管理StorageGRID

StorageGRID

NetApp
October 03, 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

這些說明說明說明如何使用Grid Manager來設定群組和使用者、建立租戶帳戶、讓S3和Swift用戶端應用程式儲存和擷取物件、設定和管理StorageGRID 各種不同的靜態網路、設定AutoSupport 各種功能、管理節點設定等。

這些指示適用於StorageGRID 安裝好後、將會設定、管理及支援某個系統的技術人員。

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。

立即開始StorageGRID 使用

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	96
Microsoft Edge	96
Mozilla Firefox	94

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。

您需要的產品

- 您擁有登入認證資料。
- 您有Grid Manager的URL。
- 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。
- 您擁有特定的存取權限。

關於這項工作

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：

- 在一個管理節點上發出的警示認可（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。

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。

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：

   https://*FQDN_or_Admin_Node_IP*/`

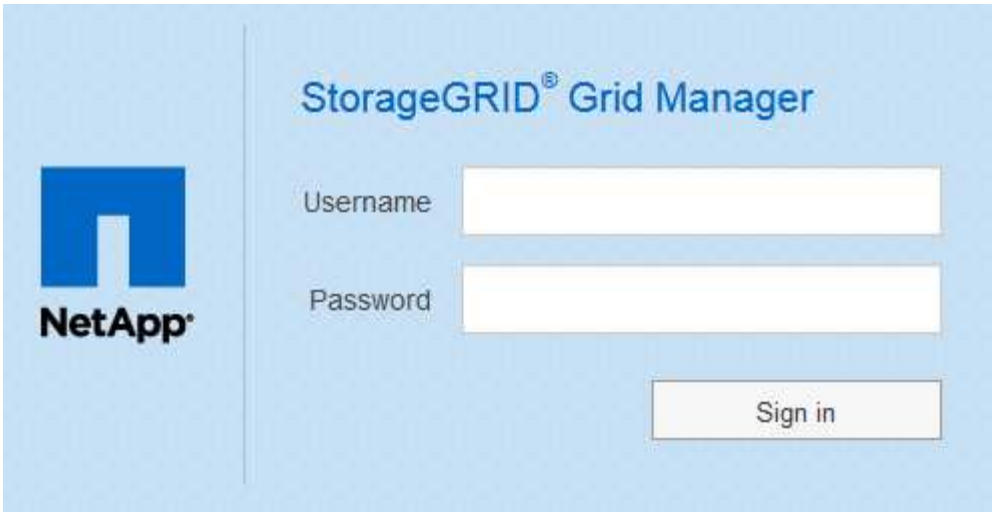
   其中，「_FQDN」或「管理節點」是完整網域名稱或管理節點的IP位址，或是管理節點HA群組的虛擬IP位址。

   如果您必須在HTTPS（443）的標準連接埠以外的連接埠上存取Grid Manager、請輸入下列內容、其中「_FQDN」或「ADD_節點_IP」是完整網域名稱或IP位址、而連接埠是連接埠號碼：

   https://*FQDN_or_Admin_Node_IP:port*/`

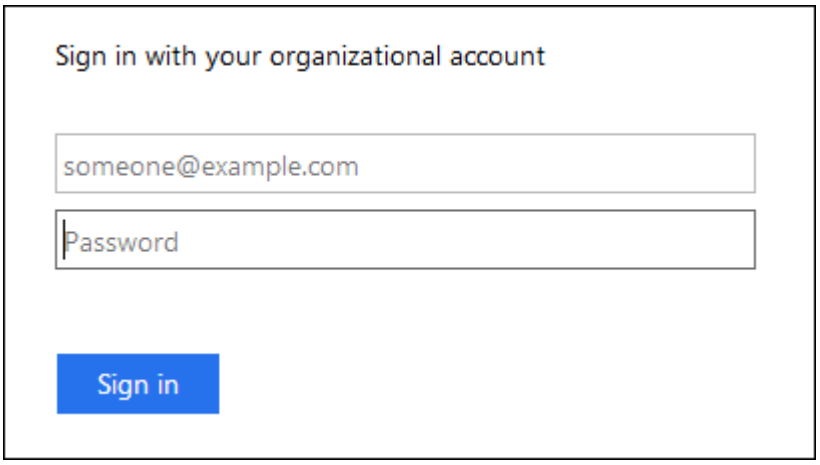
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證（請參閱 關於安全性憑證）。
4. 登入Grid Manager：

   - 如果StorageGRID 您的作業系統未使用單一登入（SSO）：
     i. 輸入Grid Manager的使用者名稱和密碼。
     ii. 選擇*登入*。



- 如果StorageGRID 您的系統啟用SSO、而且這是您第一次存取此瀏覽器上的URL：
  i. 選擇*登入*。您可以將「帳戶ID」欄位保留空白。

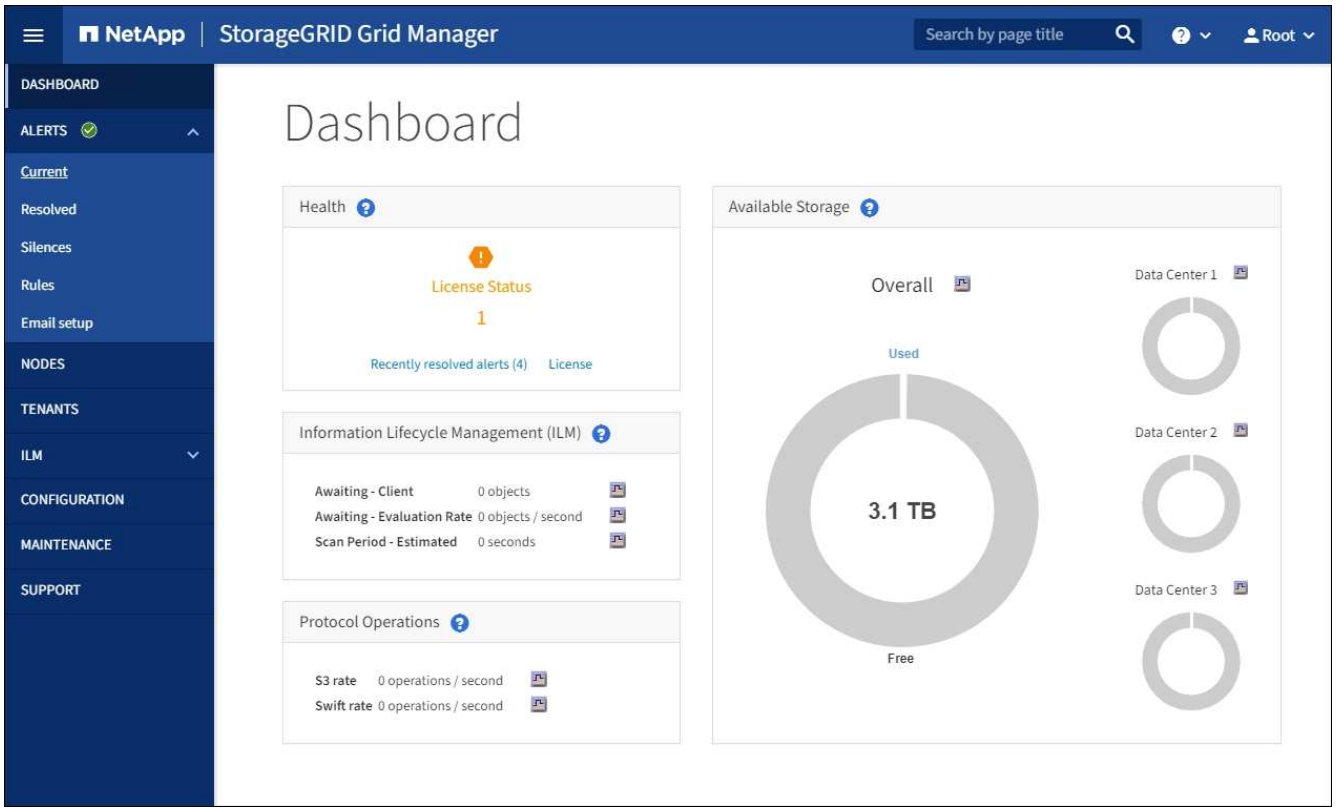
  ii. 在組織的SSO登入頁面上輸入標準SSO認證。例如：



- 如果StorageGRID 您的不支援系統已啟用SSO、且您先前曾存取Grid Manager或租戶帳戶：
  i. 執行下列任一項：

- 輸入* 0*（Grid Manager的帳戶ID）、然後選取*登入*。
- 如果* Grid Manager*出現在最近的帳戶清單中、請選取*登入*。

ii. 在組織的SSO登入頁面上、以標準SSO認證登入。當您登入時、會顯示Grid Manager的首頁、其中包括儀表板。若要瞭解提供的資訊、請參閱 檢視儀表板。



5. 若要登入其他管理節點：

選項	步驟
未啟用SSO	a. 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。 b. 輸入Grid Manager的使用者名稱和密碼。 c. 選擇*登入*。
SSO已啟用	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。 如果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。不過、如果SSO工作階段過期、系統會再次提示您輸入認證資料。 附註： SSO無法在受限網格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

- 透過防火牆控制存取
- 設定單一登入
- 管理管理群組
- 管理高可用度群組
- 使用租戶帳戶
- 監控及疑難排解

登出Grid Manager

使用Grid Manager之後、您必須登出、以確保未獲授權的使用者無法存取StorageGRID 該系統。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。 *附註：*如果啟用SSO、而且您也已登入租戶管理程式、您也必須登出租戶帳戶、才能登出SSO。

相關資訊

- 設定單一登入
- 使用租戶帳戶

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。

您需要的產品

您將使用登入Grid Manager 支援的網頁瀏覽器。

關於這項工作

如果StorageGRID 您以聯盟使用者的身分登入至支援單一登入（SSO）、則無法在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*。

變更瀏覽器工作階段逾時

您可以控制Grid Manager和Tenant Manager使用者是否在超過一定時間內處於非作用中狀態時登出。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

GUI無活動逾時預設為900秒（15分鐘）。如果使用者的瀏覽器工作階段在這段時間內未處於作用中狀態、工作階段就會逾時。

視需要、您可以設定GUI無活動逾時顯示選項來增加或減少逾時期間。

如果啟用單一登入（SSO）、且使用者的瀏覽器工作階段逾時、系統的運作方式就如同使用者手動選取*登出*。使用者必須重新輸入SSO認證資料、StorageGRID 才能再次存取功能。請參閱 設定單一登入。

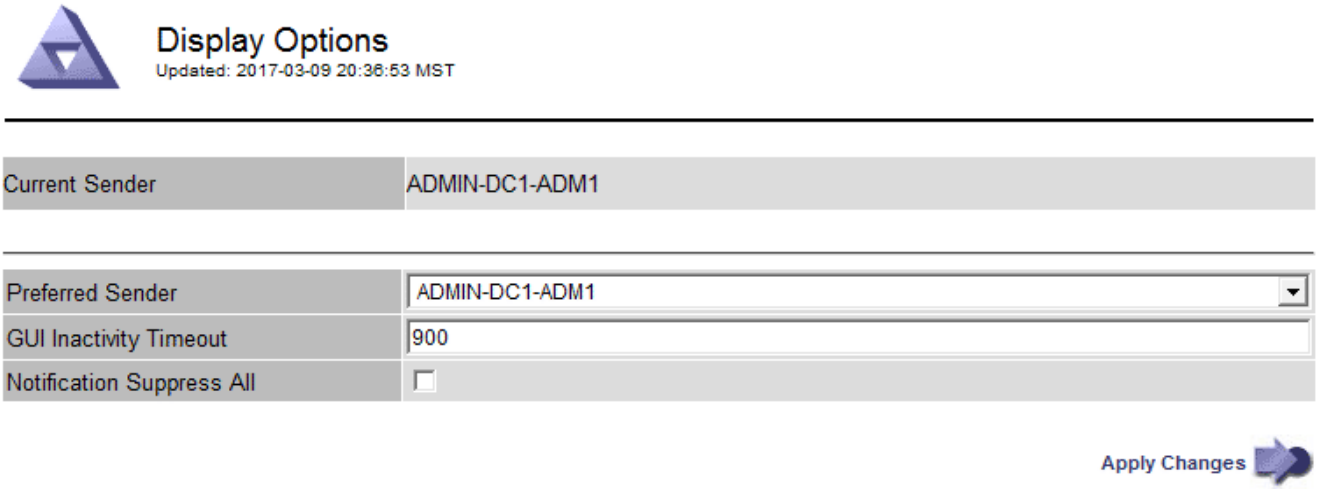
使用者工作階段逾時也可由下列項目控制：

- 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。根據預設、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、即使未達到GUI閒置逾時的值、該使用者仍會自動登出。若要續約權杖、使用者必須重新登入。
- 身分識別供應商的逾時設定、假設啟用SSO StorageGRID 以供執行功能。

步驟

1. 選擇*組態*>*系統*>*顯示選項*。
2. 若為* GUI無活動逾時*、請輸入60秒以上的逾時期間。

   如果您不想使用此功能、請將此欄位設為0。使用者登入後16小時內即會登出、驗證權杖即過期。



3. 選取*套用變更*。

   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。

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。

關於這項工作

如果StorageGRID 此款作業系統的軟體授權發生問題、儀表板上的「健全狀況」面板會顯示「授權狀態」圖示和*授權*連結。此數字表示有多少與授權相關的問題。

步驟

若要檢視授權、請執行下列其中一項：

- 從儀表板的「健全狀況」面板中、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。
- 選擇*維護*>*系統*>*授權*。

此時會出現「授權」頁面、並提供下列有關目前授權的唯讀資訊：

- 系統ID、這是此安裝的唯一識別號碼StorageGRID StorageGRID
- 授權序號
- 網格的授權儲存容量
- 軟體授權結束日期
- 支援服務合約結束日期
- 授權文字檔的內容

若為StorageGRID 在發行版本不含於Es11的授權、授權儲存容量將不包含在授權檔案中、並會顯示「請參閱授權合約」訊息、而非數值。

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。

您需要的產品

- 您有新的授權檔案可套用StorageGRID 到您的作業系統。
- 您擁有特定的存取權限。

- 您有資源配置通關密碼。

步驟

1. 選擇*維護*>*系統*>*授權*。
2. 在StorageGRID * Provisioning Passphrase *（*配置密碼）文字方塊中、輸入您的供應系統的密碼。
3. 選擇*瀏覽*。
4. 在「Open（開啟）」對話方塊中、找出並選取新的授權檔案（`.txt'）、然後選取「* Open*（開啟*）」。

   系統會驗證並顯示新的授權檔案。

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：

- 「/網格」：僅限Grid Manager使用者存取、並以設定的群組權限為基礎。
- 「/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。
- 「/私有」：存取權限僅限Grid Manager使用者使用、且取決於設定的群組權限。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。

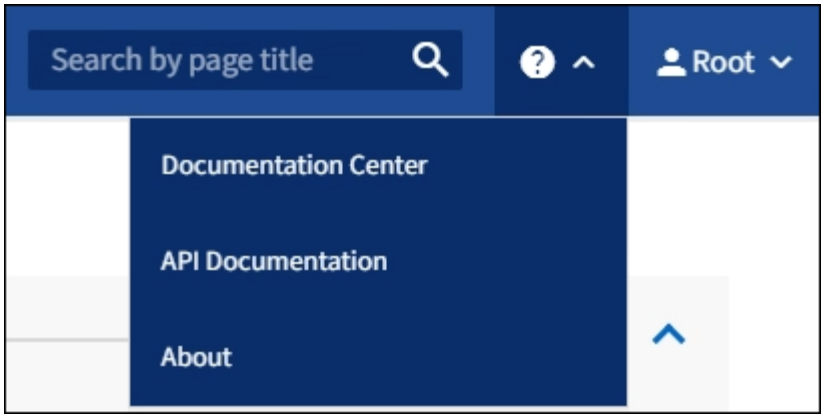
您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

> 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標頭中、選取說明圖示、然後選取* API Documentation *。



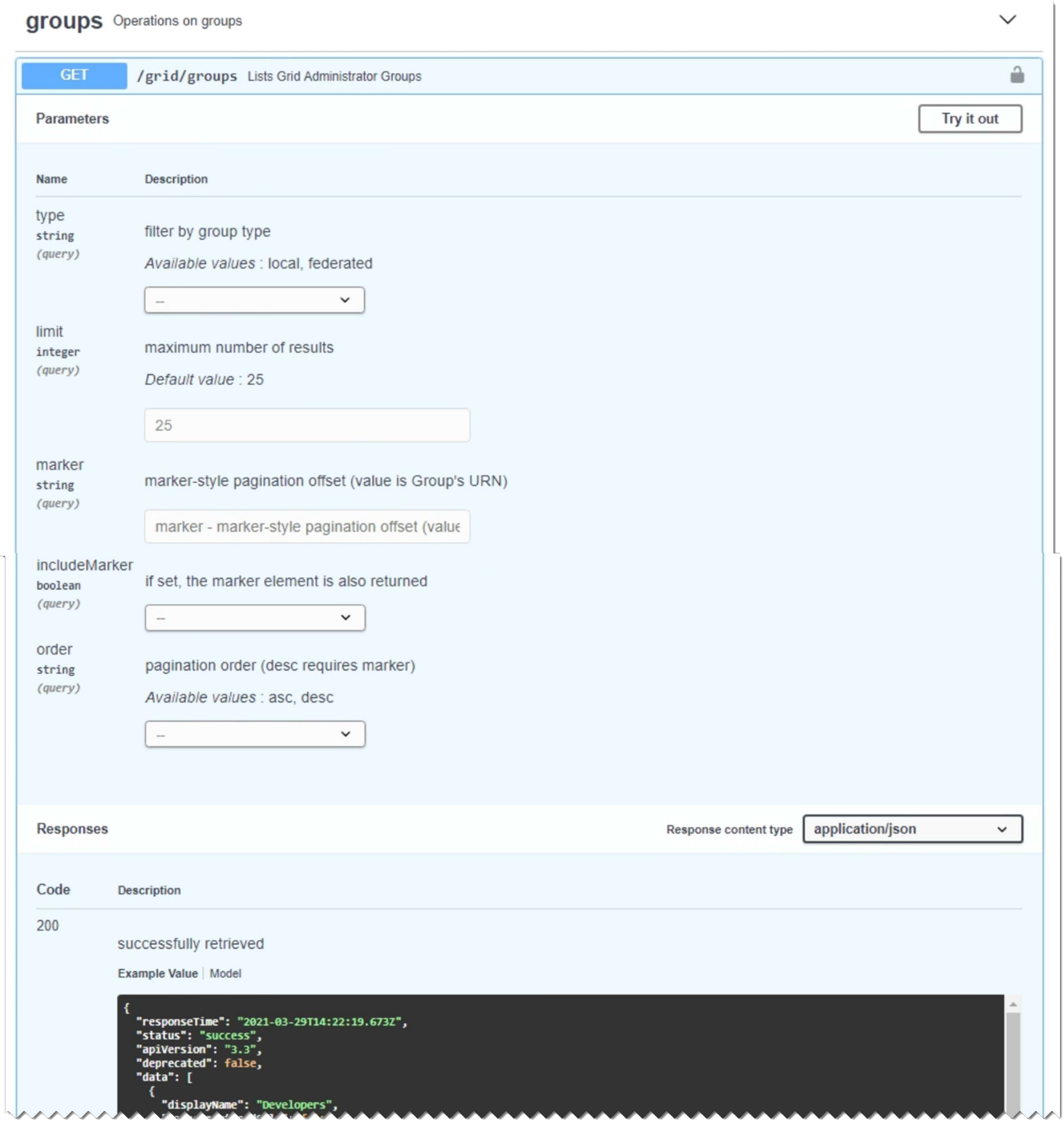
2. 若要使用私有API執行作業、請選取StorageGRID 「畫面管理API」頁面上的*前往私有API文件*。

   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、包括建立新帳戶及擷取特定帳戶的儲存使用量。
- 警示：列出目前警示（舊系統）的作業、並傳回有關網格健全狀況的資訊、包括目前警示和節點連線狀態摘要。
- 警示歷史記錄-已解決警示的作業。
- 警示接收器-警示通知接收器（電子郵件）上的作業。
- 警示規則-警示規則上的作業。
- 警示靜音-警示靜音作業。
- 警示：警示操作。
- 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/授權」）。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_」）。

  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「若啟用單一登入、則驗證API」。

  請參閱「防範跨網站要求偽造」、以取得改善驗證安全性的資訊。

- 用戶端-憑證-作業設定用戶端憑證、以便StorageGRID 使用外部監控工具安全存取。
- 組態-與Grid Management API產品版本相關的作業。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-檢視可能已停用之功能的作業。
- * DNS伺服器*：列出及變更已設定外部DNS伺服器的作業。
- 端點-網域名稱-列出及變更端點網域名稱的作業。
- 銷毀編碼-刪除編碼設定檔的作業。
- 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。
- 網格密碼-網格密碼管理作業。
- 群組：管理本機Grid系統管理員群組的作業、以及從外部LDAP伺服器擷取聯盟Grid系統管理員群組。
- 身分識別來源-作業：設定外部身分識別來源、以及手動同步處理聯盟群組與使用者資訊。

- * ILM *-資訊生命週期管理（ILM）的營運。
- 授權-擷取StorageGRID 及更新此功能的作業。
- 記錄：收集及下載記錄檔的作業。
- 指標：StorageGRID 針對包括即時度量查詢在單一時間點進行的運算、以及在一段時間內進行的範圍度量查詢。Grid Management API使用Prometheus系統監控工具作為後端資料來源。如需建構Prometheus查詢的相關資訊、請參閱Prometheus網站。

> 名稱中包含「_Private」的指標僅供內部使用。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-節點詳細資料上的作業。
- 節點健全狀況-節點健全狀況狀態的作業。
- * 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-恢復程序的作業。
- 恢復套件-下載恢復套件的作業。
- 地區-檢視及建立區域的作業。
- * S3物件鎖定*-全域S3物件鎖定設定的作業。
- 伺服器認證-檢視及更新Grid Manager伺服器認證的作業。
- * SNMP *-目前SNMP組態上的作業。
- 流量類別-流量分類原則的作業。
- 不受信任的用戶端網路：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版本3。

https://*hostname_or_ip_address*/api/v3/authorize`

當進行*不相容*的變更時、會使租戶管理API的主要版本與舊版相容。當做出*與舊版相容*的變更時、租戶管理API的次要版本會被提升。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 時、只會啟用最新版本的Grid Management 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。

> 您可以使用Grid Management API來設定支援的版本。如需詳細資訊、請參閱Swagger API文件的「config」一節。您應該在更新所有Grid Management API用戶端以使用較新版本之後、停用對較舊版本的支援。

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 v1 API at POST "/api/v1/authorize"
```

判斷目前版本支援哪些**API**版本

使用下列API要求傳回支援的API主要版本清單：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定要求的**API**版本

您可以使用路徑參數（`/API/v3）或標頭（'API-版本：3'）來指定API版本。如果您同時提供這兩個值、則標頭值會覆寫路徑值。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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、請在驗證期間將「csrfToken」參數設為「true」。預設值為「假」。

```
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"
```

如果為真、「GridCsrfToken」Cookie會以隨機值設定、以供登入Grid Manager、而「AccountCsrfToken」Cookie則會以隨機值設定、以供登入租戶管理程式。

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、其標頭值設為CSRF權杖Cookie的值。
- 對於接受格式編碼實體的端點：「csrfToken」格式編碼的要求實體參數。

如需其他範例與詳細資料、請參閱線上API文件。

> 若要求具有CSRF權杖Cookie集、也會針對任何要求執行「Content-Type：application/json」標頭、以進一步保護Json要求實體免受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。

您需要的產品

- 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：

- "storagegride-ssoauth.py" Python指令碼、位於StorageGRID 下列目錄中：安裝檔案目錄（如Red Hat Enterprise Linux或CentOS、Ubuntu或DEBIANS的"./rpms"、VMware的"./vSphere."）。
- 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：「在此回應中找不到有效的SubjectConfirmation」。

  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、可能會看到錯誤：「Unsupported SAML version（不支援的SAML版本）」。

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用"storagegrid sosoauth.py" Python指令碼。前往步驟2。
   - 使用Curl要求。前往步驟3。
2. 如果要使用"storagegrid ssoauth.py"指令碼、請將指令碼傳遞給Python解譯程式、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作為「TENANTACCOUNTID」。

b. 若要接收已簽署的驗證URL、請向「/API/v3/授權-SAML」發出POST要求、並從回應中移除其他Json編碼。

此範例顯示「TENANTACCOUNTID」的已簽署驗證URL的POST要求。結果將傳送至「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://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 從回應中儲存「AMLRequest」、以便在後續命令中使用。

```
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. 從回應中儲存「ISAUTH」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. 從隱藏欄位儲存「AMLResponse"：

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

j. 使用儲存的「AMLResponse"（AMLResponse"）、提出StorageGRID（/API/SAML-Response"）要

求、以產生StorageGRID 一個反映驗證權杖。

若為「RelayState」、請使用租戶帳戶ID、若您想登入Grid Management API、請使用0。

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

回應包括驗證權杖。

```
{
    "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儲存為「MoYTOKEN」。

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

您現在可以將「MoYTOKEN」用於其他要求、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

如有需要、StorageGRID 只要從貴組織的單一登出頁面登出、即可登出此功能。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"」傳遞給SLO API：

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

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」、使用者將登出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
```

「204無內容」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

您需要的產品

- 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：

- "storagegRide-ssoauth-azure.py" Python指令碼
- "storagegRide-ssoauth-azure.js" Node.js指令碼

這兩個指令碼都位於StorageGRID 支援Red Hat Enterprise Linux或CentOS的版本/rpmss目錄（適用於Ubuntu或DEBIANS的版本/debs目錄、以及適用於VMware的版本/vSphere目錄）。

若要寫入您自己與Azure的API整合、請參閱「storagegRide-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、可能會看到錯誤：「Unsupported SAML version（不支援的SAML版本）」。

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）：

      "npPM install -g <module>

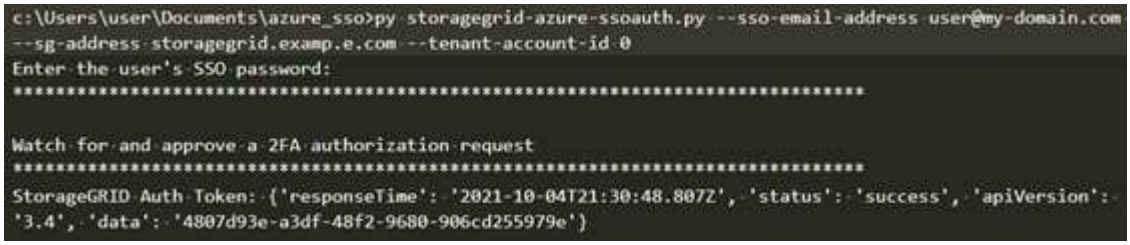
2. 將Python指令碼傳遞給Python解譯器以執行指令碼。

   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（例如輸入透過文字訊息接收的程式碼）。

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

您需要的產品

- 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：

- "storagegride-ssoauth.py" Python指令碼、位於StorageGRID 下列目錄中：安裝檔案目錄（如Red Hat Enterprise Linux或CentOS、Ubuntu或DEBIANS的"./rpms"、VMware的"./vSphere."）。
- 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：「在此回應中找不到有效的SubjectConfirmation」。

  > 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、可能會看到錯誤：「Unsupported SAML version（不支援的SAML版本）」。

步驟

1. 選取下列方法之一以取得驗證權杖：

- 使用"storagegrid sosoauth.py" Python指令碼。前往步驟2。
- 使用Curl要求。前往步驟3。

2. 如果要使用"storagegrid ssoauth.py"指令碼、請將指令碼傳遞給Python解譯程式、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」（Pingfederate、pingfederate等）的任何變化。
   - 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作為「TENANTACCOUNTID」。

   b. 若要接收已簽署的驗證URL、請向「/API/v3/授權-SAML」發出POST要求、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. 從回應中儲存「AMLRequest」、以便在後續命令中使用。

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

d. 匯出回應和Cookie、並回應回應回應：

```
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. 從隱藏欄位儲存「AMLResponse"：

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

j. 使用儲存的「AMLResponse"（AMLResponse"）、提出StorageGRID（/API/SAML-Response"）要求、以產生StorageGRID 一個反映驗證權杖。

若為「RelayState」、請使用租戶帳戶ID、若您想登入Grid Management API、請使用0。

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

回應包括驗證權杖。

```
{
    "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儲存為「MoYTOKEN」。

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

您現在可以將「MoYTOKEN」用於其他要求、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

如有需要、StorageGRID 只要從貴組織的單一登出頁面登出、即可登出此功能。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"」傳遞給SLO API：

