM**中介軟體的連線

在 Archive Node 能夠與 Tivoli Storage Manager （ TSM ）中介軟體通訊之前、您必須先設定數項設定。

開始之前

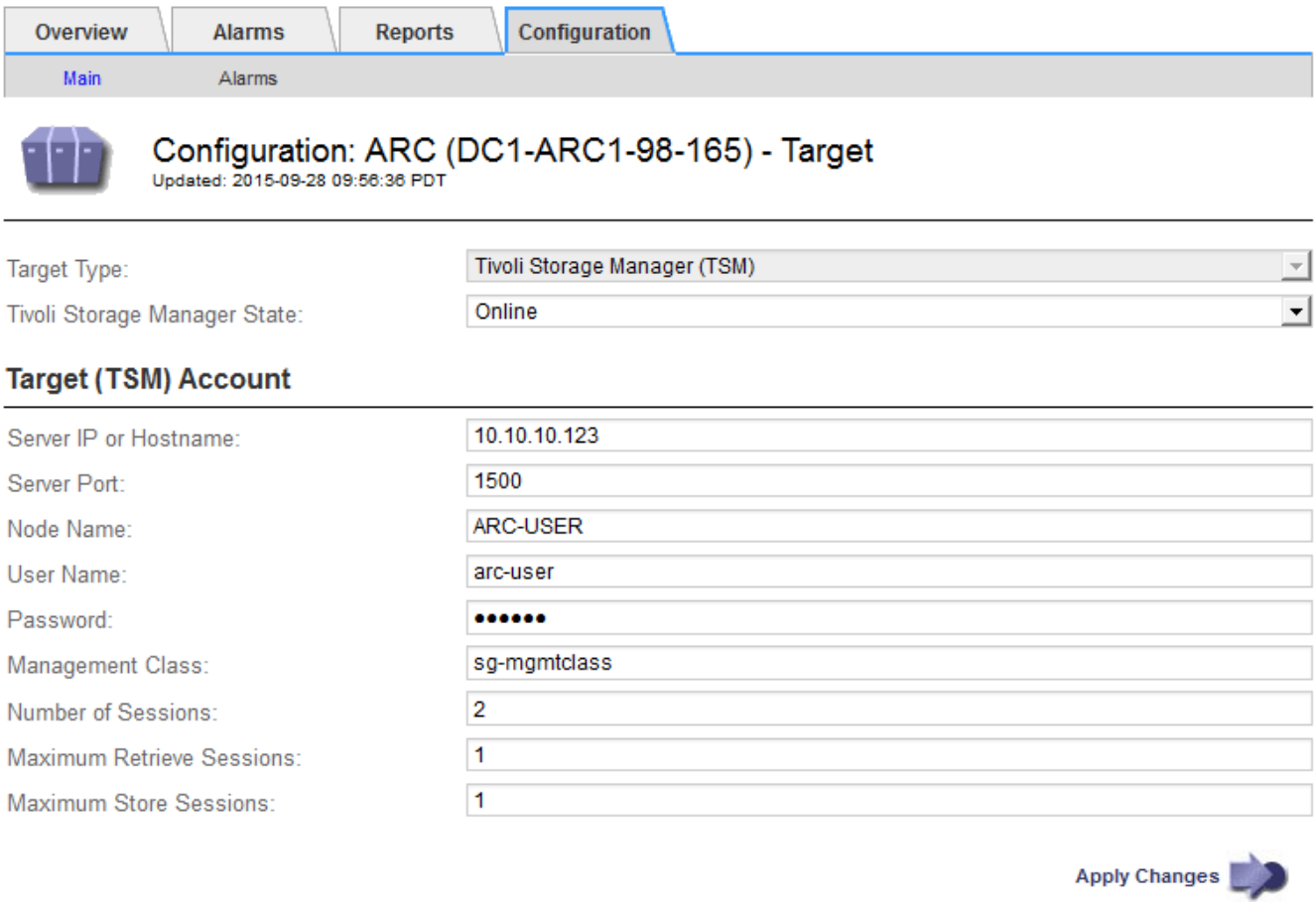
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。

關於這項工作

在設定這些設定之前、由於無法與Tivoli Storage Manager通訊、因此ARC服務會維持在主要警示狀態。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*目標*」。
3. 選擇*組態*>*主要*。



4. 從*目標類型*下拉式清單中、選取* Tivoli Storage Manager（TSM）*。
5. 若為* Tivoli Storage Manager State*、請選取*離線*以防止從TSM中介軟體伺服器擷取資料。

   根據預設、Tivoli Storage Manager狀態設為「線上」、表示歸檔節點能夠從TSM中介軟體伺服器擷取物件資料。

6. 請填寫下列資訊：

   - 伺服器**IP**或主機名稱：指定用於ARC服務的TSM中介軟體伺服器IP位址或完整網域名稱。預設IP位址為127.0.0.1。
   - 伺服器連接埠：在TSM中介軟體伺服器上指定連接埠號碼、以便讓ARC服務連線至該伺服器。預設值為1500 。
   - 節點名稱：指定歸檔節點的名稱。您必須輸入您在TSM中介軟體伺服器上註冊的名稱（旋轉式使用者） 。
   - 使用者名稱：指定使用者名稱、以便讓ARC服務用來登入TSM伺服器。輸入您為歸檔節點指定的預設使用者名稱（ar任何 使用者）或管理使用者。
   - 密碼：指定ARC服務用來登入TSM伺服器的密碼。
   - 管理類：指定在將對象保存到StorageGRID 該系統時未指定管理類時使用的默認管理類，或未在TSM中間件服務器上定義指定的管理類時使用的管理類。
   - 工作階段數：指定TSM中介軟體伺服器上專用於歸檔節點的磁帶機數量。歸檔節點可同時建立每個掛載點最多一個工作階段、外加少量額外工作階段（少於五個）。

