StorageGRID 12.1 軟體文件

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid/index.html on July 22, 2026.
Always check docs.netapp.com for the latest.

目錄

StorageGRID 12.1 軟體文件 1
了解 StorageGRID 設備硬體 2
版本資訊 3
StorageGRID 12.1 的新功能 3
容量 3
控制存取 3
聯邦 3
可管理性 3
S3 3
安全性 4
租戶 4
升級 5
使用者介面 5
StorageGRID 中已移除或已棄用的功能 5
定義 5
StorageGRID 功能支援結束 6
StorageGRID 中 Grid Management API 的變更 7
用於變更 BMC 密碼和 LAN IP 設定的新端點 7
StorageGRID 中租戶管理 API 的變更 8
用於物件複製的新 API 8
StorageGRID S3 REST API 支援變更 8
開始使用 StorageGRID 系統 13
深入瞭解StorageGRID 13
什麼是StorageGRID 功能？ 13
混合雲StorageGRID 與功能 14
架構與網路拓撲StorageGRID 15
網格節點和服務 19
如何管理資料StorageGRID 30
探索 StorageGRID 42
網路準則 49
StorageGRID 的網路準則 49
網路類型StorageGRID 50
網路拓撲範例 54
StorageGRID 的網路需求 60
StorageGRID 的網路特定需求 62
部署特定的網路考量 63
StorageGRID 的網路安裝與資源配置 66
StorageGRID 的安裝後準則 67
網路連接埠參考 67

StorageGRID 快速入門 74
安裝、升級及 Hotfix StorageGRID 77
安裝 StorageGRID 節點 77
了解 StorageGRID 設備硬體 77
安裝軟體型節點 77
配置網格並完成安裝 164
了解安裝 StorageGRID 後所需和選用的步驟 176
升級StorageGRID 版軟體 177
升級StorageGRID 版軟體 177
規劃及準備升級 178
升級軟體 183
疑難排解 StorageGRID 升級問題 198
套用 StorageGRID Hotfix 200
修復程序StorageGRID 200
應用熱修復程式後 StorageGRID 會受到怎樣的影響 201
取得 StorageGRID 熱修復程式所需的材料 202
下載 StorageGRID Hotfix 檔案 202
在套用 StorageGRID 熱修復程式之前、請先檢查系統狀況 203
在 StorageGRID 中套用 Hotfix 204
設定及管理 StorageGRID 系統 208
管理StorageGRID 208
StorageGRID 管理快速入門 208
開始使用 Grid Manager 209
控制StorageGRID 對功能的存取 234
使用網格同盟 302
管理安全性 346
管理租戶 407
設定用戶端連線 425
管理網路和連線 462
管理儲存節點 480
管理管理節點 492
使用ILM管理物件 494
使用 ILM 管理 StorageGRID 中的物件 494
ILM與物件生命週期 494
在 StorageGRID 中建立並指派儲存等級 514
使用儲存池 516
使用雲端儲存資源池 524
在 StorageGRID 中管理銷毀編碼設定檔 542
為StorageGRID配置 S3 區域 545
建立ILM規則 546
管理 ILM 原則 561

在 StorageGRID 中使用 ILM 原則和 ILM 規則 576
使用S3物件鎖定 580
ILM規則與原則範例 587
StorageGRID 的系統強化 607
了解 StorageGRID 的系統強化 607
StorageGRID 軟體升級的強化準則 607
強化有關資訊網路的準則StorageGRID 608
強化有關節點的準則StorageGRID 609
StorageGRID 中 TLS 和 SSH 的強化準則 612
StorageGRID 中日誌、密碼和稽核訊息的強化準則 614
StorageGRID 搭配 FabricPool 615
使用 StorageGRID 搭配 FabricPool 的設定工作流程 615
將 StorageGRID 附加為 FabricPool 雲端層所需的資訊 616
使用 FabricPool 設定精靈 617
手動設定 StorageGRID 630
配置 ONTAP System Manager，將 StorageGRID 新增為 FabricPool 雲端層 639
使用 FabricPool 為 StorageGRID 配置 DNS 伺服器項目 640
適用於 FabricPool 的 StorageGRID 最佳實務做法 641
從 StorageGRID 移除 FabricPool 資料 644
使用 StorageGRID 租戶和用戶端 646
使用租戶帳戶 646
使用StorageGRID 綁定帳戶 646
如何登入及登出 647
StorageGRID 中的租戶管理器儀表板 649
租戶管理API 651
使用網格同盟連線 656
管理群組和使用者 665
管理S3存取金鑰 681
管理S3儲存區 686
管理S3平台服務 712
使用S3 REST API 742
StorageGRID S3 REST API 支援的版本和更新 742
StorageGRID 中支援的 S3 API 要求 746
測試 StorageGRID S3 REST API 組態 765
如何實作S3 REST API StorageGRID 767
支援 Amazon S3 REST API 781
StorageGRID 自訂作業 829
管理存取策略 848
StorageGRID 稽核日誌中追蹤的 S3 操作 874
使用 Swift REST API （生命週期結束） 875
StorageGRID 中的 Swift REST API 支援 875

監控 StorageGRID 系統並進行疑難排解 876
監控 StorageGRID 系統 876
使用AutoSupport 876
監控StorageGRID 一個系統 889
在 StorageGRID 中檢視及管理儀表板 889
檢視「節點」頁面 892
定期監控的資訊 918
管理警示 943
記錄檔參考 975
設定日誌管理和外部系統日誌伺服器 993
設定郵件伺服器 1006
使用SNMP監控 1008
收集其他StorageGRID 的資料 1019
疑難排解 StorageGRID 系統 1032
疑難排解StorageGRID 作業系統 1032
疑難排解物件和儲存問題 1038
疑難排解 StorageGRID 中的中繼資料問題 1053
疑難排解 StorageGRID 中的憑證錯誤 1055
疑難排解 StorageGRID 中的管理節點和使用者介面問題 1057
疑難排解 StorageGRID 中的網路、硬體和平台問題 1060
疑難排解 StorageGRID 的外部 syslog 伺服器錯誤訊息 1068
了解 StorageGRID 中的負載平衡器快取問題 1070
檢閱稽核記錄 1071
稽核訊息和記錄 1071
稽核訊息如何透過 StorageGRID 系統傳輸到 audit.log 檔案以進行保留 1071
從 StorageGRID 管理節點命令列存取稽核記錄檔 1074
了解 StorageGRID 中的稽核記錄檔輪替 1075
稽核記錄檔格式 1075
稽核訊息格式 1087
稽核訊息和物件生命週期 1091
稽核訊息 1098
擴充StorageGRID系統的容量或功能 1137
了解如何擴充您的StorageGRID系統 1137
擴張計劃 1138
StorageGRID中複製資料的擴展規劃 1138
StorageGRID中糾刪碼（EC）資料的擴充規劃 1139
了解StorageGRID中擴充後的 EC 重新平衡 1139
擴充指南 1143
StorageGRID中新增物件容量的指南 1143
StorageGRID元資料容量新增指南 1145
StorageGRID中新增網格節點的指南 1146

StorageGRID新增網站的指南 1147
準備擴展您的StorageGRID系統 1148
下載並解壓縮StorageGRID 安裝檔案 1149
驗證硬體與網路 1154
新增網格節點或站台 1154
在StorageGRID中新增網格節點或新站點的工作流程概述 1154
在StorageGRID中新增或更新網格網路子網路以進行擴展 1155
在StorageGRID中部署新的網格節點 1156
執行StorageGRID擴展 1159
新增儲存磁碟區 1164
在StorageGRID系統新增儲存磁碟區 1164
在StorageGRID中為 VMware 儲存節點新增儲存磁碟區 1167
在StorageGRID中為 Linux 儲存節點新增直連磁碟區或 SAN 卷 1168
設定擴充系統 1172
在StorageGRID中配置新新增的節點和站點 1172
在StorageGRID擴充後，驗證儲存節點是否處於活動狀態。 1173
將 Prometheus 指標複製到StorageGRID中的新管理節點 1173
將稽核日誌複製到StorageGRID中的新管理節點 1175
在StorageGRID系統新增節點後，重新平衡糾刪碼資料。 1176
排除StorageGRID中的擴充錯誤 1179
維護 StorageGRID 系統 1180
StorageGRID 網格維護 1180
開始之前 1180
設備的維護程序 1180
下載 StorageGRID 恢復套件 1180
取消委任節點或站台 1181
停用 StorageGRID 節點或站台 1181
取消委任節點 1181
取消委任網站 1196
重新命名網格、站台或節點 1217
使用 StorageGRID 重新命名程序 1217
新增或更新 StorageGRID 顯示名稱 1221
節點程序 1226
StorageGRID 節點維護程序 1227
在 StorageGRID 中移動 ADC 服務 1227
將 StorageGRID Storage Node 轉換為僅資料節點 1228
重新開機、關機和電源程序 1229
連接埠重新對應程序 1241
Server Manager 程序 1244
網路程序 1253
更新 StorageGRID Grid Network 的子網路 1253

設定IP位址 1255
新增介面至現有節點 1273
在 StorageGRID 中設定 DNS 伺服器 1276
修改單一 StorageGRID 節點的 DNS 組態 1278
在 StorageGRID 中管理 NTP 伺服器 1280
恢復隔離的 StorageGRID 節點的網路連線 1281
主機和中介軟體程序 1282
將 StorageGRID 節點遷移到新的 Linux 主機 1282
在 StorageGRID 中配置 VMware 虛擬機器以自動重新啟動 1285
恢復或更換節點 1286
StorageGRID 節點恢復的警告和注意事項 1286
恢復網格節點的先決條件 1286
如果託管多個網格節點的伺服器故障、則節點恢復順序 1286
恢復節點的IP位址 1286
收集 StorageGRID 網格節點恢復所需的材料 1287
下載並解壓縮StorageGRID 安裝檔案 1287
選擇 StorageGRID 節點還原程序 1293
從儲存節點故障中恢復 1293
從 StorageGRID 儲存節點故障中恢復 1293
恢復應用裝置儲存節點 1294
從系統磁碟機不受影響的儲存磁碟區故障中恢復 1307
從系統磁碟機故障中恢復 1314
從管理節點故障中恢復 1325
StorageGRID 中的主要或非主要管理節點恢復 1325
使用同一個主要管理節點從主要管理節點故障中恢復 1325
使用非主要管理節點從主要管理節點故障中恢復 1333
從非主要管理節點故障中恢復 1340
從閘道節點故障中恢復 1346
替換 StorageGRID Gateway Node 1346
選擇 Start Recovery 以設定 StorageGRID Gateway Node 1347
從歸檔節點故障中恢復 1348
從 StorageGRID 歸檔節點故障中恢復 1348
取代 Linux 節點 1348
更換 StorageGRID 中的 Linux 節點 1348
為 StorageGRID 部署新的 Linux 主機 1349
將 StorageGRID 節點還原至主機 1350
執行額外的 StorageGRID 節點還原步驟 1354
將 StorageGRID 中的 VMware 節點替換為恢復節點 1355
將 StorageGRID 中的 VMware 節點替換為 SG1000 或 SG100 1356
步驟 1：替換 VMware 節點 1356
步驟 2：完成節點恢復 1361

使用服務應用裝置來更換故障節點 1361
使用服務應用裝置更換故障的 StorageGRID 節點 1361
安裝 StorageGRID 服務應用裝置（僅限平台變更） 1361
準備 StorageGRID 設備以進行重新安裝 （僅限平台更換） 1362
在服務設備上啟動 StorageGRID 軟體安裝 1362
監控 StorageGRID 服務應用裝置安裝 1365
技術支援如何恢復 StorageGRID 站台 1366
StorageGRID解決方案和資源 1368
如何使用NetApp控制台管理StorageGRID 1369
法律聲明 1370
版權 1370
商標 1370
專利 1370
隱私權政策 1370
API許可證 1370
開放原始碼 1370

StorageGRID 12.1 軟體文件

了解 StorageGRID 設備硬體

前往 "StorageGRID 應用裝置文件"了解如何安裝、設定和維護 StorageGRID 儲存設備和服務設備。

版本資訊

StorageGRID 12.1 的新功能

StorageGRID 12.1 引進了以下功能與功能變更。

有關 StorageGRID 12.1 最新版本中已修復問題和已知問題的詳細資訊，請參閱 "StorageGRID 12.1 版本說明"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。

容量

EC 重新平衡現在使用可用空間

EC 重新平衡現在使用可用空間而不是已使用空間。請參閱"了解StorageGRID中擴充後的 EC 重新平衡"。

中繼資料允許空間

現在您可以將允許的最大中繼資料值從 3.96 TB 增加到 7.92 TB。請參閱"允許的中繼資料空間"。

控制存取

使用 **OIDC** 的 **SSO**

現在可以了"使用 OpenID Connect (OIDC) 在 StorageGRID 中設定單一登入 （SSO）"。

聯邦

全域命名空間

現在您可以設定全域命名空間，以允許租戶存取跨多個 StorageGRID 系統的儲存桶。請參閱"了解全域命名空間"。

可管理性

自動移動 **ADC** 服務

"當需要滿足 ADC 法定人數要求時"，當您"將儲存節點轉換為僅資料節點"或"停用儲存節點"時，ADC 服務現在將自動遷移。

主管理節點恢復

現在您可以從非主管理節點恢復任何節點。請參閱"從主要管理節點故障中恢復"。

S3

對現有儲存桶啟用 **S3** 物件鎖定

啟用「允許對現有儲存桶啟用 S3 物件鎖定」設定後，S3 租戶帳戶即可對現有儲存桶啟用 S3 物件鎖定。S3 租

戶帳戶啟用現有儲存桶的 S3 物件鎖定後，將無法停用此功能。

允許對啟用了 **S3** 物件鎖定的儲存桶進行複寫

現在您可以使用 CloudMirror 在啟用 S3 物件鎖定的儲存桶中複寫物件。請參閱 "了解平台服務"。

為非空白儲存桶啟用跨網格複寫

現在您可以為非空白儲存桶啟用跨網格複寫。請參閱"跨網格複寫的需求"。

S3 批量操作（僅限 **FPVR**）

您可以使用 S3 批次操作，複寫已啟用版本控制的儲存桶中的現有物件，並計劃將該儲存桶設定為跨網格複寫。

此功能需要 FPVR 核准才能用於 StorageGRID 12.1。若要使用此功能，請聯絡您的客戶代表。

無法正常運作的 **S3 REST API** 標頭

`If-Match`和 `If-None-Match`標頭已被接受，但對於 S3 REST API xref:{relative_path}../s3/put-object.html["PuttObject"]、link:../s3/complete-multipart-upload.html["完成多個部分上傳"]、link:../s3/put-object-copy.html["CopyObject"]和link:../s3/operations-on-objects.html["刪除物件"]而言不具功能性。

如需更多資訊，請參閱"StorageGRID S3 REST API 支援變更"。

支援預先計算的 **Checksum** 值

S3 REST SPI 現在支援預先計算的 Checksum 值和 `x-amz-checksum-type`請求標頭。請參閱"REST API 支援更新"。

安全性

多重管理員驗證

多重管理員驗證 (MAV) 有助於防止對 StorageGRID 系統進行意外或未經授權的變更。請參閱"了解 StorageGRID 多管理員驗證"。

FIPS 安全性原則更新

FIPS 嚴格原則標準已更新。請參閱"在「管理 TLS 和 SSH 原則」中選擇安全性原則"。

租戶

帳戶同步

帳戶 *Clone* 功能現在是指對特定租戶帳戶資訊進行一次性 Clone。

「帳戶同步」是一項新功能，可讓您在一個或多個網格聯合連線中的 StorageGRID 系統之間自動且持續地複寫

租戶帳戶、租戶群組、租戶用戶和 S3 存取金鑰。請參閱 "了解 StorageGRID 中的帳戶同步"。

Kafka 端點和 mTLS 驗證

Kafka 端點現已支援相互傳輸層安全協定 (mTLS)。請參閱"設定平台服務端點"。

最大儲存桶數

StorageGRID 系統現在為每個 S3 租戶帳戶支援最多 20,000 個儲存桶。

升級

啟用功能所需時間增加

在 StorageGRID 升級至版本 12.1 期間，啟用功能所需的時間從不到五分鐘增加至一小時。請參閱"估算完成 StorageGRID 升級所需的時間"。

使用者介面

BMC 設定頁面

Grid Manager 的「節點」頁面新增了「BMC 設定」索引標籤，用於重設 BMC 密碼和變更 BMC LAN IP 設定。請參閱 "更改應用裝置 BMC 密碼" 和 "更改應用裝置節點 BMC LAN IP 設定"。此外，還新增了 API 端點以支援這些功能。請參閱 "用於變更 BMC 密碼和 LAN IP 設定的新端點"。

電子郵件通知

Grid Manager 現在提供一個通用的電子郵件頁面，用於設定和管理警報、AutoSupport 及多管理員驗證 (MAV) 的電子郵件通知。請參閱"設定郵件伺服器"。

連結成本頁面更新

StorageGRID 12.1 提供了更詳細的連結成本資訊和設定。請參閱"管理連結成本"。

USB 連接埠控制

現在您可以透過 Grid Manager 啟用或停用 USB 連接埠。請參閱"透過 USB 連接埠控制遠端存取"。

StorageGRID 中已移除或已棄用的功能

了解 StorageGRID 12.1.0 中已移除或棄用的功能和特性。升級前，請檢查已移除或棄用的功能是否會影響您的用戶端應用程式或網格組態。

定義

已過時

您*不應該*在新生產環境中使用此功能。現有生產環境可以繼續使用此功能。

生命週期終止

支援此功能的上次出貨版本。在某些情況下、此功能的文件可能會在此階段移除。

已移除

* 不 * 支援此功能的第一個版本。

StorageGRID 功能支援結束

在 N+1 主要版本中、已過時的功能將會移除。例如、如果在版本 N 中某項功能已過時（例如 6.3 ）、則該功能將存在的最後一個版本為 N+1 （例如 6.4 ）。版本 N+1 （例如 6.5 ）是產品中不存在此功能的第一個版本。

如需其他資訊、請參閱 "軟體版本支援頁面"。

在某些情況下、 NetApp 可能會比指定時間更快終止對特定功能的支援。

功能	已過時	生命週期終止	已移除	先前文件的連結
AES-128 加密的全域 SSE 設定	12.1	12.2	12.3	從 StorageGRID 12.1.0 開始，對新儲存物件靜態資料進行 AES-128 加密的支援已過時。對於最初以 AES-128 加密的儲存物件，仍繼續支援其擷取作業。
警報，舊版（非警示）	11.7	11.8	11.9	"警告參考資料（ StorageGRID 11.8 ）"
歸檔節點支援	11.7	11.8	11.9	"汰換歸檔節點的考量（ StorageGRID 11.8 ）" • 注意 * ：開始升級之前、您必須： 1. 停用所有歸檔節點。請參閱 "Grid 節點汰換（ StorageGRID 11.8 doc 網站）"。 2. 從儲存設備集區和 ILM 原則中移除所有歸檔節點參考。請參閱 "NetApp 知識庫： StorageGRID 11.9 軟體升級解決方案指南"。
透過 CIFS/Samba 進行稽核匯出	11.1	11.6	11.7	
CLB 服務	11.4.11.4	11.6	11.7	
Docker Container Engine	11.8	11.9	待定	不再支援將 Docker 作為純軟體部署的容器引擎。 Docker 將在未來的版本中被另一個容器引擎取代。請參閱"基於軟體的節點的軟體要求"了解目前支援的 Docker 版本清單。

功能	已過時	生命週期終止	已移除	先前文件的連結
電子郵件設定（舊版）	11.9	12.0	12.1	"設定警報通知（舊系統）（StorageGRID 11.8）"
NFS 稽核匯出	11.8	11.9	12.0	"設定 NFS 的稽核用戶端存取（ StorageGRID 11.8 ）"
連接埠重映射	12.0	12.1	12.2	
Swift API 支援	11.7	11.9	12.0	"使用 Swift REST API （ StorageGRID 11.8 ）"
RHEL 8.8	11.9	11.9	12.0	
RHEL 9.0	11.9	11.9	12.0	
RHEL 9.2	11.9	11.9	12.0	
Ubuntu 18.04	11.9	11.9	12.0	
Ubuntu 20.04	11.9	11.9	12.0	
DEBIAN11	11.9	11.9	12.0	

另請參閱：

- "網格管理API的變更"
- "租戶管理API變更"

StorageGRID 中 Grid Management API 的變更

StorageGRID 12.1 使用 Grid Management API 的第 4 版。第 4 版已棄用第 3 版；但是，第 1 版、第 2 版和第 3 版仍受支援。

> 您可以繼續使用已棄用的 StorageGRID 管理 API 版本；但是，StorageGRID 的未來版本將不再支援這些 API 版本。升級至 StorageGRID 12.0 或更新版本後，您可以使用 `PUT /grid/config/management` API 停用已棄用的 API。

若要深入瞭解"使用Grid Management API"、請前往。

用於變更 BMC 密碼和 LAN IP 設定的新端點

已新增以下端點，以便您可以"更改應用裝置 BMC 密碼"。

`PUT /bmc-configuration/root-password`

已新增以下端點，以便您可以"更改或檢視 BMC LAN IP 設定"。

`PUT /grid/bmc/{node-id}/lan-ip-config`

`GET /grid/bmc/{node-id}/lan-ip-config`

StorageGRID 中租戶管理 API 的變更

StorageGRID 12.1 使用租戶管理 API 的第 4 版。第 4 版已棄用第 3 版；但是，第 1 版、第 2 版和第 3 版仍受支援。

> 您可以繼續在 StorageGRID 中使用已棄用的租戶管理 API 版本；但是，StorageGRID 的未來版本將不再支援這些 API 版本。升級至 StorageGRID 12.0 或更新版本後，您可以使用 `PUT /grid/config/management` API 停用已棄用的 API。

若要深入瞭解"瞭解租戶管理API"、請前往。

用於物件複製的新 API

您可以使用 `/org/cross-grid-replication/{versionId}/replicate`用於在新配置了跨網格複製的現有儲存桶上手動複製物件的 API。

StorageGRID S3 REST API 支援變更

StorageGRID 所使用的 S3 REST API 會定期更新。

版本	註解
12.1.0	• `If-Match` The `If-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。 • `If-None-Match` The `If-None-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-None-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。 • 為以下請求和支援的標頭新增了對預先計算 Checksum 值的支援： ◦ CompleteMultipartUpload： `x-amz-checksum-crc32`， `x-amz-checksum-crc32c`，和 `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload： `CRC32`， `CRC32C`，以及 `CRC64NVME`，適用於 `x-amz-checksum-algorithm` ◦ CopyObject： `CRC32`， `CRC32C`， `CRC64NVME`，以及 `SHA256`（適用於 `x-amz-checksum-algorithm`） ◦ PutObject： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ UploadPart： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` • 新增了對 `x-amz-checksum-type` 的支援，適用於 CreateMultipartUpload 和 CompleteMultipartUpload。 • 增加了對 `s3:x-amz-copy-source`原則條件索引鍵的支援。 • 允許在現有儲存桶上啟用 S3 物件鎖定。
12.0	• 增加了對管理介面的跨域資源共用 (CORS) 支持，允許另一個網域使用管理 API 存取StorageGRID中的資料。"深入瞭解" 。 • 新增對 STS AssumeRole 和工作階段原則的支援。請參閱 "會話策略範例"。您可以在租戶群組下設定 AssumeRole。

版本	註解
11.9	• 新增下列要求和支援標頭的預先計算 SHA-256 檢查值支援。您可以使用此功能來驗證上傳物件的完整性： ◦ CompleteMultpartUpload ： `x-amz-checksum-sha256` ◦ CreateMultpartUpload ： `x-amz-checksum-algorithm` ◦ GetObject ： `x-amz-checksum-mode` ◦ 標題物件： `x-amz-checksum-mode` ◦ 清單零件 ◦ PutObject ： `x-amz-checksum-sha256` ◦ 上傳部分： `x-amz-checksum-sha256` • 新增網格管理員控制租戶層級保留和法規遵循設定的功能。這些設定會影響 S3 物件鎖定設定。 ◦ 貯體預設保留模式和物件保留模式：監管或法規遵循（如果網格管理員允許）。 ◦ 貯體預設保留期間和物件保留截止日期：必須小於或等於網格管理員所設定的保留期間上限所允許的值。 • 改善內容編碼與串流 `x-amz-content-sha256`值的支援 `aws-chunked`。限制： ◦ 如果存在、 `chunk-signature`則為選用且未驗證 ◦ 如果存在、 `x-amz-trailer`內容會被忽略
11.8	更新 S3 作業的名稱，以符合中使用的名稱 "Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"。
11.7	• 已新增"快速參考：支援的 S3 API 要求"。 • 新增對使用 S3 物件鎖定的治理模式的支援。 • 新增「取得物件」和「標頭物件」要求的 StorageGRID 特定回應標頭支援 `x-ntap-sg-cgr-replication-status`。此標頭提供物件的跨網格複寫狀態。 • SelectObjectContent 要求現在支援 Parquet 物件。
11.6	• 新增支援、可在「取得物件」和「標題物件要求」中使用 `partNumber`要求參數。 • 新增S3物件鎖定的預設保留模式支援、以及儲存區層級的預設保留期間。 • 新增對原則條件金鑰的支援 `s3:object-lock-remaining-retention-days`、可設定物件的允許保留期間範圍。 • 將單一「放置物件」作業的最大大小 _ 建議 _ 變更為 5 GiB （ 5 、 368,709,120 位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

版本	註解
11.5	• 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • `Content-MD5`現在已正確支援要求標頭。
11.4.11.4	• 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 新增對活動類型的儲存庫通知的支援 `s3:ObjectRestore:Post`。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增 TLS 1.3 支援
11.3	• 新增支援使用客戶提供的金鑰（SSE-C）進行物件資料的伺服器端加密。 • 新增刪除、取得及放置 Bucket 生命週期作業（僅限到期動作）及回應標頭的支援 `x-amz-expiration`。 • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 不再支援TLS 1.1密碼。
11.2	新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。 *附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID （包括用於自訂的版本功能）並未變更。
11.1	新增支援跨來源資源共享（ CORS ）、 HTTP for S3 用戶端連線至網格節點、以及儲存區的法規遵循設定。
11.0	新增支援、可設定適用於儲存區的平台服務（CloudMirror複寫、通知及Elasticsearch整合）。此外、也新增對貯體物件標記位置限制的支援、以及可用的一致性。
10.4	新增對ILM掃描版本設定、端點網域名稱頁面更新、原則、原則範例及PuttoverwriteObject權限中的條件和變數的支援。
10.3	新增版本管理支援。
10.2	新增對群組和庫位存取原則的支援、以及多部份複本（上傳零件-複本）的支援。

版本	註解
10.1	新增對多部分上傳、虛擬主機式請求和 v4 驗證的支援。
10.0	StorageGRID系統初步支援 S3 REST API。 _簡單儲存服務 API 參考_目前支援的版本是 2006-03-01。

請參閱 "S3 REST API 支援的版本與更新" 以取得更多資訊。

開始使用 StorageGRID 系統

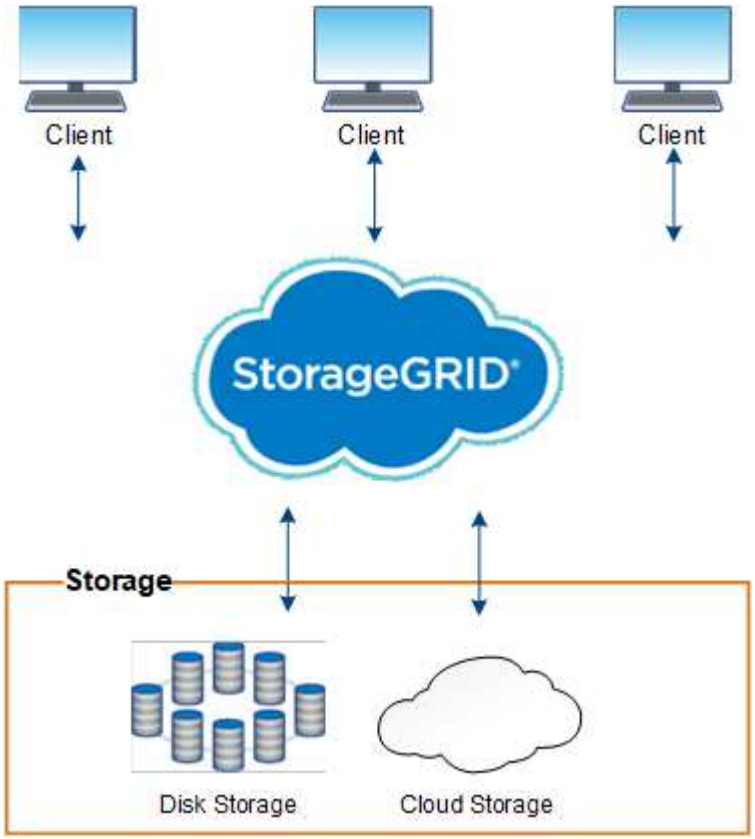
深入瞭解StorageGRID

什麼是StorageGRID 功能？

NetApp ® StorageGRID ® 是一套軟體定義的物件儲存套件、可在公有雲、私有雲和混合式多雲端環境中支援各種使用案例。StorageGRID 提供 Amazon S3 API 的原生支援、並提供領先業界的創新技術、例如自動化生命週期管理、可長期以符合成本效益的方式儲存、保護、保護及保留非結構化資料。

提供安全、持久的大規模儲存非結構化資料。StorageGRID以中繼資料為導向的整合式生命週期管理原則、可在資料生命週期中最佳化資料的存放位置。內容會放置在適當的位置、適當的時間、以及適當的儲存層、以降低成本。

由分散各地、備援的異質節點所組成、可與現有和新一代用戶端應用程式整合。StorageGRID



已移除對歸檔節點的支援。透過 S3 API 將物件從歸檔節點移至外部歸檔儲存系統"ILM 雲端儲存資源池"、已由取代、提供更多功能。

StorageGRID 的優點

這個系統的優點StorageGRID 包括：

- 可大幅擴充且易於使用的地理分散式資料儲存庫、適用於非結構化資料。
- Amazon Web Services 簡單儲存服務 (S3) 標準物件儲存協定。
- 混合雲已啟用。原則型資訊生命週期管理（ILM）會將物件儲存至公有雲、包括Amazon Web Services（AWS）和Microsoft Azure。透過支援內容複寫、事件通知及中繼資料搜尋儲存至公有雲的物件。StorageGRID
- 靈活的資料保護功能、確保持久性與可用度。您可以使用複寫和分層銷毀編碼來保護資料。閒置和飛行中資料驗證可確保完整性、以利長期保留。
- 動態資料生命週期管理、有助於管理儲存成本。您可以建立 ILM 規則、在物件層級管理資料生命週期、自訂資料位置、耐用性、效能、成本、 和保留時間。
- 高可用度的資料儲存設備和部分管理功能、搭配整合式負載平衡功能、以最佳化StorageGRID 整個VMware資源的資料負載。
- 支援多個儲存租戶帳戶、可將儲存在系統上的物件依不同實體分隔。
- 監控StorageGRID 您的整套系統健全狀況的眾多工具、包括全方位警示系統、圖形儀表板、以及所有節點和站台的詳細狀態。
- 支援基於軟體或硬體的部署。您可以將 StorageGRID 部署在以下任何平台上：
  - 在VMware中執行的虛擬機器。
  - Linux主機上的Container引擎。
  - StorageGRID工程設備。
    - 儲存設備提供物件儲存。
    - 服務設備提供網格管理和負載平衡服務。
- 符合下列法規的相關儲存需求：
  - 17 CFR中的證券交易委員會（SEC）第240.17A-4（f）條規範交易所會員、經紀商或交易商。
  - 金融業監管局（FINRA）第4511（c）條、遵守SEC第17A-4（f）條的格式和媒體要求。
  - 《商品期貨交易委員會（CFTC）規範商品期貨交易的條例》第17 CFR第1.31（c）至（d）條。
- 不中斷的升級與維護作業。在升級、擴充、取消委任及維護程序期間、維持對內容的存取。
- 聯合身分管理。與 Active Directory、OpenLDAP 或 Oracle Directory Service 整合，用於使用者身分驗證。支援使用安全性斷言標記語言 2.0 （SAML 2.0） 或 OpenID Connect （OIDC） 的單一登入 （SSO），以在 StorageGRID 和外部身分供應商（例如 Active Directory Federation Services （AD FS））之間交換驗證和授權資料。

混合雲**StorageGRID** 與功能

在混合雲組態中使用 StorageGRID 、方法是實作原則導向的資料管理、將物件儲存在雲端儲存池中、運用 StorageGRID 平台服務、並使用 NetApp FabricPool 將資料從 ONTAP 分層到 StorageGRID 。

雲端儲存資源池

雲端儲存池允許您將物件儲存在 StorageGRID 系統之外。例如，您可能想要將不常存取的物件移至成本較低的雲端儲存，例如 Amazon S3 Glacier、S3 Glacier Deep Archive、Google Cloud 或 Microsoft Azure Blob Storage 中的封存存取層。或者，您可能想要維護 StorageGRID 物件的雲端備份，以便在儲存設備 Volume 或儲存節點故障時恢復遺失的資料。

也支援協力廠商合作夥伴儲存設備、包括磁碟與磁帶儲存設備。

> 由於從雲端儲存資源池目標擷取物件的延遲增加、因此不支援使用FabricPool 含有支援功能的雲端儲存資源池。

S3平台服務

S3平台服務可讓您使用遠端服務做為物件複寫、事件通知或搜尋整合的端點。平台服務獨立運作於網格的ILM規則、並可針對個別S3儲存區啟用。支援下列服務：

- CloudMirror複寫服務會自動將指定的物件鏡射至目標S3儲存區、該儲存區可位於Amazon S3或第二StorageGRID 個支援系統上。
- 事件通知服務將指定操作的訊息傳送至支援接收簡單通知服務 (Amazon SNS) 事件的外部端點。
- 搜尋整合服務將物件中繼資料傳送到外部 Elasticsearch 服務，從而可以使用第三方工具搜尋、視覺化和分析中繼資料。

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。

使用 **FabricPool** 進行 **ONTAP** 資料分層

您可以ONTAP 使用StorageGRID 效益技術將資料分層至資料以降低資料的儲存成本FabricPool 。FabricPool 可將資料自動分層至低成本的物件儲存層、無論是內部部署或外部部署。

與手動分層解決方案不同， FabricPool透過自動化資料分層來降低儲存成本，從而降低整體擁有成本。它透過分層到公有雲和私有雲（包括StorageGRID）來提供雲端經濟的優勢。

相關資訊

- "什麼是雲端儲存池？"
- "管理平台服務"
- "設定StorageGRID 適用於FabricPool 靜態的"

架構與網路拓撲**StorageGRID**

這個系統包含多種類型的網格節點、位於一或多個資料中心站台。StorageGRID

了解"網格節點類型"。

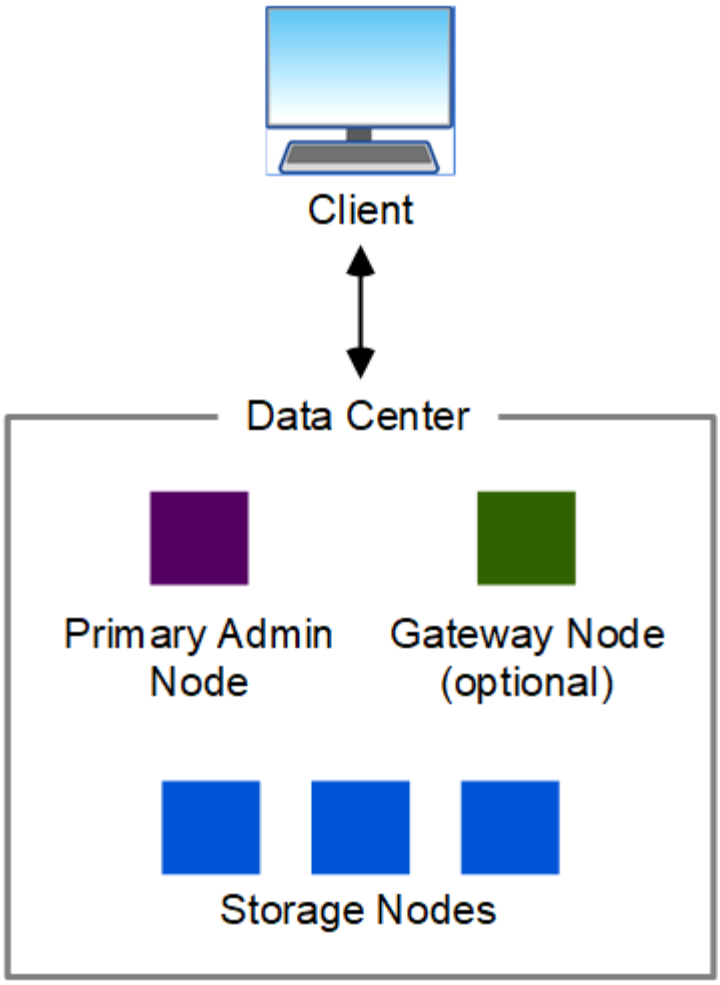
有關 StorageGRID 網路拓撲、需求和網格通訊的詳細資訊，請參閱 "網路準則"。

部署拓撲

StorageGRID系統可以部署到單一資料中心站點或多個資料中心站點。每個部署的最大站點數為 16 個。

單一站台

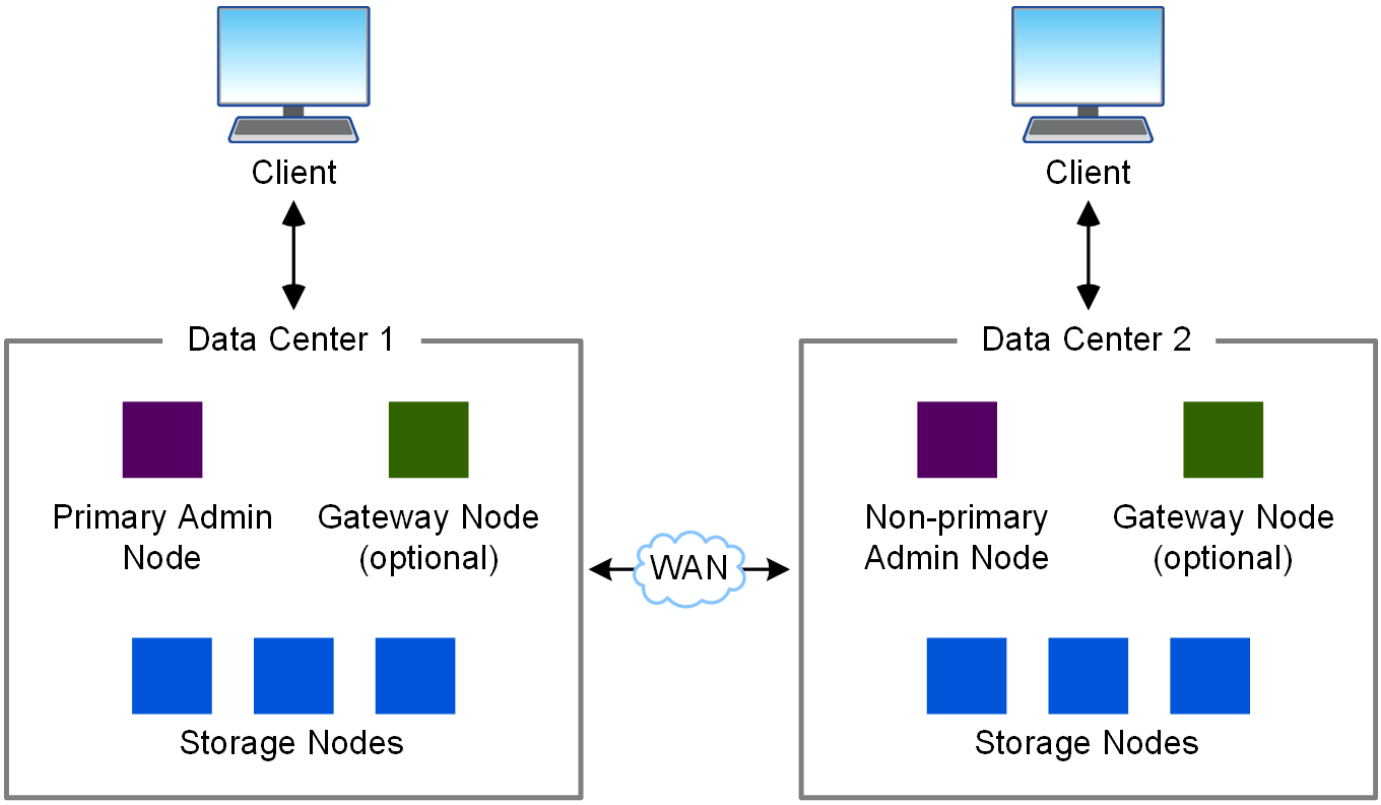
在部署單一站台的StorageGRID 情況下、將會集中化整個過程中的基礎架構和運作。



多個站台

在部署多個站台的情況下、StorageGRID 每個站台都能安裝不同類型和數量的支援資源。例如、一個資料中心可能需要比另一個資料中心更多的儲存設備。

站點通常位於不同故障域的地理位置，例如地震斷層線或洪氾區。透過將資料自動分發到其他站點，實現資料共享和災難復原。



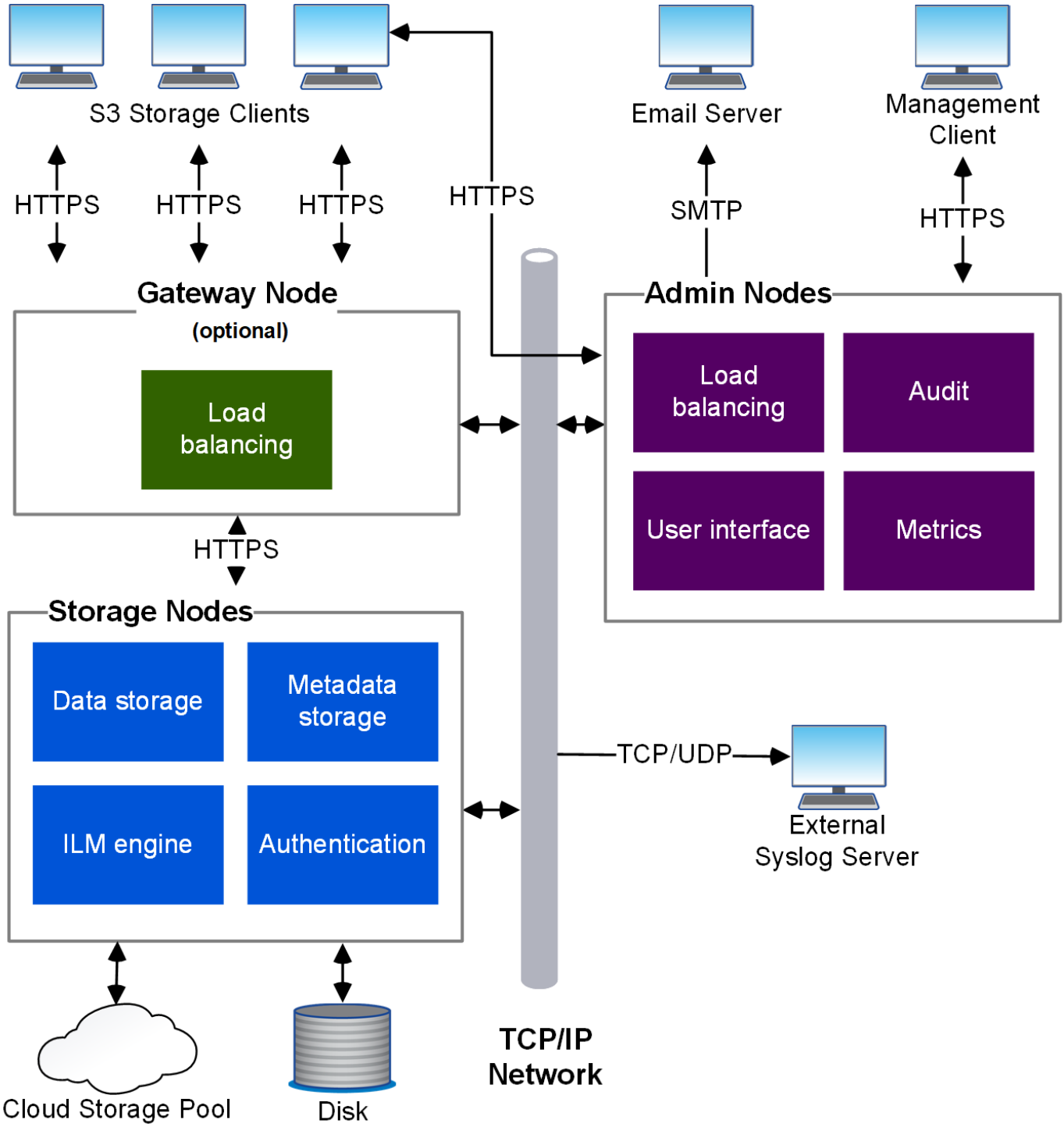
單一資料中心內還可以存在多個邏輯站點，以允許使用分散式複製和擦除編碼來提高可用性和彈性。

網格節點備援

在單一站台或多站台部署中、您可以選擇性地包含多個管理節點或閘道節點來提供備援。例如、您可以在單一站台或多個站台上安裝多個管理節點。不過StorageGRID 、每個功能完善的系統只能有一個主要管理節點。

系統架構

下圖顯示StorageGRID 如何在一個E不到 位的系統中排列網格節點。



S3 用戶端用於在 StorageGRID 中儲存和擷取物件。其他用戶端用於存取 StorageGRID 管理介面，並可選擇存取稽核共享。此外，StorageGRID 還可以選擇透過外部 SMTP 伺服器傳送電子郵件警報。

S3 用戶端可以連線至閘道節點或管理節點、以使用負載平衡介面來連接儲存節點。或者、 S3 用戶端也可以使用 HTTPS 直接連線至儲存節點。

物件可以儲存在 StorageGRID 的軟體或硬體型儲存節點上，也可以儲存在雲端儲存集區中，雲端儲存集區由外部 S3 儲存貯體或 Azure Blob Storage Container 組成。

網格節點和服務

StorageGRID 網格節點與服務

整個系統的基本建置區塊StorageGRID 是網格節點。節點包含服務、這些是軟體模組、可為網格節點提供一組功能。

網格節點類型

StorageGRID系統使用三種類型的網格節點：

管理節點

提供系統組態、監控和記錄等管理服務。登入 Grid Manager 後，您將連線到一個管理節點。每個網格必須有一個主要管理節點，並且可能還有其他非主要管理節點以實現備援。您可以連接到任何管理節點，每個管理節點顯示的 StorageGRID 系統檢視都類似。但是，您必須使用主要管理節點執行大多數維護程序。

管理節點也可用於平衡 S3 用戶端流量的負載。

請參閱 "什麼是管理節點？"

儲存節點

管理及儲存物件資料和中繼資料。StorageGRID 系統中的每個站台必須至少有三個儲存節點。

在首次安裝新的儲存節點時，您可以指定它僅用於"儲存中繼資料或資料"。

請參閱 "什麼是儲存節點？"

閘道節點（選用）

提供負載平衡介面、讓用戶端應用程式可用來連線至 StorageGRID 。負載平衡器可將用戶端無縫導向至最佳儲存節點、使節點或甚至整個站台的故障透明化。

請參閱 "什麼是閘道節點？"

硬體和軟體節點

StorageGRID節點可以部署為StorageGRID設備節點或基於軟體的節點。每個系統的最大節點數（包括所有節點類型）為 220。

應用裝置節點StorageGRID

用作作業系統的各種硬體應用。StorageGRID StorageGRID有些應用裝置可做為儲存節點。其他應用裝置可做為管理節點或閘道節點。您可以將應用裝置節點與軟體型節點結合、或部署完全工程設計的全應用裝置網格、而這些網格不需依賴外部Hypervisor、儲存設備或運算硬體。

請參閱下列內容、瞭解可用的應用裝置：

- "StorageGRID 應用裝置文件"
- "NetApp Hardware Universe"

軟體型節點

基於軟體的網格節點可以部署為 VMware 虛擬機器或 Linux 主機上的容器引擎內。看"在基於軟體的節點上安裝StorageGRID" 。

使用 "NetApp互通性對照表工具IMT （不含）"確定支援的版本。

支援服務StorageGRID

以下是StorageGRID 完整的支援服務清單。

服務	說明	位置
帳戶服務轉發器	提供介面、讓負載平衡器服務查詢遠端主機上的帳戶服務、並通知負載平衡器端點組態變更負載平衡器服務。	管理節點和閘道節點上的負載平衡器服務
ADC （管理網域控制器）	維護拓撲資訊、提供驗證服務、並回應來自LMR和CMN服務的查詢。	每個站台至少有三個儲存節點包含 ADC 服務
AMS （稽核管理系統）	監控所有已稽核的系統事件和交易、並將其記錄到文字記錄檔中。	管理節點
Avahi 守護程式	處理 mDNS，用於本地網路內的名稱解析和服務發現。	所有節點
快取服務	在負載平衡器（網關）節點上執行並管理物件內容的本機快取。	閘道節點
Cassandra	管理物件元資料的分散式資料庫。	儲存節點（僅限資料）
Cassandra Reaper	自動修復物件中繼資料。	儲存節點
區塊服務	管理銷毀編碼的資料和同位元檢查片段。	儲存節點
CMN （組態管理節點）	管理全系統的組態和網格工作。每個網格都有一項 CMN 服務。	主要管理節點
DDS （分散式資料儲存區）	與Cassandra資料庫介面、以管理物件中繼資料。	儲存節點
DMV （ Data Mover ）	將資料移至雲端端點。	儲存節點
動態 IP （ dynip ）	監控網格、以取得動態IP變更並更新本機組態。	所有節點

服務	說明	位置
gdu-server	用於網格維護和佈建操作的後端工作執行器。接受來自 `mgmt-api`和其他公用程式腳本的請求，驗證這些請求，並將每個行動分派給適當的 GDU 工作處理程序，例如佈建、擴充、退役和升級。	管理節點
Grafana	用於Grid Manager中的度量視覺化。	管理節點
高可用度	管理在「高可用度群組」頁面上設定的節點上的高可用度虛擬 IP。此服務也稱為 *keepalived* 服務。	管理和閘道節點
身分識別（idnt）	管理本機使用者和群組、驗證並聯合來自 LDAP 和 Active Directory 的使用者身分。	使用 ADC 服務的儲存節點
Lambda 仲裁者	管理S3 Select SelectObjectContent要求。	所有節點
負載平衡器（ Nginx)	提供從用戶端到儲存節點的 S3 流量負載平衡。	管理和閘道節點
LDR （本機配送路由器）	管理網格內內容的儲存與傳輸。	儲存節點
mgmt-api	Grid Manager 後端 API。它公開經過驗證的 REST 端點，用於管理網格（組態、監控和維護工作流程），強制執行驗證和權限，並協調長時間執行的作業。它是 Grid Manager 介面和自動化用戶端使用的主要控制平面 API。	管理節點
MISCd 資訊服務控制精靈	提供一個介面、用於查詢及管理其他節點上的服務、以及管理節點上的環境組態、例如查詢其他節點上執行的服務狀態。	所有節點
恩靈思	做為各種網格服務（例如Prometheus和動態IP）的驗證與安全通訊機制、可透過HTTPS API與其他節點上的服務進行對話。	所有節點
nginx-gw 負載平衡器	提供從用戶端到儲存節點的 S3 流量負載平衡。	管理和閘道節點
NMS （網路管理系統）	為透過Grid Manager顯示的監控、報告和組態選項提供電源。	管理節點
節點導出器（Prometheus 資料收集）	發布 Prometheus 時間序列指標收集的系統級統計資料。	所有節點

服務	說明	位置
NTP	網路時間協定 (NTP) 服務。	所有節點
持續性	管理根磁碟上需要在重新開機後持續存在的檔案。	所有節點
Prometheus	從所有節點上的服務收集時間序列指標。	管理節點
RSM （複寫狀態機器）	確保平台服務要求會傳送至各自的端點。	使用 ADC 服務的儲存節點
SSM （伺服器狀態監控器）	監控硬體狀況、並向NMS服務報告。	每個網格節點上都有一個執行個體
伺服器管理員	管理StorageGRID服務。	所有節點
SNMP代理	回應 SNMP 請求。	管理節點
SNMP連接埠管理服務	處理 SNMP 連接埠的動態管理。	所有節點
SSH（安全外殼）	處理安全存取和遠端系統管理。	所有節點
SSM（系統狀態監視器）	監控硬體狀況、並向NMS服務報告。	所有節點
統計	記錄與 S3 儲存桶相關的其他指標。	儲存節點
追蹤代理（jaeger-agent）	接收並處理追蹤收集器（jaeger-collector）提交的追蹤資訊。	所有節點
追蹤收集器（jaeger-collector）	執行追蹤收集、以收集資訊供技術支援人員使用。追蹤收集器服務使用開放原始碼 Jaeger 軟體。	管理節點

什麼是 **StorageGRID** 管理節點？

管理節點提供系統組態、監控及記錄等管理服務。管理節點也可用於平衡 S3 用戶端流量的負載。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。

主要和非主要管理節點之間的差異

當您登入網格管理器或租戶管理器時，您正在連線到管理節點。您可以連接到任何管理節點，每個管理節點都會顯示StorageGRID系統的類似視圖。但是，主管理節點比非主管理節點提供更多功能。例如，大多數維護程序必須從主管理節點執行。

下表摘要說明主要和非主要管理節點的功能。

功能	主要管理節點	非主要管理節點
包括AMS服務	是的	是的
包括CMN服務	是的	否
包括NMS服務	是的	是的
包括Prometheus服務	是的	是的
包括超棒服務	是的	是的
包括負載平衡器和高可用度服務	是的	是的
支援管理應用程式介面（ mgmt-API ）	是的	是的
可用於所有網路相關的維護工作、例如 IP 位址變更和更新 NTP 伺服器	是的	否
可以下載恢復包	是的	是的
可在儲存節點擴充後執行 EC 重新平衡	是的	否
可用於磁碟區還原程序	是的	是的
可從一或多個節點收集記錄檔和系統資料	是的	是的
可以恢復儲存、網關和非主管理節點	是的	是的
可以恢復主管理節點	是的	是的
傳送警示通知、 AutoSupport 套件和 SNMP 設陷並通知	是的。用作偏好的寄件者。	是的。做為待命傳送者。

偏好的寄件者管理節點

如果您的 StorageGRID 部署包含多個管理節點、則主要管理節點是警示通知、 AutoSupport 套件和 SNMP 設陷及通知的慣用寄件者。

在正常系統操作下，只有首選發送者發送通知。但是，所有其他管理節點都會監控首選發送者。如果偵測到問題，其他管理節點將充當備用發送者。

在以下情況下可能會發送多條通知：

- 如果管理節點彼此「中斷」、偏好的寄件者和待命寄件者都會嘗試傳送通知、而且可能會收到多份通知複本。

- 如果備用發送器偵測到首選發送器出現問題並開始發送通知，則首選發送器可能會重新獲得發送通知的能力。如果發生這種情況，可能會發送重複的通知。當備用發送器不再偵測到首選發送器上的錯誤時，它將停止發送通知。

> 測試 AutoSupport 套件時、所有管理節點都會傳送測試。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。

管理節點的主要服務

下表顯示管理節點的主要服務、但此表並未列出所有節點服務。

服務	按鍵功能
稽核管理系統（ AMS ）	追蹤系統活動和事件。
組態管理節點（ CMN ）	管理全系統組態。
高可用度	管理管理節點和閘道節點群組的高可用度虛擬IP位址。 *附註：*此服務也可在閘道節點上找到。
負載平衡器	提供從用戶端到儲存節點的 S3 流量負載平衡。 *附註：*此服務也可在閘道節點上找到。
[mgmt-API] 管理應用程式介面（ mgmt-API ）	處理來自Grid Management API和租戶管理API的要求。
網路管理系統（ NMS ）	提供Grid Manager的功能。
Prometheus	從所有節點上的服務收集和儲存時間序列度量。
伺服器狀態監視器（ SSM ）	監控作業系統和基礎硬體。

什麼是 **StorageGRID** 儲存節點？

儲存節點可管理及儲存物件資料和中繼資料。儲存節點包括在磁碟上儲存、移動、驗證及擷取物件資料和中繼資料所需的服務和程序。

StorageGRID 系統中的每個站台必須至少有三個儲存節點。

儲存節點類型

在安裝期間、您可以選取要安裝的儲存節點類型。這些類型適用於軟體型儲存節點、以及支援此功能的應用裝置型儲存節點：

- 結合資料與中繼資料儲存節點

- 純中繼資料儲存節點
- 純資料儲存節點

在下列情況下、您可以選取「儲存節點」類型：

- 初次安裝儲存節點時
- 在 StorageGRID 系統擴充期間新增儲存節點時

資料與中繼資料儲存節點（組合）

預設情況下，所有新建的儲存節點都會同時儲存物件資料和中繼資料。這種類型的儲存節點稱為_組合_儲存節點。

純中繼資料儲存節點

如果您的網格儲存了大量的小物件、則只使用儲存節點來儲存中繼資料是很有意義的。安裝專用中繼資料容量可在大量小型物件所需的空間與這些物件的中繼資料所需空間之間取得更好的平衡。此外、在高效能應用裝置上託管的純中繼資料儲存節點也能提升效能。

純中繼資料儲存節點有特定的硬體需求：

- 使用 StorageGRID 應用裝置時，您只能在配備十二個 1.9 TB 或十二個 3.8 TB 磁碟機的 SGF6112 應用裝置上設定僅中繼資料節點。
- 使用軟體型節點時，必須確保僅中繼資料節點資源與現有儲存節點的資源相符。例如：
  - 如果現有的 StorageGRID 站台使用 SG6000 或 SG6100 應用裝置，則僅限軟體型中繼資料節點必須符合下列最低需求：
    - 128 GB RAM
    - 8 核心 CPU
    - 8 TB SSD 或與 Cassandra 資料庫相同的儲存設備（ rangedb/0 ）
  - 如果現有的StorageGRID站點使用具有 24 GB RAM、8 核心 CPU 和 3 TB 或 4TB 元資料儲存的虛擬儲存節點，則基於軟體的僅元資料節點應使用類似的資源（24 GB RAM、8 核心 CPU 和 4TB 元資料儲存（rangedb/0））。
- 新增新的StorageGRID站點時，新站點的總元資料容量至少應與現有站點相符。新站點的資源應與現有站點的儲存節點相符。

> 雖然純中繼資料儲存節點包含且可處理 S3 用戶端要求、但 LDR 服務StorageGRID 效能可能不會提高。

純資料儲存節點

如果您的儲存節點具有不同的效能特性、則只使用儲存節點來處理資料可能是有意義的。例如、若要提高效能、您可以使用僅限資料的大容量旋轉磁碟儲存節點、以及僅限中繼資料的高效能儲存節點。

此外，您可以透過從 Cassandra 中刪除低 RAM 節點來獲得更多元資料容量，這會增加每個節點的元資料容量限制。請參閱"管理物件中繼資料儲存" 。

您可以將組合儲存節點轉換為僅資料儲存節點。如果儲存節點包含 ADC 服務，且符合轉換的先決條件，則在轉

換過程中，服務將自動移至同一站台上的另一個儲存節點。如需先決條件和詳細步驟，請參閱 "將儲存節點轉換為僅資料節點"。

每個網格和每個站點所需的儲存節點

在選擇拓撲中使用的儲存節點時，請記住網格或網格中的每個網站必須包含以下內容：

- 每個站點（在單一站點或多站點網格中）：三個類比數位轉換器儲存節點（可以是組合儲存節點和僅元資料儲存節點的任意組合）
- 單站點網格：至少兩個物件儲存節點（可以是任意組合或僅資料）
- 多站點網格：每個站點至少一個物件儲存節點（可以是組合的，也可以是僅資料）

儲存節點的主要服務

下表顯示儲存節點的主要服務、但此表並未列出所有節點服務。

有些服務（例如、ADC服務和RSM服務）通常只存在於每個站台的三個儲存節點上。

服務	按鍵功能
帳戶（帳戶）	管理租戶帳戶。 僅資料儲存節點不提供此服務。

服務	按鍵功能
管理網域控制站 (ADC)	維護拓撲和整個網格的組態。 僅資料儲存節點不提供此服務。 詳細資料 管理網域控制器（ADC）服務會驗證網格節點及其彼此的連線。ADC 服務至少託管在一個站台的三個儲存節點上。 ADC 服務維護拓撲資訊，包括服務的位置和可用度。當一個網格節點需要從另一個網格節點取得資訊或需要另一個網格節點執行行動，它會聯絡 ADC 服務以找到最適合處理其請求的網格節點。此外，ADC 服務還保留 StorageGRID 部署的組態套件組合複本，允許任何網格節點擷取目前組態資訊。 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 ADC 服務無法使用、系統仍能繼續使用已知網格節點運作。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。
Cassandra	儲存及保護物件中繼資料。 僅資料儲存節點不提供此服務。
Cassandra Reaper	自動修復物件中繼資料。 僅資料儲存節點不提供此服務。
區塊	管理銷毀編碼的資料和同位元檢查片段。
資料移轉（DMV）	將資料移至雲端儲存資源池。

服務	按鍵功能
分散式資料儲存區（DDS）	監控物件中繼資料儲存。 詳細資料 每個儲存節點都包含分散式資料儲存區（ DDS ）服務。此服務會與 Cassandra 資料庫進行介面、以對儲存在 StorageGRID 系統中的物件中繼資料執行背景工作。 DDS 服務會追蹤寫入 StorageGRID 系統的物件總數、以及透過每個系統支援介面（ S3 ）擷取的物件總數。
身分識別（idnt）	聯盟LDAP和Active Directory的使用者身分識別。 僅資料儲存節點不提供此服務。

服務	按鍵功能
本機發佈路由器（ LDR ）	處理物件儲存傳輸協定要求、並管理磁碟上的物件資料。 詳細資料 每個 _ 組合 _ 、 _ 僅資料 _ 和 _ 僅中繼資料 _ 儲存節點都包含本機發佈路由器（ LDR ）服務。此服務可處理內容傳輸功能、包括資料儲存、路由和要求處理。LDR 服務可處理資料傳輸負載和資料傳輸功能、以完成 StorageGRID 系統的大部分工作。 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 • S3 傳輸協定介面 LDR 服務也會將每個 S3 物件對應至其唯一 UUID 。 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。 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。物件儲存區填滿容量時、其餘物件儲存區會繼續儲存物件、直到儲存節點上沒有空間為止。 中繼資料保護 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。此複寫無法設定、而且會自動執行。如需詳細資訊、請參閱 "管理物件中繼資料儲存"。

服務	按鍵功能
複寫狀態機器（RSM）	確保 S3 平台服務要求會傳送至各自的端點。 僅資料儲存節點不提供此服務。
伺服器狀態監視器（SSM）	監控作業系統和基礎硬體。

什麼是 **StorageGRID** 閘道節點？

閘道節點提供專用的負載平衡介面、 S3 用戶端應用程式可用來連線至 StorageGRID 。負載平衡可在多個儲存節點之間分配工作負載、以最大化速度和連線容量。閘道節點為選用項目。

StorageGRID 負載平衡器服務會在所有管理節點和所有閘道節點上提供。它會對用戶端要求執行傳輸層安全性（TLS）終止、檢查要求、並建立新的安全連線至儲存節點。負載平衡器服務可無縫地將用戶端導向至最佳儲存節點、讓節點甚至整個站台的故障都能透明化。

您可以設定一或多個負載平衡器端點、以定義傳入和傳出用戶端要求用來存取 Gateway 和管理節點上負載平衡器服務的連接埠和網路傳輸協定（ HTTPS 或 HTTP ）。負載平衡器端點也會定義用戶端類型（ S3 ）、繫結模式、以及選擇性的允許或封鎖租戶清單。請參閱。 "負載平衡考量"

視需要、您可以將多個閘道節點和管理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失敗、備份介面就能管理用戶端應用程式工作負載。請參閱。 "管理高可用度（ HA ）群組"

閘道節點的主要服務

下表顯示閘道節點的主要服務、但此表並未列出所有節點服務。

服務	按鍵功能
快取服務	管理物件內容的本機快取。
高可用度	管理管理節點和閘道節點群組的高可用度虛擬IP位址。 *附註：*此服務也可在管理節點上找到。
負載平衡器	提供從用戶端到儲存節點的 S3 流量第 7 層負載平衡。這是建議的負載平衡機制。 *附註：*此服務也可在管理節點上找到。
伺服器狀態監視器（SSM）	監控作業系統和基礎硬體。

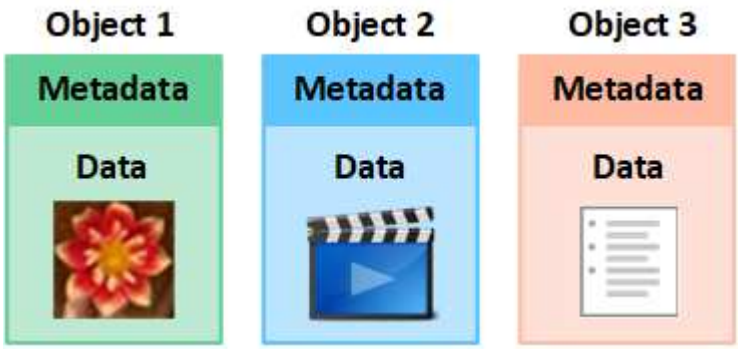
如何管理資料**StorageGRID**

什麼是 **StorageGRID** 物件

使用物件儲存時、儲存單元是物件、而非檔案或區塊。不同於檔案系統或區塊儲存設備的樹狀階層、物件儲存設備會以無結構化的平面配置來組織資料。

物件儲存設備可將資料的實體位置與用來儲存及擷取該資料的方法分離。

物件型儲存系統中的每個物件都有兩個部分：物件資料和物件中繼資料。



什麼是物件資料？

物件資料可能是任何內容、例如照片、影片或醫療記錄。

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

物件中繼資料包含下列資訊：

- 系統中繼資料、包括每個物件的唯一 ID （ UUID ）、物件名稱、 S3 貯體名稱、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。
- 每個物件複本或銷毀編碼片段的目前儲存位置。
- 與物件相關聯的任何使用者中繼資料。

物件中繼資料可自訂且可擴充、使應用程式更靈活地使用。

如需 StorageGRID 儲存物件中繼資料的方式及位置的詳細資訊"管理物件中繼資料儲存"、請前往。

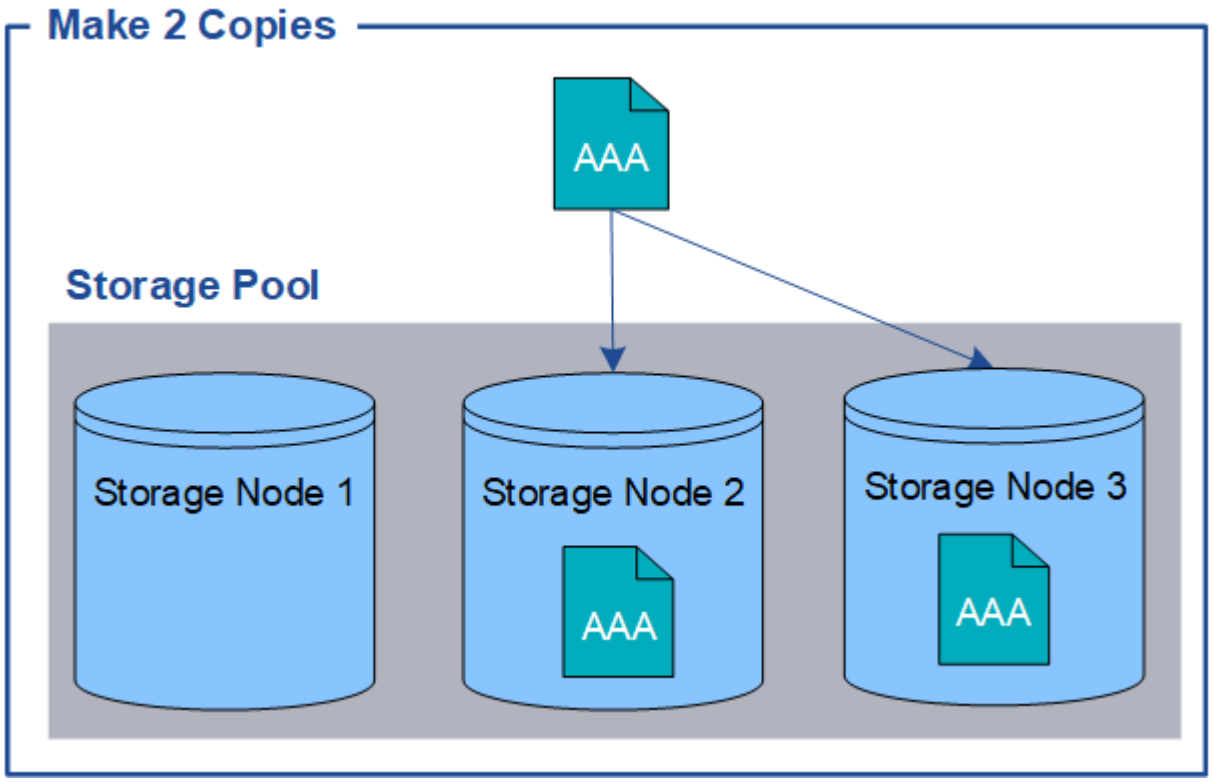
物件資料如何受到保護？

此系統提供兩種機制、可保護物件資料免於遺失：複寫和銷毀編碼。StorageGRID

複寫

當 StorageGRID 將物件與設定為建立複寫複本的資訊生命週期管理（ ILM ）規則配對時、系統會建立物件資料的確切複本、並將其儲存在儲存節點或雲端儲存池中。ILM規則會規定複本的複本數量、複本的儲存位置、以及系統保留多久。如果遺失複本（例如儲存節點遺失）、則物件若存在StorageGRID 於任何物件的副本、仍可在該物件的其他地方使用。

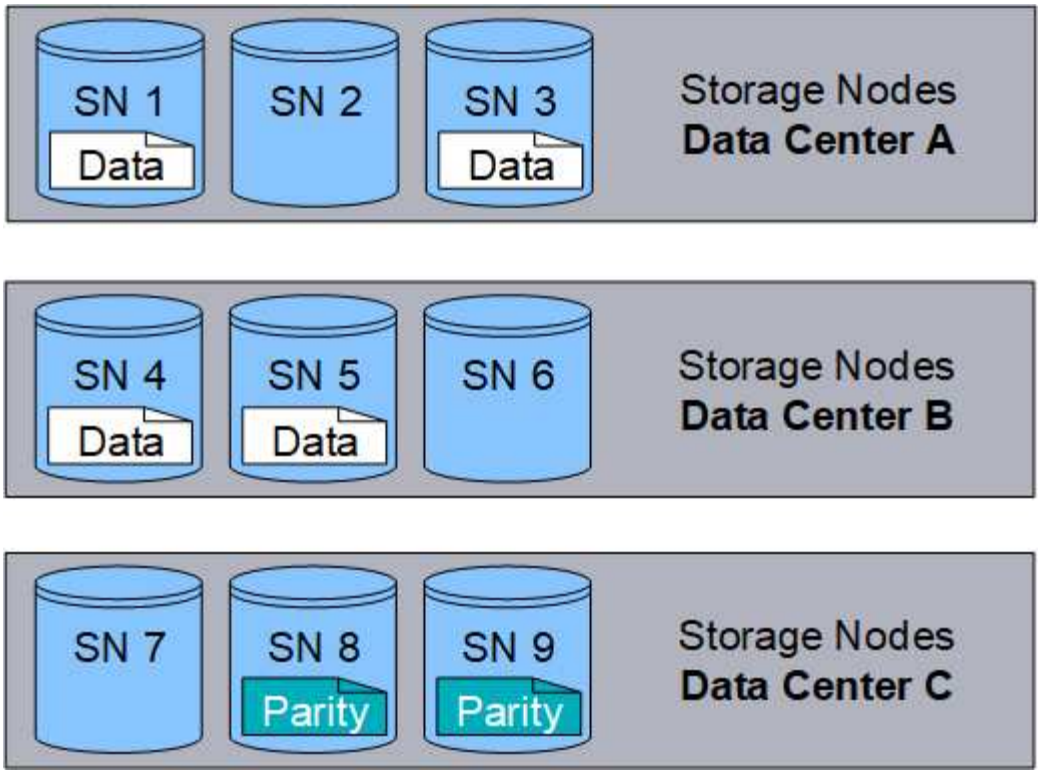
在下列範例中、「製作2份複本」規則會指定將每個物件的兩個複寫複本放在包含三個儲存節點的儲存資源池中。



銷毀編碼

當物件符合設定為建立銷毀編碼複本的ILM規則時、它會將物件資料分成資料片段、計算額外的同位元檢查片段、並將每個片段儲存在不同的儲存節點上。StorageGRID存取物件時、會使用儲存的片段重新組裝物件。如果資料或同位元檢查片段毀損或遺失、則銷毀編碼演算法可利用其餘資料和同位元檢查片段的子集來重新建立該片段。ILM 規則和銷毀編碼設定檔會決定所使用的銷毀編碼配置。

以下範例說明在物件資料上使用銷毀編碼。在此範例中、ILM規則使用4+2銷毀編碼方案。每個物件會分割成四個等量資料片段、並從物件資料計算兩個同位元檢查片段。這六個片段中的每個片段都儲存在三個資料中心的不同儲存節點上、以針對節點故障或站台遺失提供資料保護。



相關資訊

- "使用ILM管理物件"
- "使用資訊生命週期管理"

StorageGRID 中的物件生命週期

物件的生命週期由不同階段組成。每個階段都代表物件所執行的作業。

物件的壽命包括擷取、複本管理、擷取及刪除等作業。

- * 內嵌 * ： S3 用戶端應用程式透過 HTTP 將物件儲存至 StorageGRID 系統的程序。在這個階段StorageGRID 、這個物件的物件由整個系統開始管理。
- * 複製管理 * ：在 StorageGRID 中管理複寫和刪除編碼複本的程序、如使用中 ILM 原則中的 ILM 規則所述。在複本管理階段、 StorageGRID 會在儲存節點或雲端儲存池中建立及維護指定數量和類型的物件複本、以保護物件資料不受遺失。
- 擷取：用戶端應用程式存取StorageGRID 由該系統儲存之物件的程序。用戶端會讀取物件、該物件是從儲存節點或雲端儲存池擷取而來。
- 刪除：從網格中移除所有物件複本的程序。物件可因用戶端應用程式傳送刪除要求至StorageGRID 該系統而刪除、或StorageGRID 是因物件壽命到期時執行的自動程序而刪除。

相關資訊

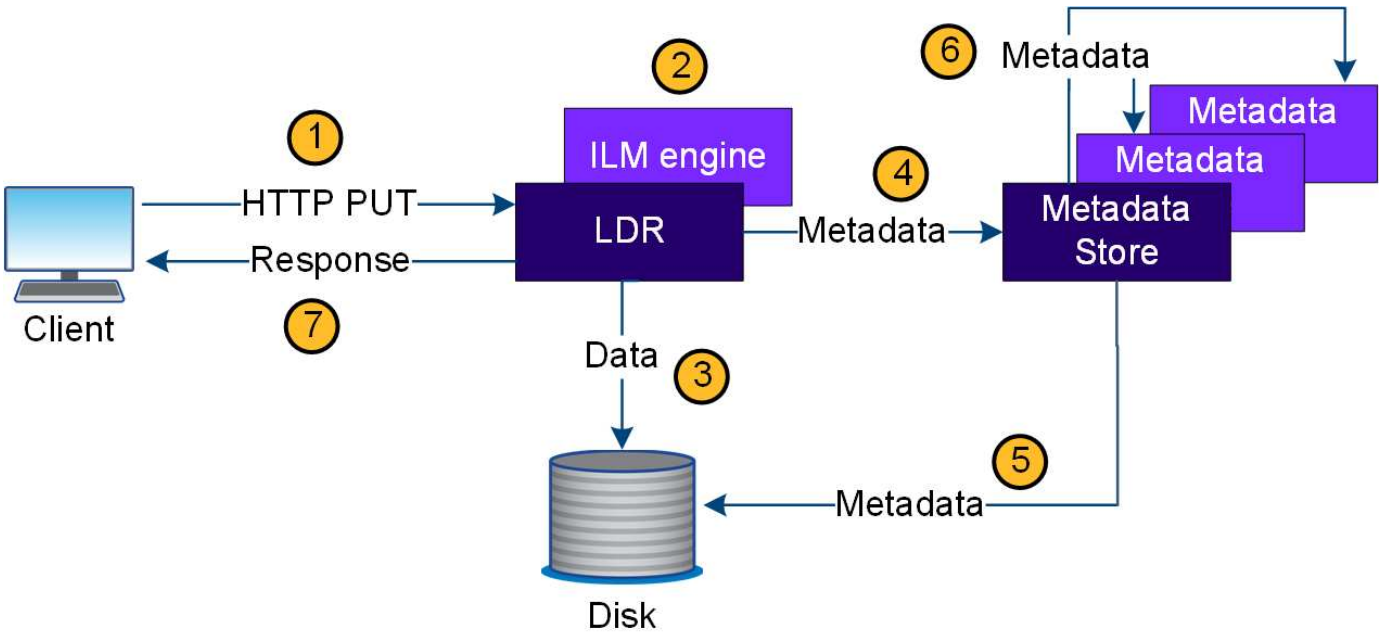
- "使用ILM管理物件"
- "使用資訊生命週期管理"

StorageGRID 如何處理物件擷取

擷取或儲存作業是由用戶端與StorageGRID 該系統之間定義的資料流所組成。

資料流

當用戶端將物件擷取至StorageGRID 物件系統時、儲存節點上的LMR服務會處理要求、並將中繼資料和資料儲存至磁碟。



1. 用戶端應用程式會建立物件、StorageGRID 並透過HTTP PUT要求將物件傳送至該系統。
2. 系統會根據系統的ILM原則來評估物件。
3. LDR 服務會將物件資料儲存為複寫複本、或儲存為銷毀編碼複本。（圖中顯示了將複本儲存到磁碟的簡化版本。）
4. LDR服務會將物件中繼資料傳送至中繼資料儲存區。
5. 中繼資料儲存區會將物件中繼資料儲存至磁碟。
6. 中繼資料儲存區會將物件中繼資料複本傳播至其他儲存節點。這些複本也會儲存至磁碟。
7. LDR服務會傳回HTTP 200 OK回應給用戶端、以確認已擷取物件。

StorageGRID 如何管理物件副本

物件資料是由主動式 ILM 原則和相關的 ILM 規則來管理。ILM 規則會建立複寫或刪除編碼的複本、以保護物件資料不受遺失。

物件複本的類型或位置可能會在物件生命週期的不同時間要求不同。ILM規則會定期評估、以確保物件會根據需

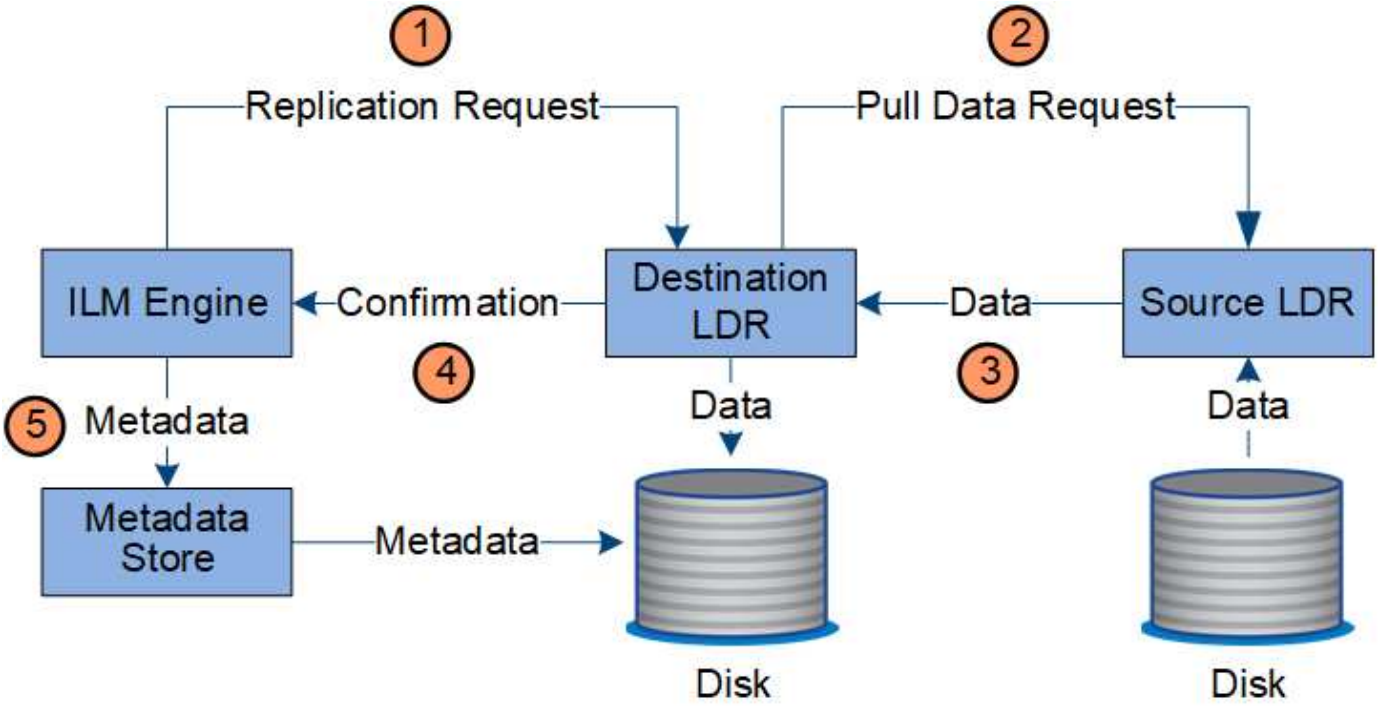
要放置。

物件資料是由LDR服務管理。

內容保護：複寫

如果ILM規則的內容放置指示需要複寫物件資料複本、則複本會由組成設定儲存資源池的儲存節點製作並儲存至磁碟。

LMR服務中的ILM引擎可控制複寫、並確保正確的複本數量儲存在正確的位置、且時間正確。

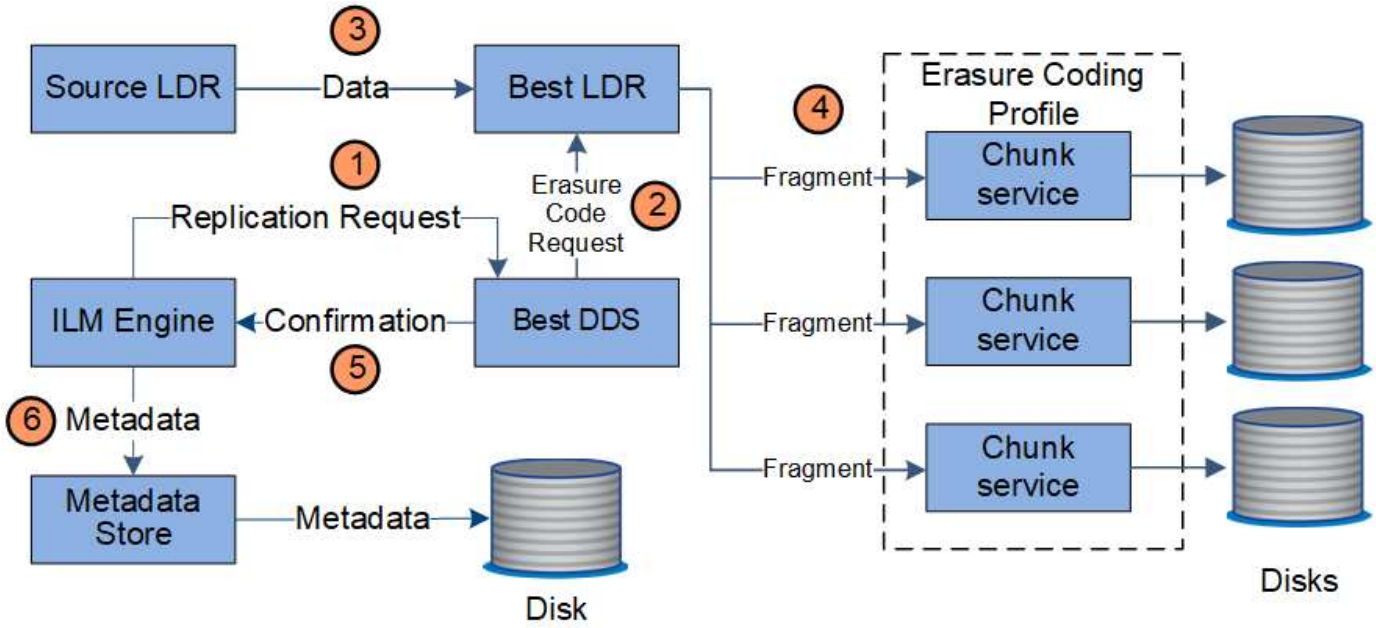


1. ILM引擎會查詢ADC服務、以判斷ILM規則所指定之儲存資源池內的最佳目的地LMR服務。然後、它會傳送命令給該LMR服務、以啟動複寫。
2. 目的地LDR服務會查詢ADC服務、以找出最佳來源位置。然後將複寫要求傳送至來源LdR服務。
3. 來源LMR服務會將複本傳送至目的地LdR服務。
4. 目的地LDR服務會通知ILM引擎物件資料已儲存。
5. ILM引擎會使用物件位置中繼資料來更新中繼資料存放區。

內容保護：銷毀編碼

如果 ILM 規則包含建立物件資料銷毀編碼複本的指示、則適用的銷毀編碼方案會將物件資料中斷至資料和同位元檢查片段、並在銷毀編碼設定檔中設定的儲存節點之間散佈這些片段。

ILM 引擎是 LDR 服務的元件、可控制銷毀編碼、並確保將銷毀編碼設定檔套用至物件資料。

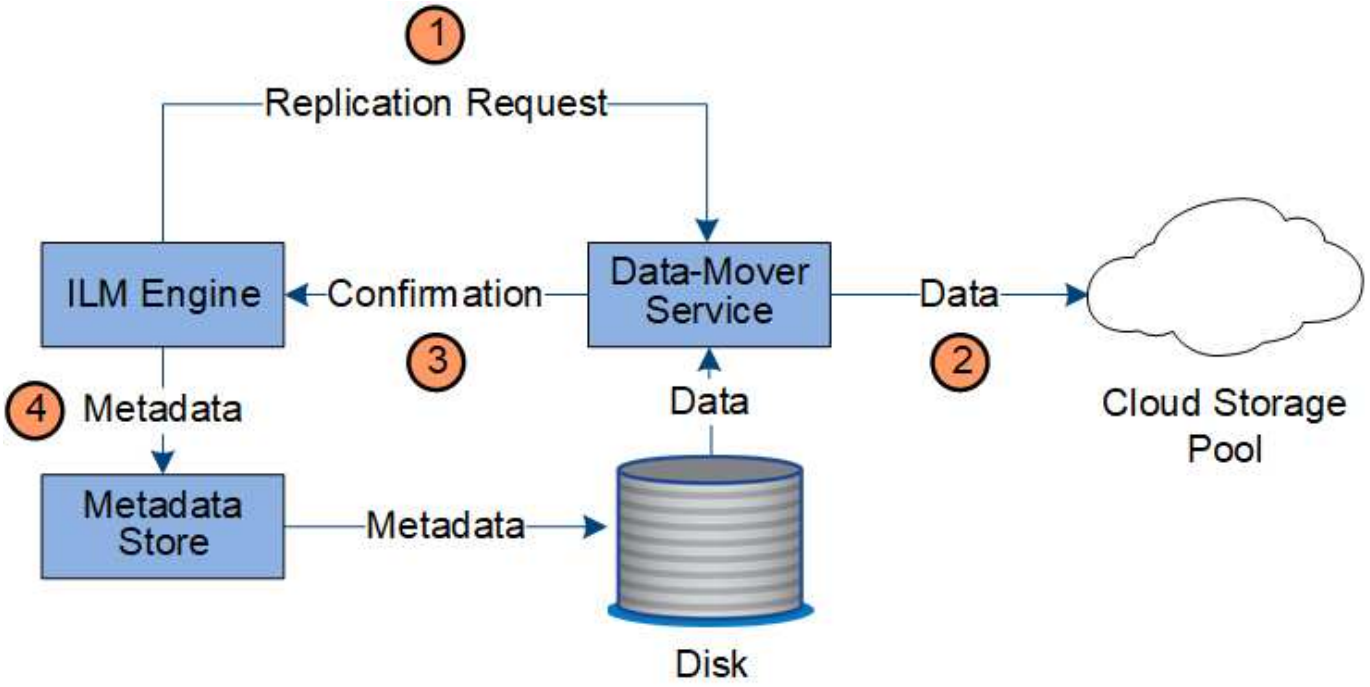


1. ILM引擎會查詢ADC服務、以判斷哪些DDS服務最能執行銷毀編碼作業。確定後、 ILM 引擎會傳送「初始化」要求給該服務。
2. DDS服務會指示LMR銷毀物件資料的程式碼。
3. 來源LDR服務會將複本傳送至選取用於銷毀編碼的LDR服務。
4. 在建立適當數量的同位元檢查和資料片段之後、 LDR 服務會將這些片段散佈到構成抹除編碼設定檔儲存資源池的儲存節點（區塊服務）上。
5. LDR服務會通知ILM引擎、確認物件資料已成功散佈。
6. ILM引擎會使用物件位置中繼資料來更新中繼資料存放區。

內容保護：雲端儲存資源池

如果 ILM 規則的內容放置說明要求將物件資料的複寫複本儲存在雲端儲存池中，物件資料將複製到為雲端儲存池指定的外部 S3 儲存貯體或 Azure Blob Storage Container。

ILM引擎是LDR服務的一項元件、而Data Mover服務則可控制物件移至雲端儲存池的動作。



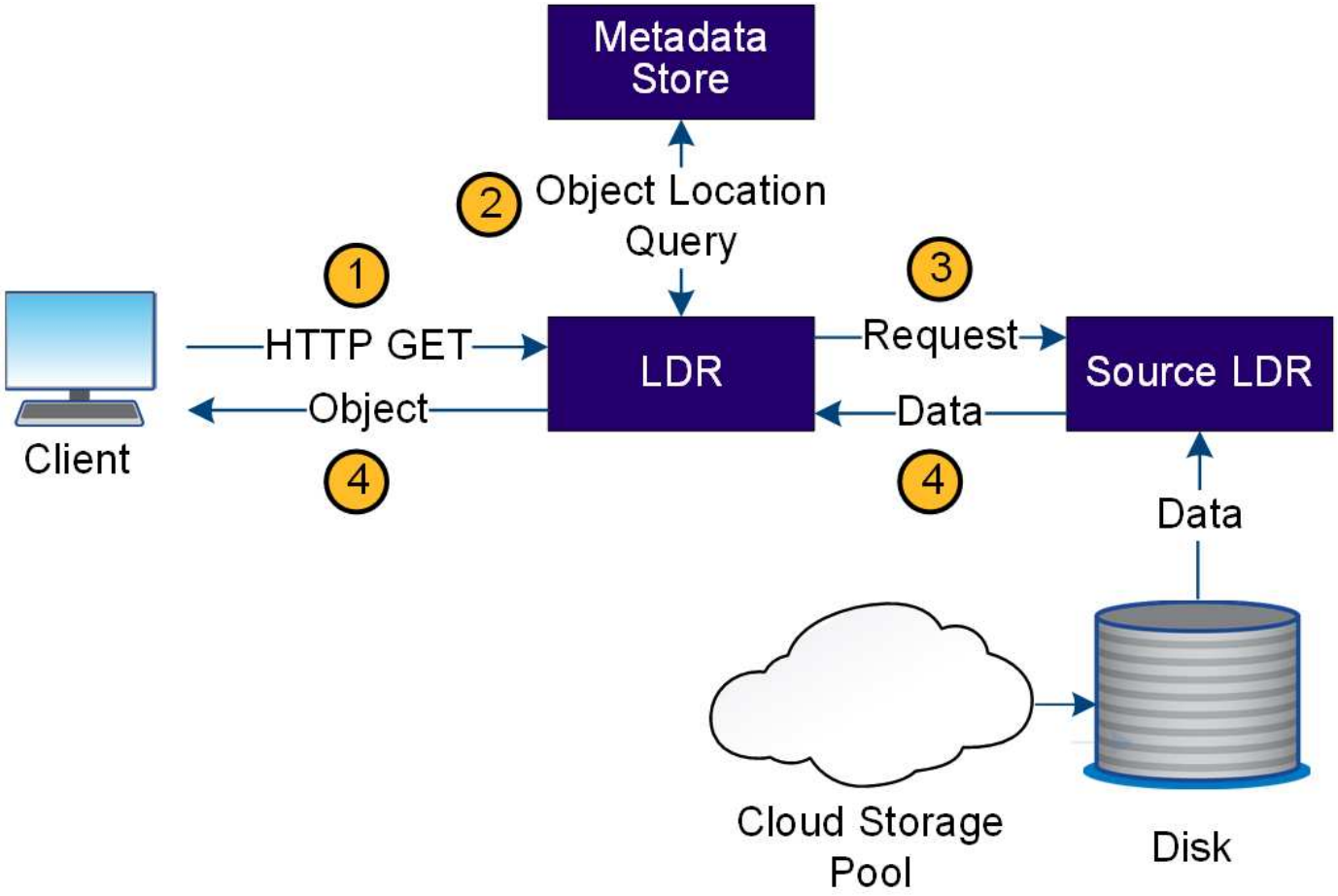
1. ILM引擎會選取要複寫至雲端儲存資源池的Data Mover服務。
2. Data Mover服務會將物件資料傳送至Cloud Storage Pool。
3. Data Mover服務會通知ILM引擎物件資料已儲存。
4. ILM引擎會使用物件位置中繼資料來更新中繼資料存放區。

StorageGRID 如何處理物件擷取

擷取作業由定義的StorageGRID 資料流組成、可在支援系統和用戶端之間進行。系統會使用屬性來追蹤從儲存節點或雲端儲存池擷取物件的情況（如有必要）。

Storage Node的LMR服務會查詢中繼資料存放區以找出物件資料的位置、然後從來源LMR服務擷取資料。優先的是從儲存節點擷取。如果物件在儲存節點上無法使用、則擷取要求會導向至雲端儲存池。

如果唯一的物件複本位於 AWS Glacier 儲存設備或 Azure 歸檔層、則用戶端應用程式必須發出 S3 RestoreObject 要求、才能將可擷取的複本還原至 Cloud Storage Pool 。



1. LMR服務會從用戶端應用程式接收擷取要求。
2. LDR服務會查詢中繼資料存放區、以取得物件資料位置和中繼資料。
3. LMR服務會將擷取要求轉送至來源LMR服務。
4. 來源 LDR 服務將擷取的物件資料傳回給被查詢的 LDR 服務，系統將物件傳回給用戶端應用程式。

StorageGRID 如何處理物件刪除

當用戶端執行刪除作業或物件的壽命到期時、觸發自動移除時、所有物件複本都會從StorageGRID 該系統移除。已定義刪除物件的資料流程。

刪除階層架構

支援多種方法來控制何時保留或刪除物件。StorageGRID物件可以由用戶端要求刪除、也可以自動刪除。不只是用戶端刪除要求、而且S3物件鎖定設定的優先順序總是高於S3儲存區生命週期和ILM放置指示。StorageGRID

- * S3物件鎖定*：如果已啟用網格的全域S3物件鎖定設定、S3用戶端就能建立啟用S3物件鎖定的儲存區、然後使用S3 REST API為新增至該儲存區的每個物件版本指定保留直到日期和合法保留設定。
  - 合法持有的物件版本無法由任何方法刪除。
  - 在物件版本達到保留截止日期之前、任何方法都無法刪除該版本。
  - 啟用 S3 物件鎖定的貯體中物件會由 ILM 「永遠」保留。不過、在達到保留截止日期之後、用戶端要求或儲存庫生命週期到期時、即可刪除物件版本。

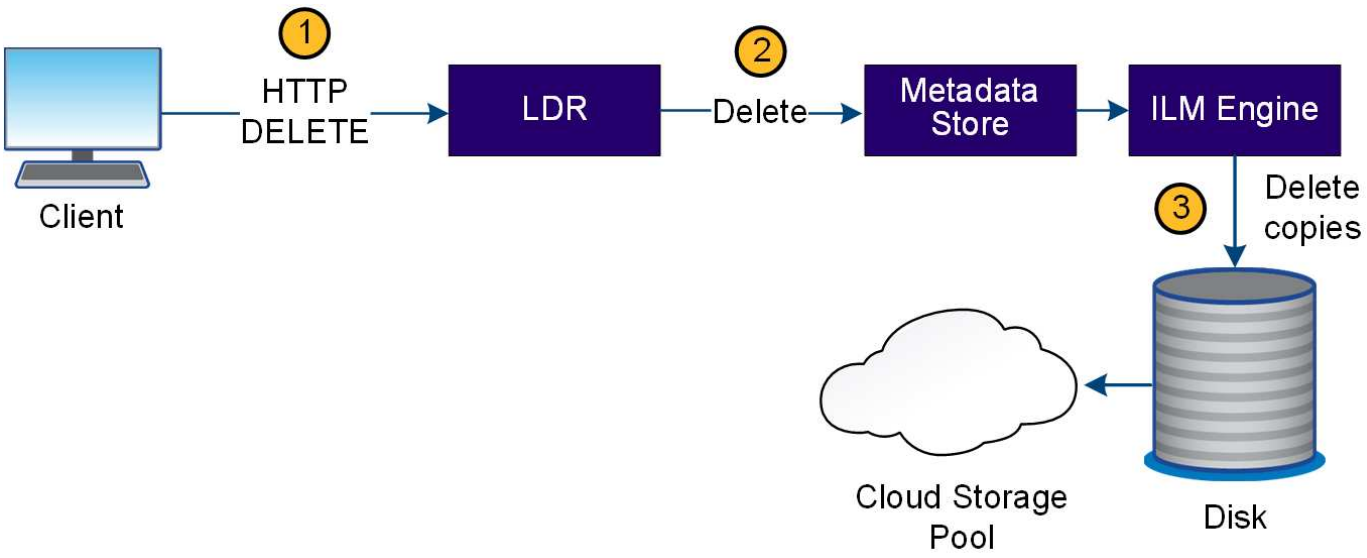
。如果 S3 用戶端將預設的保留日期套用至貯體、則不需要為每個物件指定保留日期。

- * 用戶端刪除要求 * ： S3 用戶端可以發出刪除物件要求。當用戶端刪除物件時、物件的所有複本都會從StorageGRID 作業系統中移除。
- * 刪除貯體中的物件 * ：租戶管理員使用者可以使用此選項、從 StorageGRID 系統中永久移除所選貯體中物件和物件版本的所有複本。
- * S3儲存區生命週期*：S3用戶端可將生命週期組態新增至其儲存區、以指定到期行動。如果儲存區生命週期存在、StorageGRID 除非用戶端先刪除物件、否則當符合到期行動中指定的日期或天數時、將自動刪除物件的所有複本。
- * ILM放置指示*：假設儲存區未啟用S3物件鎖定、且沒有儲存區生命週期、StorageGRID 則當ILM規則中的最後一個時間段結束、且未指定任何物件的進一步放置位置時、即可自動刪除物件。

> 當 S3 貯體生命週期設定完成時、生命週期到期動作會覆寫符合生命週期篩選器之物件的 ILM 原則。因此、即使放置物件的任何ILM指示失效、物件仍可能保留在網格上。

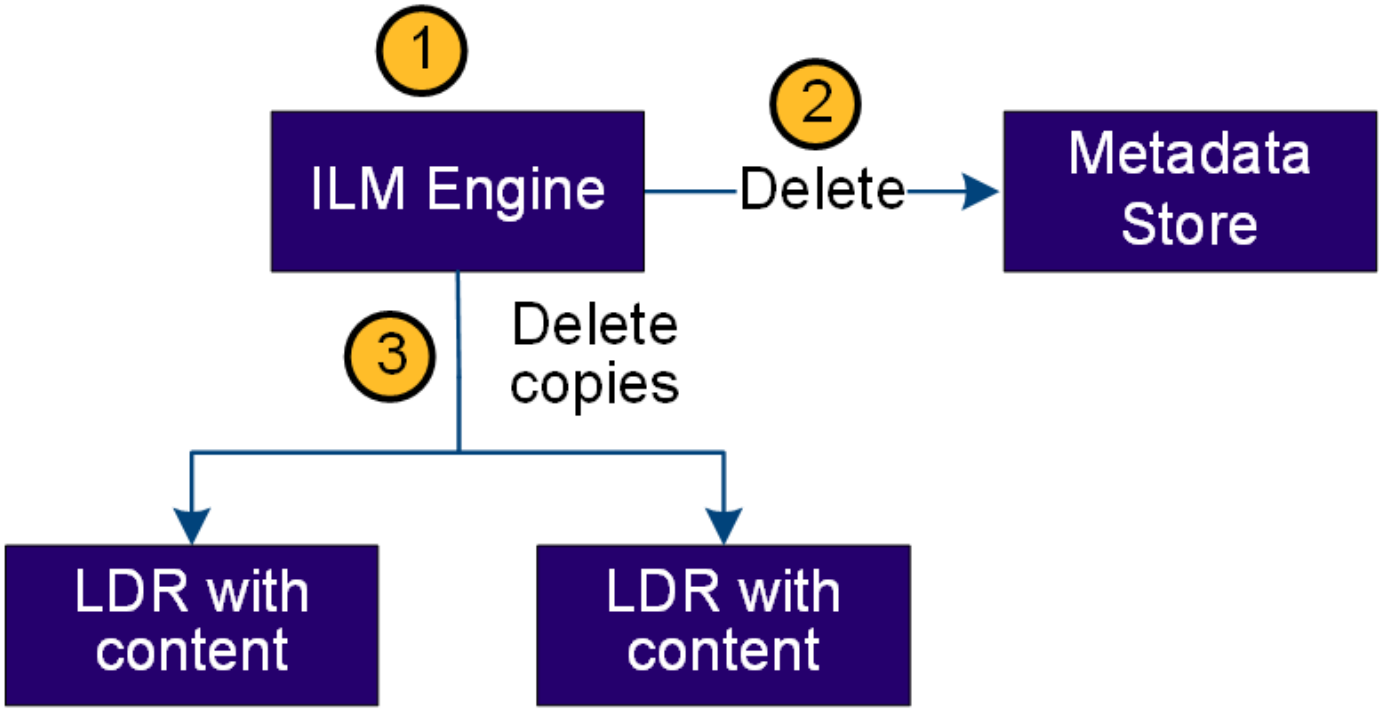
如需詳細資訊、請參閱 "如何刪除物件" 。

用戶端刪除的資料流



1. LMR服務會從用戶端應用程式接收刪除要求。
2. LDR服務會更新中繼資料存放區、使物件看起來會被用戶端要求刪除、並指示ILM引擎移除所有物件資料複本。
3. 物件會從系統中移除。中繼資料儲存區會更新以移除物件中繼資料。

ILM刪除的資料流



1. ILM引擎會判斷物件需要刪除。
2. ILM引擎會通知中繼資料存放區。中繼資料儲存區會更新物件中繼資料、使物件看起來會被刪除以供用戶端要求使用。
3. ILM引擎會移除物件的所有複本。中繼資料儲存區會更新以移除物件中繼資料。

StorageGRID 中的資訊生命週期管理

您可以使用資訊生命週期管理 (ILM) 來控制StorageGRID系統中所有物件的放置、持續時間和攝取行為。 ILM 規則決定了StorageGRID如何隨時間儲存物件。您可以設定一個或多個 ILM 規則，然後將它們新增至 ILM 策略。一個網格可以同時具有多個活動策略。

ILM規則定義：

- 應該儲存哪些物件。規則可以套用到所有對象，或者您可以指定篩選器來確定規則適用於哪些對象。例如，規則只能套用於與特定租用戶帳戶、特定 S3 儲存桶或特定元資料值相關聯的物件。
- 儲存類型與位置。物件可以儲存在儲存節點或雲端儲存池中。
- 所製作的物件複本類型。複本可以複寫或銷毀編碼。
- 複寫複本的複本數量。
- 對於銷毀編碼複本、使用的銷毀編碼方案。
- 隨著時間變更至物件的儲存位置和複本類型。
- 物件資料如何在物件擷取到網格時受到保護（同步放置或雙重提交）。

請注意、物件中繼資料並非由ILM規則管理。相反地、物件中繼資料會儲存在Cassandra資料庫的中繼資料儲存區中。每個站台會自動維護三個物件中繼資料複本、以保護資料免於遺失。

ILM規則範例

以 ILM 規則為例、可以指定下列項目：

- 僅套用至屬於 Tenant A. 的物件
- 為這些物件製作兩個複寫複本、並將每個複本儲存在不同的站台上。
- 保留這兩個複本「永遠」、表示 StorageGRID 不會自動刪除它們。相反地StorageGRID 、在用戶端刪除要求刪除這些物件之前、或是在庫位生命週期到期之前、將會保留這些物件。
- 使用平衡選項來擷取行為：只要租戶 A 將物件儲存至 StorageGRID 、就會套用雙站台放置指示、除非無法立即製作兩個必要的複本。

  例如、如果租戶A儲存物件時無法連線站台2、StorageGRID 則會在站台1的儲存節點上製作兩份臨時複本。一旦網站2推出、StorageGRID 就會在該網站上製作所需的複本。

ILM原則如何評估物件

StorageGRID 系統的主動式 ILM 原則可控制所有物件的放置、持續時間和擷取行為。

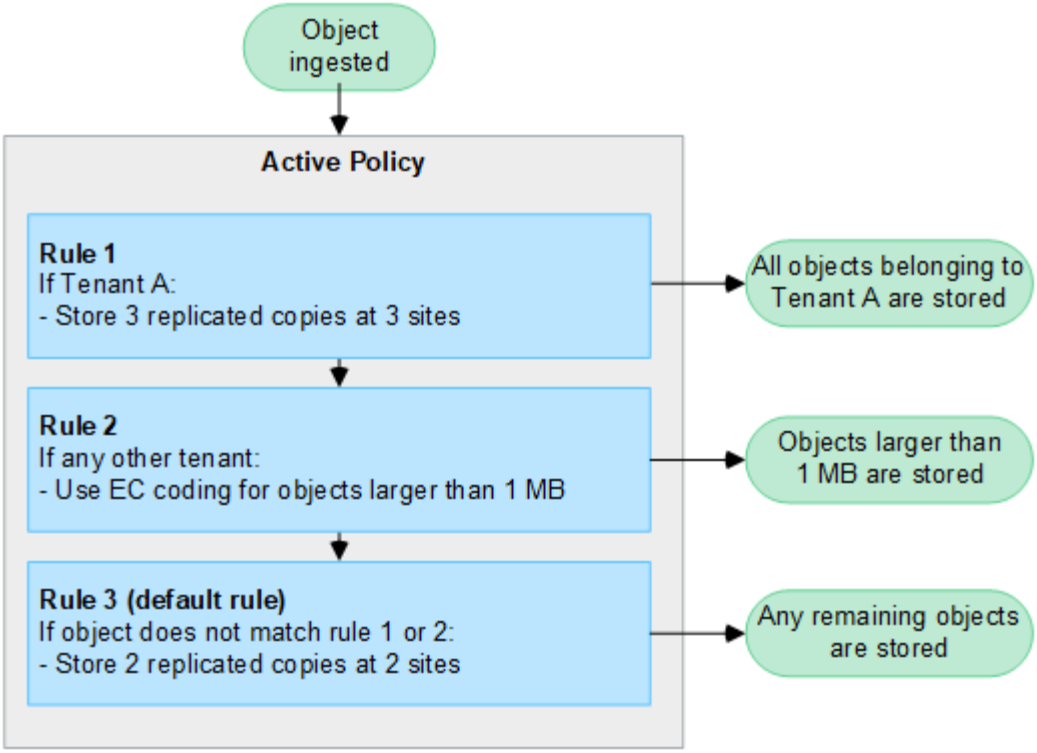
當用戶端將物件儲存StorageGRID 至物件以供參考時、會根據作用中原則中的順序ILM規則集來評估物件、如下所示：

1. 如果原則中第一個規則的篩選器符合物件、則會根據該規則的擷取行為擷取物件、並根據該規則的放置指示加以儲存。
2. 如果第一個規則的篩選條件與物件不符、則會根據原則中的每個後續規則來評估物件、直到進行符合為止。
3. 如果沒有符合物件的規則、則會套用原則中預設規則的擷取行為和放置指示。預設規則是原則中的最後一個規則、無法使用任何篩選器。它必須套用至所有租戶、所有貯體及所有物件版本。

ILM原則範例

舉例來說、 ILM 原則可能包含三個 ILM 規則、其中指定下列項目：

- * 規則 1 ：租戶 A* 的複寫複本
  - 比對屬於 Tenant A. 的所有物件
  - 將這些物件儲存為三個站台的三個複寫複本。
  - 屬於其他租戶的物件不符合規則 1 、因此會根據規則 2 進行評估。
- * 規則 2 ： 1 MB* 以上物件的銷毀編碼
  - 比對其他租戶的所有物件、但只有在物件大於 1 MB 時才會比對。這些較大的物件使用6+3銷毀編碼儲存在三個站台。
  - 不符合 1 MB 或更小的物件、因此會根據規則 3 來評估這些物件。
- * 規則 3 ： 2 份複本 2 個資料中心 * （預設）
  - 是原則中的最後一個和預設規則。不使用篩選器。
  - 為規則 1 或規則 2 不相符的所有物件建立兩個複寫複本（不屬於租戶 A 且小於 1 MB 的物件）。



相關資訊

- "使用ILM管理物件"

探索 StorageGRID

探索 StorageGRID Grid Manager

Grid Manager是瀏覽器型的圖形介面、可讓您設定、管理StorageGRID 及監控您的作業系統。

Grid Manager 會隨每個版本一起更新、可能與此頁面上的範例螢幕擷取畫面不符。

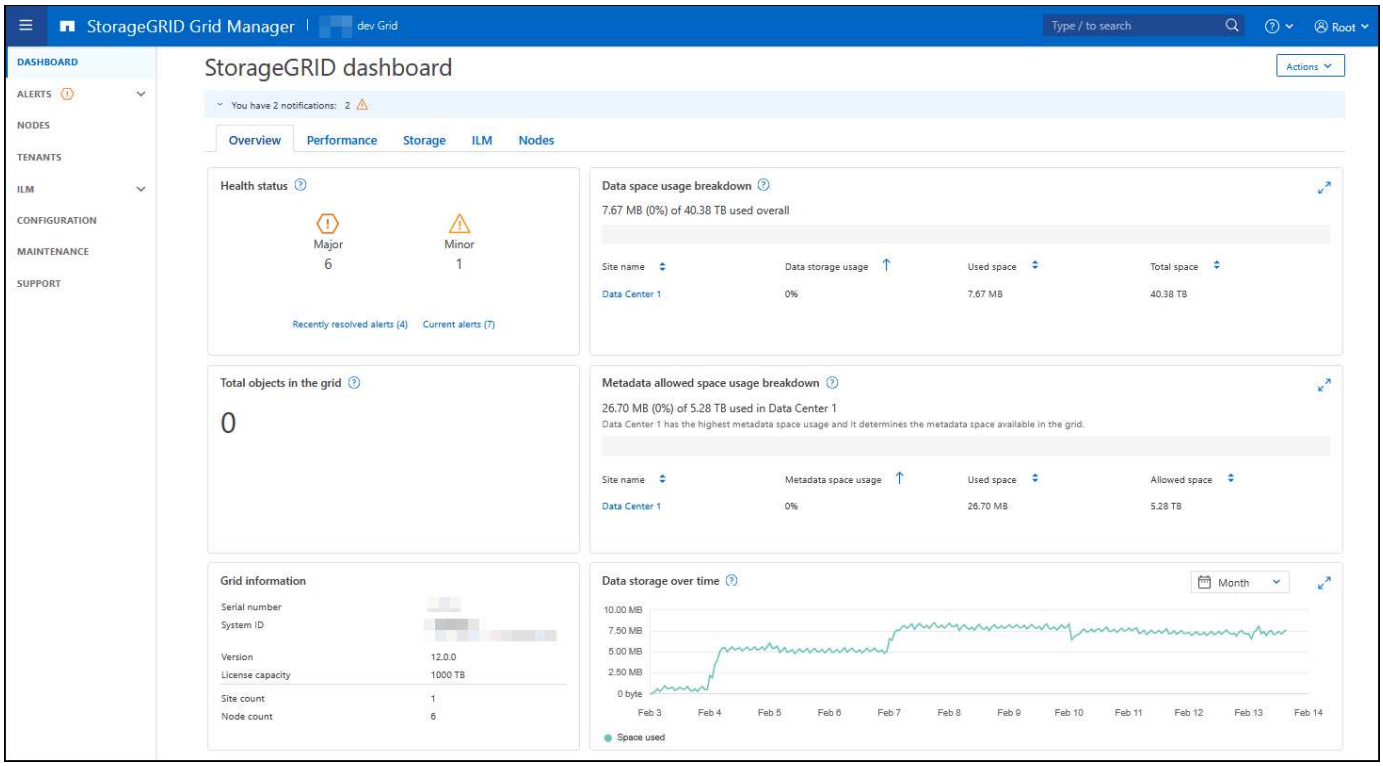
當您登入Grid Manager時、即連線至管理節點。每StorageGRID 個系統包含一個主要管理節點和任意數量的非主要管理節點。您可以連線至任何管理節點、每個管理節點都會顯示StorageGRID 類似的畫面、顯示有關該系統的資訊。

您可以使用存取 Grid Manager "支援的網頁瀏覽器"。

Grid Manager儀表板

第一次登入 Grid Manager 時、您可以使用儀表板"監控系統活動"一覽無遺。

儀表板包含有關系統健全狀況和效能、儲存使用、 ILM 程序、 S3 作業和網格中節點的資訊。您可以"設定儀表板"從內含有效監控系統所需資訊的卡片集合中進行選擇。



若要了解每張卡片上顯示的資訊，請選擇該卡片的說明圖示 。

搜尋欄位

標頭列中的*搜尋*欄位可讓您快速瀏覽至Grid Manager中的特定頁面。例如、您可以輸入 * km * 來存取金鑰管理伺服器（ KMS ）頁面。

您可以使用*搜尋*來尋找Grid Manager側邊列和組態、維護及支援功能表上的項目。您也可以依名稱搜尋網格節點和租戶帳戶等項目。

說明功能表

說明選單 提供以下項目的存取：

- 這"FabricPool"和"S3 設定"巫師
- 目前版本的StorageGRID文件站點
- "API 文件"
- 關於目前安裝的 StorageGRID 版本的資訊

警示功能表

警示功能表提供易於使用的介面、可偵測、評估及解決StorageGRID 可能在執行過程中發生的問題。

從「警示」功能表、您可以執行下列"管理警示"動作：

- 檢閱目前的警示
- 檢閱已解決的警示
- 設定靜音以隱藏警示通知

- 針對觸發警示的條件定義警示規則
- 設定 StorageGRID 警示的電子郵件通知

節點頁面

這"節點頁面"顯示有關整個網格、網格中每個站點以及站點上每個節點的資訊。若要查看特定站點或節點的信息，請選擇該站點或節點。

租戶頁面

"租戶頁面"可讓您使用 "建立及監控儲存租戶帳戶"StorageGRID 系統。您必須建立至少一個租戶帳戶、以指定誰可以儲存及擷取物件、以及哪些功能可供他們使用。

「租戶」頁面也會提供每個租戶的使用詳細資料、包括使用的儲存容量和物件數目。如果您在建立租戶時設定配額、就可以查看該配額的使用量。

ILM功能表

"ILM功能表"可讓您"設定資訊生命週期管理（ ILM ）規則和原則"管理資料的耐用度和可用度。您也可以輸入物件識別碼、以檢視該物件的中繼資料。

您可以從 ILM 功能表檢視及管理 ILM ：

- 規則
- 原則
- 原則標籤
- 儲存資源池
- 儲存等級
- 區域
- 物件中繼資料查詢

組態功能表

「組態」功能表可讓您指定網路設定、安全性設定、系統設定、監控選項及存取控制選項。

網路工作

網路工作包括：

- "管理高可用度群組"
- "管理負載平衡器端點"
- "設定 S3 端點網域名稱"
- "管理流量分類原則"
- "設定VLAN介面"
- "為管理介面啟用StorageGRID CORS"

安全性工作

安全性工作包括：

- "管理安全性憑證"
- "管理內部防火牆控制"
- "設定金鑰管理伺服器"
- 配置安全設置，包括"TLS 和 SSH 原則"，"網路和物件安全選項" ，"介面安全性設定" ， 和"SSH 存取選項"
- 配置設定"儲存代理伺服器"或"管理 Proxy"

系統工作

系統工作包括：

- 使用 "網格同盟" 在兩個 StorageGRID 系統之間同步租戶帳戶資訊和複寫物件資料
- （可選）啟用"壓縮儲存的物件"選項
- 或者，配置"預設桶一致性設定"
- "管理 S3 對象鎖"
- 了解儲存設置，例如"儲存Volume浮點"
- "管理銷毀編碼設定檔"

監控工作

監控工作包括：

- "設定郵件伺服器"
- "設定日誌管理"
- "使用SNMP監控"

存取控制工作

存取控制工作包括：

- "管理管理群組"
- "管理管理員用戶"
- 變更"資源配置複雜密碼"或者"節點主控台密碼"
- "使用身分識別聯盟"
- "配置 SSO"
- "設定多管理員驗證"

維護功能表

「維護」功能表可讓您執行維護工作、系統維護和網路維護。

工作

維護工作包括：

- "取消委任作業" 移除未使用的網格節點和站台
- "擴充作業"新增網格節點和站台
- "網格節點還原程序"更換故障節點並還原資料
- "重新命名程序"可更改網格、站點和節點的顯示名稱
- "物件存在檢查作業"驗證物件資料是否存在（雖然不是正確的）
- 執行"循環重新開機"重新啟動多個網格節點
- 恢復物件資料
  - "將物件資料還原至應用裝置的儲存磁碟區"
  - "將物件資料還原至系統磁碟機不受影響的儲存磁碟區"
  - "將物件資料還原至儲存磁碟區（系統磁碟機故障）"

系統

您可以執行的系統維護工作包括：

- "檢視StorageGRID 本授權資訊"或者"更新許可證信息"
- 產生並下載"恢復包"
- 在選定設備上執行 StorageGRID 軟體更新、包括軟體升級、 Hotfix 及 SANtricity OS 軟體更新
  - "升級程序"
  - "修復程序"
  - "使用 Grid Manager 升級 SG6000 儲存控制器上的 SANtricity OS"
  - "使用 Grid Manager 升級 SG5700 儲存控制器上的 SANtricity OS"

網路

您可以執行的網路維護工作包括：

- "設定 DNS 伺服器"
- "更新網格網路子網"
- "管理NTP伺服器"

支援功能表

「支援」功能表提供的選項可協助技術支援人員分析及疑難排解您的系統。

工具

從「支援」功能表的「工具」區段、您可以：

- "設定AutoSupport 功能"
- "執行診斷" 位於網格的目前狀態
- "收集記錄檔和系統資料"
- "檢視支援指標"

* Metrics *選項提供的工具、是專供技術支援使用。這些工具中的某些功能和功能表項目是刻意無法運作的。

其他

從「支援」功能表的其他區段、您可以：

- 配置"I/O 優先權"
- 管理"連結成本"
- 查看節點服務ID
- 管理"儲存浮水印"

探索 **StorageGRID Tenant Manager**

"租戶管理程式"是以瀏覽器為基礎的圖形化介面、租戶使用者可存取此介面來設定、管理及監控其儲存帳戶。

租戶管理程式會隨每個版本一起更新、可能與本頁的範例螢幕擷取畫面不符。

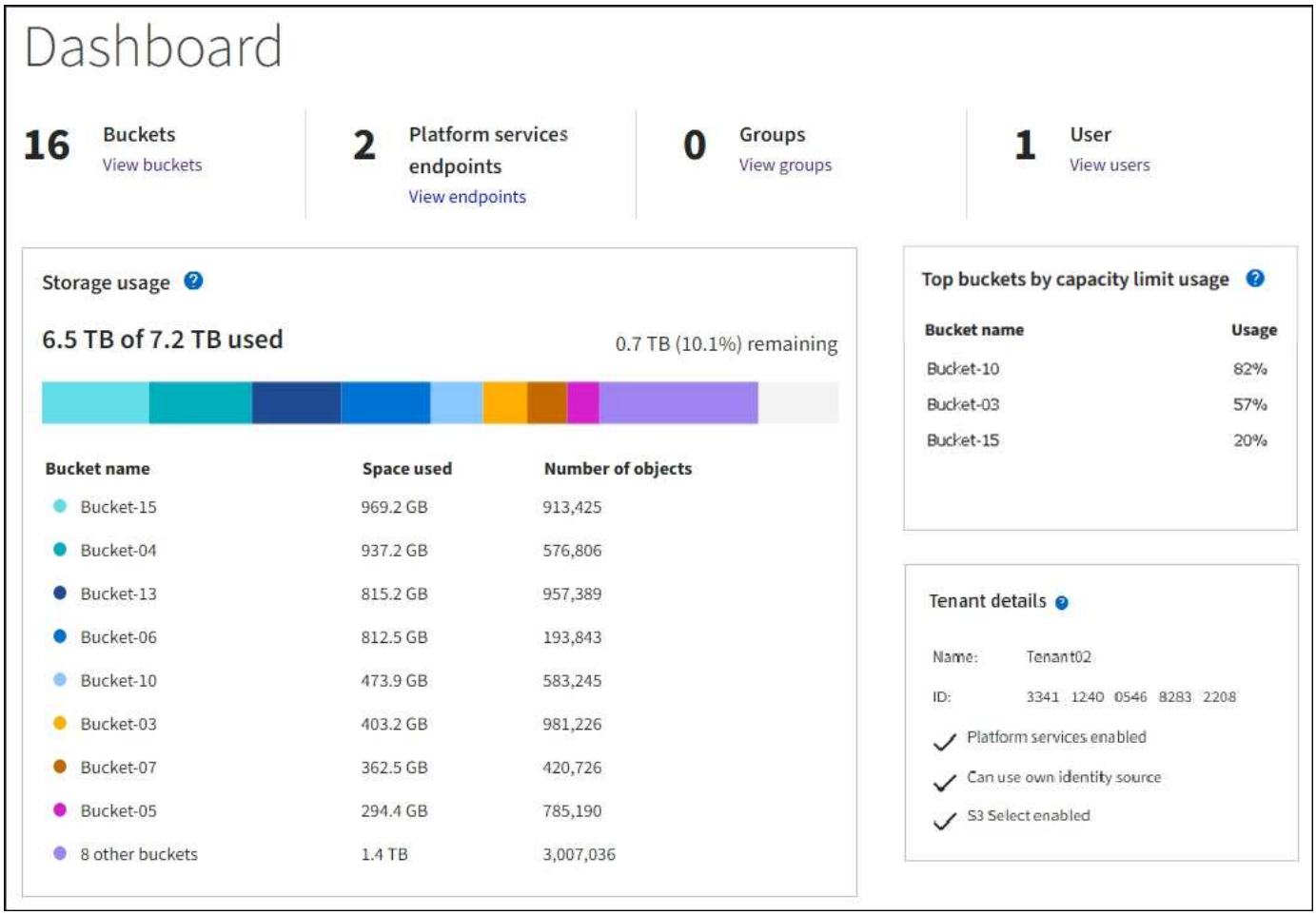
當租戶使用者登入租戶管理程式時、他們會連線至管理節點。

租戶管理器儀表板

網格管理員使用Grid Manager或Grid Management API建立租戶帳戶之後、租戶使用者就可以登入租戶管理程式。

租戶管理器儀表板允許租戶使用者一目了然地監控儲存使用情況。儲存使用情況面板包含租戶最大的 S3 儲存桶清單。已用空間值是儲存桶或容器中的物件資料總量。長條圖表示這些桶子或容器的相對大小。

長條圖上方顯示的值是租戶所有貯體或容器所使用空間的總和。如果在建立帳戶時指定租戶可用的GB、TB或PB上限、也會顯示已使用及剩餘的配額量。



儲存功能表（ **S3** ）

此選單允許 S3 用戶：

- 管理存取密鑰
- 建立、管理和刪除儲存桶
- 管理平台服務端點
- 查看他們被允許使用的任何電網聯合連接

我的存取金鑰

S3租戶使用者可以管理存取金鑰、如下所示：

- 擁有「管理您自己的 S3 認證」權限的使用者、可以建立或移除自己的 S3 存取金鑰。
- 擁有「根」存取權限的使用者可以管理 S3 根帳戶、自己的帳戶及所有其他使用者的存取金鑰。除非儲存區原則明確停用、否則根存取金鑰也能提供租戶的儲存區和物件的完整存取權。

> 透過存取管理選單可以管理其他使用者的存取金鑰。

桶

擁有適當權限的 S3 租戶使用者可為其貯體執行下列工作：

- 建立貯體
- 為新的儲存區啟用S3物件鎖定（假設StorageGRID 已啟用S3物件鎖定功能以供整個系統使用）
- 更新一致性值
- 啟用和停用上次存取時間更新
- 啟用或暫停物件版本設定
- 更新 S3 物件鎖定預設保留
- 設定跨來源資源共用（CORS）
- 刪除貯體中的所有物件
- 刪除空的儲存區
- 使用"S3 主控台"來管理貯體物件

如果網格管理員已啟用使用租戶帳戶的平台服務、具有適當權限的S3租戶使用者也可以執行下列工作：

- 設定 S3 事件通知、可傳送至支援 Amazon Simple Notification Service 的目的地服務。
- 設定CloudMirror複寫、讓租戶能夠自動將物件複寫到外部S3儲存區。
- 設定搜尋整合、每當物件建立、刪除或更新中繼資料或標記時、會將物件中繼資料傳送至目的地搜尋索引。

平台服務端點

如果網格管理員已為租戶帳戶啟用平台服務、具有「管理端點」權限的 S3 租戶使用者可以為每個平台服務設定目的地端點。

網格同盟連線

如果網格管理員已啟用租戶帳戶的網格同盟連線、則具有「根」存取權限的 S3 租戶使用者可以檢視連線名稱、存取已啟用跨網格複寫的每個儲存格的儲存格詳細資料頁面、 並檢視儲存區資料複寫到連線中其他網格時發生的最新錯誤。請參閱。 "檢視網格同盟連線"

存取管理功能表

「存取管理」功能表可讓StorageGRID 無權從聯盟身分識別來源匯入使用者群組、並指派管理權限。租戶也可以管理本機租戶群組和使用者、除非整個StorageGRID 作業系統都有單一登入（SSO）功能。

網路準則

StorageGRID 的網路準則

請使用這些準則來瞭StorageGRID 解有關架構和網路拓撲的資訊、並瞭解網路組態和資源配置的需求。

關於這些指示

這些準則提供您在StorageGRID 部署和設定StorageGRID 節點之前、可用來建立「資訊」網路基礎架構的資訊。使用這些準則有助於確保網格中的所有節點之間、網格與外部用戶端和服務之間都能進行通訊。

外部用戶端和外部服務需要連線StorageGRID 至無法分享的網路、才能執行下列功能：

- 儲存及擷取物件資料
- 接收電子郵件通知
- 存取StorageGRID 功能完善的管理介面（Grid Manager與Tenant Manager）
- 存取稽核共用區（選用）
- 提供下列服務：
  - 網路時間傳輸協定（NTP）
  - 網域名稱系統（ DNS ）
  - 金鑰管理伺服器（KMS）

必須適當設定以處理這些功能及其他功能的流量。StorageGRID

開始之前

若要設定StorageGRID 適用於某個效能不穩定系統的網路功能、需要具備乙太網路交換、TCP/IP網路、子網路、網路路由和防火牆等豐富經驗。

設定網路之前、請先熟悉 StorageGRID 架構"深入瞭解StorageGRID"、如所述。

在您決定StorageGRID 要使用哪些靜態網路、以及如何設定這些網路之後、StorageGRID 您可以依照適當的指示來安裝和設定這些節點。

安裝應用裝置節點

- "安裝應用裝置硬體"

安裝軟體型節點

- "在基於軟體的節點上安裝StorageGRID"

設定及管理**StorageGRID** 功能

- "管理StorageGRID"
- "版本資訊"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。

網路類型**StorageGRID**

系統中的網格節點StorageGRID 會處理_GRID交通量_、*admin*交通量_和_*Client*交通量。您必須適當設定網路、以管理這三種流量類型、並提供控制與安全性。

流量類型

流量類型	說明	網路類型
網格流量	在網格中所有節點之間傳輸的內部StorageGRID 不完整流量。所有網格節點都必須能夠透過此網路與所有其他網格節點通訊。	網格網路（必填）
管理流量	用於系統管理與維護的流量。	管理網路（選用）、VLAN網路（選用）
用戶端流量	在外部用戶端應用程式和網格之間傳輸的流量、包括來自 S3 用戶端的所有物件儲存要求。	用戶端網路（選用）、VLAN網路（選用）

您可以使用下列方式設定網路：

- 僅限網格網路
- 網格和管理網路
- 網格和用戶端網路
- 網格、管理和用戶端網路

Grid Network是強制性的、可管理所有的網格流量。安裝時可納入管理網路和用戶端網路、或是稍後新增、以因應需求變更。雖然管理網路和用戶端網路是選用的、但當您使用這些網路來處理管理和用戶端流量時、網格網路可以隔離且安全無虞。

內部連接埠只能透過Grid Network存取。外部連接埠可從所有網路類型存取。這種靈活度提供多種選項、可設計StorageGRID 出一套功能豐富的功能、並在交換器和防火牆中設定外部IP和連接埠篩選功能。請參閱"內部網格節點通訊"和"外部通訊"。

網路介面

使用下列特定介面將各個節點連線至各個網路：StorageGRID

網路	介面名稱
網格網路（必填）	eth0
管理網路（選用）	eth1
用戶端網路（選用）	eth2

有關將虛擬或實體連接埠對應到節點網路介面的詳細信息，請參閱"在基於軟體的節點上安裝StorageGRID"。

應用裝置節點

- "SG6160 儲存設備"
- "SGF6112 儲存設備"
- "SG6000 儲存設備"
- "SG5800 儲存設備"

- "SG5700 儲存設備"
- "SG110 和 SG1100 服務應用裝置"
- "SG100 和 SG1000 服務應用裝置"

每個節點的網路資訊

您必須為節點上啟用的每個網路設定下列項目：

- IP 位址
- 子網路遮罩
- 閘道 IP 位址

您只能為每個網格節點上的三個網路中的每個網路設定一個IP位址/遮罩/閘道組合。如果您不想為網路設定閘道、則應該使用 IP 位址做為閘道位址。

高可用度群組

高可用度（HA）群組可將虛擬IP（VIP）位址新增至Grid或Client Network介面。如需更多資訊、請參閱 "管理高可用度群組"。

網格網路

網格網路為必填項目。它用於所有內部StorageGRID 的資訊流量。Grid Network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。Grid Network上的所有節點都必須能夠與所有其他節點通訊。Grid Network可由多個子網路組成。包含關鍵網格服務（例如NTP）的網路也可新增為網格子網路。

> 不支援節點之間的網路位址轉譯（NAT）StorageGRID 。

即使已設定管理網路和用戶端網路、網格網路仍可用於所有管理流量和所有用戶端流量。除非節點已設定用戶端網路、否則Grid Network閘道是節點的預設閘道。

> 設定Grid Network時、您必須確保網路受到不受信任用戶端的保護、例如開放式網際網路上的用戶端。

請注意Grid Network閘道的下列需求與詳細資料：

- 如果有多個網格子網路、則必須設定網格網路閘道。
- 網格網路閘道是節點的預設閘道、直到網格組態完成為止。
- 所有節點的靜態路由都會自動產生、以到達全域網格網路子網路清單中所設定的所有子網路。
- 如果新增了用戶端網路、則當網格組態完成時、預設閘道會從網格網路閘道切換至用戶端網路閘道。

管理網路

管理網路為選用網路。設定後、即可用於系統管理和維護流量。管理網路通常是私有網路、不需要在節點之間進行路由傳送。

您可以選擇哪些網格節點應啟用管理網路。

當您使用管理網路時、管理和維護流量不需要跨越Grid Network。管理網路的一般用途包括：

- 存取Grid Manager和Tenant Manager使用者介面。
- 存取關鍵服務、例如NTP伺服器、DNS伺服器、外部金鑰管理伺服器（KMS）和輕量型目錄存取傳輸協定（LDAP）伺服器。
- 存取管理節點上的稽核記錄。
- 安全Shell傳輸協定（SSH）存取、以進行維護與支援。

管理網路絕不用於內部網格流量。系統會提供管理網路閘道、並允許管理網路與多個外部子網路通訊。不過、管理網路閘道永遠不會用作節點的預設閘道。

請注意管理網路閘道的下列需求和詳細資料：

- 如果要從管理網路子網路外部建立連線、或是設定了多個管理網路子網路、則需要管理網路閘道。
- 會針對節點的管理網路子網路清單中所設定的每個子網路建立靜態路由。

用戶端網路

用戶端網路為選用項目。設定後、它會用於為 S3 等用戶端應用程式提供網格服務的存取。如果您計畫讓StorageGRID 外部資源（例如雲端儲存資源池或StorageGRID CloudMirror複寫服務）能夠存取這些資料、則外部資源也可以使用用戶端網路。網格節點可透過用戶端網路閘道與任何可連線的子網路進行通訊。

您可以選擇哪些網格節點上應該啟用「用戶端網路」。所有節點不必位於同一個用戶端網路上、而且節點絕不會透過用戶端網路彼此通訊。在網格安裝完成之前、用戶端網路不會運作。

為了增加安全性、您可以指定節點的用戶端網路介面不受信任、以便用戶端網路對允許的連線有更多限制。如果節點的用戶端網路介面不受信任、介面會接受傳出連線、例如CloudMirror複寫所使用的連線、但只接受已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"管理防火牆控制"和"設定負載平衡器端點"。

當您使用用戶端網路時、用戶端流量不需要跨越Grid Network。網格網路流量可分隔至安全、不可路由的網路。下列節點類型通常是以用戶端網路進行設定：

- 閘道節點、因為這些節點提供對 StorageGRID 負載平衡器服務的存取、以及 S3 用戶端對網格的存取。
- 儲存節點、因為這些節點可存取 S3 傳輸協定、 Cloud Storage Pool 和 CloudMirror 複寫服務。
- 管理節點、確保租戶使用者無需使用管理網路即可連線至租戶管理員。

請注意下列用戶端網路閘道的資訊：

- 如果已設定用戶端網路、則需要用戶端網路閘道。
- 當網格組態完成時、用戶端網路閘道會成為網格節點的預設路由。

選用的**VLAN**網路

視需要、您可以選擇性地使用虛擬LAN（VLAN）網路來處理用戶端流量和某些類型的管理流量。不過、網格流量無法使用 VLAN 介面。節點之間的內部不間斷流量必須一律使用eth0上的Grid Network。StorageGRID

若要支援使用VLAN、您必須將節點上的一個或多個介面設定為交換器的主幹介面。您可以將網格網路介面（ eth0 ）或用戶端網路介面（ eth2 ）設定為主幹、也可以將主幹介面新增至節點。

如果將eth0設定為主幹、Grid Network流量會透過主幹原生介面（如交換器上所設定）傳輸。同樣地、如果eth2設定為主幹、而用戶端網路也設定在同一個節點上、則用戶端網路會使用交換器上設定的主幹連接埠原生VLAN。

VLAN網路僅支援傳入管理流量、例如用於SSH、Grid Manager或Tenant Manager流量。VLAN網路不支援用於NTP、DNS、LDAP、KMS及雲端儲存資源池的傳出流量。

> VLAN介面只能新增至管理節點和閘道節點。您無法使用 VLAN 介面來存取用戶端或管理儲存節點。

請參閱"設定VLAN介面"以取得指示與準則。

VLAN介面僅用於HA群組、並在作用中節點上指派VIP位址。請參閱"管理高可用度群組"以取得指示與準則。

網路拓撲範例

StorageGRID 的網格網路拓撲

最簡單的網路拓撲是透過僅設定Grid Network來建立。

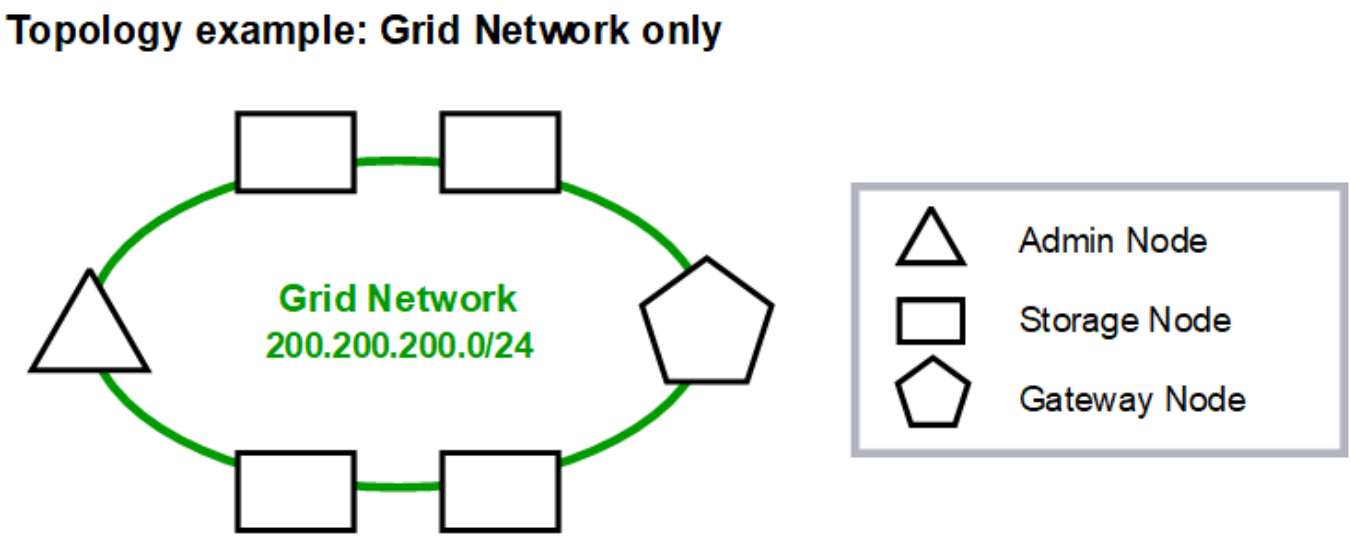
當您設定Grid Network時、會為每個網格節點的eth0介面建立主機IP位址、子網路遮罩和閘道IP位址。

在組態期間、您必須將所有網格網路子網路新增至網格網路子網路清單（GNSL）。此清單包含所有站台的所有子網路、也可能包含外部子網路、可讓您存取NTP、DNS或LDAP等關鍵服務。

安裝時、Grid Network介面會針對GNSL中的所有子網路套用靜態路由、並設定節點通往Grid Network閘道的預設路由（如果已設定）。如果沒有用戶端網路、而Grid Network閘道是節點的預設路由、則不需要GNSL。也會產生通往網格中所有其他節點的主機路由。

在此範例中、所有流量都共用相同的網路、包括與 S3 用戶端要求相關的流量、以及管理和維護功能。

> 此拓撲適用於外部無法使用的單一站台部署、概念驗證或測試部署、或協力廠商負載平衡器做為用戶端存取界限。如有可能、網格網路應僅用於內部流量。管理網路和用戶端網路都有額外的防火牆限制、可封鎖外部的內部服務流量。支援將Grid Network用於外部用戶端流量、但這種使用方式可提供較少的保護層。



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

StorageGRID 的管理網路拓撲

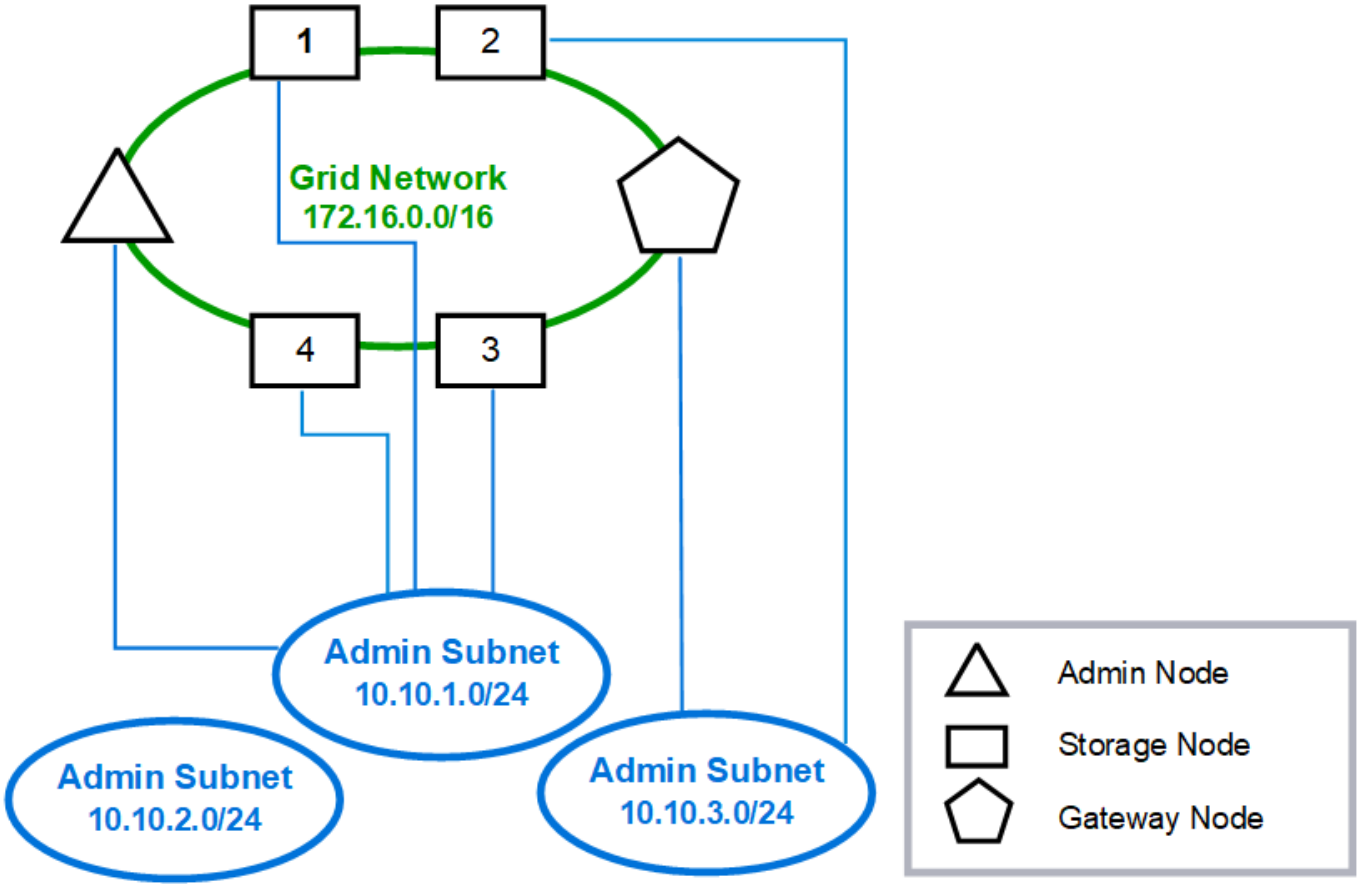
擁有管理網路是選擇性的。使用管理網路和網格網路的其中一種方法、就是為每個節點設定可路由的網格網路和有邊界的管理網路。

當您設定管理網路時、會為每個網格節點的eth1介面建立主機IP位址、子網路遮罩和閘道IP位址。

管理網路可為每個節點唯一、並可由多個子網路組成。每個節點均可設定管理外部子網路清單（Aesl）。Aesl會列出每個節點可透過管理網路連線的子網路。Aesl也必須包含網格透過管理網路存取的任何服務子網路、例如NTP、DNS、KMS和LDAP。靜態路由會套用至Aesl中的每個子網路。

在此範例中、 Grid Network 用於 S3 用戶端要求和物件管理相關的流量、而管理網路則用於管理功能。

Topology example: Grid and Admin Networks



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	**Routes**			**Type**	**From**
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

StorageGRID 的用戶端網路拓撲

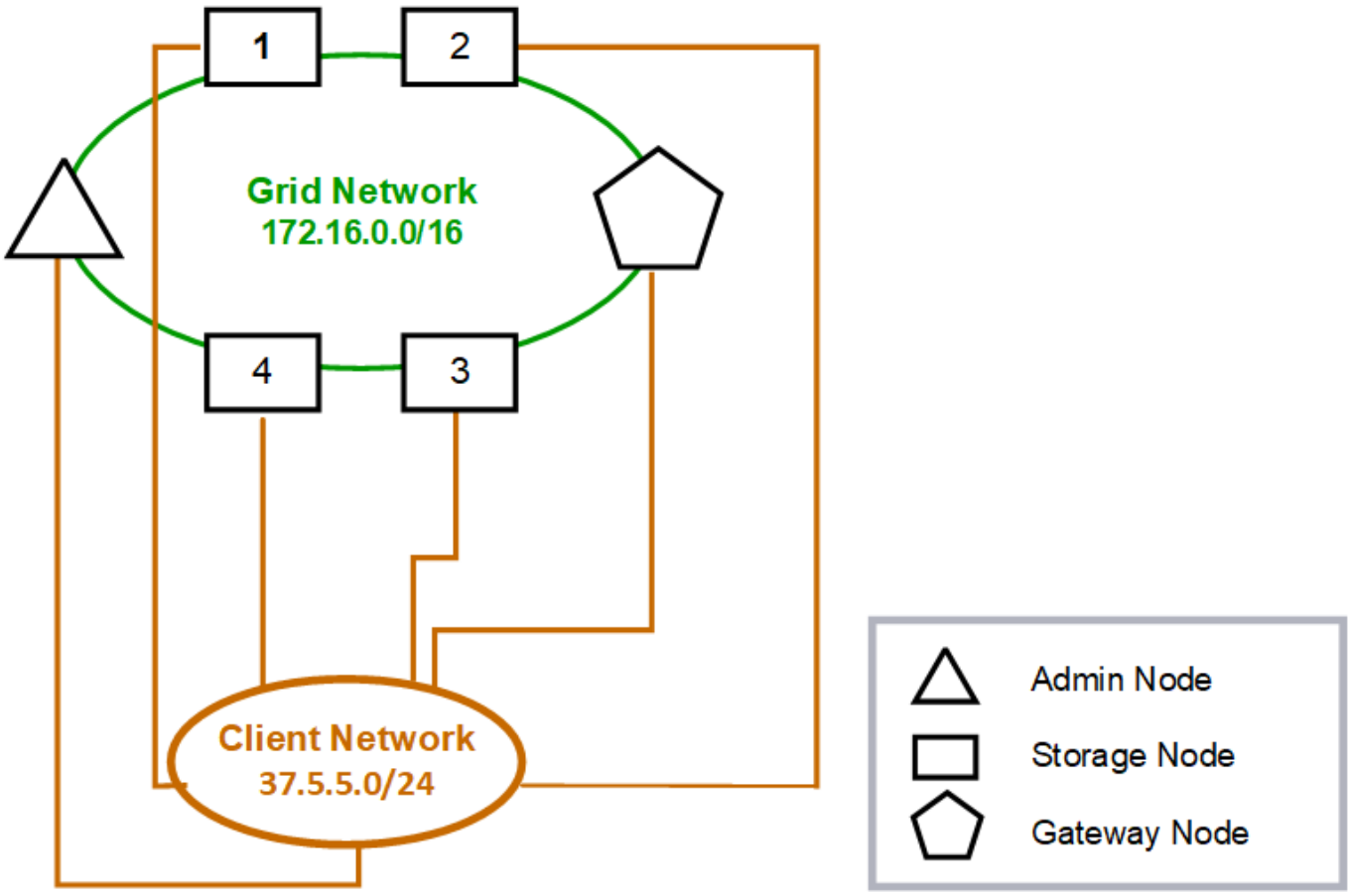
擁有用戶端網路為選用功能。使用用戶端網路可將用戶端網路流量（例如 S3 ）與網格內部流量分開、使網格網路更安全。未設定管理網路時、用戶端或網格網路均可處理管理流量。

當您設定用戶端網路時、會為所設定節點的eth2介面建立主機IP位址、子網路遮罩和閘道IP位址。每個節點的用戶端網路可以獨立於任何其他節點上的用戶端網路。

如果您在安裝期間為節點設定用戶端網路、節點的預設閘道會在安裝完成時從Grid Network閘道切換至Client Network閘道。如果稍後新增用戶端網路、則節點的預設閘道交換器會採用相同的方式。

在此範例中、用戶端網路用於 S3 用戶端要求和管理功能、而 Grid Network 則專用於內部物件管理作業。

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

相關資訊

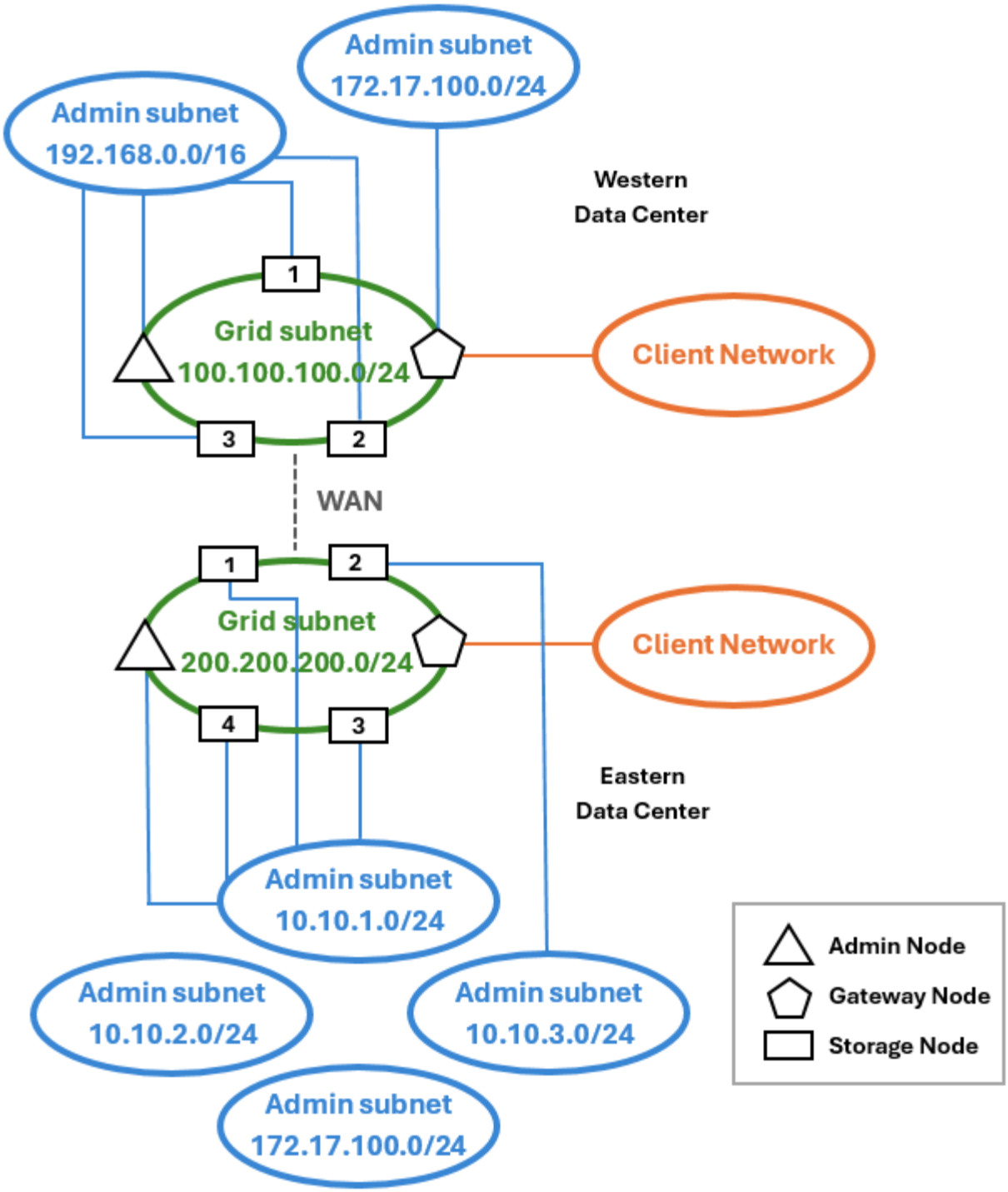
"變更節點網路組態"

所有三個 **StorageGRID** 網路的網路拓撲

您可以將這三個網路設定為一個網路拓撲、其中包含私有網格網路、限定站台專屬的管理網路和開放式用戶端網路。使用負載平衡器端點和不受信任的用戶端網路、可視需要提供額外的安全性。

在此範例中：

- Grid Network用於與內部物件管理作業相關的網路流量。
- 管理網路用於與管理功能相關的流量。
- 用戶端網路用於 S3 用戶端要求的相關流量。
- 拓撲範例：網格、管理和用戶端網路 *



StorageGRID 的網路需求

您必須驗證目前的網路基礎架構和組態是否可支援計畫StorageGRID 性的網路設計。

一般網路需求

所有StorageGRID 的支援部署都必須能夠支援下列連線。

這些連線可透過Grid、Admin或Client Networks進行、或是如網路拓撲範例所示的這些網路組合。

- 管理連線：系統管理員與節點之間的傳入連線、通常是透過SSH。網頁瀏覽器可存取Grid Manager、租戶管理程式及StorageGRID 《NetApp應用裝置安裝程式」。
- *NTP 伺服器連線 * ：接收傳入 UDP 回應的傳出 UDP 連線。

  主要管理節點必須至少能連線到一部NTP伺服器。
- *DNS 伺服器連線 * ：接收傳入 UDP 回應的傳出 UDP 連線。
- * LDAP/Active Directory伺服器連線*：儲存節點上身分識別服務的傳出TCP連線。
- * AutoSupport * ：從管理節點到任一或客戶設定的 Proxy 的輸出 TCP 連線 `support.netapp.com`。
- 外部金鑰管理伺服器：從每個應用裝置節點連出TCP連線、並啟用節點加密。
- 來自 S3 用戶端的傳入 TCP 連線。
- 來自諸如CloudMirror複寫或來自雲端儲存資源池等平台服務的傳出要求StorageGRID 。

如果 StorageGRID 無法使用預設路由規則連絡任何已佈建的 NTP 或 DNS 伺服器、只要指定 DNS 和 NTP 伺服器的 IP 位址、就會自動嘗試連絡所有網路（網格、管理和用戶端）。如果可以在任何網路上連線到NTP或DNS伺服器、StorageGRID 則會自動建立額外的路由規則、以確保未來所有連線的嘗試都會使用網路。

雖然您可以使用這些自動探索的主機路由、但一般而言、您應該手動設定DNS和NTP路由、以確保自動探索失敗時的連線能力。

如果您尚未準備好在部署期間設定選用的管理和用戶端網路、則可在組態步驟中核准網格節點時、設定這些網路。此外、您可以在安裝後使用變更 IP 工具來設定這些網路（請參閱"設定IP位址"）。

VLAN 介面僅支援 S3 用戶端連線和 SSH 、 Grid Manager 和 Tenant Manager 管理連線。傳出連線、例如 NTP、DNS、LDAP、AutoSupport 支援、及KMS伺服器、 必須直接跳過用戶端、管理或網格網路介面。如果介面設定為主幹以支援VLAN介面、則此流量會透過介面原生VLAN（如交換器所設定）傳輸。

廣域網路（**WAN**）、適用於多個站台

在設定StorageGRID 包含多個站台的支援系統時、站台之間的WAN連線在計算用戶端流量之前、每個方向的頻寬必須至少為25 Mbit/秒。站台、節點或站台擴充、節點還原及其他作業或組態之間的資料複寫或銷毀編碼、將需要額外的頻寬。