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

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」、使用者將登出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
```

   「204無內容」回應表示使用者現在已登出。

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

控制StorageGRID 對功能的存取

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。

您需要的產品

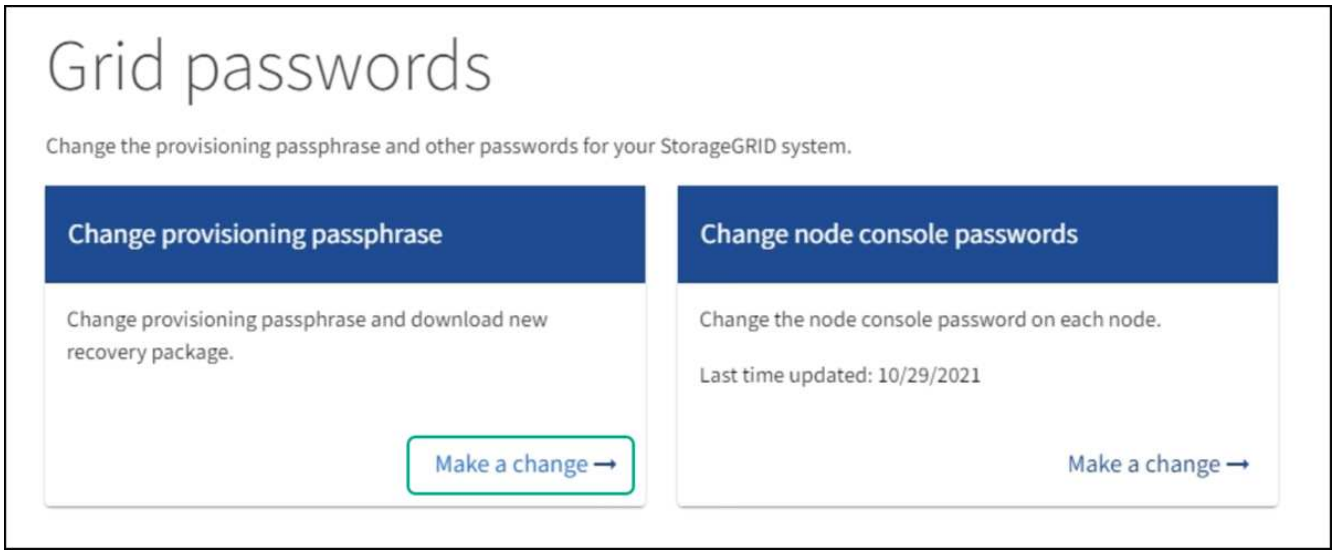
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您具有「維護」或「根」存取權限。
- 您有目前的資源配置通關密碼。

關於這項工作

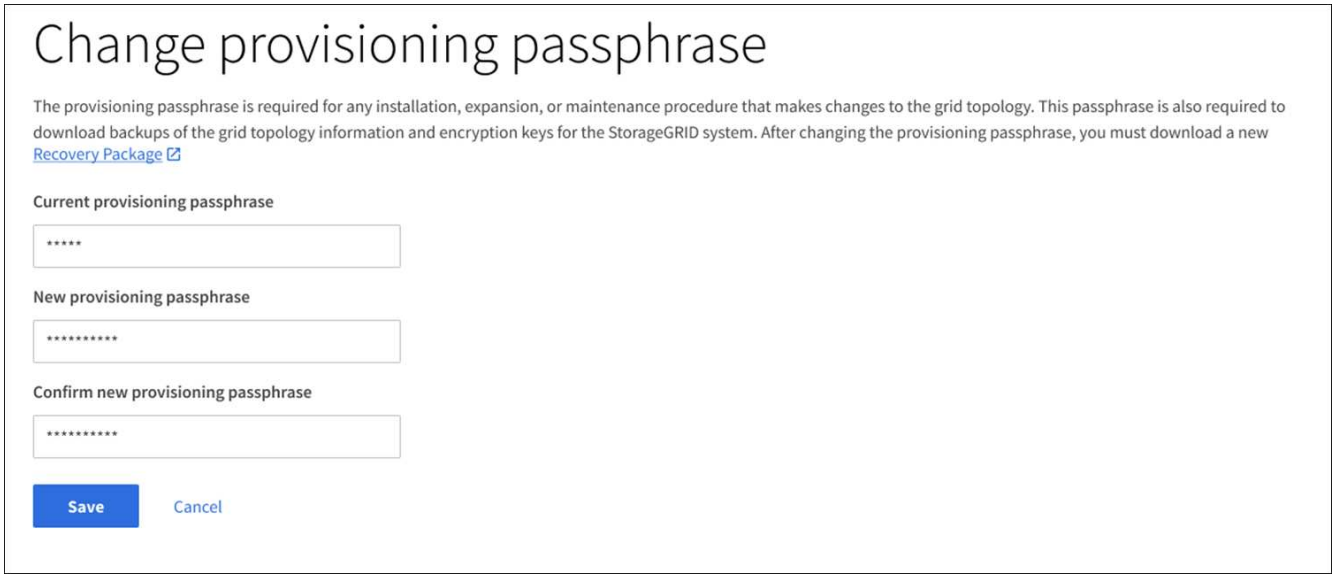
許多安裝和維護程序以及的都需要資源配置通關密碼 正在下載恢復套件。資源配置通關密碼未列在「pes密碼」檔案中。請務必記錄資源配置通關密碼、並將密碼保存在安全的位置。

步驟

1. 選擇*組態*>*存取控制*網格密碼。

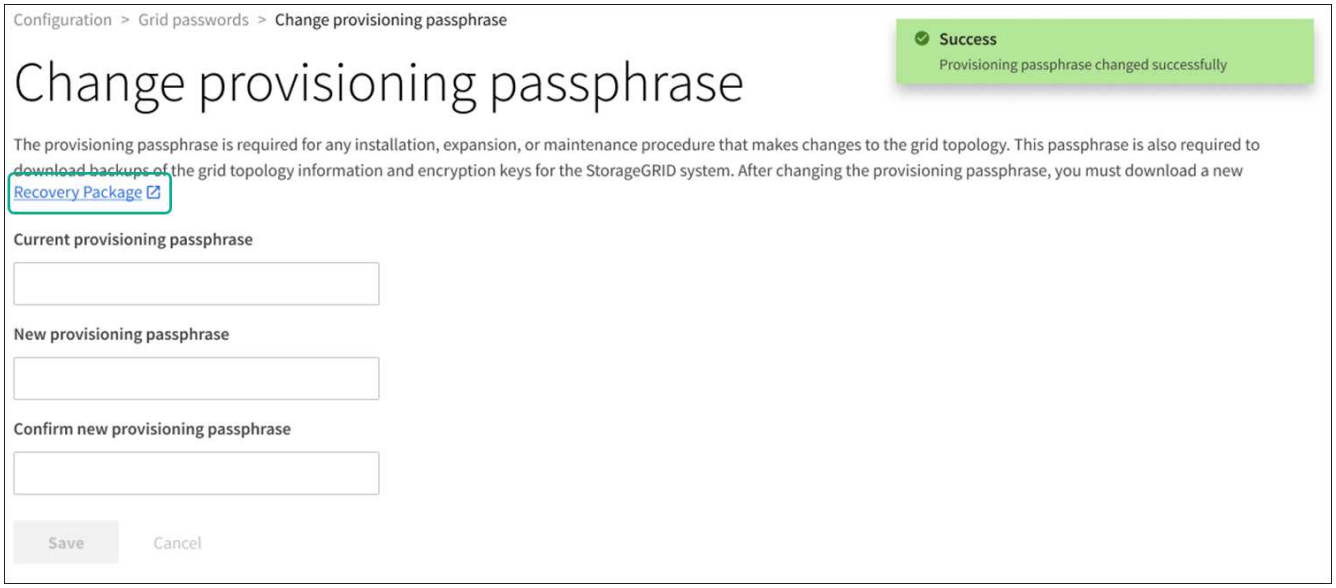


2. 在「變更資源配置通關密碼」下選取「進行變更」。



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。

您需要的產品

- 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

使用節點主控台密碼、以「admin」身分使用SSH登入節點、或以VM/實體主控台連線登入root使用者。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。密碼會列在中的「密碼」欄中 `Passwords.txt` 檔案：

> 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。

   必須保護恢復套件檔案、因為其中包含可用於從StorageGRID 該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、會產生包含新密碼的新恢復套件。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、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。

   必須保護恢復套件檔案、因為其中包含可用於從StorageGRID 該系統取得資料的加密金鑰和密碼。

4. 選取此核取方塊、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. 您也可以使用*恢復套件*連結下載新的恢復套件的其他複本。

透過防火牆控制存取

當您想要透過防火牆控制存取時、可以在外部防火牆開啟或關閉特定的連接埠。

控制外部防火牆的存取

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。

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程式或租戶管理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

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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 使用單一登入的需求。
- 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。

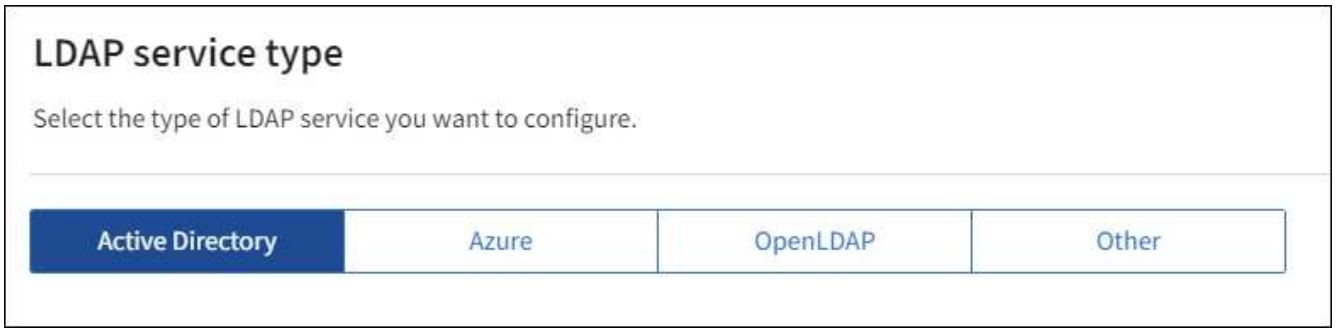
關於這項工作

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。
- 租戶使用者群組、適用於不使用自己身分識別來源的租戶。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

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Active Directory的「shamAccountName」和OpenLDAP的「uid」。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Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。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Active Directory的「shamAccountName」和OpenLDAP的「CN」。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Active Directory的「objectGuid」和OpenLDAP的「entryUUID」。如果要配置Oracle Directory Server、請輸入「nssiuniuniid」。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：

     - 「AMAccountName」或「uid」
     - "objectGUID"、"entryUUUID"或"nssiuniuniid"
     - 《中國》
     - 「memberof」或「isMemberOf」
     - * Active Directory *：「objectSid」、「primaryGroupID」、「userAccountControl」及「userPrincipalName」

- * Azure *：「帳戶已啟用」和「userPrincipalName」

- 密碼：與使用者名稱相關的密碼。
- 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StorageGRID 無法自動判斷模式、則應使用預設的使用者名稱模式。

  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：

  - 使用者主體名稱模式（**Active Directory**和**Azure**）：「[username]@*example*.com」
  - 低層級登入名稱模式（**Active Directory**和**Azure**）：「*example*\[username]」
  - 辨別名稱模式：「CN=[username]、CN=Users、DC=*examends*、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。

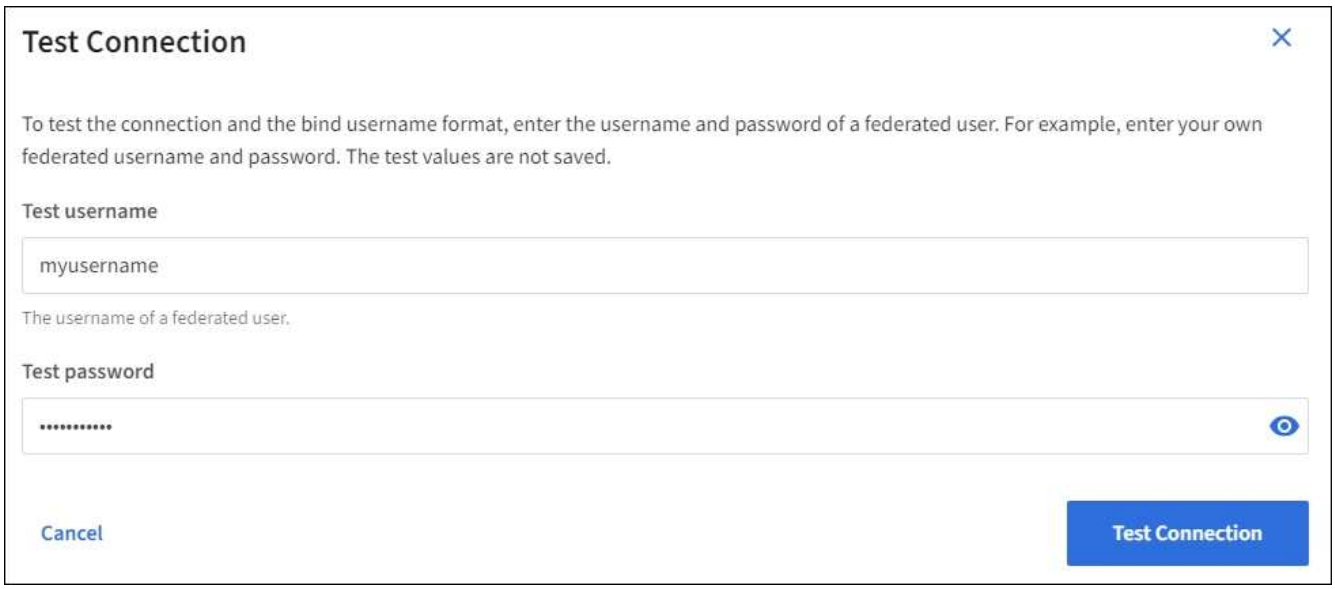
     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

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

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、則會出現「Test connection Successful（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、則會出現「test connection Could not be connection…（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、則會出現「Test connection Successful（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。
- 如果單一登入（SSO）設定為*已啟用*或*沙箱模式*、則「啟用身分聯盟」核取方塊會停用。「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. 取消核取「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 無法自動封鎖S3存取外部停用的使用者。若要封鎖S3存取、請刪除使用者的任何S3金鑰、並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http://www.openldap.org/doc/admin24/index.html["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http://www.openldap.org/doc/admin24/index.html["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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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

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

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

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

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 [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）

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*。

工作	「行動」功能表	詳細資料頁面
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、選取或取消選取 [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、選取或取消選取 [群組權限]。 d. 選取*儲存變更*。

複製群組

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。

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

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）
- 在「組態與維護」頁面上檢視特定資訊

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將無法看到*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
- 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>*安全性*：
  - 憑證
  - 網域名稱
- 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。此權限也可讓您使用Grid Management API的* Metrics *區段、存取自訂的Prometheus度量查詢。

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>*網路*：
  - 連結成本
- 組態>*系統*：
  - 顯示選項
  - 網格選項
  - 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

儲存應用裝置管理員

此權限可SANtricity 讓您透過Grid Manager存取儲存設備上的E系列支援系統管理程式。

租戶帳戶

此權限可讓您存取「租戶」頁面、以便建立、編輯及移除租戶帳戶。此權限也可讓使用者檢視現有的流量分類原則。

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：

「 {"網格"： {"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、任何嘗試變更租戶根密碼的API要求都會失敗、並顯示「'403. Forbididbid禁 用」。

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。

無法重新啟動*活動功能*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}

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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包含一個預先定義的本機使用者、名為「root」。 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 到介紹。

存取精靈

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

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

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。

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。

1. 從「使用者」頁面中、選取您要移除的每個使用者核取方塊。
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 到無法使用的功能。

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

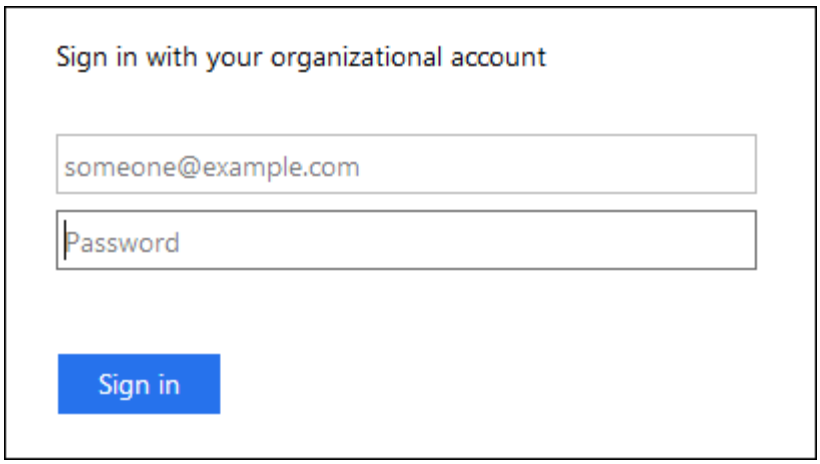
   。如果這是您第一次存取此瀏覽器上的URL、系統會提示您輸入帳戶ID：

- 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：

> 當您輸入租戶帳戶的完整URL（即完整網域名稱或IP位址、後面接著「//?AccountID=*20-digit Account-id*」）時、不會顯示「協助登入」頁面。StorageGRID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. 在使用者介面的右上角找到*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。

如果您已登入...	您也可以登出...	您已登出...
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。

使用單一登入的需求

在啟用StorageGRID 適用於某個作業系統的單一登入（SSO）之前、請先檢閱本節的要求。

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。

- Windows Server 2012 R2更新或更新版本隨附的AD FS 3.0。

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

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並移至「/var/local/mgmt-API」目錄、以存取管理節點的伺服器憑證。自訂伺服器憑證的名稱為「custom-server.crt」。節點的預設伺服器憑證名稱為「sherver.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 透過防火牆控制存取。

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 您已設定身分識別聯盟。

步驟

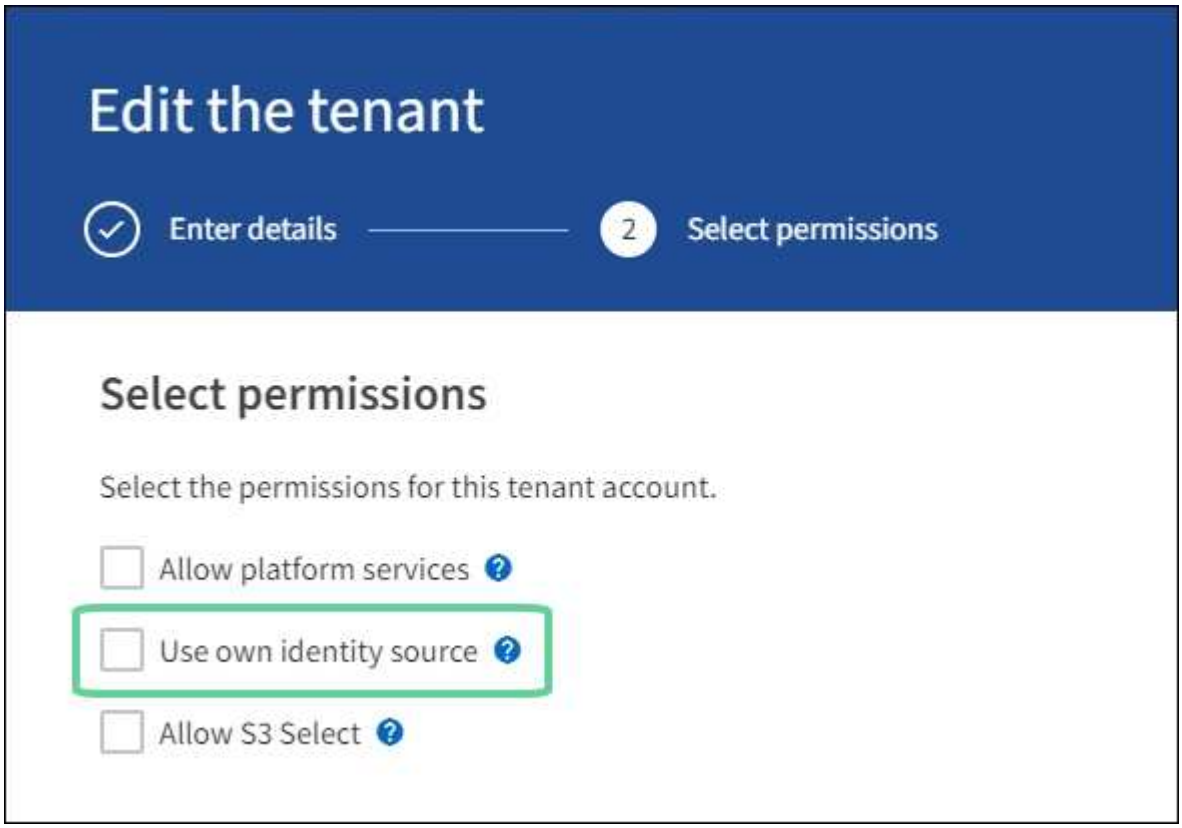
1. 如果有現有的租戶帳戶、請確認沒有租戶使用自己的身分識別來源。

> 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、請確認不再需要任何可能用於此租戶帳戶的聯盟群組、取消選取核取方塊、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*使用自己的身分識別來源*核取方塊、請取消核取方塊、然後選取*儲存*。



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

- 使用單一登入的需求
- 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。

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。
- 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）。

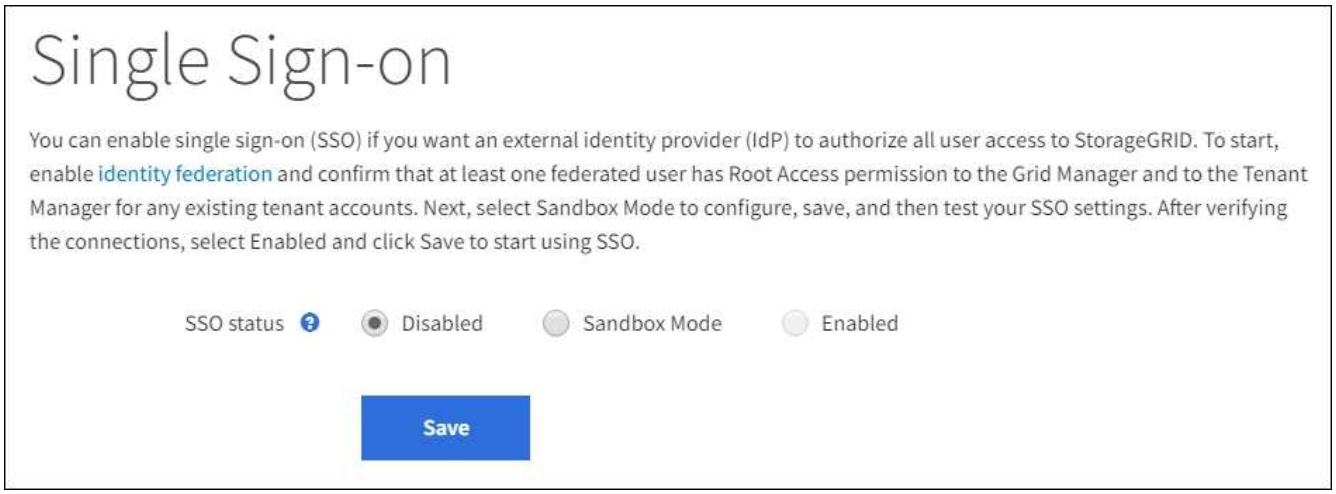
若要讓StorageGRID 服務供應商（服務供應商）和SSO身分識別供應商能夠安全地溝通使用者驗證要求、您必須在StorageGRID 支援中心中設定某些設定。接下來、您必須使用SSO身分識別供應商的軟體、為每個管理節點建立信賴方信任（AD FS）、企業應用程式（Azure）或服務供應商（PingFedate）。最後、您必須返回StorageGRID 到支援SSO的功能。

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

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。



如果未顯示SSO狀態選項、請確認您已將身分識別供應商設定為聯盟身分識別來源。請參閱使用單一登入的需求。

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

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。

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「G」或StorageGRID 「歇歇歇」。
   - 如果網格包含多個管理節點、請在識別碼中加入字串「[hostname]」。例如、「G-[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。

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「G」或StorageGRID 「歇歇歇」。
- 如果網格包含多個管理節點、請在識別碼中加入字串「[hostname]」。例如、「G-[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。
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「G」或StorageGRID 「歇歇歇」。
   - 如果網格包含多個管理節點、請在識別碼中加入字串「[hostname]」。例如、「G-[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

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

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

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。

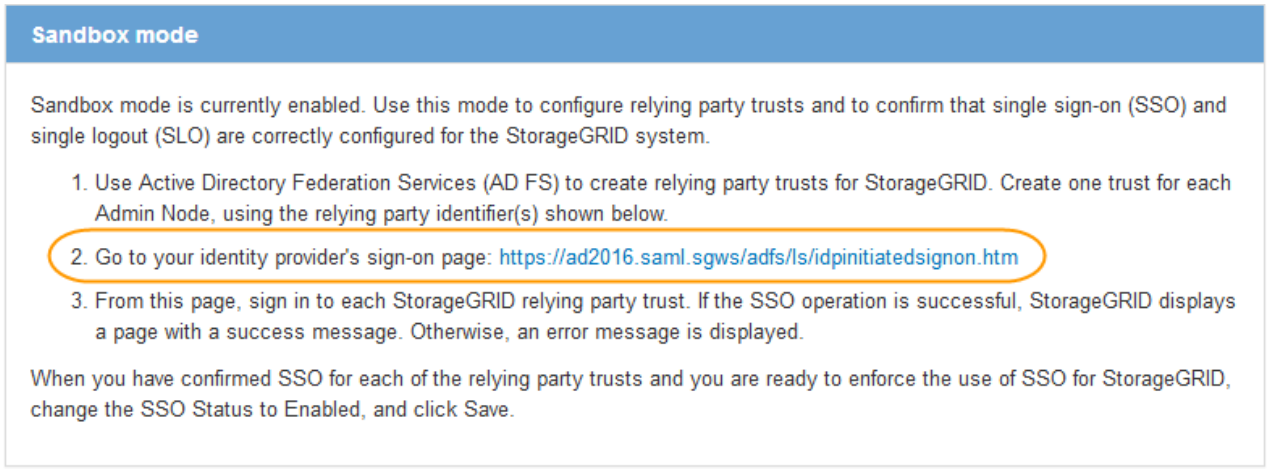
測試SSO連線

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

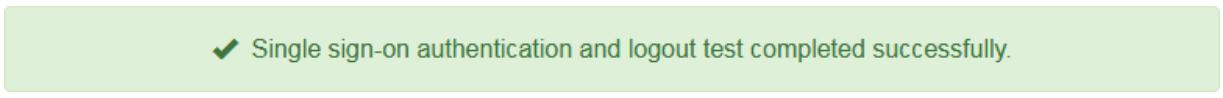
1. 從「功能表單一登入」頁面、找到沙箱模式訊息中的連結。StorageGRID

   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

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。

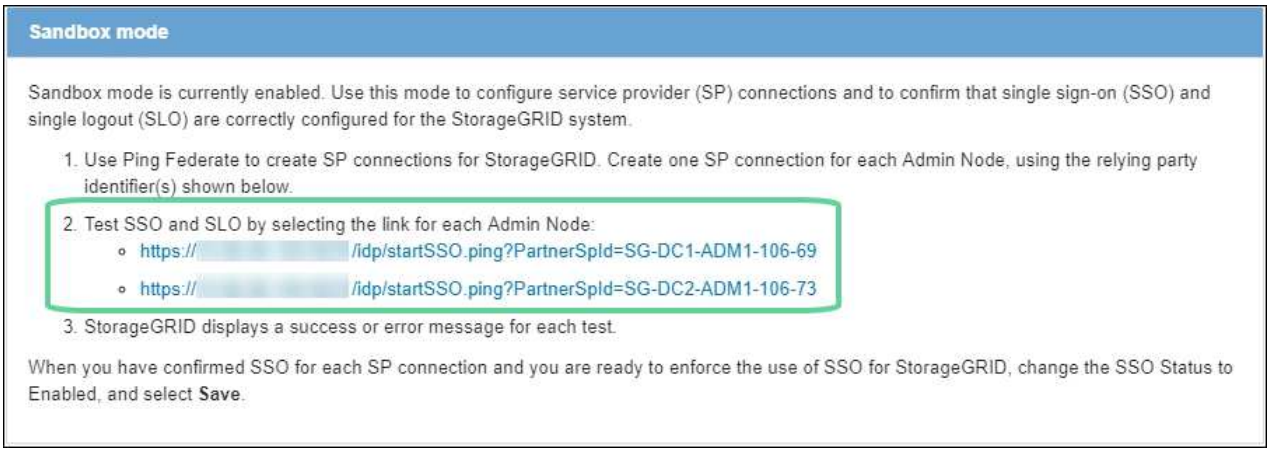
     ✔ Single sign-on authentication and logout test completed successfully.

   - 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

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。

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。

您需要的產品

- 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 "<a href="https://Admin_Node_FQDN/api/saml-metadata"`" class="bare">https://<em>Admin_Node_FQDN</em>/api/saml-metadata"`

   。對於「*admin_Node_Identifier*」、請輸入管理節點的信賴方識別碼、如同「單一登入」頁面所示。例

如「G-DC1-ADM1」。

- 針對「_admin_Node_FQDN」、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、* ObjectGuid至Name 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*。
   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、或只是手動輸入值。

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。

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`

   針對「_admin_Node_FQDN」、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「G-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、* ObjectGuid至Name 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*。
   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、或只是手動輸入值。

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。

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「G-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`

      針對「_admin_Node_FQDN」、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*」

      對於「*admin_Node_Identifier*」、請輸入管理節點的信賴方識別碼、如同「單一登入」頁面所示。例如「G-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、* ObjectGuid至Name 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*。

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`

針對「_admin_Node_FQDN」、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、移至管理節點的「/var/local/mgmt-API」目錄、然後新增「custom-server.crt」憑證檔案。

*注意：*不建議使用管理節點的預設憑證（「Server.crt」）。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。

您需要的產品

- 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**

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

為了將Azure的SSO組態儲存在StorageGRID 功能性的環境中、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。

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。

針對每個管理節點重複下列步驟：

1. 從管理節點登入StorageGRID 到這個功能。
2. 選擇*組態*>*存取控制*>*單一登入*。

3. 選取按鈕、即可下載該管理節點的SAML中繼資料。
4. 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：

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。

您需要的產品

- 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https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["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PingFedate伺服器的管理權限。

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。

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。

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。

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

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

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

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」、這是未使用的項目。

對應介面卡執行個體

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*物件GUID*屬性並加以新增。
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」索引標籤上、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*。
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

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（聲明消費者服務URL）索引標籤上、接受從StorageGRID 支援SAML中繼資料（* POST *用於繫結、而「/API/SAML-RESPONSE」用於端點URL）匯入的預設值。
3. 在「SLO服務URL」索引標籤上、接受從StorageGRID 「物件SAML中繼資料」（「連結的*重新導向*」和「端點URL的「/API/SAML-logout」）匯入的預設值。
4. 在允許的SAML繫結索引標籤上、取消選取*雜訊*和* SOAP*。只需要* POST 和*重新導向。
5. 在「簽章原則」索引標籤上、勾選「需要簽署驗證要求*」和「永遠簽署聲明」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

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。

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

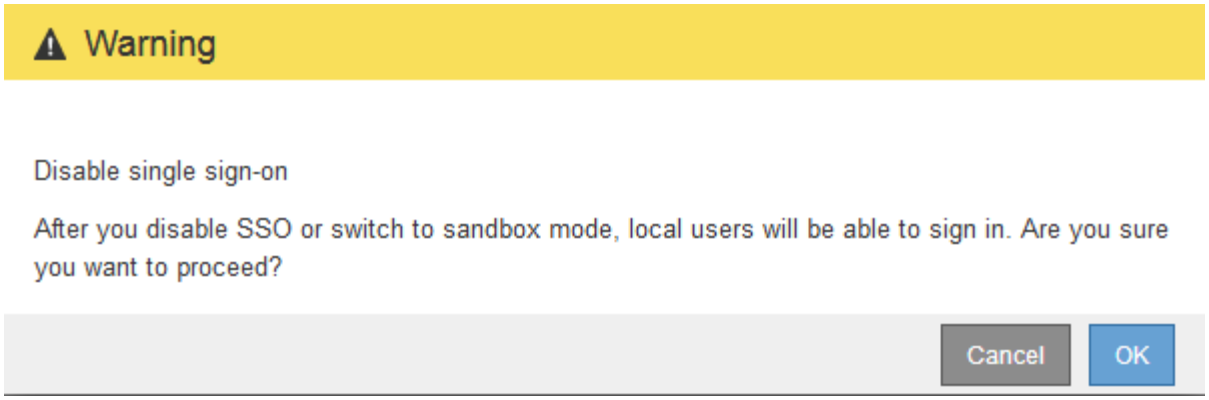
步驟

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。

您需要的產品

- 您擁有特定的存取權限。
- 您有「pes密碼」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SSSSO *」核取方塊會保持選取狀態、除非您更新所有現有的SSO設定、否則這些設定都會維持不變。

步驟

1. 登入管理節點：
   a. 輸入下列命令：「sh admin@admin_Node_IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。

2. 執行下列命令：「'd停 用-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」（重新開機）
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。

管理安全性設定

管理憑證

關於安全性憑證

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。不具證書的不安全連線也受到支援、但不建議使用。

- 自訂CA憑證不會移除內部憑證；不過、自訂憑證應該是為驗證伺服器連線所指定的憑證。
- 所有自訂憑證都必須符合 系統強化準則 適用於伺服器憑證。
- 支援將CA的憑證整合至單一檔案（稱為CA憑證套件）StorageGRID 。

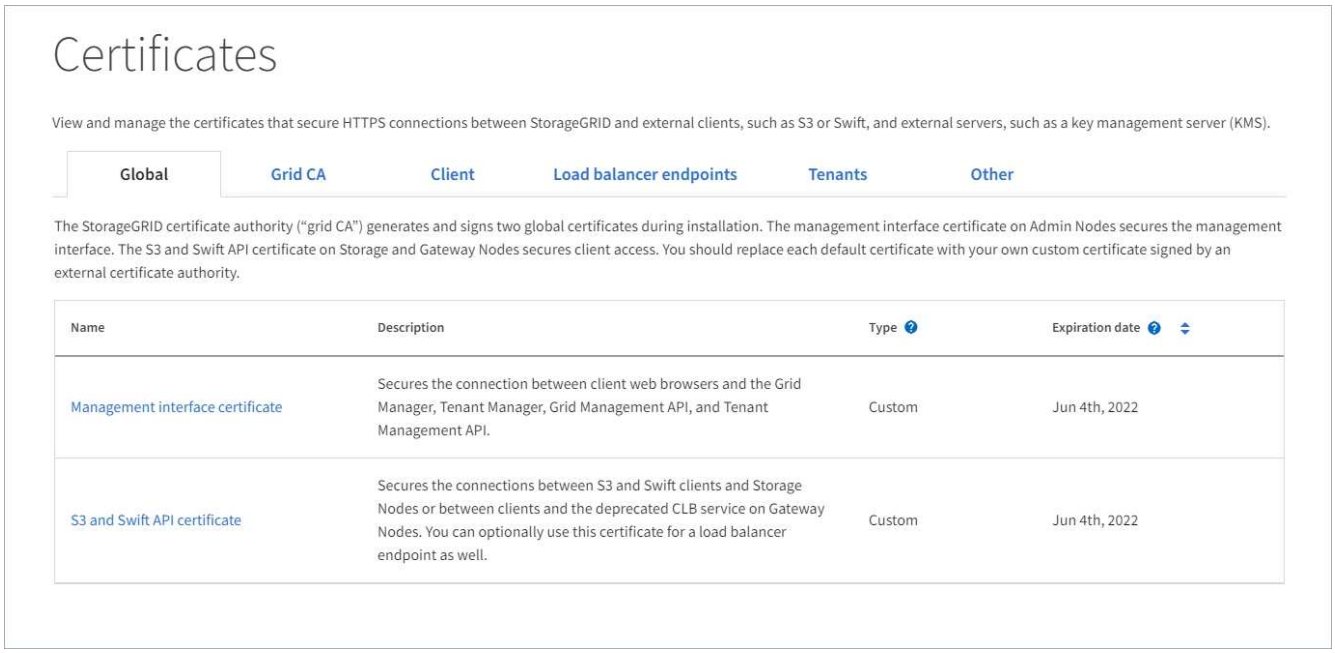
> 此外、還包括所有網格上相同的作業系統CA憑證。StorageGRID在正式作業環境中、請務必指定由外部憑證授權單位簽署的自訂憑證、以取代作業系統CA憑證。

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。

1. 從Grid Manager中選擇*組態設定*>*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。您只能在擁有適當權限的情況下存取索引標籤。

   - 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。+您應該永遠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、CLB服務（已過時）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上傳或產生時、請確保S3和Swift用戶端之間的連線安全、並確保StorageGRID 閘道節點和管理節點上的「穩定負載平衡器」服務安全無虞。

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：

- 選取端點名稱以開啟包含負載平衡器端點相關資訊的瀏覽器索引標籤、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：

- 身分識別聯盟憑證
- 雲端儲存資源池認證
- 金鑰管理伺服器（KMS）憑證
- 單一登入憑證
- 電子郵件警示通知憑證

- 外部syslog伺服器憑證

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。

您只能在擁有適當權限的情況下檢視及存取其他憑證的資訊。

您可以：

- 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