     當歸檔節點登錄或更新時、您必須將此值變更為與MAXNUMMP（掛載點的最大數目）的設定值相同。

（在登錄命令中、如果未設定任何值、則使用的MAXNUMMP預設值為1。）

您也必須將TSM伺服器的MAXSESSIONS值變更為至少與設定用於該ARC服務的工作階段數目一樣大的數字。TSM伺服器上MAXSESSIONS的預設值為25。

- 最大擷取工作階段數：指定ARC服務可開啟至TSM中介軟體伺服器以進行擷取作業的工作階段數上限。在大多數情況下、適當的值是「工作階段數」減去「最大儲存工作階段數」。如果您需要共用一個磁帶機以供儲存和擷取、請指定一個值、此值等於工作階段數。
- 最大儲存工作階段數：指定可開啟至TSM中介軟體伺服器進行歸檔作業的同時工作階段數上限。

  除非目標歸檔儲存系統已滿、而且只能執行擷取、否則此值應設為一個。將此值設為零、以使用所有工作階段進行擷取。

7. 選取*套用變更*。

針對**TSM**中介軟體工作階段最佳化歸檔節點

您可以設定歸檔節點的工作階段、將連接到Tivoli Server Manager（TSM）的歸檔節點效能最佳化。

開始之前

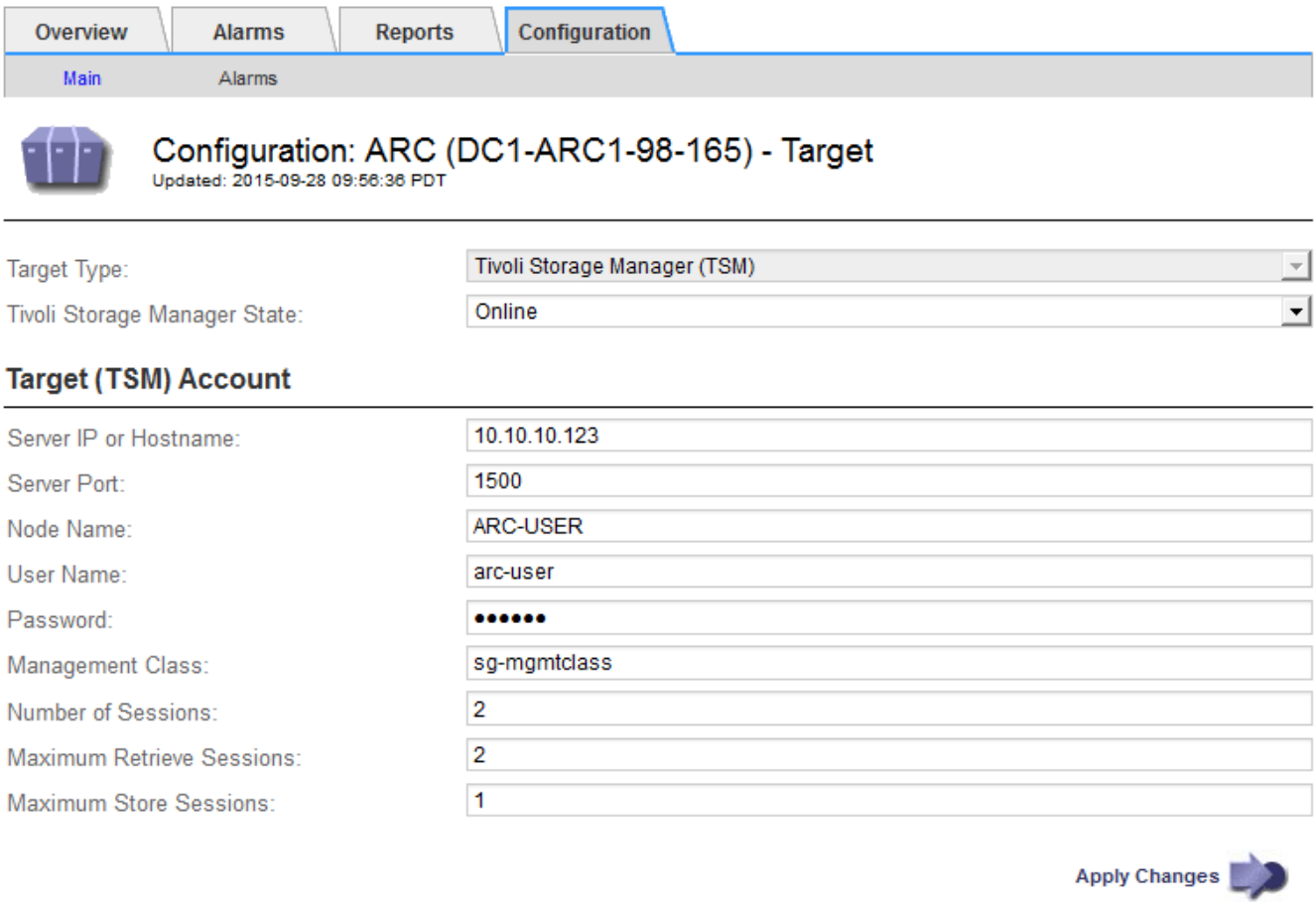
- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。