實際的最低 WAN 頻寬需求取決於用戶端活動和 ILM 保護方案。如需估算 WAN 頻寬最低需求的協助、請聯絡您的 NetApp 專業服務顧問。

管理節點和閘道節點的連線

管理節點必須始終受到不受信任用戶端（例如開放式網際網路上的用戶端）的保護。您必須確保任何不受信任的用戶端都無法存取Grid Network、管理網路或用戶端網路上的任何管理節點。

您要新增至高可用度群組的管理節點和閘道節點必須設定靜態IP位址。如需更多資訊、請參閱 "管理高可用度群組"。

使用網路位址轉譯（**NAT**）

請勿在網格網路上的網格節點之間或 StorageGRID 站台之間使用網路位址轉譯（ NAT ）。當您將私有的IPv4位址用於Grid Network時、這些位址必須從每個站台的每個網格節點直接路由傳送。不過、您可以視需要在外部用戶端和網格節點之間使用NAT、例如為閘道節點提供公有IP位址。只有當您採用對網格中所有節點透明的通道應

用程式時、才支援使用NAT來橋接公共網路區段、亦即網格節點不需要知道公有IP位址。

StorageGRID 的網路特定需求

請遵循StorageGRID 每種類型的需求。

網路閘道和路由器

- 如果已設定、則指定網路的閘道必須位於特定網路的子網路內。
- 如果使用靜態定址設定介面、則必須指定0.00.0以外的閘道位址。
- 如果您沒有閘道、最佳做法是將閘道位址設定為網路介面的 IP 位址。

子網路

每個網路都必須連線至自己的子網路、而不會與節點上的任何其他網路重疊。

下列限制會在部署期間由Grid Manager強制執行。此處提供這些工具、可協助您進行部署前的網路規劃。

- 任何網路 IP 位址的子網路遮罩不得為 255.255.255.254 或 255.255.255.255 （ /31 或 /32 為 CIDR 表示法）。
- 由網路介面 IP 位址和子網路遮罩（ CIDR ）所定義的子網路、不能與在同一個節點上設定的任何其他介面子網路重疊。
- 請勿對任何節點的網格網路、管理網路或用戶端網路使用包含下列 IPv4 位址的子網路：
  - 192,168,130,101
  - 192,168,130,121
  - 192,168,131,101
  - 192,168,131,121
  - 192,168,130,102
  - 192,168,130,122
  - 192,168,131,102
  - 192,168,131,122
  - 198.51.100.2
  - 198.51.100.4

  例如，不要對任何節點的網格網路、管理網路或客戶端網路使用下列子網路範圍：

  - 192.168.130.0/24，因為此子網路範圍包含 IP 位址 192.168.130.101 和 192.168.130.102
  - 192.168.131.0/24，因為此子網路範圍包含 IP 位址 192.168.131.101 和 192.168.131.102
  - 198.51.100.0/24，因為此子網路範圍包含 IP 位址 198.51.100.2 和 198.51.100.4
- 每個節點的Grid Network子網路必須包含在GNSL中。
- 管理網路子網路不能與 Grid Network 子網路、 Client Network 子網路或 GNSL 中的任何子網路重疊。
- AESL 中的子網路不能與 GNSL 中的任何子網路重疊。

- 用戶端網路子網路不能重疊網格網路子網路、管理網路子網路、 GNSL 中的任何子網路、或是 AESL 中的任何子網路。

網格網路

- 在部署時、每個網格節點都必須附加至網格網路、而且必須能夠使用部署節點時指定的網路組態與主要管理節點通訊。
- 在正常的網格作業期間、每個網格節點都必須能夠透過網格網路與所有其他網格節點通訊。

> Grid Network必須在每個節點之間直接路由傳送。不支援節點之間的網路位址轉譯（NAT）。

- 如果網格網路由多個子網路組成、請將其新增至網格網路子網路清單（GNSL）。會在GNSL中的每個子網路的所有節點上建立靜態路由。
- 如果網格網路介面設定為主幹以支援VLAN介面、主幹原生VLAN必須是用於網格網路流量的VLAN。所有網格節點都必須透過主幹原生VLAN存取。

管理網路

管理網路為選用網路。如果您計畫設定管理網路、請遵循下列要求與準則。

管理網路的典型用途包括管理連線、 AutoSupport 、 KMS 、以及連線至關鍵伺服器的連線、例如 NTP 、 DNS 和 LDAP 、如果這些連線不是透過網格網路或用戶端網路提供。

> 只要能夠連線所需的網路服務和用戶端、每個節點都可以使用管理網路和Aesl。

> 您必須在管理網路上定義至少一個子網路、才能啟用來自外部子網路的傳入連線。在Aesl的每個子網路中、會自動在每個節點上產生靜態路由。

用戶端網路

用戶端網路為選用項目。如果您打算設定用戶端網路、請注意下列考量事項。

- 用戶端網路的設計可支援來自 S3 用戶端的流量。如果已設定、用戶端網路閘道會成為節點的預設閘道。
- 如果您使用用戶端網路、StorageGRID 只有在明確設定的負載平衡器端點上接受傳入用戶端流量、才能保護不受惡意攻擊的可靠性。請參閱。 "設定負載平衡器端點"
- 如果用戶端網路介面設定為主幹以支援VLAN介面、請考慮是否需要設定用戶端網路介面（eth2）。如果已設定、用戶端網路流量將會透過主幹原生VLAN（如交換器所設定）傳輸。

相關資訊

"變更節點網路組態"

部署特定的網路考量

StorageGRID Linux 部署的網路配置

為了提高效率、可靠性和安全性、StorageGRID 此功能可在Linux上執行、作為容器引擎的集合。在一個不需要與容器引擎相關的StorageGRID 網路組態設定的情況下、

將非連結裝置（例如VLAN或虛擬乙太網路（varth）配對）用於容器網路介面。將此裝置指定為節點組態檔中的網路介面。

> 請勿直接使用連結或橋接裝置做為容器網路介面。這樣做可能會因為在Container命名空間中使用含Bond和Bridge裝置的Macvlan時發生核心問題、而導致節點無法啟動。

查看"安裝說明"。

用於容器引擎部署的主機網路組態

在StorageGRID 容器引擎平台上開始進行功能性部署之前、請先判斷每個節點將使用哪些網路（Grid、管理、用戶端）。您必須確保每個節點的網路介面都設定在正確的虛擬或實體主機介面上、而且每個網路都有足夠的頻寬。

實體主機

如果您使用實體主機來支援網格節點：

- 確保所有主機都對每個節點介面使用相同的主機介面。此策略可簡化主機組態、並可在未來進行節點移轉。
- 取得實體主機本身的IP位址。

> 主機上的實體介面可由主機本身和主機上執行的一或多個節點使用。使用此介面指派給主機或節點的任何IP位址都必須是唯一的。主機和節點無法共用 IP 位址。

- 開啟主機所需的連接埠。
- 如果您打算在StorageGRID 支援中使用VLAN介面、主機必須有一個或多個主幹介面、才能存取所需的VLAN。這些介面可以以eth0、eth2或其他介面的形式傳送到節點容器。若要新增主幹或存取介面、請參閱下列內容：
  - **Linux**（安裝節點之前）：*建立節點組態檔*
  - **Linux**（安裝節點後）：*向節點新增中繼或存取介面*

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

建議的最低頻寬

下表針對每種類型的 StorageGRID 節點和每種類型的網路、提供最低 LAN 頻寬建議。您必須為每部實體或虛擬主機配置足夠的網路頻寬、以符合StorageGRID 您計畫在該主機上執行的所有節點數和類型的總頻寬需求。

節點類型	網路類型		
	網格	管理	用戶端
	• 最小 LAN 頻寬 *	管理	10 Gbps
1 Gbps	1 Gbps	閘道	10 Gbps

節點類型	網路類型		
1 Gbps	10 Gbps	儲存設備	10 Gbps
1 Gbps	10 Gbps	歸檔	10 Gbps

此表不包含存取共享儲存設備所需的SAN頻寬。如果您使用透過乙太網路存取的共享儲存設備（iSCSI或FCoE）、則應在每個主機上配置個別的實體介面、以提供足夠的SAN頻寬。為了避免出現瓶頸、特定主機的SAN頻寬應大致符合該主機上執行之所有儲存節點的Aggregate Storage Node網路頻寬。

請根據StorageGRID 您計畫在該主機上執行的各個節點數量和類型、使用表格來判斷每個主機上要配置的網路介面數量下限。

例如、若要在單一主機上執行一個管理節點、一個閘道節點和一個儲存節點：

- 連接管理節點上的網格和管理網路（需要10 + 1 = 11 Gbps）
- 在閘道節點上連接網格和用戶端網路（需要10 + 10 = 20 Gbps）
- 連接儲存節點上的網格網路（需要10 Gbps）

在此案例中、您應提供至少11 + 20 + 10 = 41 Gbps的網路頻寬、 可由兩個40 Gbps介面或五個10 Gbps介面滿足、這些介面可能會集合成主幹、然後由三個以上的VLAN共用、這些VLAN會將Grid、Admin和用戶端子網路裝載到包含主機的實體資料中心。

有關在StorageGRID叢集中的主機上設定實體和網路資源以準備StorageGRID部署的一些建議方法，請參閱"設定主機網路"。

適用於平台服務和雲端儲存資源池的網路和連接埠

如果您計畫使用StorageGRID 支援不支援的平台服務或雲端儲存資源池、則必須設定網格網路和防火牆、以確保能夠到達目的地端點。

平台服務的網路功能

如和"管理平台服務"所述"管理租戶平台服務"、平台服務包括提供搜尋整合、事件通知和 CloudMirror 複寫的外部服務。

平台服務需要從儲存節點存取、而儲存節點則是StorageGRID 將此項目裝載到外部服務端點。提供存取的範例包括：

- 在具有ADC服務的儲存節點上、使用Aesl項目來設定唯一的管理網路、這些項目會路由傳送至目標端點。
- 仰賴用戶端網路提供的預設路由。如果您使用預設路由、則可以使用"不受信任的用戶端網路功能"來限制傳入連線。

雲端儲存資源池的網路功能

雲端儲存集區也需要儲存節點存取所用外部服務（例如 Amazon S3 Glacier 或 Microsoft Azure Blob Storage）提供的端點。如需相關資訊，請參閱 "什麼是雲端儲存池"。

平台服務與雲端儲存資源池的連接埠

根據預設、平台服務和雲端儲存資源池通訊會使用下列連接埠：

- **80** ：適用於以開頭的端點 URI `http`
- **443** ：適用於以開頭的端點 URI `https`

建立或編輯端點時、可以指定不同的連接埠。請參閱。 "網路連接埠參考"

如果您使用非透明 Proxy 伺服器、也必須"設定儲存Proxy設定"允許訊息傳送至外部端點、例如網際網路上的端點。

VLAN及平台服務與雲端儲存資源池

您無法將 VLAN 網路用於平台服務或雲端儲存池。目的地端點必須可透過Grid、Admin或Client Network存取。

StorageGRID 設備節點的網路配置

您可以設定StorageGRID 使用連接埠綁定模式的網路連接埠、以符合處理量、備援和容錯移轉的需求。

您可以在固定或集合式連結模式中設定適用於連接至Grid Network和Client Network的10/25-GbE連接埠StorageGRID 。

1-GbE管理網路連接埠可設定為獨立或主動備份模式、以連線至管理網路。

請參閱有關應用裝置連接埠連結模式的資訊：

- "連接埠連結模式（ SG6160 ）"
- "連接埠連結模式（ SGF6112 ）"
- "連接埠連結模式（ SG6000-CN 控制器）"
- "連接埠連結模式（ SG5800 控制器）"
- "連接埠連結模式（ E5700SG 控制器）"
- "連接埠連結模式（ SG110 和 SG1100 ）"
- "連接埠連結模式（ SG100 和 SG1000 ）"

StorageGRID 的網路安裝與資源配置

您必須瞭解在節點部署和網格組態期間、如何使用Grid Network以及選用的管理和用戶端網路。

節點的初始部署

當您第一次部署節點時、必須將節點附加至Grid Network、並確保其具有主要管理節點的存取權。如果網格網路已隔離、您可以在主要管理節點上設定管理網路、以便從網格網路外部進行組態和安裝存取。

在部署期間、已設定閘道的Grid Network會成為節點的預設閘道。預設閘道可讓個別子網路上的網格節點在設定網格之前、先與主要管理節點通訊。

如有必要、也可將包含NTP伺服器或需要存取Grid Manager或API的子網路設定為網格子網路。

使用主要管理節點自動登錄節點

部署節點之後、他們會使用Grid Network向主要管理節點註冊。然後、您可以使用 Grid Manager 、 Python 指令碼或安裝 API 來設定網格、 `configure-storagegrid.py`並核准已登錄的節點。在網格組態期間、您可以設定多個網格子網路。完成網格組態時、將會在每個節點上建立經由網格網路閘道通往這些子網路的靜態路由。

停用管理網路或用戶端網路

如果您想要停用管理網路或用戶端網路、您可以在節點核准程序期間從這些網路或用戶端網路移除組態、或是在安裝完成後使用變更 IP 工具（請參閱"設定IP位址"）。

StorageGRID 的安裝後準則

完成網格節點部署與組態之後、請遵循下列原則進行DHCP定址和網路組態變更。

- 如果使用DHCP來指派IP位址、請為使用中網路上的每個IP位址設定DHCP保留。

  您只能在部署階段設定DHCP。您無法在組態期間設定 DHCP 。

  > 當網格網路組態由 DHCP 變更時、節點會重新開機、如果 DHCP 變更同時影響多個節點、這可能會導致中斷運作。

- 如果您想要變更網格節點的IP位址、子網路遮罩和預設閘道、則必須使用變更IP程序。請參閱。 "設定IP位址"
- 如果您進行網路組態變更（包括路由和閘道變更）、則可能會失去與主要管理節點和其他網格節點的用戶端連線。視所套用的網路變更而定、您可能需要重新建立這些連線。

網路連接埠參考

StorageGRID 的內部網格節點通訊

StorageGRID 內部防火牆允許連入網格網路上的特定連接埠。負載平衡器端點所定義的連接埠也接受連線。

> NetApp建議您在網格節點之間啟用網際網路控制訊息傳輸協定（ICMP）流量。當無法到達網格節點時、允許 ICMP 流量可改善容錯移轉效能。

除了ICMP和表中所列的連接埠之外、StorageGRID VMware還使用虛擬路由器備援傳輸協定（VRP）。VRP是一種使用IP傳輸協定編號112的網際網路傳輸協定。僅在單點傳播模式中使用VRP。StorageGRID僅在設定時才需要 VRRP "高可用度群組"。

Linux型節點準則

如果企業網路策略限制對任何這些連接埠的訪問，您可以在部署時使用部署設定參數重新對應連接埠。有關連接埠重新映射和部署配置參數的更多信息，請參閱"在基於軟體的節點上安裝StorageGRID"。

對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"移除裸機主機上的連接埠重新對應"。

VMware型節點的準則

只有在需要定義VMware網路外部的防火牆限制時、才需設定下列連接埠。

如果企業網路策略限制對任何這些連接埠的訪問，您可以在使用 VMware vSphere Web Client 部署節點時重新對應端口，或在自動化網格節點部署時使用設定檔設定重新對應連接埠。有關連接埠重新映射和部署配置參數的更多信息，請參閱"在 VMware 上安裝StorageGRID"。

對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"移除裸機主機上的連接埠重新對應"。

應用裝置節點準則

如果企業網路原則限制存取任何這些連接埠、您可以使用StorageGRID 《不可靠設備安裝程式》重新對應連接埠。請參閱。 "選用：重新對應應用裝置的網路連接埠"

對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"刪除StorageGRID設備上的連接埠重新映射"。

內部連接埠**StorageGRID**

連接埠	**TCP**或**udp**	寄件者	至	詳細資料
22	TCP	主要管理節點	所有節點	在維護程序中、主要管理節點必須能夠使用連接埠22上的SSH與所有其他節點通訊。允許來自其他節點的SSH流量為選用功能。
80	TCP	應用裝置	主管理節點與非主管理節點	由不受應用裝置使用StorageGRID 、可與主要管理節點進行通訊、以開始安裝。
123	UDP	所有節點	所有節點	網路時間傳輸協定服務。每個節點都會使用NTP與其他節點同步時間。
443	TCP	所有節點	主管理節點與非主管理節點	用於在安裝和其他維護程序期間、將狀態傳達給主要管理節點。
1055	TCP	所有節點	主管理節點與非主管理節點	用於安裝、擴充、恢復和其他維護程序的內部流量。
1139	TCP	儲存節點	儲存節點	儲存節點之間的內部流量。

連接埠	**TCP**或**udp**	寄件者	至	詳細資料
1501	TCP	所有節點	具有ADC的儲存節點	報告、稽核及組態內部流量。
1502	TCP	所有節點	儲存節點	S3相關的內部流量。
1504	TCP	所有節點	管理節點	NMS服務報告與組態內部流量。
1505	TCP	所有節點	管理節點	AMS服務內部流量。
1506	TCP	所有節點	所有節點	伺服器狀態內部流量。
1507	TCP	所有節點	閘道節點	負載平衡器內部流量。
1508	TCP	所有節點	主要管理節點	組態管理內部流量：
1511	TCP	所有節點	儲存節點	中繼資料內部流量。
5353	UDP	所有節點	所有節點	提供用於全網格 IP 變更以及安裝、擴充和復原期間的主要管理節點發現的多重播送 DNS (mDNS) 服務。 注意：配置此連接埠是可選的。
7001	TCP	儲存節點	儲存節點	Cassandra TLS節點間叢集通訊。
7443	TCP	所有節點	主管理節點與非主管理節點	用於安裝、擴充、恢復、其他維護程序和錯誤報告的內部流量。
8011	TCP	所有節點	主管理節點與非主管理節點	用於安裝、擴充、恢復和其他維護程序的內部流量。
8443	TCP	主要管理節點	應用裝置節點	與維護模式程序相關的內部流量。
9042	TCP	儲存節點	儲存節點	Cassandra用戶端連接埠。
9999	TCP	所有節點	所有節點	多項服務的內部流量。包括維護程序、指標和網路更新。
10226	TCP	儲存節點	主要管理節點	由 StorageGRID 應用裝置使用、將 AutoSupport 套件從 E 系列 SANtricity 系統管理員轉寄至主要管理節點。

連接埠	TCP或udp	寄件者	至	詳細資料
10342	TCP	所有節點	主管理節點與非主管理節點	用於安裝、擴充、恢復和其他維護程序的內部流量。
18000	TCP	所有節點	具有ADC的儲存節點	帳戶服務內部流量。
18001	TCP	所有節點	具有ADC的儲存節點	身分識別聯盟內部流量。
18002	TCP	所有節點	儲存節點	與物件傳輸協定相關的內部API流量。
18003	TCP	所有節點	具有ADC的儲存節點	平台服務內部流量。
18017	TCP	管理/儲存節點	儲存節點	Cloud Storage Pool的Data Mover服務內部流量。
18019	TCP	所有節點	所有節點	用於擦除編碼和複製的區塊服務內部流量
18082	TCP	管理/儲存節點	儲存節點	S3相關的內部流量。
18086	TCP	所有節點	儲存節點	與 LDR 服務相關的內部流量。
18200	TCP	管理/儲存節點	儲存節點	有關用戶端要求的其他統計資料。
19000	TCP	管理/儲存節點	具有ADC的儲存節點	Keystone服務內部流量。

相關資訊

"外部通訊"

StorageGRID 的外部通訊

用戶端需要與網格節點通訊、才能擷取和擷取內容。使用的連接埠取決於所選的物件儲存傳輸協定。用戶端需要存取這些連接埠。

限制存取連接埠

如果企業網路原則限制存取任何連接埠、您可以執行下列其中一項：

- 用於"負載平衡器端點"允許存取使用者定義的連接埠。

- 部署節點時重新對應連接埠。不過、您不應該重新對應負載平衡器端點。請參閱 StorageGRID 節點的連接埠重新對應相關資訊：

> 對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"刪除StorageGRID設備上的連接埠重新映射"或者"移除裸機主機上的連接埠重新對應"。

- "在 Red Hat Enterprise Linux 上重新對應 StorageGRID 的連接埠金鑰"
- "重新對應 VMware 上 StorageGRID 的連接埠"
- "選用：重新對應應用裝置的網路連接埠"

用於外部通訊的連接埠

下表顯示用於流量進入節點的連接埠。

> 此清單不包含可能設定為"負載平衡器端點"的連接埠。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
22	TCP	SSH	服務筆記型電腦	所有節點	包含控制台步驟的過程需要 SSH 或控制台存取。或者，您可以使用連接埠 2022 而不是 22。 注意：僅當需要啟用 SSH 存取以進行某些維護操作時才需要此連接埠。
25	TCP	SMTP	管理節點	電子郵件伺服器	用於警示和電子郵件AutoSupport 導向的功能。您可以使用「電子郵件伺服器」頁面覆寫預設的連接埠設定25。
53	TCP/ udp	DNS	所有節點	DNS 伺服器	用於 DNS 。
67	UDP	DHCP	所有節點	DHCP 服務	（可選）用於支援DHCP型網路組態。對於靜態設定的網格、則不會執行dhClient服務。
68	UDP	DHCP	DHCP 服務	所有節點	（可選）用於支援DHCP型網路組態。對於使用靜態IP位址的網格、dhClient服務不會執行。
80	TCP	HTTP	瀏覽器	管理節點	連接埠80會針對管理節點使用者介面重新導向至連接埠443。
80	TCP	HTTP	瀏覽器	應用裝置	連接埠80重新導向至StorageGRID 連接埠8443、以供使用。
80	TCP	HTTP	具有ADC的儲存節點	AWS	用於傳送至 AWS 或其他使用 HTTP 的外部服務的平台服務訊息。建立端點時、租戶可以覆寫預設的 HTTP 連接埠設定 80 。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
80	TCP	HTTP	儲存節點	AWS	雲端儲存池會將要求傳送至使用 HTTP 的 AWS 目標。網格管理員在設定雲端儲存池時、可以覆寫預設的 HTTP 連接埠設定 80 。
123	UDP	NTP	主要NTP節點	外部NTP	網路時間傳輸協定服務。選取為主要NTP來源的節點也會將時鐘時間與外部NTP時間來源同步。
161	TCP/ udp	SNMP	SNMP 用戶端	所有節點	用於SNMP輪詢。所有節點均提供基本資訊；管理節點也提供警示資料。設定時、預設為udp連接埠161。 *附註：*此連接埠僅為必要、且僅在設定SNMP時於節點防火牆上開啟。如果您打算使用SNMP、可以設定替代連接埠。 *附註：*如需使用SNMP搭配StorageGRID 使用功能的相關資訊、請聯絡您的NetApp客戶代表。
162	TCP/ udp	SNMP通知	所有節點	通知目的地	傳出SNMP通知和設陷預設為UDP連接埠162。 *附註：*此連接埠僅在啟用SNMP且已設定通知目的地時才需要。如果您打算使用SNMP、可以設定替代連接埠。 *附註：*如需使用SNMP搭配StorageGRID 使用功能的相關資訊、請聯絡您的NetApp客戶代表。
389	TCP/ udp	LDAP	具有ADC的儲存節點	Active Directory / LDAP	用於連線至Active Directory或LDAP伺服器以進行身分識別聯盟。
443	TCP	HTTPS	瀏覽器	管理節點	由 Web 瀏覽器和管理 API 用戶端用來存取網格管理員和租用戶管理員。 注意：如果您關閉網格管理器連接埠 443 或 8443，則目前連接到被封鎖連接埠的任何使用者（包括您）都將失去對網格管理員的存取權限，除非他們的 IP 位址已新增至特權位址清單中。參考"設定防火牆控制項"配置特權IP位址。
443	TCP	HTTPS	管理節點	Active Directory	如果啟用單一登入（SSO）、則管理節點會使用此選項來連線至Active Directory。
443	TCP	HTTPS	具有ADC的儲存節點	AWS	用於傳送至 AWS 或其他使用 HTTPS 的外部服務的平台服務訊息。建立端點時、租戶可以覆寫預設的 HTTP 連接埠設定 443 。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
443	TCP	HTTPS	儲存節點	AWS	雲端儲存池會將要求傳送至使用 HTTPS 的 AWS 目標。網格管理員在設定雲端儲存池時、可以覆寫預設的 HTTPS 連接埠設定 443 。
636	TCP/ udp	LDAP	具有ADC的儲存節點	Active Directory / LDAP	用於連線至Active Directory或LDAP伺服器以進行身分識別聯盟。
5353	UDP	mDNS	所有節點	所有節點	提供用於全網格 IP 變更以及安裝、擴充和復原期間的主要管理節點發現的多重播送 DNS (mDNS) 服務。 注意：配置此連接埠是可選的。
5696	TCP	KMIP	應用裝置	公里	金鑰管理互通性傳輸協定（KMIP）、從設定為節點加密的應用裝置、到金鑰管理伺服器（KMS）的外部流量、除非StorageGRID 在《與眾不同的應用程式安裝程式》的KMS組態頁面上指定不同的連接埠。
8443	TCP	HTTPS	瀏覽器	管理節點	選修的。由 Web 瀏覽器和管理 API 用戶端用來存取網格管理員。可用於分離網格管理器和租戶管理器通訊。 注意：如果您關閉網格管理器連接埠 443 或 8443，則目前連接到被封鎖連接埠的任何使用者（包括您）都將失去對網格管理員的存取權限，除非他們的 IP 位址已新增至特權位址清單中。參考"設定防火牆控制項"配置特權IP位址。
8443	TCP	HTTPS	瀏覽器	應用裝置	由 Web 瀏覽器和管理 API 用戶端用於存取StorageGRID Appliance Installer。 注意：連接埠 443 重定向到StorageGRID設備安裝程式的連接埠 8443。
9022	TCP	SSH	服務筆記型電腦	應用裝置	允許以StorageGRID 預先組態模式存取不支援和疑難排解功能。在網格節點之間或正常作業期間、不需要存取此連接埠。
9091	TCP	HTTPS	外部Grafana服務	管理節點	由外部Grafana服務所使用、可安全存取StorageGRID 《The》《The》《The》《The》《The》《The》》《The *附註：*此連接埠僅在啟用憑證型Prometheus存取時才需要。

連接埠	TCP或udp	傳輸協定	寄件者	至	詳細資料
9092	TCP	卡夫卡	具有ADC的儲存節點	Kafka 叢集	用於傳送至 Kafka 叢集的平台服務訊息。建立端點時、租戶可以覆寫預設的 Kafka 連接埠設定 9092 。
9443	TCP	HTTPS	瀏覽器	管理節點	選修的。由 Web 瀏覽器和管理 API 用戶端用來存取租用戶管理員。可用於分離網格管理器和租戶管理器通訊。
18082	TCP	HTTPS	S3用戶端	儲存節點	S3 用戶端流量直接傳輸至儲存節點（ HTTPS ）。
18084	TCP	HTTP	S3用戶端	儲存節點	S3 用戶端流量直接傳輸至儲存節點（ HTTP ）。
23000-23999	TCP	HTTPS	來源網格上的所有節點都可進行跨網格複寫	目的地網格上的管理節點和閘道節點、用於跨網格複寫	此連接埠範圍保留給網格同盟連線。指定連線中的兩個網格都使用相同的連接埠。

StorageGRID 快速入門

請依照這些高階步驟來設定及使用任何 StorageGRID 系統。

1 學習、規劃及收集資料

與 NetApp 客戶代表合作、瞭解選項並規劃新的 StorageGRID 系統。請思考以下類型的問題：

- 您預期最初和之後會儲存多少物件資料？
- 您需要多少個網站？
- 每個站台需要多少個節點、以及哪些類型的節點？
- 您會使用哪些 StorageGRID 網路？
- 誰會使用您的網格來儲存物件？他們會使用哪些應用程式？
- 您是否有任何特殊的安全性或儲存需求？
- 您是否需要遵守任何法律或法規要求？

您也可以選擇與 NetApp 專業服務顧問合作、存取 NetApp ConfigBuilder 工具、以完成組態工作簿、以便在安裝和部署新系統時使用。您也可以使用此工具來協助自動化任何 StorageGRID 應用裝置的組態。請參閱。 "自動化應用裝置的安裝與組態"

審查 "深入瞭解StorageGRID" 和 "網路準則"。

2 安裝節點

StorageGRID 系統由個別的硬體型和軟體型節點所組成。您必須先為每個應用裝置節點安裝硬體、然後設定每個 Linux 或 VMware 主機。

若要完成安裝、請在每個應用裝置或軟體主機上安裝 StorageGRID 軟體、並將節點連接至網格。在此步驟中、您會提供 NTP 和 DNS 伺服器的站台和節點名稱、子網路詳細資料和 IP 位址。

瞭解如何：

- "安裝應用裝置硬體"
- "在基於軟體的節點上安裝StorageGRID"

3 登入並檢查系統健全狀況

網格安裝完成後，您可以登入網格管理器。從那裡，您可以查看新系統的整體健康狀況，啟用AutoSupport和警報電子郵件，並設定 S3 端點網域。

瞭解如何：

- "登入Grid Manager"
- "監控系統健全狀況"
- "設定AutoSupport 功能"
- "設定警示的電子郵件通知"
- "設定 S3 端點網域名稱"

4 設定與管理

您需要為新的 StorageGRID 系統執行的組態工作、取決於您使用網格的方式。您至少需要設定系統存取、使用 FabricPool 和 S3 精靈、以及管理各種儲存和安全性設定。

瞭解如何：

- "控制StorageGRID 功能存取"
- "使用 S3 設定精靈"
- "使用 FabricPool 設定精靈"
- "管理安全性"
- "系統強化"

5 設定 **ILM**

您可以設定由一或多個 ILM 規則組成的資訊生命週期管理（ ILM ）原則、來控制 StorageGRID 系統中每個物件的放置和持續時間。ILM 規則會指示 StorageGRID 如何建立及散佈物件資料複本、以及如何隨時間管理這些複本。

瞭解如何："使用ILM管理物件"

6 使用 StorageGRID

完成初始組態後、 StorageGRID 租戶帳戶可以使用 S3 用戶端應用程式來擷取、擷取及刪除物件。

瞭解如何：

- "使用租戶帳戶"
- "使用 S3 REST API"

7 監控和疑難排解

當系統啟動並執行時、您應該定期監控其活動、並疑難排解及解決任何警示。您可能也想要設定外部 Syslog 伺服器、使用 SNMP 監控或收集其他資料。

瞭解如何：

- "監控 StorageGRID"
- "疑難排解 StorageGRID"

8 擴充、維護及恢復

您可以新增節點或站台來擴充系統的容量或功能。您也可以執行各種維護程序、以從故障中恢復、或讓 StorageGRID 系統保持最新狀態並有效率地執行。

瞭解如何：

- "展開網格"
- "維護您的網格"
- "恢復節點"

安裝、升級及 Hotfix StorageGRID

安裝 StorageGRID 節點

了解 StorageGRID 設備硬體

前往 "StorageGRID 應用裝置文件"了解如何安裝、設定和維護 StorageGRID 儲存設備和服務設備。

安裝軟體型節點

在基於軟體的節點上安裝StorageGRID 的快速入門

請依照這些進階步驟安裝 Linux 或 VMware StorageGRID節點。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

1 準備

- 瞭解 "架構與網路拓撲StorageGRID"。
- 瞭解的細節"網路連線StorageGRID"。
- 收集並準備"必要資訊與資料"。
- （僅限 VMware）安裝與設定"VMware vSphere Hypervisor 、 vCenter 和 ESX 主機"。
- 準備所需的"CPU 和 RAM"。
- 提供"儲存與效能需求"。
- （僅限 Linux）"準備 Linux 伺服器"將託管您的StorageGRID節點。

2 部署

部署網格節點。當您部署網格節點時、這些節點會建立為StorageGRID 整個系統的一部分、並連線至一或多個網路。

- （僅限 Linux）若要在步驟 1 中準備的主機上部署基於軟體的網格節點，請使用 Linux 命令列和"節點組態檔案"。
- （僅限 VMware）使用 VMware vSphere Web Client、.vmdk 檔案和一組 .ovf 檔案範本來"將軟體型節點部署為虛擬機器（ VM ）"在步驟 1 中準備的伺服器上。
- 若要部署 StorageGRID 應用裝置節點、請遵循 "硬體安裝快速入門"。

3 組態

當所有節點都已部署完畢時、請使用 Grid Manager 來"設定網格並完成安裝"。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

Linux

為了節省時間並提供一致性、您可以自動化 StorageGRID 主機服務的安裝和網格節點的組態。

- 使用 Ansible 、 Puppet 或 Chef 等標準協調架構來自動化：
  - Linux 的安裝
  - 網路與儲存設備的組態
  - 安裝容器引擎和 StorageGRID 主機服務
  - 部署虛擬網格節點

  看"自動化StorageGRID 安裝及設定整套的支援服務" 。
- 部署網格節點後，"自動化 StorageGRID 系統的組態"使用安裝檔案中提供的 Python 設定腳本。
- "自動化設備網格節點的安裝與組態"
- 如果您是 StorageGRID 部署的進階開發人員，請使用來自動化網格節點的安裝"安裝 REST API"。

VMware

為了節省時間並提供一致性、您可以自動化網格節點的部署和組態、以及 StorageGRID 系統的組態。

- "使用 VMware vSphere 自動化網格節點部署"。
- 部署網格節點之後、"自動化 StorageGRID 系統的組態"請使用安裝歸檔文件中提供的 Python 組態指令碼。
- "自動化設備網格節點的安裝與組態"
- 如果您是 StorageGRID 部署的進階開發人員，請使用來自動化網格節點的安裝"安裝 REST API"。

規劃並準備在基於軟體的節點上進行安裝

StorageGRID 所需的資訊和資料

安裝 StorageGRID 之前、請收集並準備所需的資訊和資料。

必要資訊

網路計畫

您打算連接至每個 StorageGRID 節點的網路。StorageGRID 支援多個網路、提供流量分離、安全性和管理便利性。

請參閱 "網路準則"。

網路資訊

指派給每個網格節點的 IP 位址、以及 DNS 和 NTP 伺服器的 IP 位址。

網格節點的伺服器

識別一組伺服器（實體、虛擬或兩者）、這些伺服器集合在一起、提供足夠的資源來支援StorageGRID 您計畫部署的各個節點數量和類型。

如果您的 StorageGRID 安裝將不會使用 StorageGRID 應用裝置（硬體）儲存節點、則必須使用硬體 RAID 儲存設備搭配電池備援寫入快取（ BBWC ）。StorageGRID 不支援使用虛擬儲存區域網路（ VSAN ）、軟體 RAID 或無 RAID 保護。

節點遷移（如果需要，僅限 **Ubuntu** 和 **Debian**）

"節點移轉需求"如果您想在不中斷任何服務的情況下、於實體主機上執行排程維護、請瞭解。

相關資訊

"NetApp 互通性對照表工具"

必要資料

NetApp StorageGRID 產品授權

您必須擁有有效且經過數位簽署的NetApp授權。

非正式作業授權可用於測試和概念驗證網格、包含在 StorageGRID 安裝歸檔中。

安裝歸檔**StorageGRID**

"下載 StorageGRID 安裝歸檔文件並解壓縮檔案"。

服務筆記型電腦

此系統是透過維修用筆記型電腦來安裝。StorageGRID

服務型筆記型電腦必須具備：

- 網路連接埠
- SSH用戶端（例如Putty）
- "支援的網頁瀏覽器"

本文檔**StorageGRID**

- "版本資訊"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。
- "關於管理StorageGRID 功能的說明"

下載並解壓縮**StorageGRID** 安裝檔案

您必須下載StorageGRID 安裝檔案庫、並擷取所需的檔案。您也可以手動驗證安裝套件中的檔案。

步驟

1. 前往 "NetApp下載頁StorageGRID 面"。
2. 選取下載最新版本的按鈕、或從下拉式功能表中選取其他版本、然後選取*執行*。
3. 以您NetApp帳戶的使用者名稱和密碼登入。
4. 如果出現「 Caution/MustRead 」說明、請閱讀並選取核取方塊。

   安裝StorageGRID 完此版本的更新後、您必須套用所有必要的修補程式。如需詳細資訊、請參閱"修復與維護指示中的修復程序程序"

5. 閱讀終端使用者授權合約、選取核取方塊、然後選取 * 接受並繼續 * 。
6. 在 安裝**StorageGRID** 欄位中，選擇適合您基於軟體的節點類型的 .tgz 或 .zip 安裝檔案：RHEL、Ubuntu 或 Debian 或 VMware。

   如果您在服務筆記型電腦上執行 Windows 、請使用 `.zip`此檔案。

7. 儲存安裝歸檔。
8. 程式碼簽章驗證在 Linux 節點上是手動的。或者，如果您需要驗證安裝檔案：
   a. 下載 StorageGRID 程式碼簽章驗證套件。此套件的檔案名稱使用格式 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`、其中 `<version-number>`是 StorageGRID 軟體版本。
   b. 依照步驟"手動驗證安裝檔案"。
9. 從安裝歸檔中擷取檔案。
10. 選擇您需要的檔案。

    您需要的檔案取決於您規劃的網格拓撲、以及 StorageGRID 系統的部署方式。

    表中列出的路徑是相對於擷取安裝歸檔所安裝的最上層目錄。

紅帽企業版

路徑和檔案名稱	說明
	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	不提供產品任何支援權利的免費授權。
	用於在 RHEL 主機上安裝 StorageGRID 節點映像的 RPM 套件。
	用於在 RHEL 主機上安裝 StorageGRID 主機服務的 RPM 套件。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行 Ping 聯合整合。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	範例 Ansible 角色和教戰手冊、用於設定 StorageGRID 容器部署的 RHEL 主機。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。

路徑和檔案名稱	說明
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

Ubuntu或DEBIAN

路徑和檔案名稱	說明
每個問題/讀我檔案	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	非正式作業的NetApp授權檔案、可用於測試及概念驗證部署。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝不含節點的映像。
	檔案的 MD5 Checksum `/debs/storagegrid-webscale-images-version-SHA.deb` 。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝支援功能主機服務。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行 Ping 聯合整合。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。

路徑和檔案名稱	說明
/扣款/額外費用/可選	範例Ansible角色與方針、可用來設定Ubuntu或Debian主機以StorageGRID 進行列舉容器部署。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
/debs/storagegRID -soaut-azure.js	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

VMware

路徑和檔案名稱	說明
/vSphere/README	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	不提供產品任何支援權利的免費授權。
/vSphere/NetApp-SG-version -SHA-vmdk	用來做為建立網格節點虛擬機器範本的虛擬機器磁碟檔案。
/vSphere/vSphere-primer-admin.OVF ./vSphere/vSphere-prime-admin.mf	開放式虛擬化格式模板文件(`.mf`）(`.ovf`和清單文件），用於部署主管理節點。
/vSphere/vSphere-non-prime-admin.OVF ./vSphere/vSphere-non-prime-admin.mf	模板文件(`.mf`）(`.ovf`和清單文件），用於部署非主管理員節點。
/vSphere/vSphere-gateway.OVF ./vSphere/vSphere-gateway.mf	模板文件(`.mf`）(`.ovf`和清單文件），用於部署網關節點。
/vSphere/vSphere-storage。OVF ./vSphere/vSphere-storage	模板文件(`.mf`）(`.ovf`和清單文件），用於部署基於虛擬機的存儲節點。
部署指令碼工具	說明

路徑和檔案名稱	說明
	Bash Shell指令碼、用於自動化虛擬網格節點的部署。
	用於指令碼的範例組態檔 `deploy-vsphere-ovftool.sh`。
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入（ SSO ）時、您可以使用 Python 指令碼範例登入 Grid Management API 。您也可以使用此指令碼來進行 Ping 聯合整合。
/vSphere/configure-storagegrid、same.json	用於指令碼的範例組態檔 `configure-storagegrid.py`。
/vSphere/configure-storagegrid、blank.json	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
/vSphere/Extras / API架構	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

驗證 **StorageGRID** 安裝檔案

如有必要、您可以手動驗證 StorageGRID 安裝歸檔中的檔案。

開始之前

你有"已下載驗證套件"從 "NetApp下載頁StorageGRID 面"。

步驟

1. 從驗證套件擷取成品：

```
tar -xf StorageGRID_12.1.0_Code_Signature_Verification_Package.tar.gz
```

2. 確保擷取這些假影：
   - 葉證書： `Leaf-Cert.pem`
   - 憑證鏈結： `CA-Int-Cert.pem`
   - 時間戳記回應鏈： `TS-Cert.pem`
   - Checksum 檔案： `sha256sum`
   - Checksum 簽章： `sha256sum.sig`
   - 時間戳記回應檔案： `sha256sum.sig.tsr`
3. 使用鏈結來確認葉憑證有效。
   - 範例 * ： `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`
   - 預期輸出 * ： `Leaf-Cert.pem: OK`
4. 如果步驟 *2* 因為過期的葉憑證而失敗、請使用 `tsr`檔案來驗證。
   - 範例 * ： `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`
   - 預期輸出包括 * ： `Verification: OK`
5. 從葉憑證建立公開金鑰檔案。
   - 範例 * ： `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`
   - 預期輸出 * ： *none*
6. 使用公開金鑰來對照驗證 `sha256sum`檔案 `sha256sum.sig`。
   - 範例 * ： `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`
   - 預期輸出 * ： `Verified OK`
7. 對照新建立的校驗和來驗證 `sha256sum`檔案內容。
   - 範例 * ： `sha256sum -c sha256sum`
   - 預期輸出 * ： *<filename>*: OK
     <filename> 是您下載的歸檔檔案名稱。
8. "完成其餘步驟"從安裝檔案中提取並選擇適當的文件。

StorageGRID 的軟體需求

您可以使用虛擬機器來裝載任何類型的 StorageGRID 節點。每個網格節點都需要一部虛擬機器。

紅帽企業版

要在 RHEL 上安裝StorageGRID ，您必須安裝一些第三方軟體包。某些支援的 Linux 發行版預設不包含這些軟體包。 StorageGRID安裝測試的軟體包版本包括本頁列出的版本。

如果您選取需要這些套件之一的 Linux 發佈套件和容器執行階段安裝選項、但 Linux 發佈套件並不會自動安裝這些套件、請安裝此處列出的其中一個版本（如果您的供應商或 Linux 發佈套件的支援廠商提供）。否則、請使用廠商提供的預設套件版本。

所有安裝選項都需要使用 Podman 或 Docker 。請勿同時安裝兩個套件。只安裝安裝選項所需的套件。

> 將 Docker 作為僅限軟體部署的容器引擎的支援已過時。Docker 將在未來版本中以另一個 Container 引擎取代。

測試的 **Python** 版本

- 3.5.2-2
- 3.6.8-2.
- 3.6.8-38.
- 3.6.9-1.
- 3.7.3-1.
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2.
- 3.9.16-1.
- 3.10.6-1.
- 3.11.2-6.

已測試的 **Podman** 版本

- 3.2.3-0
- 3.4.4+DS1
- 4.1.1-7.
- 4.2.0-11.
- 4.3.1+DS1-8+B1
- 4.4.1-8.
- 4.4.1-12.

測試的 **Docker** 版本

> Docker 支援已過時、將在未來版本中移除。

- Docker CE 20.10.7
- Docker CE 20.10.20-3

- Docker CE 23.0-1
- Docker CE 24.0.2-1
- Docker CE 24.0.4-1
- Docker CE 24.0.5-1
- Docker CE 24.0.7-1
- 1.5-2

Ubuntu與DEBIAN

若要在 Ubuntu 或 Debian 上安裝 StorageGRID 、您必須安裝一些協力廠商軟體套件。部分支援的 Linux 套裝作業系統預設不包含這些套件。StorageGRID 安裝所測試的軟體套件版本包括本頁所列的版本。

如果您選取需要這些套件之一的 Linux 發佈套件和容器執行階段安裝選項、但 Linux 發佈套件並不會自動安裝這些套件、請安裝此處列出的其中一個版本（如果您的供應商或 Linux 發佈套件的支援廠商提供）。否則、請使用廠商提供的預設套件版本。

所有安裝選項都需要使用 Podman 或 Docker 。請勿同時安裝兩個套件。只安裝安裝選項所需的套件。

> 將 Docker 作為僅限軟體部署的容器引擎的支援已過時。Docker 將在未來版本中以另一個 Container 引擎取代。

測試的 **Python** 版本

- 3.5.2-2
- 3.6.8-2.
- 3.6.8-38.
- 3.6.9-1.
- 3.7.3-1.
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2.
- 3.9.16-1.
- 3.10.6-1.
- 3.11.2-6.

已測試的 **Podman** 版本

- 3.2.3-0
- 3.4.4+DS1
- 4.1.1-7.
- 4.2.0-11.
- 4.3.1+DS1-8+B1
- 4.4.1-8.
- 4.4.1-12.

測試的 **Docker** 版本

Docker 支援已過時、將在未來版本中移除。

- Docker CE 20.10.7
- Docker CE 20.10.20-3
- Docker CE 23.0-1
- Docker CE 24.0.2-1
- Docker CE 24.0.4-1
- Docker CE 24.0.5-1
- Docker CE 24.0.7-1
- 1.5-2

VMware

VMware vSphere 虛擬機器管理程式

您必須在準備好的實體伺服器上安裝VMware vSphere Hypervisor。安裝VMware軟體之前、必須正確設定硬體（包括韌體版本和BIOS設定）。

- 視需要在Hypervisor中設定網路功能、以支援StorageGRID 您安裝的整個作業系統的網路功能。

  "網路準則"

- 確保資料存放區足夠大、足以容納裝載網格節點所需的虛擬機器和虛擬磁碟。
- 如果您建立多個資料存放區、請命名每個資料存放區、以便在建立虛擬機器時、輕鬆識別每個網格節點要使用的資料存放區。

ESX 主機設定需求

您必須在每個ESX主機上正確設定網路時間傳輸協定（NTP）。如果主機時間不正確、可能會產生負面影響、包括資料遺失。

VMware 配置要求

在部署 StorageGRID 節點之前、您必須先安裝和設定 VMware vSphere 和 vCenter 。

如需 VMware vSphere Hypervisor 和 VMware vCenter Server 軟體的支援版本、請參閱 "NetApp 互通性對照表工具"。

如需安裝這些VMware產品所需的步驟、請參閱VMware文件。

StorageGRID 的 **CPU** 和 **RAM** 需求

安裝StorageGRID 支援功能軟體之前、請先確認並設定硬體、使其準備好支援StorageGRID 該系統。

每StorageGRID 個支援節點都需要下列最低資源：

- CPU核心：每個節點8個
- RAM ：視可用的總 RAM 和系統上執行的非 StorageGRID 軟體數量而定
  - 一般而言、每個節點至少 24 GB 、比系統總 RAM 少 2 至 16 GB
  - 如果多個租戶各自擁有最多 5,000 個儲存桶，則每個節點至少需要 64 GB 的空間。

    StorageGRID 系統為每個 S3 租戶帳戶支援最多 20,000 個儲存桶。

軟體型中繼資料專用節點資源必須符合現有的儲存節點資源。例如：

- 如果現有的 StorageGRID 站台使用 SG6000 或 SG6100 應用裝置，則僅限軟體型中繼資料節點必須符合下列最低需求：
  - 128 GB RAM
  - 8 核心 CPU
  - 8 TB SSD 或與 Cassandra 資料庫相同的儲存設備（ rangedb/0 ）
- 如果現有的StorageGRID站點使用具有 24 GB RAM、8 核心 CPU 和 3 TB 或 4TB 元資料儲存的虛擬儲存節點，則基於軟體的僅元資料節點應使用類似的資源（24 GB RAM、8 核心 CPU 和 4TB 元資料儲存（rangedb/0））。

新增 StorageGRID 站台時，新站台的中繼資料總容量至少應與現有的 StorageGRID 站台和新站台資源相符，且應與現有 StorageGRID 站台的儲存節點相符。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

Linux

確保StorageGRID 您計畫在每個實體或虛擬主機上執行的各個節點數量、不會超過CPU核心數量或可用的實體RAM。如果主機並非專屬執行 StorageGRID （不建議）、請務必考慮其他應用程式的資源需求。

VMware

VMware 支援每部虛擬機器一個節點。確保 StorageGRID 節點不超過可用的實體 RAM 。每個虛擬機器都必須專用於執行 StorageGRID 。

定期監控 CPU 和記憶體容量使用情況，確保這些資源持續容納您的工作負載。例如，將虛擬儲存節點的 RAM 和 CPU 分配增加一倍，即可獲得與 StorageGRID 應用裝置節點類似的資源。此外，如果每個節點的中繼資料量超過 500 GB，請考慮將每個節點的 RAM 增加至 48 GB 或更多。有關管理物件中繼資料儲存設備、增加中繼資料保留空間設定以及監控 CPU 和記憶體容量使用情況的資訊，請參閱 "管理"、"監控" 和 "升級" StorageGRID 的相關說明。

如果在基礎實體主機上啟用超執行緒、您可以為每個節點提供8個虛擬核心（4個實體核心）。如果基礎實體主機上未啟用超執行緒、則每個節點必須提供8個實體核心。

如果您使用虛擬機器做為主機、並控制VM的大小和數量、您應該為每StorageGRID 個支援節點使用單一VM、並據此調整VM大小。

（僅限 RHEL、Debian 和 Ubuntu）對於生產部署，您不應在相同實體儲存硬體或虛擬主機上執行多個儲存節

點。單一StorageGRID部署中的每個儲存節點都應位於其自己的隔離故障域中。如果確保單一硬體故障僅影響單一儲存節點，則可以最大限度地提高物件資料的持久性和可用性。

請參閱 "儲存與效能需求"。

StorageGRID 的儲存與效能需求

您必須了解 StorageGRID 節點的儲存設備需求，以確保您有足夠的空間來支援初始組態和未來的儲存擴充。

儲存和效能要求根據基於軟體的節點實現而有所不同。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

儲存類別

不需使用下列三種邏輯儲存設備：StorageGRID

- **Container pool** — 節點 Container 的效能層（10K SAS 或 SSD）儲存設備，當您在支援 StorageGRID 節點的主機上安裝和設定 Container 引擎時，該儲存設備將指派給 Container 引擎儲存設備驅動程式。
- 系統資料 — 效能層（10K SAS 或 SSD）儲存設備，用於每個節點持續儲存系統資料和交易日誌，StorageGRID 主機服務使用這些儲存設備並將其對應到各個節點。
- 物件資料：效能層（10K SAS或SSD）儲存與容量層（NL-SAS/SATA）大量儲存、可持續儲存物件資料和物件中繼資料。

所有儲存設備類別都必須使用 RAID 支援的區塊設備。不支援非冗餘磁碟、SSD 或 JBOD。任何儲存設備類別都可以使用共享的或本機 RAID 儲存設備。若要在 StorageGRID 中移轉節點，必須將系統資料和物件資料都儲存在共享儲存設備上。如需詳細資訊，請參閱 "節點容器移轉需求"。

效能要求

用於容器集區、系統資料和物件中繼資料的磁碟區效能、會大幅影響系統的整體效能。您應該為這些磁碟區使用效能層（10K SAS或SSD）儲存設備、以確保在延遲、每秒輸入/輸出作業（IOPS）和處理量等方面達到適當的磁碟效能。您可以使用容量層（NL-SAS/SATA）儲存設備來持續儲存物件資料。

用於容器集區、系統資料和物件資料的磁碟區必須啟用回寫快取。快取必須位於受保護或持續的媒體上。

使用 **NetApp ONTAP** 儲存設備的主機需求

如果 StorageGRID 節點使用從 NetApp ONTAP 系統指派的儲存設備、請確認該磁碟區未啟用 FabricPool 分層原則。停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

切勿使用FabricPool 無法將StorageGRID 任何與還原StorageGRID 本身相關的資料分層。將StorageGRID 資料分層還原StorageGRID 至物件、可增加疑難排解和作業複雜度。

所需的主機數量

每StorageGRID 個站台至少需要三個儲存節點。

在正式作業部署時，請勿在單一實體主機或虛擬主機上執行多個儲存節點。每個儲存節點使用專用主機可提供隔離的故障網域。

您可以在同一主機上部署其他類型的節點，例如管理節點或閘道節點，也可以視需要將其部署在專用主機上。

您不能使用磁碟快照來還原網格節點。請參考"網格節點恢復"每種節點類型的復原步驟。

每個節點的儲存卷數量

下表顯示每個主機所需的儲存 Volume （LUN）數量，以及每個 LUN 所需的最小大小，視該主機上部署了哪些節點而定。

測試的最大 LUN 大小為 100 TiB。

這些數字適用於每個主機、而非整個網格。

LUN 用途	儲存類別	**LUN**數量	最小大小/**LUN**
Container引擎儲存資源池	Container Pool	1	節點總數x 100 GB
`/var/local`Volume	系統資料	此主機上的每個節點各1個	100GB
儲存節點	物件資料	3：針對此主機上的每個儲存節點 *附註：*基於 Linux 軟體的儲存節點和基於 VMware 軟體的儲存節點可擁有 1 至 48 個儲存 Volume。建議至少擁有 3 個儲存 Volume。	12 TB（最低 4 TB/LUN） 最大測試 LUN 大小：100 TiB。 請參閱 儲存節點的儲存需求 以取得更多資訊。
儲存節點（僅中繼資料）	物件中繼資料	1	最低 4 TB/LUN 最大測試 LUN 大小：100 TiB。 請參閱 儲存節點的儲存需求 以取得更多資訊。 • 附註 * ：僅中繼資料儲存節點只需要一個 rangedb 。
管理節點稽核記錄	系統資料	此主機上的每個管理節點各1個	200GB

LUN 用途	儲存類別	LUN數量	最小大小/LUN
管理節點表格	系統資料	此主機上的每個管理節點各1個	200GB

根據設定的稽核層級、使用者輸入（例如 S3 物件鍵名）的大小以及需要保留的稽核日誌資料量，您可能需要增加每個管理節點上的稽核日誌 LUN 的大小。通常，網格每次 S3 操作會產生約 1 KB 的稽核資料，這意味著 200 GB 的 LUN 可支援每天 7000 萬次操作，或每秒 800 次操作，持續兩到三天。

主機的最小儲存空間

下表顯示每種節點類型所需的最小儲存空間。您可以根據部署在該主機上的節點，使用此表格確定每個儲存設備類別中必須為主機提供的最小儲存空間。

您不能使用磁碟快照來還原網格節點。請參考"網格節點恢復"每種節點類型的復原步驟。

每個節點主機需要一個 100 GB 的 LUN 用於作業系統。

節點類型	Container Pool	系統資料	物件資料
儲存節點	100GB	100GB	4,000GB
管理節點	100GB	500 GB（3 個 LUN）	不適用
閘道節點	100GB	100GB	不適用

範例：計算主機或虛擬機器的儲存需求

假設您打算在同一台主機或虛擬機器上部署三個節點：一個 Storage Node、一個 Admin Node 和一個 Gateway Node。您至少需要為主機提供九個儲存 Volume。您至少需要 300 GB 的效能層儲存設備用於節點 Container、700 GB 的效能層儲存設備用於系統資料和交易日誌，以及 12 TB 的容量層儲存設備用於物件資料。

Linux 主機範例

節點類型	**LUN** 用途	**LUN**數量	**LUN** 大小
儲存節點	Container引擎儲存資源池	1	300 GB（每節點100 GB）
儲存節點	`/var/local`Volume	1	100GB
儲存節點	物件資料	3	12 TB（4 TB/LUN）
管理節點	`/var/local`Volume	1	100GB
管理節點	管理節點稽核記錄	1	200GB
管理節點	管理節點表格	1	200GB
閘道節點	`/var/local`Volume	1	100GB
總計		• 9 *	• Container Pool：* 300 GB 系統資料： 700 GB 物件資料： 12、000 GB

VMware 虛擬機器範例

節點類型	**LUN** 用途	**LUN**數量	**LUN** 大小
儲存節點	作業系統磁碟區	1	100GB
儲存節點	物件資料	3	12 TB（4 TB/LUN）
管理節點	作業系統磁碟區	1	100GB
管理節點	管理節點稽核記錄	1	200GB
管理節點	管理節點表格	1	200GB
閘道節點	作業系統磁碟區	1	100GB
總計		**8**	系統資料： 700 GB 物件資料： 12、000 GB

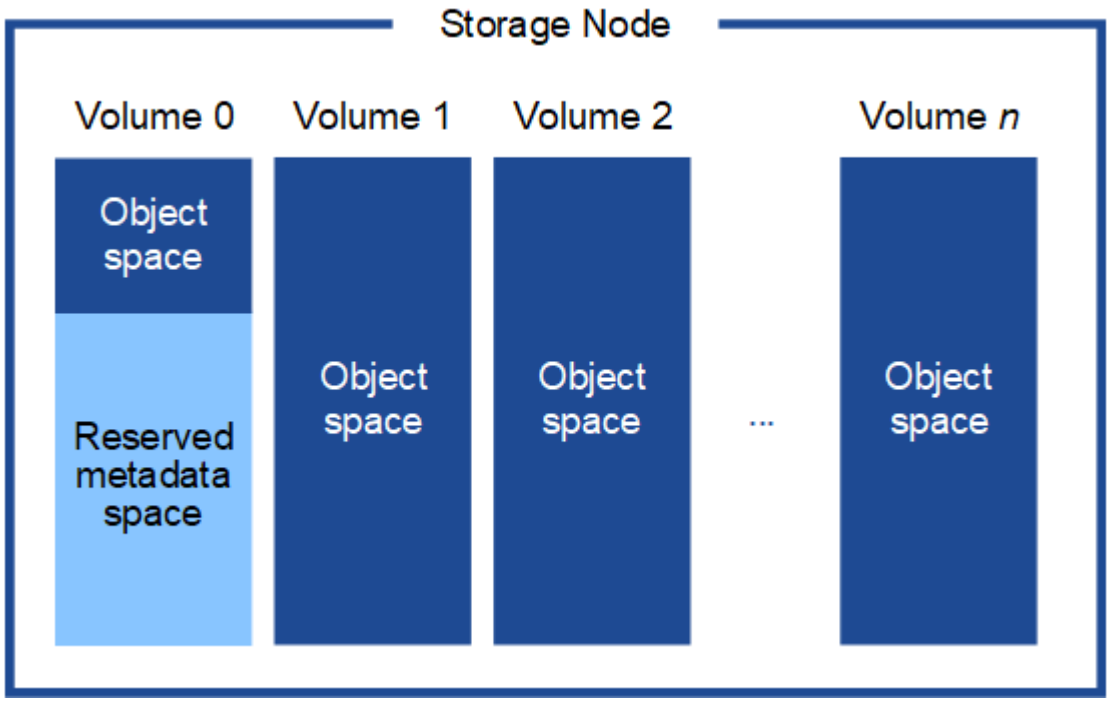
儲存節點的特定儲存要求

Linux 和 VMware 對儲存節點有以下儲存設備需求：

- 基於 Linux 軟體的儲存節點可以擁有 1 到 48 個儲存 Volume。
- 基於 VMware 軟體的儲存節點可以擁有 1 到 48 個儲存 Volume。
- 建議使用三個或更多儲存卷。
- 每個儲存磁碟區應為 4 TB 或更大。

設備儲存節點還可以擁有最多 48 個儲存磁碟區。

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。儲存Volume 0和儲存節點中任何其他儲存磁碟區上的任何剩餘空間、均專供物件資料使用。



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。

安裝含有僅中繼資料 Storage Nodes 的網格時，此網格還必須包含最少數量的物件儲存節點。如需有關僅中繼資料 Storage Nodes 的詳細資訊，請參閱 "儲存節點類型"。

- 對於單一站台網格、至少會針對物件和中繼資料設定兩個儲存節點。
- 對於多站台網格、每個站台至少要設定一個儲存節點、用於物件和中繼資料。

當您將空間指派給新儲存節點的Volume 0時、必須確保該節點的所有物件中繼資料都有足夠空間。

- 至少您必須將至少4 TB指派給Volume 0。

如果儲存節點只使用一個儲存磁碟區、而您將 4 TB 或更少容量指派給該磁碟區、則儲存節點可能會在啟動時進入儲存區唯讀狀態、並僅儲存物件中繼資料。

如果您指派小於 500 GB 的磁碟區 0 （僅限非正式作業使用）、則儲存磁碟區的容量的 10% 會保留給中繼資料。

- 軟體型中繼資料專用節點資源必須符合現有的儲存節點資源。例如：
  - 如果現有的 StorageGRID 站台使用 SG6000 或 SG6100 應用裝置，則僅限軟體型中繼資料節點必須符合下列最低需求：
    - 128 GB RAM
    - 8 核心 CPU
    - 8 TB SSD 或與 Cassandra 資料庫相同的儲存設備（ rangedb/0 ）
  - 如果現有的StorageGRID站點使用具有 24 GB RAM、8 核心 CPU 和 3 TB 或 4TB 元資料儲存的虛擬儲存節點，則基於軟體的僅元資料節點應使用類似的資源（24 GB RAM、8 核心 CPU 和 4TB 元資料儲存（rangedb/0））。

    新增 StorageGRID 站台時，新站台的中繼資料總容量至少應與現有的 StorageGRID 站台和新站台資源相符，且應與現有 StorageGRID 站台的儲存節點相符。
- 如果您要安裝新的系統（ StorageGRID 11.6 或更新版本）、且每個儲存節點都有 128 GB 以上的 RAM 、請將 8 TB 或更多的 RAM 指派給 Volume 0 。使用較大的Volume 0值、可增加每個儲存節點上中繼資料所允許的空間。
- 為網站設定不同的儲存節點時，請盡可能對 Volume 0 使用相同的設定。如果網站包含不同大小的儲存節點，則 Volume 0 容量最小的儲存節點決定該網站的中繼資料容量。

如需詳細資訊"管理物件中繼資料儲存"、請前往。

StorageGRID 節點容器遷移需求 (Linux)

節點移轉功能可讓您手動將節點從一部主機移至另一部主機。一般而言、這兩個主機都位於同一個實體資料中心。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

節點移轉可讓您在不中斷網格作業的情況下執行實體主機維護。將所有 StorageGRID 節點（一次一個）移至另一主機、然後再將實體主機離線。移轉節點只需要短暫的停機時間、不應影響網格服務的運作或可用度。

如果您想要使用StorageGRID 「資訊節點移轉」功能、您的部署必須符合其他需求：

- 在單一實體資料中心的主機之間、提供一致的網路介面名稱
- 共享儲存功能、適用於StorageGRID 單一實體資料中心內所有主機皆可存取的中繼資料和物件儲存庫磁碟區。例如、您可以使用NetApp E系列儲存陣列。

如果您使用的是虛擬主機、而基礎 Hypervisor 層支援 VM 移轉、則可能需要使用此功能、而非 StorageGRID 中的節點移轉功能。在此情況下、您可以忽略這些額外需求。

在執行移轉或Hypervisor維護之前、請先正常關閉節點。請參閱的說明"關閉網格節點"。

不支援**VMware**即時移轉

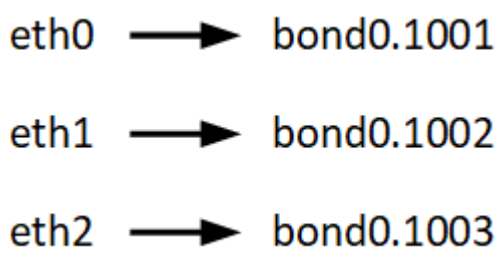
在 VMware VM 上執行裸機安裝時、 OpenStack Live Migration 和 VMware Live VMotion 會導致虛擬機器時鐘時間跳轉、而且不支援任何類型的網格節點。雖然不多見、但時鐘時間不正確可能導致資料遺失或組態更新。

支援冷移轉。在冷移轉中、StorageGRID 您需要先關閉各個節點、然後再在主機之間進行移轉。請參閱的說明"關閉網格節點"。

一致的網路介面名稱

若要將節點從一部主機移至另一部主機、 StorageGRID 主機服務需要對節點目前所在位置的外部網路連線能力、在新位置進行複製有一定信心。在主機中使用一致的網路介面名稱、就能獲得這種信心。

舉例來StorageGRID 說、假設在主機1上執行的支援節點a已設定下列介面對應：



箭頭的左側對應StorageGRID 於從一個包含網格、管理和用戶端網路介面的資訊（分別為網格、管理和用戶端網路介面）的舊介面。箭頭的右側對應於提供這些網路的實際主機介面、這些網路是三個附屬於同一個實體介面連結的VLAN介面。

現在、假設您要將節點A移轉至主機2。如果主機2也有名為bond0.1001、bond0.1002和bond0.1003的介面、則系統會允許移動、假設同名介面將在主機2上提供與主機1相同的連線能力。如果主機2沒有名稱相同的介面、則不允許移動。

有許多方法可以在多個主機之間實現一致的網路介面命名；如需一些範例、請參閱"設定主機網路"。

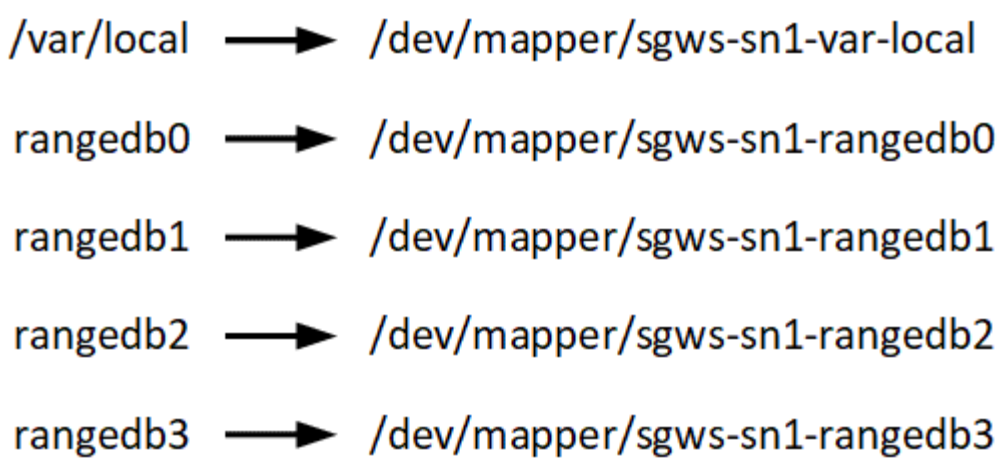
共享儲存設備

為了實現快速、低成本的節點移轉、 StorageGRID 節點移轉功能不會實際移動節點資料。相反地、節點移轉是以一對匯出與匯入作業的形式執行、如下所示：

- 在「節點匯出」作業期間、會從主機 A 上執行的節點容器擷取少量的持續狀態資料、並快取到該節點的系統資料 Volume 上。然後、將會對主機A上的節點容器進行個體化。
- 在「節點匯入」作業期間、主機 B 上使用與主機 A 相同網路介面和區塊儲存對應的節點容器會產生。然後、快取的持續狀態資料會插入新執行個體。

在這種操作模式下、必須可從主機A和主機B存取節點的所有系統資料和物件儲存磁碟區、才能允許移轉及運作。此外、它們必須使用名稱對應至節點、這些名稱必須保證能參照主機A和主機B上相同的LUN。

以下範例顯示 StorageGRID 儲存節點的區塊裝置對應解決方案、其中主機上正在使用 DM 多重路徑、而別名欄位已用於 `/etc/multipath.conf`提供所有主機上一致且易記的區塊裝置名稱。



準備主機（**Linux**）

StorageGRID 如何變更主機範圍的設定

在裸機系統上、 StorageGRID 會對主機範圍的設定進行一些變更 `sysctl`。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

會進行下列變更：

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
```

```
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
```

```
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

在 **Linux** 網格主機上安裝 **StorageGRID**

您必須在所有 Linux 網格主機上安裝StorageGRID 。若要取得受支援版本的列表，請使用NetApp互通性表工具。

開始之前

確保您的作業系統符合 StorageGRID 的最低核心版本需求、如下所列。使用命令 `uname -r`取得作業系統的核心版本、或洽詢作業系統廠商。

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

紅帽企業版

RHEL 版本	最低核心版本	核心套件名稱
8.8 （已過時）	4.18.0-477.10.1.el8_8.x86_64	核心 -4.18.0-477.10.1.el8_8.x86_64
8.10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 （已過時）	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 （已過時）	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9.4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9.6	5.14.0-570.18.1.el9_6.x86_64	內核-5.14.0-570.18.1.el9_6.x86_64

Ubuntu

- 注意： * Ubuntu 版本 18.04 和 20.04 的支援已過時、將於未來版本中移除。

Ubuntu 版本	最低核心版本	核心套件名稱
22.04.1.	5.15.0-47- 一般	Linux-image-5.15.0-47-generic/jammy-updates,jammy-security,now 5.15.0-47.51
24.04	6.8.0-31-generic	Linux-image-6.8.0-31-generic/grine, 現在 6.8.0-31.31

Debian

- 備註： * 支援 Debian 版本 11 已被淘汰、將於未來版本中移除。

Debian 版本	最低核心版本	核心套件名稱
11 （已過時）	5.10.0-18-amd64	Linux-image-5.10.0-18-amd64/Stable 、現為 5.10.150-1
12	6.1.0-9-amd64	Linux-image-6.1.0-9-amd64/Stable 、現為 6.1.27-1

步驟

1. 根據代理商的指示或您的標準程序、在所有實體或虛擬網格主機上安裝Linux。

   不要安裝任何圖形桌面環境。

   ◦ 如果在安裝 RHEL 時使用標準 Linux 安裝程序，請選擇「計算節點」軟體配置（如果可用）或「最小安裝」基礎環境。

◦ 安裝 Ubuntu 時，您必須選擇*標準系統實用程式*。建議選擇 **OpenSSH** 伺服器 以啟用對 Ubuntu 主機的 ssh 存取。所有其他選項可以保持清除狀態。

2. 確保所有主機都可以存取軟體包儲存庫，包括 RHEL 的 Extras 頻道。
3. 如果已啟用交換：
   a. 執行下列命令： `$ sudo swapoff --all`
   b. 移除中的所有交換項目 `/etc/fstab`、以保留設定。

> 如果無法完全停用交換、可能會嚴重降低效能。

了解 **Ubuntu** 和 **Debian** 上 **StorageGRID** 的 **AppArmor** 設定檔

如果您是在自行部署的Ubuntu環境中操作、並使用強制使用的AppArmor存取控制系統、則與您安裝在基礎系統上的套件相關聯的AppArmor設定檔可能會遭到安裝StorageGRID有支援此功能的相應套件封鎖。

根據預設、會針對您安裝在基礎作業系統上的套件安裝AppArmor設定檔。當您從StorageGRID 作業系統Container執行這些套件時、會封鎖該系統的AppArmor設定檔。DHCP、MySQL、NTP和tcdump基礎套件與AppArmor衝突、其他基礎套件也可能衝突。

您有兩種選擇可以處理AppArmor設定檔：

- 停用安裝在基礎系統上且與StorageGRID 更新系統容器中套件重疊的套件個別設定檔。當您停用個別設定檔時、StorageGRID 會有一個項目出現在「資訊安全記錄檔」中、表示已啟用AppArmor。

  使用下列命令：

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  範例：

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- 完全停用 AppArmor。對於 Ubuntu 9.10 或更新版本，請按照 "Ubuntu 線上社群"中的說明操作。在較新的 Ubuntu 版本上，可能無法完全停用 AppArmor。

  停用 AppArmor 之後、 StorageGRID 記錄檔中不會出現表示已啟用 AppArmor 的項目。

為 **Linux** 部署配置 **StorageGRID** 主機網路

在主機上完成Linux安裝之後、您可能需要執行一些額外的組態、以便在每個主機上準備一組適合對應至StorageGRID 稍後部署之支援節點的網路介面。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

開始之前

- 您已查看 "網路準則" 中的資訊。
- 您已檢閱有關的資訊"節點容器移轉需求"。
- 如果您正在使用虛擬主機，您已經閱讀了MAC位址複製的考量與建議在配置主機網路之前。

如果您使用VM做為主機、應該選取VMXNET 3做為虛擬網路介面卡。VMware E1000網路介面卡在StorageGRID 某些Linux版本上部署了VMware vCenter Container、導致連線問題。

關於這項工作

網格節點必須能夠存取網格網路、以及管理網路和用戶端網路（可選）。您可以建立對應、將主機的實體介面與每個網格節點的虛擬介面建立關聯、藉此提供此存取。建立主機介面時、請使用易記的名稱來協助跨所有主機進行部署、並啟用移轉。

同一個介面可在主機與一個或多個節點之間共用。例如、您可以使用相同的介面進行主機存取和節點管理網路存取、以利主機和節點維護。雖然主機與個別節點之間可以共用相同的介面、但所有介面都必須有不同的IP位址。IP 位址無法在節點之間或主機與任何節點之間共用。

您可以使用相同的主機網路介面、為StorageGRID 主機上的所有支援節點提供Grid Network介面；您可以為每個節點使用不同的主機網路介面；也可以在兩者之間執行某些作業。不過、您通常不會為單一節點提供與Grid和管理網路介面相同的主機網路介面、也不會提供與某個節點相同的Grid Network介面、以及與另一個節點相同的Client Network介面。

您可以透過多種方式完成此工作。例如、如果您的主機是虛擬機器、而且您要為每個主機部署一或兩個 StorageGRID 節點、則可以在 Hypervisor 中建立正確數量的網路介面、並使用一對一對應。如果您要在裸機主機上部署多個節點以供正式作業使用、您可以利用Linux網路堆疊的VLAN和LACP支援來實現容錯能力和頻寬共用。以下各節提供這兩個範例的詳細方法。您不需要使用上述任一範例、也可以使用任何符合您需求的方法。

請勿直接使用連結或橋接裝置做為容器網路介面。這樣做可能會防止節點啟動、因為在容器命名空間中使用含有連結和橋接裝置的MAC VLAN時發生核心問題。而是使用非連結裝置、例如VLAN或虛擬乙太網路（vith）配對。將此裝置指定為節點組態檔中的網路介面。

MAC位址複製的考量與建議

MAC 位址複製使 Container 使用主機的 MAC 位址，而主機則使用您指定的位址或隨機產生的位址的 MAC 位址。

啟用**MAC**複製

在某些環境中，可以透過 MAC 位址複製來增強安全性，因為它可讓您為管理網路、Grid 網路和用戶端網路使用專用虛擬 NIC。

Mac位址複製是設計用於虛擬伺服器安裝、可能無法在所有實體應用裝置組態中正常運作。

如果某個節點因為MAC複製目標介面正忙線而無法啟動、您可能需要在啟動節點之前將連結設定為「關閉」。此外、虛擬環境可能會在連結啟動時、防止網路介面上的MAC複製。如果某個節點因為介面忙碌而無法設定MAC位址並啟動、請在啟動節點之前將連結設定為「關閉」、這樣可能可以解決此問題。

Mac位址複製預設為停用、必須由節點組態金鑰設定。安裝StorageGRID 時應啟用此功能。

每個網路都有一個金鑰：

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

將金鑰設定為「true」會導致容器使用主機NIC的MAC位址。此外、主機也會使用指定容器網路的MAC位址。根據預設、容器位址是隨機產生的位址、但如果您已使用節點組態金鑰設定位址、則 `_NETWORK_MAC`會改用該位址。主機和容器將永遠擁有不同的MAC位址。

Mac複製使用案例

有兩種使用案例可考慮使用MAC複製：

- MAC 複製未啟用：當 `_CLONE_MAC`節點組態檔案中的金鑰未設定或設定為「false」時，主機將使用主機 NIC MAC 位址，Container 將使用 StorageGRID 產生的 MAC 位址，除非在 `_NETWORK_MAC`金鑰中指定了 MAC 位址。如果在 `_NETWORK_MAC`金鑰中設定了位址，則 Container 將使用 `_NETWORK_MAC`金鑰中指定的位址。
- MAC 複製已啟用：當 `_CLONE_MAC`節點組態檔案中的金鑰設為「true」時，Container 將使用主機 NIC MAC 位址，而主機將使用 StorageGRID 產生的 MAC 位址，除非在 `_NETWORK_MAC`金鑰中指定了 MAC 位址。如果在 `_NETWORK_MAC`金鑰中設定了位址，則主機將使用指定的位址，而非產生的位址。

如果您不想使用 MAC 位址克隆，而是希望允許所有介面接收和傳送除 Hypervisor 指派的 MAC 位址之外的其他 MAC 位址的資料，請確保虛擬交換器和連接埠群組層級的安全性屬性設定為 **Accept**，以用於 MAC Address Changes 和 Forged Transmits。虛擬交換器上的設定值可能會被連接埠群組層級的設定值覆蓋，因此請確保兩處的設定相同。

若要啟用 MAC 複製"建立節點組態檔的指示"、請參閱。

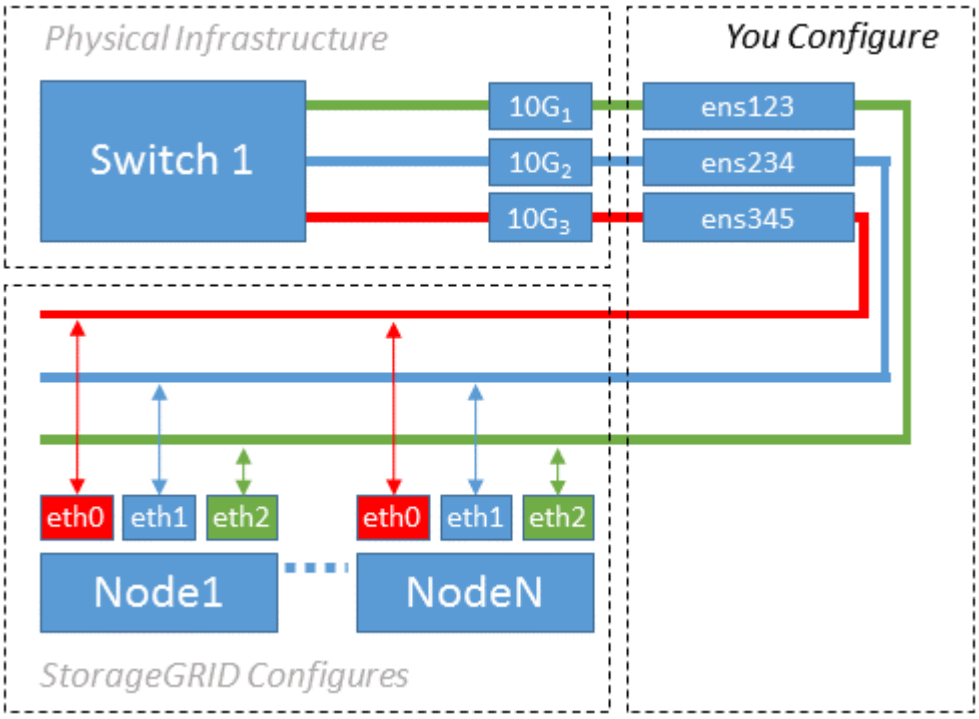
Mac複製範例

以 MAC 位址為 11 ： 22 ： 33 ： 44 ： 55 ： 66 的主機啟用 MAC 複製範例、適用於介面 ens256 、並在節點組態檔案中使用下列金鑰：

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`
- 結果 * ： ens256 的主機 MAC 為 B2:9c ： 02 ： C2 ： 27 ： 10 、管理網路 MAC 為 11 ： 22 ： 33 ： 44 ： 55 ： 66

範例1：1對1對應至實體或虛擬NIC

範例1說明簡單的實體介面對應、只需極少或不需要主機端組態。



Linux 作業系統創建 `ensXYZ`在安裝或啟動期間自動新增接口，或在熱添加接口時新增接口。除了確保介面設定為啟動後自動啟動之外，不需要進行任何設定。您必須確定哪個 ensXYZ 對應哪個StorageGRID網路（網格、管理或用戶端），以便您可以在稍後的設定過程中提供正確的對應。

請注意、圖中顯示了多StorageGRID 個支援節點、不過您通常會將此組態用於單節點VM。

如果交換器1是實體交換器、您應該將連接至介面10G1到10G3的連接埠設定為存取模式、然後將它們放在適當的VLAN上。

範例2：LACP連結傳輸VLAN

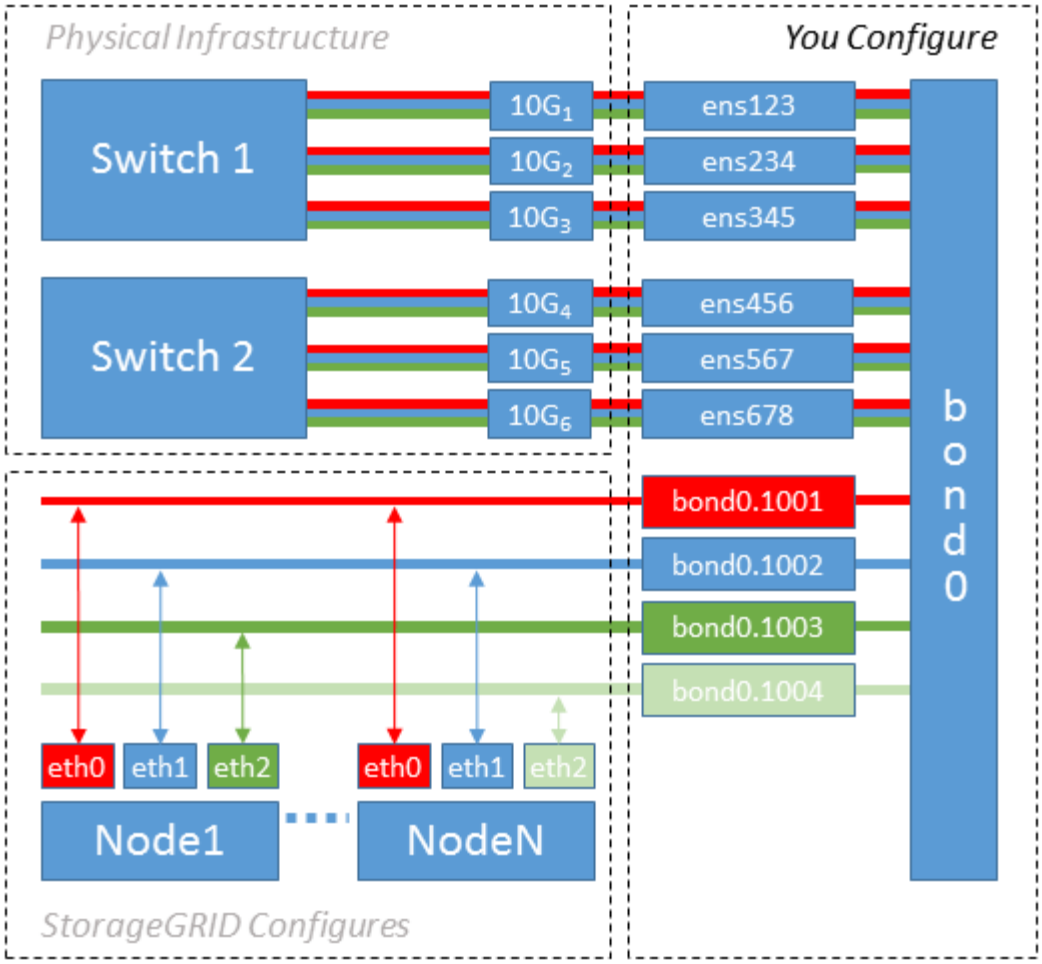
範例2假設您熟悉連結網路介面、以及在所使用的Linux發佈版本上建立VLAN介面。

關於這項工作

範例2說明通用、靈活、以VLAN為基礎的配置、可在單一主機上的所有節點之間共享所有可用的網路頻寬。此範例特別適用於裸機主機。

若要瞭解此範例、假設每個資料中心的Grid、Admin和Client Networks各有三個子網路。子網路位於不同的VLAN（1001、1002和1003）上、並以LACP連結主幹連接埠（bond0）呈現給主機。您可以在連結上設定三個VLAN介面：bond0.1001、bond0.1002和bond0.1003。

如果同一主機上的節點網路需要不同的VLAN和子網路、您可以在連結上新增VLAN介面、然後將它們對應到主機（如圖中的bond0.1004所示）。



步驟

1. 將StorageGRID 用於實現無線網路連接的所有實體網路介面、整合到單一LACP連結中。

   在每個主機上對綁定使用相同的名稱，例如， `bond0` 。

2. 使用標準的 VLAN 介面命名慣例、建立將此連結作為其相關「實體裝置」的 VLAN 介面 `physdev-name.VLAN ID`。

   請注意、步驟1和步驟2需要在邊緣交換器上進行適當的組態、以終止網路連結的其他端點。邊緣交換器連接埠也必須整合至LACP連接埠通道（設定為主幹）、並允許通過所有必要的VLAN。

   提供此每個主機網路組態配置方案的介面組態檔範例。

相關資訊

- "Ubuntu 和 Debian 的範例 /etc/network/interfaces"
- "RHEL 的範例 /etc/sysconfig/network-scripts"

為 **Linux** 部署配置 **StorageGRID** 主機儲存

您必須為每個 Linux 主機指派區塊儲存磁碟區。

開始之前

您已檢閱下列主題、其中提供完成此工作所需的資訊：

- "儲存與效能需求"
- "節點容器移轉需求"

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

關於這項工作

將區塊儲存磁碟區（ LUN ）分配給主機時、請使用「儲存需求」中的表格來判斷下列事項：

- 每個主機所需的磁碟區數量（根據將部署在該主機上的節點數量和類型而定）
- 每個磁碟區的儲存類別（即系統資料或物件資料）
- 每個Volume的大小

當您在StorageGRID 主機上部署支援節點時、您將會使用此資訊、以及Linux指派給每個實體Volume的持續名稱。

您不需要分割、格式化或掛載任何這些磁碟區、只需確保主機可以看到這些磁碟區即可。

僅中繼資料專用儲存節點只需要一個物件資料 LUN 。

(`/dev/sdb`例如、在您撰寫磁碟區名稱清單時、請避免使用「原始」特殊裝置檔案。這些檔案可能會在主機重新開機後變更、進而影響系統的正常運作。如果您使用的是 `iSCSI LUN` 和 `Device Mapper` 多路徑、請考慮在目錄中使用多重路徑別名 `/dev/mapper`、尤其是當 SAN 拓撲包含通往共用儲存設備的備援網路路徑時。或者、您也可以使用下的系統建立的軟體連結 `/dev/disk/by-path/`來命名持續性的裝置名稱。

例如：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

每個安裝的結果將有所不同。

為每個區塊儲存磁碟區指派易記名稱、以簡化初始StorageGRID 的版本安裝及未來的維護程序。如果您使用裝置對應程式多重路徑驅動程式來備援存取共用儲存磁碟區、則可以使用 `alias`檔案中的欄位 `/etc/multipath.conf`。

例如：

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

以這種方式使用別名欄位、可讓別名在主機的目錄中顯示為區塊裝置 `/dev/mapper`、讓您在組態或維護作業需要指定區塊儲存磁碟區時、可以指定易用且易於驗證的名稱。

如果您要設定共用儲存設備來支援 StorageGRID 節點移轉、並使用裝置對應程式多重路徑、則可以在所有代管主機上建立並安裝通用的 `/etc/multipath.conf`。只要確定在每個主機上使用不同的Container Engine儲存磁碟區即可。使用別名並將目標主機名稱納入每個容器引擎儲存Volume LUN的別名、將會讓您輕鬆記住、建議您這麼做。

將 Docker 作為僅限軟體部署的容器引擎的支援已過時。Docker 將在未來版本中以另一個 Container 引擎取代。

相關資訊

- "設定Container Engine儲存Volume"
- "儲存與效能需求"
- "節點容器移轉需求"

在 **Linux** 上為 **StorageGRID** 配置容器引擎儲存磁碟區

在安裝 Docker 或 Podman 容器引擎之前，您可能需要格式化儲存磁碟區並掛載它。

將 Docker 作為僅限軟體部署的容器引擎的支援已過時。Docker 將在未來版本中以另一個 Container 引擎取代。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

關於這項工作

如果您打算將根卷用於 Docker 或 Podman 儲存卷，並且主機分割區上有足夠的可用空間，則可以跳過以下步驟：

- Podman： `/var/lib/containers`
- Docker： `/var/lib/docker`

步驟

1. 在容器引擎儲存磁碟區上建立檔案系統：

紅帽企業版

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

Ubuntu或DEBIAN

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. 掛載Container Engine儲存磁碟區：

紅帽企業版

- 適用於Docker：

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

- 若為Podman：

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

Ubuntu或DEBIAN

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

- 若為Podman：

```
sudo mkdir -p /var/lib/podman
sudo mount container-storage-volume-device /var/lib/podman
```

3. 將容器儲存磁碟區裝置的條目新增至 /etc/fstab。
   - RHEL：容器儲存卷設備
   - Ubuntu 或 Debian：docker-storage-volume-device

   此步驟可確保儲存磁碟區在主機重新開機後自動重新掛載。

安裝Docker

StorageGRID系統可以作為容器集合在 Linux 上運作。

- 在為 Ubuntu 或 Debian 安裝StorageGRID之前，您必須安裝 Docker。
- 如果您選擇使用 Docker 容器引擎，請依照下列步驟安裝 Docker。否則，安裝Podman 。

> 將 Docker 作為僅限軟體部署的容器引擎的支援已過時。Docker 將在未來版本中以另一個 Container 引擎取代。

步驟

1. 請依照Linux套裝作業系統的指示來安裝Docker。

如果您的Linux套裝作業系統未隨附Docker、您可以從Docker網站下載。

2. 執行下列兩個命令、確保已啟用及啟動Docker：

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 輸入下列命令、確認您已安裝Docker的預期版本：

```
sudo docker version
```

用戶端和伺服器版本必須為 1.11.0 或更新版本。

安裝Podman

StorageGRID系統作為容器集合運作。如果您選擇使用 Podman 容器引擎，請依照以下步驟安裝 Podman。否則，安裝Docker 。

步驟

1. 依照Linux套裝作業系統的指示、安裝Podman和Podman-Docker。

安裝Podman時、您也必須安裝Podman-Docker套件。

2. 輸入下列命令、確認您已安裝Podman和Podman-Docker的預期版本：

```
sudo docker version
```

使用Podman-Docker套件可以使用Docker命令。

用戶端和伺服器版本必須為 3.2.3 或更新版本。

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

相關資訊

"設定主機儲存設備"

在 **Linux** 上安裝 **StorageGRID** 主機服務

您可以使用適合您的作業系統類型的StorageGRID套件來安裝StorageGRID主機服務。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

紅帽企業版

您可以使用StorageGRID 支援支援的RPM套件來安裝StorageGRID 支援的主機服務。

關於這項工作

這些指示說明如何從RPM套件安裝主機服務。此外、您也可以使用安裝歸檔中所包含的 DNF 儲存庫中繼資料、遠端安裝 RPM 套件。請參閱適用於您Linux作業系統的DNF儲存庫說明。

步驟

1. 將StorageGRID 此功能複製到您的每個主機、或是將其複製到共享儲存設備上。

   例如、將它們放在目錄中 `/tmp`、以便在下一步中使用範例命令。

2. 以root身分或使用具有Sudo權限的帳戶登入每個主機、然後依照指定順序執行下列命令：

   ```
   sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
   ```

   ```
   sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
   ```

   您必須先安裝映像套件、然後再安裝服務套件。

   如果將軟件包放在其他目錄 `/tmp`中，請修改命令以反映所用的路徑。

Ubuntu或DEBIAN

您可以使用StorageGRID DEB 套件為 Ubuntu 或 Debian 安裝StorageGRID主機服務。

關於這項工作

這些指示說明如何從Deb套件安裝主機服務。此外、您也可以使用安裝歸檔中隨附的APT儲存庫中繼資料、從遠端安裝Deb套件。請參閱適用於您Linux作業系統的APT儲存庫說明。

步驟

1. 將StorageGRID 《不適用資料》套件複製到每個主機、或是在共享儲存設備上提供。

   例如、將它們放在目錄中 `/tmp`、以便在下一步中使用範例命令。

2. 以root身分或使用具有Sudo權限的帳戶登入每個主機、然後執行下列命令。

   您必須先安裝套件、 `service`然後再安裝 `images`套件。如果將軟件包放在其他目錄 `/tmp`中，請修改命令以反映所用的路徑。

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
   ```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-
SHA.deb
```

在安裝StorageGRID套件之前，必須先安裝 Python 3。這 `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb`直到您完成此操作後，命令才會失敗。

自動化基於軟體的節點安裝

在 **Linux** 系統上自動安裝 **StorageGRID** 主機服務並設定網格節點

您可以自動化StorageGRID 安裝支援服務和網格節點的組態。

關於這項工作

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

在下列任一情況下、自動化部署可能會很有用：

- 您已經使用標準協調架構（例如Ansible、Puppet或Chef）來部署及設定實體或虛擬主機。
- 您打算部署多StorageGRID 個實例。
- 您正在部署一個龐大且複雜StorageGRID 的實體執行個體。

這個支援服務是由套件安裝、並由組態檔案驅動。StorageGRID您可以使用下列其中一種方法來建立組態檔：

- "建立組態檔"在手動安裝期間互動。
- 如本文所述、預先準備組態檔案（或以程式設計方式）、以使用標準協調架構來啟用自動化安裝。

  StorageGRID 提供選用的 Python 指令碼、可將 StorageGRID 應用裝置和整個 StorageGRID 系統（「網格」）的組態自動化。您可以直接使用這些指令碼、也可以檢查這些指令碼、瞭解如何在您自己開發的網格部署和組態工具中使用"安裝REST API StorageGRID"。

自動化**StorageGRID** 安裝及設定整套的支援服務

您可以StorageGRID 使用Ansible、Puppet、Chef、Fabric或SaltStack等標準協調架構來自動化安裝支援服務。

StorageGRID主機服務打包在 DEB（Ubuntu 或 Debian）或 RPM（RHEL）中，並由您可以提前（或以程式設計方式）準備的設定檔驅動，以實現自動安裝。如果您已經使用標準編排框架來安裝和設定您的 Linux 部署，那麼將StorageGRID新增至您的劇本或配方應該很簡單。

您可以自動化準備主機和部署虛擬網格節點的所有步驟。

Ansible角色與方針範例

範例 Ansible 角色和教戰手冊隨附於資料夾中的安裝封存 `/extras`。Ansible 教戰手冊說明角色如何`storagegrid`準備主機、並將 StorageGRID 安裝到目標伺服器上。您可以視需要自訂角色或方針。

範例播放手冊不包含在開始StorageGRID 執行「支援服務」之前建立網路裝置所需的步驟。在完成及使用本方針之前、請先新增這些步驟。

紅帽企業版

對於 RHEL，提供的安裝任務 `storagegrid`角色範例使用 `ansible.builtin.dnf`模組從本機 RPM 檔案或遠端 Yum 儲存庫執行安裝。如果模組不可用或不受支持，您可能需要編輯以下文件中的相應 Ansible 任務以使用 `yum`或者 `ansible.builtin.yum`模組：

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Ubuntu或DEBIAN

對於 Ubuntu 或 Debian，提供的安裝任務 `storagegrid`角色範例使用 `ansible.builtin.apt`模組從本機 DEB 檔案或遠端 apt 儲存庫執行安裝。如果模組不可用或不受支持，您可能需要編輯以下文件中的相應 Ansible 任務以使用 `ansible.builtin.apt`模組：

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

自動化**StorageGRID** 功能組態

部署完網格節點之後、您可以自動化StorageGRID 設定該系統。

開始之前

- 您可以從安裝歸檔中得知下列檔案的位置。

檔案名稱	說明
configure-storagegrid.py	Python指令碼用於自動化組態
設定-storagegrid。same.json	用於指令碼的組態檔範例
設定-storagegrid。blank.json	與指令碼搭配使用的空白組態檔

- 您已建立 `configure-storagegrid.json`組態檔案。要創建此文件，您可以修改示例配置文件（`configure-storagegrid.blank.json`）（`configure-storagegrid.sample.json`或空白配置文件）。

儲存修改後的密碼部分的管理密碼和設定密碼 `configure-storagegrid.json`設定檔保存在安全的位置。安裝、擴充和維護過程都需要這些密碼。您還應該備份修改後的 `configure-storagegrid.json`設定檔並將其儲存在安全的位置。

關於這項工作

您可以使用 `configure-storagegrid.py` Python 指令碼和 `configure-storagegrid.json`組態檔來自動化 StorageGRID 系統的組態。

您也可以使用Grid Manager或安裝API來設定系統。

步驟

1. 登入您用來執行Python指令碼的Linux機器。
2. 切換至您擷取安裝歸檔的目錄。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 `platform`是 `debs、 rpms`或 `vsphere。

3. 執行Python指令碼並使用您建立的組態檔。

   例如：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

結果

恢復套件 `.zip`檔案會在組態程序期間產生、並下載到執行安裝和組態程序的目錄。您必須備份「恢復套件」檔案、以便StorageGRID 在一個或多個網格節點故障時、恢復該系統。例如、將其複製到安全的備份網路位置、以及安全的雲端儲存位置。

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。

如果您指定應產生隨機密碼、請開啟檔案、 `Passwords.txt`並尋找存取 StorageGRID 系統所需的密碼。

```
#####################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#####################################################################
```

系統會在顯示確認訊息時安裝及設定您的系統。StorageGRID

```
StorageGRID has been configured and installed.
```

使用 **VMware vSphere** 在 **StorageGRID** 中自動部署網格節點

您可以使用 VMware OVF 工具來自動化網格節點的部署。您也可以自動化StorageGRID

執行功能組態設定。

自動化網格節點部署

使用 VMware OVF 工具來自動化網格節點的部署。

開始之前

- 您可以使用Bash 3.2或更新版本存取Linux/Unix系統。
- 您擁有 VMware vSphere with vCenter
- 您已安裝並正確設定 VMware OVF Tool。
- 您知道使用 OVF Tool 存取 VMware vSphere 的使用者名稱和密碼
- 您有足夠的權限從 OVF 檔案部署 VM 並開啟其電源、以及建立附加至 VM 的其他磁碟區的權限。如需詳細資訊、請參閱 `ovftool`文件。
- 您知道vSphere中要部署StorageGRID VMware虛擬機器之位置的虛擬基礎架構（VI）URL。此URL通常是vApp或資源池。例如： `vi://vcenter.example.com/vi/sgws`

> 您可以使用 VMware `ovftool` 公用程式來判斷此值（請參閱 `ovftool`文件以取得詳細資料）。

> 如果您要部署至vApp、虛擬機器將不會在第一次自動啟動、而且您必須手動啟動。

- 您已收集部署組態檔案所需的所有資訊。如需詳細資訊、請參閱"收集部署環境的相關資訊"。
- 您可以從VMware的StorageGRID VMware安裝歸檔文件存取下列檔案、以供VMware使用：

檔案名稱	說明
NetApp-SG-VERSION SHA-VMDK	用來做為建立網格節點虛擬機器範本的虛擬機器磁碟檔案。 • 注意： * 此檔案必須與和檔案位於同一個 `.mf`資料夾中 `.ovf`。
vSphere-primer-admin.OVF vSphere-prime-admin.mf	開放式虛擬化格式模板文件(`.mf`)（`.ovf`和清單文件），用於部署主管理節點。
vsphere-non-prime-admin.OVF vsphere-non-prime-admin.mf	模板文件(`.mf`)（`.ovf`和清單文件），用於部署非主管理員節點。
vSphere-gateway.OVF vSphere-gateway.mf	模板文件(`.mf`)（`.ovf`和清單文件），用於部署網關節點。
vSphere-storage。OVF vSphere-storage。mf	模板文件(`.mf`)（`.ovf`和清單文件），用於部署基於虛擬機的存儲節點。
deploy-vsphere-ovftool.sh	Bash Shell指令碼用於自動化虛擬網格節點的部署。

檔案名稱	說明
deploy-vsphere-ovftool-sample.ini	用於指令碼的範例組態檔 `deploy-vsphere-ovftool.sh`。

定義部署的組態檔

您可以在 Bash 指令碼所使用的組態檔中、指定部署 StorageGRID 虛擬網格節點所需的資訊 `deploy-vsphere-ovftool.sh`。您可以修改範例組態檔案、這樣就不需要從頭建立檔案。

步驟

1. 複製範例組態檔案(`deploy-vsphere-ovftool.sample.ini`）。將新檔案另存為 `deploy-vsphere-ovftool.ini`與相同的目錄 `deploy-vsphere-ovftool.sh`。
2. 打開。 `deploy-vsphere-ovftool.ini`
3. 輸入部署VMware虛擬網格節點所需的所有資訊。

   如需詳細資訊、請參閱組態檔設定。

4. 輸入並驗證所有必要資訊後、請儲存並關閉檔案。

組態檔設定

`deploy-vsphere-ovftool.ini`組態檔包含部署虛擬網格節點所需的設定。

組態檔會先列出全域參數、然後在節點名稱所定義的區段中列出節點專屬的參數。使用檔案時：

- _Global參數_會套用至所有網格節點。
- _Node專屬參數_會覆寫全域參數。

全域參數

除非個別區段中的設定會覆寫全域參數、否則會套用至所有網格節點。將套用至多個節點的參數放在「通用參數」區段中、然後視需要在個別節點的區段中覆寫這些設定。

- * OFFTOOL_arguments*：您可以將OFFTOOL_arguments*指定為全域設定、也可以個別將引數套用至特定節點。例如：

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  您可以使用 `--powerOffTarget`和 `--overwrite`選項來關閉和取代現有的虛擬機器。

  您應該將節點部署至不同的資料存放區、並為每個節點指定OFFTOOL_arguments、而非全域。

- * 來源 * ： StorageGRID 虛擬機器範本(`.vmdk`的路徑）檔案、以及 `.ovf`個別網格節點的和 `.mf`檔案。這會預設為目前目錄。

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- 目標：VMware vSphere虛擬基礎架構（VI）URL、用於StorageGRID 部署VMware vSphere的位置。例如：

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- * GRID_NETWORD_config*：用於獲取IP位址的方法、靜態或DHCP。預設為靜態。如果所有或大部分節點都使用相同的方法來擷取IP位址、您可以在此處指定該方法。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
GRID_NETWORK_CONFIG = STATIC
```

- * GRID_NETWORD_Target *：用於Grid Network的現有VMware網路名稱。如果所有或大部分節點使用相同的網路名稱、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
GRID_NETWORK_TARGET = SG Admin Network
```

- * GRID_NETWORD_MANON*：Grid Network的網路遮罩。如果所有或大部分節點都使用相同的網路遮罩、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
GRID_NETWORK_MASK = 255.255.255.0
```

- * GRID_NETWORD_gateway*：Grid Network的網路閘道。如果所有或大部分節點都使用相同的網路閘道、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * GRID_NETWORD_MTU*：選用。Grid Network上的最大傳輸單位（MTU）。如果指定、則值必須介於1280和9216之間。例如：

```
GRID_NETWORK_MTU = 9000
```

  如果省略、則使用1400。

  如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。

網路的 MTU 值必須符合節點所連接之 vSphere 中虛擬交換器連接埠上所設定的值。否則、可能會發生網路效能問題或封包遺失。

為獲得最佳網路效能、所有節點都應在其Grid Network介面上設定類似的MTU值。如果個別節點上Grid Network的MTU設定有顯著差異、則會觸發* Grid Network MTU mismis*警示。所有網路類型的 MTU 值都不一定相同。

- 管理網路組態：用於取得IP位址的方法、包括停用、靜態或DHCP。預設為停用。如果所有或大部分節點都使用相同的方法來擷取IP位址、您可以在此處指定該方法。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_CONFIG = STATIC
```

- 管理網路目標：要用於管理網路的現有VMware網路名稱。除非已停用管理網路、否則此設定為必填。如果所有或大部分節點使用相同的網路名稱、您可以在此處指定。與 Grid Network 不同的是、所有節點都不需要連線至相同的管理網路。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- 管理網路的網路遮罩：管理網路的網路遮罩。如果您使用靜態IP定址、則必須使用此設定。如果所有或大部分節點都使用相同的網路遮罩、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- 管理網路網路閘道：管理網路的網路閘道。如果您使用靜態IP定址、並在admin_network_esl設定中指定外部子網路、則必須使用此設定。（也就是說、如果 Admin_network_esl 是空的、則不需要。）如果所有或大部分節點都使用相同的網路閘道、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * admin_network_esl*：管理網路的外部子網路清單（路由）、指定為以逗號分隔的CIDR路由目的地清單。如果所有或大部分節點都使用相同的外部子網路清單、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- *管理網路MTU *：選用。管理網路上的最大傳輸單元（MTU）。如果 Admin_network_config = DHCP 、請勿指定。如果指定、則值必須介於1280和9216之間。如果省略、則使用1400。如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。如果所有或大部分節點都使用相同的MTU來管理網路、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
ADMIN_NETWORK_MTU = 8192
```

- 用戶端網路組態：用於取得IP位址的方法、包括停用、靜態或DHCP。預設為停用。如果所有或大部分節點都使用相同的方法來擷取IP位址、您可以在此處指定該方法。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * Client_network_target *：用於用戶端網路的現有VMware網路名稱。除非停用「用戶端網路」、否則此設定為必填。如果所有或大部分節點使用相同的網路名稱、您可以在此處指定。與 Grid Network 不同的是、所有節點都不需要連線到同一個 Client Network 。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- 用戶端網路遮罩：用戶端網路的網路遮罩。如果您使用靜態IP定址、則必須使用此設定。如果所有或大部分節點都使用相同的網路遮罩、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- 用戶端網路閘道：用戶端網路的網路閘道。如果您使用靜態IP定址、則必須使用此設定。如果所有或大部分節點都使用相同的網路閘道、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- *用戶端網路MTU *：選用。用戶端網路上的最大傳輸單位（MTU）。不要指定 client_network_config = DHCP 。如果指定、則值必須介於1280和9216之間。如果省略、則使用1400。如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。如果所有或大部分節點都使用相同的MTU來連接用戶端網路、您可以在此處指定。然後、您可以為一個或多個個別節點指定不同的設定、以覆寫全域設定。例如：

```
CLIENT_NETWORK_MTU = 8192
```

- * port_remap*：重新對應節點用於內部網格節點通訊或外部通訊的任何連接埠。如果企業網路原則限制StorageGRID 了一個或多個由效益管理所使用的連接埠、則必須重新對應連接埠。如需 StorageGRID 使用的連接埠清單、請參閱中的內部網格節點通訊和外部通訊"網路準則"。

> 不要重新對應您打算用來設定負載平衡器端點的連接埠。

如果只設定port_remap、則您指定的對應會同時用於傳入和傳出通訊。如果也指定port_remap_inbound、則port_remap僅適用於傳出通訊。

使用的格式為： *network type/protocol/default port used by grid node/new port*、其中網路類型為網格、管理或用戶端、且傳輸協定為 TCP 或 UDP 。

例如：

```
PORT_REMAP = client/tcp/18082/443
```

如果單獨使用、此範例設定會對稱地將網格節點的傳入和傳出通訊從連接埠18082對應至連接埠443。如果與port_remap_inbound搭配使用、此範例設定會將連接埠18082的傳出通訊對應至連接埠443。

您也可以使用以逗號分隔的清單來重新對應多個連接埠。

例如：

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- * port_remap_inbound *：重新對應指定連接埠的傳入通訊。如果您指定 port_remap_inbound 、但未指定 port_remap 值、則連接埠的輸出通訊將維持不變。

  不要重新對應您打算用來設定負載平衡器端點的連接埠。

  使用的格式為： *network type/protocol/_default port used by grid node/new port*、其中網路類型為網格、管理或用戶端、且傳輸協定為 TCP 或 UDP 。

  例如：

  ```
  PORT_REMAP_INBOUND = client/tcp/443/18082
  ```

  此範例會將傳送至連接埠443的流量引導至連接埠18082、讓網格節點偵聽S3要求。

  您也可以使用以逗號分隔的清單來重新對應多個傳入連接埠。

  例如：

  ```
  PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
  ```

- * 暫存密碼類型 * ：在節點加入網格之前、存取 VM 主控台或 StorageGRID 安裝 API 或使用 SSH 時所使用的暫存安裝密碼類型。

如果所有或大部分節點都使用相同類型的暫存安裝密碼、請在全域參數區段中指定類型。然後、您也可以針對個別節點使用不同的設定。例如，如果選擇全局使用自定義密碼 * ，則可以使用 <password> 來設置每個節點的密碼。

- 暫用密碼類型 * 可以是下列其中一項：
  - * 使用節點名稱 * ：節點名稱用作臨時安裝密碼、並提供對 VM 主控台、 StorageGRID 安裝 API 和 SSH 的存取。
  - * 停用密碼 * ：不會使用暫存安裝密碼。如果您需要存取 VM 以偵錯安裝問題、請參閱"疑難排解安裝問題"。
  - * 使用自訂密碼 * ： * 自訂暫存密碼 = <password> * 所提供的值會用作暫存安裝密碼、並提供對 VM 主控台、 StorageGRID 安裝 API 和 SSH 的存取。

    您也可以省略 * 暫存密碼類型 * 參數、只指定 * 自訂暫存密碼 = <password> * 。

- **custom_entime_password=Windows** <password> 選用。在安裝期間存取 VM 主控台、 StorageGRID 安裝 API 和 SSH 時所使用的暫存密碼。如果將 *Temporary 密碼類型 * 設定為 * 使用節點名稱 * 或 * 停用密碼 * 、則會忽略。

節點專屬參數

每個節點都位於其本身的組態檔區段中。每個節點都需要下列設定：

- 區段標題會定義網格管理器中顯示的節點名稱。您可以指定節點的選用節點名稱參數來覆寫該值。
- * 節點類型 * ： VM_Admin_Node 、 VM_Storage_Node 或 VM_API_Gateway_Node
- * 儲存類型 * ：組合、資料或中繼資料。如果未指定、儲存節點的此選用參數預設為組合（資料和中繼資料）。如需更多資訊、請參閱 "儲存節點類型"。
- * GRID_NETWORD_IP*：網格網路上節點的IP位址。
- *管理網路IP：管理網路上節點的IP位址。僅當節點連接至管理網路且admin_network_config設為靜態時才需要。
- * Client_network_ip*：用戶端網路上節點的IP位址。僅當節點連接至用戶端網路時才需要、且此節點的用戶端網路組態設定為靜態時才需要。
- *管理IP：網格網路上主要管理節點的IP位址。使用您指定為主要管理節點GRID_NETNET_IP的值。如果省略此參數、節點會嘗試使用mDNS探索主要管理節點IP。如需更多資訊、請參閱 "網格節點如何探索主要管理節點"。

  主管理節點會忽略admin_ip參數。

- 未全域設定的任何參數。例如、如果節點附加至管理網路、但您未全域指定admin_network參數、則必須為節點指定這些參數。

主要管理節點

主要管理節點需要下列額外設定：

- 節點類型：VM_admin_Node
- 管理角色：主要

此範例項目適用於三個網路上的主要管理節點：

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

下列額外設定為主要管理節點的選用項目：

- 磁碟：根據預設、管理節點會額外指派兩個200 GB硬碟以供稽核和資料庫使用。您可以使用磁碟參數來增加這些設定。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  對於管理節點、執行個體必須永遠等於2。

儲存節點

儲存節點需要下列額外設定：

- 節點類型：VM_Storage_Node

  此範例項目適用於網格和管理網路上的儲存節點、但不適用於用戶端網路。此節點使用ADD_IP設定、在Grid Network上指定主要管理節點的IP位址。

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  第二個範例是針對用戶端網路上的儲存節點、客戶的企業網路原則指出、S3用戶端應用程式只能使用連接埠80或443存取儲存節點。範例組態檔使用port_remap、讓Storage Node在連接埠443上傳送和接收S3訊息。

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

最後一個範例會建立從連接埠22到連接埠3022的ssh流量對稱重新對應、但會明確設定傳入和傳出流量的值。

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

儲存節點可選用下列其他設定：

- 磁碟：根據預設、儲存節點會指派三個4 TB磁碟供R地理DB使用。您可以使用磁碟參數來增加這些設定。例如：

```
DISK = INSTANCES=16, CAPACITY=4096
```

- * Storage_type* ：根據預設、所有新的儲存節點都會設定為同時儲存物件資料和中繼資料、稱為 _ 組合 _ 儲存節點。您可以變更儲存節點類型、以僅儲存含有儲存類型參數的資料或中繼資料。例如：

```
STORAGE_TYPE = data
```

閘道節點

閘道節點需要下列額外設定：

- 節點類型：VM_API_Gateway

此範例項目是所有三個網路上的閘道節點範例。在此範例中、未在組態檔的全域區段中指定任何用戶端網路參數、因此必須為節點指定這些參數：

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG Client Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

非主要管理節點

非主要管理節點需要下列額外設定：

- 節點類型：VM_admin_Node
- 管理角色：非主要

此範例項目適用於不在用戶端網路上的非主要管理節點：

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG Grid Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

非主要管理節點可選用下列額外設定：

- 磁碟：根據預設、管理節點會額外指派兩個200 GB硬碟以供稽核和資料庫使用。您可以使用磁碟參數來增加這些設定。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  對於管理節點、執行個體必須永遠等於2。

執行Bash指令碼

您可以使用 `deploy-vsphere-ovftool.sh` Bash 指令碼和修改後的 deploy-vsphere-ovftool.ini 組態檔、在 VMware vSphere 中自動化 StorageGRID 節點的部署。

開始之前

您已為環境建立deploy-vsphere-ovftool.ini組態檔。

您可以輸入說明命令來使用 Bash 指令碼的可用說明(`-h/--help`）。例如：

```
./deploy-vsphere-ovftool.sh -h
```

或

```
./deploy-vsphere-ovftool.sh --help
```

步驟

1. 登入您用來執行Bash指令碼的Linux機器。
2. 切換至您擷取安裝歸檔的目錄。

   例如：

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. 若要部署所有網格節點、請執行Bash指令碼、並針對您的環境提供適當的選項。

   例如：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. 如果網格節點因為錯誤而無法部署、請解決此錯誤、然後僅針對該節點重新執行Bash指令碼。

   例如：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

當每個節點的狀態為「通過」時、即表示部署已完成。

```
Deployment Summary
+-----------------------------+----------+----------------------+
| node                        | attempts | status               |
+-----------------------------+----------+----------------------+
| DC1-ADM1                    |        1 | Passed               |
| DC1-G1                      |        1 | Passed               |
| DC1-S1                      |        1 | Passed               |
| DC1-S2                      |        1 | Passed               |
| DC1-S3                      |        1 | Passed               |
+-----------------------------+----------+----------------------+
```

自動化**StorageGRID** 功能組態

部署完網格節點之後、您可以自動化StorageGRID 設定該系統。

開始之前

- 您可以從安裝歸檔中得知下列檔案的位置。

檔案名稱	說明
configure-storagegrid.py	Python指令碼用於自動化組態
設定-storagegrid。same.json	用於指令碼的組態檔範例
設定-storagegrid。blank.json	與指令碼搭配使用的空白組態檔

- 您已建立 `configure-storagegrid.json`組態檔案。要創建此文件，您可以修改示例配置文件（`configure-storagegrid.blank.json`）（`configure-storagegrid.sample.json`或空白配置文件）。

> 儲存修改後的密碼部分的管理密碼和設定密碼 `configure-storagegrid.json`設定檔保存在安全的位置。安裝、擴充和維護過程都需要這些密碼。您還應該備份修改後的 `configure-storagegrid.json`設定檔並將其儲存在安全的位置。

關於這項工作

您可以使用 `configure-storagegrid.py` Python 指令碼和 `configure-storagegrid.json`網格組態檔來自動化 StorageGRID 系統的組態。

> 您也可以使用Grid Manager或安裝API來設定系統。

步驟

1. 登入您用來執行Python指令碼的Linux機器。
2. 切換至您擷取安裝歸檔的目錄。

   例如：

```
cd StorageGRID-Webscale-version/platform
```

其中 `platform`是 debs 、 rpms 或 vSphere 。

3. 執行Python指令碼並使用您建立的組態檔。

   例如：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

結果

恢復套件 `.zip`檔案會在組態程序期間產生、並下載到執行安裝和組態程序的目錄。您必須備份「恢復套件」檔案、以便StorageGRID 在一個或多個網格節點故障時、恢復該系統。例如、將其複製到安全的備份網路位置、以及安全的雲端儲存位置。

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。

如果您指定應產生隨機密碼、請開啟檔案、 `Passwords.txt`並尋找存取 StorageGRID 系統所需的密碼。

```
#####################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#####################################################################
```

系統會在顯示確認訊息時安裝及設定您的系統。StorageGRID

```
StorageGRID has been configured and installed.
```

相關資訊

- "瀏覽至Grid Manager"
- "安裝 REST API"

部署虛擬網格節點

收集有關您的 **VMware** 環境的 **StorageGRID** 資訊

在部署網格節點之前、您必須先收集網路組態和VMware環境的相關資訊。

更有效率的做法是對所有節點執行單一安裝、而非現在安裝部分節點、稍後再安裝部分節點。

VMware資訊

您必須存取部署環境、並收集有關VMware環境、為Grid、Admin和Client Networks建立的網路、以及您計畫用於儲存節點的儲存Volume類型的資訊。

您必須收集有關VMware環境的資訊、包括：

- 具有完成部署之適當權限的VMware vSphere帳戶使用者名稱和密碼。
- 每個 StorageGRID 節點虛擬機器的主機、資料存放區和網路組態資訊。

> VMware Live VMotion會使虛擬機器時鐘時間跳過、而且不支援任何類型的網格節點。雖然不多見、但時鐘時間不正確可能導致資料遺失或組態更新。

網格網路資訊

您必須收集StorageGRID 有關為「VMware Grid Network」（必填）所建立之VMware網路的資訊、包括：

- 網路名稱。
- 用於指派IP位址的方法、靜態或DHCP。
  - 如果您使用靜態IP位址、則每個網格節點（IP位址、閘道、網路遮罩）的必要網路詳細資料。
  - 如果您使用的是 DHCP 、則是 Grid Network 上主要管理節點的 IP 位址。如需詳細資訊、請參閱 "網格節點如何探索主要管理節點" 。

管理網路資訊

若節點將連線至選用StorageGRID 的「VMware管理網路」、您必須收集有關為此網路所建立的VMware網路的資訊、包括：

- 網路名稱。
- 用於指派IP位址的方法、靜態或DHCP。
  - 如果您使用靜態IP位址、則每個網格節點（IP位址、閘道、網路遮罩）的必要網路詳細資料。
  - 如果您使用的是 DHCP 、則是 Grid Network 上主要管理節點的 IP 位址。如需詳細資訊、請參閱 "網格節點如何探索主要管理節點" 。
- 管理網路的外部子網路清單（英文）。

用戶端網路資訊

對於要連線至選用StorageGRID 的「VMware用戶端網路」的節點、您必須收集有關為此網路建立的VMware網路的資訊、包括：

- 網路名稱。
- 用於指派IP位址的方法、靜態或DHCP。
- 如果您使用靜態IP位址、則每個網格節點（IP位址、閘道、網路遮罩）的必要網路詳細資料。

其他介面的相關資訊

安裝節點之後、您可以選擇性地在vCenter中新增主幹或存取介面至VM。例如、您可能想要將主幹介面新增至管理或閘道節點、以便使用VLAN介面來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、以便在高可用度（HA）群組中使用。

您新增的介面會顯示在「VLAN介面」頁面和「Grid Manager」的「HA群組」頁面上。

- 如果您新增主幹介面、請為每個新的父介面設定一或多個VLAN介面。請參閱。 "設定VLAN介面"
- 如果您新增存取介面、則必須將其直接新增至HA群組。請參閱。 "設定高可用度群組"

虛擬儲存節點的儲存磁碟區

您必須針對虛擬機器型儲存節點收集下列資訊：

- 您計劃新增的儲存磁碟區（儲存 LUN ）數量和大小。請參閱"儲存與效能需求"。

網格組態資訊

您必須收集資訊才能設定網格：

- Grid授權
- 網路時間傳輸協定（NTP）伺服器IP位址
- DNS 伺服器 IP 位址

為 **Linux** 部署建立 **StorageGRID** 節點組態檔

節點組態檔案是小型的文字檔、可提供StorageGRID 支援此支援所需的資訊、以啟動節點並將其連線至適當的網路和區塊儲存資源。節點組態檔案用於虛擬節點、不用於應用裝置節點。

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

節點組態檔案的位置

將每個 StorageGRID 節點的組態檔放在要執行節點的主機上的目錄中 `/etc/storagegrid/nodes`。例如、如果您計畫在主機 A 上執行一個管理節點、一個閘道節點和一個儲存節點、則必須在主機 A 上放置三個節點組態檔案 `/etc/storagegrid/nodes`。

您可以使用文字編輯器（例如vim或nANO）直接在每個主機上建立組態檔、也可以在其他位置建立組態檔、然後將其移至每個主機。

節點組態檔案的命名

組態檔的名稱很重要。格式為 `node-name.conf`、其中 `node-name`是您指派給節點的名稱。此名稱會顯示在StorageGRID 《Iserfor Installer（英文）：用於節點維護作業（例如節點移轉）。

節點名稱必須遵循下列規則：

- 必須是唯一的
- 必須以字母開頭
- 可以包含A到Z和a到z的字元
- 可包含0到9的數字
- 可包含一或多個連字號（-）
- 不得超過 32 個字元、不包括 `.conf`副檔名

主機服務不會剖析中任何不遵循這些命名慣例的檔案 `/etc/storagegrid/nodes`。

如果您的網格規劃了多站台拓撲、則一般的節點命名方案可能是：

```
site-nodetype-nodenumber.conf
```

例如、您可以在 Data Center 1 中使用第一個管理節點、在 Data Center 2 中使用 `dc1-adm1.conf`、第三個儲存節點 `dc2-sn3.conf`。不過、只要所有節點名稱都遵循命名規則、您就可以使用任何想要的配置。

節點組態檔案的內容

組態檔案包含金鑰 / 值配對、每行一個金鑰和一個值。針對每個金鑰 / 值配對、請遵循下列規則：

- 密鑰和值必須用等號分隔(=）和可選空格。
- 金鑰不得包含空格。
- 這些值可以包含內嵌空格。
- 任何前置或後置空白都會被忽略。

下表定義所有支援金鑰的值。每個金鑰都有下列指定之一：

- * 必要 * ：每個節點或指定節點類型都需要
- * 最佳實務做法 * ：雖然建議選用
- * 選用 * ：所有節點皆可選用

管理網路金鑰

管理IP

價值	指定
您要用於安裝基於 Linux 的節點的管理節點的網格網路 IPv4 位址。對於恢復，如果可用，請使用主管理節點的 IP；否則，使用非主管理節點的 IP。如果省略此參數，節點將嘗試使用 mDNS 發現主管理節點。 "網格節點如何探索主要管理節點"	最佳實務做法

admin_network_config

價值	指定
DHCP、靜態或停用	選用

admin_network_esl

價值	指定
以逗號分隔的子網路清單、以 CIDR 表示法表示此節點應使用管理網路閘道進行通訊。 範例： `172.16.0.0/21,172.17.0.0/21`	選用

管理網路閘道

價值	指定

此節點的本機管理網路閘道的IPv4位址。必須位於由admin_network_ip和admin_network_mask定義的子網路上。DHCP設定的網路會忽略此值。
 	
範例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	如果指定、則為必`ADMIN_NETWORK_ESL`填。否則為選用。

admin_network_ip

價值	指定

管理網路上此節點的IPV4位址。只有當 Admin_network_config = 靜態時才需要此金鑰；請勿將其指定為其他值。
 	
範例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	當 Admin_network_config = 靜態時為必填。
	
	否則為選用。

admin_network_MAC

價值	指定
容器中管理網路介面的MAC位址。 此欄位為選用欄位。如果省略、會自動產生MAC位址。 必須為6對以分號分隔的十六進位數字。 範例： `b2:9c:02:c2:27:10`	選用

admin_network_mask

價值	指定

管理網路上此節點的IPv4網路遮罩。當 Admin_network_config = 靜態時、請指定此機碼；不要指定其他值。
 	
範例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	如果指定了 Admin_network_ip 且 Admin_network_config = static 、則為必填。
	
	否則為選用。

admin_network_MTU

價值	指定

管理網路上此節點的最大傳輸單元（MTU）。如果 Admin_network_config = DHCP 、請勿指定。如果指定、則值必須介於1280和9216之間。如果省略、則使用1500。
 	
如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。
 	
重要：網路的MTU值必須符合節點所連接之交換器連接埠上所設定的值。否則、可能會發生網路效能問題或封包遺失。
 	
範例：
 	
`1500`
 	
`8192`
	選用

管理網路目標

價值	指定

將用於StorageGRID 由節點存取管理網路的主機裝置名稱。僅支援網路介面名稱。一般而言、您使用的介面名稱不同於GRID_NETWORD_Target或用戶端網路目標所指定的介面名稱。
 	
• 注意 * ：請勿使用連結或橋接裝置作為網路目標。在連結裝置上設定VLAN（或其他虛擬介面）、或使用橋接器和虛擬乙太網路（vith）配對。
 	
最佳實務做法：即使此節點最初沒有管理網路IP位址、仍請指定值。然後、您可以在稍後新增管理網路IP位址、而不需重新設定主機上的節點。
 	
範例：
 	
`bond0.1002`
 	
`ens256`
	最佳實務做法

管理網路目標類型

價值	指定
DedicatedInterface（這是唯一支援的值。）	選用

管理網路目標類型介面複製**_MAC**

價值	指定
是非題 將金鑰設為「true」、以使用StorageGRID 管理網路上主機目標介面的MAC位址來使該容器失效。 有關 Linux 的 MAC 克隆的更多詳細信息，請參閱"MAC位址複製的考量與建議"	最佳實務做法

admin_role

價值	指定
主要或非主要 只有當 node_type = vm_admin_Node 時、才需要此金鑰；請勿針對其他節點類型指定此金鑰。	node_type = vm_admin_Node 時需要 否則為選用。

封鎖裝置金鑰

block_device_napping_logs

價值	指定

此節點將用於持續儲存稽核記錄的區塊裝置特殊檔案路徑和名稱。
 	
範例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	節點的 node_type = vm_admin_Node 為必要項目。請勿為其他節點類型指定。

block_device_RANGEDB_nnn

價值	指定

此節點將用於持續物件儲存的區塊裝置特殊檔案路徑和名稱。只有節點類型 = VM_Storage_Node 的節點才需要此金鑰；請勿針對其他節點類型指定此金鑰。
 	
只需要block_device_rNGedb_000；其餘的則為選用項目。為block_device_RANGEDB_000指定的區塊裝置必須至少為4 TB、其他的則可能較小。
 	
不要留下落差。如果您指定block_device_RANGEDB_005、您也必須指定block_device_RANGEDB_004。
 	
附註：為了與現有部署相容、升級的節點支援兩位數金鑰。
 	
範例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	必要：
	
	BLOCK_DEVICE_RANGEDB_000
	
	選用：
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

block_device_Tables

價值	指定

此節點將用於持續儲存資料庫表格的區塊裝置特殊檔案路徑和名稱。只有節點類型 = VM_Admin_Node 的節點才需要此金鑰；請勿針對其他節點類型指定此金鑰。
 	
範例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	必要

block_device_var_local

價值	指定

此節點將用於其持續儲存的區塊裝置特殊檔案路徑和名稱 `/var/local`。
 	
範例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	必要

用戶端網路金鑰

用戶端網路組態

價值	指定
DHCP、靜態或停用	選用

用戶端網路閘道

價值	指定

此節點的本機用戶端網路閘道的IPv4位址、必須位於用戶端網路IP和用戶端網路遮罩所定義的子網路上。DHCP設定的網路會忽略此值。
 	
範例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	選用

用戶端網路**IP**

價值	指定

用戶端網路上此節點的IPv4位址。
 	
只有當 client_network_config = static 時才需要此金鑰；請勿將其指定為其他值。
 	
範例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	client_network_config = 靜態時需要
	
	否則為選用。

用戶端網路**_MAC**

價值	指定
容器中用戶端網路介面的MAC位址。 此欄位為選用欄位。如果省略、會自動產生MAC位址。 必須為6對以分號分隔的十六進位數字。 範例： `b2:9c:02:c2:27:20`	選用

用戶端網路遮罩

價值	指定

用戶端網路上此節點的IPV4網路遮罩。
 	
當 client_network_config = static 時、請指定此機碼；不要指定其他值。
 	
範例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	如果指定了 client_network_ip 且 client_network_config = static 、則為必要
	
	否則為選用。

用戶端網路**MTU**

價值	指定

用戶端網路上此節點的最大傳輸單位（MTU）。不要指定 client_network_config = DHCP 。如果指定、則值必須介於1280和9216之間。如果省略、則使用1500。
 	
如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。
 	
重要：網路的MTU值必須符合節點所連接之交換器連接埠上所設定的值。否則、可能會發生網路效能問題或封包遺失。
 	
範例：
 	
`1500`
 	
`8192`
	選用

用戶端網路目標

價值	指定

供客戶端網路存取使用StorageGRID 的主機裝置名稱、由支援節點存取。僅支援網路介面名稱。一般而言、您使用的介面名稱不同於GRID_NETWORD_Target或admin_network_target所指定的介面名稱。
 	
• 注意 * ：請勿使用連結或橋接裝置作為網路目標。在連結裝置上設定VLAN（或其他虛擬介面）、或使用橋接器和虛擬乙太網路（vith）配對。
 	
*最佳實務做法：*指定值、即使此節點一開始不會有用戶端網路IP位址。之後您可以新增用戶端網路IP位址、而不需重新設定主機上的節點。
 	
範例：
 	
`bond0.1003`
 	
`ens423`
	最佳實務做法

用戶端網路目標類型

價值	指定
DedicatedInterface（這是唯一支援的值。）	選用

用戶端網路目標類型介面複製_**MAC**

價值	指定
是非題 將金鑰設為「true」、使StorageGRID 「支援」容器使用用戶端網路上主機目標介面的MAC位址。 有關 Linux 的 MAC 克隆的更多詳細信息，請參閱"MAC位址複製的考量與建議"	最佳實務做法

網格網路金鑰

GRID_NET_CONFIG

價值	指定
靜態或DHCP 如果未指定、則預設為靜態。	最佳實務做法

GRID_NET_gateway

價值	指定
此節點的本機網格網路閘道的IPv4位址、必須位於GRID_NETNET_IP和GRID_NET_MASK定義的子網路上。DHCP設定的網路會忽略此值。 如果Grid Network是沒有閘道的單一子網路、請使用子網路的標準閘道位址（X YY.1）或此節點的GRID_NETNET_IP值；這兩個值都能簡化未來可能的Grid Network擴充。	必要

GRID_NET_IP

價值	指定

Grid Network上此節點的IPv4位址。只有當 GRIN_NETWORD_CONFIG = STATIC 時才需要此機碼；不要為其他值指定此機碼。
 	
範例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	grid_network_config = 靜態時需要
	
	否則為選用。

GRID_NET_MAC

價值	指定
容器中Grid Network介面的MAC位址。 必須為6對以分號分隔的十六進位數字。 範例： `b2:9c:02:c2:27:30`	選用 如果省略、會自動產生MAC位址。

GRID_NET_MA遮 罩

價值	指定

Grid Network上此節點的IPV4網路遮罩。當 GRIN_NETWORD_CONFIG = 靜態時指定此機碼；不要為其他值指定此機碼。
 	
範例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	指定 GRIDE_NETWORD_IP 且 GRID_NETWORD_CONFIG = 靜態時需要。
	
	否則為選用。

GRID_NET_MTU

價值	指定

Grid Network上此節點的最大傳輸單位（MTU）。不要指定grid_network_config = DHCP 。如果指定、則值必須介於1280和9216之間。如果省略、則使用1500。
 	
如果您要使用巨型框架、請將MTU設為適合巨型框架的值、例如9000。否則、請保留預設值。
 	
重要：網路的MTU值必須符合節點所連接之交換器連接埠上所設定的值。否則、可能會發生網路效能問題或封包遺失。
 	
重要：為獲得最佳網路效能、所有節點都應在其Grid Network介面上設定類似的MTU值。如果個別節點上Grid Network的MTU設定有顯著差異、則會觸發* Grid Network MTU mismis*警示。所有網路類型的 MTU 值都不一定相同。
 	
範例：
 	
`1500`
 	
`8192`
	選用

GRID_NETWORD_target

價值	指定

您將用於StorageGRID 由節點存取Grid Network的主機裝置名稱。僅支援網路介面名稱。一般而言、您使用的介面名稱與針對admin_network_target或client_network_target所指定的介面名稱不同。
 	
• 注意 * ：請勿使用連結或橋接裝置作為網路目標。在連結裝置上設定VLAN（或其他虛擬介面）、或使用橋接器和虛擬乙太網路（vith）配對。
 	
範例：
 	
`bond0.1001`
 	
`ens192`
	必要

GRID_NETWORD_TAR_type

價值	指定
DedicatedInterface（這是唯一支援的值。）	選用

GRID_NETWORD_PROM_type_interface_clone _MAC

價值	指定
是非題 將金鑰的值設為「true」、使StorageGRID 該容器使用Grid Network上主機目標介面的MAC位址。 有關 Linux 的 MAC 克隆的更多詳細信息，請參閱"MAC位址複製的考量與建議"	最佳實務做法

安裝密碼金鑰（暫時）

Custom_Temporary 密碼雜湊

價值	指定
對於主要管理節點、請在安裝期間為 StorageGRID 安裝 API 設定預設的暫時密碼。 • 注意 * ：僅在主要管理節點上設定安裝密碼。如果您嘗試在其他節點類型上設定密碼、節點組態檔案的驗證將會失敗。 安裝完成後、設定此值不會生效。 如果省略此金鑰、則預設不會設定暫存密碼。或者、您也可以使用 StorageGRID 安裝 API 來設定暫時密碼。 密碼必須是 SHA-512 密碼雜湊、格式 `$6$<salt>$<password hash>`必須 `crypt()`至少 8 個字元、不得超過 32 個字元。 此雜湊可以使用 CLI 工具產生、例如在 SHA-512 模式中使用 `openssl passwd`命令。	最佳實務做法

介面金鑰

interface_target_nnnn

價值	指定
要新增至此節點的額外介面名稱和選用說明。您可以為每個節點新增多個額外介面。 對於 *nnn* 、請為您要新增的每個 interface_target 項目指定唯一的編號。 針對該值、指定裸機主機上實體介面的名稱。接著、您可以選擇性地新增一個逗號、並提供介面說明、該介面會顯示在「VLAN介面」頁面和「HA群組」頁面上。 範例： `INTERFACE_TARGET_0001=ens256, Trunk` 如果您新增主幹介面、則必須在StorageGRID 功能鏈路的資訊鏈路中設定VLAN介面。如果您新增存取介面、可以直接將介面新增至 HA 群組、而不需要設定 VLAN 介面。	選用

最大 **RAM** 金鑰

最大**RAM**

價值	指定
允許此節點使用的最大RAM量。如果省略此金鑰、則節點沒有記憶體限制。為正式作業層級節點設定此欄位時、請指定至少24 GB、且16至32 GB的值、小於系統總RAM。 附註：RAM值會影響節點的實際中繼資料保留空間。請參閱"中繼資料保留空間的說明"。 此欄位的格式為 *numberunit*、其中 *unit*`可以是 `b、、 `km`或 `g。  範例：  `24g`  `38654705664b` 附註：如果您要使用此選項、則必須啟用記憶體cGroups的核心支援。	選用

節點類型金鑰

節點類型

價值	指定
節點類型： • VM_admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway	必要

儲存類型

價值	指定
定義儲存節點包含的物件類型。如需更多資訊、請參閱 "儲存節點類型"。只有節點類型 = VM_Storage_Node 的節點才需要此金鑰；請勿針對其他節點類型指定此金鑰。儲存類型： • 合併 • 資料 • 中繼資料 • 注意 * ：如果未指定儲存節點類型、則預設會將儲存節點類型設為組合（資料和中繼資料）。	選用

連接埠重新對應鍵

對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"移除裸機主機上的連接埠重新對應"。

連接埠重新對應

價值	指定
重新對應節點用於內部網格節點通訊或外部通訊的任何連接埠。如果企業網路原則限制 StorageGRID 使用的一或多個連接埠"外部通訊"、則必須重新對應連接埠、如或中所述"內部網格節點通訊"。 • 重要 * ：請勿重新對應您打算用來設定負載平衡器端點的連接埠。 附註：如果只設定port_remap、則指定的對應會同時用於傳入和傳出通訊。如果也指定port_remap_inbound、則port_remap僅適用於傳出通訊。 使用的格式為： *network type/protocol/default port used by grid node/new port*、其中 `*network type*`是網格、管理或用戶端、而且 `*protocol*` 是 TCP 或 UDP 。 範例： `PORT_REMAP = client/tcp/18082/443` 您也可以使用以逗號分隔的清單來重新對應多個連接埠。 範例： `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	選用

連接埠_remap_inbound

價值	指定
將傳入通訊重新對應至指定的連接埠。如果您指定 port_remap_inbound 、但未指定 port_remap 值、則連接埠的輸出通訊將維持不變。 • 重要 * ：請勿重新對應您打算用來設定負載平衡器端點的連接埠。 使用的格式為： *network type/protocol/remapped port /default port used by grid node*、其中 `*network type*`是網格、管理或用戶端、而且 `*protocol*` 是 TCP 或 UDP 。 範例： `PORT_REMAP_INBOUND = grid/tcp/3022/22` 您也可以使用以逗號分隔的清單來重新對應多個傳入連接埠。 範例： `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	選用

網格節點如何在 **StorageGRID** 中探索主要管理節點

網格節點會與主要管理節點進行通訊、以進行組態和管理。每個網格節點都必須知道網格網路上主要管理節點的IP位址。

若要確保網格節點可以存取主要管理節點、您可以在部署節點時執行下列任一動作：

- 您可以使用admin_IP參數手動輸入主管理節點的IP位址。
- 您可以省略admin_ip參數、讓網格節點自動探索該值。當Grid Network使用DHCP將IP位址指派給主要管理節點時、自動探索特別有用。

主要管理節點的自動探索是使用多點傳送網域名稱系統（ mDNS ）來完成。當主要管理節點初次啟動時、它會使用mDNS發佈其IP位址。然後、同一子網路上的其他節點便可查詢IP位址、並自動取得該位址。不過、由於多點傳送 IP 流量通常無法在子網路之間路由、因此其他子網路上的節點無法直接取得主要管理節點的 IP 位址。

如果您使用自動探索：

- 您必須在主管理節點未直接附加的任何子網路上、包含至少一個網格節點的Admin_IP設定。然後、此網格節點會發佈子網路上其他節點的主要管理節點IP位址、以便使用mDNS進行探索。
- 確保您的網路基礎架構支援在子網路內傳遞多點傳送IP流量。

使用 **VMware vSphere** 將網格節點部署為 **StorageGRID** 的虛擬機

您可以使用VMware vSphere Web Client將每個網格節點部署為虛擬機器。在部署期間、每個網格節點都會建立並連線至一個或多個StorageGRID 站台網路。

如果您需要部署任何 StorageGRID 應用裝置儲存節點、請參閱 "部署應用裝置儲存節點"。

您也可以選擇重新對應節點連接埠、或在開啟節點電源之前增加節點的CPU或記憶體設定。

開始之前

- 您已檢閱如何"規劃並準備安裝"、並瞭解軟體、 CPU 和 RAM 、以及儲存和效能的需求。
- 您熟悉VMware vSphere Hypervisor、並有在此環境中部署虛擬機器的經驗。

此 `open-vm-tools`套件是類似 VMware Tools 的開放原始碼實作、隨附於 StorageGRID 虛擬機器中。您不需要手動安裝 VMware Tools 。

- 您已下載並擷取StorageGRID 適用於VMware的正確版本的安裝檔案。

如果您將新節點部署為擴充或還原作業的一部分、則必須使用StorageGRID 目前在網格上執行的版本版本。

- 您有虛擬機器磁碟(`.vmdk` （ StorageGRID Virtual Machine Disk ）檔案：

```
NetApp-SG-version-SHA.vmdk
```

- 您可以 `.ovf`為要部署的每種網格節點提供和 `.mf`檔案：

檔案名稱	說明
vSphere-primer-admin.OVF vSphere-prime-admin.mf	主要管理節點的範本檔案和資訊清單檔案。

檔案名稱	說明
vsphere-non-prime-admin.OVF vsphere-non-prime-admin.mf	非主要管理節點的範本檔案和資訊清單檔案。
vSphere-storage。OVF vSphere-storage。mf	儲存節點的範本檔案和資訊清單檔案。
vSphere-gateway.OVF vSphere-gateway.mf	閘道節點的範本檔案和資訊清單檔案。

- `.vdmk .ovf`、和 `.mf`檔案都位於同一個目錄中。
- 您有計畫將故障網域降至最低。例如、您不應在單一 vSphere ESXi 主機上部署所有閘道節點。

> 在正式作業部署中、請勿在單一虛擬機器上執行多個儲存節點。如果這會造成無法接受的故障網域問題、請勿在同一 ESXi 主機上執行多個虛擬機器。

- 如果您要將節點部署為擴充或還原作業的一部分、則您擁有"擴充StorageGRID 功能的說明"或"恢復與維護指示"。
- 如果您要將 StorageGRID 節點部署為虛擬機器、並從 NetApp ONTAP 系統指派儲存設備、則您已確認該磁碟區未啟用 FabricPool 分層原則。例如、如果 StorageGRID 節點在 VMware 主機上以虛擬機器的形式執行、請確保節點的資料存放區備份磁碟區未啟用 FabricPool 分層原則。停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

> 切勿使用FabricPool 無法將StorageGRID 任何與還原StorageGRID 本身相關的資料分層。將StorageGRID 資料分層還原StorageGRID 至物件、可增加疑難排解和作業複雜度。

關於這項工作

請遵循下列指示、在開始部署VMware節點、在擴充中新增VMware節點、或是在還原作業中更換VMware節點。除步驟中所述者外、所有節點類型（包括管理節點、儲存節點和閘道節點）的節點部署程序都相同。

如果您要安裝新StorageGRID 的一套功能完善的系統：

- 您可以依任何順序部署節點。
- 您必須確保每個虛擬機器都能透過Grid Network連線至主要管理節點。
- 您必須先部署所有網格節點、才能設定網格。

如果您要執行擴充或還原作業：

- 您必須確保新的虛擬機器可透過 Grid Network 連線至所有其他節點。

如果您需要重新對應任何節點的連接埠、請在連接埠重新對應組態完成之前、不要開啟新節點的電源。

> 對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"移除裸機主機上的連接埠重新對應"。

步驟

1. 使用vCenter部署OVF範本。

如果您指定URL、請指向包含下列檔案的資料夾。否則、請從本機目錄中選取每個檔案。

```
NetApp-SG-version-SHA.vmdk
vsphere-node.ovf
vsphere-node.mf
```

例如、如果這是您要部署的第一個節點、請使用這些檔案來部署StorageGRID 適用於您的列舉系統的主要管理節點：

```
NetApp-SG-version-SHA.vmdk
vsphere-primary-admin.ovf
vsphere-primary-admin.mf
```

2. 提供虛擬機器的名稱。

   標準做法是針對虛擬機器和網格節點使用相同的名稱。

3. 將虛擬機器放置在適當的vApp或資源池中。
4. 如果您要部署主要管理節點、請閱讀並接受終端使用者授權合約。

   視您的vCenter版本而定、接受終端使用者授權合約、指定虛擬機器名稱及選取資料存放區的步驟順序會有所不同。

5. 選取虛擬機器的儲存設備。

   如果您要將節點部署為還原作業的一部分、請執行中的指示儲存恢復步驟、以新增虛擬磁碟、從故障的網格節點重新附加虛擬硬碟、或兩者。

   部署儲存節點時、請使用3個以上的儲存磁碟區、每個儲存磁碟區大小為4 TB以上。您必須將至少4 TB指派給Volume 0。

   > Storage Node .OVF檔案定義多個VMDK以供儲存。除非這些VMDK符合您的儲存需求、否則在開啟節點電源之前、您應該先將其移除、並指派適當的VMDK或RDM用於儲存設備。VMDK更常用於VMware環境、而且易於管理、而對於使用較大物件大小（例如大於100 MB）的工作負載、RDM則可提供較佳的效能。

   > 有些StorageGRID 版本的安裝可能會使用比一般虛擬化工作負載更大、更活躍的儲存磁碟區。您可能需要調整某些 Hypervisor 參數、例如 `MaxAddressableSpaceTB`、才能達到最佳效能。如果效能不佳、請聯絡您的虛擬化支援資源、以判斷您的環境是否能從工作負載特定的組態調校中獲益。

6. 選取「網路」。

   為每個來源網路選取目的地網路、以判斷StorageGRID 節點將使用哪些哪些「樣」網路。

   - 網格網路為必填項目。您必須在vSphere環境中選取目的地網路。+ 網格網路用於所有內部 StorageGRID 流量。它可在網格中的所有節點之間、跨越所有站台和子網路提供連線。Grid Network上

的所有節點都必須能夠與所有其他節點通訊。

- 如果您使用管理網路、請在vSphere環境中選取不同的目的地網路。如果您不使用管理網路、請選取您為網格網路選取的相同目的地。
- 如果您使用用戶端網路、請在vSphere環境中選取不同的目的地網路。如果您不使用用戶端網路、請選取您為 Grid Network 選取的相同目的地。
- 如果您使用管理或用戶端網路、則節點不必位於同一個管理或用戶端網路上。

7. 對於 * 自訂範本 * 、請設定所需的 StorageGRID 節點內容。

a. 輸入*節點名稱*。

> ⓘ 如果要恢復網格節點、則必須輸入要恢復的節點名稱。

b. 使用 * 暫存安裝密碼 * 下拉式清單來指定暫存安裝密碼、以便在新節點加入網格之前、您可以存取 VM 主控台或 StorageGRID 安裝 API 、或使用 SSH 。

> ⓘ 暫存安裝密碼僅在節點安裝期間使用。將節點新增至網格之後、您可以使用存取該節點"節點主控台密碼"、此功能列於「恢復套件」的檔案中 `Passwords.txt`。

- * 使用節點名稱 * ：您為「 * 節點名稱 * 」欄位提供的值會用作暫時安裝密碼。
- * 使用自訂密碼 * ：使用自訂密碼作為暫時安裝密碼。
- * 停用密碼 * ：不會使用暫存安裝密碼。如果您需要存取 VM 以偵錯安裝問題、請參閱"疑難排解安裝問題"。

c. 如果選擇 * 使用自定義密碼 * ，請在 * 自定義密碼 * 字段中指定要使用的臨時安裝密碼。

d. 在「* Grid Network（eth0）」區段中、針對 Grid網路IP組態*選取「Static」（靜態）或「DHCP」（DHCP）。

- 如果選擇靜態、請輸入* Grid網路IP*、* Grid網路遮罩*、* Grid網路閘道*及* Grid網路MTU*。
- 如果選擇DHCP、* Grid網路IP*、* Grid網路遮罩*和* Grid網路閘道*會自動指派。

e. 在*主管理IP*欄位中、輸入Grid Network主要管理節點的IP位址。

如果您省略主要管理節點IP位址、當主要管理節點或至少有一個已設定ADD_IP的其他網格節點存在於同一個子網路時、就會自動探索IP位址。不過、建議您在此處設定主要管理節點IP位址。

f. 在*管理網路（eth1*）*區段中、針對*管理網路IP組態*選取靜態、DHCP或停用。

- 如果您不想使用管理網路、請選取「已停用」、然後輸入 * 0.0.0.0* 作為管理網路 IP 。您可以將其他欄位保留空白。
- 如果選擇靜態、請輸入*管理網路IP*、管理網路遮罩、管理網路閘道*和*管理網路**MTU**。
- 如果選擇靜態、請輸入*管理網路外部子網路清單*。您也必須設定閘道。
- 如果您選取DHCP、系統會自動指派*管理網路IP*、管理網路遮罩*和*管理網路閘道。

g. 在*用戶端網路（eth2）*區段中、針對*用戶端網路IP組態*選取靜態、DHCP或停用。

- 如果您不想使用用戶端網路、請選取「已停用」、然後輸入 **0.0.0.0** 作為用戶端網路 IP 。您可以將其他欄位保留空白。
- 如果選擇靜態、請輸入*用戶端網路IP*、用戶端網路遮罩、*用戶端網路閘道*及*用戶端網路MTU *。

- 如果選擇DHCP、用戶端網路**IP**、*用戶端網路遮罩*和*用戶端網路閘道*會自動指派。

8. 檢閱虛擬機器組態並進行必要的變更。
9. 準備好完成後、選取* Finish（完成）*即可開始上傳虛擬機器。
10. [[stae_recovery儲存設備]如果您將此節點部署為還原作業的一部分、但這不是完整節點還原、請在部署完成後執行下列步驟：

    a. 在虛擬機器上按一下滑鼠右鍵、然後選取*編輯設定*。

    b. 選取已指定用於儲存設備的每個預設虛擬硬碟、然後選取*移除*。

    c. 視您的資料還原情況而定、請根據儲存需求新增虛擬磁碟、重新連接先前移除的故障網格節點所保留的任何虛擬硬碟、或兩者。

    請注意下列重要準則：

    - 如果您要新增磁碟、則應該使用與節點還原之前使用的相同類型儲存設備。
    - Storage Node .OVF檔案定義多個VMDK以供儲存。除非這些VMDK符合您的儲存需求、否則在開啟節點電源之前、您應該先將其移除、並指派適當的VMDK或RDM用於儲存設備。VMDK更常用於VMware環境、而且易於管理、而對於使用較大物件大小（例如大於100 MB）的工作負載、RDM則可提供較佳的效能。

11. 如果您需要重新對應此節點使用的連接埠、請依照下列步驟進行。

    如果您的企業連網原則限制對 StorageGRID 所使用的一個或多個連接埠的存取，則可能需要重新對應連接埠。請參閱 "網路準則" 以了解 StorageGRID 使用的連接埠。

    > ⓘ 請勿重新對應負載平衡器端點中使用的連接埠。

    a. 選取新的VM。

    b. 從「Configure（設定）」索引標籤、選取「* Settings*>* vApp Options （*設定>* vApp選項vApp選項*的位置取決於vCenter的版本。

    c. 在「內容」表格中、找出port_remap_inbound和port_remap。

    d. 若要對稱對應連接埠的傳入和傳出通訊、請選取* port_remap*。

    > ⓘ 對連接埠重新映射的支援已棄用，並將在未來的版本中刪除。若要刪除重新映射的端口，請參閱"移除裸機主機上的連接埠重新對應"。

    > ⓘ 如果只設定port_remap、則您指定的對應會同時套用至傳入和傳出通訊。如果也指定port_remap_inbound、則port_remap僅適用於傳出通訊。

    i. 選擇*設定值*。

    ii. 輸入連接埠對應：

    ```
    <network type>/<protocol>/<default port used by grid node>/<new port>
    ```

    `<network type>`為網格、管理或用戶端、且 `<protocol>`為 TCP 或 UDP 。

    例如、若要從連接埠22重新對應ssh流量至連接埠3022、請輸入：

```
client/tcp/22/3022
```

您可以使用以逗號分隔的清單重新對應多個連接埠。

例如：

```
client/tcp/18082/443, client/tcp/18083/80
```

i. 選擇*確定*。

e. 若要指定用於節點傳入通訊的連接埠、請選取* port_remap_inbound *。

> 如果您指定 port_remap_inbound 、但未指定 port_remap 值、則連接埠的輸出通訊將維持不變。

i. 選擇*設定值*。

ii. 輸入連接埠對應：

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

`<network type>`為網格、管理或用戶端、且 `<protocol>`為 TCP 或 UDP 。

例如、若要重新對應傳送至連接埠3022的傳入SSH流量、以便網格節點在連接埠22接收該流量、請輸入下列命令：

```
client/tcp/3022/22
```

您可以使用以逗號分隔的清單重新對應多個傳入連接埠。

例如：

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. 選擇*確定*

12. 如果您要從預設設定增加節點的CPU或記憶體：

a. 在虛擬機器上按一下滑鼠右鍵、然後選取*編輯設定*。

b. 視需要變更CPU數量或記憶體容量。

將*記憶體保留*設為與分配給虛擬機器的*記憶體*大小相同的大小。

c. 選擇*確定*。

13. 開啟虛擬機器電源。

完成後

如果您將此節點部署為擴充或還原程序的一部分、請返回這些指示以完成此程序。

您可以使用範例節點組態檔來協助設定StorageGRID 適用於您的整套系統的節點組態檔。這些範例顯示所有類型網格節點的節點組態檔。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

對於大多數節點、您可以在使用Grid Manager或安裝API設定網格時、新增管理和用戶端網路定址資訊（IP、遮罩、閘道等）。例外情況是主要管理節點。若要瀏覽至主要管理節點的管理網路IP以完成網格組態（例如、網格網路未路由傳送）、您必須在其節點組態檔中設定主要管理節點的管理網路連線。範例中顯示了這一點。

在這些範例中、用戶端網路目標已設定為最佳實務做法、即使用戶端網路預設為停用。

主管理節點範例

- 範例檔案名稱 * ： `/etc/storagegrid/nodes/dc1-adm1.conf`

範例檔案內容：

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

儲存節點範例

- 範例檔案名稱： * `/etc/storagegrid/nodes/dc1-sn1.conf`

範例檔案內容：

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

閘道節點範例

- 範例檔案名稱：* `/etc/storagegrid/nodes/dc1-gw1.conf`

範例檔案內容：

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非主要管理節點的範例

- 範例檔案名稱：* `/etc/storagegrid/nodes/dc1-adm2.conf`

範例檔案內容：

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

在 **Linux** 上驗證 **StorageGRID** 組態

在中為每個 StorageGRID 節點建立組態檔案之後 `/etc/storagegrid/nodes`、您必須驗證這些檔案的內容。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

若要驗證組態檔的內容、請在每個主機上執行下列命令：

```
sudo storagegrid node validate all
```

如果檔案正確、輸出會顯示每個組態檔的* passed *、如範例所示。

當僅在中繼資料節點上使用一個 LUN 時、您可能會收到可忽略的警告訊息。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

對於自動安裝，您可以使用命令中的或 `--quiet`選項 `storagegrid`（例如 `storagegrid --quiet…`）來抑制此輸出 `-q`。如果您抑制輸出、則在偵測到任何組態警告或錯誤時、命令會有非零的結束值。

如果組態檔不正確、問題會顯示為*警告*和*錯誤*、如範例所示。如果發現任何組態錯誤、您必須先加以修正、

才能繼續安裝。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

在 **Linux** 上啟動 **StorageGRID** 主機服務

若要啟動StorageGRID 您的支援節點、並確保在主機重新開機後重新啟動節點、您必須啟用StorageGRID 並啟動該支援中心服務。

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

步驟

1. 在每個主機上執行下列命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 執行下列命令以確保部署繼續進行：

```
sudo storagegrid node status node-name
```

3. 如果有任何節點傳回「未執行」或「已停止」的狀態、請執行下列命令：

```
sudo storagegrid node start node-name
```

4. 如果您先前已啟用並啟動StorageGRID 了「支援服務」（或如果您不確定服務是否已啟用並啟動）、請同時執行下列命令：