- 指定S3、C2S S3或Azure的雲端儲存池憑證
- 手動指定SSO憑證以供信賴方信任
- 指定警示電子郵件通知的憑證
- 指定外部syslog伺服器憑證

安全性憑證詳細資料

每種類型的安全性憑證都會在下方說明、並附上包含實作指示的文章連結。

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S3或Swift用戶端連線至儲存節點、閘道節點上已過時的連線負載平衡器（CLB）服務、以及負載平衡器端點（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、則不需要上傳或為每個負載平衡器端點產生個別的憑證。 *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

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

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

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

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）

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

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*、然後選取*設定外部系統記錄伺服器*	設定外部syslog伺服器

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

如需StorageGRID 更多關於如何保護REST API用戶端連線的資訊、請參閱 使用S3 或 使用Swift。

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為失敗的伺服器憑證而中斷、當此伺服器憑證即將過期時、會觸發* Management Interface*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（`.key'）。

     EC私密金鑰必須大於或等於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。儲存副檔名為「.pem」的檔案。

   例如：「toragegrid憑證.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*。+自訂管理介面憑證可用於所有後續新連線至Grid Manager、Tenant Manager、Grid Manager API或Tenant Manager API。

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：

   - 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*：一個或多個IP位址要納入憑證中。
   - 主體：憑證擁有者的X・509主體或辨別名稱（DN）。
   - 有效天數：憑證建立後到期的天數。

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。儲存副檔名為「.pem」的檔案。

例如：「toragegrid憑證.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*。+自訂管理介面憑證可用於所有後續新連線至Grid Manager、Tenant Manager、Grid Manager API或Tenant Manager API。

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PEE。

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*。

還原預設管理介面憑證時、您設定的自訂伺服器憑證檔案將會刪除、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。

您需要的產品

- 您擁有特定的存取權限。
- 您有「pes密碼」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：「sh admin@primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

以root登入時、提示會從「$」變更為「#」。

3. 使用StorageGRID 新的自我簽署憑證來設定功能。

   「$ Sudo make證書-網域_萬用字元-admin-node-fqd_-類型管理」

   - 對於「-domaines」、請使用萬用字元來代表所有管理節點的完整網域名稱。例如、「*.ui.storagegrid.example.com」使用*萬用字元來表示「admin1.ui.storagegrid.example.com」和「admin2.ui.storagegrid.example.com」。
   - 將「-type（類型）」設為「management（管理）」、以設定Grid Manager和Tenant Manager所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 "引數來覆寫預設的有效期間。

     憑證的有效期間始於執行「make憑證」時。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。$'出口'
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套裝組合「.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。儲存副檔名為「.pem」的檔案。

   例如：「toragegrid憑證.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. 儲存副檔名為「.pem」的文字檔。

   例如：「toragegrid憑證.pem」

設定**S3**和**Swift API**憑證

您可以取代或還原用於S3或Swift用戶端連線至儲存節點、閘道節點上已過時的連線負載平衡器（CLB）服務、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為失敗的伺服器憑證而中斷、當根伺服器憑證即將過期時、會觸發「S3的全域伺服器憑證過期」和「Swift API*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（`.key'）。

     EC私密金鑰必須大於或等於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。儲存副檔名為「.pem」的檔案。

     例如：「toragegrid憑證.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：

   - 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*：一個或多個IP位址要納入憑證中。
   - 主體：憑證擁有者的X・509主體或辨別名稱（DN）。
   - 有效天數：憑證建立後到期的天數。

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。儲存副檔名為「.pem」的檔案。

例如：「toragegrid憑證.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PEE。

還原預設的**S3**和**Swift API**憑證

您可以針對S3和Swift用戶端連線至儲存節點、以及閘道節點上已過時的CLB服務、恢復使用預設的S3和Swift API認證。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*。

還原全域S3和Swift API憑證的預設版本時、您設定的自訂伺服器憑證檔案將會刪除、無法從系統中還原。預設的S3和Swift API憑證將用於後續的S3和Swift用戶端連線至儲存節點、以及閘道節點上已過時的CLB服務。

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套裝組合「.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。儲存副檔名為「.pem」的檔案。

   例如：「toragegrid憑證.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. 儲存副檔名為「.pem」的文字檔。

   例如：「toragegrid憑證.pem」

相關資訊

- 使用S3
- 使用Swift
- 設定S3 API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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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**PEP**」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。儲存副檔名為「.pem」的檔案。

例如：「toragegrid憑證.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. 儲存副檔名為「.pem」的文字檔。

例如：「toragegrid憑證.pem」

設定**StorageGRID** 適用**FabricPool** 的驗證

如果S3用戶端執行嚴格的主機名稱驗證、但不支援停用嚴格的主機名稱驗證、例如ONTAP使用FabricPool 支援功能的支援功能、則您可以在設定負載平衡器端點時、產生或上傳伺服器憑證。

您需要的產品

- 您擁有特定的存取權限。
- 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。

閘道節點上的個別連線負載平衡器（CLB）服務已過時、不建議搭配FabricPool 使用。

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。

請參閱相關資訊 一般安全性憑證使用 和 設定自訂伺服器憑證。

為了確保作業不會因為失敗的伺服器憑證而中斷、當此伺服器憑證即將過期時、會觸發「憑證頁面*」警示中設定的用戶端憑證過期。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「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。

您需要的產品

- 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

依照案例中的程序新增用戶端憑證：

- [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. 輸入至少包含1個且不超過32個字元的憑證名稱。
4. 若要使用外部監控工具存取Prometheus指標、請選取*允許Prometheus*。
5. 在「憑證類型」區段中、上傳管理介面憑證「.pem」檔案。
   a. 選擇*上傳認證*、然後選擇*繼續*。
   b. 上傳管理介面憑證檔案（`.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。
6. 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。
   f. 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。

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. 輸入至少包含1個且不超過32個字元的憑證名稱。
5. 若要使用外部監控工具存取Prometheus指標、請選取*允許Prometheus*。
6. 在「憑證類型」區段中、上傳用戶端憑證、私密金鑰和CA套裝組合「.pem」檔案：
   a. 選擇*上傳認證*、然後選擇*繼續*。
   b. 上傳用戶端憑證、私密金鑰和CA套裝組合檔案（`.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. 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。
   f. 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。

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. 輸入至少包含1個且不超過32個字元的憑證名稱。
4. 若要使用外部監控工具存取Prometheus指標、請選取*允許Prometheus*。
5. 在*憑證類型*區段中、選取*產生憑證*。
6. 指定憑證資訊：
   - 網域名稱：要包含在憑證中的管理節點之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個或多個管理節點IP位址。
   - 主體：憑證擁有者的X・509主體或辨別名稱（DN）。
7. 選取*產生*。
8. [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。儲存副檔名為「.pem」的檔案。

   例如：「toragegrid憑證.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。

9. 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。

10. 在Grid Manager中、選取*組態*>*安全性*>*憑證*、然後選取*全域*索引標籤。
11. 選擇*管理介面認證*。
12. 選擇*使用自訂憑證*。
13. 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*「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。

14. 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：+

- 管理介面用戶端憑證同時提供給「 **CA**認證」和「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。

f. 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. 輸入至少包含1個且不超過32個字元的憑證名稱。
5. 若要使用外部監控工具存取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。儲存副檔名為「.pem」的檔案。

     例如：「toragegrid憑證.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：

   - 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*：一個或多個IP位址要納入憑證中。
   - 主體：憑證擁有者的X．509主體或辨別名稱（DN）。
   - 有效天數：憑證建立後到期的天數。

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。儲存副檔名為「.pem」的檔案。

     例如：「toragegrid憑證.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。儲存副檔名為「.pem」的檔案。

例如：「toragegrid憑證.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. 儲存副檔名為「.pem」的文字檔。

例如：「toragegrid憑證.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。

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。設備磁碟區加密之後、除非節點可以與KMS通訊、否則您無法存取應用裝置上的任何資料。

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。

檢閱**StorageGRID** 功能加密方法

提供許多加密資料的選項。StorageGRID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）	您可以為StorageGRID 該站台設定金鑰管理伺服器（組態>*安全性*>*金鑰管理伺服器*）、並為該應用裝置啟用節點加密。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。 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
在《支援資料保護系統》中提升安全性SANtricity	如果儲存應用裝置已啟用磁碟機安全功能、您可以使用SANtricity 「支援系統管理程式」來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。	具有完整磁碟加密（FDE）磁碟機或聯邦資訊處理標準（FIPS）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。無法與部分儲存設備或任何服務應用裝置搭配使用。 • SG6000儲存設備 • SG5700儲存設備 • SG5600儲存設備
儲存的物件加密網格選項	您可以在Grid Manager中啟用*儲存的物件加密*選項（組態>*系統*>*網格選項*）。啟用時、任何未在儲存區層級或物件層級加密的新物件、都會在擷取期間加密。	新擷取的S3和Swift物件資料。 現有的儲存物件不會加密。物件中繼資料和其他敏感資料不會加密。 • 設定儲存的物件加密
S3儲存區加密	您發出一個「放入庫位」加密要求、以啟用庫位加密。任何未在物件層級加密的新物件、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。現有的儲存區物件不會加密。物件中繼資料和其他敏感資料不會加密。 • 使用S3
S3物件伺服器端加密（SSe）	您發出S3要求來儲存物件、並附上「x-amz-server端加密」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S3
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端加密-customer-演算 法」 • 「X-amz-server端加密客戶金鑰」 • 「X-amz-server端加密-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S3

加密選項	運作方式	適用於
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：

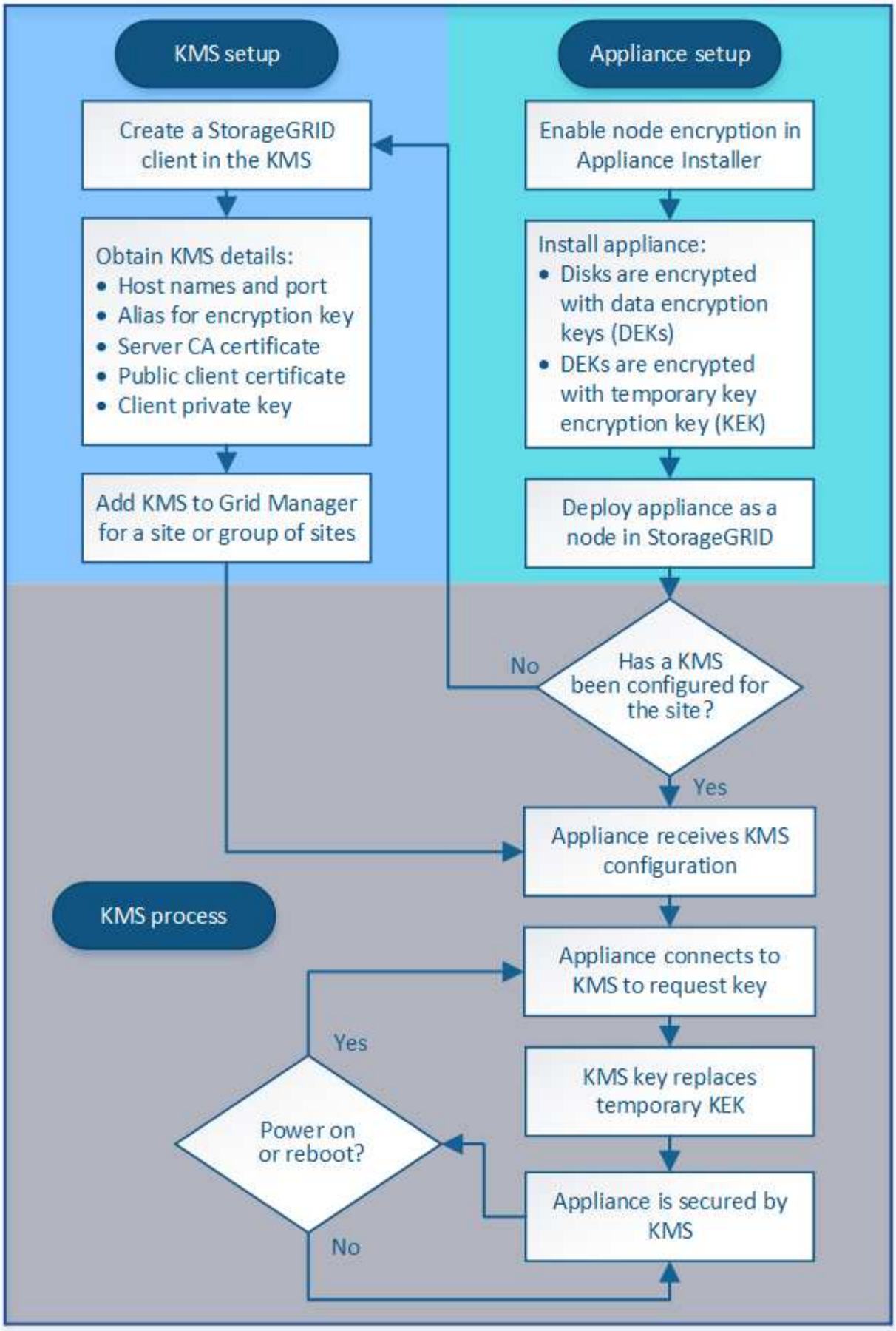
- 您可以使用KMS來保護應用裝置節點、也可以使用SANtricity 支援系統管理程式中的磁碟機安全功能、在同一個應用裝置中的自我加密磁碟機上「雙重加密」資料。
- 您可以使用KMS來保護應用裝置節點上的資料安全、也可以使用「儲存的物件加密」網格選項、在擷取所有物件時加密所有物件。

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。

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 Unified Key Setup（LUKS）磁碟加密產生、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

如需詳細資料、請參閱下列內容：

- SG100與SG1000服務應用裝置
- SG6000儲存設備
- SG5700儲存設備
- SG5600儲存設備

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、無法在電力中斷或重新開機後繼續運作。

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。

KMIP需求為何？

支援KMIP 1.4版。StorageGRID

"關鍵管理互通性傳輸協定規格1.4版"

應用裝置節點與設定的KMS之間的通訊使用安全的TLS連線。支援下列TLS v1.2加密算法的KMIP ：StorageGRID

- TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
- TLS_ECDHE_ECDSa_with _AES-256_GCM_SHA384

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。

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。

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。

您可以將設定的KMS用於下列StorageGRID 的不含技術的應用程式和應用裝置節點：

應用裝置	節點類型
SG1000服務應用裝置	管理節點或閘道節點

應用裝置	節點類型
SG100服務應用裝置	管理節點或閘道節點
SG6000儲存應用裝置	儲存節點
SG5700儲存應用裝置	儲存節點
SG5600儲存應用裝置	儲存節點

您無法將設定的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。

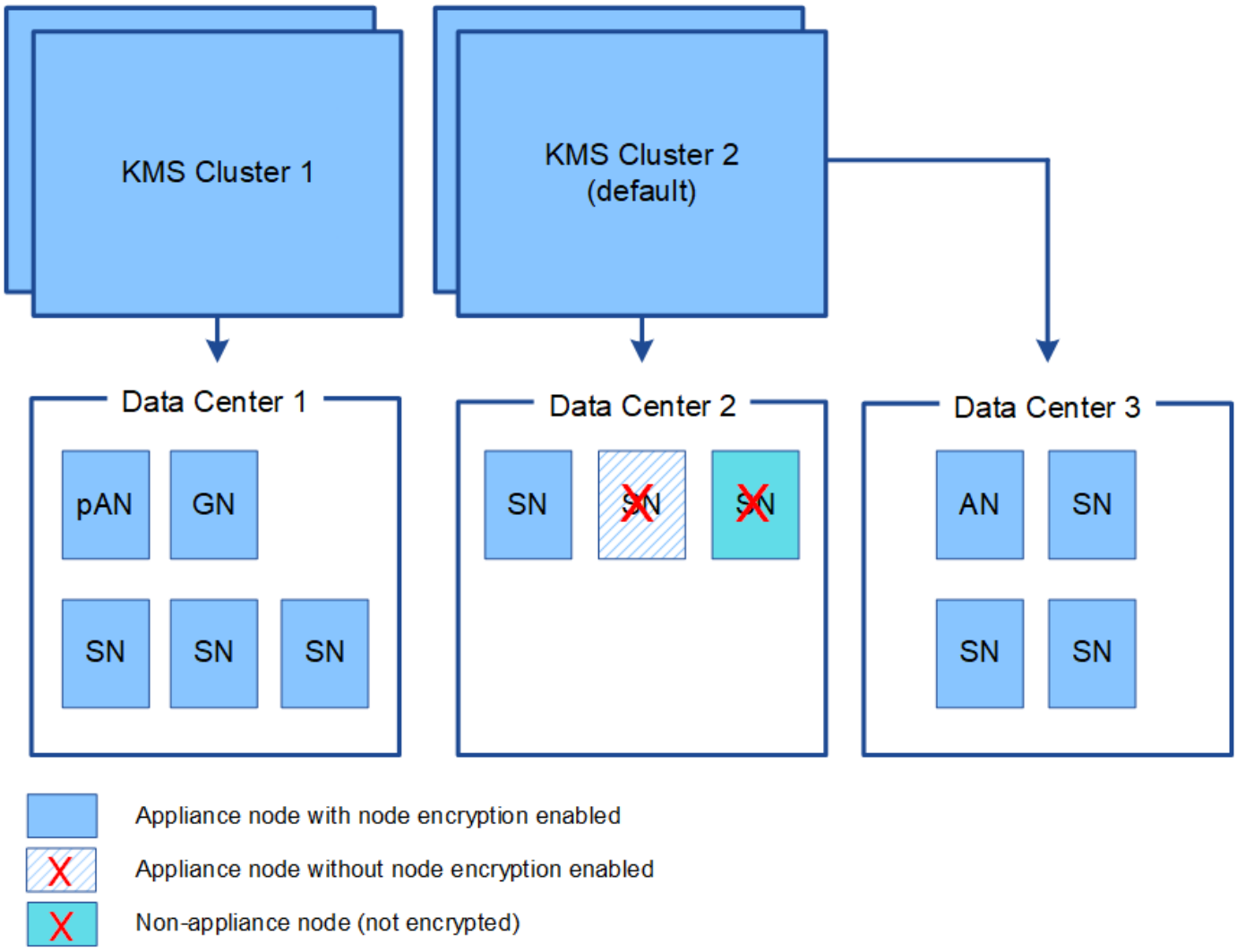
我需要多少個關鍵管理伺服器？

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、您無法在非應用裝置節點或安裝期間未啟用*節點加密*設定的任何應用裝置節點上使用KMS。



當金鑰旋轉時會發生什麼事？

最佳安全做法是定期旋轉每個設定KMS所使用的加密金鑰。

旋轉加密金鑰時、請使用KMS軟體、從上次使用的金鑰版本轉換成相同金鑰的新版本。請勿旋轉至完全不同的按鍵。

> 切勿嘗試在Grid Manager中變更KMS的金鑰名稱（別名）來旋轉金鑰。而是更新KMS軟體中的金鑰版本來旋轉金鑰。對新金鑰使用與先前金鑰相同的金鑰別名。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。

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。
- 如果新的金鑰版本因故無法加密應用裝置磁碟區、則會觸發應用裝置節點的* 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 《不知道如何使用產品安裝程式來清除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。

相關資訊

- SG100與SG1000服務應用裝置
- SG6000儲存設備
- SG5700儲存設備
- SG5600儲存設備

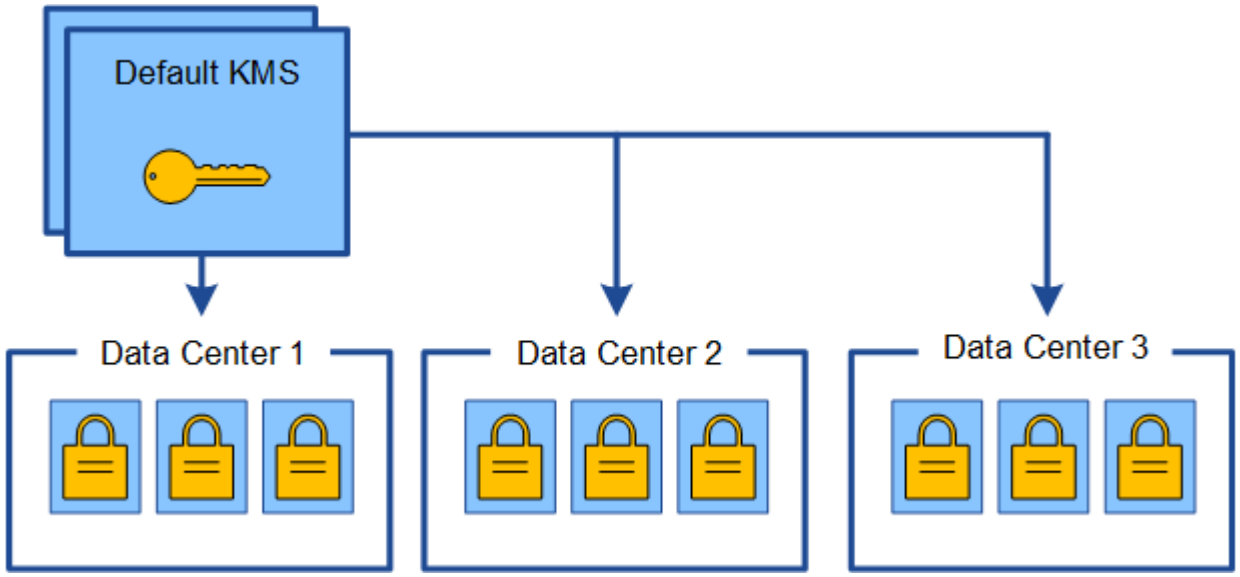
變更網站**KMS**的考量事項

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。

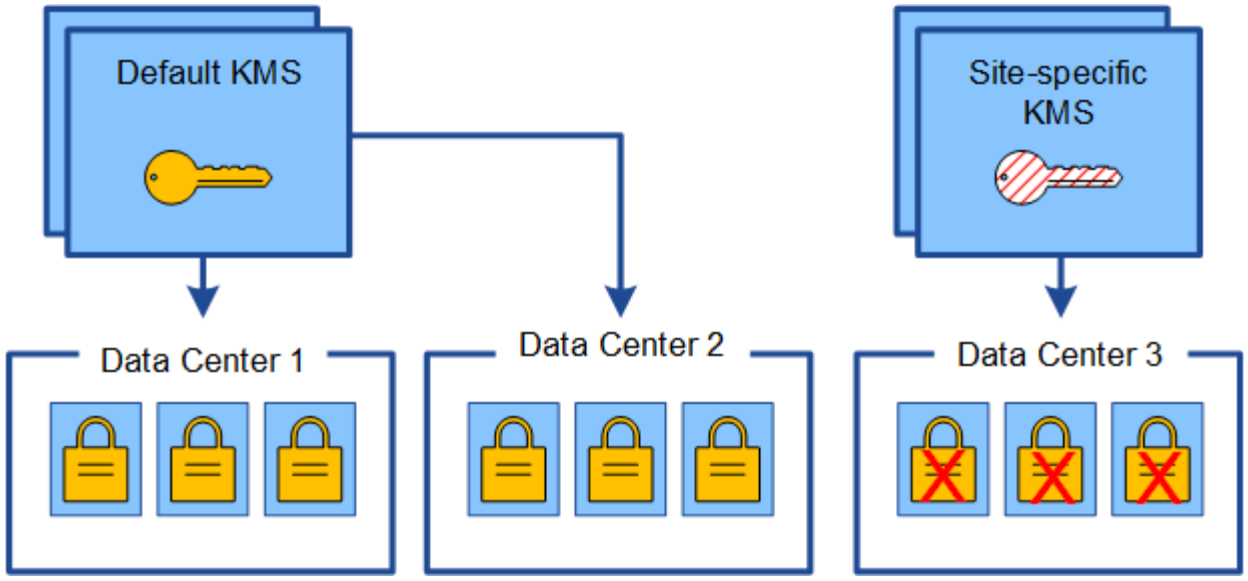
例如：

1. 您一開始會設定適用於所有沒有專屬KMS的站台的預設KMS。
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。

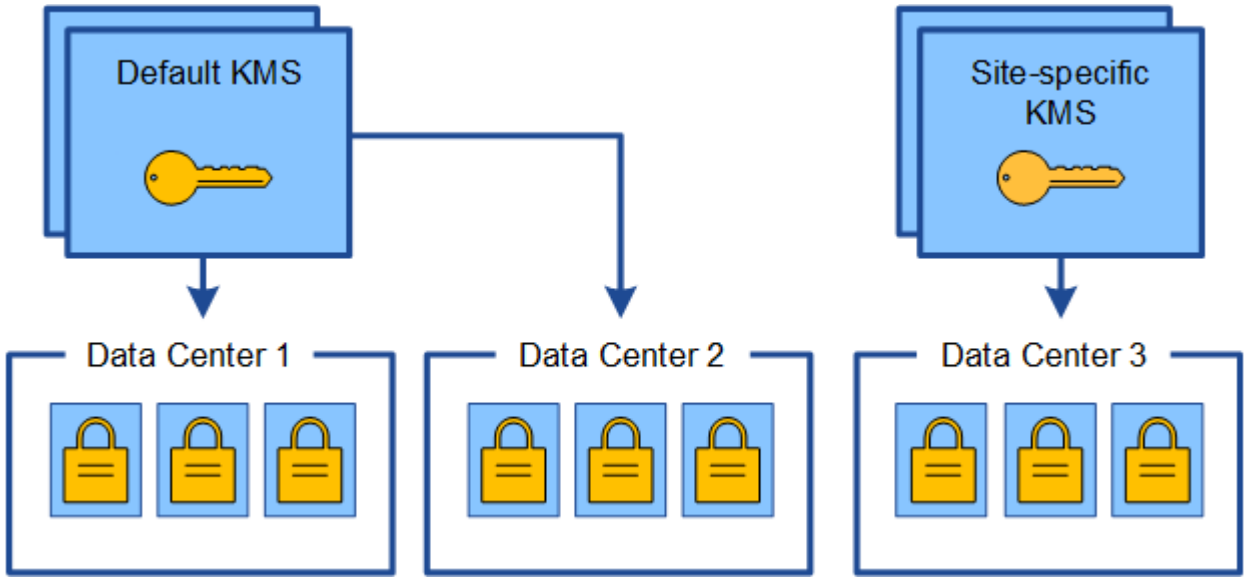


3. 您決定為單一站台新增站台專屬的KMS（圖中的資料中心3）。不過、由於應用裝置節點已加密、因此當您嘗試儲存站台特定KMS的組態時、就會發生驗證錯誤。發生此錯誤的原因是站台特定的KMS沒有正確的金鑰

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。此套用至任何沒有專屬KMS的站台。 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。您不想將預設KMS用於新網站。	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。

關於這項工作

這些指示適用於Thales CSpherTrust Manager k170v、2.0、2.1及2.2版。如果您對使用不同的關鍵管理伺服器StorageGRID 搭配使用方面有任何疑問、請聯絡技術支援部門。

"Thales CiperTrust經理"

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. 從KMS軟體為每個KMS或KMS叢集建立AES加密金鑰。

   加密金鑰必須可匯出。

3. 記錄每個KMS或KMS叢集的下列資訊。

   當您將KMS新增StorageGRID 至原地時、您需要這些資訊。

   - 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。

   KMS中必須已存在加密金鑰。不建立或管理KMS金鑰。StorageGRID

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。

您需要的產品

- 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。

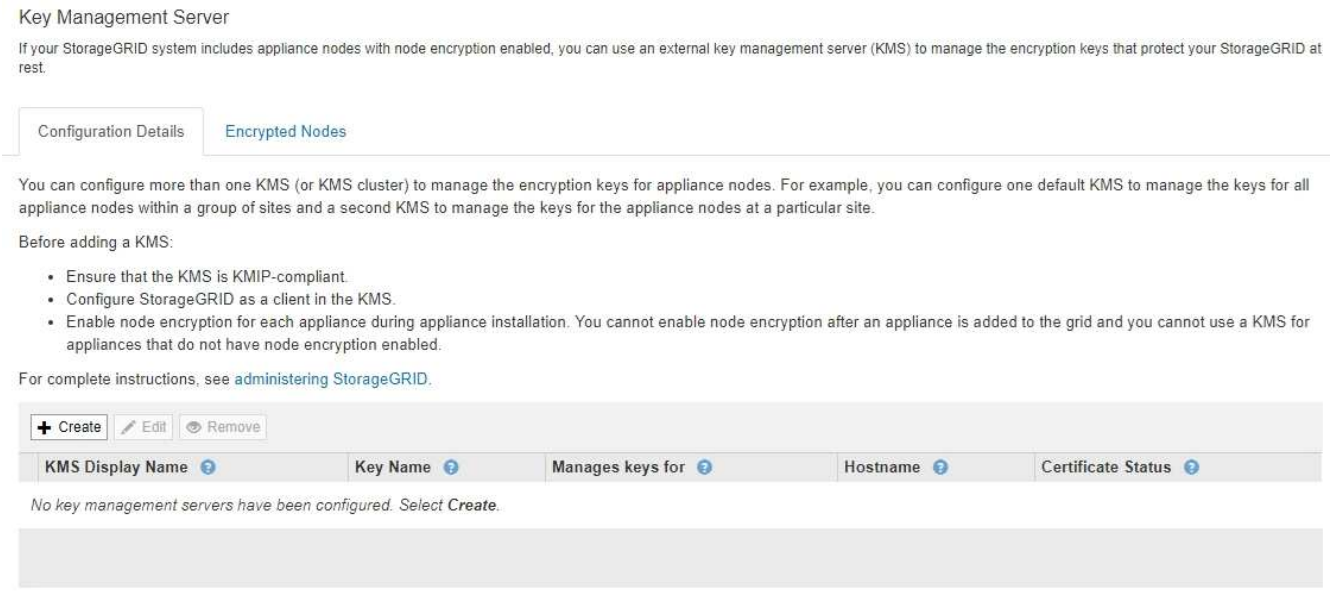
步驟**1**：輸入**KMS**詳細資料

在「新增金鑰管理伺服器」精靈的步驟1（輸入KMS詳細資料）中、您將提供有關KMS或KMS叢集的詳細資料。

步驟

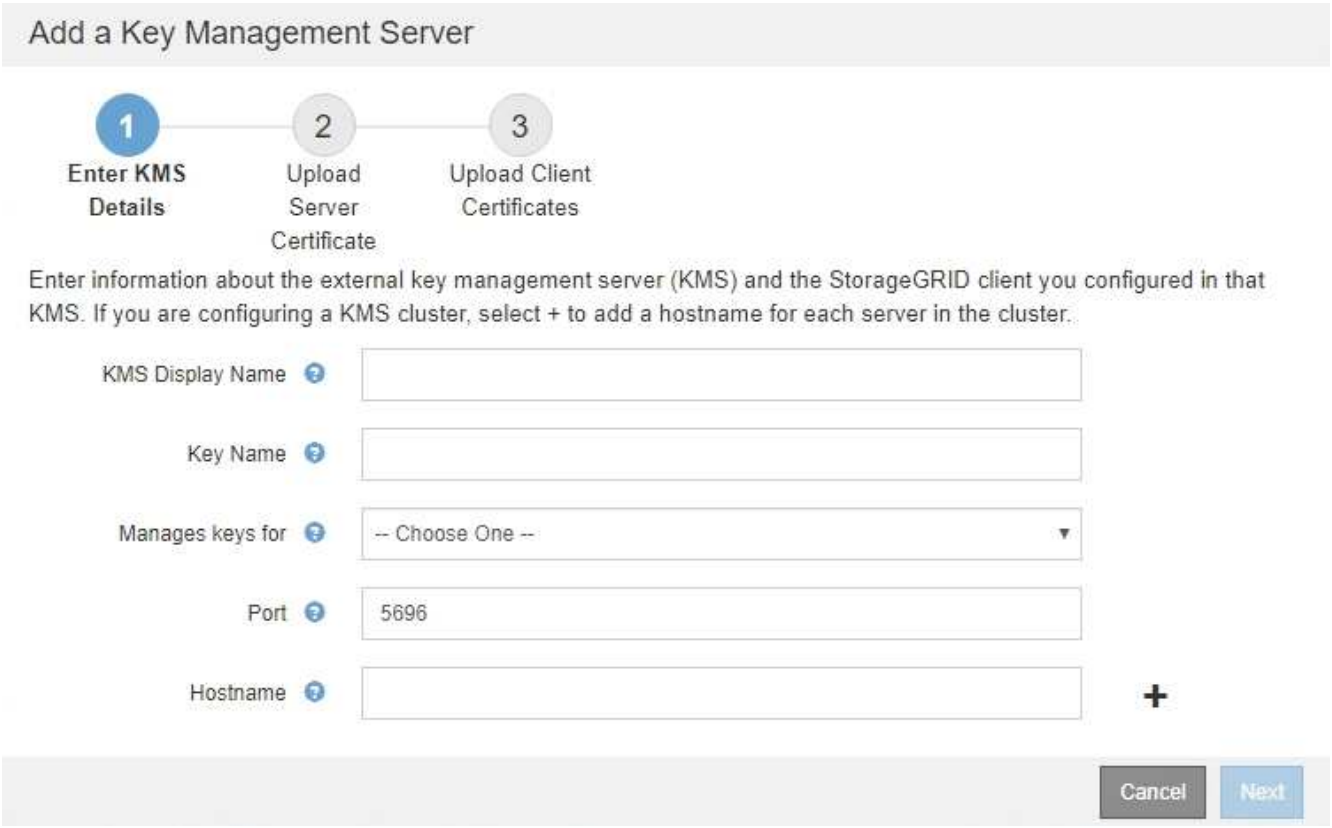
1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   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）。

   此時會出現「Add a Key Management Server（新增金鑰管理伺服器）」精靈的步驟1（輸入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
公里顯示名稱	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。
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管理的站台（預設KMS）*來設定預設KMS、以套用至任何沒有專屬KMS的站台、以及您在後續擴充中新增的任何站台。 *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。 *附註：*伺服器憑證的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。

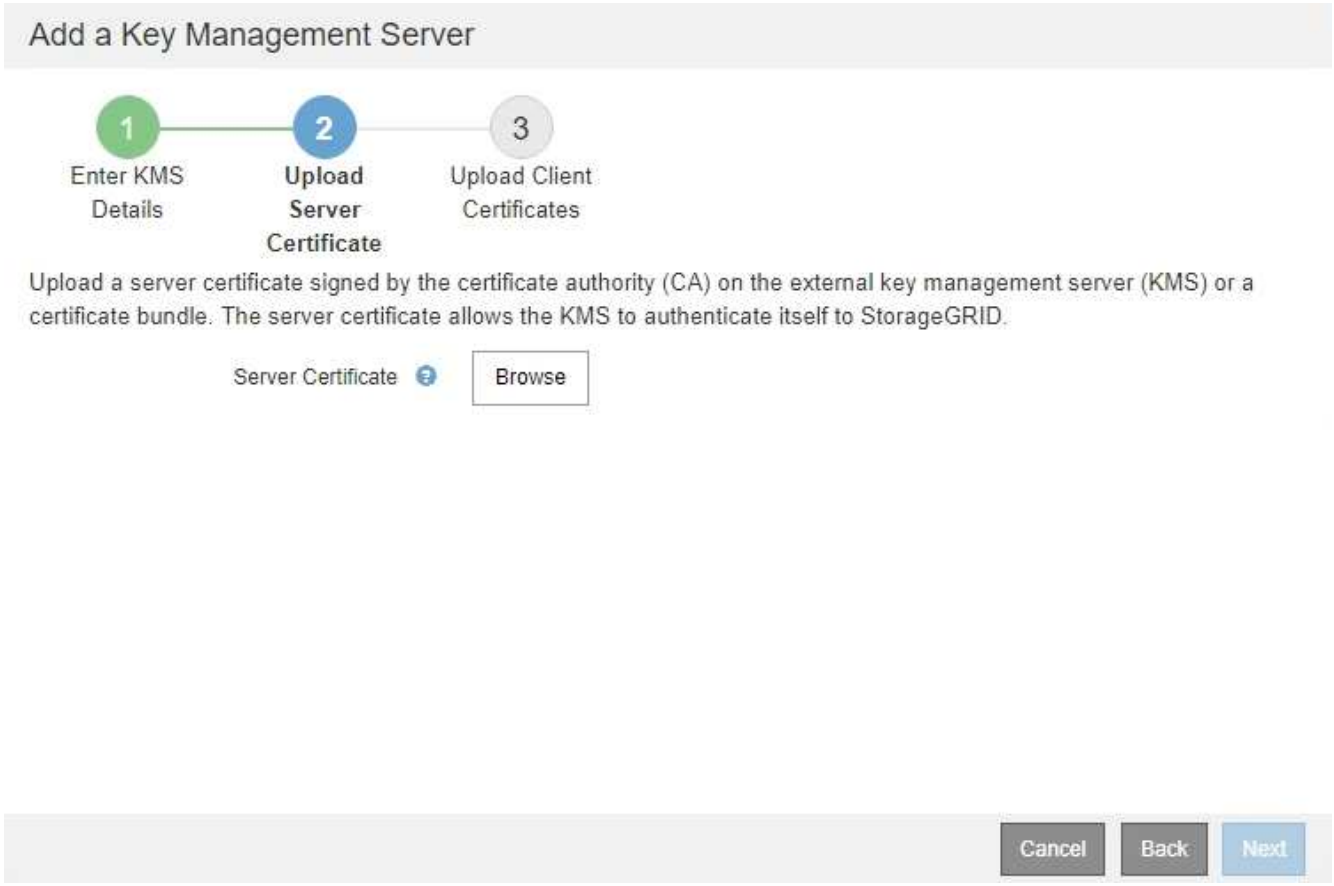
4. 如果您使用KMS叢集、請選取加號 ➕ 為叢集中的每個伺服器新增主機名稱。
5. 選擇*下一步*。

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、您會上傳KMS的伺服器憑證（或憑證套件組合）。伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

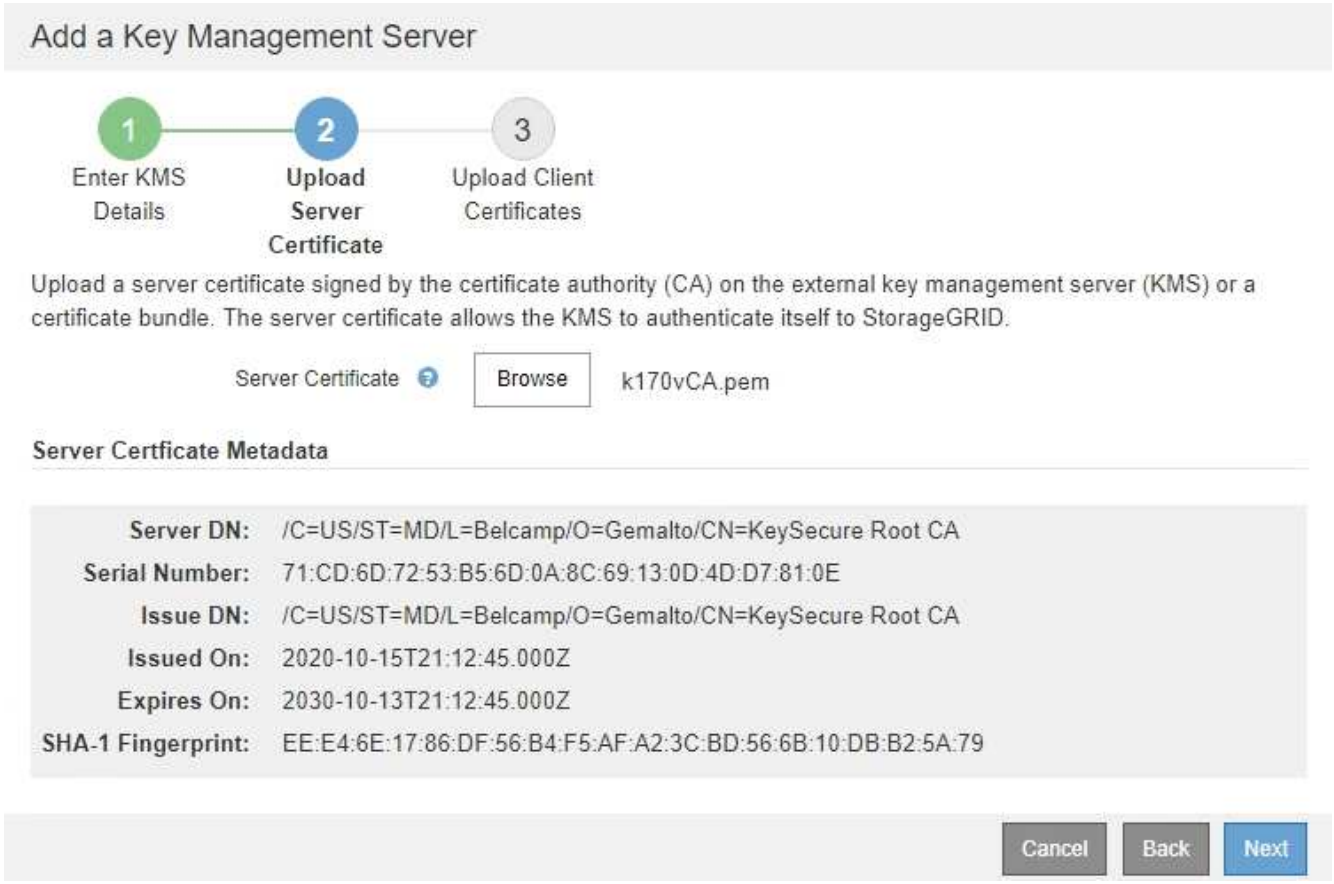
步驟

1. 從*步驟2（上傳伺服器憑證）*瀏覽至儲存的伺服器憑證或憑證套裝組合位置。



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。

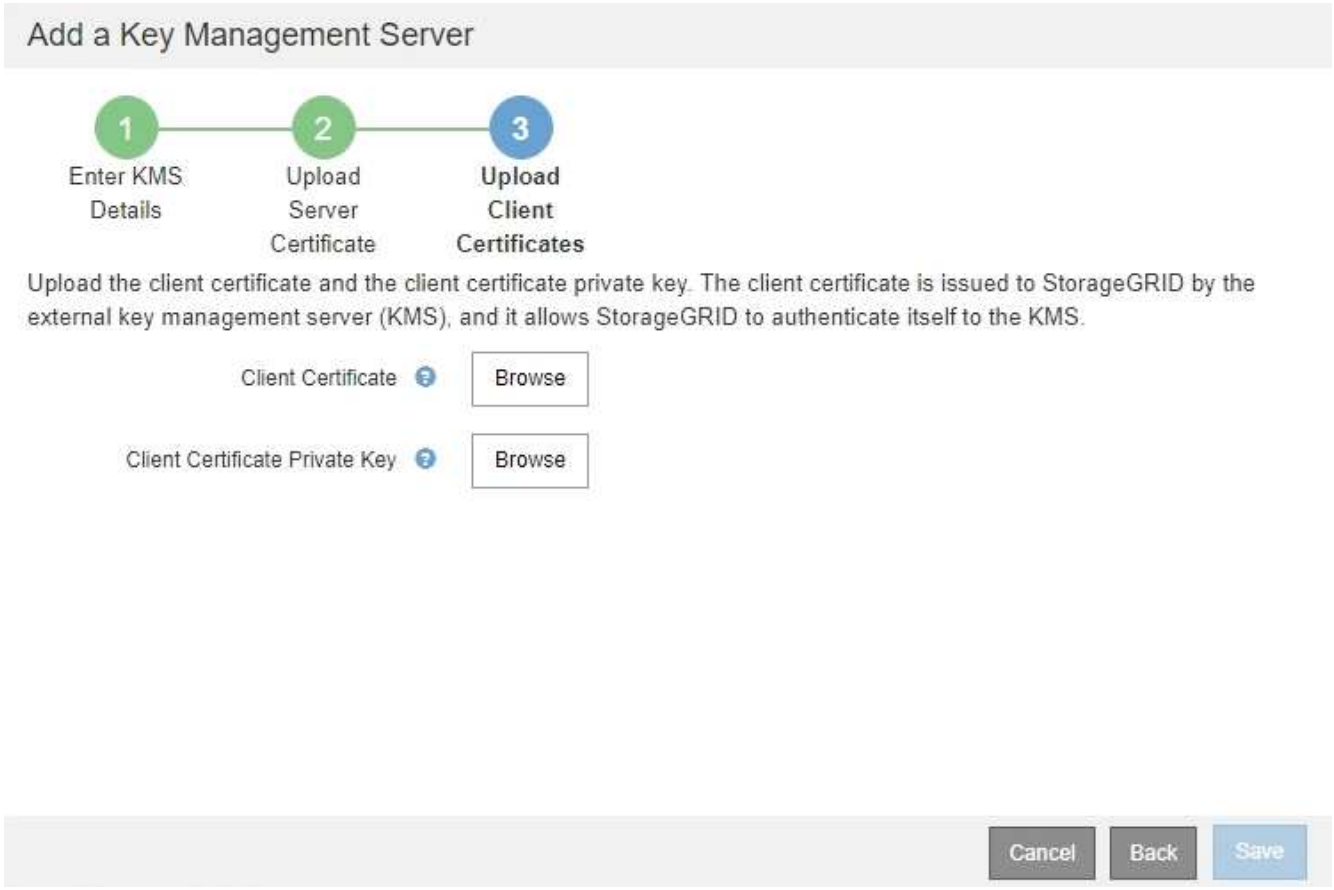
3. 選擇*下一步*。

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、您會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。

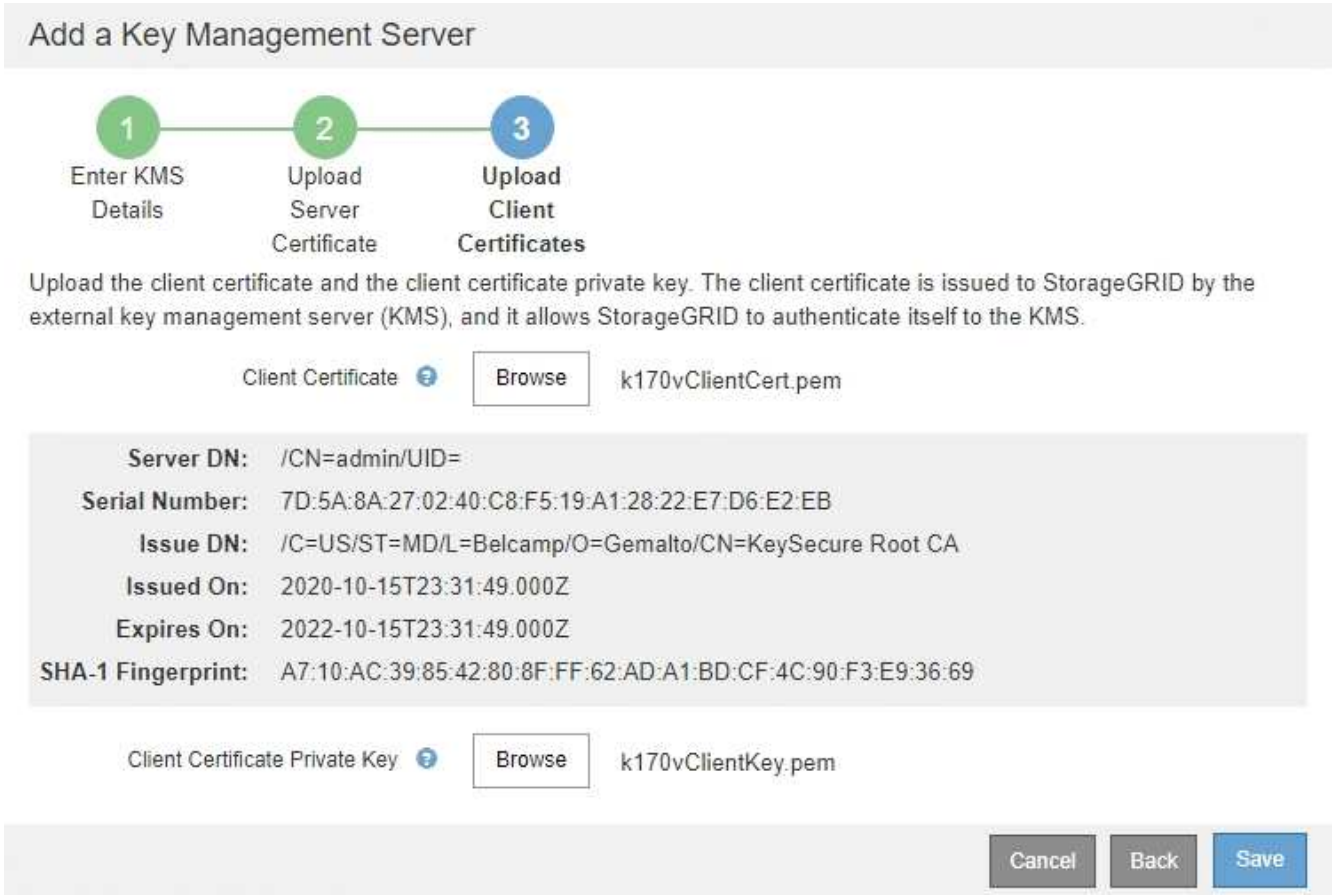


2. 上傳用戶端憑證檔案。

   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。

   此時會顯示用戶端憑證和用戶端憑證私密金鑰的中繼資料。



5. 選擇*保存*。

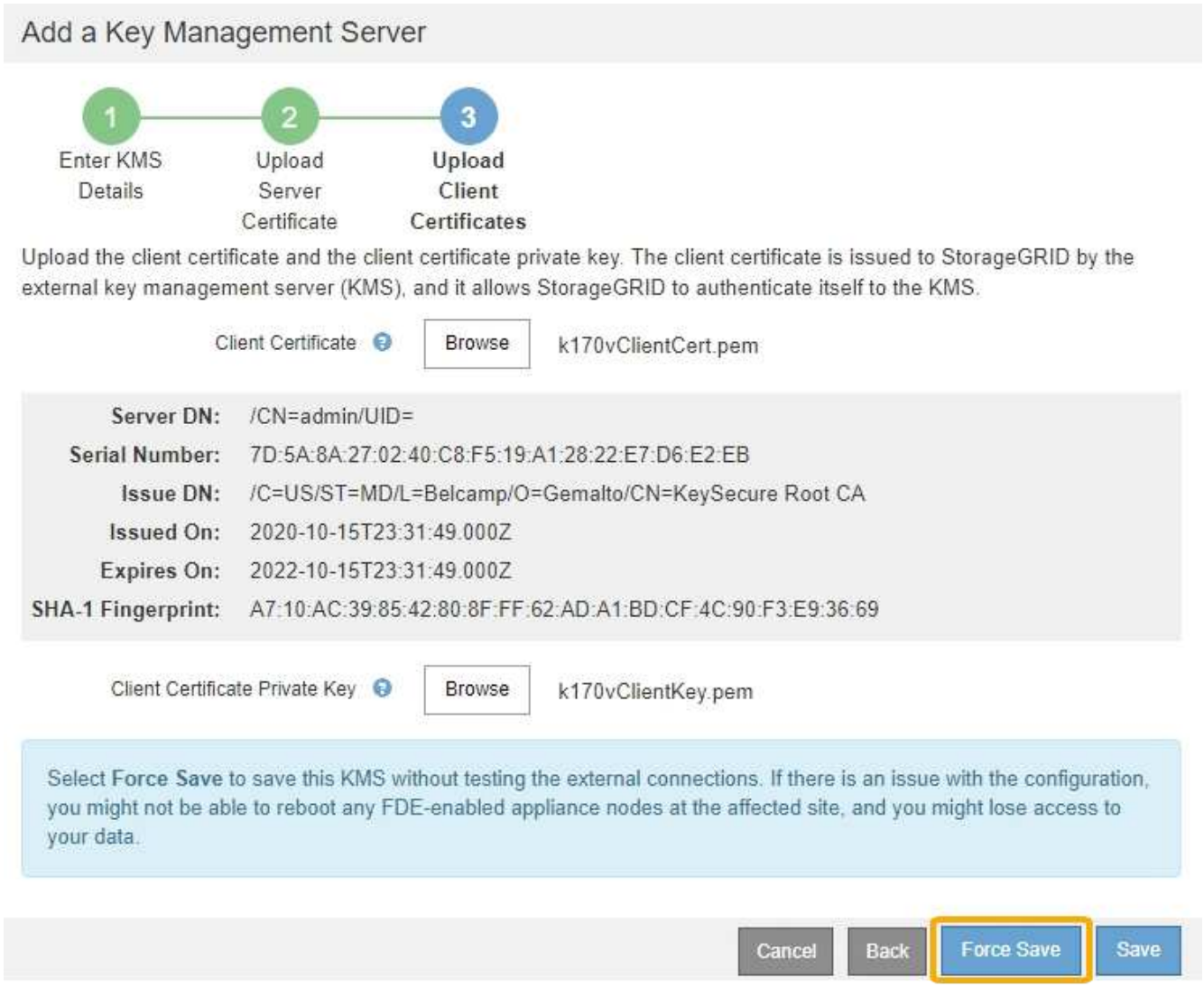
測試金鑰管理伺服器與應用裝置節點之間的連線。如果所有連線都有效、且KMS上找到正確的金鑰、新的金鑰管理伺服器就會新增至金鑰管理伺服器頁面的表格。

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. 如果在選擇*保存*時出現錯誤訊息、請檢閱訊息詳細資料、然後選擇*確定*。

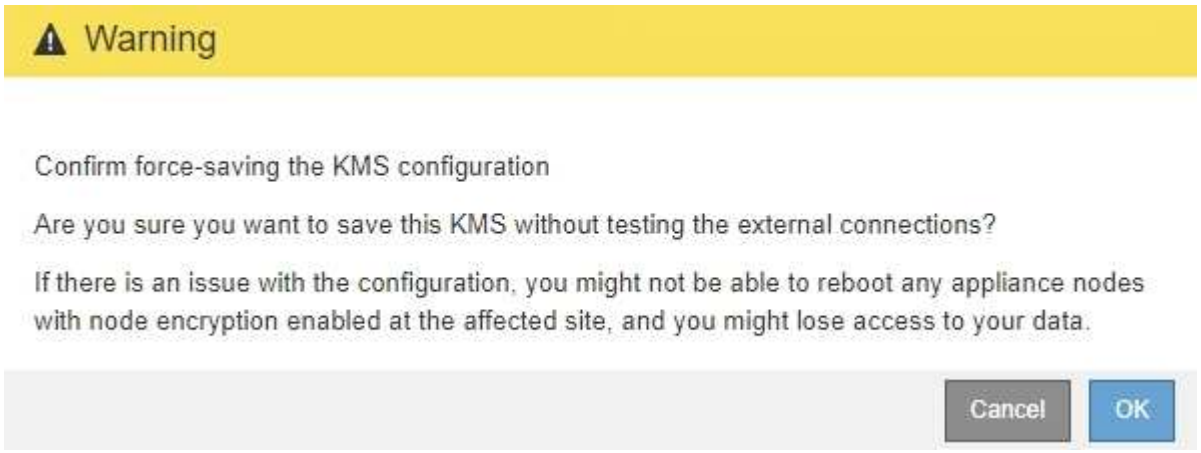
例如、如果連線測試失敗、您可能會收到「無法處理的實體」錯誤。

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、但不會測試每個應用裝置與該KMS之間的外部連線。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。

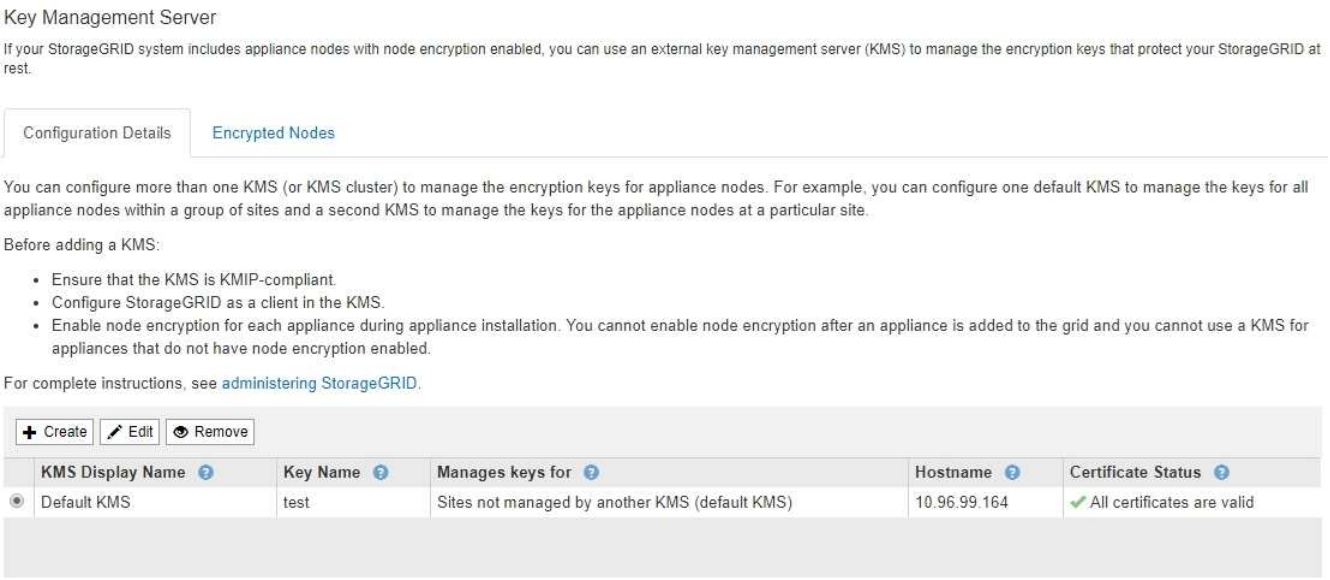
檢視**KMS**詳細資料

您可以檢視StorageGRID 有關您的作業系統中每個金鑰管理伺服器（KMS）的資訊、包括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。「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. 檢閱表格中每個KMS的資訊。

欄位	說明
公里顯示名稱	KMS的描述性名稱。
金鑰名稱	KMS中的核心用戶端別名StorageGRID 。
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）。*

欄位	說明
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和10.10.10.11」或「10.10.10.10和2等」。 若要檢視叢集中的所有主機名稱、請選取KMS、然後選取*編輯*。
憑證狀態	伺服器憑證、選用CA憑證和用戶端憑證的目前狀態：有效、過期、即將到期或不明。 附註： StorageGRID 更新憑證狀態可能需要30分鐘的時間。您必須重新整理網頁瀏覽器、才能查看目前值。

3. 如果「憑證狀態」為「未知」、請等待30分鐘、然後重新整理您的網頁瀏覽器。

> 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、才能查看實際狀態。

4. 如果「憑證狀態」欄指出某個憑證已過期或即將到期、請盡快解決此問題。

請參閱相關說明中有關* KMS CA憑證過期*、* KMS用戶端憑證過期*及* KMS伺服器憑證過期*警示的建議動作 監控StorageGRID 與疑難排解。

> 您必須盡快解決任何憑證問題、才能維持資料存取。

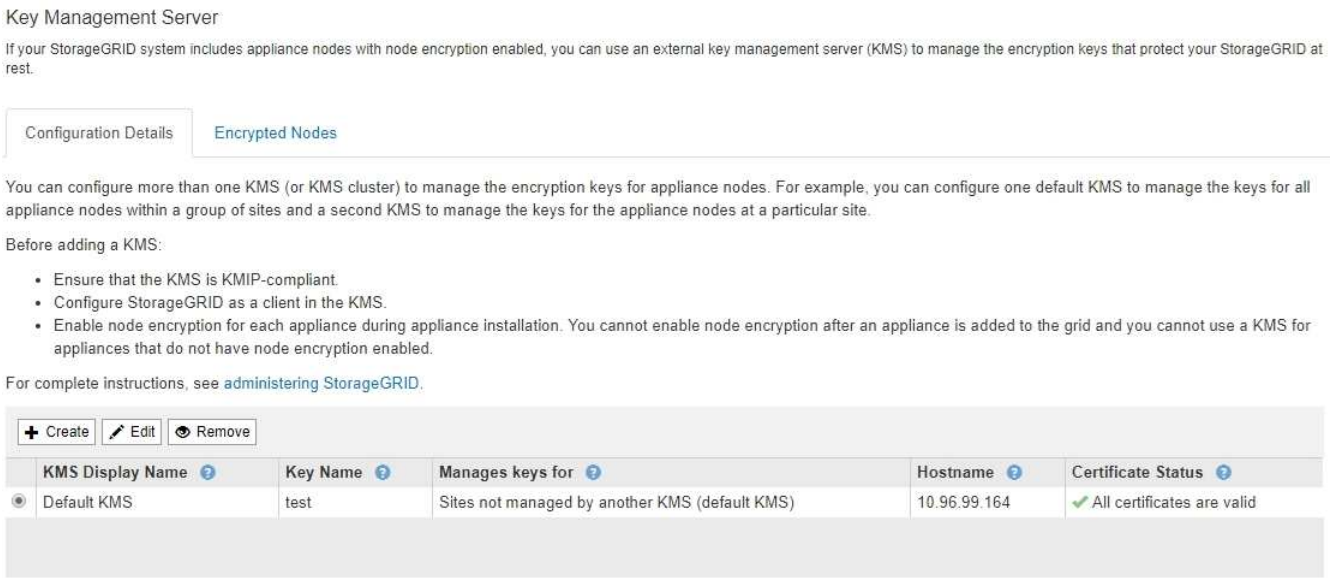
檢視加密節點

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 啟用*節點加密*設定的支援系統中的應用裝置節點。

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

欄位	說明
公里顯示名稱	用於節點的KMS描述性名稱。 如果未列出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。若要檢視完整的金鑰UID、請將游標暫留在儲存格上。 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。 *注意：*您必須重新整理網頁瀏覽器、才能看到新的值。