關於這項工作

歸檔節點開放給TSM中介軟體伺服器的並行工作階段數目、通常會設定為TSM伺服器專用於歸檔節點的磁帶機數目。其中一個磁帶機分配給儲存設備、其餘則分配給擷取。不過、在從歸檔節點複本重建儲存節點、或歸檔節點以唯讀模式運作的情況下、您可以將擷取工作階段的最大數量設定為與並行工作階段數相同、以最佳化TSM伺服器效能。因此、所有磁碟機都可同時用於擷取、而且如果適用、最多也可將其中一個磁碟機用於儲存設備。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*目標*」。
3. 選擇*組態*>*主要*。
4. 將*最大擷取工作階段*變更為*工作階段數*。



5. 選取*套用變更*。

設定**TSM**的歸檔狀態和計數器

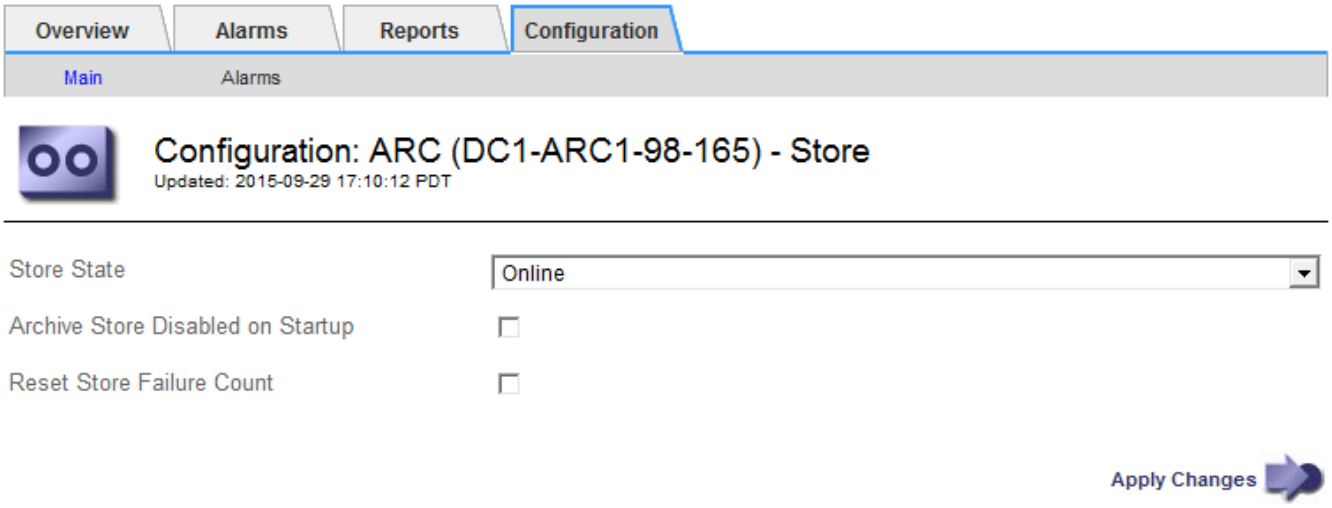
如果您的歸檔節點連線至TSM中介軟體伺服器、您可以將歸檔節點的歸檔儲存區狀態設定為「線上」或「離線」。您也可以在歸檔節點首次啟動時停用歸檔儲存區、或是重設追蹤相關警示的故障數。

開始之前

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

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*儲存*」。
3. 選擇*組態*>*主要*。



4. 視需要修改下列設定：
   - 儲存狀態：將元件狀態設為：
     - 線上：「歸檔節點」可用於處理儲存至歸檔儲存系統的物件資料。
     - 離線：歸檔節點無法處理儲存至歸檔儲存系統的物件資料。
   - 啟動時停用歸檔存放區：選取此選項時、重新啟動時歸檔存放區元件會保持唯讀狀態。用於持續停用目標歸檔儲存系統的儲存設備。當目標歸檔儲存系統無法接受內容時、此功能非常實用。
   - 重設零售店失敗計數：針對零售店故障重設計數器。這可用來清除ARVf（儲存故障）警示。
5. 選取*套用變更*。

相關資訊

"當TSM伺服器達到容量時、管理歸檔節點"

當**TSM**伺服器達到容量時、管理歸檔節點

TSM伺服器無法在TSM資料庫或TSM伺服器管理的歸檔媒體儲存設備即將達到容量時通知歸檔節點。這種情況可透過主動監控TSM伺服器來避免。

開始之前

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

關於這項工作

在TSM伺服器停止接受新內容之後、歸檔節點會繼續接受物件資料以傳輸至TSM伺服器。此內容無法寫入由TSM 伺服器管理的媒體。如果發生這種情況、就會觸發警示。

防止**ARC**服務傳送內容至**TSM**伺服器

若要防止ARC服務傳送更多內容到TSM伺服器、您可以將歸檔節點離線、方法是將其* ARC/>* Store*元件離線。當TSM伺服器無法進行維護時、此程序也有助於防止警示。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。

2. 選擇「歸檔節點_>* ARC*>*儲存*」。
3. 選擇*組態*>*主要*。

4. 將*儲存狀態*變更為 `Offline`。
5. 選擇*在啟動時停用歸檔儲存區*。
6. 選取*套用變更*。

如果**TSM**中介軟體達到容量、請將歸檔節點設為唯讀

如果目標TSM中介軟體伺服器達到容量、則歸檔節點可最佳化、僅執行擷取。

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>*目標*」。
3. 選擇*組態*>*主要*。
4. 將擷取工作階段上限變更為與工作階段數目中所列的並行工作階段數目相同。
5. 將「最大儲存區工作階段數」變更為0。