```
sudo systemctl reload-or-restart storagegrid
```

了解 **StorageGRID** 安裝 **REST API**

提供執行安裝工作所需的安裝API。StorageGRID StorageGRID

API使用Swagger開放原始碼API平台來提供API文件。Swagger可讓開發人員和非開發人員在使用者介面中與API互動、說明API如何回應參數和選項。本文件假設您熟悉標準網路技術和 JSON 資料格式。

> 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。

每個REST API命令都包含API的URL、HTTP動作、任何必要或選用的URL參數、以及預期的API回應。

安裝**API StorageGRID**

StorageGRID 安裝 API 僅在您初次設定 StorageGRID 系統、以及需要執行主要管理節點還原時可用。安裝API可透過HTTPS從Grid Manager存取。

若要存取 API 文件、請前往主要管理節點上的安裝網頁、然後從功能表列選取 * 說明 * > * API 文件 * 。

《程式集安裝API》包含下列各節：StorageGRID

- **config**：與產品版本和 API 版本相關的操作。您可以列出產品發行版本以及該版本支援的 API 主要版本。
- **grid**：網格層級組態操作。您可以取得和更新網格設定，包括網格詳細資訊、Grid Network 子網路、網格密碼以及 NTP 和 DNS 伺服器 IP 位址。
- 節點：節點層級組態操作。您可以擷取網格節點清單、刪除網格節點、設定網格節點、檢視網格節點、重設網格節點的組態。
- **provision**：資源配置操作。您可以啟動資源配置操作並檢視資源配置操作的狀態。

- 恢復：主要管理節點恢復作業。您可以重設資訊、上傳 Recovery Package、啟動恢復，以及檢視恢復作業的狀態。
- **recovery-package**：下載 Recovery Package 的操作。
- **sites**：站台層級的組態操作。您可以建立、檢視、刪除和修改站台。
- **temporary-password**: 在安裝期間對臨時密碼執行操作，以保護 mgmt-api 的安全。

疑難排解 StorageGRID 安裝問題

如果在安裝StorageGRID 您的作業系統時發生任何問題、您可以存取安裝記錄檔。技術支援人員也可能需要使用安裝記錄檔來解決問題。

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

Linux

下列安裝記錄檔可從執行每個節點的容器取得：

- `/var/local/log/install.log`（可在所有網格節點上找到）
- `/var/local/log/gdu-server.log`（可在主要管理節點上找到）

下列安裝記錄檔可從主機取得：

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

若要瞭解如何存取記錄檔，請參閱"收集記錄檔和系統資料"。

VMware

以下是主要的安裝記錄檔、可能需要技術支援才能解決問題。

- `/var/local/log/install.log`（可在所有網格節點上找到）
- `/var/local/log/gdu-server.log`（可在主要管理節點上找到）

虛擬機器資源預留需要調整

OVF檔案包含一項資源保留、旨在確保每個網格節點都有足夠的RAM和CPU、以有效運作。如果您透過在VMware 上部署這些 OVF 檔案來建立虛擬機器、且無法使用預先定義的資源數量、則虛擬機器將無法啟動。

關於這項工作

如果您確定VM主機有足夠的資源可用於每個網格節點、請手動調整每個虛擬機器的資源配置、然後嘗試啟動虛擬機器。

步驟

1. 在VMware vSphere Hypervisor用戶端樹狀結構中、選取尚未啟動的虛擬機器。
2. 以滑鼠右鍵按一下虛擬機器、然後選取*編輯設定*。
3. 從Virtual Machines Properties（虛擬機屬性）窗口中，選擇* Resources（資源）*選項卡。
4. 調整分配給虛擬機器的資源：
   a. 選取「* CPU*」、然後使用「保留」滑桿來調整保留給此虛擬機器的MHz。
   b. 選取*記憶體*、然後使用保留滑桿調整此虛擬機器保留的MB。
5. 選擇*確定*。
6. 視需要重複相同VM主機上裝載的其他虛擬機器。

臨時安裝密碼已停用

部署 VMware 節點時、您可以選擇性地指定暫時安裝密碼。您必須擁有此密碼才能存取 VM 主控台、或在新節點加入網格之前使用 SSH 。

如果您選擇停用暫存安裝密碼、則必須執行其他步驟來偵錯安裝問題。

您可以執行下列其中一項：

- 重新部署虛擬機器、但請指定暫時安裝密碼、以便您存取主控台或使用 SSH 來偵錯安裝問題。
- 使用 vCenter 設定密碼：
  a. 關閉虛擬機器電源。
  b. 移至 * VM* 、選取 * 組態 * 索引標籤、然後選取 * 應用程式選項 * 。
  c. 指定要設定的暫存安裝密碼類型：
     - 選取 * custom_entime_password* 以設定自訂的暫存密碼。
     - 選取 * 暫存密碼類型 * 以使用節點名稱做為暫存密碼。
  d. 選擇*設定值*。
  e. 設定暫時密碼：
     - 將 **custom_entime_password** 變更為自訂密碼值。
     - 使用 * 使用節點名稱 * 值更新 * 暫用密碼類型 * 。
  f. 重新啟動 VM 以套用新密碼。

相關資訊

- 若要瞭解如何存取記錄檔，請參閱"記錄檔參考"。
- "疑難排解StorageGRID 作業系統"
- 如果您需要其他協助、請聯絡 "NetApp支援"。

腳本範例

以下範例展示如何在 **RHEL** 上將 **StorageGRID** 的四個實體介面合併為一個綁定。

您可以使用範例檔案、將四個Linux實體介面集合成單一LACP連結、然後建立三個VLAN介面將連結子化、做StorageGRID 為「物件網格」、「管理」和「用戶端網路」介面。

實體介面

請注意、位於連結另一端的交換器也必須將四個連接埠視為單一LACP主幹或連接埠通道、而且必須至少通過三個帶有標籤的參考VLAN。

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Bond介面

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN 介面

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

在 **Ubuntu** 和 **Debian** 上聚合 **StorageGRID** 實體介面的範例

`/etc/network/interfaces`檔案包含三個區段、分別定義實體介面、連結介面和 VLAN 介面。您可以將這三個範例區段合併成單一檔案、將四個Linux實體介面集合成單一LACP連結、然後建立三個VLAN介面將連結子化、作為StorageGRID 「電網」、「管理」和「用戶端網路」介面使用。

實體介面

請注意、位於連結另一端的交換器也必須將四個連接埠視為單一LACP主幹或連接埠通道、而且必須至少通過三個帶有標籤的參考VLAN。

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Bond介面

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN 介面

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

配置網格並完成安裝

導航至 **StorageGRID Grid Manager**

您可以使用Grid Manager來定義設定StorageGRID 您的一套系統所需的所有資訊。

開始之前

必須部署主管理節點、並完成初始啟動順序。

步驟

1. 開啟您的網頁瀏覽器、然後瀏覽至：

   `https://primary_admin_node_ip`

   或者、您也可以從連接埠8443存取Grid Manager：

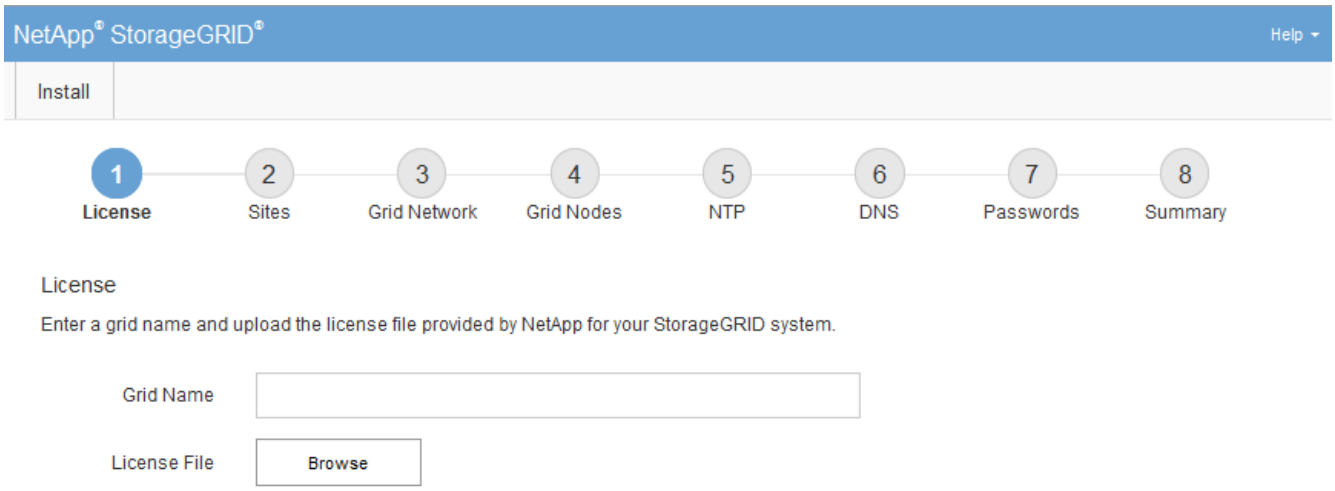
   `https://primary_admin_node_ip:8443`

   您可以根據網路組態、在Grid Network或管理網路上使用主要管理節點IP的IP位址。您可能需要使用瀏覽器中的安全性 / 進階選項來瀏覽至不受信任的憑證。

2. 視需要管理臨時安裝程式密碼：
   - 如果已使用下列其中一種方法設定密碼、請輸入密碼以繼續。
     - 使用者在先前存取安裝程式時設定密碼
     - 對於 Linux，密碼會自動從節點設定檔匯入 `/etc/storagegrid/nodes/<node_name>.conf`
     - 對於 VMware，SSH/控制台密碼已從 OVF 屬性自動匯入
   - 如果尚未設定密碼、請選擇性地設定密碼以保護 StorageGRID 安裝程式。

3. 選取 * 安裝 StorageGRID 系統 * 。

   此時會出現用來設定StorageGRID 資訊網格的頁面。



指定**StorageGRID** 不含授權的資訊

您必須指定StorageGRID 您的系統名稱、並上傳NetApp提供的授權檔案。

步驟

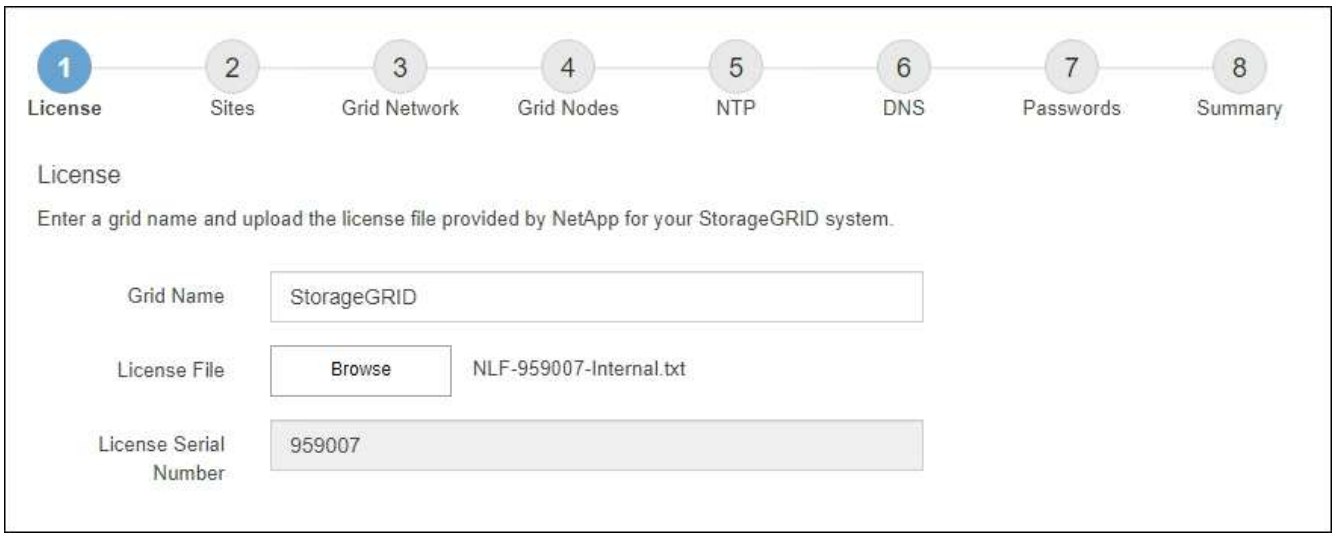
1. 在「授權」頁面上的 * 網格名稱 * 欄位中、輸入 StorageGRID 系統的有意義名稱。

   安裝後、名稱會顯示在節點功能表頂端。

2. 選取 * 瀏覽 * 、找到 NetApp 授權檔案(`NLF-unique-id.txt`) 、然後選取 * 開啟 * 。

   授權檔案已驗證、並顯示序號。

   此產品的安裝歸檔包含免費授權、不提供任何產品的支援權利。StorageGRID您可以更新至安裝後提供支援的授權。



3. 選擇*下一步*。

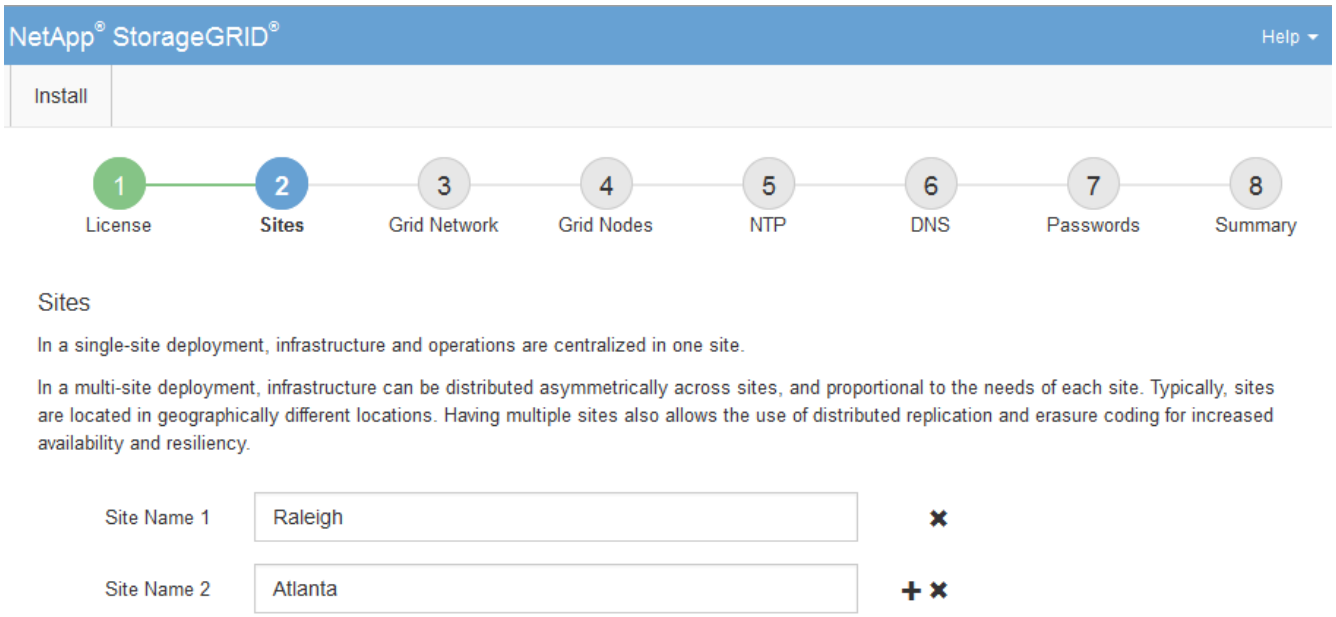
在 **StorageGRID** 中新增站台

安裝StorageGRID 時、您必須至少建立一個站台。您可以建立額外的站台、以提升StorageGRID 您的作業系統的可靠性和儲存容量。

步驟

1. 在「網站」頁面上，輸入*網站名稱*。
2. 若要新增其他站台，請選擇最後一個站台項目旁邊的加號，然後在新的 **Site name** 文字方塊中輸入名稱。

   根據網格拓撲的需求新增更多站台。您最多可以新增16個站台。



3. 選擇*下一步*。

指定 **StorageGRID** 的 **Grid Network** 子網路

您必須指定網格網路上使用的子網路。

關於這項工作

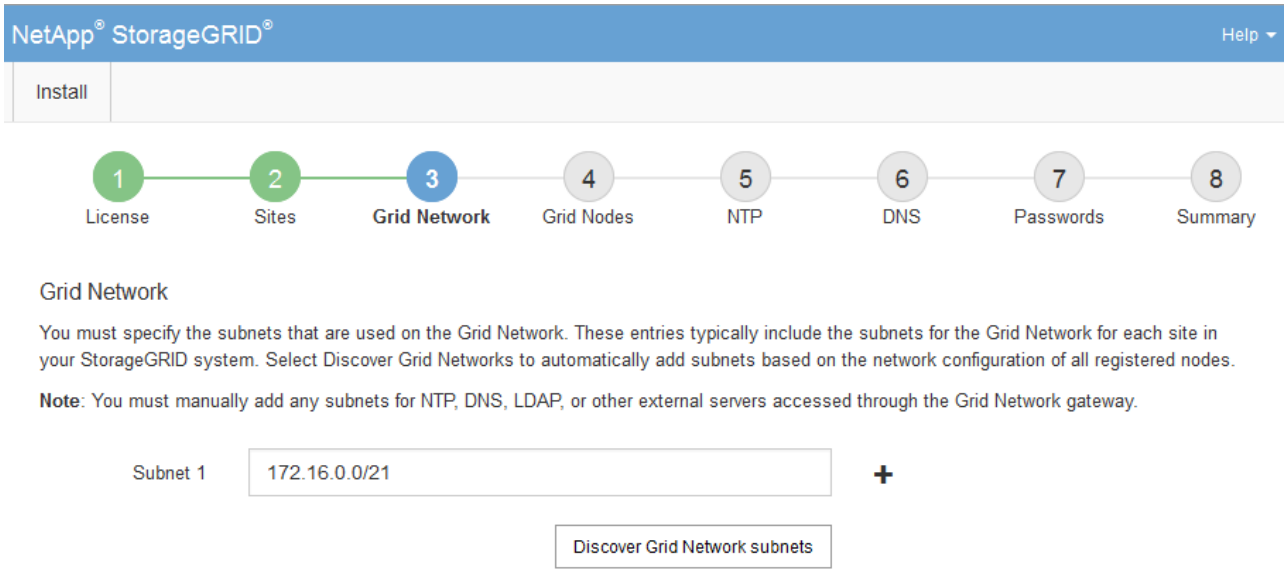
子網路項目包括 StorageGRID 系統中每個站台的網格網路子網路、以及任何需要透過網格網路存取的子網路。

如果您有多個網格子網路、則需要網格網路閘道。指定的所有網格子網路都必須透過此閘道才能連線。

步驟

1. 在*子網路1*文字方塊中、指定至少一個網格網路的CIDR網路位址。
2. 選擇最後一個條目旁的加號，即可新增其他網路條目。您必須為 Grid Network 中的所有站台指定所有子網路。
   - 如果您已部署至少一個節點，請選取 **Discover Grid Networks subnets**，以自動將已向 Grid Manager 註冊的網格節點所回報的子網路填入 Grid Network 子網路清單中。

◦ 您必須手動新增 NTP 、 DNS 、 LDAP 或其他透過網格網路閘道存取的外部伺服器的任何子網路。



3. 選擇*下一步*。

批准 **StorageGRID** 的待處理網格節點

您必須先核准每個網格節點、才能加入StorageGRID 該系統。

開始之前

您已部署所有虛擬和StorageGRID 不完整的應用裝置網格節點。

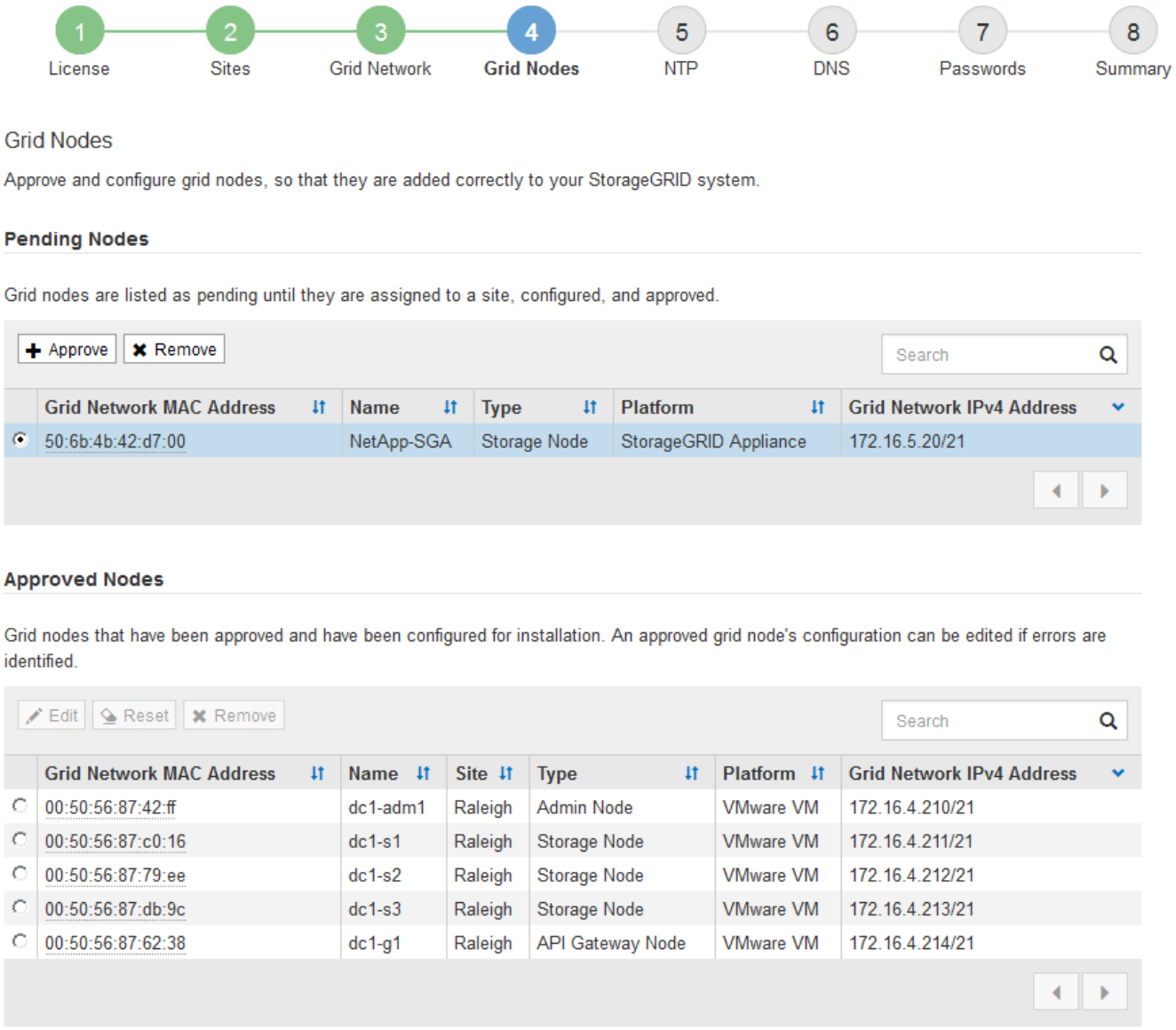
更有效率的做法是對所有節點執行單一安裝、而非現在安裝部分節點、稍後再安裝部分節點。

步驟

1. 檢閱「Pending Node」（擱置的節點）清單、並確認其顯示您部署的所有網格節點。

如果缺少網格節點、請確認已成功部署該節點、並為 Admin_IP 設定正確的主管理節點網格網路 IP 。

2. 選取您要核准之擱置節點旁的選項按鈕。



3. 選取*核准*。
4. 在「一般設定」中、視需要修改下列內容的設定：
   - * 站台 * ：此網格節點的站台系統名稱。
   - * 名稱 * ：節點的系統名稱。此名稱預設為您在設定節點時所指定的名稱。

     內部 StorageGRID 作業需要系統名稱、完成安裝後無法變更。不過、在安裝程序的這個步驟中、您可以視需要變更系統名稱。

     對於VMware節點、您可以在此變更名稱、但此動作不會變更vSphere中的虛擬機器名稱。

   - * NTP角色*：網格節點的網路時間傳輸協定（NTP）角色。選項包括*自動*、主要*和*用戶端。選取*自動*會將主要角色指派給管理節點、具有ADC服務的儲存節點、閘道節點、以及任何具有非靜態IP位址的網格節點。所有其他網格節點都會被指派「用戶端」角色。

請確定每個站台至少有兩個節點可以存取至少四個外部NTP來源。如果站台只有一個節點可以連線至NTP來源、則當該節點當機時、就會發生計時問題。此外、將每個站台的兩個節點指定為主要NTP來源、可確保站台與網格的其他部分隔離時、能確保準確的時間安排。

- * 儲存類型 * （僅限儲存節點）：指定新的儲存節點僅用於資料、僅用於中繼資料或兩者。選項包括 * 資料和中繼資料 * （「組合」）、 * 僅資料 * 和 * 僅中繼資料 * 。

  如需這些節點類型需求的相關資訊、請參閱"儲存節點類型"。

- * ADC服務*（僅限儲存節點）：選取*自動*、讓系統判斷節點是否需要管理網域控制器（ADC）服務。ADC服務會追蹤網格服務的位置和可用度。每個站台至少必須有三個儲存節點包含ADC服務。您無法在部署 ADC 服務之後、將其新增至節點。

5. 在Grid Network中、視需要修改下列內容的設定：

   - * IPV4位址（CIDR）*：Grid Network介面的CIDR網路位址（容器內的eth0）。例如：192.168.1.234/21
   - 閘道：網格網路閘道。例如：192・168・0・1

     如果有多個網格子網路、則需要閘道。

     如果您在Grid Network組態中選取DHCP、並在此變更值、則新值會在節點上設定為靜態位址。您必須確定設定的 IP 位址不在 DHCP 位址集區內。

6. 如果您要設定網格節點的管理網路、請視需要新增或更新「管理網路」區段中的設定。

   在「子網路（**CIDR**）」文字方塊中、輸入此介面的路由目的地子網路。如果有多個子網路、則需要管理閘道。

   如果您在管理網路組態中選取DHCP、並在此變更值、新值將會設定為節點上的靜態位址。您必須確定設定的 IP 位址不在 DHCP 位址集區內。

   - 應用裝置： * 對於 StorageGRID 應用裝置、如果在初次安裝時未使用 StorageGRID 應用裝置安裝程式設定管理網路、則無法在此 Grid Manager 對話方塊中設定。您必須改為執行下列步驟：

     a. 重新啟動應用裝置：在應用裝置安裝程式中、選取*進階*>*重新開機*。

        重新開機可能需要數分鐘的時間。

     b. 選擇*設定網路*>*連結組態*、然後啟用適當的網路。
     c. 選擇*設定網路*>* IP組態*、然後設定啟用的網路。
     d. 返回首頁並選擇 **Start installation**。
     e. 在 Grid Manager 中：如果節點列在 Approved Nodes 表中、請移除該節點。
     f. 從「Pending Node」（擱置的節點）表格中移除節點。
     g. 等待節點重新出現在「Pending Node」（擱置的節點）清單中。
     h. 確認您可以設定適當的網路。您應已在應用裝置安裝程式的 IP 組態頁面上填入您所提供的資訊。

如需更多資訊、請參閱 "硬體安裝快速入門"以找出產品的相關指示。

7. 如果您要設定網格節點的用戶端網路、請視需要新增或更新「用戶端網路」區段中的設定。如果已設定用戶端網路、則需要閘道、而且在安裝之後、閘道會成為節點的預設閘道。

   如果您選取DHCP作為用戶端網路組態、並在此變更值、新值將會設定為節點上的靜態位址。您必須確定設定的 IP 位址不在 DHCP 位址集區內。

   - 應用裝置： * 對於 StorageGRID 應用裝置、如果在初次安裝期間未使用 StorageGRID 應用裝置安裝程式設定用戶端網路、則無法在此 Grid Manager 對話方塊中設定。您必須改為執行下列步驟：

     a. 重新啟動應用裝置：在應用裝置安裝程式中、選取*進階*>*重新開機*。

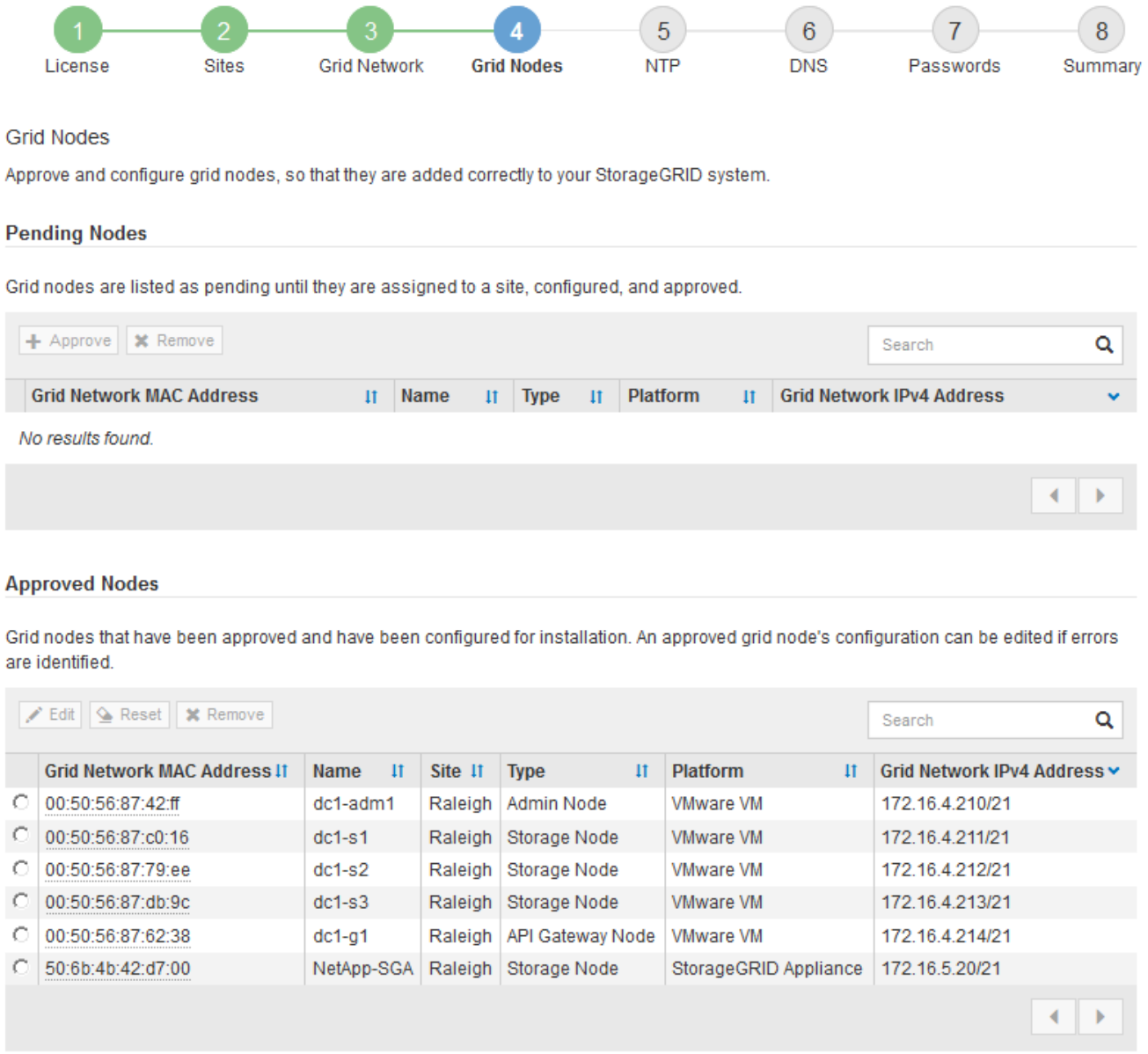
        重新開機可能需要數分鐘的時間。

     b. 選擇*設定網路*>*連結組態*、然後啟用適當的網路。
     c. 選擇*設定網路*>* IP組態*、然後設定啟用的網路。
     d. 返回首頁並選擇 **Start installation**。
     e. 在 Grid Manager 中：如果節點列在 Approved Nodes 表中、請移除該節點。
     f. 從「Pending Node」（擱置的節點）表格中移除節點。
     g. 等待節點重新出現在「Pending Node」（擱置的節點）清單中。
     h. 確認您可以設定適當的網路。您應已在應用裝置安裝程式的 IP 組態頁面上填入您所提供的資訊。

        如需更多資訊、請參閱 "硬體安裝快速入門"以找出產品的相關指示。

8. 選擇*保存*。

   網格節點項目會移至「核准的節點」清單。



9. 針對您要核准的每個擱置的網格節點、重複這些步驟。

   您必須批准網格中所有要新增的節點。不過，在「摘要」頁面上選擇 **Install** 之前，您可以隨時返回此頁面。您可以透過選擇單選按鈕並選擇 **Edit** 來修改已核准網格節點的屬性。

10. 批准網格節點完成後，選擇 **Next**。

指定 StorageGRID 的網路時間協定伺服器資訊

您必須為StorageGRID 該系統指定網路時間傳輸協定（NTP）組態資訊、以便在不同的伺服器上執行的作業能夠保持同步。

關於這項工作

您必須為NTP伺服器指定IPV4位址。

您必須指定外部NTP伺服器。指定的NTP伺服器必須使用NTP傳輸協定。

您必須指定階層3或更高層級的四個NTP伺服器參考資料、以避免時間浪費問題。

> 指定正式作業層級 StorageGRID 安裝的外部 NTP 來源時、請勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 時間（ W32Time ）服務。舊版Windows上的時間服務不夠準確、Microsoft不支援在StorageGRID 高準確度環境中使用、例如：
>
> "高精度時間的支援邊界"

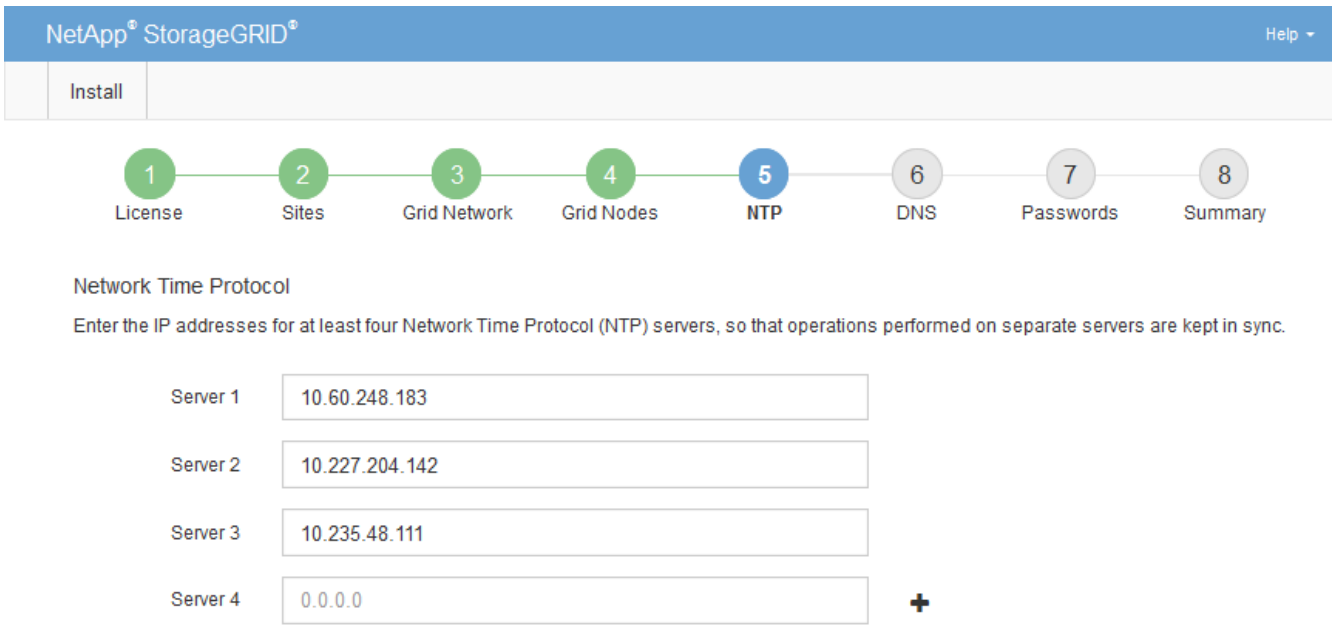
外部NTP伺服器是由您先前指派主要NTP角色的節點所使用。

> 請確定每個站台至少有兩個節點可以存取至少四個外部NTP來源。如果站台只有一個節點可以連線至NTP來源、則當該節點當機時、就會發生計時問題。此外、將每個站台的兩個節點指定為主要NTP來源、可確保站台與網格的其他部分隔離時、能確保準確的時間安排。

（僅限 VMware）對 VMware 執行額外檢查，例如確保虛擬機器管理程式使用與虛擬機器相同的 NTP 來源，並使用 VMTools 停用虛擬機器管理程式和StorageGRID虛擬機器之間的時間同步。

步驟

1. 在「伺服器**1***到*伺服器**4**」文字方塊中、指定至少四部NTP伺服器的IPV4位址。
2. 如有必要、請選取最後一個項目旁的加號、以新增其他伺服器項目。



3. 選擇*下一步*。

相關資訊

"網路準則"

指定 **StorageGRID** 的 **DNS** 伺服器資訊

您必須指定 StorageGRID 系統的 DNS 資訊、才能使用主機名稱而非 IP 位址來存取外部伺服器。

關於這項工作

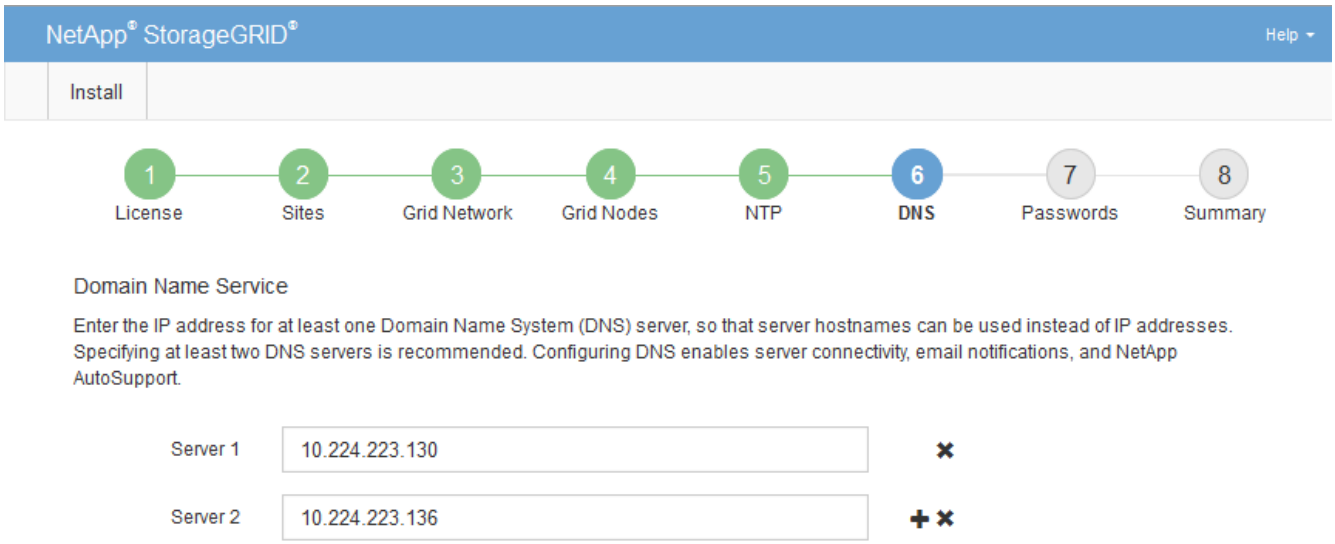
指定 "DNS伺服器資訊"可讓您使用完整網域名稱（ FQDN ）主機名稱、而非電子郵件通知和 AutoSupport 的 IP 位址。

若要確保正常運作、請指定兩或三個 DNS 伺服器。如果您指定超過三個、可能只會使用三個、因為某些平台的已知作業系統限制。如果您在環境中有路由限制、則可"自訂 DNS 伺服器清單"讓個別節點（通常是站台上的所有節點）使用最多三個 DNS 伺服器的不同組別。

如有可能、請使用每個站台都能在本機存取的 DNS 伺服器、以確保某個著陸站台可以解析外部目的地的 FQDN 。

步驟

1. 在「伺服器**1**」文字方塊中、指定至少一個DNS伺服器的IPV4位址。
2. 如有必要、請選取最後一個項目旁的加號、以新增其他伺服器項目。



最佳實務做法是指定至少兩部DNS伺服器。您最多可以指定六個DNS伺服器。

3. 選擇*下一步*。

指定**StorageGRID** 「系統密碼」

在安裝StorageGRID 您的支援資料系統時、您必須輸入密碼、才能確保系統安全並執行維護工作。

關於這項工作

使用「安裝密碼」頁面來指定資源配置通關密碼和網格管理root使用者密碼。

- 資源配置通關密碼是作為加密金鑰使用、StorageGRID 並非由作業系統儲存。
- 您必須擁有配置通關密碼、才能執行安裝、擴充及維護程序、包括下載恢復套件。因此、請務必將資源配置通關密碼儲存在安全的位置。
- 如果您有目前的網格管理程式、可以從網格管理程式變更資源配置通關密碼。
- 可使用 Grid Manager 變更網格管理根使用者密碼。

- 隨機產生的命令列主控台和 SSH 密碼會儲存在 `Passwords.txt` Recovery Package 的檔案中。

步驟

1. 在 **Provisioning passphrase** 中，輸入對 StorageGRID 系統的網格拓撲進行變更所需的 Provisioning passphrase。

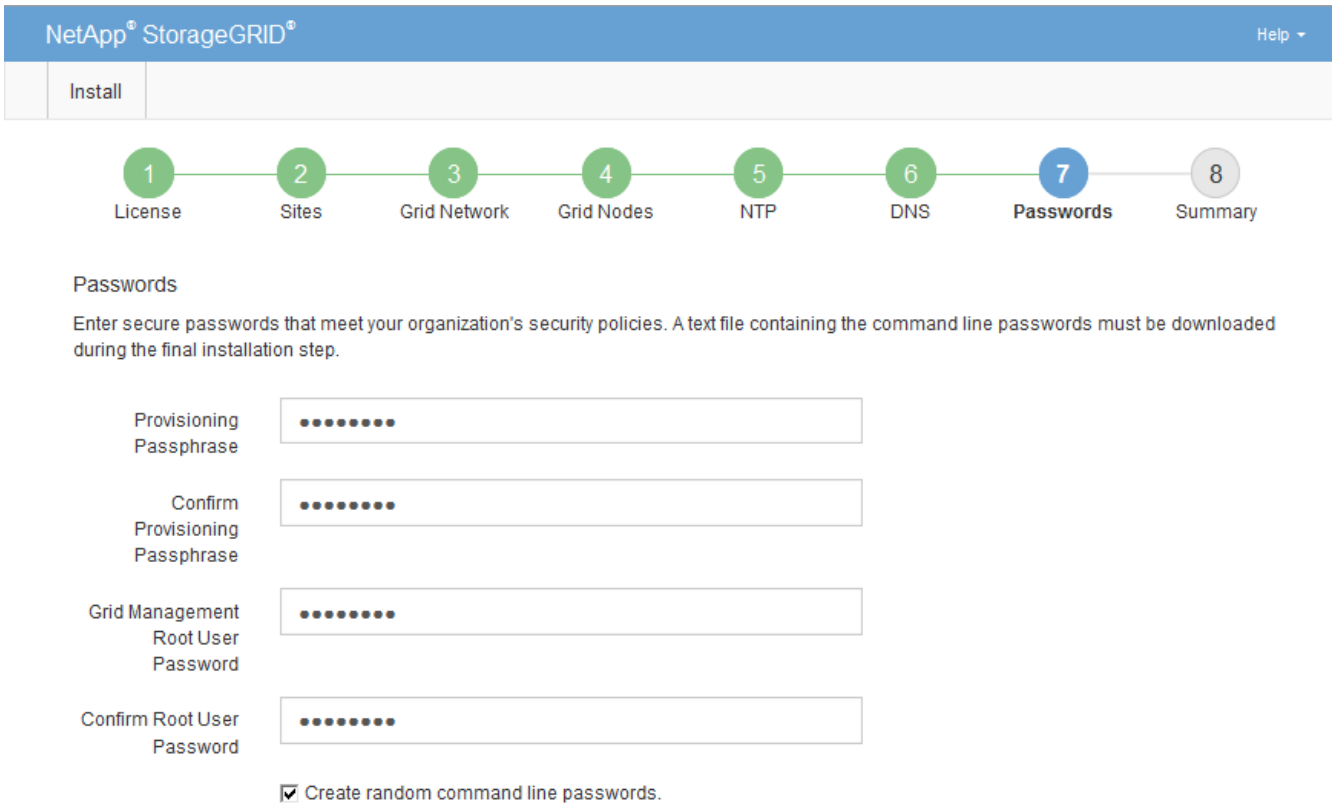
   將資源配置通關密碼儲存在安全的地方。

   > 如果安裝完成後您想稍後變更設定密碼，則可以使用網格管理員。選擇*設定* > 存取控制 > 電網密碼。

2. 在「確認資源配置密碼」中，重新輸入資源配置密碼以進行確認。
3. 在 * 網格管理根使用者密碼 * 中、輸入密碼以「根」使用者身分存取 Grid Manager 。

   > 將配置密碼儲存在安全的位置。它是安裝、擴充和維護過程所必需的。

4. 在*確認root使用者密碼*中、重新輸入Grid Manager密碼以進行確認。



5. 如果您要安裝網格以進行概念驗證或示範、請選擇性清除 * 建立隨機命令列密碼 * 核取方塊。

   在正式作業部署中、基於安全考量、應一律使用隨機密碼。如果您想使用預設密碼從命令列使用「 root 」或「 admin 」帳戶存取網格節點、請清除 * 僅為示範網格建立隨機命令列密碼 * 。

   > 在「摘要」頁面選擇 **Install** 後，系統會提示您下載復原套件檔案(`sgws-recovery-package-id-revision.zip`。您必須"下載此檔案"完成安裝。存取系統所需的密碼儲存在 `Passwords.txt`檔案中，該檔案包含於復原套件檔案內。

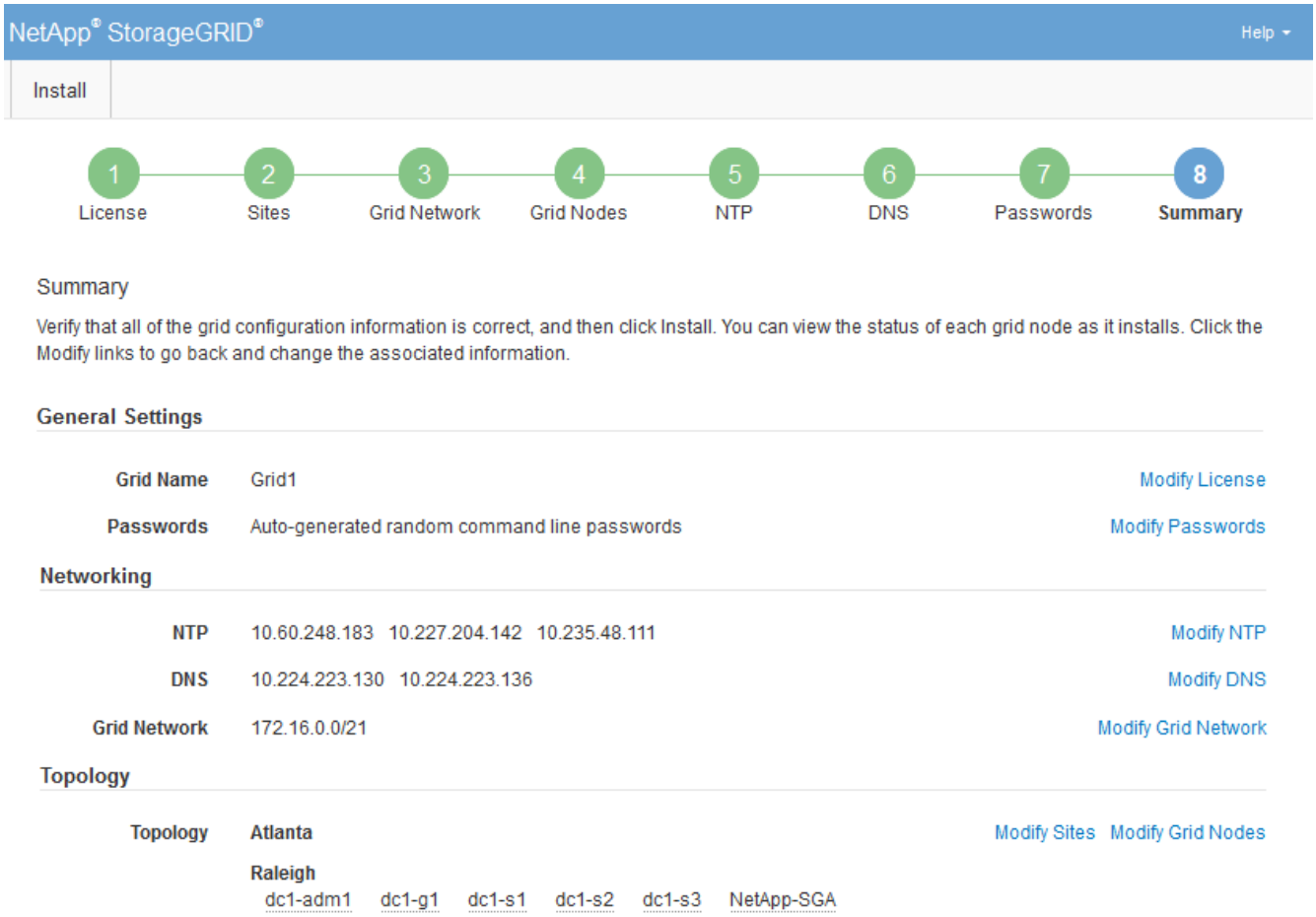
6. 選擇*下一步*。

檢查您的 **StorageGRID** 組態

您必須仔細檢閱輸入的組態資訊、以確保安裝順利完成。

步驟

1. 查看* Summary（摘要）*頁面。



2. 確認所有網格組態資訊均正確無誤。使用「摘要」頁面上的「修改」連結、即可返回並修正任何錯誤。
3. 選擇 **Install**。

> 如果某個節點設定為使用用戶端網路，則當您選擇 **Install** 時，該節點的預設閘道將從 Grid Network 切換到 Client Network。如果連線中斷，您必須確保透過可存取的子網路存取主要管理節點。如需詳細資訊、請參閱 "網路準則"。

4. 選擇*下載恢復套件*。

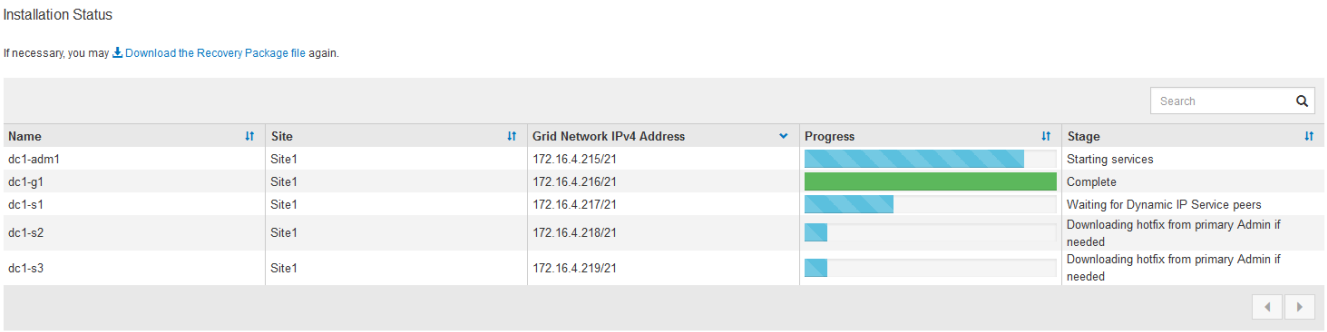
當安裝過程進入網格拓撲定義點時，系統會提示您下載恢復軟件包文件(`.zip`），並確認您可以成功訪問此文件的內容。您必須下載「恢復套件」檔案、以便StorageGRID 在一個或多個網格節點發生故障時、恢復該系統。安裝會在背景繼續進行、但在您下載並驗證此檔案之前、您無法完成安裝並存取 StorageGRID 系統。

5. 確認您可以擷取檔案內容 `.zip`、然後將其儲存在兩個安全且獨立的位置。

   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。

6. 選取「我已成功下載並驗證 **Recovery Package** 檔案」核取方塊，然後選取「下一步」。

   如果安裝仍在進行中、則會顯示狀態頁面。此頁面會指出每個網格節點的安裝進度。



   當到達所有網格節點的完整階段時、會出現Grid Manager的登入頁面。

7. 使用「root」使用者和您在安裝期間指定的密碼登入Grid Manager。

安裝 **StorageGRID** 後的網路和 **DHCP** 需求

完成網格節點部署與組態之後、請遵循下列原則進行DHCP定址和網路組態變更。

- 如果使用DHCP來指派IP位址、請為使用中網路上的每個IP位址設定DHCP保留。

  您只能在部署階段設定DHCP。您無法在組態期間設定 DHCP 。

  當網格網路組態由 DHCP 變更時、節點會重新開機、如果 DHCP 變更同時影響多個節點、這可能會導致中斷運作。

- 如果您想要變更網格節點的IP位址、子網路遮罩和預設閘道、則必須使用變更IP程序。請參閱。 "設定IP位址"
- 如果您進行網路組態變更（包括路由和閘道變更）、則可能會失去與主要管理節點和其他網格節點的用戶端連線。視所套用的網路變更而定、您可能需要重新建立這些連線。

了解安裝 **StorageGRID** 後所需和選用的步驟

完成安裝後、請執行必要的整合與組態工作。您可以視需要執行選用工作。

必要的工作

- （僅限 VMware）配置 VMware vSphere Hypervisor 以實現自動重新啟動。

  您必須設定Hypervisor、以便在伺服器重新啟動時重新啟動虛擬機器。如果不自動重新啟動、虛擬機器和網格節點會在伺服器重新啟動後持續關機。如需詳細資料、請參閱VMware vSphere Hypervisor文件。

- "建立租戶帳戶"適用於將用於儲存 StorageGRID 系統物件的 S3 用戶端傳輸協定。
- "控制系統存取"設定群組和使用者帳戶。您也可以"設定同盟身分識別來源"（例如 Active Directory 或 OpenLDAP ）匯入管理群組和使用者。或者，您可以"建立本機群組和使用者"。
- 整合並測試"S3 API"您將用來將物件上傳至 StorageGRID 系統的用戶端應用程式。
- "設定資訊生命週期管理（ ILM ）規則和 ILM 原則"您想要用來保護物件資料。
- 如果您的安裝包含應用裝置儲存節點、請使用 SANtricity OS 來完成下列工作：
  - 連接每StorageGRID 個產品。
  - 驗證AutoSupport 是否收到不實資料。

    請參閱。 "設定硬體"
- 檢閱並遵循"StorageGRID 系統強化準則"以消除安全風險。
- "設定系統警示的電子郵件通知"。

選用工作

- "更新網格節點 IP 位址"如果自您計劃部署並產生復原套件以來它們已經發生了變化。
- "設定儲存加密"（如果需要）。
- "設定儲存壓縮"以減少儲存物件的大小（如有需要）。
- "設定VLAN介面"如有需要、可隔離及分割網路流量。
- "設定高可用度群組"如有需要、可改善 Grid Manager 、 Tenant Manager 和 S3 用戶端的連線可用度。
- "設定負載平衡器端點"如有需要、適用於 S3 用戶端連線。

升級StorageGRID 版軟體

升級StorageGRID 版軟體

請依照下列指示將StorageGRID 更新版的更新版更新至更新版本。

執行升級時、 StorageGRID 系統中的所有節點都會升級。

> 如果您急需擴展儲存以增加容量（如果您的儲存幾乎已滿），請不要開始升級。及時完成升級程序。如果需要恢復，請聯絡技術支援。

升級之前

請查看這些主題，了解 StorageGRID 12.1 中的新功能和增強功能、確認是否有任何功能已過時或移除，以及了解 StorageGRID API 的變更。

- "系統在升級期間的影響"
- "StorageGRID 12.1 的新功能"
- "已移除或已過時的功能"

- "網格管理API的變更"
- "租戶管理API變更"

規劃及準備升級

估算完成 StorageGRID 升級所需的時間

請根據升級所需的時間考慮何時升級。請注意在升級的每個階段中、您可以執行哪些作業、哪些作業無法執行。

關於這項工作

完成升級所需的時間StorageGRID 取決於多種因素、例如用戶端負載和硬體效能。

下表摘要說明主要的升級工作、並列出每項工作所需的大約時間。表格後的步驟提供您可用來預估系統升級時間的指示。

升級工作	說明	大約所需時間	在此工作期間
執行預先檢查並升級主要管理節點	系統會執行升級預先檢查、並停止、升級及重新啟動主要管理節點。	30 分鐘到 1 小時、服務應用裝置節點需要最多時間。 未解決的預先檢查錯誤將會增加這次時間。	您無法存取主要管理節點。可能會回報連線錯誤、您可以忽略這些錯誤。 在開始升級之前執行升級預先檢查、可讓您在排定的升級維護時間之前解決任何錯誤。
開始升級服務	軟體檔案隨即散佈、並啟動升級服務。	每個網格節點 3 分鐘	
升級其他網格節點	所有其他網格節點上的軟體均按照您批准節點的順序進行升級。一個管理節點或網關節點與一個儲存節點同時升級。	每個節點15分鐘到1小時、應用裝置節點最需要時間 • 注意 * ：對於應用裝置節點、StorageGRID 應用裝置安裝程式會自動更新至最新版本。	• 請勿變更網格組態。 • 請勿變更稽核層級組態。 • 請勿更新 ILM 組態。 • 您無法執行其他維護程序、例如修復程式、取消委任或擴充。 • 注意 * ：如果您需要執行恢復、請聯絡技術支援部門。
啟用功能	新版本的新功能已啟用。	最多 1 小時	• 請勿變更網格組態。 • 請勿變更稽核層級組態。 • 請勿更新 ILM 組態。 • 您無法執行其他維護程序。
最終升級步驟	移除暫用檔案、並完成新版本的升級。	5 分鐘	當 * 最終升級步驟 * 工作完成時、您可以執行所有維護程序。

估計升級時間

步驟

1. 預估升級所有網格節點所需的時間。
   a. 將您的支援系統中的節點數乘StorageGRID 以1小時/節點。

      一般而言、應用裝置節點的升級時間比軟體型節點長。

   b. 在此時間加上 1 小時、以說明下載檔案、執行預先檢查驗證、以及完成最終升級步驟所需的時間 `.upgrade`。
2. 如果您有Linux節點、請為每個節點新增15分鐘、以說明下載及安裝RPM或Deb套件所需的時間。
3. 新增步驟1和步驟2的結果、計算升級的預估總時間。

範例：升級至 **StorageGRID 12.1** 的預計時間

假設您的系統有14個網格節點、其中8個是Linux節點。

1. 將14乘以1小時/節點。
2. 加1小時以說明下載、預先檢查及最終步驟。

   升級所有節點的預估時間為15小時。

3. 將8乘以15分鐘/節點、以計算在Linux節點上安裝RPM或Deb套件的時間。

   此步驟的預估時間為2小時。

4. 將這些值加在一起。

   您應該預留最多 18 小時來完成系統升級至 StorageGRID 12.1.0。

> 視需要、您可以核准網格節點的子集以在多個工作階段中升級、將維護時段分割成較小的視窗。例如、您可能偏好在一個工作階段中升級站台 A 的節點、然後在稍後的工作階段中升級站台 B 的節點。如果您選擇在多個工作階段中執行升級、請注意、在所有節點都升級之前、您無法開始使用新功能。

StorageGRID 升級如何影響您的系統

瞭解 StorageGRID 系統在升級期間會受到哪些影響。

升級完成前允許外部 **SSH** 訪問

升級期間允許外部 SSH 存取。升級完成後，外部 SSH 存取預設會被阻止。升級後，您可以使用“網格管理器”>“安全性設定”頁面上的“阻止 SSH”選項卡來"管理外部 SSH 訪問"。網格節點之間的 SSH 存取不受影響。

不中斷升級**StorageGRID**

整個升級過程中、這個系統可以從用戶端應用程式擷取及擷取資料。StorageGRID如果您核准所有類型相同的節點進行升級（例如儲存節點）、則節點會一次關閉一個節點、因此當某種類型的所有網格節點或所有網格節點都無法使用時、就不會有任何時間。

為了確保持續可用、請確保 ILM 原則包含指定儲存每個物件多個複本的規則。您也必須確定所有外部 S3 用戶端都已設定為傳送要求至下列其中一項：

- 高可用度（ HA ）群組虛擬 IP 位址
- 高可用度協力廠商負載平衡器
- 每個用戶端有多個閘道節點
- 每個用戶端有多個儲存節點

用戶端應用程式可能會遭遇短期中斷

StorageGRID 系統可在整個升級程序中從用戶端應用程式擷取和擷取資料、但是、如果升級需要在這些節點上重新啟動服務、用戶端與個別閘道節點或儲存節點的連線可能會暫時中斷。升級程序完成後、連線能力將會恢復、而服務會在個別節點上恢復。

如果連線中斷一段短時間是不可接受的、您可能需要排程停機時間來套用升級。您可以使用選擇性核准來排程特定節點的更新時間。

> 您可以使用多個閘道和高可用度（ HA ）群組、在升級過程中提供自動容錯移轉。請參閱的說明"設定高可用度群組"。

後台修復無法在具有混合版本節點的網格上運行

當網格包含混合版本節點時，升級期間不會執行背景修復。在網站中斷期間出現的任何不一致問題在升級完成之前都不會修復。

應用裝置韌體已升級

StorageGRID 12.1 升級期間：

- 所有 StorageGRID 應用裝置節點會自動升級至 StorageGRID Appliance Installer 韌體版本 12.1。
- SG6060 和 SGF6024 設備自動升級到 BIOS 韌體版本 3B08.EX 和BMC韌體版本 4.01.07。
- SG100 和 SG1000 裝置自動升級至 BIOS 韌體版本 3B13.EC 和BMC韌體版本 4.75.07。
- SGF6112、SG6160、SG110 和 SG1100 應用裝置將自動升級至 BIOS 韌體版本 3A14.QD 和 BMC 韌體版本 3.21.07。

ILM 原則的處理方式會因其狀態而異

- 升級後、作用中原則將維持不變。
- 升級時只會保留最新的 10 項歷史原則。
- 如果有建議的原則、則會在升級期間刪除。

可能會觸發警示

當服務啟動和停止時、StorageGRID 以及當作業系統以混合版本環境運作時、可能會觸發警示（部分網格節點執行較早版本、而其他節點則已升級至較新版本）。升級完成後、可能會觸發其他警示。

例如，當服務停止時，您可能會看到 **Unable to communicate with node** 警示；或者，當某些節點已升級至 StorageGRID 12.0 或更高版本，而其他節點仍在執行舊版 StorageGRID 時，您可能會看到 **Cassandra**

communication error 警示。通常、這些警示會在升級完成後消失。

在升級至 StorageGRID 12.0 或更新版本期間，若儲存節點停止運作，可能會觸發 **ILM placement unachievable** 警示。此警示可能在升級完成後持續 1 天。

升級完成後、您可以從 Grid Manager 儀表板選取 * 最近解決的警示 * 或 * 目前警示 * 、來檢閱任何與升級相關的警示。

組態變更受到限制

組態變更限制因版本而異。如果您要升級至其他 StorageGRID 版本，請參閱該版本升級說明中的受限變更清單。

在*啟用新功能*工作完成之前：

- 請勿變更任何網格組態。
- 請勿啟用或停用任何新功能。
- 請勿更新 ILM 組態。否則、您可能會遇到不一致且非預期的ILM行為。
- 請勿套用 Hotfix 或恢復網格節點。

  如果您需要在升級期間恢復節點、請聯絡技術支援部門。

- 升級期間，請勿管理 HA 群組、VLAN 介面或負載平衡器端點。
- 升級完成前請勿刪除任何高可用性 (HA) 組。否則，其他 HA 群組中的虛擬 IP 位址可能無法存取。

直到*最終升級步驟*工作完成為止：

- 請勿執行擴充程序。
- 請勿執行取消委任程序。

在升級前驗證已安裝的 **StorageGRID** 版本

在開始升級之前、請確認先前版本的 StorageGRID 目前已安裝、並套用最新的可用 Hotfix。

關於這項工作

在升級至 StorageGRID 12.1 之前，您的網格必須安裝 StorageGRID 12.0 或更新版本。如果您目前使用的是舊版 StorageGRID，則必須安裝所有先前的升級檔案及其最新的 Hotfix（強烈建議），直到您的網格目前版本至少達到 StorageGRID 12.0.0。

中顯示了一個可能的升級途徑範例。

NetApp強烈建議您在升級到下一個版本之前為每個StorageGRID版本應用最新的修補程序，並且還為您安裝的每個新版本應用最新的修補程序。在某些情況下，您必須套用修補程式以避免資料遺失的風險。參考 "NetApp下載StorageGRID"以及每個修補程式的發行說明以了解更多資訊。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 從網格管理器的頂端、選取*說明*>*關於*。
3. 驗證*版本*是否為 11.9.0.8 或更高版本。
4. 如果*版本*不是 11.9.0.8 或更高版本，請前往 "NetApp下載StorageGRID"下載您需要的升級和修補程式檔案。
5. "請按照升級說明進行操作"對於您下載的每個版本。"應用最新的修補程序"對於每個版本（強烈建議）。

參考以下升級範例。

範例：從版本 **11.8** 升級到**StorageGRID 12.0**

以下範例說明從 StorageGRID 版本 11.9 升級至版本 12.0 的步驟，以準備進行 StorageGRID 12.1 升級。

請依下列順序下載並安裝軟體、以準備系統進行升級：

1. 升級至 StorageGRID 11.8.0 主要版本。
2. 套用最新的 StorageGRID 11.8.0.*y* Hotfix 。
3. 升級到StorageGRID 11.9.0 主要版本。
4. 應用StorageGRID 11.9.0.8 或更高版本的修補程式。

取得 **StorageGRID** 軟體升級所需的材料

開始軟體升級之前、請先取得所有必要資料。

項目	附註
服務筆記型電腦	服務型筆記型電腦必須具備： • 網路連接埠 • SSH用戶端（例如Putty）
"支援的網頁瀏覽器"	瀏覽器支援通常會針對每StorageGRID 個版本進行變更。請確定您的瀏覽器與新StorageGRID 版的更新版本相容。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼未列在 `Passwords.txt`檔案中。
Linux RPM 或 Deb 歸檔	如果在 Linux 主機上部署了任何節點、則必須"在所有主機上下載並安裝 RPM 或 Deb 套件"在開始升級之前進行。 確保您的 Linux 作業系統符合 StorageGRID 的最低核心版本要求。看"在 Linux 主機上安裝StorageGRID" 。

項目	附註
本文檔StorageGRID	• "版本資訊"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。請務必在開始升級前仔細閱讀這些說明。 • "StorageGRID 軟體升級解決方案指南"您要升級至的主要版本（需要登入） • 其他 "本文檔StorageGRID"、視需要。

在升級之前、請檢查 **StorageGRID** 系統的狀況

在升級 StorageGRID 系統之前、請確認系統已準備好接受升級。確保系統正常執行、且所有網格節點均可運作。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 檢查並解決任何作用中警示。
3. 請參閱 "內部網格節點通訊" 和 "外部通訊"，以確保在升級之前已開啟 StorageGRID 12.1 所需的所有連接埠。

> ⓘ 升級至 StorageGRID 12.1 時，不需要額外的連接埠。

升級軟體

StorageGRID 升級快速入門

開始升級之前、請先檢閱一般工作流程。「升級版」頁面會引導您完成每個升級步驟。StorageGRID

準備 **Linux** 主機

如果在 Linux 主機上部署了任何 StorageGRID 節點、則"在每個主機上安裝RPM或Deb套件"在開始升級之前。

上傳升級和 **Hotfix** 檔案

如果需要、請從主要管理節點存取 StorageGRID 升級頁面、並上傳升級檔案和 Hotfix 檔案。

下載恢復包

在開始升級之前下載目前的復原包。

執行升級預先檢查

升級預先檢查可協助您偵測問題、以便您在開始實際升級之前先解決這些問題。

5 開始升級

當您開始升級時、會再次執行預先檢查、並自動升級主要管理節點。當主要管理節點正在升級時、您無法存取 Grid Manager 。稽核記錄也無法使用。此升級可能需要30分鐘。

6 下載恢復包

主管理節點升級後，下載新的復原包。

7 核准節點

您可以核准個別的網格節點、網格節點群組或所有網格節點。

除非您確定節點已準備好停止並重新開機、否則請勿核准網格節點的升級。

8 恢復作業

當所有網格節點都已升級時、系統會啟用新功能、您可以繼續作業。您必須等到背景 * 升級資料庫 * 工作和 * 最終升級步驟 * 工作完成後、才能執行取消委任或擴充程序。

相關資訊

"預估完成升級所需的時間"

在所有 **Linux** 主機上下載並安裝 **RPM** 或 **DEB** 套件以供 **StorageGRID** 使用

如果在 Linux 主機上部署了任何 StorageGRID 節點、請在開始升級之前、先在這些主機上下載並安裝額外的 RPM 或 Deb 套件。

下載升級、 **Linux** 和 **Hotfix** 檔案

當您從 Grid Manager 執行 StorageGRID 升級時、系統會提示您下載升級歸檔和任何必要的 Hotfix 作為第一步。不過、如果您需要下載檔案來升級 Linux 主機、您可以事先下載所有必要的檔案、以節省時間。

步驟

1. 前往 "NetApp下載StorageGRID"。
2. 選取下載最新版本的按鈕、或從下拉式功能表中選取其他版本、然後選取*執行*。

   下列格式的軟件版本：11.*x.y*。StorageGRID下列格式的更新程式為：11.*x.y.z*。StorageGRID
3. 以您NetApp帳戶的使用者名稱和密碼登入。
4. 如果出現「注意」 / 「 MustRead 」通知、請記下 Hotfix 編號、然後選取核取方塊。
5. 閱讀終端使用者授權合約（ EULA ）、選取核取方塊、然後選取 * 接受並繼續 * 。

   此時將顯示所選版本的下載頁面。頁面包含三欄。
6. 從第二欄（ * 升級 StorageGRID * ）下載兩個檔案：

- 最新版本的升級歸檔文件（這是標有 * VMware 、 SG1000 或 SG100 主要管理節點 * 的部分中的檔案）。雖然在您執行升級之前不需要此檔案、但現在下載將可節省時間。
- RPM 或 Deb 歸檔 `.tgz` `.zip`格式。如果您在服務筆記型電腦上執行 Windows 、請選取 `.zip`檔案。
  - RHEL
    `StorageGRID-Webscale-version-RPM-uniqueID.zip`
    `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
  - Ubuntu 或 Debian
    `StorageGRID-Webscale-version-DEB-uniqueID.zip`
    `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

7. 如果您因為需要 Hotfix 而需要同意「注意」 / 「 MustRead 」通知、請下載 Hotfix ：
   a. 返回 "NetApp下載StorageGRID"。
   b. 從下拉式清單中選取 Hotfix 編號。
   c. 再次同意「注意」通知和 EULA 。
   d. 下載並儲存 Hotfix 及其 README 。

      當您開始升級時、系統會提示您上傳 StorageGRID 升級頁面上的 Hotfix 檔案。

8. 程式碼簽章驗證在 Linux 節點上是手動的。或者，驗證安裝檔案：
   a. 下載 StorageGRID 程式碼簽章驗證套件。此套件的檔案名稱使用格式 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`、其中 `<version-number>`是 StorageGRID 軟體版本。
   b. 依照步驟"手動驗證安裝檔案"。

在所有 **Linux** 主機上安裝歸檔

在升級 StorageGRID 軟體之前、請先執行這些步驟。

步驟

1. 從安裝檔案擷取RPM或Dub套件。
2. 在所有Linux主機上安裝RPM或Deb套件。

   請參閱安裝 Linux StorageGRID主機服務的步驟"安裝StorageGRID 支援主機服務"。

   新的套件會以其他套件的形式安裝。

移除舊版的安裝封存

若要釋放 Linux 主機上的空間、您可以移除不再需要的舊版 StorageGRID 安裝歸檔。

步驟

1. 移除舊的 StorageGRID 安裝封存。

紅帽企業版

1. 擷取安裝的 StorageGRID 套件清單 `dnf list | grep -i storagegrid`：。

   範例：

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. 移除先前的 StorageGRID 套件：`dnf remove images-package service-package`

   > 請勿移除您目前執行的 StorageGRID 版本或您打算升級至的 StorageGRID 版本的安裝封存。

   您可以安全地忽略出現的警告。它們是指您安裝較新的 StorageGRID 套件時所取代的檔案。

   範例：

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
================================================================================
========
```

```
Package            Architecture      Version           Repository
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
```

```
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  2/2
Installed products updated.
```

```
Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu與DEBIAN

1. 擷取已安裝的 StorageGRID 套件清單： `dpkg -l | grep storagegrid`

   範例：

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. 移除先前的 StorageGRID 套件： `dpkg -r images-package service-package`

   > 請勿移除您目前執行的 StorageGRID 版本或您打算升級至的 StorageGRID 版本的安裝封存。

   範例：

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. 移除 StorageGRID Container 映像。

Docker

1. 擷取已安裝的容器映像清單： `docker images`

   範例：

```
[root@docker-example ~]# docker images
REPOSITORY           TAG             IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node      610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node    7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway     2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node    7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node      404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node    c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway     1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node    1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node      872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node    121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway     5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node      ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node    f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node    5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway     cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. 移除舊版 StorageGRID 的容器映像： `docker rmi image id`

   請勿移除您目前執行的 StorageGRID 版本或您打算升級至的 StorageGRID 版本的容器映像。

範例：

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

Podman

1. 擷取已安裝的容器映像清單： `podman images`

   範例：

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. 移除舊版 StorageGRID 的容器映像：`podman rmi *image id*`

> 請勿移除您目前執行的 StorageGRID 版本或您打算升級至的 StorageGRID 版本的容器映像。

範例：

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

執行 **StorageGRID** 升級

您可以升級至 StorageGRID 12.1，並同時套用該版本的最新 Hotfix。StorageGRID 升級頁面提供了建議的升級途徑，並直接連結至正確的下載頁面。

開始之前

您已檢閱所有考量事項、並完成所有規劃與準備步驟。

如果您急需擴展儲存以增加容量（如果您的儲存幾乎已滿），請不要開始升級。及時完成升級程序。如果需要恢復，請聯絡技術支援。

存取 **StorageGRID** 升級頁面

第一步是在 Grid Manager 中存取 StorageGRID 升級頁面。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 選擇*維護* > 系統 > 軟體更新。
3. 從 StorageGRID 升級方塊中、選取 * 升級 * 。

選取檔案

StorageGRID 升級頁面上的升級途徑指示了要升級到最新 StorageGRID 版本，必須安裝哪些主要版本（例如 12.1.0）和 Hotfix（例如 12.1.0.1）。您應該按照所示順序安裝建議的版本和 Hotfix。

如果沒有顯示更新路徑，您的瀏覽器可能無法存取NetApp支援站點，或AutoSupport頁面（支援 > 工具 > **AutoSupport** > 設定）上的 *檢查軟體更新*複選框可能已停用。

步驟

1. 如需 * 選取檔案 * 步驟、請檢閱更新路徑。
2. 從「下載檔案」區段中、選取每個 * 下載 * 連結、即可從 NetApp 支援網站 下載所需的檔案。

   如果沒有顯示更新路徑、請前往 "NetApp下載StorageGRID"以判斷是否有新版本或 Hotfix 可用、並下載您需要的檔案。

   如果您需要在所有 Linux 主機上下載並安裝 RPM 或 Deb 套件、您可能已經在更新路徑中列出 StorageGRID 升級和 Hotfix 檔案。

3. 選擇 **Browse** 將版本升級檔案上傳到 StorageGRID：
   `NetApp_StorageGRID_12.1.0_Software_uniqueID.upgrade`

   上傳和程式碼簽署驗證完成後，檔案名稱旁邊會出現一個綠色複選標記。

4. 如果您下載了 Hotfix 檔案、請選取 * 瀏覽 * 來上傳該檔案。Hotfix 將會在版本升級時自動套用。
5. 選擇*繼續*。

執行預先檢查

執行預先檢查可讓您在開始升級網格之前、先偵測並解決任何升級問題。

步驟

1. 在「 * 執行預先檢查 * 」步驟中、請先輸入您網格的資源配置複雜密碼。
2. 選擇*下載恢復套件*。

   在升級主管理節點之前，您應該下載復原包檔案的目前副本。如果發生故障，恢復包檔案可讓您恢復系統。

3. 下載檔案後、請確認您可以存取內容、包括 `Passwords.txt`檔案。
4. 將下載(`.zip`的檔案複製到兩個安全且獨立的位置。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

5. 選取 * 執行預先檢查 * 、然後等待預先檢查完成。
6. 請查看每項已報告的預先檢查的詳細資訊，並解決所有已報告的錯誤。請參閱 "StorageGRID 軟體升級解決方案指南"，以取得 StorageGRID 12.1 版本的相關說明。

   您必須先解決所有預先檢查錯誤 _ 、才能升級系統。不過、您不需要在升級前先處理預先檢查 _ 警告 _ 。

   如果您已開啟任何自訂防火牆連接埠、系統會在預先檢查驗證期間通知您。您必須先聯絡技術支援部門、才能繼續升級。

7. 如果您進行任何組態變更以解決回報的問題、請再次選取 * 執行預先檢查 * 以取得更新的結果。

   如果所有錯誤都已解決、系統會提示您開始升級。

開始升級並升級主要管理節點

當您開始升級時、升級預先檢查會再次執行、而且會自動升級主要管理節點。此部分升級最多可能需要 30 分鐘。

當主要管理節點正在升級時、您將無法存取任何其他 Grid Manager 頁面。稽核記錄也無法使用。

步驟

1. 選擇 * 開始升級 * 。

   系統會出現警告、提醒您暫時失去 Grid Manager 的存取權。

2. 選擇 * 確定 * 以確認警告並開始升級。
3. 等待執行升級前置檢查、並讓主要管理節點升級。

   如果報告了任何預先檢查錯誤、請予以解決、然後再次選取 * 開始升級 * 。

   如果網格有另一個已上線且已就緒的管理節點、您可以使用該網格來監控主要管理節點的狀態。一旦主管理

節點升級、您就可以核准其他網格節點。

4. 視需要選取 * 繼續 * 以存取 * 升級其他節點 * 步驟。

升級其他節點

您必須升級所有網格節點、但您可以執行多個升級工作階段、並自訂升級順序。例如、您可能偏好在一個工作階段中升級站台 A 的節點、然後在稍後的工作階段中升級站台 B 的節點。如果您選擇在多個工作階段中執行升級、請注意、在所有節點都升級之前、您無法開始使用新功能。

如果節點升級順序很重要、請一次核准一個節點或節點群組、並等到每個節點上的升級完成後、再核准下一個節點或節點群組。

在網格節點上開始升級時、該節點上的服務會停止。之後、網格節點會重新開機。為了避免與節點通訊的用戶端應用程式發生服務中斷、除非您確定節點已準備好要停止並重新開機、否則請勿核准節點的升級。視需要排程維護時段或通知客戶。

步驟

1. 對於 * 升級其他節點 * 步驟、請檢閱摘要、其中提供整個升級的開始時間、以及每個主要升級工作的狀態。
   - * 開始升級服務 * 是第一項升級工作。在此工作期間、軟體檔案會發佈至網格節點、並在每個節點上啟動升級服務。
   - 當*啟動升級服務*任務完成後，*升級其他網格節點*任務啟動，並提示您下載復原套件的新副本。
2. 出現提示時，輸入您的設定密碼並下載恢復包的新副本。

主管理節點升級後，您應該下載恢復包檔案的新副本。如果發生故障，恢復包檔案可讓您恢復系統。

3. 檢閱每種節點類型的狀態表。有非主要管理節點、閘道節點和儲存節點的表格。

   當表格第一次出現時、網格節點可以處於下列其中一個階段：

   - 打開升級的包裝
   - 正在下載
   - 等待核准
4. 當您準備好選擇要升級的網格節點（或需要取消核准選取的節點）時、請使用下列指示：

對於 StorageGRID 12.1 升級，如果您想要核准單一節點而不是所有節點，最佳實務做法是在移至下一個站台之前升級整個站台。

工作	指示
搜尋要核准的特定節點、例如特定站台上的所有節點	在 * 搜尋 * 欄位中輸入搜尋字串
選取所有節點以進行升級	選取 * 核准所有節點 *

工作	指示
選取所有類型相同的節點進行升級（例如、所有儲存節點）	選取節點類型的 * 核准全部 * 按鈕 如果您核准多個相同類型的節點、則節點將一次升級一個。
選取要升級的個別節點	選取節點的 * 核准 * 按鈕
延後所有選取節點的升級	選取 * 取消核准所有節點 *
在所有相同類型的選定節點上延遲升級	選擇 * 不核准所有 * 按鈕作為節點類型
延後個別節點上的升級	選取節點的 * Unapprov* 按鈕

5. 等待核准的節點繼續進行這些升級階段：
   - 已核准、正在等待升級
   - 停止服務

     當節點的「階段」達到 * 停止服務 * 時、您無法移除該節點。「 **Unapprov** 」按鈕已停用。

   - 正在停止 Container
   - 清理 Docker 影像
   - 升級基礎作業系統套件

     當應用裝置節點到達此階段時、應用裝置上的 StorageGRID 應用裝置安裝程式軟體即會更新。此自動化程序可確保StorageGRID SynsanceAppliance Installer版本與StorageGRID 支援的更新版本保持同步。

   - 重新開機

     某些應用裝置機型可能會多次重新開機、以升級韌體和 BIOS 。

   - 重新開機後執行步驟
   - 啟動服務
   - 完成
6. 視需要重複核准步驟多次、直到所有網格節點都升級為止。

完整升級

當所有網格節點完成升級階段後、 * 升級其他網格節點 * 工作會顯示為已完成。其餘的升級工作會在背景中自動執行。

步驟

1. 「啟用功能」工作完成後（最多一小時），即可開始使用升級後的 StorageGRID 版本中的 "新功能"。
   - 最終升級步驟 * 完成後、即完成升級。第一步 * 選擇檔案 * 會以綠色成功橫幅重新顯示。
2. 確認網格作業已恢復正常：
   a. 檢查服務是否正常運作、以及是否沒有非預期的警示。
   b. 確認用戶端連線StorageGRID 至該系統的運作正常。

相關資訊

"系統在升級期間的影響"

疑難排解 StorageGRID 升級問題

如果執行升級時發生問題、您可以自行解決問題。如果您無法解決問題、請盡可能收集更多資訊、然後聯絡技術支援部門。

升級未完成

下列各節說明如何從部分升級失敗的情況中恢復。

升級預先檢查錯誤

若要偵測並解決問題、您可以在開始實際升級之前、手動執行升級前置檢查。大多數預先檢查錯誤都提供如何解決問題的相關資訊。

資源配置失敗

如果自動資源配置程序失敗、請聯絡技術支援部門。

網格節點當機或無法啟動

如果網格節點在升級過程中當機、或在升級完成後無法成功啟動、請聯絡技術支援部門以調查並修正任何潛在問題。

擷取或資料擷取中斷

如果在您不升級網格節點時、資料擷取或擷取意外中斷、請聯絡技術支援部門。

資料庫升級錯誤

如果資料庫升級失敗並出現錯誤、請重試升級。如果再次失敗、請聯絡技術支援部門。

相關資訊

"在升級軟體之前、請先檢查系統狀況"

使用者介面問題

在升級期間或之後、您可能會遇到與 Grid Manager 或 Tenant Manager 有關的問題。

Grid Manager 會在升級期間顯示多個錯誤訊息

如果您在升級主要管理節點時重新整理瀏覽器或瀏覽至其他 Grid Manager 頁面、可能會看到多則「 503 ：服務無法使用」和「連線至伺服器時發生問題」訊息。您可以安全地忽略這些訊息、這些訊息會在節點升級後立即停止顯示。

如果這些訊息在您開始升級後超過一小時出現、可能是發生了一些導致主要管理節點無法升級的情況。如果您無法自行解決問題、請聯絡技術支援部門。

Web介面未如預期回應

Grid Manager或Tenant Manager在StorageGRID 升級完更新版的更新軟體後、可能無法如預期般回應。

如果您在使用網路介面時遇到問題：

- 請確定您使用的"支援的網頁瀏覽器"是。

  瀏覽器支援通常會針對每StorageGRID 個版本進行變更。

- 清除網頁瀏覽器快取。

  清除快取會移除舊版StorageGRID 的更新資源、並允許使用者介面再次正確運作。如需相關指示、請參閱網頁瀏覽器的說明文件。

「 Docker image Availability check 」錯誤訊息

嘗試開始升級程序時、您可能會收到錯誤訊息、指出「 Docker 映像可用度檢查驗證套件已識別下列問題」。您必須先解決所有問題、才能完成升級。

如果您不確定解決已知問題所需的變更、請聯絡技術支援部門。

訊息	原因	解決方案
無法判斷升級版本。升級版本資訊檔案 `{file_path}`與預期格式不符。	升級套件毀損。	重新上傳升級套件、然後再試一次。如果問題持續發生、請聯絡技術支援部門。
找不到升級版本資訊檔案 `{file_path}`。無法判斷升級版本。	升級套件毀損。	重新上傳升級套件、然後再試一次。如果問題持續發生、請聯絡技術支援部門。
無法確定上目前安裝的版本 `{node_name}`。	節點上的重要檔案已毀損。	聯絡技術支援。
嘗試在上列出版本時發生連線錯誤 `{node_name}`	節點離線或連線中斷。	請檢查以確定所有節點均已上線、且可從主要管理節點存取、然後再試一次。

訊息	原因	解決方案
節點的主機 `{node_name}`未載入 StorageGRID `{upgrade_version}` 映像。必須先在主機上安裝映像和服務、才能繼續升級。	用於升級的RPM或Dub套件尚未安裝在執行節點的主機上、或影像仍在匯入中。 *附註：*此錯誤僅適用於以容器形式在Linux上執行的節點。	請檢查以確定已在所有執行節點的Linux主機上安裝RPM或Deb套件。確認服務和映像檔的版本都正確。請稍候幾分鐘、然後再試一次。 請參閱。 "Linux：在所有主機上安裝RPM或Deb套件"
檢查節點時發生錯誤 `{node_name}`	發生非預期的錯誤。	請稍候幾分鐘、然後再試一次。
執行預先檢查時發生未捕捉的錯誤。 `{error_string}`	發生非預期的錯誤。	請稍候幾分鐘、然後再試一次。

套用 StorageGRID Hotfix

修復程序StorageGRID

如果在功能版本之間偵測到並解決軟體問題、您可能需要將修補程式套用StorageGRID 至您的無法修復的系統。

不含功能或修補程式版本、而可在其中進行軟體變更。StorageGRID未來版本也會包含相同的變更。此外、每個修補程式版本都包含功能或修補程式版本中所有先前修復程式的彙總。

套用修補程式的考量

當另一個維護程序正在執行時、您無法套用 StorageGRID Hotfix 。例如、在執行取消委任、擴充或還原程序時、您無法套用 Hotfix 。

> 如果節點或站台停用程序暫停、您可以安全地套用修補程式。此外、StorageGRID 您也可以在更新程序的最後階段套用修補程式。如需詳細資訊、請參閱升級StorageGRID 版的介紹。

在Grid Manager中上傳此修補程式之後、此修復程式會自動套用至主要管理節點。然後、您可以核准將此修補程式應用到StorageGRID 您的靜止系統的其餘節點。

如果某個熱修復無法套用至一或多個節點、則故障原因會出現在熱修復程序進度表的詳細資料欄中。您必須解決導致故障的任何問題、然後重試整個程序。先前成功應用此修復程序的節點將跳過後續應用程序。您可以安全地重試修復程序程序程序、重試次數不限、直到所有節點都更新完畢為止。必須在所有網格節點上成功安裝此修補程式、才能完成應用程式。

雖然網格節點是以新的修補程式版本更新、但是修復程式中的實際變更可能只會影響特定類型節點上的特定服務。例如、熱修復程式可能只會影響儲存節點上的LDR服務。

如何套用修補程式來進行還原和擴充

將 Hotfix 套用至網格後，主要管理節點或非主要管理節點會自動將相同的 Hotfix 版本安裝至透過恢復作業還原

或透過擴充新增的任何節點。當您登入非主要管理節點時，可以恢復任何節點（包括主要管理節點）。如果您從非主要管理節點恢復節點，則該管理節點會將 Hotfix 套用至已恢復的節點。

如果需要從主要管理節點本身的 StorageGRID 安裝程式恢復該節點，則必須手動安裝正確的 StorageGRID 版本，然後套用 Hotfix。主要管理節點的最終 StorageGRID 版本必須與網格中其他節點的版本相符。

以下範例說明登入非主要管理節點時，如何套用 Hotfix 來恢復主要管理節點：

1. 假設網格使用StorageGRID 最新的修補程式執行的是更新版本的S11。*A.B*。「網格版本」為 11.*A.B.y* 。
2. 主管理節點故障。
3. 您可以使用StorageGRID 下列功能重新部署主管理節點：ES11.*A.B*、然後執行恢復程序。

   如需符合網格版本、您可以在部署節點時使用次要版本、而不需要先部署主要版本。

4. 然後將修補程式11._A.B.y_套用至主要管理節點。

應用熱修復程式後 **StorageGRID** 會受到怎樣的影響

您必須瞭StorageGRID 解套用修補程式時、您的整個系統將會受到什麼影響。

StorageGRID Hotfix 不中斷營運

StorageGRID 系統可在整個 Hotfix 程序中、從用戶端應用程式擷取及擷取資料。如果您將所有類型相同的節點都核准給 Hotfix （例如儲存節點）、則節點會一次關閉一個節點、因此當某種類型的所有網格節點或所有網格節點都無法使用時、就不會有任何時間。

為了確保持續可用、請確保 ILM 原則包含指定儲存每個物件多個複本的規則。您也必須確定所有外部 S3 用戶端都已設定為傳送要求至下列其中一項：

- 高可用度（ HA ）群組虛擬 IP 位址
- 高可用度協力廠商負載平衡器
- 每個用戶端有多個閘道節點
- 每個用戶端有多個儲存節點

用戶端應用程式可能會遭遇短期中斷

整個修復程序過程中、支援從用戶端應用程式擷取和擷取資料；不過、如果修復程式需要重新啟動這些節點上的服務、則個別閘道節點或儲存節點的用戶端連線可能會暫時中斷。StorageGRID在修復程序完成後、連線功能將會恢復、而服務會在個別節點上恢復。

如果連線中斷時間很短、您可能需要排定停機時間、才能套用修補程式。您可以使用選擇性核准來排程特定節點的更新時間。

您可以使用多個閘道和高可用度（HA）群組、在修復程序程序期間提供自動容錯移轉功能。請參閱的說明"設定高可用度群組"。

可能會觸發警示和**SNMP**通知

當服務重新啟動時、StorageGRID 以及當作業系統以混合版本環境運作時（某些執行舊版的網格節點、而其他節點則已升級至更新版本）、可能會觸發警示和SNMP通知。一般而言、這些警示和通知會在修復程式完成時清除。

組態變更受到限制

將修補程式套用StorageGRID 至

- 在將 Hotfix 套用至所有節點之前、請勿變更任何網格組態（例如、指定網格網路子網路或核准擱置的網格節點）。
- 在將 Hotfix 套用至所有節點之前、請勿更新 ILM 組態。

取得 **StorageGRID** 熱修復程式所需的材料

在套用修補程式之前、您必須先取得所有必要資料。

項目	附註
修復程式檔案StorageGRID	您必須下載StorageGRID 更新程式檔案。
• 網路連接埠 • "支援的網頁瀏覽器" • SSH用戶端（例如Putty）	
恢復套件(`.zip`）檔案	在應用修補程式之前，"下載最新的復原包文件"以防修復期間出現任何問題。然後，在應用修補程式後，下載恢復套件檔案的新副本並將其保存在安全的位置。更新後的恢復包檔案可讓您在發生故障時恢復系統。
Passwords.txt檔案	可選，僅當您使用 SSH 用戶端手動應用修補程式時才使用。這 `Passwords.txt`文件是恢復包的一部分 `.zip`文件。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼未列在 `Passwords.txt`檔案中。
相關文件	`readme.txt`Hotfix 的檔案。此檔案包含在修補程式下載頁面上。請務必在套用 Hotfix 之前仔細檢閱 `readme`檔案。

下載 **StorageGRID Hotfix** 檔案

您必須先下載此修復程式檔案、才能套用此修復程式。

步驟

1. 前往 "NetApp下載StorageGRID"。
2. 選取*可用軟體*下的向下箭號、即可查看可供下載的修補程式清單。

熱修復檔案版本的格式為：11.4_.x.y__。

3. 檢閱更新中包含的變更。

如果您只有"已恢復主管理節點"、而且需要套用 Hotfix 、請選取安裝在其他網格節點上的相同 Hotfix 版本。

a. 選取您要下載的修補程式版本、然後選取「執行」。
b. 使用您NetApp帳戶的使用者名稱和密碼登入。
c. 閱讀並接受終端使用者授權合約。

此時會出現所選版本的下載頁面。

d. 下載 Hotfix `readme.txt` 檔案以檢視 Hotfix 所包含變更的摘要。

4. 選取熱修復程式的下載按鈕、然後儲存檔案。

請勿變更此檔案的名稱。

如果您使用的是 macOS 裝置、 Hotfix 檔案可能會自動儲存為 `.txt`檔案。如果是、您必須重新命名檔案而不使用 `.txt`副檔名。

5. 選取下載位置、然後選取*儲存*。

在套用 StorageGRID 熱修復程式之前、請先檢查系統狀況

您必須驗證系統是否已準備好容納此修復程式。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 如有可能、請確定系統正常運作、且所有網格節點均已連接至網格。

已連線的節點在「節點」頁面上會顯示綠色對勾。

3. 如有可能、請檢查並解決任何目前的警示。
4. 確保沒有其他維護程序在進行中、例如升級、恢復、擴充或取消委任程序。

在套用修補程式之前、您應該先等待任何作用中的維護程序完成。

當另一個維護程序正在執行時、您無法套用 StorageGRID Hotfix 。例如、在執行取消委任、擴充或還原程序時、您無法套用 Hotfix 。

如果"取消委任程序已暫停"是節點或站點，則可以安全地應用修復程序。此外、StorageGRID 您也可以在更新程序的最後階段套用修補程式。請參閱的說明"升級 StorageGRID 軟體"。

在 StorageGRID 中套用 Hotfix

熱修復程式會先自動套用至主要管理節點。然後、您必須核准將此修補程式應用到其他網格節點、直到所有節點都執行相同的軟體版本為止。您可以選取核准個別的網格節點、網格節點群組或所有網格節點、以自訂核准順序。

開始之前

- 您已檢閱"套用 Hotfix 的考量事項"。
- 您有資源配置通關密碼。
- 您擁有根目錄存取權或維護權限。

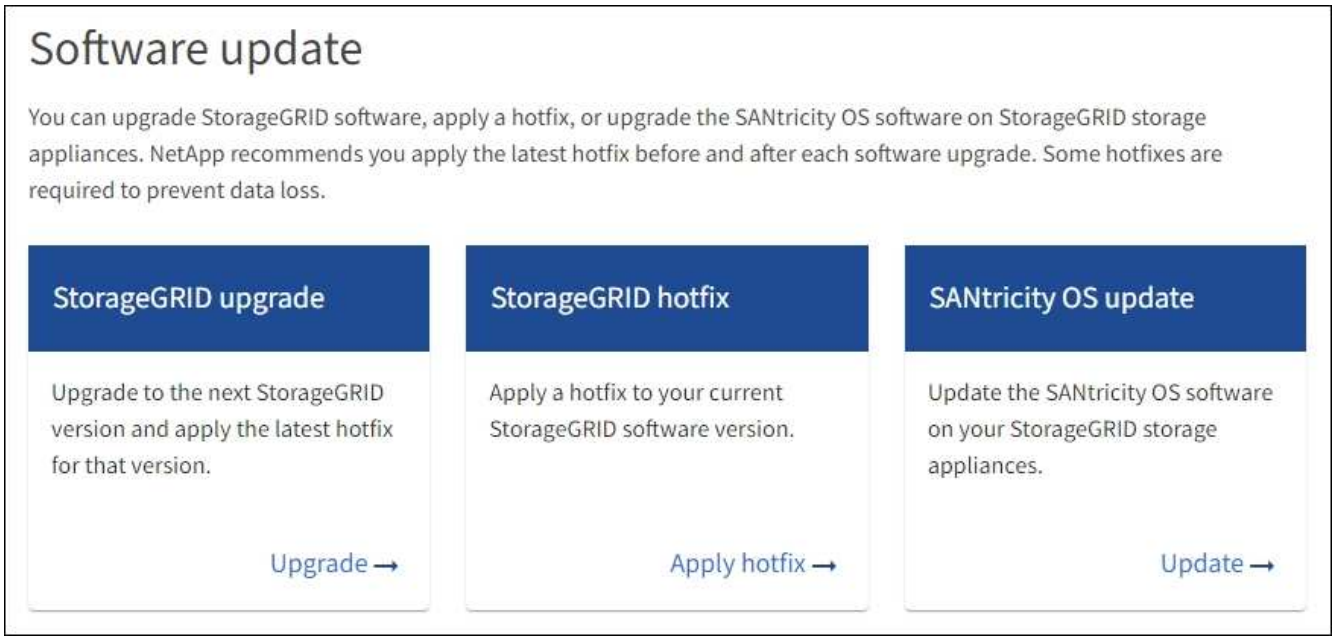
關於這項工作

- 您可以延遲將修補程式套用至節點、但在您將修補程式套用至所有節點之前、修復程序程序程序並未完成。
- 您必須先完成 Hotfix 程序、才能執行 StorageGRID 軟體升級或 SANtricity OS 更新。

步驟

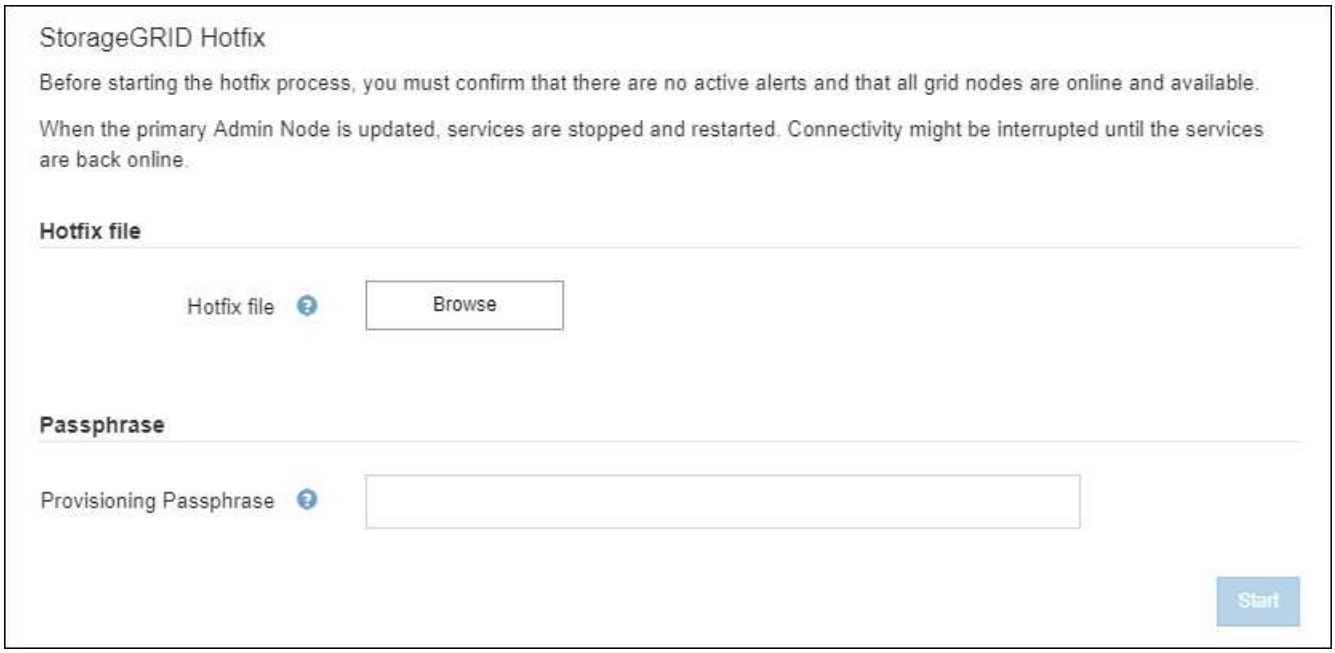
1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 選擇*維護* > 系統 > 軟體更新。

   此時會出現「軟體更新」頁面。



3. 選取*套用Hotfiy*。

   出現「此修復」頁面。StorageGRID



4. 選取您從 NetApp 支援網站 下載的 Hotfix 檔案。

   a. 選擇*瀏覽*。

   b. 找出並選取檔案。

      `hotfix-install-version`

   c. 選取*「Open*（開啟*）」。

      檔案即會上傳。上傳完成後、檔案名稱會顯示在詳細資料欄位中。

      請勿變更檔案名稱、因為它是驗證程序的一部分。

5. 在文字方塊中輸入資源配置通關密碼。

   。Start*（開始*）按鈕隨即啟用。

6. 選擇* Start*。

   此時會出現一則警告、指出當主要管理節點上的服務重新啟動時、瀏覽器的連線可能會暫時中斷。

7. 選擇*確定*、開始將此修復程式套用至主要管理節點。

   當熱修復程式啟動時：

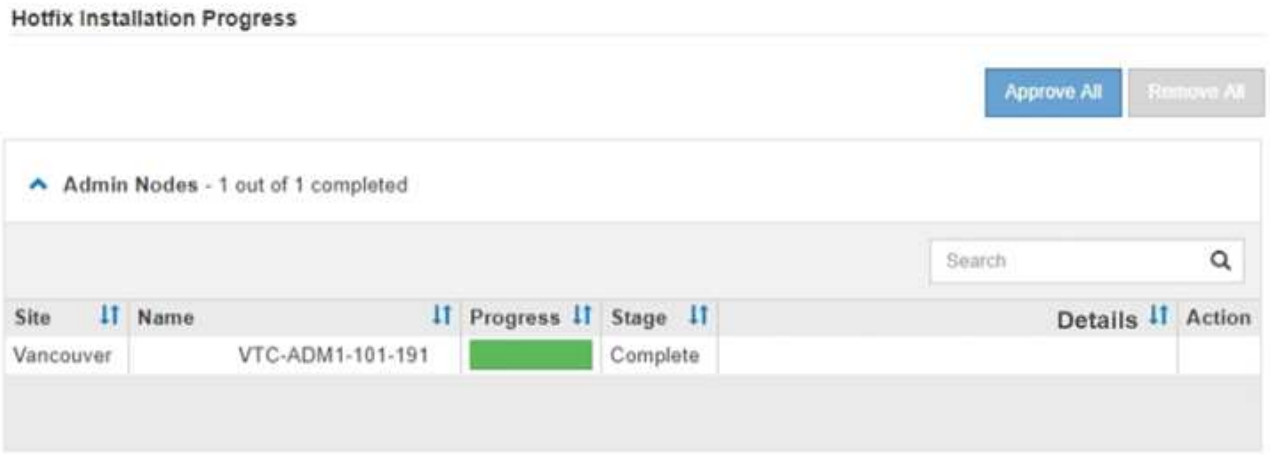
   a. 執行修補程式驗證，包括程式碼簽章驗證。

      如果報告了任何錯誤、請解決這些錯誤、重新上傳修復程式檔案、然後再次選取* Start*。

   b. 此時會出現熱修復安裝進度表。

      下表顯示網格中的所有節點、以及每個節點的目前修復程序安裝階段。表格中的節點會依類型（管理節點、閘道節點和儲存節點）分組。

c. 進度列會到達完成狀態、然後主管理節點會顯示為「完成」。



8. 或者、您也可以根據*站台*、名稱、進度、階段*或*詳細資料、以遞增或遞減順序排序每個群組中的節點清單。或者、在*搜尋*方塊中輸入詞彙、以搜尋特定節點。
9. 核准準備更新的網格節點。相同類型的核准節點一次升級一個。

除非您確定節點已準備好要更新、否則請勿核准節點的 Hotfix 。將 Hotfix 套用至網格節點時、該節點上的某些服務可能會重新啟動。這些作業可能會造成與節點通訊的用戶端服務中斷。

- 選取一或多個*核准*按鈕、將一個或多個個別節點新增至熱修復佇列。
- 選取每個群組中的「全部核准」按鈕、將同類型的所有節點新增至熱修復佇列。如果您在「搜尋」方塊中輸入搜尋條件、則「核准全部」按鈕會套用至搜尋條件所選取的所有節點。

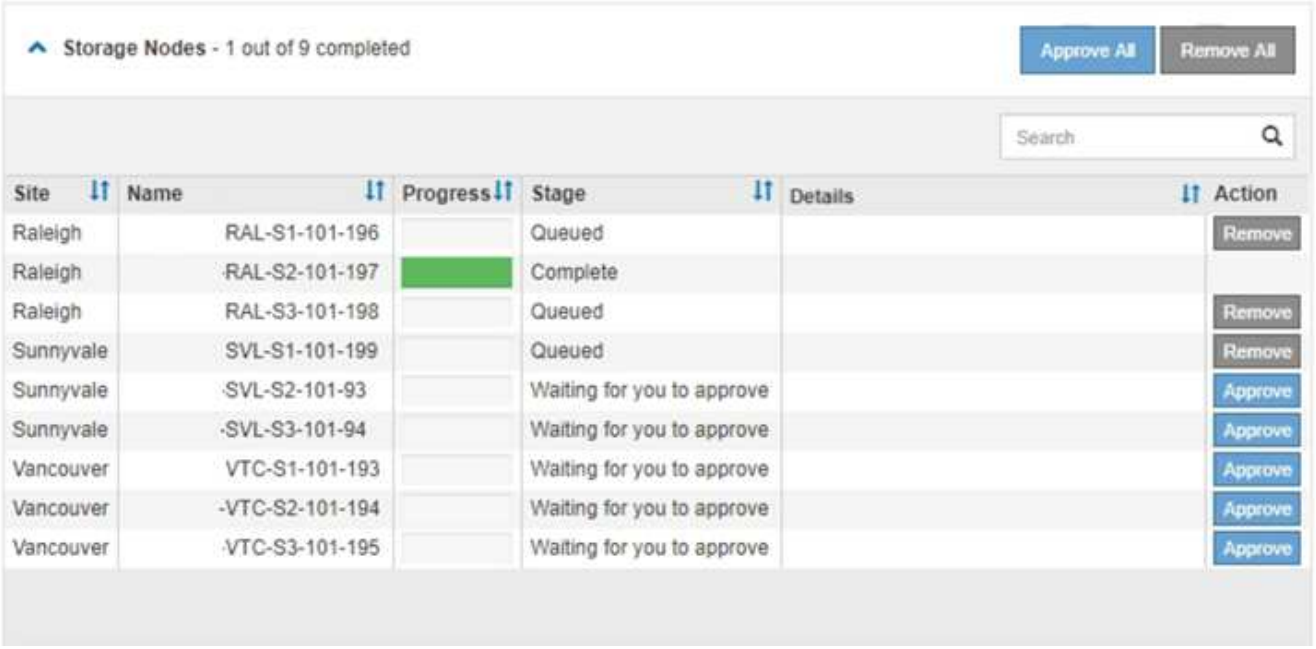
頁面頂端的「全部核准」按鈕會核准頁面上所列的所有節點、而表格群組頂端的「全部核准」按鈕只會核准該群組中的所有節點。如果節點升級順序很重要、請一次核准一個節點或節點群組、並等到每個節點上的升級完成後、再核准下一個節點。

- 選取頁面頂端的「頂層*核准全部*」按鈕、將網格中的所有節點新增至熱修復佇列。

您必須先完成StorageGRID 此解決方案、才能開始進行其他軟體更新。如果您無法完成此修補程式、請聯絡技術支援部門。

- 選取*移除*或*全部移除*、即可從熱修復佇列移除節點或所有節點。

  當「階段」進度超過「佇列中」時、 * 移除 * 按鈕會隱藏、您無法再從 Hotfix 程序中移除節點。



10. 等待熱修復程式套用至每個核准的網格節點。

    在所有節點上成功安裝此修復程序後、「修復程序安裝進度表」便會關閉。綠色橫幅會顯示修復程式完成的日期和時間。

11. 如果無法將此修復程式套用至任何節點、請檢閱每個節點的錯誤、解決問題、然後重複這些步驟。

    在所有節點上成功套用此修復程式之前、程序才會完成。您可以安全地重試修復程序程序、直到完成為止、重試次數不限。

設定及管理 StorageGRID 系統

管理StorageGRID

StorageGRID 管理快速入門

請使用這些指示來設定及管理StorageGRID 一套功能完善的系統。

請確保您對 StorageGRID 系統有基本的了解，並且對 Linux 命令 shell、連網以及伺服器硬體設定和組態有相當詳細的知識。

1 開始使用 **Grid Manager**

- "學習使用 Grid Manager 使用者介面的基本步驟"
- "了解授權資訊"
- "了解如何使用網格管理 API"

2 控制對 **StorageGRID** 的存取

- "了解通行密碼、密碼和權限"
- "設定身分識別聯盟"
- "管理管理群組"
- "管理使用者"
- "設定單一登入 (SSO)"

3 使用網格聯邦

- "設定網格聯盟連線"
- "了解帳戶同步"
- "了解跨網格複寫"
- "設定全域命名空間"

4 管理安全性

- "檢閱StorageGRID 功能加密方法"
- "管理憑證"
- "設定安全性設定"
- "設定金鑰管理伺服器"
- "管理Proxy設定"

- "控制防火牆"

5 管理租戶

- "了解並管理租戶帳戶"
- "管理租戶平台服務"
- "管理用戶帳戶的S3 Select"

6 設定用戶端連線

- "了解 S3 用戶端的安全性"
- "使用 S3 設定精靈"
- "管理高可用度群組"
- "設定 S3 端點網域名稱"

7 管理網路和連線

- "設定網路設定"
- "設定VLAN介面"
- "管理流量分類原則"
- "管理連結成本"

8 管理節點

- "管理儲存節點"
- "管理管理節點"

開始使用 **Grid Manager**

StorageGRID 的 **Web** 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	138
Microsoft Edge	138
Mozilla Firefox	140

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

Sign in 至 StorageGRID 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。

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、某些維護程序只能從主要管理節點執行。

連線至 HA 群組

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

使用 SSO

如果"已設定單一登入（ SSO ）"。

在第一個管理節點上登入 Grid Manager

開始之前

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

  `https://FQDN_or_Admin_Node_IP/`

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

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

  `https://FQDN_or_Admin_Node_IP:port/`

步驟

1. 啟動支援的網頁瀏覽器。
2. 在瀏覽器的網址列中、輸入 Grid Manager 的 URL 。
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。請參閱。 "管理安全性憑證"
4. 登入Grid Manager。

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

未使用 **SSO**

a. 輸入Grid Manager的使用者名稱和密碼。

b. 選擇*登入*。

使用 **SSO**

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

  i. 選擇*登入*。您可以將 0 留在「帳戶」欄位中。

  ii. 在您組織的 SSO 登入頁面上輸入您的標準 SSO 憑證。

  例如，如果StorageGRID正在使用 SSO 並且您之前曾造訪網格管理器或租用戶帳戶：

  A. 輸入 * 0* （ Grid Manager 的帳戶 ID ）、或選擇 * Grid Manager* （如果它出現在最近帳戶清單中）。

  B. 選擇*登入*。

  C. 在組織的SSO登入頁面上、以標準SSO認證登入。

登入後、會出現 Grid Manager 首頁、其中包含儀表板。若要瞭解所提供的資訊，請參閱"檢視及管理儀表板"。

登入另一個管理節點

請依照下列步驟登入其他管理節點。

未使用 **SSO**

步驟

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

使用 **SSO**

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

步驟

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

登出 **StorageGRID Grid Manager**

完成 Grid Manager 的使用後、您必須登出、以確保未經授權的使用者無法存取 StorageGRID 系統。根據瀏覽器Cookie設定、關閉瀏覽器可能不會將您登出系統。

步驟

1. 在右上角選取您的使用者名稱。
2. 選取 * 登出 * 。

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

更改 **StorageGRID Grid Manager** 密碼

如果您是Grid Manager的本機使用者、可以變更自己的密碼。

開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

關於這項工作

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

步驟

1. 從Grid Manager標頭中、選取*您的名稱_*>*變更密碼*。
2. 輸入您目前的密碼。
3. 輸入新密碼。

   您的密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。

4. 重新輸入新密碼。
5. 選擇*保存*。

檢視**StorageGRID** 本授權資訊

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

開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

關於這項工作

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

步驟

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

     僅當授權發生問題時、才會顯示此連結。
2. 檢視目前授權的唯讀詳細資料：
   - 系統ID、這是此安裝的唯一識別號碼StorageGRID StorageGRID
   - 授權序號
   - 授權類型、 * 永久 * 或 * 訂閱 *
   - 網格的授權儲存容量
   - 支援的儲存容量
   - 授權結束日期。* 不適用 * 代表永久授權。
   - 支援結束日期

     此日期是從目前的授權檔案中讀取的，如果您在取得授權檔案後延長或續約了支援服務合約，則此日期可能已過期。若要更新此值，請參閱 "更新StorageGRID 版本的授權資訊"。您也可以使用 Digital Advisor 檢視實際的合約到期日期。
   - 授權文字檔的內容

更新**StorageGRID** 版本的授權資訊

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

開始之前

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

步驟

1. 選擇*維護* > 系統 > 許可證。
2. 在「更新授權」區段中、選取 * 瀏覽 * 。
3. 找到並選擇新的許可證文件(`.txt`) 。

   系統會驗證並顯示新的授權檔案。

4. 輸入資源配置通關密碼。
5. 選擇*保存*。

使用API

使用 StorageGRID Grid Management API

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

頂級資源

Grid Management API提供下列頂級資源：

- `/grid`：存取權限僅限 Grid Manager 使用者使用、並以設定的群組權限為基礎。
- `/org`：只有屬於租戶帳戶之本機或同盟 LDAP 群組的使用者才能存取。如需詳細資訊、請參閱 "使用租戶帳戶"。
- `/private`：存取權限僅限 Grid Manager 使用者使用、並以設定的群組權限為基礎。私有API如有變更、恕不另行通知。私有端點也會忽略該要求的API版本。StorageGRID

發出API要求

Grid Management API使用Swagger開放原始碼API平台。Swagger提供直覺式使用者介面、可讓開發人員和非開發人員StorageGRID 利用API在Real-Time中執行作業。

Swagger使用者介面提供每個API作業的完整詳細資料和文件。

開始之前

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

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

步驟

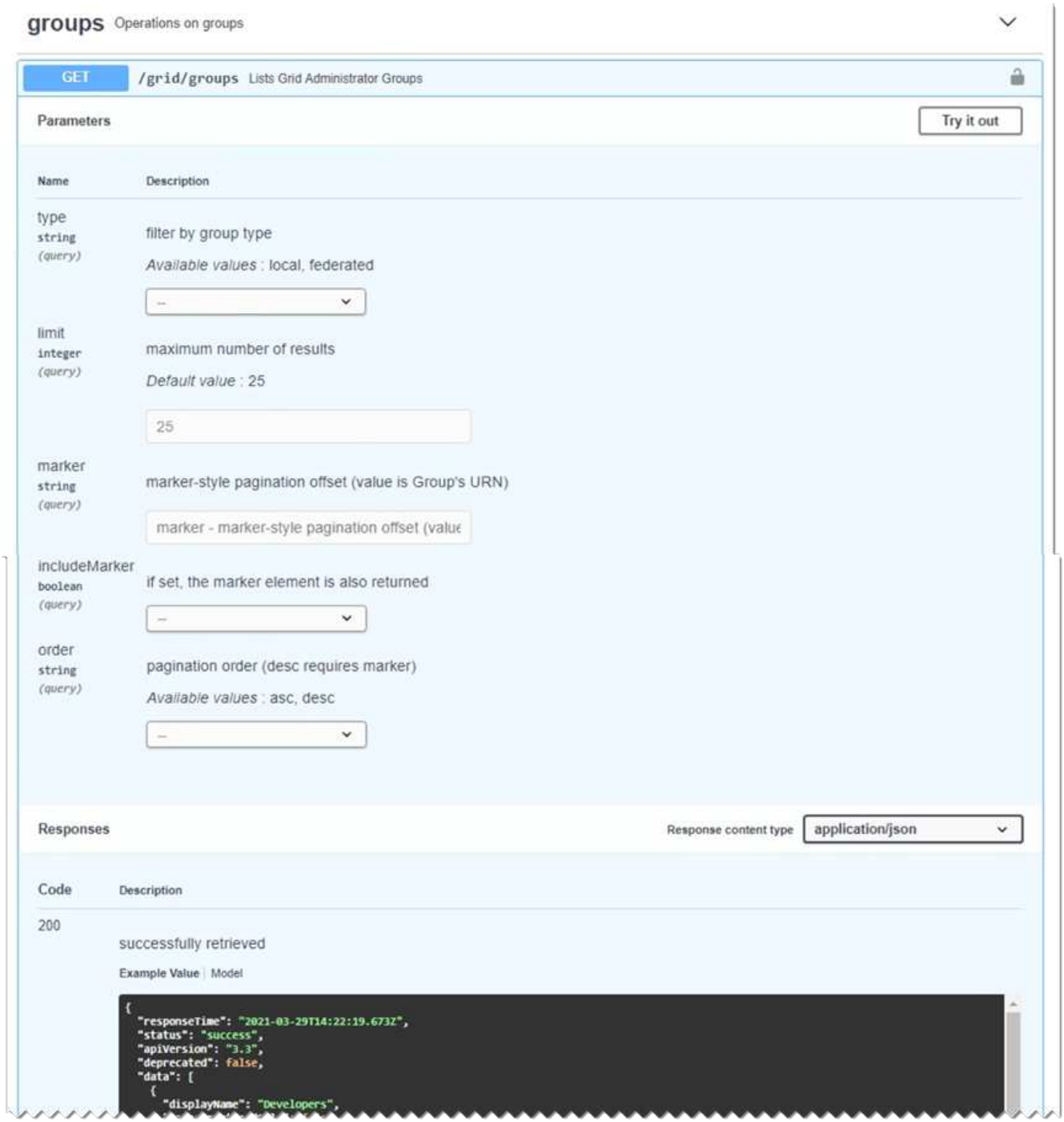
1. 從 Grid Manager 標題列中，選擇說明圖示 並選取 **API documentation**。
2. 若要使用私有API執行作業、請選取StorageGRID 「畫面管理API」頁面上的*前往私有API文件*。

   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。

StorageGRID 中的 Grid Management API 操作

Grid Management API會將可用的作業組織到下列各節中。

此清單僅包含公用API中可用的作業。

- * 帳戶 * ：管理儲存租戶帳戶的作業、包括建立新帳戶和擷取指定帳戶的儲存使用量。
- * 警示記錄 * ：已解決警示的操作。
- * 警示接收者 * ：警示通知接收者的作業（電子郵件）。
- * 警示規則 * ：警示規則的作業。
- * 警示 / 靜音 * ：警示靜音作業。
- * 警示 * ：警示作業。
- * 稽核 * ：列出及更新稽核組態的作業。
- * 驗證 * ：執行使用者工作階段驗證的作業。

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

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

  如需改善驗證安全性的資訊、請參閱「防範跨網站要求偽造」。

- * 用戶端憑證 * ：設定用戶端憑證的作業，以便使用外部監控工具安全地存取 StorageGRID 。
- * 組態 * ：與 Grid Management API 產品版本和版本相關的作業。您可以列出該版本所支援的產品版本和Grid Management API主要版本、也可以停用已過時的API版本。
- * 停用功能 * ：檢視可能已停用功能的作業。
- * DNS 伺服器 * ：列出及變更已設定外部 DNS 伺服器的作業。
- * 磁碟機詳細資料 * ：特定儲存設備機型的磁碟機操作。
- * 端點網域名稱 * ：列出及變更 S3 端點網域名稱的作業。
- * 銷毀編碼 * ：銷毀編碼設定檔的操作。
- * 擴充 * ：擴充作業（程序層級）。

- * 擴充節點 * ：擴充作業（節點層級）。
- * 擴充站台 * ：擴充作業（站台層級）。
- * 網格網路 * ：列出及變更網格網路清單的作業。
- *GRID 密碼 * ：網格密碼管理作業。
- * 群組 * ：管理本機 Grid Administrator 群組及從外部 LDAP 伺服器擷取同盟 Grid Administrator 群組的作業。
- * 身分識別來源 * ：設定外部身分識別來源及手動同步同盟群組與使用者資訊的作業。
- * ILM * ：資訊生命週期管理（ ILM ）作業。
- * 進行中程序 * ：擷取目前進行中的維護程序。
- * 授權 * ：擷取及更新 StorageGRID 授權的作業。
- * 日誌 * ：收集和下載日誌文件的操作
- * 指標 * ： StorageGRID 指標上的作業、包括單一時間點的即時指標查詢、以及一段時間內的範圍指標查詢。Grid Management API使用Prometheus系統監控工具作為後端資料來源。如需建構Prometheus查詢的相關資訊、請參閱Prometheus網站。

> 名稱中包含的計量*private*僅供內部使用。這些指標可能會在StorageGRID 不另行通知的情況下於各個版本之間變更。

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

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

Grid Management API使用版本管理來支援不中斷營運的升級。

例如、此 Request URL 會指定 API 的版本 4 。

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

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

下列範例說明如何根據所做的變更類型來提高API版本。

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

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

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

過時的要求會以下列方式標示為已過時：

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

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

判斷目前版本支援哪些**API**版本

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

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

指定要求的**API**版本

您可以使用路徑參數(`/api/v4`（）或標頭(`Api-Version: 4`（）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/v4/grid/accounts

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

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

您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、請在驗證期間將參數設 `csrfToken`為 `true`。預設值為 `false`。

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

如果為 True 、則 `GridCsrfToken`會以隨機值設定 Cookie 來登入 Grid Manager 、並以隨機值 `AccountCsrfToken`將 Cookie 設定為登入 Tenant Manager 。

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、標頭的值設為 CSRF Token Cookie 的值。
- 對於接受表單編碼實體的端點： `csrfToken`表單編碼的要求本文參數。

如需其他範例與詳細資料、請參閱線上API文件。

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

如果啟用了單一登入（Active Directory），請使用 StorageGRID API

如果你有"已設定並啟用單一登入（SSO）"並且您使用 Active Directory 作為 SSO 提供程序，則必須發出一系列 API 請求以取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用單一登入、請登入API

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

開始之前

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

關於這項工作

若要取得驗證權杖、您可以使用下列其中一個範例：

- 這 `storagegrid-ssoauth.py`Python 腳本，位於StorageGRID安裝檔目錄中 (./rpms`對於 RHEL，`./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。
- Curl要求的工作流程範例。

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

  範例Curl工作流程無法防止其他使用者看到密碼。

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

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2 。
   - 使用Curl要求。前往步驟 3 。
2. 如果您想要使用 `storagegrid-ssoauth.py`指令碼、請將指令碼傳送至 Python 解譯器、然後執行指令碼。

   出現提示時、請輸入下列引數的值：

   - SSO方法。輸入「ADFS」或「ADFS」。
   - SSO使用者名稱
   - 安裝了鏡面的網域StorageGRID
   - 解決這個StorageGRID 問題
   - 租戶帳戶ID（如果您要存取租戶管理API）。

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

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

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

3. 如果您要使用捲髮要求、請使用下列程序。

   a. 宣告登入所需的變數。

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

   若要存取 Grid Management API 、請使用 0 做為 `TENANTACCOUNTID`。

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

   此範例顯示的是簽署驗證 URL 的 POST 要求 `TENANTACCOUNTID`。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. 儲存 `SAMLRequest`來自回應的以供後續命令使用。

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

d. 取得完整的URL、其中包含AD FS的用戶端要求ID。

其中一個選項是使用先前回應的URL來要求登入表單。

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

回應包括用戶端要求ID：

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

e. 從回應中儲存用戶端要求ID。

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

f. 將您的認證資料傳送至先前回應的表單動作。

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

AD FS會傳回302重新導向、並在標頭中顯示其他資訊。

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

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

g. 儲存 `MSISAuth`回應中的 Cookie 。

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

h. 從驗證貼文傳送內含Cookie的Get要求至指定位置。

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

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

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

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

i. 從隱藏欄位儲存 `SAMLResponse`：

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

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

對於 `RelayState`、如果您想登入 Grid Management API 、請使用租戶帳戶 ID 或使用 0 。

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

回應包括驗證權杖。

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

a. 將回應中的驗證權杖另存為 `MYTOKEN`。

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

您現在可以用於其他要求、類似於未使用 SSO 時使用 `MYTOKEN` API 的方式。

如果啟用單一登入、請登出API

如果已啟用單一登入（SSO）、您必須發出一系列API要求、以登出Grid Management API或租戶管理API。如果您使用Active Directory做為SSO身分識別供應商、則適用這些指示

關於這項工作

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

步驟

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

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

會傳回登出URL：

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

2. 儲存登出URL。

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

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

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

會傳回302回應。重新導向位置不適用於純API登出。

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

4. 刪除StorageGRID 不記名權杖。

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

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

`204 No Content`回應表示使用者現在已登出。

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

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

如果你有"已設定並啟用單一登入（SSO）"並且您使用 Entra ID 作為 SSO 提供程序，您可以使用兩個範例腳本來取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用了 **Entra ID** 單一登入，**Sign inAPI**

如果您使用 Entra ID 作為 SSO 身分提供者，則適用這些說明

開始之前

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

關於這項工作

若要取得驗證權杖、您可以使用下列範例指令碼：

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

這兩個腳本都位於StorageGRID安裝檔目錄中(`./rpms`對於 RHEL， `./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。

要編寫您自己的與 Entra ID 的 API 集成，請參閱 `storagegrid-ssoauth-azure.py`腳本。 Python 腳本直接向StorageGRID發出兩個請求（先取得 SAMLRequest，然後取得授權令牌），同時呼叫 Node.js 腳本與 Entra ID 互動以執行 SSO 操作。

SSO 操作可以透過一系列 API 請求來執行，但這樣做並不簡單。 Puppeteer Node.js 模組用於抓取 Entra ID SSO 介面。

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

步驟

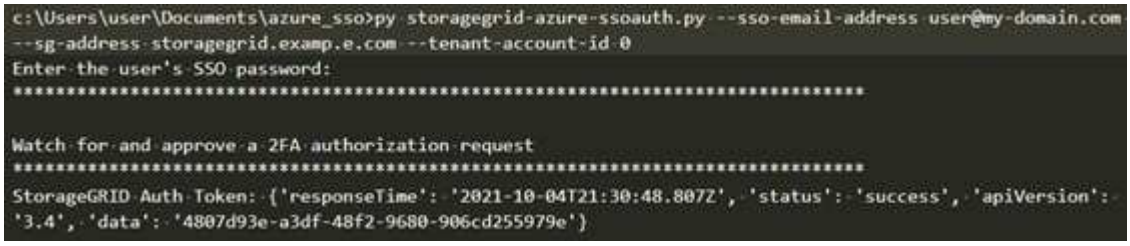
1. 安裝所需的相依性、如下所示：
   a. 安裝 Node.js （請參閱 "https://nodejs.org/en/download/"）。
   b. 安裝所需的Node.js模組（puppeteer和jsdom）：

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

2. 將Python指令碼傳遞給Python解譯器以執行指令碼。

   然後，Python 腳本將呼叫對應的 Node.js 腳本來執行 Entra ID 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 Entra ID 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，輸入密碼並準備在要求時向 Entra ID 提供 MFA 授權。



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

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

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

如果你有"已設定並啟用單一登入（SSO）"並且您使用 PingFederate 作為 SSO 提供程序，則必須發出一系列 API 請求以取得對網格管理 API 或租用戶管理 API 有效的身份驗證令牌。

如果啟用單一登入、請登入**API**

如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

開始之前

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

關於這項工作

若要取得驗證權杖、您可以使用下列其中一個範例：

- 這 `storagegrid-ssoauth.py`Python 腳本，位於StorageGRID安裝檔目錄中 (./rpms`對於 RHEL，`./debs`適用於 Ubuntu 或 Debian，以及 `./vsphere`對於 VMware)。
- Curl要求的工作流程範例。

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

  範例Curl工作流程無法防止其他使用者看到密碼。

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

步驟

1. 選取下列方法之一以取得驗證權杖：
   - 使用 `storagegrid-ssoauth.py` Python 指令碼。前往步驟 2 。
   - 使用Curl要求。前往步驟 3 。
2. 如果您想要使用 `storagegrid-ssoauth.py`指令碼、請將指令碼傳送至 Python 解譯器、然後執行指令碼。

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

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

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

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

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

3. 如果您要使用捲髮要求、請使用下列程序。

   a. 宣告登入所需的變數。

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

   若要存取 Grid Management API 、請使用 0 做為 `TENANTACCOUNTID`。

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

   此範例顯示TENANTACCOUNTID的簽署驗證URL的POST要求。結果會傳遞至python -m json.tool以移除Json編碼。

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

   此範例的回應包含URL編碼的已簽署URL、但不包含其他JSON-encoding層。

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

c. 儲存 `SAMLRequest`來自回應的以供後續命令使用。

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

d. 匯出回應和Cookie、並回應回應回應：

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

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

e. 匯出「pf.adaperId」值、並回應回應回應：

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

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

f. 匯出「Ha」值（移除結尾斜槓/）、然後回應回應：

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

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

g. 匯出「行動」值：

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

h. 傳送內含認證的Cookie：

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

i. 從隱藏欄位儲存 `SAMLResponse`：

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

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

對於 `RelayState`、如果您想登入 Grid Management API 、請使用租戶帳戶 ID 或使用 0 。

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

回應包括驗證權杖。

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

a. 將回應中的驗證權杖另存為 `MYTOKEN`。

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

您現在可以用於其他要求、類似於未使用 SSO 時使用 `MYTOKEN` API 的方式。

如果啟用單一登入、請登出API

如果已啟用單一登入（SSO）、您必須發出一系列API要求、以登出Grid Management API或租戶管理API。如果您使用PingFedate做為SSO身分識別供應商、則適用這些指示

關於這項工作

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

步驟

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

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

會傳回登出URL：

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

2. 儲存登出URL。

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

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

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

會傳回302回應。重新導向位置不適用於純API登出。

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

4. 刪除StorageGRID 不記名權杖。

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

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

`204 No Content`回應表示使用者現在已登出。

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

使用 **API** 停用 **StorageGRID** 功能

您可以使用Grid Management API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。透過在 Grid Manager （ UI 和 API ）中完全停用 * 變更租戶根密碼 * 功能、 A 公司可確保管理員使用者（包括 root 使用者和擁有 * 根存取 * 權限的群組使用者）無法變更任何租戶帳戶根使用者的密碼。 _

步驟

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

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

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

重新啟動停用的功能

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

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

步驟

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

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

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

上一個範例會重新啟動_all_停用的功能。如果停用其他應保持停用狀態的功能、您必須在PUT要求中明確指定這些功能。例如、若要重新啟動變更租戶根密碼功能、並繼續停用 storageAdmin 管理權限、請傳送此 PUT 要求：

```
{ "grid": {"storageAdmin": true} }
```

控制StorageGRID 對功能的存取

控制StorageGRID 功能存取

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

控制對Grid Manager的存取

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

使用"身分識別聯盟"可 "使用者"加快設定"群組"速度、並可讓使用者使用熟悉的認證登入 StorageGRID 。如果您使用Active Directory、OpenLDAP或Oracle Directory Server、則可以設定身分識別聯盟。

如果您想要使用另一項LDAP v3服務、請聯絡技術支援部門。

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

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

啟用單一登入

StorageGRID 系統支援使用安全性斷言標記語言 2.0 （SAML 2.0） 或 OpenID Connect （OIDC） 標準的單一登入 （SSO） 。在您 "設定並啟用 SSO" 之後，所有使用者必須先透過外部身分供應商進行驗證，才能存取

Grid Manager、Tenant Manager、Grid Management API 或 Tenant Management API。本機使用者無法登入 StorageGRID。

變更資源配置複雜密碼

許多安裝和維護過程以及下載StorageGRID恢復包都需要設定密碼。下載StorageGRID系統的網格拓樸資訊和加密金鑰的備份也需要密碼。你可以"變更複雜密碼"按要求。

變更節點主控台密碼

網格中的每個節點都有一個節點控制台密碼，您需要使用 SSH 以「管理員」身分登入節點，或以 VM/實體控制台連線上的 root 使用者身分登入。根據需要，您可以"變更節點主控台密碼"對於每個節點。

使用多管理員驗證

您可以使用多重管理員驗證 (MAV) 來確保某些 StorageGRID 操作只能在指定管理員核准後才能執行。MAV 可防止遭入侵、惡意或經驗不足的管理員進行不必要的變更或刪除資料。

更改 **StorageGRID** 佈建通關密碼

使用此程序更改StorageGRID配置密碼。恢復、擴充和維護過程都需要密碼。下載恢復包備份也需要密碼，其中包括網格拓撲資訊、網格節點控制台密碼和StorageGRID系統的加密金鑰。

開始之前

- 您已使用登入 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

許多安裝和維護過程都需要配置密碼，並且"下載恢復包"。配置密碼未在 `Passwords.txt`文件。確保記錄配置密碼並將其保存在安全的地方。

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在 * 變更資源配置密碼 * 下、選取 * 進行變更 *
3. 輸入您目前的資源配置通關密碼。
4. 輸入新的通關密碼。通關密碼必須包含至少8個字元、且不得超過32個字元。密碼區分大小寫。

   將配置密碼儲存在安全的位置。它是安裝、擴充和維護過程所必需的。

5. 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。

6. 選擇*恢復套件*。
7. 輸入新的設定密碼來下載新的復原包。

更改配置密碼後，您必須立即下載新的恢復包。如果發生故障，恢復包檔案可讓您恢復系統。

在 StorageGRID 中變更節點主控台密碼

網格中的每個節點都有一個節點控制台密碼，您可以使用該密碼登入該節點。預設情況下，每個節點都有一個唯一的密碼。您可以將每個密碼變更為新的唯一密碼，也可以將每個節點的密碼變更為使用全域密碼。密碼儲存在恢復包中。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"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

您可以使用節點控制台密碼透過 SSH 以「管理員」身分登入節點，或透過 VM/實體控制台連線以 root 使用者身分登入。您可以使用下列選項之一變更節點控制台密碼：

- 自動對每個節點應用隨機密碼
- 指定一個全域密碼並將其應用於所有節點
- 指定並將唯一密碼套用至一個或多個節點

密碼儲存在更新的 `Passwords.txt`恢復包中的檔案。密碼列在檔案的密碼列中。

這"SSH 訪問密碼"用於節點間通訊的 SSH 金鑰與節點控制台密碼是分開的。此程序不會變更 SSH 存取密碼。

存取精靈

步驟

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

下載目前的恢復套件

在變更節點控制台密碼之前，請下載目前的復原包。如果任何節點的密碼變更過程失敗，您可以使用此檔案中的密碼。

步驟

1. 輸入您網格的資源配置密碼。
2. 選擇*下載恢復套件*。
3. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的位置。

復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 選擇*繼續*。

提供新密碼

1. 選擇您想要使用的密碼變更方法。
   - 自動： StorageGRID會自動為所有節點指派一個新的隨機控制台密碼。
   - 自訂：您提供控制台密碼。

自動的

1. 選擇*繼續*。

自訂

1. 選取下列其中一項：
   - 全域控制台密碼：對所有節點套用相同的控制台密碼。
   - 唯一的控制台密碼：在一個或多個節點上套用不同的密碼。
2. 如果您選擇了*全域控制台密碼*，請輸入您想要用於所有節點的密碼。
3. 如果選擇了“唯一控制台密碼”，請為一個或多個節點輸入唯一密碼。
4. 選擇*繼續*。

完成密碼修改

1. 當確認對話方塊出現時，如果您準備好讓StorageGRID開始變更節點控制台密碼，請選擇 是。

   您無法在程序啟動後取消此程序。

   StorageGRID產生一個包含新密碼的新復原包。

2. 當新的恢復包準備好後，選擇*下載新的恢復包*並保存恢復包。
3. 開啟 `.zip`檔案。
4. 確認您可以存取包含新節點主控台密碼的內容、包括 `Passwords.txt`檔案。
5. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

   不要覆蓋舊的恢復包。

   您必須保護復原文件，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

6. 選取核取方塊表示您已下載新的復原套件並驗證了內容。
7. 選擇*繼續*。

   StorageGRID更新每個節點的密碼。

如果更新過程中出現錯誤，進度條會列出密碼變更失敗的節點數。系統將自動在密碼變更失敗的任何節點上重試該過程。如果該過程結束時某些節點仍未更改密碼，則會出現「重試」按鈕。

8. 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。

9. 當進度條顯示沒有剩餘更新時，選擇*完成*。
10. 更改所有節點的節點控制台密碼後，刪除您下載的第一個復原包。

變更 **StorageGRID** 管理節點的 **SSH** 存取密碼

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

使用 SSH 金鑰、以 VM 或實體主控台連線上的 root 使用者身分或登入節點 `admin`。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"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

管理節點的新存取密碼和每個節點的新內部金鑰儲存在 `Passwords.txt`恢復包中的檔案。密鑰列在該文件中的密碼列中。

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

存取精靈

步驟

1. 選擇*設定* > 存取控制 > 電網密碼。
2. 在 * 變更 SSH 金鑰 * 下、選取 * 進行變更 * 。

下載目前的恢復套件

在變更 SSH 存取金鑰之前，請下載目前的復原包。如果任何節點的金鑰變更過程失敗，您可以使用此文件中的金鑰。

步驟

1. 輸入您網格的資源配置密碼。
2. 選擇*下載恢復套件*。

3. 複製復原包文件(`.zip`）到兩個安全、可靠且獨立的位置。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 選擇*繼續*。
5. 當確認對話方塊出現時、如果您已準備好開始變更 SSH 存取金鑰、請選取 * 是 * 。

   您無法在程序啟動後取消此程序。

變更 **SSH** 存取金鑰

當變更 SSH 存取金鑰程序開始時，將產生一個包含新金鑰的新復原包。然後，在每個節點上更新金鑰。

步驟

1. 等待新的恢復包生成，這可能需要幾分鐘。
2. 當「下載新的復原包」按鈕啟用時，選擇「下載新的復原包」並儲存新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。
3. 下載完成時：

   a. 開啟 `.zip`檔案。

   b. 確認您可以存取包含新 SSH 存取金鑰的內容、包括 `Passwords.txt`檔案。

   c. 複製新的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

      不要覆蓋舊的恢復包。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

4. 等待每個節點上的金鑰更新、可能需要幾分鐘的時間。

   如果所有節點的金鑰都已變更、就會出現綠色成功橫幅。

   如果在更新過程中發生錯誤、橫幅訊息會列出無法變更其金鑰的節點數。系統會在任何無法變更其金鑰的節點上、自動重試該程序。如果程序結束時、有些節點仍沒有變更金鑰、則會出現 * 重試 * 按鈕。

   如果一個或多個節點的金鑰更新失敗：

   a. 檢閱表中所列的錯誤訊息。

   b. 解決問題。

   c. 選擇*重試*。

      重試只會變更先前金鑰變更嘗試失敗的節點上的 SSH 存取金鑰。

5. 在所有節點的 SSH 存取金鑰變更後，刪除您下載的第一個復原包。
6. 或者，選擇「維護」>「系統」>「復原包」下載新復原包的附加副本。

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

如果您希望在另一個系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server ）中管理管理群組和用戶，則可以在網格管理器中設定身份聯合。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 你已經"特定存取權限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作為身分識別提供者。

  如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

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

關於這項工作

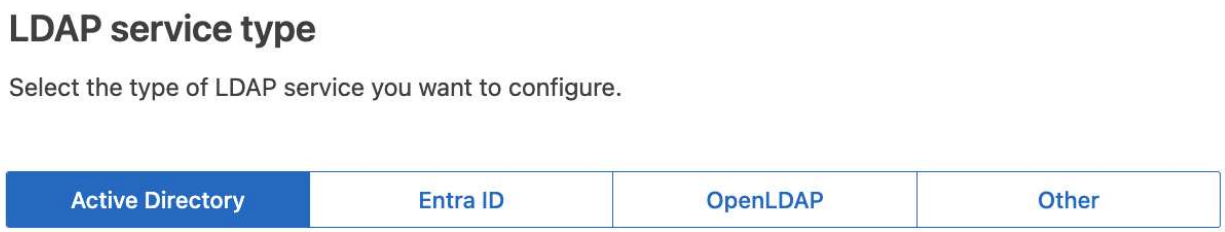
如果您想要從其他系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）匯入群組，則可以為網格管理員設定身分識別來源。您可以匯入以下類型的群組：

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

輸入組態

步驟

1. 選擇*配置* > 存取控制 > 身份聯合。
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：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName`對於 `Active Directory` 和 `uid`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `uid`。
   - 使用者 **UUID**：包含 LDAP 使用者的永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID`對於 `Active Directory` 和 `entryUUID`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `nsuniqueid`。每個使用者的指定屬性值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
   - 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性的名稱。此屬性相當於 `sAMAccountName`對於 `Active Directory` 和 `cn`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `cn`。
   - 群組 **UUID**：包含 LDAP 群組的永久唯一識別碼的屬性的名稱。此屬性相當於 `objectGUID`對於 `Active Directory` 和 `entryUUID`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `nsuniqueid`。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
5. 對於所有LDAP服務類型、請在「設定LDAP伺服器」區段中輸入所需的LDAP伺服器和網路連線資訊。
   - 主機名稱：LDAP伺服器的完整網域名稱（FQDN）或IP位址。
   - 連接埠：用於連接LDAP伺服器的連接埠。

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

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

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

     指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

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

`userPrincipalName

- 入口 **ID**: `accountEnabled`和 `userPrincipalName`

- 密碼：與使用者名稱相關的密碼。

> 如果您在未來變更密碼、您必須在此頁面上更新密碼。

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

> 「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

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

> *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

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

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

  輸入下列其中一種模式：

  - **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
  - 下級登入名稱模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
  - * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    請準確附上所寫的*（使用者名稱）*。

6. 在傳輸層安全性（TLS）區段中、選取安全性設定。
   - 使用 **STARTTLS**：使用 STARTTLS 確保與 LDAP 伺服器的通訊安全。這是 Active Directory 、OpenLDAP 或其他的建議選項，但 Microsoft Entra ID 不支援此選項。
   - 使用 **LDAPS**：LDAPS（透過 SSL 的 LDAP）選項使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Microsoft Entra ID 選擇此選項。
   - 請勿使用 **TLS**： StorageGRID系統和 LDAP 伺服器之間的網路流量將不安全。 Microsoft Entra ID 不支援此選項。

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

7. 如果您選取了ARTTLS或LDAPS、請選擇用來保護連線安全的憑證。
   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設Grid CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂安全性憑證。

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

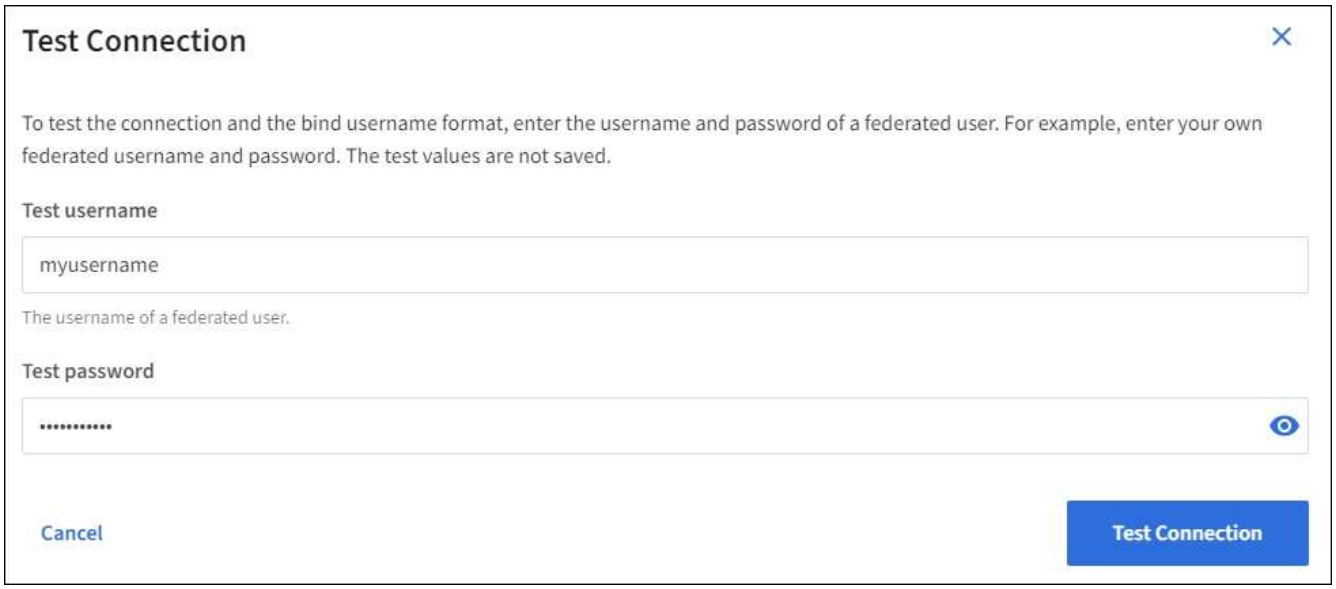
測試連線並儲存組態

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

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
   - 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定無效、就會出現「無法建立測試連線」訊息。選擇*關閉*。然後、解決所有問題、並再次測試連線。
3. 如果您提供連結使用者名稱格式、請輸入有效同盟使用者的使用者名稱和密碼。

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



   - 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定、連結使用者名稱格式或測試使用者名稱和密碼無效、則會出現錯誤訊息。解決所有問題、然後再次測試連線。

強制與身分識別來源同步

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

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

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

停用身分識別聯盟

您可以暫時或永久停用群組和使用者的身份聯合。當身分聯合被停用時， StorageGRID和身分來源之間就沒有通訊。但是，您配置的任何設定都會保留，以便您將來可以輕鬆地重新啟用身份聯合。

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。
- StorageGRID系統和身分來源之間不會發生同步，並且不會對尚未同步的帳戶發出警報。
- 如果單一登入 (SSO) 狀態為 已啟用 或 沙盒模式，則 啟用身分聯合 核取方塊將會停用。在停用身分聯合之前，單一登入頁面上的 SSO 狀態必須為 已停用。看"停用單一登入" 。

步驟

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

設定**OpenLDAP**伺服器的準則

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

對於非 Active Directory 或 Microsoft Entra ID 的識別來源， StorageGRID不會自動阻止外部停用的使用者存取 S3。若要封鎖 S3 訪問，請刪除使用者的所有 S3 金鑰或從所有群組中刪除該使用者。

memberOf和**refert**覆疊

應啟用memberof和refert覆疊。如需詳細資訊，請參閱中的反向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。

請參閱中有關反向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"^]。

相關資訊

"用於外部通訊的連接埠"

管理 StorageGRID 中的管理員群組

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

開始之前

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

建立管理群組

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

存取精靈

步驟

1. 選擇*設定* > 存取控制 > 管理群組。
2. 選取*建立群組*。

選擇群組類型

您可以建立本機群組或匯入同盟群組。

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

本機群組

步驟

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

聯盟群組

步驟

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

管理群組權限

步驟

1. 若為*存取模式*、請選取群組中的使用者是否可以在Grid Manager和Grid Management API中變更設定及執行作業、或是只能檢視設定和功能。
   - 讀寫（預設）：使用者可以變更設定、並執行其管理權限所允許的作業。
   - 唯讀：使用者只能檢視設定和功能。他們無法在 Grid Manager 或 Grid Management API 中進行任何變更或執行任何作業。本機唯讀使用者可以變更自己的密碼。

   > ⓘ 如果使用者屬於多個群組、且任何群組設定為*唯讀*、則使用者將擁有所有選取設定和功能的唯讀存取權。

2. 選擇一個或多個"管理群組權限"。

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

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

新增使用者（僅限本機群組）

步驟

1. 您也可以為此群組選取一或多個本機使用者。

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

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. 選擇編輯圖示 。 c. 輸入新名稱。 d. 選取*儲存變更*。
編輯存取模式或權限	a. 選取群組的核取方塊。 b. 選取*「動作*」>*「檢視群組詳細資料*」。 c. 或者、變更群組的存取模式。 d. （可選）選擇或清除"管理群組權限"。 e. 選取*儲存變更*。	a. 選取群組名稱以顯示詳細資料。 b. 或者、變更群組的存取模式。 c. （可選）選擇或清除"管理群組權限"。 d. 選取*儲存變更*。

複製群組

步驟

1. 選取群組的核取方塊。
2. 選取*「動作*」>*「重複群組*」。
3. 完成「複製群組」精靈。

刪除群組

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

步驟

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

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
- 檢視目前和已解決的警示
- 變更自己的密碼（僅限本機使用者）
- 檢視「組態與維護」頁面上提供的特定資訊

權限與存取模式之間的互動

對於所有權限、群組的「存取模式」設定會決定使用者是否可以變更設定及執行作業、或是只能檢視相關的設定與功能。如果使用者屬於多個群組、且任何群組設定為*唯讀*、則使用者將擁有所有選取設定和功能的唯讀存取權。

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

root存取權

此權限可讓您存取所有網格管理功能。

變更租戶根密碼

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

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

ILM

此權限可讓您存取下列* ILM *功能表選項：

- 規則
- 原則
- 原則標籤
- 儲存資源池
- 儲存等級

- 區域
- 物件中繼資料查詢

使用者必須具有*其他網格配置*權限才能管理儲存等級。

維護

使用者必須擁有維護權限、才能使用下列選項：

- 組態 > 存取控制
  - 網格密碼
- 組態 > 網路
  - S3 端點網域名稱
- 維護 > 任務
  - 取消委任
  - 擴充
  - 物件存在檢查
  - 恢復
- 維護 > 系統
  - 恢復套件
  - 軟體更新
- 支援 > 工具
  - 記錄

沒有維護權限的使用者可以檢視但無法編輯這些頁面：

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

管理警示

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

度量查詢

此權限可讓您存取：

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

物件中繼資料查詢

此權限可讓您存取「* ILM >*物件中繼資料查詢」頁面。

其他網格組態

此權限提供對這些附加網格配置選項的存取：

- **ILM**
  - 儲存等級
- 組態 > 系統
- 支援 > 其他
  - I/O 優先權
  - 節點服務
  - 儲存設備浮水印

鏈路成本需要 Root 存取。

儲存應用裝置管理員

此權限提供：

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

租戶帳戶

此權限可讓您：

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

在 StorageGRID 中管理使用者

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

開始之前

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

建立本機使用者

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

您只能建立本機使用者。使用外部身分識別來源來管理同盟使用者和群組。

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

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

存取精靈

步驟

1. 選擇*配置* > 存取控制 > 管理員使用者。
2. 選取*建立使用者*。

輸入使用者認證資料

步驟

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

指派給群組

步驟

1. 或者、將使用者指派給一或多個群組、以決定使用者的權限。

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

   如果使用者屬於多個群組、則權限會累計。如需詳細資訊、請參閱 "管理管理群組" 。

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。
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. 選擇編輯圖示 。 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*。

工作	「行動」功能表	詳細資料頁面
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*。

導入聯合用戶

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

步驟

1. 選擇*配置* > 存取控制 > 管理員使用者。
2. 選擇*導入聯合用戶*。
3. 輸入一個或多個聯合使用者的 UUID 或使用者名稱。

   對於多個條目，請在新行上新增每個 UUID 或使用者名稱。

4. 選擇*導入*。

   如果將一個或多個使用者匯入「使用者」欄位失敗，請執行下列步驟：

   a. 展開*未匯入的使用者*並選擇*複製使用者*。
   b. 透過選擇「上一個」並將複製的使用者貼上到「匯入聯合使用者」對話方塊中，重新嘗試匯入。

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

複製使用者

您可以複製現有使用者、以建立具有相同權限的新使用者。

步驟

1. 選取使用者的核取方塊。
2. 選取*「動作*」>*「重複使用者*」。
3. 完成複製使用者精靈。

刪除使用者

您可以刪除本機使用者、將該使用者從系統中永久移除。

您無法刪除 root 使用者。

步驟

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

使用單一登入（SSO）

了解 StorageGRID 單一登入

啟用單一登入 (SSO) 後，只有使用貴組織實作的 SSO 登入流程授權使用者的憑證後，使用者才可以存取網格管理員、租用戶管理器、網格管理 API 或租用戶管理 API。本機使用者無法登入StorageGRID。

StorageGRID 系統支援使用安全性斷言標記語言 2.0 （SAML 2.0） 標準或 OpenID Connect 的單一登入（SSO）。

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

   - 如果這是您第一次透過此瀏覽器存取該 URL，系統會提示您輸入帳戶 ID。
   - 如果您之前曾造訪過網格管理器或租用戶管理器，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 位址後面的）時、不會顯示「StorageGRID 登入」頁面 `/?accountId=20-digit-account-id`。而是會立即將您重新導向至組織的 SSO 登入頁面使用SSO認證登入、您可以在其中進行。

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

   可將您重新導向至組織的SSO登入頁面。StorageGRID例如：

4. [[signin_SSO]使用您的SSO認證登入。

如果SSO認證資料正確：

a. 身分識別供應商（IDP）提供驗證回應StorageGRID 功能以回應功能。

b. 驗證驗證回應。StorageGRID

c. 如果回應有效、且您屬於具有StorageGRID 下列存取權限的聯盟群組、您將會登入Grid Manager或租戶管理程式、視您選取的帳戶而定。

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

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

   您不需要重新輸入 SSO 認證。

啟用**SSO**時登出

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

步驟

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

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

> 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。

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 *注意：*如果您使用 Entra ID 進行 SSO，則可能需要幾分鐘才能退出所有管理節點。
一或多個管理節點上的租戶管理程式	任何管理節點上的租戶管理程式	所有管理節點上的租戶管理程式
Grid Manager與租戶管理程式	網格管理程式	僅限Grid Manager。您也必須登出租戶管理程式、才能登出SSO。

StorageGRID 單一登入的要求和注意事項

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

身分識別供應商要求

StorageGRID 支援多個 SSO 身分提供者 (IdP)。

OIDC

以下 SSO IdPs 支援 OpenID Connect (OIDC)：

- Active Directory Federation Service（AD FS）
- 微軟Entra ID
- Keycloak
- PingFedate
- Okta

SAML

以下 SSO IdPs 支援安全性聲明標記語言 2.0 （SAML 2.0）：

- Active Directory Federation Service（AD FS）
- 微軟Entra ID
- 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 • Keycloak • Okta • 進入 ID • PingFedate
進入 ID	進入 ID

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 應使用 "KB3201845更新"、或更新版本。

其他需求

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

Entra ID 的注意事項

如果您使用 Entra ID 作為 SSO 類型，且使用者的使用者主體名稱不使用 sAMAccountName 作為前綴，則當StorageGRID與 LDAP 伺服器失去連線時，可能會發生登入問題。若要允許使用者登入，您必須恢復與 LDAP 伺服器的連線。

伺服器憑證需求

預設情況下， StorageGRID在每個管理節點上使用管理介面憑證來保護對網格管理器、租用戶管理員、網格管理 API 和租用戶管理 API 的存取。為StorageGRID設定信賴方信任 (AD FS)、企業應用程式 (Entra ID) 或服務供應商連線 (PingFederate) 時，您可以使用伺服器憑證作為StorageGRID要求的簽章憑證。

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

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

您可以登入節點的命令 Shell 並前往目錄、以存取管理節點的伺服器憑證 `/var/local/mgmt-api`。自訂伺服器憑證的名稱為 `custom-server.crt`。節點的預設伺服器憑證命名為 `server.crt`。

連接埠需求

單一登入（SSO）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。請參閱。 "控制外部防火牆的存取"

確認聯合使用者可以登入 **StorageGRID**

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

開始之前

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

步驟

1. 如果有現有的租戶帳戶、請確認沒有租戶使用自己的身分識別來源。

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

a. 登入每個租戶帳戶的租戶管理程式。
b. 選擇*存取管理* > 身分聯合。
c. 確認未選取 * 啟用身分識別聯盟 * 核取方塊。
d. 如果是、請確認不再需要此租戶帳戶使用的任何聯盟群組、清除核取方塊、然後選取 * 儲存 * 。

2. 確認聯盟使用者可以存取Grid Manager：
   a. 從網格管理員中，選擇*配置* > 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. 從網格管理員中，選擇*租戶*。
   b. 選取租戶帳戶、然後選取*「Actions」（動作）>「Edit」（編輯）*。
   c. 在Enter details（輸入詳細資料）選項卡上、選取* Continue（繼續）*。
   d. 如果選中 * 使用自己的身份來源 * 複選框，則取消選中該複選框並選擇 * 保存 * 。