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

   請參閱的說明中的這些警示建議動作 監控StorageGRID 與疑難排解。

   您必須立即解決任何問題、確保資料受到完整保護。

編輯金鑰管理伺服器（**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。

您需要的產品

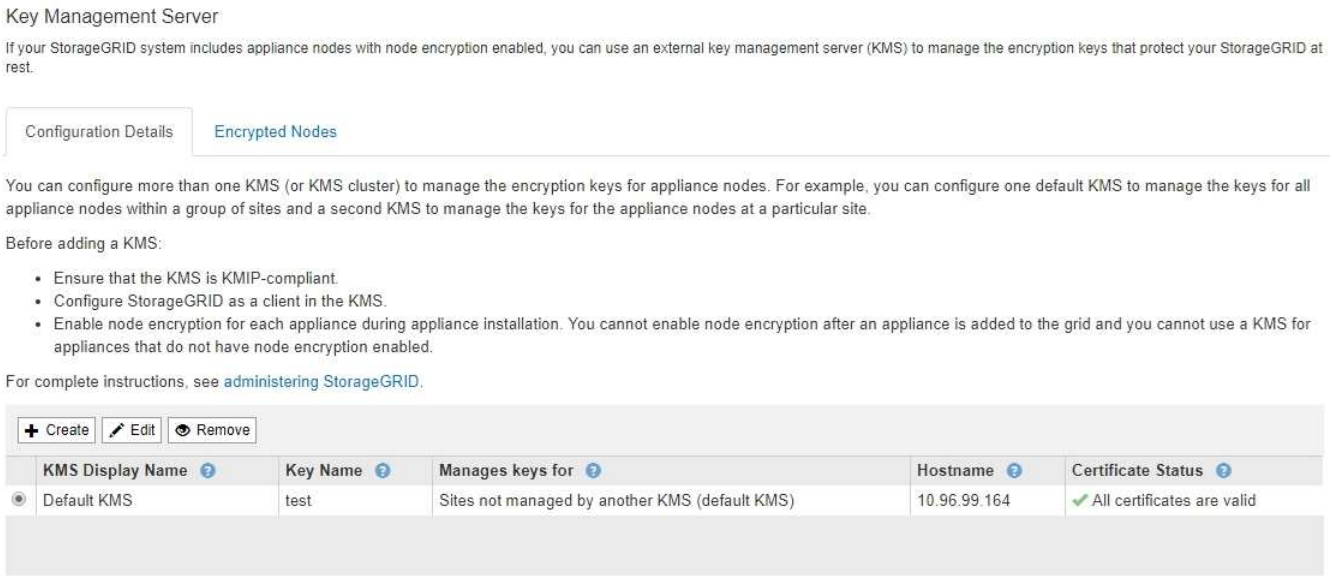
- 您已檢閱 使用金鑰管理伺服器的考量與要求。
- 如果您打算更新選取的KMS網站、則表示您已檢閱 變更網站KMS的考量事項。
- 您將使用登入Grid Manager 支援的網頁瀏覽器。

- 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*。

   「金鑰管理伺服器」頁面隨即出現、並顯示所有已設定的金鑰管理伺服器。



2. 選取您要編輯的KMS、然後選取*編輯*。
3. 您也可以更新編輯金鑰管理伺服器精靈*步驟1（輸入KMS詳細資料）*中的詳細資料。

欄位	說明
公里顯示名稱	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。 切勿嘗試變更KMS的金鑰名稱（別名）來旋轉金鑰。而是更新KMS軟體中的金鑰版本來旋轉金鑰。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。 使用金鑰管理伺服器的考量與要求

欄位	說明
管理的金鑰	如果您正在編輯網站專屬的KMS、但尚未擁有預設的KMS、請選擇*不受其他KMS管理的網站（預設KMS）*。此選項會將站台專屬的KMS轉換成預設KMS、適用於所有沒有專屬KMS的站台、以及任何新增至擴充中的站台。 *注意：*如果您正在編輯站台專屬的KMS、則無法選取其他站台。如果您正在編輯預設KMS、則無法選取特定網站。
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。
主機名稱	KMS的完整網域名稱或IP位址。 *附註：*伺服器憑證的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、請選取加號 ➕ 為叢集中的每個伺服器新增主機名稱。
5. 選擇*下一步*。

   此時會出現「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*下一步*。

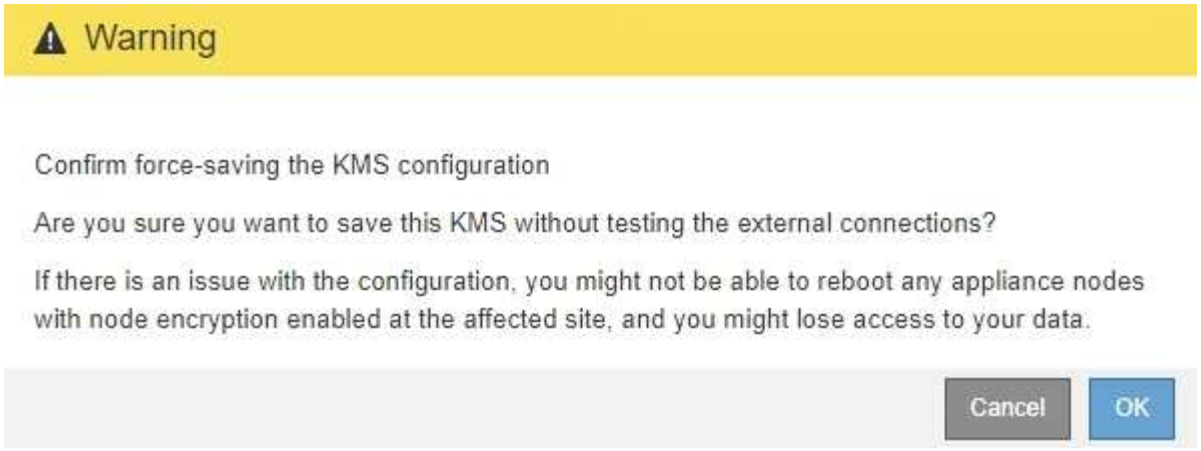
   此時會出現「Edit a Key Management Server（編輯金鑰管理伺服器）」精靈的步驟3（上傳用戶端憑證）。
8. 如果您需要更換用戶端憑證和用戶端憑證私密金鑰、請選取*瀏覽*並上傳新檔案。
9. 選擇*保存*。

   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、但不會測試每個應用裝置與該KMS之間的外部連線。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 *。



系統會儲存KMS組態、但不會測試與KMS的連線。

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。

您需要的產品

- 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

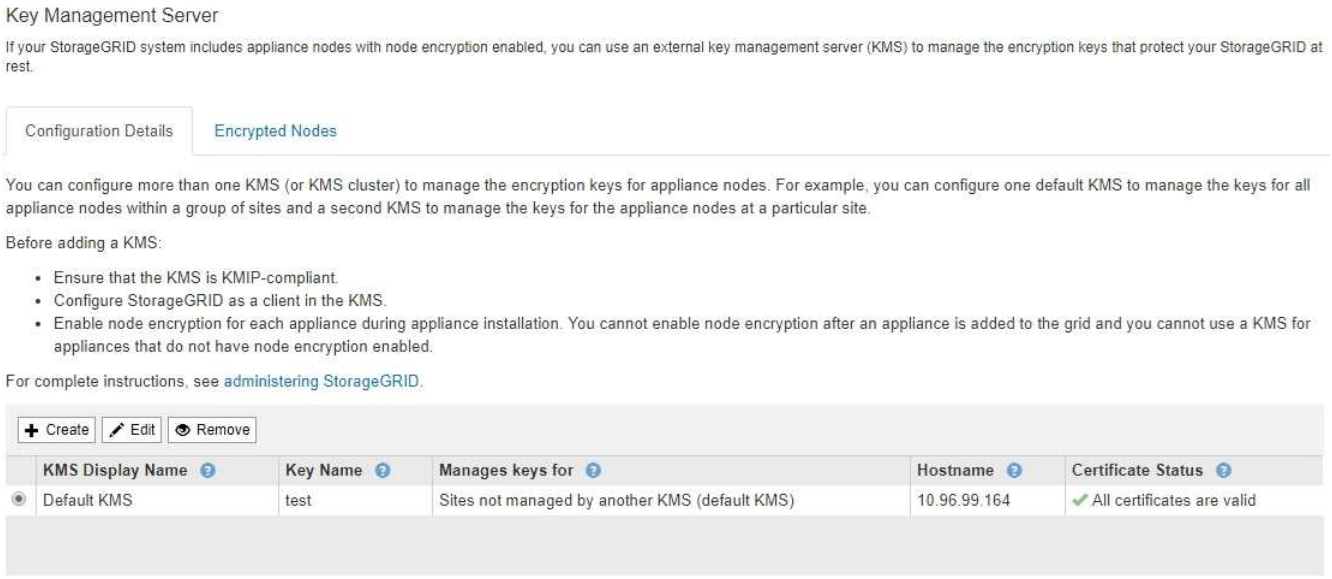
在下列情況下、您可以移除KMS：

- 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。

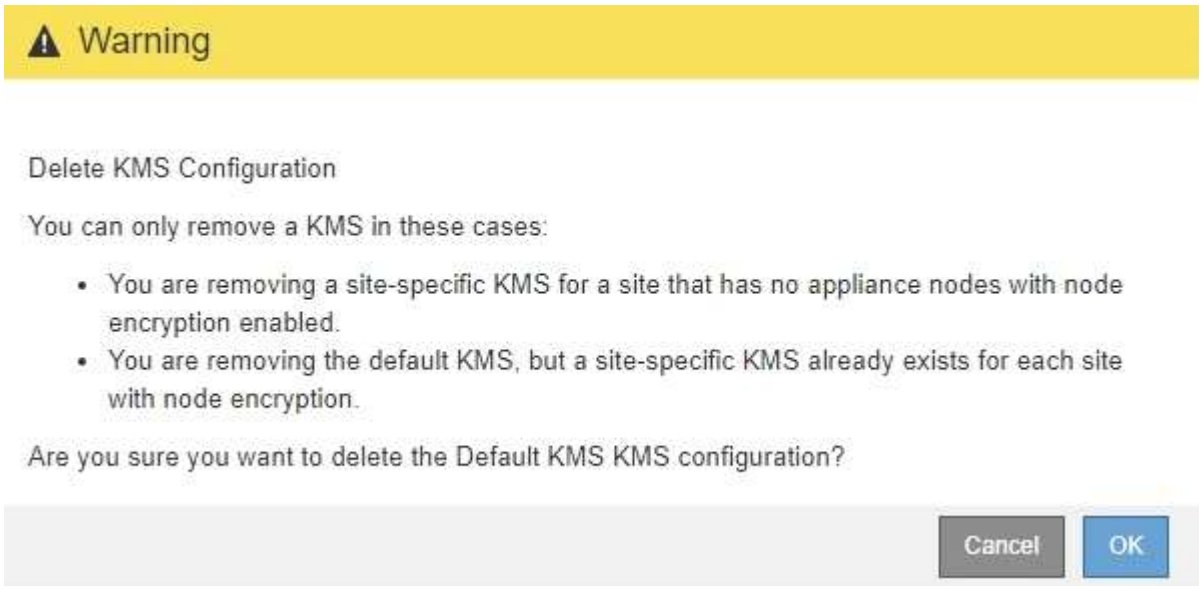
步驟

1. 選擇*組態*>*安全性*>*金鑰管理伺服器*。

   「金鑰管理伺服器」頁面隨即出現、並顯示所有已設定的金鑰管理伺服器。



2. 選取您要移除之KMS的選項按鈕、然後選取*移除*。
3. 檢閱警告對話方塊中的考量事項。



4. 選擇*確定*。

   KMS組態隨即移除。

管理Proxy設定

設定儲存Proxy設定

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。

您需要的產品

- 您擁有特定的存取權限。
- 您將使用登入Grid Manager 支援的網頁瀏覽器。

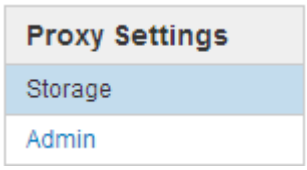
關於這項工作

您可以設定單一儲存Proxy的設定。

步驟

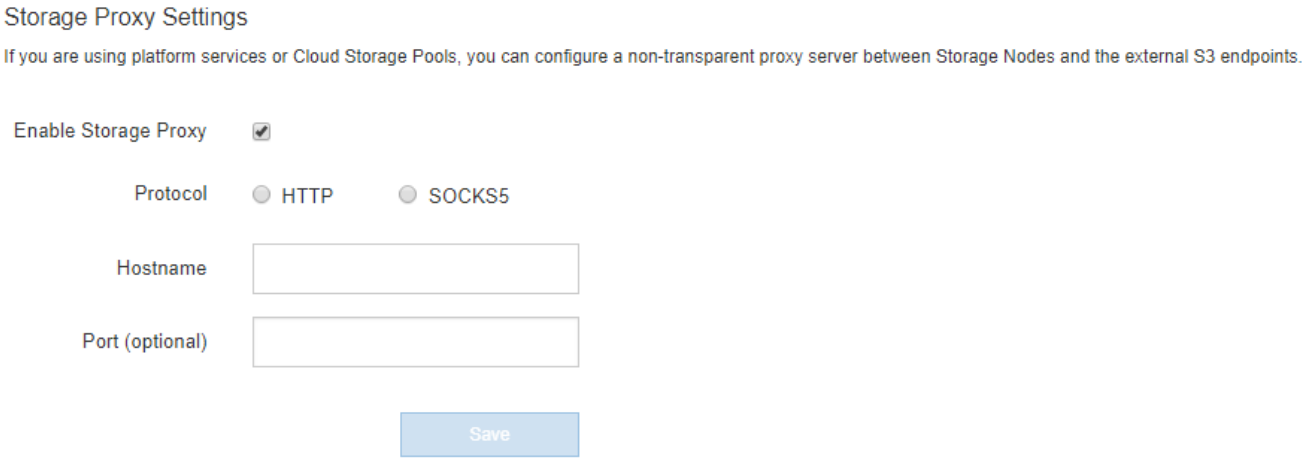
1. 選擇*組態*>*安全性*>* Proxy設定*。

   此時會出現「儲存Proxy設定」頁面。預設會在側邊列功能表中選取* Storage *。



2. 選取*啟用儲存Proxy *核取方塊。

   此時會顯示用於設定儲存Proxy的欄位。



3. 選取不透明儲存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。

   如果您使用傳輸協定的預設連接埠：HTTP為80、SOCKS5為1080、則可將此欄位留白。

6. 選擇*保存*。

   儲存Proxy之後、即可設定及測試平台服務或雲端儲存資源池的新端點。

   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。

完成後

如果您需要停用儲存Proxy、請取消選取「啟用儲存**Proxy**」核取方塊、然後選取「*儲存」。

相關資訊

- 平台服務的網路和連接埠
- 使用ILM管理物件

設定管理**Proxy**設定

如果您使用AutoSupport HTTP或HTTPS傳送不實訊息（請參閱 設定AutoSupport 功能）、您可以在管理節點和技術支援AutoSupport （例如、）之間設定不透明的Proxy伺服器。

您需要的產品

- 您擁有特定的存取權限。
- 您將使用登入Grid Manager 支援的網頁瀏覽器。

關於這項工作

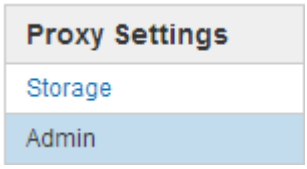
您可以設定單一管理Proxy的設定。

步驟

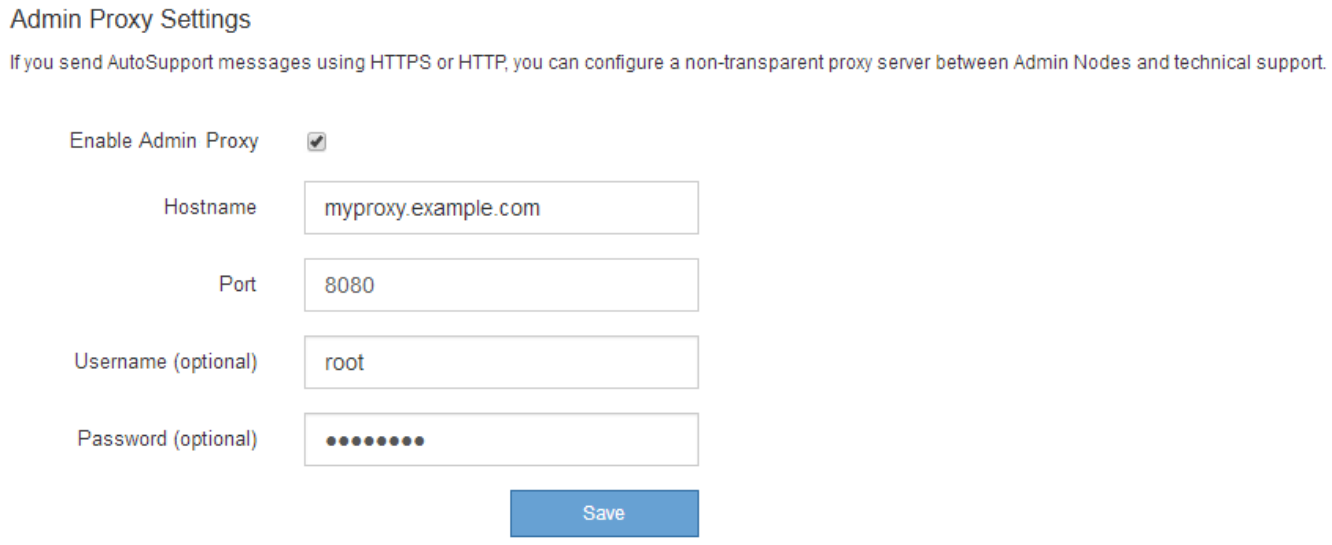
1. 選擇*組態*>*安全性*>* Proxy設定*。

   此時會出現「管理Proxy設定」頁面。預設會在側邊列功能表中選取* Storage *。

2. 從側欄功能表中、選取*管理*。



3. 選中*啓用管理代理*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. 或者、輸入Proxy使用者名稱。

   如果您的Proxy伺服器不需要使用者名稱、請將此欄位留白。

7. 或者、輸入Proxy密碼。

   如果您的Proxy伺服器不需要密碼、請將此欄位留白。

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Proxy、請取消選取*啟用管理Proxy 核取方塊、然後選取*儲存。

管理不受信任的用戶端網路

管理不受信任的用戶端網路：總覽

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StorageGRID 根據預設、不信任所有可用外部連接埠上每個網格節點的傳入連線（請參閱中的外部通訊資訊 網路準則）。

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。

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、在連接埠443上設定S3 over HTTPS的負載平衡器端點。
2. 在「不受信任的用戶端網路」頁面中、指定閘道節點上的用戶端網路不受信任。

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傳出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：

- 在「不受信任的用戶端網路」頁面中、指出儲存節點上的用戶端網路不受信任。

儲存組態之後、儲存節點不再接受用戶端網路上的任何傳入流量、而是繼續允許傳出要求至Amazon Web

Services。

指定節點的用戶端網路不受信任

如果您使用的是用戶端網路、則可以指定每個節點的用戶端網路是否受信任或不受信任。您也可以為新增至擴充中的新節點指定預設設定。

您需要的產品

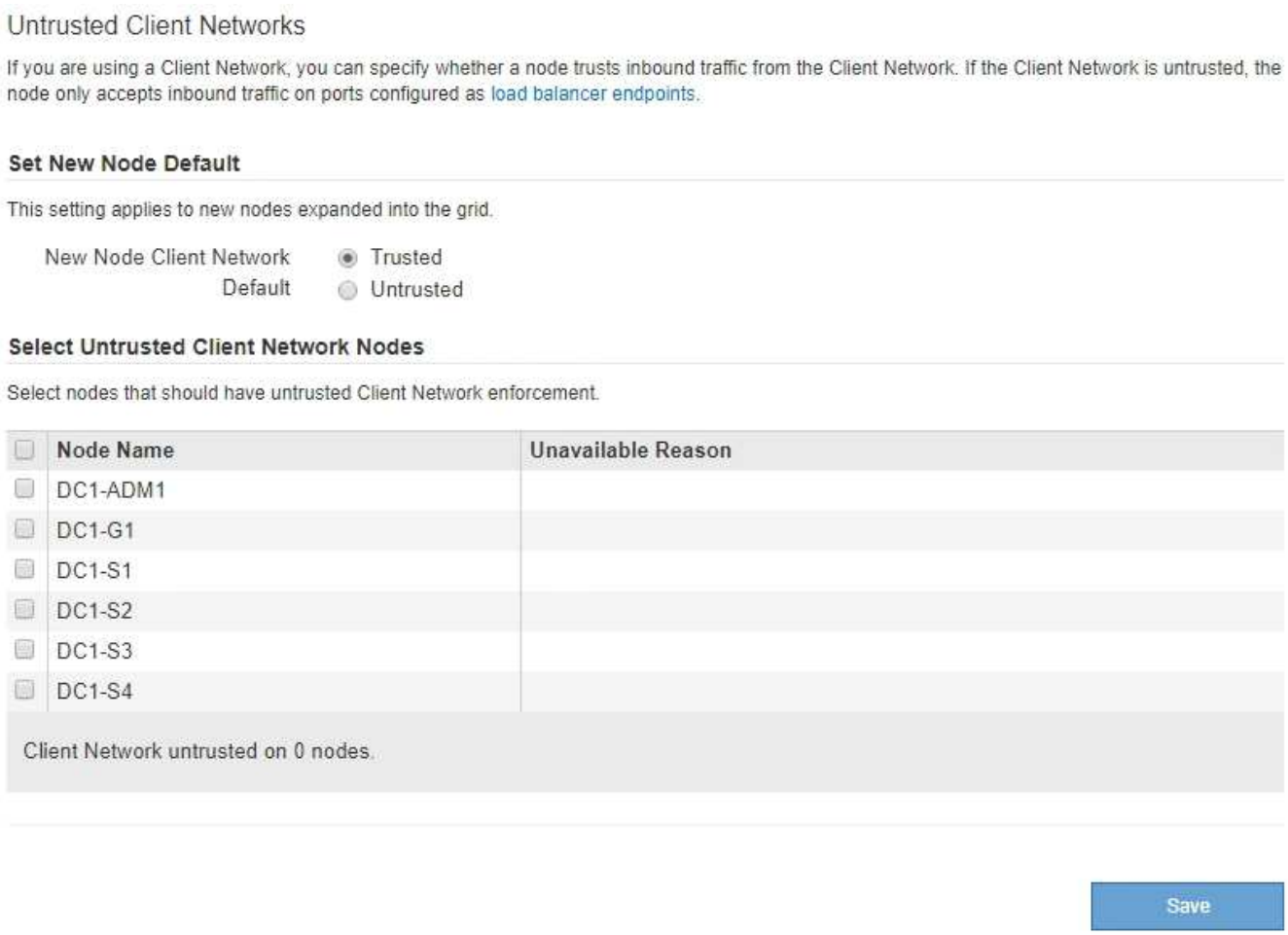
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有root存取權限。
- 如果您希望管理節點或閘道節點僅接受明確設定的端點上的傳入流量、則表示您已定義負載平衡器端點。

> 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。

步驟

1. 選擇*組態*>*安全性*>*不受信任的用戶端網路*。

   「不受信任的用戶端網路」頁面會列出StorageGRID 您的整個作業系統中的所有節點。如果節點上的用戶端網路必須信任、則「不可用原因」欄會包含一個項目。



2. 在「設定新節點預設」區段中、指定在擴充程序中將新節點新增至網格時、應採用的預設設定。

- 信任：在擴充中新增節點時、其用戶端網路是受信任的。
- 不受信任：在擴充中新增節點時、其用戶端網路不受信任。您可以視需要返回此頁面、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. 在「選取不受信任的用戶端網路節點」區段中、選取只允許用戶端連線到明確設定的負載平衡器端點的節點。

   您可以選取或取消選取標題中的核取方塊、以選取或取消選取所有節點。

4. 選擇*保存*。

   新的防火牆規則會立即新增並強制執行。如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

管理租戶

管理租戶

身為網格管理員、您可以建立及管理S3和Swift用戶端用來儲存及擷取物件、監控儲存使用量、以及管理用戶端使用StorageGRID 您的作業系統所能執行的動作的租戶帳戶。

什麼是租戶帳戶？

租戶帳戶可讓使用簡易儲存服務（S3）REST API或Swift REST API的用戶端應用程式、將物件儲存及擷取StorageGRID 到無法使用的物件上。

每個租戶帳戶都支援使用單一傳輸協定、您可以在建立帳戶時指定。若要使用StorageGRID 這兩種通訊協定將物件儲存並擷取至某個支援系統、您必須建立兩個租戶帳戶：一個用於S3儲存區和物件、另一個用於Swift容器和物件。每個租戶帳戶都有自己的帳戶ID、授權群組和使用者、儲存區或容器、以及物件。

或者、如果您想要將儲存在系統上的物件依不同實體分隔、您也可以建立其他租戶帳戶。例如、您可以在下列任一使用案例中設定多個租戶帳戶：

- *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、只要使用S3儲存區和儲存區原則、即可在企業的各部門之間隔離物件。您不需要使用租戶帳戶。如需詳細資訊、請參閱實作S3用戶端應用程式的指示。

- *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。

建立及設定租戶帳戶

建立租戶帳戶時、請指定下列資訊：

- 顯示租戶帳戶的名稱。
- 租戶帳戶（S3或Swift）將使用哪種用戶端傳輸協定。
- 對於S3租戶帳戶：租戶帳戶是否有權使用S3時段的平台服務。如果您允許租戶帳戶使用平台服務、則必須確保網格已設定為支援其使用。請參閱「老舊平台服務」。
- 或者、租戶帳戶的儲存配額、也就是租戶物件可用的GB、TB或PB上限。如果超過配額、租戶就無法建立新物件。

> 租戶的儲存配額代表邏輯容量（物件大小）、而非實體容量（磁碟大小）。

- 如果啟用StorageGRID 身分識別聯盟以供支援整個系統、則哪個聯盟群組具有root存取權限、可設定租戶帳戶。
- 如果StorageGRID 不使用單一登入（SSO）進行支援、則租戶帳戶是使用自己的身分識別來源、還是共用網格的身分識別來源、以及租戶本機root使用者的初始密碼。

建立租戶帳戶之後、您可以執行下列工作：

- 管理網格平台服務：如果您為租戶帳戶啟用平台服務、請確保您瞭解平台服務訊息的傳遞方式、以及StorageGRID 使用平台服務在您的支援範圍內的網路需求。
- 監控租戶帳戶的儲存使用量：租戶開始使用其帳戶之後、您可以使用Grid Manager來監控每個租戶使用的儲存量。

> 如果節點與網格中的其他節點隔離、則租戶的儲存使用量值可能會過期。當網路連線恢復時、總計將會更新。

  如果您已為租戶設定配額、您可以啟用*租戶配額使用量高*警示、以判斷租戶是否正在使用配額。如果啟用、當租戶使用90%的配額時、就會觸發此警示。如需詳細資訊、請參閱監控StorageGRID 和疑難排解功能的說明中的警示參考資料。

- 設定用戶端作業：您可以設定是否禁止某些類型的用戶端作業。

設定**S3**租戶

建立S3租戶帳戶之後、租戶使用者就能存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、並建立本機群組和使用者
- 管理S3存取金鑰
- 建立及管理S3儲存區
- 監控儲存使用量
- 使用平台服務（若已啟用）

> S3租戶使用者可以使用租戶管理程式來建立及管理S3存取金鑰和儲存區、但必須使用S3用戶端應用程式來擷取和管理物件。

設定**Swift**租戶

建立Swift租戶帳戶之後、租戶的root使用者就能存取租戶管理程式來執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）、以及建立本機群組和使用者
- 監控儲存使用量

> 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。

相關資訊

使用租戶帳戶

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。

當您建立租戶帳戶時、可以指定名稱、用戶端傳輸協定及儲存配額（選用）。如果啟用StorageGRID 單一登入（SSO）來執行功能、您也可以指定哪個聯盟群組具有root存取權限來設定租戶帳戶。如果StorageGRID 不使用單一登入、您也必須指定租戶帳戶是否會使用自己的身分識別來源、並為租戶的本機root使用者設定初始密碼。

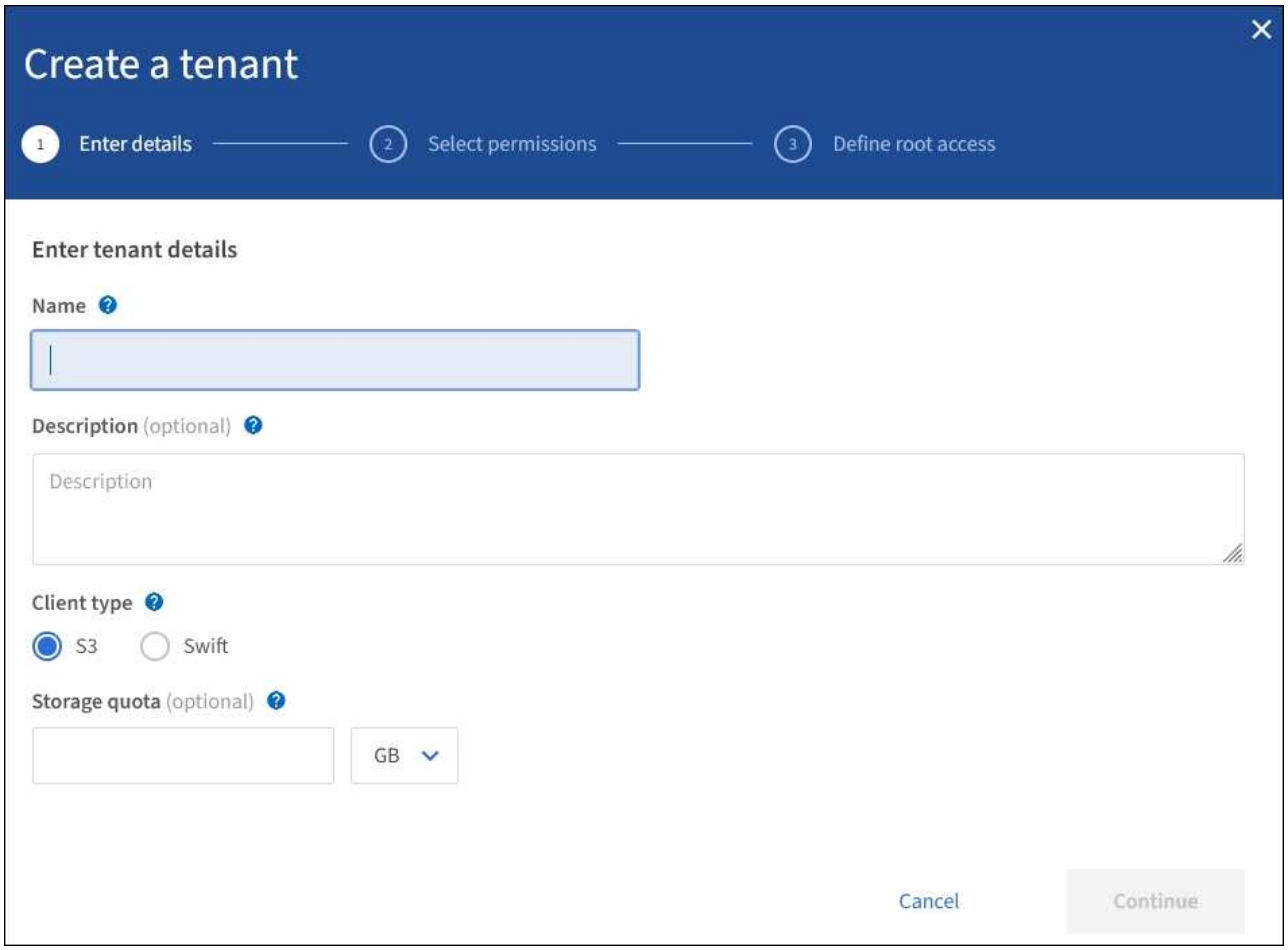
Grid Manager提供精靈、可引導您完成建立租戶帳戶的步驟。這些步驟會因是否有所不同而有所差異 身分識別聯盟 和 單一登入 已設定、以及您用來建立租戶帳戶的Grid Manager帳戶是否屬於具有root存取權限的管理群組。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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。您不需要將任何Grid Manager權限指派給此管理群組。請參閱 管理管理群組的指示。

步驟

1. 選取*租戶*。
2. 選取*「Create」（建立）*、然後輸入租戶的下列資訊：
   a. 名稱：輸入租戶帳戶的名稱。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。
   b. 說明（選用）：輸入有助於識別租戶的說明。
   c. 用戶端類型：選取* S2*或* Swift的用戶端類型。
   d. 儲存配額（選用）：如果您想要此租戶擁有儲存配額、請輸入配額的數值、然後選取正確的單位（GB、TB或PB）。



3. 選擇*繼續*並設定S3或Swift租戶。

S3租戶

為租戶選取適當的權限。其中有些權限有額外的需求。如需詳細資料、請參閱每項權限的線上說明。

- 允許平台服務
- 使用自己的身分識別來源（僅在未使用SSO時才可選取）
- 允許S3選取（請參閱 管理用戶帳戶的S3 Select）

Swift租戶

如果租戶將使用自己的身分識別來源、請選取*使用自己的身分識別來源*（僅在未使用SSO時才可選取）。

1. 選取*繼續*並定義租戶帳戶的root存取權。

未設定身分識別聯盟

1. 輸入本機root使用者的密碼。
2. 選取*建立租戶*。

SSO已啟用

啟用SSO StorageGRID 以供執行功能時、租戶必須使用為Grid Manager設定的身分識別來源。沒有本機使用者可以登入。您可以指定哪個同盟群組具有根存取權限、以設定租戶帳戶。

1. 從Grid Manager中選取現有的聯盟群組、即可擁有租戶的初始根存取權限。

   如果您有足夠的權限、則選取欄位時、會列出Grid Manager中現有的聯盟群組。否則、請輸入群組的唯一名稱。

2. 選取*建立租戶*。

未啟用**SSO**

1. 根據租戶是否要管理自己的群組和使用者、或使用為Grid Manager設定的身分識別來源、完成表格中所述的步驟。

如果租戶將...	執行此動作...
管理自己的群組和使用者	a. 選擇*使用自己的身分識別來源*。 附註：如果選取此核取方塊、而您想要將身分識別聯盟用於租戶群組和使用者、則租戶必須設定自己的身分識別來源。請參閱 租戶帳戶使用說明。 b. 為租戶的本機root使用者指定密碼、然後選取*建立租戶*。 c. 選取*以root登入*來設定租戶、或選取* Finish *來稍後設定租戶。
使用為Grid Manager設定的群組和使用者	a. 請執行下列任一或兩項操作： ◦ 從Grid Manager中選取一個現有的聯盟群組、該群組應具有租戶的初始根存取權限。 附註：如果您有足夠的權限、則選取欄位時、會列出Grid Manager中現有的聯盟群組。否則、請輸入群組的唯一名稱。 ◦ 為租戶的本機root使用者指定密碼。 b. 選取*建立租戶*。

1. 若要立即登入租戶：

   ◦ 如果您在受限連接埠上存取Grid Manager、請在Tenant表格中選取*受限*、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*/`

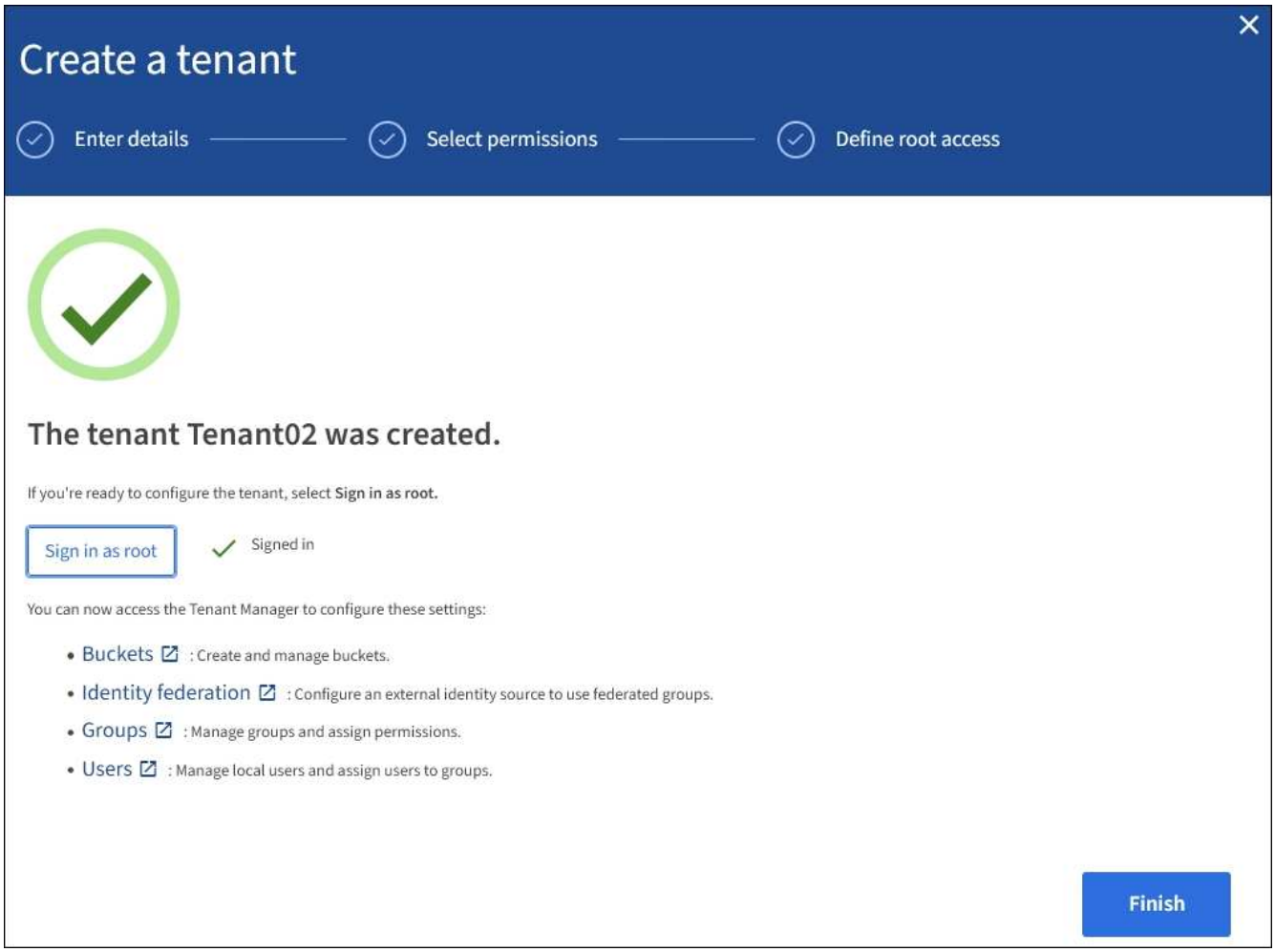
- 「_FQDN」或「管理節點」是管理節點的完整網域名稱或IP位址
- 「*port*」是租戶專用的連接埠
- 「20位數帳戶ID」是租戶的唯一帳戶ID

◦ 如果您在連接埠443上存取Grid Manager、但未設定本機根使用者的密碼、請在Grid Manager的租戶表格中選取*登入*、然後在根存取聯盟群組中輸入使用者的認證資料。

◦ 如果您在連接埠443上存取Grid Manager、並為本機root使用者設定密碼：

i. 選取*以root登入*以立即設定租戶。

當您登入時、會顯示用於設定儲存區或容器、身分識別聯盟、群組和使用者的連結。



i. 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。

ii. 否則、請選取*完成*以稍後存取租戶。

2. 若要稍後存取租戶：

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」或「管理節點」是管理節點的完整網域名稱或IP位址 ◦ 「20位數帳戶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」或「管理節點」是管理節點的完整網域名稱或IP位址 ◦ 「*port*」是僅限租戶的受限連接埠 ◦ 「20位數帳戶ID」是租戶的唯一帳戶ID

相關資訊

- 透過防火牆控制存取
- 管理S3租戶帳戶的平台服務

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。

您需要的產品

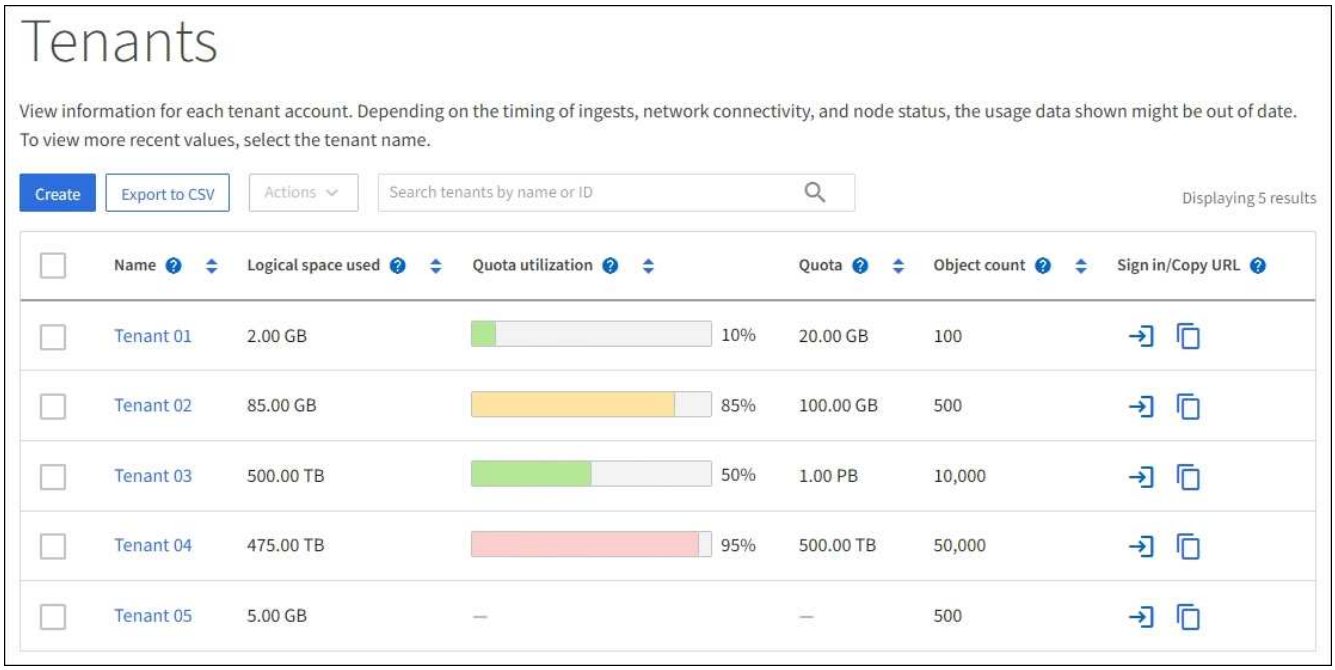
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

如果StorageGRID 您的作業系統啟用單一登入（SSO）、則本機root使用者無法登入租戶帳戶。若要執行root使用者工作、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. 選取您要編輯的租戶帳戶。

   「動作」按鈕隨即啟用。

3. 從「動作」下拉式清單中、選取「變更**root**密碼」。
4. 輸入租戶帳戶的新密碼。
5. 選擇*保存*。

編輯租戶帳戶

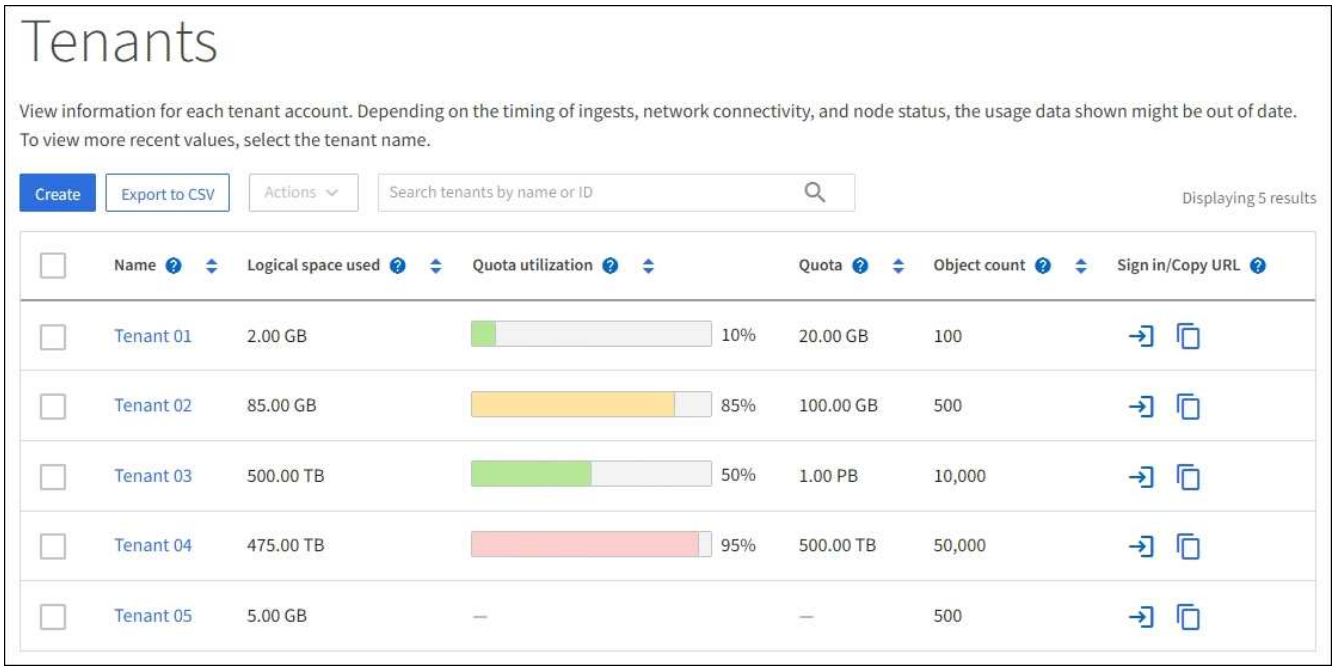
您可以編輯租戶帳戶以變更顯示名稱、變更身分識別來源設定、允許或禁止平台服務、或輸入儲存配額。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

步驟

1. 選取*租戶*。

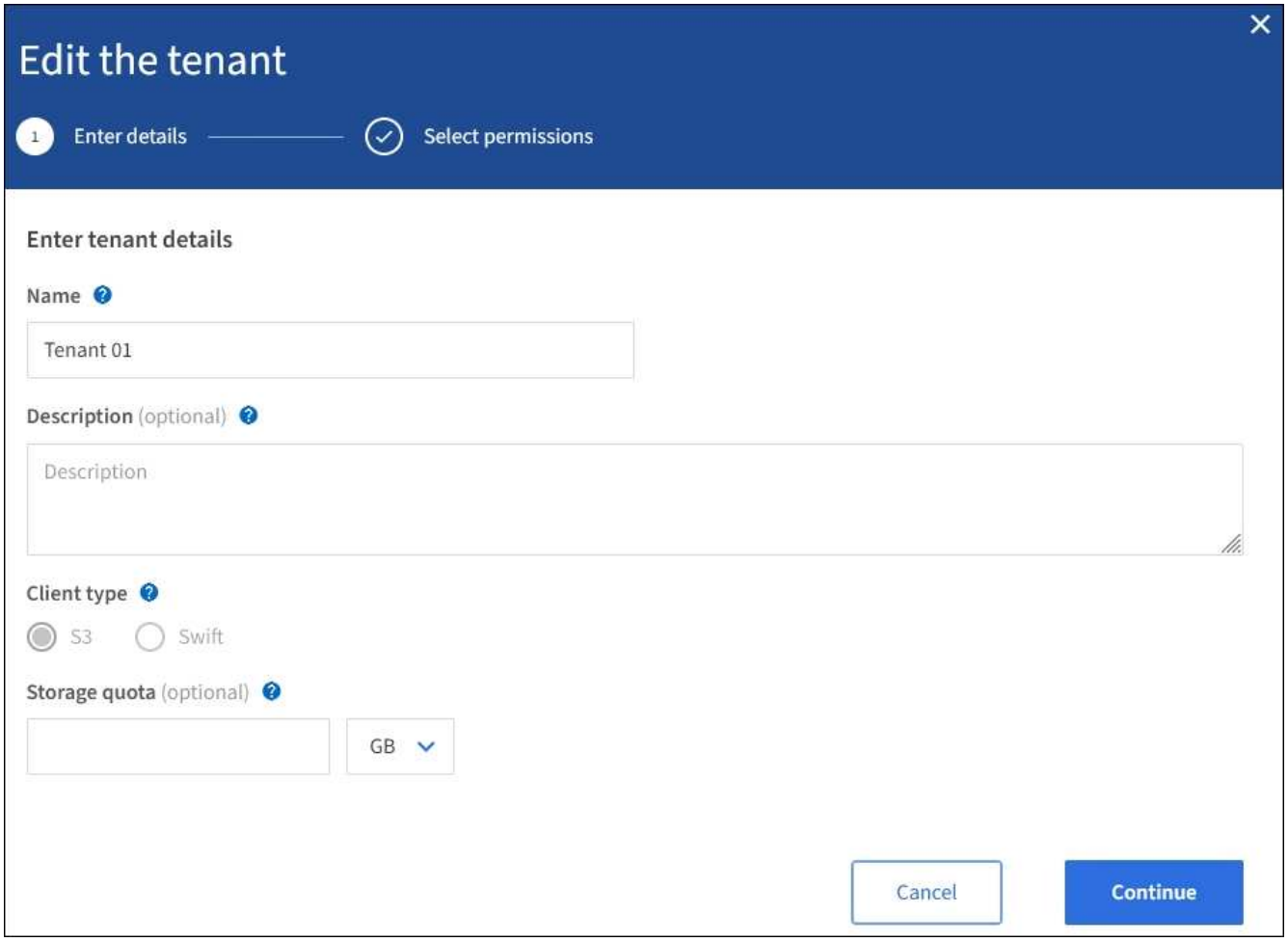


2. 選取您要編輯的租戶帳戶。

   使用搜尋方塊、依名稱或租戶ID搜尋租戶帳戶。

3. 從「動作」下拉式清單中、選取*「編輯」*。

   此範例適用於不使用單一登入（SSO）的網格。此租戶帳戶尚未設定自己的身分識別來源。



4. 視需要變更這些欄位的值：
   - 名稱
   - 說明
   - 用戶端類型
   - 儲存配額
5. 選擇*繼續*。
6. 選取或取消選取租戶帳戶的權限。
   - 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。
   - 變更*使用自己的身分識別來源*核取方塊的設定、以判斷租戶帳戶是否使用自己的身分識別來源、或是為Grid Manager設定的身分識別來源。

     如果*使用自己的身分識別來源*核取方塊為：

     - 停用並勾選、表示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。
     - 停用或取消核取、StorageGRID SSO會啟用以供整個作業系統使用。租戶必須使用為Grid Manager設定的身分識別來源。

◦ 視需要啟用或停用* S3 Select *。請參閱 管理用戶帳戶的S3 Select。

7. 選擇*保存*。

相關資訊

- 管理S3租戶帳戶的平台服務
- 使用租戶帳戶

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。

您需要的產品

- 您必須使用登入Grid Manager 支援的網頁瀏覽器。
- 您必須擁有特定的存取權限。
- 您必須移除所有與租戶帳戶相關的貯體（S3）、容器（Swift）和物件。

步驟

1. 選取*租戶*。
2. 選取您要刪除的租戶帳戶。

   使用搜尋方塊、依名稱或租戶ID搜尋租戶帳戶。

3. 從「動作」下拉式清單中選取「刪除」。
4. 選擇*確定*。

管理平台服務

管理**S3**租戶帳戶的平台服務

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。

這些服務可讓租戶在S3儲存區中使用下列功能：

- * CloudMirror複寫*：StorageGRID 《Sirror CloudMirror複寫服務》可用來將特定物件從StorageGRID 一個物件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。

  如果來源儲存區已啟用S3物件鎖定、則不支援CloudMirror複寫。

- 通知：每個儲存區事件通知用於將針對物件執行的特定動作通知傳送至指定的外部Amazon Simple Notification Service™（SNS）。

  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Elasticsearch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。

使用平台服務的建議

在使用平台服務之前、請注意下列建議：

- 如果StorageGRID 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。
- 無法完成的端點要求將排入最多50、000個要求的佇列。此限制在作用中租戶之間平均分攤。新租戶可暫時超過這50萬個限額、因此新增租戶不會受到不公平的懲罰。

相關資訊

- 使用租戶帳戶
- 設定儲存Proxy設定
- 監控及疑難排解

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
- 支援接收簡單通知服務（SNS）訊息的本機應用程式
- 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
- * 443*：適用於以https開頭的端點URI

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。

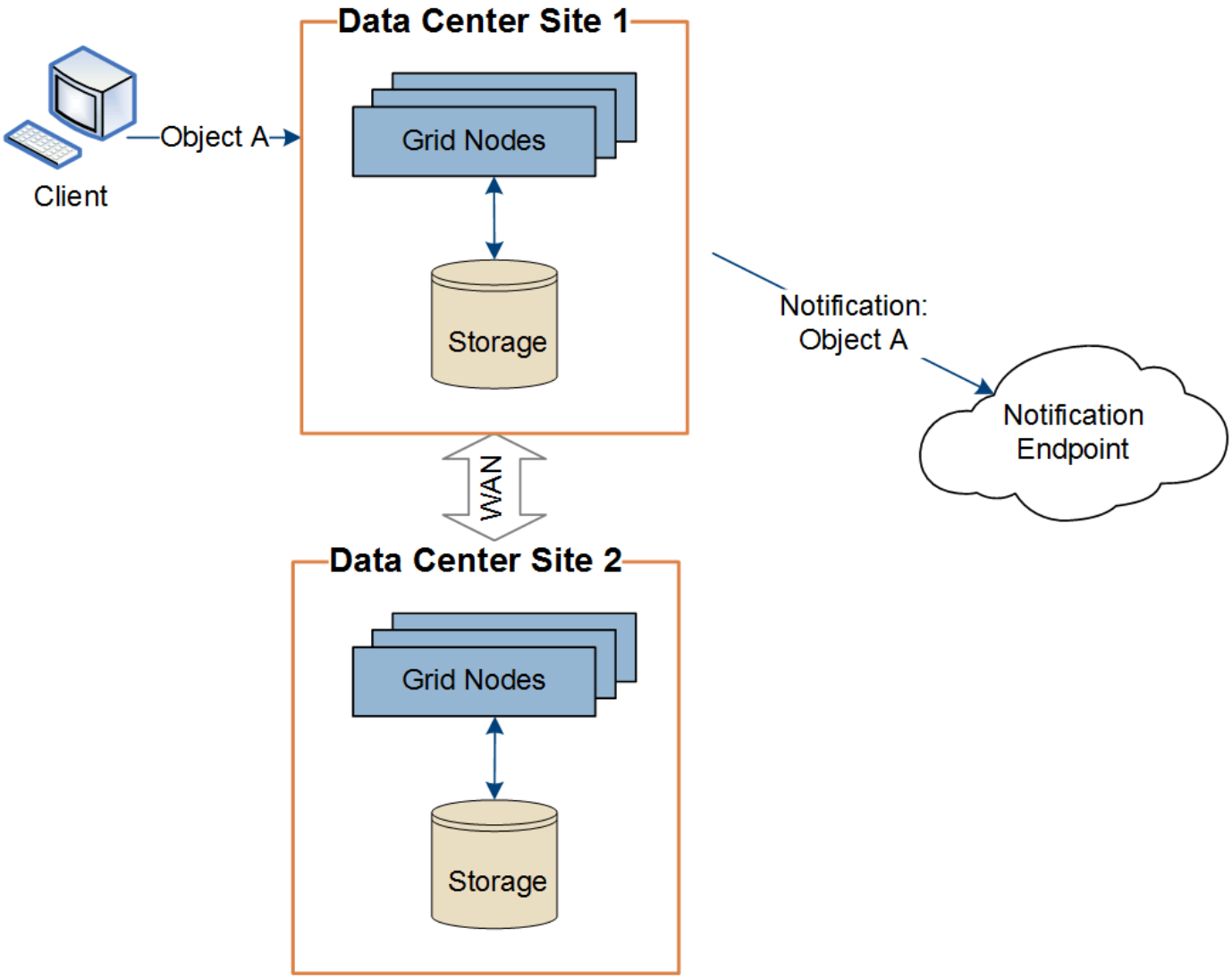
相關資訊

- 使用租戶帳戶

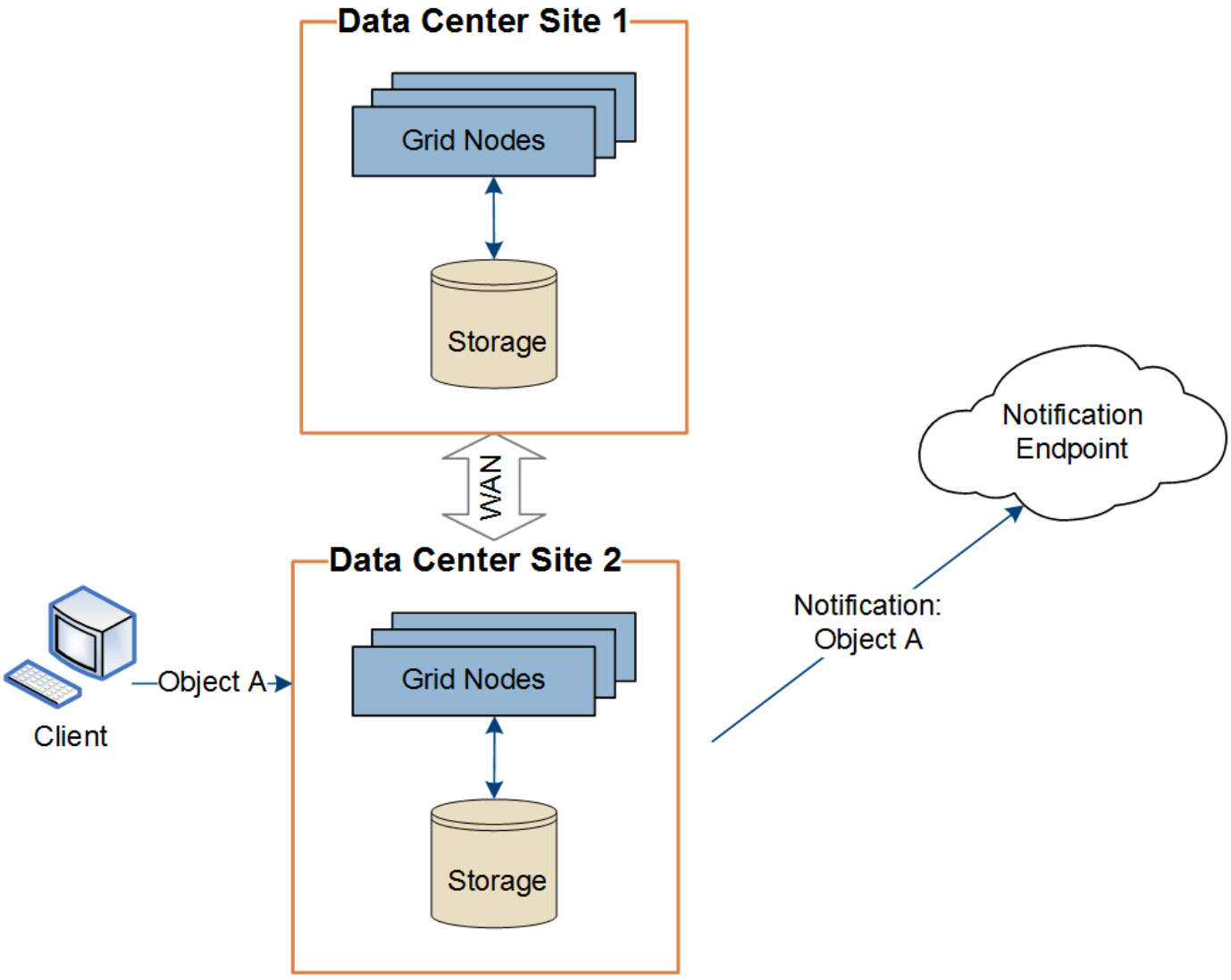
每個站台提供平台服務訊息

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。每個端點都代表一個平台服務的外部目的地、例如StorageGRID 一個支援對象、一個支援Amazon Web Services的資源庫、一個簡單通知服務主題、或是在本機或AWS上代管的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。

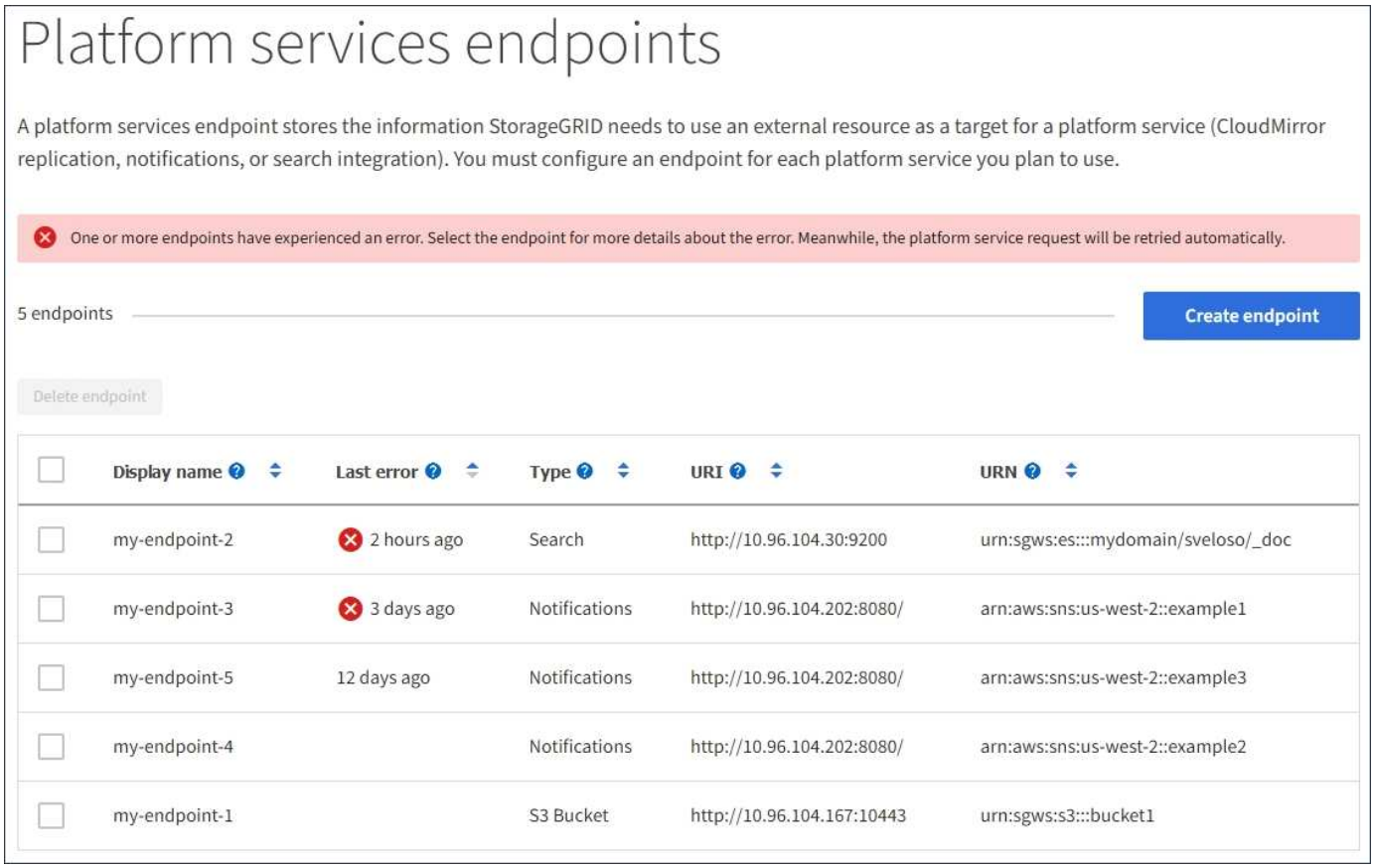
如果未啟用租戶帳戶的平台服務、端點建立將會失敗。

現有端點的問題

如果在嘗試連線至現有端點時發生錯誤StorageGRID 、則會在浮動授權管理員的儀表板上顯示一則訊息。

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

租戶使用者可前往「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

如果您已在儲存節點和平台服務端點之間設定儲存Proxy、則當Proxy服務不允許StorageGRID 來自該端點的訊息時、可能會發生錯誤。若要解決這些問題、請檢查Proxy伺服器的設定、確保平台服務相關訊息不會遭到封鎖。

確定是否發生錯誤

如果在過去7天內發生任何端點錯誤、則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」。

   事件訊息也會列在「/var/local/log/bycast-err.log」中。
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。

如果由於無法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 Event（SMT）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。

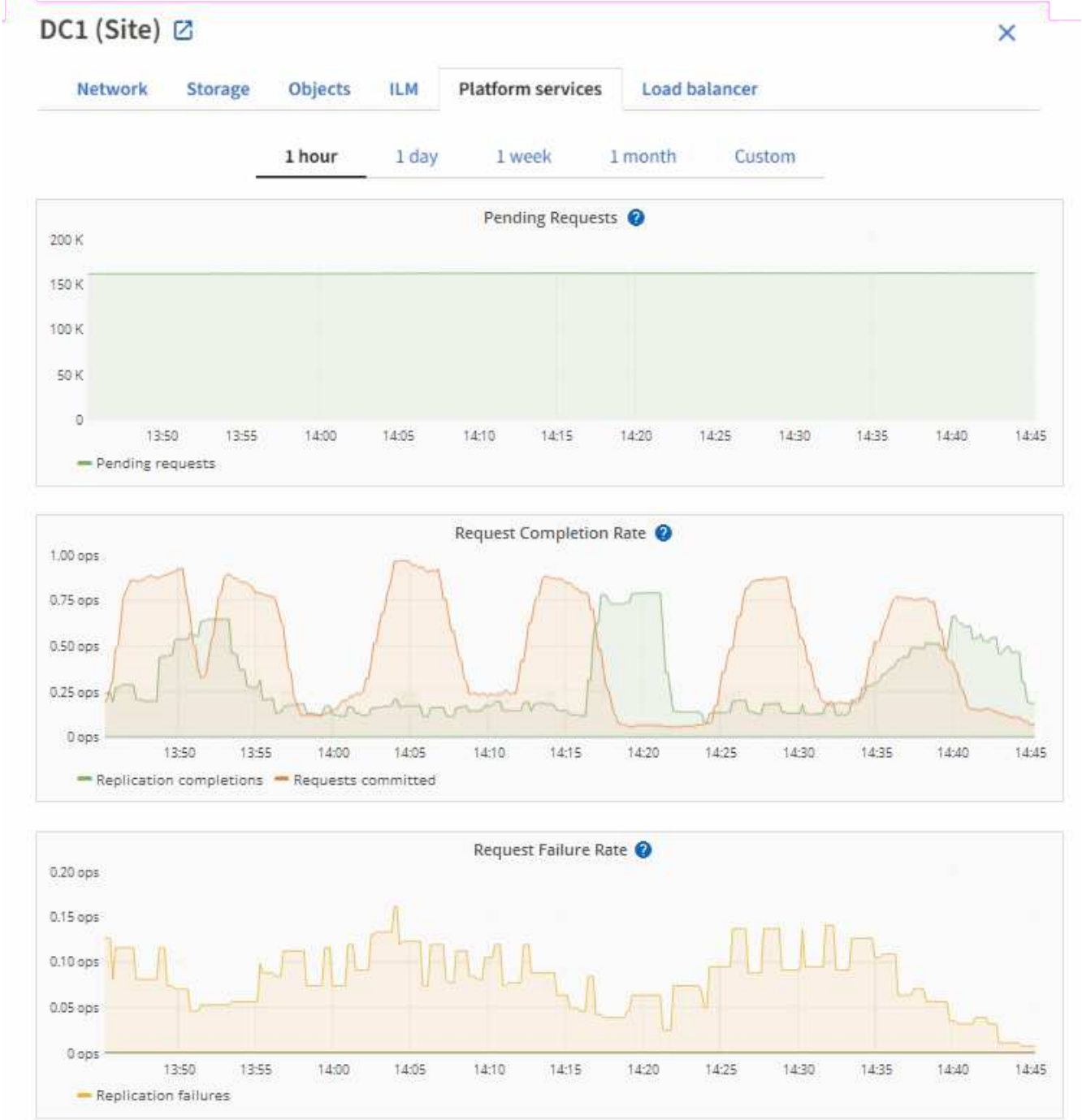
唯一的可見效果是傳入S3要求執行時間較長。如果您開始偵測到效能大幅降低、應該降低擷取速度、或是使用容量較大的端點。如果要求的待處理項目持續增加、用戶端S3作業（例如PUT要求）最終將會失敗。

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。

如需平台服務端點疑難排解的其他資訊、請參閱的說明 使用租戶帳戶。

相關資訊

- 監控及疑難排解
- 設定儲存Proxy設定

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

S3 Select查詢需要下列項目：StorageGRID

- 您要查詢的物件為CSV格式、或是含有CSV格式檔案的GZIP或bzip2壓縮檔。
- 租戶必須由網格管理員授予S3 Select功能。選取*「允許S3選取*時機」 建立租戶 或 編輯租戶。
- 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SG100或SG1000應用裝置節點、或是VMware軟體節點。

請注意下列限制：

- 不支援裸機負載平衡器節點。
- 查詢無法直接傳送至儲存節點。
- 不支援透過過時CLB服務傳送的查詢。

> 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S3和Swift用戶端連線

關於S3和Swift用戶端連線

身為網格管理員、您可以管理組態選項、以控制S3和Swift租戶如何將用戶端應用程式連線

至StorageGRID 您的作業系統、以儲存和擷取資料。有許多不同的選項可滿足不同的用戶端和租戶需求。

用戶端應用程式可連線至下列任一項目、以儲存或擷取物件：

- 管理節點或閘道節點上的負載平衡器服務、或是管理節點或閘道節點之高可用度（HA）群組的虛擬IP位址（可選）
- 閘道節點上的CLB服務、或是閘道節點高可用度群組的虛擬IP位址（可選）

> CLB服務已過時。在發佈版推出之前設定的用戶端StorageGRID 、可以繼續在閘道節點上使用CLB服務。所有其他仰賴StorageGRID 以提供負載平衡的用戶端應用程式、都應該使用負載平衡器服務進行連線。

- 儲存節點、無論是否有外部負載平衡器

您可以選擇在StorageGRID 您的作業系統上設定下列功能：

- * 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、以隔離及分割用戶端和租戶流量、以確保安全性、靈活度和效能。建立VLAN介面之後、您可以將其新增至高可用度（HA）群組。
- 高可用度群組：您可以為閘道節點或管理節點建立介面的HA群組、以建立主動備份組態、也可以使用循環DNS或協力廠商負載平衡器及多個HA群組、來達成主動-主動式組態。用戶端連線是使用HA群組的虛擬IP位址進行。
- 負載平衡器服務：您可以建立用戶端連線的負載平衡器端點、讓用戶端使用負載平衡器服務。建立負載平衡器端點時、請指定連接埠編號、端點是否接受HTTP或HTTPS連線、使用端點的用戶端類型（S3或Swift）、以及用於HTTPS連線的憑證（若適用）。
- 不受信任的用戶端網路：您可以將用戶端網路設定為不受信任、使其更安全。當用戶端網路不受信任時、用戶端只能使用負載平衡器端點進行連線。

您也可以針對直接連線StorageGRID 至儲存節點或使用CLB服務（已過時）的用戶端、啟用HTTP、並可為S3用戶端設定S3 API端點網域名稱。

摘要：用於用戶端連線的**IP**位址和連接埠

用戶端應用程式可以StorageGRID 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功能區。如果已設定高可用度（HA）群組、用戶端應用程式就可以使用HA群組的虛擬IP位址進行連線。

關於這項工作

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。本指示說明如何在已設定負載平衡器端點和高可用度（HA）群組的情況下、於Grid Manager中找到此資訊。

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	• 負載平衡器端點連接埠

連線位置	用戶端連線的服務	IP 位址	連接埠
HA群組	CLB 附註： CLB服務已過時。	HA群組的虛擬IP位址	預設S3連接埠： • HTTPS：8082 • HTTP：8084 預設Swift連接埠： • HTTPS：8083 • HTTP：8085
管理節點	負載平衡器	管理節點的IP位址	• 負載平衡器端點連接埠
閘道節點	負載平衡器	閘道節點的IP位址	• 負載平衡器端點連接埠
閘道節點	CLB 附註： CLB服務已過時。	閘道節點的IP位址 *附註：*根據預設、不會啟用CLB和LDR的HTTP連接埠。	預設S3連接埠： • HTTPS：8082 • HTTP：8084 預設Swift連接埠： • HTTPS：8083 • HTTP：8085
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

範例

若要將S3用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- 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S3負載平衡器端點的連接埠號碼為10443、則S3用戶端可以使用下列URL連線StorageGRID 到SESH:

- https://192.0.2.5:10443`

若要將Swift用戶端連線至閘道節點HA群組的負載平衡器端點、請使用結構如下所示的URL：