> 如果歸檔節點為唯讀、則不需要將最大儲存工作階段變更為0。不會建立零售店工作階段。

6. 選取*套用變更*。

設定歸檔節點擷取設定

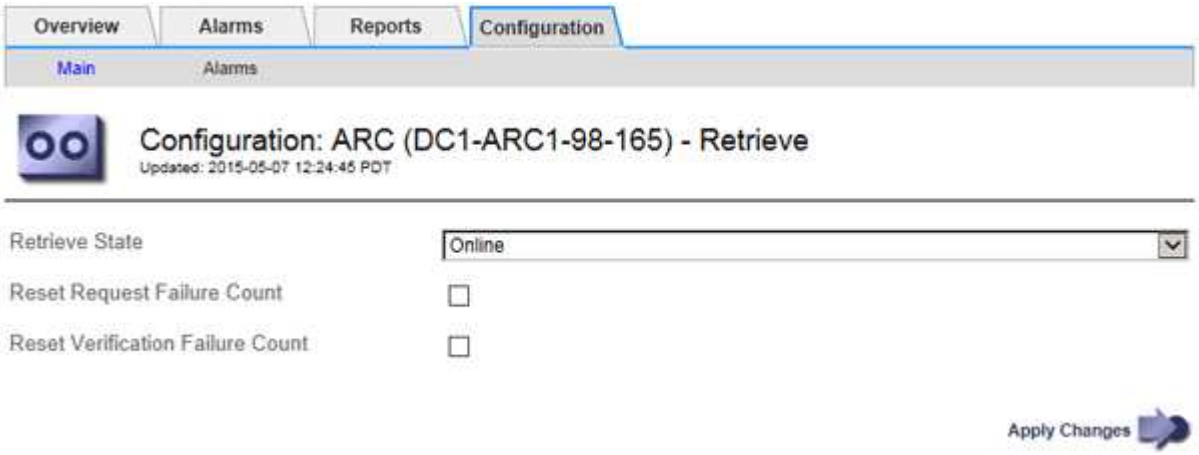
您可以設定歸檔節點的擷取設定、將狀態設定為「線上」或「離線」、或重設要追蹤相關警示的故障計數。

開始之前

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

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇*歸檔節點*>* ARC/>*擷取*。
3. 選擇*組態*>*主要*。



4. 視需要修改下列設定：
   - 擷取狀態：將元件狀態設為：
     - 線上：網格節點可從歸檔媒體裝置擷取物件資料。
     - 離線：網格節點無法擷取物件資料。
   - 重設要求失敗計數：勾選核取方塊以重設要求失敗的計數器。這可用來清除ARRF（要求失敗）警示。
   - 重設驗證失敗計數：勾選核取方塊以重設計數器、以針對擷取的物件資料進行驗證失敗。這可用來清除AR休 旅車（驗證失敗）警報。
5. 選取*套用變更*。

設定歸檔節點複寫

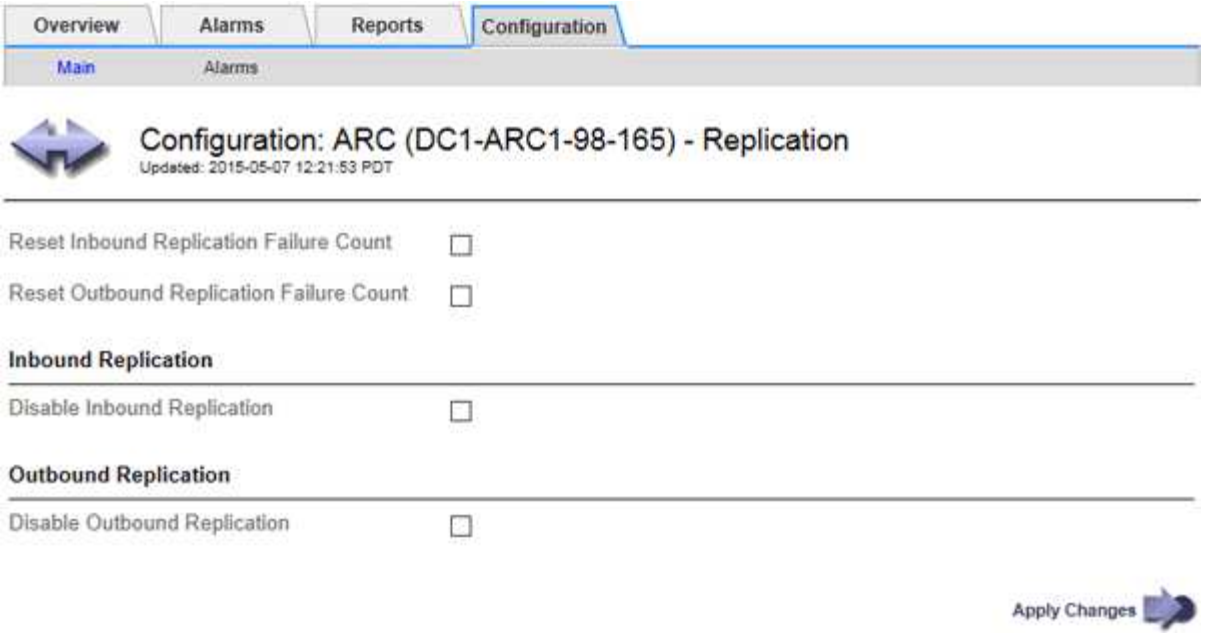
您可以設定歸檔節點的複寫設定、停用傳入和傳出複寫、或是重設追蹤相關警示的失敗計數。