      隨即顯示「租戶」頁面。

   e. 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。
   f. 從租用戶管理員中，選擇*存取管理*>*群組*。
   g. 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。
   h. 登出。
   i. 確認您可以以同盟群組中的使用者身分重新登入租戶。

相關資訊

- "單一登入的要求與考量"
- "管理管理群組"
- "使用租戶帳戶"

使用 **OIDC** 設定 **SSO**

了解如何使用 **OIDC** 在 **StorageGRID** 中設定 **SSO**

在 StorageGRID 中設定單一登入 （SSO） 可讓 StorageGRID （服務供應商）和 SSO 身分供應商安全地就使用者身分驗證請求進行通訊。

您可以使用 OpenID Connect (OIDC) 或 SAML 在 StorageGRID 中設定 SSO。請依照以下高階步驟使用 OIDC 在 StorageGRID 中設定 SSO，或了解 "使用 SAML 設定 SSO"。

1 設定身分識別供應商

根據您計劃使用的 SSO 身分供應商，您可以選擇 Active Directory 或 Entra ID 作為身分聯合 LDAP 服務類型。

- 對於 Active Directory Federation Service (AD FS)，您可以使用 AD FS、Entra ID、Keycloak、Okta 或 PingFederate 身分供應商。
- 對於 Entra ID，您只能使用 Entra ID 身分供應商。

使用 SSO 身分供應商的軟體為網格中的每個管理節點設定 OIDC。

- 了解 Active Directory 中的 "為每個管理節點建立一個應用程式群組"
- 了解 "為每個管理節點建立一個應用程式" 在 Entra ID 中的資訊
- 了解 Keycloak 中的 "為每個管理節點建立一個用戶端"
- 瞭解 "為每個管理節點建立一個 Okta 應用程式"
- 了解 "為每個管理節點建立服務供應商連線" 在 PingFederate 中的相關資訊

2 設定 **SSO**

選擇 OIDC 的「設定 SSO」精靈。然後，使用您的身分識別供應商設定 SSO，並進入沙盒模式以設定和測試 SSO，再為 StorageGRID 使用者啟用此功能。

瞭解 "使用 OIDC 設定 SSO"

3 啟用 **SSO**

確認可以使用 SSO 登入每個管理節點後，為所有 StorageGRID 使用者啟用 SSO。

瞭解 "為 StorageGRID 使用者啟用 SSO"

在 **AD FS** 中為 **StorageGRID** 中的 **OIDC** 建立應用程式群組

您必須使用 Active Directory Federation Services （AD FS） 為系統中每個 OpenID Connect （OIDC） 管理節點建立一個應用程式群組。

開始之前

- 您擁有系統中每個管理節點的完整網域名稱（或 IP 位址）和信賴方識別碼。

> StorageGRID 系統中的每個管理節點都必須擁有一個應用程式群組。這可確保使用者可以安全地登入和登出任何管理節點。您可以為所有管理節點建立單一應用程式群組（建議），也可以為每個管理節點建立一個不同的應用程式群組。

- 您有在 AD FS 中建立應用程式群組的經驗，或者您可以存取 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。

關於這項工作

這些說明適用於 Windows Server 2022 AD FS。如果您使用的是其他版本的 AD FS，您會發現操作步驟略有不同。如有疑問，請參閱 Microsoft AD FS 文件。

步驟 **1**：建立應用程式群組

您可以使用 Windows PowerShell 快速建立應用程式群組。

步驟

1. 從Windows Server Manager中、選取* Tools **>** AD FS Management *。
2. 選擇 **Application Groups** > **Add Application Group**
3. 對於 **Name**，請輸入信賴方識別碼。
4. 在「範本」下，選擇「用戶端-伺服器應用程式」>「存取 Web API 的伺服器應用程式」。
5. 選擇*下一步*。
6. 記錄 **Client Identifier** 值。
7. 在 **Redirect URI** 下，輸入管理節點的 FQDN （或 IP 位址） `callback` 和 `logged-out` URI：
   - `https://<FQDN>/api/v4/oidc-callback` 或 `https://<IP_address>/api/v4/oidc-callback`
   - `https://<FQDN>/api/v4/oidc-logged-out` 或 `https://<IP_address>/api/v4/oidc-logged-out`

   如果您對所有管理節點使用同一個應用程式群組，請輸入每個管理節點的 URI。如果您為每個管理節點使用不同的應用程式群組，則只需輸入對應管理節點的 URI。
8. 選取*「Add*」。
9. 選擇 **Generate a shared secret**，記錄 **Secret** 的值，然後選擇 **Next**。
10. 請輸入 **Identifier** 的用戶端識別碼。
11. 選擇 新增，然後選擇 下一步。
12. 選擇 **Permit everyone**。
13. 請確認已在「用戶端應用程式（呼叫方）」下選擇伺服器應用程式。
14. 在「允許的範圍」下，確認僅選取以下選項：
    - allatclaims
    - 電子郵件
    - openid
    - 設定檔
15. 選擇 下一步 > 下一步。
16. 選取 **Close** 。

步驟 **2**：設定簽發轉換規則

為每個應用程式群組設定發行轉換規則。

步驟

1. 在「AD FS 管理」頁面中，以滑鼠右鍵按一下應用程式群組，然後選取「內容」。
2. 選擇先前建立的 Web API，然後選擇「編輯」。

3. 選擇 **Issuance Transform Rules** > **Add Rule ……**。
4. 在 **Claim rule template:** 下，選擇 **Send LDAP Attribute as Claims**。
5. 選擇*下一步*。
6. 輸入聲明規則名稱。
7. 選擇 **Active Directory** 作為屬性儲存區。
8. 將 LDAP 屬性映射新增至傳出聲明類型：
   - `E-Mail Addresses - E-Mail Address`
   - `Token-Groups - Unqualified Names - Group`
9. 選擇*完成*。
10. 選擇 **Apply** > **OK** > **OK**。

接下來

建立應用程式群組之後，"使用 OIDC 設定 SSO"。

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

使用 Entra ID 為系統中每個 Admin Node 建立 OpenID Connect (OIDC) 的企業應用程式。

開始之前

- 您的系統中每個管理節點都有信賴方識別碼和完整網域名稱 (FQDN) 或 IP 位址。

> StorageGRID 系統中的每個管理節點都必須配備企業應用程式。這可確保使用者可以安全地登入和登出任何管理節點。您可以為所有管理節點建立單一企業應用程式（建議），也可以為每個管理節點建立一個不同的企業應用程式。

- 您有在 Entra ID 中建立應用程式的經驗。
- 您有一個具有有效訂閱的 Entra ID 帳戶。
- 您在 Entra ID 帳戶中擁有以下角色之一：全域管理員、雲端應用程式管理員、應用程式管理員或服務主體的擁有者。

步驟 **1**：存取 **Entra ID**

步驟

1. 登入 "Azure Portal"。
2. 選擇 "微軟Entra ID"。
3. 選擇 "應用程式註冊"。

步驟 **2**：註冊新應用程式

為系統中的每個管理節點註冊一個新的企業應用程式。

步驟

1. 在 Entra ID Enterprise 應用程式窗格中，選取「應用程式註冊」>「新增註冊」。
2. 對於 **Name**，請輸入信賴方識別碼。
3. 在「支援的帳戶類型」下，選擇可以使用該應用程式或存取 API 的帳戶類型，例如「僅限單一租戶 - <tenant_name>」。
4. 在「重新導向 URI」下，選取「選取平台」>「Web」。
5. 輸入管理節點的 FQDN（或 IP 位址）重新導向 URI： `https://<FQDN>/api/v4/oidc-callback` 或 `https://<IP_address>/api/v4/oidc-callback`

   如果您所有管理節點都使用同一個企業應用程式，請輸入每個管理節點的 URI。如果您每個管理節點使用不同的企業應用程式，則只需輸入對應管理節點的 URI。

6. 選擇 **Register**。
7. 在新應用程式註冊的「概覽」頁面上，記錄 **Application （client） ID** 和 **Directory （tenant） ID**。

步驟 **3**：設定用戶端密鑰

為每個新應用程式註冊一個用戶端密鑰。

步驟

1. 在新應用程式註冊的「概觀」頁面上，選取 管理 > 憑證和密碼 > 新用戶端密碼。
2. 輸入用戶端密鑰並設定所需的過期日期。
3. 選擇 **Add** 以建立用戶端密鑰。
4. 複製密鑰*值*。

   重新整理頁面或離開用戶端金鑰頁面後，金鑰值將不可見。

步驟 **4**：設定 **API** 權限

為每個新應用程式設定 API 權限。

步驟

1. 在新應用程式註冊的「概覽」頁面上，選擇 **Manage** > **API permissions** > **Add a permission**。
2. 選擇 **Microsoft APIs** > **Microsoft Graph** > **Delegated permissions**。
3. 展開 **OpenId** 權限，然後選擇 **email**、**offline_access**、**openid** 和 **profile**。
4. 選擇 新增權限。
5. 選取 授予管理員同意 **<tenant>**，然後選取 是。

步驟 **5**：新增登出重新導向 **URI**

為每個新應用程式新增登出重新導向 URI。

步驟

1. 在新應用程式註冊的「概覽」頁面上，選取 **Manage** > **Authentication**。

2. 選擇 **Add Redirect URI** > **Web**。
3. 輸入管理節點的 FQDN （或 IP 位址）重新導向 URI： `https://<FQDN>/api/v4/oidc-logged-out` 或 `https://<IP_address>/api/v4/oidc-logged-out`

   如果您對所有管理節點使用同一個應用程式群組，請輸入每個管理節點的 URI。如果您為每個管理節點使用不同的應用程式群組，則只需輸入對應管理節點的 URI。

4. 選擇 **Configure**。

接下來

建立企業應用程式之後，"使用 OIDC 設定 SSO"。

在 **Keycloak** 中為 **StorageGRID** 中的 **OIDC** 建立用戶端

使用 Keycloak 為 StorageGRID 系統中的每個管理節點建立 OpenID Connect (OIDC) 用戶端連線。

開始之前

- 您有使用 Keycloak 建立用戶端的經驗，或者您可以存取 Keycloak 文件。
- 您擁有一個專用帳戶（Bind DN），用於目錄查詢和登入憑證。
- 您擁有 Keycloak 管理員存取權限。

關於這項工作

StorageGRID 系統中的每個管理節點都必須具有用戶端連線。這可確保使用者可以安全地登入和登出任何管理節點。您可以為所有管理節點建立單一用戶端連線（建議），也可以為每個管理節點建立一個不同的用戶端連線。

除非另有說明，否則請使用預設設定。在某些情況下，您可以使用組織要求的設定。

步驟 **1**：（可選）建立領域

建立 Keycloak 域以設定 LDAP 供應商和 OIDC 用戶端，或使用 Keycloak 預設域。

步驟

1. 選取 **Create Realm**。
2. 請輸入領域名稱。
3. 選取 **Enabled**。
4. 選擇* Create （建立）。

步驟 **2**：設定 **LDAP** 供應商

設定 LDAP 供應商，使 Keycloak 連接到 Active Directory 聯合驗證服務 (AD FS) LDAP 伺服器。

步驟

1. 選擇「使用者聯合」>「新增 LDAP 提供者」。
2. 在「設定」標籤下：

a. 請輸入以下建議值：

- UI 顯示名稱：輸入唯一值。
- 供應商：**Active Directory**
- 連結 URL： `ldap://<ldap_IP_address>` 或 `ldaps://<ldap_IP_address>`
- 連線池：**ON**
- 繫結 DN：輸入您的繫結 DN
- 繫結憑證：輸入密碼
- 編輯模式：**READ_ONLY**
- 使用者 DN：例如， `CN=Users， DC=saml， DC=sgws`
- 使用者名稱 LDAP 屬性：**sAMAccountName**
- RDN LDAP 屬性：**cn**
- UUID LDAP 屬性：**objectGUID**
- 使用者物件類別： `person，organizationalPerson，user`
- 使用者 LDAP 過濾器： `(sAMAccountName=*)`
- 搜尋範圍：子樹
- 分頁：**ON**
- 導入使用者：**ON**
- 同步註冊：**ON**
- 搜尋過程中移除無效使用者：**ON**

b. 選擇 **Test connection** 和 **Test authentication**。

請先解決可能出現的任何問題，然後再繼續。

3. 選擇*保存*。

步驟 **3**：設定 **LDAP** 映射

設定 LDAP 對應，將 AD 作為屬性對應至 Keycloak。

步驟

1. 前往 **User federation** > **LDAP**
2. 選擇您建立的LDAP 供應商。
3. 在「映射器」標籤上，選擇 **Add mapper** > **Create new mapper**。
4. 對於 Mapper Type，選擇 **user-attribute-ldap-mapper**。
5. 選擇 **Save**，然後輸入以下資訊：
   - 使用者模型屬性：**userPrincipalName**
   - LDAP 屬性：**userPrincipalName**
   - 唯讀：**ON**

- 始終從 LDAP 讀取值：**ON**
- LDAP 中是否必填：**OFF**
- 強制設定預設值：**ON**
- 二進位屬性：**OFF**

6. 選擇*保存*。

步驟 **4**：建立 **OIDC** 用戶端

為您的系統建立 OIDC 用戶端。

步驟

1. 前往 **Clients** > **Create client**。
2. 在「一般設定」中，輸入以下資訊：
   - 名稱：輸入用戶端的顯示名稱。
   - 用戶端類型：**OIDC Connect**
   - 用戶端 ID：請輸入唯一值。儲存此值以備後用。
3. 選擇*下一步*。
4. 在 Capability 組態中，輸入以下資訊：
   - 用戶端驗證：**ON**
   - 標準流程：啟用
   - 直接存取權限：啟用
   - 服務帳戶角色：啟用
5. 選擇*下一步*。
6. 在登入設定中，輸入重新導向 URI：

> 如果為管理介面設定了一個或多個負載平衡器端點，請為每個連接埠新增重新導向 URI。例如： `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` 和 `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

   - 有效的重新導向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback` 和 `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
   - 有效的登出後重新導向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
   - Web 來源: `https://<Admin_IP_address_or_FQDN>`
7. 選擇*保存*。

步驟 **5**：產生用戶端密鑰

為建立的 OIDC 用戶端產生用戶端金鑰。

步驟

1. 前往 用戶端，然後選擇您建立的 OIDC 用戶端。
2. 在「憑證」標籤上，輸入以下資訊：
   - 用戶端驗證者：用戶端 **ID** 和金鑰
   - 用戶端密碼：產生或設定用戶端密碼。儲存此值以供後續使用。

步驟 **6**：定義範圍

在 Keycloak 中定義作用域。

步驟

1. 前往 **Client scopes** > **Create client scope**，然後輸入以下資訊：
   - 類型：無
   - 協定：**OpenID Connect**
   - 在同意畫面上顯示：已啟用
   - 包含在 OpenID 提供者元資料中：已啟用
2. 選擇*保存*。
3. 在 Mappers 索引標籤上，選取 **Configure a new mapper** > **User Attribute**，然後輸入下列資訊：
   - 名稱：請輸入唯一值。
   - 使用者屬性：**userPrincipalName**
   - 令牌宣告名稱：**upn**
   - 聲明 JSON 類型：字串
   - 新增至 ID 令牌：**ON**
   - 新增至存取權杖：**ON**
   - 新增至使用者資訊：**ON**
   - 新增至令牌內省：**ON**
4. 選擇*保存*。
5. 前往 **Clients** 並選擇您建立的 OIDC 用戶端。
6. 選擇 **Client Scopes** > **Add client scope**。
7. 選擇您建立的用戶端範圍。
8. 選取*「Add*」。

步驟 **7**：準備使用 **OIDC** 設定 **SSO**

儲存在 StorageGRID 系統中使用 Keycloak 設定 OIDC SSO 所需的資訊。

步驟

1. 檢查您是否已儲存您建立的 OIDC 用戶端中的 用戶端 ID 和 用戶端機密。
2. 儲存領域的 OpenID Connect 探索端點。此端點可在 `well-known`組態端點中找到：

```
https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/.well-known/openid-configuration
```

（可選）包含網路連接埠：

```
https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>/.well-known/openid-configuration
```

接下來

建立 OIDC 用戶端後，"使用 OIDC 設定 SSO"。

在 **StorageGRID** 中為 **OIDC** 建立 **Okta** 應用程式

為 StorageGRID 系統中所有管理節點的 OpenID Connect （OIDC） 建立 Okta 應用程式。

開始之前

- 您有建立 Okta 應用程式的經驗，或者您可以存取 Okta 文件。
- 您擁有 Okta 管理員存取權限。

關於這項工作

Okta 應用程式必須包含所有管理節點的登入和登出重新導向 URI。重新導向 URI 可確保使用者能夠安全地登入和登出任何管理節點。您可以為所有管理節點建立單一 Okta 應用程式（建議），也可以為每個管理節點建立不同的應用程式。

除非另有說明，否則請使用預設設定。在某些情況下，您可以使用組織要求的設定。

步驟 **1**：建立 **Okta** 應用程式

使用 Okta UI 建立 Okta 應用程式。

步驟

1. 在 Okta 中，前往 應用程式 > 應用程式。
2. 選擇 **Create App Integration**，然後輸入以下資訊：
   - 登入方式：**OIDC - OpenID Connect**
   - 應用程式類型：**Web Application**
3. 選擇*下一步*。
4. 在「應用程式整合」欄位中輸入應用程式名稱。
5. 確認核心授權已選取「授權碼」（預設）。
6. 為每個管理節點新增登入和登出重新導向 URI：
   - 登入重新導向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
   - 登出重新導向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`

如果為管理介面設定了一個或多個負載平衡器端點，請為每個連接埠新增重新導向 URI。例如： `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` 和 `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

7. 選擇 **Save**。儲存用戶端 ID 和用戶端金鑰值以備後用。

步驟 **2**：新增聯邦組

為 StorageGRID 建立群組或使用 Active Directory Federation Service （AD FS） 伺服器中的現有群組。

步驟

1. 在 GRID Manager 中，選擇 **Configuration** > **Admin groups** > **Create group** > **Federate Group**。
2. 輸入 AD FS 伺服器群組名稱。
3. 選擇「讀寫」作為存取模式，「Root 存取」作為權限設定。
4. 選取*建立群組*。

步驟 **3**：匯入 **AD FS** 伺服器群組和使用者

在 AD FS 伺服器上安裝 Okta Active Directory 用戶端。然後，匯入 AD FS 伺服器群組和使用者。

步驟

1. 在 Okta 中，前往 **Directory** > **Directory Integrations** > **Add Directory** > **Add Active Directory**。
2. 選擇 **Set Up Active Directory** > **Download Agent**。
3. 立即按照設定流程進行操作。

   如果拖延，設定可能會停滯，您將需要重新開始。

   a. 選擇 Active Directory 網域。
   b. 建立 OktaService 帳戶，而不是連結現有使用者。
   c. 選擇包含使用者的組織單元和包含群組的組織單元。
   d. 選擇使用 AD UPN 作為 Okta 使用者名稱的使用者主體名稱 (UPN)。例如：user@domain.com
4. 搜尋 **Okta AD Agent Management Utility** 應用程式。然後，執行該應用程式並確認狀態訊息 `The agent is running`是否出現。

   當您想要使用 Okta 執行 AD FS 伺服器同步和匯入時，Okta AD 用戶端必須處於運作狀態。

5. 在 Okta 中，前往 **Directory** > **Directory Integrations**。
6. 選擇您建立的目錄整合。
7. 選擇 **Import** > **Import Now**。
8. 選擇要匯入的使用者，然後選擇 **Confirm Assignments**。
9. 前往 **Directory** > **People**，確認使用者已成功匯入。

如果使用者狀態不是「Active」，請選擇 **Activate** ，然後持續重新整理頁面，直到使用者狀態變成「Active」。

10. 前往 **Directory** > **Groups**，確認匯入使用者的群組已自動匯入。
11. 選擇該群組並確認匯入的使用者是否屬於該群組。

步驟 **4**：設定申請

設定一個聲明，將 AD FS 伺服器群組包含在存取權杖中。然後，驗證該聲明是否包含已匯入使用者和 Okta 應用程式的已匯入群組。

步驟

1. 在 Okta 中，前往 **Directory** > **Groups**。
2. 選取匯入使用者的匯入群組。
3. 選擇 應用程式 > 指派應用程式 > 指派。
4. 前往 **Security** > **API**。
5. 選擇*預設*授權伺服器。
6. 選擇 **Claims** > **Add Claim**。然後，使用以下憑證建立聲明：
   - 名稱：群組
   - 包含在權杖類型中：**ID Token - Always**
   - 值類型：**Expression**
   - 值：**Groups.startsWith("active_directory","",100)**
   - 包含範圍：任何範圍
7. 前往 **Security** > **API**。
8. 選擇*預設*授權伺服器。
9. 選取 **Token Preview** 索引標籤，然後輸入以下 Request Properties 的憑證：
   - OAuth/OIDC 用戶端：**<application name>**
   - 授權類型：**Authorization Code**
   - 使用者：匯入使用者（電子郵件地址）
   - 範圍：**email, profile, openid**
10. 選擇*執行*。

    導入的群組出現在有效負載的「預覽 id_token」標籤中。

接下來

建立 Okta 應用程式後，"使用 OIDC 設定 SSO"。

在 **StorageGRID** 中為 **OIDC** 建立 **PingFederate** 服務供應商連接

使用 PingFederate 為系統中每個管理節點建立 OpenID Connect (OIDC) 的服務供應商（SP） 連線。

開始之前

- 您在PingFedate伺服器上建立SP連線的經驗豐富。
- 您擁有 "系統管理員參考指南"PingFederate Server 。PingFedate文件提供詳細的逐步指示和說明。
- 你有"管理員權限"用於 PingFederate 伺服器。

關於這項工作

以下說明概述如何將 PingFederate 伺服器版本 12.1.10 設定為 StorageGRID 的 SSO 供應商。如果您使用的是其他版本的 PingFederate，則可能需要調整這些說明。有關您所用版本的詳細說明，請參閱 PingFederate 伺服器文件。

除非另有說明，否則請使用預設設定。在某些情況下，您可以使用組織要求的設定，例如身分驗證方法設定。

步驟 **1**：建立資料儲存區

如果還沒有建立資料儲存區，請建立一個以將 PingFederate 連接到 AD FS LDAP 伺服器。

步驟

1. 前往 **System** > **Data & Credentials Stores**。
2. 選擇 **New Data Store**。
3. 對於類型，選擇 **Directory** （**LDAP**）。
4. 選擇*下一步*。
5. 在 LDAP 組態下：
   - 請輸入*主機名稱*、使用者 **DN**（使用者名稱）和*密碼*的值。

     使用您"設定身分識別聯盟"在 StorageGRID 中使用的值。
   - 對於 Active Directory，請選擇 **LDAP** 類型。

步驟 **2**：建立密碼認證資料驗證器

如果您還沒有、請建立密碼認證驗證程式。

步驟

1. 選擇 **Password Credential Validators** > **Create New instance**。
2. 在「類型」標籤上，輸入以下資訊：
   a. 執行個體名稱和執行個體 ID：兩者可以使用相同的值。
   b. 類型：選擇 **LDAP Username Password Credential Validator**。
3. 選擇*下一步*。
4. 在「執行個體組態」索引標籤上，輸入以下資訊：
   - LDAP 資料儲存區：選擇您建立的 資料儲存區。
   - 搜尋庫：輸入 LDAP 組態 的相關資訊。
   - 搜尋篩選器：輸入 **sAMAccountName=${username}**。

- 搜尋範圍：選擇*Subtree*。

5. 選擇*下一步*。
6. 在「擴充合約」標籤上，新增下列屬性： `memberOf`， `objectGUID`， `sAMAccountName`， `sn`，以及 `userPrincipalName`
7. 選擇 **Next** > **Save**。

步驟 **3**：建立 **IdP** 介面卡執行個體

如果還沒有建立 IdP（身分供應商）介面卡執行個體，請建立一個。

> StorageGRID 系統中的每個管理節點都必須具有身分識別提供者 （IdP） 連線。這可確保使用者可以安全地登入和登出任何管理節點。您可以為所有管理節點建立單一 IdP 連線（建議），也可以為每個管理節點建立一個不同的 IdP 連線。

步驟

1. 轉至*驗證*>*整合*>* IDP介面卡*。
2. 選擇* Create New Instance*（創建新實例*）。
3. 在「類型」標籤上，輸入以下資訊：
   - 執行個體名稱和執行個體 ID：兩者可以使用相同的值。
   - 類型：選擇 **HTML Form IdP Adapter**。
4. 選擇*下一步*。
5. 在「IdP Adapter」索引標籤上，選取「Add a new row to 'Credential Validators'」。
6. 選擇您建立的密碼認證驗證工具。
7. 選擇*下一步*。
8. 在「擴充合約」標籤上，新增您為 密碼認證驗證工具 對應的屬性。
9. 選擇*下一步*。
10. 在「介面卡屬性」標籤上，選擇「Pseudonym」的 **username** 屬性。
11. 選擇 下一步 > 下一步。
12. 查看摘要並選擇 **Save**。

步驟 **4**：設定 **OAuth** 伺服器和授權伺服器設定

設定授權伺服器以支援 StorageGRID 接受的授權類型。

步驟

1. 前往 **System** > **Authorization Server Settings**。
2. 請確認已為「重複使用現有持久存取授權」選取下列授權類型：
   - 隱含
   - 授權碼
   - 資源所有者密碼憑證

如果貴公司限制使用 RESOURCE OWNER PASSWORD CREDENTIALS，則只能使用 AUTHORIZATION CODE。

3. 對於 OAuth 管理 Web 服務設定，請選擇您建立的 密碼認證驗證工具。

步驟 **5**：定義範圍

在 PingFederate 中定義範圍。

步驟

1. 前往 **System** > **OAuth Settings** > **Scope Management**。
2. 在「通用範圍」標籤上，如果 **openid**、**email** 和 **profile** 的值尚不存在，請新增這些值。

步驟 **6**：設定 **IdP** 介面卡對應

設定 IdP Adapter Mapping，將 IdP 的屬性對應到核發給用戶端的持久授權，例如存取權杖或重新整理權杖。

步驟

1. 前往 **Authentication** > **Policy Contract Grant Mapping**。
2. 選擇「IdP Adapter Grant Mapping」。
3. 從「來源介面卡執行個體」下拉式選單中，選擇您建立的HTML 表單介面卡。
4. 選擇 新增映射 > 合約履行。
5. 在「來源」下，為 USER_KEY 和 USER_NAME 選擇 **Adapter**。
6. 在「值」下，選擇 **sAMAccountName** 作為 USER_KEY，選擇 **username** 作為 USER_NAME。
7. 選擇「下一步」>「下一步」進入摘要頁面。
8. 選擇*保存*。

步驟 **7**：設定資源擁有者憑證映射

設定資源擁有者憑證映射，以確保在驗證期間正確驗證使用者憑證。

步驟

1. 前往 **Authentication** > **Policy Contract Grant Mapping**。
2. 選擇「Resource Owner Credentials Grant Mapping」。
3. 從「來源密碼驗證器執行個體」下拉式選單中，選擇您建立的密碼認證驗證工具。
4. 選擇 新增映射 > 合約履行。
5. 新增 USER_KEY 的映射：
   - 在「來源」下，選取 **Password Credential Validator**。
   - 在「值」下，選擇 **sAMAccountName**。
6. 選擇「下一步」>「下一步」進入摘要頁面。
7. 選擇*保存*。

步驟 **8**：建立或匯入簽署憑證

如果您尚未建立簽署憑證、請建立或匯入簽署憑證。

步驟

1. 請前往*安全*>*簽署與解密金鑰與憑證*。
2. 選擇 **Create New**，然後輸入以下資訊：
   - 通用名稱（CN）：這應該是伺服器的完整網域名稱（FQDN）。
   - 組織（Org）：請輸入您的組織名稱。
   - 國家：請提供兩位字母的國家代碼，例如，美國為 US。
   - 金鑰演算法：選擇合適的金鑰演算法，例如 **RSA**。
   - 金鑰長度：設定為 **2048** 位元。
   - 簽署演算法：選擇 **RSA with SHA256** 作為簽署演算法，以確保安全的加密操作。

步驟 **9**：設定存取權杖管理

StorageGRID 使用存取權杖來驗證和授權 PingFederate 中的 API 請求。

步驟

1. 導覽至 **Applications** > **Access Token Management**。
2. 選擇* Create New Instance*（創建新實例*）。
3. 在「類型」標籤上，輸入以下資訊：
   - 執行個體名稱和執行個體 ID：兩者可以使用相同的值。
   - 類型：驗證該值是否為 **JSON Web Tokens**。
4. 選擇*下一步*。
5. 在「執行個體組態」索引標籤中，輸入以下憑證資訊：
   - 密鑰 ID：輸入密鑰的唯一識別碼。
   - 憑證：新增您建立的 證書。
   - JWS 演算法：選擇 **RSA using SHA256**。
   - 活動簽章憑證金鑰 ID：選擇您在此步驟中建立的 金鑰 **ID**。
6. 選擇 下一步 > 下一步。
7. 在「存取令牌屬性合約」標籤上，選擇 **USER_KEY** 作為主體屬性名稱，選擇 **username** 作為擴充合約。
8. 選取*「Add*」。
9. 選擇 **Next** > **Next** > **Next** 以瀏覽至摘要頁面。
10. 選擇*保存*。

步驟 **10**：設定存取令牌映射

設定存取權杖對應，以使用您建立的存取權杖。

步驟

1. 前往 **Applications** > **Access Token Mappings**。
2. 選取 **Access Token Mappings**。
3. 選擇 新增映射。
4. 對於內容，請選擇 **Default**。
5. 對於 Access Token Manager，請選擇您建立的 存取權杖。
6. 選擇 **Next** > **Contract Fulfillment**：
7. 在「來源」下，為使用者名稱選擇 **Persistent Grant**。
8. 在「值」下，選擇 **USER_KEY** 作為使用者名稱。
9. 選擇 **Next** > **Save**。

步驟 **11**：設定 **OpenID Connect** 原則

定義 OpenID Connect 原則，以供用戶端存取根據 OpenID 規範對應的屬性。

步驟

1. 前往 **Applications** > **OAuth Clients**。
2. 選擇「OpenId Connect 原則管理」>「新增原則」。
3. 在「管理原則」索引標籤上，輸入下列資訊：
   - 原則 ID：原則的唯一識別碼。
   - 原則名稱：原則的描述性名稱。
   - ACCESS TOKEN MANAGER：選擇您建立的 存取權杖。
   - ID TOKEN LIFETIME：設定 ID 令牌所需的壽命，例如 60 分鐘或 1 小時。
   - 在 ID 令牌中包含使用者資訊：勾選此方塊可在 ID 令牌中包含使用者詳細資訊。
4. 選擇*下一步*。
5. 在「屬性契約」標籤上，移除您建立的 資料儲存區 不需要的任何現有屬性。僅保留您希望從 Ping Authentication 傳遞到 StorageGRID 的屬性。

   這是關鍵的一步。它決定了 ID 權杖中包含哪些屬性值。StorageGRID 在驗證過程中繼承這些值。

6. 選擇 下一步 > 下一步。
7. 在「屬性來源和使用者尋找」標籤上，選取 **Add Attribute Source**。然後輸入以下資訊：
   - ATTRIBUTE SOURCE ID 和 ATTRIBUTE SOURCE DESCRIPTION：兩者可以使用相同的值。
   - 活動資料儲存區：選擇您建立的 資料儲存區。
8. 選擇*下一步*。
9. 在LDAP目錄搜尋索引標籤上：
   a. 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。
   b. 從「根物件類別」下拉式選單中選擇 **objectClass**。

c. 從「屬性」下拉式選單中，為每個要對應的物件類別新增一個屬性。例如：

- InetOrgPerson：新增 displayName、givenName 或 HomePhone。
- 使用者：新增 LocalID 或 userPrincipalName （upn）。
- 頂部：新增 memberOf 或名稱。
- 人員：新增 sn。

10. 選擇*下一步*。
11. 在LDAP Filter（LDAP篩選器）索引標籤上、輸入* sAMAccountName=${userName}*。

    您需要自訂 LDAP 篩選器，以確保 StorageGRID 能根據您組織的特定 Active Directory 或 LDAP 結構擷取使用者屬性。請諮詢您的 LDAP/AD 系統管理員，以取得適合您設定的篩選器表示式。

12. 選擇 **Save** 並審查摘要。
13. 在「合約履行」標籤上，輸入以下資訊：
    - 來源：選擇您建立的LDAP 資料儲存區。
    - 值：將每個屬性合約對應至各自的值。
14. 選擇 下一步 > 下一步。
15. 查看摘要並選擇 **Save**。
16. 前往「應用程式」>「OAuth 用戶端」>「OpenID Connect 原則管理」。
17. 確認您建立的原則已設定為預設原則。

步驟 **12**：為 **OAuth** 伺服器建立 **OAuth** 用戶端

建立新的 OAuth 用戶端，以設定必要的用戶端憑證並授權 PingFederate 與 StorageGRID 之間的連線。

步驟

1. 前往 **Applications** > **OAuth Clients**。
2. 選擇 **Add Client**，然後輸入以下資訊：
    - 用戶端 ID：請輸入唯一值。
    - 用戶端驗證：選取 **Client Secret**。
    - 用戶端密碼：選擇 **CHANGE SECRET** > **Generate Secret**。

      這將為用戶端產生密鑰。請儲存此密鑰以備後用。

    - 重新導向 URI：請在「重新導向 URI」區段中提供 StorageGRID 返回 URL。這些 URL 應與 StorageGRID 中為 OAuth 設定的 URL 相符：例如：
    - `https://<Admin IP or Hostname>/api/v4/oidc-callback`
    - `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
    - 允許的授權類型：請選擇以下選項：
      - 授權碼：用於啟動 OAuth 流程。
      - **Refresh Token**：當存取權杖過期時，取得新的權杖。

- **Resource Owner Password Credentials**：如果您需要直接存取使用者憑證進行驗證。

◦ OPENID CONNECT：選擇 **RSA using SHA-256** 作為 ID Token 簽章演算法。

◦ 登出模式：選擇 **OIDC Back-Channel**。

◦ 前端通道登出 URI、後端通道登出 URI 和登出後重新導向 URI：新增 StorageGRID 登出 URI：`https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

3. 選擇*保存*。

接下來

建立 SP 連線後，"使用 OIDC 設定 SSO"。

使用 **OIDC** 在 **StorageGRID** 中設定 **SSO**

依照 OpenID Connect (OIDC) 的 SSO 設定精靈操作，進入沙盒模式，在為所有 StorageGRID 使用者啟用單一登入 (SSO) 之前，先設定並測試 SSO。啟用 SSO 後，您可以根據需要返回沙盒模式來變更或重新測試組態。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 您已在 StorageGRID 系統的 SSO 身分識別供應商中設定 OIDC 用戶端。
- 您的 StorageGRID 系統需要 "已設定的身分識別聯盟"。

步驟 **1**：提供身分識別供應商詳細資訊

開啟精靈，填寫「提供身分供應商詳細資料」頁面上的欄位。

步驟

1. 存取精靈以設定 SSO 設定：
   a. 選擇*設定* > 存取控制 > 單一登入。出現「單一登入」頁面。

      如果設定 SSO 設定按鈕已停用，請確認您已將身分提供者設定為聯合身分識別來源。請參閱"單一登入的要求與考量"。

   b. 選擇*配置 SSO 設定*。出現提供身分提供者詳細資訊頁面。
2. 在 **Protocol** 下，選擇 **OIDC**。
3. 從下拉式清單中選取* SSO類型*。
4. 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。

      如果您選擇此設定：

i. 瀏覽至 CA 憑證的位置。

ii. 上傳 CA 憑證檔案。

- 請勿使用 **TLS**：請勿使用 TLS 憑證來保護連線的安全。

> 如果您變更 CA 憑證、請立即"在管理節點上重新啟動 mgmt-API 服務"在 Grid Manager 中測試成功的 SSO 。

5. 選擇*繼續*。出現「提供依賴方識別碼」頁面。

步驟 **2**：輸入用戶端資訊

請在精靈的「輸入用戶端資訊」步驟中填寫各個欄位。

步驟

1. 為 StorageGRID 指定*信賴方識別碼*。此值控制您為每個 OIDC 組態使用的名稱。
   - 例如，如果您的網格只有一個管理節點，而且您預期未來不會新增更多管理節點，請輸入 `SG`或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請在識別碼中包含字串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字串後，將產生一個表格，根據節點的主機名稱顯示網格中每個管理節點的 OIDC 組態。

> 您必須為 StorageGRID 系統中的管理節點設定 OIDC。這可確保使用者可以安全地登入和登出任何管理節點。您可以為所有管理節點使用相同的 OIDC 組態（建議），也可以為每個管理節點設定不同的 OIDC 組態。

2. 請輸入每個信賴方識別碼的*用戶端 ID*、用戶端金鑰*和***OpenID** 端點 **URL**。
3. 選擇*儲存並進入沙盒模式*。

步驟 **3**：測試組態

進入沙盒模式後，您可以完成並測試您選擇的 SSO 類型的組態。

沙盒模式便於進行來回組態，並在啟用 SSO 之前測試所有設定。StorageGRID 可視需要保持在沙盒模式下。但是，只有同盟使用者和本機使用者才能登入。

步驟

1. 在設定 SSO 頁面上，找到精靈的測試設定步驟上的連結。

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

2. 選擇連結，或將 URL 複製並貼上到新標籤頁中，即可存取您的身分供應商的登入頁面。
3. 請輸入您的聯合身分驗證使用者名稱和密碼。
   - 如果 SSO 登入和登出操作成功，則會顯示綠色橫幅。
   - 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. 請依照精靈中的步驟存取網格中每個管理節點的測試組態頁面。
5. 重複步驟 2 和 3，驗證每個管理節點的 SSO 連線。

步驟 **4**：啟用單一登入

當您確認可以使用 SSO 登入每個管理節點後，即可為整個 StorageGRID 系統啟用 SSO。

啟用 SSO 後，所有使用者必須使用 SSO 存取 Grid Manager、Tenant Manager、Grid Management API 和 Tenant Management API。本機使用者將無法再存取 StorageGRID 。StorageGRID 並未為所有支援的 SSO 供應商提供範例驗證指令碼。

步驟

1. 從設定 SSO 精靈的測試設定步驟中，選擇*啟用 SSO*。
2. 查看警告訊息，然後選擇*啟用 SSO*。

   單一登入現已啟用。出現「單一登入」頁面，其中現在包含您剛剛設定的 SSO 的詳細資訊。

3. 若要編輯配置，請選擇*編輯*。
4. 若要停用單一登入，請選擇「停用」。

如果您使用 Azure 門戶，並且從用於存取 Entra ID 的相同電腦存取StorageGRID ，請確保 Azure 入口網站使用者也是授權的StorageGRID使用者（已匯入StorageGRID 的聯合群組中的使用者），或在嘗試登入StorageGRID之前登出 Azure 入口網站。

使用 **SAML** 設定 **SSO**

了解如何使用 **SAML** 在 **StorageGRID** 中設定 **SSO**

在 StorageGRID 中設定單一登入 （SSO） 可讓 StorageGRID （服務供應商）和 SSO 身分供應商安全地就使用者身分驗證請求進行通訊。

您可以使用 OpenID Connect (OIDC) 或 SAML 在 StorageGRID 中設定 SSO。請依照以下高階步驟使用 SAML 在 StorageGRID 中設定 SSO，或了解更多資訊"使用 OIDC 設定 SSO"。

1 設定 **SSO**

選擇「設定 SAML 單一登入」精靈。然後，設定身分供應商的單一登入，並進入沙盒模式。

瞭解 "使用 SAML 設定 SSO"

2 設定身分識別供應商

根據您計劃使用的 SSO 身分供應商，您可以選擇 Active Directory 或 Entra ID 作為身分聯合 LDAP 服務類型。

- 對於 Active Directory Federation Service (AD FS)，您可以使用 AD FS、Entra ID 或 PingFederate 身分供應商。
- 對於 Entra ID，您只能使用 Entra ID 身分供應商。

使用 SSO 身分識別供應商的軟體為網格中的每個管理節點設定 SAML。

- 了解 Active Directory 中的 "為每個管理節點建立一個應用程式群組"
- 了解 "為每個管理節點建立一個應用程式" 在 Entra ID 中的資訊
- 了解 "為每個管理節點建立服務供應商連線" 在 PingFederate 中的相關資訊

3 測試組態

為每個管理節點設定 SAML 後，返回設定單一登入精靈並測試組態。

瞭解 "測試 SSO 組態"

4 啟用 **SSO**

為所有 StorageGRID 使用者啟用 SSO。

瞭解 "為 StorageGRID 使用者啟用 SSO"

使用 **SAML** 在 **StorageGRID** 中設定 **SSO**

依照 SAML 單一登入 （SSO） 設定精靈的步驟操作，進入沙盒模式，在為所有 StorageGRID 使用者啟用 SSO 之前，先設定並測試單一登入 （SSO）。啟用 SSO 後，您可以根據需要返回沙盒模式來變更或重新測試組態。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 您已為StorageGRID 您的整套系統設定身分識別聯盟。
- 對於身分聯合 **LDAP** 服務類型，您可以根據計畫使用的 SSO 身分提供者選擇 Active Directory 或 Entra ID。

已設定的**LDAP**服務類型	**SSO**身分識別供應商選項
Active Directory Federation Service（AD FS）	• Active Directory • 進入 ID • PingFedate
進入 ID	進入 ID

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）。
- Entra ID 的回應包括使用者主體名稱 (UPN)。

為了允許 StorageGRID （服務供應商）和 SSO 身分供應商就使用者身分驗證請求進行安全通訊，您需要完成以下任務：

1. 在StorageGRID中配置設定。
2. 使用 SSO 身分提供者的軟體，為每個管理節點建立信賴方信任（AD FS）、企業應用程式（Entra ID）或服務供應商（PingFederate）。
3. 返回StorageGRID以啟用 SSO。

沙盒模式可以輕鬆執行此來回配置，並在啟用 SSO 之前測試所有設定。當您使用沙盒模式時，使用者無法使用 SSO 登入。

步驟 **1**：提供身分識別供應商詳細資訊

開啟精靈，填寫「提供身分供應商詳細資料」頁面上的欄位。

步驟

1. 存取精靈：
   a. 選擇*設定* > 存取控制 > 單一登入。出現「單一登入」頁面。

      如果設定 SSO 設定按鈕已停用，請確認您已將身分提供者設定為聯合身分識別來源。請參閱"單一登入的要求與考量" 。

   b. 選擇*配置 SSO 設定*。出現提供身分提供者詳細資訊頁面。
2. 在 **Protocol** 下，選擇 **SAML**。
3. 從下拉式清單中選取* SSO類型*。
4. 如果您選擇 Active Directory 作為 SSO 類型，請輸入身分提供者的 聯合驗證服務名稱，與 Active Directory 聯合驗證服務 (AD FS) 中顯示的完全一致。

   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。

5. 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 憑證來保護連線的安全。

     如果您變更 CA 憑證、請立即"在管理節點上重新啟動 mgmt-API 服務"在 Grid Manager 中測試成功的 SSO 。

6. 選擇*繼續*。出現「提供依賴方識別碼」頁面。

步驟 **2**：提供信賴方信任、企業應用程式或 **SP** 連線

根據您選擇的 SSO 類型，填寫精靈步驟 2 中的欄位。

Active Directory

填寫「提供信賴方識別碼」步驟中的欄位。

步驟

1. 指定StorageGRID的 依賴方識別碼。此值控制您在 AD FS 中為每個信賴方信任所使用的名稱。
   - 例如，如果您的網格只有一個管理節點，而且您預期未來不會新增更多管理節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]` 在標識符中。例如， `SG-[HOSTNAME]` 。包含此字串將產生一個表，該表根據節點的主機名稱顯示網格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。

2. 選擇*儲存並進入沙盒模式*。

進入 **ID**

完成「設定企業應用程式」步驟中的欄位。

步驟

1. 在企業應用程式部分，指定StorageGRID的 企業應用程式名稱。此值控制您在 Entra ID 中為每個企業應用程式使用的名稱。
   - 例如，如果您的網格只有一個管理節點，而且您預期未來不會新增更多管理節點，請輸入 `SG` 或 `StorageGRID`。
   - 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]` 在標識符中。例如， `SG-[HOSTNAME]` 。包含此字串將產生一個表，該表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。

2. 依照"在 Entra ID 中建立企業應用程式"中的步驟，為表格中列出的每個管理節點建立一個企業應用程式。
3. 從 Entra ID 複製每個企業應用程式的聯合元資料 URL。然後，將此 URL 貼到StorageGRID中對應的 **Federation metadata URL** 欄位中。
4. 複製並貼上所有管理節點的聯合元資料 URL 後，選擇 儲存並進入沙盒模式。

PingFedate

填寫「提供 SP 連線 ID」步驟中的欄位。

步驟

1. 在「服務供應商（SP）」區段中、指定* SP連線ID* StorageGRID 以供參考。此值可控制您在PingFedate中用於每個SP連線的名稱。
   - 例如，如果您的網格只有一個管理節點，而且您預期未來不會新增更多管理節點，請輸入 `SG` 或 `StorageGRID`。

◦ 如果您的網格包含多個管理節點，請包含字串 `[HOSTNAME]`在標識符中。例如， `SG-[HOSTNAME]` 。包含此字串將產生一個表，該表根據節點的主機名稱顯示系統中每個管理節點的SP連線 ID。

> 您必須為StorageGRID 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。

2. 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>
   ```

3. 選擇*儲存並進入沙盒模式*。

步驟 **3**：設定信賴方信任、企業應用程式或 **SP** 連線

儲存配置並進入沙盒模式後，您可以完成並測試所選 SSO 類型的配置。

StorageGRID可依需求維持沙盒模式。但是，只有聯合用戶和本地用戶可以登入。

Active Directory

步驟

1. 移至Active Directory Federation Services（AD FS）。
2. 使用「設定 SSO」頁面上的表格中顯示的每個依賴方標識符，為StorageGRID建立一個或多個依賴方信任。

   您必須為表格中顯示的每個管理節點建立一個信任關係。

   有關說明，請前往 "在AD FS中建立依賴方信任"。

進入 **ID**

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*設定* > 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 入口網站。
4. 請依照 "在 Entra ID 中建立企業應用程式" 中的步驟，將每個管理節點的 SAML 中繼資料檔案上傳至其對應的 Entra ID 企業應用程式。

PingFedate

步驟

1. 從您目前登入之管理節點的「單一登入」頁面、選取按鈕以下載並儲存SAML中繼資料。
2. 然後、針對網格中的任何其他管理節點、重複下列步驟：
   a. 登入節點。
   b. 選擇*設定* > 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（顯示在「設定 SSO」頁面上的表格中）以及您為該管理節點下載的 SAML 中繼資料。

   您必須為表中所示的每個管理節點建立一個SP連線。

步驟 **4**：測試組態

在強制整個StorageGRID系統使用單一登入之前，請確認每個管理節點的單一登入和單一登出均已正確設定。

Active Directory

步驟

1. 在設定 SSO 頁面上，找到精靈的測試設定步驟上的連結。

   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。

進入 **ID**

步驟

1. 前往Azure入口網站的「單一登入」頁面。
2. 選擇*測試此應用程式*。
3. 輸入同盟使用者的認證資料。
   - 如果SSO登入和登出作業成功、就會出現成功訊息。
   - 如果SSO作業不成功、會出現錯誤訊息。請修正問題、清除瀏覽器的Cookie、然後再試一次。
4. 重複這些步驟、驗證網格中每個管理節點的SSO連線。

PingFedate

步驟

1. 在設定 SSO 頁面中，選擇沙盒模式訊息中的第一個連結。

   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。
   - 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。

步驟 **5**：啟用單一登入

當您確認可以使用 SSO 登入每個管理節點後，即可為整個 StorageGRID 系統啟用 SSO。

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

步驟

1. 從設定 SSO 精靈的測試設定步驟中，選擇*啟用 SSO*。
2. 查看警告訊息，然後選擇*啟用 SSO*。

   單一登入現已啟用。出現「單一登入」頁面，其中現在包含您剛剛設定的 SSO 的詳細資訊。

3. 若要編輯配置，請選擇*編輯*。
4. 若要停用單一登錄，請選擇“停用 **SSO**”。

如果您使用 Azure 門戶，並且從用於存取 Entra ID 的相同電腦存取StorageGRID ，請確保 Azure 入口網站使用者也是授權的StorageGRID使用者（已匯入StorageGRID 的聯合群組中的使用者），或在嘗試登入StorageGRID之前登出 Azure 入口網站。

接下來呢？

使用 SAML 設定 SSO 後，為管理節點設定身分供應商。

如果您的身分供應商是.....	您需要.....
Active Directory	"為每個管理節點建立一個應用程式群組"
進入 ID	"為每個管理節點建立一個應用程式"
PingFedate	"為每個管理節點建立服務供應商連線"

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

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

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* AD FS*作為SSO類型。
- 您在 Grid Manager 中擁有 "進入沙盒模式"。
- 您知道系統中每個管理節點的完全限定網域名稱（或 IP 位址）和信賴方識別碼。您可以在StorageGRID設定 SSO 頁面上的管理節點詳細資料表中找到這些值。

  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_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 對於 *Admin_Node_Identifier*、請輸入「管理節點」的信賴方識別碼、其內容與「單一登入」頁面上顯示的內容完全相同。例如 `SG-DC1-ADM1`：。
   - 對於 *Admin_Node_FQDN*、請輸入相同管理節點的完整網域名稱。（如有必要、您可以改用節點的IP位址。不過、如果您在此輸入IP位址、請注意、如果該IP位址有任何變更、您必須更新或重新建立此信賴關係人信任。）
3. 從Windows Server Manager中、選取* Tools **>** AD FS Management *。

   隨即顯示AD FS管理工具。
4. 選取「* AD FS*>*信賴廠商信任*」。

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

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

f. 針對屬性存放區、選取* Active Directory *。

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

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

i. 選擇*完成*、然後選擇*確定*。

7. 確認中繼資料已成功匯入。

a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。

b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

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

9. 完成後，返回 StorageGRID 並"測試所有依賴方信任"確認其組態是否正確。

透過匯入聯盟中繼資料來建立依賴方信任

您可以存取每個管理節點的SAML中繼資料、以匯入每個信賴方信任的值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。

2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方

3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。

4. 選取*匯入線上發佈的依賴方相關資料、或是本機網路上的相關資料*。

5. 在*聯盟中繼資料位址（主機名稱或URL）*中、輸入此管理節點的SAML中繼資料位置：

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

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

6. 完成「信賴方信任」精靈、儲存信賴方信任、然後關閉精靈。

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

7. 新增報銷規則：

a. 以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。

b. 選擇*新增規則*：

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

d. 在「設定規則」頁面上、輸入此規則的顯示名稱。

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

e. 針對屬性存放區、選取* Active Directory *。

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

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

h. 選擇*完成*、然後選擇*確定*。

8. 確認中繼資料已成功匯入。

a. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。

b. 確認已填入*端點*、*識別項*和*簽名*索引標籤上的欄位。

如果中繼資料遺失、請確認同盟中繼資料位址正確、或手動輸入值。

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

10. 完成後，返回 StorageGRID 並"測試所有依賴方信任"確認其是否已正確設定。

手動建立依賴方信任

如果您選擇不匯入依賴零件信任的資料、您可以手動輸入值。

步驟

1. 在Windows Server Manager中、選取*工具*、然後選取* AD FS管理*。

2. 在「Actions（動作）」下、選取「* Add S依賴 方Trust（*新增信賴方

3. 在歡迎頁面上、選擇* Claims感知*、然後選取* Start*。

4. 選取*手動輸入依賴方的相關資料*、然後選取*下一步*。

5. 完成信賴廠商信任精靈：

a. 輸入此管理節點的顯示名稱。

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

b. 跳過設定選用權杖加密憑證的步驟。

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

d. 輸入管理節點的SAML服務端點URL：

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

對於 *`Admin_Node_FQDN`*、請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、其內容與「單一登入」頁面上顯示的內容完全相同。例如 `SG-DC1-ADM1`：。

f. 檢閱設定、儲存信賴關係人信任、然後關閉精靈。

此時會出現「編輯請款核發原則」對話方塊。

如果對話方塊未出現、請以滑鼠右鍵按一下信任、然後選取*編輯請款簽發原則*。

6. 若要啟動「請款規則」精靈、請選取*「新增規則*」：

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

b. 在「設定規則」頁面上、輸入此規則的顯示名稱。

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

c. 針對屬性存放區、選取* Active Directory *。

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

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

f. 選擇*完成*、然後選擇*確定*。

7. 在依賴方信任上按一下滑鼠右鍵、開啟其內容。

8. 在「端點」索引標籤上、設定單一登出（SLO）的端點：

a. 選擇* Add SAML（添加SAML）*。

b. 選擇*端點類型*>* SAML登出*。

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

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

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

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

a. 選擇*確定*。

9. 在*簽名*索引標籤上、指定此信賴憑證方信任的簽名證書：

a. 新增自訂憑證：

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

(`server.crt`不建議使用管理節點的預設憑證）。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，返回 StorageGRID 並"測試所有依賴方信任"確認其是否已正確設定。

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

使用 Entra ID 為系統中每個 Admin Node 建立一個適用於 SAML 的企業應用程式。

開始之前

- 您已開始為StorageGRID設定單一登錄，並選擇 **Entra ID** 作為 SSO 類型。
- 您在 Grid Manager 中擁有 "進入沙盒模式"。
- 您的系統中的每個管理節點都有*企業應用程式名稱*。您可以從設定 SSO 頁面上的管理節點詳細資料表中複製這些值。

> 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 Entra ID 中建立企業應用程式的經驗。
- 您有一個具有有效訂閱的 Entra ID 帳戶。
- 您在 Entra ID 帳戶中擁有以下角色之一：全域管理員、雲端應用程式管理員、應用程式管理員或服務主體的擁有者。

步驟 **1**：存取 **Entra ID**

步驟

1. 登入 "Azure Portal"。
2. 導航至 "進入 ID"。
3. 選擇。 "企業應用程式"

步驟 **2**：建立企業應用程式並儲存 **StorageGRID SSO** 組態

若要在StorageGRID中儲存 Entra ID 的 SSO 配置，您必須使用 Entra ID 為每個管理節點建立一個企業應用程式。您將從 Entra ID 複製聯合元資料 URL，並將其貼上到配置 SSO 頁面上對應的 聯合元資料 **URL** 欄位中。

步驟

1. 針對每個管理節點重複下列步驟。
   a. 在 Entra ID Enterprise 應用程式窗格中，選擇 新應用程式。
   b. 選取*建立您自己的應用程式*。
   c. 對於名稱，請輸入從設定 SSO 頁面上的管理節點詳細資料表複製的*企業應用程式名稱*。
   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. 前往設定 SSO 頁面，並將 URL 貼到與您使用的 企業應用程式名稱 相對應的 聯合元資料 **URL** 欄位中。

2. 為每個管理節點貼上聯合元資料 URL 並對 SSO 配置進行所有其他必要的變更後，在設定 SSO 頁面上選擇儲存。

步驟 **3**：下載每個管理節點的 **SAML** 中繼資料

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

步驟

1. 針對每個管理節點重複這些步驟。

a. 從管理節點登入StorageGRID 到這個功能。

b. 選擇*設定* > 存取控制 > 單一登入。

c. 選取按鈕、即可下載該管理節點的SAML中繼資料。

d. 儲存文件，然後將其上傳到 Entra ID。

步驟 **4**：將 **SAML** 中繼資料上傳到每個企業應用程式

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

步驟

1. 返回Azure Portal。

2. 針對每個企業應用程式重複這些步驟：

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

a. 前往企業應用程式的「內容」頁面。

b. 將*需要指派*設為*否*（除非您要個別設定指派）。

c. 前往單一登入頁面。

d. 完成SAML組態。

e. 選取*上傳中繼資料檔案*按鈕、然後選取您為對應的管理節點下載的SAML中繼資料檔案。

f. 載入檔案後、選取*「Save"（儲存）、然後選取「 X*」以關閉窗格。您將返回「使用SAML設定單一登入」頁面。

3. "測試每個應用程式"。

在 **StorageGRID** 中為 **SAML** 建立 **PingFederate** 服務供應商連接

使用 PingFederate 為系統中的每個管理節點建立 SAML 服務供應商 （SP） 連線。為了加快流程，您需要從 StorageGRID 匯入 SAML 中繼資料。

開始之前

- 您已設定StorageGRID 單一登入以供使用、並選擇* Ping federate*作為SSO類型。
- 您在 Grid Manager 中擁有 "進入沙盒模式"。

- 您系統中每個管理節點都有* SP連線 ID *。您可以在「設定 SSO」頁面上的管理節點詳細資料表中找到這些值。
- 您已下載系統中每個管理節點的* SAML中繼資料*。
- 您在PingFedate伺服器上建立SP連線的經驗豐富。
- 您擁有 "系統管理員參考指南"PingFederate Server 。PingFedate文件提供詳細的逐步指示和說明。
- 你有"管理員權限"用於 PingFederate 伺服器。

關於這項工作

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

完整的**PingFedate**必備條件

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

建立資料儲存區**[data-store]**

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

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

建立密碼認證驗證器**[**密碼 驗證器**]**

如果您還沒有、請建立密碼認證驗證程式。

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

建立**IDP**介面卡執行個體**[[**介 面卡執行個體**]**

如果您尚未建立IDP介面卡執行個體、請建立一個IDP介面卡執行個體。

步驟

1. 轉至*驗證*>*整合*>* IDP介面卡*。
2. 選擇* Create New Instance*（創建新實例*）。
3. 在類型索引標籤上、選取* HTML表單IDP介面卡*。
4. 在IDP介面卡索引標籤上、選取*新增一列至「認證驗證程式」*。

5. 選擇密碼認證驗證工具你創造的。
6. 在Adapter Attributes*（適配器屬性）選項卡上，選擇* pseudonyation*的* username*屬性。
7. 選擇*保存*。

建立或匯入簽署憑證[[Signing認證證]

如果您尚未建立簽署憑證、請建立或匯入簽署憑證。

步驟

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

在PingFedate建立SP連線

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

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

選擇SP連線類型

步驟

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

匯入SP中繼資料

步驟

1. 在匯入中繼資料索引標籤上、選取*檔案*。
2. 選擇從管理節點的設定 SSO 頁面下載的 SAML 元資料檔。
3. 檢閱中繼資料摘要和一般資訊索引標籤上提供的資訊。

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

4. 選擇*下一步*。

設定IDP瀏覽器SSO

步驟

1. 從瀏覽器SSO索引標籤、選取*設定瀏覽器SSSSO *。

2. 在「SAML設定檔」索引標籤上、選取「* SP啟動的SSO*」、「* SP初始SLO*」、「* IDP啟動的SSO*」和「* IDP啟動的SLO*」選項。
3. 選擇*下一步*。
4. 在Assertion壽命索引標籤上、不做任何變更。
5. 在Assertion Creation（聲明創建）選項卡上，選擇* Configure Assertion creation （配置聲明創建）。
   a. 在「身分識別對應」索引標籤上、選取「標準」。
   b. 在「屬性合約」索引標籤上、使用* SAML Subject *做為「屬性合約」、以及匯入的未指定名稱格式。
6. 若要延長合約期限、請選取 * 刪除 * 以移除 `urn:oid`、但未使用。

對應介面卡執行個體

步驟

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

設定傳輸協定設定

步驟

1. 在* SP Connection*>*瀏覽器SSSSO >*傳輸協定設定*索引標籤上、選取*設定傳輸協定設定。
2. 在「聲明消費者服務 URL 」標籤上、接受從 StorageGRID SAML 中繼資料匯入的預設值（ * 用於連結和 `/api/saml-response`端點 URL ）。
3. 在「 SLO 服務 URL 」標籤上、接受從 StorageGRID SAML 中繼資料匯入的預設值（ * 重新導向 * 用於連結和端點 URL ） `/api/saml-logout`。

4. 在允許的 SAML 繫結標籤上、清除 * 成品 * 和 * SOAP* 。只需要* POST 和*重新導向。
5. 在「簽章原則」索引標籤上、保留「 * 需要簽署驗證要求 * 」和「 * 永遠簽署聲明 * 」核取方塊的核取方塊。
6. 在加密原則索引標籤上、選取*無*。
7. 檢閱摘要並選取*完成*以儲存傳輸協定設定。
8. 檢閱摘要並選取*完成*以儲存瀏覽器SSO設定。

設定認證資料

步驟

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

建立其他**SP**連線

您可以複製第一個SP連線、為網格中的每個管理節點建立所需的SP連線。您上傳每個複本的新中繼資料。

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

步驟

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

停用 StorageGRID 中的 SSO

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

開始之前

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

步驟

1. 選擇*設定* > 存取控制 > 單一登入。

   此時會出現「單一登入」頁面。

2. 選取*停用*。
3. 選擇*是*。

   此時會出現一則警告訊息、指出本機使用者現在可以登入。

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 StorageGRID 管理節點的 SSO

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

開始之前

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

關於這項工作

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

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

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 根據您的 SSO 組態，執行以下命令之一：

SAML

```
disable-saml
```

OIDC

```
disable-oidc
```

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*設定* > 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。

。重新啟動網格節點： `reboot`

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

使用多管理員驗證

了解 **StorageGRID** 多管理員驗證

身為 StorageGRID 系統管理員，您可以使用多重管理員驗證 (MAV) 來確保某些操作只能在獲得指定系統管理員核准後才能執行。MAV 有助於防止對 StorageGRID 系統進行意外或未經授權的變更。

MAV 預設為停用。

MAV 組態總覽

要設定 MAV，您需要執行以下任務：

- 建立一個或多個系統管理員群組。MAV 系統管理員擁有審批和否決權。
- 啟用多重管理員驗證功能。
- 從一組受保護的操作中進行選擇。

使用者必須擁有 Root 存取權限，才能執行初始組態並在日後進行修改。

MAV 下如何處理受保護的作業

啟用 MAV 後，完成每個受保護的操作都需要以下步驟：

1. 當使用者發起操作時，會產生一個請求。
2. 操作執行前，至少需要一名 MAV 系統管理員批准。
3. 獲得批准後，受 MAV 保護的作業將自動執行。

設定 **StorageGRID** 多管理員驗證

設定 StorageGRID 多管理員驗證 (MAV) 系統涉及建立和管理 MAV 系統管理員群組和使用者、啟用 MAV 功能以及選擇或設定受保護的作業。

MAV 系統管理員對受保護的操作擁有批准權和否決權。

開始之前

- 您有"root 存取權限"。
- 您已從主要管理節點登入 Grid Manager。

步驟 **1**：建立 **MAV** 系統管理員群組和使用者

您可以將現有系統管理員新增至 MAV 群組，也可以建立新的系統管理員。

您可以將 Active Directory (AD) 使用者設定為 MAV 系統管理員。AD 使用者必須設定為 StorageGRID 系統管理員。

步驟

1. 若要建立 MAV 系統管理員群組，請依照下列步驟操作 "建立本機或聯合群組"。
2. 對於群組權限，請選擇 **Root access** 或 **Multi-admin verification requests**。
3. 將本機使用者或聯合使用者新增至群組，或建立新的本機使用者並將其新增至群組，請依照以下步驟操作 "建立本機使用者"。

步驟 2：啟用或停用 MAV

您必須明確啟用多重管理員驗證 (MAV)。如果 MAV 已啟用，而您在有待處理的 MAV 要求時決定停用它，則會收到通知，說明待處理的要求將被刪除。

步驟

1. 選擇 **Configuration** > **Access control** > **Multi-admin verification** > **MAV settings**。
2. 選取 **Enable MAV** 核取方塊以啟用多管理員驗證。
3. 「核准者群組」區段列出 MAV 系統管理員群組和核准者。
4. 在「操作」部分，選取要使用 MAV 保護的操作的核取方塊。
5. （可選）如果您想使用電子郵件通知來提醒 MAV 系統管理員有待核准的請求：
   a. 如果您尚未設定電子郵件伺服器，請依照下列步驟操作 "設定電子郵件伺服器"。
   b. 請輸入寄件者的電子郵件地址。
   c. 請輸入一個或多個電子郵件通知收件者。
6. 選擇 **Save** 以儲存變更。

> 如果您決定不設定電子郵件通知，MAV 系統管理員可以檢視 Grid Manager 儀表板或檢查待審核要求的核准佇列。若要檢查審核佇列，請在多重管理員驗證頁面上選擇 **Other requests**。

步驟 3：管理受保護的作業

啟用多管理員驗證後，您可以透過選取或取消選取要使用 MAV 保護的作業核取方塊來管理受保護的作業。

> 對於 StorageGRID 12.1，唯一受保護的作業是 ILM 原則啟動。如果要啟用 MAV，則必須選取 ILM 原則啟動的核取方塊。

MAV 請求可以具有以下幾種狀態之一：

- 待處理。要求已發起。
- 已過期。要求未在 30 天內處理。或者，具有 Root 存取權限的使用者停用了 MAV，這表示所有待處理的要求都已過期。
- 已撤回。使用者已撤回其請求。
- 已核准。MAV 系統管理員已核准待處理的請求。
- 已拒絕。MAV 系統管理員已拒絕待處理的請求。

排除 **MAV** 電子郵件通知故障

如果 MAV 系統管理員沒有收到待處理要求的電子郵件通知，請依照下列步驟解決問題。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。

步驟

1. 驗證您的設定。
   a. 選擇 組態 > 監控 > 電子郵件伺服器。
   b. 確認電子郵件（SMTP）伺服器設定正確。
   c. 確認您已為收件者指定有效的電子郵件地址。
2. 檢查垃圾郵件篩選器、確定電子郵件未傳送至垃圾郵件資料夾。
3. 請要求您的電子郵件管理員確認寄件者地址的電子郵件並未遭到封鎖。
4. 收集管理節點的記錄檔、然後聯絡技術支援部門。

   技術支援人員可以使用記錄中的資訊來協助判斷發生問題的原因。例如、prometheus.log檔案在連線至您指定的伺服器時可能會顯示錯誤。

   請參閱 "收集記錄檔和系統資料"。

請求核准 **StorageGRID** 中受 **MAV** 保護的作業

身為 StorageGRID 系統管理員或用戶，當您在 StorageGRID 中啟動受 MAV 保護的作業時，系統會自動產生一個請求。同時，會顯示一則訊息，告知您該作業需要獲得核准。

StorageGRID 系統定義哪些作業受 MAV 保護。當您啟動受 MAV 保護的作業時，要求將傳送給 MAV 系統管理員以取得核准。

步驟

StorageGRID 系統通知您，您已啟動受 MAV 保護的作業。

1. 根據需要，執行以下任何任務：
   a. 請依序選取 **Configuration** > **Access control** > **Multi-admin verification** > **My requests**，查看您的要求狀態。
      - 待處理。要求已發起。
      - 已過期。要求未在 30 天內處理。或者，具有 Root 存取權限的使用者停用了 MAV，這表示所有待處理的要求都已過期。
      - 已撤回。使用者已撤回其請求。
      - 已核准。MAV 系統管理員已核准待處理的請求。
      - 已拒絕。MAV 系統管理員已拒絕待處理的請求。
   b. 選擇 **Configuration** > **Access control** > **Multi-admin verification** > **Other requests**，查看其他使用者的待處理要求。

c. 若要取消作業，請選擇「我的請求」>「要取消的請求」>「撤回」。

MAV 系統管理員核准請求後，操作將自動執行。

如果您的請求遭到拒絕，則操作將不會執行，您可以視需要提交新的請求。

在 **StorageGRID** 中管理受 **MAV** 保護的操作請求

身為 MAV 系統管理員，您可以管理 StorageGRID 中受 MAV 保護的操作請求。您可以檢視自己或其他使用者的待處理請求、批准或拒絕請求，以及檢視過往請求的歷史記錄。

開始之前

- 您屬於 MAV 系統管理員群組，並且擁有"root 存取權限"。
- 您已從主要管理節點登入 Grid Manager。

步驟

1. 如果您收到有關 MAV 要求的電子郵件通知，請選擇 **Configuration** > **Multi-admin verification** > **Other requests**。

   此外，Grid Manager 儀表板也會顯示待處理 MAV 請求的通知。

2. 選擇要管理的每個請求對應的單選按鈕。
3. 選取 **Approve** 或 **Reject** 以核准或拒絕所選的要求。
4. 若要檢視過去的請求記錄，請選擇 **History**。

使用網格同盟

了解 **StorageGRID** 網格聯邦

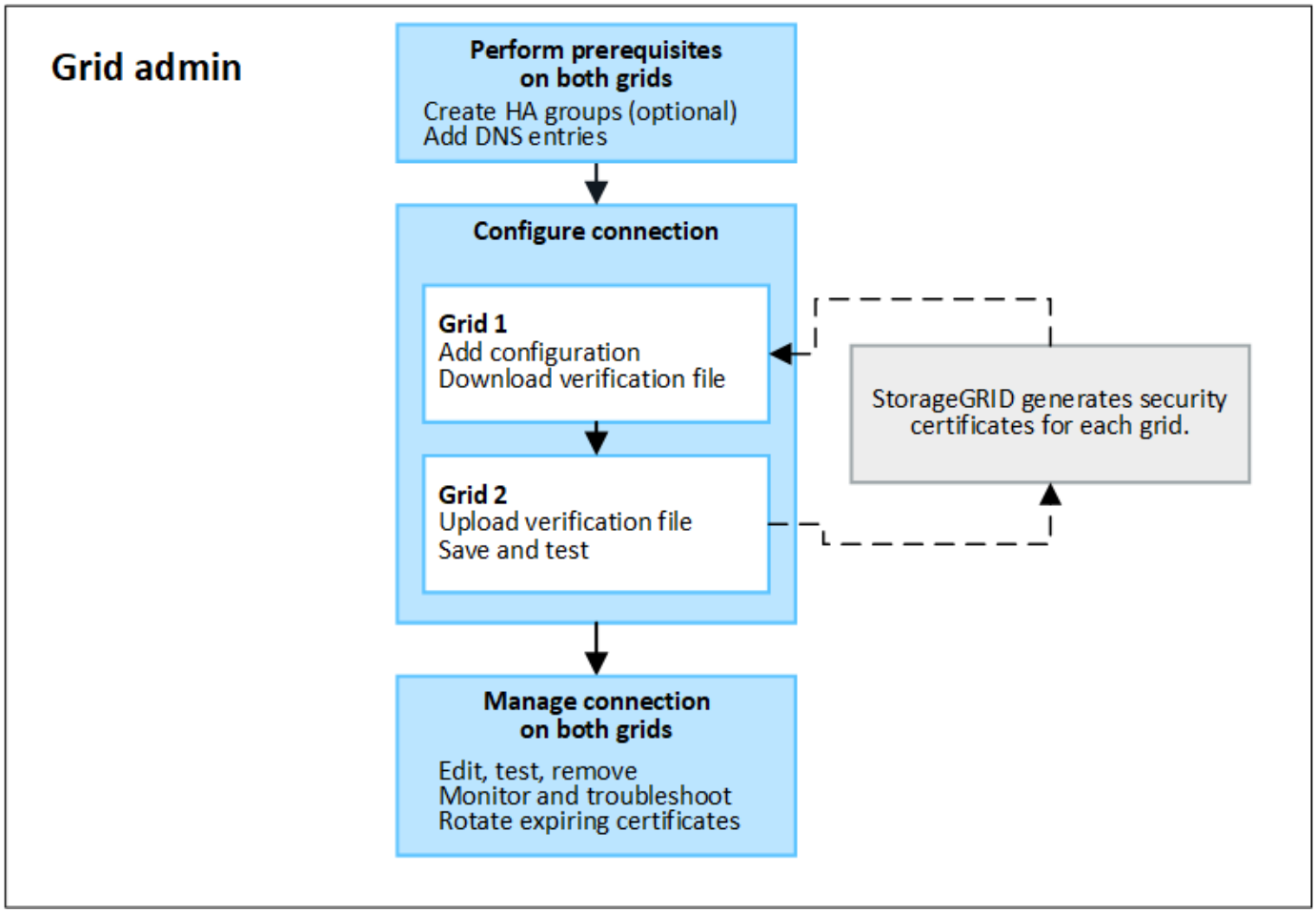
您可以使用網格聯合來同步租戶，並在多個 StorageGRID 系統之間複寫其物件，以實現災難恢復。

什麼是網格同盟連線？

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

網格同盟的工作流程

工作流程圖摘要說明在兩個網格之間設定網格同盟連線的步驟。



網格同盟連線的考量與需求

- 用於網格同盟的網格必須執行相同的 StorageGRID 版本、或兩者之間的主要版本差異不超過一個。

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

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

網路和 **IP** 位址需求

- 網格同盟連線可能發生在網格網路、管理網路或用戶端網路上。
- 網格同盟連線會將一個網格連接到另一個網格。每個網格的組態會在另一個網格上指定一個網格聯盟端點、該端點由管理節點、閘道節點或兩者組成。
- 最佳做法是在每個網格上連接"高可用度（ HA ）群組"閘道和管理節點。使用 HA 群組有助於確保當節點無法使用時、網格同盟連線將保持在線上狀態。如果任一 HA 群組中的作用中介面失敗、連線就可以使用備份介面。
- 不建議建立使用單一管理節點或閘道節點 IP 位址的網格同盟連線。如果節點無法使用、網格同盟連線也將無法使用。

- "跨網格複寫"物件數量要求每個網格上的儲存節點能夠存取另一個網格上設定的管理節點和閘道節點。對於每個網格、請確認所有儲存節點都有高頻寬路由、以做為連線所使用的管理節點或閘道節點。

使用 **FQDN** 來平衡連線負載

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

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

當您使用多個 DNS 項目時、使用連線的要求是負載平衡的、如下所示：

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

連接埠需求

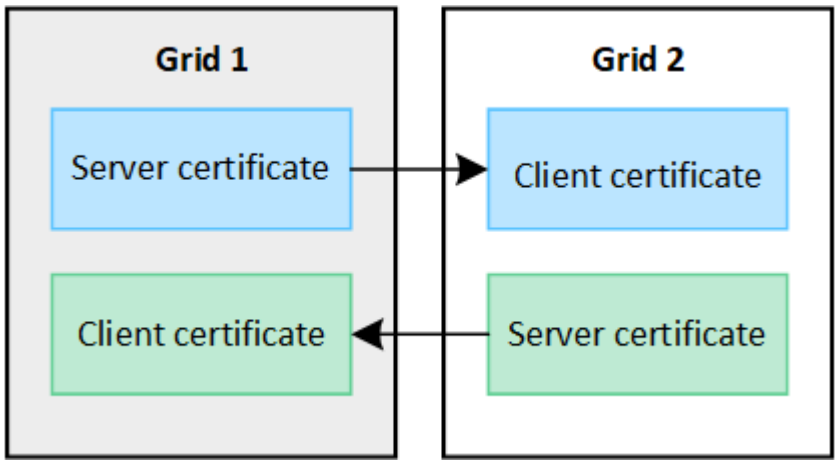
建立網格同盟連線時、您可以指定任何未使用的連接埠號碼、範圍從 23000 到 23999 。此連線中的兩個網格都會使用相同的連接埠。

您必須確保任一網格中的任何節點都不會使用此連接埠進行其他連線。

憑證需求

當您設定網格同盟連線時、 StorageGRID 會自動產生四個 SSL 憑證：

- 伺服器和用戶端憑證、用於驗證和加密從網格 1 傳送至網格 2 的資訊
- 伺服器和用戶端憑證、用於驗證和加密從網格 2 傳送至網格 1 的資訊



依預設、憑證的有效期限為 730 天（ 2 年）。當這些憑證接近到期日時、「 * 網格聯合憑證到期日 * 」警示會提醒您旋轉憑證、您可以使用 Grid Manager 來進行。

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

深入瞭解

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

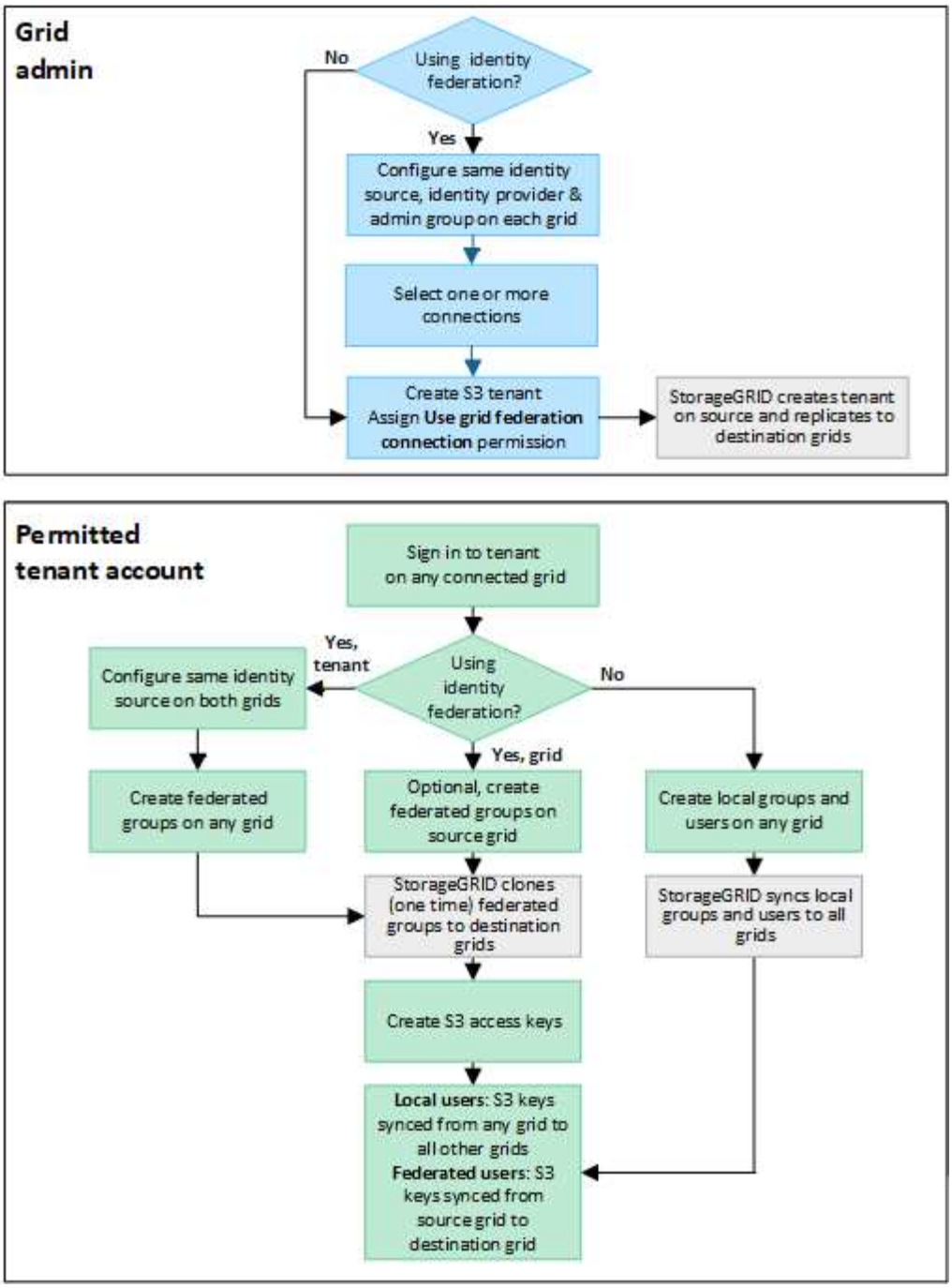
了解 **StorageGRID** 中的帳戶同步

帳戶同步是指在一個或多個 "網格同盟連線" 中的 StorageGRID 系統之間，自動且持續地複寫租戶帳戶、租戶群組、租戶使用者，以及（可選的）S3 存取金鑰。

帳戶同步是 "跨網格複寫" 所必需的。在 StorageGRID 系統之間同步帳戶資訊，可確保租戶使用者和群組能夠存取任何已連接網格上的對應儲存桶和物件。

帳戶同步工作流程

工作流程圖顯示了網格管理員和獲准租戶為設定帳戶同步而需要執行的步驟。這些步驟在 "已設定網格同盟連線" 之後執行。



Grid 管理工作流程

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

設定帳戶同步的單一登入（選用）

如果網格同盟連線中的任一 StorageGRID 系統使用 SSO 、則兩個網格都必須使用 SSO 。在建立網格同盟的租戶帳戶之前、租戶來源和目的地網格的網格管理員必須執行這些步驟。

步驟

1. 為兩個網格設定相同的身分識別來源。請參閱。 "使用身分識別聯盟"
2. 為兩個網格配置相同的 SSO 身分提供者 (IdP)。看"設定單一登入" 。

3. "建立相同的管理群組"在兩個網格上匯入相同的同盟群組。

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

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

設定帳戶同步的網格層級身分識別聯盟（選用）

如果任一 StorageGRID 系統使用無 SSO 的身分識別聯盟、則兩個網格都必須使用身分識別聯盟。在建立網格同盟的租戶帳戶之前、租戶來源和目的地網格的網格管理員必須執行這些步驟。

步驟

1. 為兩個網格設定相同的身分識別來源。請參閱。 "使用身分識別聯盟"
2. 或者、如果同盟群組在兩個網格上都有來源和目的地租戶帳戶的初始根存取權限"建立相同的管理群組"、請匯入相同的同盟群組。

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

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

建立允許的 **S3** 租戶帳戶

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

步驟

1. 決定要將哪個網格作為租戶帳戶同步作業的來源網格。

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

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

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

5. 選取特定的網格同盟連線。
6. 儲存新的或修改過的租戶。

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

   - 兩個租戶帳戶都具有相同的帳戶 ID 、名稱、儲存配額和指派的權限。
   - 如果您選擇讓某個聯合群組擁有租戶的 Root 存取權限，則該群組將被 Clone 到目的地租戶。但是，聯合群組和使用者不會進行持續同步。只會進行一次性 Clone。

- 如果您選擇本機使用者擁有租戶的 Root 存取權限，則該使用者將同步至目的地租戶。

如需詳細資訊，請參閱 "管理網格同盟的允許租戶"。

允許的租戶帳戶工作流程

將具有「使用網格聯合連線」權限的租戶複製到目的地網格後，獲得許可的租戶帳戶可以執行下列步驟來同步租戶群組、使用者和 S3 存取金鑰。

步驟

1. 在任何已連接的網格登入租戶帳戶。
2. 如果允許，請在來源租戶帳戶和目的地租戶帳戶上設定身分識別聯盟。
3. 在任何已連接的網格上建立群組和使用者。

   當在租戶上建立新群組或使用者時，StorageGRID 會自動將其同步到目的地租戶。

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

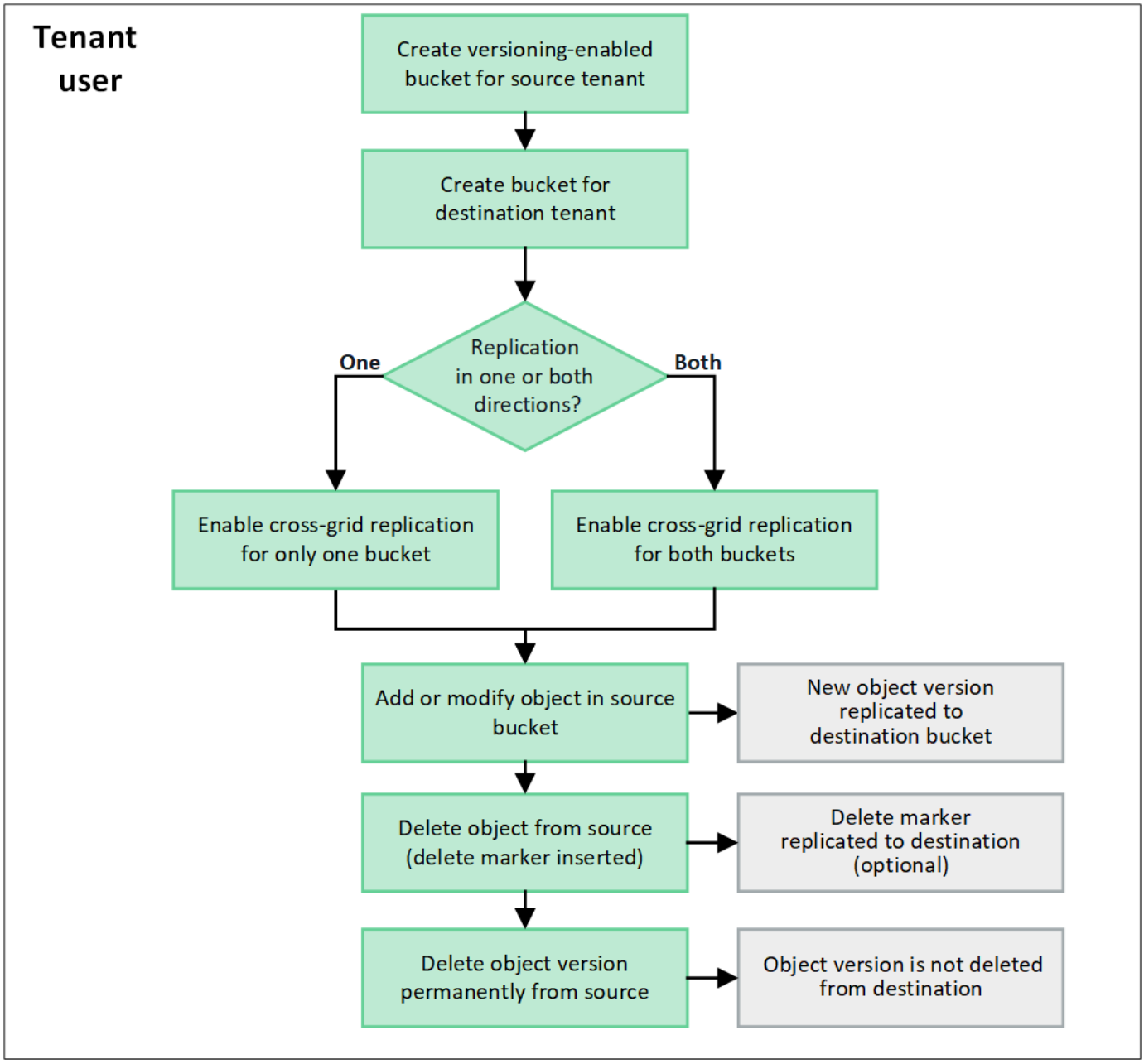
有關允許的租戶帳戶工作流程的詳細資訊，以及如何同步群組、使用者和 S3 存取金鑰，請參閱 "同步租戶群組和使用者"。

瞭解 **StorageGRID** 中的跨網格複寫

跨網格複寫是指在兩個以某種方式連接的 StorageGRID 系統中，在選定的 S3 儲存桶之間自動複寫物件"網格同盟連線"。"帳戶同步"跨網格複寫需要進行設定。

跨網格複寫的工作流程

工作流程圖總結了在兩個網格上的儲存桶之間配置跨網格複製的步驟。



跨網格複寫的需求

如果租戶帳戶擁有「使用網格聯合連線」權限，可使用一或多個 "網格同盟連線"，則具有根存取權限的租戶使用者可以在每個網格的對應租戶帳戶中建立儲存貯體（「來源」儲存貯體和「目的地」儲存貯體）。這些儲存貯體：

- 可以有不同的名稱
- 可以有不同的區域
- 必須啟用版本設定
- 必須採用下列其中一種 S3 物件鎖定組態：
  - 來源：已停用，目的地：已停用
  - 來源：已啟用，目的地：已啟用
  - 來源：已停用，目的地：已啟用

建立完兩個儲存桶後，您可以為其中一個或兩個儲存桶設定跨網格複寫。

深入瞭解

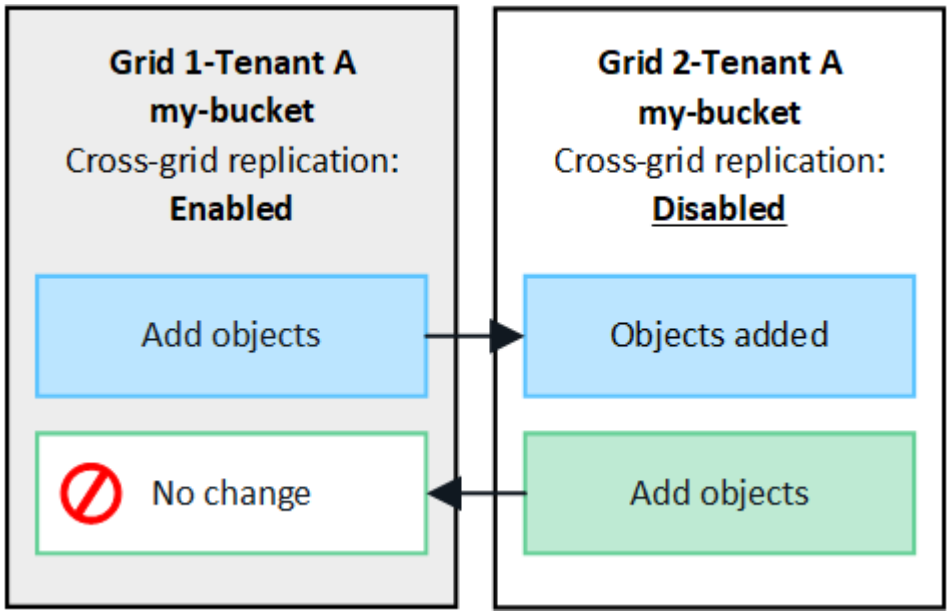
"管理跨網格複寫"

跨網格複寫的運作方式

您可以將跨網格複製配置為單向或雙向進行。

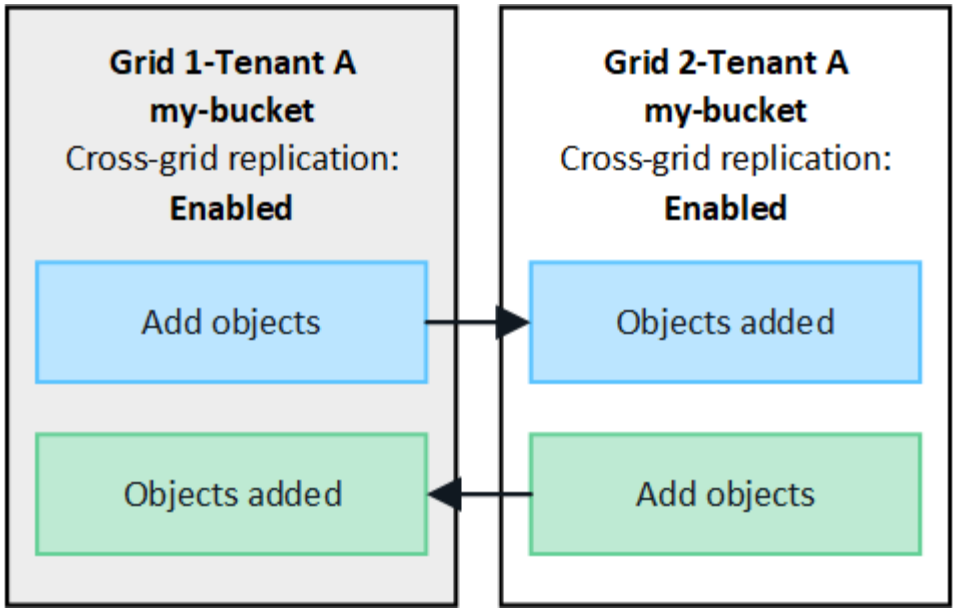
單向複寫

如果僅為一個網格上的儲存桶啟用跨網格複製，則新增至該儲存桶（來源儲存桶）的物件將複製到另一個網格上的對應儲存桶（目標儲存桶）。但是，新增到目標儲存桶的物件不會被複製回來源。圖中，啟用了跨網格複製 `my-bucket`從網格 1 到網格 2，但在另一個方向則無法啟用。



雙向複寫

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



擷取物件時會發生什麼情況？

當 S3 用戶端將物件新增至已啟用跨網格複寫的貯體時、會發生下列情況：

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

   S3 用戶端可以透過發出 GetObject 或 HeadObject 請求來驗證物件的複製狀態。響應包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status`響應頭，其值為以下之一：

網格	複寫狀態
來源	• * 已完成 * ：所有網格連線的複寫都成功。 • * 擱置 * ：物件尚未複寫至至少一個網格連線。 • 失敗：複製未等待任何電網連接，且至少有一個電網連接發生永久性故障。使用者必須解決該錯誤。
目的地	• 複本 * ：物件已從來源網格複寫。

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

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

刪除物件時會發生什麼情況？

如中所述"刪除資料流程"， StorageGRID 可以刪除物件，原因如下：

- S3 用戶端發出刪除要求。
- 租戶管理器使用者可選擇"刪除貯體中的物件"從貯體移除所有物件的選項。

- 貯體具有生命週期組態、已過期。
- ILM 規則中的物件最後一個時間週期結束、而且沒有指定其他放置位置。

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

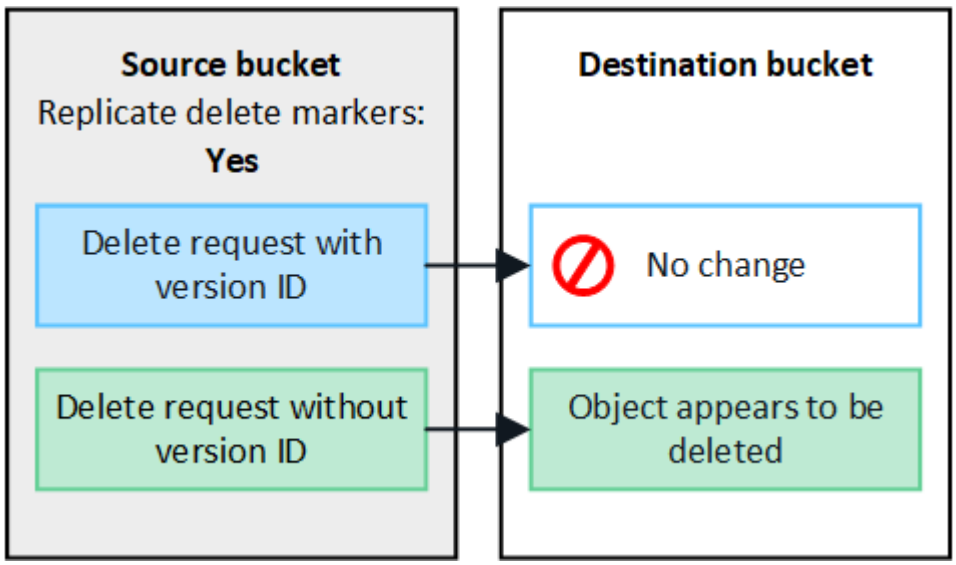
若要瞭解 S3 用戶端從已啟用跨網格複寫的儲存區刪除物件時會發生什麼情況、請檢閱 S3 用戶端如何從已啟用版本設定的儲存區刪除物件、如下所示：

- 如果 S3 用戶端發出包含版本 ID 的刪除要求、該版本的物件將會永久移除。貯體中不會新增刪除標記。
- 如果 S3 用戶端發出不包含版本 ID 的刪除請求， StorageGRID不會刪除任何物件版本。相反，它會向儲存桶添加一個刪除標記。刪除標記使StorageGRID表現得好像物件已被刪除：
  - 沒有版本 ID 的 GetObject 請求失敗，並顯示 `404 No Object Found`
  - 具有有效版本 ID 的 GetObject 請求成功並傳回請求的物件版本。

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

- 如果刪除請求包含版本 ID，則該物件版本將從來源網格中永久刪除。但是， StorageGRID不會複製包含版本 ID 的刪除請求，因此相同的物件版本不會從目標中刪除。
- 如果刪除請求不包含版本 ID， StorageGRID可以根據儲存桶的跨網格複製配置方式選擇性地複製刪除標記：
  - 如果您選擇複寫刪除標記（預設）、則會將刪除標記新增至來源貯體、並複寫至目的地貯體。實際上、這兩個網格上的物件似乎都會被刪除。
  - 如果您選擇不複製刪除標記，則刪除標記將新增至來源儲存桶，但不會複製到目標儲存桶。實際上，在來源網格上刪除的物件不會在目標網格上刪除。

在圖中，當"已啟用跨網格複寫"。包含版本 ID 的來源儲存桶的刪除請求不會從目標儲存桶中刪除物件。不包含版本 ID 的來源儲存桶的刪除請求似乎會刪除目標儲存桶中的物件。



如果您想要在網格之間保持物件刪除同步、請為兩個網格上的儲存格建立對應的物件刪除"S3 生命週期組態"。

加密物件的複寫方式

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

若要加密個別物件、您可以在將物件新增至來源貯體時、使用 SSE （伺服器端加密搭配 StorageGRID 託管金鑰）。使用 `x-amz-server-side-encryption`**請求標頭並指定** `AES256`。請參閱。 "使用伺服器端加密"

跨網格複製不支援使用 SSE-C（使用客戶提供的金鑰的伺服器端加密）。擷取操作將會失敗。

若要使用儲存庫的預設加密、請使用 PuttBucketEncryption 要求、並將參數設定 `SSEAlgorithm`**為** `AES256`。貯體層級加密適用於不含要求標頭的任何擷取物件 `x-amz-server-side-encryption`。請參閱。 "在貯體上作業"

若要使用網格層級加密、請將 * 儲存的物件加密 * 選項設定為 * AES-256* 。網格層級加密適用於任何未在儲存區層級加密、或是在沒有要求標頭的情況下擷取的物件 `x-amz-server-side-encryption`。請參閱。 "設定網路和物件選項"

SSE 不支援 AES-128。如果使用 **AES-128** 選項為來源網格啟用了 儲存物件加密 選項，則 AES-128 演算法的使用不會傳播到複製的物件。相反，複製的物件使用目標的預設儲存桶或網格級加密設定（如果可用）。

在決定如何加密來源物件時、 StorageGRID 會套用下列規則：

1. 使用 `x-amz-server-side-encryption`擷取標頭（如果有）。
2. 如果不存在擷取標頭，則使用儲存桶預設加密設定（如果已配置）。
3. 如果未配置儲存桶設置，則使用網格範圍的加密設定（如果已配置）。
4. 如果不存在網格範圍的設置，則不要加密來源物件。

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

1. 除非來源物件使用 AES-128 加密、否則請使用與來源物件相同的加密。
2. 如果來源物件未加密或使用 AES-128，則使用目標儲存桶的預設加密設定（如果已配置）。
3. 如果目標儲存桶沒有加密設置，則使用目標的網格範圍加密設定（如果已配置）。
4. 如果不存在網格範圍的設置，則不要加密目標物件。

使用 **S3** 物件鎖定進行跨網格複製

您可以在下列情況下配置啟用了 S3 物件鎖定的StorageGRID桶之間的跨網格複製。

當來源儲存桶上的 **S3** 物件鎖定是…	目標儲存桶上的 **S3** 物件鎖是…
已啟用	已啟用

當來源儲存桶上的 **S3** 物件鎖定是…	目標儲存桶上的 **S3** 物件鎖是…
已停用	已啟用

您可以對現有儲存桶啟用 S3 物件鎖定，這可能會導致日後發生組態錯誤。

如果在來源儲存桶上啟用了 S3 Object Lock，請確保在目的地儲存桶上也啟用了此功能。如果在目的地儲存桶上停用了 S3 Object Lock，則在複寫期間會發生錯誤。請參閱 "跨網格複寫警示和錯誤"。

當來源儲存桶上的 S3 物件鎖定啟用時：

- 物件按照以下順序在目標處使用保留設定進行鎖定：
  a. 來源物件的保留標頭值為：

     `x-amz-object-lock-mode`

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

  b. 來源儲存桶的預設保留（如果設定）。
  c. 目標儲存桶的預設保留（如果設定）。

  目標儲存桶的預設保留不會覆蓋從來源物件複製的保留設定。
- 您可以使用以下方式設定目標物件的合法保留狀態 `x-amz-object-lock-legal-hold`上傳對象時。
- 如果目標租用戶或儲存桶不支援來源物件的 S3 物件鎖定設置，則會發生錯誤。請參閱"跨網格複製警報和錯誤。"

當來源儲存桶上的 S3 物件鎖定已停用時：

- 您可以設定目標儲存桶上的預設保留，以將 S3 物件鎖定保留設定套用至目標物件。
- 目標物件無法設定合法保留狀態。

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

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

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

不支援 **PutObjectRetention** 和 **PutObjectLegalHold**

對於啟用了跨網格複製的儲存桶中的對象，PutObjectRetention 和 PutObjectLegalHold 請求不完全支援。

如果 S3 用戶端發出 PutObjectRetention 或 PutObjectLegalHold 請求，則會修改來源物件的設置，但變更不會套用到目標。

分割物件的複寫方式

來源網格的最大段大小適用於複製到目標網格的物件。當物件被複製到另一個網格時，兩個網格都會使用來源網格的*最大段大小*設定（配置 > 系統 > 儲存選項）。例如，假設來源網格的最大段大小為 1 GB，而目標網格的最大段大小為 50 MB。如果您在來源網格上提取一個 2 GB 的對象，則該對象將保存為兩個 1 GB 的段。它也會作為兩個 1 GB 的段複製到目標網格，儘管該網格的最大段大小為 50 MB。

比較 StorageGRID 中的跨網格複寫和 CloudMirror 複寫

開始使用網格同盟時，請檢閱與之間的相似點和差異"跨網格複寫""CloudMirror複寫服務StorageGRID"。

> 您不能在透過跨網格複製複製的儲存桶上使用 CloudMirror，反之亦然。

	跨網格複寫	**CloudMirror**複寫服務
主要目的為何？	一個 StorageGRID 系統可做為災難恢復系統。貯體中的物件可在網格之間以一個或兩個方向複寫。	可讓租戶自動將物件從 StorageGRID （來源）的貯體複寫到外部 S3 貯體（目的地）。 CloudMirror 複製在獨立的 S3 基礎架構中建立物件的獨立副本。此獨立副本不用作備份，但通常在雲端中進一步處理。
如何設定？	1. 設定兩個網格之間的網格同盟連線。 2. 新增租戶帳戶，這些帳戶會自動同步到另一個網格。 3. 新增新的租戶群組和使用者，這些內容也會同步更新。 4. 在每個網格上建立對應的儲存格、並可在一個或兩個方向進行跨網格複寫。	1. 租戶使用者使用租戶管理程式或S3 API定義CloudMirror端點（IP位址、認證等）來設定CloudMirror複寫。 2. 該租戶帳戶擁有的任何貯體都可以設定為指向 CloudMirror 端點。
誰負責設定？	• 網格管理員會設定連線和租戶。 • 租戶使用者可設定群組、使用者、金鑰和貯體。	一般而言、租戶使用者。
目的地為何？	網格聯合連線中其他 StorageGRID 系統上對應且相同的 S3 儲存貯體。	• 任何相容的 S3 基礎架構（包括 Amazon S3 ）。 • Google Cloud Platform（GCP）
是否需要物件版本設定？	是的、來源和目的地貯體都必須啟用物件版本設定。	否、 CloudMirror 複寫支援來源和目的地上的任何未版本控制和版本控制的貯體組合。
什麼原因會將物件移至目的地？	物件新增至已啟用跨網格複寫的儲存區時、會自動複寫。	將物件新增至已設定 CloudMirror 端點的儲存區時、物件會自動複寫。除非經過修改、否則不會複寫在使用 CloudMirror 端點設定儲存區之前存在於來源儲存區中的物件。

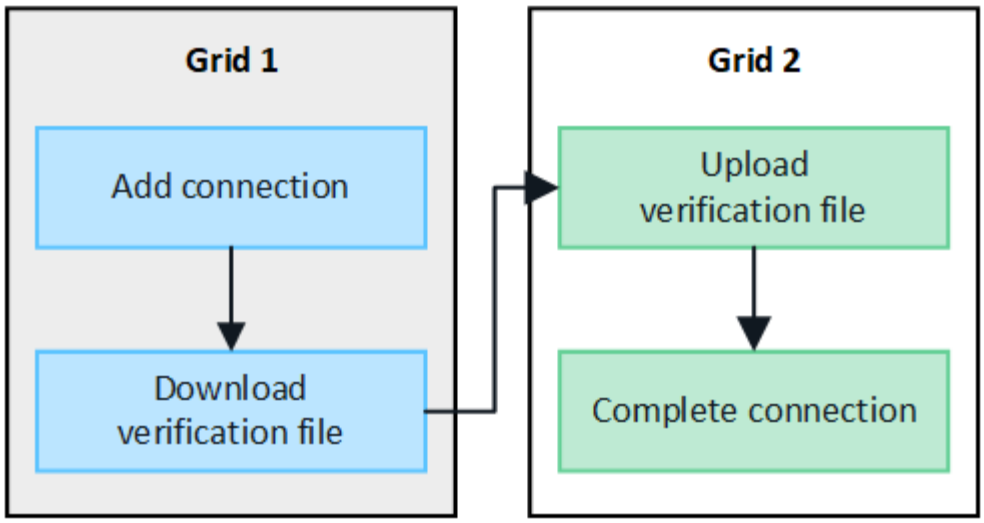
	跨網格複寫	**CloudMirror**複寫服務
物件如何複寫？	跨網格複寫會建立版本控制的物件、並將版本 ID 從來源貯體複寫到目的地貯體。如此一來、就能在兩個網格上維護版本順序。	CloudMirror 複寫不需要啟用版本控制的儲存區、因此 CloudMirror 只能維護網站內金鑰的訂購。對於不同站台的物件要求、我們無法保證會維持訂購。
如果物件無法複寫該怎麼辦？	物件會排入佇列進行複寫、但受中繼資料儲存限制規範。	物件會排入佇列進行複寫、但必須遵守平台服務限制（請參閱"使用平台服務的建議"）。
物件的系統中繼資料是否已複寫？	是的、當物件複寫到其他網格時、也會複寫其系統中繼資料。兩個網格上的中繼資料將相同。	否、當物件複寫到外部儲存區時、系統中繼資料會更新。中繼資料會因位置而異、視擷取時間和 S3 基礎架構的行為而定。
如何擷取物件？	應用程式可向任一網格上的儲存格提出要求、以擷取或讀取物件。	應用程式可以向 StorageGRID 或 S3 目的地提出要求、以擷取或讀取物件。例如、假設您使用CloudMirror複寫將物件鏡射到合作夥伴組織。合作夥伴可以使用自己的應用程式、直接從S3目的地讀取或更新物件。不需要使用此功能。StorageGRID
如果刪除物件會發生什麼情況？	• 包含版本 ID 的刪除要求絕不會複寫到目的地網格。 • 刪除不包含版本 ID 的要求、將刪除標記新增至來源貯體、可選擇性地複寫至目的地網格。 • 如果只針對一個方向設定跨網格複寫、則可刪除目的地儲存區中的物件、而不會影響來源。	結果會因來源和目的地儲存區的版本設定狀態而異（不需要相同）： • 如果兩個儲存區都已版本化、則刪除要求會在兩個位置新增刪除標記。 • 如果只有來源貯體已版本化、則刪除要求會將刪除標記新增至來源、但不會新增至目的地。 • 如果兩個貯體都沒有版本化、則刪除要求會從來源中刪除物件、而非從目的地刪除物件。 同樣地、也可以刪除目的地儲存區中的物件、而不會影響來源。

建立 **StorageGRID** 網格聯合連線

如果要同步租戶詳細資料和複寫物件資料，可以在 StorageGRID 系統之間建立網格聯合連接。

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

您也可以選擇"自動化建立、編輯及維護網格聯盟連線"。



開始之前

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

新增連線

在兩個 StorageGRID 系統中的任一系統上執行這些步驟。

步驟

1. 從任一網格上的主要管理節點登入 Grid Manager 。
2. 選擇*配置* > 系統 > 網格聯合。
3. 選取 * 新增連線 * 。
4. 輸入連線名稱，該名稱必須是唯一的，以便您識別此連線。例如， `Grid 1-Grid 2`。
5. 如果需要"設定全域命名空間"，請選擇 **Enable global namespace**。
6. 選擇*繼續*。
7. 輸入網格詳細資訊，如下所示：

欄位	說明
此網格的 FQDN 或 IP	下列其中一項： • 您目前登入之網格的 FQDN • 此網格上 HA 群組的 VIP 位址 • 此網格上管理節點或閘道節點的 IP 位址。IP 可以位於目的地網格所能到達的任何網路上。

欄位	說明
連接埠	您要用於此連線的連接埠。您可以輸入任何未使用的連接埠號碼、範圍從 23000 到 23999 。 此連線中的兩個網格都會使用相同的連接埠。您必須確保任一網格中的任何節點都不會使用此連接埠進行其他連線。
此網格的憑證有效天數	您希望此連線網格的安全性憑證有效的天數。預設值為 730 天（ 2 年）、但您可以輸入 1 至 762 天的任何值。 當您儲存連線時、 StorageGRID 會自動為每個網格產生用戶端和伺服器憑證。
此網格的資源配置複雜密碼	您已登入之網格的資源配置複雜密碼。
其他網格的 FQDN 或 IP	下列其中一項： • 您要連線的網格 FQDN • 其他網格上 HA 群組的 VIP 位址 • 另一個網格上管理節點或閘道節點的 IP 位址。IP 可以位於來源網格所能到達的任何網路上。

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

   在其他網格上完成連線後、您就無法再從任一網格下載驗證檔案。

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

   此檔案包含機密（以遮罩 *****）及其他敏感詳細資料、必須安全地儲存及傳輸。

4. 選取 * 關閉 * 以返回「 Grid Federation 」頁面。
5. 確認已顯示新連線、且其 * 連線狀態 * 為 * 正在等待連線 * 。
6. 將檔案提供 `*connection-name*.grid-federation`給網格管理員以供其他網格使用。

完整連線

在您要連線的 StorageGRID 系統（另一個網格）上執行這些步驟。

步驟

1. 從主要管理節點登入 Grid Manager 。
2. 選擇*配置* > 系統 > 網格聯合。
3. 選取 * 上傳驗證檔案 * 以存取「上傳」頁面。
4. 選取 * 上傳驗證檔案 * 。然後，瀏覽並選擇從第一個網格下載的文件(*connection-name*.grid-

federation）。

畫面會顯示連線的詳細資料。

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

   一般而言、在連線的兩端、使用相同天數的憑證。

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

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

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

   如果出現錯誤訊息、請解決任何問題。請參閱。 "疑難排解網格同盟錯誤"

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

   如果您編輯此連線、將會建立新的驗證檔案。原始檔案無法重複使用。

完成後

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

在 **StorageGRID** 中自動化網格聯盟連線

安裝並設定兩個或多個執行 12.1 或更高版本的 StorageGRID 系統後，您可以使用 `manage-grid-federation.py` Python 指令碼和 JSON 組態檔案自動化建立、編輯和維護網格聯合連線。

開始之前

- 所有網格均執行 StorageGRID 12.1 或更新版本。
- 如果任何網格上已啟用單一登入 （SSO），您已將其停用。
- 您的 Linux 機器上已安裝 Python 3.6 或更新版本。
- 您知道安裝封存中以下檔案的位置：

檔案名稱	說明
manage-grid-federation.py	用於自動化網格聯盟連線管理的 Python 指令碼
manage-grid-federation.sample.json	用於指令碼的組態檔範例

- 您已建立 `manage-grid-federation.json`組態檔案。若要建立此檔案，您可以修改範例組態檔案 `manage-grid-federation.sample.json`。

> 將網格管理員密碼和佈建密碼短語從您的 `manage-grid-federation.json`組態檔案儲存在安全的位置。如果檔案中缺少憑證，指令碼將以互動方式提示輸入。您還應該將修改後的組態檔案備份儲存在安全的位置。

組態檔案欄位

JSON 組態檔案是一個物件陣列。每個物件代表一個網格，並支援以下欄位：

欄位	必要	說明
主機名稱	是的	網格的管理節點主機名稱或 IP 位址
網格名稱	是的	網格的顯示名稱（最多 12 個字元）
使用者名稱	否	網格管理員使用者名稱（如果省略，則會以互動方式提示）
密碼	否	網格管理員密碼（如果省略，則會以互動方式提示）
口令	否	佈建複雜密碼（如果省略，則會以互動方式提示）
`ca_bundle`	否	用於 SSL 驗證的自訂 CA 憑證套裝組合的路徑
區域	否	全域命名空間連線的期望預設 S3 區域
`CNAME`	否	全域命名空間連線所需的 CNAME
`globalEndpoint`	否	所需的全域命名空間端點

> 如果您設定了任何全域命名空間欄位(`region` `CNAME` `globalEndpoint`），則必須為每個網格提供所有三個欄位。請確保區域和 CNAME 在所有網格中是唯一的，且 `globalEndpoint`值在所有網格中均相同。

關於這項工作

您可以使用 `manage-grid-federation.py` Python 指令碼和 `manage-grid-federation.json`組態檔案來自動化網格聯盟連線管理。該指令碼執行以下操作：

- 使用 Grid Management API 對每個網格進行驗證
- 驗證所有網格是否執行 StorageGRID 12.1 或更新版本。
- 驗證每個網格上的單一登入是否已停用
- 檢索現有網格聯盟連線和 S3 組態
- 設定完成後，更新 S3 區域、CNAME 和全域命名空間端點設定。
- 為尚未連接的網格對建立新的網格聯邦連線。

- 當顯示名稱或全域命名空間設定變更時，編輯現有連線
- 顯示所有連線及其狀態的摘要

您也可以使用 Grid Manager UI 或 Grid Management API 直接管理網格聯合連線。

步驟

1. 登入您用來執行Python指令碼的Linux機器。
2. 切換到包含指令碼的目錄。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 **platform** 為 `debs`、 `rpms`或 `vsphere`。

3. 執行Python指令碼並使用您建立的組態檔。

   例如：

   ```
   ./manage-grid-federation.py -i manage-grid-federation.json
   ```

   您可以使用以下命令列選項：

選項	預設	說明
`-i, --input-json-file`	（必需的）	包含網格清單的 JSON 組態檔案路徑
`-b, --base-port`	23001	新的網格聯邦連線的起始連接埠號
`--no-verify-ssl`	已啟用 SSL 驗證	停用本機對網格連線的 SSL 憑證驗證

編輯現有連線

如果指令碼偵測到現有連線需要變更（例如，網格顯示名稱已變更或全域命名空間設定需要更新），它將顯示建議的編輯執行摘要，並在繼續之前提示確認。

當需要在啟用了全域命名空間的網格上進行 S3 組態更新（(`region`、 `CNAME` 或 `globalEndpoint`）時，指令碼必須暫時停用全域命名空間才能套用變更。在這種情況下，確認提示將警告路由暫時中斷：

```
*** Global Namespace Disable Required ***
Global Namespace must be disabled to update region/CNAME/globalEndpoint
settings.
Routing requests will not work until Global Namespace is re-enabled.
Grids requiring S3 updates: grid1.example.com, grid2.example.com
Proceed with these edits and the temporary routing outage? [y/N]:
```

在 S3 組態更新期間，全域命名空間將暫時停用，全域命名空間路由請求將無法正常運作。請計劃在維護所需時間期間執行此操作。

完成後

當指令碼顯示類似以下內容的確認摘要時，表示您的網格聯盟連線已建立並設定完成：

```
===== Newly Established Connections =====
 • Grid-A and Grid-B — grid-a.example.com and grid-b.example.com on port
23001

Total new connections: 1

===== All Grid-Federation Connections =====
  Name               Source                Target                Port
Status    Global Namespace
  ----------------  --------------------  --------------------  -----
--------  ----------------
  Grid-A and Grid-B grid-a.example.com    grid-b.example.com    23001  new
enabled

Total connections listed: 1

===== Grid S3 Configuration Summary =====
 grid-a.example.com:
    Default Region: us-east-1
    CNAME: s3-a.example.com
    Global namespace endpoint: gn.example.com
 grid-b.example.com:
    Default Region: us-west-1
    CNAME: s3-b.example.com
    Global namespace endpoint: gn.example.com
```

退出狀態

程式碼	說明
0	指令碼已成功執行
1	驗證失敗或網格 API 呼叫傳回錯誤（請檢查日誌輸出）

如果任何連線失敗，指令碼將繼續處理剩餘的連線對，並將所有失敗情況報告在輸出的「失敗連線」部分。請查看錯誤訊息並解決任何問題，然後再重新執行指令碼。

了解網格聯邦的全域命名空間

全域命名空間允許租戶存取跨多個 StorageGRID 系統的儲存桶。在網格聯合連線上啟用全

域命名空間後，以全域命名空間端點為目標的 S3 CreateBucket 和 ListBuckets 請求可以傳送到任何網格的負載平衡器端點，並根據請求中的簽章區域自動路由到正確的網格。

什麼是全域命名空間？

全域命名空間允許租戶存取跨多個 StorageGRID 系統的儲存桶。在網格聯合連線上啟用全域命名空間後，以全域命名空間端點為目標的 S3 CreateBucket 和 ListBuckets 請求可以傳送到任何網格的負載平衡器端點，並根據請求中的簽章區域自動路由到正確的網格。

您應該設定 DNS 解析器，將儲存桶 URL 的 DNS 對應到特定的網格。如有需要，請諮詢您的網路管理員，以確保 DNS 解析器設定正確。請參閱 "設定 DNS 解析"。

StorageGRID 不會強制要求全域命名空間內的各個網格使用唯一的儲存桶名稱，因此同名儲存桶可能存在於不同的網格中。要求中的簽署區域用於確定哪個網格擁有該儲存桶並應接收該要求。

例如，如果網格 A 使用區域 `us-east-1`，網格 B 使用區域 `us-west-1`，傳送到任何具有該區域 `us-west-1`之網格的 CreateBucket 請求都會自動路由到網格 B。

如需網格聯盟的詳細資訊，請參閱 "什麼是網格同盟？"。

全域命名空間範例

網格 **1**

- 預設區域： `region-1`
- 預設 CNAME： `s3.region-1.company.com`
- 全域端點： `s3.company.com`

網格 **2**

- 預設區域： `region-2`
- 預設 CNAME： `s3.region-2.company.com`
- 全域端點： `s3.company.com`

網格 **3**

- 預設區域： `region-3`
- 預設 CNAME： `s3.region-3.company.com`
- 全域端點： `s3.company.com`

CreateBucket 和 **ListBuckets** 作業

如果您建立儲存貯體 (`bucket123`)，其具有簽署區域 `region-2` 且以全域端點 `s3.company.com` 為目標，則任何接收到此要求的網格都將在 Grid 2 上建立該儲存貯體。

儲存桶特定物件操作和通用物件操作

在指定網格上建立儲存桶後，您的 DNS 解析器會將儲存桶 URL 解析為儲存桶和網格 CNAME。

在 以上範例 中，DNS 解析器應將 `bucket123.s3.company.com` 解析為

`bucket123.s3.grid3.company.com`（儲存桶和網格的 CNAME）。換句話說，所有請求都直接傳送至該網格，無需額外的路由。

範例

`PutObject to bucket123.s3.company.com` 解析為 `bucket123.s3.grid3.company.com`

S3 與全域命名空間的行為

全域命名空間完全設定完成後，S3 將採取以下行為。

區域強制執行

除了 "建立庫位" 和 "列表桶" 之外，所有發送到全域命名空間端點的 S3 請求都要求 V4 驗證標頭中的簽署區域與網格的預設區域相符。

- 如果簽署區域不符，請求將遭拒，並顯示以下錯誤訊息：