- https://*VIP-of-HA-group:LB-endpoint-port*`

例如、如果HA群組的虛擬IP位址為192.0.2.6、而Swift負載平衡器端點的連接埠號碼為104444、則Swift用戶端可使用下列URL連線StorageGRID 到Sender:

- https://192.0.2.6:10444`

您可以為用戶端用來連線StorageGRID 到靜態的IP位址設定DNS名稱。請聯絡您的本機網路管理員。

步驟

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*。

      此時會出現「負載平衡器端點」頁面、顯示已設定的端點清單。

   b. 選取端點、然後選取*編輯端點*。

      「編輯端點」視窗隨即開啟、並顯示端點的其他詳細資料。

   c. 確認您選取的端點已設定為使用正確的傳輸協定（S3或Swift）、然後選取*取消*。
   d. 記下您要用於用戶端連線的端點連接埠號碼。

如果連接埠號碼為80或443、則端點只會在閘道節點上設定、因為這些連接埠會保留在管理節點上。所有其他連接埠都在閘道節點和管理節點上設定。

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、您無法在同一個閘道節點上同時使用Grid Network介面和Client Network介面、作為同一個VLAN的父介面。
- 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或CentOS（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、CentOS、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

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。
- 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

1. 選擇*組態*>*網路*>* VLAN介面*。
2. 選擇* Create （建立）。

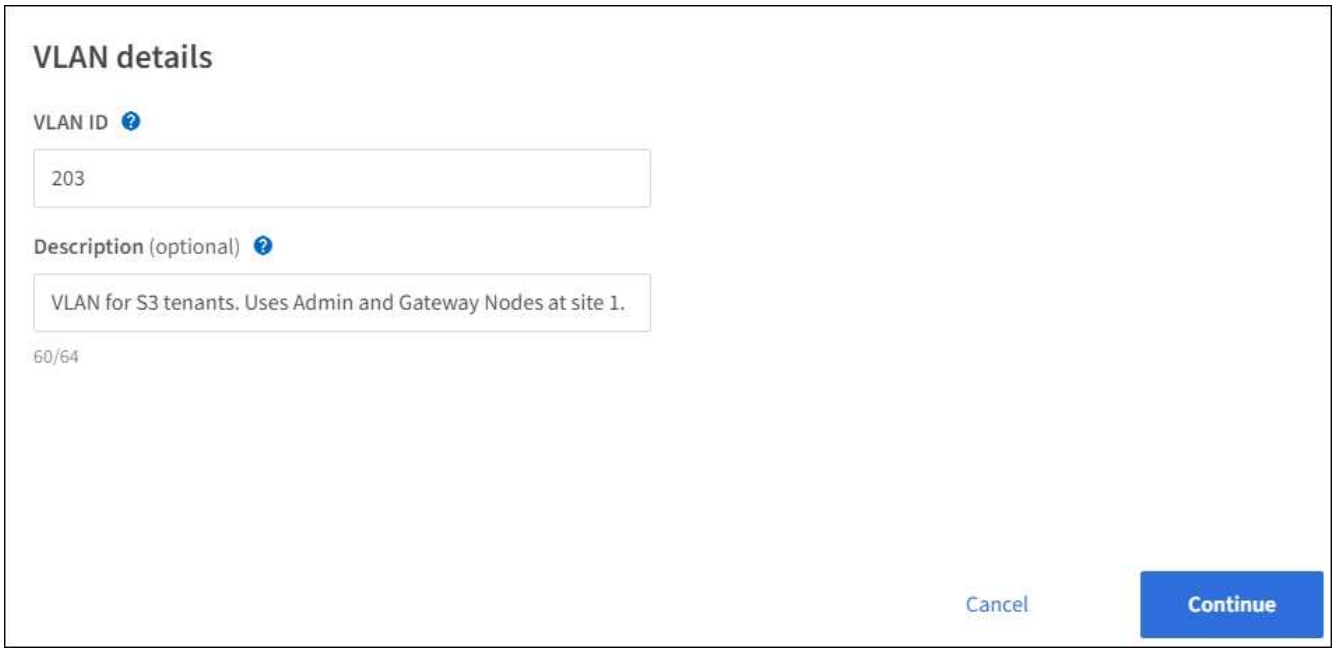
輸入**VLAN**介面的詳細資料

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不需要是唯一的。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、具有相同ID的兩個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。您可以繼續為相同的VLAN ID建立另一個VLAN介面、也可以選取*取消*、然後編輯現有的ID。

2. （可選）輸入VLAN介面的簡短說明。



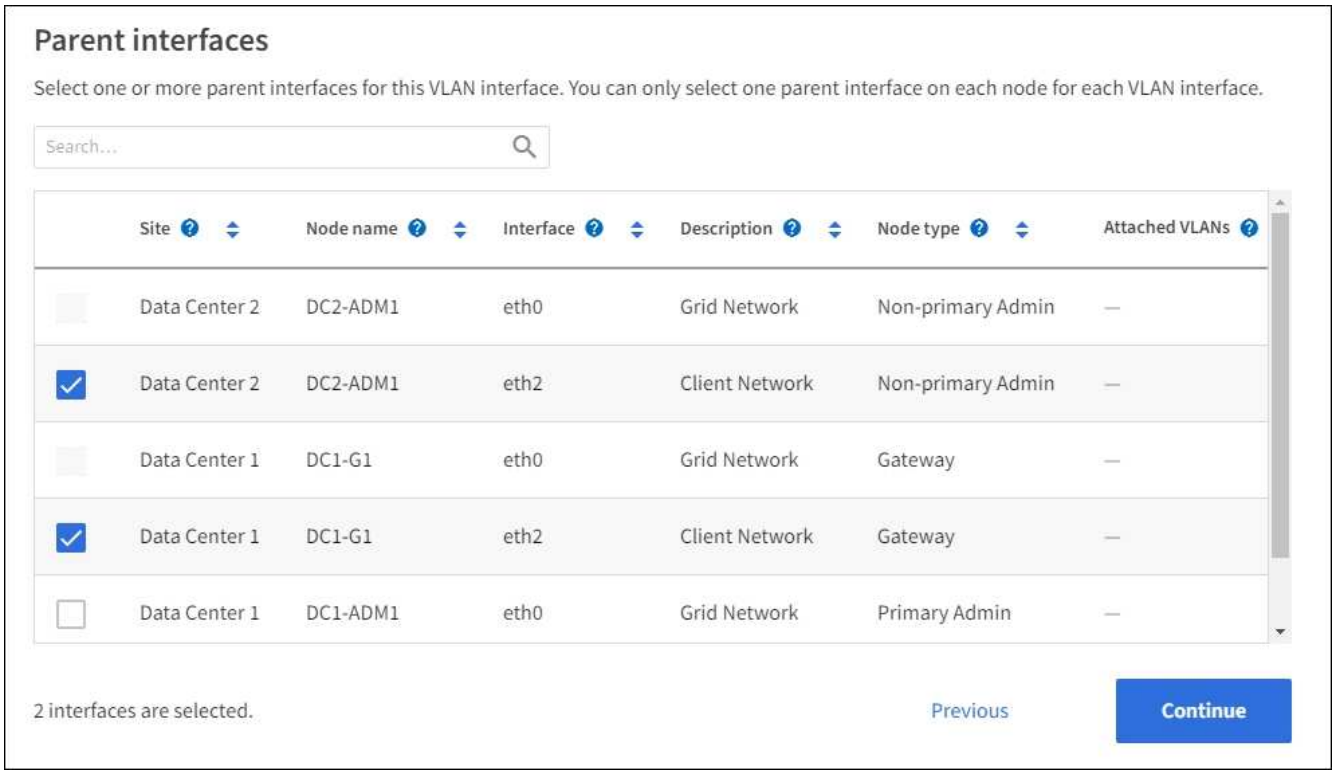
3. 選擇*繼續*。

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）介面無法作為父介面使用、因此不會顯示。

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

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群組使用VLAN 200介面作為節點A、而eth2介面用於節點B、則可以移除節點B的未使用父介面、但無法移除節點A的已用父介面

步驟

1. 選擇*組態*>*網路*>* VLAN介面*。
2. 選取您要編輯之VLAN介面的核取方塊。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. 或者、選取或取消選取核取方塊以新增父介面或移除未使用的介面。然後選擇*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。

管理高可用度群組

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。
- 僅包含SG100或SG1000應用裝置及VMware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該群組。

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。也就是在正常操作期間、主要介面是群組的「主動」介面。

同樣地、在正常運作期間、HA群組的任何較低優先順序介面都會做為「備份」介面。除非主要（目前作用中）介面無法使用、否則不會使用這些備份介面。

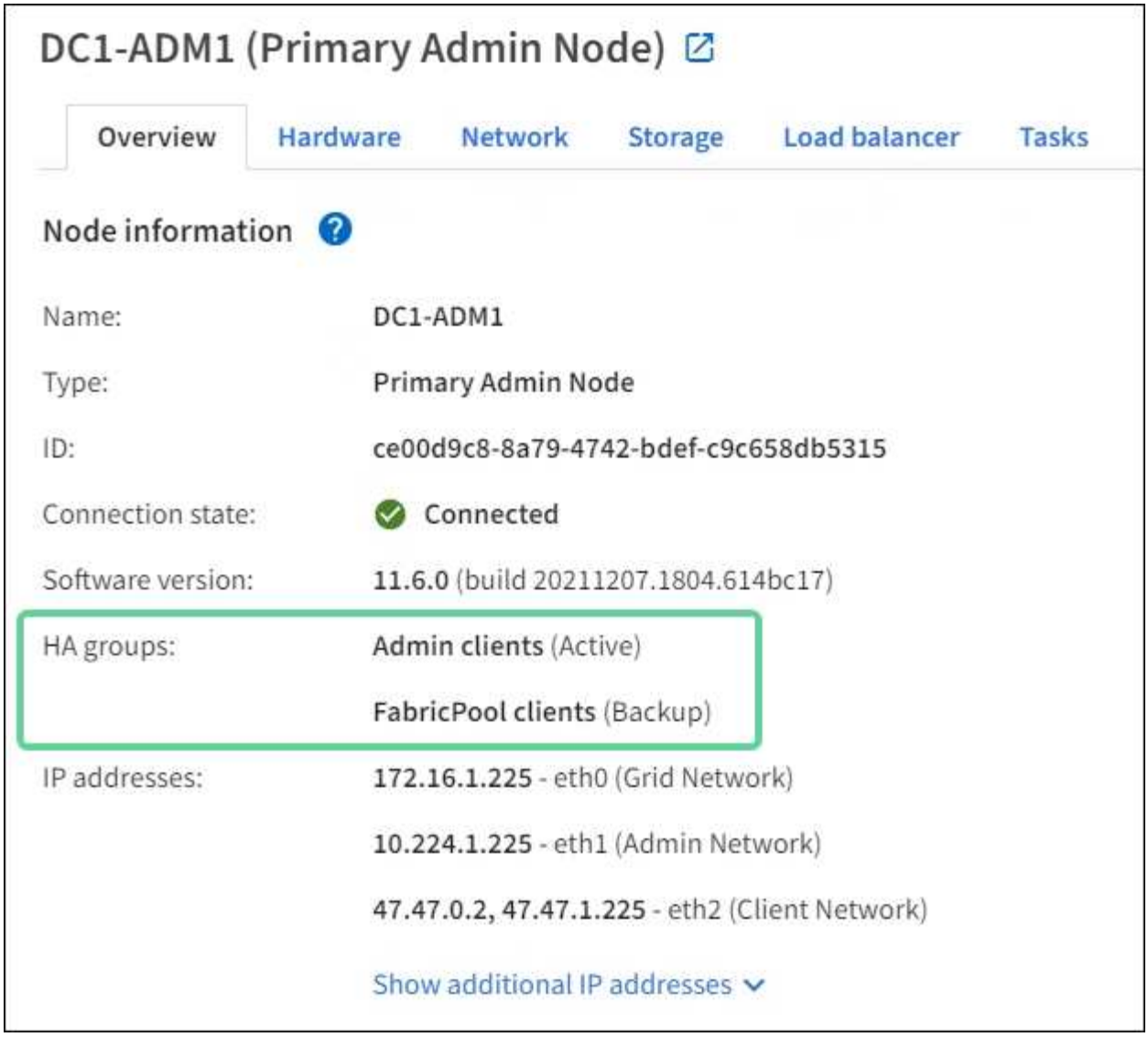
檢視節點的目前**HA**群組狀態

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：HA群組無法裝載在此節點上、因為高可用度（保留）服務已手動停止。
- * fault*：由於下列一項或多項原因、HA群組無法裝載在此節點上：
  - 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、容錯移轉也不會因為Grid Manager或租戶管理程式的CLB服務（已過時）或服務故障而觸發。

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和CLB服務（已過時）。

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
的S3用戶端存取 S3 Select	• SG100或SG1000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。
S3或Swift用戶端存取- CLB服務 附註： CLB服務已過時。	• 閘道節點

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。

部分維護程序無法在主要管理節點無法使用時執行。容錯移轉期間、您可以使用Grid Manager監控StorageGRID 您的作業系統。

HA群組搭配CLB服務的使用限制

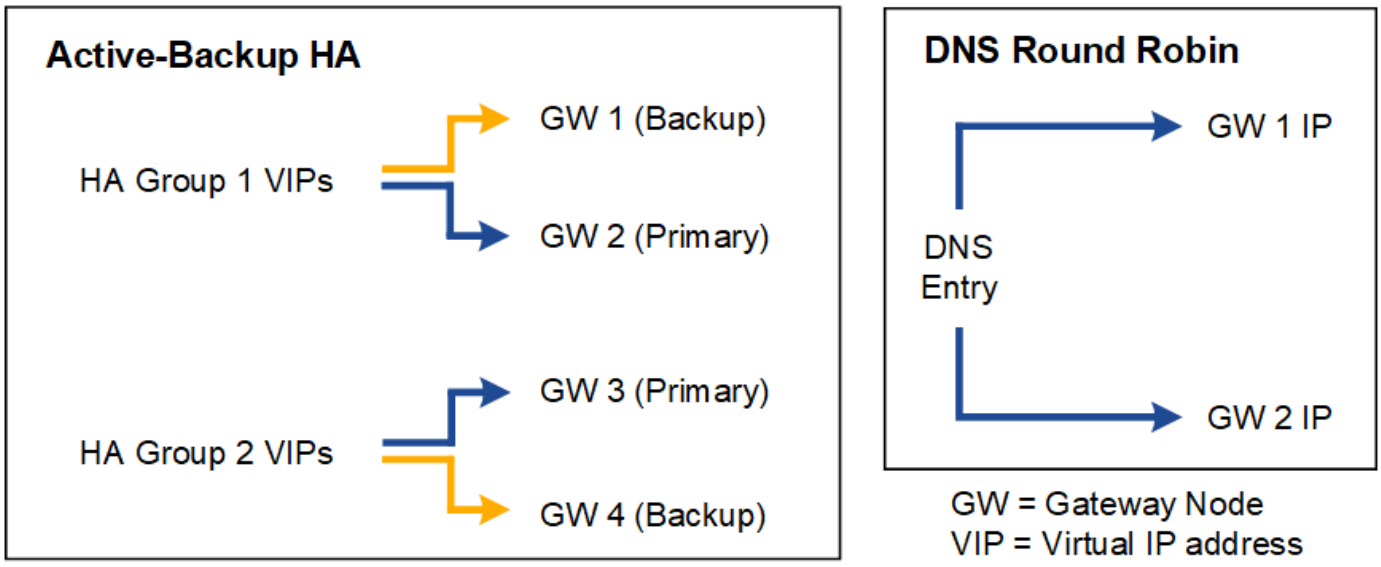
CLB服務故障不會觸發HA群組內的容錯移轉。

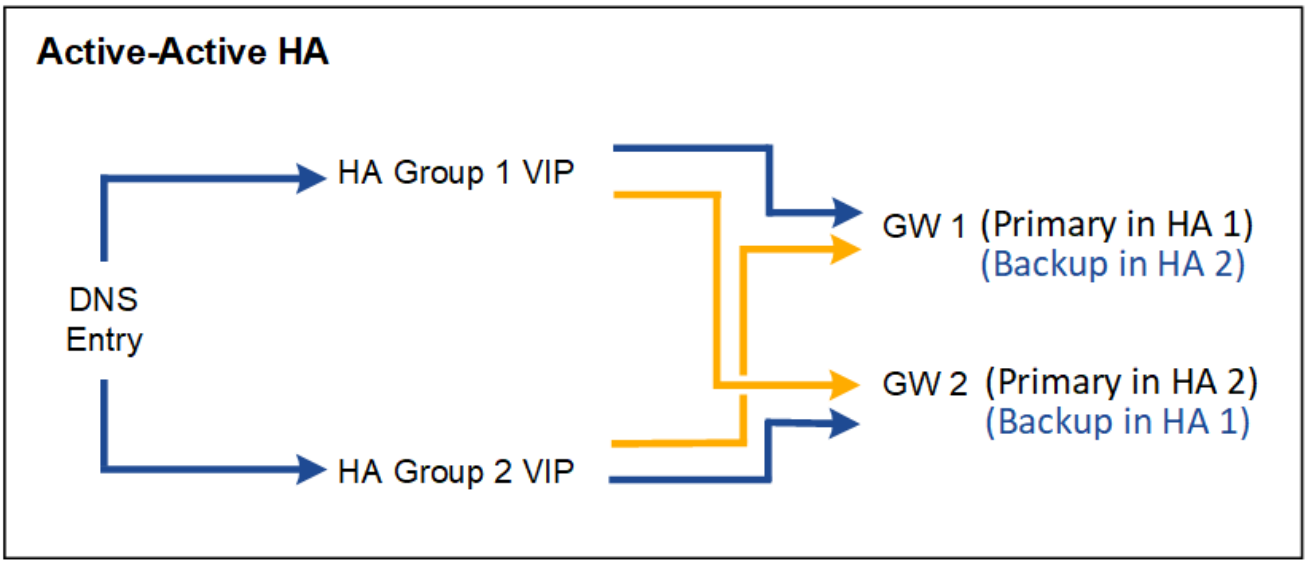
CLB服務已過時。

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。

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。
- 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或CentOS（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。

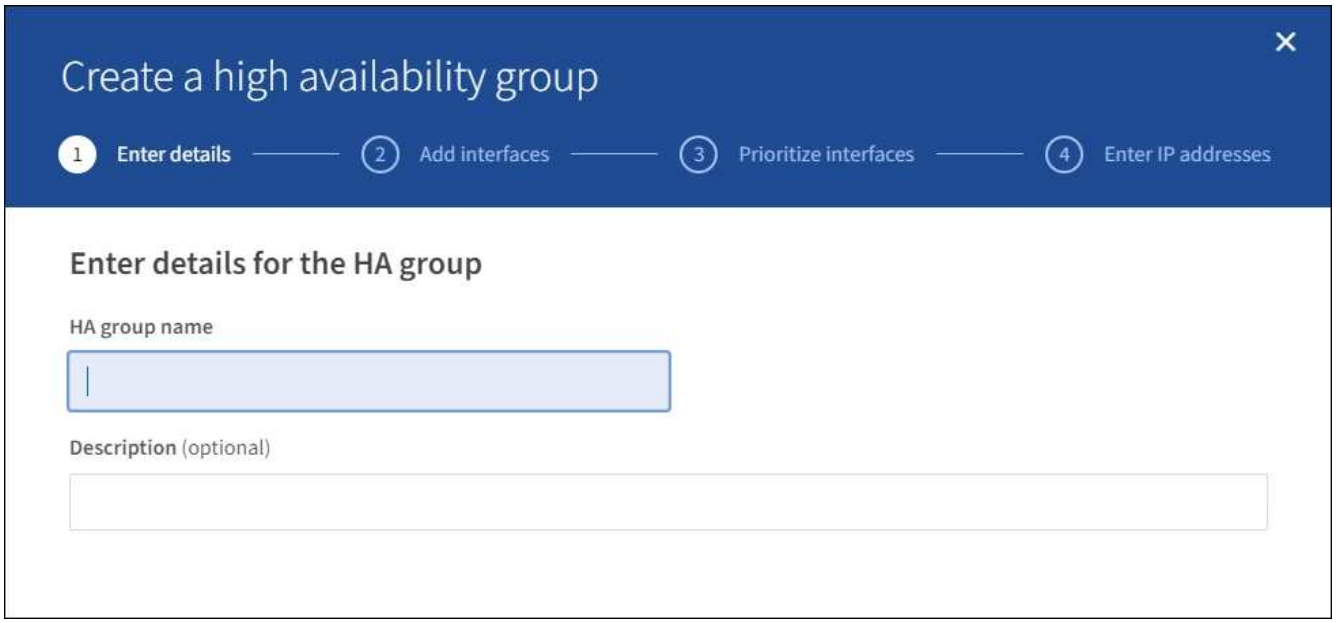
介面必須是要納入HA群組的閘道節點或管理節點。HA群組只能將一個介面用於任何指定節點、但同一個節點的其他介面可用於其他HA群組。

存取精靈

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

1. 為HA群組提供唯一名稱。

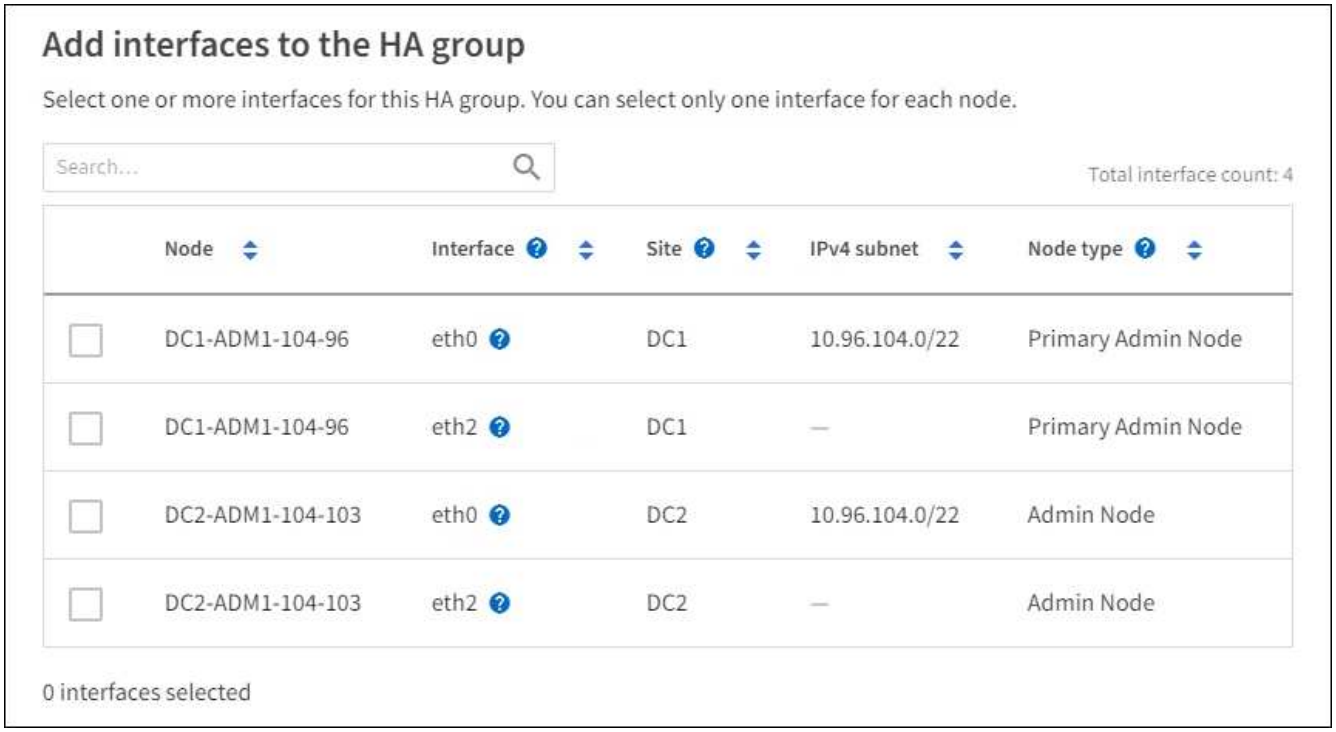


2. （可選）輸入HA群組的說明。
3. 選擇*繼續*。

新增介面至**HA**群組

1. 選取一或多個介面以新增至此HA群組。

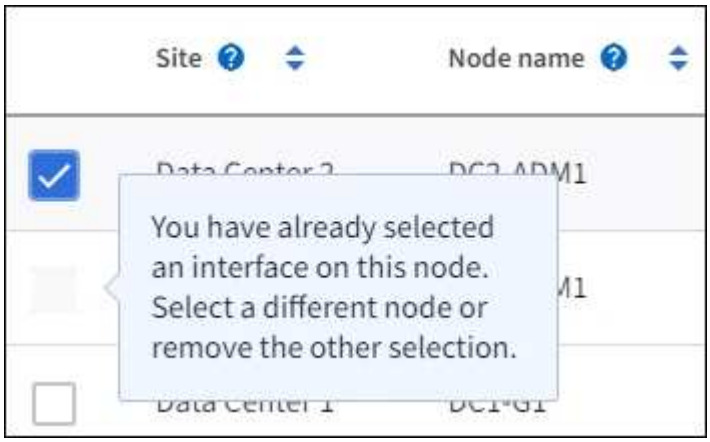
   使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。



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HA群組用於HA保護已過時的CLB服務、請選取「僅閘道節點上的介面」。
- 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、備份閘道節點無法為管理節點服務提供HA保護。同樣地、備份管理節點也無法執行主要管理節點可以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。



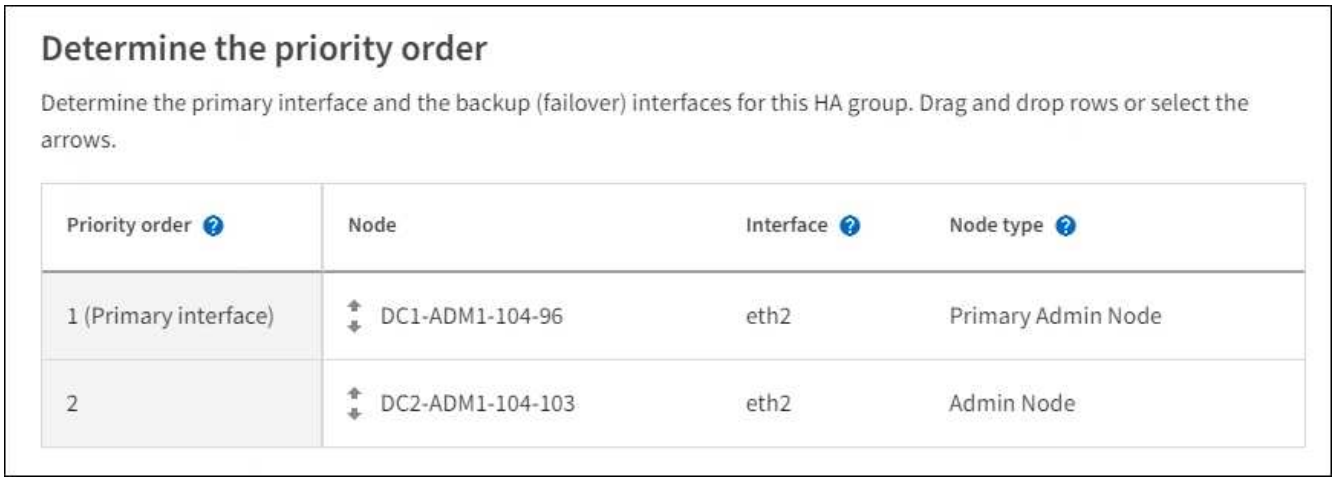
- 如果介面的子網路值或閘道與其他選取的介面發生衝突、則無法選取介面。
- 如果設定的介面沒有靜態IP位址、則無法選取該介面。

2. 選擇*繼續*。

決定優先順序

1. 確定此HA群組的主要介面和任何備份（容錯移轉）介面。

   拖放列以變更*優先順序*欄中的值。



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。

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、而主要介面故障、則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。

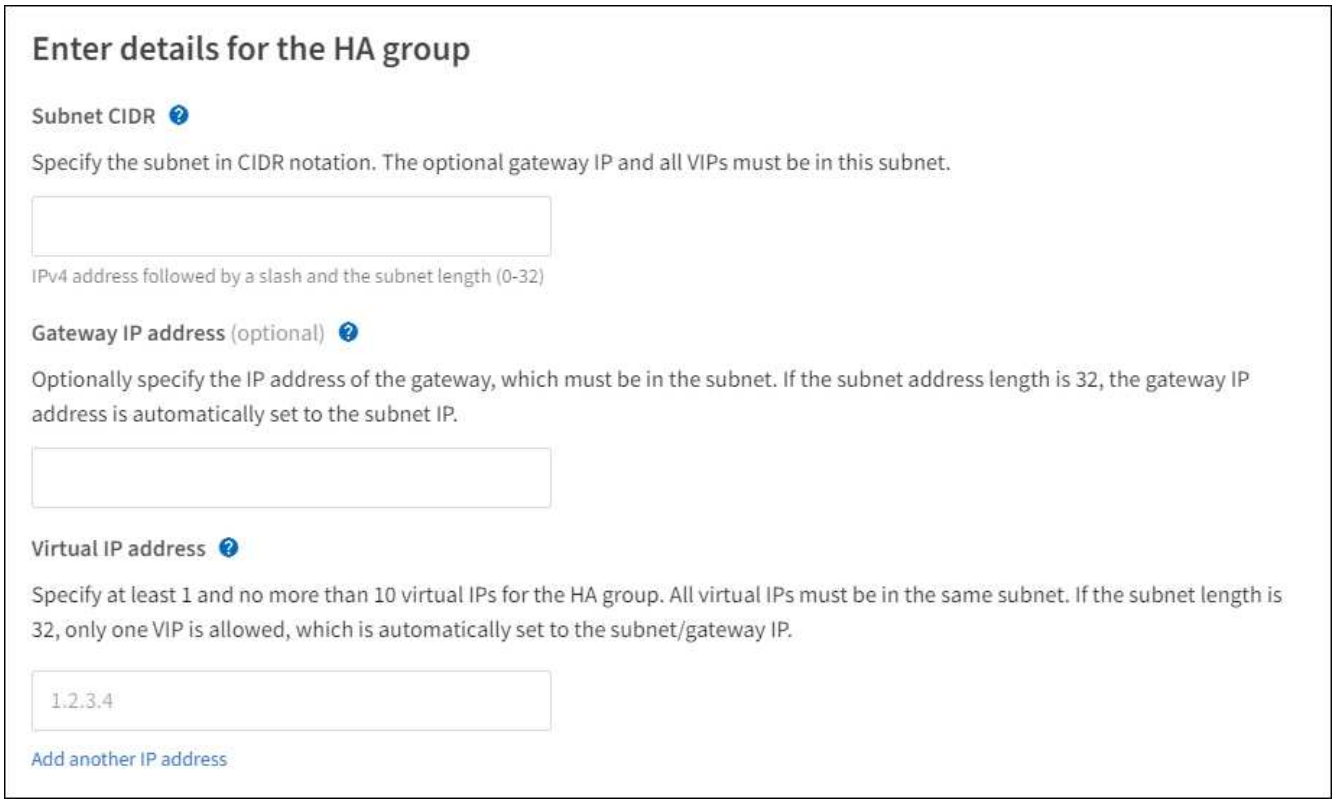
2. 選擇*繼續*。

輸入**IP**位址

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. 輸入HA群組的一個或多個*虛擬IP位址*。您最多可以新增10個IP位址。所有VIP都必須位於VIP子網路內。

   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。

   等待15分鐘、讓HA群組的變更套用至所有節點。

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

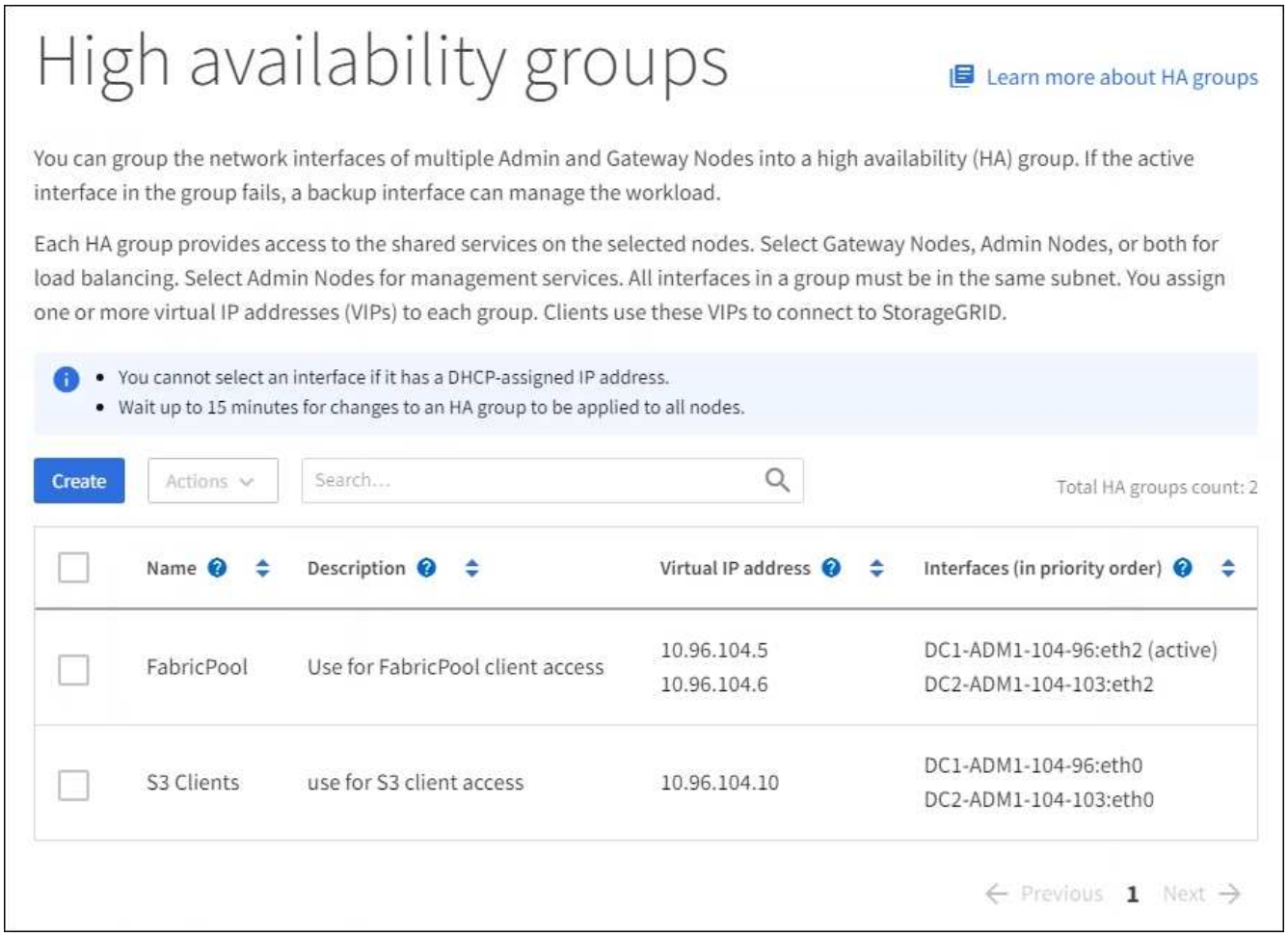
您可以編輯高可用度（HA）群組、以變更其名稱和說明、新增或移除介面、變更優先順序、或新增或更新虛擬IP位址。

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、選取或取消選取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. 您也可以拖放列、以變更此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）」*。

等待15分鐘、讓HA群組的變更套用至所有節點。

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。不過、如果HA群組繫結至一或多個負載平衡器端點、則無法移除。

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. 選取您要移除之每個HA群組的核取方塊。然後選擇* Actions **>***移除**HA**群組。
3. 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

管理負載平衡：總覽

您可以使用StorageGRID S動靈 負載平衡功能來處理S3和Swift用戶端的擷取和擷取工作負載。負載平衡功能可將工作負載和連線分散到多個儲存節點、以最大化速度和連線容量。

您可以使用下列方式來平衡用戶端工作負載：

- 使用安裝在管理節點和閘道節點上的負載平衡器服務。負載平衡器服務提供第7層負載平衡、並對用戶端要求執行TLS終止、檢查要求、以及建立新的安全連線至儲存節點。這是建議的負載平衡機制。

  請參閱 負載平衡的運作方式-負載平衡器服務。

- 使用過時的Connection Load Balancer（CLB）服務、該服務僅安裝在閘道節點上。CLB服務提供第4層負載平衡、並支援連結成本。

  請參閱 負載平衡的運作方式- CLB服務（已過時）。

- 整合協力廠商負載平衡器。如需詳細資料、請聯絡您的NetApp客戶代表。

負載平衡的運作方式-負載平衡器服務

負載平衡器服務會將傳入的網路連線從用戶端應用程式分散到儲存節點。若要啟用負載平衡、您必須使用Grid Manager來設定負載平衡器端點。

您只能為管理節點或閘道節點設定負載平衡器端點、因為這些節點類型包含負載平衡器服務。您無法設定儲存節

點或歸檔節點的端點。

每個負載平衡器端點都會指定連接埠、網路傳輸協定（HTTP或HTTPS）、用戶端類型（S3或Swift）和繫結模式。HTTPS端點需要伺服器憑證。連結模式可讓您將端點連接埠的存取限制為：

- 特定高可用度（HA）群組的虛擬IP位址（VIP）
- 特定管理和閘道節點的特定網路介面

連接埠考量

用戶端可以存取您在任何執行負載平衡器服務的節點上設定的任何端點、但有兩個例外：管理節點上保留連接埠80和443、因此這些連接埠上設定的端點僅支援閘道節點上的負載平衡作業。

如果您已重新對應任何連接埠、則無法使用相同的連接埠來設定負載平衡器端點。您可以使用重新對應的連接埠來建立端點、但這些端點會重新對應至原始CLB連接埠和服務、而非負載平衡器服務。請依照中的步驟進行 移除連接埠重新對應。

CLB服務已過時。

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。
- 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只能使用SG100或SG1000應用裝置和VMware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。

  憑證可以使用萬用字元來代表執行負載平衡器服務之所有管理節點和閘道節點的完整網域名稱。例如、「*.storagegrid.*example*.com」使用*萬用字元來表示「adm1.storagegrid.*example*.com」和「gn1.storagegrid.*example*.com」。請參閱 設定S3 API端點網域名稱。

建立負載平衡器端點

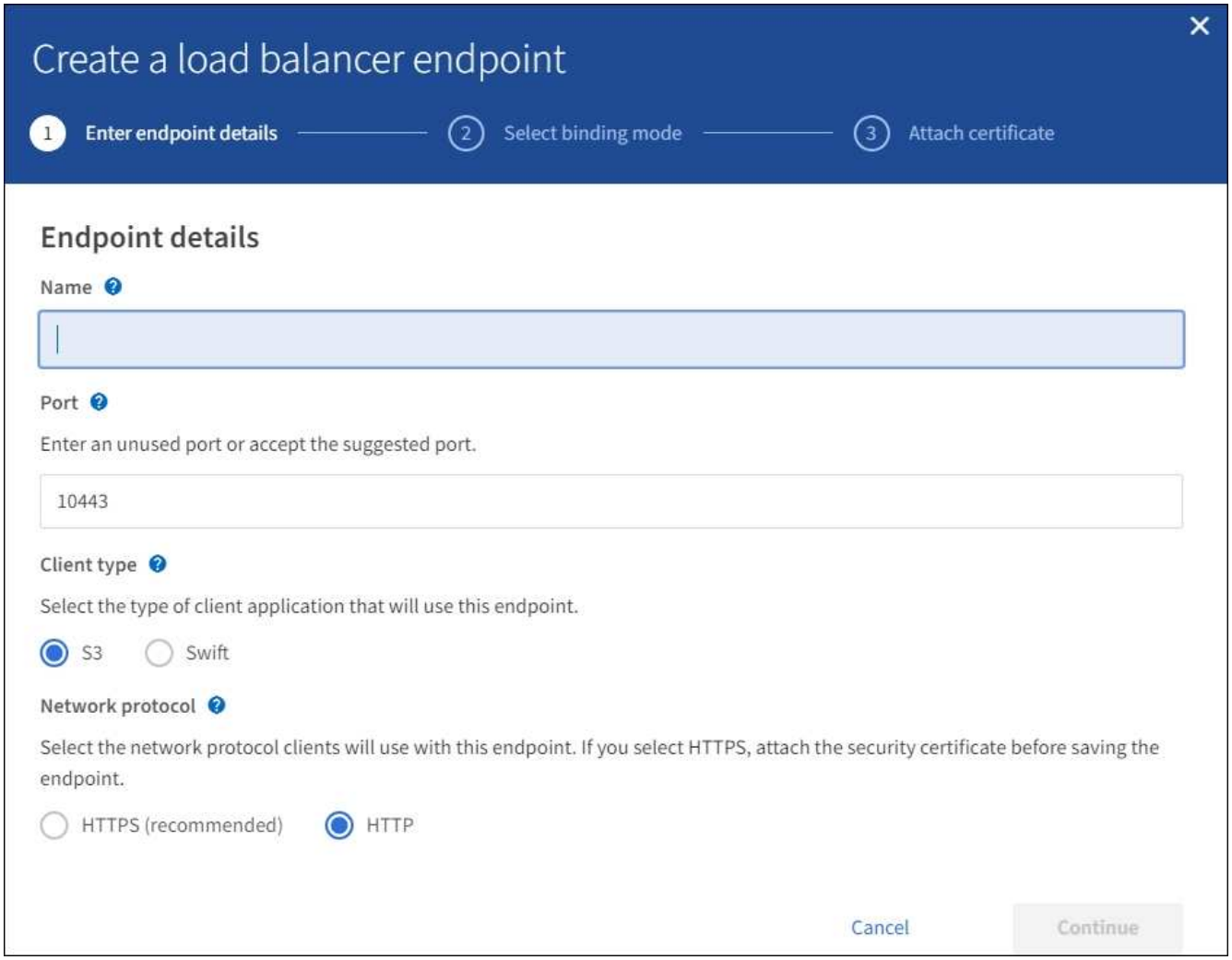
每個負載平衡器端點都會指定連接埠、用戶端類型（S3或Swift）和網路傳輸協定（HTTP或HTTPS）。

存取精靈

1. 選擇*組態*>*網路*>*負載平衡器端點*。
2. 選擇* Create （建立）。

輸入端點詳細資料

1. 輸入端點的詳細資料。



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	連接埠用戶端將用來連線至管理節點和閘道節點上的負載平衡器服務。 接受建議的連接埠號碼、或輸入其他網格服務未使用的任何外部連接埠。輸入介於1和65535.之間的值。 如果輸入* 80*或* 443*、則端點只會在閘道節點上設定。這些連接埠保留在管理節點上。 請參閱 網路準則 以取得外部連接埠的相關資訊。
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。

2. 選擇*繼續*。

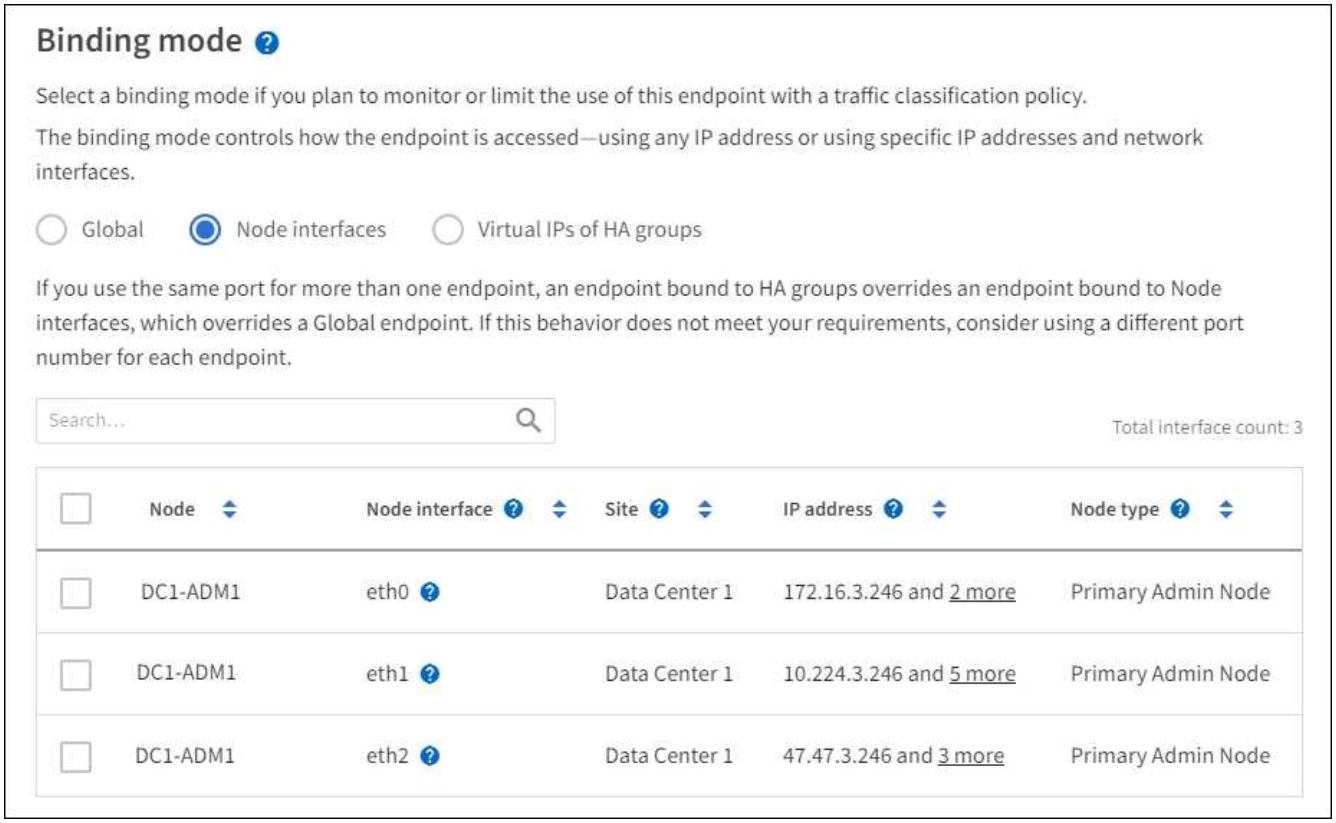
選取繫結模式

1. 選取端點的繫結模式、以控制端點的存取方式。

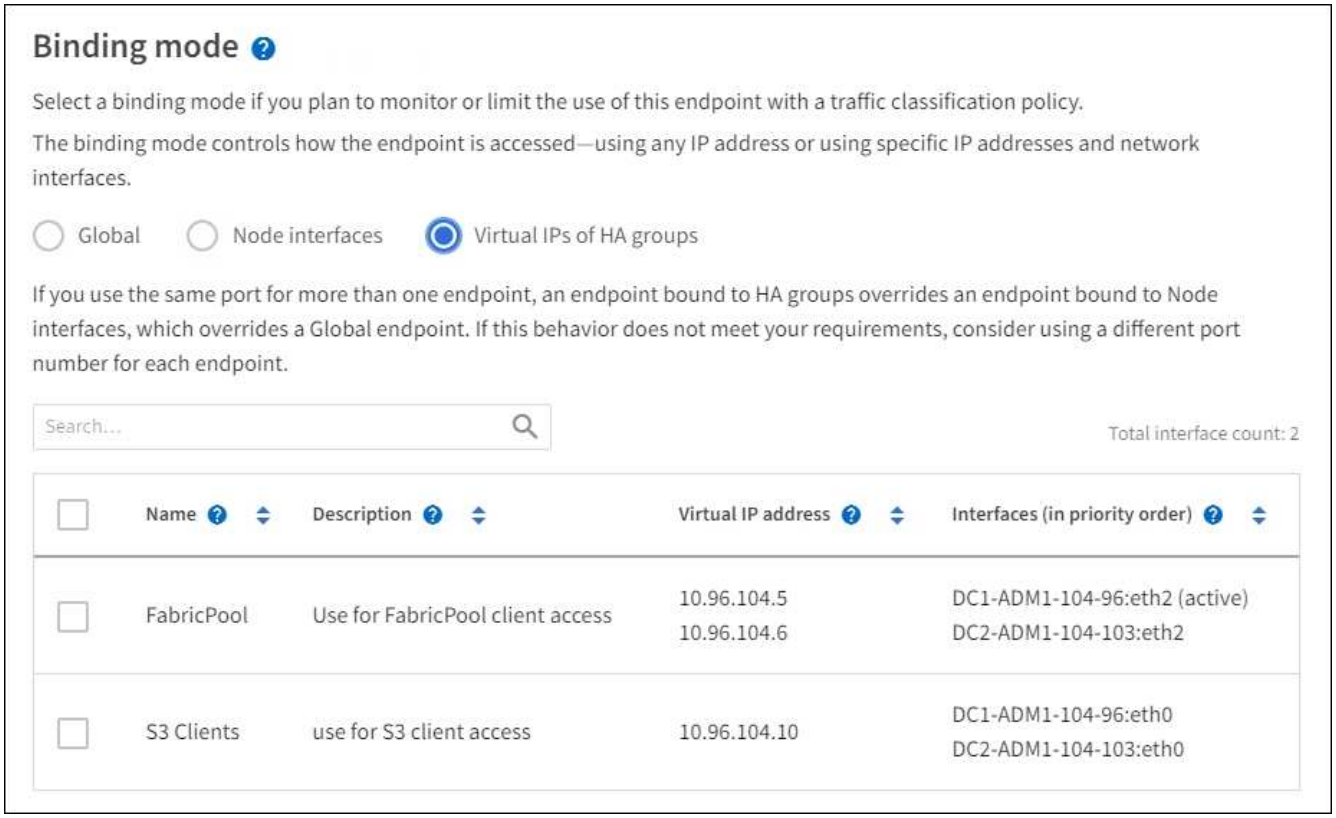
選項	說明
全域（預設）	用戶端可以使用完整網域名稱（FQDN）、任何閘道節點或管理節點的IP位址、或任何網路上任何HA群組的虛擬IP位址來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
節點介面	用戶端必須使用所選節點和網路介面的IP位址來存取此端點。
HA群組的虛擬IP	用戶端必須使用HA群組的虛擬IP位址來存取此端點。 只要您為端點選取的HA群組不重疊、具有此繫結模式的端點都可以使用相同的連接埠號碼。 只要您為端點選取的介面不重疊、使用此模式的端點都可以使用相同的連接埠號碼。

如果您對多個端點使用相同的連接埠、則使用* HA群組的虛擬IP *模式的端點會使用*節點介面*模式覆寫端點、此模式會使用*全域*模式覆寫端點。

2. 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。



3. 如果您選取* HA群組的虛擬IP *、請選取一或多個HA群組。



4. 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

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來取代由網格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。

2. 如果您未使用StorageGRID Ss3和Swift認證、請上傳或產生認證。

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（`.key'）。

     EC私密金鑰必須大於或等於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。儲存副檔名為「.pem」的檔案。

     例如：「toragegrid憑證.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）。+已建立負載平衡器端點。自訂憑證用於S3和Swift用戶端與端點之間的所有後續新連線。

產生憑證

a. 選擇*產生憑證*。

b. 指定憑證資訊：

   - 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*：一個或多個IP位址要納入憑證中。
   - 主體：憑證擁有者的X・509主體或辨別名稱（DN）。
   - 有效天數：憑證建立後到期的天數。

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。儲存副檔名為「.pem」的檔案。

     例如：「toragegrid憑證.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和Swift用戶端與此端點之間的所有後續新連線。

[[完成後]]完成

1. 如果您使用網域名稱系統（DNS）、請確定DNS包含一筆記錄、將StorageGRID 完整網域名稱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、用戶端將使用任何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。

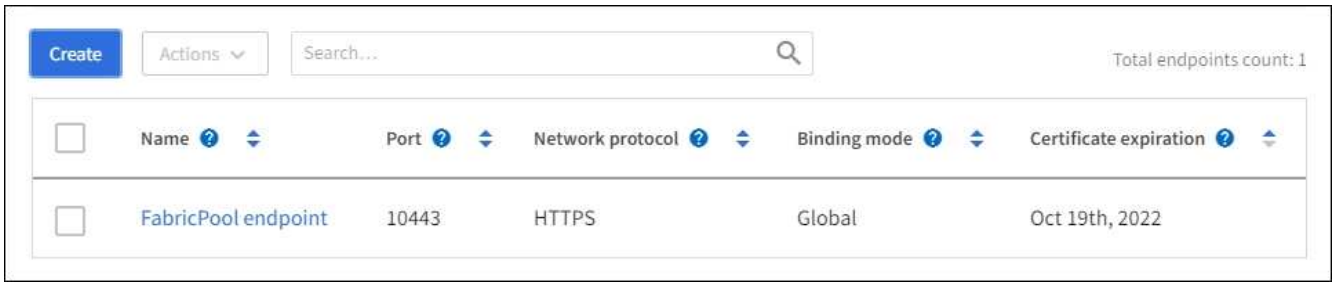
2. 提供S3和Swift用戶端連線至端點所需的資訊：
   - 連接埠號碼
   - 完整網域名稱或IP位址
   - 任何必要的憑證詳細資料

檢視及編輯負載平衡器端點

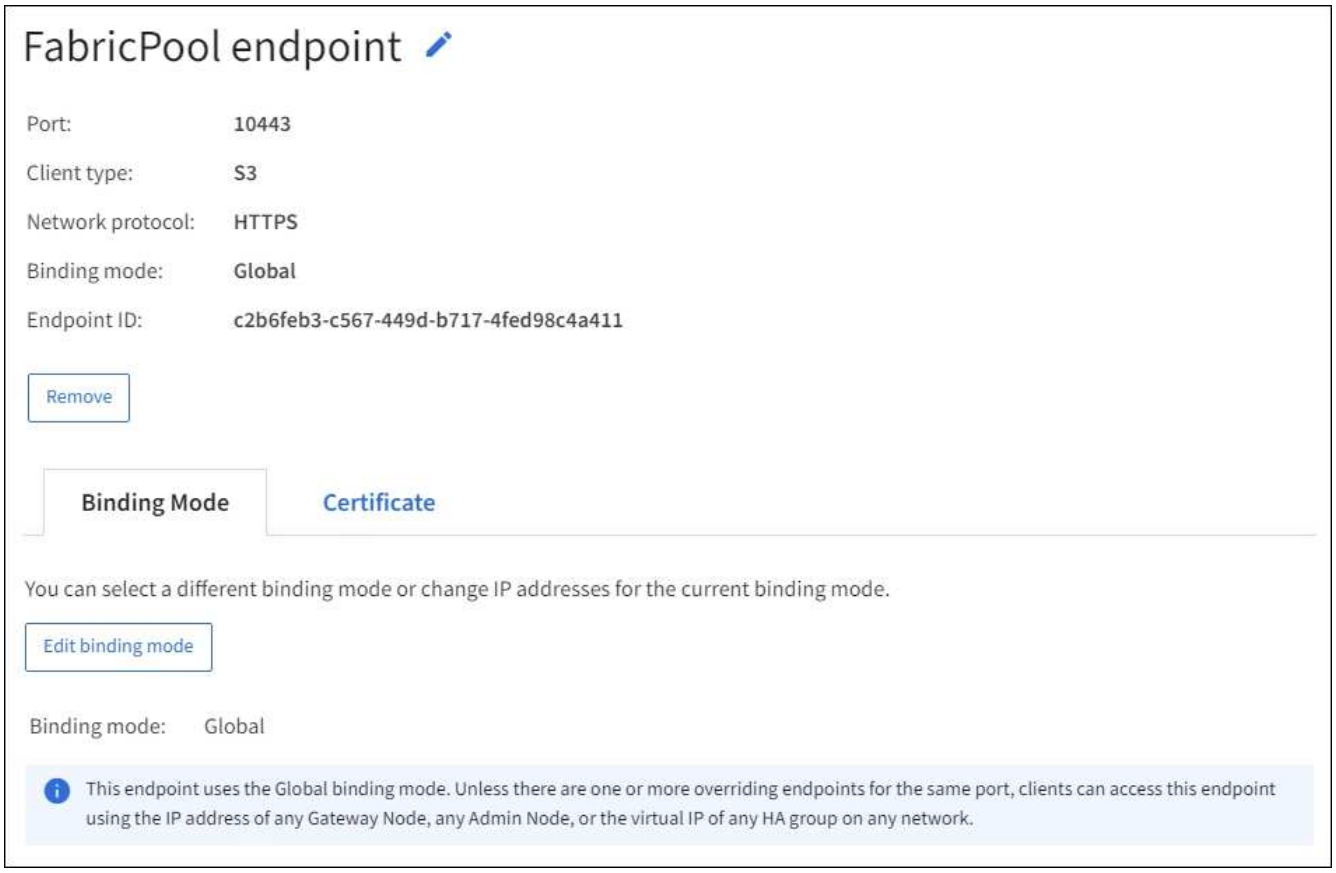
您可以檢視現有負載平衡器端點的詳細資料、包括安全端點的憑證中繼資料。您也可以變更端點的名稱或繫結模式、並更新任何相關的憑證。

您無法變更服務類型（S3或Swift）、連接埠或傳輸協定（HTTP或HTTPS）。

- 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。



- 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、或使用特定端點的詳細資料頁面。

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*。
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*。

工作	「行動」功能表	詳細資料頁面
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*。

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。

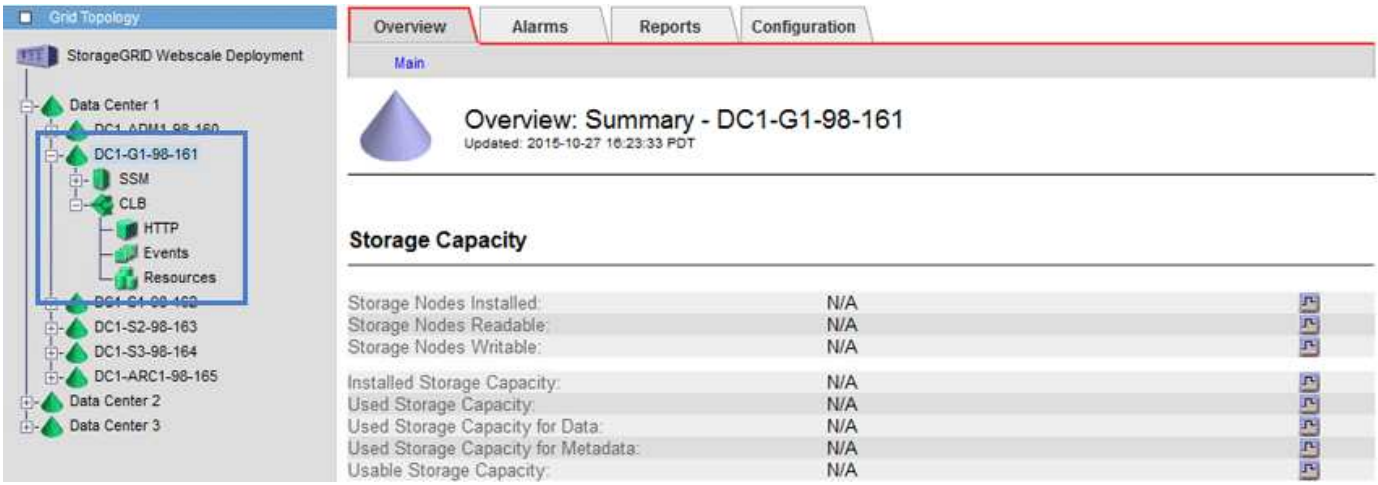
- 若要移除一或多個端點：
  a. 在「負載平衡器」頁面中、選取您要移除的每個端點核取方塊。
  b. 選擇*「Actions」（動作）>「Remove*」（移除
  c. 選擇*確定*。
- 若要從詳細資料頁面移除一個端點：
  a. 從「負載平衡器」頁面。選取端點名稱。
  b. 在詳細資料頁面上選取*移除*。
  c. 選擇*確定*。

負載平衡的運作方式**- CLB**服務（已過時）

閘道節點上的連線負載平衡器（CLB）服務已過時。負載平衡器服務現在是建議的負載平衡機制。

CLB服務使用第4層負載平衡、根據可用度、系統負載及系統管理員設定的連結成本、將傳入的TCP網路連線從用戶端應用程式分散到最佳儲存節點。選擇最佳化儲存節點時、CLB服務會建立雙向網路連線、並將流量轉送至所選節點、或從所選節點轉送流量。當引導傳入網路連線時、CLB並不考慮Grid Network組態。

若要檢視CLB服務的相關資訊、請選取*支援*>*工具*>*網格拓撲*、然後展開閘道節點、直到您選取* CLB*及其下方的選項為止。



如果您選擇使用CLB服務、則應考慮設定StorageGRID 您的故障系統連結成本。

- 什麼是連結成本
- 更新連結成本

設定S3 API端點網域名稱

若要支援S3虛擬託管樣式要求、您必須使用Grid Manager來設定S3用戶端所連線的端點網域名稱清單。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 您已確認網格升級尚未進行。

> 進行網格升級時、請勿對網域名稱組態進行任何變更。

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。
- 請確認用戶端用於HTTPS連線StorageGRID 的驗證書已針對用戶端所需的所有網域名稱簽署。

  例如、如果端點是「3.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。針對用戶端用來建立連線的IP位址、加入DNS記錄、並確保記錄會參考所有必要的端點網域名稱、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。

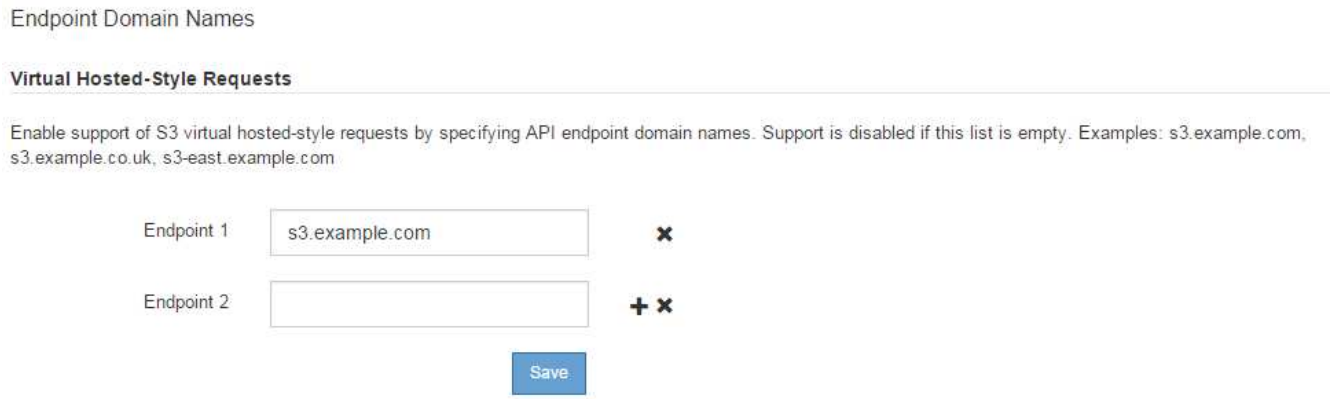
使用HTTPS連線（建議）到網格的用戶端可使用下列任一憑證：

- 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端點網域名稱。
- 連接負載平衡器端點、直接連接至儲存節點、或直接連接至閘道節點上已過時的CLB服務的用戶端、可以自訂全域S3和Swift API憑證、以包含所有必要的端點網域名稱。

步驟

1. 選擇*組態*>*網路*>*網域名稱*。

   此時會出現「端點網域名稱」頁面。



2. 在*端點*欄位中輸入S3 API端點網域名稱清單。使用 ➕ 圖示以新增其他欄位。

   如果此清單為空白、則會停用S3虛擬託管樣式要求的支援。

3. 選擇*保存*。
4. 確保用戶端使用的伺服器憑證符合所需的端點網域名稱。
   - 如果用戶端連線到使用自己憑證的負載平衡器端點、請更新與端點相關的憑證。
   - 如果用戶端連線至使用全域S3和Swift API憑證的負載平衡器端點、直接連線至儲存節點、或連線至閘道節點上的CLB服務、請更新全域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「bucket.s3.company.com`」時、DNS伺服器會解析為正確的端點、而且憑證會依預期驗證端點。

相關資訊

- 使用S3
- 檢視IP位址
- 設定高可用度群組
- 設定S3和Swift API憑證
- 設定負載平衡器端點

啟用**HTTP**以進行用戶端通訊

根據預設、用戶端應用程式會使用HTTPS網路傳輸協定來連線至儲存節點或閘道節點上已過時的CLB服務。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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

只有當S3和Swift用戶端需要直接建立HTTP連線至儲存節點或閘道節點上已過時的CLB服務時、才需完成此工作。

您不需要為只使用HTTPS連線的用戶端或連線至負載平衡器服務的用戶端完成此工作（因為您可以將每個負載平衡器端點設定為使用HTTP或HTTPS）。如需詳細資訊、請參閱設定負載平衡器端點的相關資訊。

請參閱 摘要：用於用戶端連線的IP位址和連接埠 以瞭解使用HTTP或HTTPS連線至儲存節點或過時的CLB服務時、S3和Swift用戶端會使用哪些連接埠

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。

步驟

1. 選擇*組態*>*系統*>*網格選項*。
2. 在「網路選項」區段中、選取「啟用**HTTP**連線」核取方塊。

3. 選擇*保存*。

相關資訊

- 設定負載平衡器端點
- 使用S3
- 使用Swift

控制允許哪些用戶端作業

您可以選取「防止用戶端修改」網格選項、以拒絕特定的HTTP用戶端作業。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

「防止用戶端修改」是全系統設定。選取「阻止用戶端修改」選項時、下列要求將遭拒：

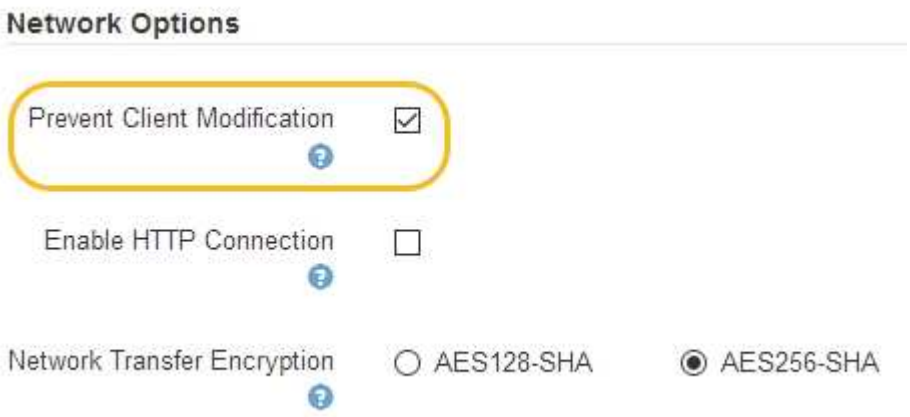
- * S3 REST API*
  - 刪除時段要求
  - 任何修改現有物件資料、使用者定義中繼資料或S3物件標記的要求

> 此設定不適用於已啟用版本管理的儲存區。版本管理功能已防止修改物件資料、使用者定義的中繼資料及物件標記。

- * 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。

步驟

1. 選擇*組態*>*系統*>*網格選項*。
2. 在「網路選項」區段中、選取「防止用戶端修改」核取方塊。



3. 選擇*保存*。

管理網路和連線

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StorageGRID 個支援網格的節點都需要一個專屬的網路介面、IP位址、子網路遮罩和閘道、以供指派給每個節點的網路使用。
- 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）	eth2

- 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
- * RHEL或CentOS（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、CentOS、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。

您需要的產品

您將使用登入Grid Manager 支援的網頁瀏覽器。

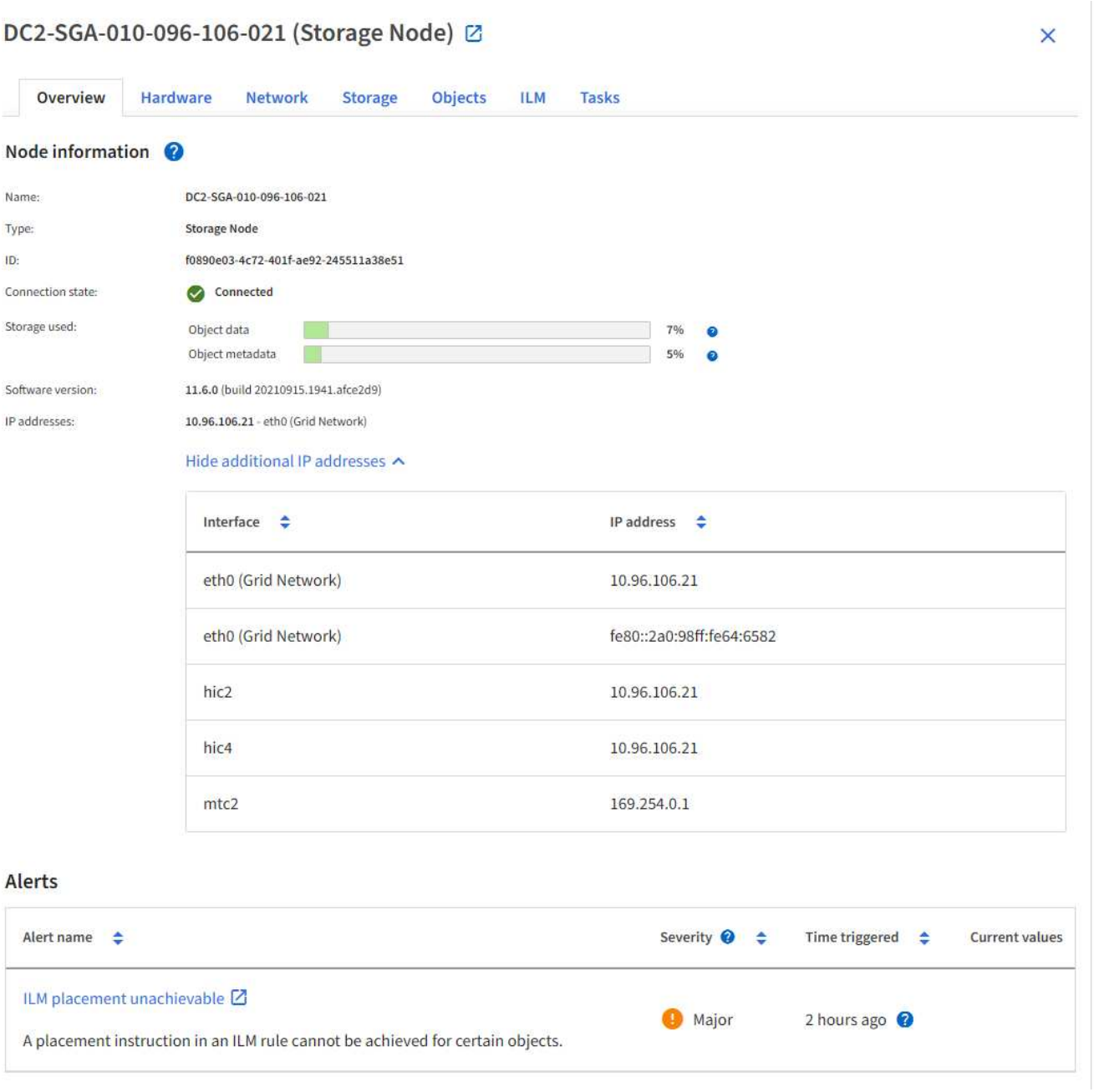
關於這項工作

如需變更IP位址的資訊、請參閱 恢復與維護。

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。



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。

TLS組態選項、例如傳輸協定版本、密碼、金鑰交換演算法和MAC演算法、在StorageGRID 無法在支援中設定。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。

支援的**TLS 1.2**加密套件

支援下列TLS 1.2加密套件：

- TLS_ECDHE_RSA_with _AES-122_GCM_SHA256
- TLS_ECDHE_RSA_with _AES-256_GCM_SHA384
- TLS_ECDHE_ECDSa_with _AES-122_GCM_SHA256
- TLS_ECDHE_ECDSa_with _AES-256_GCM_SHA384
- TLS_ECDHE_RSA_with _CHACHA20_POLY1305
- TLS_ECDHE_ECDSa_with _CHACHA20_POLY1305
- TLS_RSA_AT_AES-122_GCM_SHA256
- TLS_RSA_AT_AES-256_GCM_SHA384

支援的**TLS 1.3**加密套件

支援下列TLS 1.3加密套件：

- TLS_AES-256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES-128_GCM_SHA256

變更網路傳輸加密

此系統使用傳輸層安全（TLS）StorageGRID 來保護網格節點之間的內部控制流量。「網路傳輸加密」選項可設定TLS用來加密網格節點之間的控制流量的演算法。此設定不會影響資料加密。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

依預設、網路傳輸加密使用ES256-SHA演算法。控制流量也可使用ES128/SHA演算法加密。

步驟

1. 選擇*組態*>*系統*>*網格選項*。
2. 在「Network Options（網路選項）」區段中、將「Network Transfer Encryption（網路傳輸加密）」變更為* AES128/SHA*或* AES256-SHA*（預設）。

3. 選擇*保存*。

管理流量分類原則

管理流量分類原則

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
- 租戶
- 子網路（包含用戶端的IPv4子網路）
- 端點（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

您也可以根據下列參數、為原則設定限制：

- 中的Aggregate頻寬
- Aggregate Bandwidth Out
- 並行讀取要求
- 並行寫入要求
- 中的每個要求頻寬
- 每個要求頻寬輸出
- 讀取要求率
- 寫入要求率

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 、不能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。

每個負載平衡器都會實作流量分類限制。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。

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	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 K個要求 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

如果您想要依儲存區、租戶、IP子網路或負載平衡器端點來監控及選擇性地限制網路流量、請建立流量分類原則。您也可以根據頻寬、並行要求數或要求率、來設定原則限制。

您需要的產品

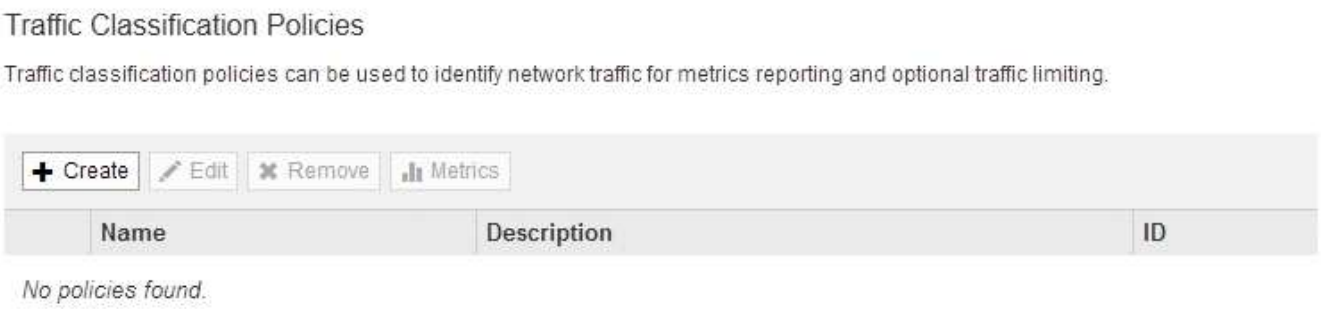
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有root存取權限。
- 您已建立任何想要比對的負載平衡器端點。

- 您已建立任何想要比對的租戶。

步驟

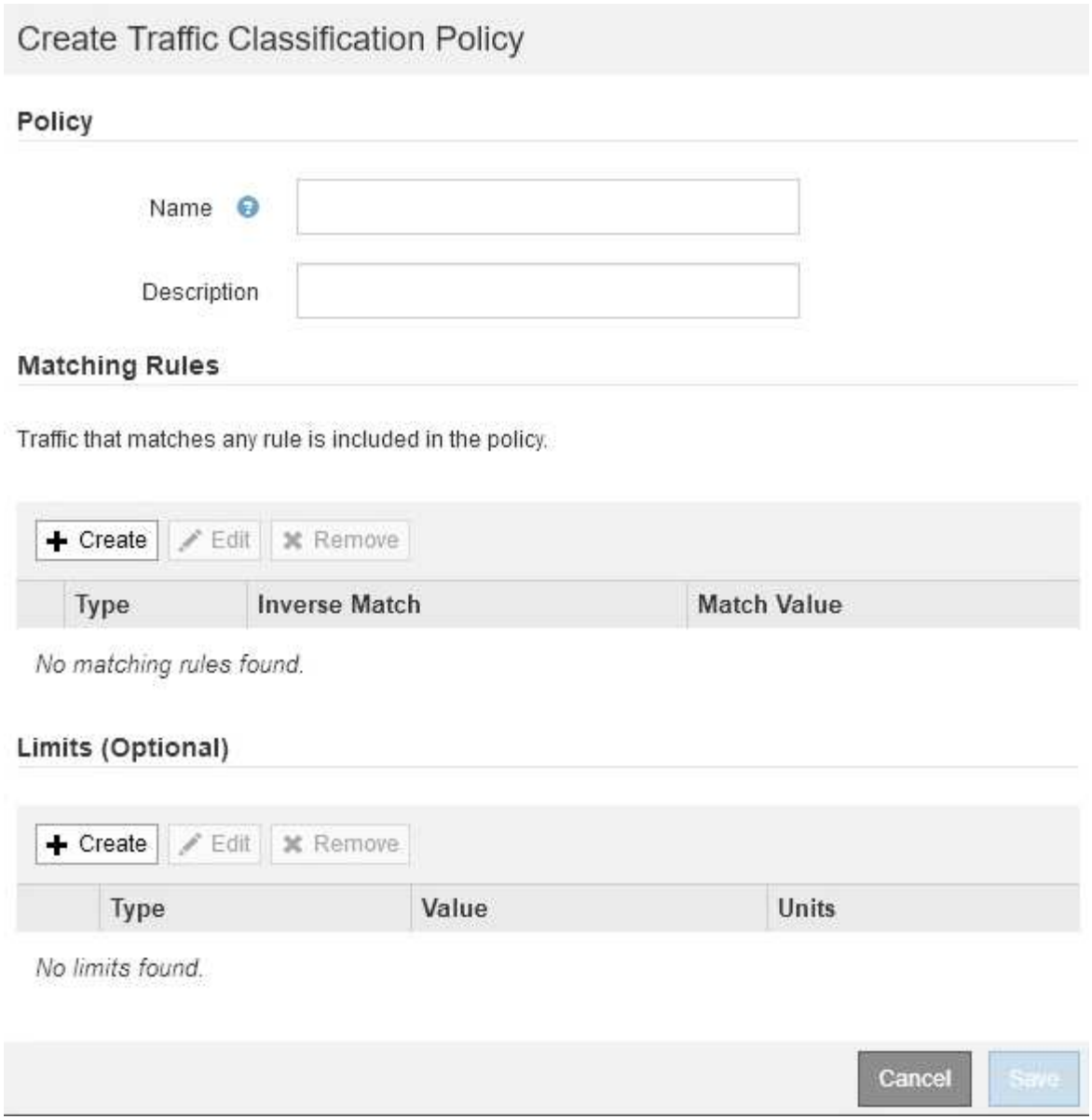
1. 選擇*組態*>*網路*>*流量分類*。

   此時會出現「流量分類原則」頁面。



2. 選擇* Create （建立）。

   此時會出現「建立流量分類原則」對話方塊。



3. 在*名稱*欄位中、輸入原則的名稱。

   輸入描述性名稱、以便辨識原則。

4. 或者、您也可以在「說明」欄位中新增原則的說明。

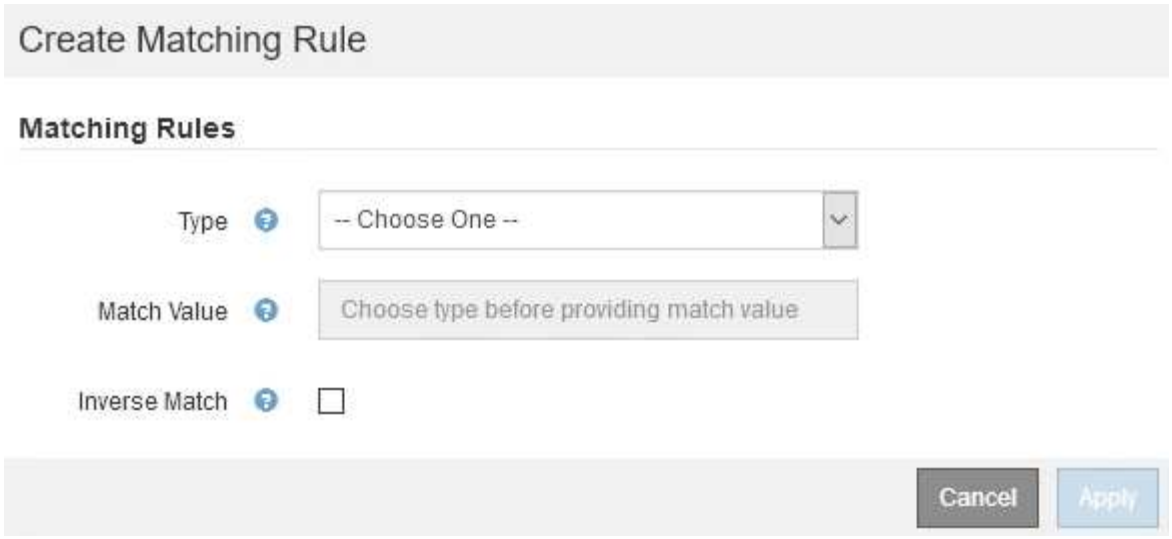
   例如、請說明此流量分類原則的適用範圍及限制。

5. 為原則建立一或多個相符的規則。

   相符的規則可控制哪些實體會受到此流量分類原則的影響。例如、如果您要將此原則套用至特定租戶的網路流量、請選取租戶。或者、如果您想要將此原則套用至特定負載平衡器端點上的網路流量、請選取「端點」。

   a. 在*匹配規則*部分中選擇*創建*。

      此時將出現Create Matching Rule（建立符合規則）對話方塊。



b. 從*類型*下拉式清單中、選取要納入比對規則的實體類型。

c. 在*符合值*欄位中、根據您選擇的實體類型輸入相符值。

- 儲存區：輸入儲存區名稱。
- Bucket Regex：輸入將用於符合一組儲存貯體名稱的規則運算式。