開始之前

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

步驟

1. 選取*支援*>*工具*>*網格拓撲*。
2. 選擇「歸檔節點_>* ARC*>* Replication （*複寫）」。
3. 選擇*組態*>*主要*。



4. 視需要修改下列設定：
   - 重設傳入複寫失敗計數：選取此選項可重設傳入複寫失敗的計數器。這可用來清除RIRF（傳入複製-失敗）警示。
   - 重設傳出複寫失敗計數：選取此選項可重設傳出複寫失敗的計數器。這可用來清除RORF（傳出複製-失敗）警示。
   - 停用傳入複寫：選取以停用傳入複寫、作為維護或測試程序的一部分。正常操作期間保持清除狀態。

     停用傳入複寫時、可從 ARC 服務擷取物件資料、以複寫至 StorageGRID 系統中的其他位置、但無法從其他系統位置將物件複寫至此 ARC 服務。ARC服務為唯讀。
   - * 停用外傳複寫 * ：勾選核取方塊以停用外傳複寫（包括 HTTP 擷取的內容要求）、作為維護或測試程序的一部分。在正常操作期間保持未核取狀態。

     停用輸出複寫時、可以將物件資料複製到此 ARC 服務以符合 ILM 規則、但無法從 ARC 服務擷取物件資料、將其複製到 StorageGRID 系統的其他位置。ARC服務是純寫入的。
5. 選取*套用變更*。

設定歸檔節點的自訂警示

您應針對ARQL和ARRL屬性建立自訂警示、以監控歸檔節點從歸檔儲存系統擷取物件資料的速度和效率。

- ARQL：平均佇列長度。物件資料從歸檔儲存系統中佇列以供擷取的平均時間（以微秒為單位）。
- ARRL：平均要求延遲。歸檔節點從歸檔儲存系統擷取物件資料所需的平均時間（以微秒為單位）。

這些屬性的可接受值取決於歸檔儲存系統的設定與使用方式。（請前往* ARC/>* Retrieve > Overview > Main*。） 針對要求逾時所設定的值、以及可用於擷取要求的工作階段數量、尤其具有影響力。

整合完成後、請監控歸檔節點的物件資料擷取、以建立正常擷取時間和佇列長度的值。然後、針對ARQL和ARRL建立自訂警示、以便在發生異常作業情況時觸發。請參閱的說明 "管理警示（舊系統）"。

整合Tivoli Storage Manager

歸檔節點組態與作業

您的系統可將歸檔節點管理為永久儲存物件且隨時可供存取的位置。StorageGRID

擷取物件時、會根據為 StorageGRID 系統定義的資訊生命週期管理（ ILM ）規則、將複本複製到所有必要位置、包括歸檔節點。歸檔節點可做為TSM伺服器的用戶端、而TSM用戶端程式庫則是StorageGRID 透過安裝此軟體的程序安裝在歸檔節點上。導向至歸檔節點以供儲存的物件資料會在收到時直接儲存至TSM伺服器。歸檔節點在將物件資料儲存至TSM伺服器之前、不會將其登入、也不會執行物件集合體。不過、如果資料傳輸率有保證、歸檔節點可以在單一交易中、將多個複本提交給TSM伺服器。

歸檔節點將物件資料儲存至TSM伺服器之後、物件資料會由TSM伺服器使用其生命週期/保留原則來管理。必須定義這些保留原則、才能與歸檔節點的作業相容。也就是、歸檔節點儲存的物件資料必須無限期儲存、而且歸檔節點必須隨時都能存取、除非歸檔節點將其刪除。

在不影響StorageGRID 整個系統的ILM規則與TSM伺服器的生命週期/保留原則之間沒有任何關聯。每個物件彼此獨立運作、但當每個物件被擷取到StorageGRID 這個系統時、您可以指派一個TSM管理類別給它。此管理類別會連同物件資料一起傳遞給TSM伺服器。將不同的管理類別指派給不同的物件類型、可讓您設定TSM伺服器、將物件資料放在不同的儲存資源池中、或視需要套用不同的移轉或保留原則。例如、識別為資料庫備份的物件（暫存內容無法以較新的資料覆寫）處理方式可能與應用程式資料（必須無限期保留的固定內容）不同。

歸檔節點可與新的或現有的TSM伺服器整合、不需要專用的TSM伺服器。TSM伺服器可與其他用戶端共用、前提是TSM伺服器的大小必須符合預期的最大負載。TSM必須安裝在與歸檔節點不同的伺服器或虛擬機器上。

您可以將多個歸檔節點設定為寫入同一個TSM伺服器、但只有在歸檔節點將不同的資料集寫入TSM伺服器時、才建議使用此組態。當每個歸檔節點將相同物件資料的複本寫入歸檔時、不建議將多個歸檔節點設定為寫入相同的TSM伺服器。在後一種情況下、這兩個複本都會受到單點故障（TSM伺服器）的影響、因為這兩個複本應該是獨立的物件資料備援複本。

歸檔節點不會使用 TSM 的階層式儲存管理（ HSM ）元件。

組態最佳實務做法

當您調整和設定TSM伺服器時、您應該套用最佳實務做法、將其最佳化以搭配歸檔節點使用。

在調整和設定TSM伺服器規模時、您應該考慮下列因素：

- 由於歸檔節點在將物件儲存至TSM伺服器之前不會集合物件、因此必須調整TSM資料庫的大小、以保留所有要寫入歸檔節點的物件參考資料。
- 歸檔節點軟體無法容忍將物件直接寫入磁帶或其他卸除式媒體所需的延遲。因此、TSM伺服器必須設定磁碟儲存池、以便在使用卸除式媒體時、用於歸檔節點所儲存的資料初始儲存。
- 您必須設定TSM保留原則、才能使用事件型保留。歸檔節點不支援建立型TSM保留原則。請使用保留原則中的Retmin=0和retver=0（表示保留會在歸檔節點觸發保留事件時開始、保留時間會在該事件之後保留0天）建議設定。不過、重複時間和重複時間的值是選用的。