```
An error occurred (AuthorizationHeaderMalformed) when calling the
<operation> operation: The authorization header is malformed; the region
'<signing-region>' is wrong; expecting '<grid-default-region>'
```

- 區域強制執行適用於網格上的所有儲存桶，包括在啟用全域命名空間之前建立的儲存桶。
- 區域限制僅適用於 V4 驗證請求。匿名請求和 V2 請求不受區域限制。

CreateBucket 路由

CreateBucket 發送到全域命名空間端點的請求(`s3.company.com`）可以導向至任何網格的負載平衡器端點。請求會自動路由到預設區域與請求中簽署區域相符的網格。

例如：

- 網格 A 有預設區域 `us-east-1`，網格 B 有預設區域 `us-west-1`。
- 用戶端傳送 CreateBucket 請求至 `s3.company.com`，並帶有簽署區域 `us-west-1`。
- 循環 DNS 將請求導向網格 A。
- 網格 A 將請求路由至網格 B。
- 儲存桶建立在網格 B 上。

CreateBucket 的其他考量事項：

- 該 `LocationConstraint`元素可以設定為網格的任何預設或非預設區域。這只會影響 `ILM` 原則，而不會影響建立儲存桶的網格（與 `AWS` 的行為不同 `us-east-1`）。
- 請求中的簽署區域決定哪個網格建立儲存桶（簽署區域必須與目標網格的預設區域相符）。
- 支援預簽章 V4 請求。
- 全域命名空間路由不支援匿名請求和 V2 請求。

ListBuckets 路由

ListBuckets 發送到全域命名空間端點的請求與 CreateBucket 請求的路由方式類似，使用簽章區域來確定正確的網格。

HEAD Bucket 和 ListBuckets 回應均不包含網格的預設區域。預設區域由簽署區域隱含，且簽署區域必須與網格的預設區域相符。

帳戶和存取金鑰管理

租用戶帳戶和 S3 存取金鑰可以透過 "帳戶同步" 在所有網格之間同步，但即使每個網格都有自己獨立的存取金鑰集，全域命名空間也同樣適用。如果使用獨立的存取金鑰，請確保 S3 用戶端在向每個網格發送請求時使用正確的存取金鑰。

接下來呢？

現在您已準備好"設定全域命名空間"。

設定網格聯邦的全域命名空間

設定全域命名空間，允許租戶存取多個 StorageGRID 系統中的儲存桶。

有關全域命名空間的詳細資訊，請參閱 "了解網格聯邦的全域命名空間"。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入每個網格上的 Grid Manager。
- 您擁有每個網格的 "root 存取權限"。
- 您已審核網格聯邦連線的 "考量與要求"。

配置全域命名空間的要求

- 全域命名空間中的所有網格必須具有網格聯合連接，且每對網格之間必須啟用全域命名空間。
- 單一全域命名空間中最多可包含 11 個網格（本機網格和 10 個遠端網格）。

> 10 個網格的限制受 StorageGRID 部署所支援的網格聯合連線總數上限所約束。連線總數限制適用於部署中的*所有*網格聯合連線，包括未啟用全域命名空間的連線，因此您必須確保完全連線的全域命名空間與任何其他網格聯合連線的總和不超過此整體限制。

- S3 用戶端必須使用簽署版本 4 (SigV4) 驗證。全域命名空間路由操作不支援匿名請求和簽署版本 2 請求。
  - 正常的簽名請求依照以下說明指定 "驗證要求：使用授權標頭（AWS Signature Version 4）"。
  - 預簽名請求的具體說明請見 "驗證請求：使用查詢參數（AWS Signature Version 4）"。

所需連線數

在全域命名空間中，每對網格都必須連接。所需的連接數取決於網格的數量：

網格數量	所需連線數
2	1
3	3
4	6
5	10
n	*n* × (*n* − 1) / 2

步驟 **1**：為每個網格設定唯一的預設區域

全域命名空間中的每個網格都必須有一個唯一的預設區域。預設區域用於識別擁有儲存桶的網格。

CreateBucket 和 ListBuckets 請求會根據此區域進行路由，所有其他請求必須與它們被傳送到的預設區域相符。

如需詳細資訊、請參閱 "配置 S3 區域"。

步驟

1. 在每個網格上"將預設區域設為唯一值"。例如，將 Grid A 設定為 `us-east-1`，將 Grid B 設定為 `us-west-1`。

> 您仍然可以使用非預設區域（透過 `LocationConstraint` 元素在 "CreateBucket 請求" 中設定），以供 ILM 原則使用。非預設區域不會在全域命名空間中的網格之間進行唯一性驗證。

2. 對全域命名空間中的每個網格重複上述步驟。每個網格必須具有不同的預設區域。
3. 視需要設定其他區域。

步驟 **2**：設定 **S3** 全域命名空間設定

在全域命名空間中的每個網格上，新增兩個 S3 端點網域名稱：

- 一個在所有網格上都相同的全域命名空間端點
- 網格的唯一 CNAME

您需要設定外部 DNS，以便全域命名空間端點解析至一個或多個網格，且唯一的 CNAME 端點解析至特定網格。

> 您必須設定預設區域才能設定 S3 全域命名空間設定。啟用全域命名空間設定後，如果 S3 請求未指定正確的區域，則請求將失敗。所有 S3 請求都需要使用網格的預設區域進行簽署。

步驟

1. 在每個網格中，選擇 組態 > 網路 > **S3** 端點網域名稱 > 網域名稱。
2. 新增一個在所有網格中都相同的全域命名空間端點網域名稱。例如： `s3.example.com`。

3. 為網格新增唯一的 CNAME。例如， `s3.company.com`。
4. 選擇*保存*。
5. 選擇 **Global namespace settings**。
   a. 選擇全域命名空間端點。
   b. 選擇網格的唯一 CNAME 網域名稱。
6. 選擇*保存*。
7. 確保用戶端使用的伺服器憑證包含新的 S3 端點網域名稱。
   - 如果用戶端連線到使用其本身憑證的負載平衡器端點，請參閱"更新與端點相關的憑證"。
   - 如果用戶端連線到使用全域 S3 API 憑證的負載平衡器端點、"更新全域 S3 API 憑證"或直接連線到 Storage Nodes 、。
8. 在全域命名空間中的每個網格上重複這些步驟。

如需詳細資訊，請參閱 "設定 S3 端點網域名稱"。

步驟 3：建立啟用全域命名空間的網格聯合連線

在所有網格上設定 S3 端點網域名稱和預設區域後，即可建立啟用全域命名空間的網格聯合連線。

關於這項工作

建立網格聯合連線並啟用全域命名空間時，全域命名空間端點、CNAME 和預設區域欄位將使用您在先前步驟中設定的值自動填入。如果這些欄位未正確設定，Grid Manager 將阻止啟用全域命名空間。

> 建立具有全域命名空間的網格聯合連線後，該連線中網格的全域命名空間端點、CNAME 和預設區域將無法變更。

步驟

1. 在第一個網格中，請按照 "建立網格同盟連線" 中所述的步驟進行操作。
2. 輸入連線詳細資料時，選取 **Enable global namespace**。

   全域命名空間端點、CNAME 和預設區域的欄位會自動填入您在先前步驟中設定的值。如果任何值缺失或無效，您將無法啟用全域命名空間，直到解決這些問題為止。
3. 下載驗證檔案並將其上傳到另一個網格，完成連接。
4. 對全域命名空間中的每一對網格重複上述步驟。

   例如，3 個網格需要 3 個連線（網格 A–網格 B、網格 A–網格 C、網格 B–網格 C）。4 個網格需要 6 個連線。一個全域命名空間中最多可以有 10 個網格。請參閱 所需連線數。

步驟 4：設定負載平衡器端點

"設定負載平衡器端點" 對於全域命名空間中的每個網格。請為每個端點使用相同的連接埠。

> 請確保在設定 DNS 解析之前設定負載平衡器端點。

步驟 **5**：設定 **DNS** 解析

StorageGRID 並沒有提供用於全域命名空間的內建 DNS 解析器。您必須設定外部 DNS 基礎架構，才能將 S3 請求路由到正確的網格。

您的 DNS 解析器應該：

1. 將全域命名空間端點（例如， `s3.example.com`）解析為一個或多個網格的負載平衡器端點，通常使用輪詢 DNS。
2. 將每個網格的唯一 CNAME（例如， `s3.grid-a.example.com`）解析為該特定網格的負載平衡器端點。
3. 對於虛擬託管風格的儲存桶請求（例如 *`bucket`*`.s3.example.com`），請使用您組織的路由原則將儲存桶名稱對應至適當網格的 CNAME。

   StorageGRID 不提供基於 DNS 的機制來決定儲存桶所屬的網格。如果您需要基於儲存桶所有權的自動路由，請使用 "租戶管理API" 發出 ListBucket 請求以傳回儲存桶的 UUID。維護從儲存桶 UUID 到網格的內部對應。您的外部 DNS 應使用此對應，而非直接查詢 StorageGRID。

相關資訊

- "什麼是網格同盟？"
- "建立網格同盟連線"
- "設定 S3 端點網域名稱"
- "管理網格同盟連線"

管理 **StorageGRID** 網格聯合連線

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

開始之前

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

[[edit_grid_fed_connection]] 編輯網格同盟連線

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

在編輯連線期間，帳戶同步或跨網格複寫請求將繼續使用現有的連線設定。您必須一次編輯一個連線，並為每個連線上傳一個驗證檔案到遠端網格。編輯內容將在上傳到遠端網格後生效。

開始編輯連線

步驟

1. 從任一網格上的主要管理節點登入 Grid Manager 。
2. 選擇*節點*並確認系統中的所有其他管理節點都在線上。

編輯網格同盟連線時、 StorageGRID 會嘗試在第一個網格上的所有管理節點上儲存「候選組態」檔案。如果無法將此檔案儲存至所有管理節點、當您選取 * 儲存並測試 * 時、會出現警告訊息。

3. 選擇*配置* > 系統 > 網格聯合。
4. 使用 Grid Federation 頁面上的 * Actions* 功能表或特定連線的詳細資料頁面、編輯連線詳細資料。請參閱"建立網格同盟連線"以瞭解要輸入的內容。

   「行動」功能表

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

   詳細資料頁面

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

5. 輸入您登入網格的資源配置密碼。
6. 選取 * 儲存並繼續 * 。

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

7. 選擇 * 下載驗證檔案 * 。

   若要稍後下載此檔案、請前往連線的詳細資料頁面。

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

   驗證檔案包含機密資料、必須安全地儲存及傳輸。

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

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

11. 將檔案提供 `*connection-name*.grid-federation`給網格管理員以供其他網格使用。

完成連線編輯

將驗證檔案上傳至其他網格、即可完成連線編輯。

步驟

1. 從主要管理節點登入 Grid Manager 。

2. 選擇*配置* > 系統 > 網格聯合。
3. 選取 * 上傳驗證檔案 * 以存取上傳頁面。
4. 選取 * 上傳驗證檔案 * 。然後、瀏覽並選取從第一個網格下載的檔案。
5. 輸入您目前登入網格的資源配置密碼。
6. 選取 * 儲存並測試 * 。

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

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

[[test_grid_fed_connection] 測試網格同盟連線

步驟

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

   「行動」功能表

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

   詳細資料頁面

   a. 選取連線名稱以顯示其詳細資料。
   b. 選擇*測試連線*。

4. 檢閱連線狀態：

連線狀態	說明
連線	兩個網格都已連線並正常通訊。
錯誤	連線處於錯誤狀態。例如、憑證已過期或組態值不再有效。
擱置編輯	您已編輯此網格上的連線、但連線仍在使用現有的組態。若要完成編輯、請將新的驗證檔案上傳至其他網格。
正在等待連線	您已在此網格上設定連線、但其他網格上的連線尚未完成。從這個網格下載驗證檔案、並將其上傳至其他網格。

連線狀態	說明
不明	連線處於未知狀態、可能是因為網路問題或離線節點。

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

旋轉連線憑證

每個網格同盟連線都會使用四個自動產生的 SSL 憑證來保護連線安全。當每個網格的兩個憑證接近到期日時、* 網格聯合憑證過期 * 警示會提醒您旋轉憑證。

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

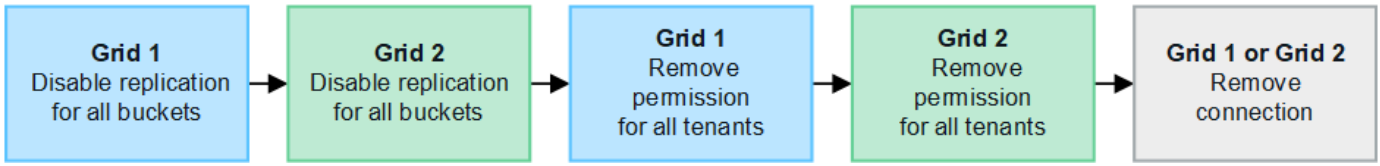
步驟

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

   一般而言、在連線的兩端、使用相同天數的憑證。

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

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



移除連線之前、請注意下列事項：

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

停用所有租戶貯體的複寫

步驟

1. 從任一網格開始、從主要管理節點登入 Grid Manager 。
2. 選擇*配置* > 系統 > 網格聯合。
3. 選取連線名稱以顯示其詳細資料。
4. 在 * 允許的租戶 * 標籤上、判斷是否有任何租戶正在使用連線。
5. 如果列出任何租戶、請指示所有租戶"停用跨網格複寫"在連線中的兩個網格上安裝所有貯體。

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

移除每個租戶的權限

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

步驟

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

移除連線

步驟

1. 當任一網格上沒有租戶正在使用連線時、請選取 * 移除 * 。
2. 檢閱確認訊息、然後選取 * 移除 * 。
   - 如果可以移除連線、就會顯示成功訊息。網格同盟連線現在已從兩個網格中移除。
   - 如果無法移除連線（例如、連線仍在使用中或發生連線錯誤）、則會顯示錯誤訊息。您可以執行下列其中一項：
     - 解決錯誤（建議）。請參閱。 "疑難排解網格同盟錯誤"
     - 強制移除連線。請參閱下一節。

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

如有必要、您可以強制移除狀態為 * 已連線 * 的連線。

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

步驟

1. 在確認對話方塊中、選取 * 強制移除 * 。

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

2. 從連線中的其他網格、從主要管理節點登入 Grid Manager 。

3. 選擇*配置* > 系統 > 網格聯合。
4. 選取連線名稱以顯示其詳細資料。
5. 選取 * 移除 * 和 * 是 * 。
6. 選取 * 強制移除 * 可移除此網格的連線。

管理 **StorageGRID** 網格聯盟的允許租戶

您可以允許 S3 租戶帳戶在多個 StorageGRID 系統之間使用一個或多個網格聯合連線。如果允許租戶使用某個連線，則需要執行特殊步驟才能編輯租戶詳細資料或永久移除租戶使用該連線的權限。

開始之前

- 您可以使用登入任一網格上的 Grid Manager "支援的網頁瀏覽器"。
- 您擁有已登入的"root 存取權限"網格。
- 您有"已建立網格同盟連線"兩個網格。
- 您已審核了 "帳戶同步" 和 "跨網格複寫" 的工作流程。
- 根據要求，您已為連線中的兩個網格設定了單一登入 (SSO) 或身分聯合。請參閱"了解網格聯盟的帳戶同步"。

建立允許的租戶

如果您希望允許新的或現有的租戶帳戶使用網格聯合連線進行帳戶同步和跨網格複寫，請按照一般說明 "建立新的 S3 租戶" 或 "編輯租戶帳戶"，並附註以下事項：

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

  本機根使用者必須先登入目的地網格上複寫的租用戶、該網格的網格管理員才能登入"變更本機 root 使用者的密碼"。

- 新的或編輯過的租用戶在兩個網格上都可用之後、租戶使用者就可以執行這些作業：
  - 從任何已連接的網格中建立群組和本機使用者，這些群組和本機使用者會自動同步到所有其他已連接的網格。請參閱"同步租戶群組和使用者"。
  - 為本機使用者建立新的 S3 存取金鑰，當為租戶啟用存取金鑰同步時，這些金鑰會自動同步到其他連線的網格。

    聯合使用者的 S3 存取金鑰在建立時會從來源 Clone 到目標一次。如果這些 S3 存取金鑰被刪除，這些變更不會同步到其他網格。您必須手動刪除其他網格上的 S3 存取金鑰。

- 在連線的兩個網格上建立相同的儲存格、並在單一方向或雙向啟用跨網格複寫。請參閱。 "管理跨網格複寫"

檢視允許的租戶

您可以查看允許使用網格同盟連線之租用戶的詳細資料。

步驟

1. 選擇*租戶*。
2. 從「租戶」頁面中、選取租戶名稱以檢視租戶詳細資料頁面。
3. （可選）選擇 **Grid federation** 索引標籤以 "監控網格聯盟連線"。

編輯允許的租戶

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

- 如果租戶擁有「使用網格聯合連線」權限：
- 您可以從連線中的任何網格編輯租戶詳細資訊。對租戶層級設定（例如名稱、執行摘要或配額）以及群組、本機使用者和本機使用者擁有的 S3 存取金鑰的變更會自動同步到所有已連線的網格。
- 您只能在來源網格上變更*允許的網格同盟連線*。
- 您可以新增網格聯邦連線。

> 您無法取消選擇任何現有連線。若要移除連線，請前往租戶的詳細資料頁面，選擇 **Grid federation** 索引標籤，然後移除權限。

- 如果在編輯租戶時新增連線，則該租戶將複寫到該新連線指定的遠端網格。

刪除允許的租戶

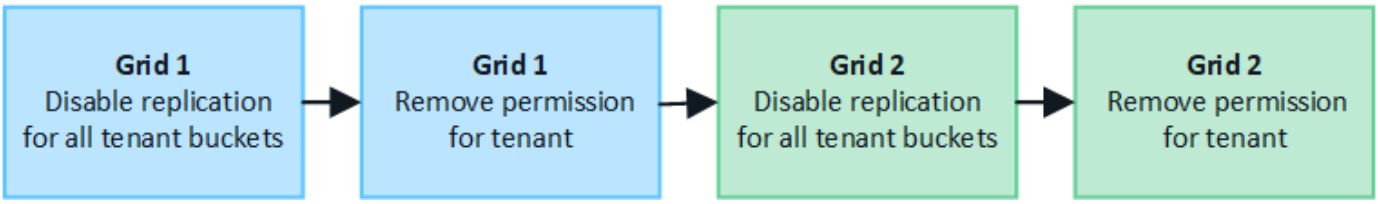
> 如果從來源網格中移除原始租戶或從目的地網格中移除同步租戶，則該租戶將從所有網格中移除，因此帳戶將無法再使用。

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

- 在來源網格中移除租戶之前，必須先從來源網格中移除該帳戶的所有儲存桶。
- 在目的地網格上移除已同步的租戶之前，必須先移除目的地網格上該帳戶的所有儲存桶。
- 如果移除原始租戶或同步租戶，則帳戶將無法再用於跨網格複寫。
- 如果您要移除來源或任何目的地網格上的原始租戶，則同步到目的地網格的租戶群組、使用者和金鑰也會一併移除。

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

若要防止租戶使用網格同盟連線、您必須移除 * 使用網格同盟連線 * 權限。



移除租戶使用網格同盟連線的權限之前、請注意下列事項：

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

重新啟用「使用網格聯合連接」權限後，本機網格將成為來源網格，並觸發與所選網格聯合連接指定的遠端網格的同步。如果租戶帳戶已存在於遠端網格中，則同步將導致衝突錯誤。

開始之前

- 您使用的是"支援的網頁瀏覽器"。
- 您有"root 存取權限"兩個網格的。

停用租戶貯體的複寫

第一步是停用所有租戶貯體的跨網格複寫。

步驟

1. 從任一網格開始、從主要管理節點登入 Grid Manager 。
2. 選擇*配置* > 系統 > 網格聯合。
3. 選取連線名稱以顯示其詳細資料。
4. 在 * 允許的租戶 * 索引標籤上、判斷租戶是否正在使用連線。
5. 如果列出租戶、請指示他們"停用跨網格複寫"在連線的兩個網格上使用所有的貯體。

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

移除租戶權限

停用租戶貯體的跨網格複寫之後、您可以移除租戶使用網格同盟連線的權限。

步驟

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

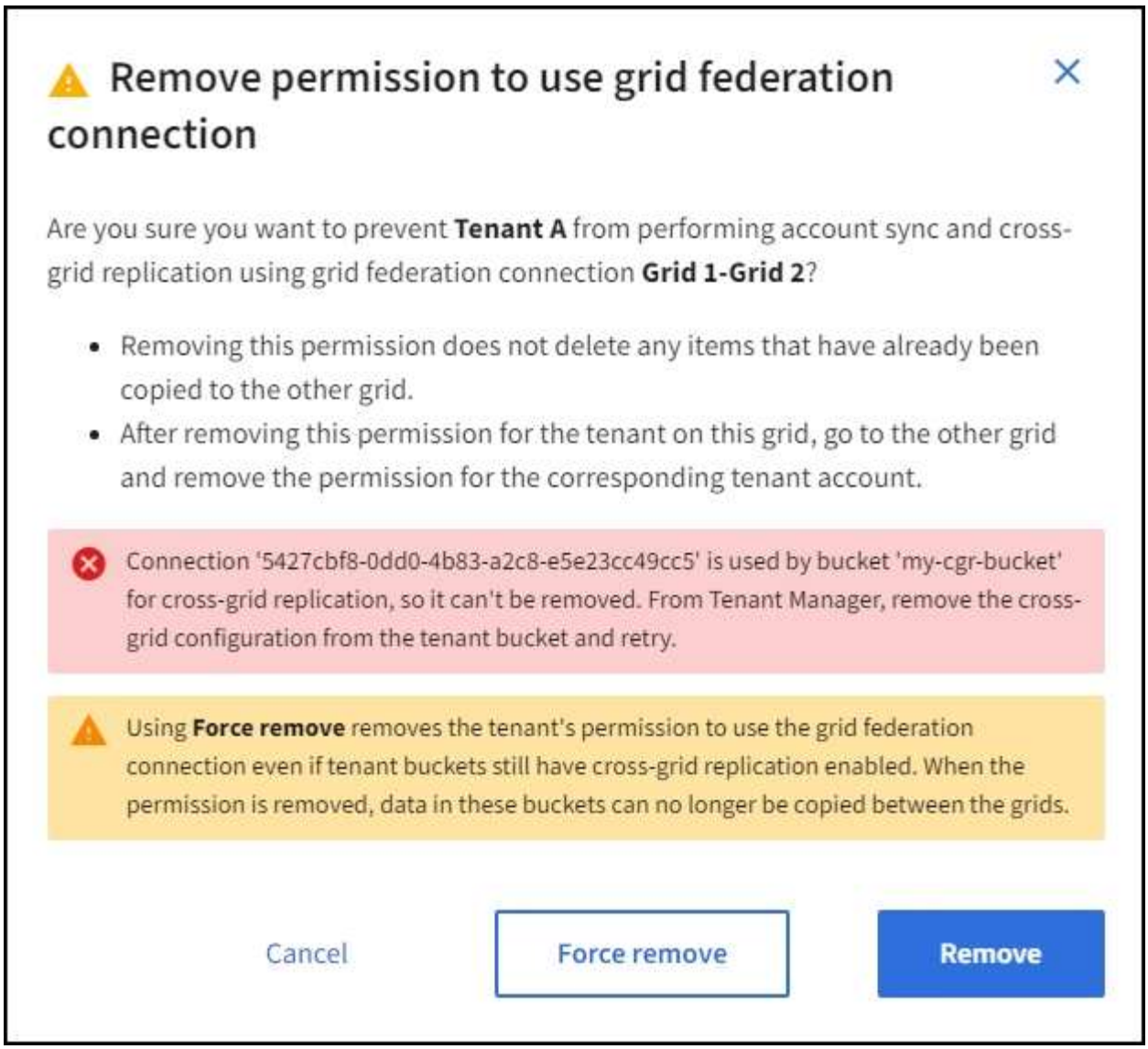
網格同盟頁面

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

租戶頁面

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

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



您可以執行下列其中一項：

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

4. 移至其他網格並重複這些步驟、以移除其他網格上相同租用戶的權限。

強制移除權限

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

在以強制方式移除租戶權限之前、請注意的一般考量事項移除權限以及下列其他考量事項：

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

步驟

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

   隨即顯示成功訊息。此租用戶無法再使用網格同盟連線。

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

排查 **StorageGRID** 中的網格聯合錯誤

您可能需要排查與網格聯合連線、帳戶同步和跨網格複寫相關的警報和錯誤。

[[grid-Federation 錯誤]] Grid 聯盟連線警示和錯誤

您可能會收到網格同盟連線的警示或錯誤。

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

Grid Federation 連線失敗警示

問題

觸發 * Grid Federation 連線失敗 * 警示。

詳細資料

此警示表示網格之間的網格同盟連線無法運作。

建議採取的行動

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

Grid Federation 憑證警示過期

問題

觸發了 * 網格聯合憑證過期 * 警示。

詳細資料

此警示表示一或多個網格同盟憑證即將過期。

建議採取的行動

請參閱中有關旋轉連線憑證"管理網格同盟連線"的說明。

編輯網格同盟連線時發生錯誤

問題

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

詳細資料

編輯網格同盟連線時、 StorageGRID 會嘗試在第一個網格上的所有管理節點上儲存「候選組態」檔案。如果無法將此檔案儲存至所有管理節點、例如管理節點離線、就會出現警告訊息。

建議採取的行動

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

帳戶同步錯誤

無法登入已同步的租戶帳戶

問題

您無法登入已同步的租戶帳戶。Tenant Manager 登入頁面上的錯誤訊息為「此帳戶的憑證無效。請重試。」

詳細資料

您為租戶的本機 root 使用者和其他本機使用者設定的密碼會自動同步。但是，您可能需要在目的地網格上變更租戶的本機 root 使用者密碼，才能登入該網格上的租戶帳戶。

建議採取的行動

根使用者必須先在目的地網格上登入租戶的目的地網格、然後才能登入租戶的目的地"變更本機 root 使用者的密碼"網格。

租戶建立時未進行同步

問題

使用 **Use grid federation connection** 權限建立新租戶後，您會看到訊息「Tenant created without a sync」。

詳細資料

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

建議採取的行動

1. 檢閱錯誤訊息中列出的原因、並解決可能導致連線無法正常運作的任何網路或其他問題。請參閱。 Grid Federation 連線警示和錯誤
2. 請依照中的指示測試網格同盟連線"管理網格同盟連線"、確認問題已解決。

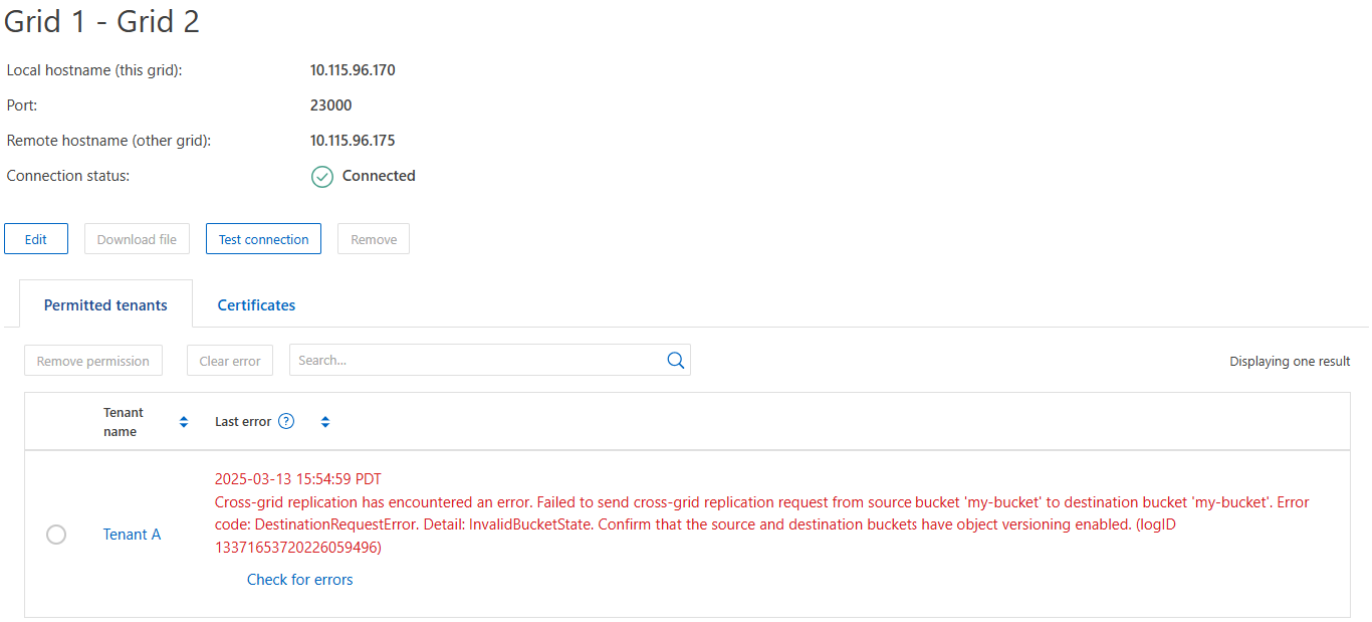
3. 從租戶的來源網格中，選擇*租戶*。
4. 找到同步失敗的租戶帳戶。
5. 選取租戶名稱以顯示詳細資料頁面。
6. 選取 **Retry sync**。如果錯誤已解決，租戶帳戶現在將同步到另一個網格。

跨網格複寫警示和錯誤

顯示連線或租戶的最後一個錯誤

問題

當"檢視網格同盟連線"（或連線時"管理允許的租戶"）您在連線詳細資料頁面的 * 最後一個錯誤 * 欄中發現錯誤。例如：



詳細資料

對於每個網格聯合連接，*最後一個錯誤*列顯示租戶資料複製到另一個網格時發生的最近錯誤（如果有）。此列僅顯示最後發生的跨網格複製錯誤；不會顯示可能發生的先前錯誤。此列中的錯誤可能由於以下原因之一而發生：

- 未找到來源物件版本。
- 未找到來源儲存桶。
- 目的地貯體已刪除。
- 目的地貯體是由不同的帳戶重新建立。
- 目的地貯體已暫停版本設定。
- 目的地貯體是由相同的帳戶重新建立、但現在已取消版本管理。
- 來源物件的 S3 物件鎖定設定不符合目標網格的租戶級保留設定。
- 來源物件具有 S3 物件鎖定設置，且目標儲存桶上的 S3 物件鎖定已停用。

建議採取的行動

如果在 * 最後一個錯誤 * 欄中出現錯誤訊息、請遵循下列步驟：

1. 檢閱訊息文字。
2. 執行所有建議的操作。

   例如，如果跨網格複寫的目的地儲存桶的版本控制功能被暫停，請重新啟用該儲存桶的版本控制功能。或者，如果跨網格複寫的目的地儲存桶的 S3 Object Lock 已停用，請啟用該儲存桶的 S3 Object Lock。

3. 從表格中選取連線或租戶帳戶。
4. 選取 * 清除錯誤 * 。
5. 選擇 * 是 * 以清除訊息並更新系統狀態。
6. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

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

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

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

跨網格複寫永久故障警示

問題

觸發 * 跨網格複寫永久失敗 * 警示。

詳細資料

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

建議採取的行動

1. 登入觸發警示的網格。
2. 前往*配置* > 系統 > 網格聯合，然後找到警報中列出的連接名稱。
3. 在「允許的租戶」標籤上、查看 * 最後一個錯誤 * 欄、以判斷哪些租戶帳戶有錯誤。
4. 若要深入瞭解故障、請參閱檢閱跨網格複寫計量的指示"監控網格同盟連線"。
5. 對於每個受影響的租戶帳戶：
   a. 請參閱中的指示"監控租戶活動"、確認租戶在跨網格複寫的目的地網格上並未超過配額。
   b. 視需要增加目標網格上的租戶配額、以允許儲存新物件。
6. 對於每個受影響的租戶、請在兩個網格上登入租戶管理器、以便比較貯體清單。
7. 針對已啟用跨網格複寫的每個貯體、請確認下列事項：
   - 另一個網格上有相同租戶的對應貯體（必須使用正確名稱）。
   - 兩個儲存格都已啟用物件版本設定（任一格線上都無法暫停版本設定）。
   - 兩個貯體都不處於 * 刪除物件：唯讀 * 狀態。

8. 若要確認問題是否已解決、請參閱中的指示"監控網格同盟連線"、以檢閱跨網格複寫指標、或執行下列步驟：

   a. 返回「 Grid Federation 」頁面。

   b. 選取受影響的租戶、然後在 * 上次錯誤 * 欄中選取 * 清除錯誤 * 。

   c. 選擇 * 是 * 以清除訊息並更新系統狀態。

   d. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

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

   警示解決後、可能需要一天的時間才能清除。

   a. 請移至"識別並重試失敗的複寫作業"以識別無法複寫到其他網格的任何物件或刪除標記、並視需要重試複寫。

跨網格複寫資源無法使用警示

問題

觸發 * 跨網格複寫資源 Unavailable * 警示。

詳細資料

此警示表示跨網格複寫要求因資源無法使用而擱置中。例如、可能發生網路錯誤。

建議採取的行動

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

問題解決後、跨網格複寫將會正常進行。

識別並重試失敗的 **StorageGRID** 複寫作業

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

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

判斷是否有任何物件無法複寫

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

您可以使用"稽核說明工具"將結果轉換成更容易閱讀的格式。

開始之前

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

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。

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

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

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

   此命令的結果將類似於此範例、其中包含六個 CGRR 訊息的項目。在範例中、所有跨網格複寫要求都會傳回一般錯誤、因為物件無法複寫。前三個錯誤是用於「複寫物件」作業、最後三個錯誤是用於「複寫刪除標記」作業。

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

每個項目都包含下列資訊：

欄位	說明
CGRR 跨網格複寫要求	要求的名稱
租戶	租戶的帳戶 ID
連線	網格同盟連線的 ID
營運	嘗試的複寫作業類型： • Replicate 物件 • 複寫刪除標記 • 複寫多個部分物件
鏟斗	貯體名稱
物件	物件名稱
版本	物件的版本 ID

欄位	說明
錯誤	錯誤類型。如果跨網格複寫失敗、則錯誤為「一般錯誤」。

重試失敗的複製

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

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

步驟

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

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

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

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

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

   請務必保留字串周圍的雙引號。

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

   擱置表示已將跨網格複寫要求新增至內部佇列以進行處理。

監控複寫重試次數

您應該監控複寫重試作業、以確保其完成。

物件或刪除標記複寫到另一個網格可能需要幾個小時或更久的時間。

您可以使用下列兩種方式來監控重試作業：

- 使用 S3 "標題物件" 或"GetObject"要求。回應包含 StorageGRID 專屬回應標頭、其中包含 `x-ntap-sg-cgr-replication-status`下列其中一個值：

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

- 如所述、使用 Grid Management 私有 API 。

步驟

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

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

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

管理安全性

在 **StorageGRID** 中管理安全性

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

管理加密

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

管理憑證

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

設定金鑰管理伺服器

使用"金鑰管理伺服器"可讓您保護 StorageGRID 資料、即使設備已從資料中心移除也沒問題。應用裝置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

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

管理**Proxy**設定

如果您使用的是 S3 平台服務或雲端儲存資源池、您可以在儲存節點和外部 S3 端點之間設定"儲存 Proxy 伺服器"。如果您使用 HTTPS 或 HTTP 傳送 AutoSupport 套件、您可以在管理節點和技術支援之間設定"管理 Proxy 伺服器"。

控制防火牆

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

檢閱**StorageGRID** 功能加密方法

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

下表提供StorageGRID 有關支援的加密方法的高階摘要。

加密選項	運作方式	適用於
Grid Manager中的金鑰管理伺服器（KMS）	"設定金鑰管理伺服器"適用於 StorageGRID 網站和 "啟用應用裝置的節點加密"的。然後、應用裝置節點會連線至KMS、以要求金鑰加密金鑰（KEK）。此金鑰會加密及解密每個Volume上的資料加密金鑰（DEK）。	安裝期間啟用*節點加密*的應用裝置節點。應用裝置上的所有資料都能受到保護、避免資料中心的實體遺失或移除。 • 注意 * ：使用 KMS 管理加密金鑰僅支援儲存節點和服務應用裝置。
StorageGRID 應用裝置安裝程式中的磁碟機加密頁面	如果應用裝置包含支援硬體加密的磁碟機、您可以在安裝期間設定磁碟機複雜密碼。當您設定磁碟機密碼時、除非任何人知道密碼短語、否則無法從已從系統移除的磁碟機中恢復有效資料。開始安裝之前、請移至 * 設定硬體 * > * 磁碟機加密 * 、設定適用於節點中所有 StorageGRID 管理的自我加密磁碟機的磁碟機密碼。	包含自我加密磁碟機的應用裝置。安全磁碟機上的所有資料都能受到保護、避免實體遺失或從資料中心移除。 磁碟機加密不適用於 SANtricity 管理的磁碟機。如果您的儲存設備具有自我加密磁碟機和 SANtricity 控制器、則可以在 SANtricity 中啟用磁碟機安全性。
在《支援資料保護系統》中提升安全性SANtricity	如果您的 StorageGRID 應用裝置已啟用磁碟機安全功能、您可以使用來 "系統管理程式SANtricity"建立及管理安全金鑰。存取受保護磁碟機上的資料需要金鑰。	具有全磁碟加密（ FDE ）磁碟機或自我加密磁碟機的儲存設備。安全磁碟機上的所有資料都能受到保護、避免實體遺失或從資料中心移除。無法與某些儲存設備或任何服務應用裝置搭配使用。
儲存的物件加密	您可以在 Grid Manager 中啟用"儲存的物件加密"選項。啟用時、在貯體層級或物件層級未加密的任何新物件、都會在擷取期間加密。	新擷取的 S3 物件資料。 現有儲存的物件不會加密。物件中繼資料和其他敏感資料不會加密。

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

使用多種加密方法

視您的需求而定、您一次可以使用多種加密方法。例如：

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

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

相關資訊

"了解 FIPS 認證的加密選項"

管理憑證

管理 **StorageGRID** 中的安全性憑證

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。

當客戶端使用 HTTPS 連接到伺服器時，伺服器會使用包含公鑰的伺服器憑證進行回應。用戶端將伺服器簽章與其憑證副本上的簽章進行比較。如果簽章匹配，客戶端將使用相同的公鑰與伺服器開始會話。

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

StorageGRID具有內建憑證授權單位 (CA)，可在系統安裝期間產生內部 Grid CA 憑證。預設情況下，使用 Grid CA 憑證來保護內部StorageGRID流量。外部憑證授權單位 (CA) 可以頒發完全符合您組織的資訊安全策略的自訂憑證。

在非生產環境中使用 Grid CA 憑證。對於生產，請使用由外部憑證授權單位簽署的自訂憑證。支援但沒有證書的不安全連接，但不建議。

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

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

伺服器和用戶端憑證類型的變種會以多種方式實作。在設定系統之前、您應該StorageGRID 準備好特定的支援

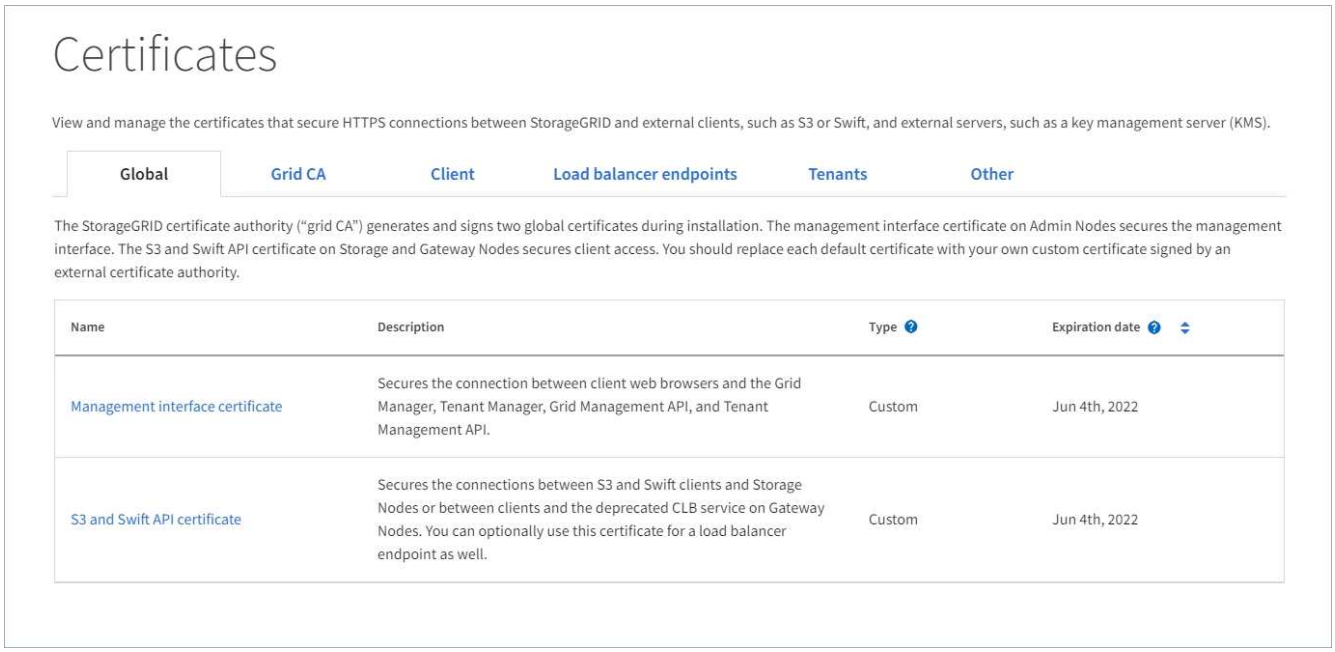
功能組態所需的所有憑證。

存取安全性憑證

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

步驟

1. 從網格管理員中，選擇*配置* > 安全性 > 證書。



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

   - 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 用戶端與 StorageGRID 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

全域憑證可保護從網頁瀏覽器和外部 S3 API 用戶端進行的 StorageGRID 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]：保護用戶端網頁瀏覽器連線至 StorageGRID 管理介面。
- S3 API 憑證：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 用戶端應用程式會使用這些節點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 API 憑證"用於儲存節點和負載平衡器端點（選用）連線。
- "還原預設的管理介面憑證"。
- "還原預設的 S3 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 API 憑證"。

網格**CA**

Grid CA憑證由 StorageGRID 憑證授權單位在 StorageGRID 安裝期間產生的、可保護所有內部 StorageGRID 流量。

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"、但無法變更。

用戶端

用戶端憑證由外部憑證授權單位所產生、可保護外部監控工具與 StorageGRID Prometheus 資料庫之間的連線。

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

負載平衡器端點

負載平衡器端點憑證保護 S3 用戶端與閘道節點和管理節點上 StorageGRID 負載平衡器服務之間的連線。

負載平衡器端點表會針對每個已設定的負載平衡器端點建立一列、並指出該端點是使用全域 S3 API 憑證還是自訂負載平衡器端點憑證。也會顯示每個憑證的到期日。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

您可以：

◦ "檢視負載平衡器端點"，包括其憑證詳細資料。

◦ "指定要FabricPool 使用的負載平衡器端點憑證。"

◦ "使用全域 S3 API 憑證"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保護自己與 StorageGRID 的連線。

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

您可以：

◦ "選取要登入租戶管理程式的租戶名稱"

◦ "選取租戶名稱以檢視租戶身分識別聯盟詳細資料"

◦ "選取租戶名稱以檢視租戶平台服務詳細資料"

◦ "在端點建立期間指定平台服務端點憑證"

其他

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

◦ 雲端儲存資源池認證

◦ 電子郵件警示通知憑證

◦ 外部syslog伺服器憑證

◦ 網格同盟連線憑證

◦ 身分識別聯盟憑證

- 金鑰管理伺服器（KMS）憑證
- 單一登入憑證

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

> 如果您有"適當的權限"，則只能檢視及存取其他憑證的資訊。

您可以：

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

安全性憑證詳細資料

每種安全性憑證類型如下所述、並提供實作指示的連結。

管理介面認證

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

S3 API 憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證安全的 S3 用戶端連線至儲存節點和負載平衡器端點（選用）。	設定 > 安全 > 憑證，選擇 全域 選項卡，然後選擇 **S3 API** 憑證	"設定 S3 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。	配置 > 安全性 > 憑證，然後選擇 用戶端 選項卡	"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 用戶端與閘道節點和管理節點上 StorageGRID 負載平衡器服務之間的連線。您可以在設定負載平衡器端點時上傳或產生負載平衡器憑證。用戶端應用程式在連線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。 您也可以使用自訂版本的通用S3 API 憑證憑證來驗證與負載平衡器服務的連線。如果使用全域憑證來驗證負載平衡器連線、您就不需要為每個負載平衡器端點上傳或產生個別的憑證。 *附註：*用於負載平衡器驗證的憑證、是正常StorageGRID 執行過程中最常使用的憑證。	配置 > 網路 > 負載平衡器端點	• "設定負載平衡器端點" • "建立FabricPool 負載平衡器端點以供使用"

雲端儲存資源池端點憑證

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

電子郵件警示通知憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證用於StorageGRID 警示通知的SMTP電子郵件伺服器與功能鏈之間的連線。 • 如果與SMTP伺服器的通訊需要傳輸層安全性（TLS）、您必須指定電子郵件伺服器CA憑證。 • 只有在SMTP電子郵件伺服器需要用戶端憑證進行驗證時、才指定用戶端憑證。	警報 > 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。	配置 > 監控 > 審計和系統日誌伺服器	"使用外部syslog伺服器"

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

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

身分識別聯盟憑證

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

金鑰管理伺服器（**KMS**）憑證

憑證類型	說明	導覽位置	詳細資料
伺服器與用戶端	驗證StorageGRID 支援功能與外部金鑰管理伺服器（KMS）之間的連線、此伺服器可為StorageGRID 應用裝置節點提供加密金鑰。	配置 > 安全 > 金鑰管理伺服器	"新增金鑰管理伺服器（KMS）"

平台服務端點憑證

憑證類型	說明	導覽位置	詳細資料
伺服器	驗證StorageGRID 從SReals功能 平台服務到S3儲存資源的連線。	租戶管理程式>*儲存設備（S3）>*平台服務端點	"建立平台服務端點" "編輯平台服務端點"

單一登入（**SSO**）憑證

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

憑證範例

範例**1**：負載平衡器服務

在此範例中StorageGRID 、用作伺服器的是功能。

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

2. 您可以設定 S3 用戶端連線至負載平衡器端點、並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. 用戶端將伺服器簽章與其憑證副本上的簽章進行比較。如果簽章匹配，客戶端將使用相同的公鑰開始會話。
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。

StorageGRID 中支援的伺服器憑證類型

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

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

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

在 **StorageGRID** 中設定管理介面憑證

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。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，會觸發*管理介面伺服器憑證過期*警報。根據需要，您可以透過選擇「設定」>「安全性」>「憑證」並查看「全域」標籤上管理介面憑證的到期日期來查看目前憑證的到期時間。

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。
- 從自訂管理介面憑證還原為預設伺服器憑證您。

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

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

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

     EC 私密金鑰必須大於 224 位元。RSA 私密金鑰必須大於 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。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

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

d. 選擇*保存*。+自訂管理介面憑證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：

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

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

c. 選取*產生*。

d. 選取*憑證詳細資料*以查看所產生憑證的中繼資料。

   ▪ 選取*下載憑證*以儲存憑證檔案。

   指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   ▪ 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。+自訂管理介面憑證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*設定* > 安全 > 憑證。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選擇*使用預設憑證*。

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

4. 重新整理頁面以確保網頁瀏覽器已更新。

使用指令碼來產生新的自我簽署管理介面憑證

如果需要嚴格的主機名稱驗證、您可以使用指令碼來產生管理介面憑證。

開始之前

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

關於這項工作

正式作業環境的最佳實務做法是使用外部憑證授權單位所簽署的憑證。

步驟

1. 取得每個管理節點的完整網域名稱（FQDN）。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 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-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 對於 `--domains`、請使用萬用字元來代表所有管理節點的完整網域名稱。例如 `*.ui.storagegrid.example.com`，使用 * 萬用字元來表示 `admin1.ui.storagegrid.example.com`和 `admin2.ui.storagegrid.example.com`。
   - 設 `--type`為 `management`可設定 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。

     憑證的有效期間從執行開始 `make-certificate`。您必須確保管理用戶端與StorageGRID 其他來源同步、否則用戶端可能會拒絕該憑證。

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

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

   在您的選擇中加入開始標記和結束標記。
5. 登出命令 Shell 。 `$ exit`

6. 確認已設定憑證：
   a. 存取Grid Manager。
   b. 選擇“配置”>“安全”>“證書”
   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*設定* > 安全 > 憑證。
2. 在* Global*索引標籤上、選取*管理介面認證*。
3. 選取「伺服器」或「* CA套裝組合*」索引標籤、然後下載或複製憑證。

   下載憑證檔案或**CA**套裝組合

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

   a. 選擇*下載憑證*或*下載CA套裝組合*。

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

   b. 指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

      例如： `storagegrid_certificate.pem`

   複製憑證或**CA**套裝組合**PEE**

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

   a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

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

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

      例如： `storagegrid_certificate.pem`

在 **StorageGRID** 中設定 **S3 API** 憑證

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

Swift 詳細資料已從此文件網站版本中移除。請參閱。 "StorageGRID 11.8 ：設定 S3 和 Swift API 憑證"

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後、您可能還需要在 S3 API 用戶端中安裝 Grid CA 憑證、以供存取系統、視您使用的根憑證授權單位（ CA ）而定。

為了確保操作不會因伺服器憑證失敗而中斷，當根伺服器憑證即將過期時，會觸發*S3 API 的全域伺服器憑證過期*警報。根據需要，您可以透過選擇「設定」>「安全性」>「憑證」並查看「全域」標籤上 S3 API 憑證的到期日來查看目前憑證的到期時間。

您可以上傳或產生自訂的 S3 API 憑證。

新增自訂的 **S3 API** 憑證

步驟

1. 選擇*設定* > 安全 > 憑證。
2. 在 * 全球 * 標籤上、選取 * S3 API 憑證 * 。
3. 選擇*使用自訂憑證*。
4. 上傳或產生憑證。

上傳憑證

上傳所需的伺服器憑證檔案。

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

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

     EC 私密金鑰必須大於 224 位元。RSA 私密金鑰必須大於 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、以顯示上傳的每個自訂 S3 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。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

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

d. 選擇*保存*。

   自訂伺服器憑證用於後續的新 S3 用戶端連線。

產生憑證

產生伺服器憑證檔案。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

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

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

c. 選取*產生*。

d. 選取 * 憑證詳細資料 * 以顯示產生之自訂 S3 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。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

- 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇*保存*。

自訂伺服器憑證用於後續的新 S3 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 API 憑證之後、 S3 API 憑證頁面會顯示使用中之自訂 S3 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 API** 憑證

您可以將 S3 用戶端連線至儲存節點的預設 S3 API 憑證還原為使用。不過、您無法將預設的 S3 API 憑證用於負載平衡器端點。

步驟

1. 選擇*設定* > 安全 > 憑證。
2. 在 * 全球 * 標籤上、選取 * S3 API 憑證 * 。
3. 選擇*使用預設憑證*。

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

4. 選取 * 確定 * 以確認警告並還原預設的 S3 API 憑證。

如果您具有根存取權限、且已將自訂 S3 API 憑證用於負載平衡器端點連線、則會顯示負載平衡器端點的清單、無法再使用預設的 S3 API 憑證來存取這些端點。移至"設定負載平衡器端點"以編輯或移除受影響的端點。

5. 重新整理頁面以確保網頁瀏覽器已更新。

下載或複製 S3 API 憑證

您可以儲存或複製 S3 API 憑證內容、以便在其他地方使用。

步驟

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

下載憑證檔案或CA套裝組合

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

a. 選擇*下載憑證*或*下載CA套裝組合*。

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

b. 指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證或CA套裝組合PEE

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

a. 選擇*複製憑證PEP*或*複製CA套裝組合PEP*。

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

b. 將複製的憑證貼到文字編輯器中。

c. 使用副檔名儲存文字檔 `.pem`。

   例如： `storagegrid_certificate.pem`

相關資訊

- "使用S3 REST API"
- "設定 S3 端點網域名稱"

複製 StorageGRID Grid CA 憑證

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

開始之前

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

關於這項工作

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

步驟

1. 選擇 配置 > 安全性 > 憑證，然後選擇 **Grid CA** 標籤。
2. 在 * 憑證 PEM* 區段中、下載或複製憑證。

下載憑證檔案

下載憑證 `.pem`檔案。

a. 選擇*下載憑證*。

b. 指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

複製憑證**PE**

複製憑證文字以貼到其他位置。

a. 選擇*複製憑證PEP*。

b. 將複製的憑證貼到文字編輯器中。

c. 使用副檔名儲存文字檔 `.pem`。

例如： `storagegrid_certificate.pem`

設定StorageGRID 適用FabricPool 的驗證

對於執行嚴格主機名稱驗證且不支援停用嚴格主機名稱驗證的 S3 用戶端、例如使用 FabricPool 的 ONTAP 用戶端、您可以在設定負載平衡器端點時產生或上傳伺服器憑證。

開始之前

- 您有 "特定存取權限"。
- 您已使用登入 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。如需更多詳細資訊與程序"設定StorageGRID 適用於FabricPool 靜態的"、請參閱。

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。

在 **StorageGRID** 中設定用戶端憑證

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

如果您需要StorageGRID 使用外部監控工具存取功能、則必須使用Grid Manager上傳或產生用戶端憑證、並將憑證資訊複製到外部工具。

請參閱"管理安全性憑證"和"設定自訂伺服器憑證"。

為了確保操作不會因伺服器憑證失敗而中斷，當此伺服器憑證即將過期時，將觸發*憑證頁面上配置的用戶端憑證過期*警報。根據需要，您可以透過選擇「設定」>「安全」>「憑證」並查看「用戶端」標籤上用戶端憑證的到期日來查看目前憑證的到期時間。

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

開始之前

- 您擁有root存取權限。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 若要設定用戶端憑證：
  - 您擁有管理節點的IP位址或網域名稱。
  - 如果您已設定StorageGRID 完整套管理介面認證、則會使用CA、用戶端認證和私密金鑰來設定管理介面認證。
  - 若要上傳您自己的憑證、您可以在本機電腦上取得該憑證的私密金鑰。
  - 私密金鑰必須在建立時已儲存或記錄。如果您沒有原始的私密金鑰、則必須建立新的私密金鑰。

- 若要編輯用戶端憑證：
  - 您擁有管理節點的IP位址或網域名稱。
  - 若要上傳您自己的憑證或新的憑證、您的本機電腦上可以使用私密金鑰、用戶端憑證和CA（如果使用）。

新增用戶端憑證

若要新增用戶端憑證、請使用下列其中一個程序：

- [管理介面憑證已設定]
- CA發行的用戶端憑證
- 從Grid Manager產生憑證

管理介面憑證已設定

如果已使用客戶提供的CA、用戶端憑證和私密金鑰來設定管理介面憑證、請使用此程序來新增用戶端憑證。

步驟

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

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

CA發行的用戶端憑證

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

步驟

1. 執行步驟至"設定管理介面憑證"。
2. 在網格管理員中，選擇*配置* > 安全性 > 憑證，然後選擇*客戶端*選項卡。
3. 選取*「Add*」。

4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*。
7. 對於 * 附加憑證 * 步驟、請上傳用戶端憑證、私密金鑰和 CA 套裝組合檔案：
   a. 選擇*上傳憑證*。
   b. 選擇 * 瀏覽 * 並選擇用戶端憑證、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。
8. 設定外部監控工具例如 Grafana 。

從**Grid Manager**產生憑證

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

步驟

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

     這些延伸定義了憑證中所含金鑰的用途。

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

   關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

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

  指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

  例如： `storagegrid_certificate.pem`

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

  指定私密金鑰檔案名稱和下載位置。

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

    新的憑證會顯示在「用戶端」索引標籤上。

11. 在網格管理員中，選擇*配置* > 安全性 > 憑證，然後選擇*全域*選項卡。
12. 選擇*管理介面認證*。
13. 選擇*使用自訂憑證*。
14. 從步驟中上傳 certificate .pem 和 private _key.pem 檔案用戶端憑證詳細資料。不需要上傳CA套裝組合。
    a. 選擇*上傳認證*、然後選擇*繼續*。
    b. 上傳每個憑證檔案(`.pem`）。
    c. 選取*「儲存*」、將憑證儲存在Grid Manager中。

       新的憑證會出現在管理介面憑證頁面上。

15. 設定外部監控工具例如 Grafana 。

設定外部監控工具

步驟

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

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

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

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

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

e. 伺服器名稱：輸入管理節點的網域名稱。

伺服器名稱必須符合管理介面憑證中顯示的網域名稱。

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

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

如需有關度量的資訊、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“設定”>“安全”>“憑證”，然後選擇“用戶端”標籤。

下表列出憑證到期日和Prometheus存取權限。如果憑證即將到期或已過期、表格中會出現訊息、並觸發警示。

2. 選取您要編輯的憑證。
3. 選取*編輯*、然後選取*編輯名稱和權限*
4. 輸入憑證名稱。
5. 若要使用您的外部監控工具存取 Prometheus* 指標、請選取 * 允許 Prometheus* 。
6. 選擇*繼續*以在Grid Manager中儲存憑證。

更新的憑證會顯示在「用戶端」索引標籤上。

附加新的用戶端憑證

您可以在目前的憑證過期時上傳新的憑證。

步驟

1. 選擇“設定”>“安全”>“憑證”，然後選擇“用戶端”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。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

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

   更新的憑證會顯示在「用戶端」索引標籤上。

產生憑證

產生要貼到其他位置的憑證文字。

a. 選擇*產生憑證*。

b. 指定憑證資訊：

   - * 主旨 *（選用）：憑證擁有者的 X.509 主體或辨別名稱（ DN ）。
   - * 有效天數 * ：產生的憑證自產生之日起有效的天數。
   - * 新增金鑰使用方式延伸 * ：如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸功能會新增至產生的憑證。

     這些延伸定義了憑證中所含金鑰的用途。

     除非您在憑證包含這些副檔名時、遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取*用戶端憑證詳細資料*以顯示憑證中繼資料和憑證PEE。

   關閉對話方塊後、您將無法檢視憑證私密金鑰。將金鑰複製或下載到安全位置。

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

     指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

例如： `storagegrid_certificate.pem`

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

  指定私密金鑰檔案名稱和下載位置。

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

新的憑證會顯示在「用戶端」索引標籤上。

下載或複製用戶端憑證

您可以下載或複製用戶端憑證、以便在其他地方使用。

步驟

1. 選擇“設定”>“安全”>“憑證”，然後選擇“用戶端”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。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

複製憑證

複製憑證文字以貼到其他位置。

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

   例如： `storagegrid_certificate.pem`

移除用戶端憑證

如果不再需要系統管理員用戶端憑證、您可以將其移除。

步驟

1. 選擇“設定”>“安全”>“憑證”，然後選擇“用戶端”標籤。

2. 選取您要移除的憑證。
3. 選擇*刪除*、然後確認。

> 若要移除最多10個憑證、請在「用戶端」索引標籤上選取要移除的每個憑證、然後選取*「動作」>「刪除」*。

移除憑證後、使用該憑證的用戶端必須指定新的用戶端憑證、才能存取StorageGRID 《The動ePrometheus資料庫》。

設定安全性設定

管理 StorageGRID 中的 TLS 和 SSH 原則

TLS 和 SSH 原則決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性原則控制 TLS 和 SSH 如何加密移動中的資料。一般而言、請使用現代化相容性（預設）原則、除非您的系統需要符合一般準則、或您需要使用其他密碼。

> 某些 StorageGRID 服務尚未更新、無法在這些原則中使用密碼。

開始之前

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

選取安全性原則

步驟

1. 選擇*配置* > 安全 > 安全設定。

   「 *TLS 與 SSH 原則 * 」標籤會顯示可用的原則。目前作用中的原則會在原則方塊上以綠色核取記號表示。

2. 查看標籤以了解可用的策略。

現代化相容性（預設）

如果您需要強加密且沒有特殊要求，請使用預設策略。此策略與大多數 TLS 和 SSH 用戶端相容。

舊版相容性

如果您需要為舊用戶端提供額外的相容性選項，請使用舊版相容性原則。此策略中的附加選項可能會使其安全性低於現代相容性策略。

一般準則

如果您需要通用標準認證，請使用通用標準政策。

FIPS 嚴格

如果您需要通用準則（Common Criteria）認證，且需要使用 NetApp Cryptographic Security Module (NCSM) 3.1.2 或 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模組來進行與負載平衡器端點、租戶管理員和網格管理員的外部用戶端連線，請使用 FIPS 嚴格原則。使用此原則可能會降低效能。

NCSM 3.1.2 和 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模組用於下列操作：

- 全國運動醫學委員會
  - 以下服務之間的 TLS 連線：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api、nginx、nginx-gw 和 cache-svc
  - 用戶端和 nginx-gw 服務（負載平衡器端點）之間的 TLS 連接
  - 用戶端和 LDR 服務之間的 TLS 連接
  - SSE-S3、SSE-C 和儲存物件加密設定的物件內容加密
  - SSH 連線

  如需更多資訊，請參閱 NIST Cryptographic Algorithm Validation Program "憑證 #A7816"。

- NetApp StorageGRID核心加密 API 模組

  NetApp StorageGRID Kernel Crypto API 模組僅存在於 VM 和StorageGRID設備平台上。

  - 熵收集
  - 節點加密

    注意：本模組尚未提交認證。

  如需更多資訊，請參閱 NIST Cryptographic Algorithm Validation Program "熵證書#E223"。

注意：選擇此政策後，"執行滾動重啟"所有節點均啟動 NCSM。使用*維護* > *滾動重新啟動*來啟動和監控重新啟動。

自訂

如果您需要套用自己的密碼、請建立自訂原則。

如果您的 StorageGRID 具有 FIPS 140 密碼編譯需求，則可選擇啟用 FIPS 模式功能，以使用 NCSM 3.1.2 和 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模組：

a. 設定 `fipsMode`參數 `true`。

b. 當出現提示時，"執行滾動重啟"所有節點都啟動加密模組。使用*維護* > *滾動重新啟動*來啟動和監控重新啟動。

c. 選擇「支援」>「診斷」以查看活動的 FIPS 模組版本。

3. 若要查看每個原則的密碼、通訊協定和演算法的詳細資料、請選取 * 檢視詳細資料 * 。
4. 若要變更目前的原則、請選取 * 使用原則 * 。

   原則方塊上的 * 目前原則 * 旁會出現綠色核取記號。

建立自訂安全性原則

如果您需要套用自己的密碼、可以建立自訂原則。

步驟

1. 從最類似您要建立之自訂原則的原則方塊中、選取 * 檢視詳細資料 * 。
2. 選取 * 複製到剪貼簿 * 、然後選取 * 取消 * 。

3. 從 * 自訂原則 * 方塊中、選取 * 設定與使用 * 。
4. 貼上您複製的 JSON 、然後進行任何必要的變更。
5. 選取 * 使用原則 * 。

   「自訂原則」方塊的 * 目前原則 * 旁會出現綠色核取記號。

6. 您也可以選擇 * 編輯組態 * 來對新的自訂原則進行更多變更。

暫時恢復為預設的安全性原則

如果您設定了自訂安全性原則、如果設定的 TLS 原則與不相容"已設定的伺服器憑證"、您可能無法登入 Grid Manager 。

您可以暫時還原為預設的安全性原則。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 執行下列命令：

   ```
   restore-default-cipher-configurations
   ```
3. 從網頁瀏覽器存取同一個管理節點上的Grid Manager。
4. 請依照中的步驟選取安全性原則重新設定原則。

設定 **StorageGRID** 網路和物件安全

您可以設定網路和物件安全性來加密儲存的物件、防止某些 S3 要求、或允許用戶端連線至儲存節點使用 HTTP 而非 HTTPS 。

儲存的物件加密

儲存的物件加密可在透過 S3 擷取時、加密所有物件資料。根據預設、儲存的物件不會加密、但您可以選擇使用 AES - 128 或 AES - 256 加密演算法來加密物件。啟用此設定時、所有新擷取的物件都會加密、但不會對現有的儲存物件進行任何變更。如果停用加密、目前加密的物件仍會保持加密狀態、但新擷取的物件不會加密。

「儲存的物件加密」設定僅適用於未透過貯體層級或物件層級加密進行加密的 S3 物件。

如需 StorageGRID 加密方法的詳細資訊，請參閱"檢閱StorageGRID 功能加密方法"。

防止用戶端修改

防止用戶端修改是全系統的設定。當選擇 * 防止用戶端修改 * 選項時、會拒絕下列要求。

S3 REST API

- 刪除 Bucket 要求
- 任何修改現有物件資料、使用者定義中繼資料或S3物件標記的要求

啟用 **HTTP** 以進行儲存節點連線

根據預設、用戶端應用程式會使用 HTTPS 網路傳輸協定來直接連線至儲存節點。您可以選擇性地為這些連線啟用HTTP、例如在測試非正式作業網格時。

僅當 S3 用戶端需要直接與儲存節點建立 HTTP 連線時、才可使用 HTTP 進行儲存節點連線。您不需要將此選

項用於僅使用 HTTPS 連線的用戶端或連線到負載平衡器服務的用戶端（因為您可以"設定每個負載平衡器端點"使用 HTTP 或 HTTPS ）。

請參閱"摘要：用於用戶端連線的IP位址和連接埠"以瞭解 S3 用戶端在使用 HTTP 或 HTTPS 連線至儲存節點時所使用的連接埠。

選取選項

開始之前

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

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選取 * 網路和物件 * 索引標籤。
3. 對於儲存的物件加密、如果您不想加密儲存的物件、請使用 * 無 * （預設）設定、或選取 * AES-128* 或 * AES-256* 來加密儲存的物件。
4. 如果您想要防止 S3 用戶端提出特定要求、請選擇性地選取 * 防止用戶端修改 * 。

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

5. 如果用戶端直接連線至儲存節點、且您想使用 HTTP 連線、則可選擇 * 啟用儲存節點連線的 HTTP * 。

   啟用正式作業網格的HTTP時請務必小心、因為要求會以未加密的方式傳送。

6. 選擇*保存*。

更改 **StorageGRID** 介面安全性設定

介面安全性設定可讓您控制使用者是否在超過指定時間的非作用中狀態下登出、以及是否在 API 錯誤回應中包含堆疊追蹤。

開始之前

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

關於這項工作

「 * 安全性設定 * 」頁面包含 * 瀏覽器閒置逾時 * 和 * 管理 API 堆疊追蹤 * 設定。

瀏覽器閒置逾時

指出使用者的瀏覽器在登出之前可以停用多久。預設值為 15 分鐘。

瀏覽器閒置逾時也由下列項目控制：

- 另有一個不可設定StorageGRID 的獨立式計時功能、可用於系統安全性。每個使用者的驗證權杖會在使用者登入後 16 小時過期。當使用者的驗證過期時、該使用者會自動登出、即使瀏覽器閒置逾時已停用、

或瀏覽器逾時的值尚未達到。若要續約權杖、使用者必須重新登入。

- 假設 StorageGRID 已啟用單一登入（ SSO ）、則身分識別提供者的逾時設定。

  如果啟用了 SSO 並且使用者的瀏覽器逾時，則使用者必須重新輸入其 SSO 憑證才能再次存取StorageGRID 。看"SSO 的工作原理" 。

管理 **API** 堆疊追蹤

控制是否在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

此選項預設為停用、但您可能想要在測試環境中啟用此功能。一般而言、您應該在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇 * 介面 * 標籤。
3. 若要變更瀏覽器閒置逾時的設定：
   a. 展開折疊。
   b. 若要變更逾時期間、請指定介於 60 秒到 7 天之間的值。預設逾時為 15 分鐘。
   c. 若要停用此功能、請取消選取核取方塊。
   d. 選擇*保存*。

      新設定不會影響目前登入的使用者。使用者必須重新登入或重新整理瀏覽器、新的逾時設定才會生效。
4. 若要變更管理 API 堆疊追蹤的設定：
   a. 展開折疊。
   b. 選取此核取方塊可在 Grid Manager 和 Tenant Manager API 錯誤回應中傳回堆疊追蹤。

      在正式作業環境中停用堆疊追蹤、以避免在 API 錯誤發生時顯示內部軟體詳細資料。

   c. 選擇*保存*。

管理 **StorageGRID** 中的外部 **SSH** 存取

透過封鎖或允許外部存取來管理進入網格的入站流量的 SSH 存取。管理 SSH 外部存取不會影響網格中節點之間的流量。

開始之前

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

關於這項工作

為了增強系統安全性，預設會阻止外部 SSH 存取。如果您需要執行需要入站 SSH 存取的任務（例如故障排除），請暫時允許外部存取。完成任務後，阻止外部存取。

步驟

1. 選擇*配置* > 安全 > 安全設定。
2. 選擇"阻止 **SSH**"選項卡。
3. 使用*阻止入站 SSH 存取*選項來管理外部 SSH 存取：
   a. 選取核取方塊以阻止存取（預設）。
   b. 取消選取複選框以允許存取。

> 需要透過服務筆記型電腦和所有其他網格節點之間的連接埠 22 進行存取。維護任務完成後，移除對連接埠 22 的存取權限。

4. 選擇*保存*。

設定金鑰管理伺服器

瞭解 StorageGRID 中的金鑰管理伺服器

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。

StorageGRID 僅支援特定的金鑰管理伺服器。如需受支援產品與版本的清單，請使用 "NetApp互通性對照表工具IMT （不含）"。

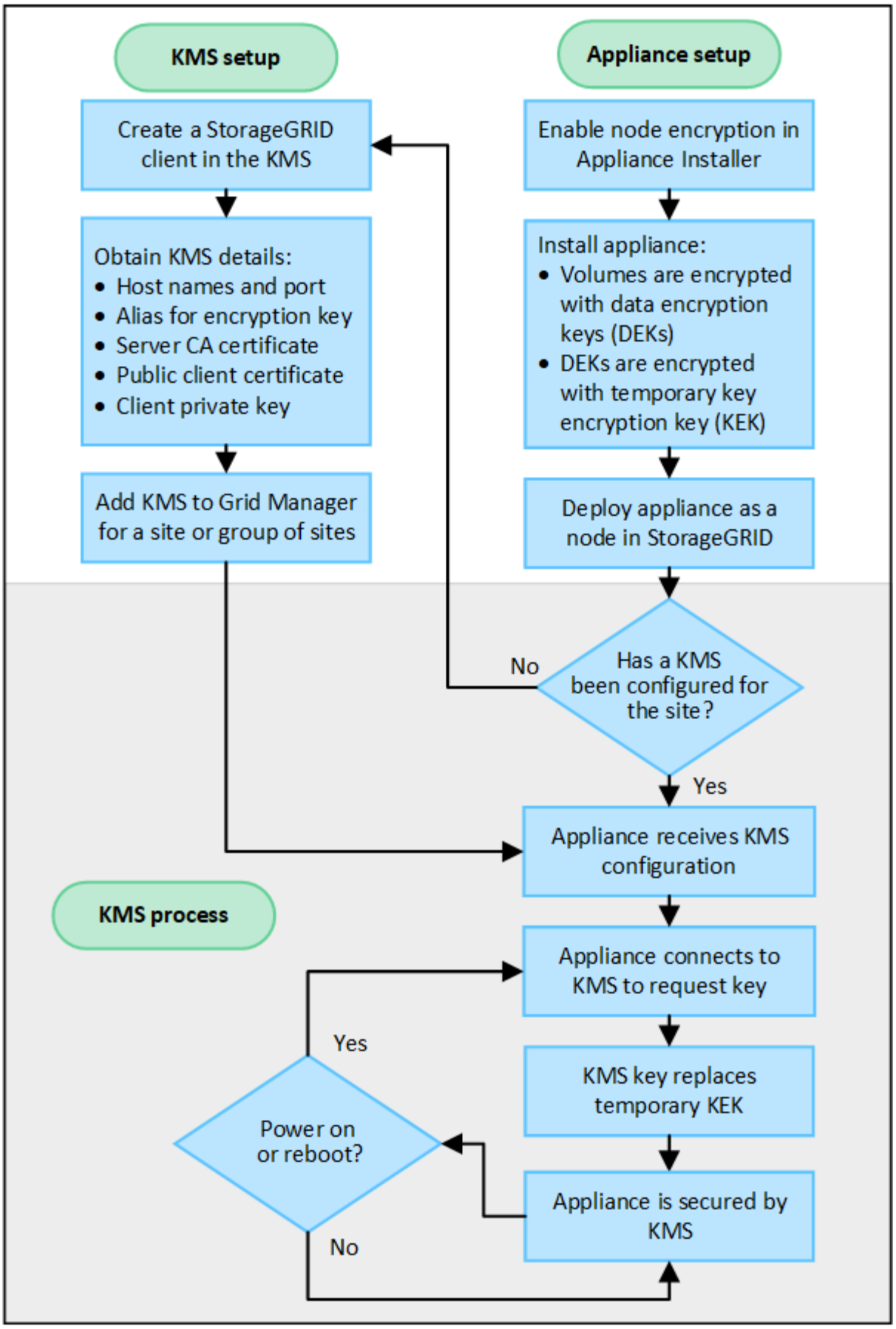
您可以使用一或多個金鑰管理伺服器、來管理StorageGRID 安裝期間啟用*節點加密*設定的任何節點的節點加密金鑰。即使從資料中心移除應用裝置、將關鍵管理伺服器與這些應用裝置節點搭配使用、也能保護資料。應用裝置磁碟區加密後、除非節點可以與 KMS 通訊、否則您無法存取應用裝置上的任何資料。

> 不建立或管理用於加密和解密應用裝置節點的外部金鑰。StorageGRID如果您打算使用外部金鑰管理伺服器來保護StorageGRID 這些資料、您必須瞭解如何設定該伺服器、而且必須瞭解如何管理加密金鑰。執行關鍵管理工作的範圍超出這些指示的範圍。如果您需要協助、請參閱金鑰管理伺服器的文件、或聯絡技術支援部門。

StorageGRID 金鑰管理伺服器和應用裝置組態

在使用金鑰管理伺服器（KMS）來保護StorageGRID 應用裝置節點上的各項資料之前、您必須先完成兩項組態工作：設定一或多個KMS伺服器、以及為應用裝置節點啟用節點加密。完成這兩項組態工作之後、就會自動執行金鑰管理程序。

流程圖顯示使用KMS保護StorageGRID 應用裝置節點上的資訊安全的高階步驟。



流程圖會顯示KMS設定與應用裝置設定並行執行、不過您可以根據需求、在新應用裝置節點啟用節點加密之前

或之後、設定金鑰管理伺服器。

設定金鑰管理伺服器（**KMS**）

設定金鑰管理伺服器包括下列高層級步驟。

步驟	請參閱
存取KMS軟體、並在StorageGRID 每個KMS或KMS叢集上新增一個用戶端以供使用。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
在StorageGRID KMS取得有關該客戶端的必要資訊。	"在StorageGRID KMS中設定以用戶端身份執行的功能"
將KMS新增至Grid Manager、指派給單一站台或預設站台群組、上傳必要的憑證、並儲存KMS組態。	"新增金鑰管理伺服器（KMS）"

設定產品

設定KMS使用的應用裝置節點包括下列高層級步驟。

1. 在設備安裝的硬體組態階段、請使用StorageGRID 「支援服務」功能的「應用程式安裝程式」來啟用應用裝置的「節點加密」設定。

   將應用裝置新增至網格後、您無法啟用 * 節點加密 * 設定、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

2. 執行StorageGRID 《程式安裝程式：在安裝期間、會將隨機資料加密金鑰（DEek）指派給每個應用裝置磁碟區、如下所示：
   - DEK用於加密每個Volume上的資料。這些金鑰是使用應用裝置作業系統中的 Linux 統一金鑰設定（ LUKS ）磁碟加密來產生、無法變更。
   - 每個個別的「DEK」都是使用主要金鑰加密金鑰（KEK）進行加密。初始KEK是加密DEK的暫用金鑰、直到應用裝置連線至KMS為止。
3. 將應用裝置節點新增StorageGRID 至

如需詳細資訊、請參閱 "啟用節點加密"。

金鑰管理加密程序（自動執行）

金鑰管理加密包括下列自動執行的高層級步驟。

1. 當您在網格中安裝已啟用節點加密的應用裝置時StorageGRID 、即可判斷包含新節點的站台是否存在KMS組態。
   - 如果站台已設定KMS、則裝置會接收KMS組態。
   - 如果尚未為站台設定KMS、則在您為站台設定KMS、且裝置收到KMS組態之前、應用裝置上的資料會繼續由暫用KEK加密。
2. 應用裝置使用KMS組態連線至KMS、並要求加密金鑰。

3. KMS會傳送加密金鑰給應用裝置。來自KMS的新金鑰取代了暫用KEK、現在用於加密和解密應用裝置磁碟區的DEK。

> 加密應用裝置節點連線至設定的KMS之前存在的任何資料、都會以暫用金鑰加密。不過、除非KMS加密金鑰取代暫用金鑰、否則應用裝置磁碟區不應被視為受到保護、以免從資料中心移除。

4. 如果裝置電源已開啟或重新開機、則會重新連線至KMS以要求金鑰。儲存在揮發性記憶體中的金鑰、無法在停電或重新開機的情況下繼續運作。

StorageGRID 金鑰管理伺服器需求和注意事項

在設定外部金鑰管理伺服器（KMS）之前、您必須先瞭解考量事項與需求。

支援哪個版本的 **KMIP** ？

支援KMIP 1.4版。StorageGRID

"關鍵管理互通性傳輸協定規格1.4版"

網路考量因素為何？

網路防火牆設定必須允許每個應用裝置節點透過金鑰管理互通性傳輸協定（KMIP）通訊所使用的連接埠進行通訊。預設KMIP連接埠為5696。

您必須確保使用節點加密的每個應用裝置節點、都能透過網路存取您為站台設定的KMS或KMS叢集。

支援哪些 **TLS** 版本？

應用裝置節點與設定的KMS之間的通訊使用安全的TLS連線。StorageGRID 可根據 KMS 支援的內容及使用的項目、在 KMIP 連線至 KMS 或 KMS 叢集時、支援 TLS 1.2 或 TLS 1.3 傳輸協定"TLS 和 SSH 原則"。

StorageGRID在建立連線時與 KMS 協商協定和密碼（TLS 1.2）或密碼套件（TLS 1.3）。要查看可用的協定版本和密碼/密碼套件，請查看 `tlsOutbound`網格的活動 TLS 和 SSH 策略部分（配置 > 安全 安全設定）。

支援哪些應用裝置？

您可以使用金鑰管理伺服器（KMS）來管理StorageGRID 網格中任何啟用「節點加密」設定的項目之加密金鑰。此設定只能在安裝應用StorageGRID 程式的硬體組態階段、使用《支援環境》安裝程式來啟用。

> 將應用裝置新增至網格後、您無法啟用節點加密、也無法將外部金鑰管理用於未啟用節點加密的應用裝置。

您可以使用已設定的 KMS for StorageGRID 應用裝置和應用裝置節點。

您無法將已設定的 KMS 用於軟體型（非應用裝置）節點、包括下列項目：

- 部署為虛擬機器（VM）的節點
- 部署在Linux主機上Container引擎內的節點

部署在這些其他平台上的節點、可以在StorageGRID 資料存放區或磁碟層級使用非功能加密。

何時應該設定金鑰管理伺服器？

對於新安裝、您通常應該先在Grid Manager中設定一或多個金鑰管理伺服器、然後再建立租戶。此順序可確保節點在儲存任何物件資料之前受到保護。

您可以在安裝應用裝置節點之前或之後、在Grid Manager中設定金鑰管理伺服器。

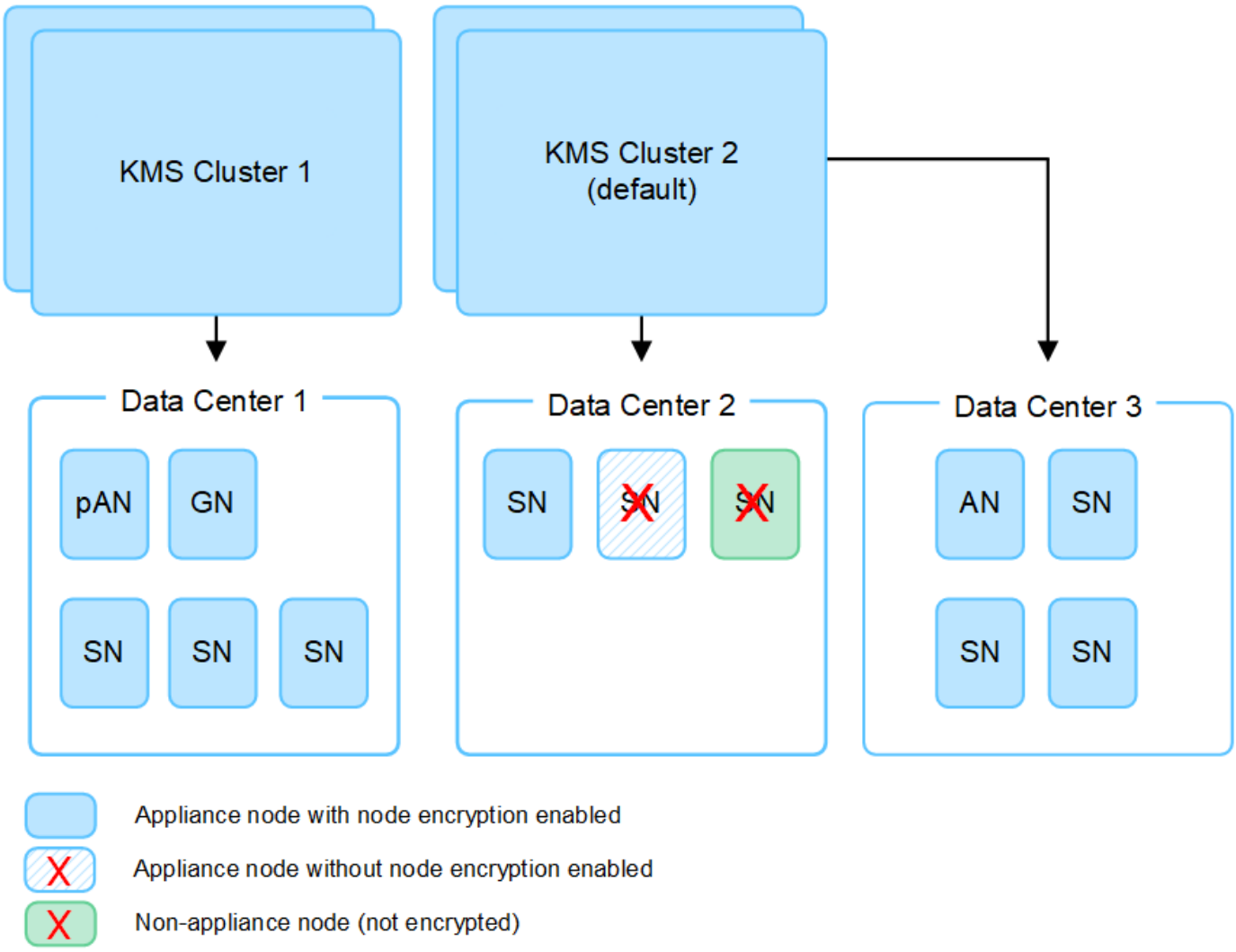
我需要多少個關鍵管理伺服器？

您可以設定一或多個外部金鑰管理伺服器、為StorageGRID 您的作業系統中的應用裝置節點提供加密金鑰。每個KMS都會在StorageGRID 單一站台或一組站台上、提供單一的加密金鑰給各個不完整的應用裝置節點。

支援使用KMS叢集。StorageGRID每個KMS叢集都包含多個複寫的金鑰管理伺服器、這些伺服器共用組態設定和加密金鑰。建議使用KMS叢集進行金鑰管理、因為它能改善高可用度組態的容錯移轉功能。

舉例來說、假設StorageGRID 您的一套系統有三個資料中心站台。您可以設定一個KMS叢集、為資料中心1的所有應用裝置節點提供金鑰、並設定第二個KMS叢集、為所有其他站台的所有應用裝置節點提供金鑰。新增第二個KMS叢集時、您可以為資料中心2和資料中心3設定預設KMS。

請注意、您無法將 KMS 用於非應用裝置節點、或用於安裝期間未啟用 * 節點加密 * 設定的任何應用裝置節點。



當金鑰旋轉時會發生什麼事？

最佳安全性做法是每個設定的 KMS 都應定期"旋轉加密金鑰"使用。

當新的金鑰版本可用時：

- 它會自動發佈至站台或與KMS相關之站台的加密應用裝置節點。發佈應在鑰匙轉動後一個小時內完成。
- 如果在發佈新金鑰版本時、加密的應用裝置節點已離線、節點會在重新開機時立即收到新金鑰。
- 如果由於任何原因而無法使用新的金鑰版本來加密應用裝置磁碟區、則會針對應用裝置節點觸發 * KMS 加密金鑰旋轉失敗 * 警示。您可能需要聯絡技術支援部門、以協助解決此警示。

我可以在設備節點加密後重複使用嗎？

如果您需要將加密的應用裝置安裝到另一個StorageGRID 版本、則必須先取消委任網格節點、才能將物件資料移到另一個節點。然後，您可以使用 StorageGRID 應用裝置安裝程式來 "清除 KMS 組態"。清除KMS組態會停用「節點加密」設定、並移除應用裝置節點與StorageGRID 本網站KMS組態之間的關聯。

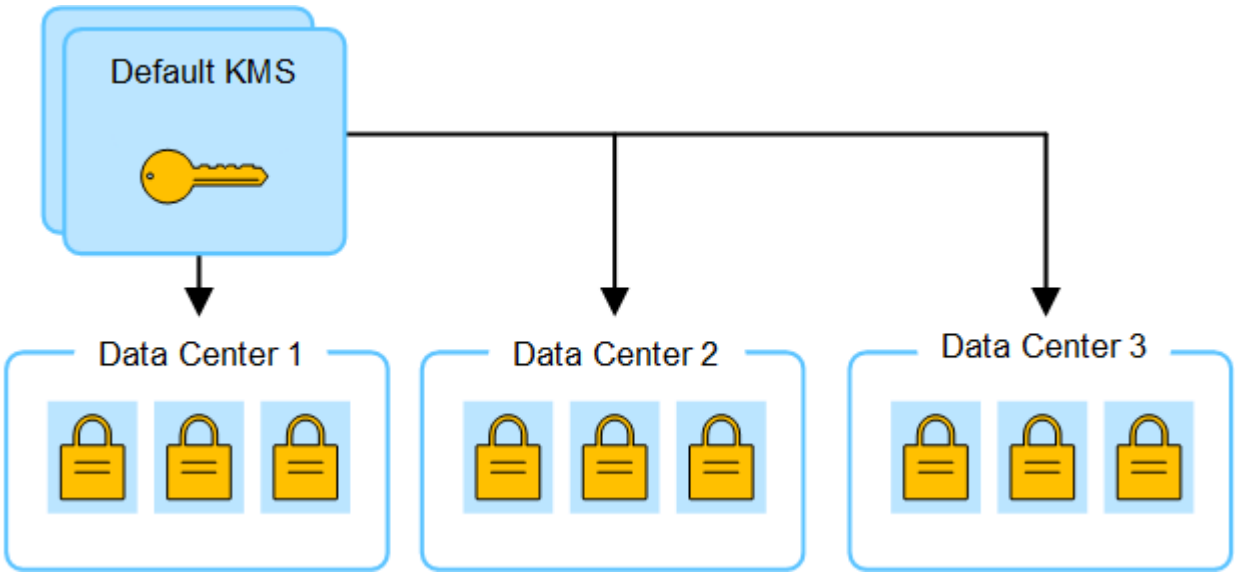
由於無法存取KMS加密金鑰、因此無法再存取設備上的任何資料、而且會永久鎖定。

每個金鑰管理伺服器（KMS）或KMS叢集都會為單一站台或一組站台的所有應用裝置節點提供加密金鑰。如果您需要變更站台使用的KMS、可能需要將加密金鑰從一個KMS複製到另一個KMS。

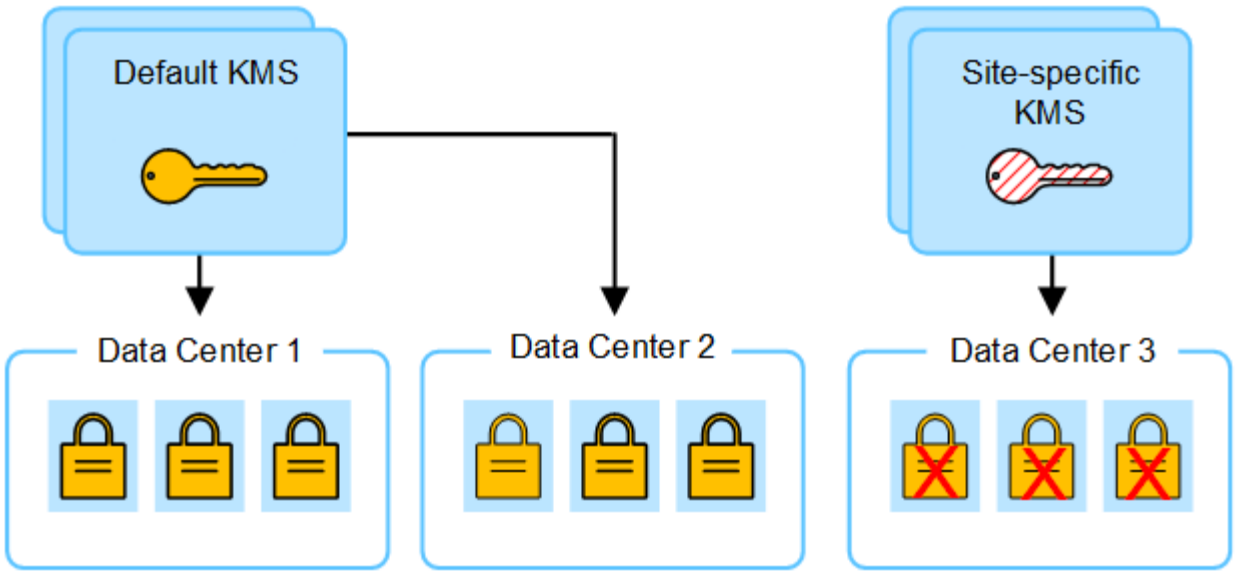
如果您變更站台使用的KMS、則必須確保該站台先前加密的應用裝置節點可以使用儲存在新KMS上的金鑰來解密。在某些情況下、您可能需要將目前版本的加密金鑰從原始KMS複製到新的KMS。您必須確保KMS擁有正確的金鑰、以便在站台上解密加密的應用裝置節點。

例如：

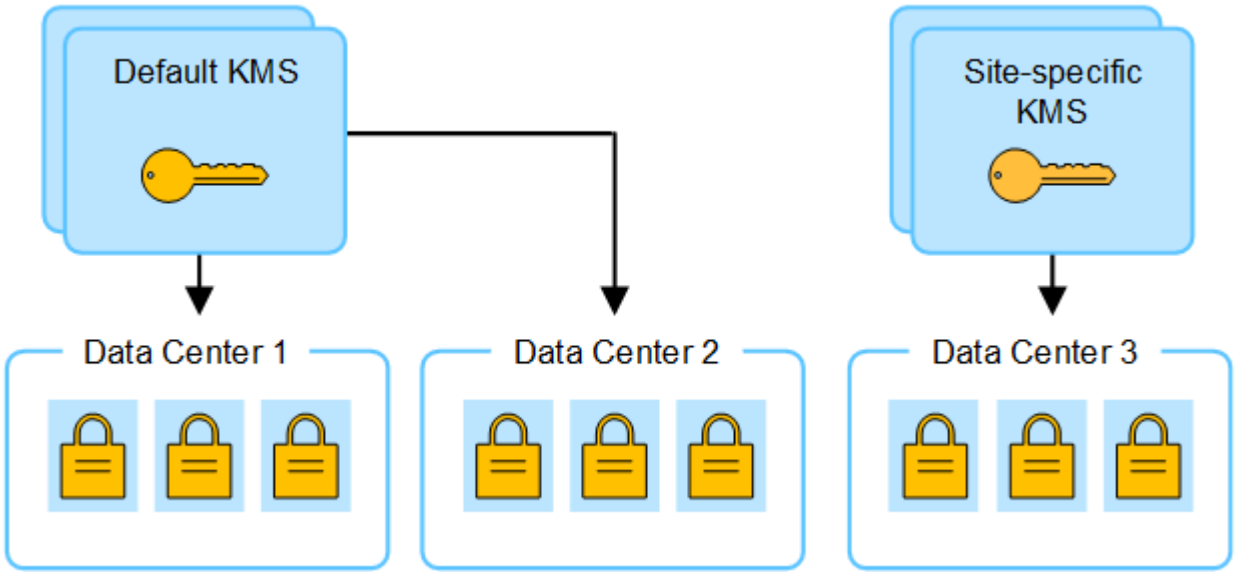
1. 您一開始會設定預設 KMS 、以套用至所有沒有專屬 KMS 的網站。
2. 儲存KMS時、所有啟用「節點加密」設定的應用裝置節點都會連線至KMS、並要求加密金鑰。此金鑰用於加密所有站台的應用裝置節點。此相同金鑰也必須用於解密這些應用裝置。



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



4. 若要解決此問題、請將目前版本的加密金鑰從預設KMS複製到新的KMS。（技術上、您可以將原始金鑰複製到具有相同別名的新金鑰。原始金鑰會成為新金鑰的先前版本。）網站專屬的 KMS 現在擁有正確的金鑰、可將資料中心 3 的應用裝置節點解密、以便儲存在 StorageGRID 中。



變更站台使用**KMS**的使用案例

下表摘要列出變更站台KMS的最常見案例所需步驟。

變更站台**KMS**的使用案例	必要步驟
您有一或多個站台專屬的KMS項目、您想要使用其中一個做為預設KMS。	編輯站台專屬的KMS。在*管理金鑰*欄位中、選取*不受其他KMS管理的站台（預設KMS）*。網站專屬KMS現在將做為預設KMS使用。它將套用至任何沒有專屬 KMS 的網站。 "編輯金鑰管理伺服器（KMS）"

變更站台**KMS**的使用案例	必要步驟
您有預設的KMS、而且您在擴充中新增了一個網站。您不想在新網站上使用預設的 KMS 。	1. 如果新站台的應用裝置節點已在預設KMS中加密、請使用KMS軟體將目前版本的加密金鑰從預設KMS複製到新的KMS。 2. 使用Grid Manager新增KMS並選取網站。 "新增金鑰管理伺服器（KMS）"
您想讓站台的KMS使用不同的伺服器。	1. 如果站台上的應用裝置節點已由現有的KMS加密、請使用KMS軟體將目前版本的加密金鑰從現有的KMS複製到新的KMS。 2. 使用Grid Manager編輯現有的KMS組態、然後輸入新的主機名稱或IP位址。 "新增金鑰管理伺服器（KMS）"

在**StorageGRID KMS**中設定以用戶端身份執行的功能

您必須先為StorageGRID 每個外部金鑰管理伺服器或KMS叢集設定用作用戶端的功能、才能將KMS新增StorageGRID 至原地。

這些指示適用於 Thales CipherTrust Manager 和 Hashicorp Vault 。如需受支援產品與版本的清單，請使用 "NetApp互通性對照表工具IMT （不含）"。

步驟

1. 在KMS軟體中、為StorageGRID 您打算使用的每個KMS或KMS叢集建立一個完善的用戶端。

   每個KMS都會在StorageGRID 單一站台或一組站台上、管理一個用於「不完整」應用裝置節點的加密金鑰。

2. [[create-key-with -kms-product]] 使用下列兩種方法之一建立金鑰：

   - 使用 KMS 產品的金鑰管理頁面。為每個 KMS 或 KMS 叢集建立 AES 加密金鑰。

     加密金鑰必須為 2 、 048 位元以上、而且必須可匯出。

   - 讓 StorageGRID 建立金鑰。測試並儲存之後"正在上傳用戶端憑證"、系統會提示您。

3. 記錄每個KMS或KMS叢集的下列資訊。

   當您將 KMS 新增至 StorageGRID 時、需要以下資訊：

   - 每個伺服器的主機名稱或IP位址。
   - KMS使用的KMIP連接埠。
   - KMS中加密金鑰的金鑰別名。

4. 對於每個KMS或KMS叢集、請取得由憑證授權單位（CA）簽署的伺服器憑證、或是包含每個以憑證鏈順序串聯的、以PEE編碼之CA憑證檔案的憑證套件。

   伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

- 憑證必須使用隱私增強型郵件（ PEF ） Base - 64 編碼的 X ・ 509 格式。
- 每個伺服器憑證中的「Subject Alternative Name（SAN）（主體替代名稱（SAN））」欄位必須包含StorageGRID 完整網域名稱（FQDN）或要連線的IP位址。

> 在StorageGRID 進行KMS設定時、您必須在*主機名稱*欄位中輸入相同的FQDN或IP位址。

- 伺服器憑證必須符合KMS KMIP介面所使用的憑證、後者通常使用連接埠5696。

5. 取得由StorageGRID 外部KMS核發的公有用戶端憑證、以及用戶端憑證的私密金鑰。

   用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

在 **StorageGRID** 中新增金鑰管理伺服器

您可以使用StorageGRID 「驗鑰管理伺服器」精靈來新增每個KMS或KMS叢集。

開始之前

- 您已檢閱"使用金鑰管理伺服器的考量與要求"。
- 您擁有"設定StorageGRID 成KMS中的用戶端"、而且擁有每個 KMS 或 KMS 叢集所需的資訊。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。

關於這項工作

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。如需詳細資訊、請參閱 "變更網站KMS的考量事項" 。

步驟 **1** ： **KMS** 詳細資料

在新增金鑰管理伺服器精靈的步驟 1 （ KMS 詳細資料）中、您會提供 KMS 或 KMS 叢集的詳細資料。

步驟

1. 選擇*設定* > 安全 > 金鑰管理伺服器。

   此時會出現金鑰管理伺服器頁面、並選取組態詳細資料索引標籤。

2. 選擇* Create （建立）。

   隨即顯示新增金鑰管理伺服器精靈的步驟 1 （ KMS 詳細資料）。

3. 針對您StorageGRID 在該KMS中設定的KMS和整套用戶端、輸入下列資訊。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於 1 到 64 個字元之間。

欄位	說明
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。必須介於 1 到 255 個字元之間。 • 注意 * ：如果您尚未使用 KMS 產品建立金鑰、系統會提示您讓 StorageGRID 建立金鑰。
管理的金鑰	將與此KMS相關聯的網站。StorageGRID如有可能、您應該先設定任何站台專屬的金鑰管理伺服器、再設定適用於其他KMS未管理之所有站台的預設KMS。 • 如果此KMS將管理特定站台應用裝置節點的加密金鑰、請選取站台。 • 選取 * 不受其他 KMS 管理的網站（預設 KMS ） * 來設定預設 KMS 、以套用至任何沒有專用 KMS 的網站、以及您在後續擴充中新增的任何網站。 *附註：*如果您選取先前已由預設KMS加密的網站、但未將目前版本的原始加密金鑰提供給新的KMS、則儲存KMS組態時會發生驗證錯誤。
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即KMIP標準連接埠。
主機名稱	KMS的完整網域名稱或IP位址。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

步驟 **2** ：上傳伺服器憑證

在新增金鑰管理伺服器精靈的步驟 2 （上傳伺服器憑證）中、您可以上傳 KMS 的伺服器憑證（或憑證套件）。伺服器憑證可讓外部KMS驗證自己StorageGRID 以供驗證。

步驟

1. 從 * 步驟 2 （上傳伺服器憑證） * 中、瀏覽至儲存伺服器憑證或憑證套件的位置。
2. 上傳憑證檔案。

   隨即顯示伺服器憑證中繼資料。

   如果您上傳了憑證套件組合、每個憑證的中繼資料都會顯示在其各自的索引標籤上。

3. 選擇*繼續*。

步驟 **3** ：上傳用戶端憑證

在新增金鑰管理伺服器精靈的步驟 3 （上傳用戶端憑證）中、您可以上傳用戶端憑證和用戶端憑證私密金鑰。用戶端憑證StorageGRID 可讓支援驗證本身到KMS。

步驟

1. 從 * 步驟 3 （上傳用戶端憑證） * 、瀏覽至用戶端憑證的位置。
2. 上傳用戶端憑證檔案。

   此時會出現用戶端憑證中繼資料。
3. 瀏覽至用戶端憑證的私密金鑰位置。
4. 上傳私密金鑰檔案。
5. 選擇 * 測試並儲存 * 。

   如果金鑰不存在、系統會提示您建立 StorageGRID 。

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

   新增KMS之後、「金鑰管理伺服器」頁面上的憑證狀態會立即顯示為「未知」。可能需要StorageGRID 30分鐘才能取得每個憑證的實際狀態。您必須重新整理網頁瀏覽器、才能查看目前狀態。
6. 如果您選取 * 測試並儲存 * 時出現錯誤訊息、請檢閱訊息詳細資料、然後選取 * 確定 * 。

   例如、如果連線測試失敗、您可能會收到「無法處理的實體」錯誤。
7. 如果您需要儲存目前的組態而不測試外部連線、請選取 * 強制儲存 * 。

   選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。
8. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

   系統會儲存KMS組態、但不會測試與KMS的連線。

在 **StorageGRID** 中管理金鑰管理伺服器

管理金鑰管理伺服器（ KMS ）包括檢視或編輯詳細資料、管理憑證、檢視加密節點、以及在不再需要時移除 KMS 。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。

檢視 **KMS** 詳細資料

您可以檢視 StorageGRID 系統中每個金鑰管理伺服器（ KMS ）的相關資訊、包括金鑰詳細資料、以及伺服器和用戶端憑證的目前狀態。

步驟

1. 選擇*設定* > 安全 > 金鑰管理伺服器。

   此時會出現「金鑰管理伺服器」頁面、並顯示下列資訊：

   - 組態詳細資料索引標籤會列出所有已設定的金鑰管理伺服器。
   - 加密節點索引標籤會列出已啟用節點加密的任何節點。

2. 若要檢視特定 KMS 的詳細資料並在該 KMS 上執行作業、請選取 KMS 的名稱。KMS 的詳細資料頁面會列出下列資訊：

欄位	說明
管理的金鑰	與KMS相關的站台。StorageGRID 此欄位會顯示特定StorageGRID 的站台名稱、或*不由其他KMS管理的站台名稱（預設KMS）。*
主機名稱	KMS的完整網域名稱或IP位址。 如果有兩個金鑰管理伺服器的叢集、則會列出兩個伺服器的完整網域名稱或IP位址。如果叢集中有兩個以上的金鑰管理伺服器、則會列出第一個KMS的完整網域名稱或IP位址、以及叢集中其他金鑰管理伺服器的數量。 例如： `10.10.10.10 and 10.10.10.11`或 `10.10.10.10 and 2 others`。 若要檢視叢集中的所有主機名稱、請選取 KMS 、然後選取 * 編輯 * 或 * 動作 * > * 編輯 * 。

3. 選取 KMS 詳細資料頁面上的索引標籤、即可檢視下列資訊：

索引標籤	欄位	說明
關鍵詳細資料	金鑰名稱	KMS中的核心用戶端別名StorageGRID 。
金鑰UID	金鑰最新版本的唯一識別碼。	上次修改時間
金鑰最新版本的日期與時間。	伺服器憑證	中繼資料

索引標籤	欄位	說明
憑證的中繼資料、例如序號、到期日和時間、以及憑證 PEM 。	憑證 PEM	憑證的 PEM （隱私強化郵件）檔案內容。
用戶端憑證	中繼資料	憑證的中繼資料、例如序號、到期日和時間、以及憑證 PEM 。

4. 根據組織安全實務做法的要求、選擇 * 旋轉機碼 * 、或使用 KMS 軟體來建立新版本的金鑰。

當金鑰旋轉成功時、會更新金鑰 UID 和上次修改的欄位。

如果您使用 KMS 軟體來旋轉加密金鑰、請將其從上次使用的金鑰版本旋轉至相同金鑰的新版本。請勿旋轉至完全不同的金鑰。

切勿嘗試變更KMS的金鑰名稱（別名）來旋轉金鑰。若要從KMS存取先前使用過的所有金鑰版本（以及未來的任何金鑰版本）、必須使用相同的金鑰別名。StorageGRIDIf您變更設定KMS的金鑰別名、StorageGRID 則可能無法解密您的資料。

管理憑證

立即解決任何伺服器或用戶端憑證問題。如有可能、請在憑證過期之前更換憑證。

您必須盡快解決任何憑證問題、才能維持資料存取。

步驟

1. 選擇*設定* > 安全 > 金鑰管理伺服器。
2. 在表格中、查看每個 KMS 的憑證到期值。
3. 如果任何 KMS 的憑證過期時間都是未知的、請等待 30 分鐘、然後重新整理您的網頁瀏覽器。
4. 如果 " 憑證到期 " 欄顯示憑證已過期或即將過期 , 請選取 KMS 前往 KMS 詳細資料頁面。
   a. 選取 * 伺服器憑證 * 、並驗證「到期日」欄位的值。
   b. 若要取代憑證、請選取 * 編輯憑證 * 來上傳新的憑證。
   c. 重複這些子步驟、然後選取 * 用戶端憑證 * 、而非伺服器憑證。
5. 當觸發 *KMS CA 憑證過期 * 、 *KMS 用戶端憑證過期 * 和 *KMS 伺服器憑證過期 * 警示時、請記下每個警示的說明、然後執行建議的動作。

StorageGRID 可能需要 30 分鐘才能取得憑證過期的更新。重新整理網頁瀏覽器以查看目前的值。

如果您的狀態為 * 伺服器憑證狀態為未知 * 、請確保 KMS 允許取得伺服器憑證、而不需要用戶端憑證。

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*設定* > 安全 > 金鑰管理伺服器。

   此時會出現「金鑰管理伺服器」頁面。「組態詳細資料」索引標籤會顯示任何已設定的金鑰管理伺服器。

2. 從頁面頂端、選取 * 加密節點 * 索引標籤。

   加密節點索引標籤會列出 StorageGRID 系統中已啟用 * 節點加密 * 設定的應用裝置節點。

3. 檢閱表格中每個應用裝置節點的資訊。

欄位	說明
節點名稱	應用裝置節點的名稱。
節點類型	節點類型：儲存設備、管理或閘道。
網站	安裝節點的站台名稱。StorageGRID
KMS 名稱	用於節點的KMS描述性名稱。 如果沒有列出 KMS 、請選取組態詳細資料索引標籤以新增 KMS 。 "新增金鑰管理伺服器（KMS）"
金鑰UID	加密金鑰的唯一ID、用於加密及解密應用裝置節點上的資料。若要檢視整個金鑰 UID 、請選取文字。 破折號（-）表示金鑰唯一碼未知、可能是因為應用裝置節點與KMS之間的連線問題。
狀態	KMS與應用裝置節點之間的連線狀態。如果節點已連線、時間戳記每30分鐘更新一次。變更KMS組態之後、連線狀態可能需要幾分鐘的時間才能更新。 • 附註： * 重新整理您的網路瀏覽器、以查看新值。

4. 如果「狀態」欄指出KMS問題、請立即解決問題。

   在一般KMS作業期間、狀態將*連線至KMS *。如果節點與網格中斷連線、則會顯示節點連線狀態（管理性關閉或未知）。

   其他狀態訊息則對應StorageGRID 於名稱相同的Ses姓名：

   ◦ 無法載入kms組態

   ◦ KMS連線錯誤

- 找不到kms加密金鑰名稱
- KMS加密金鑰旋轉失敗
- KMS金鑰無法解密應用裝置磁碟區
- 未設定公里

執行這些警示的建議動作。

> 您必須立即解決任何問題、確保資料受到完整保護。

編輯 **KMS**

您可能需要編輯金鑰管理伺服器的組態、例如、如果憑證即將過期。

開始之前

- 如果您打算更新 KMS 所選的網站，您已經檢閱"變更網站KMS的考量事項"。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。

步驟

1. 選擇*設定* > 安全 > 金鑰管理伺服器。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要編輯的 KMS 、然後選取 * 動作 * > * 編輯 * 。

   您也可以在表格中選取 KMS 名稱、然後在 KMS 詳細資料頁面上選取 * 編輯 * 來編輯 KMS 。

3. 您也可以在「編輯金鑰管理伺服器」精靈的 * 步驟 1 （ KMS 詳細資料） * 中更新詳細資料。

欄位	說明
KMS 名稱	可協助您識別此KMS的描述性名稱。必須介於 1 到 64 個字元之間。
金鑰名稱	KMS中適用於該客戶端的確切金鑰別名StorageGRID 。必須介於 1 到 255 個字元之間。 在極少數情況下、您只需要編輯金鑰名稱即可。例如、如果在KMS中重新命名別名、或是先前金鑰的所有版本都已複製到新別名的版本歷程記錄、則必須編輯金鑰名稱。
管理的金鑰	如果您正在編輯網站專屬的 KMS 、但尚未有預設的 KMS 、請選擇性地選取 * 「不是由其他 KMS 管理的網站」（預設 KMS ） * 。此選項會將網站專屬的 KMS 轉換成預設的 KMS 、適用於所有沒有專屬 KMS 的網站、以及新增至擴充中的任何網站。 • 注意： * 如果您正在編輯網站專屬的 KMS 、則無法選取其他網站。如果您正在編輯預設 KMS 、則無法選取特定網站。

欄位	說明
連接埠	KMS伺服器用於金鑰管理互通性傳輸協定（KMIP）通訊的連接埠。預設為5696、即KMIP標準連接埠。
主機名稱	KMS的完整網域名稱或IP位址。 • 注意： * 伺服器憑證的主體替代名稱（ SAN ）欄位必須包含您在此輸入的 FQDN 或 IP 位址。否則StorageGRID 、無法將無法連接至KMS或KMS叢集中的所有伺服器。

4. 如果您要設定 KMS 叢集、請選取 * 新增其他主機名稱 * 、為叢集中的每部伺服器新增主機名稱。
5. 選擇*繼續*。

   此時將顯示 Edit a Key Management Server （編輯金鑰管理伺服器）精靈的步驟 2 （上傳伺服器憑證）。
6. 如果您需要更換伺服器憑證、請選取*瀏覽*並上傳新檔案。
7. 選擇*繼續*。

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

   測試金鑰管理伺服器與受影響站台上所有節點加密應用裝置節點之間的連線。如果所有節點連線均有效、且KMS上找到正確的金鑰、則金鑰管理伺服器會新增至金鑰管理伺服器頁面的表格。
10. 如果出現錯誤訊息、請檢閱訊息詳細資料、然後選取*確定*。

    例如、如果您為此KMS選取的站台已由其他KMS管理、或連線測試失敗、您可能會收到「無法處理的實體」錯誤。
11. 如果您需要在解決連線錯誤之前儲存目前的組態、請選取 * 強制儲存 * 。

    > 選取 * 強制儲存 * 會儲存 KMS 組態、但不會測試從每個應用裝置到該 KMS 的外部連線。如果組態發生問題、您可能無法重新啟動受影響站台已啟用節點加密的應用裝置節點。在問題解決之前、您可能無法存取資料。

    系統會儲存KMS組態。
12. 檢閱確認警告、如果您確定要強制儲存組態、請選取* OK *。

    KMS 組態已儲存、但 KMS 的連線未經過測試。

移除金鑰管理伺服器（**KMS**）

在某些情況下、您可能會想要移除金鑰管理伺服器。例如、如果您已停用站台、可能會想要移除站台專屬的KMS。

開始之前

- 您已檢閱"使用金鑰管理伺服器的考量與要求"。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。

關於這項工作

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*設定* > 安全 > 金鑰管理伺服器。

   此時會出現「金鑰管理伺服器」頁面、並顯示所有已設定的金鑰管理伺服器。

2. 選取您要移除的 KMS 、然後選取 * 動作 * > * 移除 * 。

   您也可以選取表格中的 KMS 名稱、然後從 KMS 詳細資料頁面中選取 * 移除 * 來移除 KMS 。

3. 請確認下列各項正確無誤：
   - 您正在移除網站專屬 KMS 、此網站沒有啟用節點加密的應用裝置節點。
   - 您正在移除預設的 KMS 、但每個具有節點加密的站台都已存在特定站台的 KMS 。
4. 選擇*是*。

   KMS組態隨即移除。

管理Proxy設定

配置 StorageGRID 儲存代理

如果您使用的是平台服務或雲端儲存資源池、可以在儲存節點和外部S3端點之間設定不透明的Proxy。例如、您可能需要不透明的Proxy、才能將平台服務訊息傳送至外部端點、例如網際網路上的端點。

設定的儲存 Proxy 設定不適用於 Kafka 平台服務端點。

開始之前

- 您有 "特定存取權限"。
- 您已使用登入 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*配置* > 安全 > 代理設定。
2. 在 * 儲存 * 標籤上、選取 * 啟用儲存代理 * 核取方塊。
3. 選取儲存 Proxy 的傳輸協定。
4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 或者、輸入用來連線至Proxy伺服器的連接埠。

   將此欄位保留空白以使用通訊協定的預設連接埠： HTTP 為 80 、 SOCKS5 為 1080 。

6. 選擇*保存*。

   儲存儲存 Proxy 之後、即可設定並測試平台服務或雲端儲存池的新端點。

   Proxy變更可能需要10分鐘才能生效。

7. 檢查Proxy伺服器的設定、確保StorageGRID 不會封鎖來自下列項目的平台服務相關訊息。
8. 如果您需要停用儲存 Proxy 、請清除核取方塊、然後選取 * 儲存 * 。

相關資訊

"用於外部通訊的連接埠"

在 **StorageGRID** 中設定管理 **Proxy** 設定

如果您使用 HTTP 或 HTTPS 傳送 AutoSupport 套件、則可以在管理節點和技術支援（ AutoSupport ）之間設定不透明的 Proxy 伺服器。

如需更多關於 AutoSupport 的資訊，請參閱 "設定AutoSupport 功能"。

開始之前

- 您有 "特定存取權限"。
- 您已使用登入 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*配置* > 安全 > 代理設定。

   此時會顯示 Proxy 設定頁面。依預設、會在索引標籤功能表中選取儲存設備。

2. 選擇 * 管理 * 標籤。
3. 選中 **Enable Admin Proxy** 複選框。
4. 輸入Proxy伺服器的主機名稱或IP位址。
5. 輸入用來連線至Proxy伺服器的連接埠。
6. 您也可以輸入 Proxy 伺服器的使用者名稱和密碼。

如果您的 Proxy 伺服器不需要使用者名稱或密碼、請將這些欄位保留空白。

7. 選取下列其中一項：

   - 如果您想要保護與管理 Proxy 的連線、請選取 * 驗證 Proxy 憑證 * 。上傳 CA 套件以驗證管理 Proxy 伺服器所提供 SSL 憑證的真實性。

     AutoSupport on Demand 、 E 系列 AutoSupport Through StorageGRID 、以及 StorageGRID 升級頁面上的更新路徑判斷、如果驗證了 Proxy 憑證、將無法運作。

   上傳 CA 套件後、便會顯示其中繼資料。

   - 如果您不想在與管理 Proxy 伺服器通訊時驗證憑證、請選取 * 不要驗證 Proxy 憑證 * 。

8. 選擇*保存*。

   儲存管理 Proxy 之後、系統會設定管理節點與技術支援之間的 Proxy 伺服器。

   Proxy變更可能需要10分鐘才能生效。

9. 如果您需要停用管理 Proxy 、請清除 * 啟用管理 Proxy * 核取方塊、然後選取 * 儲存 * 。

控制防火牆

在外部防火牆控制 **StorageGRID** 存取

您可以在外部防火牆開啟或關閉特定連接埠。

您可以StorageGRID 在外部防火牆開啟或關閉特定連接埠、以控制對使用者介面和API的存取。例如、除了使用其他方法來控制系統存取之外、您可能還想要防止租戶連線到防火牆的Grid Manager。

如果您想要設定 StorageGRID 內部防火牆，請參閱"設定內部防火牆"。

連接埠	說明	如果連接埠已開啟...
443	管理節點的預設HTTPS連接埠	Web瀏覽器和管理API用戶端可存取Grid Manager、Grid Management API、租戶管理程式和租戶管理API。 *附註：*連接埠443也用於部分內部流量。
8443	管理節點上的受限網格管理器連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取Grid Manager和Grid Management API。 • Web 瀏覽器和管理 API 用戶端無法存取租戶管理員或租戶管理 API 。 • 系統將拒絕內部內容的要求。

連接埠	說明	如果連接埠已開啟...
9443	管理節點上的受限租戶管理程式連接埠	• Web瀏覽器和管理API用戶端可使用HTTPS存取租戶管理程式和租戶管理API。 • Web 瀏覽器和管理 API 用戶端無法存取 Grid Manager 或 Grid Management API 。 • 系統將拒絕內部內容的要求。

單一登入（SSO）無法在受限網格管理器或租戶管理器連接埠上使用。如果您想要使用者透過單一登入進行驗證、則必須使用預設的HTTPS連接埠（443）。

相關資訊

- "登入Grid Manager"
- "建立租戶帳戶"
- "外部通訊"

管理 **StorageGRID** 中的內部防火牆控制

StorageGRID 在每個節點上都包含內部防火牆、可讓您控制對節點的網路存取、藉此增強網格的安全性。使用防火牆可防止網路存取所有連接埠、但您的特定網格部署所需的連接埠除外。您在「防火牆控制」頁面上所做的組態變更會部署到每個節點。

使用「防火牆控制」頁面上的三個索引標籤、自訂您網格所需的存取權限。

- * 貴賓位址清單 * ：使用此索引標籤可允許選取的存取已關閉的連接埠。您可以使用「管理外部存取」索引標籤、以 CIDR 表示法新增 IP 位址或子網路、以存取關閉的連接埠。
- * 管理外部存取 * ：使用此索引標籤關閉預設開啟的連接埠、或重新開啟先前關閉的連接埠。
- * 不受信任的用戶端網路 * ：使用此索引標籤指定節點是否信任來自用戶端網路的傳入流量。

  此索引標籤上的設定會覆寫「管理外部存取」索引標籤中的設定。

  - 具有不受信任用戶端網路的節點只會接受在該節點上設定的負載平衡器端點連接埠（全域、節點介面和節點類型繫結端點）上的連線。
  - 無論「管理外部網路」標籤上的設定為何、負載平衡器端點連接埠 _ 都是不受信任用戶端網路上唯一開放的連接埠 _ 。
  - 當信任時、所有在「管理外部存取」索引標籤下開啟的連接埠、以及在「用戶端網路」上開啟的任何負載平衡器端點都可以存取。

您在一個索引標籤上所做的設定可能會影響您在其他索引標籤上所做的存取變更。請務必檢查所有索引標籤上的設定、以確保您的網路運作方式符合預期。

若要設定內部防火牆控制項，請參閱"設定防火牆控制項"。

如需外部防火牆和網路安全性的詳細資訊，請參閱"控制外部防火牆的存取"。

權限位址清單和管理外部存取索引標籤

「貴賓位址清單」標籤可讓您登錄一或多個 IP 位址、以存取已關閉的網格連接埠。「管理外部存取」索引標籤可讓您關閉外部存取、以存取選取的外部連接埠或所有開啟的外部連接埠（外部連接埠為非網格節點預設可存取的連接埠）。這兩個索引標籤通常可以一起使用、以自訂您需要的確切網路存取、以供網格使用。

預設情況下、特權 IP 位址沒有內部網格連接埠存取。

範例 **1** ：使用跳躍主機來執行維護工作

假設您想要使用跨接主機（安全強化的主機）進行網路管理。您可以使用下列一般步驟：

1. 使用「貴賓位址清單」標籤新增跳躍主機的 IP 位址。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

在封鎖連接埠 443 和 8443 之前、請先新增權限 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存組態之後、除了跳躍主機之外、所有主機都會封鎖網格中管理節點上的所有外部連接埠。然後、您可以使用跳躍主機更安全地在網格上執行維護工作。

範例 **2** ：鎖定敏感連接埠

假設您想要鎖定敏感連接埠和該連接埠上的服務。您可以使用以下一般步驟：

1. 使用「貴賓」位址清單標籤、僅授予需要存取服務的主機存取權。
2. 使用「管理外部存取」索引標籤來封鎖所有連接埠。

在您封鎖存取任何指派給存取 Grid Manager 和 Tenant Manager 的連接埠（預設連接埠為 443 和 8443 ）之前、請先新增特權 IP 位址。目前連線至封鎖連接埠的任何使用者（包括您）將無法存取 Grid Manager 、除非他們的 IP 位址已新增至「貴賓」位址清單。

儲存配置後，敏感連接埠和該連接埠上的服務可供特權位址清單中的主機使用。無論請求來自哪個接口，所有其他主機都被拒絕存取該服務。

範例 **3** ：停用對未使用服務的存取

在網路層級、您可以停用一些不想使用的服務。例如、若要封鎖 HTTP S3 用戶端流量、您可以使用「管理外部存取」索引標籤上的切換來封鎖連接埠 18084 。

不受信任的用戶端網路索引標籤

如果您使用的是用戶端網路、StorageGRID 只有在明確設定的端點上接受傳入用戶端流量、才能保護不受惡意攻擊的安全。

依預設、每個網格節點上的用戶端網路為_truste_。也就是說，根據預設， StorageGRID 會信任所有上每個網格節點"可用的外部連接埠"的傳入連線。

您可以StorageGRID 指定每個節點上的用戶端網路為_不受信任_、藉此減少對您的作業系統進行惡意攻擊的威脅。如果節點的用戶端網路不受信任、則節點只接受明確設定為負載平衡器端點之連接埠上的傳入連線。請參

閱"設定負載平衡器端點"和"設定防火牆控制項"。

範例**1**：閘道節點僅接受**HTTPS S3**要求

假設您希望閘道節點拒絕用戶端網路上除HTTPS S3要求以外的所有傳入流量。您可以執行下列一般步驟：

1. "負載平衡器端點"在頁面中、透過 HTTPS 在連接埠 443 上設定 S3 的負載平衡器端點。
2. 在「防火牆控制」頁面中、選取「不受信任」、以指定「閘道節點」上的「用戶端網路」不可信任。

儲存組態之後、除了連接埠443上的HTTPS S3要求和ICMP回應（ping）要求之外、閘道節點用戶端網路上的所有傳入流量都會捨棄。

範例**2**：儲存節點傳送**S3**平台服務要求

假設您想要從儲存節點啟用輸出 S3 平台服務流量、但想要防止任何傳入連線到用戶端網路上的該儲存節點。您可以執行以下一般步驟：

- 從「防火牆控制」頁面的「不受信任的用戶端網路」索引標籤、指出儲存節點上的用戶端網路不受信任。

儲存組態後、儲存節點將不再接受用戶端網路上的任何傳入流量、但仍會繼續允許傳出要求至設定的平台服務目的地。

範例 **3** ：將網格管理程式的存取限制在子網路上

假設您只想在特定子網路上允許 Grid Manager 存取。您可以執行下列步驟：

1. 將管理節點的用戶端網路連接至子網路。
2. 使用不受信任的用戶端網路索引標籤、將用戶端網路設定為不受信任。
3. 當您建立管理介面負載平衡器端點時、請輸入連接埠、然後選取連接埠將存取的管理介面。
4. 對於不受信任的用戶端網路、請選取 * 是 * 。
5. 使用管理外部存取索引標籤來封鎖所有外部連接埠（無論是否為該子網路以外的主機設定了權限 IP 位址）。

儲存組態之後、只有指定子網路上的主機才能存取 Grid Manager 。所有其他主機都會遭到封鎖。

配置 **StorageGRID** 內部防火牆

您可以設定 StorageGRID 防火牆、以控制對 StorageGRID 節點上特定連接埠的網路存取。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱和中的資訊"管理防火牆控制""網路準則"。
- 如果您希望管理節點或閘道節點僅接受明確設定的端點上的傳入流量、則表示您已定義負載平衡器端點。

> 變更用戶端網路的組態時、如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

關於這項工作

StorageGRID 在每個節點上都有內部防火牆、可讓您開啟或關閉網格節點上的某些連接埠。您可以使用「防火牆控制」索引標籤來開啟或關閉預設在 Grid Network 、 Admin Network 和 Client Network 上開啟的連接埠。您也可以建立權限 IP 位址清單、以存取已關閉的網格連接埠。如果您使用的是用戶端網路、您可以指定節點是否信任來自用戶端網路的傳入流量、也可以設定用戶端網路上特定連接埠的存取。

將開放給網格外部 IP 位址的連接埠數量限制為只有絕對必要的連接埠數量、可增強網格的安全性。您可以使用三個防火牆控制索引標籤上的每個設定、確保只開啟所需的連接埠。

有關使用防火牆控制的詳細資訊（包括範例），請參閱 "管理防火牆控制"。

有關外部防火牆和網路安全性的詳細資訊，請參閱"控制外部防火牆的存取"。

存取防火牆控制

步驟

1. 選擇*設定* > 安全 > 防火牆控制。

   本頁上的三個標籤如"管理防火牆控制"所述。

2. 選取任何索引標籤以設定防火牆控制項。

   您可以依任何順序使用這些索引標籤。您在一個索引標籤上設定的組態不會限制您可以在其他索引標籤上執行的動作；不過、您在一個索引標籤上所做的組態變更可能會變更在其他索引標籤上設定的連接埠行為。

特殊權限位址清單

您可以使用「貴賓」位址清單標籤、將預設關閉或由「管理外部存取」標籤上的設定關閉的連接埠、授予主機存取權。

預設情況下、特權 IP 位址和子網路沒有內部網格存取。此外、即使在「管理外部存取」索引標籤中遭到封鎖、仍可存取負載平衡器端點和在「貴賓」位址清單索引標籤中開啟的其他連接埠。

「特權位址清單」標籤上的設定可以置換「不受信任的用戶端網路」標籤上的設定。

步驟

1. 在「貴賓位址清單」標籤上、輸入您要授予封閉連接埠存取權的位址或 IP 子網路。
2. （可選）選擇 以 **CIDR** 表示法新增另一個 **IP** 或子網路 以新增其他特權用戶端。

   將盡可能少的位址新增至權限清單。

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

   此選項會移除內部服務的某些保護。如果可能、請將其停用。

4. 選擇*保存*。

管理外部存取

在「管理外部存取」索引標籤中關閉連接埠時、除非您將 IP 位址新增至特殊權限位址清單、否則任何非網格 IP 位址都無法存取連接埠。您只能關閉預設開啟的連接埠、而且只能開啟已關閉的連接埠。

「管理外部存取」索引標籤上的設定無法覆寫「不受信任的用戶端網路」索引標籤上的設定。例如、如果節點不受信任、則即使在「管理外部存取」索引標籤上開啟連接埠 SSH/22 、用戶端網路上的連接埠 SSH/22 也會遭到封鎖。「不受信任的用戶端網路」標籤上的設定會覆寫用戶端網路上的關閉連接埠（例如 443 、 8443 、 9443 ）。