  規則運算式未鎖定。使用 {caret} 固定標記以符合庫位名稱開頭的名稱、並使用$標記以符合名稱結尾的名稱。

- CIDR：以CIDR表示法輸入符合所需子網路的IPV4子網路。
- 端點：從現有端點清單中選取端點。這些是您在「負載平衡器端點」頁面上定義的負載平衡器端點。請參閱 設定負載平衡器端點。
- 租戶：從現有租戶清單中選取租戶。租戶配對是根據所存取的貯體所有權而定。匿名存取某個庫位符合擁有庫位的租戶。

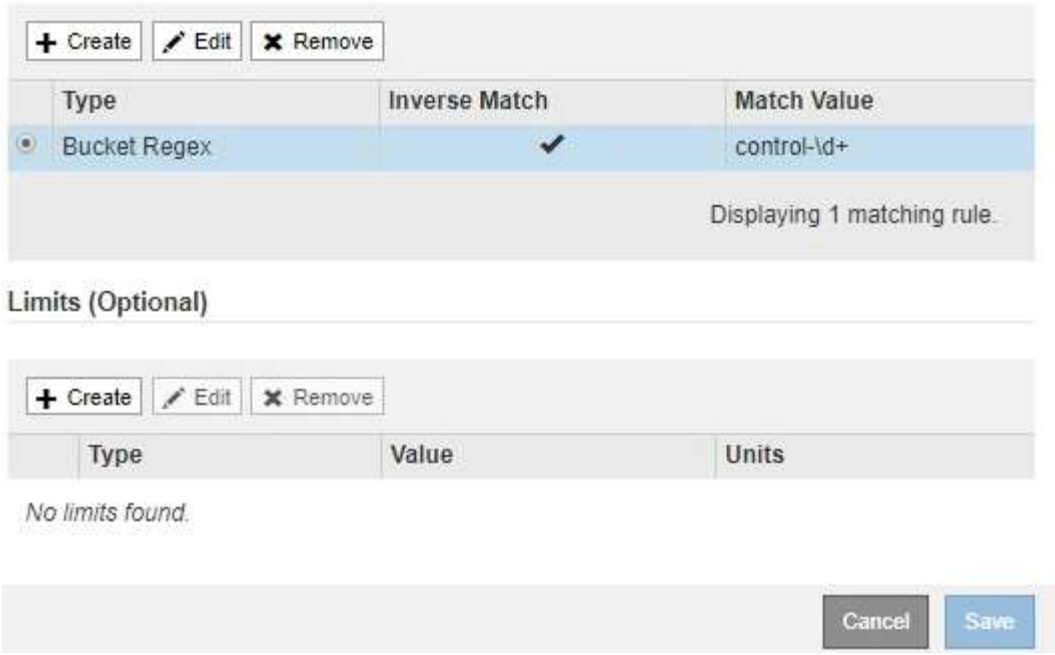
d. 如果您想要比對所有符合剛剛定義之類型與相符值的網路流量_avi__流量、請選取「* Inverse （*反轉）」核取方塊。否則、請取消選取核取方塊。

例如、如果您想要將此原則套用至除其中一個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* Inverse *。

> 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。

e. 選擇*應用*。

規則隨即建立、並列在「符合規則」表格中。



a. 針對您要為原則建立的每個規則、重複這些步驟。

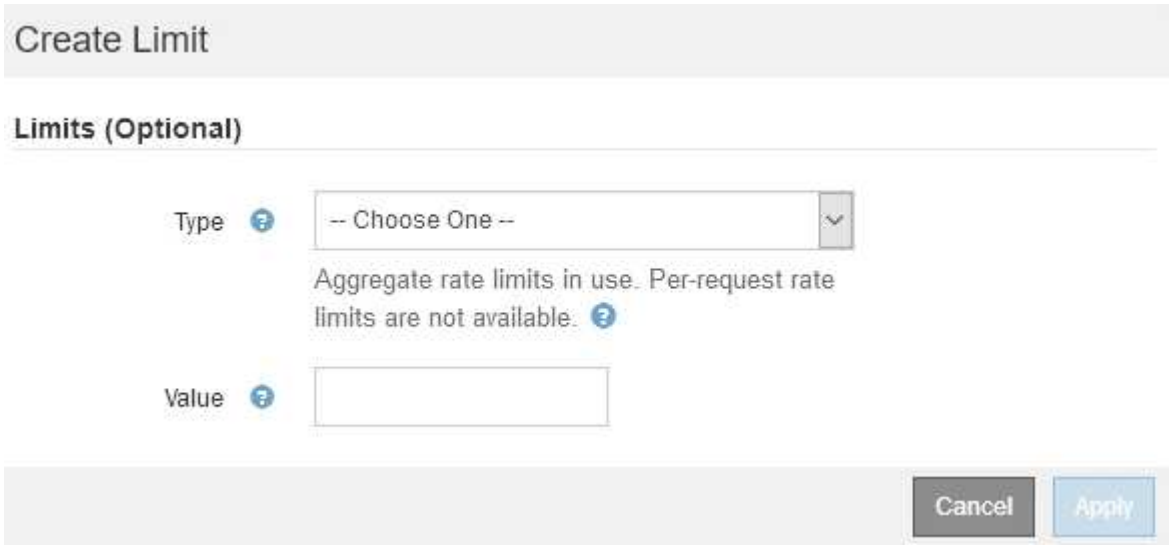
符合任何規則的流量會由原則處理。

6. 或者、為原則建立限制。

即使您未建立限制、StorageGRID 也會收集指標、以便監控符合原則的網路流量。

a. 在「限制」區段中選取「建立」。

「建立限制」對話方塊隨即出現。



b. 從*類型*下拉式清單中、選取要套用至原則的限制類型。

在下列清單中、*輸入*是指從S3或Swift用戶端到StorageGRID 平衡負載平衡器的流量、*輸出*是指從負載平衡器到S3或Swift用戶端的流量。

- 中的Aggregate頻寬
- Aggregate Bandwidth Out
- 並行讀取要求
- 並行寫入要求
- 中的每個要求頻寬
- 每個要求頻寬輸出
- 讀取要求率
- 寫入要求率

> 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 、不能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。

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。根據以下順序、執行「最佳」頻寬限制：StorageGRID

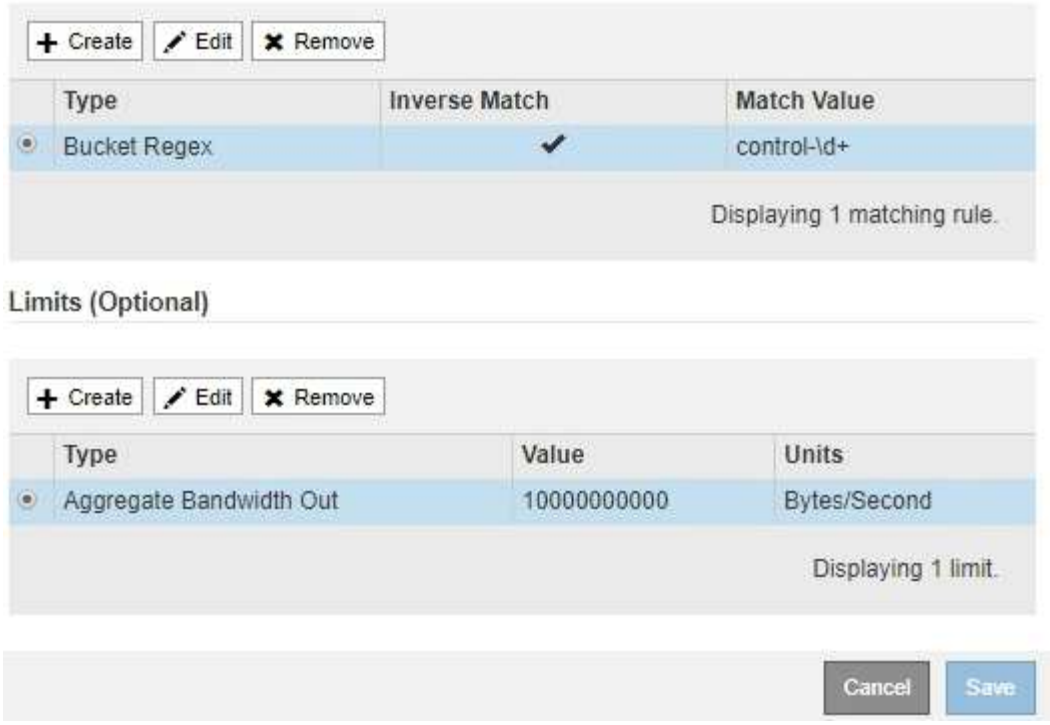
- 確切IP位址（/32遮罩）
- 確切的儲存區名稱
- 鏟斗回收系統
- 租戶
- 端點
- 非精確的CIDR相符項目（非/32）
- 反比對

c. 在*值*欄位中、輸入所選限制類型的數值。

當您選取限制時、會顯示預期的單位。

d. 選擇*應用*。

限制隨即建立、並列在「限制」表格中。



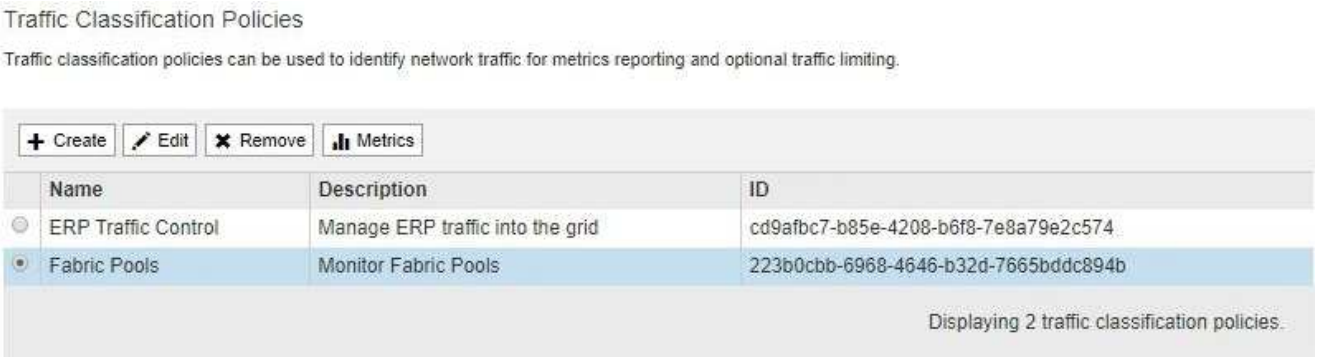
e. 針對您要新增至原則的每個限制重複這些步驟。

例如、如果您想為SLA層建立40 Gbps頻寬限制、請建立Aggregate Bandwidth In限制和Aggregate Bandwidth Out限制、並將每個限制設定為40 Gbps。

若要將每秒百萬位元組轉換為每秒十億位元組、請乘以八。例如、125 MB/s相當於1、000 Mbps或1 Gbps。

7. 當您完成規則與限制的建立後、請選取*「Save」（儲存）*。

原則隨即儲存、並列在「流量分類原則」表中。



S3和Swift用戶端流量現在是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。請參閱 檢視網路流量指標。

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。

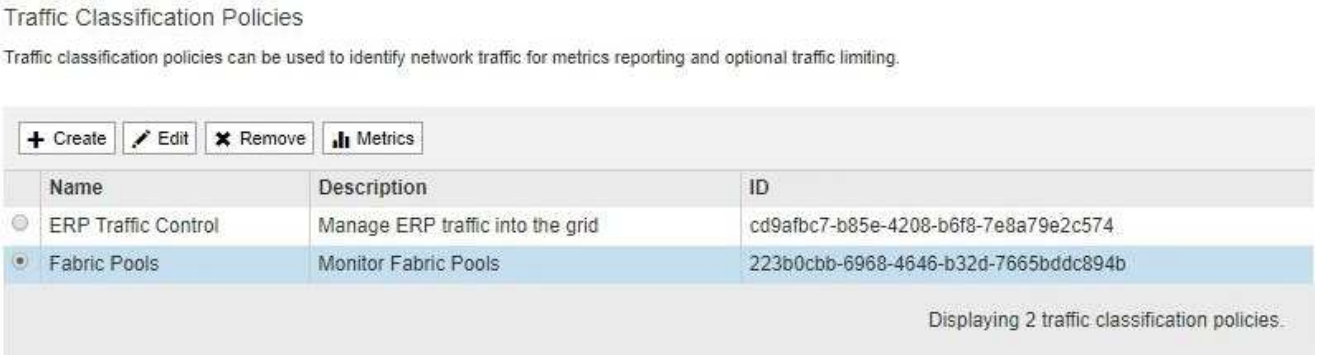
您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有root存取權限。

步驟

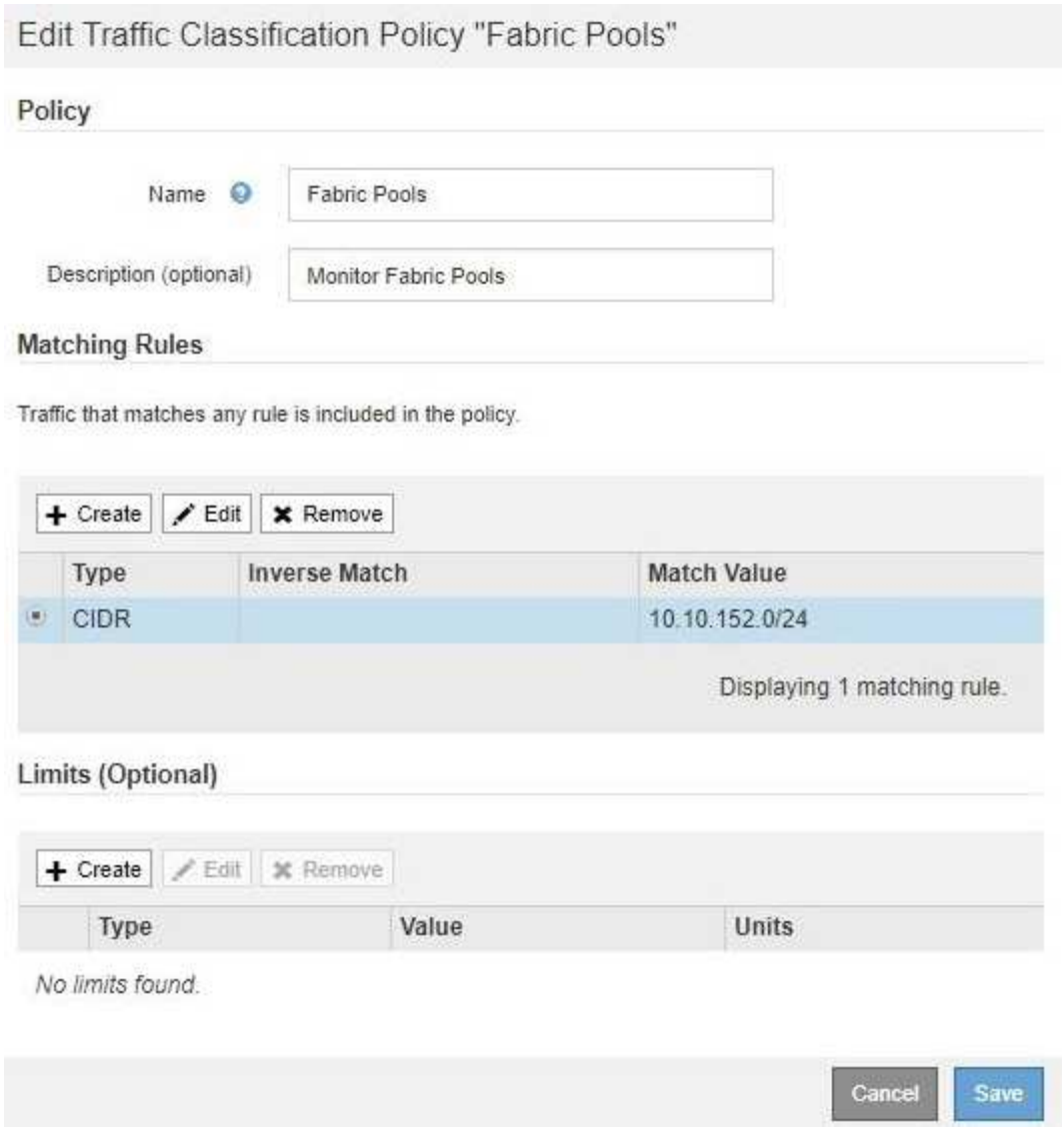
1. 選擇*組態*>*網路*>*流量分類*。

   「流量分類原則」頁面隨即出現、表中會列出現有的原則。



2. 選取您要編輯之原則左側的選項按鈕。
3. 選擇*編輯*。

   此時會出現「編輯流量分類原則」對話方塊。



4. 視需要建立、編輯或移除相符的規則和限制。
   a. 若要建立相符的規則或限制、請選取*「建立*」、然後依照指示建立規則或建立限制。
   b. 若要編輯相符的規則或限制、請選取規則或限制的選項按鈕、在「符合的規則」區段或「限制」區段中選取*編輯*、然後依照指示建立規則或建立限制。
   c. 若要移除相符的規則或限制、請選取規則或限制的選項按鈕、然後選取*移除*。然後選取*確定*以確認您要移除規則或限制。
5. 當您完成規則或限制的建立或編輯之後、請選取*套用*。
6. 編輯完原則後、請選取*儲存*。

   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

如果不再需要流量分類原則、您可以將其刪除。

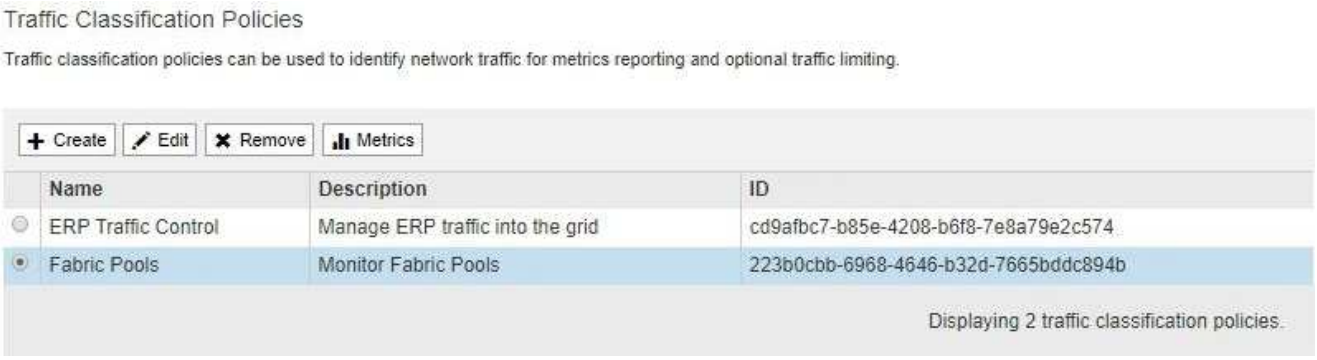
您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有root存取權限。

步驟

1. 選擇*組態*>*網路*>*流量分類*。

   「流量分類原則」頁面隨即出現、表中會列出現有的原則。



2. 選取您要刪除之原則左側的選項按鈕。
3. 選擇*移除*。

   此時會出現警告對話方塊。

4. 選擇*確定*以確認您要刪除原則。

   原則即會刪除。

檢視網路流量指標

您可以檢視「流量分類原則」頁面中可用的圖表、以監控網路流量。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您具有根存取權限或租戶帳戶權限。

關於這項工作

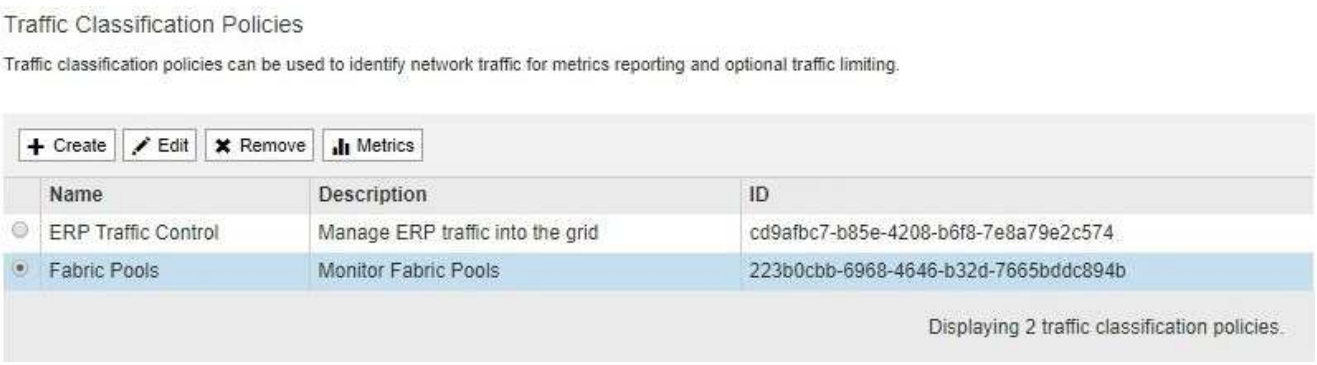
對於任何現有的流量分類原則、您都可以檢視負載平衡器服務的度量、以判斷原則是否成功限制網路上的流量。圖表中的資料可協助您判斷是否需要調整原則。

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*。

   「流量分類原則」頁面隨即出現、表中會列出現有的原則。



   如果您具有租戶帳戶權限、但您沒有根存取權限、則「建立」、「編輯」和「移除」按鈕會停用。

2. 選取您要檢視其度量的原則左側的選項按鈕。
3. 選取* Metrics *。

   隨即開啟新的瀏覽器視窗、並顯示「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。

   您可以使用* policies *下拉式清單來選取要檢視的其他原則。

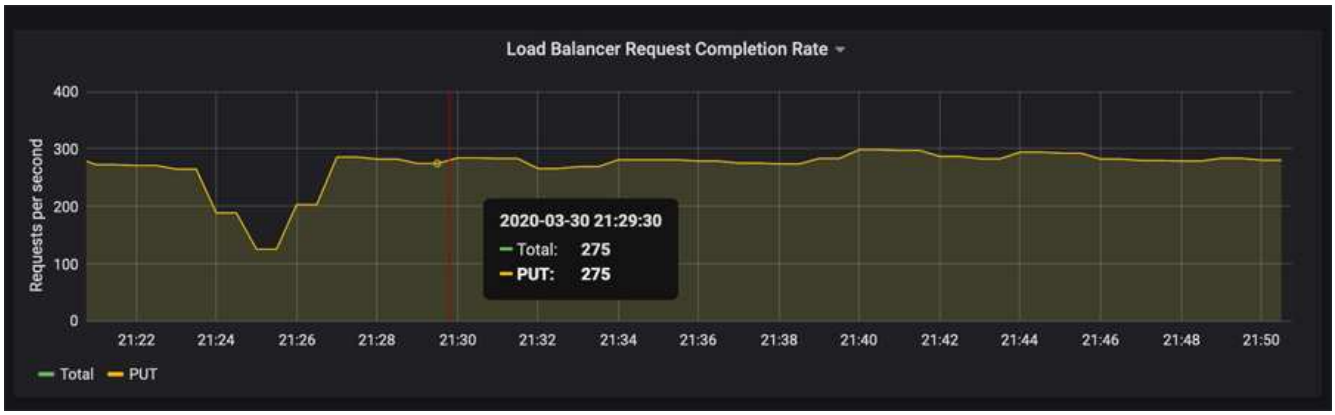
   網頁上包含下列圖表。

   - 負載平衡器要求流量：此圖表提供負載平衡器端點與提出要求之用戶端之間傳輸資料處理量的3分鐘移動

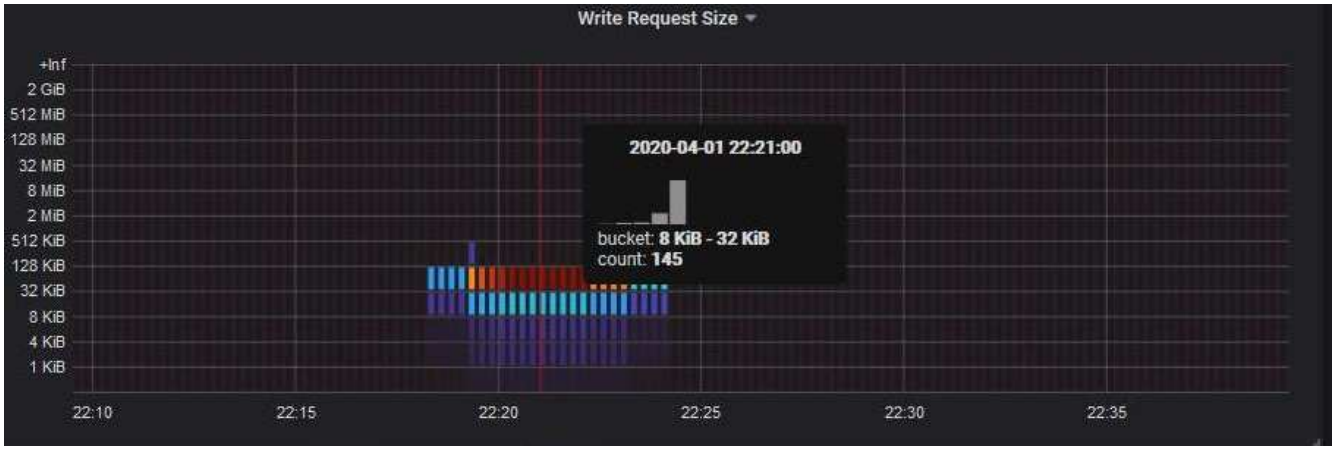
平均、單位為位元/秒。

- 負載平衡器要求完成率：此圖表提供每秒已完成要求數的3分鐘移動平均、並依要求類型（Get、PUT、HEAD和DELETE）細分。此值會在新要求的標頭經過驗證時更新。
- 錯誤回應率：此圖表提供每秒傳回用戶端的錯誤回應數移動平均3分鐘、並依錯誤回應代碼細分。
- 平均申請持續時間（非錯誤）：此圖表提供3分鐘的申請平均移動時間、並依申請類型（Get、PUT、HAD和DELETE）細分。每個要求持續時間都會在負載平衡器服務剖析要求標頭時開始、並在完整回應本文傳回用戶端時結束。
- 依物件大小寫入要求率：此熱圖提供根據物件大小完成寫入要求的3分鐘移動平均速度。在這種情況下、寫入要求僅指置入要求。
- 依物件大小讀取要求率：此熱圖提供根據物件大小完成讀取要求的3分鐘移動平均速度。在這種情況下、讀取要求只是指取得要求。熱圖中的色彩表示個別圖表中物件大小的相對頻率。較冷的色彩（例如、紫色和藍色）表示相對速率較低、較暖的色彩（例如橘色和紅色）表示相對速率較高。

4. 將游標停留在折線圖上、即可在圖表的特定部分看到值快顯視窗。



5. 將游標停留在熱圖上、即可看到快顯視窗、其中顯示樣本的日期和時間、彙總到該計數的物件大小、以及該期間每秒要求數。



6. 使用左上角的* Policy*下拉式清單來選取不同的原則。

   所選原則的圖表隨即顯示。

7. 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. 在頁面的「* Grafana*」區段中、選取「流量分類政策」。

c. 從頁面左上角的下拉式清單中選取原則。

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。

8. 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。

相關資訊

監控及疑難排解

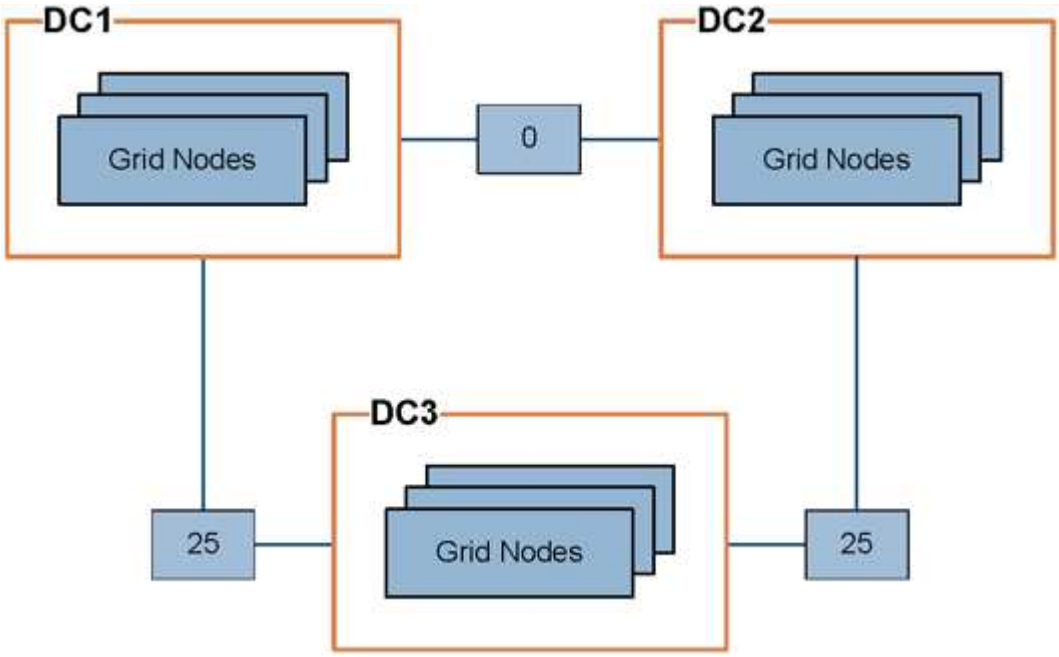
管理連結成本

什麼是連結成本

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。

- 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。
- 閘道節點上的過時連線負載平衡器（CLB）服務會使用連結成本來引導用戶端連線。請參閱 負載平衡的運作方式- CLB服務。

此圖顯示三個站台網格、其中設定站台之間的連結成本：



- 閘道節點上的CLB服務會將用戶端連線平均分配給同一個資料中心站台上的所有儲存節點、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、因為從DC1到D2的連結成本為0、低於從DC3到DC2（25）的連結成本。

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

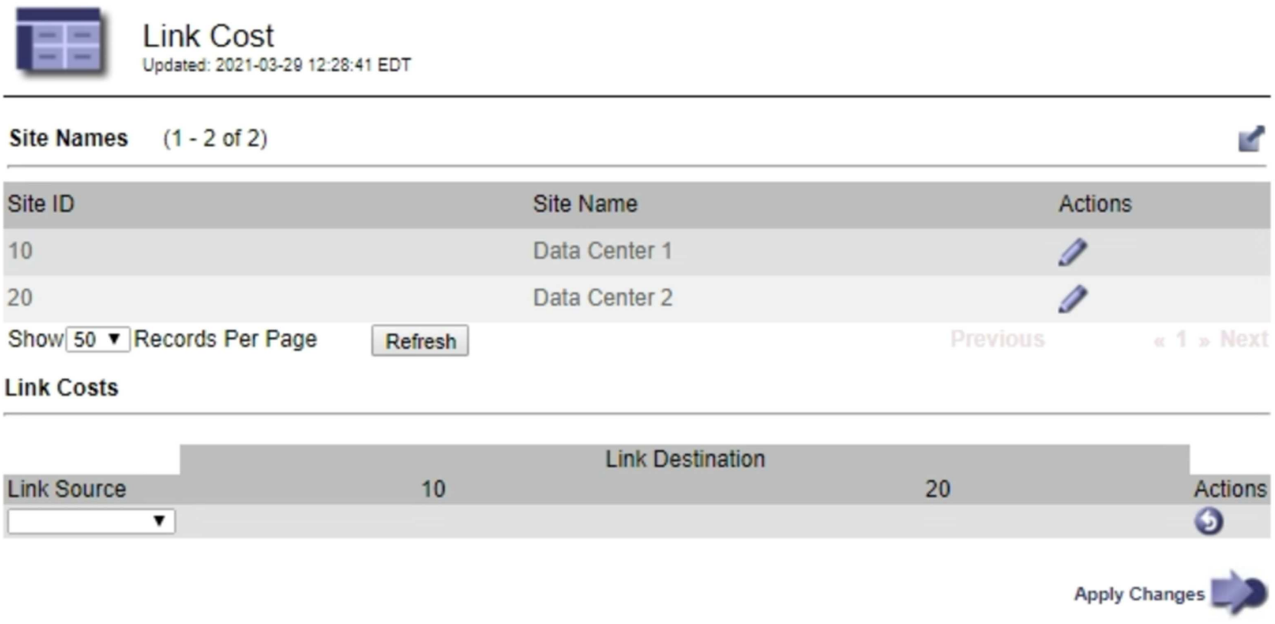
您可以更新資料中心站台之間的連結成本、以反映站台之間的延遲。

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Grid拓撲頁面組態權限。

步驟

1. 選擇*組態*>*網路*>*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

什麼是AutoSupport 功能？

利用此功能、您的整套系統可將健全狀況和狀態訊息傳送給技術支援部門。AutoSupport StorageGRID

使用NetApp可大幅加速問題的判斷與解決。AutoSupport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。或者、您可以設定AutoSupport 要傳送至另一個目的地的消息。

資訊包含在AutoSupport 消息中

包含下列資訊的資訊：AutoSupport

- 軟體版本StorageGRID
- 作業系統版本
- 系統層級和位置層級的屬性資訊
- 最近的警示和警示（舊系統）
- 所有網格工作（包括歷史資料）的目前狀態
- 管理節點資料庫使用量
- 遺失或遺失物件的數量
- 網格組態設定
- NMS實體
- 作用中ILM原則
- 已配置的網格規格檔案
- 診斷指標

您可以在AutoSupport 第一次安裝時啟用「支援」功能和個別AutoSupport 的「支援」選項StorageGRID 、也可以稍後啟用。如果AutoSupport 未啟用此功能、網格管理器儀表板上會顯示一則訊息。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。

什麼是數位顧問？

數位顧問是雲端型的，運用 NetApp 安裝基礎的預測分析和社群智慧。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。

如果您想要使用 NetApp 支援網站上的數位顧問儀表板和功能，則必須啟用 AutoSupport 。

"數位顧問文件"

傳送**AutoSupport** 資訊的通訊協定

您可以從三種傳輸協定中選擇一種來傳送AutoSupport 功能性訊息：

- HTTPS
- HTTP
- SMTP

如果使用AutoSupport HTTPS或HTTP傳送靜態訊息、您可以在管理節點和技術支援之間設定不透明的Proxy伺服器。

如果您使用SMTP做為AutoSupport 靜態訊息的傳輸協定、則必須設定一個SMTP郵件伺服器。

選項**AutoSupport**

您可以使用下列選項的任意組合、將AutoSupport 資訊傳送給技術支援人員：

- 每週：每AutoSupport 週自動傳送一次資訊。預設設定：已啟用。
- 事件觸發：AutoSupport 每小時或發生重大系統事件時、自動傳送不實訊息。預設設定：已啟用。
- 隨需：允許技術支援人員要求StorageGRID 您的支援中心AutoSupport 自動傳送功能性資訊、這在他們主動處理問題時非常實用（需要HTTPS AutoSupport 更新傳輸協定）。預設設定：停用。
- 使用者觸發：AutoSupport 隨時手動傳送不全訊息。

相關資訊

"NetApp支援"

設定**AutoSupport** 功能

您可以在AutoSupport 第一次安裝時啟用「支援」功能和個別AutoSupport 的「支援」選項StorageGRID 、也可以稍後啟用。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您具有根存取權限或其他網格組態權限。
- 如果您將使用HTTPS或HTTP傳輸協定來傳送AutoSupport 不實訊息、則表示您已直接或使用Proxy伺服器（不需要傳入連線）、提供對主要管理節點的傳出網際網路存取。
- 如果您要使用HTTPS或HTTP傳輸協定、而且想要使用Proxy伺服器、您就有了 已設定管理Proxy伺服器。
- 如果您將使用SMTP做AutoSupport 為中繼訊息的傳輸協定、則表示您已設定了一個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）。

指定**AutoSupport** 訊息的傳輸協定

您可以使用下列任一種通訊協定來傳送AutoSupport 不包含任何資訊的訊息：

- * HTTPS *：這是新安裝的預設及建議設定。HTTPS傳輸協定使用連接埠443。如果您想要啟用AutoSupport「根據需求提供支援」功能、則必須使用HTTPS傳輸協定。
- * HTTP：此傳輸協定不安全、除非用於受信任的環境、在透過網際網路傳送資料時、Proxy伺服器會轉換成HTTPS。HTTP傳輸協定使用連接埠80。
- * SMTP*：如果您想AutoSupport 要以電子郵件寄送不一樣的訊息、請使用此選項。如果您使用SMTP做為AutoSupport 不實訊息的傳輸協定、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）上設定一個SMTP郵件伺服器。

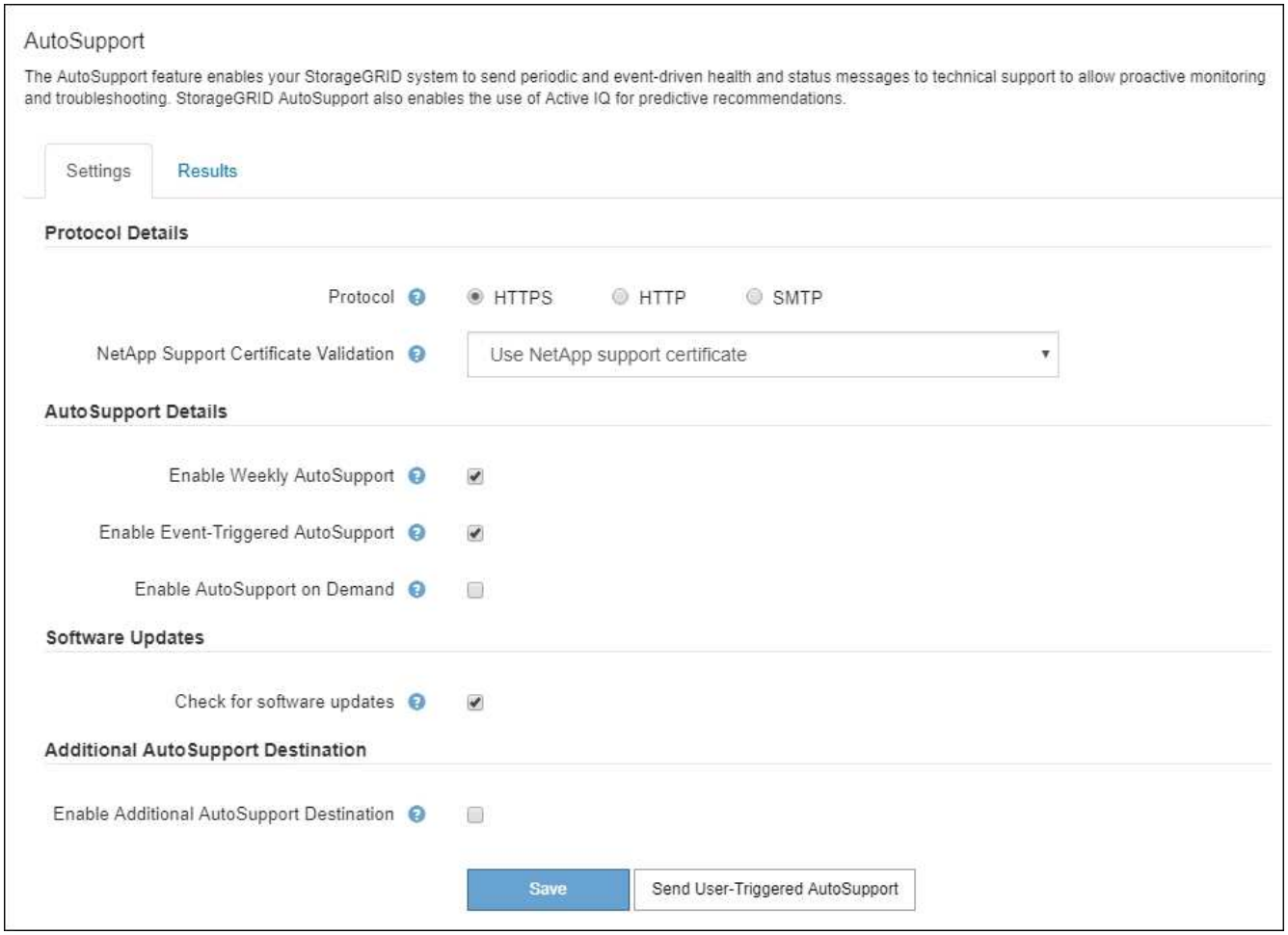
> ⓘ 在AutoSupport 發佈版更新版的過程中、只有使用SMTP作為唯一的傳輸協定、才能接收到有關消息的資訊。StorageGRID如果StorageGRID 您一開始安裝的是舊版的版本的、則可能是選取的傳輸協定。

您設定的傳輸協定用於傳送所有類型AutoSupport 的資訊。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。

   畫面會出現「the S還原」頁面、並選取「* Settings*」索引標籤。AutoSupport



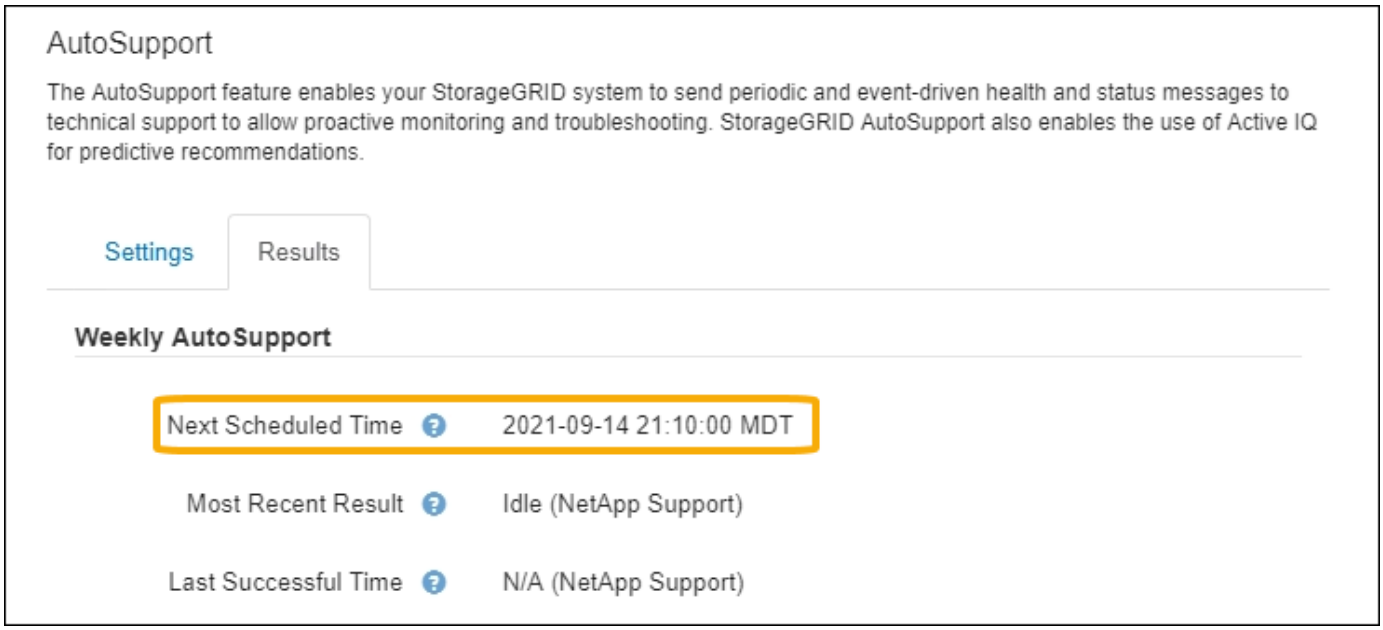
2. 選取您要用來傳送AutoSupport 資訊提示訊息的傳輸協定。
3. 如果您選取* HTTPS *、請選取是否要使用TLS憑證來保護與NetApp支援伺服器的連線安全。
   - 使用**NetApp**支援證書（預設）：憑證驗證可確保AutoSupport 傳輸不間斷的資訊安全無虞。NetApp支援證書已隨StorageGRID 支援軟體一起安裝。
   - 不驗證憑證：只有在有充分理由不使用憑證驗證時（例如憑證暫時有問題時）、才選取此選項。
4. 選擇*保存*。

   所有每週、使用者觸發和事件觸發的訊息都會使用選取的傳輸協定來傳送。

停用每週**AutoSupport** 更新訊息

根據預設StorageGRID 、將支援系統設定為每AutoSupport 週傳送一次消息給NetApp Support。

若要判斷何時AutoSupport 傳送每週更新訊息、請前往* AutoSupport 《》**>**《結果*》索引標籤。在「每週**AutoSupport** 資料」區段中、查看*下一個排程時間*的值。



您可以隨時停用自動傳送每週AutoSupport 更新訊息。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 取消選取「啟用每週**AutoSupport** 資訊」核取方塊。
3. 選擇*保存*。

停用事件觸發**AutoSupport** 的功能性訊息

根據預設、StorageGRID 當AutoSupport 發生重要警示或其他重大系統事件時、將會將此功能設定為傳送不必要訊息給NetApp支援部門。

您可以AutoSupport 隨時停用事件觸發的資訊技術訊息。

當AutoSupport 您在全系統抑制電子郵件通知時、也會抑制事件觸發的功能性訊息。（選擇*組態*>*系統*>*顯示選項*。然後選取*通知全部隱藏*。）

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 取消選取「啟用事件觸發**AutoSupport** 的**S**不到」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人員要求StorageGRID 您的支援系統AutoSupport 自動傳送各種資訊。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 隨需功能。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 選取* HTTPS *作為傳輸協定。
3. 選取「啟用每週**AutoSupport** 資訊」核取方塊。
4. 選中* Enable AutoSupport SRAID on Demand*（按需啓用）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. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 取消選取*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 此功能時、便會將健全狀況和狀態訊息傳送給NetApp支援部門。您可以為所有AutoSupport 的資訊提供額外的目的地。

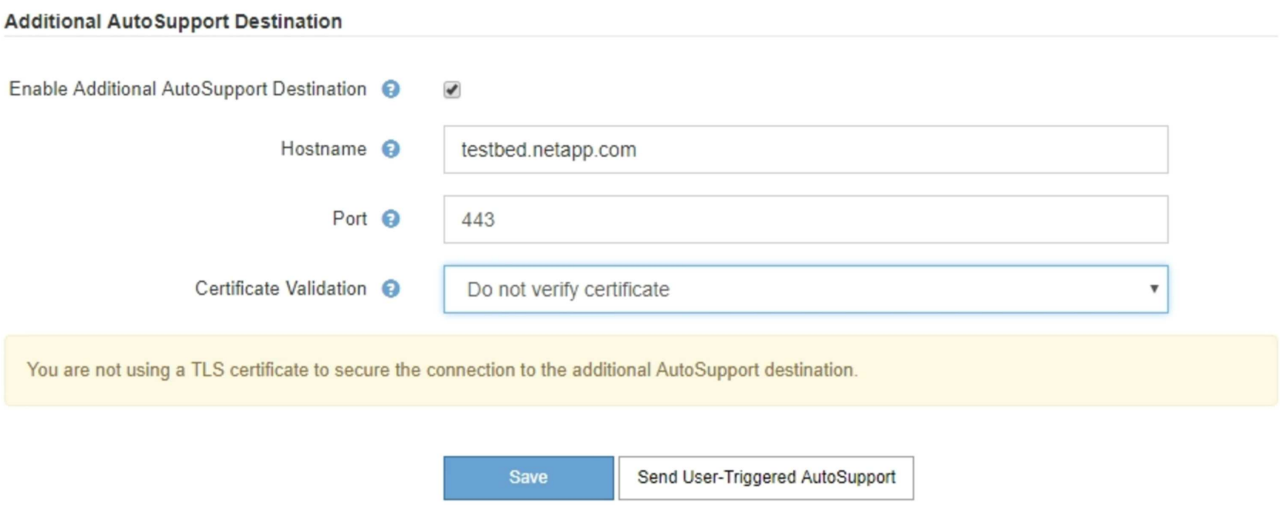
若要驗證或變更用來傳送AutoSupport 資訊提示訊息的傳輸協定、請參閱的指示 指定AutoSupport 訊息的傳輸協定。

> 您無法使用SMTP傳輸協定將AutoSupport 無法傳送的資訊傳送到其他目的地。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。
2. 選取*啟用其他AutoSupport 目的地*。

   此時會出現其他AutoSupport 的「目的地」欄位。



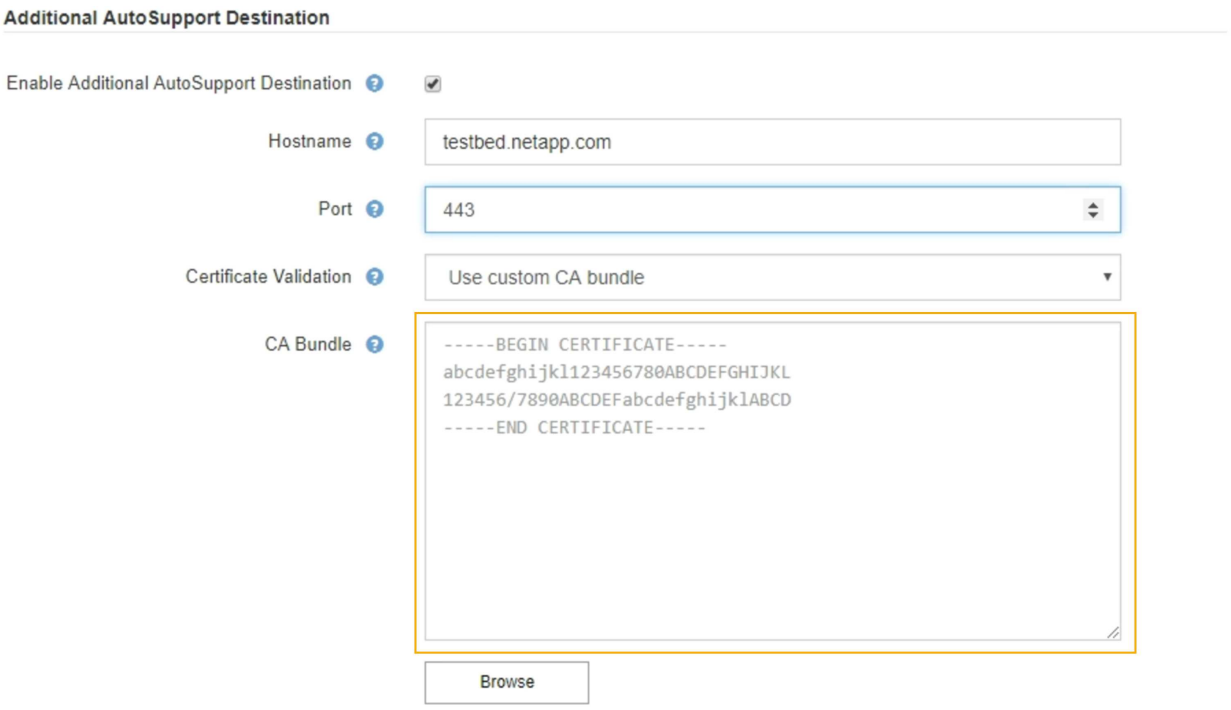
3. 輸入額外AutoSupport 的目的地伺服器的伺服器主機名稱或IP位址。

   您只能輸入一個額外的目的地。

4. 輸入用來連線至其他AutoSupport 目的地伺服器的連接埠（HTTP預設為連接埠80、HTTPS預設為連接埠443）。

5. 若要使用AutoSupport 憑證驗證傳送您的不完整訊息、請在「憑證驗證」下拉式清單中選取「使用自訂**CA**套裝組合」。然後執行下列其中一項：

   - 使用編輯工具、將每個PEP-編碼CA憑證檔案的所有內容複製貼到* CA bundch*欄位、並以憑證鏈順序串聯。您必須在選擇中加入「-begin Certificate」（開始證書）和「-end Certificate」（結束證書）。



   - 選取*瀏覽*、瀏覽至內含憑證的檔案、然後選取*開啟*上傳檔案。憑證驗證可確保AutoSupport 資訊的傳輸安全無虞。

6. 若要在AutoSupport 不驗證憑證的情況下傳送您的不實訊息、請在「憑證驗證」下拉式清單中選取「請勿驗

證憑證」。

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。

出現一則警示訊息：「您並未使用TLS憑證來保護連線至其他AutoSupport 目的地的安全。」

7. 選擇*保存*。

所有未來每週、事件觸發及使用者觸發AutoSupport 的消息都會傳送至其他目的地。

手動觸發**AutoSupport** 一個消息

為了協助技術支援人員疑難排解StorageGRID 您的故障排除、您可以手動觸發AutoSupport 要傳送的故障訊息。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您具有根存取權限或其他網格組態權限。

步驟

1. 選取*支援*>*工具*>* AutoSupport 參考*。

畫面上會出現「設定」索引標籤、並已選取此索引標籤。AutoSupport

2. 選取*傳送使用者觸發AutoSupport 的S編*。

嘗試傳送不全訊息給技術支援人員。StorageGRID AutoSupport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」、StorageGRID 而不嘗試AutoSupport 再次傳送該消息。

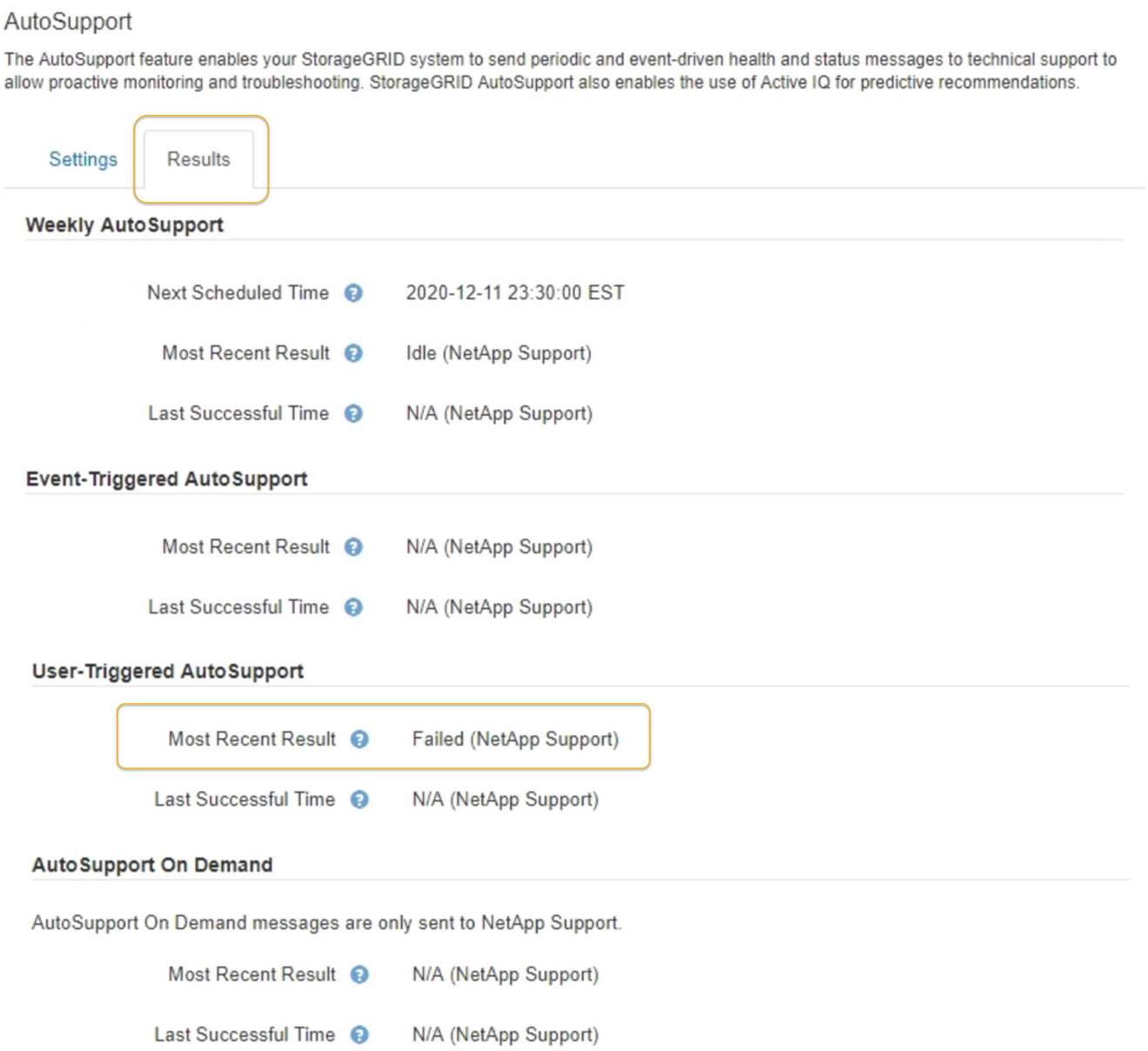
> 傳送使用者觸發AutoSupport 的資訊更新訊息後、AutoSupport 請在1分鐘後重新整理瀏覽器中的資訊頁面、以存取最近的結果。

疑難排解**AutoSupport** 資訊

如果嘗試傳送AutoSupport 資訊不成功、StorageGRID 則根據AutoSupport 資訊類型、系統會採取不同的行動。您可以選取*支援*>*工具*>* Ses*>*結果*來檢查AutoSupport 資訊的狀態AutoSupport 。

> 在全系統隱藏電子郵件通知時、事件觸發AutoSupport 的功能不顯示。（選擇*組態*>*系統*>*顯示選項*。然後選取*通知全部隱藏*。）

當無法傳送此資訊時、「'Failed'」會出現在*《》頁面的「*結果」索引標籤上。AutoSupport AutoSupport



每週**AutoSupport** 更新訊息失敗

如果每週AutoSupport 更新訊息無法傳送、StorageGRID 則無法執行下列動作：

1. 將最新的結果屬性更新為「Retrying（重新執行）」。
2. 每AutoSupport 四分鐘嘗試重新傳送一小時15次的消息。
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AutoSupport 在下次排程時間再次傳送不二訊息。
5. 如果訊息因為NMS服務無法使用、而且訊息是在七天後傳送、則維持正常AutoSupport 的故障排程。
6. 當NMS服務再次可用時、AutoSupport 如果訊息在七天或更長時間內仍未傳送、就會立即傳送一個不實訊息。

使用者觸發或事件觸發**AutoSupport** 的資訊不全訊息故障

如果使用者觸發或事件觸發AutoSupport 的故障訊息無法傳送、StorageGRID 則無法執行下列動作：

1. 如果已知錯誤、則顯示錯誤訊息。例如、如果使用者選擇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 由於電子郵件伺服器頁面上的設定不正確、無法使用SMTP傳輸協定傳送任何消息。
2. 不會再次嘗試傳送訊息。
3. 將錯誤記錄在「NMS.log」中。

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 資訊頁面上：「AutoSupport 由於電子郵件伺服器頁面上的設定不正確、無法使用SMTP傳輸協定傳送資訊。

瞭解如何在中設定電子郵件伺服器設定 監控及疑難排解指示。

修正**AutoSupport** 資訊故障

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 資訊頁面上：「AutoSupport 由於電子郵件伺服器頁面上的設定不正確、無法使用SMTP傳輸協定傳送資訊。

透過**AutoSupport** 支援功能發送**E**系列的訊息**StorageGRID**

您可以SANtricity 透過「e系統管理節點」（AutoSupport 而非儲存應用裝置管理連接埠）、將E系列的《系統管理程式》（E-系列）功能資訊傳送給技術支援部門StorageGRID 。

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Storage Appliance管理員權限或根存取權限。

> 您必須擁有SANtricity 更新版本的韌體8.70（11.7）或更新版本、SANtricity 才能使用Grid Manager存取《系統管理程式》。

關於這項工作

E系列AutoSupport 的資訊包含儲存硬體的詳細資料、比AutoSupport 其他由該系統傳送的資訊更具體StorageGRID 。

在SANtricity 不AutoSupport 使用應用裝置管理連接埠的情況StorageGRID 下、在「Ses供 系統管理程式」中設定一個特殊的Proxy伺服器位址、使其能透過「管理員節點」傳輸有關消息。以這種方式傳輸的資訊、會與Grid Manager中所設定的偏好的寄件者和管理Proxy設定相符。AutoSupport

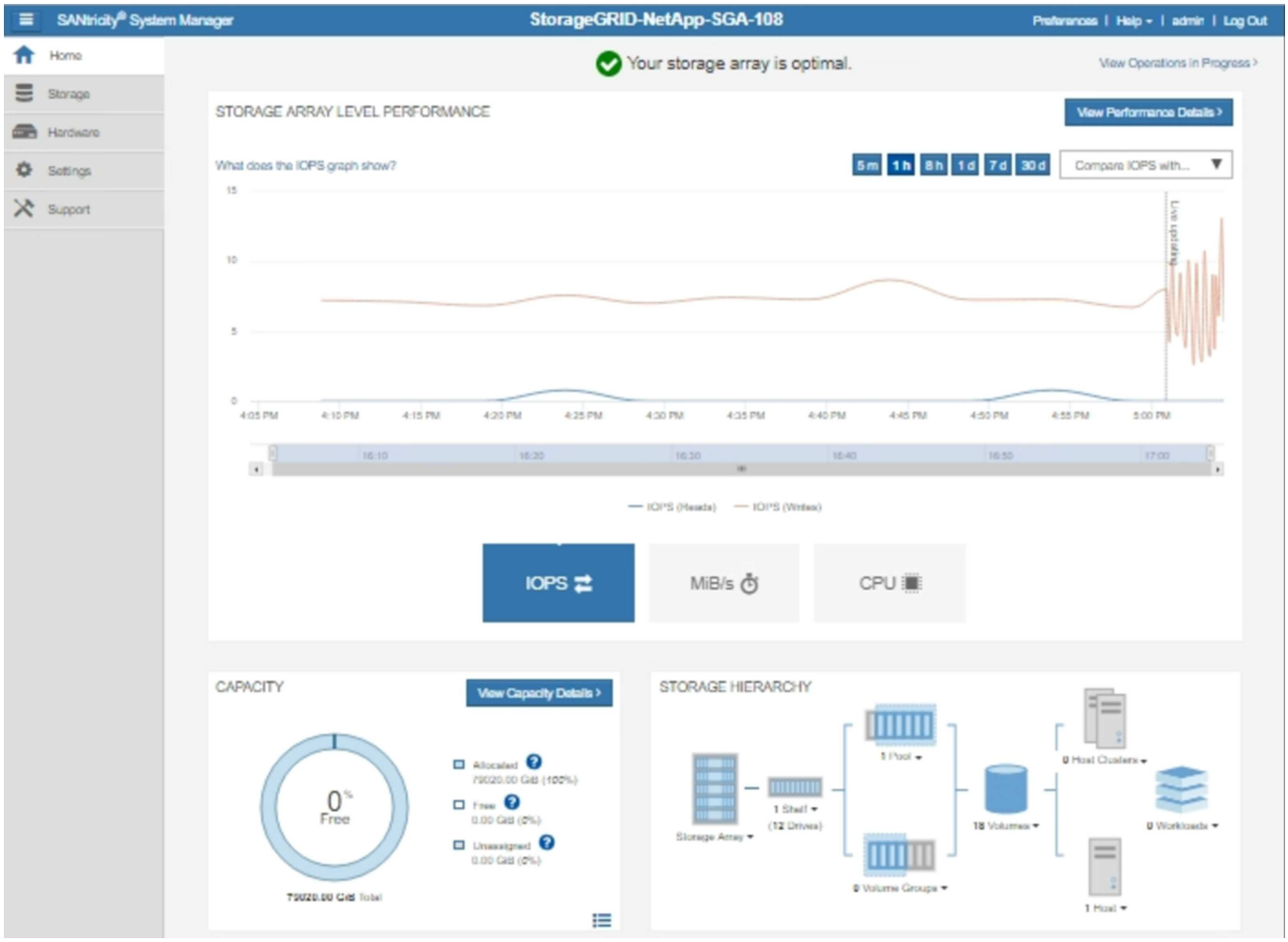
若要在Grid Manager中設定管理Proxy伺服器、請參閱 設定管理Proxy設定。

> 此程序僅適用於設定StorageGRID 適用於E系列AutoSupport 的支援服務器。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

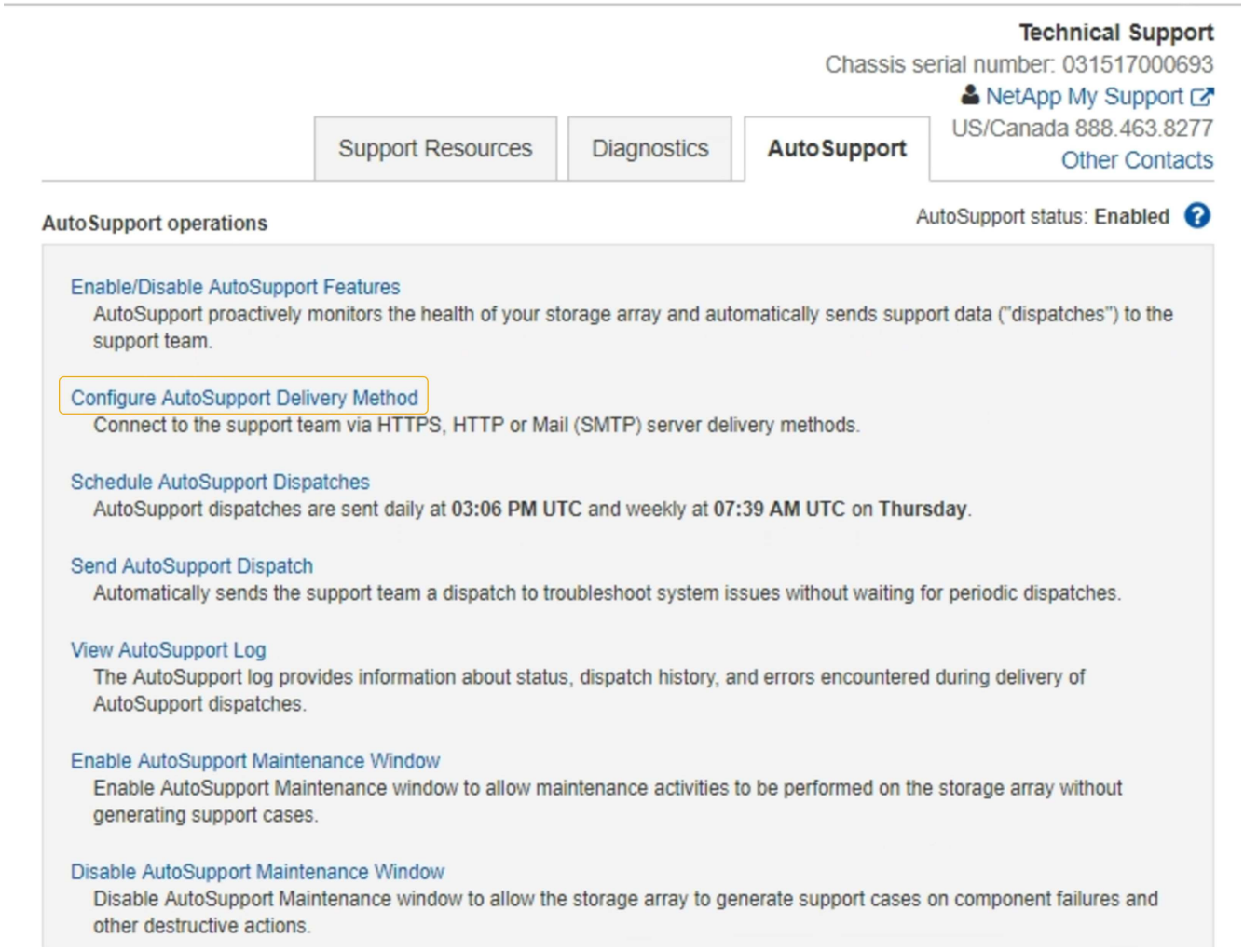
1. 在Grid Manager中、選取* nodes *。
2. 從左側節點清單中、選取您要設定的儲存應用裝置節點。
3. 選擇* SANtricity 《系統管理程式》*。

   出現「系統管理程式」首頁。SANtricity



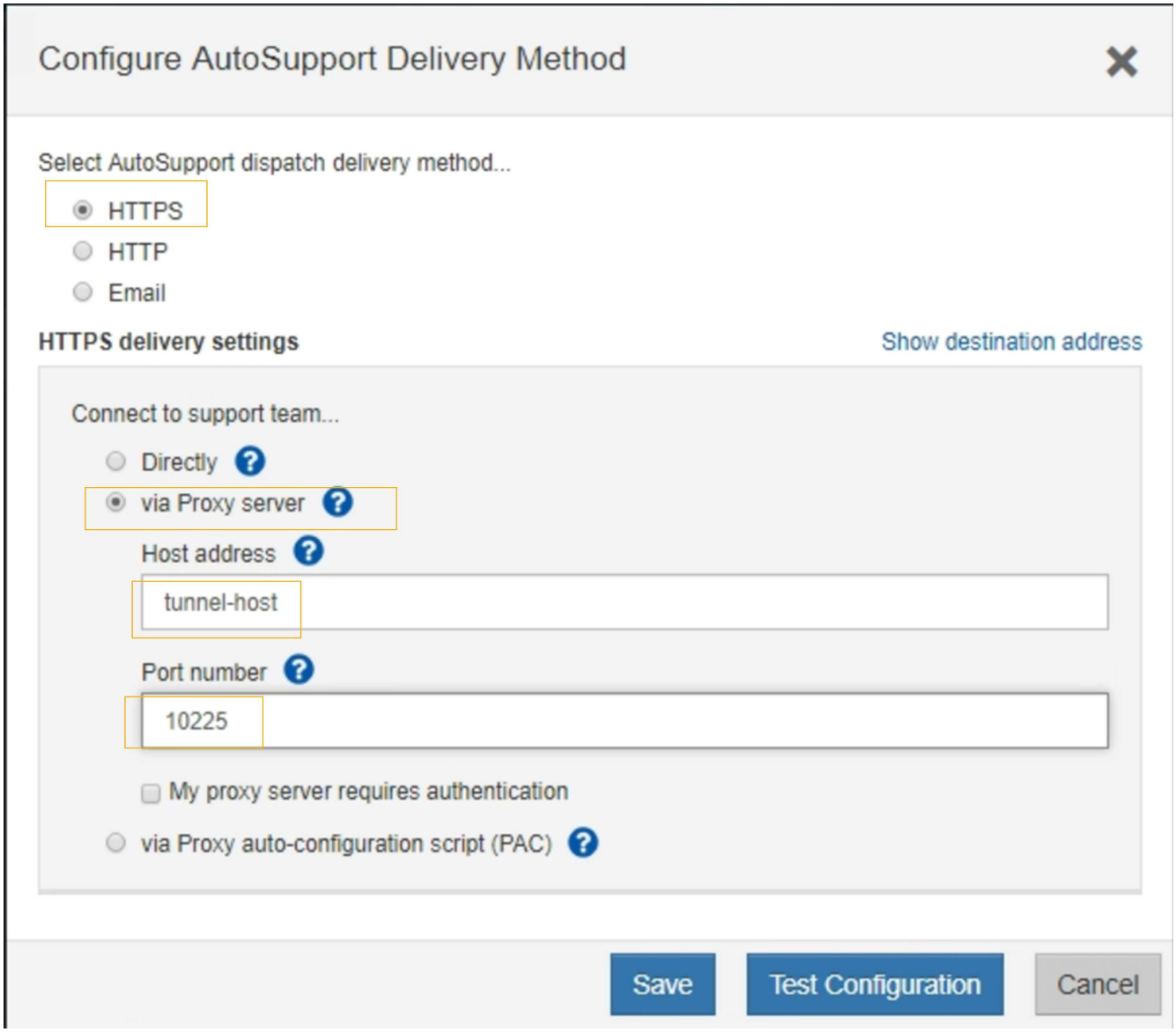
4. 選擇*支援*>*支援中心*>* AutoSupport 支援*。

   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。

   啟用HTTPS傳輸協定的憑證已預先安裝。

7. 選擇*透過Proxy伺服器*。
8. 輸入"tunnunne-host"作爲*主機地址*。

   「通道主機」是使用管理節點傳送E系列AutoSupport 資訊的特殊位址。

9. 輸入「10225」作為*連接埠號碼*。

   「10225」是StorageGRID 指從AutoSupport 應用裝置的E系列控制器接收到的功能性資訊、而該伺服器上的連接埠號碼。

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、則會出現綠色橫幅訊息：「Your AutoSupport 菜單組態已通過驗證。」

如果測試失敗、則會在紅色橫幅中顯示錯誤訊息。請檢查StorageGRID 您的支援DNS設定和網路、確定偏好的傳送者管理節點可以連線至NetApp支援網站、然後再試一次測試。

11. 選擇*保存*。

    系統會儲存組態、並顯示確認訊息：「已AutoSupport 設定『發送方法』。」

管理儲存節點

關於管理儲存節點

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

什麼是儲存節點？

儲存節點可管理及儲存物件資料和中繼資料。每StorageGRID 個支援區系統必須至少有三個儲存節點。如果您有多個站台、StorageGRID 那麼您的一套系統中的每個站台也必須有三個儲存節點。

儲存節點包含在磁碟上儲存、移動、驗證及擷取物件資料和中繼資料所需的服務和程序。您可以在「節點」頁面上檢視儲存節點的詳細資訊。

什麼是**ADC**服務？

管理網域控制器（ADC）服務會驗證網格節點及其彼此的連線。每個站台的前三個儲存節點都會裝載此ADC服務。

ADC服務負責維護拓撲資訊、包括服務的位置和可用度。當網格節點需要來自另一個網格節點的資訊、或是由另一個網格節點執行的動作時、它會聯絡某個ADC服務、以尋找處理其要求的最佳網格節點。此外、ADC服務會保留StorageGRID 一份支援所有網格節點的更新組態套裝組合、以便擷取目前的組態資訊。您可以在Grid拓撲頁面（支援>*網格拓撲*）上檢視儲存節點的ADC資訊。

為了方便分散式和分散式作業、每個ADC服務都會將憑證、組態套件、服務和拓撲的相關資訊、與StorageGRID 其他的子系統中的ADC服務進行同步。

一般而言、所有網格節點都會維持至少一項ADC服務的連線。如此可確保網格節點永遠存取最新資訊。當網格節點連線時、它們會快取其他網格節點的憑證、即使無法使用某個ADC服務、系統仍能繼續使用已知的網格節點。新的網格節點只能使用ADC服務建立連線。

每個網格節點的連線可讓ADC服務收集拓撲資訊。此網格節點資訊包括CPU負載、可用磁碟空間（如果有儲存設備）、支援的服務、以及網格節點的站台ID。其他服務則透過拓撲查詢、要求ADC服務提供拓撲資訊。ADC

服務會回應每個查詢、並提供StorageGRID 從該系統接收到的最新資訊。

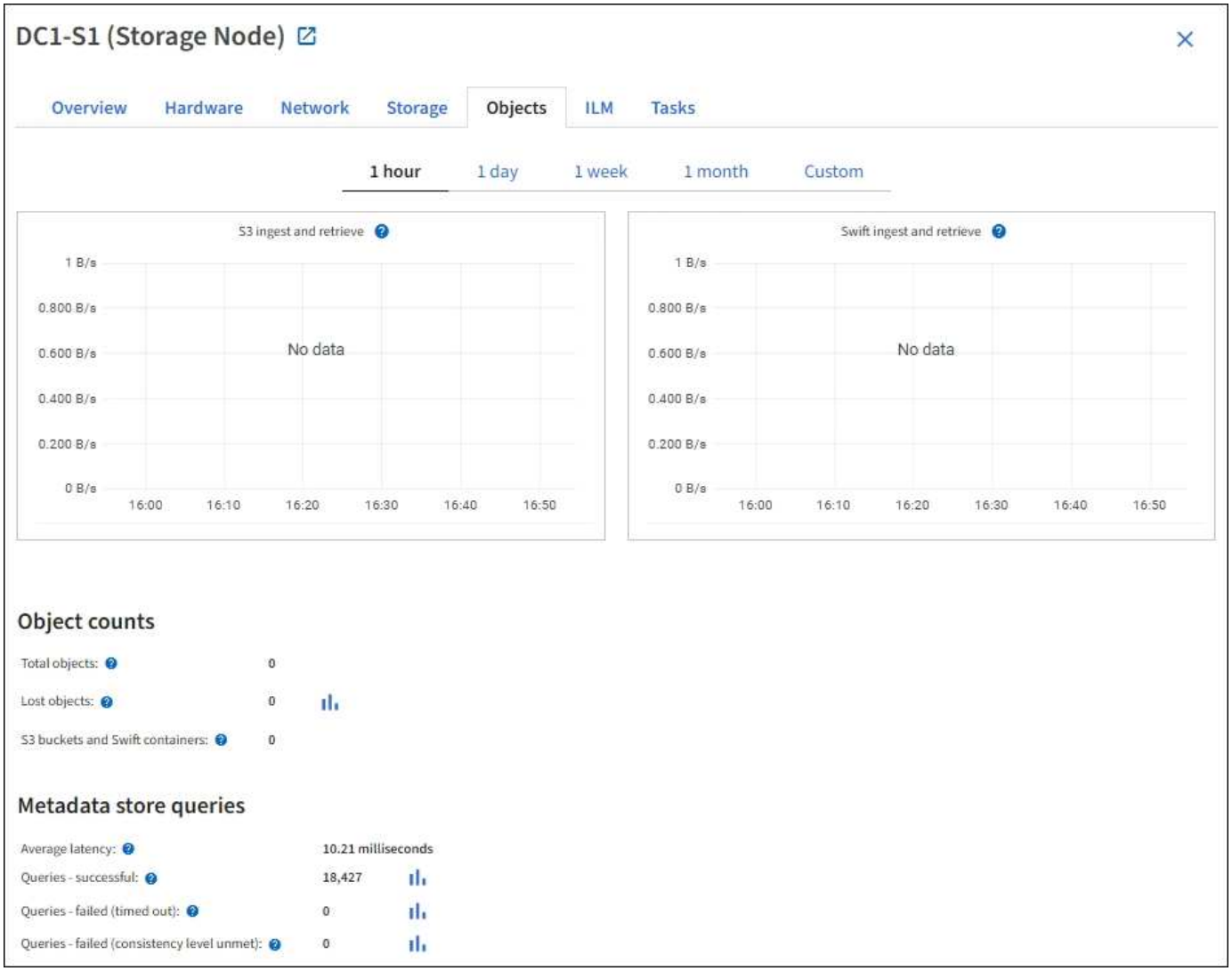
什麼是**DDS**服務？

由儲存節點代管的分散式資料儲存區（DDS）服務會與Cassandra資料庫介面、以執行StorageGRID 物件中繼資料的背景工作、這些中繼資料儲存在整個過程中。

物件數

DDS服務會追蹤擷取至StorageGRID 該系統的物件總數、以及透過每個系統支援的介面（S3或Swift）擷取的物件總數。

您可以在節點頁面>任何儲存節點的物件索引標籤上查看物件總數。



查詢

您可以識別透過特定DDS服務對中繼資料儲存區執行查詢所需的平均時間、成功查詢的總數、以及因逾時問題而失敗的查詢總數。

您可能想要檢閱查詢資訊、以監控中繼資料儲存區Cassandra的健全狀況、這會影響系統的擷取和擷取效能。例如、如果平均查詢的延遲緩慢、而且由於逾時而導致的失敗查詢數高、則中繼資料存放區可能會遇到較高的負載

或執行其他作業。

您也可以檢視因為一致性失敗而失敗的查詢總數。一致性層級失敗是因為在透過特定DDS服務執行查詢時、可用的中繼資料存放區數量不足所致。

您可以使用「診斷」頁面、取得有關網格目前狀態的其他資訊。請參閱 執行診斷。

一致性保證與控管

可確保新建立物件的寫入後讀取一致性。StorageGRID成功完成PUT作業之後的任何Get作業都能讀取新寫入的資料。覆寫現有物件、更新中繼資料及刪除資料、最終仍維持一致。

什麼是**LDR**服務？

本機經銷路由器（LMR）服務由每個儲存節點代管、負責StorageGRID 處理針對此系統的內容傳輸。內容傳輸包含許多工作、包括資料儲存、路由傳送和要求處理。LdR服務StorageGRID 處理資料傳輸負載和資料流量功能、是整個過程中大部分的功能都是由整個系統努力完成。

LDR服務負責下列工作：

- 查詢
- 資訊生命週期管理（ILM）活動
- 物件刪除
- 物件資料儲存
- 從另一個LDR服務（儲存節點）傳輸物件資料
- 資料儲存管理
- 傳輸協定介面（S3和Swift）

LdR服務也會管理S3和Swift物件對應至StorageGRID 唯一的「內容控點」（UUID）、以便將其指派給每個擷取的物件。

查詢

在擷取和歸檔作業期間、LdR查詢包括物件位置查詢。您可以識別執行查詢所需的平均時間、成功查詢的總數、以及因逾時問題而失敗的查詢總數。

您可以檢閱查詢資訊、以監控中繼資料儲存區的健全狀況、這會影響系統的擷取和擷取效能。例如、如果平均查詢的延遲緩慢、而且由於逾時而導致的失敗查詢數高、則中繼資料存放區可能會遇到較高的負載或執行其他作業。