磁碟集區必須設定為將資料移轉至磁帶集區（也就是磁帶集區必須是磁碟集區的NXTSTGPOOL）。磁帶集區不得設定為磁碟集區的複本集區、同時寫入兩個集區（也就是說、磁帶集區不可為磁碟集區的 COPYSTGPOOL ）。若要建立含有歸檔節點資料的磁帶離線複本、請將TSM伺服器設定為第二個磁帶集區、該磁帶集區是用於歸檔節點資料的磁帶集區複本集區。

完成歸檔節點設定

完成安裝程序後、歸檔節點無法正常運作。在將物件儲存至TSM歸檔節點之前StorageGRID 、您必須完成TSM伺服器的安裝與組態、並設定歸檔節點與TSM伺服器進行通訊。

當您準備TSM伺服器以整合StorageGRID 到整個作業系統的歸檔節點時、請視需要參閱下列IBM文件：

- "IBM磁帶設備驅動程式安裝與使用指南"
- "IBM磁帶設備驅動程式程式設計參考"

安裝新的**TSM**伺服器

您可以將歸檔節點與新的或現有的TSM伺服器整合。如果您要安裝新的TSM伺服器、請依照TSM文件中的指示完成安裝。

歸檔節點無法與 TSM 伺服器共同代管。

設定**TSM**伺服器

本節包括依照 TSM 最佳實務準備 TSM 伺服器的範例指示。

下列指示將引導您完成下列程序：

- 定義TSM伺服器上的磁碟儲存資源池和磁帶儲存資源池（如有需要）
- 針對從歸檔節點儲存的資料、定義使用TSM管理類別的網域原則、並登錄節點以使用此網域原則

這些指示僅供您參考、並不適用於取代 TSM 文件、或是提供適用於所有組態的完整完整完整說明。部署特定指示應由TSM管理員提供、他熟悉您的詳細需求、以及完整的TSM伺服器文件集。

定義**TSM**磁帶與磁碟儲存資源池

歸檔節點會寫入磁碟儲存池。若要將內容歸檔至磁帶、您必須設定磁碟儲存資源池、將內容移至磁帶儲存資源池。

關於這項工作

對於TSM伺服器、您必須在Tivoli Storage Manager中定義磁帶儲存資源池和磁碟儲存資源池。定義磁碟集區之後、請建立磁碟磁碟區並將其指派給磁碟集區。如果TSM伺服器使用純磁碟儲存設備、則不需要磁帶集區。

您必須先在 TSM 伺服器上完成數個步驟、才能建立磁帶儲存池。（在磁帶庫中建立磁帶庫和至少一個磁碟機。定義從伺服器到程式庫、從伺服器到磁碟機的路徑、然後定義磁碟機的裝置類別。） 這些步驟的詳細資料可能會因站台的硬體組態和儲存需求而有所不同。如需詳細資訊、請參閱TSM文件。

下列一組指示說明此程序。您應該注意、站台的需求可能會因部署需求而異。如需組態詳細資料和說明、請參閱TSM文件。

您必須以管理權限登入伺服器、並使用 dsmadmc 工具執行下列命令。

步驟

1. 建立磁帶庫。

   ```
   define library tapelibrary libtype=scsi
   ```

   其中 *tapelibrary* 是為磁帶庫選擇的任意名稱、以及的值 `libtype` 視磁帶庫類型而定。

2. 定義從伺服器到磁帶庫的路徑。

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* 是TSM伺服器的名稱
   - *tapelibrary* 是您定義的磁帶庫名稱
   - *lib-devicename* 為磁帶庫的裝置名稱

3. 定義程式庫的磁碟機。

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* 是您要指定給磁碟機的名稱
   - *tapelibrary* 是您定義的磁帶庫名稱