步驟

1. 選取 * 管理外部存取 * 。索引標籤會顯示一個表格、其中包含網格中節點的所有外部連接埠（預設為非網格節點可存取的連接埠）。
2. 使用下列選項設定您要開啟和關閉的連接埠：
   - 使用每個連接埠旁的切換開關來開啟或關閉選取的連接埠。
   - 選取 * 開啟所有顯示的連接埠 * 以開啟表格中列出的所有連接埠。
   - 選取 * 關閉所有顯示的連接埠 * 以關閉表格中列出的所有連接埠。

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

   使用表格右側的捲軸、確定您已檢視所有可用的連接埠。使用搜尋欄位、輸入連接埠編號、以尋找任何外部連接埠的設定。您可以輸入部分連接埠號碼。例如，如果您輸入 **2** ，則會顯示字串 "2" 做為其名稱一部分的所有連接埠。

3. 選擇*保存*

不受信任的用戶端網路

如果節點的用戶端網路不受信任、則節點只接受設定為負載平衡器端點的連接埠上的傳入流量、以及您在此索引標籤上選取的其他連接埠（選擇性）。您也可以使用此索引標籤來指定擴充中新增節點的預設設定。

如果尚未設定負載平衡器端點、現有的用戶端連線可能會失敗。

您在 * 不受信任的用戶端網路 * 標籤上所做的組態變更會覆寫 * 管理外部存取 * 標籤上的設定。

步驟

1. 選取 * 不受信任的用戶端網路 * 。
2. 在 Set New Node Default （設定新節點預設值）區段中、指定在擴充程序中將新節點新增至網格時的預設設定值。
   - * Trusted * （預設值）：當節點新增至擴充時、其 Client Network 會受到信任。
   - 不受信任：在擴充中新增節點時、其用戶端網路不受信任。

     視需要、您可以返回此索引標籤、變更特定新節點的設定。

此設定不會影響StorageGRID 到您的不完善系統中現有的節點。

3. 使用下列選項來選取節點、這些節點只能在明確設定的負載平衡器端點或其他選取的連接埠上允許用戶端連線：

   - 選取 * 不信任顯示的節點 * 、將表格中顯示的所有節點新增至「不受信任的用戶端網路」清單。
   - 選取 * 信任顯示的節點 * 、將表格中顯示的所有節點從「不受信任的用戶端網路」清單中移除。
   - 使用每個節點旁的切換、將所選節點的 Client Network 設為 Trusted 或 Trusted 。

   例如、您可以選取 * 在顯示的節點上不信任 * 、將所有節點新增至「不信任的用戶端網路」清單、然後使用個別節點旁的切換、將該單一節點新增至「信任的用戶端網路」清單。

   使用表格右側的捲軸、確定您已檢視所有可用的節點。使用搜尋欄位輸入節點名稱、即可尋找任何節點的設定。您可以輸入部分名稱。例如、如果您輸入 * GW* 、則會顯示字串 "Gw" 做為其名稱一部分的所有節點。

4. 選擇*保存*。

   新的防火牆設定將立即生效並強制執行。如果負載平衡器端點尚未設定，現有用戶端連線可能會失敗。

管理租戶

StorageGRID 中的租戶帳戶

租戶帳戶可讓您使用簡易儲存服務（ S3 ） REST API 來儲存及擷取 StorageGRID 系統中的物件。

Swift 詳細資料已從此文件網站版本中移除。請參閱。 "StorageGRID 11.8 ：管理租戶"

身為網格管理員、您可以建立和管理 S3 用戶端用來儲存和擷取物件的租戶帳戶。

每個租戶帳戶都有同盟或本機群組、使用者、 S3 貯體和物件。

租戶帳戶可用來分隔不同實體所儲存的物件。例如、多個租戶帳戶可用於下列任一使用案例：

- *企業使用案例：*如果您是在StorageGRID 企業應用程式中管理一套功能完善的系統、您可能會想要將網格的物件儲存區由組織中的不同部門加以隔離。在此案例中、您可以為行銷部門、客戶支援部門、人力資源部門等建立租戶帳戶。

  如果您使用 S3 用戶端協議，則可以使用 S3 儲存桶和儲存桶策略在企業各部門之間隔離物件。您不需要使用租用戶帳戶。請參閱實施說明"S3 貯體和貯體原則"了解更多。

- *服務供應商使用案例：*如果您以StorageGRID 服務供應商的身份管理一個支援系統、則可以將網格的物件儲存區、由將儲存設備租賃至網格的不同實體來分隔。在這種情況下、您會為公司A、公司B、公司C等建立租戶帳戶。

如需更多資訊、請參閱 "使用租戶帳戶"。

如何建立租戶帳戶？

使用 Grid Manager 建立租戶帳戶。建立租戶帳戶時、請指定下列資訊：

- 基本資訊、包括租戶名稱、用戶端類型（ S3 ）和選用的儲存配額。
- 租戶帳戶的權限、例如租戶帳戶是否可以使用 S3 平台服務、設定自己的身分識別來源、使用 S3 Select 或使用網格同盟連線。
- 租戶的初始根存取權、取決於 StorageGRID 系統是使用本機群組和使用者、身分識別聯盟或單一登入（ SSO ）。

此外、如果 S3 租戶帳戶需要符合法規要求、您可以為 StorageGRID 系統啟用 S3 物件鎖定設定。啟用S3物件鎖定時、所有S3租戶帳戶都能建立及管理相容的儲存區。

租戶管理程式的用途為何？

建立租戶帳戶之後、租戶使用者可以登入租戶管理員、以執行下列工作：

- 設定身分識別聯盟（除非身分識別來源與網格共用）
- 管理群組和使用者
- 使用網格聯合進行帳戶同步和跨網格複寫
- 管理S3存取金鑰
- 建立及管理 S3 儲存區
- 使用 S3 平台服務
- 使用S3 Select
- 監控儲存使用量

雖然 S3 租戶使用者可以使用 Tenant Manager 來建立和管理 S3 存取金鑰和貯體、但他們必須使用 S3 用戶端應用程式來擷取和管理物件。如需詳細資訊、請參閱 "使用S3 REST API" 。

建立 **StorageGRID** 租用戶帳戶

您必須建立至少一個租戶帳戶、以控制StorageGRID 對您的作業系統儲存設備的存取。

建立租用戶帳戶的步驟取決於"身分識別聯盟"和"單一登入"是否配置，以及用於建立租用戶帳戶的網格管理器帳戶是否屬於具有 Root 存取權限的管理員群組。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權或 Tenant 帳戶權限"。
- 如果租戶帳戶將使用為Grid Manager設定的身分識別來源、而您想要將租戶帳戶的根存取權限授予聯盟群組、則表示您已將該聯盟群組匯入Grid Manager。您不需要指派任何 Grid Manager 權限給此管理群組。請參閱。 "管理管理群組"
- 如果您希望允許 S3 租戶使用網格聯合連線將帳戶資料同步並將儲存桶物件複寫到另一個網格：
  - 您有 "已設定網格同盟連線"。

- 連線狀態為 * 已連線 * 。
- 您擁有root存取權限。
- 您已檢閱的考量事項"管理 Grid Federation 的允許租戶"。
- 如果租戶帳戶將使用為 Grid Manager 設定的身分識別來源、則您已將相同的聯盟群組匯入兩個網格上的 Grid Manager 。

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

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

存取精靈

步驟

1. 選擇*租戶*。
2. 選擇* Create （建立）。

輸入詳細資料

步驟

1. 輸入租戶的詳細資料。

欄位	說明
名稱	租戶帳戶的名稱。租戶名稱不一定是唯一的。建立租戶帳戶時、它會收到唯一的 20 位數帳戶 ID 。
說明（選用）	協助識別租戶的說明。 如果您要建立將使用網格同盟連線的租用戶、請選擇性使用此欄位來協助識別來源租戶和目的地租戶。例如、對於在 Grid 1 上建立的租戶、此描述也會顯示給複製到 Grid 2 的租戶：「此租戶是在 Grid 1 上建立的。」
用戶端類型	必須是 *S3 * 。
儲存配額（選用）	如果您想要此租用戶擁有儲存配額、則需要配額和單位的數值。

2. 選擇*繼續*。

[[admin-租 戶選取權限 **]]** 選取權限

步驟

1. 或者、選取您希望此租用戶擁有的基本權限。

   其中有些權限有額外的需求。如需詳細資料、請選取每個權限的說明圖示。

權限	如果選取 ...
允許平台服務	租戶可以使用 S3 平台服務、例如 CloudMirror 。請參閱。 "管理S3租戶帳戶的平台服務"
使用自己的身分識別來源	租用戶可以為聯合群組和使用者配置和管理自己的身分來源。如果您有以下情況，則此選項被停用"已設定 SSO"適用於您的StorageGRID系統。
允許 S3 Select	租戶可以發出 S3 SelectObjectContent API 要求、以篩選及擷取物件資料。請參閱。 "管理用戶帳戶的S3 Select" • 重要 * ： SelectObjectContent 要求可降低所有 S3 用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。

2. 或者、選取您希望此租用戶擁有的進階權限。

權限	如果選取 ...
網格同盟連線	租戶可以使用網格同盟連線，該連線具有以下功能： • 使此租戶帳戶和所有租戶群組、使用者和 S3 存取金鑰在此網格與所選連線中的其他網格之間同步。 如果出於安全性或法規遵循原因需要，您可以取消選擇「啟用存取金鑰同步」。 • 允許此租戶在每個網格上對應的儲存格之間設定跨網格複寫。 請參閱。 "管理 Grid Federation 的允許租戶"
S3物件鎖定	允許租戶使用 S3 物件鎖定的特定功能： • * 設定最大保留期間 * 定義新增至此貯體的物件應保留多久、從擷取開始算起。 • * 允許規範模式 * 可防止使用者在保留期間覆寫或刪除受保護的物件版本。

3. 選擇*繼續*。

定義 **root** 存取權並建立租戶

步驟

1. 根據您的 StorageGRID 系統是使用身分識別聯盟、單一登入（ SSO ）或兩者、定義租戶帳戶的根存取權。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。

選項	請這麼做
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

2. 選取*建立租戶*。

   成功訊息隨即出現、新的租戶會列在租戶頁面上。若要瞭解如何檢視租戶詳細資料及監控租戶活動，請參閱"監控租戶活動"。

   根據網路連線能力、節點狀態和 Cassandra 作業、在整個網格套用租戶設定可能需要 15 分鐘或更長的時間。

3. 如果您為租戶選擇了「使用網格聯合連線」權限，請確認已將相同的租戶複寫到連線中的另一個網格。兩個網格上的租戶將具有相同的 20 位數帳戶 ID、名稱、執行摘要、配額和權限。

   如果您看到錯誤訊息，指示租戶帳戶已在此網格上建立，但未同步到其他網格，請參閱 "疑難排解網格同盟錯誤" 中的說明。

登入租戶（選用）

視需要、您可以立即登入新租戶以完成組態、或是稍後登入租戶。登入步驟取決於您是使用預設連接埠（ 443 ）還是受限連接埠登入 Grid Manager 。請參閱。 "控制外部防火牆的存取"

立即登入

如果您使用...	執行此動作...
連接埠 443 和您為本機 root 使用者設定密碼	1. 選取 * 以 root 登入 * 。 當您登入時、會出現連結以設定貯體、身分識別聯盟、群組和使用者。 2. 選取連結以設定租戶帳戶。 每個連結都會在租戶管理程式中開啟對應的頁面。若要完成此頁面，請參閱"租戶帳戶使用說明"。
連接埠 443 並未設定本機根使用者的密碼	選取 * 登入 * 、然後在根存取聯盟群組中輸入使用者的認證。

如果您使用...	執行此動作...
受限連接埠	1. 選擇 * 完成 * 2. 請在「租戶」表格中選取 * 限制 * 、以深入瞭解如何存取此租戶帳戶。 租戶管理程式的URL格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完整網域名稱或 IP 位址 ◦ `port`是僅租戶連接埠 ◦ `20-digit-account-id`是租戶的唯一帳戶 ID

稍後登入

如果您使用...	請執行下列其中一項...
連接埠 443	• 從網格管理員中，選擇“租戶”，然後選擇租戶名稱右側的“Sign in”。 • 在網頁瀏覽器中輸入租戶的URL： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完整網域名稱或 IP 位址 ◦ `20-digit-account-id`是租戶的唯一帳戶 ID
受限連接埠	• 從網格管理員中，選擇*租戶*，然後選擇*受限*。 • 在網頁瀏覽器中輸入租戶的URL： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`是管理節點的完整網域名稱或 IP 位址 ◦ `port`是僅限租戶的限制連接埠 ◦ `20-digit-account-id`是租戶的唯一帳戶 ID

設定租戶

依照"使用租戶帳戶"中的指示管理租戶群組和使用者、S3 存取金鑰、儲存桶、平台服務、帳戶同步和跨網格複寫。

編輯 StorageGRID 租用戶帳戶

您可以編輯租戶帳戶、以變更顯示名稱、儲存配額或租戶權限。

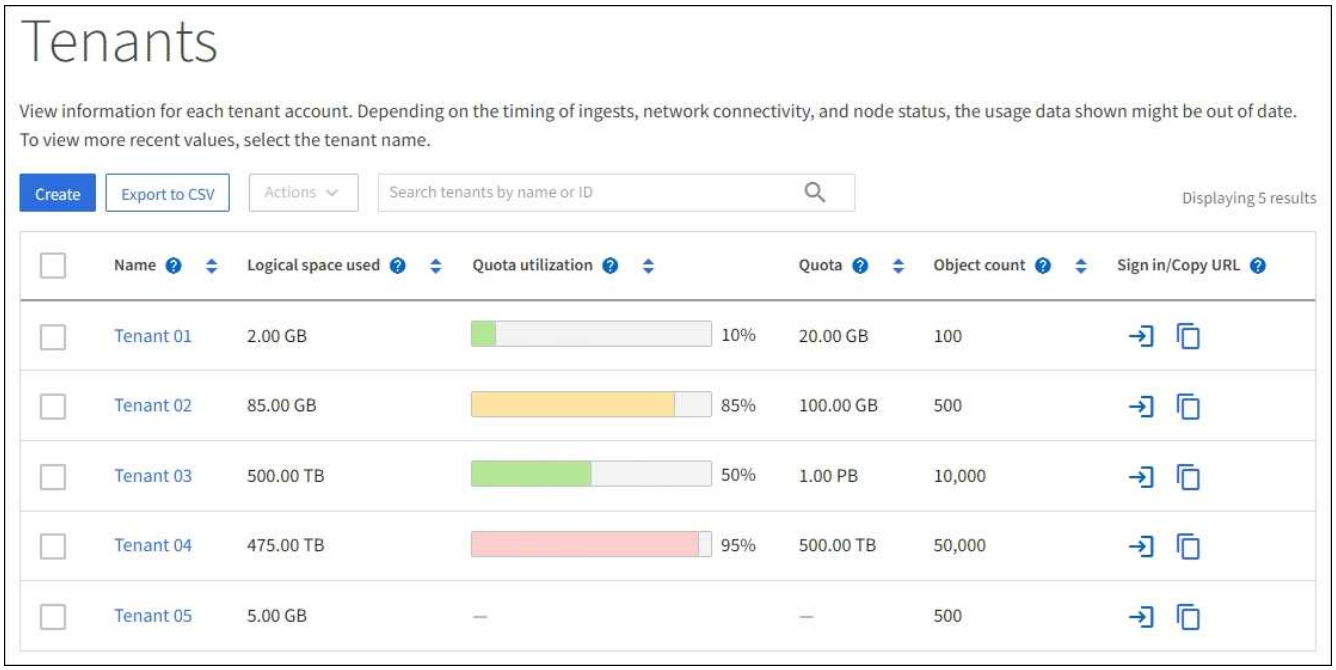
開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權或 Tenant 帳戶權限"。

根據網路連線能力、節點狀態和 Cassandra 作業、在整個網格套用租戶設定可能需要 15 分鐘或更長的時間。

步驟

1. 選擇*租戶*。



2. 找出您要編輯的租戶帳戶。

   使用搜尋方塊、依名稱或租戶 ID 搜尋租戶。

3. 選取租戶。您可以執行下列其中一項：
   - 選取租戶的核取方塊、然後選取 * 動作 * > * 編輯 * 。
   - 選取租戶名稱以顯示詳細資料頁面、然後選取 * 編輯 * 。
4. 您也可以變更這些欄位的值：
   - 名稱
   - 說明
   - 儲存配額
5. 選擇*繼續*。
6. 選取或清除租戶帳戶的權限。
   - 如果您停用已在使用的租戶*平台服務*、則他們針對S3儲存區所設定的服務將停止運作。不會傳送錯誤訊息給租戶。例如、如果租戶已設定S3儲存區的CloudMirror複寫、他們仍可將物件儲存在儲存區中、但這些物件的複本將不再建立在已設定為端點的外部S3儲存區中。請參閱。 "管理S3租戶帳戶的平台服務"

- 變更 * 使用自己的身分識別來源 * 的設定、以判斷租戶帳戶是使用自己的身分識別來源、還是使用為 Grid Manager 設定的身分識別來源。

  如果 * 使用自己的身分識別來源 * 是：

  - 已停用並選取、租戶已啟用自己的身分識別來源。租戶必須先停用其身分識別來源、才能使用為Grid Manager設定的身分識別來源。
  - 已停用且未選取、 StorageGRID 系統會啟用 SSO 。租戶必須使用為Grid Manager設定的身分識別來源。

- 視需要選取或清除 * 允許 S3 選取 * 權限。請參閱。 "管理用戶帳戶的S3 Select"
- 若要移除 * 使用網格同盟連線 * 權限：
  i. 在租戶詳細資料頁面上選擇「Grid federation」標籤。
  ii. 選擇要移除的連線。
  iii. 選取 * 移除權限 * 。
- 若要新增 * 使用網格同盟連線 * 權限：
  i. 選取 * Grid Federation * 標籤。
  ii. 選中 * 使用網格聯合連接 * 複選框。
  iii. 或者、選取 * 複製現有的本機使用者和群組 * 、將其複製到遠端網格。如果需要、您可以停止正在進行的複製、或是在完成最後一次複製作業之後、如果無法複製某些本機使用者或群組、請重試複製。

  如果出於安全性或法規遵循原因需要，您可以取消選擇「啟用存取金鑰同步」。

- 若要設定最長保留期間或允許符合性模式：

  您必須先在網格上啟用 S3 物件鎖定、才能使用這些設定。

  i. 選取 *S3 物件鎖定 * 索引標籤。
  ii. 對於 * 設定最大保留期間 * 、請輸入一個值、然後從下拉式清單中選取時間週期。
  iii. 對於 * 允許規範模式 * 、請選取核取方塊。

變更 **StorageGRID** 租戶本機 **root** 使用者的密碼

如果root使用者被鎖定在帳戶之外、您可能需要變更租戶本機root使用者的密碼。

開始之前

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

關於這項工作

如果您的 StorageGRID 系統已啟用單一登入（ SSO ）、則本機根使用者無法登入租戶帳戶。若要執行root使用者工作、使用者必須屬於擁有租戶根存取權限的聯盟群組。

步驟

1. 選擇*租戶*。

2. 選取租戶帳戶。您可以執行下列其中一項：
   - 選取租戶的核取方塊、然後選取 * 動作 * > * 變更 root 密碼 * 。
   - 選取租戶名稱以顯示詳細資料頁面、然後選取 * 動作 * > * 變更 root 密碼 * 。
3. 輸入租戶帳戶的新密碼。
4. 選擇*保存*。

刪除 **StorageGRID** 租用戶帳戶

若要永久移除租戶對系統的存取權、您可以刪除租戶帳戶。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已移除與租戶帳戶相關的所有 S3 儲存區和物件。
- 如果允許租戶使用網格聯合連線，您已審查了相關注意事項"刪除具有使用網格同盟連線權限的租用戶"。刪除操作會同步，因此如果在任何網格中刪除租戶，則會在所有選定的網格中刪除。

步驟

1. 選擇*租戶*。
2. 找出您要刪除的租戶帳戶。

   使用搜尋方塊、依名稱或租戶 ID 搜尋租戶。
3. 若要刪除多個租戶、請選取核取方塊、然後選取 * 動作 * > * 刪除 * 。
4. 若要刪除單一租戶、請執行下列其中一項：

- 選取核取方塊、然後選取 * 動作 * > * 刪除 * 。
- 選取租戶名稱以顯示詳細資料頁面、然後選取 * 動作 * > * 刪除 * 。

5. 選擇*是*。

管理平台服務

了解 **StorageGRID** 平台服務

平台服務包括CloudMirror複寫、事件通知及搜尋整合服務。

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。

平台服務不支援"分支桶"。

CloudMirror複寫

StorageGRID CloudMirror 複寫服務用於將特定物件從 StorageGRID 儲存庫鏡射到指定的外部目的地。

例如、您可以使用CloudMirror複寫將特定的客戶記錄鏡射到Amazon S3、然後利用AWS服務對資料執行分析。

CloudMirror 複寫與跨網格複寫功能有一些重要的相似之處和差異。若要深入瞭解"比較跨網格複寫和 CloudMirror 複寫"、請參閱。

通知

每個儲存桶事件通知用於將有關對物件執行的特定操作的通知傳送到指定的外部 Kafka 叢集、webhook 端點或 Amazon Simple Notification Service。

例如、您可以設定要傳送警示給系統管理員、以通知新增至儲存區的每個物件、其中物件代表與重大系統事件相關的記錄檔。

> 雖然事件通知可在已啟用S3物件鎖定的儲存區上設定、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

搜尋整合服務

搜尋整合服務用於將 S3 物件中繼資料傳送至指定的彈性搜尋索引、以便使用外部服務搜尋或分析中繼資料。

例如、您可以設定儲存區、將S3物件中繼資料傳送至遠端Elasticsearch服務。然後您可以使用Elasticsearch來執行跨儲存區的搜尋、並對物件中繼資料中的模式進行精密分析。

> 雖然可在啟用S3物件鎖定的儲存區上設定Elasticsearch整合、但通知訊息中不會包含物件的S3物件鎖定中繼資料（包括「保留直到日期」和「法定保留」狀態）。

平台服務可讓租戶將外部儲存資源、通知服務、以及搜尋或分析服務與資料一起使用。由於平台服務的目標位置通常是StorageGRID 不適用於您的非執行部署、因此您必須決定是否允許租戶使用這些服務。如果您這麼做、則必須在建立或編輯租戶帳戶時啟用平台服務的使用。您也必須設定網路、讓租戶產生的平台服務訊息能夠到達目的地。

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。
- 對於無法完成的端點的要求、將會排入最多 50 、 000 個要求的佇列。此限制在作用中租戶之間平均分攤。新租戶可暫時超逾這 50 萬個限額，以免新增租戶受到不公平的懲罰。

相關資訊

- "管理平台服務"
- "設定儲存Proxy設定"
- "監控 StorageGRID"

StorageGRID 平台服務的網路和連接埠

如果您允許S3租戶使用平台服務、則必須設定網格的網路連線、以確保平台服務訊息可傳送至目的地。

您可以在建立或更新租戶帳戶時、為S3租戶帳戶啟用平台服務。如果已啟用平台服務、租戶可以建立端點、做為CloudMirror複寫、事件通知或從S3儲存區搜尋整合訊息的目的地。這些平台服務訊息會從執行ADC服務的儲存節點傳送至目的地端點。

例如、租戶可能會設定下列類型的目的地端點：

- 本機代管的彈性搜尋叢集
- 支援接收 Amazon Simple Notification Service 訊息的本機應用程式
- 本地託管的 Kafka 叢集
- 支援 HTTP POST 通知請求的外部或本機託管的 webhook 端點。

  此端點可以託管在各種 Web 伺服器、框架或資料處理工具（例如 Fluentd）上。
- 本地託管的S3儲存區位於StorageGRID 相同或其他的例子
- 外部端點、例如Amazon Web Services上的端點。

若要確保平台服務訊息能夠傳送、您必須設定含有「ADC儲存節點」的網路。您必須確保下列連接埠可用於傳送平台服務訊息至目的地端點。

根據預設、平台服務訊息會在下列連接埠上傳送：

- **80** ：適用於以 http 開頭的端點 URI （大多數端點）
- **443** ：適用於以 https 開頭的端點 URI （大多數端點）
- **9092** ：適用於以 http 或 https 開頭的端點 URI （僅限 Kafka 端點）

租戶在建立或編輯端點時、可以指定不同的連接埠。

如果StorageGRID 將某個支援區部署做為CloudMirror複寫的目的地、則複寫訊息可能會在80或443以外的連接埠接收。確保StorageGRID 端點中已指定目的地支援的S3連接埠。

如果您使用非透明 Proxy 伺服器、也必須"設定儲存Proxy設定"允許訊息傳送至外部端點、例如網際網路上的端點。

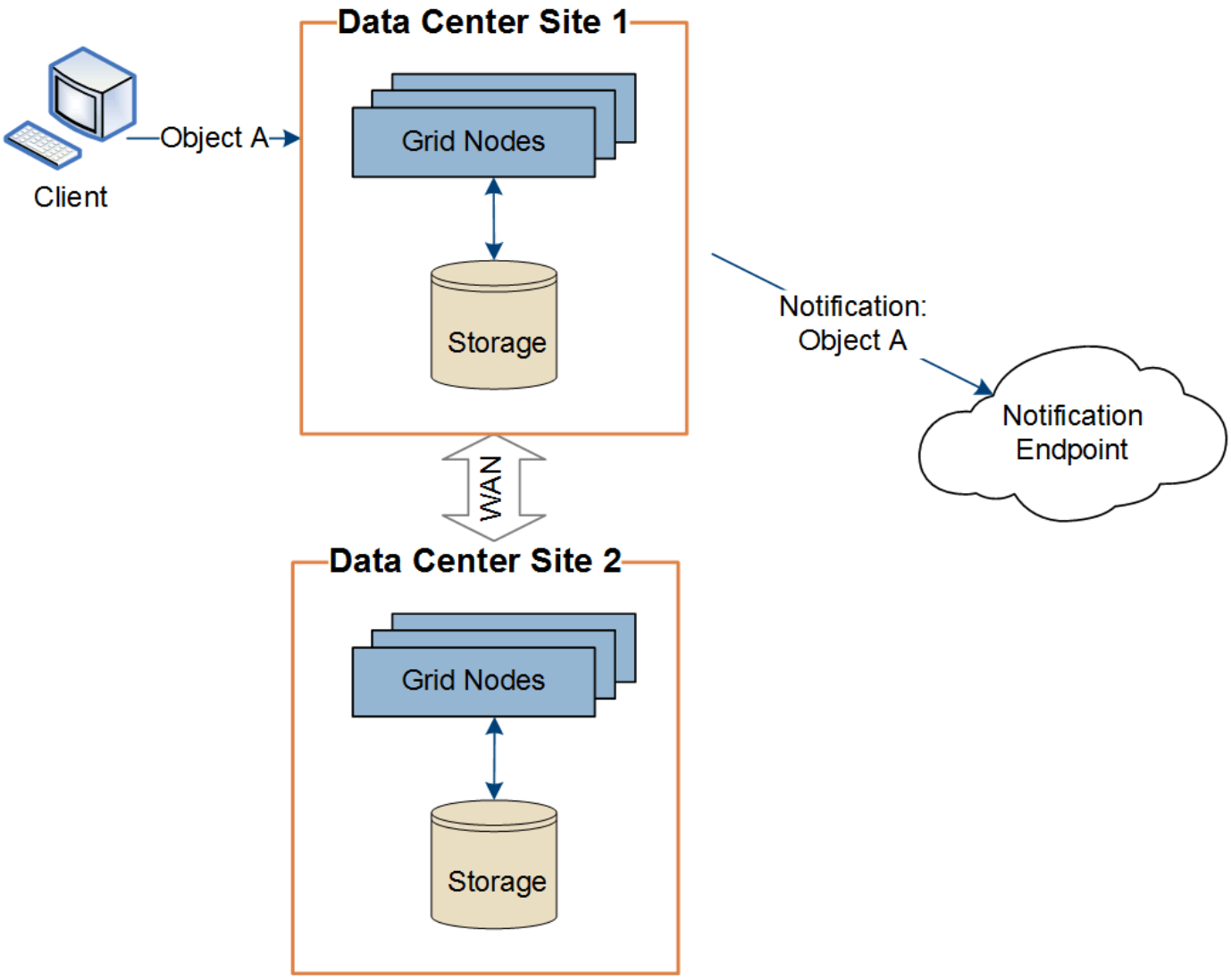
相關資訊

- "使用租戶帳戶"
- "用於外部通訊的連接埠"

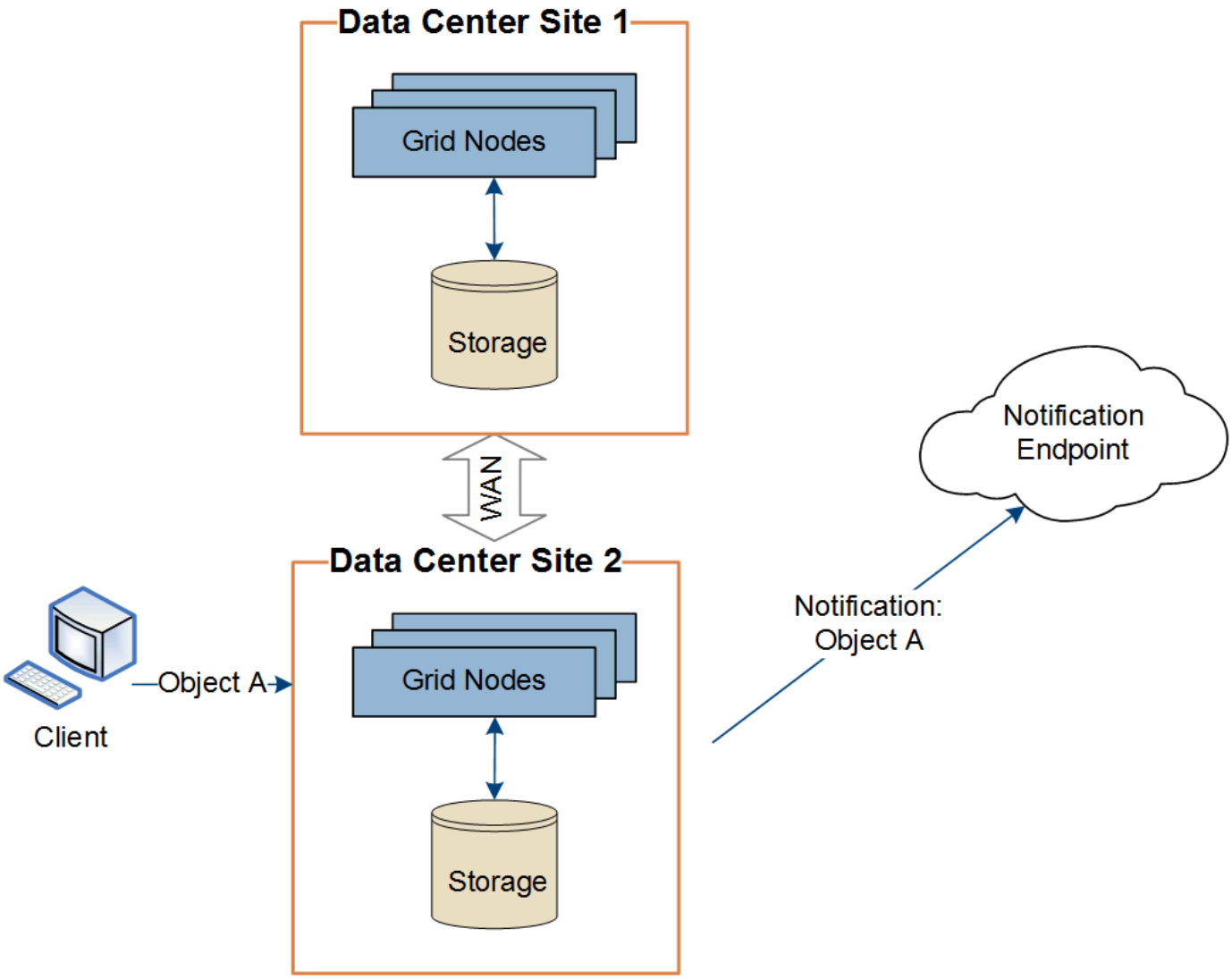
按站點交付 **StorageGRID** 平台服務訊息

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 **StorageGRID** 平台服務

平台服務中使用的端點由租用戶使用者在 Tenant Manager 中建立和維護。但是，如果租用戶在設定或使用平台服務時遇到問題，您可以嘗試使用 Grid Manager 來協助解決問題。

新端點的問題

租戶必須先使用租戶管理程式建立一或多個端點、才能使用平台服務。每個端點代表一個平台服務的外部目的地、例如 StorageGRID S3 儲存庫、 Amazon Web Services 儲存庫、 Amazon Simple Notification Service 主題、 Kafka 主題、或本地或 AWS 上託管的 ElasticSearch 叢集。每個端點都包括外部資源的位置、以及存取該資源所需的認證資料。

當租戶建立端點時StorageGRID 、此驗證系統會驗證端點是否存在、以及是否可以使用指定的認證來達到端點。端點的連線會從每個站台的一個節點驗證。

如果端點驗證失敗、會出現錯誤訊息、說明端點驗證失敗的原因。租戶使用者應解決此問題、然後再次嘗試建立端點。

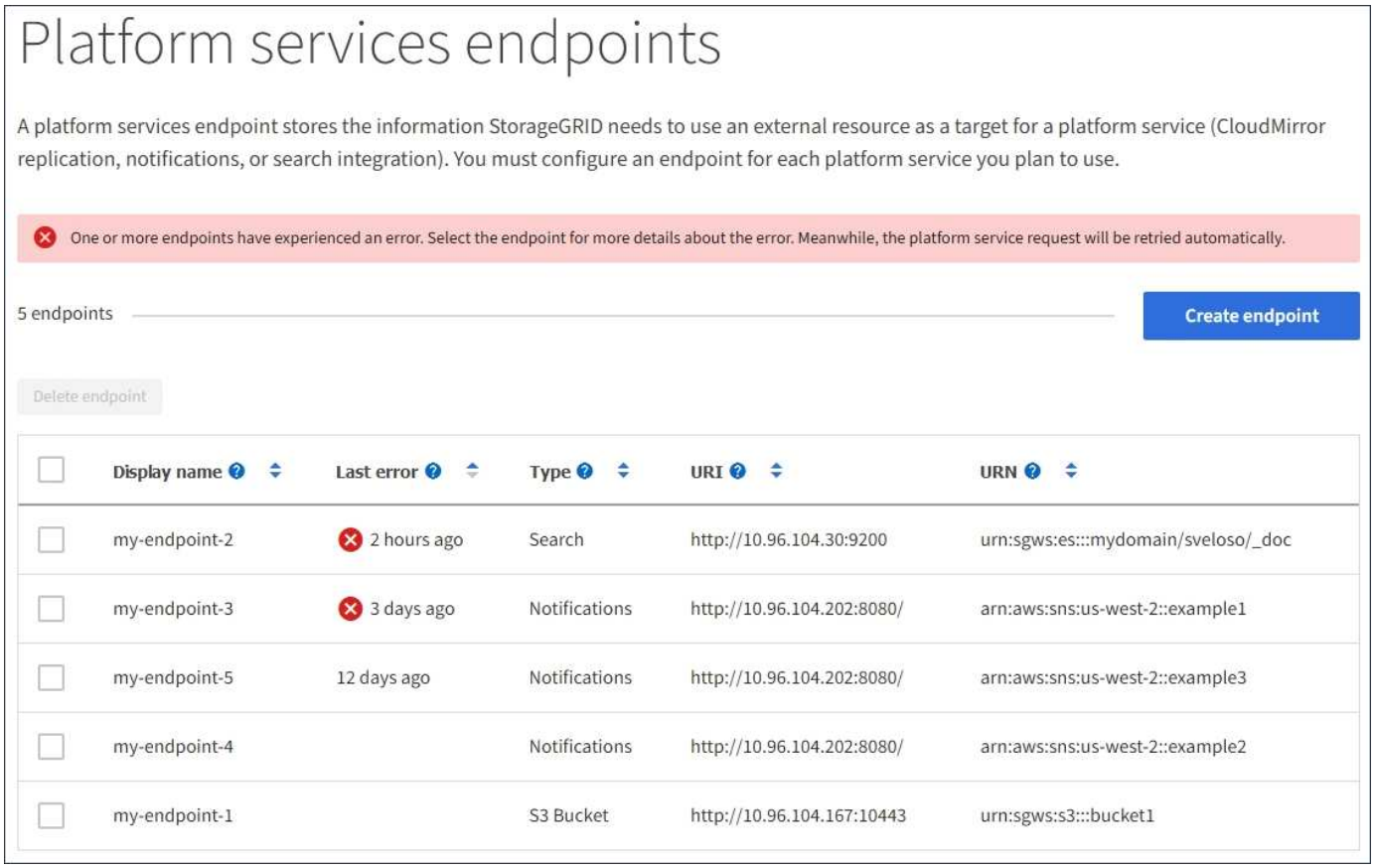
如果未啟用租戶帳戶的平台服務、端點建立將會失敗。

現有端點的問題

如果 StorageGRID 嘗試連線至現有端點時發生錯誤、租戶管理程式的儀表板上會顯示訊息。

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

租用戶使用者可以前往「端點」頁面，查看每個端點的最新錯誤訊息，並確認錯誤發生的時間。「上次錯誤」欄位顯示每個端點的最新錯誤訊息，並指示錯誤發生的時間。包含 圖示的錯誤表示過去 7 天內發生的錯誤。



*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

如果您已配置"儲存代理伺服器"在儲存節點和平台服務端點之間，如果您的代理服務不允許來自StorageGRID的訊息，則可能會發生錯誤。若要解決這些問題，請檢查代理伺服器的設置，以確保與平台服務相關的訊息不會被封鎖。

確定是否發生錯誤

如果過去 7 天內發生任何端點錯誤、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. 選擇 節點 > 網站 > 儲存節點 > 概覽*。
2. 檢查警報表中的活動警報。
3. 解決所有活動警報。如有需要，請聯絡技術支援。

可恢復和不可恢復的端點錯誤

建立端點之後、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。
- 目標儲存桶不存在。
- 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

其他錯誤是無法恢復的。例如，以下原因可能會發生不可恢復的錯誤：

- 端點已刪除。
- Webhook 端點目標透過以下方式回應通知請求 `400 Bad Request`錯誤。

如果 StorageGRID 遇到無法恢復的端點錯誤：

- 在 Grid Manager 中、前往 * 支援 * > * 工具 * > * 指標 * > * Grafana* > * 平台服務總覽 * 、檢視錯誤詳細資料。
- 在 Tenant Manager 中、前往 * 儲存設備 （ S3 ） * > * 平台服務端點 * 檢視錯誤詳細資料。
- 檢查 `/var/local/log/bycast-err.log`相關錯誤。具有 ADC 服務的儲存節點包含此記錄檔。

無法傳送平台服務訊息

如果目標遇到問題而無法接受平台服務訊息，則儲存桶上的用戶端操作會成功，但平台服務訊息不會被傳遞。例如，如果在目標上更新憑證，使得StorageGRID無法再對目標服務進行身份驗證，則可能會發生此錯誤。

檢查相關警示。

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。

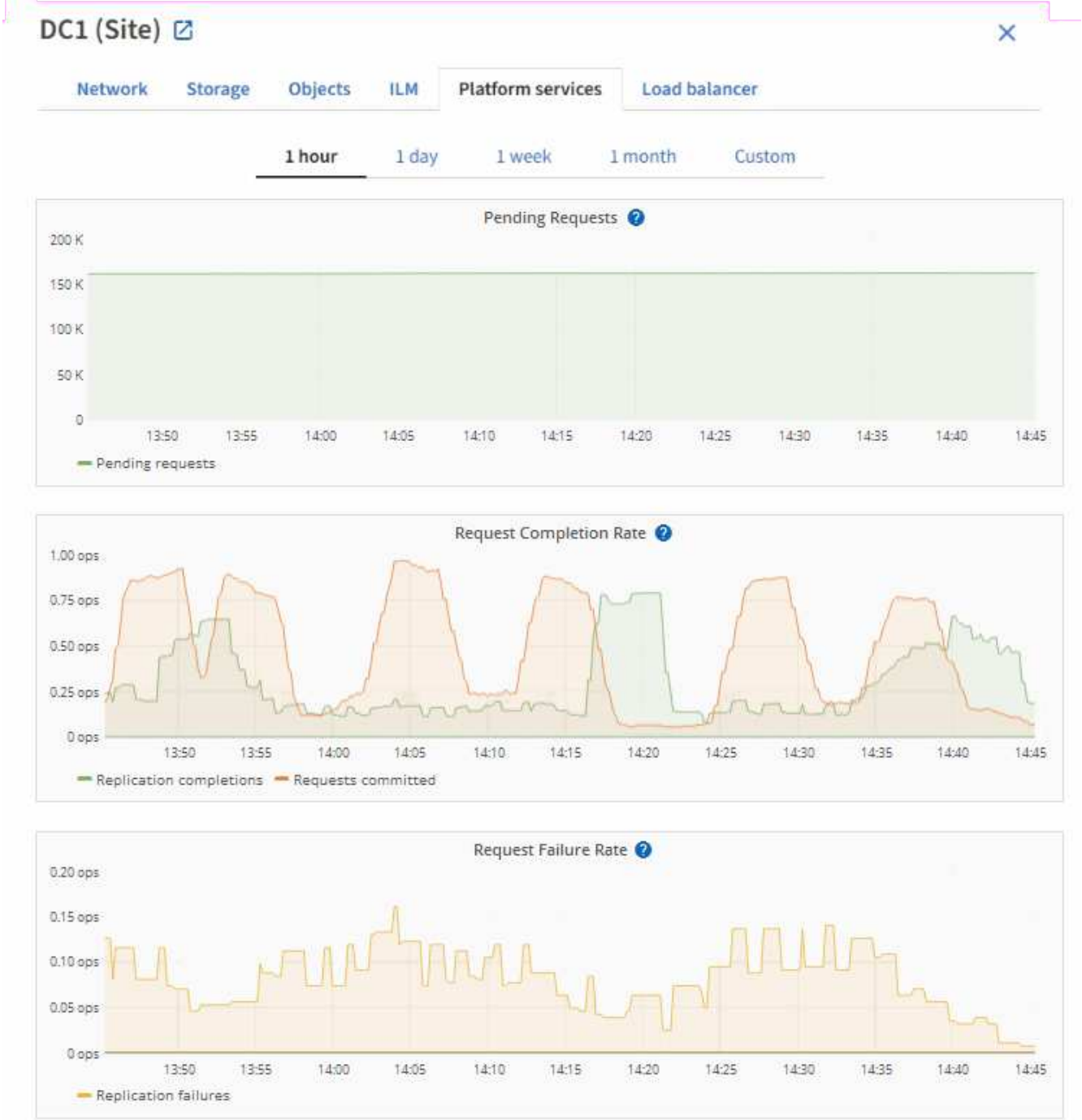
唯一的可見效果是傳入S3要求執行時間較長。如果您開始偵測到效能大幅降低、應該降低擷取速度、或是使用容量較大的端點。如果要求的待處理項目持續增加、用戶端S3作業（例如PUT要求）最終將會失敗。

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。（儲存節點上也包含 ADC 服務的 RSM 服務。）然後、請確保大多數儲存節點都在執行中且可供使用。

如果站台上有多個包含RSM服務的儲存節點故障、您就會遺失該站台的任何擱置中平台服務要求。

平台服務端點的其他疑難排解指南

如需其他資訊使用租戶帳戶 › 疑難排解平台服務端點、請參閱。

相關資訊

"疑難排解 StorageGRID 系統"

在 **StorageGRID** 中為租戶帳戶管理 **S3 Select**

您可以允許某些S3租戶使用S3 Select針對個別物件發出SelectObjectContent要求。

S3 Select提供一種有效率的方法來搜尋大量資料、而不需要部署資料庫和相關資源來啟用搜尋。它也能降低擷取資料的成本與延遲。

什麼是**S3 Select**？

S3 Select可讓S3用戶端使用SelectObjectContent要求來篩選及擷取物件所需的資料。S3 Select的支援功能包括S3 Select命令與功能的子集。StorageGRID

使用**S3 Select**的考量與要求

網格管理需求

網格管理員必須授予租戶 S3 Select 權限。當或時選擇 * 允許 S3 Select* "建立租戶""編輯租戶"。

物件格式需求

您要查詢的物件必須採用下列其中一種格式：

- * CSV* 。可依原樣使用、也可壓縮至 GZIP 或 bzip2 歸檔。
- * 硬地板 * 。硬地板物件的其他需求：
  - S3 Select 僅支援使用 GZIP 或 Snappy 進行柱式壓縮。S3 Select 不支援 Parquet 物件的全物件壓縮。
  - S3 Select 不支援硬地板輸出。您必須將輸出格式指定為 CSV 或 JSON 。
  - 最大未壓縮列群組大小為 512 MB 。
  - 您必須使用物件架構中指定的資料類型。
  - 您無法使用時間間隔、 JSON 、清單、時間或 UUID 邏輯類型。

端點需求

SelectObjectContent 要求必須傳送至"負載平衡器端點StorageGRID"。

端點使用的管理節點和閘道節點必須是下列其中一項：

- 服務應用裝置節點
- VMware 型軟體節點
- 執行核心且啟用 cgroup v2 的裸機節點

一般考量

查詢無法直接傳送至儲存節點。

SelectObjectContent要求可降低所有S3用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。

請參閱"使用S3 Select的說明"。

查看"Grafana圖表"對於 S3 選擇隨時間推移的操作，在網格管理員中選擇 支援 > 工具 > 指標。

設定用戶端連線

設定 **S3** 用戶端連線至 **StorageGRID**

身為網格管理員、您可以管理組態選項、以控制 S3 用戶端應用程式如何連線至 StorageGRID 系統、以儲存及擷取資料。

Swift 詳細資料已從此文件網站版本中移除。請參閱。 "StorageGRID 11.8 ：設定 S3 和 Swift 用戶端連線"

組態工作

1. 根據用戶端應用程式與 StorageGRID 的連線方式、在 StorageGRID 中執行必要工作。

必要的工作

您必須取得：

- IP位址
- 網域名稱
- SSL 憑證

選用工作

您也可以選擇設定：

- 身分識別聯盟
- SSO

1. 使用 StorageGRID 取得應用程式連線至網格所需的值。您可以使用 S3 設定精靈、或手動設定每個 StorageGRID 實體。+

使用 **S3** 設定精靈

請依照 S3 安裝精靈中的步驟進行。

手動設定

1. 建立高可用度群組
2. 建立負載平衡器端點
3. 建立租戶帳戶
4. 建立貯體和存取金鑰
5. 設定 ILM 規則和原則

1. 使用 S3 應用程式完成與 StorageGRID 的連線。建立 DNS 項目、將 IP 位址與您打算使用的任何網域名稱建立關聯。

   視需要執行其他應用程式設定。

2. 在應用程式和 StorageGRID 中執行持續的工作、以隨時間而管理和監控物件儲存。

將 **StorageGRID** 附加至用戶端應用程式所需的資訊

在將 StorageGRID 附加到 S3 用戶端應用程式之前、您必須先在 StorageGRID 中執行組態步驟、並取得特定值。

我需要什麼價值？

下表顯示您必須在 StorageGRID 中設定的值、以及 S3 應用程式和 DNS 伺服器使用這些值的位置。

價值	其中已設定值	使用值的位置
虛擬 IP （ VIP ）位址	StorageGRID > HA 群組	DNS 項目
連接埠	StorageGRID > 負載平衡器端點	用戶端應用程式
SSL 憑證	StorageGRID > 負載平衡器端點	用戶端應用程式
伺服器名稱（ FQDN ）	StorageGRID > 負載平衡器端點	• 用戶端應用程式 • DNS 項目
S3 存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租戶與貯體	用戶端應用程式
貯體 / 容器名稱	StorageGRID > 租戶與貯體	用戶端應用程式

如何取得這些價值？

視您的需求而定、您可以執行下列任一動作來取得所需資訊：

- * 使用 "S3 設定精靈"* 。S3 安裝精靈可協助您快速設定 StorageGRID 中的必要值、並輸出一個或兩個檔案、供您在設定 S3 應用程式時使用。精靈會引導您完成必要步驟、並協助確保您的設定符合 StorageGRID 最佳實務做法。

  如果您正在設定 S3 應用程式、建議您使用 S3 安裝精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 使用 "FabricPool 設定精靈"* 。與 S3 設定精靈類似、 FabricPool 設定精靈可協助您快速設定所需的值、並輸出可在 ONTAP 中設定 FabricPool 雲端層時使用的檔案。

  如果您計畫將 StorageGRID 作為 FabricPool 雲端層的物件儲存系統、建議您使用 FabricPool 設定精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 手動設定項目 * 。如果您要連線到 S3 應用程式、而不想使用 S3 設定精靈、您可以手動執行組態來取得所需的值。請遵循下列步驟：

  a. 設定您要用於 S3 應用程式的高可用度（ HA ）群組。請參閱。 "設定高可用度群組"
  b. 建立 S3 應用程式將使用的負載平衡器端點。請參閱。 "設定負載平衡器端點"
  c. 建立 S3 應用程式將使用的租戶帳戶。請參閱。 "建立租戶帳戶"
  d. 對於 S3 租戶、請登入租戶帳戶、然後為每個存取應用程式的使用者產生存取金鑰 ID 和秘密存取金鑰。請參閱。 "建立您自己的存取金鑰"
  e. 在租戶帳戶內建立一或多個 S3 儲存區。對於 S3 ，請參閱"建立S3儲存區"。
  f. 若要為屬於新租戶或貯體 / 容器的物件新增特定放置指示、請建立新的 ILM 規則、並啟動新的 ILM 原則以使用該規則。請參閱"建立ILM規則"和"建立ILM原則"。

StorageGRID 中 **S3** 用戶端的安全性

StorageGRID 租戶帳戶使用 S3 用戶端應用程式、將物件資料儲存至 StorageGRID 。您應該檢閱為用戶端應用程式實作的安全性措施。

摘要

下表摘要說明如何實作 S3 REST API 的安全性：

連線安全性
: TLS

伺服器驗證
: 由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證

用戶端驗證
: S3 帳戶存取金鑰 ID 和秘密存取金鑰

用戶端授權
: 貯體擁有權及所有適用的存取控制原則

StorageGRID 如何為用戶端應用程式提供安全性

S3 用戶端應用程式可以連線至 Gateway 節點或管理節點上的負載平衡器服務、或直接連線至 Storage Node 。

- 連接到負載平衡器服務的用戶端可以根據您的方式使用 HTTPS 或 HTTP "設定負載平衡器端點"。

  HTTPS 提供安全的 TLS 加密通訊、建議使用。您必須將安全性憑證附加至端點。

  HTTP 提供較不安全的未加密通訊、只能用於非正式作業或測試網格。

- 連線至儲存節點的用戶端也可以使用 HTTPS 或 HTTP 。

  HTTPS 是預設值、建議使用。

  HTTP 提供較不安全的未加密通訊、但可選擇性"已啟用"用於非正式作業或測試網格。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。
- 用戶端必須提供"HTTP 驗證標頭"給 StorageGRID 才能執行 REST API 作業。

安全性憑證與用戶端應用程式

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線到負載平衡器服務時、會使用為負載平衡器端點設定的憑證。每個負載平衡器端點都有自己的憑證 &#8212 ；網格管理員上傳的自訂伺服器憑證、或是網格管理員在設定端點時在 StorageGRID 中產生的憑證。

  請參閱。 "負載平衡考量"

- 當用戶端應用程式直接連線至儲存節點時、它們會使用安裝 StorageGRID 系統（由系統憑證授權單位簽署）時為儲存節點產生的系統產生的伺服器憑證、 或是由網格管理員提供給網格的單一自訂伺服器憑證。請參閱。 "新增自訂的 S3 API 憑證"

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

TLS程式庫支援的雜湊和加密演算法

StorageGRID系統支援一組用戶端應用程式在建立 TLS 會話時可以使用的密碼套件。若要設定密碼，請前往*設定*>*安全*>*安全設定*並選擇*TLS 和 SSH 原則*。

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

> 不再支援SSLv3和TLS 1.1（或更早版本）。

使用 **S3** 設定精靈

StorageGRID S3 設定精靈的考量與需求

您可以使用 S3 設定精靈、將 StorageGRID 設定為 S3 應用程式的物件儲存系統。

何時使用 **S3** 設定精靈

S3 安裝精靈會引導您完成每個步驟、設定 StorageGRID 以搭配 S3 應用程式使用。在完成精靈的過程中、您可以下載檔案、以便在 S3 應用程式中輸入值。使用精靈可更快速地設定您的系統、並確保您的設定符合 StorageGRID 最佳實務做法。

如果您有"root 存取權限"、可以在開始使用 StorageGRID Grid Manager 時完成 S3 設定精靈、也可以在稍後隨時存取並完成精靈。視您的需求而定、您也可以手動設定部分或全部必要項目、然後使用精靈來組合 S3 應用程式所需的值。

使用精靈之前

使用精靈之前、請確認您已完成這些先決條件。

取得 **IP** 位址並設定 **VLAN** 介面

如果您要設定高可用度（ HA ）群組、就會知道 S3 應用程式將連線到哪些節點、以及將使用哪個 StorageGRID 網路。您也知道要輸入哪些子網路 CIDR 、閘道 IP 位址和虛擬 IP （ VIP ）位址值。

如果您打算使用虛擬 LAN 來分隔 S3 應用程式的流量、則表示您已經設定了 VLAN 介面。請參閱。 "設定VLAN介面"

設定身分識別聯盟和 **SSO**

如果您打算對StorageGRID系統使用身分聯合或單一登入 (SSO)，則您已啟用這些功能。您也知道哪個聯合群組應該對 S3 應用程式將使用的租用戶帳戶具有根存取權限。看"使用身分識別聯盟"和"設定單一登入"。

取得及設定網域名稱

您知道 StorageGRID 要使用哪個完整網域名稱（ FQDN ）。網域名稱伺服器（ DNS ）項目會將此 FQDN 對應到您使用精靈建立的 HA 群組的虛擬 IP （ VIP ）位址。

如果您打算使用 S3 虛擬託管式請求，則應該"已設定 S3 端點網域名稱"。建議使用虛擬託管式請求。

檢閱負載平衡器和安全性憑證需求

如果您計畫使用 StorageGRID 負載平衡器、您已檢閱負載平衡的一般考量事項。您擁有要上傳的憑證或產生憑證所需的值。

如果您打算使用外部（第三方）負載平衡器端點、則該負載平衡器具有完整網域名稱（ FQDN ）、連接埠和憑證。

設定任何網格同盟連線

如果您希望允許 S3 租戶使用網格聯合連線將帳戶資料同步並複寫儲存桶物件到另一個網格，請在啟動精靈之前確認以下內容：

- 您有 "已設定網格同盟連線"。
- 連線狀態為 * 已連線 * 。

- 您擁有root存取權限。

在 **StorageGRID** 中存取並完成 **S3** 設定精靈

您可以使用 S3 設定精靈來設定 StorageGRID 、以便搭配 S3 應用程式使用。安裝精靈提供應用程式存取 StorageGRID 儲存區和儲存物件所需的值。

開始之前

- 您有"root 存取權限"。
- 您已檢閱"考量與要求"以使用精靈。

存取精靈

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 如果儀表板上出現「* FabricPool and S3 設定精靈*」橫幅，請選擇橫幅中的連結。如果橫幅不再顯示，請從 Grid Manager 的標題列中選擇說明圖示 ，然後選擇「* FabricPool and S3 設定精靈*」。
3. 在 FabricPool and S3 安裝精靈頁面的 S3 應用程式區段中、選取 * 立即設定 * 。

步驟 **6** 之 **1** ：設定 **HA** 群組

HA 群組是每個節點包含 StorageGRID 負載平衡器服務的集合。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用 HA 群組來協助保持 S3 資料連線可用。如果 HA 群組中的作用中介面發生故障、備份介面就能管理工作負載、對 S3 作業幾乎沒有影響。

如需此工作的詳細資訊，請參閱"管理高可用度群組"。

步驟

1. 如果您打算使用外部負載平衡器、則不需要建立 HA 群組。選擇 * 跳過此步驟 * 並轉至步驟 2 、共 6 步：設定負載平衡器端點。
2. 若要使用 StorageGRID 負載平衡器、您可以建立新的 HA 群組或使用現有的 HA 群組。

建立**HA**群組

a. 若要建立新的 HA 群組、請選取 * 建立 HA 群組 * 。

b. 如需 * 輸入詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
HA 群組名稱	此 HA 群組的唯一顯示名稱。
說明（選用）	此 HA 群組的描述。

c. 在 * 新增介面 * 步驟中、選取您要在此 HA 群組中使用的節點介面。

使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。

您可以選取一或多個節點、但每個節點只能選取一個介面。

d. 對於「介面優先順序」步驟、請判斷此 HA 群組的主要介面和任何備份介面。

拖曳列以變更 * 優先順序 * 欄中的值。

清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。

如果 HA 群組包含多個介面、且作用中介面故障、則虛擬 IP （ VIP ）位址會依照優先順序移至第一個備份介面。如果該介面故障、VIP位址會移至下一個備份介面、依此類推。解決故障時、 VIP 位址會移回可用的最高優先順序介面。

e. 在 * 輸入 IP 位址 * 步驟中、請填寫下列欄位。

欄位	說明
子網路 CIDR	以 CIDR 表示法和 #8212 表示的 VIP 子網路位址； IPv4 位址後面接著斜線和子網路長度（ 0-32 ）。 網路位址不得設定任何主機位元。例如 `192.16.0.0/22`：。
閘道 IP 位址（選用）	如果用於存取 StorageGRID 的 S3 IP 位址與 StorageGRID VIP 位址不在同一子網路上、請輸入 StorageGRID VIP 本機閘道 IP 位址。本機閘道IP位址必須位於VIP子網路內。
虛擬 IP 位址	為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內。 至少一個位址必須是 IPv4 。您也可以指定其他的IPv6位址。

f. 選取 * 建立 HA 群組 * 、然後選取 * 完成 * 以返回 S3 設定精靈。

g. 選取 * 繼續 * 以移至負載平衡器步驟。

使用現有 **HA** 群組

a. 若要使用現有的 HA 群組、請從 * 選取 HA 群組 * 中選取 HA 群組名稱。

b. 選取 * 繼續 * 以移至負載平衡器步驟。

步驟 **2** 、共 **6** 步：設定負載平衡器端點

StorageGRID 使用負載平衡器從用戶端應用程式管理工作負載。負載平衡可將多個儲存節點的速度和連線容量最大化。

您可以使用 StorageGRID 負載平衡器服務（存在於所有閘道和管理節點上）、也可以連線至外部（第三方）負載平衡器。建議使用 StorageGRID 負載平衡器。

如需此工作的詳細資訊，請參閱"負載平衡考量"。

若要使用 StorageGRID 負載平衡器服務、請選取 * StorageGRID 負載平衡器 * 索引標籤、然後建立或選取您要使用的負載平衡器端點。若要使用外部負載平衡器、請選取 * 外部負載平衡器 * 索引標籤、並提供您已設定之系統的詳細資料。

建立端點

步驟

1. 若要建立負載平衡器端點、請選取 * 建立端點 * 。
2. 如需 * 輸入端點詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
名稱	端點的描述性名稱。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為您建立的第一個端點為 10433 、但您可以輸入任何未使用的外部連接埠。如果您輸入 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。 *注意：*不允許使用其他網格服務使用的連接埠。看"內部連接埠StorageGRID" 。
用戶端類型	必須是 *S3 * 。
網路傳輸協定	選擇* HTTPS *。 • 注意 * ：支援與 StorageGRID 通訊、但不建議使用 TLS 加密。

3. 對於 *Select 綁定模式 * 步驟，請指定綁定模式。繫結模式可控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

模式	說明
全域（預設）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。

4. 對於租戶存取步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

5. 對於 * 附加憑證 * 步驟、請選取下列其中一項：

欄位	說明
上傳憑證（建議）	使用此選項可上傳 CA 簽署的伺服器憑證、憑證私密金鑰及選用的 CA 套件組合。
產生憑證	使用此選項可產生自我簽署的憑證。如需詳細的輸入內容、請參閱"設定負載平衡器端點"。
使用 StorageGRID S3 憑證	只有在您已上傳或產生 StorageGRID 通用憑證的自訂版本時、才可使用此選項。如需詳細資訊、請參閱 "設定 S3 API 憑證" 。

6. 選擇 * 完成 * 返回 S3 設定精靈。
7. 選擇 * 繼續 * 以前往租戶和貯體步驟。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

使用現有負載平衡器端點

步驟

1. 若要使用現有的端點、請從 * 選取負載平衡器端點 * 中選取其名稱。
2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

使用外部負載平衡器

步驟

1. 若要使用外部負載平衡器、請填寫下列欄位。

欄位	說明
FQDN	外部負載平衡器的完整網域名稱（ FQDN ）。
連接埠	S3 應用程式用來連線到外部負載平衡器的連接埠編號。
憑證	複製外部負載平衡器的伺服器憑證、然後貼到此欄位。

2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

步驟 **3** 、共 **6** 步：建立租戶和貯體

租戶是可以使用 S3 應用程式在 StorageGRID 中儲存及擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、貯體、物件和一組特定功能。

貯體是用來儲存租戶物件和物件中繼資料的容器。雖然租戶可能有許多貯體、但精靈可協助您以最快且最簡單的方式建立租戶和貯體。如果您稍後需要新增儲存區或設定選項、可以使用租戶管理程式。

有關此任務的詳細信息，請參閱"建立租戶帳戶"和"建立S3儲存區"。

步驟

1. 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。

2. 根據您的StorageGRID系統是否使用，定義租用戶帳戶的根存取權限"身分識別聯盟"，"單一登入（ SSO ）"，或兩者兼而有之。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。
如果已啟用身分識別聯盟	a. 選取要提供給租用戶的現有同盟群組"root 存取權限"。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取要提供給租用戶的現有同盟群組"root 存取權限"。沒有本機使用者可以登入。

3. 如果您希望精靈為 root 使用者建立存取金鑰 ID 和秘密存取金鑰、請選取 * 自動建立 root 使用者 S3 存取金鑰 * 。

   如果租戶的唯一使用者是 root 使用者、請選取此選項。如果其他使用者將使用此租用戶、則"使用 Tenant Manager"可設定金鑰和權限。

4. 如果您現在想為此租戶建立貯體、請選取 * 為此租戶建立貯體 * 。

   如果已啟用網格的 S3 物件鎖定功能、則在此步驟建立的儲存格並未啟用 S3 物件鎖定功能。如果您需要為此 S3 應用程式使用 S3 物件鎖定貯體、請勿現在選擇建立貯體。請改用 Tenant Manager "建立貯體"稍後再執行。

   a. 輸入 S3 應用程式將使用的儲存區名稱。例如 `s3-bucket` ：。

      您無法在建立貯體之後變更貯體名稱。

   b. 為此貯體選取 * 區域 * 。

使用預設區域(`us-east-1`）、除非您預期未來會使用 ILM 來根據貯體的區域篩選物件。

5. 選取 * 建立並繼續 * 。

步驟 **4** 、共 **6** 步：下載資料

在下載資料步驟中、您可以下載一或兩個檔案、以儲存您剛設定的詳細資料。

步驟

1. 如果您選取 * 自動建立 root 使用者 S3 存取金鑰 * 、請執行下列其中一項或兩項操作：
   - 選取 * 下載存取金鑰 * 以下載 `.csv`包含租戶帳戶名稱、存取金鑰 ID 和秘密存取金鑰的檔案。
   - 選擇複製圖示（）將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。
2. 選取 * 下載組態值 * 以下載 `.txt`包含負載平衡器端點、租戶、貯體和根使用者設定的檔案。
3. 將此資訊儲存至安全的位置。

> 在複製兩個存取金鑰之前、請勿關閉此頁面。關閉此頁面後、金鑰將無法使用。請務必將此資訊儲存在安全的位置、因為此資訊可用於從 StorageGRID 系統取得資料。

4. 如果出現提示、請選取核取方塊、確認您已下載或複製金鑰。
5. 選取 * 繼續 * 以移至 ILM 規則和原則步驟。

第 **5** 步、共 **6** 步：審查 **S3** 的 **ILM** 規則和 **ILM** 原則

資訊生命週期管理（ ILM ）規則可控制 StorageGRID 系統中所有物件的放置、持續時間和擷取行為。StorageGRID 隨附的 ILM 原則會為所有物件建立兩個複寫複本。此原則會生效、直到您至少啟動一個新原則為止。

步驟

1. 檢閱頁面上提供的資訊。
2. 如果您要新增屬於新租戶或貯體之物件的特定指示、請建立新規則和新原則。請參閱"建立ILM規則"和"使用 ILM 原則"。
3. 請選擇 * 我已檢閱這些步驟、並瞭解我需要做什麼 * 。
4. 選取核取方塊、表示您瞭解接下來該怎麼做。
5. 選擇 * 繼續 * 前往 * 摘要 * 。

步驟 **6** 之 **6** ：檢視摘要

步驟

1. 檢閱摘要。
2. 請記下後續步驟中的詳細資料、其中說明在連線到 S3 用戶端之前可能需要的其他組態。例如、選取 * 以 root 身分登入 * 會將您帶到租戶管理員、您可以在其中新增租戶使用者、建立其他貯體、以及更新貯體設定。
3. 選擇*完成*。
4. 使用您從 StorageGRID 下載的檔案或手動取得的值來設定應用程式。

了解 **StorageGRID** 高可用性群組

高可用度（ HA ）群組可為 S3 用戶端提供高可用度的資料連線、以及與 Grid Manager 和 Tenant Manager 的高可用度連線。

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。

每個HA群組均可存取所選節點上的共享服務。

- 包括閘道節點、管理節點或兩者的 HA 群組、可為 S3 用戶端提供高可用度的資料連線。
- 僅包含管理節點的HA群組可提供高可用度的網格管理程式和租戶管理程式連線。
- 只包含服務應用裝置和 VMware 軟體節點的 HA 群組可為提供高可用度"使用S3 Select的S3租戶"的連線。使用S3 Select時建議使用HA群組、但不需要。

如何建立**HA**群組？

1. 您可以為一個或多個管理節點或閘道節點選取網路介面。您可以使用Grid Network（eth0）介面、用戶端網路（eth2）介面、VLAN介面、或是新增至節點的存取介面。

   如果 HA 群組具有 DHCP 指派的 IP 位址、則無法將介面新增至 HA 群組。

2. 您可以指定一個介面做為主要介面。主介面是作用中介面、除非發生故障。
3. 您可以決定任何備份介面的優先順序。
4. 您可以為群組指派一到10個虛擬IP（VIP）位址。用戶端應用程式可以使用這些VIP位址來連線StorageGRID至

有關說明，請參閱"設定高可用度群組"。

什麼是作用中介面？

正常運作期間、HA群組的所有VIP位址都會新增至主要介面、這是優先順序中的第一個介面。只要主介面仍可用、當用戶端連線至群組的任何VIP位址時、就會使用該介面。也就是說、在正常作業期間、主要介面是群組的「作用中」介面。

同樣地、在正常作業期間、 HA 群組的任何低優先順序介面都會做為「備份」介面。除非主要（目前使用中）介面無法使用、否則不會使用這些備份介面。

檢視節點的目前**HA**群組狀態

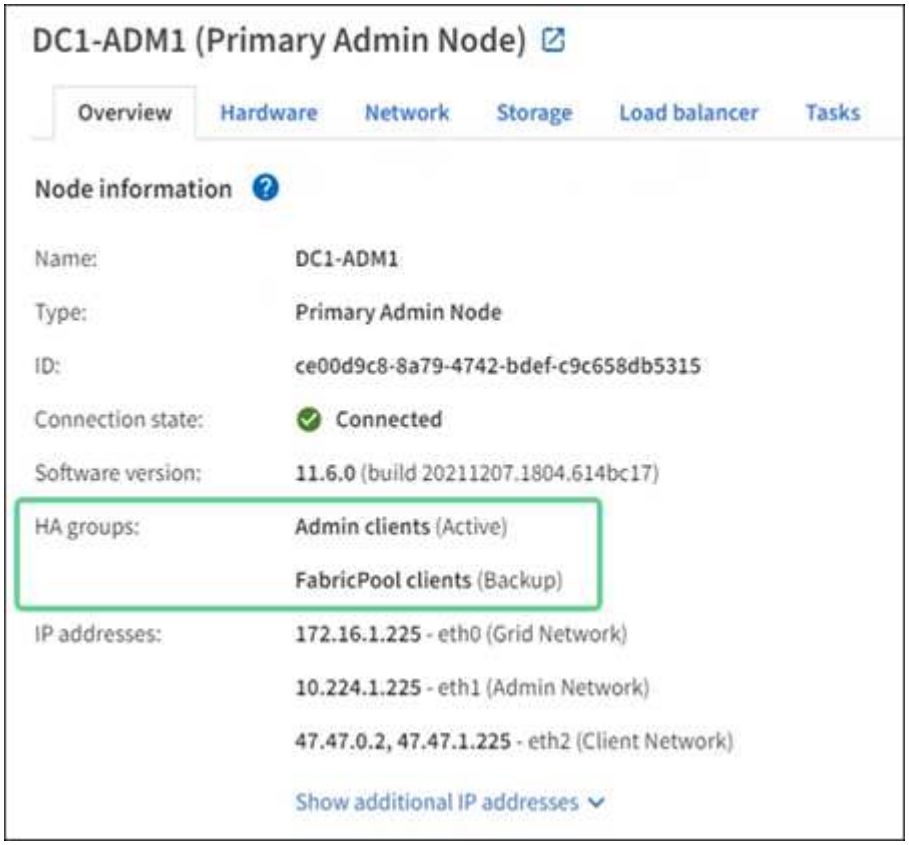
若要查看某個節點是否已指派給 HA 群組並確定其目前狀態，請選擇 **Nodes** > ***node***。

如果「總覽」索引標籤包含* HA群組*的項目、則該節點會指派給列出的HA群組。群組名稱後面的值是HA群組中節點的目前狀態：

- * Active*：HA群組目前裝載於此節點上。
- 備份：HA群組目前未使用此節點、這是備份介面。

- * 停止 * ：由於已手動停止高可用度（ keepalive ）服務、因此無法在此節點上裝載 HA 群組。
- * 故障 * ：由於下列一項或多項原因、因此無法在此節點上裝載 HA 群組：
  - 負載平衡器（Ngine-GW）服務未在節點上執行。
  - 節點的eth0或VIP介面關閉。
  - 節點當機。

在此範例中、主要管理節點已新增至兩個HA群組。此節點目前是管理用戶端群組的作用中介面、FabricPool 也是適用於「支援客戶」群組的備份介面。



當作用中介面故障時會發生什麼事？

目前裝載VIP位址的介面是作用中介面。如果HA群組包含多個介面、且作用中介面故障、VIP位址會依照優先順序移至第一個可用的備份介面。如果該介面故障、VIP位址會移至下一個可用的備份介面、依此類推。

容錯移轉可因下列任一原因觸發：

- 介面設定所在的節點會停機。
- 介面設定所在的節點至少失去與所有其他節點的連線2分鐘。
- 作用中介面關閉。
- 負載平衡器服務會停止。
- 高可用度服務停止。

主控作用中介面的節點外部網路故障可能不會觸發容錯移轉。同樣地、 Grid Manager 或 Tenant Manager 的服務也不會觸發容錯移轉。

容錯移轉程序通常只需幾秒鐘、而且速度足夠快、用戶端應用程式只會遇到些微影響、而且可以仰賴正常的重試行為來繼續作業。

當故障得以解決且優先順序較高的介面再次可用時、VIP位址會自動移至可用的最高優先順序介面。

StorageGRID HA 群組如何提供高可用性

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 用戶端提供高可用度的資料連線。
- 僅包含一個介面的HA群組可讓您提供多個VIP位址、並明確設定IPv6位址。

只有當群組中包含的所有節點都提供相同的服務時、HA群組才能提供高可用度。建立HA群組時、請從提供所需服務的節點類型新增介面。

- 管理節點：包括負載平衡器服務、並可存取Grid Manager或租戶管理程式。
- * 閘道節點 * ：包括負載平衡器服務。

HA群組的用途	將此類型的節點新增至**HA**群組
存取Grid Manager	• 主管理節點（主） • 非主要管理節點 *附註：*主要管理節點必須是主要介面。部分維護程序只能從主要管理節點執行。
僅限租戶管理程式存取	• 主要或非主要管理節點
S3客戶端存取—負載平衡器服務	• 管理節點 • 閘道節點
的 S3 用戶端存取"S3 Select"	• 服務應用裝置 • VMware軟體節點 附註：使用S3 Select時建議使用HA群組、但不需要。

搭配**Grid Manager**或**Tenant Manager**使用**HA**群組的限制

如果Grid Manager或Tenant Manager服務失敗、HA群組容錯移轉就不會觸發。

如果您在容錯移轉發生時登入Grid Manager或租戶管理程式、系統將會登出、您必須再次登入才能繼續執行工

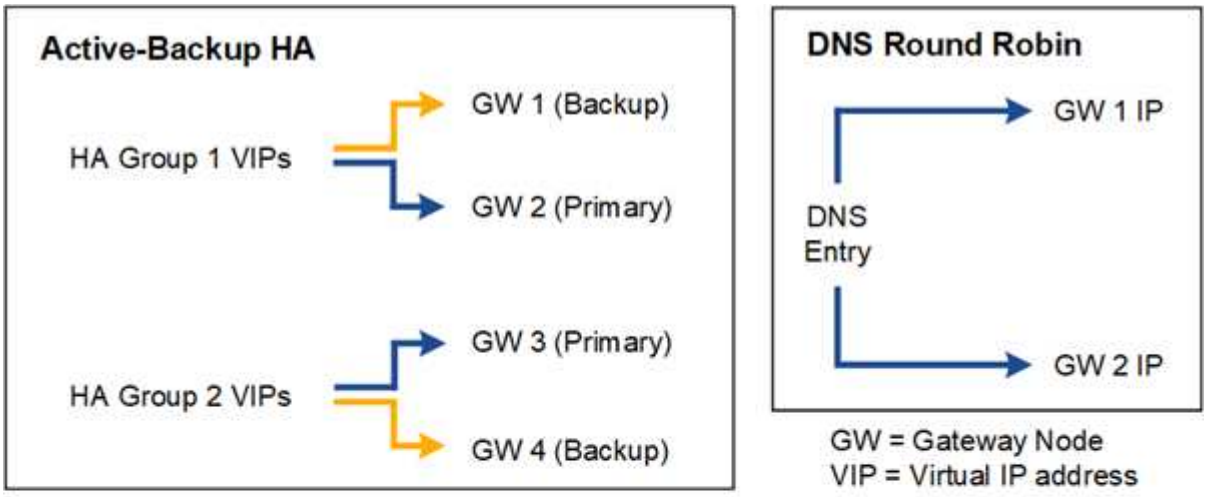
作。

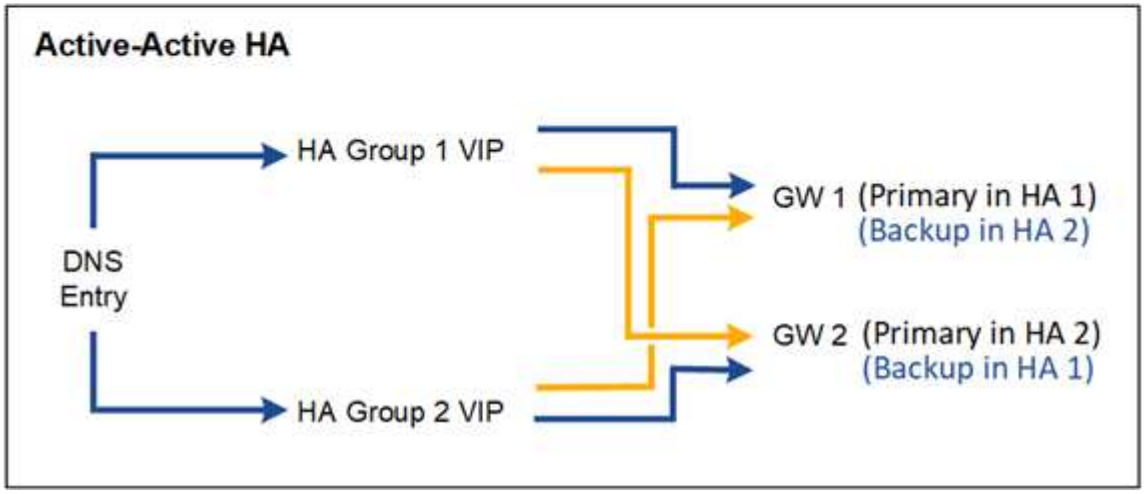
當主要管理節點無法使用時、無法執行某些維護程序。容錯移轉期間、您可以使用Grid Manager監控StorageGRID 您的作業系統。

StorageGRID 高可用性群組的設定選項

以下圖表提供了配置高可用性（ HA ）群組的不同方法範例。每個選項都有優點和缺點。

在圖中、藍色表示HA群組中的主要介面、黃色表示HA群組中的備份介面。





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。

組態	優勢	缺點
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。

在 **StorageGRID** 中設定高可用性群組

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。

StorageGRID系統最多可以有 255 個 HA 組。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"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：
  - **Linux**（安裝節點之前）："建立節點組態檔"
  - **Linux**（安裝節點後）："向節點新增中繼或存取介面"
  - **VMware**（安裝節點後）："向節點新增中繼或存取介面"

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

建立高可用度群組

當您建立高可用度群組時、請選取一或多個介面、然後依優先順序加以組織。然後、您將一個或多個VIP位址指派給群組。

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

存取精靈

步驟

1. 選擇*設定* > 網路 > 高可用性群組。

2. 選擇* Create （建立）。

輸入**HA**群組的詳細資料

步驟

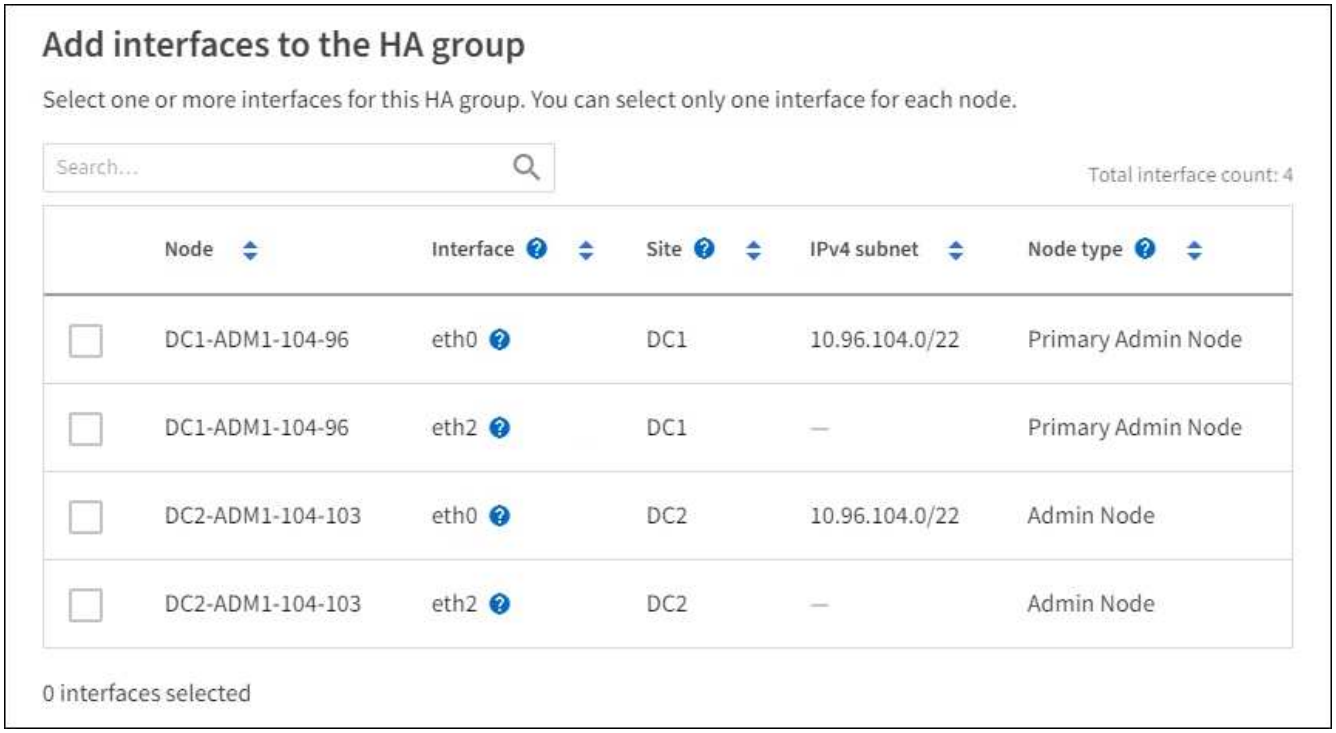
1. 為HA群組提供唯一名稱。
2. （可選）輸入HA群組的說明。
3. 選擇*繼續*。

新增介面至**HA**群組

步驟

1. 選取一或多個介面以新增至此HA群組。

   使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。



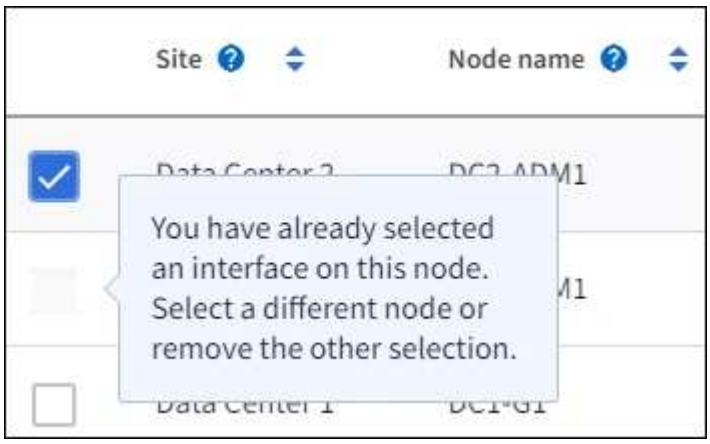
   建立VLAN介面之後、請等待5分鐘、讓新介面出現在表格中。

   選擇介面的準則

   - 您必須選取至少一個介面。
   - 您只能為節點選取一個介面。
   - 如果HA群組用於管理節點服務的HA保護（包括Grid Manager和Tenant Manager）、請選取「僅管理節點上的介面」。
   - 如果 HA 群組用於 S3 用戶端流量的 HA 保護、請選取管理節點、閘道節點或兩者的介面。
   - 如果您在不同類型的節點上選取介面、則會顯示資訊注意事項。系統會提醒您、如果發生容錯移轉、先前作用中節點所提供的服務可能無法在新作用中節點上使用。例如、備份閘道節點無法提供管理節點服

務的 HA 保護。同樣地、備份管理節點也無法執行主要管理節點所能提供的所有維護程序。

- 如果您無法選取介面、則其核取方塊會停用。工具提示提供更多資訊。



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

2. 選擇*繼續*。

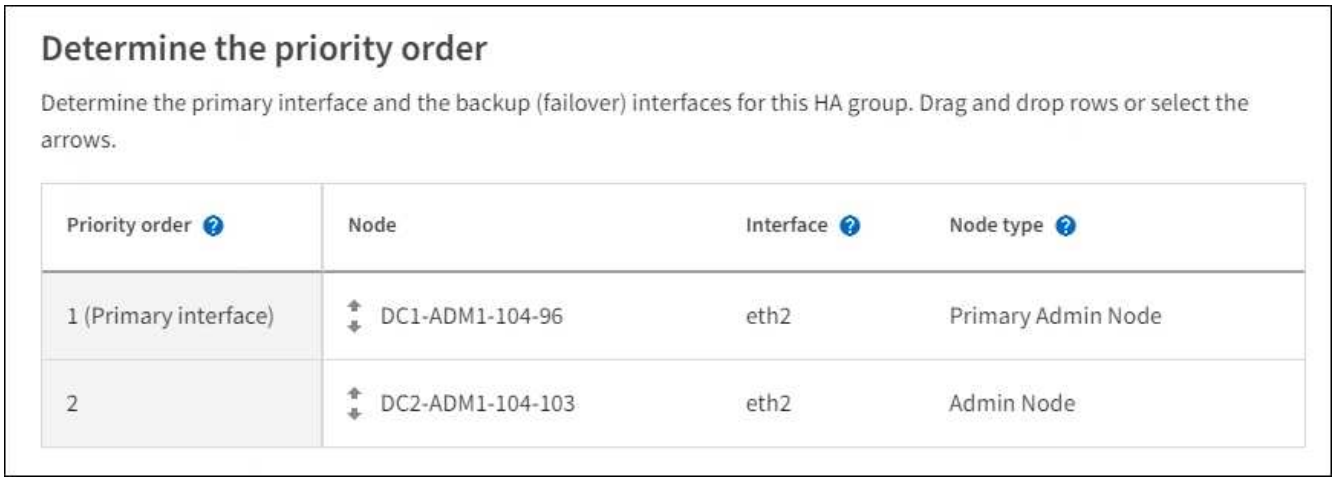
決定優先順序

如果 HA 群組包含多個介面、您可以判斷哪個是主要介面、哪些是備份（容錯移轉）介面。如果主要介面故障、VIP 位址會移至可用的最高優先順序介面。如果該介面故障、VIP位址會移至下一個可用的最高優先順序介面、依此類推。

步驟

1. 在 * 優先順序 * 欄中拖曳列、以決定主要介面和任何備份介面。

   清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。



如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行。

2. 選擇*繼續*。

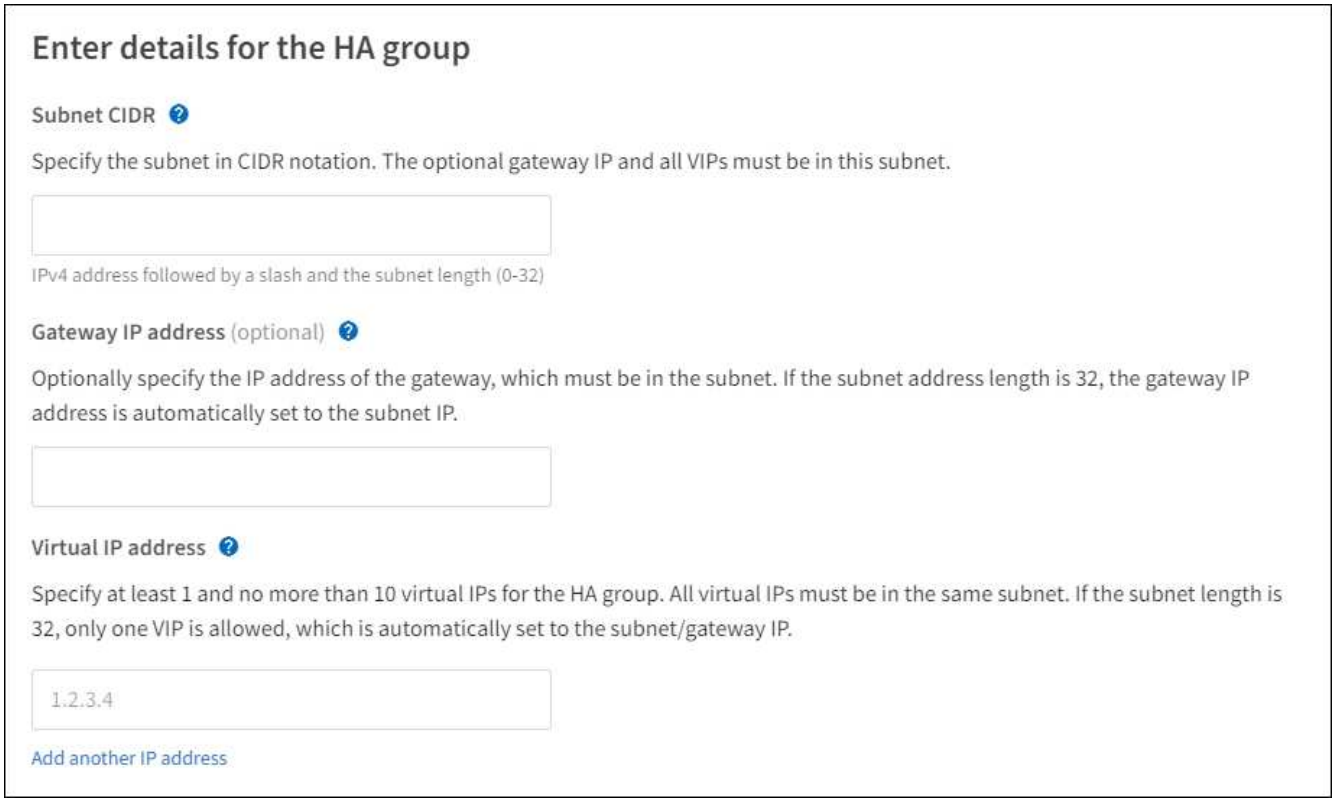
輸入**IP**位址

步驟

1. 在*子網路CID*欄位中、以CIDR表示法指定VIP子網路、即一種IPV4位址、後面接著一條斜槓和子網路長度（0-32）。

   網路位址不得設定任何主機位元。例如 `192.16.0.0/22`：。

   如果您使用32位元前置碼、VIP網路位址也會做為閘道位址和VIP位址。



2. 或者、如果任何 S3 管理用戶端或租戶用戶端將從不同的子網路存取這些 VIP 位址、請輸入 * 閘道 IP 位址 *。閘道位址必須位於VIP子網路內。

   用戶端和管理使用者將使用此閘道來存取虛擬IP位址。

3. 為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內、而且所有位址都會同時在作用中介面上作用。

   您必須至少提供一個IPV4位址。您也可以指定其他的IPv6位址。

4. 選擇* Create HA group（建立HA群組）、然後選取 Finish（完成）*。

   HA群組隨即建立、您現在可以使用已設定的虛擬IP位址。

後續步驟

如果您要使用此HA群組進行負載平衡、請建立負載平衡器端點、以判斷連接埠和網路傳輸協定、並附加任何必要的憑證。請參閱。 "設定負載平衡器端點"

編輯高可用度群組

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

例如、如果您想要在站台或節點取消委任程序中移除與所選介面相關聯的節點、則可能需要編輯HA群組。

步驟

1. 選擇*設定* > 網路 > 高可用性群組。

   「高可用度群組」頁面會顯示所有現有的HA群組。

2. 選取您要編輯之 HA 群組的核取方塊。
3. 根據您要更新的內容、執行下列其中一項：
   - 選取*「動作*」>*「編輯虛擬IP位址*」以新增或移除VIP位址。
   - 選取*「動作*」>*「編輯HA群組*」以更新群組的名稱或說明、新增或移除介面、變更優先順序、或新增或移除VIP位址。
4. 如果您選取*編輯虛擬IP位址*：
   a. 更新HA群組的虛擬IP位址。
   b. 選擇*保存*。
   c. 選擇*完成*。
5. 如果您選取*編輯HA群組*：
   a. 或者、請更新群組的名稱或說明。
   b. 或者、選取或清除核取方塊以新增或移除介面。

      如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行

   c. 您也可以拖曳資料列來變更此 HA 群組的主要介面和任何備份介面的優先順序。
   d. 或者、更新虛擬IP位址。
   e. 選取*「Save（儲存）」、然後選取「Finish（完成）」*。

移除高可用度群組

您可以一次移除一或多個高可用度（HA）群組。

如果 HA 群組繫結至負載平衡器端點、則無法移除該群組。若要刪除 HA 群組、您必須將其從任何使用它的負載平衡器端點中移除。

若要防止用戶端中斷、請在移除 HA 群組之前、更新任何受影響的 S3 用戶端應用程式。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*設定* > 網路 > 高可用性群組。

2. 檢閱您要移除之每個 HA 群組的 * 負載平衡器端點 * 欄。如果列出任何負載平衡器端點：
   a. 前往*配置* > 網路 > 負載平衡器端點。
   b. 選取端點的核取方塊。
   c. 選取*「動作*」>*「編輯端點繫結模式*」。
   d. 更新繫結模式以移除 HA 群組。
   e. 選取*儲存變更*。
3. 如果未列出負載平衡器端點、請選取您要移除的每個 HA 群組的核取方塊。
4. 選取 * 動作 * > * 移除 HA 群組 * 。
5. 檢閱訊息並選擇*刪除HA群組*以確認您的選擇。

   您選取的所有HA群組都會移除。「高可用度群組」頁面上會出現綠色的成功橫幅。

管理負載平衡

了解 **StorageGRID** 負載平衡

您可以使用負載平衡來處理來自 S3 用戶端的擷取和擷取工作負載。

什麼是負載平衡？

當用戶端應用程式從 StorageGRID 系統儲存或擷取資料時、 StorageGRID 會使用負載平衡器來管理擷取和擷取工作負載。負載平衡可在多個儲存節點之間分配工作負載、以最大化速度和連線容量。

此功能可在所有管理節點和所有閘道節點上安裝支援程式、並提供第7層負載平衡功能。StorageGRID它會對用戶端要求執行傳輸層安全性（TLS）終止、檢查要求、並建立新的安全連線至儲存節點。

將用戶端流量轉送至儲存節點時、每個節點上的負載平衡器服務都會獨立運作。透過加權程序、負載平衡器服務會將更多要求路由傳送至CPU可用度較高的儲存節點。

> ⓘ 儘管StorageGRID負載平衡器服務是建議的負載平衡機制，但您可能希望整合第三方負載平衡器。如需了解更多信息，請聯繫您的NetApp客戶代表或參考以下內容： "將第三方負載平衡器與StorageGRID結合使用"。

我需要多少個負載平衡節點？

一般最佳實務做法StorageGRID 是、您的一套系統應該在負載平衡器服務中包含兩個或多個節點。例如、站台可能包含兩個閘道節點、或同時包含一個管理節點和一個閘道節點。無論您使用的是服務應用裝置、裸機節點或虛擬機器（ VM ）型節點、請確定每個負載平衡節點都有足夠的網路、硬體或虛擬化基礎架構。

什麼是負載平衡器端點？

負載平衡器端點會定義傳入和傳出用戶端應用程式要求用來存取包含負載平衡器服務之節點的連接埠和網路傳輸協定（ HTTPS 或 HTTP ）。端點也會定義用戶端類型（ S3 ）、繫結模式、以及選擇性的允許或封鎖租戶清單。

若要建立負載平衡器端點，請使用網格管理器或完成 S3 設定和FabricPool精靈：

- "設定負載平衡器端點"
- "使用 S3 設定精靈"
- "使用 FabricPool 設定精靈"

負載平衡器快取的注意事項

當工作負載對資料子集進行操作並多次存取物件時，快取可以顯著提高效能。此外，快取無需完整的網格部署即可提供對物件儲存的遠端存取。負載平衡器快取僅適用於網關節點。

在建立負載平衡器端點時：

- 僅為可快取的工作負載啟用快取。如果工作負載存取未快取的資料的頻率高於存取快取的資料的頻率，那麼其效能將比未使用快取提供服務時的效能更差。在某些情況下，覆蓋率和驅逐率較高的工作負載也可能超過保證的驅動器寫入耐久性。
- 考慮新增額外的端點或節點來快取適合快取的單一工作負載。
- 對可快取和不可快取的工作負載使用不同的端點。這種分離確保快取機制得到適當應用並且不會幹擾不可快取的資料處理。
- 透過將潛在的可快取工作負載定向到啟用快取的端點來評估它。監視並驗證快取命中率以確定工作負載是否適合快取。此評估有助於優化效能並確保有效利用快取資源。
- "檢閱稽核記錄"確定現有工作負載是否適合快取。對於給定的時間段，確定針對唯一物件的 GET 百分比。為了適合緩存，該值應低於 50%。

適合用於快取的工作負載範例

- 資料湖
- 高效能運算 (HPC)
- AI/ML 訓練
- 內容傳遞網路（CDN）
- 媒體資產管理
- 影片製作

- 可以快取多個物件版本。
- 支援範圍讀取操作。

不適合用於快取的工作負載範例

- 布料池
- 備份應用程式
- 儲存分層

如果快取提供的任何內容需要靜態加密， "啟用節點或磁碟機加密"在快取節點上。

不會被快取的物件和請求類型

- 這 `response-content-encoding`查詢參數
- 這 `partNumber`查詢參數
- 條件標題
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- 使用以下任意方式靜態加密的請求：
  - SSE（使用StorageGRID管理金鑰的伺服器端加密）
  - SSE-C（使用客戶提供的金鑰進行伺服器端加密）
  - 儲存的物件加密

任何未快取的請求都會被轉送到上游 LDR，就好像未啟用快取一樣。

相關資訊

- "排查負載平衡器快取問題"
- 有關負載平衡器快取的更多信息，請聯繫技術支援。

連接埠的考量事項

對於您建立的第一個端點、負載平衡器端點的連接埠預設為 10433 、但您可以指定介於 1 到 65535 之間的任何未使用的外部連接埠。如果您使用連接埠 80 或 443 、端點將僅使用 Gateway 節點上的負載平衡器服務。這些連接埠保留在管理節點上。如果您對多個端點使用相同的連接埠、則必須為每個端點指定不同的繫結模式。

不允許使用其他網格服務使用的連接埠。看"內部連接埠StorageGRID" 。

網路傳輸協定的考量事項

在大多數情況下、用戶端應用程式與 StorageGRID 之間的連線應該使用傳輸層安全性（ TLS ）加密。支援但不建議連線至無 TLS 加密的 StorageGRID 、尤其是在正式作業環境中。當您選取 StorageGRID 負載平衡器端點的網路傳輸協定時、應該選取 **HTTPS** 。

負載平衡器端點憑證的考量事項

如果選擇 **HTTPS** 作爲負載平衡器端點的網絡協議，則必須提供安全證書。建立負載平衡器端點時、您可以使用以下三個選項中的任何一個：

- * 上傳簽署的憑證（建議） * 。此憑證可由公開信任或私有憑證授權單位（ CA ）簽署。最佳做法是使用公開信任的 CA 伺服器憑證來保護連線安全。與產生的憑證不同、 CA 簽署的憑證可以不中斷地旋轉、有助於避免過期問題。

  您必須先取得下列檔案、才能建立負載平衡器端點：

  - 自訂伺服器憑證檔案。

- 自訂伺服器憑證私密金鑰檔案。
- 或者、每個中繼發行憑證授權單位的憑證 CA 套裝組合。

- * 產生自我簽署的憑證 * 。
- * 使用全球 StorageGRID S3 憑證 * 。您必須上傳或產生此憑證的自訂版本、才能為負載平衡器端點選取該憑證。請參閱。 "設定 S3 API 憑證"

我需要什麼價值？

若要建立憑證、您必須知道 S3 用戶端應用程式用來存取端點的所有網域名稱和 IP 位址。

憑證的 * 主體 DN* （辨別名稱）項目必須包含用戶端應用程式將用於 StorageGRID 的完整網域名稱。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

必要時、憑證可以使用萬用字元來代表執行負載平衡器服務的所有管理節點和閘道節點的完整網域名稱。例如 `*.storagegrid.example.com`，使用 * 萬用字元來表示 `adm1.storagegrid.example.com`和 `gn1.storagegrid.example.com`。

如果您打算使用 S3 虛擬主機風格的要求，則憑證也必須包含您已設定的每個 "S3 端點網域名稱" 的*備用名稱*項目，包括任何萬用字元名稱。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果您使用萬用字元做為網域名稱，請參閱"伺服器憑證的強化準則"。

您也必須為安全性憑證中的每個名稱定義 DNS 項目。

如何管理過期的憑證？

如果用於保護 S3 應用程式與 StorageGRID 之間連線的憑證過期、應用程式可能會暫時失去對 StorageGRID 的存取權。

若要避免憑證過期問題、請遵循下列最佳實務做法：

- 請仔細監控任何警告即將到期的憑證、例如 * 負載平衡器端點憑證到期 * 和 * S3 API* 警示的通用伺服器憑證到期日。
- 請務必讓 StorageGRID 和 S3 應用程式的憑證版本保持同步。如果您更換或更新用於負載平衡器端點的憑證、則必須更換或更新 S3 應用程式所使用的同等憑證。
- 使用公開簽署的 CA 憑證。如果您使用由 CA 簽署的憑證、您可以不中斷地更換即將過期的憑證。
- 如果您已產生自我簽署的 StorageGRID 憑證、且該憑證即將過期、則必須在現有憑證過期之前、手動在 StorageGRID 和 S3 應用程式中置換憑證。

綁定模式的注意事項

繫結模式可讓您控制哪些 IP 位址可用於存取負載平衡器端點。如果端點使用繫結模式、則用戶端應用程式只有在使用允許的 IP 位址或其對應的完整網域名稱（ FQDN ）時、才能存取端點。使用任何其他 IP 位址或 FQDN 的用戶端應用程式無法存取端點。

您可以指定下列任何一種繫結模式：

- * 通用 *（預設）：用戶端應用程式可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。除非您需要限制端點的存取、否則請使用此設定。
- * HA 群組的虛擬 IP * 。用戶端應用程式必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）。
- * 節點介面 * 。用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）。
- * 節點類型 * 。根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）、或任何閘道節點的 IP 位址（或對應的 FQDN ）。

租戶存取的考量事項

租戶存取是一項選擇性的安全功能、可讓您控制哪些 StorageGRID 租戶帳戶可以使用負載平衡器端點來存取他們的貯體。您可以允許所有租戶存取端點（預設）、也可以指定每個端點的允許或封鎖租戶清單。

您可以使用此功能、在租戶與其端點之間提供更好的安全隔離。例如、您可以使用此功能來確保某個租戶擁有的最高機密或高度機密資料、不會被其他租戶完全存取。

> 為了進行存取控制、如果在要求中未提供存取金鑰（例如匿名存取）、則租戶會根據用戶端要求中使用的存取金鑰來決定租戶。

租戶存取範例

若要瞭解此安全功能的運作方式、請考慮下列範例：

1. 您已建立兩個負載平衡器端點、如下所示：
   - * 公有 * 端點：使用連接埠 10443 並允許存取所有租戶。
   - *Top secret * 端點：使用連接埠 10444 、僅允許存取 *Top secret * 租戶。所有其他租戶都會被封鎖、無法存取此端點。
2. `top-secret.pdf`位於 *top secret * 租戶擁有的貯體中。

若要存取 `top-secret.pdf`、 * 最高機密 * 租戶中的使用者可以向發出 GET 要求 `https://w.x.y.z:10444/top-secret.pdf`。由於此租戶可以使用 10444 端點、因此使用者可以存取物件。不過、如果屬於任何其他租戶的使用者向相同的 URL 發出相同的要求、他們就會收到立即存取遭拒訊息。即使認證和簽章有效、存取仍會遭到拒絕。

CPU可用度

將 S3 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各自運作。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。

負載平衡器端點決定連接到閘道和管理節點上的 StorageGRID 負載平衡器時、 S3 用戶端可以使用的連接埠和網路傳輸協定。您也可以使用端點來存取 Grid Manager 、 Tenant Manager 或兩者。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 您已檢閱"負載平衡考量"。
- 如果您先前已重新對應要用於負載平衡器端點的連接埠、則您有"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"
- 如果負載平衡器端點將由使用"S3租戶選擇"、則不得使用任何裸機節點的 IP 位址或 FQDN 。S3 Select 所使用的負載平衡器端點僅允許使用服務應用裝置和 VMware 型軟體節點。
- 您已設定任何打算使用的VLAN介面。請參閱。 "設定VLAN介面"
- 如果您要建立HTTPS端點（建議）、您就有伺服器憑證的資訊。

  對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

  - 若要上傳憑證、您需要伺服器憑證、憑證私密金鑰、以及選擇性的CA套裝組合。
  - 若要產生憑證、您需要 S3 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 S3 API 憑證（也可用於直接連線至儲存節點）、則您已使用外部憑證授權單位簽署的自訂憑證來取代預設憑證。請參閱。 "設定 S3 API 憑證"

建立負載平衡器端點

每個 S3 用戶端負載平衡器端點指定一個連接埠、一個客戶端類型（S3）和一個網路協定（HTTP 或 HTTPS ）。管理介面負載平衡器端點指定連接埠、介面類型和不受信任的客戶端網路。

存取精靈

步驟

1. 選擇*設定* > 網路 > 負載平衡器端點。
2. 若要為 S3 用戶端建立端點，請選擇 **S3** 用戶端 標籤。
3. 若要建立端點以存取 Grid Manager 、 Tenant Manager 或兩者、請選取 * 管理介面 * 索引標籤。
4. 選擇* Create （建立）。

輸入端點詳細資料

步驟

1. 選取適當的指示、以輸入您要建立的端點類型的詳細資料。

S3用戶端

欄位	說明
名稱	端點的描述性名稱、會出現在「負載平衡器端點」頁面的表格中。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為 10433 、表示您建立的第一個端點、但您可以輸入 1 到 65535 之間的任何未使用的外部連接埠。 如果您輸入 **80** 或 **8443** ，則端點僅在網關節點上配置，除非您已釋放端口 8443 。然後、您可以使用連接埠 8443 做為 S3 端點、而且連接埠將同時在 Gateway 和 Admin Node 上設定。 如果要為某個"全域命名空間"設定負載平衡器端點，請為每個端點使用相同的連接埠。
用戶端類型	必須是 *S3 * 。
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。
啟用快取	啟用或停用"網關節點上的緩存"用於此負載平衡器端點。 如果出現快取問題，請參閱"排查負載平衡器快取問題"。

管理介面

欄位	說明
名稱	端點的描述性名稱、會出現在「負載平衡器端點」頁面的表格中。
連接埠	您要用來存取 Grid Manager 、 Tenant Manager 或兩者的 StorageGRID 連接埠。 • 網格管理器： **8443** • 租戶經理： **9443** • Grid Manager 和 Tenant Manager ： **443** • 注意 * ：您可以使用這些預設連接埠或其他可用的連接埠。
介面類型	選取您要使用此端點存取的 StorageGRID 介面選項按鈕。

欄位	說明
不受信任的用戶端網路	如果不受信任的用戶端網路應該可以存取此端點、請選取 * 是 * 。否則、請選取 * 否 * 。 當您選取 * 是 * 時、連接埠會在所有不受信任的用戶端網路上開啟。 • 注意 * ：當您建立負載平衡器端點時、您只能將連接埠設定為開放或關閉給不受信任的用戶端網路。

1. 選擇*繼續*。

選取繫結模式

步驟

1. 選取端點的繫結模式、以控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

   有些繫結模式適用於用戶端端端點或管理介面端點。此處列出兩種端點類型的所有模式。

模式	說明
全域（用戶端端端點的預設值）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取、否則請使用 * 全域 * 設定。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型（僅限用戶端端端點）	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。
所有管理節點（管理介面端點的預設值）	用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）來存取此端點。

   如果多個端點使用相同的連接埠、 StorageGRID 會使用此優先順序來決定要使用的端點： * HA 群組的虛擬 IP * > * 節點介面 * > * 節點類型 * > * 全域 * 。

   如果您要建立管理介面端點、則只允許使用管理節點。

2. 如果您選取* HA群組的虛擬IP *、請選取一或多個HA群組。

   如果您要建立管理介面端點、請選取僅與管理節點相關聯的 VIP 。

3. 如果您選取*節點介面*、請針對您要與此端點建立關聯的每個管理節點或閘道節點、選取一或多個節點介面。
4. 如果您選取 * 節點類型 * 、請選取管理節點（包括主要管理節點和任何非主要管理節點）或閘道節點。

控制租戶存取

管理介面端點只有當端點具有租戶管理器的介面類型時、才能控制租戶存取。

步驟

1. 對於 * 租戶存取 * 步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。 如果您尚未建立任何租戶帳戶、則必須選取此選項。新增租戶帳戶之後、您可以編輯負載平衡器端點、以允許或封鎖特定帳戶。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

2. 如果您要建立 **HTTP** 端點、則不需要附加憑證。選取*「Create」（建立）*以新增負載平衡器端點。然後，轉至完成後。否則、請選取*繼續*以附加憑證。

附加憑證

步驟

1. 如果您要建立* HTTPS *端點、請選取要附加到端點的安全性憑證類型。

   憑證可保護 S3 用戶端與管理節點或閘道節點上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 S3 憑證 * 。如果您想要使用全域 S3 API 憑證、也可用於直接連線至儲存節點、請選取此選項。

     除非您以外部憑證授權單位簽署的自訂憑證取代由網格 CA 簽署的預設 S3 API 憑證、否則無法選取此選項。請參閱。 "設定 S3 API 憑證"

   - * 使用管理介面憑證 * 。如果您想要使用通用管理介面憑證、也可用於直接連線至管理節點、請選取此選項。
2. 如果您未使用 StorageGRID S3 憑證、請上傳或產生憑證。

上傳憑證

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

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

     EC 私密金鑰必須大於 224 位元。RSA 私密金鑰必須大於 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。使用副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

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

d. 選擇* Create （建立）。+已建立負載平衡器端點。自訂憑證用於 S3 用戶端或管理介面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：

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

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

c. 選取*產生*。

d. 選取*憑證詳細資料*以查看所產生憑證的中繼資料。

   ▪ 選取*下載憑證*以儲存憑證檔案。

   指定憑證檔案名稱和下載位置。使用副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   ▪ 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇* Create （建立）。

   隨即建立負載平衡器端點。自訂憑證用於 S3 用戶端或管理介面與此端點之間的所有後續新連線。

完成後

步驟

1. 如果您使用 DNS 、請確定 DNS 包含一筆記錄、將 StorageGRID 完整網域名稱（ FQDN ）與用戶端用來建立連線的每個 IP 位址建立關聯。

   您在DNS記錄中輸入的IP位址取決於您是否使用HA負載平衡節點群組：

   ◦ 如果您已設定 HA 群組、用戶端將會連線至該 HA 群組的虛擬 IP 位址。

   ◦ 如果您不使用 HA 群組、用戶端將使用閘道節點或管理節點的 IP 位址連線至 StorageGRID 負載平衡器服務。

   您也必須確保DNS記錄會參考所有必要的端點網域名稱、包括任何萬用字元名稱。

2. 向 S3 用戶端提供連線至端點所需的資訊：

   ◦ 連接埠號碼

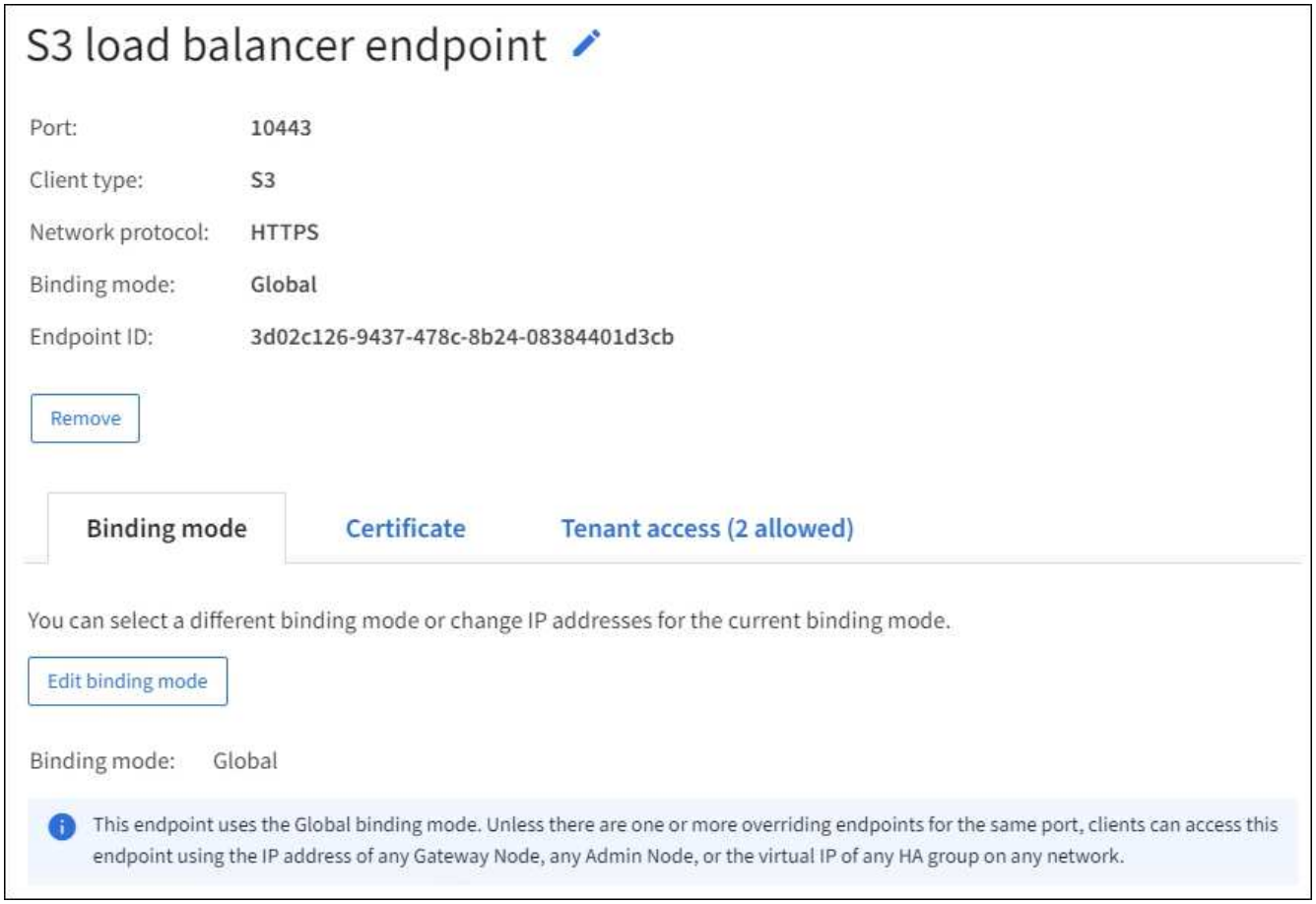
   ◦ 完整網域名稱或IP位址

   ◦ 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。您可以變更端點的特定設定。

- 若要檢視所有負載平衡器端點的基本資訊、請檢閱「負載平衡器端點」頁面上的表格。
- 若要檢視特定端點的所有詳細資料、包括憑證中繼資料、請在表格中選取端點的名稱。顯示的資訊會因端點類型及其設定方式而異。



- 若要編輯端點、請使用負載平衡器端點頁面上的 * 動作 * 功能表。

如果您在編輯管理介面端點的連接埠時、無法存取 Grid Manager 、請更新 URL 和連接埠以重新取得存取權。

編輯端點之後、您可能需要等待15分鐘、才能將變更套用至所有節點。

工作	「行動」功能表	詳細資料頁面
編輯端點名稱	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點名稱*」。 c. 輸入新名稱。 d. 選擇*保存*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇編輯圖示 。 c. 輸入新名稱。 d. 選擇*保存*。

工作	「行動」功能表	詳細資料頁面
編輯端點連接埠	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯端點連接埠 * c. 輸入有效的連接埠號碼。 d. 選擇*保存*。	*n*
編輯端點繫結模式	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點繫結模式*」 。 c. 視需要更新連結模式。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇*編輯綁定模式*。 c. 視需要更新連結模式。 d. 選取*儲存變更*。
編輯端點憑證	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點憑證*」 。 c. 視需要上傳或產生新的自訂憑證、或開始使用全域 S3 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 憑證。 e. 選取*儲存變更*。
編輯租戶存取	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯租戶存取 * 。 c. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇 * 租戶存取 * 標籤。 c. 選取 * 編輯租戶存取 * 。 d. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 e. 選取*儲存變更*。

移除負載平衡器端點

您可以使用* Actions（動作）*功能表移除一或多個端點、也可以從詳細資料頁面移除單一端點。

若要防止用戶端中斷、請在移除負載平衡器端點之前、更新任何受影響的 S3 用戶端應用程式。使用指派給另一個負載平衡器端點的連接埠、更新每個用戶端以進行連線。請務必同時更新任何必要的憑證資訊。

如果您在移除管理介面端點時失去對 Grid Manager 的存取權、請更新 URL 。

- 若要移除一或多個端點：
  a. 在「負載平衡器」頁面中、選取您要移除的每個端點的核取方塊。
  b. 選擇*「Actions」（動作）>「Remove*」（移除

c. 選擇*確定*。

- 若要從詳細資料頁面移除一個端點：
  a. 從「負載平衡器」頁面中選取端點名稱。
  b. 在詳細資料頁面上選取*移除*。
  c. 選擇*確定*。

在 **StorageGRID** 中設定 **S3** 端點網域名稱

若要支援 S3 虛擬代管型要求、您必須使用 Grid Manager 來設定 S3 用戶端所連線的 S3 端點網域名稱清單。

不支援將 IP 位址用於端點網域名稱。未來的版本將會阻止此組態。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已確認網格升級尚未進行。

網格升級進行中時、請勿變更網域名稱組態。

關於這項工作

若要讓用戶端使用S3端點網域名稱、您必須執行下列所有動作：

- 使用Grid Manager將S3端點網域名稱新增StorageGRID 至整個系統。
- 請確定"用戶端用於 StorageGRID HTTPS 連線的憑證"已簽署用戶端所需的所有網域名稱。

  例如，如果端點是 `s3.company.com`，則必須確保用於 HTTPS 連接的證書包括 `s3.company.com`端點和端點的通配符主體替代名稱（ SAN ）： `*.s3.company.com`。

- 設定用戶端使用的DNS伺服器。為用戶端用來建立連線的 IP 位址加入 DNS 記錄、並確保記錄會參照所有必要的 S3 端點網域名稱、包括任何萬用字元名稱。

用戶端可以StorageGRID 使用閘道節點、管理節點或儲存節點的IP位址、或是連線至高可用度群組的虛擬IP位址、來連線至功能區。您應該瞭解用戶端應用程式如何連線至網格、以便在DNS記錄中包含正確的IP位址。

使用HTTPS連線（建議）到網格的用戶端可使用下列任一憑證：

- 連線到負載平衡器端點的用戶端可以使用該端點的自訂憑證。每個負載平衡器端點都可設定為辨識不同的 S3 端點網域名稱。
- 連線至負載平衡器端點或直接連線至儲存節點的用戶端可以自訂全域 S3 API 憑證、以包含所有必要的 S3 端點網域名稱。

如果您沒有新增 S3 端點網域名稱、而且清單是空的、則會停用 S3 虛擬託管樣式要求的支援。

新增 S3 端點網域名稱

步驟

1. 選擇*設定* > 網路 > **S3** 端點網域。
2. 在 * 網域名稱 1* 欄位中輸入網域名稱。選取 * 新增其他網域名稱 * 以新增更多網域名稱。
3. 選擇*保存*。
4. 確定用戶端使用的伺服器憑證符合所需的 S3 端點網域名稱。
   - 如果用戶端連線到使用其本身憑證的負載平衡器端點，請參閱"更新與端點相關的憑證"。
   - 如果用戶端連線到使用全域 S3 API 憑證的負載平衡器端點、"更新全域 S3 API 憑證"或直接連線到 Storage Nodes 、。
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、而且憑證會如預期般驗證端點。

重新命名 S3 端點網域名稱

如果您變更 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇*設定* > 網路 > **S3** 端點網域。
2. 選取您要編輯的網域名稱欄位、然後進行必要的變更。
3. 選擇*保存*。
4. 選擇 * 是 * 以確認您的變更。

刪除 S3 端點網域名稱

如果您移除 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇*設定* > 網路 > **S3** 端點網域。
2. 選擇網域名稱旁邊的刪除圖示 ✕。
3. 選擇 * 是 * 以確認刪除。

相關資訊

- "使用S3 REST API"
- "檢視IP位址"
- "設定高可用度群組"

StorageGRID 客戶端連線的 IP 位址和連接埠

若要儲存或擷取物件、 S3 用戶端應用程式會連線到負載平衡器服務（包含在所有管理節點和閘道節點上）、或是連接到所有儲存節點上的本機分配路由器（ LDR ）服務。

用戶端應用程式可以使用網格節點的 IP 位址和該節點上服務的連接埠號碼、來連線至 StorageGRID 。您也可以建立高可用度（ HA ）負載平衡節點群組、以提供使用虛擬 IP （ VIP ）位址的高可用度連線。如果您想要使用完整網域名稱（ FQDN ）而非 IP 或 VIP 位址連線至 StorageGRID 、您可以設定 DNS 項目。

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如果您已經建立負載平衡器端點和高可用度（ HA ）群組、請參閱何處可以找到 IP 位址如何在 Grid Manager 中找到這些值。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA 群組	負載平衡器	HA群組的虛擬IP位址	指派給負載平衡器端點的連接埠
管理節點	負載平衡器	管理節點的IP位址	指派給負載平衡器端點的連接埠
閘道節點	負載平衡器	閘道節點的IP位址	指派給負載平衡器端點的連接埠
儲存節點	LdR	儲存節點的IP位址	預設S3連接埠： • HTTPS ： 18082 • HTTP ： 18084

URL 範例

若要將用戶端應用程式連線至 HA 群組的閘道節點負載平衡器端點、請使用如下所示的 URL 結構：

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

例如、如果 HA 群組的虛擬 IP 位址為 192.0.2.5 、而負載平衡器端點的連接埠號碼為 10443 、則應用程式可以使用下列 URL 連線至 StorageGRID ：

`https://192.0.2.5:10443`

何處可以找到 **IP** 位址

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 若要尋找網格節點的IP位址：
   a. 選擇*節點*。
   b. 選取您要連線的管理節點、閘道節點或儲存節點。
   c. 選擇* Overview（概述）*選項卡。
   d. 在「節點資訊」區段中、記下節點的IP位址。
   e. 選取*顯示更多*以檢視IPv6位址和介面對應。

      您可以從用戶端應用程式建立連線至清單中的任何IP位址：

- * eth0：* Grid Network
- * eth1：*管理網路（選用）
- * eth2：*用戶端網路（選用）

> 如果您正在檢視管理節點或閘道節點、且該節點是高可用度群組中的作用中節點、則HA群組的虛擬IP位址會顯示在eth2上。

3. 若要尋找高可用度群組的虛擬IP位址：
   a. 選擇*設定* > 網路 > 高可用性群組。
   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*設定* > 網路 > 負載平衡器端點。
   b. 記下您要使用的端點連接埠編號。

> 如果連接埠號碼為 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。所有其他連接埠都在閘道節點和管理節點上設定。

   c. 從表格中選取端點名稱。
   d. 確認 * 用戶端類型 * （ S3 ）符合將使用端點的用戶端應用程式。

管理網路和連線

配置 StorageGRID 網路設定

您可以從Grid Manager設定各種網路設定、以微調StorageGRID 您的系統運作。

設定VLAN介面

您可以"建立虛擬 LAN （ VLAN ）介面"隔離和分割流量、以確保安全性、靈活度和效能。每個VLAN介面都會與管理節點和閘道節點上的一個或多個父介面相關聯。您可以使用HA群組和負載平衡器端點中的VLAN介面、依應用程式或租戶來隔離用戶端或管理流量。

流量分類原則

您可以使用"流量分類原則"來識別及處理不同類型的網路流量、包括與特定貯體、租戶、用戶端子網路或負載平衡器端點相關的流量。這些原則可協助限制流量及監控。

關於鏈路的準則StorageGRID

您可以使用Grid Manager來設定及管理StorageGRID 各種不一致的網路和連線。

請參閱"設定 S3 用戶端連線"以瞭解如何連接 S3 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 用戶端應用程式的存取、因此 Grid Network 可以隔離和保護。用戶端網路可透過本機閘道與任何可連線的子網路進行通訊。

準則

- 每個 StorageGRID 節點都需要專屬的網路介面、 IP 位址、子網路遮罩、以及指派給它的每個網路的閘道。
- 網格節點在網路上不能有多個介面。
- 每個網路支援單一閘道、每個網格節點、而且必須與節點位於相同的子網路上。您可以視需要在閘道中實作更複雜的路由。
- 在每個節點上、每個網路都會對應至特定的網路介面。

網路	介面名稱
網格	eth0
管理（選用）	eth1
用戶端（選用）	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、以便用來"VLAN 介面"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"
  - **Linux**（安裝節點之前）："建立節點組態檔"
  - **Linux**（安裝節點後）："向節點新增中繼或存取介面"

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

在 **StorageGRID** 中檢視 **IP** 位址

您可以檢視StorageGRID 您的系統的各個網格節點的IP位址。然後、您可以使用此 IP 位址登入命令列的網格節點、並執行各種維護程序。

開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

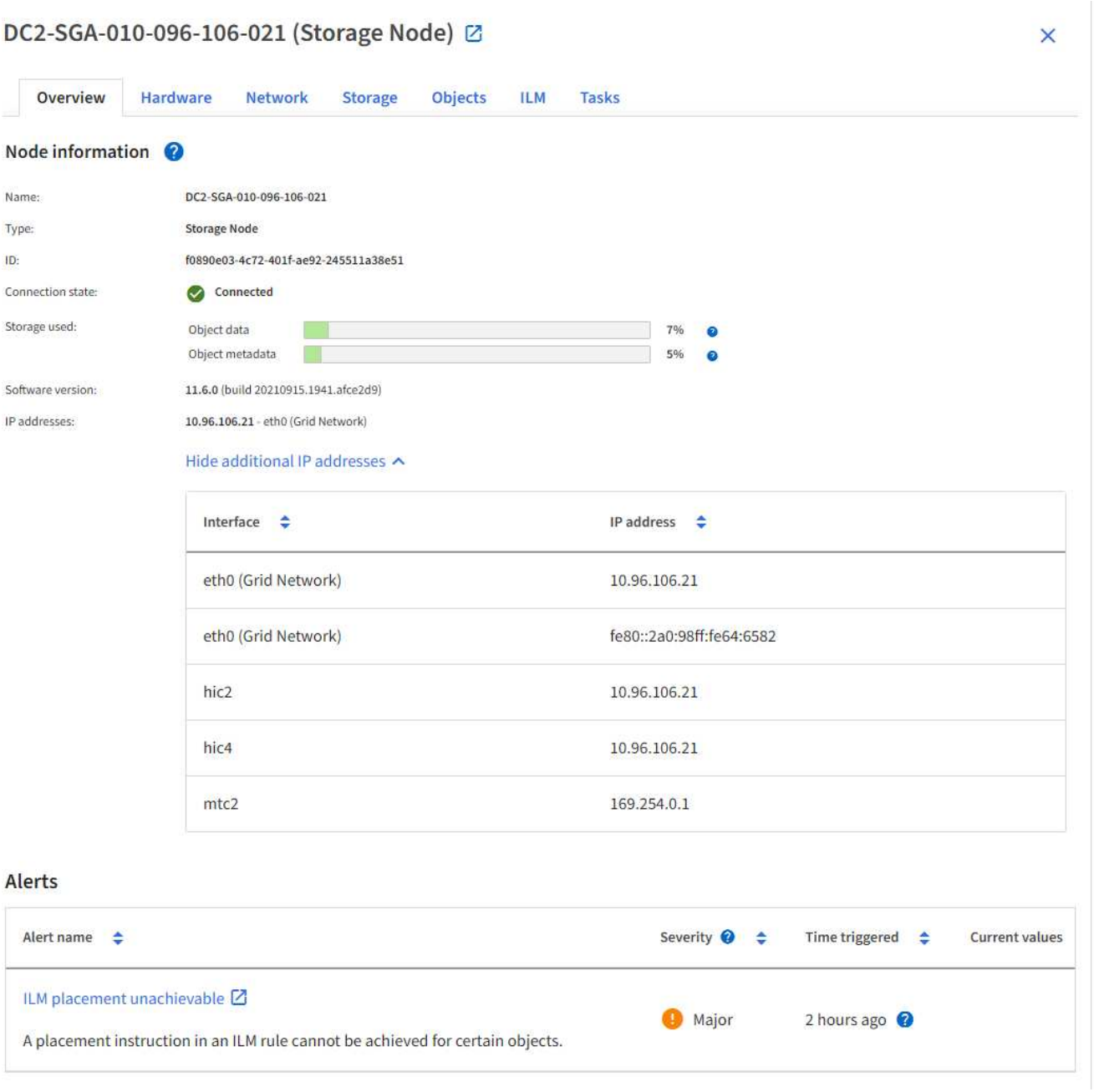
關於這項工作

如需變更 IP 位址的相關資訊，請參閱"設定IP位址"。

步驟

1. 選擇*節點* > ***grid node*** > 概覽。
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。



在 **StorageGRID** 中設定 **VLAN** 介面

在管理節點和網關節點上建立虛擬 LAN (VLAN) 接口，並在 HA 群組和負載平衡器端點中使用它們來隔離和分區流量，從而實現安全性、靈活性和效能。HA 群組中選定的節點可以使用 VLAN 介面共用最多 10 個虛擬 IP 位址，這樣，如果一個節點發生故障，另一個節點將接管往返虛擬 IP 位址的流量。

VLAN介面考量

- 您可以輸入VLAN ID、然後在一個或多個節點上選擇父介面、藉此建立VLAN介面。
- 父介面必須設定為交換器的主幹介面。
- 父介面可以是Grid Network（eth0）、Client Network（eth2）、或VM或裸機主機的其他主幹介面（例

如、ens256）。

- 對於每個VLAN介面、您只能為指定節點選取一個父介面。例如、您無法在同一個 VLAN 的父介面上、同時使用 Grid Network 介面和 Client Network 介面。
- 如果VLAN介面適用於管理節點流量、包括與Grid Manager和租戶管理程式相關的流量、請選取「僅管理節點」上的介面。
- 如果 VLAN 介面用於 S3 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"
  - **Linux**（安裝節點之前）："建立節點組態檔"
  - **Linux**（安裝節點後）："向節點新增中繼或存取介面"

「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

建立**VLAN**介面

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 已在網路中設定主幹介面、並附加至VM或Linux節點。您知道主幹介面的名稱。
- 您知道正在設定的VLAN ID。

關於這項工作

您的網路管理員可能已設定一或多個主幹介面和一或多個VLAN、以隔離屬於不同應用程式或租戶的用戶端或管理流量。每個VLAN都會以數字ID或標記來識別。例如、您的網路可能會使用VLAN 100作為FabricPool 不二次流量傳輸、而使用VLAN 200作為歸檔應用程式。

您可以使用Grid Manager建立VLAN介面、讓用戶端能夠在StorageGRID 特定VLAN上存取功能。當您建立VLAN介面時、請指定VLAN ID並選取一或多個節點上的父（主幹）介面。

存取精靈

步驟

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

輸入**VLAN**介面的詳細資料

步驟

1. 指定網路中VLAN的ID。您可以輸入介於1和4094之間的任何值。

   VLAN ID 不一定是唯一的。例如、您可以使用VLAN ID 200來管理某個站台的流量、使用相同的VLAN ID來處理另一個站台的用戶端流量。您可以在每個站台建立具有不同父介面的獨立VLAN介面組。不過、兩個 ID 相同的 VLAN 介面無法在節點上共用相同的介面。如果您指定已使用的ID、則會出現訊息。

2. （可選）輸入VLAN介面的簡短說明。
3. 選擇*繼續*。

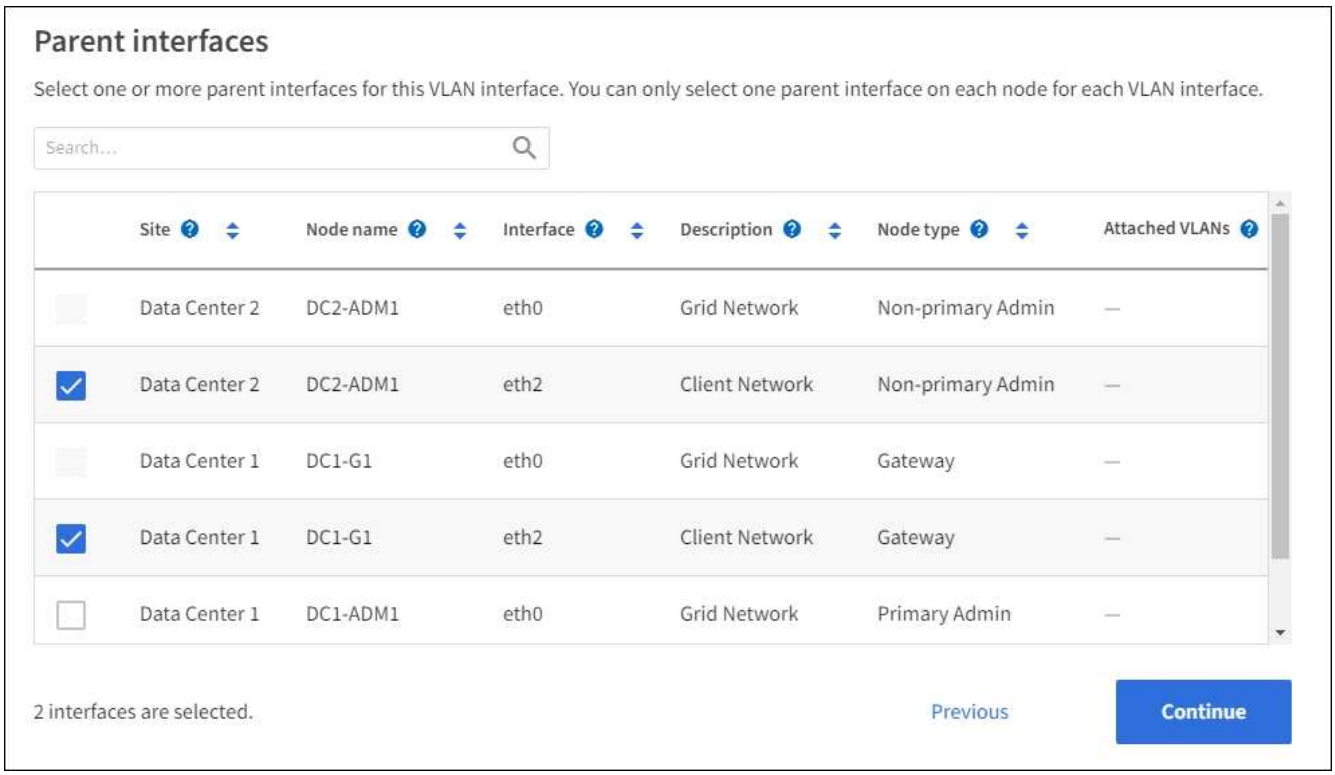
選擇父介面

下表列出網格中每個站台所有管理節點和閘道節點的可用介面。管理網路（ eth1 ）介面無法用作父介面、也無法顯示。

步驟

1. 選取一個或多個父介面來附加此VLAN。

   例如、您可能想要將VLAN附加至閘道節點和管理節點的用戶端網路（eth2）介面。



2. 選擇*繼續*。

確認設定

步驟

1. 檢閱組態並進行任何變更。
   - 如果您需要變更VLAN ID或說明、請選取頁面頂端的*輸入VLAN詳細資料*。
   - 如果您需要變更父介面、請選取頁面頂端的*選擇父介面*、或選取*上一個*。
   - 如果需要刪除父級介面，請選擇垃圾桶圖示。
2. 選擇*保存*。
3. 等待最多 5 分鐘，新的介面才會作為選擇出現在「高可用性群組」頁面上，並列在節點的 網路介面 表中（節點 > 父介面節點 > 網路）。

編輯**VLAN**介面

編輯VLAN介面時、您可以進行下列類型的變更：

- 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 已附加至節點 A 和 B 上的父介面。如果 HA 群組使用 VLAN 200 介面作為節點 A 和節點 B 的 eth2 介面、您可以移除節點 B 的未使用父介面、但無法移除節點 A 的已使用父介面

步驟

1. 選擇*設定* > 網路 > **VLAN** 介面。
2. 選取您要編輯的 VLAN 介面核取方塊。然後選取*「動作*」>*「編輯*」。
3. 或者、請更新VLAN ID或說明。然後選擇*繼續*。

   如果在HA群組中使用VLAN、則無法更新VLAN ID。

4. 您也可以選取或清除核取方塊、以新增父介面或移除未使用的介面。然後選擇*繼續*。
5. 檢閱組態並進行任何變更。
6. 選擇*保存*。

移除**VLAN**介面

您可以移除一或多個VLAN介面。

如果VLAN介面目前用於HA群組、則無法移除。您必須先從HA群組移除VLAN介面、才能將其移除。

若要避免用戶端流量中斷、請考慮執行下列其中一項：

- 移除此VLAN介面之前、請先將新的VLAN介面新增至HA群組。
- 建立不使用此VLAN介面的新HA群組。
- 如果您要移除的VLAN介面目前是作用中介面、請編輯HA群組。將您要移除的VLAN介面移至優先順序清單的底部。等到新的主要介面建立通訊之後、再從HA群組移除舊介面。最後、刪除該節點上的VLAN介面。

步驟

1. 選擇*設定* > 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。

為管理介面啟用**StorageGRID CORS**

身為網格管理員，如果您希望另一個網域可以使用管理 API 存取StorageGRID中的數據，則可以為對StorageGRID 的管理 API 請求啟用跨網域資源共用 (CORS)。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 這"root 存取權限"提供對所有 CORS 配置請求的存取。

關於這項工作

CORS 是一種安全機制，可讓一個網域中的客戶端 Web 應用程式存取不同網域中的資源。例如，假設您想要在網域中為StorageGRID建立一個監控儀表板 `http://www.example.com`。透過在StorageGRID中啟用 CORS `http://www.example.com`和"網格管理器"， `StorageGRID`域響應來自 `\http://www.example.com`。

管理 API (mgmt-api) 請求 `application/json`或者 `multipart/formdata`請求 `Content-Type`支援 CORS。

步驟

1. 在網格管理器中，請前往*配置* > 網路 > 管理介面 **CORS** 設定。
2. 選擇*網格管理員*、*租戶管理員*或兩個選項。
   - 網格管理器：為跨域網格管理 API 請求啟用 CORS。
   - 租用戶管理器：為跨域租用戶管理 API 請求啟用 CORS。
3. 在「域」欄位中輸入其他網域的 URL。

   如果您想在StorageGRID中為多個網域啟用 CORS，請選擇「新增另一個網域」。
4. 選擇*保存*。

相關資訊

"為儲存桶和物件配置StorageGRID CORS"

管理流量分類原則

StorageGRID 中的流量分類原則

流量分類原則可讓您識別及監控不同類型的網路流量。這些原則有助於限制和監控流量、以提升您的服務品質（ QoS ）產品。

流量分類原則會套用至StorageGRID 閘道節點和管理節點的「動態負載平衡器」服務上的端點。若要建立流量分類原則、您必須已經建立負載平衡器端點。

符合的規則

每個流量分類原則都包含一或多個相符的規則、用以識別與下列一或多個實體相關的網路流量：

- 桶
- 子網路

- 租戶
- 負載平衡器端點

此功能可根據規則的目標、監控符合原則中任何規則的流量。StorageGRID符合原則任何規則的任何流量都會由該原則處理。相反地、您可以設定規則以符合指定實體以外的所有流量。

流量限制

您也可以選擇將下列限制類型新增至原則：

- Aggregate 頻寬
- 每個要求的頻寬
- 並行要求
- 要求率

限制值是以每個負載平衡器為基礎強制執行。如果流量同時分散於多個負載平衡器、則總最大傳輸率是您指定的速率限制的倍數。

> 您可以建立原則來限制Aggregate頻寬或限制每個要求的頻寬。不過、 StorageGRID 無法同時限制這兩種頻寬類型。Aggregate頻寬限制可能會對不受限制的流量造成額外的次要效能影響。

對於 Aggregate 或單次請求頻寬限制，請求將按照您設定的速率進行入站或出站。StorageGRID 只能強制執行一種速度，因此將依比對器類型強制執行最特定的原則比對項目。請求所消耗的頻寬不會計入其他包含 Aggregate 頻寬限制原則的較不具體的比對原則。對於所有其他類型的限制，用戶端請求將延遲 250 毫秒，且超過任何比對原則限制的請求將收到 503 Slow Down 回應。

在 Grid Manager 中，您可以檢視流量圖表，並驗證原則是否正在執行您預期的流量限制。

將流量分類原則與**SLA**搭配使用

您可以將流量分類原則與容量限制和資料保護搭配使用、以強制執行服務層級協議（SLA）、以提供容量、資料保護和效能的詳細資訊。

以下範例顯示SLA的三層。您可以建立流量分類原則、以達成每個SLA層級的效能目標。

服務層級	容量	資料保護	允許的最大效能	成本
金級	允許1 PB儲存容量	3 複製 ILM 規則	每秒 25 K 個要求 每秒 5 Gb （ 40 Gbps ）頻寬	每月$$
銀級	允許 250 TB 儲存容量	2 複製 ILM 規則	每秒 10 萬次申請 1.25 GB/ 秒（ 10 Gbps ）頻寬	每月$

服務層級	容量	資料保護	允許的最大效能	成本
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 **StorageGRID** 流量分類原則

如果您想要監控流量分類原則、並選擇性地根據貯體、貯體 regex 、 CIDR 、負載平衡器端點或租戶來限制網路流量、則可以建立流量分類原則。您也可以根據頻寬、並行要求數或要求率、來設定原則限制。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"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*配置* > 網路 > 流量分類。
2. 選擇* Create （建立）。
3. 輸入原則的名稱和說明（選用）、然後選取 * 繼續 * 。

   例如、請說明此流量分類原則的適用範圍及限制。

4. 選取 * 新增規則 * 並指定下列詳細資料、以建立原則的一或多個相符規則。您建立的任何原則都應該至少有一個相符的規則。選擇*繼續*。

欄位	說明
類型	選取符合規則所套用的流量類型。流量類型包括貯體、貯體 regex 、 CIDR 、負載平衡器端點和租戶。

欄位	說明
符合值	輸入符合所選類型的值。 • 貯體：輸入一個或多個貯體名稱。 • 貯體 regex ：輸入一個或多個用於與一組貯體名稱相符的規則運算式。 規則運算式未鎖定。使用 ^ 錨點來比對貯體名稱的開頭、並使用 $ 錨點來比對名稱的結尾。規則運算式比對支援 PCRE （ Perl 相容規則運算式）語法子集。 • CIDR ：以 CIDR 表示法輸入一個或多個符合所需子網路的 IPv4 子網路。 • 負載平衡器端點：選取端點名稱。這些是您在上定義的負載平衡器端點"設定負載平衡器端點"。 • 租戶：租戶比對使用存取金鑰 ID 。如果要求不包含存取金鑰 ID （例如匿名存取）、則會使用存取的貯體所有權來決定租戶。
反轉比對	如果您想要比對所有網路流量（除了 _ 流量與剛定義的類型和比對值一致）、請選取 * 反轉比對 * 核取方塊。否則、請保留核取方塊的核取方塊。 例如、如果您想要將此原則套用至負載平衡器端點以外的所有端點、請指定要排除的負載平衡器端點、然後選取 * 逆向比對 * 。 對於包含多個資料處理者的原則、其中至少有一個是反向資料處理者、請注意不要建立符合所有要求的原則。

5. 您也可以選擇 * 新增限制 * 、然後選取下列詳細資料、以新增一或多個限制、以控制與規則相符的網路流量。

> StorageGRID 會收集指標、即使您沒有新增任何限制、也能瞭解流量趨勢。

欄位	說明
類型	您要套用至規則所對應網路流量的限制類型。例如、您可以限制頻寬或要求率。 • 注意 * ：您可以建立原則來限制彙總頻寬或限制每個要求的頻寬。不過、StorageGRID 無法同時限制這兩種頻寬類型。當使用 Aggregate 頻寬時、無法使用每個要求的頻寬。相反地、當每個要求的頻寬正在使用中時、就無法使用集合頻寬。Aggregate頻寬限制可能會對不受限制的流量造成額外的次要效能影響。 在頻寬限制方面StorageGRID 、餐廳會套用最符合限制類型的原則。例如、如果您的原則只限制一個方向的流量、則相反方向的流量將不受限制、即使有流量符合具有頻寬限制的其他原則。StorageGRID 以下列順序實作頻寬限制的「最佳」比對： • 確切IP位址（/32遮罩） • 確切的儲存區名稱 • 鏟斗回收系統 • 租戶 • 端點 • 非精確的CIDR相符項目（非/32） • 反比對
適用於	此限制是否適用於用戶端讀取要求（ GET 或 HEAD ）或寫入要求（ PUT 、 POST 或 DELETE ）。
價值	根據您選擇的單位、網路流量將受限於的值。例如、輸入 10 並選取 MIB/s 、以防止符合此規則的網路流量超過 10 MIB/s • 附註 * ：視單位設定而定、可用的單位為二進位（例如 GiB ）或十進位（例如 GB ）。若要變更單位設定、請選取 Grid Manager 右上角的使用者下拉式清單、然後選取 * 使用者偏好設定 * 。
單位	描述您輸入值的單位。

例如，如果您想要為 SLA 層建立 4 GB/s 的頻寬限制，請建立兩個聚合頻寬限制：GET/HEAD 為 4 GB/s ，PUT/POST/DELETE 為 4 GB/s。

6. 選擇*繼續*。
7. 閱讀並檢閱流量分類原則。使用 * 上一頁 * 按鈕返回並視需要進行變更。當您對原則感到滿意時、請選取 * 儲存並繼續 * 。

   S3 用戶端流量現在會根據流量分類原則進行處理。

完成後

"檢視網路流量指標"驗證原則是否強制執行您預期的流量限制。

編輯 **StorageGRID** 流量分類原則

您可以編輯流量分類原則來變更其名稱或說明、或建立、編輯或刪除原則的任何規則或限制。

開始之前

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

步驟

1. 選擇*配置* > 網路 > 流量分類。

   此時會出現「流量分類原則」頁面、並在表格中列出現有的原則。

2. 使用「動作」功能表或「詳細資料」頁面編輯原則。請參閱"建立流量分類原則"以瞭解要輸入的內容。

   「行動」功能表

   a. 選取原則的核取方塊。

   b. 選取 * 動作 * > * 編輯 * 。

   詳細資料頁面

   a. 選取原則名稱。

   b. 選取原則名稱旁邊的 * 編輯 * 按鈕。

3. 對於 Enter policy name （輸入策略名稱）步驟，可選擇編輯策略名稱或說明，然後選擇 **Continue** 。
4. 對於 Add matched rules （添加匹配規則）步驟，可選擇添加規則或編輯現有規則的 **Type** 和 **Match Value** ，然後選擇 **Continue** 。
5. 對於設定限制步驟、您可以選擇性地新增、編輯或刪除限制、然後選取 * 繼續 * 。
6. 檢閱更新的原則、然後選取 * 儲存並繼續 * 。

   您對原則所做的變更將會儲存、而且網路流量現在會根據流量分類原則來處理。您可以檢視交通路況圖表、並驗證原則是否強制執行預期的流量限制。

刪除 **StorageGRID** 流量分類原則

如果您不再需要流量分類原則、可以刪除該原則。請務必刪除正確的原則、因為刪除時無法擷取原則。

開始之前

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

步驟

1. 選擇*配置* > 網路 > 流量分類。

此時會出現「流量分類原則」頁面、並在表格中列出現有的原則。

2. 使用「動作」功能表或「詳細資料」頁面刪除原則。

「行動」功能表

a. 選取原則的核取方塊。

b. 選擇*「Actions」（動作）>「Remove*」（移除

原則詳細資料頁面

a. 選取原則名稱。

b. 選取原則名稱旁邊的 * 移除 * 按鈕。

3. 選取 * 是 * 以確認您要刪除原則。

原則即會刪除。

在 StorageGRID 中檢視網路流量指標

您可以從「流量分類原則」頁面檢視可用的圖表、以監控網路流量。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權或 Tenant 帳戶權限"。

關於這項工作

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

即使流量分類原則未設定任何限制、也會收集指標、圖表也會提供實用資訊、協助您瞭解流量趨勢。

步驟

1. 選擇*配置* > 網路 > 流量分類。

此時會顯示「流量分類原則」頁面、並在表格中列出現有的原則。

2. 選取您要檢視其度量的流量分類原則名稱。
3. 選取 * 指標 * 索引標籤。

此時會出現流量分類原則圖表。這些圖表只會顯示符合所選原則之流量的度量。

頁面中包含下列圖表。

- 要求速率：此圖表提供所有負載平衡器所處理之此原則的頻寬量。收到的資料包括所有要求的要求標頭、以及包含實體資料的回應的實體資料大小。「已傳送」包含所有要求的回應標頭、以及回應中包含實體資料之要求的回應實體資料大小。

當要求完成時、此圖表只會顯示頻寬使用量。對於慢速或大型物件要求、實際的即時頻寬可能與此圖表中報告的值不同。

- 錯誤回應率：此圖表提供與此原則相符的要求將錯誤（ HTTP 狀態代碼 >=400 ）傳回用戶端的大約速率。
- 平均要求持續時間（非錯誤）：此圖表提供符合此原則之成功要求的平均持續時間。
- 原則頻寬使用量：此圖表提供所有負載平衡器所處理之符合此原則的頻寬量。收到的資料包括所有要求的要求標頭、以及包含實體資料的回應的實體資料大小。「已傳送」包含所有要求的回應標頭、以及回應中包含實體資料之要求的回應實體資料大小。

4. 將游標放在折線圖上、即可在圖表的特定部分上看到值的快顯視窗。
5. 選取 Metrics 標題下方的 * Grafana Dashboard * 、即可檢視原則的所有圖形。除了 * 指標 * 索引標籤中的四個圖形之外、您還可以檢視另外兩個圖形：
   - 依物件大小寫入要求率：符合此原則的放置 / 張貼 / 刪除要求的速率。個別儲存格上的定位會顯示每秒的速率。懸停檢視中顯示的速率會被截斷為整數數、當貯體中有非零要求時、可能會報告 0 。
   - 依物件大小讀取要求率：符合此原則的 GET / HEAD 要求率。個別儲存格上的定位會顯示每秒的速率。懸停檢視中顯示的速率會被截斷為整數數、當貯體中有非零要求時、可能會報告 0 。
6. 或者，從*支援*選單存取圖表。
   a. 選擇*支援* > 工具 > 指標。
   b. 從 **Grafana** 區段中選取 * 交通分類政策 * 。
   c. 從頁面左上角的功能表中選取原則。
   d. 將游標放在圖形上方、即可看到快顯視窗、其中顯示樣本的日期和時間、彙總至計數的物件大小、以及該期間內每秒的要求數。

      流量分類原則會以其ID來識別。原則 ID 會列在「流量分類原則」頁面上。
7. 分析圖表、判斷原則限制流量的頻率、以及是否需要調整原則。

StorageGRID 中支援的用於出站 **TLS** 連線的加密套件

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

已選擇支援與外部系統一起使用的 TLS 密碼，以確保與一系列外部系統相容。此清單大於支援與 S3 用戶端應用程式一起使用的密碼清單。若要設定密碼，請前往*設定*>*安全*>*安全設定*並選擇*TLS 和 SSH 原則*。

StorageGRID 中無法設定 TLS 組態選項、例如傳輸協定版本、加密算法、金鑰交換演算法和 MAC 演算法。如果您有關於這些設定的特定要求、請聯絡您的NetApp客戶代表。

StorageGRID 中活動、閒置和並行 **HTTP** 連線的優勢

如何設定HTTP連線、可能會影響StorageGRID 到整個系統的效能。組態會因HTTP連線為

作用中或閒置狀態、或是您同時有多個連線而有所不同。

您可以找出下列類型HTTP連線的效能優勢：

- 閒置HTTP連線
- 作用中HTTP連線
- 並行HTTP連線

保持閒置**HTTP**連線開啟的優點

當客戶端應用程式空閒時，請保持 HTTP 連線開啟以允許後續事務。保持空閒 HTTP 連線開啟最多 10 分鐘。StorageGRID可能會自動關閉處於開啟狀態且空閒時間超過 10 分鐘的 HTTP 連線。

開放式和閒置的HTTP連線提供下列優點：

- 縮短延遲時間、從StorageGRID 由整個過程中、由整個過程中的資訊系統判斷它必須執行HTTP交易到StorageGRID 整個系統能夠執行交易的時間

  縮短延遲是主要優勢、尤其是在建立TCP/IP和TLS連線所需的時間內。

- 使用先前執行的傳輸來初始化TCP/IP慢速啟動演算法、藉此提高資料傳輸率
- 即時通知多種故障情況、可中斷用戶端應用程式與StorageGRID 該系統之間的連線

透過平衡慢啟動優勢和資源分配來決定保持空閒連線開啟的時間。

作用中**HTTP**連線的優點

對於直接連線至儲存節點的連線、即使 HTTP 連線持續執行交易、您仍應將作用中 HTTP 連線的持續時間限制為最多 10 分鐘。

判斷連線應保持開啟的最長時間、是在連線持續性的優點與連線至內部系統資源的理想分配之間取得平衡。

對於用戶端連線至儲存節點、限制作用中的 HTTP 連線有下列優點：

- 在StorageGRID 整個支援過程中實現最佳負載平衡。

  隨著時間的推移，由於負載平衡要求的變化，HTTP 連接可能不再是最佳的。當用戶端應用程式為每個事務建立單獨的 HTTP 連線時，系統會執行最佳的負載平衡，但這種方法會抵消與持久連線相關的寶貴效益。

- 允許用戶端應用程式將HTTP交易導向具有可用空間的LDR服務。
- 可啟動維護程序。

  部分維護程序只會在所有進行中的HTTP連線完成後才會開始。

對於連接到負載平衡器服務的用戶端連線、限制開放連線的持續時間、有助於讓部分維護程序立即啟動。如果用戶端連線的持續時間不受限制、則自動終止作用中連線可能需要幾分鐘的時間。

並行**HTTP**連線的優點

您應該StorageGRID 將多個TCP/IP連線保持開放狀態、以允許平行處理、進而提升效能。最佳的平行連線數量

取決於各種因素。

並行HTTP連線提供下列優點：

- 縮短延遲時間

  交易可以立即開始、而非等待其他交易完成。

- 提高處理量

  此系統可執行平行交易、並提高集合交易處理量。StorageGRID

用戶端應用程式應建立多個HTTP連線。當用戶端應用程式必須執行交易時、它可以選取並立即使用任何目前未處理交易的已建立連線。

每個StorageGRID系統的拓撲對於並發事務和連接都有不同的峰值吞吐量。峰值吞吐量取決於計算、網路、儲存資源、WAN 連結以及StorageGRID系統支援的伺服器、服務和應用程式的數量。

StorageGRID系統通常支援多個客戶端應用程式。在確定最大並發連線數時請記住這一點。如果用戶端應用程式由多個軟體實體組成，每個實體都與StorageGRID系統建立連接，則將跨實體的所有連接加起來。在以下情況下，您可能需要調整最大並發連線數：

- 此系統的拓撲會影響系統可支援的並行交易和連線數量上限。StorageGRID
- 在StorageGRID 頻寬有限的網路上與該系統互動的用戶端應用程式、可能必須降低並行度、以確保在合理的時間內完成個別交易。
- 當許多用戶端應用程式共用StorageGRID 該系統時、您可能必須減少並行處理的程度、以避免超出系統限制。

分隔**HTTP**連線集區以進行讀取和寫入作業

您可以使用不同的HTTP連線集區進行讀取和寫入作業、並控制每個集區的使用量。獨立的HTTP連線集區可讓您更有效地控制交易並平衡負載。

用戶端應用程式可建立擷取主導（讀取）或儲存主導（寫入）的負載。有了個別的HTTP連線集區、即可針對讀寫交易調整每個集區的專屬容量、以處理讀寫交易。

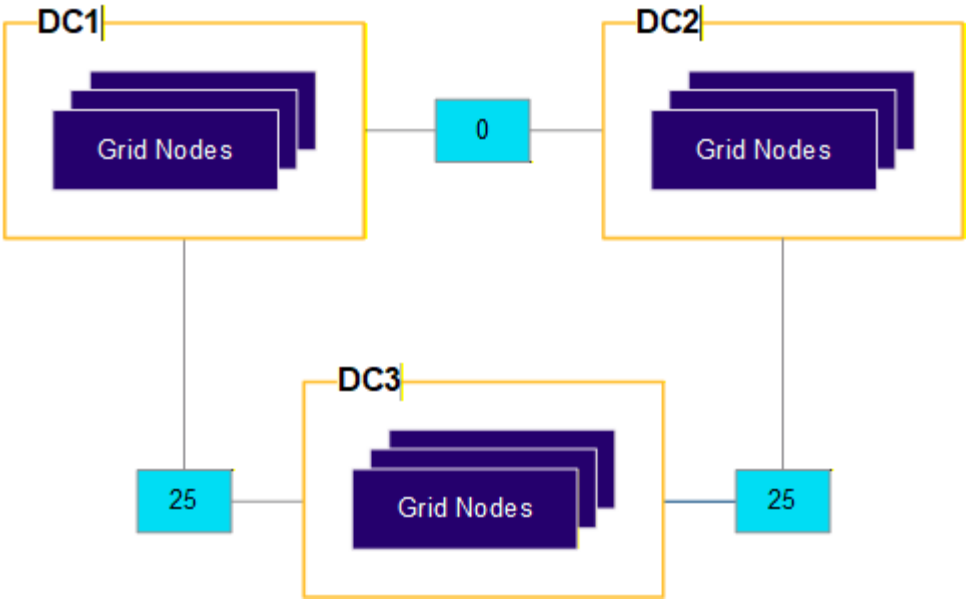
在 **StorageGRID** 中管理連結成本

連結成本可讓您在有兩個以上的資料中心站台存在時、排定哪個資料中心站台提供所要求的服務的優先順序。您可以調整連結成本、以反映站台之間的延遲。

什麼是連結成本？

- 連結成本用於排定要使用哪個物件複本來完成物件擷取的優先順序。
- Grid Management API和租戶管理API會使用連結成本來判斷要StorageGRID 使用哪些內部的哪些服務。
- 連結成本由管理節點和閘道節點上的負載平衡器服務用於引導用戶端連線。請參閱"負載平衡考量"。

此圖顯示一個由三個站點組成的網格，其中站點之間已設定連結成本：



- 管理節點和閘道節點上的負載平衡器服務會將用戶端連線平均分散到同一個資料中心站台的所有儲存節點、以及連結成本為 0 的任何資料中心站台。

  在此範例中、資料中心站台1（DC1）的閘道節點會將用戶端連線平均分配給DC1的儲存節點、以及DC2的儲存節點。DC3的閘道節點只會將用戶端連線傳送至DC3的儲存節點。

- 當擷取以多個複寫複本形式存在的物件時、StorageGRID 會在連結成本最低的資料中心擷取複本。

  在範例中、如果 DC2 的用戶端應用程式擷取同時儲存在 DC1 和 DC3 的物件、則會從 DC1 擷取該物件、因為 DC1 到 DC2 的連結成本為 0 、低於 DC3 到 DC2 的連結成本（ 25 ）。

連結成本是任意的相對數字、沒有特定的計量單位。例如、連結成本50的優先使用成本低於連結成本25。下表顯示常用的連結成本。

連結	連結成本	附註
在實體資料中心站台之間	25 （預設）	透過WAN連結連線的資料中心。
在同一個實體位置的邏輯資料中心站台之間	0	邏輯資料中心位於同一實體建築物或園區內、由LAN連接。

更新連結成本

您可以更新資料中心站台之間的連結成本、以反映站台之間的延遲。

開始之前

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

步驟

1. 選擇*支援* > 其他 > 連結成本。

2. 對於「站台/連結成本」欄中列出的每個站台，請為其他站台輸入 0 到 100 的成本值。

   如果來源與目的地相同、則無法變更連結成本。

3. 放棄或儲存變更：
   - 若要捨棄變更，請選取 **Clear changes**。
   - 若要儲存變更，請選取 **Save**。

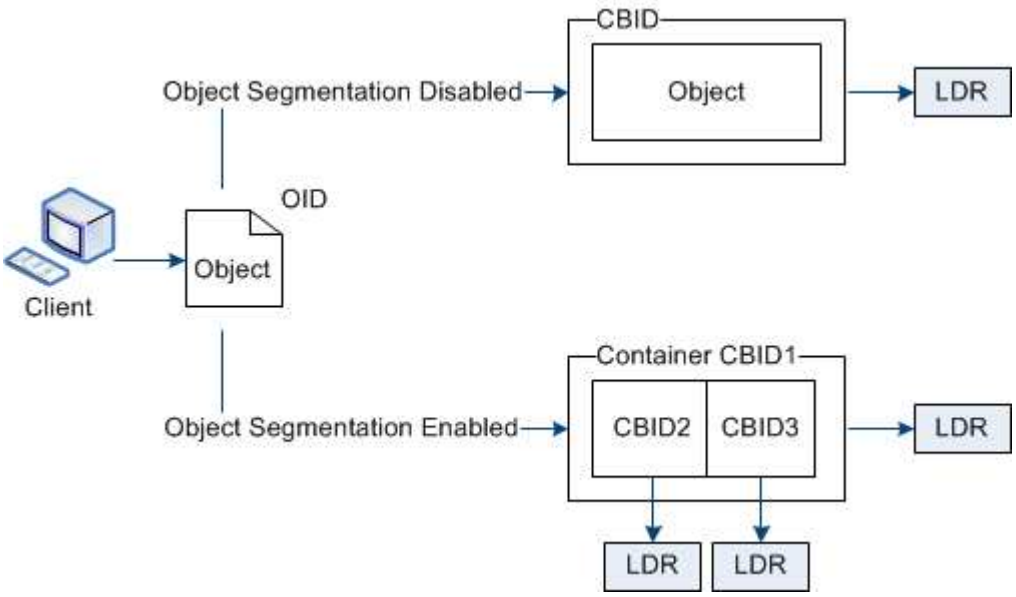
管理儲存節點

使用儲存選項

了解 StorageGRID 中的物件分割

物件分割是將物件分割成一組較小的固定大小物件、以最佳化大型物件的儲存和資源使用量的程序。S3多重部分上傳也會建立分段物件、並有代表每個部分的物件。

將物件擷取至StorageGRID 物件系統時、LdR服務會將物件分割成區段、並建立區段容器、將所有區段的標頭資訊列為內容。



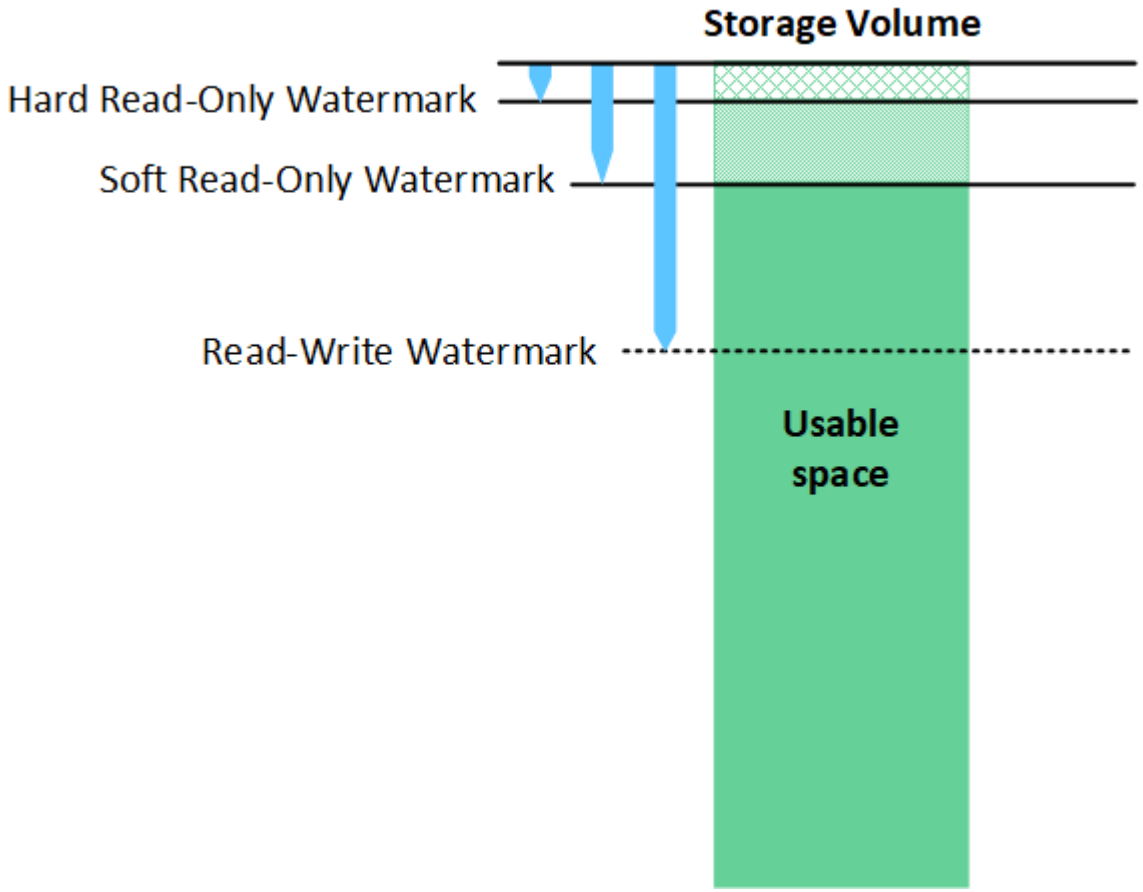
在擷取區段容器時、LMR服務會從區段組合原始物件、並將物件傳回用戶端。

容器和區段不一定儲存在同一個儲存節點上。容器和區段可儲存在ILM規則中指定之儲存資源池內的任何儲存節點上。

每個區段均由StorageGRID 整個系統獨立處理、並有助於計算託管物件和儲存物件等屬性的數量。例如、如果將儲存在StorageGRID 物件叢集系統中的物件分割成兩個區段、則在擷取完成後、「Managed物件」的值會增加三倍、如下所示：