您也可以檢視因為一致性失敗而失敗的查詢總數。一致性層級失敗的原因是在透過特定的LDR服務執行查詢時、可用的中繼資料存放區數量不足。

您可以使用「診斷」頁面、取得有關網格目前狀態的其他資訊。請參閱 執行診斷。

ILM活動

資訊生命週期管理（ILM）指標可讓您監控評估ILM實作物件的速度。您可以在儀表板或*節點*>*儲存節點*>* ILM *上檢視這些度量。

物件存放區

LDR服務的基礎資料儲存區分為固定數量的物件存放區（也稱為儲存磁碟區）。每個物件存放區都是個別的掛載點。

您可以在節點頁面>儲存索引標籤上查看儲存節點的物件存放區。

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

儲存節點中的物件會以介於0000到002F之間的十六進位數字來識別、這稱為Volume ID。空間會保留在第一個物件存放區（Volume 0）中、以供Cassandra資料庫中的物件中繼資料使用；該磁碟區上的任何剩餘空間都會用於物件資料。所有其他物件存放區僅用於物件資料、包括複寫複本和銷毀編碼的片段。

為了確保複寫複本的空間使用率、會根據可用的儲存空間、將特定物件的物件資料儲存至單一物件存放區。當一個或多個物件儲存空間達到容量時、其餘物件儲存區會繼續儲存物件、直到儲存節點上沒有更多空間為止。

中繼資料保護

物件中繼資料是與物件相關的資訊或物件說明、例如物件修改時間或儲存位置。將物件中繼資料儲存在Cassandra資料庫中、該資料庫與LDR服務介面。StorageGRID

為了確保備援並保護資料免於遺失、每個站台都會保留三份物件中繼資料複本。複本會平均分散於每個站台的所有儲存節點。此複寫無法設定、而且會自動執行。

管理物件中繼資料儲存

管理儲存選項

儲存選項包括物件分割設定、儲存Volume浮點的目前值、以及中繼資料保留空間設定。您也可以檢視閘道節點上已過時的CLB服務所使用的S3和Swift連接埠、以及儲存節點上的LDR服務所使用的連接埠。

如需連接埠指派的相關資訊、請參閱 摘要：用於用戶端連線的IP位址和連接埠。

Storage Options
Overview
Configuration

Storage Options Overview
Updated: 2021-11-23 11:01:41 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

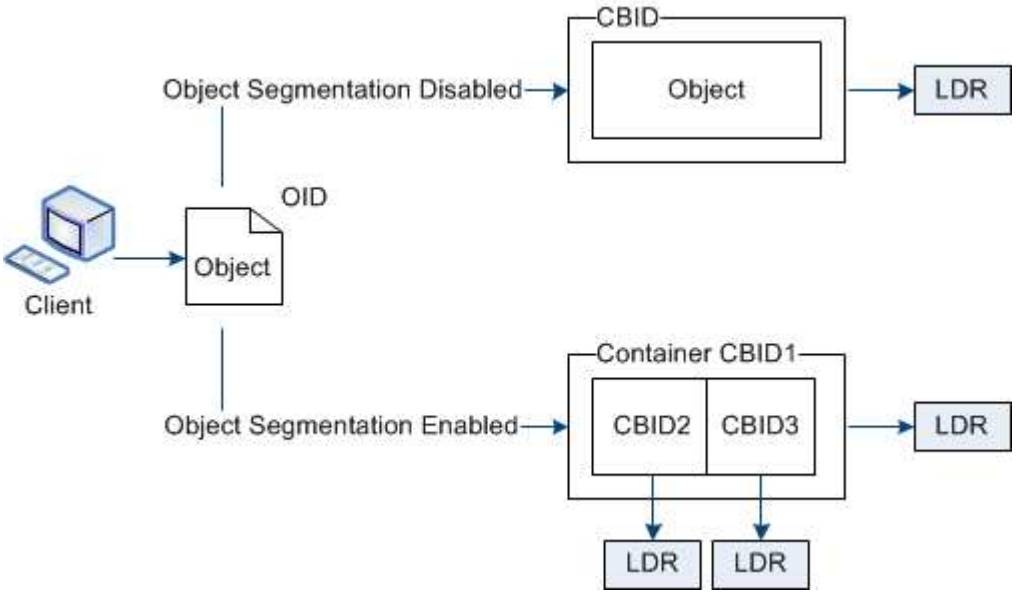
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

什麼是物件區隔？

物件分割是將物件分割成較小的固定大小物件集合的程序、以最佳化大型物件的儲存和資源使用量。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相同的儲存節點上。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：

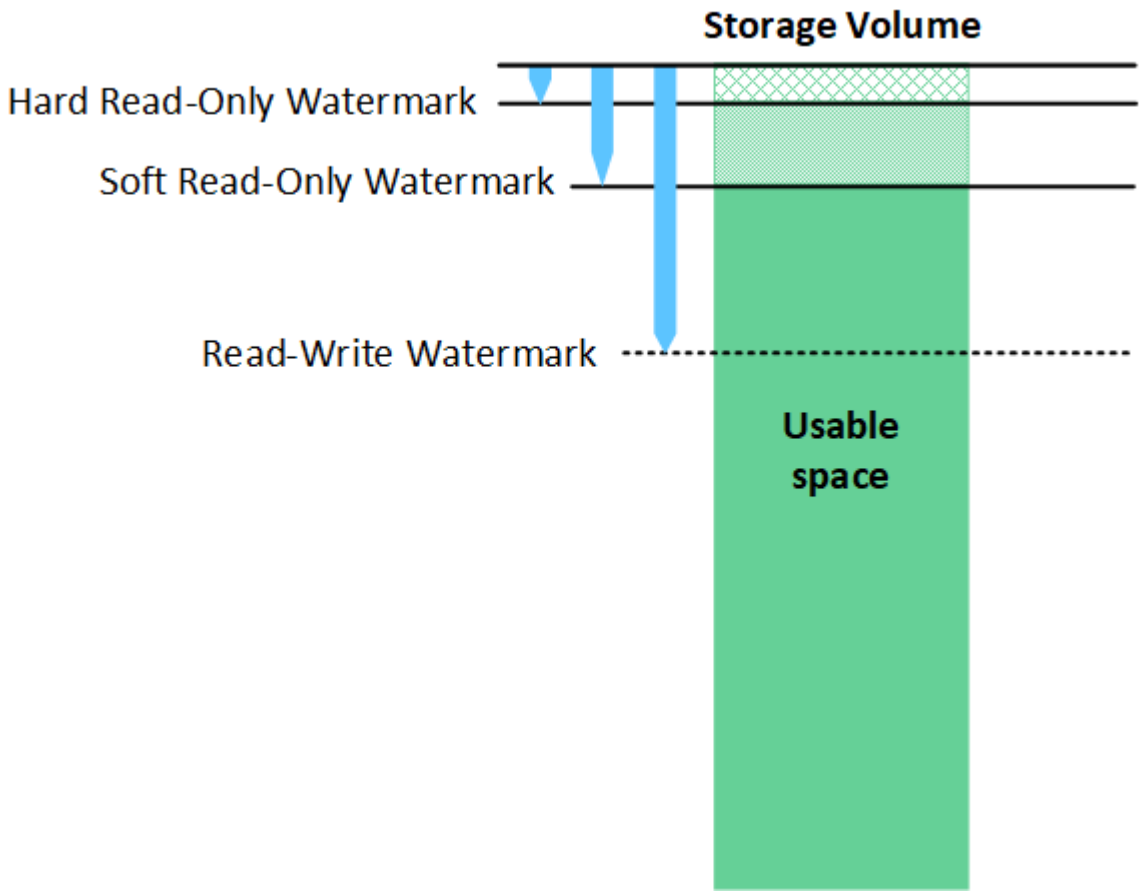
區段Container +區段1 +區段2 =三個儲存物件

您可以確保：

- 每個閘道和儲存節點都有足夠的網路頻寬來處理所需的處理量。例如、在10 Gbps乙太網路介面上設定個別的Grid和Client Networks。
- 已部署足夠的閘道和儲存節點、以滿足所需的處理量。
- 每個儲存節點都有足夠的磁碟IO效能來處理所需的處理量。

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點、您可以決定是否可以或應該調整設定。

您需要的產品

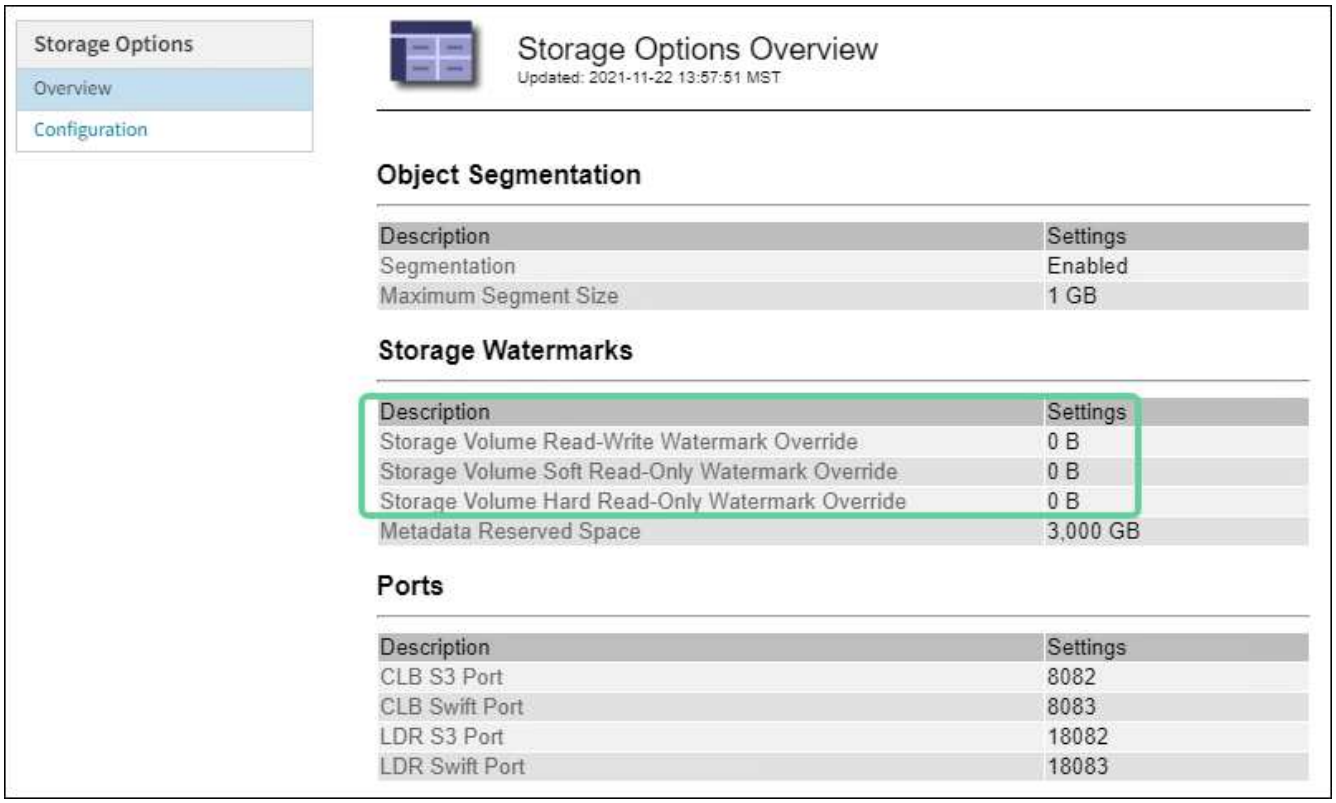
- 您已完成StorageGRID 升級至版本611..
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有root存取權限。

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*組態*>*系統*>*儲存選項*。
2. 在「Storage Watermark（儲存浮點）」區段中、查看三個儲存Volume浮點覆寫的設定。



- 如果浮水印覆寫為* 0*、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這三個浮點。

  這是預設和建議的設定。您不應該更新這些值。視需要、您可以選擇 [檢視最佳化的儲存浮水印]。

- 如果浮水印覆寫為非0值、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。

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*：

   「toragegRid_Storage_volume最小值_最佳化_軟體_readonly浮水印」

   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*：

   「toragegRid_Storage_Volume最大值_imized_soft_readonly浮水印」

   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

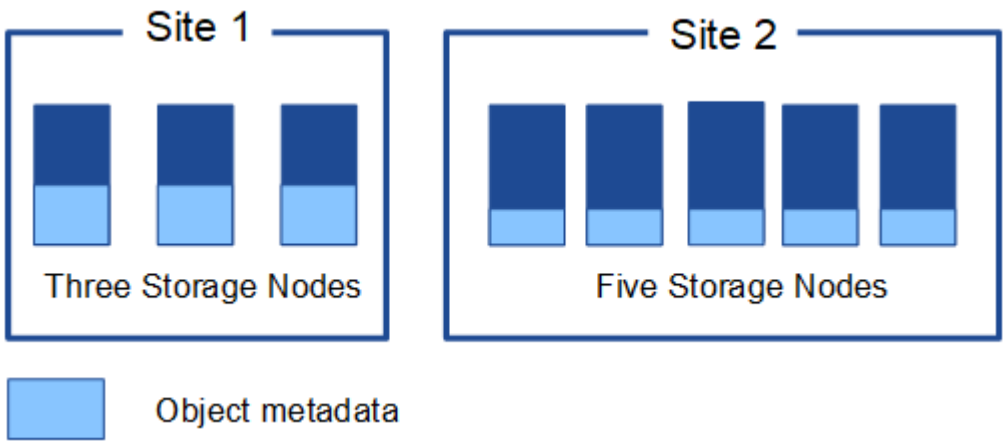
對於物件的物件、物件中繼資料包含下列類型的資訊：StorageGRID

- 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？

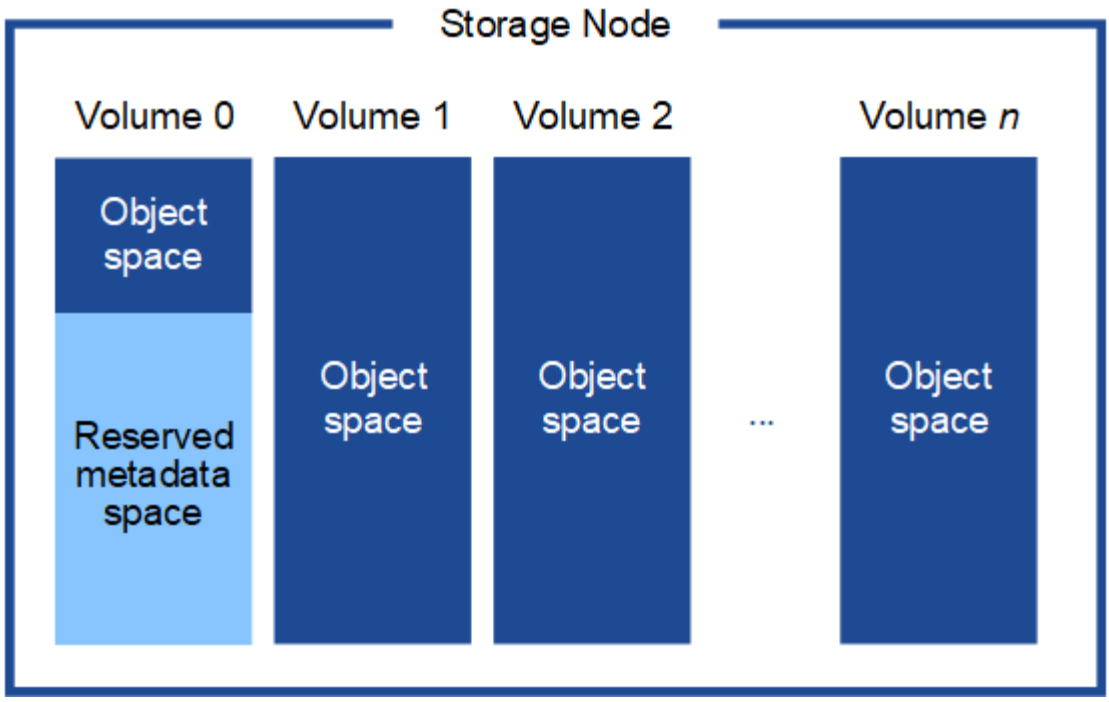
此功能可在Cassandra資料庫中維護物件中繼資料、並獨立儲存物件資料。StorageGRID為了提供備援並保護物件中繼資料免於遺失、StorageGRID 我們在每個站台儲存系統中所有物件的三份中繼資料複本。物件中繼資料的三個複本會平均分散於每個站台的所有儲存節點。

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、這些資料會平均分散於該站台的儲存節點。



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）。

保留給特定儲存節點上物件中繼資料的空間量、取決於下列幾項因素。

中繼資料保留空間設定

_Metadata保留空間_是全系統設定、代表保留給每個儲存節點Volume 0上中繼資料的空間量。如表所示StorageGRID 、此項設定的預設值為下列項目：

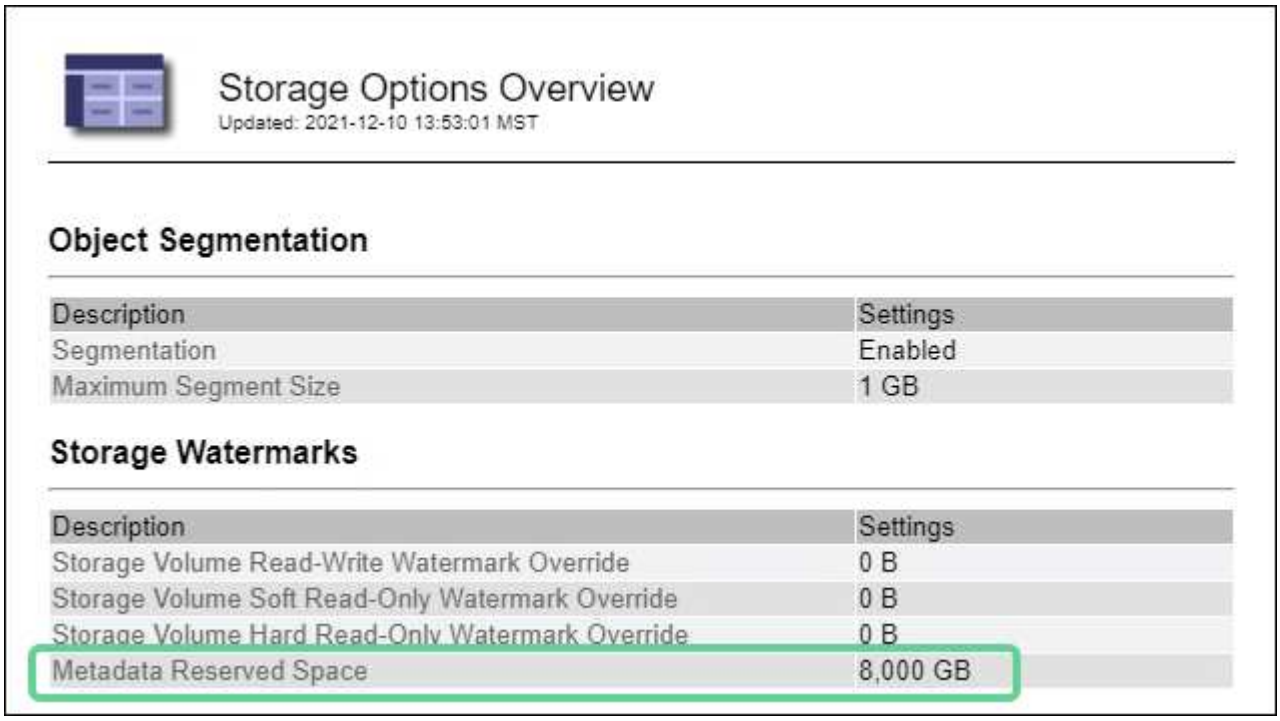
- 您剛開始安裝StorageGRID 時使用的軟體版本。
- 每個儲存節點上的RAM容量。

用於初始**StorageGRID** 安裝的版本	儲存節點上的**RAM**容量	預設的**StorageGRID** 中繼資料保留空間設定、適用於
11.5/11.6%	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）

用於初始**StorageGRID** 安裝的版本	儲存節點上的**RAM**容量	預設的**StorageGRID** 中繼資料保留空間設定、適用於
11.0或更早版本	任何金額	2 TB（2、000 GB）

若要檢視StorageGRID 您的功能區系統的中繼資料保留空間設定：

1. 選擇*組態*>*系統*>*儲存選項*。
2. 在Storage Watermarks表中、找到*中繼資料保留空間*。



在快照中、*中繼資料保留空間*值為8、000 GB（8 TB）。這是全新StorageGRID 安裝的更新版的預設設定、其中每個儲存節點都有128 GB以上的RAM。

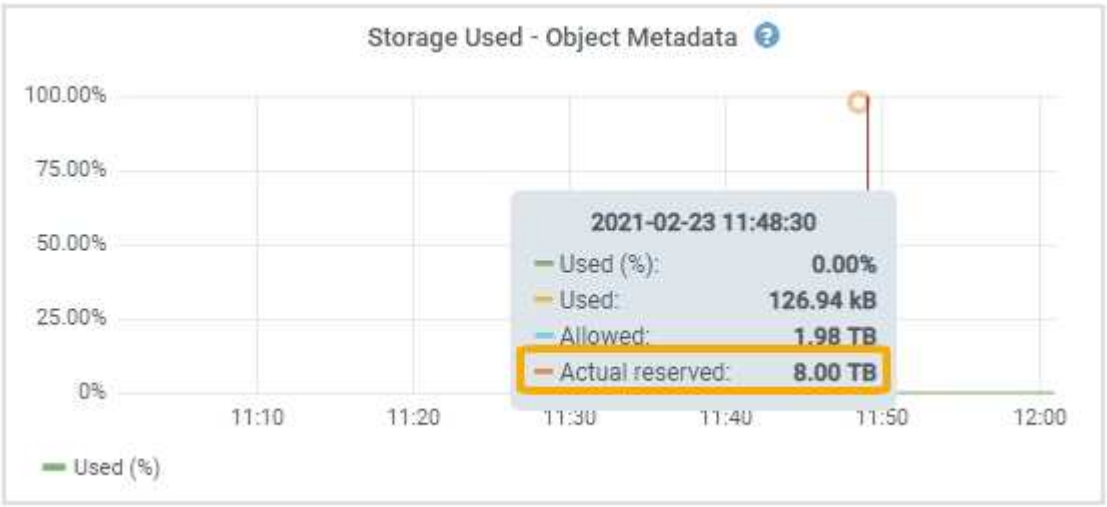
中繼資料的實際保留空間

相較於全系統的中繼資料保留空間設定、會針對每個儲存節點來決定物件中繼資料的實際保留空間_。對於任何給定的儲存節點、中繼資料的實際保留空間取決於節點的Volume 0大小、以及系統整體*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
500 GB以上	這些值越小： • Volume 0 • 中繼資料保留空間設定

若要檢視特定儲存節點上中繼資料的實際保留空間：

1. 從Grid Manager中選擇* nodes > Storage Node_*。
2. 選擇* Storage*（儲存設備）選項卡。
3. 將游標暫留在「使用的儲存設備」-「物件中繼資料」圖表上、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。由於此儲存節點的全系統中繼資料保留空間設定小於Volume 0、因此此節點的實際保留空間等於中繼資料保留空間設定。

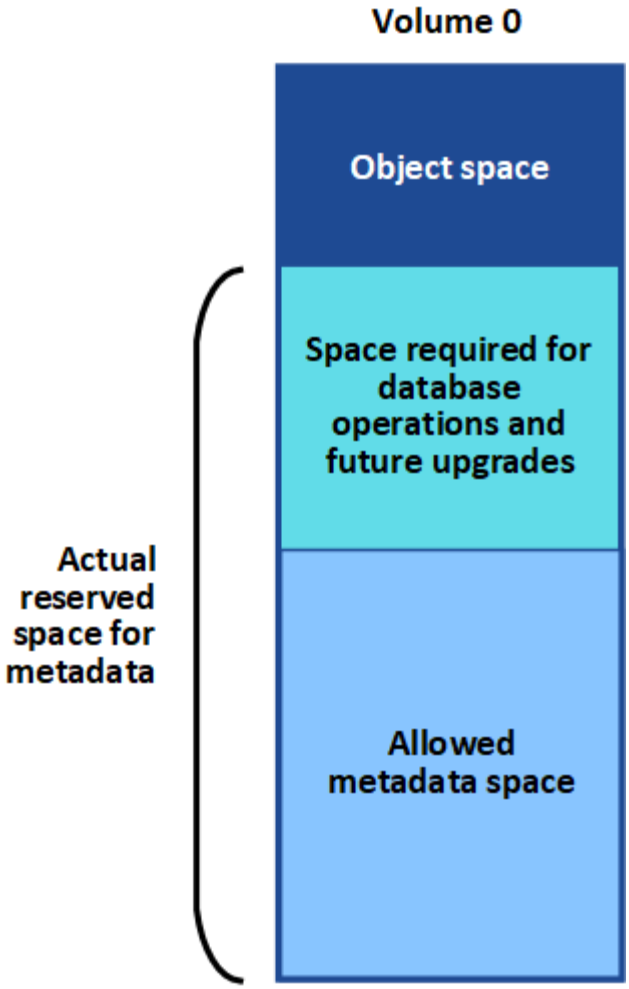
實際保留的中繼資料空間範例

假設您使用StorageGRID 11.6%版來安裝新的效能不全系統。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：

- 全系統*中繼資料保留空間*設定為8 TB。（StorageGRID 如果每個儲存節點的RAM超過128 GB、這是新版的更新版的預設值。）
- 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。

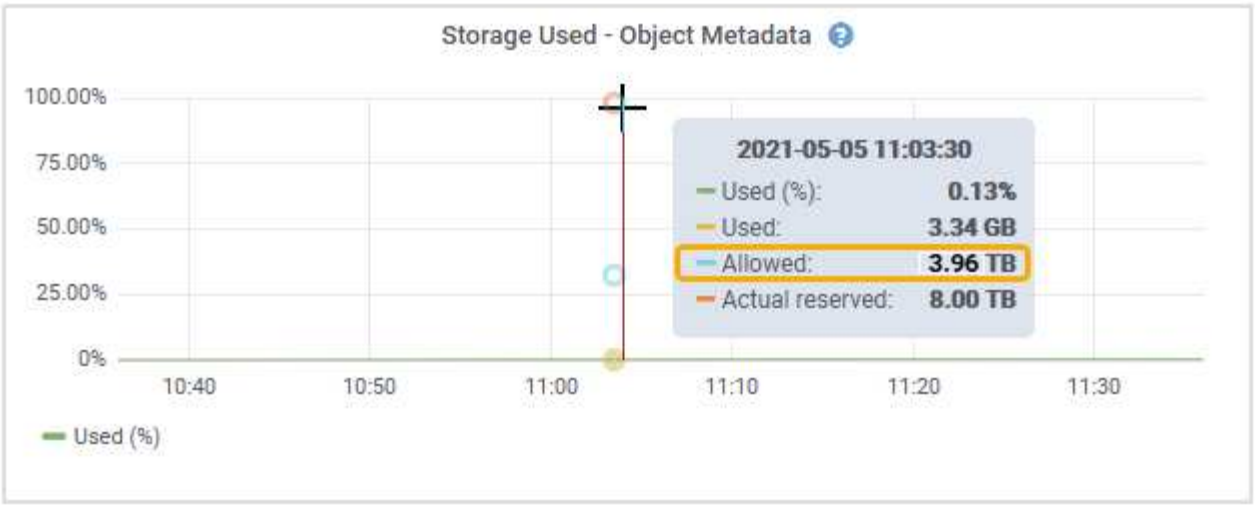


下表顯示StorageGRID 根據節點的記憶體容量和中繼資料的實際保留空間、如何針對不同的儲存節點計算*允許的中繼資料空間*。

		*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	實際保留空間的60%用於中繼資料、最高1.98 TB	4 TB

若要檢視儲存節點允許的中繼資料空間：

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. 將游標暫留在「使用的儲存設備」-「物件中繼資料」圖表上、找出*允許的*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：

' toragegRid_storage使用率中繼資料允許的位元組'

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：

- 全系統*中繼資料保留空間*設定為8 TB。（StorageGRID 當每個儲存節點的RAM超過128 GB時、此為預設值。）
- 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。

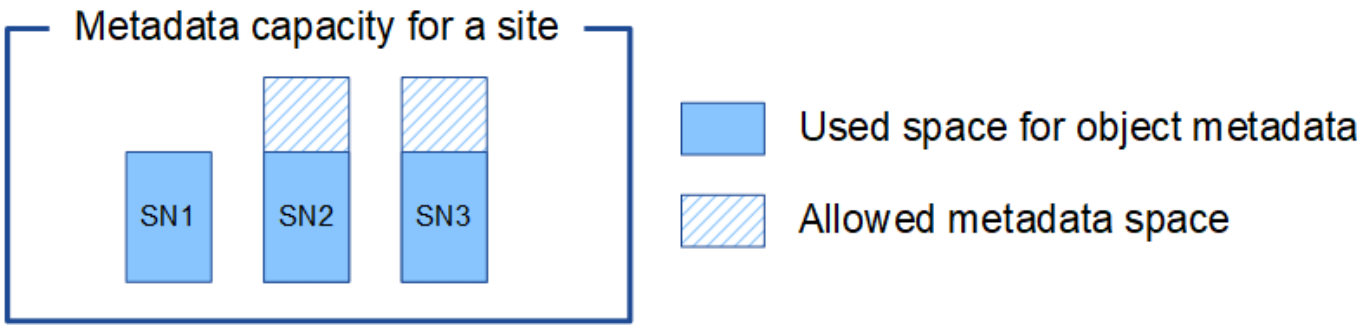
請考慮下列範例：

- 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

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
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。SN2和SN3所允許的額外0.66 TB中繼資料空間無法使用。



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、請前往 監控及疑難排解。
- 若要增加系統的物件中繼資料容量、請新增儲存節點。前往 擴充網格。

設定儲存物件的全域設定

設定儲存的物件壓縮

您可以使用「壓縮儲存的物件」網格選項來減少StorageGRID 儲存在物件中的物件大小、以減少物件佔用的儲存空間。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

「壓縮儲存的物件」網格選項預設為停用。如果啟用此選項、StorageGRID 則使用無損壓縮功能、在儲存每個物件時、會嘗試壓縮該物件。

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。

啟用此選項之前、請注意下列事項：

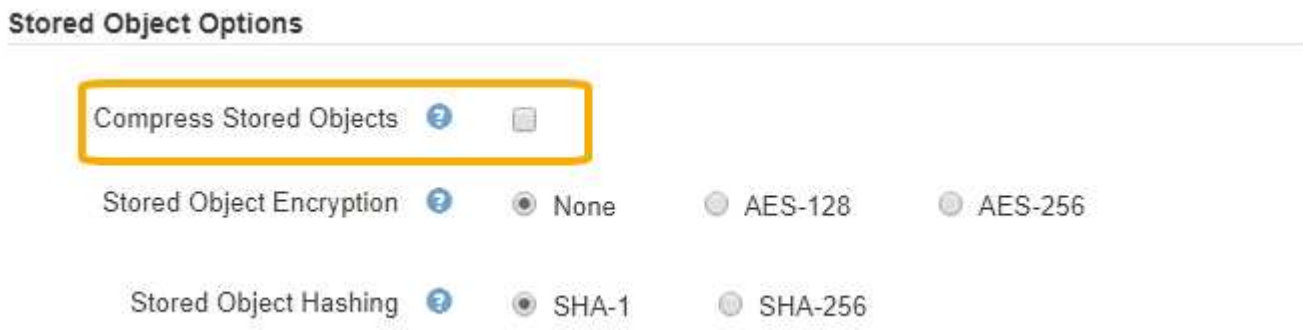
- 除非您知道儲存的資料是可壓縮的、否則不應啟用壓縮。
- 將物件儲存StorageGRID 至物件的應用程式可能會先壓縮物件、然後再儲存物件。如果用戶端應用程式在將物件儲存StorageGRID 至物件之前、已經壓縮物件、則啟用「壓縮儲存物件」不會進一步縮小物件的大小。
- 如果您使用NetApp FabricPool 解決方案StorageGRID 搭配使用時、請勿啟用壓縮功能。
- 如果已啟用「壓縮儲存的物件」網格選項、S3和Swift用戶端應用程式應避免執行「取得物件」作業、以指定要傳回的位元組範圍。這些「範圍讀取」作業效率不彰、因為StorageGRID 必須有效解壓縮物件才能存取所要求的位元組。從非常大的物件要求少量位元組的「Get Object」（取得物件）作業效率特別低；例如、從50 GB壓縮物件讀取10 MB範圍的效率不彰。

  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*>*網格選項*。
2. 在「儲存的物件選項」區段中、選取「壓縮儲存的物件」核取方塊。



3. 選擇*保存*。

設定儲存的物件加密

如果您想要確保在物件存放區遭到入侵時、無法以可讀取的格式擷取資料、可以加密儲存的物件。依預設、物件不會加密。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

儲存的物件加密可在透過S3或Swift擷取時、加密所有物件資料。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、目前加密的物件會保持加密狀態、但新擷取的物件不會加密。

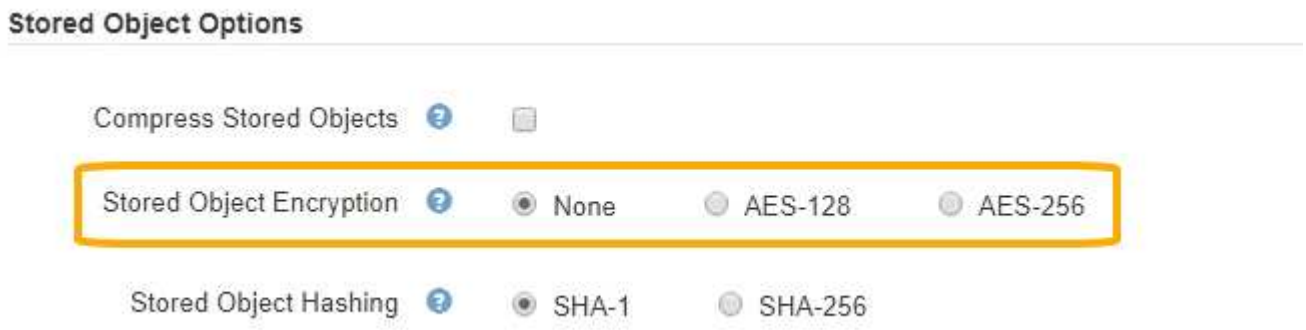
如果您變更此設定、則需要約一分鐘的時間才能套用新設定。系統會快取設定的值、以利效能與擴充。

儲存的物件可使用AES-128或AES-256加密演算法進行加密。

「儲存的物件加密」設定僅適用於尚未透過儲存區層級或物件層級加密進行加密的S3物件。

步驟

1. 選擇*組態*>*系統*>*網格選項*。
2. 在「儲存的物件選項」區段中、將「儲存的物件加密」變更為*「無」（預設）、AES-128*或* AES-256*。



3. 選擇*保存*。

設定儲存的物件雜湊

「儲存的物件雜湊」選項會指定用來驗證物件完整性的雜湊演算法。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

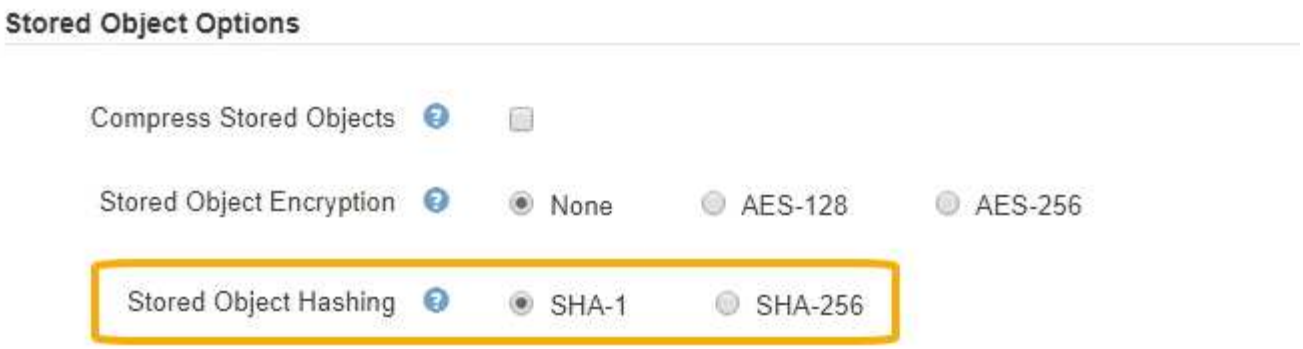
關於這項工作

根據預設、物件資料會使用SHA-1演算法進行雜湊處理。SHA-256演算法需要額外的CPU資源、一般不建議用於完整性驗證。

> 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。

步驟

1. 選擇*組態*>*系統*>*網格選項*。
2. 在「儲存的物件選項」區段中、將「儲存的物件雜湊」變更為* SHA-1*（預設）或* SHA-256*。



3. 選擇*保存*。

儲存節點組態設定

每個儲存節點都會使用許多組態設定和計數器。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。

若要存取儲存節點的組態設定和計數器：

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及其他內部StorageGRID 的各種資訊流量的HTTP傳輸協定目前狀態： • 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

屬性名稱	程式碼	說明
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、LMR服務會將儲存狀態移至唯讀、並停止接受新內容。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。如需詳細資訊、請參閱監控StorageGRID 和疑難排解功能的說明。
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。
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。 當停用傳入複寫時、可以從儲存節點擷取物件、以便複製到StorageGRID 該系統的其他位置、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、以便複製到StorageGRID 故障恢復系統的其他位置。LDR服務為純寫入。

相關資訊

監控及疑難排解

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 諸如SG6060的物件應用儲存節點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

什麼是管理節點

管理節點提供系統組態、監控及記錄等管理服務。每個網格都必須有一個主要管理節點、而且可能有任意數量的非主要管理節點來提供備援。

當您登入Grid Manager或租戶管理程式時、即連線至管理節點。您可以連線至任何管理節點、每個管理節點都會顯示StorageGRID 類似的畫面、顯示有關該系統的資訊。不過、維護程序必須使用主要管理節點來執行。

管理節點也可用於負載平衡S3和Swift用戶端流量。

管理節點裝載下列服務：

- AMS服務
- CMN服務
- NMS服務
- Prometheus服務
- 負載平衡器和高可用度服務（支援S3和Swift用戶端流量）

管理節點也支援管理應用程式程式介面（mgmt-API）、以處理來自Grid Management API和租戶管理API的要求。請參閱 使用Grid Management API。

AMS服務是什麼

稽核管理系統（AMS）服務會追蹤系統活動和事件。

CMN服務是什麼

組態管理節點（CMN）服務可管理全系統的連線組態、以及所有服務所需的傳輸協定功能。此外、CMN服務也可用來執行及監控網格工作。每StorageGRID 個版本部署只有一個CMN服務。主控CMN服務的管理節點稱為主要管理節點。

NMS服務是什麼

網路管理系統（NMS）服務可透過Grid Manager（StorageGRID 即整個系統的瀏覽器型介面）、提供監控、報告及組態選項的功能。

什麼是**Prometheus**服務

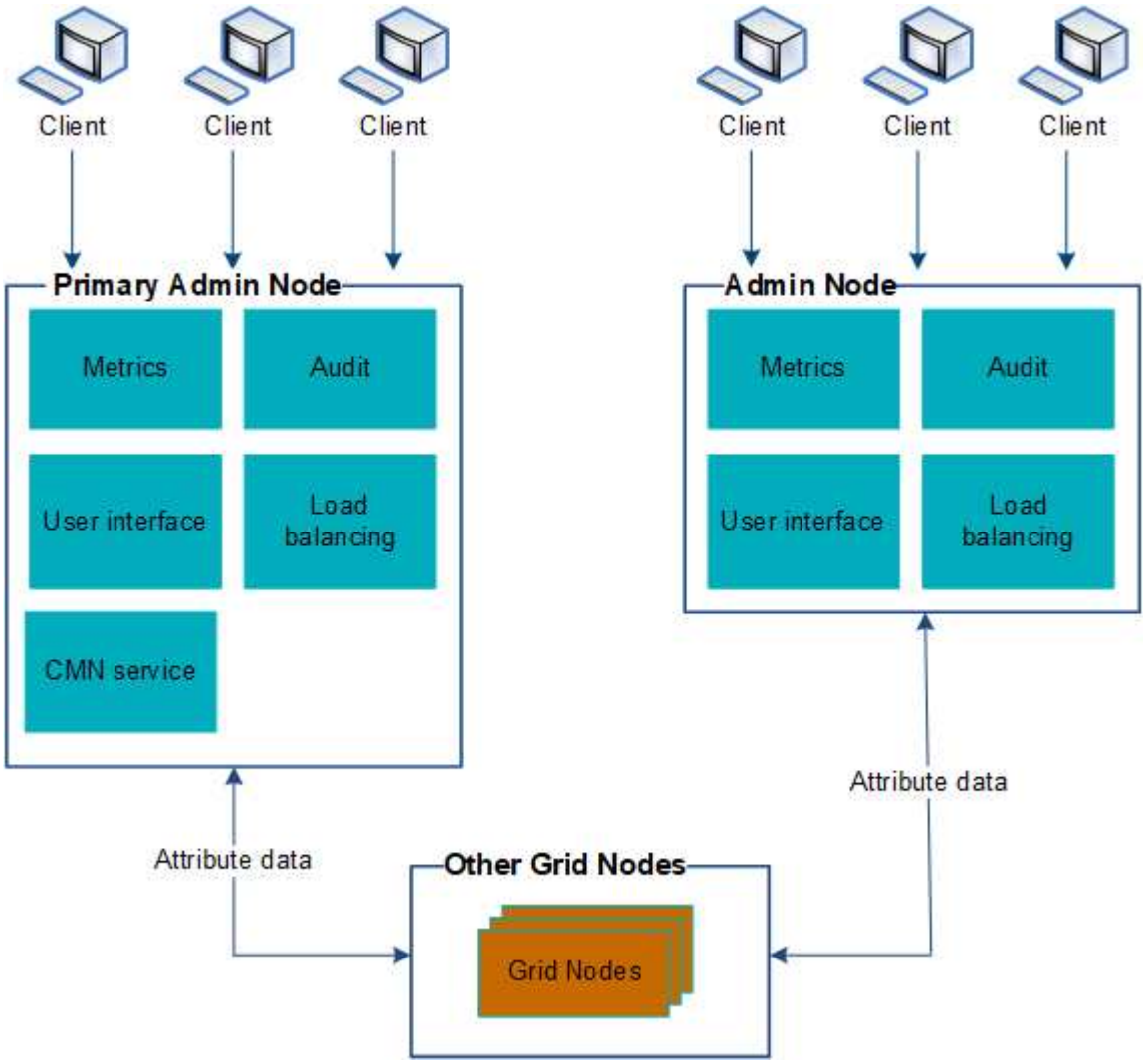
Prometheus服務會從所有節點上的服務收集時間序列數據。

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（舊系統）仍會觸發、電子郵件通知和AutoSupport 資訊

仍會傳送。不過、擁有多個管理節點並不提供容錯移轉保護、除了通知和AutoSupport 顯示的資訊之外。尤其是、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、如果主管理節點故障、存取將會中斷。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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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。

選取偏好的寄件者

如果StorageGRID 您的支援範圍包括多個管理節點、您可以選擇哪一個管理節點應該是通知的偏好傳送者。預設會選取主要管理節點、但任何管理節點都可以是偏好的傳送者。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

關於這項工作

「組態>*系統*>*顯示選項*」頁面會顯示目前選取要做為慣用傳送者的管理節點。預設會選取主要管理節點。

在正常系統作業下、只有偏好的傳送者會傳送下列通知：

- 資訊AutoSupport
- SNMP通知
- 警示電子郵件
- 警示電子郵件（舊系統）

但是、所有其他管理節點（待命傳送者）都會監控偏好的傳送者。如果偵測到問題、待命傳送者也可以傳送這些通知。

在下列情況下、偏好的傳送者和待命傳送者都可能會傳送通知：

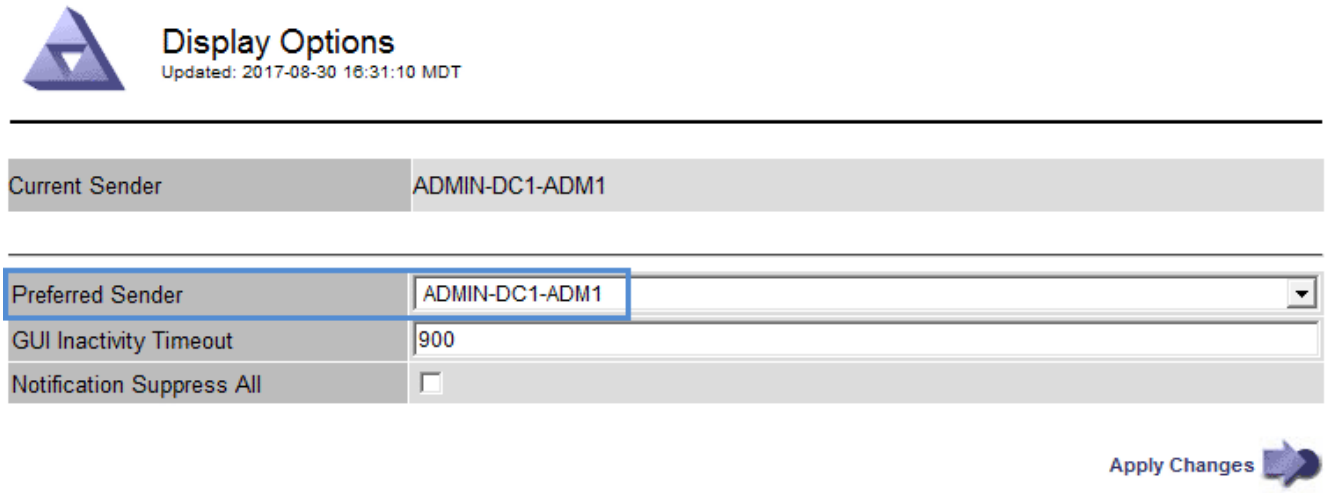
- 如果管理節點彼此變成「islacked」、偏好的傳送者和待命傳送者都會嘗試傳送通知、而且可能會收到多份通知複本。
- 待機傳送者偵測到偏好的傳送者問題並開始傳送通知之後、偏好的傳送者可能會重新取得傳送通知的能力。如果發生這種情況、可能會傳送重複的通知。當待命傳送者不再偵測到偏好的傳送者錯誤時、它將停止傳送通知。

> ⓘ 當您測試警示通知和AutoSupport 資訊內容時、所有管理節點都會傳送測試電子郵件。測試警示通知時、您必須登入每個管理節點以驗證連線能力。

步驟

1. 選擇*組態*>*系統*>*顯示選項*。

2. 從「顯示選項」功能表中、選取*選項*。
3. 從下拉式清單中選取您要設定為慣用寄件者的管理節點。



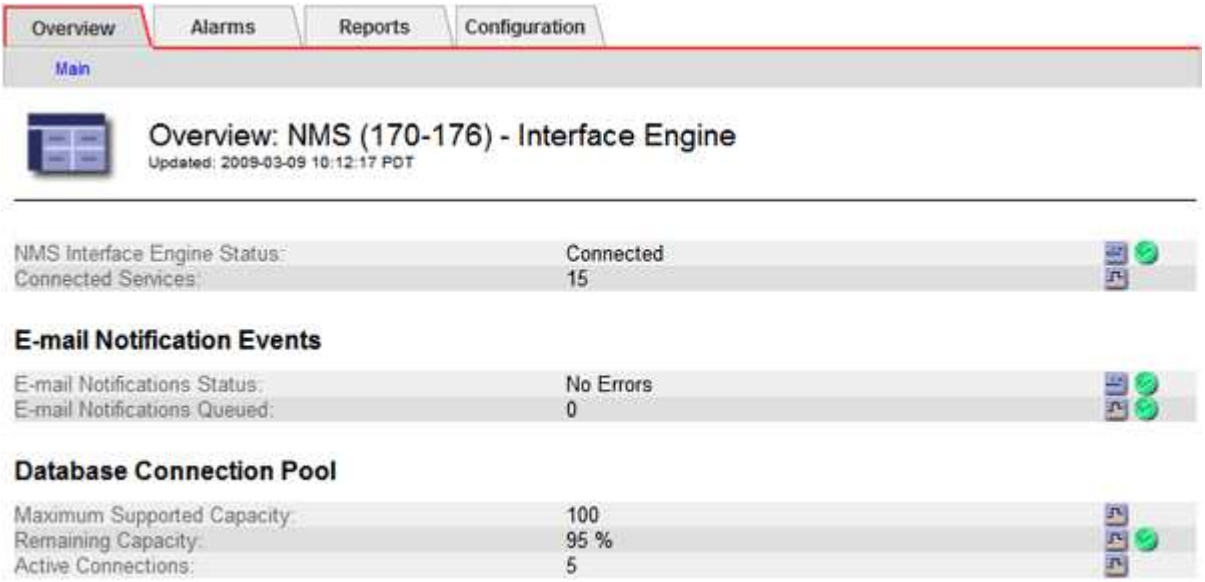
4. 選取*套用變更*。

   系統會將管理節點設為通知的偏好傳送者。

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*。



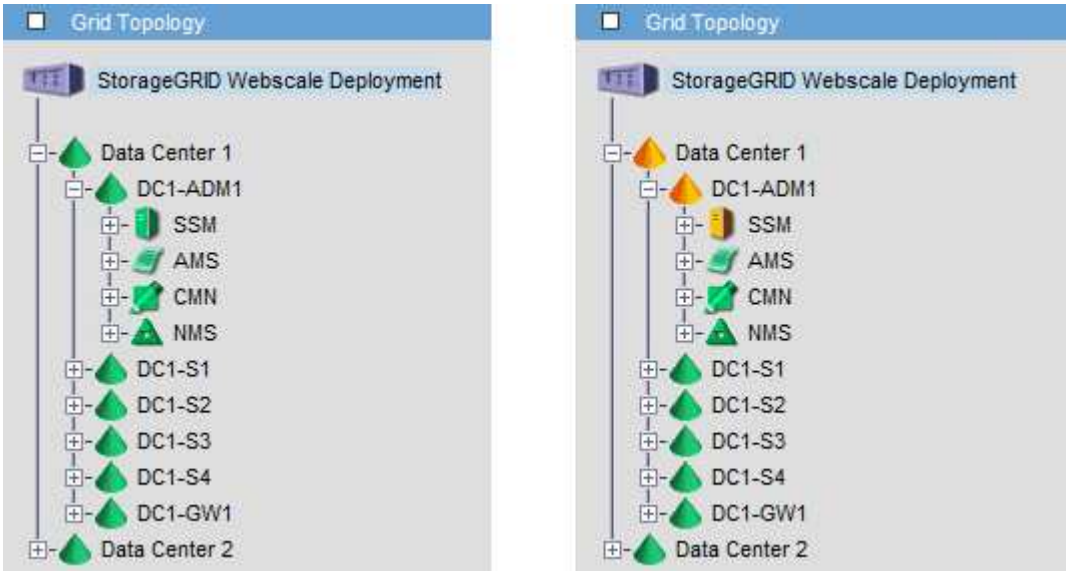
通知會透過電子郵件通知佇列處理、並依觸發順序逐一傳送至郵件伺服器。如果發生問題（例如、網路連線錯誤）、且郵件伺服器在嘗試傳送通知時無法使用、則會繼續嘗試將通知重新傳送至郵件伺服器60秒。如果通知在60秒後未傳送至郵件伺服器、則通知會從通知佇列中捨棄、並嘗試傳送佇列中的下一個通知。由於通知可從通知佇列中捨棄而不傳送、因此可能在未傳送通知的情況下觸發警示。如果通知從佇列中捨棄而未傳送、則會觸

發分鐘（電子郵件通知狀態）次要警示。

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。由於不會將確認複製到其他管理節點、因此每個管理節點的Grid拓撲樹狀結構可能看起來不一樣。

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

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。為了方便存取稽核記錄、您可以設定用戶端存取CIFS和NFS的稽核共用。

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。

> 透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。如果您有使用CIFS或NFS的選項、請選擇NFS。

設定**CIFS**的稽核用戶端

用來設定稽核用戶端的程序取決於驗證方法：Windows工作群組或Windows Active Directory（AD）。新增時、稽核共用區會自動啟用為唯讀共用區。

> 透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

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。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin帳戶密碼（可在上述套件中找到）。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。

關於這項工作

透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。

2. 確認所有服務的狀態均為執行中或已驗證：「toragegrid狀態」

   如果所有服務均未執行或「已驗證」、請先解決問題再繼續。

3. 返回命令列、按* Ctrl-+* C*。
4. 啟動CIFS組態公用程式：「config_CIFs.rb」

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. 設定Windows工作群組的驗證：

   如果已設定驗證、則會顯示摘要報告訊息。如果已設定驗證、請前往下一步。

   a. 輸入：「et驗證」
   b. 當系統提示您安裝Windows工作群組或Active Directory時、請輸入：「workgroup」（工作群組）

c. 出現提示時、請輸入工作群組名稱：「*workgroup*名稱」

d. 出現提示時、請建立有意義的NetBios名稱：「*netbios_name*'」

或

按* Enter *以使用管理節點的主機名稱做為NetBios名稱。

指令碼會重新啟動Samba伺服器、並套用變更。這應不到一分鐘。設定驗證之後、請新增稽核用戶端。

a. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

6. 新增稽核用戶端：

a. 輸入：「add-稽 核共用區」

共用區會自動新增為唯讀。

b. 出現提示時、請新增使用者或群組：「*user*」

c. 出現提示時、請輸入稽核使用者名稱：「*nap_user_name*」

d. 出現提示時、請輸入稽核使用者的密碼：「_password」

e. 出現提示時、請重新輸入相同的密碼進行確認：「*password*」

f. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

不需要輸入目錄。稽核目錄名稱已預先定義。

7. 如果允許多個使用者或群組存取稽核共用區、請新增其他使用者：

a. 輸入：「add-user-to共享」

隨即顯示已啟用共享區的編號清單。

b. 出現提示時、請輸入稽核匯出共用區的數量：「*share_number*」

c. 出現提示時、請新增使用者或群組：「user」

或「團體」

d. 出現提示時、請輸入稽核使用者或群組的名稱：「_nap_user」或「nap_group」

e. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

f. 針對每個具有稽核共用存取權的其他使用者或群組、重複這些子步驟。

8. 或者、請驗證您的組態：「valide-config」

系統會檢查並顯示這些服務。您可以安全地忽略下列訊息：

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. 出現提示時、請按* Enter *。

隨即顯示稽核用戶端組態。

b. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

9. 關閉CIFS組態公用程式：「Exit（結束）」
10. 啟動Samba服務：「service smbd start」
11. 如果StorageGRID 這個部署是單一站台、請前往下一步。

或

或者、如果StorageGRID 此功能的支援包括其他站台的管理節點、請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：「sh admin@*grid_node_ip*`」
   ii. 輸入「passwords.txt」檔案中所列的密碼。
   iii. 輸入下列命令以切換至root：「u -」
   iv. 輸入「passwords.txt」檔案中所列的密碼。
b. 重複這些步驟、為每個額外的管理節點設定稽核共用區。
c. 關閉遠端管理節點的遠端安全Shell登入：「Exit（結束）」

12. 登出命令Shell：「exit」

設定**Active Directory**的稽核用戶端

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。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin帳戶密碼（可在上述套件中找到）。
- 您有CIFS Active Directory使用者名稱和密碼。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。

透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。

2. 確認所有服務的狀態均為執行中或已驗證：「toragegrid狀態」

   如果所有服務均未執行或「已驗證」、請先解決問題再繼續。

3. 返回命令列、按* Ctrl-+* C*。
4. 啟動CIFS組態公用程式：「config_CIFs.rb」

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. 設定Active Directory驗證：「設定驗證」

   在大多數部署中、您必須先設定驗證、才能新增稽核用戶端。如果已設定驗證、則會顯示摘要報告訊息。如果已設定驗證、請前往下一步。

   a. 當系統提示您進行工作群組或Active Directory安裝時：「ad」（廣告）
   b. 出現提示時、請輸入AD網域名稱（簡短網域名稱）。
   c. 出現提示時、請輸入網域控制器的IP位址或DNS主機名稱。
   d. 出現提示時、請輸入完整的網域領域名稱。

      使用大寫字母。

   e. 當系統提示您啟用winbind支援時、請輸入* y*。

winbind用於從AD伺服器解析使用者和群組資訊。

f. 出現提示時、請輸入NetBios名稱。

g. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

6. 加入網域：

a. 如果尚未啟動、請啟動CIFS組態公用程式：「config_CIFs.rb」

b. 加入網域：「join網域」

c. 系統會提示您測試管理節點目前是否為網域的有效成員。如果此管理節點先前尚未加入網域、請輸入：「no」

d. 出現提示時、請提供系統管理員的使用者名稱：「*Administrator _username*'」

其中、「*Administrator*使用者名稱」是CIFS Active Directory使用者名稱、而非StorageGRID 指不實的使用者名稱。

e. 出現提示時、請提供系統管理員的密碼：「*Administrator*密碼」

「_Administrator密碼」是CIFS Active Directory使用者名稱、而非StorageGRID 「功能密碼」。

f. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

7. 確認您已正確加入網域：

a. 加入網域：「join網域」

b. 當系統提示您測試伺服器目前是否為網域的有效成員時、請輸入：「y」

如果您收到訊息「Join is OK、」、表示您已成功加入網域。如果您沒有收到此回應、請嘗試設定驗證並再次加入網域。

c. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

8. 新增稽核用戶端：「add-稽 核共用區」

a. 當系統提示您新增使用者或群組時、請輸入：「user'（使用者）」

b. 當系統提示您輸入稽核使用者名稱時、請輸入稽核使用者名稱。

c. 出現提示時、請按* Enter *。

此時會顯示CIFS組態公用程式。

9. 如果允許多個使用者或群組存取稽核共用區、請新增其他使用者：「add-user-to共用區」

隨即顯示已啟用共享區的編號清單。

a. 輸入稽核匯出共用的數量。
b. 當系統提示您新增使用者或群組時、請輸入：「group（群組）」

   系統會提示您輸入稽核群組名稱。

c. 當系統提示您輸入稽核群組名稱時、請輸入稽核使用者群組的名稱。
d. 出現提示時、請按* Enter *。

   此時會顯示CIFS組態公用程式。

e. 針對每個具有稽核共用存取權的其他使用者或群組、重複此步驟。

10. 或者、請驗證您的組態：「valide-config」

    系統會檢查並顯示這些服務。您可以安全地忽略下列訊息：

    - 找不到包含檔案「/etc/samba/includes/cifs-interfaces.inc`」
    - 找不到包含檔案「/etc/samba/includes/cifs-filesystem.inc`」
    - 找不到包含檔案「/etc/samba/includes/cifs-interfaces.inc`」
    - 找不到包含檔案「/etc/samba/includes/cifs-custom-config.inc`」
    - 找不到包含檔案「/etc/samba/includes/cifs-shares.inc`」