     視硬體組態而定、您可能需要設定其他磁碟機。（例如、如果TSM伺服器連接至光纖通道交換器、且該交換器具有磁帶庫的兩個輸入、您可能會想要為每個輸入定義一個磁碟機。）

4. 定義從伺服器到所定義磁碟機的路徑。

   ```
   define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname
   ```

   - *drive-dname* 為磁碟機的裝置名稱
   - *tapelibrary* 是您定義的磁帶庫名稱

     針對您為磁帶庫定義的每個磁碟機、使用不同的磁碟機重複上述步驟 *drivename* 和 *drive-dname* 每個磁碟機。

5. 定義磁碟機的裝置類別。

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype
   ```

   - *DeviceClassName* 為裝置類別的名稱
   - *lto* 是連接至伺服器的磁碟機類型
   - *tapelibrary* 是您定義的磁帶庫名稱
   - *tapetype* 是磁帶類型、例如ultum3

6. 將磁帶磁碟區新增至磁帶庫的庫存。

   ```
   checkin libvolume tapelibrary
   ```

tapelibrary 是您定義的磁帶庫名稱。

7. 建立主要磁帶儲存資源池。

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* 為歸檔節點的磁帶儲存池名稱。您可以為磁帶儲存資源池選取任何名稱（只要名稱使用TSM伺服器所預期的語法慣例）。
   - *DeviceClassName* 為磁帶庫的裝置類別名稱。
   - *description* 是可在TSM伺服器上使用顯示之儲存資源池的說明 `query stgpool` 命令。例如：「保存節點的磁帶儲存池」。
   - *collocate=filespace* 指定TSM伺服器應將相同檔案空間的物件寫入單一磁帶。
   - XX 是下列其中一項：
     - 磁帶庫中的空白磁帶數（如果歸檔節點是唯一使用磁帶庫的應用程式）。
     - 分配給StorageGRID 由該系統使用的磁帶數量（在共享磁帶庫的情況下）。

8. 在TSM伺服器上、建立磁碟儲存資源池。在TSM伺服器的管理主控台輸入

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* 為歸檔節點磁碟集區的名稱。您可以為磁碟儲存資源池選取任何名稱（只要名稱使用TSM預期的語法慣例）。
   - *description* 是可在TSM伺服器上使用顯示之儲存資源池的說明 `query stgpool` 命令。例如、「歸檔節點的磁碟儲存池」。
   - *maximum_file_size* 強制將大於此大小的物件直接寫入磁帶、而非快取到磁碟集區。建議您設定 *maximum_file_size* 至10 GB。
   - *nextstgpool=SGWSTapePool* 將磁碟儲存資源池指向為歸檔節點定義的磁帶儲存資源池。
   - *percent_high* 設定磁碟集區開始將其內容移轉到磁帶集區的值。建議您設定 *percent_high* 至0、以便立即開始資料移轉
   - *percent_low* 設定移轉至磁帶集區的停止值。建議您設定 *percent_low* 至0以清除磁碟集區。

9. 在TSM伺服器上、建立磁碟磁碟區（或磁碟區）並將其指派給磁碟集區。

   ```
   define volume SGWSDiskPool volume_name formatsize=size
   ```

   - *SGWSDiskPool* 為磁碟集區名稱。
   - *volume_name* 是磁碟區位置的完整路徑（例如、 `/var/local/arc/stage6.dsm`）在TSM伺服器上寫入磁碟集區的內容、以準備傳輸至磁帶。
   - *size* 是磁碟區的大小（以MB為單位）。

     例如、若要建立單一磁碟區、使磁碟集區的內容填滿單一磁帶、請在磁帶磁碟區的容量為200 GB時、將大小值設為200000。

不過、可能需要建立大小較小的多個磁碟區、因為TSM伺服器可以寫入磁碟集區中的每個磁碟區。例如、如果磁帶大小為250 GB、請建立25個磁碟區、每個磁碟區大小為10 GB（10000）。

TSM伺服器會預先配置磁碟區目錄中的空間。這可能需要一段時間才能完成（200 GB磁碟區的時間超過三小時）。

定義網域原則並登錄節點

您需要針對從歸檔節點儲存的資料、定義使用TSM管理類別的網域原則、然後登錄節點以使用此網域原則。

如果Tivoli Storage Manager（TSM）中歸檔節點的用戶端密碼過期、歸檔節點程序可能會洩漏記憶體。請確定已設定TSM伺服器、使歸檔節點的用戶端使用者名稱/密碼永不過期。

在TSM伺服器上登錄節點以使用歸檔節點（或更新現有節點）時、您必須在登錄節點命令中指定MAXNUMMP參數、以指定節點可用於寫入作業的掛載點數目。掛載點的數量通常相當於分配給歸檔節點的磁帶機磁頭數量。TSM 伺服器上針對 MAXNUMMP 指定的數字必須至少與下列項目設定的值相同： * ARC* > * Target * > * Configuration* > * Main* > * Maximum Store SESSESSESS* for the Archive Node 、 此值設為 0 或 1 、因為歸檔節點不支援並行儲存區工作階段。

TSM伺服器的MAXSESSIONS設定值、可控制所有用戶端應用程式可開啟至TSM伺服器的工作階段數目上限。TSM上指定的MAXSESSIONS值必須至少大到在Grid Manager中為歸檔節點指定的* ARC/>* Target > Configuration > Main*>*工作階段數目*值。歸檔節點會同時建立每個掛載點最多一個工作階段、再加上少量（< 5）的額外工作階段。

指派給歸檔節點的TSM節點使用自訂網域原則 `tsm-domain`。。 `tsm-domain` 網域原則是「標準」網域原則的修改版本、設定為寫入磁帶、並將歸檔目的地設為 StorageGRID 系統的儲存集區 (*`SGWSDiskPool`*）。

您必須以系統管理權限登入TSM伺服器、然後使用dsmadmc工具來建立及啟動網域原則。

建立及啟動網域原則

您必須建立網域原則、然後啟動該原則、以設定TSM伺服器來儲存從歸檔節點傳送的資料。

步驟

1. 建立網域原則。

   ```
   copy domain standard tsm-domain
   ```

2. 如果您不使用現有的管理類別、請輸入下列其中一項：

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` 為部署的預設管理類別。

3. 建立複本群組至適當的儲存資源池。輸入（一行）：

```
define copygroup tsm-domain standard default type=archive
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

default 為歸檔節點的預設管理類別。的值 `retinit`、 `retmin`和 `retver` 已選擇以反映歸檔節點目前使用的保留行為

> 請勿設定 `retinit` 至 `retinit=create`。設定 `retinit=create` 因為保留事件用於從 TSM 伺服器移除內容、所以會阻止保存節點刪除內容。