```
segment container + segment 1 + segment 2 = three stored objects
```

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。若要瞭解磁碟區 0 上保留給物件中繼資料的空間、請前往"管理物件中繼資料儲存"。

什麼是軟式唯讀浮水印？

- 儲存磁碟區軟式唯讀浮水印 * 是第一個指出儲存節點的物件資料可用空間已滿的浮水印。

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水印、儲存節點就會切換至 _ 唯讀模式 _ 。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 的軟式唯讀浮水印。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。

什麼是強制唯讀浮水印？

- 儲存磁碟區硬式唯讀浮水印 * 是下一個浮水印、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水印、寫入磁碟區將會失敗。不過、寫入其他磁碟區的資料仍會繼續、直到這些磁碟區的可用空間低於其硬式唯讀浮水印為止。

例如、假設儲存節點中的每個磁碟區都有 5 GB 的硬式唯讀浮水印。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。

硬式唯讀浮水印一律小於軟式唯讀浮水印。

什麼是讀寫浮水印？

- 儲存磁碟區讀寫浮水印 * 僅適用於已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。當儲存節點中任一儲存磁碟區的可用空間大於該磁碟區的讀寫浮水印時、節點會自動轉換回讀寫狀態。

例如、假設儲存節點已轉換為唯讀模式。此外、假設每個磁碟區都有 30 GB 的讀寫浮水印。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。

讀寫浮水印一律大於軟式唯讀浮水印和硬式唯讀浮水印。

檢視儲存**Volume**浮點

您可以檢視目前的浮水印設定和系統最佳化的值。如果未使用最佳化的浮水印、您可以判斷是否可以或應該調整設定。

開始之前

- 您已完成 StorageGRID 11.6 或更新版本的升級。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。

檢視目前的浮水印設定

您可以在Grid Manager中檢視目前的儲存浮水印設定。

步驟

1. 選擇*支援* > 其他 > 儲存浮水印。
2. 在「儲存浮水印」頁面上、查看「使用最佳化值」核取方塊。
   - 如果選取此核取方塊、則會根據儲存節點的大小和磁碟區的相對容量、針對每個儲存節點上的每個儲存磁碟區最佳化所有三個浮水印。

     這是預設和建議的設定。請勿更新這些值。您也可以檢視最佳化的儲存浮水印選擇。
   - 如果取消選取 [使用最佳化值] 核取方塊，則會使用自訂（非最佳化）浮水印。不建議使用自訂浮水印設定。請依照的指示"疑難排解低唯讀浮水印會覆寫警示"、判斷您可以或應該調整設定。

     指定自訂浮水印設定時、您必須輸入大於 0 的值。

[[view-優 化的儲存浮水印 **]]** 檢視最佳化的儲存浮水印

StorageGRID 使用兩個 Prometheus 指標來顯示其針對儲存 Volume 軟唯讀浮水印所計算的最佳化值。您可以檢視網格中每個儲存節點的最小和最大最佳化值。

1. 選擇*支援* > 工具 > 指標。

2. 在Prometheus區段中、選取連結以存取Prometheus使用者介面。
3. 若要查看建議的最小軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*執行*：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後一欄顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印最小最佳化值。如果此值大於儲存磁碟區軟唯讀浮水印的自訂設定、則會針對儲存節點觸發 * 低唯讀浮水印置換 * 警示。

4. 若要查看建議的最大軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*執行*：

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後一欄顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印最大最佳化值。

在 **StorageGRID** 中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

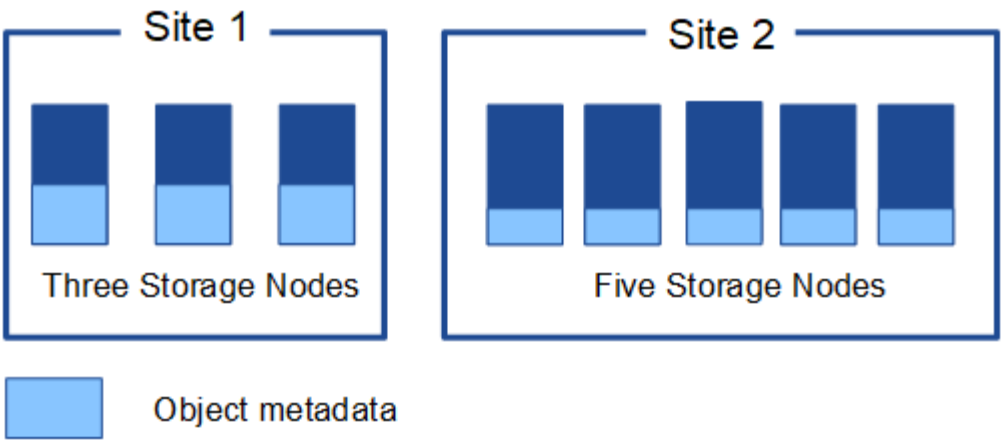
對於物件的物件、物件中繼資料包含下列類型的資訊：StorageGRID

- 系統中繼資料、包括每個物件的唯一 ID （ UUID ）、物件名稱、 S3 貯體名稱、租戶帳戶名稱或 ID 、物件的邏輯大小、物件第一次建立的日期和時間、以及物件上次修改的日期和時間。
- 任何與物件相關聯的自訂使用者中繼資料金鑰值配對。
- 對於S3物件、任何與物件相關聯的物件標記金鑰值配對。
- 對於複寫的物件複本、每個複本的目前儲存位置。
- 對於以銷毀編碼的物件複本、每個片段的目前儲存位置。
- 對於Cloud Storage Pool中的物件複本、物件的位置、包括外部儲存區名稱和物件的唯一識別碼。
- 對於分段物件和多部分物件、區段識別碼和資料大小。

物件中繼資料如何儲存？

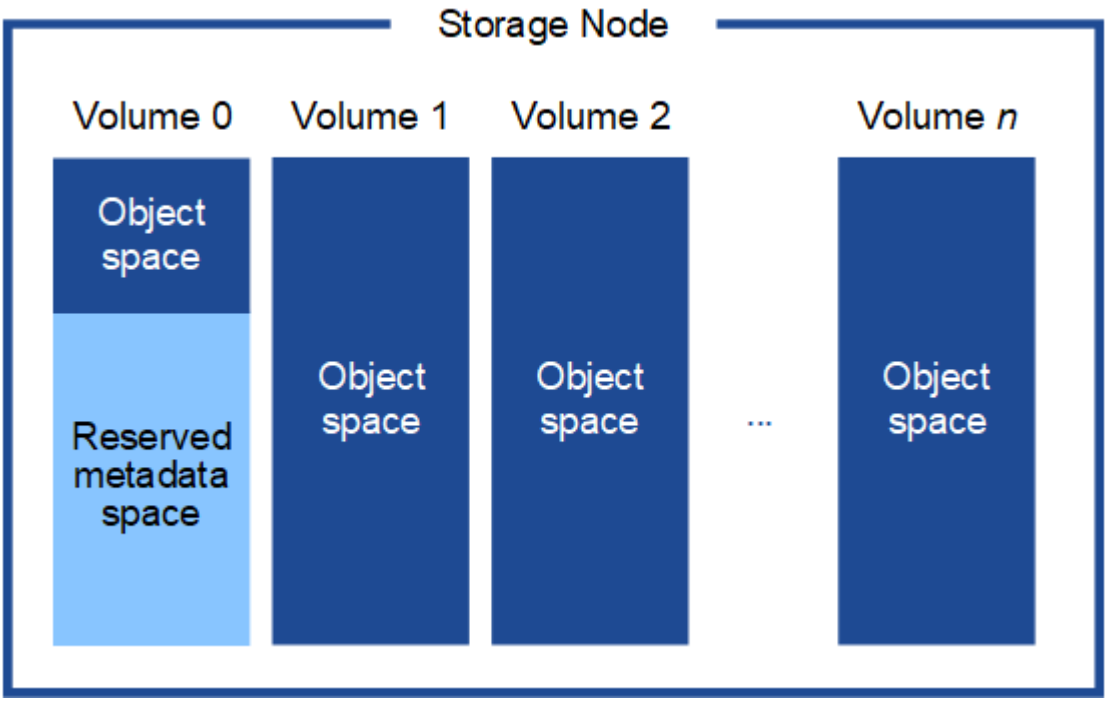
此功能可在Cassandra資料庫中維護物件中繼資料、並獨立儲存物件資料。StorageGRID為了提供備援並保護物件中繼資料免於遺失、StorageGRID 我們在每個站台儲存系統中所有物件的三份中繼資料複本。

此圖代表兩個站台的儲存節點。每個站台都有相同數量的物件中繼資料、而且每個站台的中繼資料會在該站台的所有儲存節點之間細分。



物件中繼資料儲存在何處？

此圖代表單一儲存節點的儲存磁碟區。



如圖所示StorageGRID 、在每個儲存節點的儲存磁碟區0上、利用此功能保留空間來儲存物件中繼資料。它會使用保留空間來儲存物件中繼資料、並執行必要的資料庫作業。儲存磁碟區0和儲存節點中所有其他儲存磁碟區的剩餘空間、僅用於物件資料（複寫複本和銷毀編碼片段）。

在特定儲存節點上、保留給物件中繼資料的空間量取決於以下說明的幾個因素。

中繼資料保留空間設定

_中繼 資料保留空間 _ 是系統範圍的設定、代表將保留給每個儲存節點的磁碟區 0 上中繼資料的空間量。如表所示、此設定的預設值是根據：

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

用於初始**StorageGRID** 安裝的版本	儲存節點上的**RAM**容量	預設中繼資料保留空間設定
12.1	在網格中的每個儲存節點上提供128 GB以上的容量	20 TB（20,000 GB）
	在網格中的任何儲存節點上小於128 GB	3 TB（3、000 GB）
11.5 至 12.0	在網格中的每個儲存節點上提供128 GB以上的容量	8 TB（8、000 GB）
	在網格中的任何儲存節點上小於128 GB	3 TB（3、000 GB）
11.1 至 11.4	在任一站台的每個儲存節點上提供128 GB以上的容量	4 TB（4、000 GB）
	每個站台上的任何儲存節點均小於128 GB	3 TB（3、000 GB）
11.0 或更早版本	任何金額	2 TB（2、000 GB）

檢視中繼資料保留空間設定

請依照下列步驟檢視 StorageGRID 系統的中繼資料保留空間設定。

步驟

1. 選擇*配置* > 系統 > 儲存設定。
2. 在「儲存設定」頁面上、展開 * 中繼資料保留空間 * 區段。

對於 StorageGRID 11.8 或更高版本、中繼資料保留空間值必須至少為 100 GB 、且不得超過 1 PB 。

對於每個儲存節點具有 128 GB 或更多 RAM 的新 StorageGRID 12.1 或更高版本的安裝，預設設定為 20,000 GB （20 TB）。

中繼資料的實際保留空間

與系統範圍的中繼資料保留空間設定不同、物件中繼資料的實際保留空間 _ 是針對每個儲存節點所決定。對於任何指定的儲存節點、中繼資料的實際保留空間取決於節點的 Volume 0 大小和系統範圍的中繼資料保留空間設定。

節點的**Volume 0**大小	中繼資料的實際保留空間
低於 500 GB （非正式作業用途）	10%的Volume 0

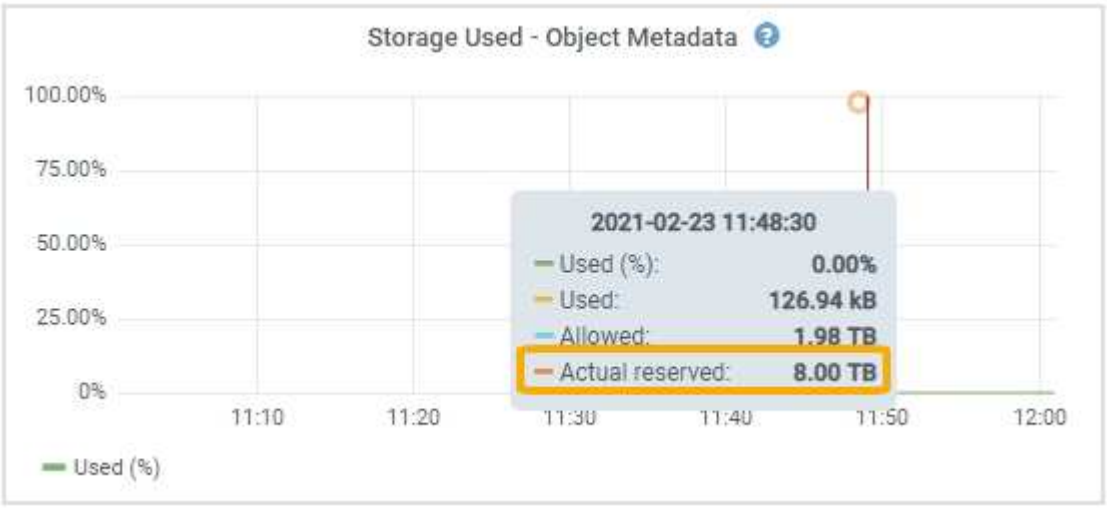
節點的**Volume 0**大小	中繼資料的實際保留空間
500 GB 以上 + 或 + 僅中繼資料儲存節點	這些值越小： • Volume 0. • 中繼資料保留空間設定 • 附註 * ：僅中繼資料儲存節點只需要一個 rangedb 。

檢視中繼資料的實際保留空間

請依照下列步驟、檢視特定儲存節點上的中繼資料實際保留空間。

步驟

1. 從網格管理器中，選擇*節點* > 儲存節點。
2. 選擇* Storage*（儲存設備）選項卡。
3. 將游標放在「已使用的儲存空間 - 物件中繼資料」圖表上、然後找出 * 實際保留 * 值。



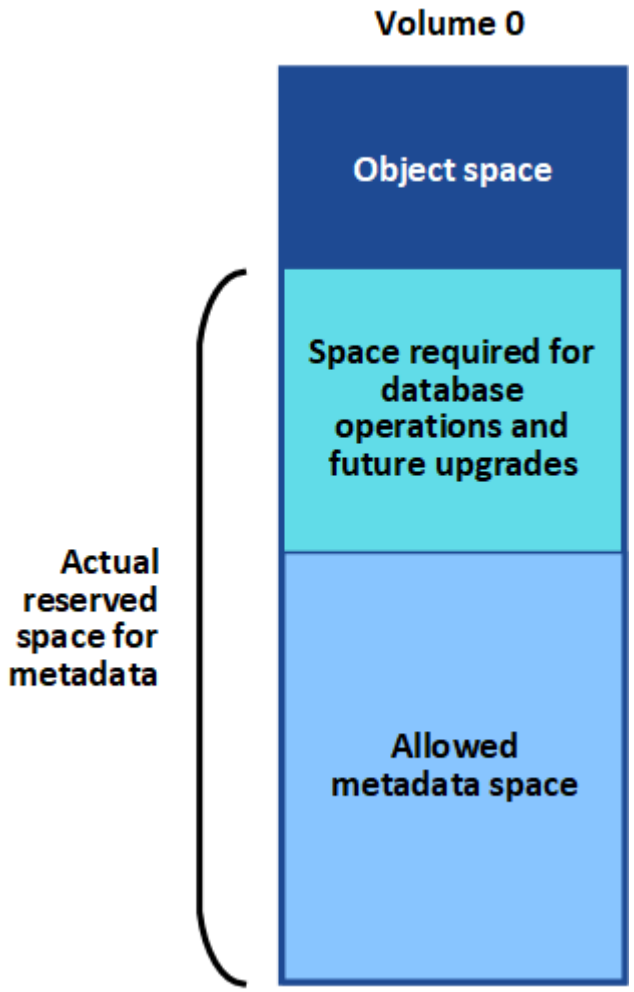
快照中，「實際保留空間」值為 20 TB。此快照適用於新安裝的 StorageGRID 12.1 中的大型儲存節點。Volume 0 至少為 20 TB，因此使用預設的系統層級中繼資料保留空間設定。

實際保留中繼資料空間範例

假設您安裝了一個新的 StorageGRID 系統，版本為 12.1 或更高版本。在本例中，假設每個儲存節點擁有超過 128 GB 的 RAM，且儲存節點 1 （SN1） 的 Volume 0 為 6 TB。基於這些值：

- 系統級 中繼資料保留空間 設定為 20 TB。（如果每個儲存節點的 RAM 超過 128 GB，則這是新安裝 StorageGRID 12.1 或更高版本時的預設值。）
- 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」設定值，因此整個 Volume 都已保留。）

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*。

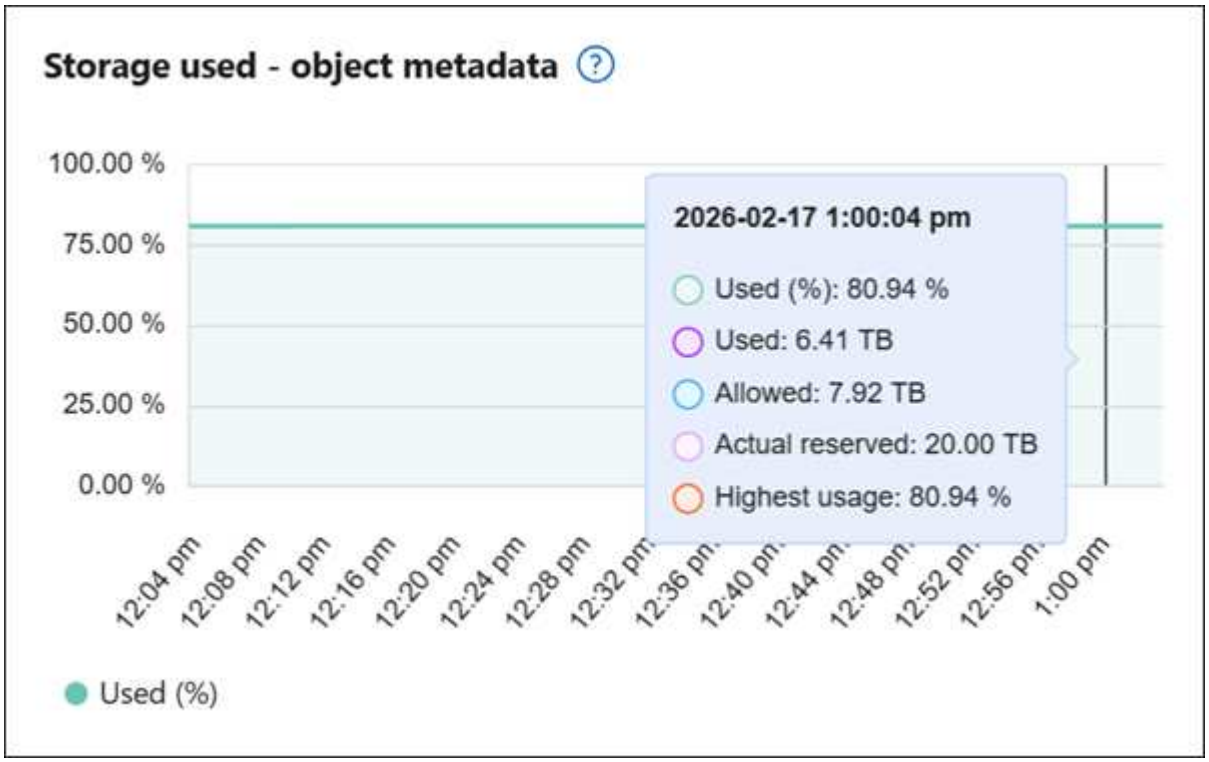
		*儲存節點*上的記憶體容量	
	&lt ； 128 GB	>= 128 GB	中繼資料的實際保留空間
&lt ； = 4 TB	實際保留空間的 75% 用於中繼資料，最大可達 1.32 TB	實際保留空間的 75% 用於中繼資料，最大可達 1.98 TB	4 TB

檢視允許的中繼資料空間

請遵循下列步驟、檢視儲存節點允許的中繼資料空間。

步驟

1. 從網格管理器中選擇*節點*。
2. 選取儲存節點。
3. 選擇* Storage*（儲存設備）選項卡。
4. 將游標放在「已使用的儲存空間 - 物件中繼資料」圖表上、然後找出 * 允許 * 值。



在快照中，允許 值為 7.92 TB，這是儲存節點的最大值，該儲存節點的實際中繼資料保留空間超過 4 TB。

*允許*值對應於此Prometheus指標：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允許的中繼資料空間範例

假設您安裝了一個新的 StorageGRID 系統，版本為 12.1 或更高版本。在本例中，假設每個儲存節點擁有超過 128 GB 的 RAM，且儲存節點 1 （SN1） 的 Volume 0 為 6 TB。基於這些值：

- 系統級 中繼資料保留空間 設定為 20 TB。（如果每個儲存節點的 RAM 超過 128 GB，則這是新安裝 StorageGRID 12.1 或更高版本時的預設值。）
- 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」設定值，因此整個 Volume 都已保留。）
- 根據 允許用於中繼資料空間的表格 中所示的計算，SN1 上中繼資料的*允許*空間為 3.75 TB：（中繼資料的實際保留空間 – 1 TB）× 75%，最大可達 7.92 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

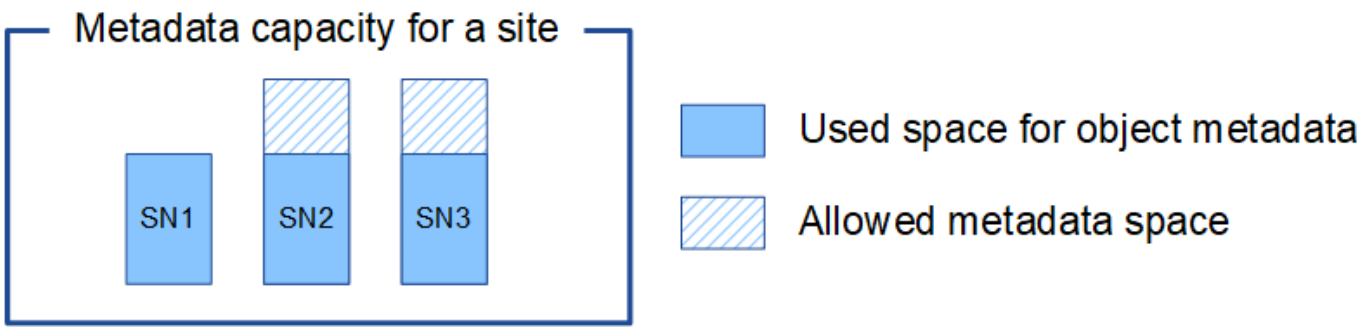
大小不同的儲存節點、站台上最小的節點就會決定站台的中繼資料容量。

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	2.2TB	2.2TB	1.32TB
SN2	5TB	4TB	1.98TB
SN3	6TB	4TB	1.98TB

由於物件中繼資料會平均分散於站台的儲存節點、因此本範例中的每個節點只能容納1.32 TB的中繼資料。無法使用額外的 0.66 TB 的 SN2 和 SN3 中繼資料空間。



同樣地、StorageGRID 由於每StorageGRID 個站台的所有物件中繼資料都是由每個站台的StorageGRID 物件中繼資料容量所決定、因此整個作業系統的中繼資料容量取決於最小站台的物件中繼資料容量。

此外、由於物件中繼資料容量可控制最大物件數、因此當某個節點的中繼資料容量不足時、網格實際上已滿。

相關資訊

- 若要瞭解如何監控每個儲存節點的物件中繼資料容量，請參閱的指示"監控 StorageGRID"。
- 若要增加系統的物件中繼資料容量、請"展開網格"新增儲存節點。

在 **StorageGRID** 中增加 **Metadata Reserved Space** 設定

如果您的儲存節點符合 RAM 和可用空間的特定需求、您可能可以增加中繼資料保留空間系統設定。

您需要的產品

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 你有"Root 存取權限或其他網格配置權限"。

關於這項工作

您可以手動將全系統的中繼資料保留空間設定增加至 8 TB 。

只有當這兩個陳述均為真時、您才能增加全系統中繼資料保留空間設定的值：

- 系統中任何站台的儲存節點都有128 GB以上的RAM。
- 系統中任何站台的儲存節點、在儲存Volume 0上都有足夠的可用空間。

請注意、如果您增加此設定、您將會同時減少所有儲存節點之儲存Volume 0上的物件儲存可用空間。因此、您可能偏好根據預期的物件中繼資料需求、將中繼資料保留空間設為小於8 TB的值。

> 一般而言、最好使用較高的值、而非較低的值。如果「中繼資料保留空間」設定太大、您可以稍後再加以減少。相反地、如果您稍後增加值、系統可能需要移動物件資料以釋放空間。

如需中繼資料保留空間設定如何影響特定儲存節點上物件中繼資料儲存空間的詳細說明，請參閱"管理物件中繼資料儲存"。

步驟

1. 判斷目前的中繼資料保留空間設定。
   a. 選擇*配置* > 系統 > 儲存設定。
   b. 注意*元資料保留空間*的值。
2. 確保每個儲存節點的儲存Volume 0上有足夠的可用空間來增加此值。
   a. 選擇*節點*。
   b. 選取網格中的第一個儲存節點。
   c. 選取「Storage（儲存）」索引標籤。
   d. 在Volumes（磁碟區）區段中、找到*/var/local/rangedb/0*項目。
   e. 確認可用值等於或大於您要使用的新值與目前中繼資料保留空間值之間的差異。

      例如、如果中繼資料保留空間設定目前為4 TB、而您想要將其增加至6 TB、則可用值必須為2 TB或更大。

   f. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點沒有足夠的可用空間、則無法增加中繼資料保留空間值。請勿繼續執行此程序。
      - 如果每個儲存節點在Volume 0上有足夠的可用空間、請前往下一步。
3. 確保每個儲存節點上至少有128 GB的RAM。
   a. 選擇*節點*。
   b. 選取網格中的第一個儲存節點。
   c. 選取*硬體*索引標籤。
   d. 將游標暫留在「記憶體使用量」圖表上。確保*總記憶體*至少128 GB。
   e. 對所有儲存節點重複這些步驟。
      - 如果一個或多個儲存節點沒有足夠的可用總記憶體、則無法增加中繼資料保留空間值。請勿繼續執

行此程序。

- 如果每個儲存節點的總記憶體容量至少為128 GB、請執行下一步。

4. 更新中繼資料保留空間設定。
   a. 選擇*配置* > 系統 > 儲存設定。
   b. 選擇*元資料保留空間*。
   c. 輸入新值。

      例如、若要輸入最大支援值8 TB、請輸入* 80000000000000000*（8、接著12個零）

   d. 選擇*保存*。

壓縮 **StorageGRID** 中儲存的物件

您可以啟用物件壓縮、以減少儲存在 StorageGRID 中的物件大小、讓物件消耗的儲存空間更少。

開始之前

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

關於這項工作

根據預設、物件壓縮會停用。如果您啟用壓縮、 StorageGRID 會在儲存每個物件時、使用無損壓縮來嘗試壓縮每個物件。

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

啟用物件壓縮之前、請注意下列事項：

- 除非您知道儲存的資料是可壓縮的、否則不應選取 * 壓縮儲存的物件 * 。
- 將物件儲存StorageGRID 至物件的應用程式可能會先壓縮物件、然後再儲存物件。如果用戶端應用程式在將物件儲存至 StorageGRID 之前已壓縮物件、選取此選項將不會進一步縮小物件的大小。
- 如果您使用 NetApp FabricPool 搭配 StorageGRID 、請勿選取 * 壓縮儲存的物件 * 。
- 如果選取 * 壓縮儲存的物件 * 、 S3 用戶端應用程式應避免執行 GetObject 作業、以指定傳回位元組範圍。這些「範圍讀取」作業效率不彰、因為 StorageGRID 必須有效地解壓縮物件以存取要求的位元組。從非常大的物件要求少量位元組的 GetObject 作業尤其缺乏效率、例如從 50 GB 壓縮物件讀取 10 MB 範圍是效率不彰的。

  如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

  > 如果您需要壓縮物件、而用戶端應用程式必須使用範圍讀取、請增加應用程式的讀取逾時。

步驟

1. 選擇*配置* > 系統 > 儲存設定 > 物件壓縮。

2. 選中 **Compress Stored objects** 複選框。
3. 選擇*保存*。

在 **StorageGRID** 中管理已滿的 **Storage Nodes**

當儲存節點達到容量時、您必須StorageGRID 透過新增的儲存設備來擴充此功能。有三種選項可供選擇：新增儲存磁碟區、新增儲存擴充櫃、以及新增儲存節點。

新增儲存磁碟區

每個儲存節點都支援最大數量的儲存磁碟區。所定義的最大值會因平台而異。如果儲存節點包含的儲存磁碟區數量少於最大儲存磁碟區數量、您可以新增磁碟區來增加其容量。請參閱的說明"擴充StorageGRID 功能"。

新增儲存擴充櫃

某些 StorageGRID 應用裝置儲存節點（例如 SG6060 或 SG6160 ）可支援額外的儲存櫃。如果StorageGRID 您擁有擴充功能尚未擴充至最大容量的不完整產品、您可以新增儲存櫃來增加容量。請參閱的說明"擴充StorageGRID 功能"。

新增儲存節點

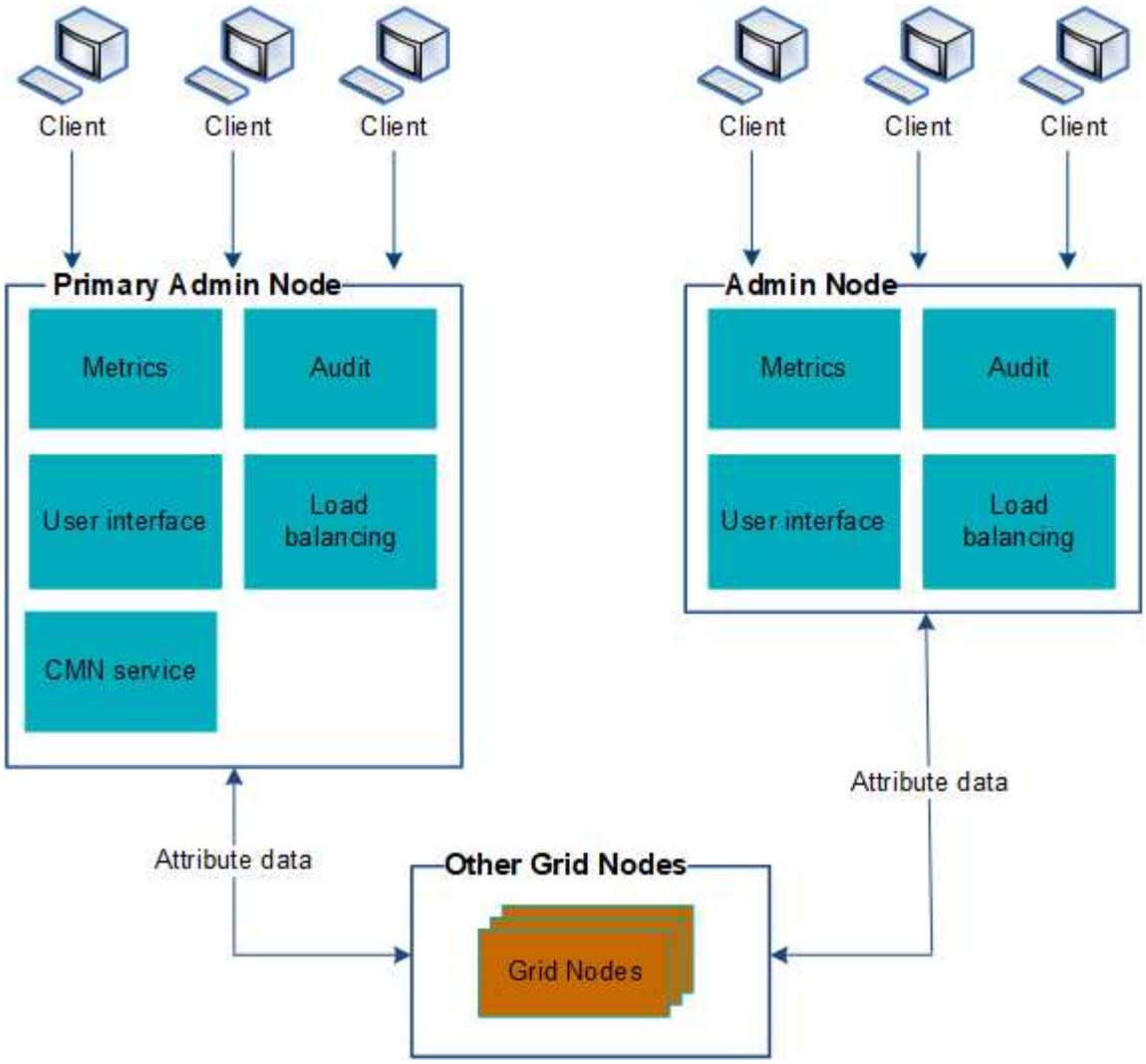
您可以新增儲存節點來增加儲存容量。新增儲存設備時、必須仔細考量目前使用中的ILM規則和容量需求。請參閱的說明"擴充StorageGRID 功能"。

管理管理節點

在 **StorageGRID** 中使用多個管理節點

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、警示仍會觸發、電子郵件通知和 AutoSupport 套件仍會傳送。不過、擁有多個管理節點並不提供容錯移轉保護、只有通知和 AutoSupport 套件除外。



如果管理節點故障、有兩個選項可以繼續檢視及設定StorageGRID 功能不全的系統：

- Web用戶端可重新連線至任何其他可用的管理節點。
- 如果系統管理員已設定管理節點的高可用度群組、則網路用戶端可使用HA群組的虛擬IP位址、繼續存取Grid Manager或租戶管理程式。請參閱。 "管理高可用度群組"

> 使用 HA 群組時、如果作用中的管理節點故障、存取就會中斷。使用者必須在HA群組的虛擬IP位址容錯移轉至群組中的另一個管理節點之後、再次登入。

部分維護工作只能使用主要管理節點來執行。如果主要管理節點故障、則必須先將其恢復、才能StorageGRID使該系統再次完全正常運作。

識別 **StorageGRID** 中的主要管理節點

主要管理節點提供的功能比非主要管理節點更多。例如、某些維護程序必須使用主要管理節點來執行。

如需管理節點的詳細資訊、請參閱"什麼是管理節點"。

開始之前

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

步驟

1. 選擇*節點*。
2. 在搜尋方塊中輸入 * primary * 。

   在搜尋結果中、以「類型」欄中顯示的「主要管理節點」來識別節點。應列出一個主要管理節點。

使用ILM管理物件

使用 ILM 管理 StorageGRID 中的物件

ILM 原則中的資訊生命週期管理（ ILM ）規則會指示 StorageGRID 如何建立及散佈物件資料複本、以及如何隨時間管理這些複本。

關於這些指示

設計及實作 ILM 規則與原則需要仔細規劃。您必須瞭StorageGRID 解作業需求、您的作業系統拓撲、物件保護需求、以及可用的儲存類型。然後、您必須決定要如何複製、分散及儲存不同類型的物件。

請依照下列指示：

- 瞭解 StorageGRID ILM 、包括"ILM 如何在物件生命週期中運作"。
- 瞭解如何設定"儲存資源池"、"雲端儲存資源池"和"ILM規則"。
- 瞭解如何"建立、模擬及啟動 ILM 原則"保護一或多個站台的物件資料。
- 瞭解如何"使用 S3 物件鎖定來管理物件"、有助於確保特定 S3 儲存區中的物件不會在指定的時間內遭到刪除或覆寫。

深入瞭解

若要深入瞭解、請觀看以下影片：

ILM 規則概述

ILM 策略概述

ILM與物件生命週期

ILM 在 StorageGRID 中物件生命週期內的運作方式

瞭解StorageGRID 如何在物件生命週期的每個階段使用ILM來管理物件、有助於您設計更有效的原則。

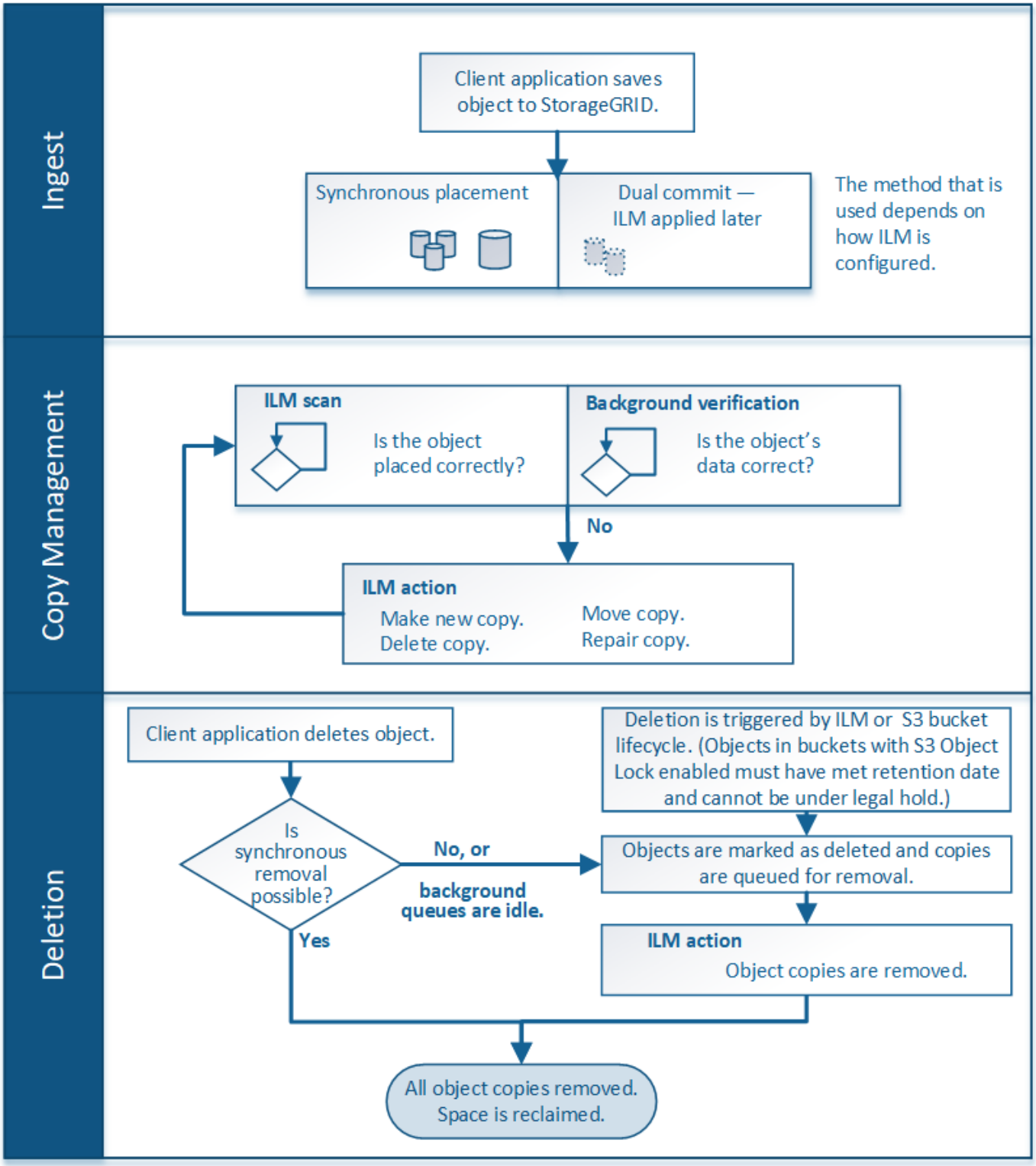
- * 擷取 * ：擷取從 S3 用戶端應用程式建立連線以將物件儲存至 StorageGRID 系統開始、並在 StorageGRID 將「擷取成功」訊息傳回用戶端時完成。物件資料在擷取期間會受到保護、方法是立即套用ILM指令（同步

放置）、或是建立過渡複本、並在稍後套用ILM（雙重提交）、視ILM需求的指定方式而定。

- 複製管理：建立ILM放置說明中所指定的物件複本數量和類型之後StorageGRID 、此功能可管理物件位置、並保護物件免於遺失。
  - * ILM 掃描與評估 * ： StorageGRID 會持續掃描儲存在網格中的物件清單、並檢查目前的複本是否符合 ILM 要求。當需要不同類型、數字或物件複本位置時、StorageGRID 會視需要建立、刪除或移動複本。
  - * 背景驗證 * ： StorageGRID 會持續執行背景驗證、以檢查物件資料的完整性。如果發現問題、StorageGRID 則在符合目前ILM需求的位置、由NetApp自動建立新的物件複本或替換的銷毀編碼物件片段。請參閱。 "驗證物件完整性"
- 物件刪除：當所有複本都從StorageGRID 作業系統中移除時、物件的管理就會結束。物件可因為用戶端的刪除要求而移除、或是因為ILM刪除或S3儲存區生命週期到期而刪除。

> 如果儲存庫中的物件處於合法保留狀態、或是指定了保留日期但尚未達到、則無法刪除已啟用 S3 物件鎖定的物件。

此圖摘要說明ILM在物件生命週期內的運作方式。



物件擷取方式

StorageGRID 中的 **ILM** 擷取選項

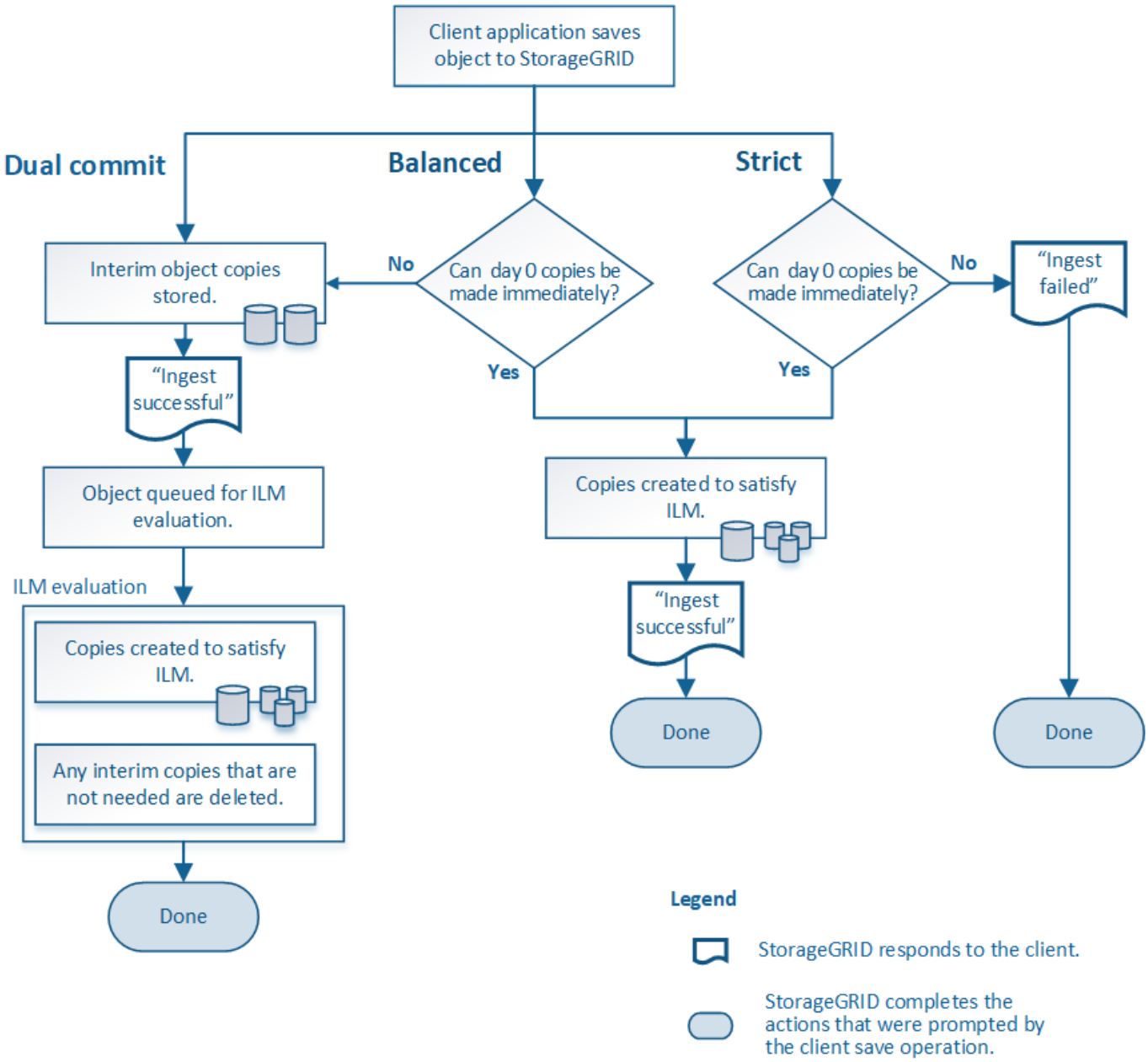
建立 ILM 規則時、您可以指定三個選項之一來保護擷取時的物件：雙重認可、嚴格或平衡。

根據您的選擇、StorageGRID 將會製作過渡複本、並將物件排入佇列、以便稍後進行ILM評估、或是使用同步放

置、並立即製作複本以符合ILM需求。

擷取選項的流程圖

流程圖會顯示當物件與使用三個擷取選項中每個選項的ILM規則相符時、會發生什麼情況。



雙重承諾

當您選取雙重提交選項時、 StorageGRID 會立即在兩個不同的儲存節點上製作臨時物件複本、並將「擷取成功」訊息傳回給用戶端。物件會排入ILM評估佇列、之後會製作符合規則放置指示的複本。如果在雙重提交之後無法立即處理 ILM 原則、則站台遺失保護可能需要一些時間才能達成。

在下列任一情況下、請使用「雙重提交」選項：

- 您使用的是多站台ILM規則、而用戶端擷取延遲是您的首要考量。使用雙重提交時、您必須確保您的網格能夠執行其他工作、在雙認可複本不符合 ILM 時、建立及移除這些複本。具體而言：

- 網格上的負載必須足夠低、以避免ILM待處理項目。
- 網格必須有過多的硬體資源（IOPS、CPU、記憶體、網路頻寬等）。

- 您使用的是多站台ILM規則、而站台之間的WAN連線通常具有高延遲或有限頻寬。在此案例中、使用「雙重提交」選項有助於防止用戶端逾時。在選擇「雙重提交」選項之前、您應該使用實際的工作負載來測試用戶端應用程式。

Balanced （平衡）（預設）

當您選取平衡選項時StorageGRID 、也會在擷取時使用同步放置、並立即製作規則放置說明中指定的所有複本。與嚴格選項相反、如果 StorageGRID 無法立即製作所有複本、則會改為使用雙重提交。如果 ILM 原則在多個站台上使用放置位置、而且無法立即保護站台損失、就會觸發 * ILM 放置無法達成 * 警示。

使用「平衡」選項、將資料保護、網格效能和擷取成功完美結合。Balanced （平衡）是 Create ILM Rule （建立 ILM 規則）精靈中的預設選項。

嚴格

當您選取「嚴格」選項時StorageGRID 、會在擷取中使用同步放置、並立即製作規則放置說明中指定的所有物件複本。如果 StorageGRID 無法建立所有複本、則擷取會失敗、例如、所需的儲存位置暫時無法使用。用戶端必須重試此作業。

如果您有作業或法規要求、只要將物件立即儲存在ILM規則中所述的位置、請使用嚴格選項。例如、為了滿足法規要求、您可能需要使用嚴格選項和位置限制進階篩選器、以確保物件永遠不會儲存在特定資料中心。

請參閱。 "範例5：嚴格擷取行為的ILM規則與原則"

StorageGRID 中 **ILM** 擷取選項的優點、缺點和限制

瞭解擷取時保護資料的三種選項（平衡、嚴格或雙重提交）各有哪些優缺點、可協助您決定要為ILM規則選取哪一種選項。

如需擷取選項的總覽"擷取選項"、請參閱。

平衡且嚴格的選項優勢

相較於在擷取期間建立臨時複本的「雙重提交」、兩個同步放置選項可提供下列優點：

- 更佳的資料安全性：物件資料會立即受到ILM規則放置指示中所指定的保護、您可設定此指示、以防止各種故障情況發生、包括多個儲存位置的故障。雙重提交只能防止單一本機複本遺失。
- 更有效率的網格作業：每個物件只會在擷取時處理一次。由於不需要追蹤或刪除過渡複本、因此處理負載較少、資料庫空間也較少。StorageGRID
- （平衡）建議：平衡選項可提供最佳ILM效率。除非需要嚴格的擷取行為、或網格符合使用雙重提交的所有條件、否則建議使用平衡選項。
- （嚴格）物件位置的確定性：嚴格選項可確保物件立即根據ILM規則中的放置指示儲存。

平衡且嚴格的選項缺點

相較於雙重承諾、平衡且嚴格的選項有一些缺點：

- 用戶端擷取時間較長：用戶端擷取延遲時間可能較長。當您使用平衡或嚴格選項時、除非建立並儲存所有的銷毀編碼片段或複寫複本、否則「擷取成功」訊息不會傳回用戶端。不過、物件資料很可能會更快到達最終放置位置。
- * （嚴格）較高的擷取失敗率 * ：使用嚴格選項、只要 StorageGRID 無法立即製作 ILM 規則中指定的所有複本、擷取就會失敗。如果所需的儲存位置暫時離線、或是網路問題導致站台之間複製物件時延遲、您可能會看到擷取失敗率偏高。
- （嚴格）**S3**多部份上傳放置位置在某些情況下可能不如預期：嚴格來說、您期望物件放置方式必須符合ILM規則的說明、否則擷取失敗。不過、在 S3 多部分上傳時、系統會在擷取物件的每個部分時評估 ILM 、並在多部分上傳完成時評估整個物件的 ILM 。在下列情況下、這可能會導致刊登位置與您預期的不同：
  - 如果在S3多重部分上傳進行時ILM發生變更*：由於每個部分都是根據擷取零件時作用中的規則放置、因此當多重部分上傳完成時、物件的某些部分可能無法符合目前的ILM需求。在這些情況下、物件的擷取不會失敗。相反地、任何未正確放置的零件都會排入 ILM 重新評估的佇列、稍後會移至正確的位置。
  - 當**ILM**規則根據尺寸篩選：評估零件的ILM時、StorageGRID 會根據零件大小篩選出、而非物件大小。這表示物件的部分可以儲存在不符合整體物件 ILM 需求的位置。例如、如果規則指定所有10 GB或更大的物件都儲存在DC1、而所有較小的物件則儲存在DC2、則在10部分多部分上傳的每1 GB擷取部分、都會儲存在DC2。評估物件的ILM時、物件的所有部分都會移至DC1。
- （嚴格）當物件標記或中繼資料更新且無法建立新的必要放置位置時、內嵌功能不會失敗：嚴格來說、您期望物件放置在ILM規則所述的位置、或是擷取失敗。但是、當您更新已儲存在網格中之物件的中繼資料或標記時、不會重新擷取該物件。這表示任何由更新觸發的物件放置變更、都不會立即進行。當ILM由正常背景ILM程序重新評估時、便會進行放置變更。如果無法進行必要的放置變更（例如、因為新的必要位置無法使用）、更新的物件會保留目前的放置位置、直到可能變更放置位置為止。

使用平衡且嚴格的選項來限制物件放置

平衡或嚴格的選項無法用於具有下列任一放置指示的 ILM 規則：

- 第0天放入雲端儲存資源池。
- 當規則的建立時間為使用者定義的參考時間時、放置在雲端儲存池中。

這些限制之所以存在、是因為 StorageGRID 無法同步製作複本至雲端儲存池、而使用者定義的建立時間可能會解決目前的問題。

ILM 規則與一致性如何互動、以影響資料保護

您的 ILM 規則和一致性選擇都會影響物件的保護方式。這些設定可以互動。

例如、為 ILM 規則選取的擷取行為會影響物件複本的初始放置、而儲存物件時所使用的一致性則會影響物件中繼資料的初始放置。由於 StorageGRID 需要同時存取物件的資料和中繼資料、才能滿足用戶端要求、因此針對一致性和擷取行為選擇符合的保護層級、可以提供更好的初始資料保護和更可預測的系統回應。

以下是 StorageGRID 中可用一致性值的簡短摘要：

- * 全部 * ：所有節點都會立即接收物件中繼資料、否則要求將會失敗。
- 強全域：保證所有網站上所有客戶端請求的讀寫一致性。配置 Quorum 語意時，將套用下列行為：
  - 當網格具有三個或更多站點時，允許對客戶端請求進行站點故障容忍。雙站點電網不具備站點故障容忍能力。
  - 如果一個站點發生故障，以下 S3 操作將無法成功：

- 刪除 BucketEncryption
- PutBucketBranch
- PuttBucketEncryption
- PuttBucketVersion
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObjectRetention

如果需要的話，你可以 "配置StorageGRID Quorum 語意以實現強全域一致性"。

- **Strong-site** ：物件中繼資料會立即散佈到站台上的其他節點。保證站台內所有用戶端要求的寫入後讀取一致性。
- * 新寫入後讀 * ：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
- * 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

> 在選擇一致性值之前，"閱讀一致性的完整說明" 。在更改預設值之前，您應該了解其優點和限制。

一致性與 **ILM** 規則互動方式的範例

假設您有一個三站點網格，具有以下 ILM 規則和以下一致性：

- **ILM** 規則：建立三個物件副本，一個在本機站點，另一個在每個遠端站點。使用嚴格的攝取行為。
- 一致性：強全域（物件元資料立即分發到多個站點）。

當客戶端將物件儲存到網格時， StorageGRID會複製所有三個物件並將元資料分發到多個站點，然後再將成功返回給客戶端。

在接收成功訊息時，物件將受到完全保護，不會遺失。例如，如果本機站點在攝取後不久遺失，則物件資料和物件元資料的副本仍然存在於遠端站點。該物件可以從其他站點完全檢索。

如果您使用相同的 ILM 規則和強站點一致性，則用戶端可能會在物件資料複製到遠端站點之後但在物件元資料分發到那裡之前收到成功訊息。在這種情況下，物件元資料的保護等級與物件資料的保護等級不符。如果本地站點在攝取後不久遺失，則物件元資料就會遺失。無法檢索該物件。

一致性與 ILM 規則之間的相互關係可能很複雜。如需協助、請聯絡 NetApp 。

相關資訊

"範例5：嚴格擷取行為的ILM規則與原則"

物件的儲存方式（複寫或銷毀編碼）

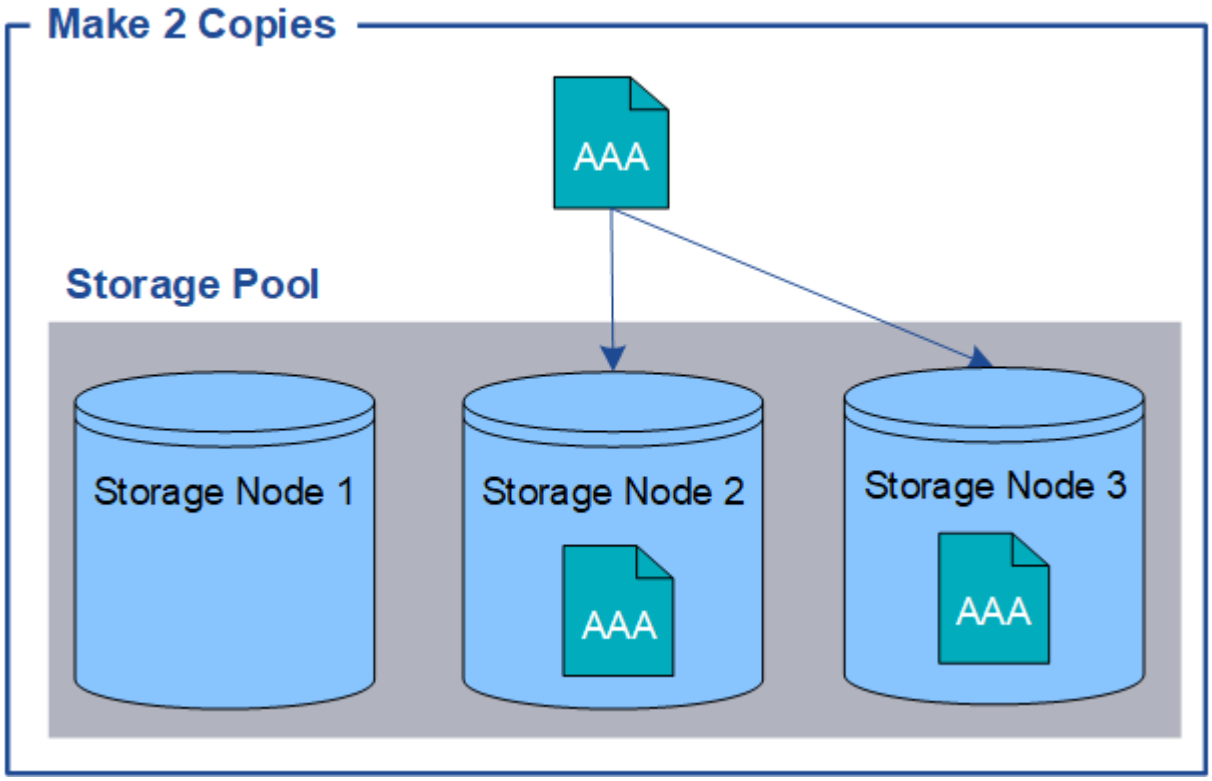
了解 **StorageGRID** 中的複寫

複寫是 StorageGRID 用來儲存物件資料的兩種方法之一（抹除編碼是另一種方法）。當物件符合使用複寫的 ILM 規則時、系統會建立物件資料的精確複本、並將複本儲存在儲存節

點上。

當您設定ILM規則以建立複寫複本時、請指定應建立多少複本、應將複本放置在何處、以及複本應儲存在每個位置的時間。

在下列範例中、ILM規則指定將每個物件的兩個複寫複本放在包含三個儲存節點的儲存資源池中。



當物件符合此規則時、它會建立物件的兩個複本、並將每個複本放在儲存資源池中的不同儲存節點上。StorageGRID這兩份複本可以放在三個可用儲存節點的任兩個上。在此情況下、規則會將物件複本放在儲存節點2和3上。因為有兩個複本、所以如果儲存資源池中的任何節點故障、就可以擷取物件。

在任何指定的儲存節點上、僅能儲存一個物件的複本複本。StorageGRID如果您的網格包含三個儲存節點、而且您建立了一個4份複本ILM規則、則只會製作三份複本、每個儲存節點只會製作一份複本。觸發「無法實現的ILM放置」警示、表示無法完全套用ILM規則。

相關資訊

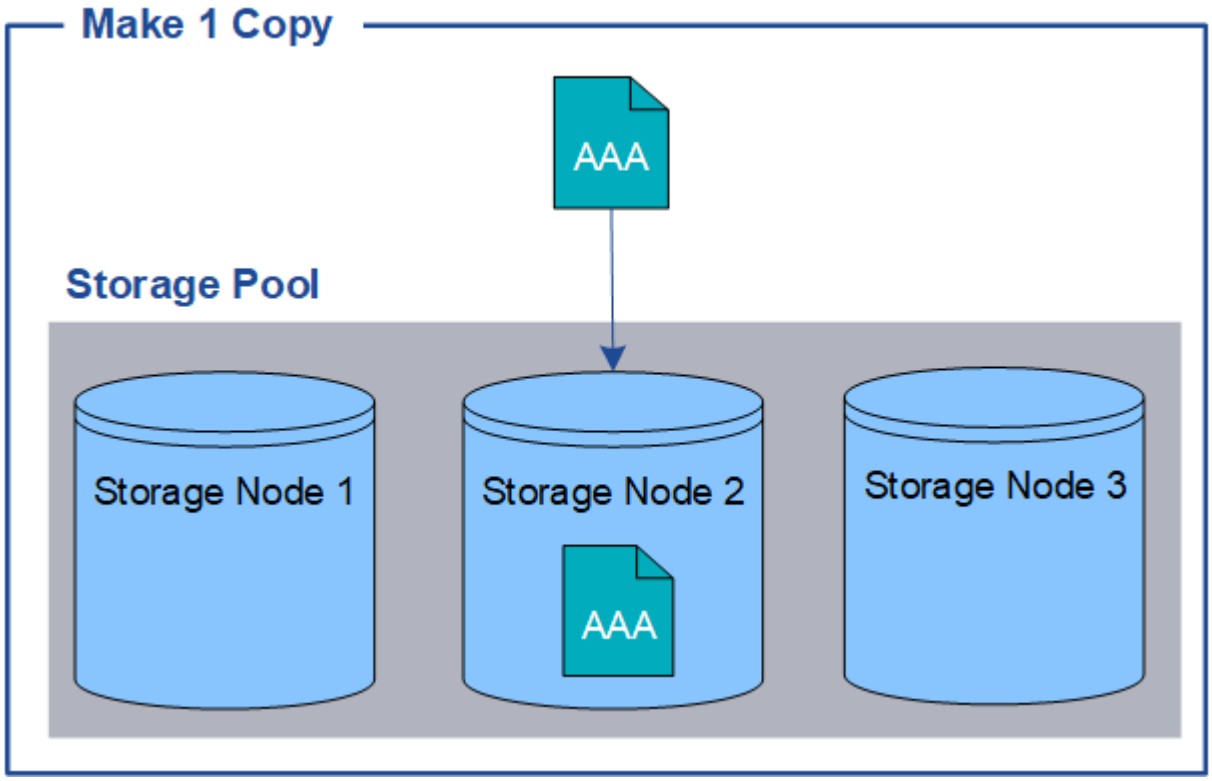
- "什麼是銷毀編碼"
- "什麼是儲存池"
- "使用複寫和銷毀編碼來啟用站台遺失保護"

StorageGRID 中單一複本複寫的風險

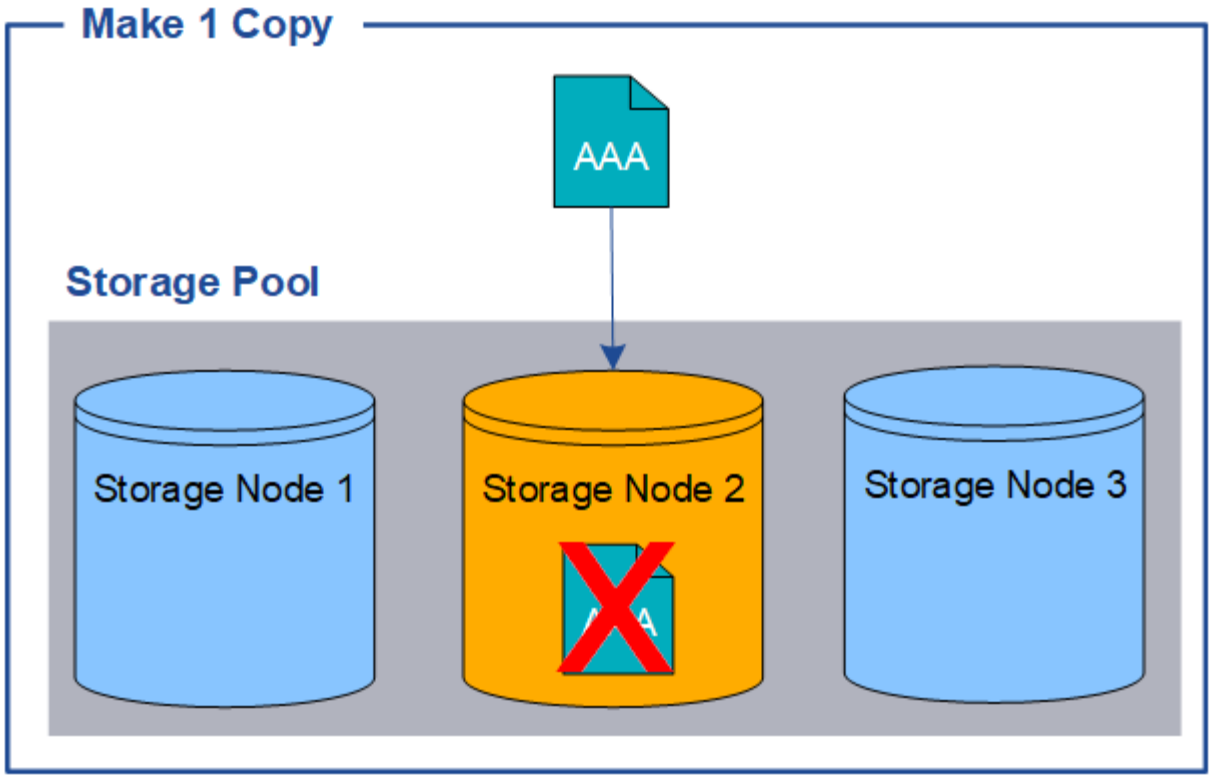
建立ILM規則以建立複寫複本時、您應該在放置指示中、隨時至少指定兩個複本。

請勿使用 ILM 規則、在任何時間段內只建立一個複寫複本。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

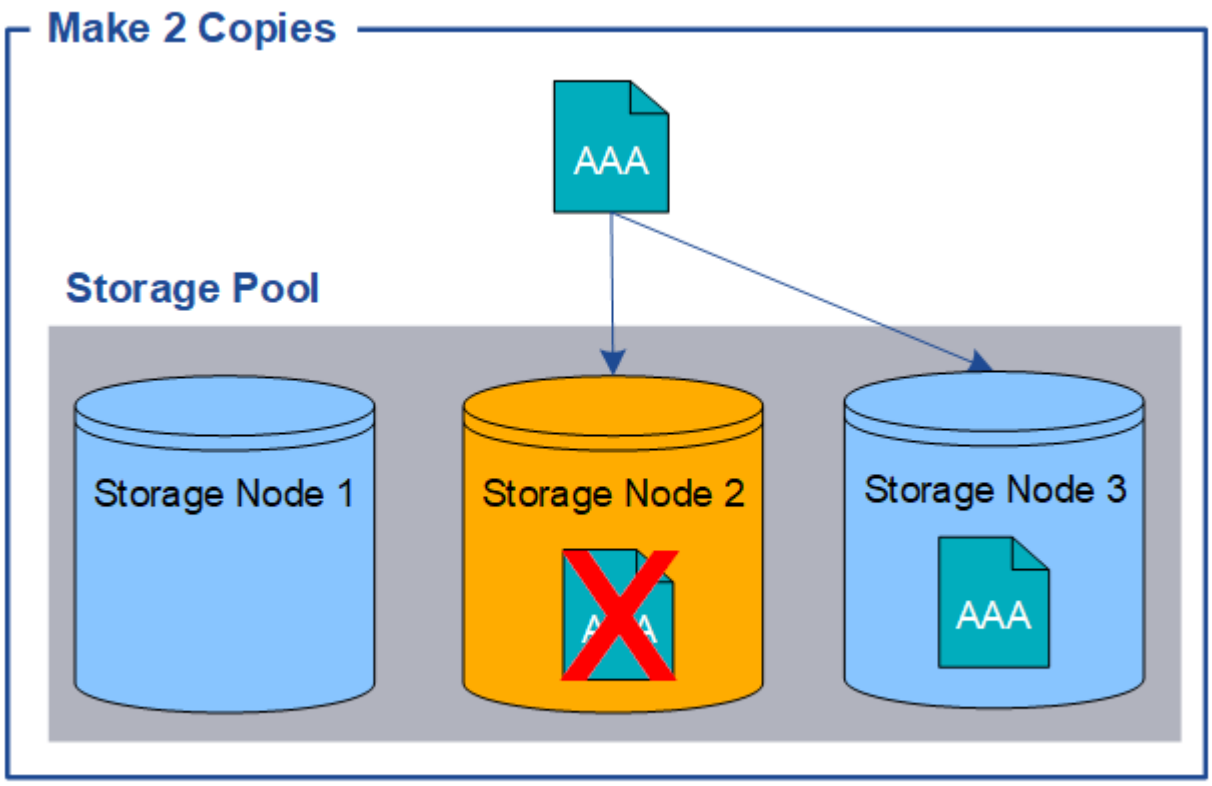
在下列範例中、「製作1複製ILM」規則會指定將物件的一個複寫複本放在包含三個儲存節點的儲存資源池中。擷取符合此規則的物件時StorageGRID 、將單一複本放在單一儲存節點上。



如果ILM規則只建立物件的一個複寫複本、則當儲存節點無法使用時、物件就無法存取。在此範例中、只要儲存節點2離線（例如在升級或其他維護程序期間）、您就會暫時失去物件aaa的存取權。如果儲存節點2故障、您將完全失去物件AAA。



為了避免遺失物件資料、您應該一律至少製作兩份複本、以複寫方式保護所有物件。如果有兩個以上的複本存在、您仍可在一個儲存節點故障或離線時存取物件。

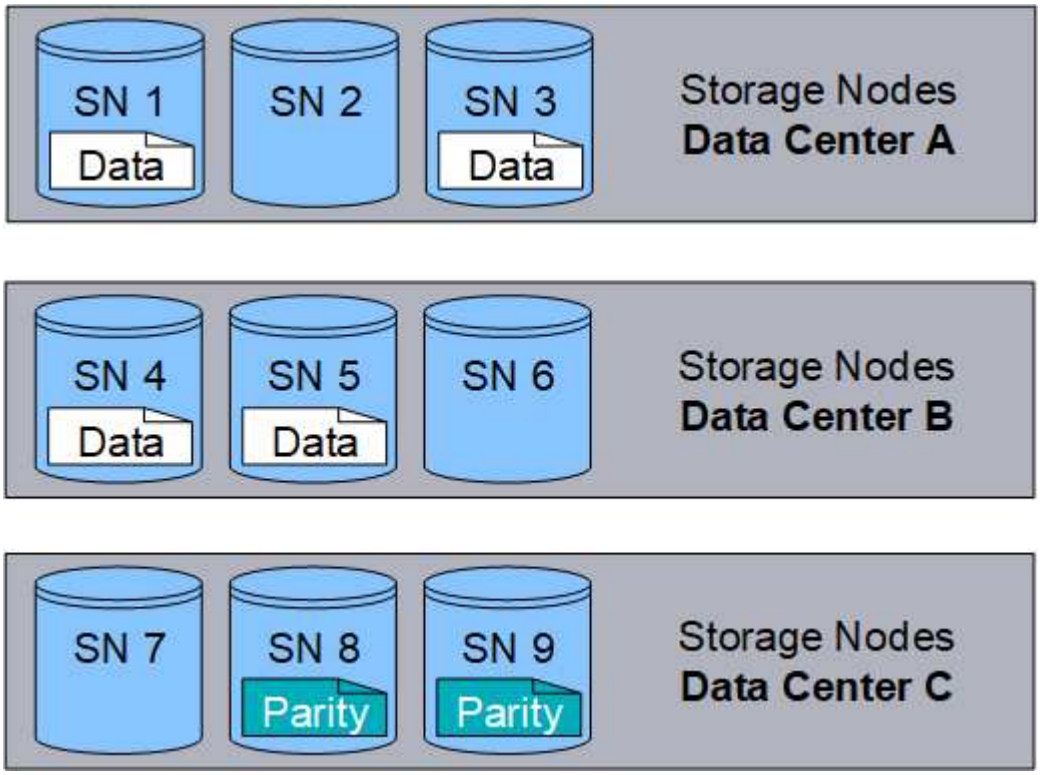


銷毀編碼是 StorageGRID 用來儲存物件資料的兩種方法之一（複寫是另一種方法）。當物件符合使用抹除編碼的 ILM 規則時、這些物件會切換成資料片段、會計算額外的同位元區隔片段、而且每個片段都會儲存在不同的儲存節點上。

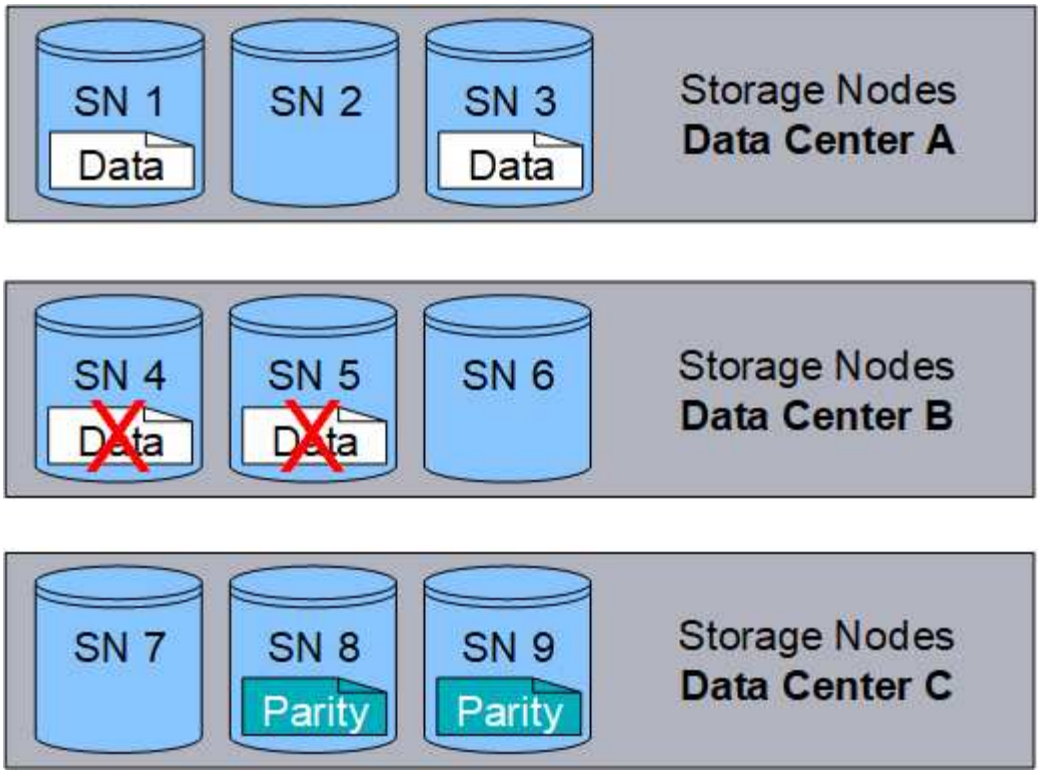
存取物件時、會使用儲存的片段重新組裝物件。如果資料或同位元檢查片段毀損或遺失、則銷毀編碼演算法可利用其餘資料和同位元檢查片段的子集來重新建立該片段。

建立 ILM 規則時、 StorageGRID 會建立支援這些規則的銷毀編碼設定檔。您可以檢視抹除編碼設定檔清單、"重新命名抹除編碼設定檔"或"如果目前未在任何 ILM 規則中使用抹除編碼設定檔、請停用該設定檔"。

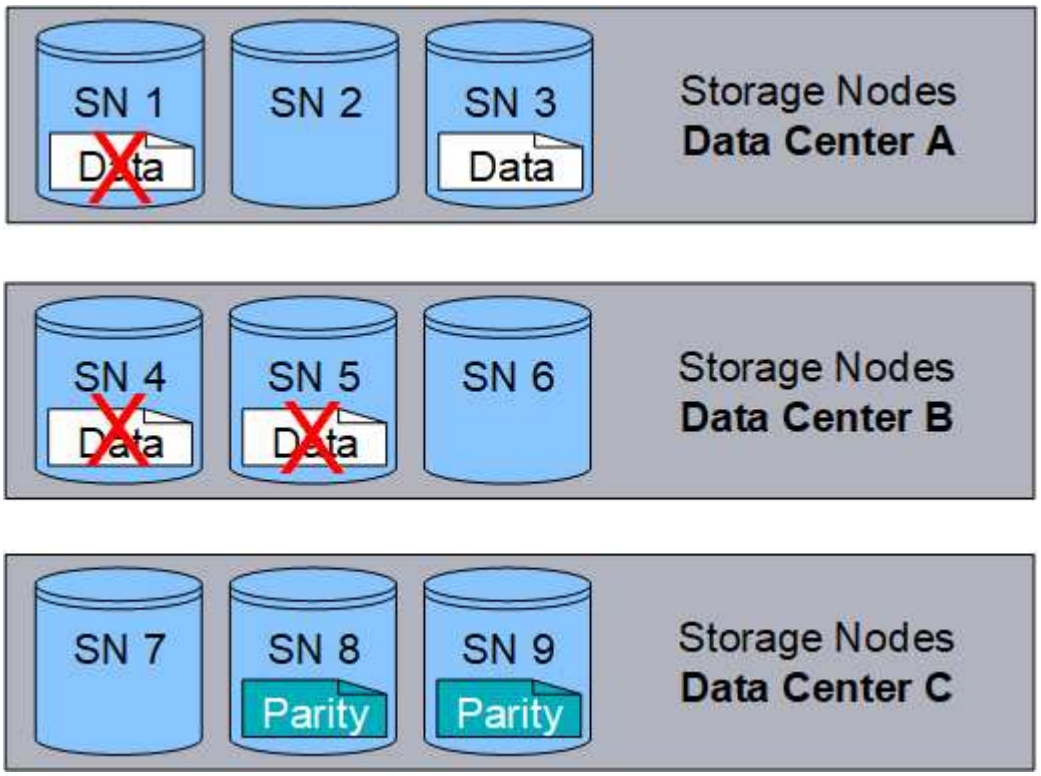
以下範例說明在物件資料上使用銷毀編碼演算法。在此範例中、ILM規則使用4+2銷毀編碼方案。每個物件會分割成四個等量資料片段、並從物件資料計算兩個同位元檢查片段。這六個片段中的每個片段都儲存在三個資料中心站台的不同節點上、以針對節點故障或站台遺失提供資料保護。



4+2 銷毀編碼方案可透過各種方式進行設定。例如、您可以設定包含六個儲存節點的單一站台儲存池。對於"站台遺失保護"、您可以使用包含三個站台的儲存池、每個站台有三個儲存節點。只要六個片段（資料或同位元檢查）中的任四個仍然可用、就能擷取物件。最多可遺失兩個片段、而不會遺失物件資料。如果整個站台遺失、只要所有其他片段仍可存取、仍可擷取或修復物件。



如果遺失兩個以上的儲存節點、則無法擷取物件。



相關資訊

- "什麼是複寫"
- "什麼是儲存池"
- "什麼是銷毀編碼方案"

- "重新命名抹除編碼設定檔"
- "停用抹除編碼設定檔"

了解 **StorageGRID** 中的抹除編碼方案

銷毀編碼方案可控制每個物件所建立的資料片段數量、以及同位元檢查片段數量。

當您建立或編輯 ILM 規則時、請選取可用的銷毀編碼配置。StorageGRID 會根據您計畫使用的儲存資源池中有多少個儲存節點和站台、自動建立銷毀編碼方案。

資料保護

此系統使用Reed-Solomon銷毀編碼演算法。StorageGRID演算法將物件分成 `k`資料片段、並計算 `m`同位元片段。

這些 `k + m = n`片段分佈在儲存節點之間 `n`、以提供下列資料保護：

- 若要擷取或修復物件、 `k`需要片段。
- 物件可承受最多 `m`遺失或毀損的片段。的值越高 `m`、容錯能力就越高。

最佳的資料保護是由銷毀編碼方案提供、其在儲存資源池中具有最高的節點或磁碟區容錯能力。

儲存負荷

擦除編碼方案的儲存負荷是通過將同位檢查片段數除(`m`以計算得出的）（`k`。您可以使用儲存負荷來計算每個銷毀編碼物件所需的磁碟空間：