    - rlim_max：將rlimation_max（1024）增加至最小Windows限制（16384）

      請勿將「ecurity=ads」設定與「密碼伺服器」參數結合使用。（根據預設、Samba會自動探索正確的DC）。

      i. 出現提示時、請按* Enter *以顯示稽核用戶端組態。
      ii. 出現提示時、請按* Enter *。

          此時會顯示CIFS組態公用程式。

11. 關閉CIFS組態公用程式：「Exit（結束）」
12. 如果StorageGRID 這個部署是單一站台、請前往下一步。

    或

    或者、如果StorageGRID 此功能的支援包括其他站台的管理節點、請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：「sh admin@*grid_node_ip*`」
       ii. 輸入「passwords.txt」檔案中所列的密碼。
       iii. 輸入下列命令以切換至root：「u -」
       iv. 輸入「passwords.txt」檔案中所列的密碼。
    b. 重複這些步驟、為每個管理節點設定稽核共用。

c. 關閉管理節點的遠端安全Shell登入：「Exit（結束）」

13. 登出命令Shell：「exit」

將使用者或群組新增至**CIFS**稽核共用區

您可以將使用者或群組新增至與AD驗證整合的CIFS稽核共用區。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin帳戶密碼（可在上述套件中找到）。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。

關於這項工作

下列程序適用於與AD驗證整合的稽核共用。

透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。

2. 確認所有服務的狀態均為「執行中」或「已驗證」。輸入：「toragegrid狀態」

   如果所有服務均未執行或「已驗證」、請先解決問題再繼續。

3. 返回命令列、按* Ctrl-+* C*。
4. 啟動CIFS組態公用程式：「config_CIFs.rb」

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. 開始新增使用者或群組：「add-user-to共享」

   隨即顯示已設定之稽核共用的編號清單。

6. 出現提示時、請輸入稽核共用（稽核匯出）的編號：「*nap_share_number*」

   系統會詢問您是否要授予使用者或群組存取此稽核共用區的權限。

7. 出現提示時、請新增使用者或群組：「使用者」或「群組」
8. 當系統提示您輸入此AD稽核共用的使用者或群組名稱時、請輸入名稱。

   使用者或群組會新增為唯讀、以供稽核共用在伺服器作業系統和CIFS服務中使用。系統會重新載入Samba組態、讓使用者或群組能夠存取稽核用戶端共用區。

9. 出現提示時、請按* Enter *。

   此時會顯示CIFS組態公用程式。

10. 針對每個擁有稽核共用存取權的使用者或群組、重複這些步驟。
11. 或者、請驗證您的組態：「valide-config」

    系統會檢查並顯示這些服務。您可以安全地忽略下列訊息：

    - 找不到包含檔案/etc/samba/includes/cifs-interfaces.inc
    - 找不到包含檔案/etc/samba/includes/cifs-filesystem.inc
    - 找不到包含檔案/etc/samba/includes/cifs-custom-config.inc
    - 找不到包含檔案/etc/samba/includes/cifs-shares.inc
      i. 出現提示時、請按* Enter *以顯示稽核用戶端組態。
      ii. 出現提示時、請按* Enter *。
12. 關閉CIFS組態公用程式：「Exit（結束）」
13. 判斷您是否需要啟用額外的稽核共用、如下所示：
    - 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：「sh admin@*grid_node_ip*`」
         B. 輸入「passwords.txt」檔案中所列的密碼。
         C. 輸入下列命令以切換至root：「u -」
         D. 輸入「passwords.txt」檔案中所列的密碼。
      ii. 重複這些步驟、為每個管理節點設定稽核共用。
      iii. 關閉遠端管理節點的遠端安全Shell登入：「Exit（結束）」
14. 登出命令Shell：「exit」

您無法移除上次允許存取稽核共用的使用者或群組。

您需要的產品

- 您的「Passwords．txt」檔案含有root帳戶密碼（可在上述套件中找到）。
- 您有「Configuration．TXT」檔案（可在上述套件中找到）。

關於這項工作

透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。

2. 啟動CIFS組態公用程式：「config_CIFs.rb」

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. 開始移除使用者或群組：「移除使用者自共用區」

   系統會顯示管理節點可用稽核共用的編號清單。稽核共用會標示為稽核匯出。

4. 輸入稽核共用區的編號：「*nap_share_number*」
5. 當系統提示您移除使用者或群組時：「使用者」或「群組」

   隨即顯示稽核共用的使用者或群組編號清單。

6. 輸入您要移除的使用者或群組對應的號碼：「*number*」

稽核共用區將會更新、且使用者或群組不再允許存取稽核共用區。例如：

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. 關閉CIFS組態公用程式：「Exit（結束）」
8. 如果StorageGRID 此功能包括其他站台的管理節點、請視需要停用每個站台的稽核共用。
9. 設定完成時、請登出每個命令Shell：「exit」

變更**CIFS**稽核共用使用者或群組名稱

您可以新增新的使用者或群組、然後刪除舊的使用者或群組、來變更CIFS稽核共用的使用者或群組名稱。

關於這項工作

透過CIFS/Samba進行的稽核匯出已過時、將在未來StorageGRID 的版本中移除。

步驟

1. 將新的使用者或群組以更新名稱新增至稽核共用區。
2. 刪除舊的使用者或群組名稱。

相關資訊

- 將使用者或群組新增至CIFS稽核共用區
- 從CIFS稽核共用區移除使用者或群組

驗證**CIFS**稽核整合

稽核共用為唯讀。記錄檔是供電腦應用程式讀取、驗證不包括開啟檔案。稽核日誌檔顯示在Windows檔案總管視窗中的驗證已足夠。連線驗證完成後、請關閉所有視窗。

設定**NFS**的稽核用戶端

稽核共用會自動啟用為唯讀共用。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin密碼（可在上述套件中找到）。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。
- 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：「sh admin@_primary管理節點IP」
   b. 輸入「passwords.txt」檔案中所列的密碼。
   c. 輸入下列命令以切換至root：「u -」
   d. 輸入「passwords.txt」檔案中所列的密碼。

      以root登入時、提示會從「$」變更為「#」。
2. 確認所有服務的狀態均為「執行中」或「已驗證」。輸入：「toragegrid狀態」

   如果未將任何服務列為「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-稽 核共用區」
   a. 出現提示時、請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、請新增額外使用者的IP位址：「add-ip-to共享區」
   a. 輸入稽核共用區的編號：「*nap_share_number*」
   b. 出現提示時、請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. 輸入下列內容：「valide-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：「sh admin@*grid_node_ip*`」

B. 輸入「passwords.txt」檔案中所列的密碼。

C. 輸入下列命令以切換至root：「u -」

D. 輸入「passwords.txt」檔案中所列的密碼。

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。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin帳戶密碼（可在上述套件中找到）。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。
- 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：「sh admin@_primary管理節點IP」

b. 輸入「passwords.txt」檔案中所列的密碼。

c. 輸入下列命令以切換至root：「u -」

d. 輸入「passwords.txt」檔案中所列的密碼。

以root登入時、提示會從「$」變更為「#」。

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共享」

隨即顯示在管理節點上啟用的NFS稽核共用清單。稽核共用區列示為：「/var/local/nvmnal/export」

4. 輸入稽核共用區的編號：「*nap_share_number*」
5. 出現提示時、請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、請驗證您的組態：「valide-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：「sh admin@*grid_node_ip*`」

ii. 輸入「passwords.txt」檔案中所列的密碼。

iii. 輸入下列命令以切換至root：「u -」

iv. 輸入「passwords.txt」檔案中所列的密碼。

b. 重複這些步驟、為每個管理節點設定稽核共用。

c. 關閉遠端管理節點的遠端安全Shell登入：「Exit（結束）」

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。

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）：

   「安裝-t nfs -o hard、intr *admin_Node_ip_address*：/var/local/nude/export *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、在上一個命令中為「*myAudit*」）。

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。

您需要的產品

- 您有「Passwords・txt」檔案、其中包含root / admin帳戶密碼（可在上述套件中找到）。
- 您有「Configuration・TXT」檔案（可在上述套件中找到）。

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：「sh admin@_primary管理節點IP」

   b. 輸入「passwords.txt」檔案中所列的密碼。

   c. 輸入下列命令以切換至root：「u -」

   d. 輸入「passwords.txt」檔案中所列的密碼。

以root登入時、提示會從「$」變更為「#」。

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：「移除IP位址、從共用區」

   隨即顯示伺服器上設定的稽核共用編號清單。稽核共用區列示為：「/var/local/nvmnal/export」

4. 輸入與稽核共用區相對應的編號：「*nap_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：「sh admin@*grid_node_ip*`」
      ii. 輸入「passwords.txt」檔案中所列的密碼。
      iii. 輸入下列命令以切換至root：「u -」
      iv. 輸入「passwords.txt」檔案中所列的密碼。
   b. 重複這些步驟、為每個額外的管理節點設定稽核共用。
   c. 關閉遠端管理節點的遠端安全Shell登入：「Exit（結束）」
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

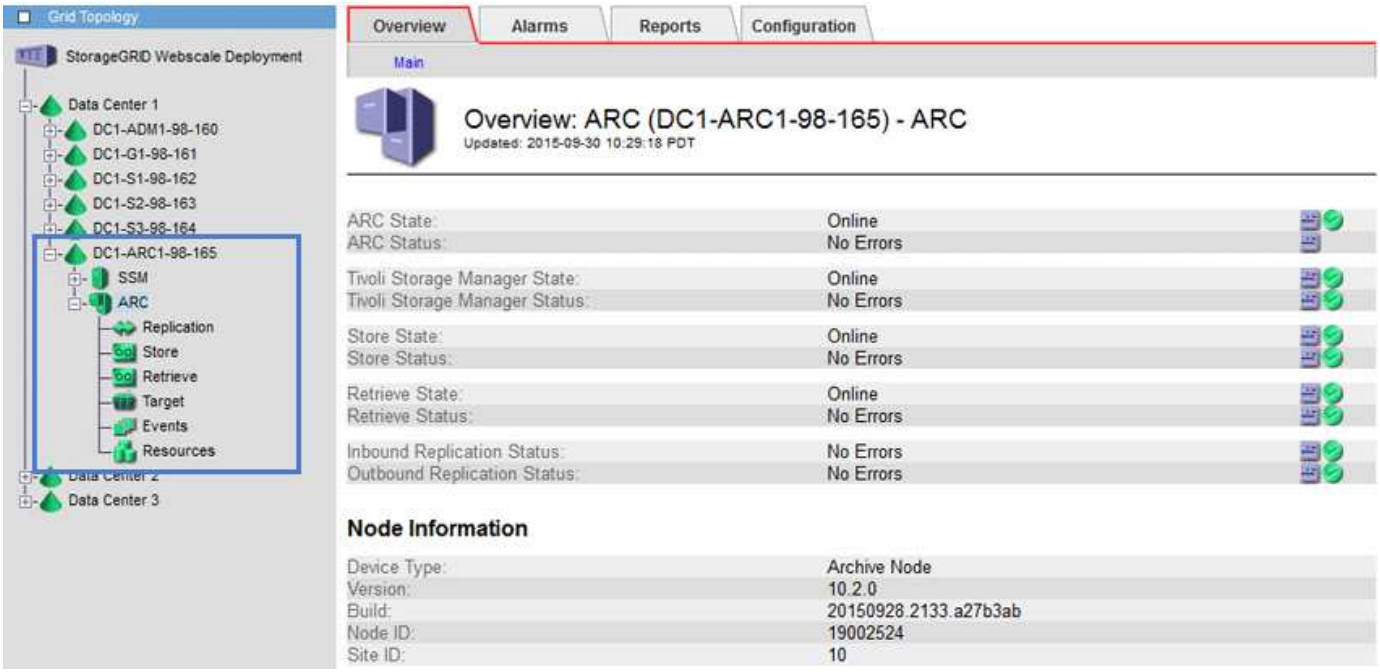
- 將NFS稽核用戶端新增至稽核共用區
- 從稽核共用區移除NFS稽核用戶端

管理歸檔節點

什麼是歸檔節點

您也可以選擇StorageGRID 使用歸檔節點來部署每個資料中心站台、以便連線至目標外部歸檔儲存系統、例如Tivoli Storage Manager（TSM）。

歸檔節點提供一個介面、您可以透過這個介面鎖定外部歸檔儲存系統、以長期儲存物件資料。歸檔節點也會監控此連線、以及StorageGRID 物件資料在整個系統與目標外部歸檔儲存系統之間的傳輸。



設定外部目標的連線之後、您可以設定歸檔節點以最佳化TSM效能、在TSM伺服器即將達到容量或無法使用時、讓歸檔節點離線、以及設定複寫和擷取設定。您也可以設定歸檔節點的自訂警示。

無法刪除但未定期存取的物件資料、可隨時從儲存節點的旋轉式磁碟移出、並移至雲端或磁帶等外部歸檔儲存設備。此物件資料歸檔是透過設定資料中心站台的歸檔節點、然後設定ILM規則、將此歸檔節點選取為內容放置指示的「目標」。歸檔節點不會自行管理歸檔的物件資料、這是由外部歸檔裝置所達成。

物件中繼資料不會歸檔、但會保留在儲存節點上。

什麼是**ARC**服務

歸檔節點上的歸檔（ARC）服務提供管理介面、可用來設定外部歸檔儲存設備的連線、例如透過TSM中介軟體建立的磁帶。

這項服務可與外部歸檔儲存系統互動、傳送近線儲存的物件資料、以及在用戶端應用程式要求歸檔物件時執行擷取。當用戶端應用程式要求歸檔物件時、儲存節點會從ARC服務要求物件資料。ARC服務會向外部歸檔儲存系統提出要求、以擷取要求的物件資料、然後將其傳送至ARC服務。ARC服務會驗證物件資料、並將其轉送至儲存節點、然後再將物件傳回要求的用戶端應用程式。

透過TSM中介軟體將物件資料歸檔至磁帶的要求、將會加以管理、以提高檢索效率。您可以訂購要求、以相同的順序要求以連續順序儲存在磁帶上的物件。然後將要求排入佇列、以便提交至儲存設備。視歸檔裝置而定、可同時處理不同磁碟區上的多個物件要求。

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。

> ⓘ 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。「雲端分層-簡易儲存服務（**S3**）」選項仍受支援、但您可能偏好實作雲端儲存資源池。

如果您目前使用的歸檔節點搭配*雲端分層-簡易儲存服務（S3）*選項、請考慮將物件移轉至雲端儲存資源池。請參閱的說明 使用ILM管理物件。

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。

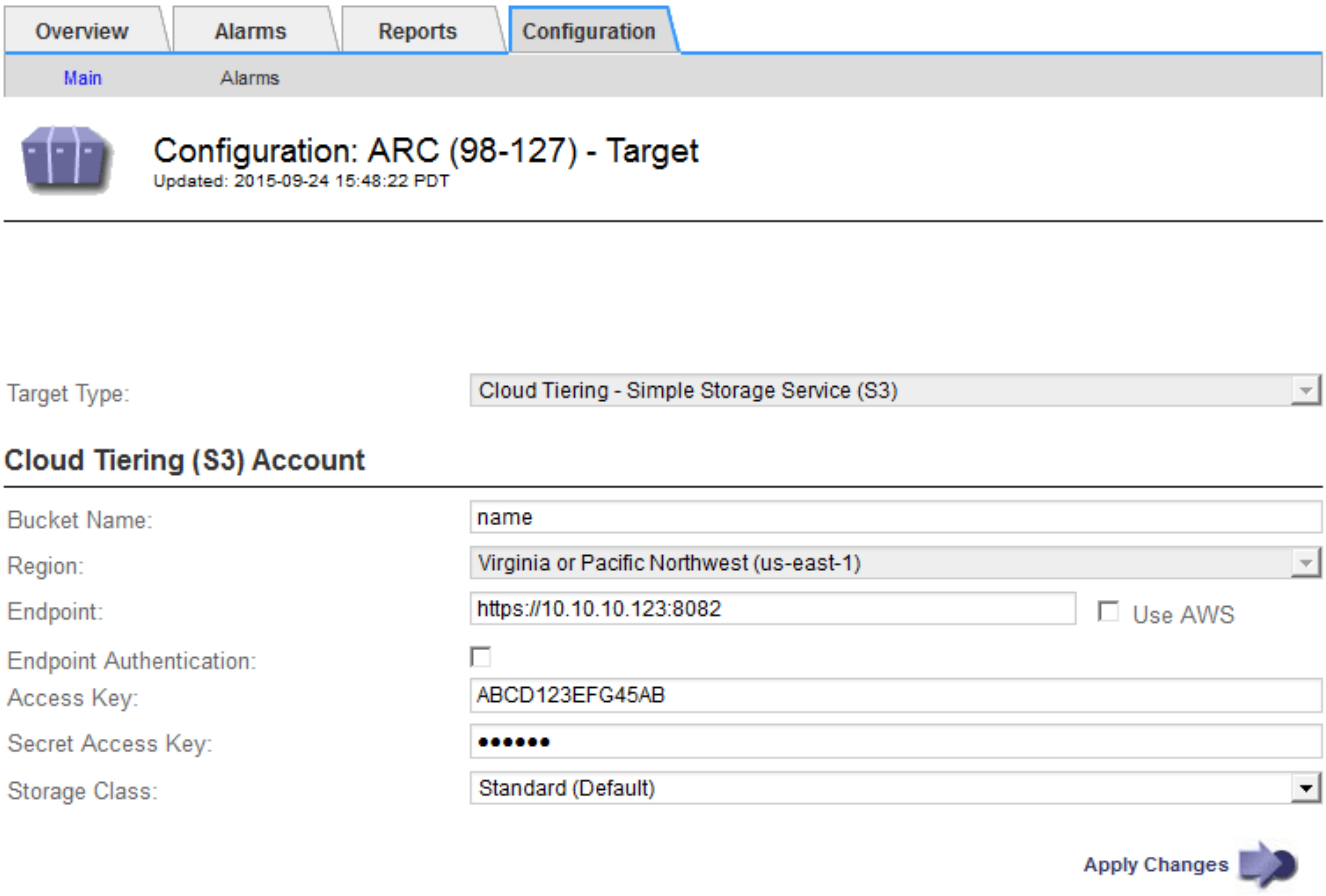
> ⓘ 透過S3 API將物件從歸檔節點移至外部歸檔儲存系統、已由ILM Cloud Storage Pool取代、提供更多功能。「雲端分層-簡易儲存服務（**S3**）」選項仍受支援、但您可能偏好實作雲端儲存資源池。
>
> 如果您目前使用的歸檔節點搭配*雲端分層-簡易儲存服務（S3）*選項、請考慮將物件移轉至雲端儲存資源池。請參閱 使用ILM管理物件。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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、您可以取消選取核取方塊、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 目標歸檔儲存設備是另一個作業系統執行個體、且系統已設定公開簽署的憑證、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。一旦設定完成、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。

您需要的產品

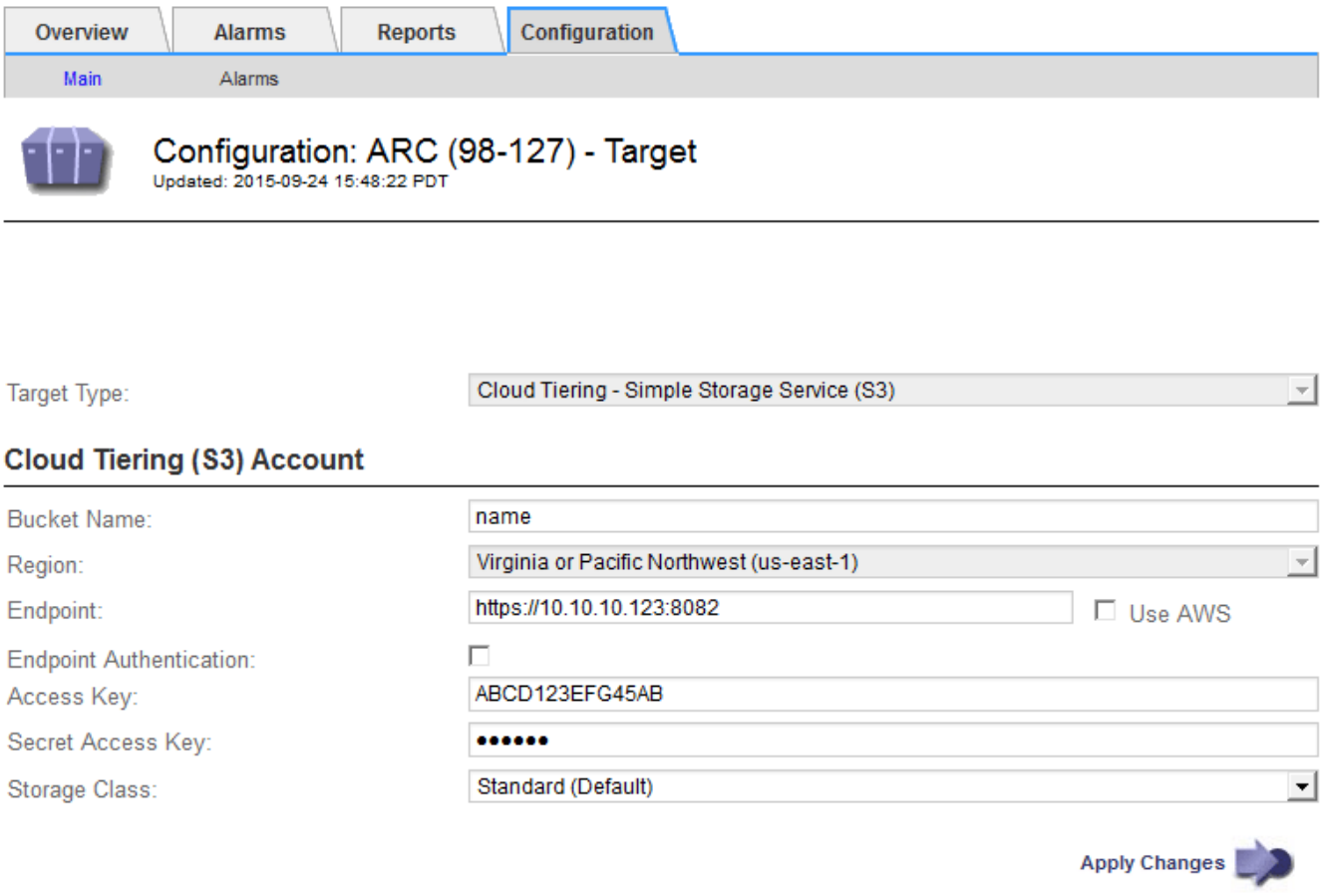
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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。

   儲存區名稱、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。

您需要的產品

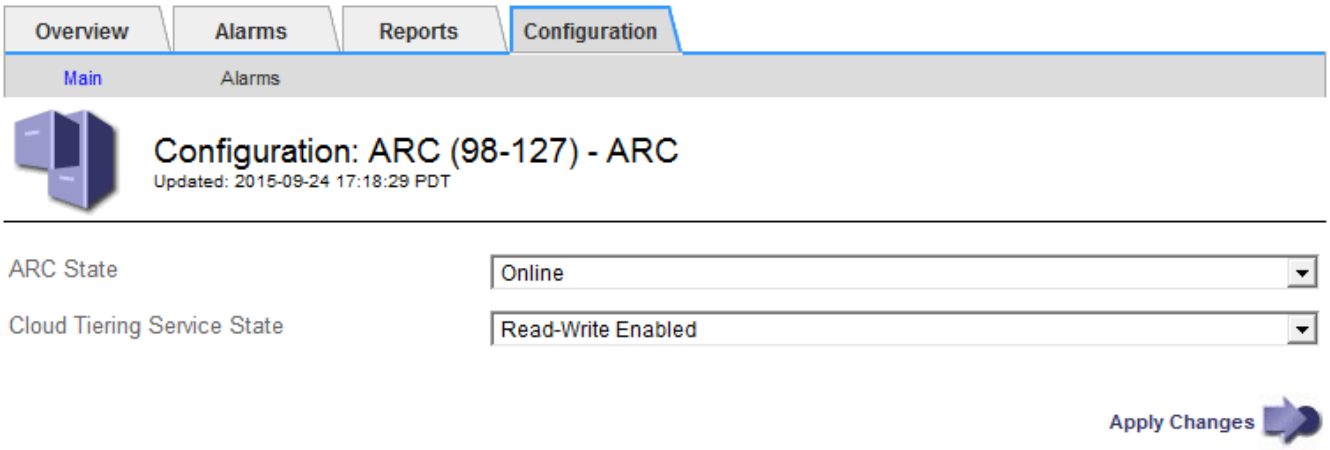
- 您必須使用登入Grid Manager 支援的網頁瀏覽器。
- 您必須擁有特定的存取權限。
- 必須設定歸檔節點。

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

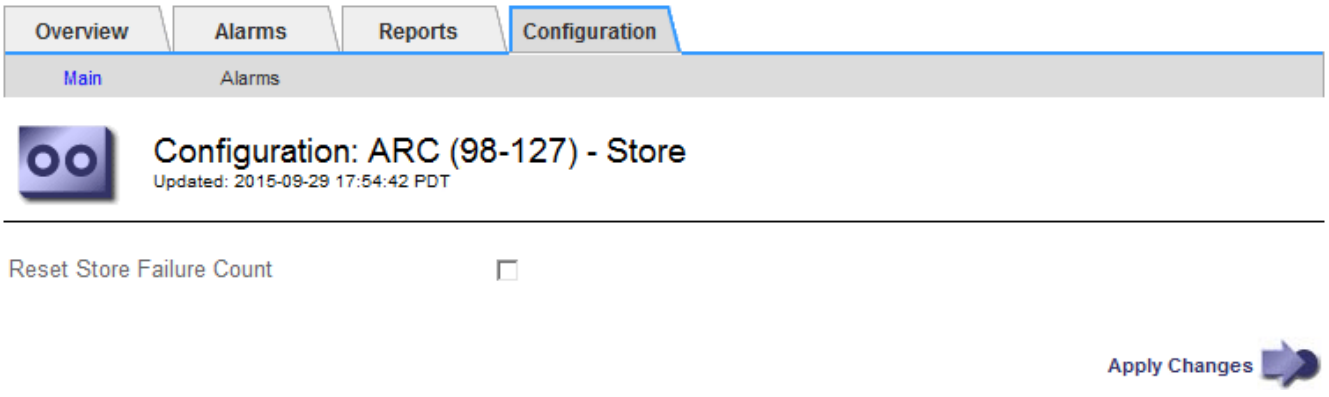
如果您的歸檔節點透過S3 API連線至歸檔儲存系統、您可以重設儲存失敗計數、以清除ARVf（儲存故障）警示。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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、請考慮改為將物件移轉至雲端儲存資源池。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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。
- 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Cloud Storage Pool中時、這些物件的複本也無法儲存在StorageGRID 實物庫中。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. 在作用中ILM原則中找出任何導致物件儲存在雲端分層儲存區的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。

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

在歸檔節點能夠與Tivoli Storage Manager（TSM）中介軟體通訊之前、您必須先設定許多設定。

您需要的產品

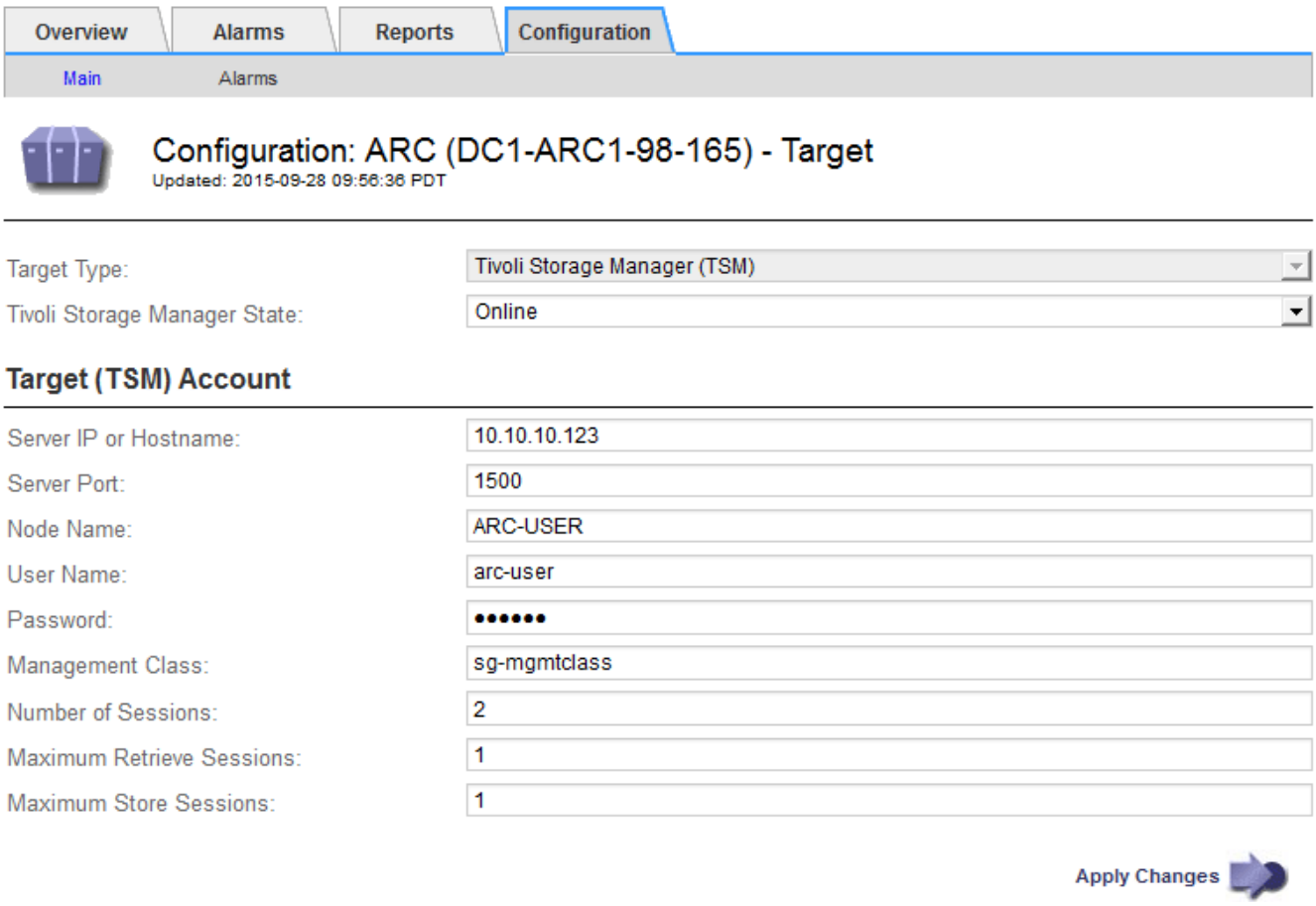
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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。

您需要的產品

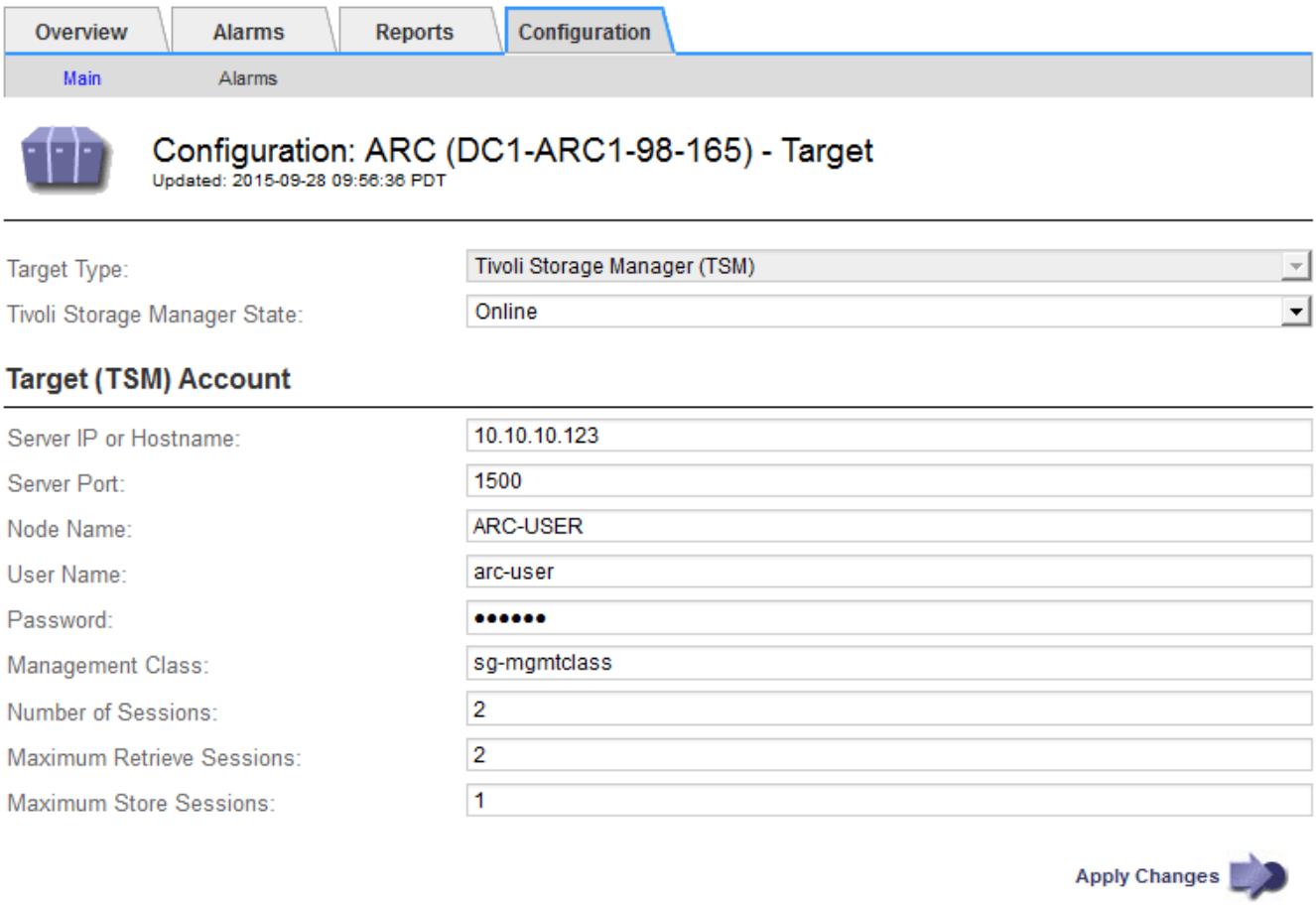
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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

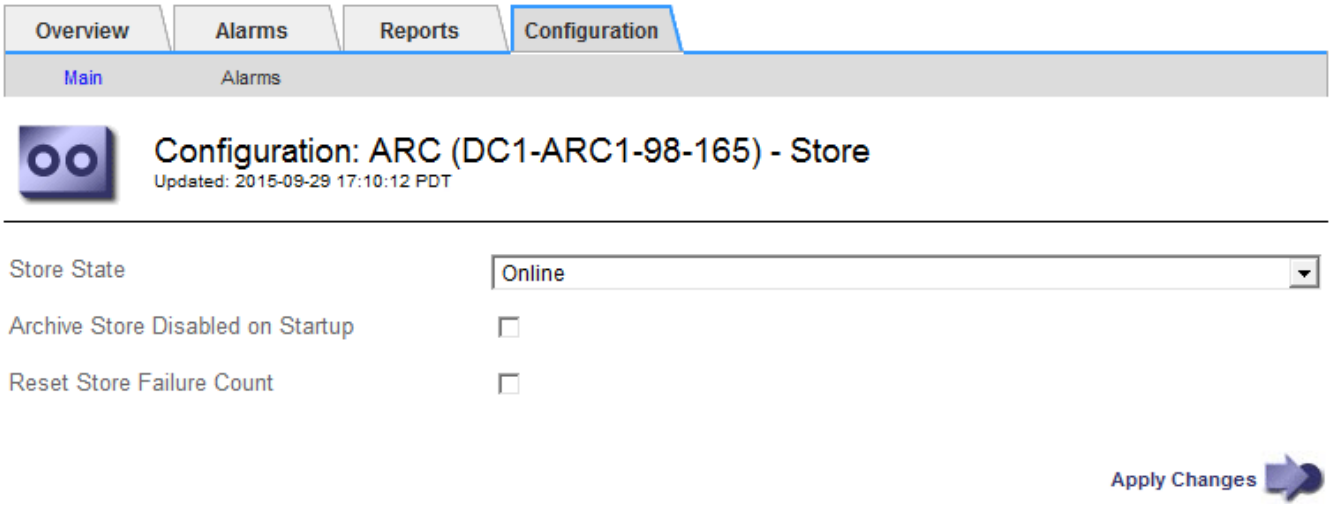
如果您的歸檔節點連線至TSM中介軟體伺服器、您可以將歸檔節點的歸檔儲存區狀態設定為「線上」或「離線」。您也可以在歸檔節點首次啟動時停用歸檔儲存區、或是重設追蹤相關警示的故障數。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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TSM伺服器所管理的媒體。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「離線」。
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

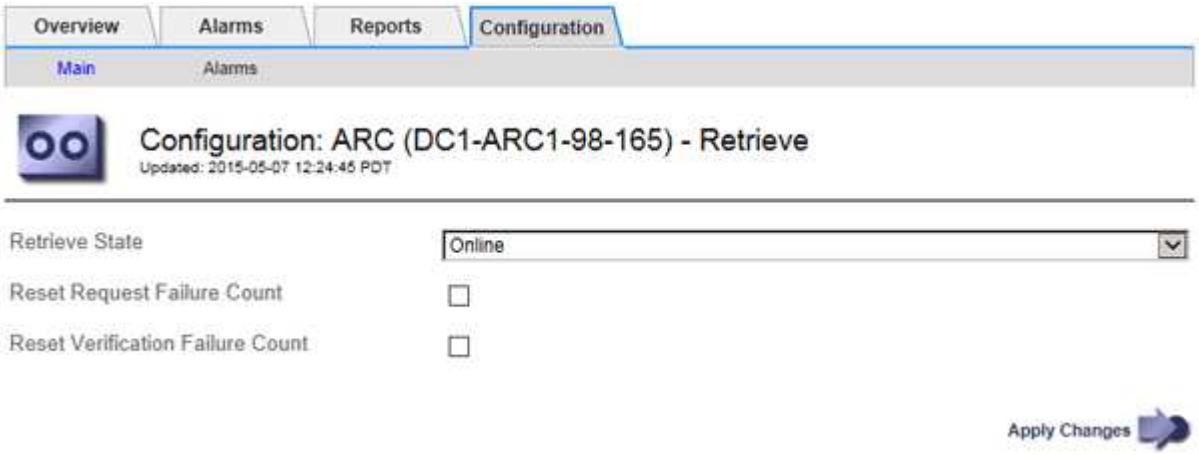
您可以設定歸檔節點的擷取設定、將狀態設定為「線上」或「離線」、或重設要追蹤相關警示的故障計數。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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：勾選此核取方塊可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：勾選此核取方塊可重設已擷取物件資料的驗證失敗計數器。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

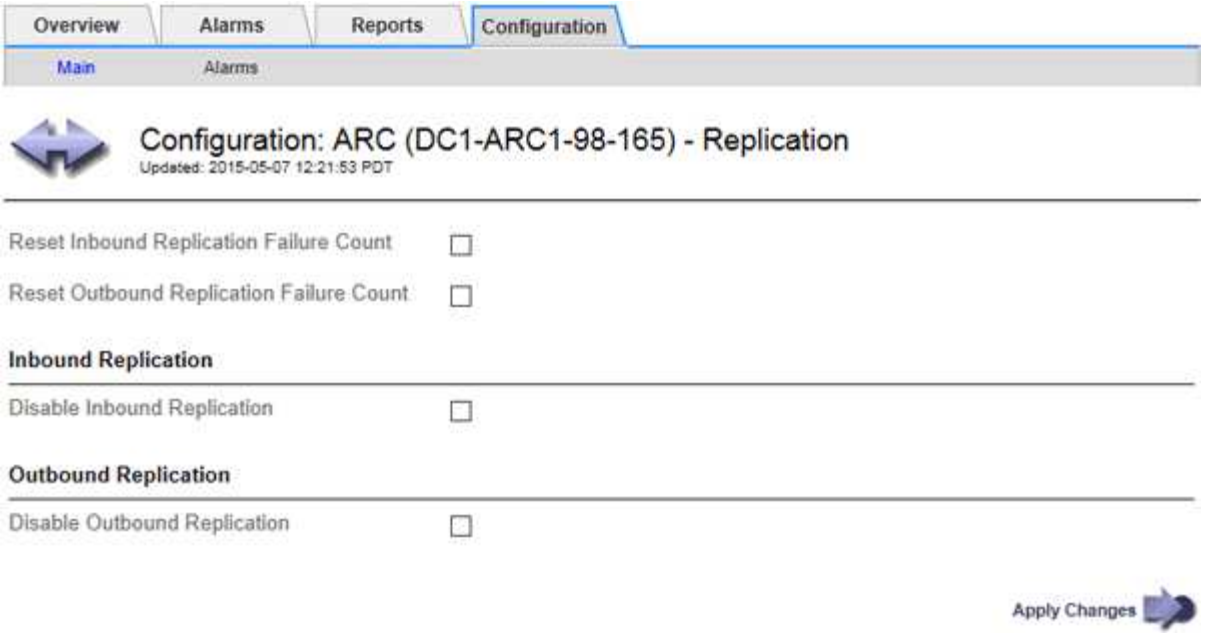
您可以設定歸檔節點的複寫設定、停用傳入和傳出複寫、或是重設追蹤相關警示的失敗計數。

您需要的產品

- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您擁有特定的存取權限。

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。

     當停用傳入複寫時、可以從ARC服務擷取物件資料、以便複寫到StorageGRID 其他系統位置的其他位置、但無法從其他系統位置將物件複寫到此ARC服務。ARC服務為唯讀。
   - 停用傳出複寫：勾選此核取方塊、即可停用傳出複寫（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。

     當停用輸出複寫時、物件資料可複製到此ARC服務以滿足ILM規則、但無法從ARC服務擷取物件資料、以便複製到StorageGRID 其他地點。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 監控及疑難排解。

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StorageGRID 針對您的一套系統所定義的資訊生命週期管理（ILM）規則、將複本複製到所有必要的位置、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涉及的延遲。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）。磁帶集區不可設定為同時寫入兩個集區的磁碟集區複本集區（也就是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

本節包含依照TSM最佳實務做法準備TSM伺服器的範例說明。

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

這些說明僅供參考、不適用於取代TSM文件、也不適用於所有組態的完整完整說明。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。

您必須在TSM伺服器上完成許多步驟、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。

您必須以系統管理權限登入伺服器、然後使用dsmadmc工具執行下列命令。

步驟

1. 建立磁帶庫。

   "Define庫_Tapelibstite_libtype=*scsi*"

   其中，"*tapelibinity*"是磁帶庫的任意名稱，而"libtype"的值則視磁帶庫類型而定。

2. 定義從伺服器到磁帶庫的路徑。

   "Define path *servername Tapelibstation* srctype=server desttype=libraryDEVICE =*lib-devicName*"

   - 「伺服器名稱」是TSM伺服器的名稱
   - 「*tapeliiliinfort*」是您定義的磁帶庫名稱
   - 「*lib-devicenam_*」是磁帶庫的裝置名稱

3. 定義程式庫的磁碟機。

   「磁碟機_磁帶庫_磁碟機名稱_」

   - "*drivename*"是您要為磁碟機指定的名稱
   - 「*tapeliiliinfort*」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 *servernames* drivename srcty=server desttype=drive library=*tapeliablestation*_設備=*_drive-dname*"

   - 「*drive-dname*」是磁碟機的裝置名稱
   - 「*tapeliiliinfort*」是您定義的磁帶庫名稱

     對您為磁帶庫定義的每個磁碟機重複上述步驟、每個磁碟機都使用單獨的「*drivename_*」和「*drive-dname*」。

5. 定義磁碟機的裝置類別。

   "Define devClass *Device*類*Name* devtype=*lto*庫=*_tapeliationstation* format =*tapetype*"

   - 「_Device類別名稱」是裝置類別的名稱
   - 「_lto」是連接至伺服器的磁碟機類型
   - 「*tapeliiliinfort*」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。

   "簽 入libvolume *tapelibsta*"

   「*tapeliiliinfort*」是您定義的磁帶庫名稱。

7. 建立主要磁帶儲存資源池。

   "Define stgpool *SGWSTapepoolDevice*類*Name descriptioncollocat=filespace* mastScature=*XX*"

   - 「_SGWSTapePool」是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）。
   - 「*Device Class Name*」是磁帶庫的裝置類別名稱。
   - 「*description*」是使用「query stgpool」命令顯示在TSM伺服器上的儲存資源池說明。例如：「適用於歸檔節點的磁帶儲存池。」
   - "*collocat=filspace*"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_*最大大小=*_Maximum_file_size nextstgpool = SGWSTapepool* highmig=*center_high_* Lowmig=*center_Low*"

   - 「SGWSDiskPool」是歸檔節點的磁碟集區名稱。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*」是使用「query stgpool」命令顯示在TSM伺服器上的儲存資源池說明。例如、「為歸檔節點建立儲存資源池」。
   - 「*imize_file_Size*」會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。建議將「*imize_file_Size*」設為10 GB。
   - nextstgPool=SGWSTapePool_'是指磁碟儲存資源池與為歸檔節點定義的磁帶儲存資源池。
   - 「_同 百分比_high」設定磁碟集區開始將其內容移轉到磁帶集區的值。建議將「_百分_high」設為0、以便立即開始資料移轉
   - 「_同 百分比_low」會設定移轉至磁帶集區的停止值。建議將「_同 百分比_low」設為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*名稱 format Size=*Size*（磁碟區大小_）"

   - 「SGWSDiskPool」是磁碟集區名稱。
   - 「Volume名稱」是TSM伺服器上磁碟區位置的完整路徑（例如、「/var/local/ars/stage6.DSM」）、其會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伺服器上為MAXNUMMP指定的數目必須至少與為「* ARC*>* Target > Configuration > Main*>*最大儲存區工作階段*」所設定的值一樣大、 設為0或1的值、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節點會使用自訂網域原則「TSM網域」。「TSM網域」網域原則是修改版的「標準」網域原則、設定為寫入磁帶、並將歸檔目的地設定為StorageGRID 「32位元系統」的儲存資源池（`_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。

   「複製網域標準TSM網域」

2. 如果您不使用現有的管理類別、請輸入下列其中一項：

   「定義政策集TSM網域標準」

   「定義mgmtClass TSM網域標準_預設_」

   缺省管理級別是部署的缺省管理級別。

3. 建立複本群組至適當的儲存資源池。輸入（一行）：

   "Define copygroup TSM網域標準_default_type=archive ditation=SGWSDiskPool retinit=Event retmin=0（定義複本群組TSM網域標準_預設_類型=歸檔目的地= SGWSDiskPool retinit=0）"

   缺省管理類是歸檔節點的缺省管理類。選擇了"retinit"、"retmin"和"retver"等值、以反映歸檔節點目前使用的

保留行為

請勿將「重複」設為「重複=建立」。由於保留事件是用來從TSM伺服器移除內容、因此設定「retinit =create」會封鎖歸檔節點刪除內容。

4. 將管理類別指派為預設類別。

   「指派defmgmtClass *tsm-domain*_標準_*default*'

5. 將新原則集設為作用中。

   「啟動policySet TSM網域標準」

   請忽略輸入activate命令時出現的「no copy group」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）：

   「移除節點arcus-user arc-passwordpassexp = 0 domain=TSM-DOMAXnucm=number-of工作階段」

   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。

下一節是瞭解並規劃將大量資料移轉至StorageGRID 該系統的指南。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 支援的不一致系統包含歸檔節點、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具有足夠的容量來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 和 監控及疑難排解。

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。

移轉對作業的影響

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章的說明進行仔細管理、以避免影響日常系統作業、或在極端情況下、在StorageGRID 不正常運作的情況下、將資料置於喪失風險之中。

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 整個系統、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、請勿在高活動期間排程資料移轉。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。