4. 將管理類別指派為預設類別。

```
assign defmgmtclass tsm-domain standard default
```

5. 將新原則集設為作用中。

```
activate policyset tsm-domain standard
```

請忽略當您輸入 activate 命令時出現的「 no backup copy group （無備份複本群組）」警告。

6. 註冊節點以使用TSM伺服器上的新原則集。在TSM伺服器上、輸入（一行）：

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

ARC-使用者和ARC-密碼與您在歸檔節點上定義的用戶端節點名稱和密碼相同、MAXNUMMP的值設定為保留給歸檔節點儲存工作階段的磁帶機數量。

> 根據預設、登錄節點會建立用戶端擁有者授權的管理使用者ID、並為節點定義密碼。

將資料移轉StorageGRID 至功能不整合

您可以將大量資料移轉至StorageGRID 整個過程、同時使用StorageGRID 本系統進行日常作業。

規劃將大量資料移轉至 StorageGRID 系統時、請使用本指南。這不是資料移轉的一般指南、也不包含執行移轉的詳細步驟。請遵循本節中的準則和指示、確保資料能有效率地移轉到StorageGRID 運轉不中斷日常作業的情況下、StorageGRID 且已移轉的資料會由效能提升系統妥善處理。

確認StorageGRID 該系統的容量

在將大量資料移轉到StorageGRID 整個過程之前、請先確認StorageGRID 該系統具備處理預期磁碟區的磁碟容量。

如果 StorageGRID 系統包含歸檔節點、且已將移轉物件的複本儲存至近線儲存設備（例如磁帶）、請確保歸檔節點的儲存設備有足夠容量可容納預期的移轉資料量。

在容量評估中、請查看您計畫移轉之物件的資料設定檔、並計算所需的磁碟容量。如需監控StorageGRID 您的作業系統磁碟容量的詳細資訊、請參閱 "管理儲存節點" 以及的指示 "監控 StorageGRID"。

判斷移轉資料的**ILM**原則

這個系統的ILM原則決定了複本的製作量、複本的儲存位置、以及複本保留的時間長度。StorageGRIDILM原則包含一組ILM規則、說明如何篩選物件及管理物件資料。

視移轉資料的使用方式和移轉資料的需求而定、您可能會想要針對移轉資料定義不同於日常作業所用ILM規則的獨特ILM規則。例如、如果日常資料管理的法規要求與移轉所含資料的法規要求不同、您可能需要不同等級的儲存設備上不同數量的移轉資料複本。

您可以設定專屬套用至移轉資料的規則、以便在移轉資料與儲存自日常作業的物件資料之間進行唯一區分。

如果您可以使用其中一個中繼資料準則來可靠地區分資料類型、您可以使用此準則來定義僅適用於移轉資料的ILM規則。

在開始資料移轉之前、請先確認您已瞭解StorageGRID 完此系統的ILM原則、以及它將如何套用至移轉的資料、並已對ILM原則進行任何變更並進行測試。請參閱 "使用ILM管理物件"。

> 未正確指定的ILM原則可能導致無法恢復的資料遺失。在啟動ILM原則之前、請仔細檢閱您對其所做的所有變更、以確保原則能如預期運作。

評估移轉對營運的影響

支援物件儲存與擷取的功能設計可有效運作、並可無縫建立物件資料與中繼資料的備援複本、提供絕佳的資料遺失保護。StorageGRID

不過、資料移轉必須依照本指南的指示小心管理、以免影響日常系統作業、或是在極端情況下、在StorageGRID 系統發生故障時、將資料置於遺失風險。

大量資料的移轉會對系統產生額外的負載。當系統負載很重時、它會更緩慢回應儲存和擷取物件的要求。StorageGRID這可能會干擾儲存區和擷取日常作業不可或缺的要求。移轉也可能導致其他作業問題。例如、當儲存節點即將達到容量時、由於批次擷取所造成的大量間歇性負載、可能會導致儲存節點在唯讀和讀寫之間循環、進而產生通知。

如果負載持續沉重、佇列就能開發出StorageGRID 各種作業、而這些作業必須由該系統執行、才能確保物件資料和中繼資料的完整備援。

資料移轉必須依照本文件中的準則仔細管理、以確保StorageGRID 在移轉過程中安全且有效率地操作此系統。移轉資料時、請以批次方式擷取物件、或持續限制擷取。然後、持續監控 StorageGRID 系統、確保不會超過各種屬性值。

排程及監控資料移轉

資料移轉必須排程並視需要進行監控、以確保資料是根據ILM原則在所需時間範圍內放置。

排程資料移轉

避免在核心作業時間內移轉資料。將資料移轉限制在系統使用率偏低的晚上、週末和其他時間。

如果可能、請勿在活動頻繁期間排程資料移轉。然而、如果完全避免高活動期間是不實際的、只要您密切監控相關屬性、並在超出可接受的值時採取行動、就可以安全地繼續。

監控資料移轉

下表列出資料移轉期間必須監控的屬性、以及它們所代表的問題。

如果您使用流量分類原則搭配速率限制來調節擷取速度、您可以搭配下表所述的統計資料來監控觀察的速率、並視需要減少限制。

監控	說明
等待ILM評估的物件數目	1. 選取*支援*>*工具*>*網格拓撲*。 2. 選擇「部署_>*總覽*>*主要*」。 3. 在ILM活動區段中、監控下列屬性所顯示的物件數量： ◦ 等待-全部（**XQUZ**）：等待ILM評估的物件總數。 ◦ 等待-用戶端（**XCQZ**）：等待用戶端作業（例如擷取）ILM評估的物件總數。 4. 如果這些屬性中任一屬性所顯示的物件數量超過100、請節流物件的擷取速度、以減少StorageGRID 整個過程中的負載。
目標歸檔系統的儲存容量	如果ILM原則將移轉資料的複本儲存到目標歸檔儲存系統（磁帶或雲端）、請監控目標歸檔儲存系統的容量、以確保移轉資料有足夠的容量。
歸檔節點>* ARC/>*儲存*	如果觸發*儲存故障（ARVF*）*屬性的警示、則目標歸檔儲存系統可能已達到容量。檢查目標歸檔儲存系統、並解決觸發警示的任何問題。