```
disk space = object size + (object size * storage overhead)
```

例如、如果您使用4+2配置儲存10 MB物件（儲存負荷為50%）、則物件會耗用15 MB的網格儲存空間。如果您使用6+2方案儲存相同的10 MB物件（其儲存負荷高達33%）、則物件會耗用約13.3MB的空間。

選取符合您需求、總價值最低的銷毀編碼方案 `k+m`。具有較少片段的銷毀編碼方案、在運算上更有效率、因為：

- 每個物件建立和散佈（或擷取）的片段較少
- 由於片段大小較大、因此效能表現較佳
- 它們可能需要在中新增較少的節點"需要更多儲存空間時進行擴充"

儲存資源池準則

當選擇要用於建立銷毀編碼複本規則的儲存池時、請針對儲存池使用下列準則：

- 儲存資源池必須包含三個或多個站台、或只包含一個站台。

  如果儲存池包含兩個站台、則無法使用抹除編碼。

  - 包含三個以上站台之儲存資源池的銷毀編碼配置
  - 單一站台儲存資源池的銷毀編碼配置

- 請勿使用包含 All Sites 網站的儲存池。
- 儲存池至少應包含 `*k+m* +1`可儲存物件資料的儲存節點。

> 可以在安裝期間配置儲存節點以包含物件資料和元資料（「組合」儲存節點）、僅包含物件元資料或僅包含物件資料。有關詳細信息，請參閱"儲存節點類型" 。

所需的最小儲存節點數為 `k+m`。不過、如果所需的儲存節點暫時無法使用、則至少要有一個額外的儲存節點、有助於防止擷取失敗或ILM待處理項目。

包含三個以上站台之儲存資源池的銷毀編碼配置

下表說明StorageGRID 目前由支援的銷毀編碼方案、適用於包含三個以上站台的儲存資源池。所有這些方案都提供站台遺失保護。一個站台可能會遺失、而且物件仍可存取。

對於提供站台遺失保護的銷毀編碼方案、儲存池中建議的儲存節點數量超過 `*k+m* +1`、因為每個站台至少需要三個儲存節點。

銷毀編碼方案（*k+m*）	已部署站台的最小數量	每個站台的建議儲存節點數	建議的儲存節點總數	站台遺失保護？	儲存負荷
4+2.	3	3	9	是的	50%
6+2.	4	3	12	是的	33%
8+2.	5	3	15	是的	25%
6+3.	3	4	12	是的	50%
9+3.	4	4	16	是的	33%
2+1.	3	3	9	是的	50%
4+1.	5	3	15	是的	25%
6+1.	7	3	21	是的	17%
7+5.	3	5	15	是的	71%

> 每個站台至少需要三個儲存節點。StorageGRID若要使用7+5方案、每個站台至少需要四個儲存節點。建議每個站台使用五個儲存節點。

選取提供站台保護的銷毀編碼方案時、請平衡下列因素的相對重要性：

- 片段數量：當片段總數較少時、效能和擴充彈性通常會較佳。
- * 容錯能力 * ：容錯能力會增加、因為同位元區段越多（也就是當值越高時 `m`）。

- * 網路流量 * ：當從故障中恢復時、使用具有更多片段的方案（即、較高的總數） `k+m`會產生更多網路流量。
- 儲存負荷：成本較高的配置需要更多的每個物件儲存空間。

例如、在4+2方案和6+3方案（兩者都有50%的儲存負荷）之間做出決定時、如果需要額外的容錯能力、請選取6+3方案。如果網路資源受到限制、請選取4+2方案。如果所有其他因素都相同、請選取4+2、因為它的片段總數較少。

如果您不確定要使用哪種方案、請選取4+2或6+3、或聯絡技術支援部門。

單一站台儲存資源池的銷毀編碼配置

只要站台有足夠的儲存節點、單一站台儲存池即可支援針對三個以上站台所定義的所有銷毀編碼方案。

所需的儲存節點最小數量為 `k+m`、但建議使用儲存節點的儲存池 `k+m +1`。例如、2+1銷毀編碼方案需要至少三個儲存節點的儲存資源池、但建議使用四個儲存節點。

銷毀編碼方案（*k+m*）	最小儲存節點數	建議的儲存節點數	儲存負荷
4+2.	6	7	50%
6+2.	8	9	33%
8+2.	10	11	25%
6+3.	9	10	50%
9+3.	12	13	33%
2+1.	3	4	50%
4+1.	5	6	25%
6+1.	7	8	17%
7+5.	12	13	71%

StorageGRID 中抹除編碼的優點、缺點和要求

在決定是否使用複寫或銷毀編碼來保護物件資料免於遺失之前、您應該先瞭解銷毀編碼的優點、缺點及要求。

銷毀編碼的優點

相較於複寫、銷毀編碼可提升可靠性、可用度及儲存效率。

- 可靠性：以在不遺失資料的情況下可以承受的同時故障次數來衡量。

- 複製：多個相同的物件副本儲存在不同的節點和跨站點上。
- 擦除編碼：將物件編碼為資料和奇偶校驗片段，並分佈在許多節點和站點上。這種分散提供了站點和節點故障保護。

- 可用性：當儲存節點發生故障或無法存取時取得物件的能力。與複製相比，擦除編碼在相當的儲存成本下提供了更高的可用性。
- 儲存效率：在可用性和可靠性相似的情況下，擦除編碼物件比複製物件佔用更少的磁碟空間。例如，複製到兩個網站的 10 MB 物件將消耗 20 MB 磁碟空間（兩個副本），而使用 6+3 擦除編碼方案在三個網站進行擦除編碼的物件僅消耗 15 MB 磁碟空間。

> 用於銷毀編碼物件的磁碟空間會以物件大小加上儲存負荷來計算。儲存負荷百分比是指同位元檢查片段的數目除以資料片段的數目。

銷毀編碼的缺點

相較於複寫、銷毀編碼有下列缺點：

- 建議增加儲存節點和站台數量、視銷毀編碼方案而定。相反地、如果您複寫物件資料、則每個複本只需要一個儲存節點。請參閱"包含三個以上站台之儲存資源池的銷毀編碼配置"和"單一站台儲存資源池的銷毀編碼配置"。
- 增加儲存擴充的成本與複雜度。若要擴充使用複寫的部署、您可以在製作物件複本的每個位置新增儲存容量。若要擴充使用銷毀編碼的部署、您必須同時考量使用中的銷毀編碼方案、以及現有的完整儲存節點。例如、如果您等待現有節點 100% 滿、則必須至少新增儲存節點、 `k+m`但如果您在現有節點已滿 70% 時進行擴充、則可以在每個站台新增兩個節點、同時仍將可用儲存容量最大化。如需更多資訊、請參閱 "新增銷毀編碼物件的儲存容量"。
- 當您在分散各地的站台上使用銷毀編碼時、擷取延遲會增加。透過 WAN 連線擷取的物件片段、若為在遠端站台之間進行銷毀編碼和散佈的物件片段、比在本機複寫且可供使用的物件（用戶端連線的相同站台）所需的時間更長。
- 當您在地理分佈的站台上使用銷毀編碼時、會有較高的WAN網路流量使用量來進行擷取和修復、尤其是對於經常擷取的物件或透過WAN網路連線進行物件修復。
- 當您跨站點使用擦除編碼時，隨著站點間網路延遲的增加，最大物件吞吐量會急劇下降。這種下降是由於 TCP 網路吞吐量下降造成的，這影響了StorageGRID系統儲存和檢索物件片段的速度。
- 更高的運算資源使用率。

何時使用銷毀編碼

使用擦除編碼來滿足以下要求：

- 大小大於1 MB的物件。

> 銷毀編碼最適合大於1 MB的物件。請勿對小於 200 KB 的物件使用抹除編碼、以避免管理非常小的銷毀編碼片段所造成的負擔。

- 長期或冷儲存、用於不常擷取的內容。
- 高資料可用度與可靠性。
- 防止完整站台和節點故障。

- 儲存效率：
- 單一站台部署、只需一個銷毀編碼複本、而非多個複製複本、即可有效保護資料。
- 站台間延遲低於100毫秒的多站台部署。

StorageGRID 如何確定物件保留

支援網格管理員和個別租戶使用者的選項、可指定儲存物件的時間長度。StorageGRID一般而言、租戶使用者所提供的任何保留指示、均優先於網格管理員所提供的保留指示。

租戶使用者如何控制物件保留

租戶使用者可以使用這些方法來控制物件在 StorageGRID 中的儲存時間：

- 如果網格已啟用全域 S3 物件鎖定設定、 S3 租戶使用者可以建立啟用 S3 物件鎖定的儲存格、然後為每個儲存格選取 * 預設保留期間 * 。
- 如果已啟用網格的全域S3物件鎖定設定、S3租戶使用者就能建立啟用S3物件鎖定的儲存區、然後使用S3 REST API來指定新增至該儲存區之每個物件版本的保留直到日期和合法保留設定。
  - 合法持有的物件版本無法由任何方法刪除。
  - 在物件版本達到保留截止日期之前、任何方法都無法刪除該版本。
  - 啟用 S3 物件鎖定的貯體中物件會由 ILM 「永遠」保留。不過、在達到保留截止日期之後、用戶端要求或儲存庫生命週期到期時、即可刪除物件版本。請參閱。 "使用S3物件鎖定來管理物件"
- S3租戶使用者可將生命週期組態新增至其指定到期行動的儲存區。如果儲存區生命週期存在、StorageGRID除非用戶端先刪除物件、否則在到期行動中指定的日期或天數之前、將會儲存物件。請參閱。 "建立S3生命週期組態"
- S3 用戶端可以發出刪除物件要求。確定要刪除或保留物件時、往往會優先處理S3儲存區生命週期或ILM上的用戶端刪除要求。StorageGRID

網格管理員如何控制物件保留

網格管理員可以使用下列方法來控制物件保留：

- 為每個租戶設定 S3 物件鎖定最長保留期間。然後、租戶使用者可以為每個貯體設定預設保留期間。對於該貯體（物件的保留至日期）的任何新擷取物件、也會強制執行最大保留期間。
- 建立 ILM 放置指示、以控制物件的儲存時間。當物件與ILM規則相符時、StorageGRID 直到ILM規則的最後一段時間結束為止、才會將這些物件儲存起來。如果為放置指示指定「永遠」、則物件會無限期保留。
- 無論物件保留的時間長短由誰控制、 ILM 設定都會控制儲存的物件複本類型（複寫或銷毀編碼）、以及複本的位置（儲存節點或雲端儲存池）。

S3儲存區生命週期與ILM之間的互動方式

當 S3 貯體生命週期設定完成時、生命週期到期動作會覆寫符合生命週期篩選器之物件的 ILM 原則。因此、即使放置物件的任何ILM指示失效、物件仍可能保留在網格上。

物件保留範例

若要更深入瞭解S3物件鎖定、儲存區生命週期設定、用戶端刪除要求和ILM之間的互動、請考慮下列範例。

範例**1**：**S3**儲存區生命週期可延長物件的壽命、而非**ILM**

ILM

儲存兩份複本一年（365天）

生命週期

物件在2年內過期（730天）

結果

將物件儲存730天。StorageGRID使用儲存區生命週期設定來決定是否要刪除或保留物件。StorageGRID

> 如果儲存區生命週期指定物件的保留時間應超過ILM指定的時間、StorageGRID 則當判斷要儲存的複本數量和類型時、NetApp會繼續使用ILM放置指示。在此範例中、物件的兩份複本將繼續儲存在StorageGRID 從第3666天到730天的地方。

範例**2**：**S3**儲存區生命週期會在**ILM**之前過期物件

ILM

儲存兩份複本2年（730天）

生命週期

物件在1年內到期（365天）

結果

支援在365天之後刪除物件的兩個複本。StorageGRID

範例**3**：用戶端刪除會覆寫儲存區生命週期和**ILM**

ILM

在儲存節點上「永遠」儲存兩份複本

生命週期

物件在2年內過期（730天）

用戶端刪除要求

於第400天發行

結果

針對用戶端刪除要求、在第400天刪除物件的兩個複本。StorageGRID

範例**4**：**S3**物件鎖定會覆寫用戶端刪除要求

S3物件鎖定

物件版本的保留截止日期為2026-03-31。合法持有並未生效。

符合**ILM**規則

在儲存節點上「永遠」儲存兩份複本

用戶端刪除要求

於 2024-03-31 發佈

結果

由於保留截止日期仍在2年前、所以無法刪除物件版本。StorageGRID

StorageGRID 如何刪除物件

由於S3儲存區生命週期到期或ILM原則要求到期、因此可直接回應用戶端要求或自動刪除物件。StorageGRID瞭解可刪除物件的不同方式、StorageGRID 以及如何處理刪除要求、有助於您更有效地管理物件。

使用下列兩種方法之一刪除物件：StorageGRID

- 同步刪除：StorageGRID 當物件接收到用戶端刪除要求時、會立即移除所有物件複本。用戶端會被告知刪除作業在複本移除之後成功。
- 物件會排入刪除佇列：StorageGRID 當收到刪除要求時、物件會排入刪除佇列、並立即通知用戶端刪除作業已成功。物件複本稍後會透過背景ILM處理移除。

刪除物件時StorageGRID 、利用最佳化刪除效能、最小化可能刪除的待處理項目、以及最快釋出空間的方法、來刪除物件。

下表摘要說明StorageGRID 各個方法的使用時機。

執行刪除的方法	使用時
物件會排入佇列以供刪除	當下列*任一*條件為真時： • 自動物件刪除已由下列其中一個事件觸發： ◦ S3儲存區生命週期組態的到期日或天數已達。 ◦ ILM規則中指定的最後一個時間週期已過。 • 附註： * 如果儲存庫中的物件已啟用 S3 物件鎖定功能、或是已指定保留日期但尚未符合、則無法刪除該物件。 • S3 用戶端要求刪除、下列一項或多項條件成立： ◦ 無法在 30 秒內刪除複本、例如物件位置暫時無法使用。 ◦ 背景刪除佇列閒置。
立即移除物件（同步刪除）	當 S3 用戶端提出刪除要求且符合下列 * 全部 * 條件時： • 所有複本均可在30秒內移除。 • 背景刪除佇列包含要處理的物件。

當 S3 用戶端提出刪除要求時、 StorageGRID 會先將物件新增至刪除佇列。然後切換至執行同步刪除。確保後臺刪除佇列有要處理的物件、StorageGRID 讓處理器能夠更有效率地處理刪除作業、特別是對於低並行用戶端、同時防止用戶端刪除待處理記錄。

刪除物件所需的時間

物件的刪除方式StorageGRID 可能會影響系統的執行方式：

- 執行同步刪除時、最多需要30秒才能將結果傳回給用戶端。StorageGRID StorageGRID這表示刪除的速度似乎較慢、即使複本實際移除速度比StorageGRID 將物件排入佇列以供刪除時更快。
- 如果您在大量刪除期間密切監控刪除效能、可能會注意到刪除某些物件之後、刪除率似乎會變慢。當從佇列物件移至執行同步刪除時、就會發生此變更StorageGRID 。刪除率明顯降低、並不代表物件複本移除速度較慢。相反地、這表示平均而言、空間現在可以更快釋出。

如果您要刪除大量物件、而且優先要快速釋放空間、請考慮使用用戶端要求來刪除物件、而非使用ILM或其他方法來刪除物件。一般而言、當用戶端執行刪除作業時、空間會更快釋出、因為StorageGRID 使用同步刪除功能時、會有更多空間。

刪除物件之後、可用空間所需的時間取決於下列幾個因素：

- 物件複本是同步移除、還是排入佇列稍後移除（適用於用戶端刪除要求）。
- 其他因素、例如當物件複本排入移除佇列時、網格中的物件數目或網格資源的可用度（適用於用戶端刪除和其他方法）。

如何刪除**S3**版本控制物件

啟用S3儲存區的版本管理時、StorageGRID 無論是來自S3用戶端、S3儲存區生命週期到期、或ILM原則需求、均會遵循Amazon S3回應刪除要求的行為。

物件版本化時、物件刪除要求不會刪除物件的目前版本、也不會釋放空間。相反地、物件刪除要求會建立零位元組刪除標記、做為物件的目前版本、使物件的舊版「非目前」。當物件刪除標記是目前版本且沒有非目前版本時、它會變成過期的物件刪除標記。

即使物件尚未移除、StorageGRID 但功能上的功能仍然如同物件的目前版本已無法使用。對該物件的要求會傳回404 NotFound.但是、由於非目前物件資料尚未移除、因此指定物件非目前版本的要求可能會成功。

如果客戶端從"分支桶"， StorageGRID隱藏了物件版本的存在，但不會在分支儲存桶中建立刪除標記。如果用戶端從分支儲存桶中刪除沒有版本 ID 的對象， StorageGRID會根據標準 S3 行為在分支儲存桶中建立刪除標記。

若要在刪除版本化物件時釋放空間、或移除刪除標記、請使用下列其中一項：

- *S3 用戶端要求 * ：在 S3 刪除物件要求中指定物件版本 ID (`DELETE /object?versionId=ID`) 。請記住、此要求只會移除指定版本的物件複本（其他版本仍佔用空間）。
- * 貯體生命週期 * ：使用 `NoncurrentVersionExpiration`貯體生命週期組態中的動作。當符合指定的NoncurrentDays數量時、StorageGRID 不同時更新的物件版本會永久移除所有複本。這些物件版本無法還原。

  `NewerNoncurrentVersions`貯體生命週期組態中的動作會指定保留在版本化 `S3` 儲存區中的非目前版本數。如果有比指定的非目前版本更多 `NewerNoncurrentVersions`、`StorageGRID` 會在 `NoncurrentDays` 值過期時移除舊版本。`NewerNoncurrentVersions`臨界值會覆寫 `ILM` 所提供的生命週期規則、表示如果 `ILM` 要求刪除、則會保留臨界值內有版本的非目前物件 `NewerNoncurrentVersions`。

若要移除過期的物件刪除標記、請使用 `Expiration`具有下列標記之一的動作：`ExpiredObjectDeleteMarker`、 `Days`或 `Date`。

- * ILM * ："複製作用中原則"並新增兩個 ILM 規則至新原則：
  - 第一條規則：使用「非目前時間」做為參考時間、以符合物件的非目前版本。在"建立 ILM 規則精靈的步驟 1 （輸入詳細資料）"中、針對「僅將此規則套用至舊版物件版本（在啟用版本設定的 S3 儲存區中）？」問題選取 * 是 * 。
  - 第二條規則：使用 * 擷取時間 * 來符合目前版本。「非目前時間」規則必須出現在 * 擷取時間 * 規則上方的原則中。

    若要移除過期的物件刪除標記、請使用 * 擷取時間 * 規則來符合目前的刪除標記。刪除標記只有在 * 天 * 的 * 期間 * 已經過去、且目前的刪除製作者已過期（沒有非目前版本）時才會移除。
- * 刪除貯體中的物件 * ：使用租戶管理員"刪除所有物件版本"從貯體中刪除標記。

刪除版本化物件時、 StorageGRID 會建立零位元組刪除標記、做為物件的目前版本。必須先移除所有物件和刪除標記、才能刪除版本化的儲存庫。

- 刪除在 StorageGRID 11.7 或更早版本中建立的標記只能透過 S3 用戶端要求移除、但不能由 ILM 、貯體生命週期規則或刪除貯體作業中的物件移除。
- 從在 StorageGRID 11.8 或更新版本中建立的貯體中刪除標記、可由 ILM 、貯體生命週期規則、貯體作業中的刪除物件、或明確刪除 S3 用戶端。

相關資訊

- "使用S3 REST API"
- "範例4：S3版本化物件的ILM規則和原則"

在 StorageGRID 中建立並指派儲存等級

儲存等級可識別儲存節點所使用的儲存類型。如果您希望 ILM 規則將特定物件放置在特定的儲存節點上、則可以建立儲存等級。

開始之前

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

關於這項工作

首次安裝 StorageGRID 時、系統會自動將 * 預設 * 儲存等級指派給系統中的每個儲存節點。視需要、您可以選擇性地定義自訂儲存等級、並將其指派給不同的儲存節點。

使用自訂儲存等級可讓您建立僅包含特定類型儲存節點的 ILM 儲存資源池。例如、您可能想要將某些物件儲存在最快的儲存節點上、例如StorageGRID ：整合式All Flash儲存設備。

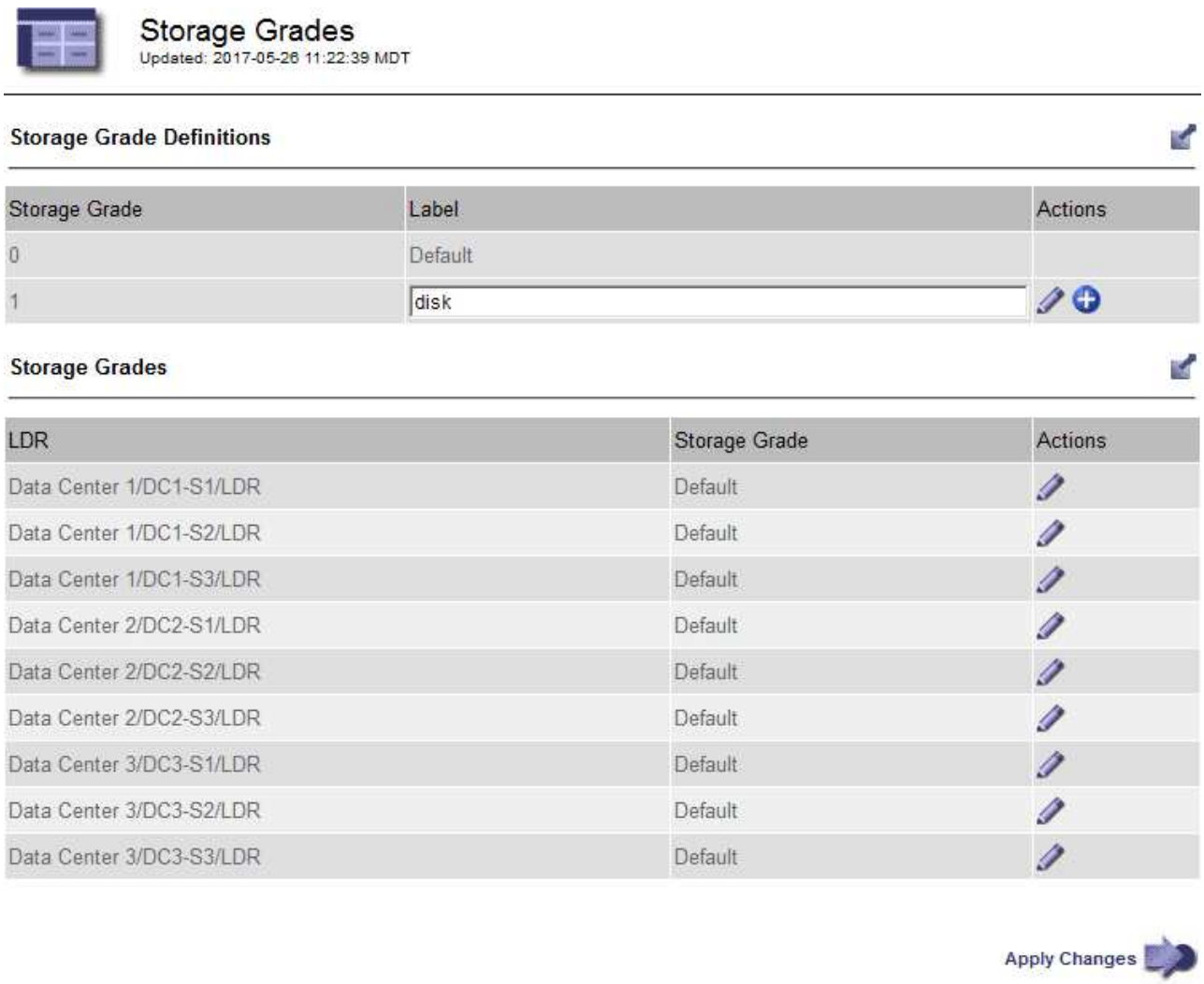
僅元資料儲存節點不能分配儲存等級。有關詳細信息，請參閱"儲存節點類型" 。

如果儲存等級不是問題（例如、所有儲存節點都相同）、您可以略過此程序、並在您選擇儲存等級時、使用 * 包括所有儲存等級 * 選項"建立儲存資源池"。使用此選項可確保儲存池將包含站台上的每個儲存節點、無論其儲存等級為何。

請勿創造超過必要的儲存等級。例如、請勿為每個儲存節點建立儲存等級。而是將每個儲存等級指派給兩個以上的節點。如果只指派給一個節點的儲存等級無法使用、可能會導致ILM待處理記錄。

步驟

1. 選擇* ILM > Storage等級*。
2. 定義自訂儲存等級：
   a. 對於要新增的每個自訂儲存等級，請選擇 **Insert** 以新增一行。
   b. 輸入描述性標籤。

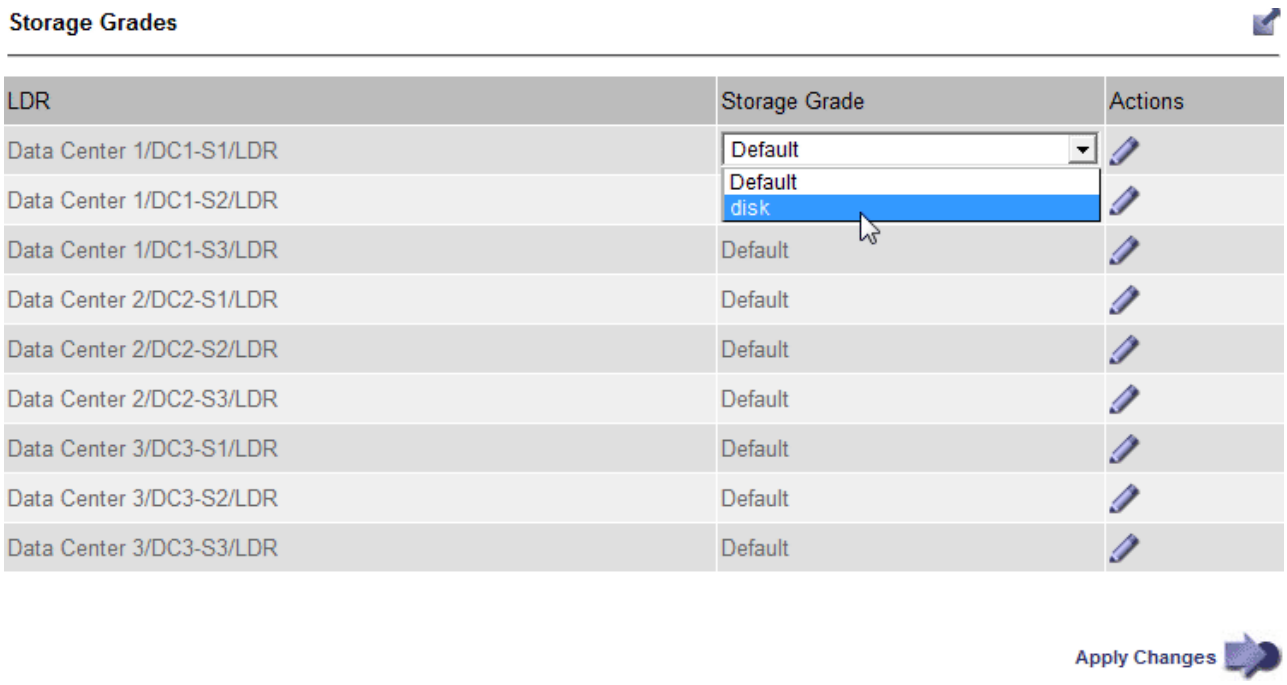


   c. 選取*套用變更*。
   d. 如果需要修改已儲存的標籤，請選擇「編輯」 並選擇「套用變更」。

   您無法刪除儲存成績。

3. 將新的儲存等級指派給儲存節點：
   a. 在 LDR 清單中找到儲存節點，然後選擇其 **Edit** 圖示 。

b. 從清單中選取適當的儲存等級。



只能將儲存等級指派給指定的儲存節點一次。從故障中恢復的儲存節點會維持先前指派的儲存等級。請勿在 ILM 原則啟動後變更此指派。如果指派變更、資料會根據新的儲存等級儲存。

a. 選取*套用變更*。

使用儲存池

了解 StorageGRID 中的儲存資源池

儲存池是儲存節點的邏輯群組。

當您安裝 StorageGRID 時、每個站台會自動建立一個儲存池。您可以視需要針對儲存需求設定其他儲存資源池。

可以在安裝期間配置儲存節點以包含物件資料和元資料（「組合」儲存節點）、僅包含物件元資料或僅包含物件資料。僅元資料儲存節點不能在儲存池中使用。有關詳細信息，請參閱"儲存節點類型" 。

儲存資源池有兩個屬性：

- 儲存等級：儲存節點的相對效能、是備用儲存設備的相對效能。
- 站點：儲存物件的資料中心。

儲存資源池用於 ILM 規則中、以判斷物件資料的儲存位置和使用的儲存類型。當您設定用於複寫的 ILM 規則時、請選取一或多個儲存集區。

StorageGRID 中的儲存資源池組態準則

設定並使用儲存資源池、透過在多個站台之間散佈資料來防止資料遺失。複寫複本和銷毀編碼複本需要不同的儲存池組態。

請參閱 "使用複寫和銷毀編碼來啟用站台遺失保護的範例"。

所有儲存資源池的準則

- 盡量簡化儲存資源池組態。請勿建立超過必要數量的儲存資源池。
- 建立盡可能多節點的儲存資源池。每個儲存資源池應包含兩個以上的節點。如果節點無法使用、節點不足的儲存資源池可能會導致ILM待處理記錄。
- 避免建立或使用重疊的儲存資源池（包含一或多個相同節點）。如果儲存資源池重疊、可能會在同一個節點上儲存多個物件資料複本。
- 一般而言、請勿使用「所有儲存節點」儲存池（ StorageGRID 11.6 以上版本）或「所有站台」網站。這些項目會自動更新、以納入您在擴充中新增的任何新網站、這可能不是您想要的行為。

複寫複本所使用的儲存資源池準則

- 對於使用的站台遺失保護"複寫"，請在中指定一或多個站台專屬"每個 ILM 規則的放置指示"的儲存集區。

  在 StorageGRID 安裝期間、會為每個站台自動建立一個儲存池。

  針對每個站台使用儲存資源池、可確保複寫的物件複本完全符合您的期望（例如、每個站台的每個物件都有一個複本、以保護站台損失）。

- 如果您在擴充中新增站台、請建立只包含新站台的新儲存池。然後、"更新 ILM 規則"控制要儲存在新網站上的物件。
- 如果複本數小於儲存集區的數量、系統就會散佈複本、以平衡集區之間的磁碟使用量。
- 如果儲存資源池重疊（包含相同的儲存節點）、則物件的所有複本可能只會儲存在一個站台。您必須確保所選的儲存資源池不包含相同的儲存節點。

用於銷毀編碼複本的儲存資源池準則

- 若要使用"銷毀編碼"進行站台遺失保護、請建立至少包含三個站台的儲存資源池。如果儲存池只包含兩個站台、您就無法使用該儲存池進行銷毀編碼。對於有兩個站台的儲存資源池、沒有可用的銷毀編碼方案。
- 儲存資源池中包含的儲存節點和站台數目、決定哪些"銷毀編碼配置"可用。
- 如果可能、儲存資源池應包含超過您所選銷毀編碼方案所需的最小儲存節點數。例如、如果您使用6+3銷毀編碼方案、則至少必須有九個儲存節點。不過、建議每個站台至少有一個額外的儲存節點。
- 將儲存節點分散至各個站台、盡量平均。例如、若要支援6+3銷毀編碼方案、請在三個站台設定至少包含三個儲存節點的儲存資源池。
- 如果您的處理量需求很高、如果站台之間的網路延遲超過 100 毫秒、則不建議使用包含多個站台的儲存池。隨著延遲時間增加、StorageGRID 由於TCP網路處理量減少、導致導致導致無法建立、放置及擷取物件片段的速度大幅降低。

  處理量的下降會影響物件擷取和檢索的最大可達速率（當選擇 Balanced 或 Strict 作為擷取行為時），或可能導致 ILM 佇列積壓（當選擇 Dual commit 作為擷取行為時）。請參閱"ILM 規則擷取行為"。

如果您的網格僅包含一個站台、您將無法在銷毀編碼設定檔中使用所有儲存節點儲存池（ StorageGRID 11.6 以上版本）或所有站台。此行為可防止在新增第二個站台時、設定檔變成無效。

StorageGRID 中使用儲存池的站台遺失保護

如果您的 StorageGRID 部署包含多個站台、您可以使用複寫和銷毀編碼搭配適當設定的儲存集區、以啟用站台遺失保護。

複寫和銷毀編碼需要不同的儲存池組態：

- 若要使用複寫來保護站台遺失、請使用在 StorageGRID 安裝期間自動建立的站台專屬儲存集區。然後建立 ILM 規則、以"放置指示"指定多個儲存資源池、以便在每個站台上放置每個物件的一個複本。
- 若要使用抹除編碼來保護站台遺失"建立由多個站台組成的儲存資源池"、請參閱。然後建立 ILM 規則、使用一個由多個站台和任何可用的銷毀編碼架構所組成的儲存資源池。

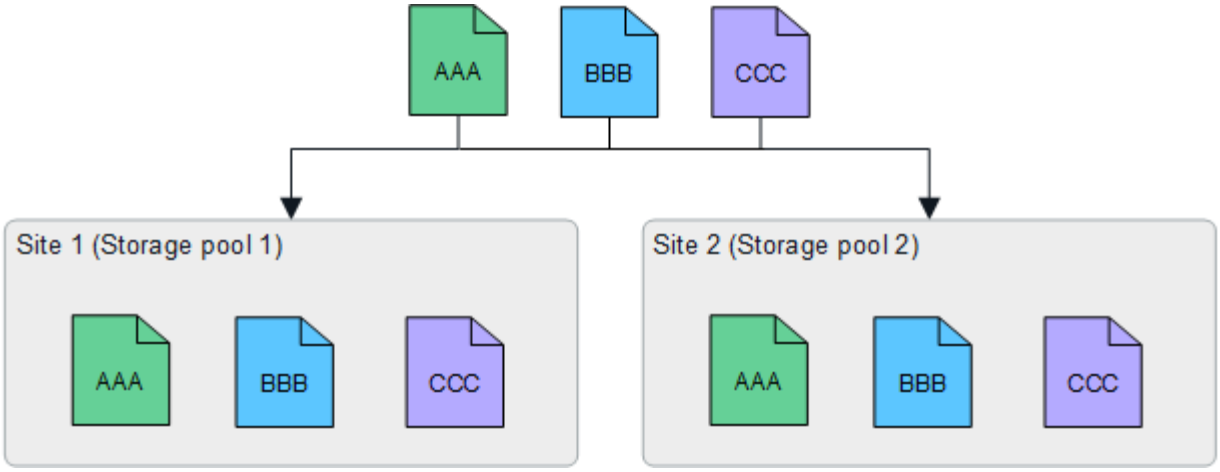
在配置StorageGRID部署以進行站點遺失保護時，也必須考慮以下因素的影響"擷取選項"和"一致性"。

複寫範例

根據預設、 StorageGRID 安裝期間會為每個站台建立一個儲存池。只有一個站台組成儲存集區、您就能設定使用複寫來保護站台遺失的 ILM 規則。在此範例中：

- 儲存池 1 包含站台 1
- 儲存池 2 包含站台 2
- ILM 規則包含兩個放置位置：
  - 在站台 1 複寫 1 個複本、以儲存物件
  - 在站台 2 複寫 1 個複本來儲存物件

ILM 規則放置位置：



如果某個站台遺失、則可在另一個站台取得物件複本。

銷毀編碼範例

每個儲存資源池包含多個站台、可讓您設定 ILM 規則、使用銷毀編碼來保護站台遺失。在此範例中：

- 儲存池 1 包含站台 1 至 3
- ILM 規則包含一個放置位置：在儲存池 1 使用 4+2 EC 配置（包含三個站台）以銷毀編碼來儲存物件

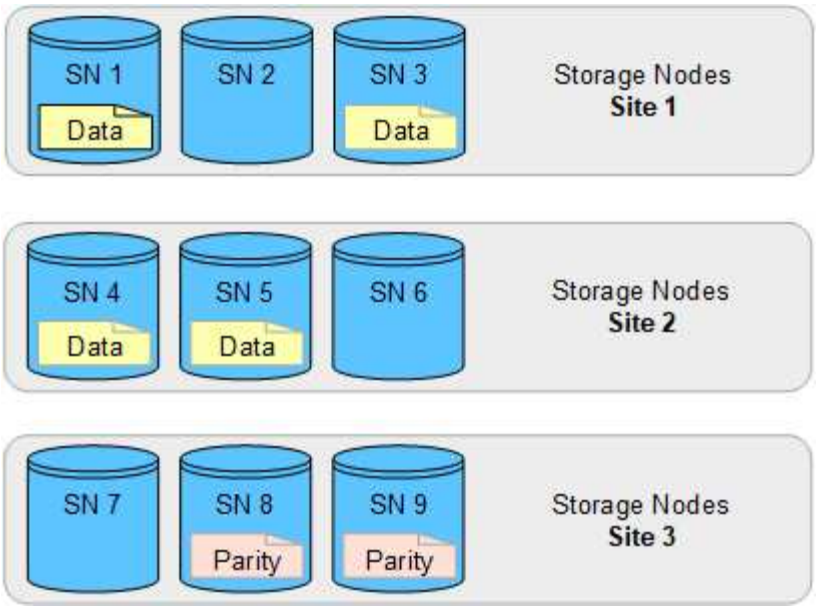
ILM 規則放置位置：

在此範例中：

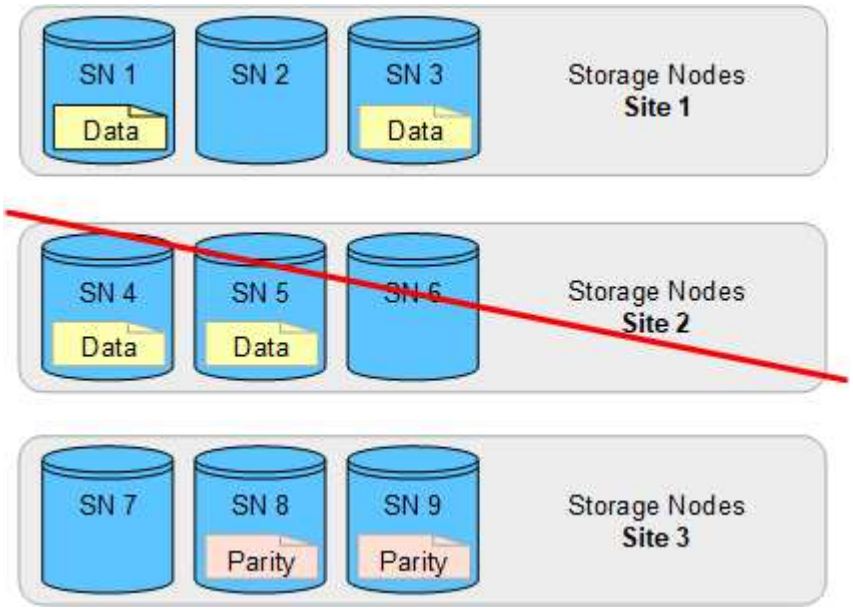
- ILM 規則使用 4+2 銷毀編碼方案。
- 每個物件會分割成四個等量資料片段、並從物件資料計算兩個同位元檢查片段。
- 這六個片段中的每個片段都儲存在三個資料中心站台的不同節點上、以針對節點故障或站台遺失提供資料保護。

> 在包含任意數量站台的儲存集區中、除了兩個站台之外、也允許進行銷毀編碼。

使用 4+2 銷毀編碼方案的 ILM 規則：



如果某個站台遺失、資料仍可恢復：



在 **StorageGRID** 中建立儲存資源池

您可以建立儲存資源池、以判斷StorageGRID 哪些地方會儲存物件資料、以及使用的儲存類型。每個儲存資源池都包含一個或多個站台、以及一個或多個儲存等級。

> ⓘ 在新網格上安裝 StorageGRID 12.0 或更高版本時，系統會自動為每個站台建立儲存資源池。但是，如果您最初安裝的是 StorageGRID 11.6 或更早版本，則不會自動為每個站台建立儲存資源池。

如果您想要建立雲端儲存資源池、將物件資料儲存在 StorageGRID 系統之外"使用雲端儲存資源池的相關資訊"、請參閱。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱建立儲存資源池的準則。

關於這項工作

儲存資源池會決定物件資料的儲存位置。您需要的儲存資源池數量取決於網格中的站台數量、以及您想要的複本類型：複寫或銷毀編碼。

- 如需複寫及單一站台銷毀編碼、請為每個站台建立儲存資源池。例如、如果您想要將複寫的物件複本儲存在三個站台、請建立三個儲存集區。
- 若要在三個以上站台進行銷毀編碼、請建立一個儲存資源池、其中包含每個站台的項目。例如、如果您想要在三個站台之間銷毀程式碼物件、請建立一個儲存資源池。

> 請勿將 All Sites 網站納入儲存池中、以用於銷毀編碼設定檔。相反地、請為儲存銷毀編碼資料的每個站台、在儲存池中新增個別項目。如需範例、請參閱此步驟。

- 如果您有多個儲存等級、請勿在單一站台建立包含不同儲存等級的儲存池。請參閱"建立儲存資源池的準則"。

步驟

1. 選擇* ILM > Storage Pools*。

   Storage Pools （儲存池）標籤會列出所有已定義的儲存池。

   > 對於 StorageGRID 11.6 或更早版本的新安裝、每當您新增資料中心站台時、所有儲存節點儲存池都會自動更新。請勿在 ILM 規則中使用此集區。

2. 若要建立新的儲存資源池、請選取*「Create」（建立）*。
3. 輸入儲存資源池的唯一名稱。使用可在您設定銷毀編碼設定檔和 ILM 規則時輕鬆識別的名稱。
4. 從*站台*下拉式清單中、選取此儲存資源池的站台。

   當您選取站台時、表格中的儲存節點數量會自動更新。

   一般而言、請勿在任何儲存池中使用「所有站台」網站。使用「所有站台」儲存資源池的ILM規則會將物件放置在任何可用的站台上、讓您較少控制物件放置。此外、「所有站台」儲存資源池會立即使用新站台的儲存節點、這可能不是您所期望的行為。

5. 從 * 儲存等級 * 下拉式清單中、選取 ILM 規則使用此儲存池時要使用的儲存類型。

   儲存等級（ _ 包括所有儲存等級 _ ）包括所選站台上的所有儲存節點。如果您為網格中的儲存節點建立額外的儲存等級、則會在下拉式清單中列出這些等級。

6. 如果您想要在多站台抹除編碼設定檔中使用儲存池、請選取 * 新增更多節點 * 、將每個站台的項目新增至儲存池。

   > 如果您為網站新增多個具有不同儲存等級的項目、則會發出警告。

   若要刪除條目，請選擇刪除圖示 ✕。

7. 當您對所選項目感到滿意時、請選取*「Save（儲存）」*。

   新的儲存資源池即會新增至清單中。

在 StorageGRID 中檢視儲存資源池詳細資料

您可以檢視儲存資源池的詳細資料、以判斷儲存資源池的使用位置、並查看其中包含哪些節點和儲存等級。

開始之前

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

步驟

1. 選擇* ILM > Storage Pools*。

   「儲存資源池」表包含每個儲存資源池的下列資訊、其中包括儲存節點：

   - 名稱：儲存資源池的唯一顯示名稱。
   - * 節點數 * ：儲存池中的節點數。
   - * 儲存使用量 * ：用於此節點上物件資料的總可用空間百分比。此值不包含物件中繼資料。
   - * 總容量 * ：儲存池的大小、等於儲存池中所有節點的物件資料可用空間總量。
   - * ILM 使用率 * ：儲存資源池目前的使用方式。儲存資源池可能未使用、或可能用於一或多個 ILM 規則、銷毀編碼設定檔、或兩者。

2. 若要檢視特定儲存池的詳細資料、請選取其名稱。

   儲存池的詳細資料頁面隨即出現。

3. 檢視 * 節點 * 索引標籤、瞭解儲存池中包含的儲存節點。

   下表包含每個節點的下列資訊：

   - 節點名稱
   - 站台名稱
   - 儲存等級
   - 儲存使用量：已用於儲存節點之物件資料的可用空間總計百分比。

   > 每個儲存節點的「已使用儲存 - 物件資料」圖表中也顯示相同的儲存使用情況（%）值（選擇「節點」>「儲存節點」>「儲存」）。

4. 檢視 * ILM 使用率 * 索引標籤、判斷儲存資源池目前是否正在任何 ILM 規則或銷毀編碼設定檔中使用。
5. 您也可以移至 * ILM 規則頁面 * 、瞭解並管理使用儲存資源池的任何規則。

   請參閱"使用 ILM 規則的指示"。

在 StorageGRID 中編輯儲存資源池

您可以編輯儲存資源池以變更其名稱、或更新站台和儲存等級。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱"建立儲存資源池的準則"。
- 如果您打算編輯使用中ILM原則中某個規則所使用的儲存資源池、則您已考慮變更如何影響物件資料放置。

關於這項工作

如果您要將新站台或儲存等級新增至使用中 ILM 原則的儲存池、請注意、新站台或儲存等級中的儲存節點不會自動使用。若要強制 StorageGRID 使用新的站台或儲存等級、您必須在儲存編輯過的儲存集區之後啟動新的 ILM 原則。

步驟

1. 選擇* ILM > Storage Pools*。
2. 選取您要編輯之儲存池的核取方塊。

   您無法編輯所有儲存節點儲存池（ StorageGRID 11.6 及更早版本）。

3. 選擇*編輯*。
4. 視需要變更儲存資源池名稱。
5. 視需要選取其他站台和儲存等級。

   如果儲存池用於銷毀編碼設定檔、則您無法變更站台或儲存等級、而變更將導致銷毀編碼配置無效。例如、如果在銷毀編碼設定檔中使用的儲存池目前僅包含一個站台的儲存等級、則您無法在兩個站台中使用儲存等級、因為變更會使銷毀編碼配置無效。

   > 從現有儲存池新增或移除站台不會移動任何現有的銷毀編碼資料。如果您想要從站台移動現有資料、您必須建立新的儲存池和 EC 設定檔、才能重新編碼資料。

6. 選擇*保存*。

完成後

如果您在使用中的 ILM 原則所使用的儲存資源池中新增了新的站台或儲存設備等級，請啟動新的 ILM 原則，強制 StorageGRID 使用新的站台或儲存設備等級。例如，Clone 現有的 ILM 原則，然後啟動該 Clone。請參閱 "使用ILM規則和ILM原則"。

移除 StorageGRID 中的儲存資源池

您可以移除未使用的儲存資源池。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。

步驟

1. 選擇* ILM **>** Storage Pools*。
2. 請查看表格中的 ILM 使用率欄、判斷您是否可以移除儲存池。

   如果儲存池正用於 ILM 規則或銷毀編碼設定檔、則無法移除該儲存池。根據需要，選擇 ***storage Pool name*** > **ILM usage** 以確定儲存池的使用位置。

3. 如果您要移除的儲存池未被使用、請選取核取方塊。
4. 選擇*移除*。
5. 選擇*確定*。

使用雲端儲存資源池

了解 **StorageGRID** 中的雲端儲存資源池

雲端儲存資源池可讓您使用 ILM 將物件資料移轉到 StorageGRID 系統之外。例如，您可能想要將不常存取的物件移轉到成本更低的雲端儲存設備，例如 Amazon S3 Glacier、S3 Glacier Deep Archive、Google Cloud 或 Microsoft Azure Blob Storage 中的封存存取層。或者，您可能想要維護 StorageGRID 物件的雲端備份，以增強災難恢復能力。

從 ILM 的角度來看，雲端儲存資源池與儲存資源池類似。若要將物件儲存在任一位置，您需要在建立 ILM 規則的放置指令時選擇對應的資源池。但是，儲存資源池由 StorageGRID 系統內的儲存節點組成，而雲端儲存資源池則由外部儲存桶（S3）或 Container（Azure Blob Storage）組成。

下表將儲存資源池與雲端儲存資源池進行比較、並顯示高層級的相似點和差異。

	儲存資源池	雲端儲存資源池
如何建立？	使用Grid Manager中的* ILM **>** Storage Pools*選項。	在 Grid Manager 中使用 **ILM** > * 儲存池 * > * 雲端儲存池 * 選項。 您必須先設定外部儲存區或容器、才能建立雲端儲存資源池。
您可以建立多少集區？	無限。	最多10個。

	儲存資源池	雲端儲存資源池
物件儲存在何處？	在 StorageGRID 中的一個或多個儲存節點上。	在 Amazon S3 儲存桶、Azure Blob Storage Container 或 StorageGRID 系統外部的 Google Cloud 中。 如果雲端儲存資源池是Amazon S3儲存區： • 您可以選擇性地設定儲存區生命週期、將物件移轉至低成本的長期儲存設備、例如Amazon S3 Glacier或S3 Glacier Deep Archive。外部儲存系統必須支援 Glacier 儲存類別和 S3 RestoreObject API 。 • 您可以建立雲端儲存資源池、以搭配支援AWS Secret Region的AWS商業雲端服務（C2S）使用。 如果雲端儲存資源池是 Azure Blob Storage Container ，StorageGRID 會將物件轉換到封存分層。 附註： 一般而言，請勿為用於雲端儲存資源池的 Container 設定 Azure Blob Storage 生命週期管理。RestoreObject 對雲端儲存資源池中物件的操作可能會受到已設定生命週期的影響。
什麼控制物件放置？	使用中 ILM 原則中的 ILM 規則。	使用中 ILM 原則中的 ILM 規則。
使用哪種資料保護方法？	複寫或銷毀編碼。	複寫：
每個物件允許多少份複本？	多重：	一份複本放在Cloud Storage Pool中、另有一或多份StorageGRID 複本可選擇放在 • 注意： * 您無法在任何指定時間將物件儲存在多個雲端儲存池中。
有哪些優點？	物件隨時都能快速存取。	低成本儲存。 • 注意 * ： FabricPool 資料無法階層化至雲端儲存資源池。

StorageGRID 中雲端儲存資源池物件的生命週期

在實作雲端儲存資源池之前、請先檢閱儲存在每種類型雲端儲存資源池中的物件生命週期。

S3：**Cloud Storage Pool**物件的生命週期

這些步驟說明儲存在 S3 Cloud Storage Pool 中物件的生命週期階段。

「 Glacier 」是指 Glacier 儲存等級和 Glacier Deep Archive 儲存等級、但有一個例外： Glacier Deep Archive 儲存等級不支援加速還原層。僅支援大量或標準擷取。

Google Cloud Platform（GCP）可支援從長期儲存設備擷取物件、而不需執行還原後作業。

1. *物件儲存在StorageGRID S編*中

   若要開始生命週期、用戶端應用程式會將物件儲存在StorageGRID

2. 物件移至**S3**雲端儲存池

   - 如果物件與使用S3 Cloud Storage Pool做為放置位置的ILM規則相符、StorageGRID 則會將物件移至Cloud Storage Pool指定的外部S3儲存區。
   - 當物件移至 S3 雲端儲存池時、用戶端應用程式可以使用 StorageGRID 的 S3 GetObject 要求來擷取它、除非物件已轉換至 Glacier 儲存設備。

3. 物件移轉至**Glacier**（無法擷取的狀態）

   - 也可以將物件移轉至Glacier儲存設備。例如、外部S3儲存區可能會使用生命週期組態、立即或在數天後將物件移轉至Glacier儲存設備。

     如果您想要轉換物件、則必須為外部 S3 儲存區建立生命週期組態、而且必須使用可實作 Glacier 儲存類別並支援 S3 RestoreObject API 的儲存解決方案。

   - 在轉換期間、用戶端應用程式可以使用 S3 HeadObject 要求來監控物件的狀態。

4. 從**Glacier**儲存設備還原物件

   如果物件已移轉至 Glacier 儲存設備、用戶端應用程式可以發出 S3 RestoreObject 要求、將可擷取的複本還原至 S3 Cloud Storage Pool 。此要求會指定在雲端儲存資源池和資料存取層中可供複本使用的天數、以供還原作業使用（加速、標準或大量）。當達到可擷取複本的到期日時、複本會自動返回無法擷取的狀態。

   如果 StorageGRID 內的儲存節點上也有一個或多個物件複本、則無需透過發出 RestoreObject 要求、從 Glacier 還原物件。而是可以使用 GetObject 要求直接擷取本機複本。

5. 物件已擷取

   物件還原之後、用戶端應用程式就可以發出 GetObject 要求來擷取還原的物件。

Azure：Cloud Storage Pool物件的生命週期

這些步驟說明儲存在 Azure Cloud Storage Pool 中物件的生命週期階段。

1. *物件儲存在StorageGRID S編*中

   若要開始生命週期、用戶端應用程式會將物件儲存在StorageGRID

2. 物件移至**Azure Cloud Storage Pool**

   當物件與使用 Azure Cloud Storage Pool 作為其放置位置的 ILM 規則相符時，StorageGRID 會將物件移至 Cloud Storage Pool 指定的外部 Azure Blob 儲存 Container。

3. 物件移轉至歸檔層（無法擷取的狀態）

將物件移至 Azure Cloud Storage Pool 後，StorageGRID 會自動將物件轉換至 Azure Blob Storage Archive 分層。

4. 物件從歸檔層還原

   如果物件已移轉至歸檔層、用戶端應用程式就可以發出 S3 RestoreObject 要求、將可擷取的複本還原至 Azure Cloud Storage Pool 。

   當 StorageGRID 收到 RestoreObject 請求時，它會將物件暫時轉換到 Azure Blob 儲存體的冷分層。一旦 RestoreObject 請求中的過期日期到達，StorageGRID 就會將物件轉換回封存分層。

   > ⓘ 如果 StorageGRID 內的儲存節點上也存在物件的一或多個複本、則無需透過發出 RestoreObject 要求、從歸檔存取層還原物件。而是可以使用 GetObject 要求直接擷取本機複本。

5. 物件已擷取

   將物件還原至 Azure Cloud Storage Pool 之後、用戶端應用程式就可以發出 GetObject 要求來擷取還原的物件。

相關資訊

"使用S3 REST API"

StorageGRID 中的 Cloud Storage Pool 使用案例

您可以使用 Cloud Storage Pool 將資料備份或分層至外部位置。此外、您可以將資料備份或分層到多個雲端。

將 StorageGRID 資料備份到外部位置

您可以使用Cloud Storage Pool將StorageGRID 物件備份到外部位置。

如果StorageGRID 無法存取中的複本、雲端儲存資源池中的物件資料可用於處理用戶端要求。不過、您可能需要發出 S3 RestoreObject 要求、才能存取 Cloud Storage Pool 中的備份物件複本。

雲端儲存資源池中的物件資料也可用於恢復StorageGRID 由於儲存磁碟區或儲存節點故障而從故障中遺失的資料。如果物件的唯一剩餘複本位於Cloud Storage Pool中、StorageGRID 則由NetApp暫時還原物件、並在恢復的儲存節點上建立新複本。

若要實作備份解決方案：

1. 建立單一雲端儲存資源池。
2. 設定ILM規則、將物件複本同時儲存在儲存節點上（複寫或銷毀編碼複本）、並將單一物件複本儲存在雲端儲存資源池中。
3. 將規則新增至ILM原則。然後、模擬並啟動原則。

將資料從 StorageGRID 分層至外部位置

您可以使用雲端儲存資源池、將物件儲存在StorageGRID 不屬於該系統的地方。例如、假設您有大量物件需要保留、但您預期很少存取這些物件（如果有的話）。您可以使用雲端儲存資源池來分層物件、以降低儲存成本、

並釋放StorageGRID 出在效益管理系統中的空間。

若要實作分層解決方案：

1. 建立單一雲端儲存資源池。
2. 設定ILM規則、將鮮少使用的物件從儲存節點移至雲端儲存資源池。
3. 將規則新增至ILM原則。然後、模擬並啟動原則。

維護多個雲端端點

如果您希望將物件資料分層或備份到多個雲端平台，可以設定多個 Cloud Storage Pool 端點。ILM 規則中的篩選器可讓您指定哪些物件儲存在每個 Cloud Storage Pool 中。例如，您可能想要將某些租戶或儲存桶中的物件儲存在 Amazon S3 Glacier 中，而將其他租戶或儲存桶中的物件儲存在 Azure Blob Storage 中。或者，您可能希望在 Amazon S3 Glacier 和 Azure Blob Storage 之間移動資料。

使用多個雲端儲存池端點時、請記住、物件一次只能儲存在一個雲端儲存池中。

若要實作多個雲端端點：

1. 建立最多10個雲端儲存資源池。
2. 設定ILM規則、以便在適當的時間將適當的物件資料儲存在每個雲端儲存資源池中。例如、將儲存區 A 中的物件儲存在 Cloud Storage Pool A 中、並將儲存區 B 中的物件儲存在 Cloud Storage Pool B 中。或者、將物件儲存在 Cloud Storage Pool A 中一段時間、然後將物件移至 Cloud Storage Pool B
3. 將規則新增至ILM原則。然後、模擬並啟動原則。

StorageGRID 中的雲端儲存資源池需求與限制

如果您打算使用雲端儲存資源池將物件移出StorageGRID 整個作業系統、則必須檢閱設定和使用雲端儲存資源池的考量事項。

一般考量

- 一般來說，雲端歸檔儲存設備（例如 Amazon S3 Glacier 或 Azure Blob 儲存設備）是儲存物件資料的一種經濟實惠的方式。然而，從雲端歸檔儲存設備擷取資料的成本相對較高。為了達到最低的整體成本，您必須考慮何時以及多久存取一次 Cloud Storage Pool 中的物件。建議僅將 Cloud Storage Pool 用於您預計存取頻率較低的內容。
- 由於從雲端儲存資源池目標擷取物件的延遲增加、因此不支援使用FabricPool 含有支援功能的雲端儲存資源池。
- 啟用 S3 物件鎖定的物件無法放置在雲端儲存資源池中。
- Cloud Storage Pool 不支援以下平台、驗證及具有 S3 物件鎖定的傳輸協定組合：
  - * 平台 * ： Google Cloud Platform 與 Azure
  - 身份驗證類型：匿名訪問
  - * 傳輸協定 * ： HTTP

雲端儲存資源池所用連接埠的考量事項

若要確保ILM規則可將物件移入或移出指定的Cloud Storage Pool、您必須設定包含系統儲存節點的網路。您必須確保下列連接埠可與Cloud Storage Pool通訊。

根據預設、Cloud Storage Pool會使用下列連接埠：

- **80**：適用於以http開頭的端點URI
- * 443*：適用於以https開頭的端點URI

您可以在建立或編輯雲端儲存資源池時、指定不同的連接埠。

如果您使用非透明 Proxy 伺服器、也必須"設定儲存 Proxy"允許訊息傳送至外部端點、例如網際網路上的端點。

成本考量

若要使用雲端儲存資源池存取雲端儲存設備、需要透過網路連線才能連線至雲端。您必須考量存取雲端所需的網路基礎架構成本、並根據使用StorageGRID Cloud Storage Pool在介於流通於流通的資料量、適當地配置雲端。

當連接到外部雲端儲存資源池端點時StorageGRID 、它會發出各種要求來監控連線能力、並確保它能執行所需的作業。雖然這些要求會帶來一些額外成本、但監控雲端儲存資源池的成本只應是S3或Azure中儲存物件的整體成本的一小部分。

如果您需要將物件從外部Cloud Storage Pool端點移回StorageGRID 至物件、可能會產生更高的成本。在StorageGRID 下列任一情況下、物件都可能移回物件的不執行功能：

- 物件的唯一複本是在Cloud Storage Pool中、您決定將物件儲存StorageGRID 在物件中、改為將物件儲存在物件中。在這種情況下、您可以重新設定 ILM 規則和原則。進行ILM評估時StorageGRID 、此功能會發出多個要求、要求從Cloud Storage Pool擷取物件。然後、在本機建立指定數量的複製或銷毀編碼複本。StorageGRID物件移回StorageGRID 物件後、雲端儲存池中的複本即會刪除。
- 物件會因為儲存節點故障而遺失。如果物件的唯一剩餘複本位於Cloud Storage Pool中、StorageGRID 則由NetApp暫時還原物件、並在恢復的儲存節點上建立新複本。

> 當物件從StorageGRID 雲端儲存資源池移回支援區時StorageGRID 、針對每個物件向雲端儲存資源池端點發出多個要求。在搬移大量物件之前、請聯絡技術支援部門、以協助評估時間範圍及相關成本。

S3：Cloud Storage Pool儲存區所需的權限

用於雲端儲存池的外部 S3 儲存區原則必須授予 StorageGRID 權限、才能將物件移至儲存區、取得物件狀態、在需要時從 Glacier 儲存區還原物件等。理想情況下、 StorageGRID 應擁有對儲存庫的完全控制存取權(`s3:*`)；不過、如果無法做到這點、儲存庫原則必須將下列 S3 權限授予 StorageGRID ：

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`

- `s3:PutObject`
- `s3:RestoreObject`

S3：外部儲存庫生命週期的考量事項

StorageGRID 和雲端儲存資源池中指定的外部 S3 儲存區之間的物件移動、是由 ILM 規則和 StorageGRID 中的主動 ILM 原則所控制。相反地、從雲端儲存資源池中指定的外部S3儲存區、移轉至Amazon S3 Glacier或S3 Glacier Deep歸檔（或移轉至實作Glacier儲存類別的儲存解決方案）的物件、則是由該儲存區的生命週期組態所控制。

如果您想要從雲端儲存池移轉物件、則必須在外部 S3 儲存區上建立適當的生命週期組態、而且您必須使用實作 Glacier 儲存類別並支援 S3 RestoreObject API 的儲存解決方案。

例如、假設您想StorageGRID 要將從靜止移至雲端儲存資源池的所有物件立即轉換至Amazon S3 Glacier儲存設備。您可以在外部S3儲存區上建立生命週期組態、以指定下列單一動作（* Transition *）：

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

這項規則會在所有庫位物件建立之日（亦即、在StorageGRID 物件從旁移至雲端儲存池當日）、將其全部移轉至Amazon S3 Glacier。

設定外部儲存庫的生命週期時、切勿使用* Expiration*動作來定義物件何時過期。過期動作會導致外部儲存系統刪除過期的物件。如果您稍後嘗試從StorageGRID 無法存取過期的物件、將無法找到刪除的物件。

如果您想要將雲端儲存池中的物件移轉至 S3 Glacier Deep Archive （而非 Amazon S3 Glacier ）、請在貯體生命週期中指定 `<StorageClass>DEEP_ARCHIVE</StorageClass>`。不過、請注意、您無法使用該 `Expedited`階層來還原 S3 Glacier Deep Archive 中的物件。

Azure：存取層的考量

當您設定Azure儲存帳戶時、可以將預設的存取層設定為「Hot」（熱）或「Cool」（冷）。建立用於雲端儲存資源池的儲存帳戶時、您應該使用熱層做為預設層。即使將物件移至雲端儲存資源池時、將層級立即設定為「歸檔」、但使用預設的Hot（熱）設定、可確保您不會在30天內收取從冷卻層移除物件的早期刪除費用。StorageGRID

Azure：不支援生命週期管理

請勿對與 Cloud Storage Pool 搭配使用的 Container 使用 Azure Blob Storage 生命週期管理。生命週期操作可能會干擾 Cloud Storage Pool 的操作。

相關資訊

"建立雲端儲存資源池"

StorageGRID 中的雲端儲存資源池與 **CloudMirror** 複寫

開始使用Cloud Storage Pool時、瞭解Cloud Storage Pool與StorageGRID VMware CloudMirror複寫服務之間的相似點和差異可能會有所幫助。

	雲端儲存資源池	**CloudMirror**複寫服務
主要目的為何？	做為歸檔目標。Cloud Storage Pool中的物件複本可以是物件的唯一複本、也可以是其他複本。也就是說、您可以在 StorageGRID 中保留一份複本、並將複本傳送至雲端儲存池、而不是將兩份複本保留在現場。	可讓租戶自動將物件從 StorageGRID （來源）的貯體複寫到外部 S3 貯體（目的地）。在個別 S3 基礎架構中建立物件的個別複本。
如何設定？	使用 Grid Manager 或 Grid Management API 、以與儲存資源池相同的方式定義。可在 ILM 規則中選取作為放置位置。雖然儲存資源池由一組儲存節點組成、但雲端儲存資源池是使用遠端S3或Azure端點（IP位址、認證等）來定義。	租戶使用者"設定CloudMirror複寫"可以使用 Tenant Manager 或 S3 API 定義 CloudMirror 端點（ IP 位址、認證等）。設定CloudMirror端點之後、該租戶帳戶擁有的任何儲存區都可設定為指向CloudMirror端點。
誰負責設定？	通常是網格管理員	通常是租戶使用者
目的地為何？	• 任何相容的S3基礎架構（包括Amazon S3） • Azure Blob歸檔層 • Google Cloud Platform（GCP）	• 任何相容的S3基礎架構（包括Amazon S3） • Google Cloud Platform（GCP）
什麼原因會將物件移至目的地？	主動式 ILM 原則中的一或多個 ILM 規則。ILM 規則定義StorageGRID 哪些物件會移至雲端儲存資源池、以及物件移動的時間。	將新物件擷取至已設定 CloudMirror 端點的來源貯體的動作。除非經過修改、否則不會複寫在使用 CloudMirror 端點設定儲存區之前存在於來源儲存區中的物件。
如何擷取物件？	應用程式必須要求StorageGRID 提供物件以擷取已移至雲端儲存資源池的物件。如果物件的唯一複本已轉換為歸檔儲存設 備、StorageGRID 則由部門管理還原物件的程序、以便擷取物件。	由於目標儲存區中的鏡射複本是獨立複本、因此應用程式可以要求StorageGRID 將物件擷取至S庫 或S3目的地。例如、假設您使用CloudMirror複寫將物件鏡射到合作夥伴組織。合作夥伴可以使用自己的應用程式、直接從S3目的地讀取或更新物件。不需要使用此功能。StorageGRID

	雲端儲存資源池	**CloudMirror**複寫服務
您可以直接從目的地讀取嗎？	否。移至雲端儲存池的物件是由 StorageGRID 管理。讀取要求必須導向StorageGRID 至指令集（StorageGRID 而非指令集將負責從雲端儲存池擷取）。	是的、因為鏡射複本是獨立的複本。
如果物件從來源中刪除、會發生什麼情況？	此物件也會從雲端儲存池中刪除。	刪除動作不會複寫。刪除的物件已不再存在StorageGRID 於這個物件庫中、但仍存在於目的地庫位中。同樣地、也可以刪除目的地儲存區中的物件、而不會影響來源。
災難發生後如何存取物件StorageGRID （無法運作的不支援系統）？	故障StorageGRID 的無法修復節點必須恢復。在此程序期間、複寫物件的複本可以使用Cloud Storage Pool中的複本來還原。	CloudMirror目的地中的物件複本不受StorageGRID 支援、因此可在StorageGRID 還原物件節點之前直接存取。

在 **StorageGRID** 中建立雲端儲存資源池

雲端儲存資源池指定單一外部 Amazon S3 儲存桶或其他 S3 相容供應商或 Azure Blob Storage Container。

建立雲端儲存資源池時，您可以指定 StorageGRID 將用於儲存物件的外部儲存桶或 Container 的名稱和位置、雲端供應商類型（Amazon S3/GCP 或 Azure Blob Storage）以及 StorageGRID 存取外部儲存桶或 Container 所需的資訊。

一旦儲存雲端儲存資源池、即可驗證其運作、因此您必須確保Cloud Storage Pool中指定的儲存庫或容器存在且可存取。StorageGRID

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。
- 您已檢閱"雲端儲存資源池的考量"。
- Cloud Storage Pool 所參照的外部儲存區或容器已經存在服務端點資訊、您擁有。
- 若要存取貯體或容器、您可以驗證類型的帳戶資訊選擇。

步驟

1. 選取 * ILM * > * 儲存池 * > * 雲端儲存池 * 。
2. 選取 * 建立 * 、然後輸入下列資訊：

欄位	說明
雲端儲存池名稱	簡短說明雲端儲存資源池及其用途的名稱。設定ILM規則時、請使用容易識別的名稱。

欄位	說明
供應商類型	您將使用哪家雲端供應商來管理此雲端儲存資源池： • * Amazon S3/GCP* ：針對 Amazon S3 、商業雲端服務（ C2S ） S3 、 Google Cloud Platform （ GCP ）或其他相容 S3 的供應商、選取此選項。 • * Azure Blob Storage *
貯體或容器	外部 S3 貯體或 Azure 容器的名稱。您無法在儲存雲端儲存池後變更此值。

3. 根據您的供應商類型選擇、輸入服務端點資訊。

Amazon S3/GCP

a. 對於通訊協定、請選取 HTTPS 或 HTTP 。

> 請勿將 HTTP 連線用於敏感資料。

b. 輸入主機名稱。範例：

`s3-aws-region.amazonaws.com`

c. 選取 URL 樣式：

選項	說明
自動偵測	根據所提供的資訊、嘗試自動偵測要使用的URL樣式。例如、如果您指定IP位址、StorageGRID 則表示功能表將使用路徑樣式URL。僅當您不知道要使用哪種特定樣式時、才選取此選項。
虛擬代管風格	使用虛擬託管型 URL 來存取貯體。虛擬託管型 URL 會將貯體名稱納入網域名稱中。範例： `https://bucket-name.s3.company.com/key-name`
路徑樣式	使用路徑樣式URL存取儲存區。路徑樣式的 URL 結尾包含貯體名稱範例： `https://s3.company.com/bucket-name/key-name` • 附註： * 不建議使用路徑樣式的 URL 選項、而且在未來的 StorageGRID 版本中將會被淘汰。

d. 您也可以輸入連接埠編號、或使用預設連接埠： 443 代表 HTTPS 、 80 代表 HTTP 。

Azure Blob儲存設備

a. 使用下列其中一種格式、輸入服務端點的 URI 。

- `https://host:port`
- `http://host:port`

範例： `https://myaccount.blob.core.windows.net:443`

如果您未指定連接埠、則預設會使用連接埠 443 做為 HTTPS 、並使用連接埠 80 做為 HTTP 。

4. 選取 * 繼續 * 。然後選取驗證類型、並輸入 Cloud Storage Pool 端點所需的資訊：

存取金鑰

_ 適用於 Amazon S3/GCP 或其他相容 S3 的供應商 _

a. * 存取金鑰 ID* ：輸入擁有外部儲存庫之帳戶的存取金鑰 ID 。
b. * 秘密存取金鑰 * ：輸入秘密存取金鑰。

IAM 角色隨處可用

適用於 AWS IAM 角色 Anywhere 服務 _

StorageGRID 使用 AWS 安全性權杖服務（ STS ）來動態產生一個短暫的權杖來存取 AWS 資源。

a. * AWS IAM 角色 Anywhere 區域 * ：選取雲端儲存池的區域。例如 `us-east-1` ：。
b. * 信任錨點 URN* ：輸入驗證短期 STS 認證要求的信任錨點 URN 。可以是根 CA 或中繼 CA 。
c. * 設定檔 URN* ：輸入 IAM 角色 Anywhere 設定檔的 URN 、其中列出可為任何信任的人假設的角色。
d. * 角色 URN* ：輸入 IAM 角色的 URN 、此角色可假設給任何受信任的人。
e. * 工作階段持續時間 * ：輸入暫時安全性認證和角色工作階段的持續時間。輸入至少 15 分鐘、不超過 12 小時。
f. * 伺服器 CA 憑證 * （選用）：一或多個受信任的 CA 憑證（ PEM 格式）、用於驗證 IAM 角色 Anywhere 伺服器。如果省略、將無法驗證伺服器。
g. * 終端實體憑證 * ：由信任標記簽署之 X509 憑證的公開金鑰、採用 PEM 格式。AWS IAM 角色 Anywhere 使用此金鑰來發行 STS Token 。
h. * 終端實體私密金鑰 * ：終端實體憑證的私密金鑰。

CAP （ **C2S** 存取入口網站）

商業雲端服務（ C2S ） S3 服務 _

a. * 暫存認證 URL* ：輸入 StorageGRID 從 CAP 伺服器取得暫存認證的完整 URL 、包括指派給您的 C2S 帳戶的所有必要和選用 API 參數。
b. * 伺服器 CA 憑證 * ：選取 * 瀏覽 * 並上傳 StorageGRID 用來驗證 CAP 伺服器的 CA 憑證。憑證必須由 PEM 編碼、並由適當的政府憑證授權單位（ CA ）核發。
c. * 用戶端憑證 * ：選取 * 瀏覽 * 、然後將 StorageGRID 用來識別自己的憑證上傳至 CAP 伺服器。用戶端憑證必須採用 PEM 編碼、由適當的政府憑證授權單位（ CA ）核發、並授予您對 C2S 帳戶的存取權。
d. * 用戶端私密金鑰 * ：選取 * 瀏覽 * 並上傳用戶端憑證的 PEM 編碼私密金鑰。
e. 如果用戶端私密金鑰已加密、請輸入密碼來解密用戶端私密金鑰。否則、請將 * 用戶端私密金鑰複雜密碼 * 欄位保留空白。

> 如果要加密用戶端憑證、請使用傳統的加密格式。不支援 PKCS #8 加密格式。

Azure Blob儲存設備

_Azure Blob 儲存設備、僅共用金鑰 _

a. * 帳戶名稱 * ：輸入擁有外部容器的儲存帳戶名稱

b. * 帳戶金鑰 * ：輸入儲存帳戶的秘密金鑰

您可以使用Azure入口網站來尋找這些價值。

匿名

不需要其他資訊。

5. 選擇*繼續*。然後選擇您要使用的伺服器驗證類型：

選項	說明
在儲存節點作業系統中使用根 CA 憑證	使用安裝在作業系統上的Grid CA憑證來保護連線安全。
使用自訂CA憑證	使用自訂CA憑證。選取 * 瀏覽 * 並上傳 PEM 編碼的憑證。
請勿驗證憑證	選取此選項表示 TLS 連線至雲端儲存池不安全。

6. 選擇*保存*。

當您儲存雲端儲存資源池時StorageGRID 、下列功能將會隨之執行：

- 驗證貯體或容器及服務端點是否存在、以及是否可使用您指定的認證來連線。
- 將標記檔案寫入貯體或容器、以將其識別為雲端儲存池。請勿移除這個名為的檔案 `x-ntap-sgws-cloud-pool-uuid`。

  如果Cloud Storage Pool驗證失敗、您會收到錯誤訊息、說明驗證失敗的原因。例如、如果發生憑證錯誤、或是您指定的貯體或容器尚未存在、則可能會回報錯誤。

7. 如果發生錯誤"疑難排解雲端儲存資源池的指示"、請參閱、解決任何問題、然後再次嘗試儲存雲端儲存池。

相關資訊

"用於外部通訊的連接埠"

在 **StorageGRID** 中檢視雲端儲存資源池詳細資料

您可以檢視 Cloud Storage Pool 的詳細資料、以判斷其使用位置、並查看其中包含哪些節點和儲存等級。

開始之前

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

步驟

1. 選取 * ILM * > * 儲存池 * > * 雲端儲存池 * 。

Cloud Storage Pools 表格包含每個包含 Storage Node 的 Cloud Storage Pool 的下列資訊：

- **Name** ：池的唯一顯示名稱。
- * URI* ：雲端儲存池的統一資源識別碼。
- * 供應商類型 * ：此雲端儲存池使用哪種雲端供應商。
- * Container * ：用於 Cloud Storage Pool 的儲存區名稱。
- * ILM 使用率 * ：目前使用資源池的方式。雲端儲存資源池可能未使用、或可能用於一或多個 ILM 規則、銷毀編碼設定檔、或兩者。
- * 最後一個錯誤 * ：此雲端儲存池執行狀況檢查期間偵測到的最後一個錯誤。

2. 若要檢視特定雲端儲存池的詳細資料、請選取其名稱。

   隨即顯示集區的詳細資料頁面。

3. 檢視 * 驗證 * 索引標籤以瞭解此雲端儲存池的驗證類型、並編輯驗證詳細資料。
4. 檢視 * 伺服器驗證 * 索引標籤、瞭解驗證詳細資料、編輯驗證、下載新憑證、或複製憑證 PEM 。
5. 檢視 * ILM 使用率 * 索引標籤、判斷雲端儲存池目前是否正在任何 ILM 規則或銷毀編碼設定檔中使用。
6. 您也可以移至 * ILM 規則頁面 * 、以"瞭解並管理任何規則"使用雲端儲存池。

在 **StorageGRID** 中編輯雲端儲存資源池

您可以編輯 Cloud Storage Pool 來變更其名稱、服務端點或其他詳細資料、但是您無法變更 Cloud Storage Pool 的 S3 儲存區或 Azure 容器。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已檢閱"雲端儲存資源池的考量"。

步驟

1. 選取 * ILM * > * 儲存池 * > * 雲端儲存池 * 。

   Cloud Storage Pools表格會列出現有的Cloud Storage Pools。

2. 選取您要編輯的雲端儲存池核取方塊、然後選取 * 動作 * > * 編輯 * 。

   或者、選取雲端儲存池的名稱、然後選取 * 編輯 * 。

3. 視需要變更雲端儲存池名稱、服務端點、驗證認證或憑證驗證方法。

   > 您無法變更雲端儲存池的供應商類型、 S3 儲存區或 Azure 容器。

   如果您先前已上傳伺服器或用戶端憑證、您可以展開 * 憑證詳細資料 * 手風琴來檢閱目前使用的憑證。

4. 選擇*保存*。

   當您儲存雲端儲存資源池時StorageGRID 、驗證資源桶或容器及服務端點是否存在、以及是否可以使用您指定的認證資料來存取。

如果Cloud Storage Pool驗證失敗、則會顯示錯誤訊息。例如、如果發生憑證錯誤、可能會報告錯誤。

請參閱的說明"疑難排解雲端儲存資源池"、解決問題、然後再次嘗試儲存 Cloud Storage Pool 。

在 **StorageGRID** 中移除雲端儲存資源池

如果 Cloud Storage Pool 未用於 ILM 規則、而且不包含物件資料、您可以將其移除。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。

如有需要、請使用 **ILM** 來移動物件資料

如果您要移除的雲端儲存池包含物件資料、則必須使用 ILM 將資料移至其他位置。例如、您可以將資料移至網格上的儲存節點、或移至不同的雲端儲存池。

步驟

1. 選取 * ILM * > * 儲存池 * > * 雲端儲存池 * 。
2. 請查看表格中的 ILM 使用率欄、以判斷您是否可以移除雲端儲存池。

   如果雲端儲存池正用於 ILM 規則或銷毀編碼設定檔中、則無法移除該集區。

3. 如果使用的是雲端儲存池、請選取 * 雲端儲存池名稱 _ * > * ILM 使用量 * 。
4. "複製每個 ILM 規則"這會將物件放置在您要移除的雲端儲存池中。
5. 決定您要移動由您複製的每個規則所管理的現有物件的位置。

   您可以使用一或多個儲存池或不同的雲端儲存池。

6. 編輯您複製的每個規則。

   對於「建立 ILM 規則」精靈的步驟 2 、請從「 * 複本於 * 」欄位中選取新位置。

7. "建立新的 ILM 原則"並以複製規則取代每個舊規則。
8. 啟動新原則。
9. 等待 ILM 從雲端儲存池移除物件、並將其置於新位置。

刪除雲端儲存池

當雲端儲存池是空的且未用於任何 ILM 規則時、您可以將其刪除。

開始之前

- 您已移除可能已使用資源池的任何 ILM 規則。
- 您已確認S3儲存區或Azure容器不含任何物件。

  如果您嘗試移除包含物件的雲端儲存池、就會發生錯誤。請參閱。 "疑難排解雲端儲存資源池"

當您建立Cloud Storage Pool時StorageGRID 、將標記檔案寫入儲存庫或容器、以將其識別為雲端儲存池。請勿移除這個名為的檔案 `x-ntap-sgws-cloud-pool-uuid`。

步驟

1. 選取 * ILM * > * 儲存池 * > * 雲端儲存池 * 。
2. 如果 ILM 使用率欄顯示未使用 Cloud Storage Pool 、請選取核取方塊。
3. 選擇*「Actions」（動作）>「Remove*」（移除
4. 選擇*確定*。

疑難排解 **StorageGRID** 中的雲端儲存資源池

使用這些疑難排解步驟、協助解決您在建立、編輯或刪除雲端儲存池時可能遇到的錯誤。

確定是否發生錯誤

StorageGRID 會讀取已知物件、以確保雲端儲存池能夠存取且正常運作、進而對每個雲端儲存池執行簡單的健全狀況檢查 `x-ntap-sgws-cloud-pool-uuid`。當 StorageGRID 在端點上遇到錯誤時、它會每分鐘從每個儲存節點執行一次健全狀況檢查。當錯誤解決時、健全狀況檢查就會停止。如果健全狀況檢查偵測到問題、「儲存池」頁面上的「雲端儲存池」表最後一個錯誤欄會顯示訊息。

下表顯示針對每個雲端儲存資源池偵測到的最新錯誤、並指出錯誤發生的時間已過多久。

此外、如果健全狀況檢查偵測到過去5分鐘內發生一或多個新的雲端儲存池錯誤、則會觸發* Cloud Storage Pool連線錯誤*警示。如果您收到此警示的電子郵件通知、請前往「儲存資源池」頁面（選擇 * ILM * > * 儲存資源池 * ）、檢閱最後一個錯誤欄中的錯誤訊息、並參閱下列疑難排解準則。

檢查錯誤是否已解決

解決任何潛在問題之後、您可以判斷錯誤是否已解決。從「雲端儲存池」頁面選取端點、然後選取 * 清除錯誤 * 。確認訊息指出StorageGRID 、由於此錯誤已清除Cloud Storage Pool的錯誤。

如果基礎問題已解決、就不會再顯示錯誤訊息。但是、如果基礎問題尚未解決（或遇到不同的錯誤）、則錯誤訊息會在幾分鐘內顯示在最後一個錯誤欄中。

錯誤：健全狀況檢查失敗。端點發生錯誤

在以下情況下，您可能會遇到此錯誤：

- 當您開始將 Amazon S3 儲存桶用於雲端儲存資源池後，啟用預設保留的 S3 物件鎖定時，會發生此錯誤。這是因為 PUT 操作缺少包含有效負載 Checksum 值的 HTTP 標頭，例如 `Content-MD5`。AWS 要求對已啟用 S3 物件鎖定的儲存桶執行 PUT 操作時，必須包含此標頭值。

  若要解決此問題，請按照 "編輯雲端儲存資源池" 中的步驟操作，無需進行任何變更。此行動將觸發雲端儲存資源池組態的驗證，該驗證會自動偵測並更新雲端儲存資源池端點組態上的 S3 物件鎖定標誌。

- 當您開始將此儲存桶用於雲端儲存資源池後，為 StorageGRID S3 儲存桶啟用具有預設保留的 S3 物件鎖定。

  要解決此問題：

- 如果您使用的是 HTTP：啟用了 S3 Object Lock 的雲端儲存資源池不受支援。請編輯端點連線，改用 HTTPS。
- 如果您使用的是 HTTPS：請依照 "編輯雲端儲存資源池" 中的步驟操作，無需進行任何變更。此行動將觸發雲端儲存資源池組態的驗證，該驗證會自動偵測並更新雲端儲存資源池端點組態上的 S3 物件鎖定標誌。

如果還有其他問題，請聯絡技術支援。

錯誤：此**Cloud Storage Pool**包含非預期的內容

當您嘗試建立、編輯或刪除雲端儲存池時、可能會遇到此錯誤。如果貯體或容器包含標記檔案、但該檔案沒有包含預期 UUID 的中繼資料欄位、就會發生此錯誤 `x-ntap-sgws-cloud-pool-uuid`。

一般而StorageGRID 言、如果您正在建立新的Cloud Storage Pool、而另一個執行個體正在使用相同的Cloud Storage Pool、則只會看到此錯誤。

請嘗試下列其中一個步驟來修正問題：

- 如果您正在設定新的 Cloud Storage Pool ，而該儲存區包含 `x-ntap-sgws-cloud-pool-uuid`類似下列範例的檔案和其他物件金鑰，請建立新的儲存區，然後改用這個新的儲存區。

  其他物件金鑰範例： `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- 如果 `x-ntap-sgws-cloud-pool-uuid`檔案是貯體中唯一的物件，請刪除此檔案。

如果這些步驟不適用於您的案例，請聯絡支援部門。

錯誤：無法建立或更新雲端儲存池。端點發生錯誤

在下列情況下、您可能會遇到此錯誤：

- 當您嘗試建立或編輯雲端儲存池時。
- 當您在設定新的雲端儲存池時、選擇不受支援的平台、驗證或與 S3 物件鎖定的傳輸協定組合。請參閱。 "雲端儲存資源池的考量"

此錯誤表示連線或組態問題導致 StorageGRID 無法寫入雲端儲存池。

若要修正問題、請檢閱端點的錯誤訊息。

- 如果錯誤訊息包含、請檢查雲端儲存池所 `Get *url*: EOF`使用的服務端點、是否未將 HTTP 用於需要 HTTPS 的容器或儲存區。
- 如果錯誤訊息包含 `Get *url*: net/http: request canceled while waiting for connection`、請確認網路組態允許儲存節點存取用於雲端儲存池的服務端點。
- 如果錯誤是因為不支援的平台、驗證或傳輸協定所造成、請使用 S3 Object Lock 變更為支援的組態、然後再次嘗試儲存新的 Cloud Storage Pool 。
- 對於所有其他端點錯誤訊息、請嘗試下列其中一項或多項：
  - 建立與您為Cloud Storage Pool輸入相同名稱的外部容器或儲存區、然後再次嘗試儲存新的Cloud Storage Pool。
  - 請更正您為Cloud Storage Pool指定的容器或儲存區名稱、然後再次嘗試儲存新的Cloud Storage Pool。

錯誤：無法剖析**CA**憑證

當您嘗試建立或編輯雲端儲存資源池時、可能會遇到此錯誤。如果在設定Cloud Storage Pool時、無法剖析您輸入的憑證、就會發生錯誤StorageGRID 。

若要修正問題、請檢查您提供的CA憑證是否有問題。

錯誤：找不到具有此**ID**的雲端儲存資源池

當您嘗試編輯或刪除雲端儲存資源池時、可能會遇到此錯誤。如果端點傳回404回應、就會發生此錯誤、這可能代表下列其中一項：

- 雲端儲存池使用的認證資料沒有儲存區的讀取權限。
- 用於雲端儲存池的貯體不包含 `x-ntap-sgws-cloud-pool-uuid`標記檔案。

請嘗試下列一或多個步驟來修正問題：

- 檢查與設定的存取金鑰相關聯的使用者是否擁有必要的權限。
- 使用具備必要權限的認證資料編輯Cloud Storage Pool。
- 如果權限正確、請聯絡支援部門。

錯誤：無法檢查**Cloud Storage Pool**的內容。端點發生錯誤

當您嘗試刪除雲端儲存資源池時、可能會遇到此錯誤。此錯誤表示某種連線或組態問題使StorageGRID 無法讀取Cloud Storage Pool儲存區儲存區內容。

若要修正問題、請檢閱端點的錯誤訊息。

錯誤：物件已放置在此儲存區中

當您嘗試刪除雲端儲存資源池時、可能會遇到此錯誤。如果雲端儲存池包含由 ILM 移至該處的資料、設定雲端儲存池之前儲存在儲存區中的資料、或是建立雲端儲存池之後由其他來源放入儲存區的資料、則您無法刪除該儲存池。

請嘗試下列一或多個步驟來修正問題：

- 請依照「雲端儲存池物件生命週期」中的指示、將物件移回 StorageGRID 。
- 如果您確定其餘的物件並非由ILM放置在雲端儲存資源池中、請手動刪除儲存區中的物件。

> 切勿手動刪除ILM可能放置在雲端儲存資源池中的物件。如果您稍後嘗試從StorageGRID 功能表存取手動刪除的物件、將無法找到刪除的物件。

錯誤：**Proxy**嘗試連至雲端儲存資源池時發生外部錯誤

如果您已在儲存節點和用於雲端儲存池的外部 S3 端點之間設定不透明儲存 Proxy 、則可能會遇到此錯誤。如果外部 Proxy 伺服器無法連線至雲端儲存池端點、就會發生此錯誤。例如、DNS伺服器可能無法解析主機名稱、或是發生外部網路問題。

請嘗試下列一或多個步驟來修正問題：

- 檢查雲端儲存資源池的設定（* ILM > Storage Pools*）。
- 檢查儲存 Proxy 伺服器的網路組態。

錯誤： **X.509** 憑證已過有效期間

當您嘗試刪除雲端儲存資源池時、可能會遇到此錯誤。當驗證需要 X.509 憑證以確保驗證正確的外部 Cloud Storage Pool 、且在刪除 Cloud Storage Pool 組態之前、外部 Pool 為空時、就會發生此錯誤。

請嘗試下列步驟來修正問題：

- 將設定用於驗證的憑證更新至雲端儲存池。
- 請確定已解決此雲端儲存池的任何憑證過期警示。

相關資訊

"Cloud Storage Pool物件的生命週期"

在 StorageGRID 中管理銷毀編碼設定檔

您可以檢視抹除編碼設定檔的詳細資料、並視需要重新命名設定檔。如果目前未在任何 ILM 規則中使用抹除編碼設定檔、您可以停用該設定檔。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。

檢視銷毀編碼設定檔詳細資料

您可以檢視銷毀編碼設定檔的詳細資料、以判斷其狀態、使用的銷毀編碼配置、以及其他資訊。

步驟

1. 選擇*配置* > 系統 > 擦除編碼。
2. 選取設定檔。設定檔的詳細資料頁面隨即出現。
3. 您也可以檢視 ILM 規則索引標籤、以取得使用設定檔的 ILM 規則清單、以及使用這些規則的 ILM 原則。
4. 您也可以檢視儲存節點索引標籤、以取得設定檔儲存池中每個儲存節點的詳細資料、例如其所在的站台和儲存使用量。

重新命名抹除編碼設定檔

您可能想要重新命名抹除編碼設定檔、以使設定檔的功能更為明顯。

步驟

1. 選擇*配置* > 系統 > 擦除編碼。
2. 選取您要重新命名的設定檔。
3. 選取*重新命名*。
4. 輸入銷毀編碼設定檔的唯一名稱。

銷毀編碼設定檔名稱會附加至 ILM 規則放置指示中的儲存資源池名稱。

> 銷毀編碼設定檔名稱必須是唯一的。如果您使用現有設定檔的名稱、即使該設定檔已停用、也會發生驗證錯誤。

5. 選擇*保存*。

停用抹除編碼設定檔

如果您不再打算使用抹除編碼設定檔、且目前未在任何 ILM 規則中使用該設定檔、則可以停用該設定檔。

> 確認沒有任何銷毀編碼的資料修復作業或取消委任程序正在進行中。如果您嘗試在其中任一項作業進行中停用銷毀編碼設定檔、就會傳回錯誤訊息。

關於這項工作

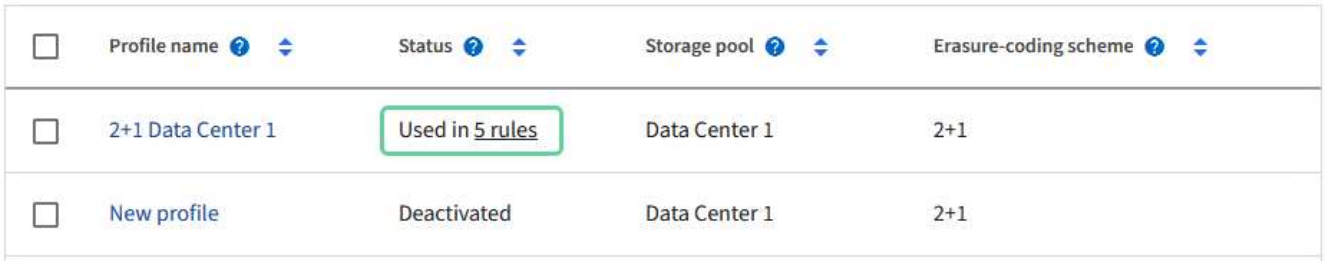
如果下列任一項為真、 StorageGRID 可防止您停用銷毀編碼設定檔：

- 銷毀編碼設定檔目前用於 ILM 規則。
- 刪除編碼設定檔不再用於任何 ILM 規則、但該設定檔的物件資料和同位元檢查片段仍存在。

步驟

1. 選擇*配置* > 系統 > 擦除編碼。
2. 在「作用中」標籤上、檢閱 * 狀態 * 欄、確認您要停用的銷毀編碼設定檔未用於任何 ILM 規則。

   如果在任何 ILM 規則中使用抹除編碼設定檔、則無法停用該設定檔。在範例中、 2+1 Data Center 1 設定檔至少用於一個 ILM 規則。



3. 如果在ILM規則中使用設定檔、請遵循下列步驟：
   a. 選擇* ILM > Rules *。
   b. 選取每個規則並檢閱保留圖表、以判斷規則是否使用您要停用的銷毀編碼設定檔。
   c. 如果 ILM 規則使用您要停用的銷毀編碼設定檔、請判斷該規則是否用於任何 ILM 原則。
   d. 根據刪除編碼設定檔的使用位置、完成表格中的其他步驟。

設定檔在哪裡使用？	停用設定檔之前要執行的其他步驟	請參閱這些額外說明
絕不用於任何ILM規則	不需執行其他步驟。繼續執行此程序。	無

設定檔在哪裡使用？	停用設定檔之前要執行的其他步驟	請參閱這些額外說明
在從未用於任何ILM原則的ILM規則中	i. 編輯或刪除所有受影響的ILM規則。如果您編輯規則、請移除所有使用抹除編碼設定檔的放置位置。 ii. 繼續執行此程序。	"使用ILM規則和ILM原則"
目前處於使用中 ILM 原則的 ILM 規則	i. 複製原則。 ii. 移除使用抹除編碼設定檔的 ILM 規則。 iii. 新增一或多個新的ILM規則、以確保物件受到保護。 iv. 儲存、模擬及啟動新原則。 v. 等待新原則套用、並根據您新增的新規則、將現有物件移至新位置。 附註： StorageGRID 視物件數量和您的一套系統尺寸而定、ILM作業可能需要數週甚至數月的時間、才能根據新的ILM規則、將物件移至新位置。 雖然您可以在銷毀編碼設定檔仍與資料相關聯的情況下、安全地嘗試停用該設定檔、但停用操作將會失敗。如果設定檔尚未準備好停用、將會出現錯誤訊息通知您。 vi. 編輯或刪除您從原則中移除的規則。如果您編輯規則、請移除所有使用抹除編碼設定檔的放置位置。 vii. 繼續執行此程序。	"建立ILM原則" "使用ILM規則和ILM原則"
目前在 ILM 原則中的 ILM 規則	i. 編輯原則。 ii. 移除使用抹除編碼設定檔的 ILM 規則。 iii. 新增一或多個新的ILM規則、確保所有物件都受到保護。 iv. 儲存原則。 v. 編輯或刪除您從原則中移除的規則。如果您編輯規則、請移除所有使用抹除編碼設定檔的放置位置。 vi. 繼續執行此程序。	"建立ILM原則" "使用ILM規則和ILM原則"

e. 重新整理「刪除編碼設定檔」頁面、以確保 ILM 規則中不會使用設定檔。

4. 如果ILM規則中未使用設定檔、請選取選項按鈕、然後選取* Deactonate*。此時會出現停用銷毀編碼設定檔對話方塊。

只要每個設定檔未用於任何規則、您就可以同時選取多個設定檔來停用。

5. 如果確定要停用設定檔、請選取* Deactivate（停用）*。

結果

- 如果 StorageGRID 能夠停用抹除編碼設定檔、其狀態就會停用。您無法再為任何ILM規則選取此設定檔。您無法重新啟動已停用的設定檔。
- 如果StorageGRID 無法停用設定檔、就會出現錯誤訊息。例如、如果物件資料仍與此設定檔相關聯、就會出現錯誤訊息。您可能需要等待數週、才能再次嘗試停用程序。

為StorageGRID配置 S3 區域

ILM 規則可以根據建立 S3 儲存桶的可選區域過濾對象，讓您可以將來自不同區域的物件儲存在不同的儲存位置。

如果您想要在規則中使用S3儲存區做為篩選條件、則必須先建立系統中的儲存區可以使用的區域。

在建立貯體之後、您無法變更貯體的區域。

開始之前

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

關於這項工作

建立S3儲存區時、您可以指定要在特定區域建立儲存區。指定區域可讓儲存庫在地理上靠近使用者、以協助最佳化延遲、將成本降至最低、並滿足法規要求。

建立ILM規則時、您可能會想要使用S3儲存區相關的區域做為進階篩選器。例如、您可以設計規則、僅適用於在區域中建立的 S3 儲存區中的物件 `us-west-2`。然後您可以指定將這些物件的複本放在該區域資料中心站台的儲存節點上、以最佳化延遲。

設定地區時、請遵循下列準則：

- 依預設、所有貯體都會被視為屬於該 `us-east-1`區域。
- 您必須先使用網格管理器建立區域，然後才能在使用租用戶管理器或租用戶管理 API 建立儲存桶時指定非預設區域，或使用 S3 PUT Bucket API 請求的 LocationConstraint 請求元素指定非預設區域。如果 PUT Bucket 要求使用StorageGRID中未定義的區域，則會發生錯誤。
- 建立S3儲存區時、您必須使用確切的區域名稱。區域名稱區分大小寫。有效字元為數字、字母和連字號。

  EU 不被視為 eu-west-1 的別名。如果您想使用 EU 或 eu-west-1 區域，則必須使用準確的名稱。

- 如果區域用於指派給任何原則的規則（作用中或非作用中）、則無法刪除或修改區域。
- 如果您在 ILM 規則中使用無效的區域做為進階篩選器、則無法將該規則新增至原則。

  如果您在 ILM 規則中使用某個區域作為進階篩選器，但後來刪除了該區域，或者您使用網格管理 API 建立規則並指定了未定義的區域，則可能會導致區域無效。

- 如果您在使用區域建立S3儲存區之後刪除該區域、則如果您想要使用位置限制進階篩選器來尋找該儲存區中的物件、則必須重新新增該區域。

步驟

1. 選擇* ILM > regions *。

   出現「區域」頁面。

2. 選擇“所有區域”或“預設區域”標籤。

   所有地區

   *所有區域*選項卡列出了目前定義的區域，包括定義的預設區域。

   > 您無法刪除或修改「所有區域」標籤中的預設區域。使用“預設區域”標籤來變更預設區域。

   a. 若要新增區域，請選擇「新增另一個區域」。

   b. 輸入建立S3儲存區時要使用的區域名稱。

      當您建立對應的S3儲存區時、必須使用此確切的區域名稱作為位置限制要求元素。

   c. 若要刪除未使用的區域，請選擇刪除圖示 ✕。

      如果您嘗試移除目前用於任何原則（作用中或非作用中）的區域、就會出現錯誤訊息。

   d. 完成變更後、請選取*「Save（儲存）」*。

      您現在可以從「建立 ILM 規則」精靈步驟 1 的「進階篩選器」區段中選取這些區域。請參閱。 "在ILM規則中使用進階篩選器"

   預設區域

   *預設區域*標籤顯示目前定義的預設區域，您可以修改它。

   a. 若要變更預設區域，請從「預設區域」下拉清單中的可用選項中選擇區域名稱。

   b. 選擇*保存*。

建立**ILM**規則

了解 **StorageGRID** 中的 **ILM** 規則

若要管理物件、請建立一組資訊生命週期管理（ILM）規則、並將其組織成ILM原則。

系統中擷取的每個物件都會根據作用中原則進行評估。當原則中的規則符合物件的中繼資料時、規則中的指示會決定StorageGRID 哪些動作需要複製及儲存該物件。

> 物件中繼資料並非由 ILM 規則管理。相反地、物件中繼資料會儲存在Cassandra資料庫的中繼資料儲存區中。每個站台會自動維護三個物件中繼資料複本、以保護資料免於遺失。

ILM規則的元素

ILM規則有三個元素：

- 篩選條件：規則的基本和進階篩選條件會定義規則所套用的物件。如果物件符合所有篩選條件、StorageGRID 則會套用規則、並建立規則放置說明中指定的物件複本。
- 放置指示：規則的放置指示會定義物件複本的編號、類型和位置。每個規則都可以包含一系列放置指示、以便隨著時間變更物件複本的編號、類型和位置。當一個放置時間到期時、下一個放置位置的指示會自動套用到下一個ILM評估。
- * 擷取行為 * ：規則的擷取行為可讓您選擇規則篩選的物件在擷取時的保護方式（當 S3 用戶端將物件儲存至網格時）。

ILM 規則篩選

建立ILM規則時、您可以指定篩選條件、以識別規則所套用的物件。

在最簡單的情況下、規則可能不會使用任何篩選器。任何不使用篩選器的規則都會套用至所有物件、因此它必須是ILM原則中的最後一個（預設）規則。預設規則會針對不符合其他規則中篩選條件的物件提供儲存指示。

- 基本篩選器可讓您將不同的規則套用至大型、不同的物件群組。這些篩選器可讓您將規則套用至特定租戶帳戶、特定 S3 儲存區或兩者。

  基本篩選器可讓您簡單地將不同規則套用至大量物件。例如、貴公司的財務記錄可能需要儲存以符合法規要求、而行銷部門的資料可能需要儲存以利日常營運。在為每個部門建立個別的租戶帳戶之後、或是將不同部門的資料分隔成不同的S3儲存區之後、您可以輕鬆建立適用於所有財務記錄的規則、以及適用於所有行銷資料的第二條規則。

- 進階篩選器可讓您精細控制。您可以建立篩選條件、根據下列物件內容來選取物件：
  - 擷取時間
  - 上次存取時間
  - 物件名稱的全部或部分（金鑰）
  - 位置限制（僅 S3 ）
  - 物件大小
  - 使用者中繼資料
  - 物件標籤（僅限 S3 ）

您可以根據非常特定的條件篩選物件。例如、醫院成像部門儲存的物件、可能會在使用時間少於30天且之後不常使用時頻繁使用、而含有病患就診資訊的物件、則可能需要複製到醫療網路總部的帳單部門。您可以建立篩選器、根據物件名稱、大小、S3物件標記或任何其他相關準則來識別每種物件類型、然後建立個別的規則來適當地儲存每組物件。

您可以視需要在單一規則中合併篩選條件。例如、行銷部門可能想要以不同於廠商記錄的方式來儲存大型映像檔、而人力資源部門可能需要將人員記錄集中儲存在特定地理區域和原則資訊中。在這種情況下、您可以建立規則、依租戶帳戶進行篩選、以將記錄與每個部門區隔、同時在每個規則中使用篩選器來識別規則所套用的特定物件類型。

放置指示可決定物件資料的儲存位置、時間及方式。ILM規則可以包含一或多個放置指示。每項放置指示均適用於單一時間段。

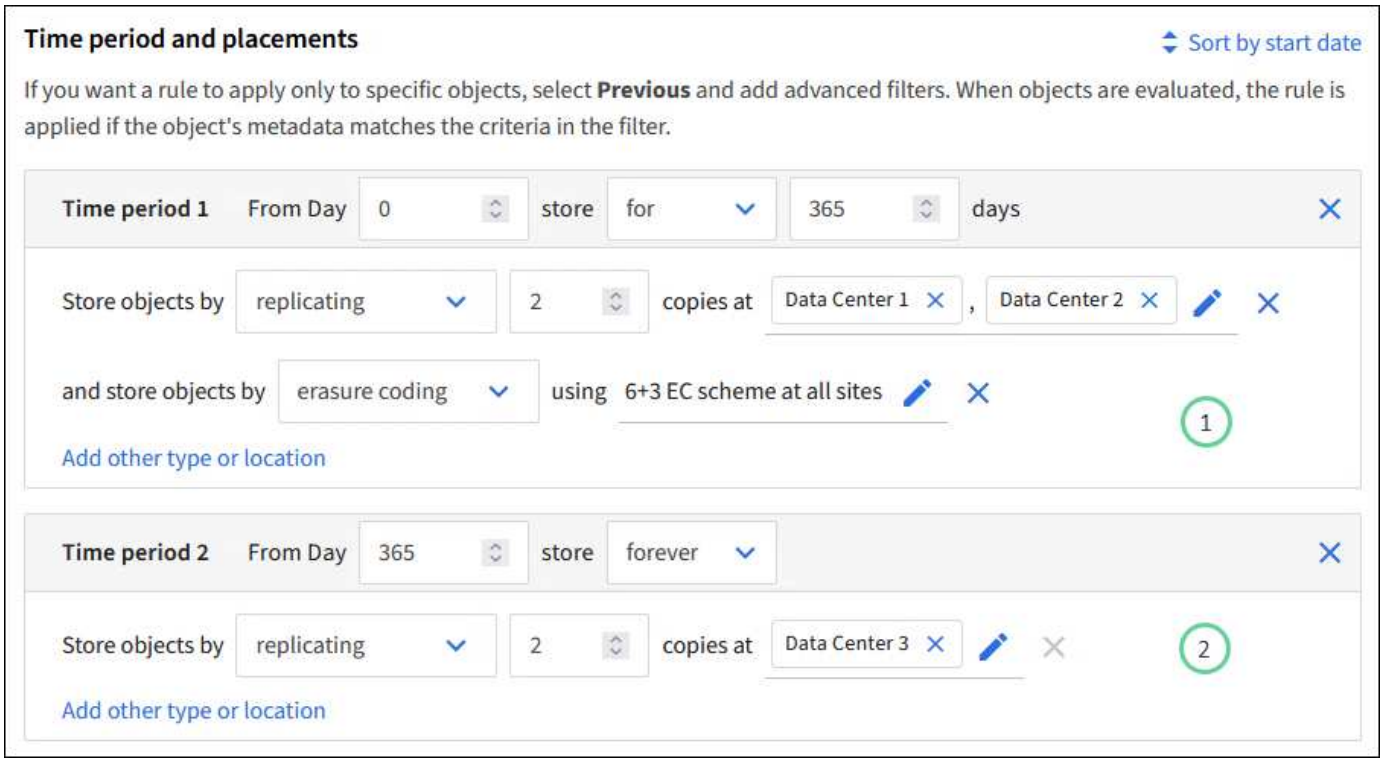
建立放置指示時：

- 您可以先指定參考時間、以決定放置指示的開始時間。參考時間可能是指：擷取物件、存取物件、版本控制物件變成非目前物件、或是使用者定義的時間。
- 接下來、您可以指定套用位置的時間、相對於參考時間。例如、相對於擷取物件的時間、放置位置可能從第0天開始、持續365天。
- 最後、您可以指定複本類型（複寫或銷毀編碼）、以及複本的儲存位置。例如、您可能想要在兩個不同站台儲存兩個複寫複本。

每個規則可定義單一時段的多個刊登位置、以及不同時段的不同刊登位置。

- 若要在單一期間內將物件放置在多個位置、請選取 * 新增其他類型或位置 * 、以在該期間新增多行。
- 若要將物件放置在不同時間週期的不同位置、請選取 * 新增其他時間週期 * 以新增下一個時間週期。然後、在期間內指定一或多行。

此範例顯示在「建立 ILM 規則」精靈的「定義放置位置」頁面上的兩個放置指示。



第一個放置指令 (1) 針對第一年有兩行：

- 第一行會在兩個資料中心站台建立兩個複寫的物件複本。
- 第二行使用所有資料中心站台建立 6+3 銷毀編碼複本。

第二項安置指示 (2) 會在一年後建立兩份副本，並永久保留這些副本。

當您定義規則的放置指示集時、必須確保至少有一個放置指示從第0天開始、且您定義的時間週期之間沒有任何落差、 最後的放置指示會持續執行、直到您不再需要任何物件複本為止。

當規則中的每個時間段到期時、將會套用下一個時間段的內容放置指示。系統會建立新的物件複本、並刪除任何不需要的複本。

ILM 規則擷取行為

擷取行為可控制物件複本是否立即根據規則中的指示放置、或是是否製作了過渡複本、並於稍後套用放置指示。下列擷取行為適用於ILM規則：

- 平衡：StorageGRID 在擷取時、會嘗試製作ILM規則中指定的所有複本；如果不可能、則會製作過渡複本、並將成功傳回給用戶端。ILM規則中指定的複本會盡可能製作。
- 嚴格：ILM規則中指定的所有複本都必須在成功傳回用戶端之前完成。
- * 雙重承諾 * ： StorageGRID 會立即製作物件的臨時複本、並將成功傳回用戶端。在ILM規則中指定的複本會盡可能製作。

相關資訊

- "擷取選項"
- "擷取選項的優點、缺點和限制"
- "一致性與 ILM 規則如何互動、以影響資料保護"

ILM規則範例

以 ILM 規則為例、可以指定下列項目：

- 僅套用至屬於 Tenant A. 的物件
- 為這些物件製作兩個複寫複本、並將每個複本儲存在不同的站台上。
- 保留這兩個複本「永遠」、表示 StorageGRID 不會自動刪除它們。相反地StorageGRID 、在用戶端刪除要求刪除這些物件之前、或是在庫位生命週期到期之前、將會保留這些物件。
- 使用平衡選項來擷取行為：只要租戶 A 將物件儲存至 StorageGRID 、就會套用雙站台放置指示、除非無法立即製作兩個必要的複本。

  例如、如果租戶A儲存物件時無法連線站台2、StorageGRID 則會在站台1的儲存節點上製作兩份臨時複本。一旦網站2推出、StorageGRID 就會在該網站上製作所需的複本。

相關資訊

- "什麼是儲存池"
- "什麼是雲端儲存池"

在 StorageGRID 中存取建立 ILM 規則精靈

ILM規則可讓您管理物件資料隨時間的放置。若要建立 ILM 規則、請使用建立 ILM 規則精靈。

如果您要建立原則的預設 ILM 規則、請"建立預設 ILM 規則的指示"改用。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 如果您想要指定此規則適用的租戶帳戶、您可以擁有"租戶帳戶權限"或知道每個帳戶的帳戶 ID 。
- 如果您希望規則根據上次存取時間中繼資料篩選物件、則必須由 S3 儲存區啟用上次存取時間更新。
- 您已設定要使用的任何雲端儲存池。請參閱。 "建立雲端儲存資源池"
- 您熟悉"擷取選項"。
- 如果您需要建立與 S3 物件鎖定搭配使用的相容規則，您就熟悉了"S3物件鎖定需求"。
- 或者，您已經觀看了影片：

  ILM 規則概述

關於這項工作

建立ILM規則時：

- 請考慮StorageGRID 使用此系統的拓撲和儲存組態。
- 思考您要製作的物件複本類型（複寫或刪除編碼）、以及每個物件所需的複本數量。
- 判斷哪些類型的物件中繼資料用於連接StorageGRID 到該系統的應用程式。ILM規則會根據物件的中繼資料來篩選物件。
- 請思考您希望物件複本隨時間放置在何處。
- 決定要使用的擷取選項（平衡、嚴格或雙重認可）。

步驟

1. 選擇* ILM > Rules *。
2. 選擇* Create （建立）。"步驟 1 （輸入詳細資料）"將顯示「建立 ILM 規則」精靈的。

輸入 **StorageGRID ILM** 規則的詳細資訊和篩選條件

「建立 ILM 規則」精靈的 * 輸入詳細資料 * 步驟可讓您輸入規則的名稱和說明、並定義規則的篩選條件。

輸入規則的說明和定義篩選是選擇性的。

關於這項工作

在對照評估物件"ILM 規則"時、 StorageGRID 會將物件中繼資料與規則的篩選器進行比較。如果物件中繼資料符合所有篩選條件、StorageGRID 則使用規則放置物件。您可以設計規則以套用至所有物件、也可以指定基本篩選條件、例如一個或多個租戶帳戶或庫位名稱、或是進階篩選條件、例如物件的大小或使用者中繼資料。

步驟

1. 在*名稱*欄位中輸入規則的唯一名稱。
2. （可選）在* Description（說明）*字段中輸入規則的簡短說明。

   您應該說明規則的用途或功能、以便日後辨識規則。

3. 您也可以選擇一個或多個 S3 租戶帳戶、以套用此規則。如果此規則適用於所有租戶、請將此欄位留白。

   如果您沒有「根目錄」存取權限或「浮動授權帳戶」權限、則無法從清單中選取「浮動授權」。請改為輸入租戶ID、或輸入多個ID作為以逗號分隔的字串。

4. 您也可以選擇指定此規則適用的 S3 儲存區。

   如果選擇 * 套用至所有儲存庫 *（預設）、則規則會套用至所有 S3 儲存區。

5. 對於 S3 租戶、您可以選擇 * 是 * 、將規則僅套用至已啟用版本設定的 S3 儲存區中較舊的物件版本。

   如果您選擇 * 是 * 、「非目前時間」將會在中自動選取作為參考時間"建立 ILM 規則精靈的步驟 2"。

   > 非目前時間僅適用於啟用版本設定的儲存區中的 S3 物件。請參閱"Pucket 作業、PuttBucketVersion作業"和"使用S3物件鎖定來管理物件"。

   您可以使用此選項來篩選非目前物件版本、以降低版本控制物件的儲存影響。請參閱。 "範例4：S3版本化物件的ILM規則和原則"

6. 或者、選取 * 新增進階篩選器 * 以指定其他篩選器。

   如果您未設定進階篩選、則規則會套用至符合基本篩選條件的所有物件。如需進階篩選的詳細資訊，請參閱在ILM規則中使用進階篩選器和[指定多種中繼資料類型和值]。

7. 選擇*繼續*。"步驟 2 （定義放置位置）"將顯示「建立 ILM 規則」精靈的。

在ILM規則中使用進階篩選器

進階篩選功能可讓您建立僅套用至特定物件的ILM規則、以其中繼資料為基礎。為規則設定進階篩選時、您可以選取要比對的中繼資料類型、選取運算子、然後指定中繼資料值。評估物件時、ILM規則僅會套用至具有符合進階篩選之中繼資料的物件。

下表顯示可在進階篩選器中指定的中繼資料類型、可用於每種中繼資料類型的運算子、以及預期的中繼資料值。

中繼資料類型	支援的運算子	中繼資料值
擷取時間	• 是 • 不是 • 之前 • 已開啟或之前 • 是之後的 • 開啟或之後	擷取物件的時間和日期。 • 注意： * 若要在啟動新的 ILM 原則時避免資源問題、您可以在任何可能變更大量現有物件位置的規則中使用「擷取時間」進階篩選器。將「擷取時間」設定為大於或等於新原則生效的大約時間、以確保現有物件不會不必要地移動。

中繼資料類型	支援的運算子	中繼資料值
金鑰	• 等於 • 不等於 • 包含 • 不包含 • 從開始 • 不從開始 • 結尾為 • 不以結束	全部或部分唯一 S3 物件金鑰。 例如、您可能想要比對結尾為或開頭為 `test-object/`的物件 `.txt`。
上次存取時間	• 是 • 不是 • 之前 • 已開啟或之前 • 是之後的 • 開啟或之後	上次擷取物件的時間和日期（讀取或檢視）。 • 注意： * 如果您計畫"使用上次存取時間"做為進階篩選器、則必須為 S3 儲存區啟用上次存取時間更新。
位置限制（僅 S3 ）	• 等於 • 不等於	建立S3儲存區的區域。使用* ILM > regions *來定義顯示的區域。 注意： us-east-1 的值將匹配在 us-east-1 區域建立的儲存桶中的物件以及未指定區域的儲存桶中的物件。看"配置 S3 區域" 。
物件大小	• 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於	物件的大小。 銷毀編碼最適合大於1 MB的物件。請勿對小於 200 KB 的物件使用抹除編碼、以避免管理非常小的銷毀編碼片段所造成的負擔。

中繼資料類型	支援的運算子	中繼資料值
使用者中繼資料	• 包含 • 結尾為 • 等於 • 存在 • 從開始 • 不包含 • 不以結束 • 不等於 • 不存在 • 不從開始	金鑰值配對、其中 * 使用者中繼資料名稱 * 為關鍵字、 * 中繼資料值 * 為值。 例如、若要篩選具有使用者中繼資料的物件 `color=blue`、請指定 `color` * 使用者中繼資料名稱 * 、運算子和 `blue` * 中繼資料 `equals`值 * 。 • 注意： * 使用者中繼資料名稱不區分大小寫；使用者中繼資料值區分大小寫。
物件標籤（僅限 S3 ）	• 包含 • 結尾為 • 等於 • 存在 • 從開始 • 不包含 • 不以結束 • 不等於 • 不存在 • 不從開始	金鑰值配對、其中 * 物件標籤名稱 * 是金鑰、 * 物件標籤值 * 是值。 例如，若要篩選物件標記為的物件 `Image=True`，請指定 `Image` * 物件標記名稱 * 、運算子及 `True` * 物件標記值 * `equals` 。 *附註：*物件標籤名稱和物件標籤值區分大小寫。您必須輸入與為物件定義的項目完全相同的項目。

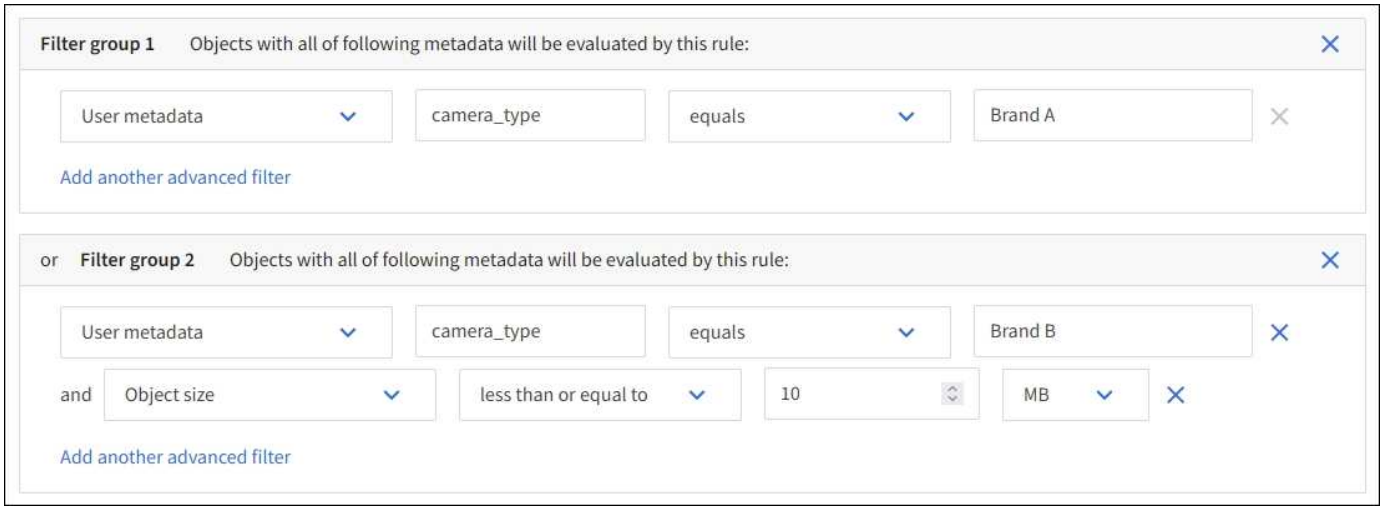
指定多種中繼資料類型和值

定義進階篩選時、您可以指定多種中繼資料類型和多個中繼資料值。例如、如果您想要規則比對大小介於 10 MB 和 100 MB 之間的物件、請選取 * 物件大小 * 中繼資料類型、然後指定兩個中繼資料值。

- 第一個中繼資料值會指定大於或等於10 MB的物件。
- 第二個中繼資料值會指定小於或等於100 MB的物件。

使用多個項目可讓您精確控制要比對的物件。在下列範例中、規則會套用至將 Brand A 或 Brand B 做為 camera

類型使用者中繼資料值的物件。不過、此規則僅適用於小於10 MB的Brand B物件。



定義 **StorageGRID ILM** 規則的放置說明

「建立 ILM 規則」精靈的 * 定義放置位置 * 步驟可讓您定義放置指示、以決定物件的儲存時間、複本類型（複寫或刪除編碼）、儲存位置及複本數量。

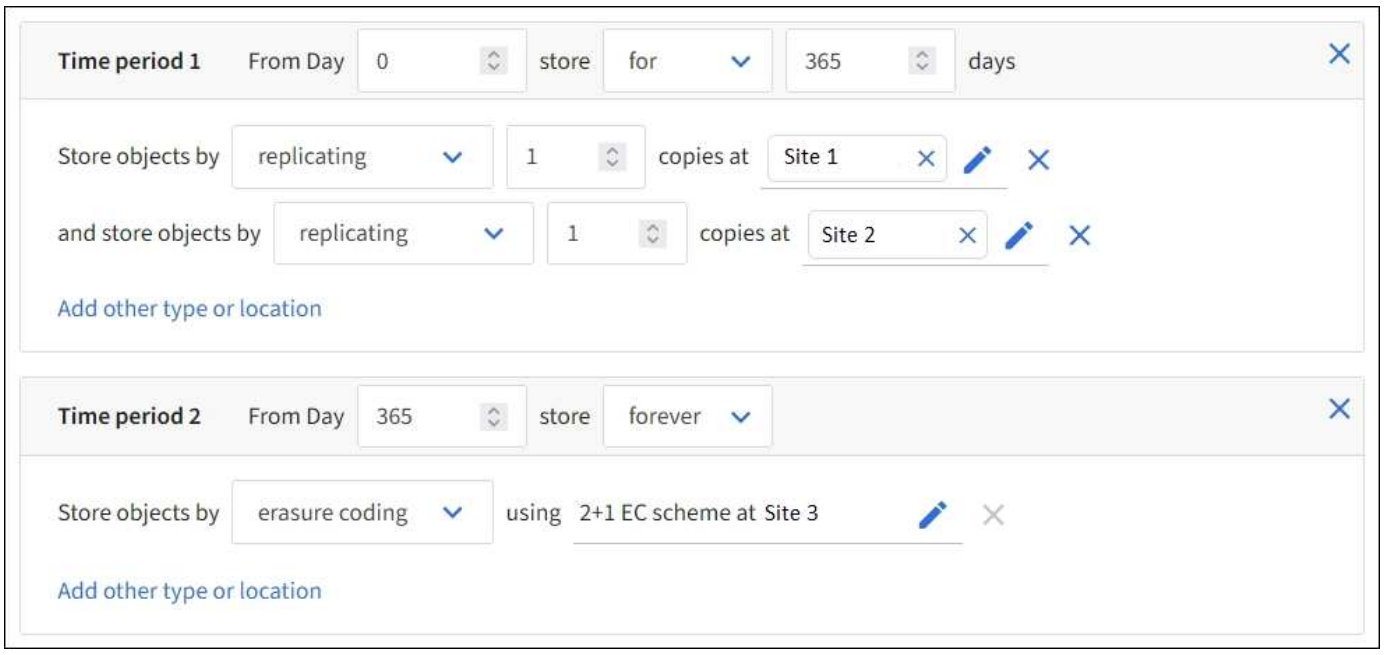
所示的螢幕擷取畫面為範例。您的結果可能會因 StorageGRID 版本而異。

關於這項工作

ILM規則可以包含一或多個放置指示。每項放置指示均適用於單一時間段。當您使用多個指示時、時間段必須是連續的、且至少必須在第0天開始一項指示。指令可以永遠繼續、或直到您不再需要任何物件複本為止。

如果您想要建立不同類型的複本、或在該期間使用不同的位置、每個放置指示都可以有多行。

在此範例中、 ILM 規則會在站台 1 中儲存一個複寫複本、並在站台 2 中儲存第一年的複寫複本。一年後、便會製作2+1銷毀編碼的複本、並僅儲存於一個站台。



步驟

1. 對於 * 參考時間 * 、請選取在計算放置指示的開始時間時要使用的時間類型。

選項	說明
擷取時間	擷取物件的時間。
上次存取時間	上次擷取（讀取或檢視）物件的時間。 若要使用此選項、必須為 S3 儲存區啟用上次存取時間的更新。請參閱 "在 ILM 規則中使用上次存取時間"。
使用者定義的建立時間	使用者定義中繼資料中指定的時間。
非目前時間	如果您在中針對「僅將此規則套用至較舊的物件版本（在啟用版本設定的 S3 儲存區中）？」問題選取 * 「是 * 」"建立 ILM 規則精靈的步驟 1"、則會自動選取「非目前時間」。

如果您想要建立 _ 相容 _ 規則、您必須選取 * 擷取時間 * 。請參閱 "使用S3物件鎖定來管理物件"。

2. 在「 * 期間與刊登位置 * 」區段中、輸入第一個時間週期的開始時間與持續時間。

例如、您可能想要指定第一年的物件儲存位置（ _ 從第 0 天儲存 365 天 _ ）。至少必須在第0天開始執行一項指示。

3. 若要建立複寫複本：

a. 從 * 依 * 儲存物件下拉式清單中、選取 * 複寫 * 。

b. 選取您要製作的份數。

如果您將複本數目變更為1、就會出現警告。ILM規則只會在任何時間段建立一個複寫複本、使資料有永久遺失的風險。請參閱 "為何不應使用單一複製複寫"。

若要避免風險、請執行下列一或多項操作：

- 增加期間的複本數量。
- 將複本新增至其他儲存池或雲端儲存池。
- 選擇 * 銷毀編碼 * 、而非 * 複製 * 。

如果此規則已為所有時間段建立多個複本、您可以安全地忽略此警告。

c. 在 * 複本於 * 欄位中、選取您要新增的儲存池。

如果您只指定一個儲存資源池、請注意StorageGRID 、在任何指定的儲存節點上、只能儲存物件的一個複製複本。如果您的網格包含三個儲存節點、而且您選取 4 做為複本數量、則只會製作三份複本？ #8212 ；每個儲存節點一份複本。

觸發「無法實現的ILM放置」警示、表示無法完全套用ILM規則。

如果您指定多個儲存資源池、請謹記下列規則：

- 複本數量不得大於儲存集區數量。
- 如果複本數量等於儲存資源池數量、則每個儲存資源池中會儲存一個物件複本。
- 如果複本數小於儲存集區的數量、則會在擷取站台儲存一個複本、然後系統會散佈其餘複本、以保持集區之間的磁碟使用率平衡、同時確保站台不會取得超過一個物件複本。
- 如果儲存資源池重疊（包含相同的儲存節點）、則物件的所有複本可能只會儲存在一個站台。因此、請勿指定「所有儲存節點」儲存池（ StorageGRID 11.6 以上版本）和其他儲存池。

4. 如果您要建立銷毀編碼複本：

   a. 從 * 依 * 儲存物件下拉式清單中、選取 * 銷毀編碼 * 。

   > ⓘ 銷毀編碼最適合大於1 MB的物件。請勿對小於 200 KB 的物件使用抹除編碼、以避免管理非常小的銷毀編碼片段所造成的負擔。

   b. 如果您未新增大於 200 KB 的物件大小篩選器、請選取 * 上一步 * 以返回步驟 1 。然後選擇 * 新增進階篩選器 * 、並將 * 物件大小 * 篩選器設定為任何大於 200 KB 的值。

   c. 選取您要新增的儲存資源池、以及您要使用的銷毀編碼配置。

      銷毀編碼複本的儲存位置包括抹除編碼配置的名稱、以及儲存池的名稱。

   可用的銷毀編碼配置受限於您所選儲存池中的儲存節點數量。在提供的方案旁邊會出現一個 `Recommended`徽章"最佳保護或最低的儲存負荷"。

5. （可選）：

   a. 選取 * 新增其他類型或位置 * 、在不同位置建立其他複本。

   b. 選取 * 新增其他時間週期 * 以新增不同的時間週期。

   > ⓘ 物件刪除是根據下列設定進行：
   >
   > - 物件會在最後一個時間週期結束時自動刪除、除非另一個時間週期以 * 永遠 * 結束。
   > - "貯體與租戶保留期間設定"即使 ILM 保留期間結束、物件也可能無法刪除、視情況而定。

6. 若要將物件儲存在雲端儲存資源池中：

   a. 在 * 依 * 儲存物件下拉式清單中、選取 * 複寫 * 。

   b. 選取 * 複本於 * 欄位、然後選取雲端儲存池。

      使用雲端儲存資源池時、請謹記下列規則：

      - 您無法在單一放置指示中選取多個雲端儲存池。同樣地、您也無法在相同的放置指示中選取雲端儲存池和儲存池。
      - 您只能在任何指定的Cloud Storage Pool中儲存物件的一份複本。如果您將*份數*設為2個以上、就會出現錯誤訊息。
      - 您無法在任何雲端儲存池中同時儲存多個物件複本。如果使用雲端儲存資源池的多個放置位置日期重疊、或同一放置位置的多行使用雲端儲存資源池、則會出現錯誤訊息。

- 您可以在將物件儲存為 StorageGRID 中的複寫或銷毀編碼複本的同時、將物件儲存在雲端儲存池中。不過、您必須在期間的放置指示中包含多行、才能指定每個位置的份數和類型。

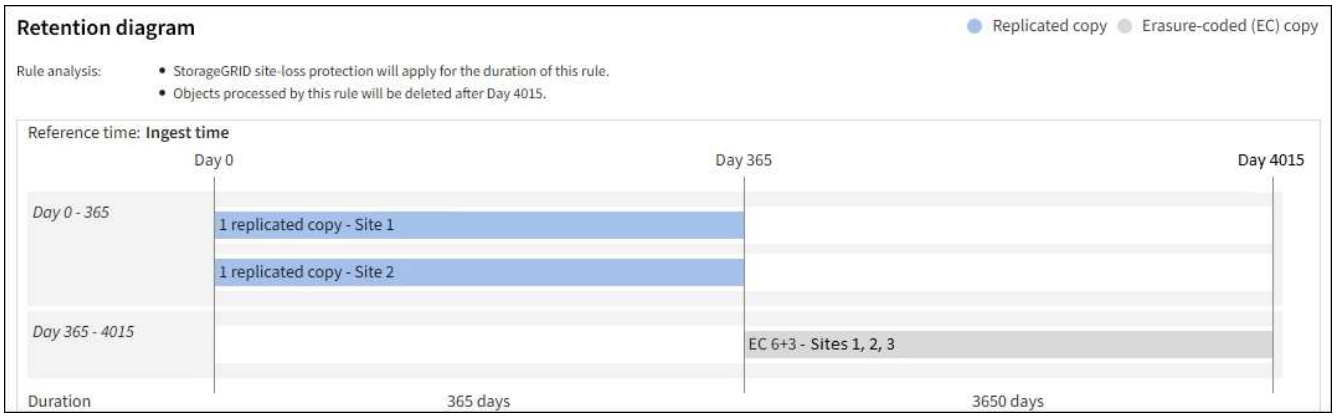
7. 在保留圖中、確認您的放置指示。

   在此範例中、 ILM 規則會在站台 1 中儲存一個複寫複本、並在站台 2 中儲存第一年的複寫複本。一年後、再加上 10 年後、將會在三個地點儲存 6+3 銷毀編碼複本。總共 11 年之後、物件將從 StorageGRID 中刪除。

   保留圖的規則分析區段說明：

   - StorageGRID 站台遺失保護將在本規則期間適用。
   - 此規則處理的物件將在第 4015 天之後刪除。

     請參閱 "啟用站台遺失保護。"



8. 選擇*繼續*。"步驟 3 （選擇擷取行為）"將顯示「建立 ILM 規則」精靈的。

在 **StorageGRID ILM** 規則中使用上次存取時間

您可以使用上次存取時間做為 ILM 規則的參考時間。例如、您可能想要保留過去三個月在本機儲存節點上檢視過的物件、同時將最近未檢視過的物件移至異地位置。如果您希望 ILM 規則僅套用至上次在特定日期存取的物件、也可以將上次存取時間用作進階篩選器。

關於這項工作

在 ILM 規則中使用上次存取時間之前、請先檢閱下列考量事項：

- 使用上次存取時間做為參考時間時、請注意變更物件的上次存取時間並不會觸發立即 ILM 評估。而是評估物件的放置位置、並在背景ILM評估物件時視需要移動物件。存取物件之後、可能需要兩週或更久的時間。

  根據上次存取時間建立 ILM 規則時、請將這段延遲納入考量、避免放置時間過短（少於一個月）。

- 將上次存取時間用作進階篩選器或參考時間時、您必須啟用 S3 儲存區的上次存取時間更新。您可以使用"租戶管理程式"或"租戶管理API"。

  根據預設、 S3 儲存區的上次存取時間更新會停用。

請注意、啟用上次存取時間更新可能會降低效能、尤其是在使用小型物件的系統中。效能影響的發生、是因為StorageGRID 每次擷取物件時、都必須使用新的時間戳記來更新物件。

下表摘要說明是否針對不同類型的要求、更新貯體中所有物件的上次存取時間。

申請類型	上次存取時間更新停用時、是否會更新上次存取時間	上次存取時間更新啟用時、是否會更新上次存取時間
要求擷取物件、其存取控制清單或其中繼資料	否	是的
要求更新物件的中繼資料	是的	是的
要求將物件從一個儲存區複製到另一個儲存區	• 否、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本
要求完成多部分上傳	是的、適用於組裝好的物件	是的、適用於組裝好的物件

選擇 **StorageGRID ILM** 規則的擷取行為

「建立 ILM 規則」精靈的 * 選取擷取行為 * 步驟可讓您選擇在此規則篩選的物件在擷取時如何受到保護。

關於這項工作

可以製作過渡複本、並將物件排入佇列、以便稍後進行ILM評估、也可以製作複本、以立即符合規則的放置指示。StorageGRID

步驟

1. 選取要使用的"擷取行為"。

   如需更多資訊、請參閱 "擷取選項的優點、缺點和限制"。

   如果規則使用下列其中一個位置、您就無法使用平衡或嚴格選項：

   - 第0天的雲端儲存資源池
   - 當規則使用使用使用者定義的建立時間做為參考時間時、即為雲端儲存池

   請參閱。 "範例5：嚴格擷取行為的ILM規則與原則"

2. 選擇* Create （建立）。

   ILM 規則即會建立。規則必須先新增至、並啟動該原則、才會生效"ILM原則"。

   若要檢視規則的詳細資料、請在 ILM 規則頁面上選取規則的名稱。

在 StorageGRID 中建立預設 ILM 規則

在建立ILM原則之前、您必須建立預設規則、將任何不符合其他規則的物件放入原則中。預設規則無法使用任何篩選器。它必須套用至所有租戶、所有貯體及所有物件版本。

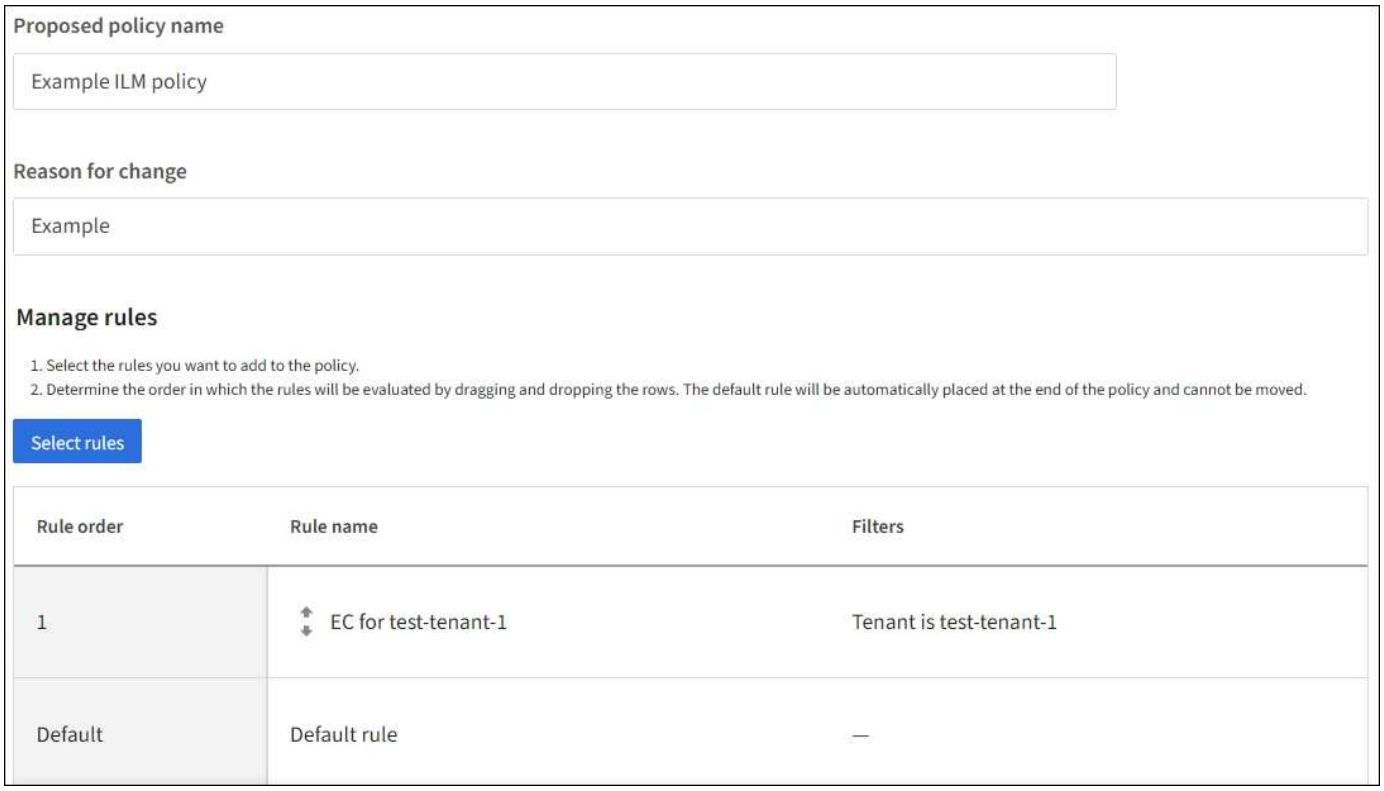
開始之前

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

關於這項工作

預設規則是 ILM 原則中最後要評估的規則、因此無法使用任何篩選器。預設規則的放置指示會套用至原則中其他規則不相符的任何物件。

在此範例原則中、第一個規則僅適用於屬於 test-租 戶 -1 的物件。最後一個預設規則會套用至屬於所有其他租戶帳戶的物件。



建立預設規則時、請謹記下列需求：

- 將預設規則新增至原則時、會自動將其設為最後一條規則。
- 預設規則無法使用任何基本或進階篩選器。
- 預設規則必須套用至所有物件版本。
- 預設規則應建立複寫複本。

> 請勿使用建立銷毀編碼複本的規則做為原則的預設規則。銷毀編碼規則應使用進階篩選器、以防止較小的物件遭到銷毀編碼。

- 一般而言、預設規則應該永遠保留物件。
- 如果您使用（或打算啟用）全域 S3 物件鎖定設定、則預設規則必須符合規定。

步驟

1. 選擇* ILM > Rules *。
2. 選擇* Create （建立）。

   隨即顯示 Create ILM Rule （建立 ILM 規則）精靈的步驟 1 （輸入詳細資料）。

3. 在 * 規則名稱 * 欄位中輸入規則的唯一名稱。
4. （可選）在* Description（說明）*字段中輸入規則的簡短說明。
5. 將 * 租戶帳戶 * 欄位保留空白。

   預設規則必須套用至所有租戶帳戶。

6. 保留「貯體名稱」下拉式選項為 * 適用於所有貯體 * 。

   預設規則必須套用至所有 S3 儲存區。

7. 對於「僅將此規則套用至較舊的物件版本（在啟用版本設定的 S3 儲存區中）」的問題、請保留預設答案 * 否 * ？
8. 請勿新增進階篩選器。

   預設規則無法指定任何篩選條件。

9. 選擇*下一步*。

   步驟 2 （定義放置位置）即會出現。

10. 針對「參考時間」、選取任何選項。

    如果您保留問題的預設答案 * 否 * ：「僅將此規則套用至舊版物件？」非目前時間不會包含在下拉式清單中。預設規則必須套用所有物件版本。

11. 指定預設規則的放置指示。
    - 預設規則應永遠保留物件。當您啟動新原則時、如果預設規則不會永久保留物件、就會出現警告。您必須確認這是您期望的行為。
    - 預設規則應建立複寫複本。

      請勿使用建立銷毀編碼複本的規則做為原則的預設規則。銷毀編碼規則應包含大於 200 kb* 進階篩選器的 * 物件大小（ MB ）、以防止較小的物件遭到銷毀編碼。

    - 如果您使用（或打算啟用）全域S3物件鎖定設定、則預設規則必須符合：
      - 它必須建立至少兩個複寫的物件複本、或一個銷毀編碼複本。
      - 這些複本必須存在於儲存節點上、且必須在放置說明中的每一行的整個期間內存在。
      - 物件複本無法儲存在雲端儲存池中。

- 至少一行放置指示必須從第 0 天開始、使用「擷取時間」做為參考時間。
- 至少一行放置指示必須為「永遠」。

12. 查看保留圖以確認您的放置指示。
13. 選擇*繼續*。

    出現步驟 3 （選擇擷取行為）。

14. 選取要使用的擷取選項、然後選取 * 建立 * 。

管理 ILM 原則

了解 StorageGRID 中的 ILM 原則

資訊生命週期管理（ILM）原則是一組依序排列的ILM規則、可決定StorageGRID 整個過程中、物件資料的管理方式。

> 如果ILM原則設定不正確、可能導致無法恢復的資料遺失。啟動ILM原則之前、請仔細檢閱ILM原則及其ILM規則、然後模擬ILM原則。請務必確認ILM原則是否正常運作。

預設 ILM 原則

當您安裝 StorageGRID 並新增站台時、系統會自動建立預設的 ILM 原則、如下所示：

- 如果您的網格包含一個站台、則預設原則會包含一個預設規則、用於複寫該站台每個物件的兩個複本。
- 如果您的網格包含多個站台、預設規則會在每個站台上複寫每個物件的一個複本。

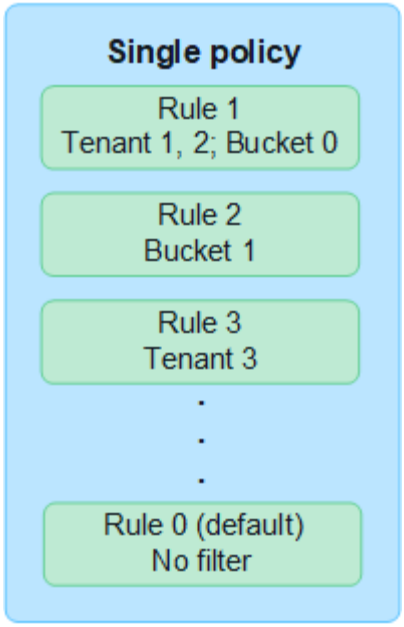
如果預設策略無法滿足您的儲存需求，您可以建立自己的規則和策略。看"建立 ILM 規則"和"建立ILM原則"。

一或多個使用中的 ILM 原則？

您一次可以有一個或多個使用中的 ILM 原則。

單一原則

如果您的網格將使用簡單的資料保護方案、其中只有少數特定租戶和特定貯體規則、請使用單一主動式 ILM 原則。ILM 規則可以包含篩選器、以管理不同的貯體或租戶。



當您只有一個原則且租戶的需求變更時、您必須建立新的 ILM 原則或複製現有原則、以套用變更、模擬、然後啟動新的 ILM 原則。變更 ILM 原則可能會導致物件移動、可能需要數天的時間、並導致系統延遲。

多個原則

若要為租戶提供不同的服務品質選項、您一次可以有多個作用中原則。每個原則都可以管理特定租戶、 S3 貯體和物件。當您為一組特定租戶或物件套用或變更一個原則時、套用至其他租戶和物件的原則不會受到影響。

ILM 原則標籤

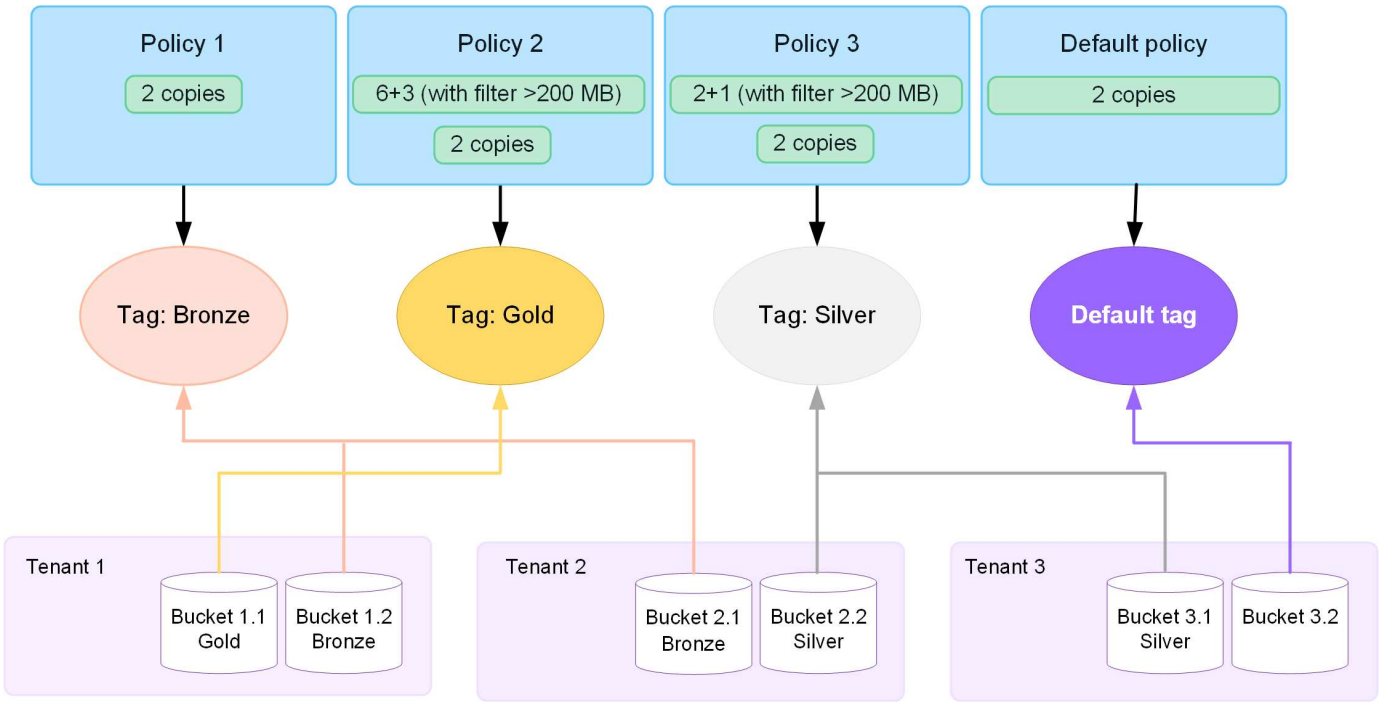
如果您想要讓租戶輕鬆地在每個貯體的多個資料保護原則之間切換、請使用多個 ILM 原則搭配 _ILM 原則標籤 _ 。您可以將每個 ILM 原則指派給標記、然後將貯體標記為標記、以將原則套用至該貯體。您只能在 S3 儲存區上設定 ILM 原則標籤。

例如、您可能會有三個標記、分別命名為「金」、「銀」和「銅」。您可以根據原則儲存物件的時間和位置、將 ILM 原則指派給每個標記。租戶可以透過標記其貯體來選擇要使用的原則。標記為 Gold 的貯體是由 Gold 原則管理、並獲得 Gold 等級的資料保護與效能。

你可以"最多可建立 10 個策略標籤"為您的網格。

預設 ILM 原則標籤

安裝 StorageGRID 時會自動建立預設的 ILM 原則標籤。每個網格都必須有一個作用中原則指派給預設標籤。預設原則適用於任何未標配的 S3 儲存區。



ILM原則如何評估物件？

主動式 ILM 原則可控制物件的放置、持續時間和資料保護。

當用戶端將物件儲存至 StorageGRID 時、會根據原則中的一組已排序的 ILM 規則來評估物件、如下所示：

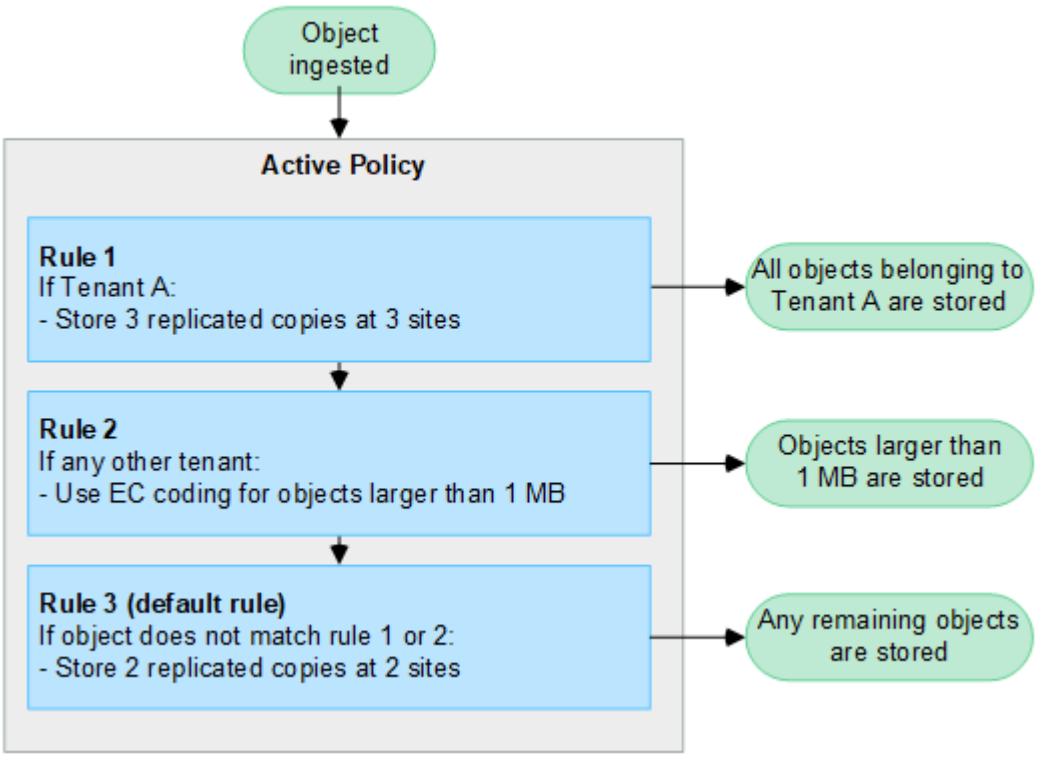
1. 如果原則中第一個規則的篩選器符合物件、則會根據該規則的擷取行為擷取物件、並根據該規則的放置指示加以儲存。
2. 如果第一個規則的篩選條件與物件不符、則會根據原則中的每個後續規則來評估物件、直到進行符合為止。
3. 如果沒有符合物件的規則、則會套用原則中預設規則的擷取行為和放置指示。預設規則是原則中的最後一個規則。預設規則必須套用至所有租戶、所有 S3 貯體和所有物件版本、而且不能使用任何進階篩選器。

ILM原則範例

舉例來說、 ILM 原則可能包含三個 ILM 規則、其中指定下列項目：

- * 規則 1 ：租戶 A* 的複寫複本
  - 比對屬於 Tenant A. 的所有物件
  - 將這些物件儲存為三個站台的三個複寫複本。
  - 屬於其他租戶的物件不符合規則 1 、因此會根據規則 2 進行評估。
- * 規則 2 ： 1 MB* 以上物件的銷毀編碼
  - 比對其他租戶的所有物件、但只有在物件大於 1 MB 時才會比對。這些較大的物件使用6+3銷毀編碼儲存在三個站台。
  - 不符合 1 MB 或更小的物件、因此會根據規則 3 來評估這些物件。
- * 規則 3 ： 2 份複本 2 個資料中心 * （預設）
  - 是原則中的最後一個和預設規則。不使用篩選器。

。為規則 1 或規則 2 不相符的所有物件建立兩個複寫複本（不屬於租戶 A 且小於 1 MB 的物件）。



什麼是作用中和非作用中原則？

每個 StorageGRID 系統必須至少有一個主動式 ILM 原則。如果您想要有多個使用中的 ILM 原則、請建立 ILM 原則標籤、並將原則指派給每個標籤。租戶接著將標籤套用至 S3 貯體。預設原則會套用至未指派原則標記的貯體中所有物件。

當您第一次建立 ILM 原則時、請選取一或多個 ILM 規則、然後依特定順序排列。模擬原則以確認其行為之後、您就會將其啟動。

當您啟動一個 ILM 原則時、 StorageGRID 會使用該原則來管理所有物件、包括現有物件和新擷取的物件。在新原則中實作ILM規則時、現有物件可能會移至新位置。

如果您一次啟動多個 ILM 原則、且租戶將原則標籤套用到 S3 貯體、則每個貯體中的物件都會根據指派給標籤的原則進行管理。

StorageGRID 系統會追蹤已啟用或停用之原則的歷程記錄。

建立**ILM**原則的考量

- 只能在測試系統中使用系統提供的原則「基準 2 複本」原則。對於 StorageGRID 11.6 及更早版本、本原則中的「製作 2 份複本」規則會使用「所有儲存節點」儲存池、其中包含所有站台。如果StorageGRID 您的作業系統有多個站台、則一個物件的兩份複本可能會放在同一個站台上。

  安裝 StorageGRID 11.6 及更早版本時、系統會自動建立 All Storage Nodes 儲存池。如果您升級至較新版本的 StorageGRID 、則所有儲存節點集區仍會存在。如果您以新安裝方式安裝 StorageGRID 11.7 或更新版本、則不會建立所有儲存節點集區。

- 設計新原則時、請考量可能擷取到網格的所有不同類型物件。請確定原則包含符合的規則、並視需要放置這

些物件。

- 盡量簡化ILM原則。這可避免在StorageGRID 物件資料不受預期保護的情況下、隨著時間而對該系統進行變更時、發生潛在的危險情況。
- 請確定原則中的規則順序正確。當原則啟動時、新物件和現有物件會依照列出的順序進行評估、從上方開始。例如、如果原則中的第一個規則符合某個物件、則任何其他規則都不會評估該物件。
- 每個 ILM 原則的最後一個規則是預設的 ILM 規則、無法使用任何篩選器。如果某個物件未被其他規則比對、則預設規則會控制該物件放置的位置、以及保留多久。
- 在啟動新原則之前、請先檢閱原則對現有物件放置位置所做的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、導致暫時性資源問題。

在 **StorageGRID** 中建立 **ILM** 原則

建立一或多個 ILM 原則以符合您的服務品質要求。

有一個主動式 ILM 原則可讓您將相同的 ILM 規則套用至所有租戶和貯體。

擁有多個主動式 ILM 原則可讓您將適當的 ILM 規則套用至特定租戶和貯體、以滿足多項服務品質要求。

建立**ILM**原則

關於這項工作

在建立自己的原則之前、請確認"預設 ILM 原則"不符合您的儲存需求。

> 在測試系統中、只能使用系統提供的原則、 2 份複本原則（適用於單一站台網格）或每個站台 1 份複本（適用於多站台網格）。對於 StorageGRID 11.6 及更早版本、此原則中的預設規則會使用「所有儲存節點」儲存池、其中包含所有站台。如果StorageGRID 您的作業系統有多個站台、則一個物件的兩份複本可能會放在同一個站台上。

> 如果"全域 S3 物件鎖定設定已啟用"，您必須確保 ILM 原則符合已啟用 S3 Object Lock 的儲存桶的要求。在本節中，請依照提及已啟用 S3 Object Lock 的說明進行操作。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。
- 您是否已"已建立 ILM 規則"啟用 S3 物件鎖定。

S3 物件鎖定未啟用

- 您已"已建立 ILM 規則"想要新增至原則。您可以視需要儲存原則、建立其他規則、然後編輯原則以新增規則。
- 您的"已建立預設ILM規則"篩選器不包含任何篩選器。

S3 物件鎖定已啟用

- "全域 S3 物件鎖定設定已啟用" 用於 StorageGRID 系統。
- 您已"已建立相容且不符合法規的 ILM 規則"想要新增至原則。您可以視需要儲存原則、建立其他規則、然後編輯原則以新增規則。
- 您擁有"已建立預設ILM規則"符合法規的原則。

- 或者，您已經觀看了影片：

ILM 策略概述

另請參閱"使用 ILM 原則"。

步驟

1. 選擇* ILM > Policies *。

   如果啟用全域 S3 物件鎖定設定、則「 ILM 原則」頁面會指出哪些 ILM 規則符合規定。

2. 決定您要如何建立 ILM 原則。

   建立新原則

   a. 選取 * 建立原則 * 。

   複製現有原則

   a. 選中要開始的策略的複選框，然後選擇 **Clone** 。

   編輯現有原則

   a. 如果原則處於非作用中狀態、您可以加以編輯。選取您要開始使用的非作用中原則核取方塊、然後選取 * 編輯 * 。

3. 在 * 原則名稱 * 欄位中、輸入原則的唯一名稱。
4. 或者、在 * 變更理由 * 欄位中、輸入您建立新原則的原因。
5. 若要將規則新增至原則、請選取 * 選取規則 * 。選取規則名稱以檢視該規則的設定。

   如果您要複製原則：

   - 您正在複製的原則所使用的規則會被選取。
   - 如果您正在複製的原則使用的任何規則都沒有非預設規則的篩選器、系統會提示您移除其中一個規則以外的所有規則。

- 如果預設規則使用篩選器、系統會提示您選取新的預設規則。
- 如果預設規則不是最後一個規則、您可以將規則移至新原則的結尾。

S3 物件鎖定未啟用

a. 為原則選取一個預設規則。若要建立新的預設規則、請選取 * ILM 規則頁面 * 。

   預設規則會套用至任何不符合原則中其他規則的物件。預設規則無法使用任何篩選條件、而且一律是最後評估的。

   > 請勿使用「製作 2 份複本」規則做為原則的預設規則。「製作2份複本」規則使用單一儲存資源池「所有儲存節點」、其中包含所有站台。如果StorageGRID 您的作業系統有多個站台、則一個物件的兩份複本可能會放在同一個站台上。

S3 物件鎖定已啟用

a. 為原則選取一個預設規則。若要建立新的預設規則、請選取 * ILM 規則頁面 * 。

   規則清單僅包含符合規定且不使用任何篩選器的規則。

   > 請勿使用「製作 2 份複本」規則做為原則的預設規則。「製作2份複本」規則使用單一儲存資源池「所有儲存節點」、其中包含所有站台。如果您使用此規則、一個物件的多個複本可能會放置在同一個站台上。

b. 如果您在不符合標準的 S3 儲存區中的物件需要不同的「預設」規則、請選取 * 包含不含不符合標準 S3 儲存區篩選器的規則 * 、然後選取不使用篩選器的不符合標準規則。

   例如、您可能想要使用雲端儲存池、將物件儲存在未啟用 S3 物件鎖定的儲存區中。

   > 您只能選取一個不符合規定的規則、而不使用篩選器。

另請參閱"範例7：S3物件鎖定的符合ILM原則"。

6. 完成選取預設規則後、請選取 * 繼續 * 。
7. 針對「其他規則」步驟、選取您要新增至原則的任何其他規則。這些規則至少使用一個篩選器（租戶帳戶、貯體名稱、進階篩選器或非目前參考時間）。然後選擇 * 選擇 * 。

   「建立原則」視窗現在會列出您選取的規則。預設規則結尾為、其上方則為其他規則。

   如果啟用 S3 物件鎖定、而且您也選取了不相容的「預設」規則、則該規則會新增為原則中的第二對最後一條規則。

   > 如果有任何規則無法永遠保留物件、則會出現警告。當您啟動此原則時、必須確認在預設規則的放置指示到期時、您希望 StorageGRID 刪除物件（除非貯體生命週期將物件保留較長的時間）。

8. 拖曳非預設規則的列、以決定評估這些規則的順序。

您無法移動預設規則。如果啟用 S3 物件鎖定、如果選取不符合的「預設」規則、您也無法移動該規則。

> 您必須確認ILM規則的順序正確。當原則啟動時、新物件和現有物件會依照列出的順序進行評估、從上方開始。

9. 視需要選取 * 選取規則 * 以新增或移除規則。
10. 完成後、請選取*「Save（儲存）」*。
11. 重複這些步驟以建立其他 ILM 原則。
12. 模擬ILM原則。您應該一律在啟動原則之前先模擬原則、以確保其正常運作。

模擬原則

在啟動原則並將其套用至正式作業資料之前、先模擬測試物件的原則。

開始之前

您知道要測試的每個物件的 S3 貯體 / 物件金鑰。

步驟

1. 使用 S3 用戶端或"S3 主控台"、擷取測試每個規則所需的物件。
2. 在「 ILM 原則」頁面上、選取原則的核取方塊、然後選取 * 模擬 * 。
3. 在 * 物件 * 欄位中、輸入測試物件的 S3 `bucket/object-key` 。例如 `bucket-01/filename.png` ：。
4. 如果啟用 S3 版本設定、可選擇在 * 版本 ID* 欄位中輸入物件的版本 ID 。
5. 選擇*模擬*。
6. 在 Simulation 結果區段中、確認每個物件都符合正確的規則。
7. 若要判斷哪個儲存池或銷毀編碼設定檔有效、請選取相符規則的名稱、以移至規則詳細資料頁面。

> 檢閱現有複寫和刪除編碼物件位置的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、導致暫時性資源問題。

結果

對策略規則的任何修改都會反映在模擬結果中，並顯示新的匹配項和先前的匹配項。「模擬策略」視窗會保留您測試的物件，直到您針對模擬結果清單中的每個物件選擇 **Clear all** 或移除圖示 ✕。

相關資訊

"ILM 原則模擬範例"

啟動原則

當您啟動單一新的 ILM 原則時、現有物件和新擷取的物件都會由該原則管理。當您啟動多個原則時、指派給儲存區的 ILM 原則標記會決定要管理的物件。

啟動新原則之前：

1. 模擬原則、確認其運作方式符合您的預期。
2. 檢閱現有複寫和刪除編碼物件位置的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、

導致暫時性資源問題。

ILM原則中的錯誤可能導致無法恢復的資料遺失。

關於這項工作

當您啟動ILM原則時、系統會將新原則發佈至所有節點。不過、在所有網格節點都可以接收新原則之前、新的作用中原則可能不會實際生效。在某些情況下、系統會等待實作新的作用中原則、以確保網格物件不會意外移除。具體而言：

- 如果您進行的原則變更 * 會增加資料備援或耐用度 * 、則這些變更會立即實作。例如、如果您啟動包含三份複本規則的新原則、而非雙份複本規則、則該原則將會立即實作、因為它會增加資料備援。
- 如果您進行的原則變更 * 可能會降低資料備援或耐用度 * 、則這些變更將不會實作、直到所有網格節點都可用為止。例如、如果您啟動使用雙份複本規則而非三份複本規則的新原則、則新原則會出現在「作用中原則」索引標籤中、但直到所有節點都已上線且可供使用為止、該原則才會生效。

步驟

請依照下列步驟啟動一或多個原則：

啟動一個原則

如果您只有一個作用中原則、請遵循下列步驟。如果您已經有一個或多個作用中原則、而且您正在啟動其他原則、請依照步驟來啟動多個原則。

1. 當您準備好啟動原則時、請選取 * ILM * > * 原則 * 。

   或者、您也可以從「 * ILM * > * 原則標記 * 」頁面啟動單一原則。

2. 在 " 原則 " 索引標籤上 , 選取您要啟動之原則的核取方塊 , 然後選取 **Activate** 。
3. 請遵循適當步驟：
   - 如果出現警告訊息提示您確認要啟動原則、請選取 * 確定 * 。
   - 如果出現包含原則詳細資料的警告訊息：
     i. 檢閱詳細資料、確保原則能如預期般管理資料。
     ii. 如果預設規則儲存物件的天數有限、請檢閱保留圖表、然後在文字方塊中輸入該天數。
     iii. 如果預設規則會永久儲存物件、但有一或多個其他規則的保留限制、請在文字方塊中輸入 * 是 * 。
     iv. 選取 * 啟動原則 * 。

啟動多個原則

要啟動多個策略，您必須建立策略標籤並為每個標籤指派一個策略。您最多可以為網格建立 10 個策略標籤。

當使用多個策略標籤時，如果租戶經常將策略標籤重新指派給儲存桶，則網格效能可能會受到影響。如果您有不受信任的租戶，請考慮僅使用預設策略標籤。

1. 選取 * ILM * > * 原則標記 * 。
2. 選擇* Create （建立）。
3. 在 [建立原則標記] 對話方塊中，輸入標記名稱，並選擇性地輸入標記的描述。

租戶可以看到標籤名稱和說明。選擇可協助租戶在選擇原則標籤指派給他們的貯體時、做出明智決策的值。例如、如果指派的原則會在一段時間後刪除物件、您可以在說明中告知該物件。請勿在這些欄位中包含敏感資訊。

4. 選取 * 建立標記 * 。
5. 在 ILM 原則標籤表格中、使用下拉式清單來選取要指派給標籤的原則。
6. 如果「原則限制」欄中出現警告、請選取 * 檢視原則詳細資料 * 以檢閱原則。
7. 確保每個原則都能如預期般管理資料。
8. 選取 * 啟動指派的原則 * 。或者、選取 * 清除變更 * 以移除原則指派。
9. 在 [使用新標記啟動原則] 對話方塊中，檢閱每個標記、原則和規則如何管理物件的描述。視需要進行變更、以確保原則能如預期般管理物件。
10. 當您確定要啟動原則時、請在文字方塊中鍵入 * 是 * 、然後選取 * 啟動原則 * 。

相關資訊

"範例6：變更ILM原則"

StorageGRID 中的 ILM 原則模擬範例

ILM 原則模擬範例提供了建構及修改環境模擬的準則。

範例 1 ：模擬 ILM 原則時驗證規則

此範例說明如何在模擬原則時驗證規則。

在此範例中、針對兩個儲存區中擷取的物件來模擬*範例ILM原則*。此原則包含三項規則、如下所示：

- 第一條規則*兩份複本（2年、2年用於Bucke-A*）僅適用於Bucke-a中的物件
- 第二條規則* EC物件> 1 MB*、適用於所有儲存區、但會篩選大於1 MB的物件。
- 第三項規則是*兩份複本、兩個資料中心*、這是預設規則。它不包含任何篩選器、也不使用非目前的參考時間。

模擬原則之後、請確認每個物件都符合正確的規則。

在此範例中：

- `bucket-a/bucket-a object.pdf`正確符合第一個規則，該規則會篩選中的物件 `bucket-a`。
- `bucket-b/test object greater than 1 MB.pdf`在中 `bucket-b`、因此不符合第一個規則。相反地、第二個規則會正確比對此規則、該規則會篩選大於1 MB的物件。
- `bucket-b/test object less than 1 MB.pdf`不符合前兩個規則中的篩選條件、因此預設規則會放置篩選條件、不包含篩選條件。

範例 2 ：模擬 ILM 原則時重新排序規則

此範例說明如何在模擬原則時重新排序規則、以變更結果。

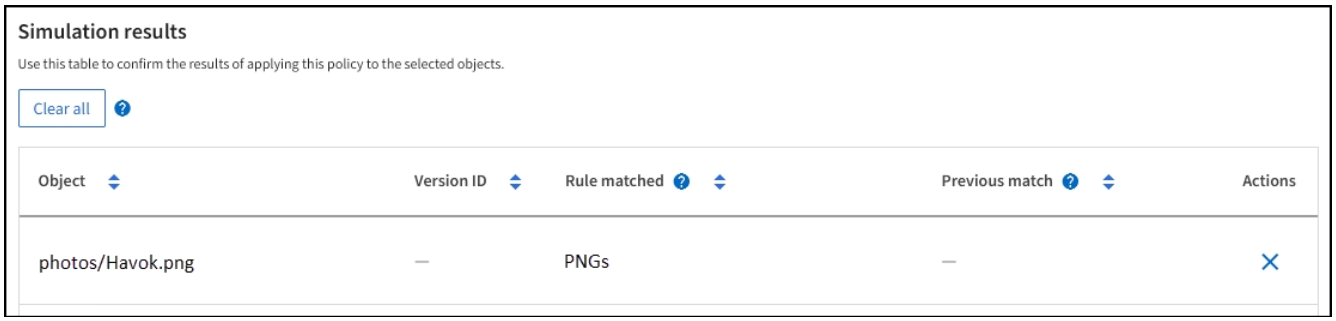
在此範例中、*示範*原則正在模擬中。此原則旨在尋找具有series=x-men使用者中繼資料的物件、其中包含三項規則、如下所示：

- 第一個規則 **PNG** 會篩選以結尾的按鍵名稱 `.png`。
- 第二個規則 * X-mant* 僅適用於租戶 A 的物件、以及使用者中繼資料的篩選器 `series=x-men`。
- 最後一個規則 * 兩個複本兩個資料中心 * 是預設規則、它會比對任何不符合前兩個規則的物件。

步驟

1. 新增規則並儲存原則之後、請選取*模擬*。
2. 在 * 物件 * 欄位中、輸入測試物件的 S3 儲存貯體 / 物件金鑰、然後選取 * 模擬 * 。

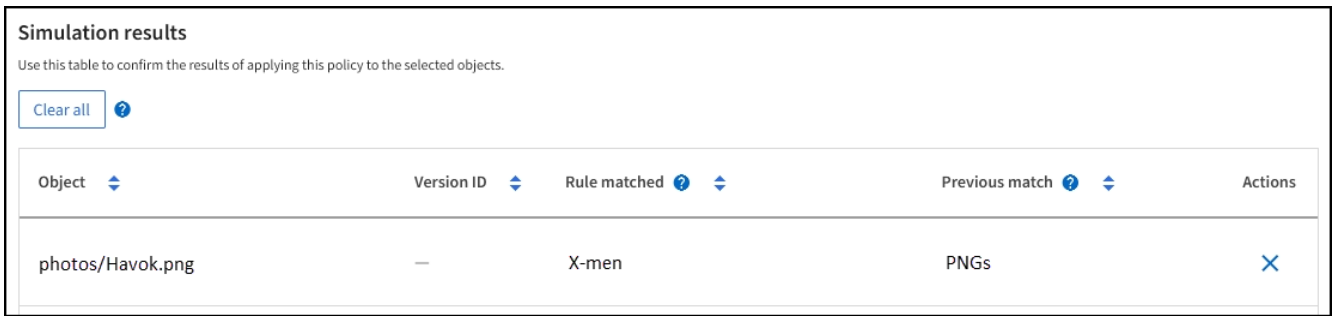
   模擬結果隨即出現、顯示 `Havok.png`物件已符合 **PNG** 規則。



   但是 `Havok.png`，它的目的是測試 *X-men * 規則。

3. 若要解決此問題、請重新排序規則。
   a. 選取 * 完成 * 以關閉「模擬 ILM 原則」視窗。
   b. 選取*編輯*以編輯原則。
   c. 將* X-men *規則拖曳到清單頂端。
   d. 選擇*保存*。
4. 選擇*模擬*。

   您先前測試的物件會根據更新的原則重新評估、並顯示新的模擬結果。在範例中、「規則相符」欄顯示`Havok.png`物件現在符合預期的 X-men 中繼資料規則。上一匹配列顯示 PNGs 規則與上一模擬中的對象匹配。

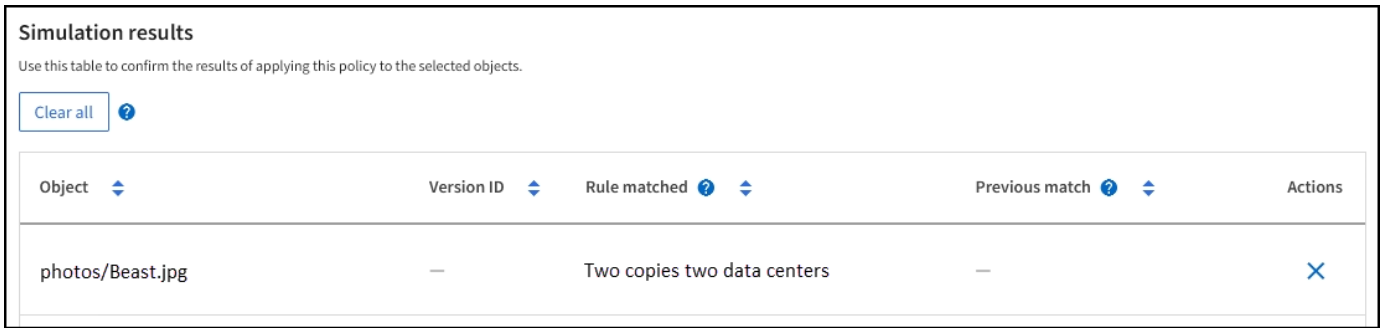


範例 **3** ：模擬 **ILM** 原則時修正規則

此範例說明如何模擬原則、修正原則中的規則、以及繼續模擬。

在此範例中、*示範*原則正在模擬中。此原則旨在尋找具有使用者中繼資料的物件 `series=x-men`。不過、針

對物件模擬此原則時、會發生非預期的結果 `Beast.jpg`。物件不符合X-men中繼資料規則、而是符合預設規則、兩個複本複製兩個資料中心。



當測試物件與原則中的預期規則不符時、您必須檢查原則中的每個規則、並修正任何錯誤。

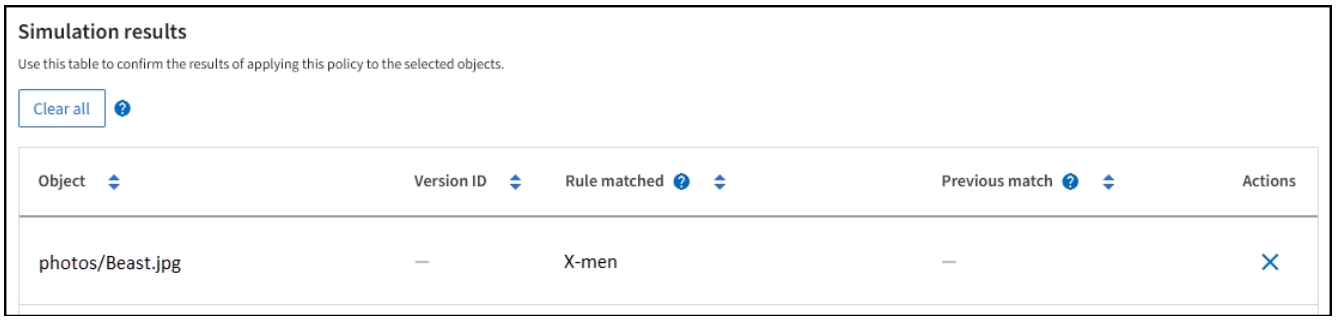
步驟

1. 選擇 * 完成 * 以關閉模擬原則對話方塊。在原則的詳細資料頁面上、選取 * 保留圖 * 。然後根據需要爲每個規則選擇 * 展開全部 * 或 * 查看詳細信息 * 。
2. 檢閱規則的租戶帳戶、參考時間及篩選條件。

   舉例來說、假設輸入 X-men 規則的中繼資料為「 x-men01 」、而非「 x-men 」。

3. 若要解決錯誤、請依照下列步驟修正規則：
   - 如果規則是原則的一部分、您可以複製規則或從原則中移除規則、然後加以編輯。
   - 如果規則是作用中原則的一部分、則必須複製規則。您無法編輯或移除作用中原則的規則。
4. 再次執行模擬。

   在此範例中、修正後的 X-men 規則現在會根據使用者中繼資料來比對 `Beast.jpg`物件 `series=x-men`、如預期般。



在 StorageGRID 中管理 ILM 原則標籤

您可以檢視 ILM 原則標籤詳細資料、編輯標籤或移除標籤。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"必要的存取權限"。

檢視 **ILM** 原則標籤詳細資料

若要檢視標記的詳細資料：

1. 選取 * ILM * > * 原則標記 * 。
2. 從表格中選取原則名稱。標籤的詳細資料頁面隨即出現。
3. 在詳細資料頁面上、檢視先前指派原則的歷程記錄。
4. 選取原則以檢視原則。

編輯 **ILM** 原則標籤

> 租戶可以看到標籤名稱和說明。選擇可協助租戶在選擇原則標籤指派給他們的貯體時、做出明智決策的值。例如、如果指派的原則會在一段時間後刪除物件、您可以在說明中告知該物件。請勿在這些欄位中包含敏感資訊。

若要編輯現有標記的說明：

1. 選取 * ILM * > * 原則標記 * 。
2. 選中標記複選框，然後選擇 **Edit** 。

   或者、選取標記的名稱。標籤的詳細資料頁面隨即出現、您可以在該頁面上選取 * 編輯 * 。

3. 視需要變更標記說明
4. 選擇*保存*。

移除 **ILM** 原則標籤

當您移除原則標籤時、任何指派該標籤的貯體都會套用預設原則。

若要移除標記：

1. 選取 * ILM * > * 原則標記 * 。
2. 選取標記的核取方塊、然後選取 * 移除 * 。隨即顯示確認對話方塊。

   或者、選取標記的名稱。標籤的詳細資料頁面隨即出現、您可以在該頁面上選取 * 移除 * 。

3. 選取 * 是 * 以刪除標記。

相關資訊

"了解如何建立 ILM 策略標籤"

使用 **StorageGRID** 中的物件中繼資料查詢來驗證 **ILM** 原則

啟動 ILM 原則後、將代表性測試物件擷取至 StorageGRID 系統、然後執行物件中繼資料查詢、確認複本是否依照預期製作、並放置在正確的位置。

開始之前

您有一個物件標識符，它可以是以下其中之一：

- **UUID**：物件的通用唯一識別碼。
- **CBID**： StorageGRID內物件的唯一識別碼。您可以從稽核日誌中取得物件的 CBID。以全部大寫的形式輸入 CBID。
- **S3** 儲存桶和物件鍵：當透過 S3 介面提取物件時，用戶端應用程式使用儲存桶和物件鍵組合來儲存和識別該物件。如果 S3 儲存桶已版本化，並且您想要使用儲存桶和物件鍵來尋找 S3 物件的特定版本，那麼您就有*版本 ID*。

步驟

1. 擷取物件。
2. 選取* ILM **>***物件中繼資料查詢。
3. 在*識別碼*欄位中輸入物件的識別碼。您可以輸入 UUID 、 CBID 或 S3 貯體 / 物件金鑰。
4. 或者、輸入物件的版本ID（僅限S3）。
5. 選擇*查詢*。

   隨即顯示物件中繼資料查詢結果。本頁列出下列資訊類型：

   - 系統中繼資料、例如物件 ID （ UUID ）、結果類型（物件、刪除標記、 S3 貯體）、以及物件的邏輯大小。如需詳細資料、請參閱以下範例螢幕擷取畫面。
   - 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、包含區段識別碼和資料大小的物件區段清單。對於超過100個區段的物件、只會顯示前100個區段。
   - 所有物件中繼資料均採用未處理的內部儲存格式。此原始中繼資料包含內部系統中繼資料、無法保證從發行到發行都會持續存在。
6. 確認物件儲存在正確的位置或位置、而且是正確的複本類型。

   如果啟用「稽核」選項、您也可以監控符合ORLM物件規則訊息的稽核記錄。ORLM 稽核訊息可提供您更多有關 ILM 評估程序狀態的資訊、但無法提供物件資料放置正確或 ILM 原則完整性的資訊。您必須自行評估。如需詳細資訊、請參閱 "檢閱稽核記錄"。

下列範例顯示儲存為兩個複寫複本之S3測試物件的物件中繼資料查詢結果。

以下螢幕擷取畫面為範例。您的結果會因 StorageGRID 版本而異。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


相關資訊

"使用S3 REST API"

在 StorageGRID 中使用 ILM 原則和 ILM 規則

隨著儲存需求的變更、您可能需要設定其他原則、或修改與原則相關的 ILM 規則。您可以檢視 ILM 指標來判斷系統效能。

開始之前

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

檢視 **ILM** 原則

若要檢視作用中和非作用中的 ILM 原則和原則啟動歷程記錄：

1. 選擇* ILM > Policies *。
2. 選取 * 原則 * 以檢視作用中和非作用中原則的清單。下表列出每個原則的名稱、原則指派的標記、以及原則是作用中或非作用中。
3. 選取 * 啟動歷程記錄 * 以檢視原則的啟動開始和結束日期清單。
4. 選取原則名稱以檢視原則的詳細資料。

如果您檢視狀態為已編輯或刪除之原則的詳細資料、會出現一則訊息、說明您正在檢視在指定時間範圍內作用中且自此之後已編輯或刪除的原則版本。

編輯 ILM 原則

您只能編輯非作用中原則。若要編輯作用中原則、請停用該原則、或建立複本並編輯複本。

編輯原則：

1. 選擇* ILM > Policies *。
2. 選中要編輯的策略的複選框，然後選擇 **Edit** 。
3. 請依照中的指示編輯原則"建立 ILM 原則"。
4. 在重新啟動原則之前、請先模擬原則。

如果ILM原則設定不正確、可能導致無法恢復的資料遺失。啟動ILM原則之前、請仔細檢閱ILM原則及其ILM規則、然後模擬ILM原則。請務必確認ILM原則是否正常運作。

複製 ILM 原則

複製 ILM 原則：

1. 選擇* ILM > Policies *。
2. 選中要克隆的策略的複選框，然後選擇 **Clone** 。
3. 依照中的指示"建立 ILM 原則"、從您複製的原則開始建立新原則。

如果ILM原則設定不正確、可能導致無法恢復的資料遺失。啟動ILM原則之前、請仔細檢閱ILM原則及其ILM規則、然後模擬ILM原則。請務必確認ILM原則是否正常運作。

移除 ILM 原則

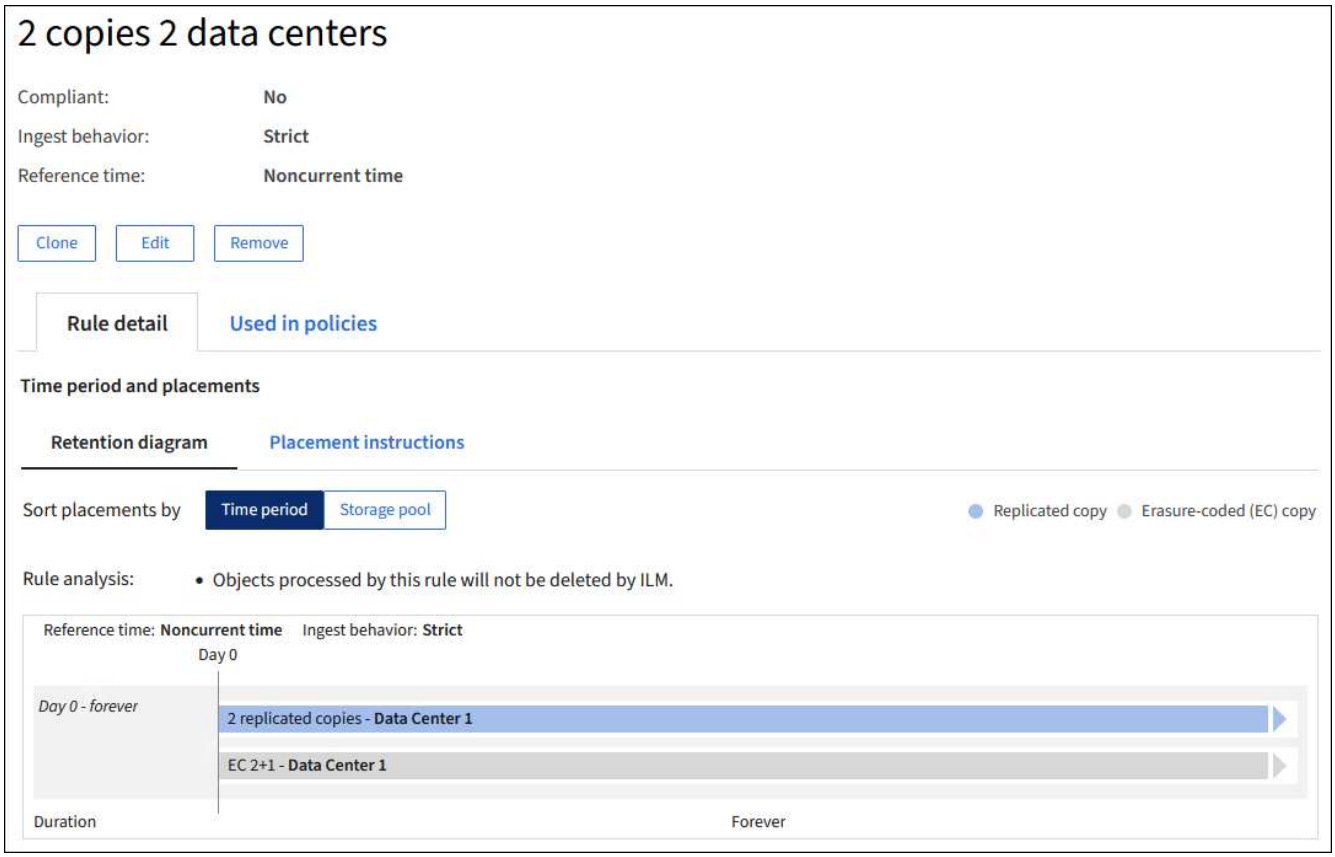
您只能移除非使用中的 ILM 原則。若要移除原則：

1. 選擇* ILM > Policies *。
2. 選取您要移除之非作用中原則的核取方塊。
3. 選擇*移除*。

檢視 **ILM** 規則詳細資料

若要檢視 ILM 規則的詳細資料、包括規則的保留圖表和放置指示：

1. 選擇* ILM > Rules *。
2. 選取您要檢視其詳細資料的規則名稱。範例：



此外、您也可以使用詳細資料頁面來複製、編輯或移除規則。如果規則用於任何原則、您就無法編輯或移除規則。

複製ILM規則

如果您想要建立使用現有規則部分設定的新規則、可以複製現有規則。如果您需要編輯任何原則中使用的規則、請改為複製規則並變更複製。變更複本之後、您可以從原則中移除原始規則、並視需要以修改版本取代原始規則。

如果 ILM 規則是使用 StorageGRID 10.2 版或更早版本所建立、則無法複製該規則。

步驟

1. 選擇* ILM > Rules *。
2. 選中要克隆的規則的複選框，然後選擇 **Clone** 。或者、選取規則名稱、然後從規則詳細資料頁面中選取 * 完整複製 * 。
3. 按照和的步驟更新克隆規則編輯 ILM 規則"在 ILM 規則中使用進階篩選器"。

   複製ILM規則時、您必須輸入新名稱。

編輯ILM規則

您可能需要編輯ILM規則、才能變更篩選或放置指示。

如果規則用於任何 ILM 原則、則無法編輯規則。您可以複製規則對複製的複本進行任何必要的變更。

> 如果ILM原則設定不正確、可能導致無法恢復的資料遺失。啟動ILM原則之前、請仔細檢閱ILM原則及其ILM規則、然後模擬ILM原則。請務必確認ILM原則是否正常運作。

步驟

1. 選擇* ILM > Rules *。
2. 確認您要編輯的規則未在任何 ILM 原則中使用。
3. 如果您要編輯的規則未在使用中、請選取規則的核取方塊、然後選取 * 動作 * > * 編輯 * 。或者、選取規則名稱、然後在規則詳細資料頁面上選取 * 編輯 * 。
4. 完成編輯 ILM 規則精靈的步驟。如有必要，請按照和"在 ILM 規則中使用進階篩選器"的步驟"建立ILM規則"操作。

   編輯 ILM 規則時、您無法變更其名稱。

移除 ILM 規則

若要讓目前的 ILM 規則清單保持可管理的狀態、請移除您不太可能使用的任何 ILM 規則。

步驟

若要移除目前用於作用中原則的 ILM 規則：

1. 複製原則。
2. 從原則複製移除 ILM 規則。
3. 儲存、模擬及啟動新原則、以確保物件受到預期的保護。
4. 請前往移除目前用於非作用中原則的 ILM 規則的步驟。

若要移除目前用於非作用中原則的 ILM 規則：

1. 選取非作用中原則。
2. 從原則或移除原則中移除 ILM 規則。
3. 請前往移除目前未使用的 ILM 規則的步驟。

移除目前未使用的 ILM 規則：

1. 選擇* ILM > Rules *。
2. 確認您要移除的規則未用於任何原則。
3. 如果您要移除的規則未在使用中、請選取規則、然後選取 * 動作 * > * 移除 * 。您可以選取多個規則、並同時移除所有規則。
4. 選取 * 是 * 以確認您要移除 ILM 規則。

檢視 **ILM** 指標

您可以檢視 ILM 的度量、例如佇列中的物件數目和評估率。您可以監控這些指標來判斷系統效能。大量佇列或評估率可能表示系統無法跟上擷取速度、用戶端應用程式的負載過大、或存在一些異常狀況。

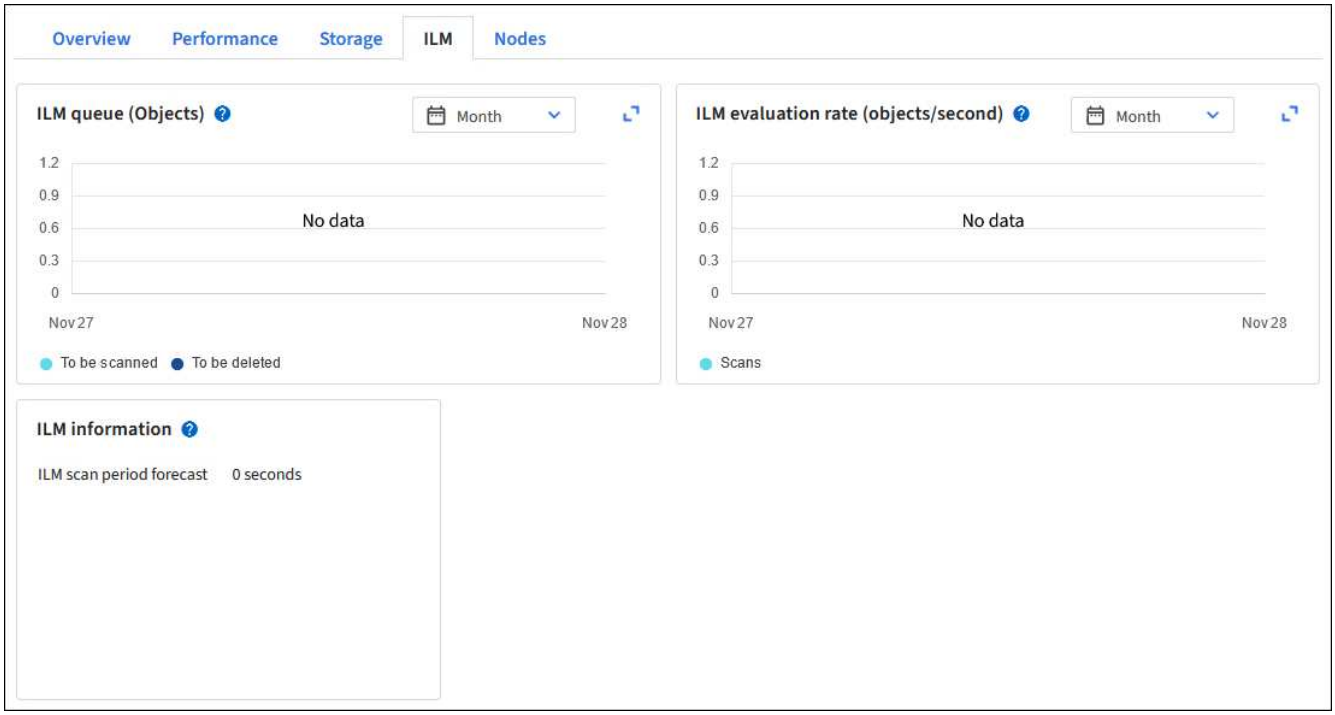
步驟

1. 選取 * 儀表板 * > * ILM * 。

   由於儀表板可以自訂、因此 ILM 索引標籤可能無法使用。

2. 監控 ILM 索引標籤上的度量。

   您可以選取問號 以查看 ILM 索引標籤上的項目說明。



使用**S3**物件鎖定

S3 物件鎖如何保護 **StorageGRID** 中的物件

身為網格管理員、您可以為 StorageGRID 系統啟用 S3 物件鎖定、並實作相容的 ILM 原則、以確保特定 S3 儲存區中的物件不會在指定的時間內遭到刪除或覆寫。

什麼是**S3**物件鎖定？

「物件鎖定」功能是物件保護解決方案、StorageGRID 相當於Amazon Simple Storage Service（Amazon S3）中的S3物件鎖定。

當 StorageGRID 系統啟用全域 S3 物件鎖定設定後，S3 租戶帳戶可以建立啟用或未啟用 S3 物件鎖定的儲存桶。當啟用「允許對現有儲存桶啟用 S3 物件鎖定」設定後，S3 租戶帳戶可以為現有儲存桶啟用 S3 物件鎖定。如果儲存桶啟用了 S3 物件鎖定，則必須啟用儲存桶版本控制，且版本控制會自動啟用。S3 租戶帳戶為新建或現有儲存桶啟用 S3 物件鎖定後，將無法停用此功能。

- 沒有 S3 物件鎖定 * 的貯體只能有未指定保留設定的物件。任何擷取的物件都不會有保留設定。
- 具有 S3 物件鎖定 * 的儲存貯體可以有物件、無論是否有 S3 用戶端應用程式指定的保留設定。某些擷取的物件會有保留設定。
- 已設定 S3 物件鎖定和預設保留 * 的貯體、可以使用指定的保留設定來上傳物件、也可以不保留設定來上傳新物件。新物件會使用預設設定、因為尚未在物件層級設定保留設定。

有效地說、所有新擷取的物件在設定預設保留時都會有保留設定。沒有物件保留設定的現有物件不會受到影響。

保留模式

StorageGRID S3 物件鎖定功能支援兩種保留模式、可將不同層級的保護套用至物件。這些模式相當於 Amazon S3 保留模式。

- 在法規遵循模式中：
  - 直到達到物件的保留日期、才能刪除物件。
  - 物件的保留日期可以增加、但不能減少。
  - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
  - 具有特殊權限的使用者可以在修改特定保留設定的要求中使用略過標頭。
  - 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
  - 這些使用者可以增加、減少或移除物件的保留到目前為止。

物件版本的保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以使用 S3 用戶端應用程式、針對新增至貯體的每個物件、選擇性地指定下列保留設定：

- * 保留模式 * ：法規遵循或治理。
- * 保留至日期 * ：如果物件版本的保留至未來日期、則可以擷取物件、但無法刪除。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。合法持有不受保留至日期的限制。

  如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

  有關物件設定的詳細資訊，請參閱"使用 S3 REST API 來設定 S3 物件鎖定"。

貯體的預設保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以選擇性地指定貯體的下列預設設定：

- * 預設保留模式 * ：法規遵循或治理。
- * 預設保留期間 * ：新增至此貯體的物件版本應保留多久、從新增物件之日起算。

預設的貯體設定僅適用於沒有自己保留設定的新物件。當您新增或變更這些預設設定時、現有的貯體物件不會受

到影響。

請參閱 "建立S3儲存區" 和 "更新 S3 物件鎖定預設保留"。

比較S3物件鎖定與舊版法規遵循

S3物件鎖定取代舊StorageGRID 版的Compliance功能。由於 S3 物件鎖定功能符合 Amazon S3 的要求、因此它取代了專屬的 StorageGRID 法規遵循功能、這項功能現在稱為「舊版法規遵循」。

> 全域合規性設定已棄用。如果您使用舊版 StorageGRID 啟用了此設定，則 S3 物件鎖定設定將自動啟用。您可以繼續使用 StorageGRID 管理現有符合法規儲存桶的設定；但是，您無法建立新的符合法規儲存桶。如需詳細資訊，請參閱 "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"。

如果您使用StorageGRID 舊版的更新版本的支援功能、請參閱下表、瞭解其與StorageGRID 更新版本中S3物件鎖定功能的比較。

	S3物件鎖定	法規遵循（舊版）
如何在全域啟用此功能？	從網格管理器中，選擇*配置* > 系統 > **S3** 物件鎖定。	不再支援。
此功能如何啟用儲存庫？	使用者必須啟用S3物件鎖定、才能使用租戶管理程式、租戶管理API或S3 REST API建立新的儲存區。	不再支援。
是否支援儲存區版本管理？	是的。儲存區版本設定是必要的、且會在啟用儲存區的S3物件鎖定時自動啟用。	不可以
如何設定物件保留？	使用者可以為每個物件版本設定保留截止日期、也可以為每個貯體設定預設保留期間。	使用者必須為整個儲存庫設定保留期間。保留期間適用於貯體中的所有物件。
保留期間可以變更嗎？	• 在規範模式中、物件版本的保留日期可以增加、但不會減少。 • 在治理模式中、具有特殊權限的使用者可以減少或甚至移除物件的保留設定。	貯體的保留期間可以增加、但不會縮短。
合法持有控制在哪裡？	使用者可以合法持有或撤銷貯體中任何物件版本的合法持有。	合法持有會置於貯體上、並影響貯體中的所有物件。

	S3物件鎖定	法規遵循（舊版）
何時可以刪除物件？	• 在符合性模式中、如果物件未處於合法保留狀態、則可在達到保留截止日期後刪除物件版本。 • 在治理模式中、具有特殊權限的使用者可以在物件達到保留截止日期之前刪除物件、前提是物件未處於合法保留狀態。	保留期間到期後、如果儲存區未處於合法保留狀態、則可刪除物件。物件可以自動或手動刪除。
是否支援庫位生命週期組態？	是的	否

StorageGRID 中的 **S3 Object Lock** 工作流程

身為網格管理員、您必須與租戶使用者密切協調、以確保物件受到保護、並符合其保留需求。

根據網路連線能力、節點狀態和 Cassandra 作業、在整個網格套用租戶設定可能需要 15 分鐘或更長的時間。

下列網格管理員和租戶使用者清單包含使用 S3 物件鎖定功能的高階工作。

網格管理員

- 為整個 StorageGRID 系統啟用全域 S3 物件鎖定設定。
- 允許使用者為現有儲存桶啟用 S3 物件鎖定。
- 確保資訊生命週期管理（ ILM ）原則符合 _ 標準 _ "啟用 S3 物件鎖定的貯體需求"、亦即符合。
- 視需要、允許租戶使用「法規遵循」做為保留模式。否則、只允許使用監管模式。
- 視需要為租戶設定最長保留期間。

租戶使用者

- 檢閱 S3 物件鎖定的貯體和物件考量事項。
- 如有需要，請聯絡網格系統管理員啟用以下設定之一：
  - 全域 S3 物件鎖定
  - 允許為現有儲存桶啟用 S3 物件鎖定
- 建立啟用 S3 物件鎖定的貯體。
- 對現有儲存桶啟用 S3 物件鎖定。
- 您也可以選擇設定貯體的預設保留設定：
  - 預設保留模式：監管或法規遵循（如果網格管理員允許）。
  - 預設保留期間：必須小於或等於網格管理員設定的最大保留期間。
- 使用 S3 用戶端應用程式來新增物件、並選擇性地設定物件特定的保留：
  - 保留模式。監管或法規遵循、如果網格管理員允許的話。

。保留截止日期：必須小於或等於網格管理員設定的保留期間上限所允許的值。

相關資訊

瞭解 "S3 物件鎖定要求"

StorageGRID 中的 **S3** 物件鎖定需求

您必須檢閱啟用全域S3物件鎖定設定的需求、建立相容ILM規則和ILM原則的需求、StorageGRID 以及使用S3物件鎖定之貯體和物件的限制等資訊。

使用全域**S3**物件鎖定設定的需求

- 您必須先使用Grid Manager或Grid Management API啟用全域S3物件鎖定設定、任何S3租戶才能建立啟用S3物件鎖定的儲存區。
- 啟用全域S3物件鎖定設定可讓所有S3租戶帳戶建立啟用S3物件鎖定的儲存區。
- 啟用全域 S3 物件鎖定設定之後、您就無法停用該設定。
- 除非所有主動式 ILM 原則中的預設規則為 _ 相容 _ （亦即、預設規則必須符合啟用 S3 物件鎖定的儲存區要求）、否則您無法啟用全域 S3 物件鎖定。
- 啟用全域 S3 物件鎖定設定時、除非原則中的預設規則符合規定、否則您無法建立新的 ILM 原則或啟動現有的 ILM 原則。啟用全域 S3 物件鎖定設定後、 ILM 規則和 ILM 原則頁面會指出哪些 ILM 規則符合規定。

允許在現有儲存桶上啟用 **S3** 物件鎖定的要求

啟用全域 S3 物件鎖定設定後，您可以選擇允許所有具有對應權限的 S3 租戶帳戶或 S3 使用者對現有儲存桶啟用 S3 物件鎖定。當 S3 租戶帳戶或 S3 使用者對現有儲存桶啟用 S3 物件鎖定時，根據您的 ILM 規則，可能會導致非預期的資料從雲端儲存資源池移轉回 StorageGRID。

一旦意外的資料移轉開始，就無法停止。

符合**ILM**規則的要求

如果您想要啟用全域 S3 物件鎖定設定、則必須確保所有主動式 ILM 原則中的預設規則都符合規定。相容的規則可同時滿足啟用S3物件鎖定的兩個儲存區需求、以及啟用舊版法規遵循的任何現有儲存區：

- 它必須建立至少兩個複寫的物件複本、或一個銷毀編碼複本。
- 這些複本必須存在於儲存節點上、且必須在放置說明中的每一行的整個期間內存在。
- 物件複本無法儲存在雲端儲存池中。
- 至少一行放置指示必須從第 0 天開始、使用 * 擷取時間 * 作為參考時間。
- 至少一行放置指示必須為「永遠」。

ILM 原則的需求

當啟用全域 S3 物件鎖定設定時、作用中和非作用中的 ILM 原則可以同時包含相容和不相容的規則。

- 作用中或非作用中 ILM 原則中的預設規則必須相容。
- 不相容的規則僅適用於未啟用 S3 物件鎖定或未啟用舊版規範功能的貯體中物件。

- 符合法規的規則可套用至任何儲存區中的物件；不需要為儲存區啟用S3物件鎖定或舊版符合法規。

"S3 物件鎖定適用的 ILM 原則範例"

啟用**S3**物件鎖定的儲存區需求

- 如果StorageGRID 已針對整個S3物件鎖定設定啟用for the S廳 系統、您可以使用租戶管理程式、租戶管理API或S3 REST API來建立啟用S3物件鎖定的儲存區。
- 當「S3物件鎖定」已啟用時、StorageGRID 即可自動啟用該儲存區的版本管理功能。您無法停用儲存區的 S3 物件鎖定或暫停版本設定。
- 您也可以選擇使用租戶管理員、租戶管理 API 或 S3 REST API 、為每個貯體指定預設保留模式和保留期間。貯體的預設保留設定僅適用於新增至貯體但沒有其本身保留設定的新物件。您可以指定保留模式來覆寫這些預設設定、並在上傳每個物件版本時保留至日期。
- 啟用 S3 物件鎖定的貯體支援貯體生命週期組態。

啟用**S3**物件鎖定之儲存區中的物件需求

- 若要保護物件版本、您可以指定貯體的預設保留設定、或是指定每個物件版本的保留設定。可以使用 S3 用戶端應用程式或 S3 REST API 來指定物件層級保留設定。
- 保留設定適用於個別物件版本。物件版本可以同時具有「保留直到日期」和「合法保留」設定、但不能有另一個設定、或兩者都沒有。指定物件的保留截止日期或合法保留設定、只會保護要求中指定的版本。您可以建立物件的新版本、而舊版物件仍會保持鎖定狀態。

啟用**S3**物件鎖定的儲存區物件生命週期

儲存在已啟用 S3 物件鎖定的儲存貯體中的每個物件都會經過下列階段：

1. 物件擷取

   當物件版本新增至啟用 S3 物件鎖定的儲存區時、保留設定會套用如下：

   - 如果為物件指定保留設定、則會套用物件層級的設定。任何預設貯體設定都會被忽略。
   - 如果未指定物件的保留設定、則會套用預設貯體設定（如果存在）。
   - 如果未指定物件或貯體的保留設定、則 S3 物件鎖定不會保護該物件。

   如果套用保留設定、則物件和任何 S3 使用者定義的中繼資料都會受到保護。

2. * 物件保留與刪除 *

   StorageGRID 會在指定的保留期間內儲存每個受保護物件的多個複本。物件複本和儲存位置的確切數量和類型取決於主動式 ILM 原則中的相容規則。受保護物件是否能在達到保留截止日期之前刪除、取決於其保留模式。

   - 如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

相關資訊

- "建立S3儲存區"
- "更新 S3 物件鎖定預設保留"
- "使用 S3 REST API 來設定 S3 物件鎖定"

- "範例7：S3物件鎖定的符合ILM原則"

在 StorageGRID 中啟用 S3 物件鎖定

如果S3租戶帳戶在儲存物件資料時需要遵守法規要求、您必須為整個StorageGRID 整個整個系統啟用S3物件鎖定。啟用全域S3物件鎖定設定、可讓任何S3租戶使用者使用S3物件鎖定來建立及管理儲存區和物件。

開始之前

- 您有"root 存取權限"。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您已檢閱 S3 物件鎖定工作流程、並瞭解考量事項。
- 您已確認目前 ILM 原則中的預設規則符合法規。詳情請參閱 "建立預設ILM規則"。

關於這項工作

網格管理員必須啟用全域S3物件鎖定設定、才能讓租戶使用者建立啟用S3物件鎖定的新儲存區。啟用此設定後、便無法停用此設定。

啟用 S3 物件鎖定後，網格系統管理員還可以允許租戶使用者在現有儲存桶上啟用 S3 物件鎖定。網格系統管理員啟用此設定後，可以將其停用。如需詳細資訊，請參閱 "S3 物件鎖定要求"。

啟用全域 S3 物件鎖定設定後、請檢閱現有租戶的法規遵循設定。啟用此設定時、 S3 物件鎖定每個租戶設定取決於建立租戶時的 StorageGRID 版本。

> 全域合規性設定已棄用。如果您使用舊版 StorageGRID 啟用了此設定，則 S3 物件鎖定設定將自動啟用。您可以繼續使用 StorageGRID 管理現有符合法規儲存桶的設定；但是，您無法建立新的符合法規儲存桶。如需詳細資訊，請參閱 "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"。

步驟

1. 選擇*配置* > 系統 > **S3** 物件鎖定。

   「S3物件鎖定設定」頁面隨即出現。

2. 選擇 **Enable S3 Object Lock** 以對整個 StorageGRID 系統啟用 S3 物件鎖定。
3. （可選）選擇 **Allow S3 Object Lock to be enabled on existing buckets**。

   > 根據您的 ILM 規則，在現有儲存桶上啟用 S3 物件鎖定可能會導致非預期的資料從雲端儲存資源池移轉回 StorageGRID。移轉一旦開始，您將無法停止。如需詳細資訊，請參閱 "S3 物件鎖定要求"。

4. 選擇*應用*。

   隨即會出現確認對話方塊、提醒您啟用 S3 物件鎖定之後、您無法停用該鎖定。

5. 如果確定要為整個系統永久啟用S3物件鎖定、請選取*確定*。

   當您選取*確定*時：

- 如果主動式 ILM 原則中的預設規則符合規定、則 S3 物件鎖定功能現在會針對整個網格啟用、因此無法停用。
- 如果預設規則不符合法規，則會顯示錯誤。您必須建立並啟動新的 ILM 原則，且該原則必須包含符合法規的規則作為其預設規則。選取 **OK**。然後，建立新原則、模擬並啟動它。如需相關指示，請參閱 "建立ILM原則"。

解決在 **StorageGRID** 中更新 **S3 Object Lock** 或舊版法規遵循設定時的一致性錯誤

如果站台上的資料中心站台或多個儲存節點無法使用、您可能需要協助S3租戶使用者將變更套用至S3物件鎖定或舊版法規遵循組態。

已啟用S3物件鎖定（或舊版法規遵循）的租戶使用者、可以變更某些設定。例如、使用S3物件鎖定的租戶使用者可能需要將物件版本置於合法持有之下。

當租戶使用者更新S3儲存區或物件版本的設定時StorageGRID 、BIOS會嘗試立即更新整個網格的儲存區或物件中繼資料。如果系統因為資料中心站台或多個儲存節點無法使用而無法更新中繼資料、則會傳回錯誤：

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

若要解決此錯誤、請依照下列步驟操作：

1. 請儘快讓所有儲存節點或站台再次可用。
2. 如果您無法在每個站台上提供足夠的儲存節點、請聯絡技術支援部門、他們可以協助您恢復節點、並確保在整個網格中一致地套用變更。
3. 解決基礎問題之後、請提醒租戶使用者重試其組態變更。

相關資訊

- "使用租戶帳戶"
- "使用S3 REST API"
- "恢復與維護"

ILM規則與原則範例

StorageGRID 中基本物件保護和保留的 **ILM** 規則和原則

定義ILM原則以符合物件保護和保留需求時、您可以使用下列範例規則和原則作為起點。

> 下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

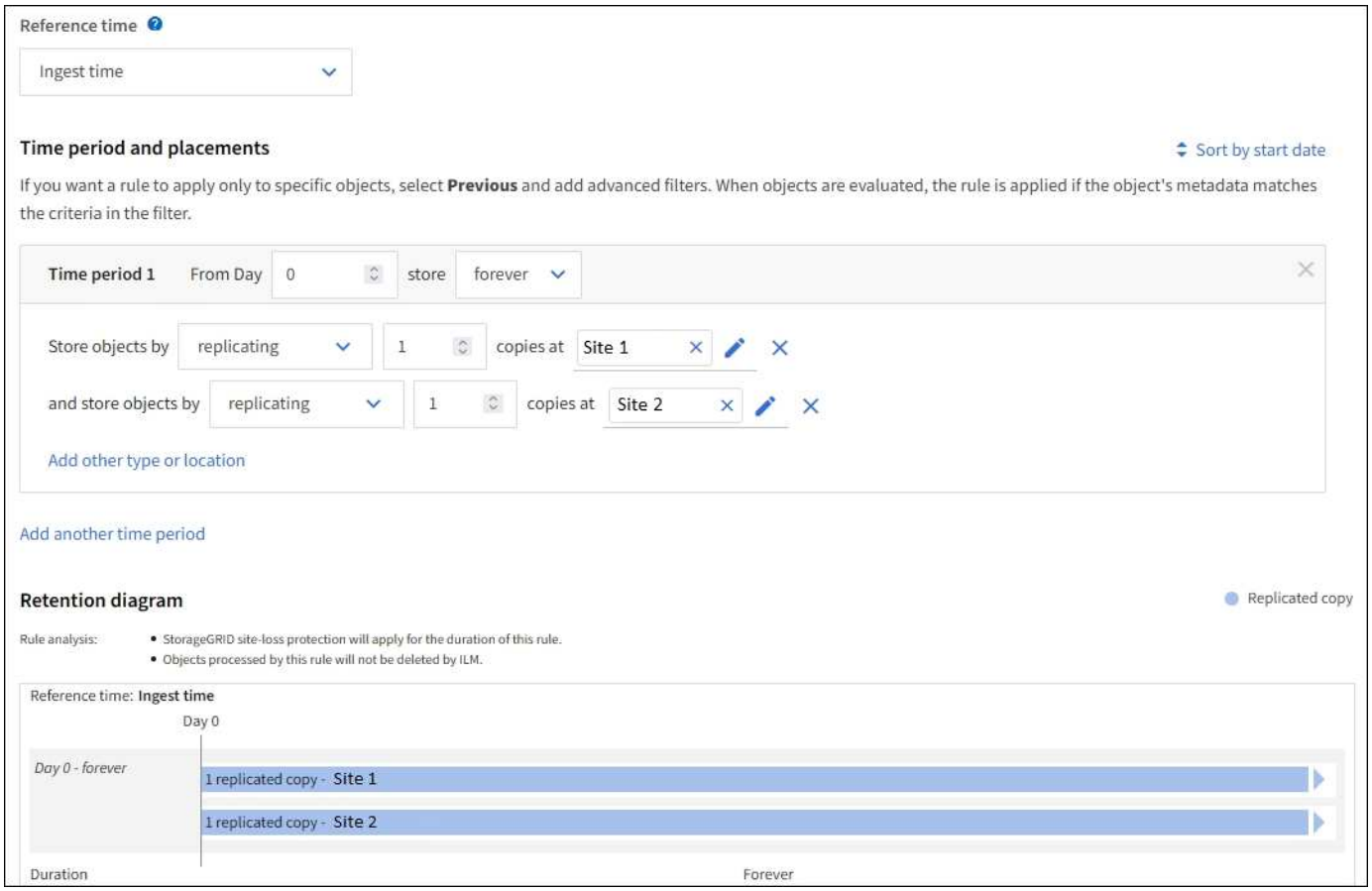
ILM 規則 **1** 例如 **1** ：將物件資料複製到兩個站台

此範例 ILM 規則會將物件資料複製到兩個站台的儲存集區。

規則定義	範例值
單站台儲存集區	兩個儲存資源池、每個資源池包含不同的站台、分別命名為站台 1 和站台 2 。
規則名稱	兩份複本、兩個站台
參考時間	擷取時間
刊登位置	在第 0 天至永遠、請在站台 1 保留一個複寫複本、並在站台 2 保留一個複寫複本。

保留圖的規則分析區段說明：

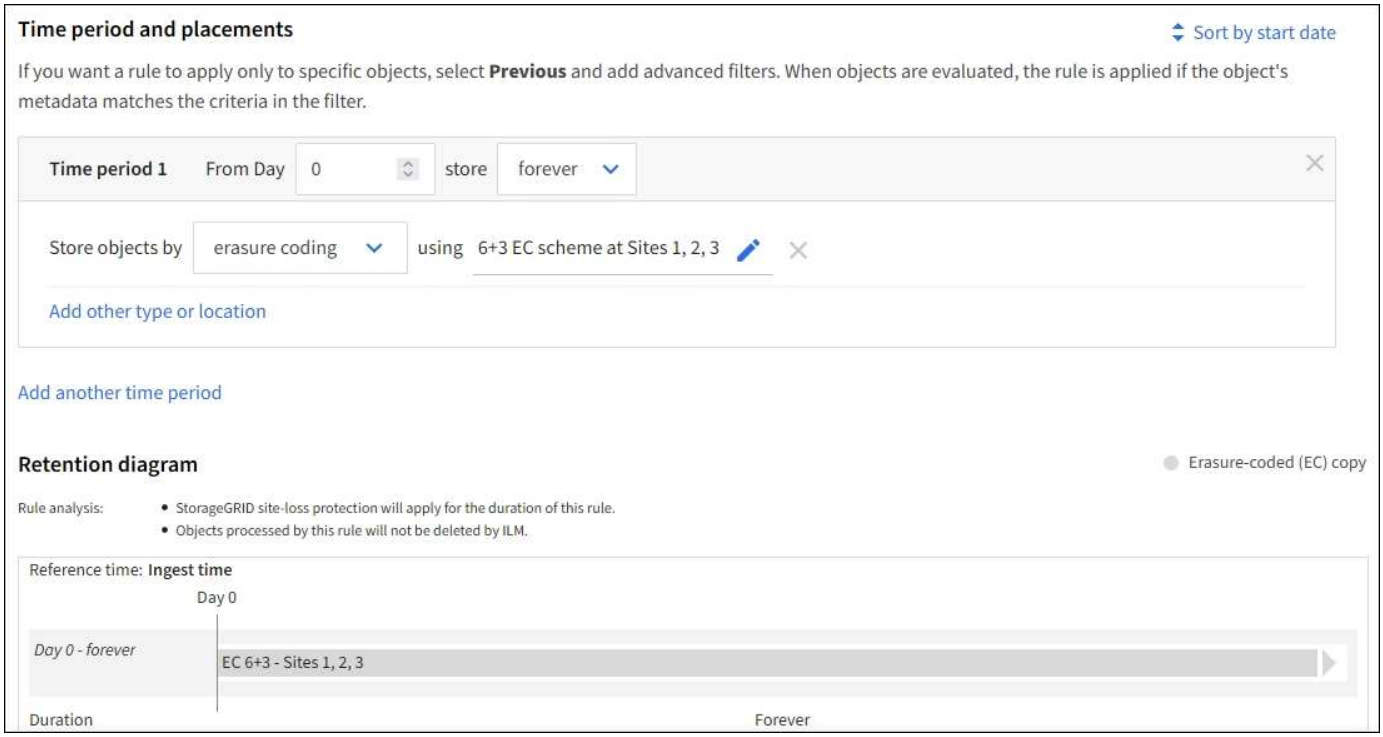
- StorageGRID 站台遺失保護將在本規則期間適用。
- ILM 不會刪除此規則處理的物件。



ILM 規則 **2** 範例 **1** ：含貯體比對的銷毀編碼設定檔

此 ILM 規則範例使用抹除編碼設定檔和 S3 儲存區、來判斷物件的儲存位置和儲存時間。

規則定義	範例值
具有多個站台的儲存池	• 跨三個站台（站台 1 、 2 、 3 ）建立一個儲存池 • 使用6+3銷毀編碼方案
規則名稱	S3 Bucket 財務記錄
參考時間	擷取時間
刊登位置	對於 S3 儲存貯體中名為財務記錄的物件、請在銷毀編碼設定檔所指定的儲存池中建立一個銷毀編碼複本。請保留此複本。

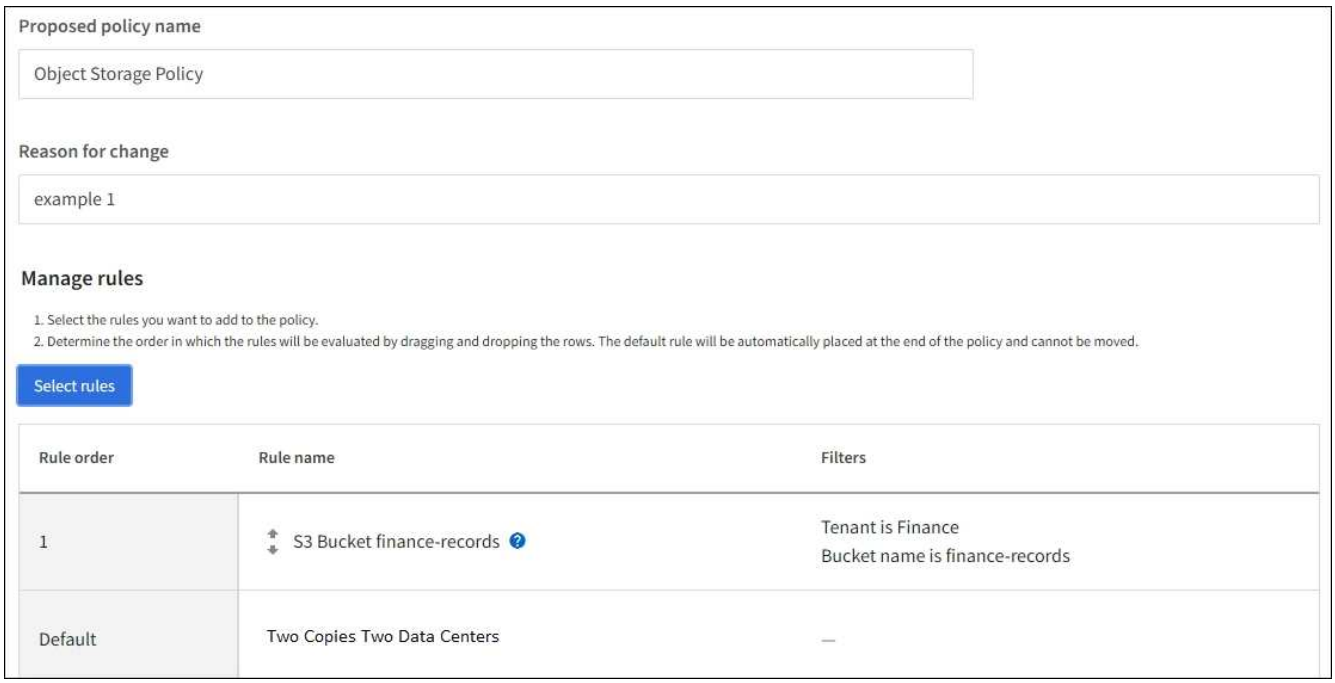


ILM原則（例如**1**）

實際上、大部分的 ILM 原則都很簡單、即使 StorageGRID 系統允許您設計複雜且複雜的 ILM 原則。

多站台網格的一般 ILM 原則可能包括 ILM 規則、例如：

- 在擷取時、將屬於 S3 儲存區（名稱為）的所有物件 `finance-records`儲存在包含三個站台的儲存池中。使用 6+3 銷毀編碼。
- 如果物件不符合第一個 ILM 規則、請使用原則的預設 ILM 規則、兩個複本兩個資料中心、將該物件的一個複本儲存在站台 1 、一個複本儲存在站台 2 。



相關資訊

- "使用 ILM 原則"
- "建立 ILM 原則"

StorageGRID 中 **EC** 物件大小篩選的 **ILM** 規則和原則

您可以使用下列範例規則和原則做為起點、定義ILM原則、根據物件大小篩選以符合建議的EC需求。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

ILM規則**1**（例如**2**）：對於大於**1 MB**的物件使用**EC**

此範例ILM規則銷毀會將大於1 MB的物件編碼。

銷毀編碼最適合大於1 MB的物件。請勿對小於 200 KB 的物件使用抹除編碼、以避免管理非常小的銷毀編碼片段所造成的負擔。

規則定義	範例值
規則名稱	僅 EC 物件 > 1 MB
參考時間	擷取時間
物件大小的進階篩選器	物件大小大於 1 MB

規則定義	範例值
刊登位置	使用三個站台建立2+1銷毀編碼複本

ILM規則**2**例如**2**：兩個複寫複本

此範例ILM規則會建立兩個複寫複本、而不會依物件大小進行篩選。此規則是原則的預設規則。由於第一個規則會篩選出大於1 MB的所有物件、因此此規則僅適用於1 MB或更小的物件。

規則定義	範例值
規則名稱	兩個複寫複本
參考時間	擷取時間
物件大小的進階篩選器	無
刊登位置	在第 0 天至永遠、請在站台 1 保留一個複寫複本、並在站台 2 保留一個複寫複本。

範例**2**的**ILM**原則：對於大於**1 MB**的物件使用**EC**

本範例ILM原則包括兩個ILM規則：

- 第一個規則銷毀會將大於1 MB的所有物件編碼。
- 第二個（預設）ILM規則會建立兩個複寫複本。由於規則1已篩選出大於1 MB的物件、因此規則2僅適用於1 MB或更小的物件。

StorageGRID 中用於保護映像檔案的 ILM 規則和原則

您可以使用下列範例規則和原則、確保大於 1 MB 的影像會被銷毀編碼、而且兩個複本會由較小的影像組成。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

ILM規則**1**例如**3**：將**EC**用於大於**1 MB**的映像檔

此範例ILM規則使用進階篩選來銷毀所有大於1 MB的映像檔。

銷毀編碼最適合大於1 MB的物件。請勿對小於 200 KB 的物件使用抹除編碼、以避免管理非常小的銷毀編碼片段所造成的負擔。

規則定義	範例值
規則名稱	EC 影像檔案 > 1 MB
參考時間	擷取時間
物件大小的進階篩選器	物件大小大於 1 MB
金鑰的進階篩選器	• 結尾為 .jpg • 結尾為 .png
刊登位置	使用三個站台建立2+1銷毀編碼複本

由於此規則已設定為原則中的第一個規則、因此銷毀編碼放置指示僅適用於大於 1 MB 的 .jpg 和 .png 檔案。

ILM規則2例如3：為所有剩餘映像檔案建立2個複寫複本

此ILM規則範例使用進階篩選功能來指定要複寫較小的映像檔。由於原則中的第一條規則已比對大於1 MB的映像檔、因此此規則適用於1 MB或更小的映像檔。

規則定義	範例值
規則名稱	2 份影像檔案複本
參考時間	擷取時間
金鑰的進階篩選器	• 結尾為 .jpg • 結尾為 .png
刊登位置	在兩個儲存池中建立 2 個複寫複本

範例3的ILM原則：為映像檔提供更好的保護

此ILM原則範例包含三個規則：

- 第一個規則銷毀會將所有大於1 MB的映像檔編碼。
- 第二個規則會建立任何剩餘映像檔的兩個複本（即1 MB或更小的映像）。
- 預設規則會套用至所有剩餘的物件（即任何非映像檔案）。

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

StorageGRID 中非當前 S3 物件版本的 ILM 規則和原則

如果您有啟用版本設定的 S3 儲存區、則可以在 ILM 原則中加入使用「非目前時間」做為參考時間的規則、以管理非目前物件版本。

如果您為物件指定有限的保留時間、這些物件將會在達到期間之後永久刪除。請務必瞭解物件的保留時間。

如本範例所示、您可以針對非目前物件版本、使用不同的放置說明來控制版本控制物件所使用的儲存容量。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

若要在物件的非目前版本上執行 ILM 原則模擬、您必須知道物件版本的 UUID 或 CBID 。若要尋找 UUID 和 CBID 、請在物件仍為最新狀態時使用"物件中繼資料查詢"。

ILM規則1（例如4）：儲存三份複本10年

本範例 ILM 規則會將每個物件的複本儲存在三個站台上 10 年。

此規則適用於所有物件、無論其版本是否為版本控制。

規則定義	範例值
儲存資源池	三個儲存資源池、每個資源池由不同的資料中心組成、分別命名為站台 1 、站台 2 和站台 3 。

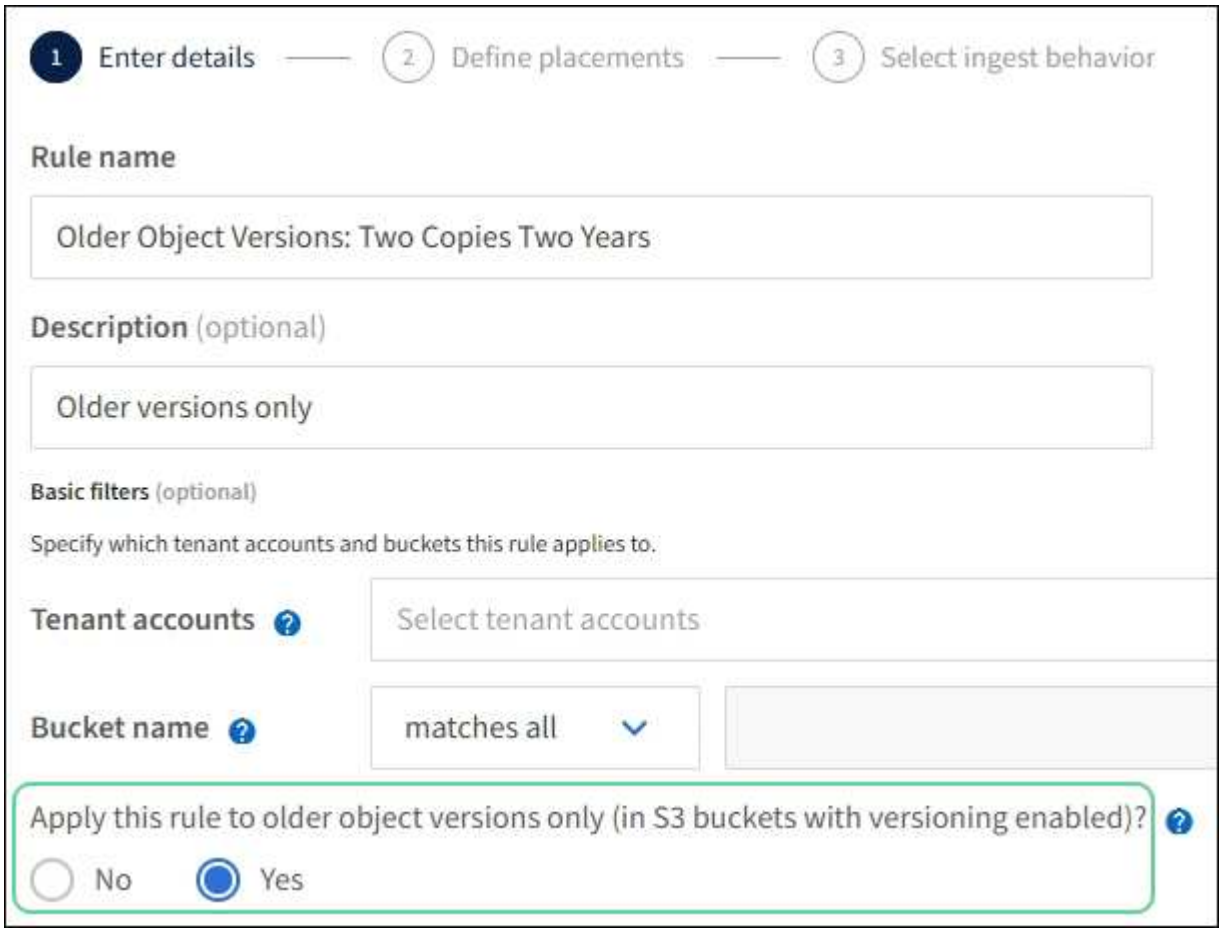
規則定義	範例值
規則名稱	三份十年
參考時間	擷取時間
刊登位置	在第 0 天、保留三個複寫複本 10 年（ 3 、 652 天）、一個在站台 1 、一個在站台 2 、一個在站台 3 。在10年結束時、請刪除物件的所有複本。

ILM規則2例如4：將兩個非目前版本的複本儲存**2**年

本範例ILM規則儲存S3版本物件的兩個非目前版本複本、為期2年。

由於ILM規則1適用於物件的所有版本、因此您必須建立另一個規則、以篩選出任何非目前版本。

若要建立使用「非目前時間」做為參考時間的規則、請針對「僅將此規則套用至較舊的物件版本（在啟用版本設定的 S3 儲存區中）」問題選取 * 是 * ？ 在「建立 ILM 規則」精靈的步驟 1 （輸入詳細資料）中。當您選取 * 是 * 時、就會自動為參考時間選取 _ 非目前時間 _ 、而且您無法選取不同的參考時間。



在此範例中、只會儲存兩個非目前版本的複本、而這些複本會儲存兩年。

規則定義	範例值
儲存資源池	兩個儲存資源池、分別位於不同的資料中心：站台 1 和站台 2 。
規則名稱	非最新版本：兩年兩份
參考時間	非目前時間 當您針對「僅將此規則套用至較舊的物件版本（在啟用版本設定的 S3 儲存區中）」問題選取 * 是 * 時、會自動選取此選項？ 在「建立 ILM 規則」精靈中。
刊登位置	第 0 天相對於非目前時間（即從物件版本變成非目前版本的那一天開始）、保留兩個非目前物件版本的複寫複本 2 年（ 730 天）、一個在站台 1 、一個在站台 2 。在2年結束時、請刪除非最新版本。

ILM原則、例如**4**：**S3**版本控制物件

如果您想要以不同於目前版本的方式來管理物件的舊版、則使用「非目前時間」做為參考時間的規則必須先出現在 ILM 原則中、然後才會套用至目前物件版本的規則。

S3版本化物件的ILM原則可能包含下列ILM規則：

- 從版本變成非最新的那一天起、將每個物件的任何舊版（非最新版）保留2年。

> 「非目前時間」規則必須出現在原則中、然後才會套用至目前物件版本的規則。否則、非目前物件版本永遠不會與「非目前時間」規則相符。

- 在擷取時、建立三個複寫複本、並在三個站台中每個站台儲存一個複本。將目前物件版本的複本保留10年。

模擬範例原則時、您預期測試物件的評估方式如下：

- 任何非目前的物件版本都會與第一個規則相符。如果非目前的物件版本早於2年、則ILM會永久刪除該版本（從網格中移除的所有非目前版本複本）。
- 目前的物件版本會與第二個規則相符。當目前的物件版本已儲存 10 年、 ILM 程序會將刪除標記新增為物件的目前版本、並將先前的物件版本設為「非目前」。下次進行 ILM 評估時、第一個規則會比對此非目前版本。如此一來、將會清除第 3 站點的複本、並將第 1 站點和第 2 站點的兩份複本再儲存 2 年。

相關資訊

"如何刪除物件"

StorageGRID 中嚴格擷取行為的 **ILM** 規則和原則

您可以使用位置篩選器和規則中嚴格的擷取行為、防止物件儲存在特定的資料中心位置。

在此範例中、以巴黎為基礎的租戶因為法規考量、不想將某些物件儲存在歐盟以外的地方。其他物件、包括來自其他租戶帳戶的所有物件、均可儲存在巴黎資料中心或美國資料中心。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

相關資訊

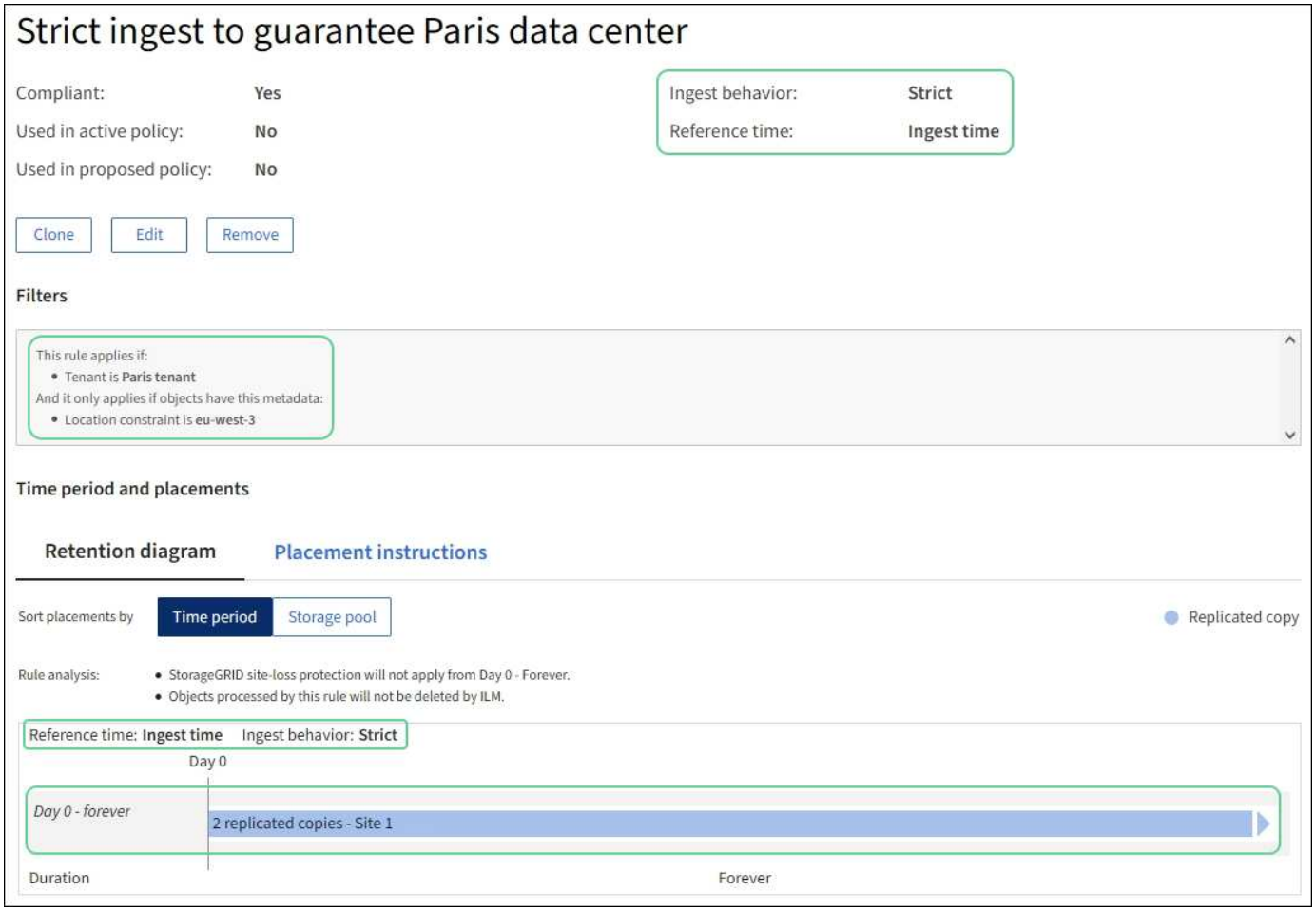
- "擷取選項"
- "建立 ILM 規則：選取擷取行為"

ILM規則1（例如5）：嚴格擷取以保證巴黎資料中心

本範例ILM規則使用嚴格的擷取行為、以保證由巴黎租戶儲存至S3儲存桶的物件、且區域設定為EU-WEST-3區域（巴黎）、永遠不會儲存在美國資料中心。

此規則適用於屬於巴黎租戶且S3儲存區設定為EU-WEST-3（巴黎）的物件。

規則定義	範例值
租戶帳戶	巴黎租戶
進階篩選器	位置限制等於 EU-WEST-3
儲存資源池	站台 1 （巴黎）
規則名稱	嚴格擷取以保證巴黎資料中心的效能
參考時間	擷取時間
刊登位置	在第 0 天、將兩個複寫複本永久保留在站台 1 （巴黎）
擷取行為	嚴格。請務必在擷取時使用此規則的放置位置。如果無法在巴黎資料中心儲存兩份物件複本、則擷取作業會失敗。



ILM規則**2**（例如**5**）：其他物件的平衡擷取

本範例ILM規則使用平衡擷取行為、為第一個規則不相符的任何物件提供最佳的ILM效率。將會儲存兩份符合此規則的所有物件複本、一份位於美國資料中心、另一份位於巴黎資料中心。如果規則無法立即滿足、則臨時複本會儲存在任何可用位置。

此規則適用於屬於任何租戶和任何區域的物件。

規則定義	範例值
租戶帳戶	忽略
進階篩選器	未指定
儲存資源池	站台 1 （巴黎）和站台 2 （美國）
規則名稱	2份複本2個資料中心
參考時間	擷取時間
刊登位置	在第0天、將兩個複寫複本永久保存在兩個資料中心

規則定義	範例值
擷取行為	平衡。如果可能、會根據規則的放置指示來放置符合此規則的物件。否則、會在任何可用位置製作過渡複本。

ILM原則範例**5**：結合擷取行為

ILM原則範例包括兩個具有不同擷取行為的規則。

使用兩種不同擷取行為的ILM原則可能包括ILM規則、例如：

- 儲存屬於巴黎租戶且S3儲存區設為EU-WEST-3（巴黎）的物件、僅適用於巴黎資料中心。如果無法使用巴黎資料中心、則無法擷取。
- 在美國資料中心和巴黎資料中心儲存所有其他物件（包括屬於巴黎租戶但有不同桶區的物件）。如果無法滿足放置指示、請在任何可用位置製作臨時複本。

模擬範例原則時、您預期測試物件的評估方式如下：

- 任何屬於巴黎租戶且S3儲存區設為EU-WEST-3的物件、都會以第一條規則進行比對、並儲存在巴黎資料中心。由於第一條規則使用嚴格的擷取、因此這些物件永遠不會儲存在美國資料中心。如果無法使用位於巴黎資料中心的儲存節點、擷取將會失敗。
- 所有其他物件都會符合第二個規則、包括屬於巴黎租戶且 S3 儲存區未設定為歐盟西部 -3 的物件。每個資料中心都會儲存一份物件複本。不過、因為第二個規則使用平衡擷取、所以如果有一個資料中心無法使用、則會在任何可用位置儲存兩個過渡複本。

變更 **ILM** 原則如何影響 **StorageGRID** 效能

如果您需要變更資料保護、或是新增網站、您可以建立並啟動新的 ILM 原則。

變更原則之前、您必須先瞭解ILM放置位置的變更如何暫時影響StorageGRID 到整個作業系統的效能。

在此範例中、擴充中新增了一個 StorageGRID 站台、需要實作新的主動式 ILM 原則、以便將資料儲存在新站台上。若要實作新的作用中原則，請先"建立原則"。之後、您必須"模擬"執行"啟動"新原則。

> 下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

變更 **ILM** 原則會如何影響效能

當您啟動新的ILM原則時、StorageGRID 可能會暫時影響到您的系統效能、尤其是新原則中的放置指示需要將許多現有物件移至新位置時。

當您啟動新的ILM原則時StorageGRID 、利用它來管理所有物件、包括現有物件和新擷取的物件。在啟動新的ILM原則之前、請先檢閱現有複寫和銷毀編碼物件放置位置的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、導致暫時性資源問題。

為了確保新的 ILM 原則不會影響現有複寫和刪除編碼物件的放置，您可以"建立內含擷取時間篩選器的 ILM 規則"。例如、 * 擷取時間 _ 在 _ _ _ <date and time> _ 之後、所以新規則僅適用於在指定日期和時間之後擷取的物件。

可能暫時影響StorageGRID 到性能不佳的ILM原則變更類型包括：

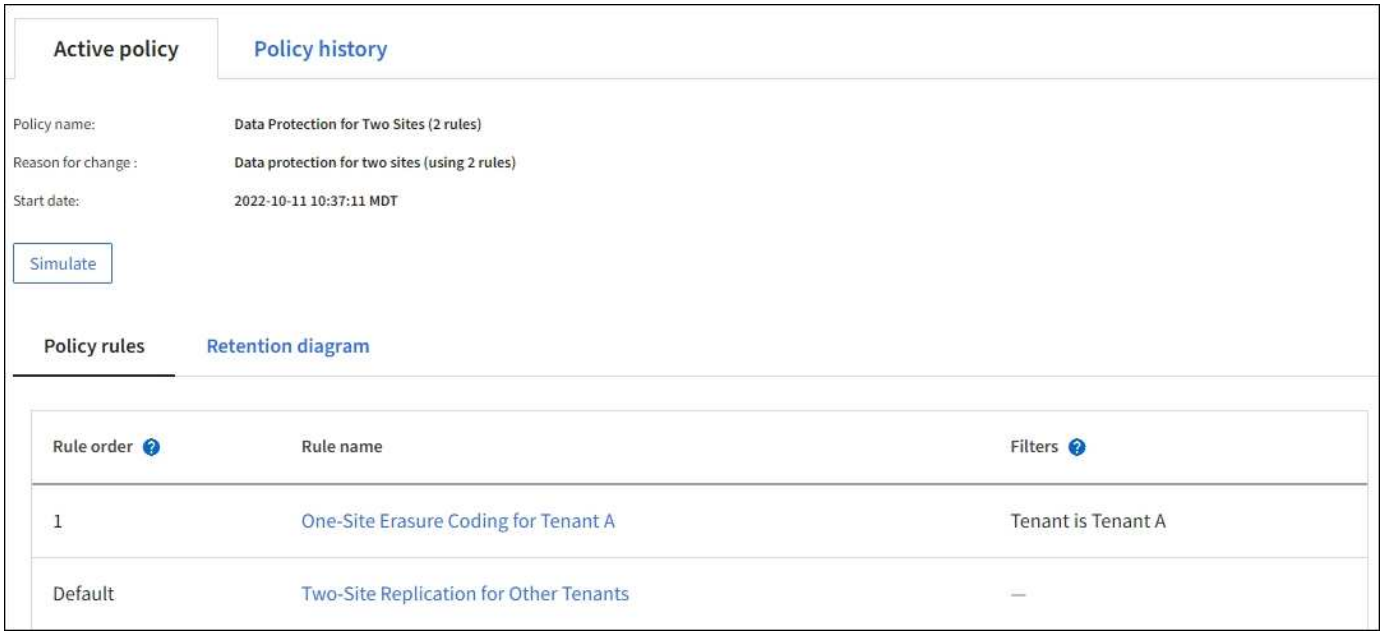
- 將不同的抹除編碼設定檔套用至現有的抹除編碼物件。

> StorageGRID 認為每個銷毀編碼設定檔都是唯一的、而且在使用新設定檔時、不會重複使用銷毀編碼片段。

- 變更現有物件所需的複本類型；例如、將大量複寫物件轉換成銷毀編碼物件。
- 將現有物件的複本移至完全不同的位置、例如、將大量物件移入或移出Cloud Storage Pool、或移至或移出遠端站台。

範例**6**的**Active ILM**原則：兩個站台的資料保護

在此範例中、主動式ILM原則最初是針對雙站台StorageGRID 的作業系統而設計、並使用兩個ILM規則。



在此ILM原則中、屬於租戶A的物件在單一站台上受到2+1銷毀編碼的保護、而屬於所有其他租戶的物件則使用雙複製複寫在兩個站台上受到保護。

規則**1**：租戶**A**的單一站台銷毀編碼

規則定義	範例值
規則名稱	租戶A的單一站台銷毀編碼
租戶帳戶	租戶A
儲存資源池	站台 1
刊登位置	2+1 從第 0 天到永遠在站台 1 進行銷毀編碼

規則**2**：為其他租戶進行雙站台複寫

規則定義	範例值
規則名稱	其他租戶的雙站台複寫
租戶帳戶	忽略
儲存資源池	站台 1 和站台 2
刊登位置	從第 0 天到永遠複寫兩份複本：在站台 1 複製一份複本、在站台 2 複製一份複本。

ILM 原則範例 **6** ：三個站台的資料保護

在此範例中、 ILM 原則正被三站台 StorageGRID 系統的新原則所取代。

在執行擴充以新增站台之後、網格管理員建立了兩個新的儲存集區：站台 3 的儲存集區、以及包含所有三個站台的儲存集區（與所有儲存節點預設儲存集區不同）。然後、管理員建立了兩個新的 ILM 規則和一個新的 ILM 原則、其設計是為了保護所有三個站台的資料。

啟動此新的ILM原則時、屬於租戶A的物件會在三個站台上受到2+1銷毀編碼的保護、屬於其他租戶（以及屬於租戶A的較小物件）的物件則會在三個站台上使用3個複製複寫來加以保護。

規則**1**：租戶**A**的三站台銷毀編碼

規則定義	範例值
規則名稱	租戶A的三站台銷毀編碼
租戶帳戶	租戶A
儲存資源池	全部 3 個站台（包括站台 1 、站台 2 和站台 3 ）
刊登位置	從第 0 天到永遠、所有 3 個站台的 2+1 銷毀編碼

規則**2**：其他租戶的三站台複寫

規則定義	範例值
規則名稱	其他租戶的三站台複寫
租戶帳戶	忽略
儲存資源池	站台 1 、站台 2 和站台 3

規則定義	範例值
刊登位置	從第 0 天到永久複製三份複本：在站台 1 複製一份、在站台 2 複製一份、在站台 3 複製一份。

啟動 **ILM** 原則、例如 **6**

當您啟動新的 ILM 原則時、現有的物件可能會移至新位置、或是根據任何新的或更新的規則中的放置指示、為現有物件建立新的物件複本。

> ILM原則中的錯誤可能導致無法恢復的資料遺失。在啟動原則之前、請仔細檢閱並模擬原則、以確認其運作正常。

> 當您啟動新的ILM原則時StorageGRID 、利用它來管理所有物件、包括現有物件和新擷取的物件。在啟動新的ILM原則之前、請先檢閱現有複寫和銷毀編碼物件放置位置的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、導致暫時性資源問題。

當銷毀編碼指令變更時會發生什麼事

在此範例中、目前作用中的 ILM 原則中、屬於租戶 A 的物件會使用站台 1 的 2+1 銷毀編碼來保護。在新的 ILM 原則中、屬於租戶 A 的物件將在站台 1 、 2 和 3 使用 2+1 銷毀編碼來保護。

啟動新的ILM原則時、會執行下列ILM作業：

- 租戶A擷取的新物件會分割成兩個資料分段、並新增一個同位元檢查分段。然後、這三個片段每個都會儲存在不同的站台上。
- 在進行中的ILM掃描程序中、會重新評估屬於租戶A的現有物件。由於 ILM 放置指示使用新的銷毀編碼設定檔、因此會建立全新的銷毀編碼片段、並將其散佈到三個站台。

> 站台 1 現有的 2+1 片段不會重複使用。StorageGRID 認為每個銷毀編碼設定檔都是唯一的、而且在使用新設定檔時、不會重複使用銷毀編碼片段。

複寫指示變更時會發生什麼事

在此範例中、目前作用中的 ILM 原則中、屬於其他租戶的物件會使用站台 1 和 2 儲存池中的兩個複寫複本來保護。在新的 ILM 原則中、屬於其他租戶的物件將使用站台 1 、 2 和 3 儲存池中的三個複寫複本加以保護。

啟動新的ILM原則時、會執行下列ILM作業：

- 當租戶以外的任何租戶都有新物件時、 StorageGRID 會建立三個複本、並在每個站台上儲存一份複本。
- 在進行中的ILM掃描程序中、會重新評估屬於這些其他租戶的現有物件。由於站台 1 和站台 2 的現有物件複本仍可滿足新 ILM 規則的複寫需求、因此 StorageGRID 只需為站台 3 建立一個新的物件複本。

啟用此原則對效能的影響

當本範例中的 ILM 原則啟動時、此 StorageGRID 系統的整體效能將暫時受到影響。若要為租戶 A 的現有物件建立新的銷毀編碼片段、以及在站台 3 為其他租戶現有物件建立新的複寫複本、則需要比一般網格資源層級更高的網格資源層級。

由於ILM原則變更、用戶端讀取和寫入要求可能會暫時超過正常延遲時間。在整個網格中完全實作放置指示之後、延遲時間會恢復正常。

若要在啟動新的 ILM 原則時避免資源問題、您可以在任何可能變更大量現有物件位置的規則中使用「擷取時間」進階篩選器。將「擷取時間」設定為大於或等於新原則生效的大約時間、以確保現有物件不會不必要地移動。

如果您需要減緩或提高ILM原則變更後處理物件的速度、請聯絡技術支援部門。

StorageGRID 中 **S3** 物件鎖定的相容 **ILM** 原則

在定義ILM原則時、您可以使用本範例中的S3儲存區、ILM規則和ILM原則作為起點、以符合已啟用S3物件鎖定之儲存區中物件的物件保護和保留需求。

如果您在先前StorageGRID 版本的支援功能中使用舊版法規遵循功能、也可以使用此範例來協助管理任何已啟用舊版法規遵循功能的現有儲存庫。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。

相關資訊

- "使用S3物件鎖定來管理物件"
- "建立ILM原則"

S3物件鎖定範例的儲存區和物件

在此範例中、名為Bank of ABC的S3租戶帳戶已使用租戶管理程式建立啟用S3物件鎖定的儲存庫、以儲存重要的銀行記錄。

儲存區定義	範例值
租戶帳戶名稱	ABC銀行
儲存區名稱	銀行記錄
桶區	美國東部-1（預設）

新增至銀行記錄庫的每個物件和物件版本、都會針對和 `legal hold`設定使用下列值 `retain-until-date`。

每個物件的設定	範例值
`retain-until-date`	「2030-12-30T23:59:59Z 」（ 2030 年 12 月 30 日） 每個物件版本都有自己的 `retain-until-date`設定。此設定可以增加、但不能減少。

每個物件的設定	範例值
`legal hold`	「 Off 」（關）（無效） 在保留期間內、任何物件版本均可隨時保留或撤銷合法保留。如果物件處於合法保留狀態、即使已到達、也無法刪除該物件 `retain-until-date`。

適用於 **S3** 物件鎖定的 **ILM** 規則 **1** 範例：使用貯體比對的抹除編碼設定檔

此範例ILM規則僅適用於名為Bank of ABC的S3租戶帳戶。它會比對貯體中的任何物件 `bank-records`、然後使用抹除編碼將物件儲存在三個資料中心站台上、使用 6+3 抹除編碼設定檔。此規則可滿足啟用 S3 物件鎖定的貯體需求：將複本從第 0 天保留在儲存節點上、以擷取時間做為參考時間、永遠保留在儲存節點上。

規則定義	範例值
規則名稱	法規遵循：銀行記錄庫中的 EC 物件 - ABC 銀行
租戶帳戶	ABC銀行
儲存區名稱	`bank-records`
進階篩選器	物件大小（ MB ）大於 1 *附註：*此篩選器可確保刪除編碼不會用於1 MB或更小的物件。

規則定義	範例值
參考時間	擷取時間
刊登位置	從第0天開始、永遠儲存
銷毀編碼設定檔	• 在三個資料中心站台的儲存節點上建立銷毀編碼複本 • 使用6+3銷毀編碼方案

S3物件鎖定範例的**ILM**規則**2**：不符合規則

本範例ILM規則一開始會在儲存節點上儲存兩個複寫的物件複本。一年後、它會將一份複本永久儲存在雲端儲存資源池中。由於此規則使用Cloud Storage Pool、因此不符合法規要求、也不會套用至啟用S3物件鎖定的儲存區中的物件。

規則定義	範例值
規則名稱	不符合規定的規則：使用雲端儲存池
租戶帳戶	未指定

規則定義	範例值
儲存區名稱	未指定、但僅適用於未啟用 S3 物件鎖定（或舊版法規遵循功能）的貯體。
進階篩選器	未指定

規則定義	範例值
參考時間	擷取時間
刊登位置	• 在第0天、將兩個複寫複本保留在資料中心1的儲存節點和資料中心2上365天 • 1年後、請將一份複寫複本永遠保留在雲端儲存資源池中

S3物件鎖定的**ILM**規則**3**範例：預設規則

此範例ILM規則會將物件資料複製到兩個資料中心的儲存資源池。此相容規則是ILM原則中的預設規則。它不含任何篩選器、不使用非目前的參考時間、並符合啟用S3物件鎖定的儲存區需求：儲存節點會從第0天一直保留兩個物件複本、使用「內嵌」作為參考時間。

規則定義	範例值
規則名稱	預設相容規則：兩份複本兩個資料中心
租戶帳戶	未指定
儲存區名稱	未指定
進階篩選器	未指定

規則定義	範例值
參考時間	擷取時間
刊登位置	從第0天到第2天、請保留兩個複寫複本：一個在資料中心1的儲存節點上、另一個在資料中心2的儲存節點上。

S3物件鎖定範例的符合**ILM**原則

若要建立可有效保護系統中所有物件（包括已啟用S3物件鎖定的儲存區中的物件）的ILM原則、您必須選取符合所有物件儲存需求的ILM規則。然後、您必須模擬並啟動原則。

新增規則至原則

在此範例中、ILM原則包含三個ILM規則、順序如下：

1. 一種相容的規則、使用銷毀編碼來保護特定儲存區中大於1 MB的物件、並啟用S3物件鎖定。物件會從第0天儲存在儲存節點上、直到永遠儲存在儲存節點上。
2. 不符合法規的規則、會在儲存節點上建立一年的兩個複寫物件複本、然後將一個物件複本永久移至雲端儲存池。此規則不適用於啟用S3物件鎖定的儲存區、因為它使用雲端儲存池。
3. 在儲存節點上建立兩個複寫物件複本的預設相容規則（從第0天到永遠）。

模擬原則

將規則新增至原則、選擇預設相容規則、並安排其他規則之後、您應該從啟用 S3 物件鎖定的儲存區和其他儲存區中測試物件、以模擬原則。例如、當您模擬範例原則時、測試物件的評估方式如下：

- 第一條規則只會比對ABC銀行租戶的貯體銀行記錄中大於1 MB的測試物件。
- 第二個規則會比對所有其他租戶帳戶的不符合規範桶中的所有物件。
- 預設規則會符合下列物件：
  - 針對ABC銀行租戶的庫位銀行記錄中的1 MB或更小物件。
  - 在任何其他已啟用S3物件鎖定的儲存區中、所有其他租戶帳戶的物件。

啟動原則

當您完全滿意新原則會依照預期保護物件資料時、就可以啟動它。

S3 儲存貯體生命週期與 **ILM** 原則在 **StorageGRID** 中的互動方式

根據您的生命週期組態、物件會遵循 S3 儲存區生命週期或 ILM 原則的保留設定。

儲存庫生命週期的範例優先於 **ILM** 原則

ILM原則

- 根據非目前時間參考的規則：在第 0 天、保留 X 份 20 天
- 規則依據擷取時間參考（預設）：在第 0 天、保留 X 份 50 天

貯體生命週期

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

結果

- 已擷取名為「 DOCS/ 文字」的物件。符合貯體生命週期篩選器的「 DOCS/ 」前置詞。
  - 100 天之後、系統會建立刪除標記、而「文件 / 文字」會變成非目前的。
  - 5 天之後、自擷取「文件 / 文字」後總共有 105 天被刪除。
  - 在 95 天之後、自擷取後總共 200 天、刪除標記建立後 100 天、刪除過期的刪除標記。
- 正在擷取名為「影片 / 影片」的物件。它與篩選器不符、並使用 ILM 保留原則。
  - 50 天後、系統會建立刪除標記、並將「影片 / 影片」變成非目前的。
  - 20 天後、自擷取影片後的 70 天內、「影片 / 影片」會被刪除。

- 30 天後、自擷取後的總計 100 天、以及刪除標記建立後的 50 天、刪除過期的刪除標記。

儲存貯體生命週期的範例則隱含永久保存

ILM原則

- 根據非目前時間參考的規則：在第 0 天、保留 X 份 20 天
- 規則依據擷取時間參考（預設）：在第 0 天、保留 X 份 50 天

貯體生命週期

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

結果

- 已擷取名為「 DOCS/ 文字」的物件。符合貯體生命週期篩選器的「 DOCS/ 」前置詞。

  此 `Expiration`動作僅適用於過期的刪除標記、這意味著將其他所有項目永遠保留（從「 docs/ 」開始）。

  刪除以「 DOCS/ 」開頭的標記會在過期時移除。

- 正在擷取名為「影片 / 影片」的物件。它與篩選器不符、並使用 ILM 保留原則。
  - 50 天後、系統會建立刪除標記、並將「影片 / 影片」變成非目前的。
  - 20 天後、自擷取影片後的 70 天內、「影片 / 影片」會被刪除。
  - 30 天後、自擷取後的總計 100 天、以及刪除標記建立後的 50 天、刪除過期的刪除標記。

使用貯體生命週期來複製 **ILM** 並清除過期刪除標記的範例

ILM原則

- 根據非目前時間參考的規則：在第 0 天、保留 X 份 20 天
- 規則以擷取時間參照為基礎（預設）：在第 0 天、永遠保留 X 份複本

貯體生命週期

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

結果

- ILM 原則會在貯體生命週期中複製。
  - ILM 原則的 Forever 規則旨在手動移除物件、並在 20 天後清理非最新版本。因此、擷取時間規則會永遠保留過期的刪除標記。
  - 貯體生命週期會在新增時重複 ILM 原則的行為 `"ExpiredObjectDeleteMarker": true`、這樣會在標記過期後移除刪除標記
- 正在擷取物件。無篩選器表示貯體生命週期會套用至所有物件、並會覆寫 ILM 保留設定。
  - 當租戶發出物件刪除要求時、會建立刪除標記、且物件變成非目前的物件。
  - 20 天後、非目前物件會刪除、刪除標記會過期。
  - 之後不久、過期的刪除標記就會刪除。

StorageGRID 的系統強化

了解 StorageGRID 的系統強化

系統強化是消除StorageGRID 儘可能多的安全風險的程序、因為這個系統是由一個系統來強化的。

在您安裝和設定 StorageGRID 時、請使用這些準則來協助您達成任何指定的機密性、完整性和可用度安全目標。

您應該已經在使用行業標準的最佳實踐來強化系統。例如，您對StorageGRID使用強密碼，使用 HTTPS 而不是 HTTP，並在可用的情況下啟用基於憑證的驗證。這些最佳實踐必須包括限制實體存取以及保護實體資料中心和支援基礎設施的實體和環境安全。您還必須參考適用於您的業務和地理位置的任何適用監管標準和建議。

StorageGRID 遵循 "NetApp 弱點處理原則"。報告的弱點會根據產品安全性事件回應程序進行驗證和解決。

強化 StorageGRID 系統時、請考慮下列事項：

- * 您已實作三個 StorageGRID 網路 * 中的哪一個。所有StorageGRID 的支援系統都必須使用Grid Network、但您也可能使用管理網路、用戶端網路或兩者。每個網路都有不同的安全考量。
- * 您用於 StorageGRID 系統中個別節點的平台類型 * 。可在VMware虛擬機器、Linux主機上的容器引擎內或專屬硬體設備上部署支援節點。StorageGRID每種平台都有自己的強化最佳實務做法。
- * 租戶帳戶的信任程度 * 。如果您是具有不受信任租戶帳戶的服務供應商、您的安全考量會與僅使用受信任的內部租戶不同。
- * 貴組織遵循哪些安全要求和慣例 * 。您可能需要遵守特定的法規或企業要求。

StorageGRID 軟體升級的強化準則

您必須保持StorageGRID 更新的不中斷系統和相關服務、才能抵禦攻擊。

升級StorageGRID 至更新版軟體

只要可能、您就應該將StorageGRID 更新版的更新版更新為最新的重大版本或先前的重大版本。保持更新有助於縮短已知弱點的作用時間、並減少整體攻擊範圍。StorageGRID此外、最新版的 StorageGRID 通常包含舊版中未包含的安全性強化功能。

請參閱 "NetApp 互通性對照表工具"（ IMT ）以判斷您應該使用的 StorageGRID 軟體版本。當需要修補程式時、NetApp會優先為最新版本建立更新。某些修補程式可能與舊版不相容。

- 若要下載最新的 StorageGRID 版本和 Hotfix 、請前往 "NetApp下載StorageGRID"。
- 若要升級 StorageGRID 軟體，請參閱"升級指示"。
- 若要套用 Hotfix ，請參閱"修復程序StorageGRID"。

升級至外部服務

外部服務可能存在間接影響StorageGRID 的漏洞。確保StorageGRID所依賴的服務保持最新。這些服務包括 LDAP、KMS（或 KMIP 伺服器）、DNS 和 NTP。

如需支援版本的清單，請參閱 "NetApp 互通性對照表工具"。

升級至**Hypervisor**

如果StorageGRID 您的VMware節點或其他Hypervisor上執行、則必須確保Hypervisor軟體和韌體為最新版本。

如需支援版本的清單，請參閱 "NetApp 互通性對照表工具"。

* 升級至 **Linux** 節點 *

如果StorageGRID 您的支援節點使用Linux主機平台、則必須確保安全性更新和核心更新已套用至主機作業系統。此外、您必須在有更新可用時、將韌體更新套用至易受影響的硬體。

如需支援版本的清單，請參閱 "NetApp 互通性對照表工具"。

強化有關資訊網路的準則**StorageGRID**

此支援每個網格節點最多三個網路介面、可讓您針對每個個別網格節點設定網路、以符合您的安全性和存取需求。StorageGRID

如需 StorageGRID 網路的詳細資訊，請參閱"網路類型StorageGRID"。

Grid Network準則

您必須為所有內部StorageGRID 的資訊流量設定Grid Network。所有的網格節點都位於網格網路上、而且必須能夠與所有其他節點交談。

設定Grid Network時、請遵循下列準則：

- 確保網路受到不受信任用戶端的保護、例如開放式網際網路上的用戶端。
- 如有可能、請將Grid Network專用於內部流量。管理網路和用戶端網路都有額外的防火牆限制、可封鎖外部的內部服務流量。支援將Grid Network用於外部用戶端流量、但這種使用方式可提供較少的保護層。
- 如果StorageGRID 此功能跨越多個資料中心、請使用Grid Network上的虛擬私有網路（VPN）或同等網路、為內部流量提供額外的保護。
- 有些維護程序需要在主要管理節點和所有其他網格節點之間的連接埠22上進行安全Shell（SSH）存取。使用外部防火牆限制SSH存取信任的用戶端。

管理網路準則

管理網路通常用於管理工作（使用Grid Manager或SSH的信任員工）、以及與其他信任的服務（例如LDAP、DNS、NTP或KMS（或KMIP伺服器）通訊。不過StorageGRID 、內部不強制使用此功能。

如果您使用的是管理網路、請遵循下列準則：

- 封鎖管理網路上的所有內部流量連接埠。請參閱"內部連接埠清單"。
- 如果不受信任的用戶端可以存取管理網路、請使用StorageGRID 外部防火牆封鎖對管理網路上的功能。

用戶端網路準則

用戶端網路通常用於租戶及與外部服務（例如CloudMirror複寫服務或其他平台服務）通訊。不過StorageGRID、內部不強制使用此功能。

如果您使用的是用戶端網路、請遵循下列準則：

- 封鎖用戶端網路上的所有內部流量連接埠。請參閱"內部連接埠清單"。
- 只接受明確設定的端點上的傳入用戶端流量。請參閱的相關資訊"管理防火牆控制"。

強化有關節點的準則StorageGRID

可在VMware虛擬機器、Linux主機上的容器引擎內或專屬硬體設備上部署支援節點。StorageGRID每種類型的平台和每種類型的節點都有自己的強化最佳實務做法。

控制遠端 IPMI 對BMC的訪問

您可以為所有包含 BMC 的應用裝置啟用或停用遠端 IPMI 存取。遠端 IPMI 介面允許任何擁有 BMC 帳戶和密碼的使用者對您的 StorageGRID 應用裝置進行底層硬體存取。如果您不需要對 BMC 進行遠端 IPMI 存取，請停用此選項。

- 若要在 Grid Manager 中控制對 BMC 的遠端 IPMI 存取，請前往 **Configuration** > **Security** > **Security settings** > **Appliances** > **Remote IPMI access**：
  - 清除 * 啟用遠端 IPMI 存取 * 核取方塊、以停用對 BMC 的 IPMI 存取。
  - 選中 **Enable remote IPMI access** （啓用遠程 IPMI 訪問 * ）複選框以啓用對 BMC 的 IPMI 訪問。

有關BMC強化的更多信息，請參閱 "強化基板管理控制器"網路安全資訊表 "國家安全局（NSA）"和 "網路安全與基礎設施安全局（CISA）"。

更改應用裝置 BMC 密碼

您可以變更應用裝置的 BMC 密碼，以限制存取並提高系統安全性。

1. 在 Grid Manager 中，前往 節點 > ***grid node*** > **BMC** 設定。
2. 在「變更密碼」部分，在「新密碼」中輸入長度為 8 到 16 個字元的新 BMC 密碼，然後在「確認新密碼」中再次輸入。
3. 選擇*保存*。

您也可以使用 `PUT /bmc-configuration/root-password` API 變更 BMC 密碼。

控制應用裝置外部 USB 連接埠的存取

您可以啟用應用裝置上的 USB 連接埠，以便技術支援存取進行診斷和疑難排解。如果您不需要存取 USB 連接埠，請基於安全性考量停用這些連接埠。初始安裝或升級後，USB 連接埠預設為啟用。

- 在 Grid Manager 中，前往 **Configuration** > **Security** > **Security settings** > **Appliances** > **USB port access**，啟用或停用 USB 連接埠：
  - 選取 **Enable USB ports** 核取方塊並儲存以啟用連接埠。

如果之前未選取 USB 複選框並已儲存，請勾選 **Enable USB ports** 複選框並儲存以再次啟用 USB 連接埠。

- 取消選取「啟用 USB 連接埠」核取方塊並儲存以停用這些連接埠。

防火牆組態

在系統強化程序中、您必須檢閱外部防火牆組態並加以修改、以便只接受來自IP位址和嚴格需要的連接埠的流量。

StorageGRID 在每個節點上都包含內部防火牆、可讓您控制對節點的網路存取、藉此增強網格的安全性。除了特定網格部署所需的連接埠之外、您應該"管理內部防火牆控制"防止所有連接埠上的網路存取。您在「防火牆控制」頁面上所做的組態變更會部署到每個節點。

具體而言、您可以管理以下領域：

- * 貴賓位址 * ：您可以允許選取的 IP 位址或子網路存取「管理外部存取」索引標籤上的設定所關閉的連接埠。
- * 管理外部存取 * ：您可以關閉預設開啟的連接埠、或重新開啟先前關閉的連接埠。
- * 不受信任的用戶端網路 * ：您可以指定節點是否信任來自用戶端網路的傳入流量、以及在設定不受信任的用戶端網路時、您要開啟的其他連接埠。

雖然此內部防火牆提供額外的保護層來抵禦某些常見的威脅、但它並不免除外部防火牆的需求。

有關StorageGRID使用的所有內部和外部連接埠的列表，請參閱"內部連接埠StorageGRID"和"用於外部通訊的連接埠"。

停用未使用的服務

對於所有StorageGRID節點，您應該停用或封鎖對未使用的服務的存取。例如，如果您不打算使用 DHCP，請使用網格管理員關閉連接埠 68。選擇*設定* > 防火牆控制 > 管理外部存取。然後將連接埠 68 的狀態切換從 開啟 變更為 關閉。

虛擬化、容器和共享硬體

對於所有StorageGRID 的物件節點、請避免在StorageGRID 不受信任的軟體所在的實體硬體上執行不可靠的功能。如果 StorageGRID 和惡意軟體位於同一實體硬體上、請勿假設 Hypervisor 保護措施可防止惡意軟體存取 StorageGRID 保護的資料。例如、Meltdown和Spetter攻擊會利用現代處理器的重大弱點、讓程式在同一部電腦的記憶體中竊取資料。

在安裝期間保護節點

安裝節點時、請勿允許不受信任的使用者透過網路存取 StorageGRID 節點。節點必須先加入網格、才能完全安全無虞。

限制對硬體的實體訪問

您必須將對StorageGRID硬體設備節點以及執行StorageGRID 的VMware 虛擬機器主機和 Linux 主機的實體存取權限限制為僅限授權管理員。實體存取控制的一些範例包括鎖、警衛、實體屏障和視訊監控。

硬體設備節點設計為僅由授權管理員安裝和操作。不允許未經授權的管理員存取硬體設備節點。

管理節點準則

管理節點提供系統組態、監控及記錄等管理服務。當您登入Grid Manager或租戶管理程式時、即連線至管理節點。

請遵循以下準則、將管理節點安全地存放在StorageGRID 您的一套系統上：

- 保護不受信任用戶端（例如開放式網際網路上的用戶端）的所有管理節點。確保任何不受信任的用戶端都無法存取Grid Network、管理網路或用戶端網路上的任何管理節點。
- 可控制Grid Manager和Tenant Manager功能的存取權限。StorageGRID授予每個使用者群組其角色所需的最低權限、並使用唯讀存取模式來防止使用者變更組態。
- 使用StorageGRID 動態負載平衡器端點時、請針對不受信任的用戶端流量、使用閘道節點而非管理節點。
- 如果您有不受信任的租戶、請勿允許他們直接存取租戶管理器或租戶管理 API 。而是讓任何不受信任的租戶使用與租戶管理API互動的租戶入口網站或外部租戶管理系統。
- 您也可以選擇使用管理 Proxy 、以更有效地控制從管理節點到 NetApp 支援的 AutoSupport 通訊。請參閱的步驟"建立管理 Proxy"。
- 您也可以選擇使用受限的843和9443連接埠來分隔Grid Manager和Tenant Manager通訊。封鎖共享連接埠443、並將租戶要求限制為連接埠9443以提供額外保護。
- 您也可以為網格管理員和租戶使用者使用個別的管理節點。

如需詳細資訊，請參閱的說明"管理StorageGRID"。

儲存節點準則

儲存節點可管理及儲存物件資料和中繼資料。請遵循以下準則、將儲存節點固定在StorageGRID 您的一套系統上。

- 不要允許不受信任的用戶端直接連線至儲存節點。請使用由 Gateway Node 或第三方負載平衡器提供的負載平衡器端點。
- 請勿為不受信任的租戶啟用外傳服務。例如、為不受信任的租戶建立帳戶時、請勿允許租戶使用自己的身分識別來源、也不允許使用平台服務。請參閱的步驟"建立租戶帳戶"。
- 針對不受信任的用戶端流量使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。
- 您也可以選擇使用儲存 Proxy 、以更有效地控制雲端儲存池、以及從儲存節點到外部服務的平台服務通訊。請參閱的步驟"建立儲存 Proxy"。
- 或者，使用客戶端網路連線到外部服務。然後，選擇*設定*>*安全*>*防火牆控制*>*不受信任的用戶端網路*，並指示儲存節點上的用戶端網路不受信任。儲存節點不再接受客戶端網路上的任何傳入流量，但它繼續允許平台服務的出站請求。

閘道節點準則

閘道節點提供選用的負載平衡介面、用戶端應用程式可用來連接StorageGRID 到VMware。請遵循下列準則、保護StorageGRID 您的整個作業系統中的任何閘道節點：

- 設定及使用負載平衡器端點。請參閱。 "負載平衡考量"
- 對於不受信任的用戶端流量、請在用戶端與閘道節點或儲存節點之間使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。如果您確實使用協力廠商負載平衡器、網路

流量仍可選擇性地設定為透過內部負載平衡器端點、或直接傳送至儲存節點。

- 如果您使用負載平衡器端點，則可以選擇讓用戶端透過用戶端網路連線。然後，選擇*設定*>*安全*>*防火牆控制*>*不受信任的用戶端網路*，並指示網關節點上的用戶端網路不受信任。網關節點僅接受明確配置為負載平衡器端點的連接埠上的入站流量。

硬體應用裝置節點準則

用作作業系統的各種硬體應用。StorageGRID StorageGRID有些應用裝置可做為儲存節點。其他應用裝置可做為管理節點或閘道節點。您可以將應用裝置節點與軟體型節點結合使用、或是部署設計完善的全應用裝置網格。

請遵循下列準則、確保StorageGRID 您的整個作業系統中的任何硬體應用裝置節點安全無虞：

- 如果應用SANtricity 程式使用NetApp系統管理程式來管理儲存控制器、請避免不受信任的用戶端SANtricity透過網路存取《系統管理程式》。
- 如果設備具有基板管理控制器 (BMC)，請注意BMC管理連接埠允許低階硬體存取。僅將BMC管理連接埠連接到安全、可信任的內部管理網路。

  您可以建立 VLAN 來隔離BMC網路連線並限制BMC對受信任網路的網際網路存取。有關強制 VLAN 分離的更多信息，請參閱 "強化基板管理控制器"網路安全資訊表 "國家安全局（NSA）"和 "網路安全與基礎設施安全局（CISA）"。

  如果沒有安全、可信任的內部管理網絡，請將BMC管理連接埠保持未連接或阻塞狀態。技術支援可能會在支援案例期間請求臨時存取權限。

- 如果應用裝置使用智慧型平台管理介面（IPMI）標準、支援透過乙太網路遠端管理控制器硬體、請封鎖連接埠623上不受信任的流量。

  您還可以停用遠端 IPMI 存取。

> ⓘ 您可以為所有包含BMC 的裝置啟用或停用遠端 IPMI 存取。遠端 IPMI 介面允許任何擁有BMC帳戶和密碼的人對您的StorageGRID設備進行低階硬體存取。如果您不需要遠端 IPMI 存取BMC，請使用下列方法之一停用此選項：+ 在 Grid Manager 中，前往 設定 > 安全 > 安全設定 > 裝置，然後清除 *啟用遠端 IPMI 存取*複選框。 + 在網格管理 API 中，使用私有端點： `PUT /private/bmc` 。

- 對於包含 SED 、 FDE 或 FIPS NL-SAS 磁碟機的應用裝置機型、您可以使用 SANtricity System Manager 來管理 "啟用和設定 SANtricity 磁碟機安全性"。
- 對於包含使用StorageGRID Appliance Installer 和 Grid Manager 管理的 SED 或 FIPS NVMe SSD 的裝置型號， "啟用及設定 StorageGRID 磁碟機加密" 。
- 對於沒有 SED、FDE 或 FIPS 磁碟機的設備，請使用金鑰管理伺服器 (KMS) "啟用並配置StorageGRID軟體節點加密" 。

相關資訊

"了解SANtricity System Manager 中的磁碟機安全性"

StorageGRID 中 TLS 和 SSH 的強化準則

您應該控制 SSH 訪問，替換預設 TLS 證書，並為 TLS 和 SSH 連線選擇適當的安全策略。

證書強化準則

您應該使用自己的自訂憑證來取代安裝期間建立的預設憑證。

對於許多組織而言StorageGRID 、自我簽署的數位憑證不符合其資訊安全政策。在正式作業系統上、您應該安裝CA簽署的數位憑證、以用於驗證StorageGRID 功能。

具體而言、您應該使用自訂伺服器憑證、而非下列預設憑證：

- 管理介面認證：用於安全存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。
- * S3 API 憑證 * ：用於保護儲存節點和閘道節點的存取安全、 S3 用戶端應用程式會使用這些節點來上傳和下載物件資料。

如需詳細資訊和指示、請參閱"管理安全性憑證"。

> 可分別管理負載平衡器端點所使用的憑證。StorageGRID若要設定負載平衡器憑證，請參閱"設定負載平衡器端點"。

使用自訂伺服器憑證時、請遵循下列準則：

- 憑證應具有 `*subjectAltName*`符合 StorageGRID DNS 項目的。如需詳細資訊、請參閱中的第 4.2.1.6 節「主旨替代名稱」 "RFC 5280：PKIX憑證與CRL設定檔"。
- 如有可能、請避免使用萬用字元憑證。此準則的例外情況是 S3 虛擬託管樣式端點的憑證、如果庫位名稱事先不清楚、則需要使用萬用字元。
- 當您必須在憑證中使用萬用字元時、應採取其他步驟來降低風險。請使用萬用字元模式、例如 `*.s3.example.com`、而不要 `s3.example.com`將後置字元用於其他應用程式。此模式也適用於路徑樣式的 `S3` 存取、例如 `dc1-s1.s3.example.com/mybucket`。
- 將憑證到期時間設為短（例如2個月）、然後使用Grid Management API自動執行憑證輪替。這對萬用字元憑證特別重要。

此外、用戶端在與StorageGRID NetApp通訊時、應使用嚴格的主機名稱檢查。

TLS 和 SSH 原則的強化準則

您可以選取安全性原則、以決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性策略控制 TLS 和 SSH 如何加密傳輸中的資料。作為最佳實踐，您應該停用應用程式相容性不需要的加密選項。使用預設的現代策略，除非您的系統需要符合通用標準、符合 FIPS 140-2，或您需要使用其他密碼

如需詳細資訊和指示、請參閱"管理 TLS 和 SSH 原則"。

管理外部 SSH 訪問

為了增強系統安全性，預設會阻止外部 SSH 存取。僅當需要執行需要入站 SSH 存取的任務（例如故障排除）時才啟用 SSH 存取。參考"管理外部 SSH 訪問"了解詳細資訊和說明。

StorageGRID 中日誌、密碼和稽核訊息的強化準則

除了遵循StorageGRID 有關「不二網」和「節點」的強化準則、您還應遵循StorageGRID 「不二網」系統其他區域的強化準則。

暫時安裝密碼

若要在安裝期間保護 StorageGRID 系統、請在 StorageGRID 安裝 UI 或安裝 API 的暫存安裝程式密碼頁面上設定密碼。設定此密碼時、會套用至所有安裝 StorageGRID 的方法、包括使用者介面、安裝 API 和 `configure-storagegrid.py`指令碼。

如需詳細資訊、請參閱：

- "在基於軟體的節點上安裝StorageGRID"
- "安裝 StorageGRID 應用裝置"

記錄與稽核訊息

請務必StorageGRID 以安全的方式保護不間斷記錄和稽核訊息輸出。從支援和系統可用度的觀點來看、支援記錄和稽核訊息可提供寶貴的資訊。StorageGRID此外StorageGRID 、包含在「資訊記錄」和「稽核訊息」輸出中的資訊和詳細資料、通常屬於敏感性質。

設定StorageGRID 將安全事件傳送至外部syslog伺服器。如果使用syslog匯出、請選取TLS和RELP/TLS做為傳輸傳輸傳輸傳輸傳輸傳輸協定。

如需 StorageGRID 記錄的詳細資訊、請參閱"記錄檔參考"。如需 StorageGRID 稽核訊息的詳細資訊、請參閱"稽核訊息"。

NetApp AutoSupport

StorageGRID 的 AutoSupport 功能可讓您主動監控系統健全狀況、並自動將套件傳送至 NetApp 支援網站 、貴組織的內部支援團隊或支援合作夥伴。根據預設、第一次設定 StorageGRID 時、會啟用傳送 AutoSupport 套件至 NetApp 。

可停用此功能。AutoSupport不過、NetApp建議您啟用此功能、因為AutoSupport 當StorageGRID 您的作業系統發生問題時、支援使用支援功能來加速問題識別與解決。

支援HTTPS、HTTP和SMTP傳輸傳輸傳輸傳輸傳輸傳輸協定。AutoSupport由於 AutoSupport 套件的敏感性質、NetApp 強烈建議使用 HTTPS 做為傳送 AutoSupport 套件至 NetApp 的預設傳輸通訊協定。

跨來源資源共享（ **CORS** ）

如果您想讓其他網域中的 Web 應用程式能夠存取 S3 貯體中的貯體和物件、則可以為 S3 貯體設定跨來源資源共享（ CORS ）。一般而言、除非需要、否則請勿啟用 CORS 。如果需要CORS、請將其限制在信任的來源。

請參閱"為儲存桶和物件配置 CORS"。

外部安全裝置

完整的強化解決方案必須能解決StorageGRID 不屬於其他功能的安全機制問題。使用額外的基礎架構裝置來篩選及限制StorageGRID 存取功能、是建立及維持嚴苛安全態勢的有效方法。這些外部安全裝置包括防火牆、入

侵防禦系統（IPS）和其他安全裝置。

不受信任的用戶端流量建議使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。

勒索軟體緩解

遵循中的建議、協助保護物件資料免遭勒索軟體攻擊 "使用 StorageGRID 進行勒索軟體防禦"。

StorageGRID 搭配 FabricPool

使用 StorageGRID 搭配 FabricPool 的設定工作流程

如果您使用 NetApp ONTAP 軟體、您可以使用 NetApp FabricPool 將非使用中資料分層至 NetApp StorageGRID 物件儲存系統。

請依照下列指示：

- 瞭解為 FabricPool 工作負載設定 StorageGRID 的考量與最佳實務做法。
- 瞭解如何設定 StorageGRID 物件儲存系統以搭配 FabricPool 使用。
- 瞭解將 StorageGRID 附加為 FabricPool 雲端層時、如何為 ONTAP 提供必要的價值。

快速開始設定 **StorageGRID for FabricPool**

1 規劃您的組態

- 決定您FabricPool 要使用哪個「功能區」分層原則、將非作用中ONTAP 的功能區資料分層到StorageGRID無法使用的地方。
- 規劃並安裝StorageGRID 一套可滿足儲存容量和效能需求的功能完善的系統。
- 熟悉 StorageGRID 系統軟體，包括"網格管理程式"和"租戶管理程式"。
- 檢閱"HA 群組"、"負載平衡"、"ILM"和的 FabricPool 最佳實務做法"更多資訊"。
- 檢閱這些額外資源、其中提供使用和設定 ONTAP 和 FabricPool 的詳細資料：

  "TR-4598 ： ONTAP 中的 FabricPool 最佳實務做法"

  "適用於 FabricPool 的 ONTAP 文件"

2 執行必要工作

取得"將 StorageGRID 附加為雲端層所需的資訊"、包括：

- IP位址
- 網域名稱
- SSL 憑證

可選地，配置"身分識別聯盟"和"單一登入"。

3 設定 **StorageGRID** 設定

使用 StorageGRID 取得 ONTAP 連線至網格所需的值。

使用"FabricPool 設定精靈"是設定所有項目的建議方法、也是最快速的方法、但您也可以視需要手動設定每個實體。

4 設定 **ONTAP** 和 **DNS**

使用 ONTAP 來"新增雲端層"使用 StorageGRID 值。然後、"設定 DNS 項目"將 IP 位址與您打算使用的任何網域名稱建立關聯。

5 監控與管理

當您的系統啟動並執行時、請在 ONTAP 和 StorageGRID 中執行持續的工作、以管理和監控隨時間而來的 FabricPool 資料分層。

什麼是**FabricPool** 功能？

VMware是一套不間斷的混合式儲存解決方案、使用高效能Flash Aggregate做為效能層、而物件存放區則做為雲端層。FabricPool ONTAP使用支援FabricPool的Aggregate可協助您降低儲存成本、而不會影響效能、效率或保護。

FabricPool 會將雲端層（外部物件存放區、例如 StorageGRID ）與本機層（ ONTAP 儲存集合體）建立關聯、以建立複合式光碟集合。然後、 FabricPool 內部的磁碟區可以利用分層功能、將作用中（熱）資料保留在高效能儲存設備（本機層）上、並將停用（冷）資料分層到外部物件儲存區（雲端層）。

無需變更架構、您也可以從中央ONTAP 的資訊儲存系統繼續管理資料和應用程式環境。

什麼是**StorageGRID** 功能？

NetApp StorageGRID 是一種儲存架構、可將資料管理為物件、而非檔案或區塊儲存等其他儲存架構。物件會保留在單一容器內（例如貯體）、不會嵌套成其他目錄內目錄內的檔案。雖然物件儲存設備的效能通常低於檔案或區塊儲存設備、但可大幅擴充。支援的資料儲存區可容納數PB的資料和數十億個物件。StorageGRID

為什麼**StorageGRID** 要使用不一樣**FabricPool** 的功能來做為一個不一樣的雲端層？

FabricPool 可以將 ONTAP 資料分層至許多物件儲存供應商、包括 StorageGRID 。公有雲可能會在庫位或容器層級設定每秒支援的輸入/輸出作業（IOPS）數量上限、但StorageGRID 不像公有雲、效能會隨系統中的節點數量而擴充。使用VMware做為VMware的雲端層、您可以將冷資料保留在私有雲端、以獲得最高效能、並完全掌控資料。StorageGRID FabricPool

此外FabricPool 、當StorageGRID 您使用效益技術做為雲端層時、不需要使用不含功能的認證。

將 **StorageGRID** 附加為 **FabricPool** 雲端層所需的資訊

在您將 StorageGRID 附加為 FabricPool 的雲端層之前、您必須先在 StorageGRID 中執行

組態步驟、並取得特定值以用於 ONTAP 。

我需要什麼價值？

下表顯示您必須在 StorageGRID 中設定的值、以及 ONTAP 和 DNS 伺服器如何使用這些值。

價值	其中已設定值	使用值的位置
虛擬 IP （ VIP ）位址	StorageGRID > HA 群組	DNS 項目
連接埠	StorageGRID > 負載平衡器端點	ONTAP 系統管理員 > 新增雲端層
SSL 憑證	StorageGRID > 負載平衡器端點	ONTAP 系統管理員 > 新增雲端層
伺服器名稱（ FQDN ）	StorageGRID > 負載平衡器端點	DNS 項目
存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租戶與貯體	ONTAP 系統管理員 > 新增雲端層
貯體 / 容器名稱	StorageGRID > 租戶與貯體	ONTAP 系統管理員 > 新增雲端層

如何取得這些價值？

視您的需求而定、您可以執行下列任一動作來取得所需資訊：

- 使用"FabricPool 設定精靈"。FabricPool 安裝精靈可協助您快速設定 StorageGRID 中所需的值、並輸出可用來設定 ONTAP 系統管理員的檔案。精靈會引導您完成必要步驟、並協助確保您的設定符合 StorageGRID 和 FabricPool 最佳實務做法。
- 手動設定每個項目。然後、在 ONTAP 系統管理員或 ONTAP CLI 中輸入值。請遵循下列步驟：
  a. "為 FabricPool 設定高可用度（ HA ）群組"。
  b. "建立FabricPool 負載平衡器端點以供使用"。
  c. "建立一個客戶帳戶FabricPool 以供使用"。
  d. 登入租戶帳戶、和"為 root 使用者建立貯體和存取金鑰"。
  e. 為 FabricPool 資料建立 ILM 規則、並將其新增至作用中的 ILM 原則。請參閱。 "設定 FabricPool 資料的 ILM"
  f. （可選）。"為 FabricPool 建立流量分類原則"

使用 **FabricPool** 設定精靈

了解 **StorageGRID FabricPool** 設定精靈

您可以使用 FabricPool 設定精靈、將 StorageGRID 設定為 FabricPool 雲端層的物件儲存系統。完成安裝精靈後、您可以在 ONTAP 系統管理員中輸入必要的詳細資料。

何時使用 **FabricPool** 設定精靈

FabricPool 安裝精靈會引導您完成設定 StorageGRID 以搭配 FabricPool 使用的每個步驟、並自動為您設定特定實體、例如 ILM 和流量分類原則。完成精靈時、您可以下載檔案、以便在 ONTAP 系統管理員中輸入值。使用精靈可更快速地設定系統、並確保您的設定符合 StorageGRID 和 FabricPool 最佳實務做法。

假設您具有「根目錄」存取權限、則可以在開始使用 StorageGRID Grid Manager 時完成 FabricPool 安裝精靈、或是在任何時候存取並完成精靈。視您的需求而定、您也可以手動設定部分或全部必要項目、然後使用精靈將 ONTAP 所需的值組合到單一檔案中。

除非您知道自己有特殊需求、否則請使用 FabricPool 安裝精靈、否則實作將需要大量自訂。

使用精靈之前

確認您已完成這些必要步驟。

檢視最佳實務做法

- 您大致瞭解"將 StorageGRID 附加為雲端層所需的資訊"。
- 您已檢閱 FabricPool 最佳實務做法、瞭解：
  - "高可用度（ HA ）群組"
  - "負載平衡"
  - "ILM 規則與原則"

取得 **IP** 位址並設定 **VLAN** 介面

如果您要設定 HA 群組、就會知道 ONTAP 將連接哪些節點、以及將使用哪個 StorageGRID 網路。您也知道要輸入哪些子網路 CIDR 、閘道 IP 位址和虛擬 IP （ VIP ）位址值。

如果您打算使用虛擬 LAN 來分隔 FabricPool 流量、則表示您已經設定了 VLAN 介面。請參閱。 "設定VLAN介面"

設定身分識別聯盟和 **SSO**

如果您打算對StorageGRID系統使用身分聯合或單一登入 (SSO)，則您已啟用這些功能。您也知道哪個聯合群組應該對ONTAP將使用的租用戶帳戶具有 root 存取權。看"使用身分識別聯盟"和"設定單一登入"。

取得及設定網域名稱

- 您知道 StorageGRID 要使用哪個完整網域名稱（ FQDN ）。網域名稱伺服器（ DNS ）項目會將此 FQDN 對應到您使用精靈建立的 HA 群組的虛擬 IP （ VIP ）位址。請參閱。 "設定 DNS 伺服器"
- 如果您打算使用 S3 虛擬託管風格的請求，則需要"已設定 S3 端點網域名稱"。ONTAP 預設使用路徑風格的 URL，但建議使用虛擬託管風格的請求。

檢閱負載平衡器和安全性憑證需求

如果您打算使用 StorageGRID 負載平衡器，則已查看了常規"負載平衡考量"。您擁有要上傳的憑證或產生憑證所需的值。

如果您打算使用外部（第三方）負載平衡器端點、則該負載平衡器具有完整網域名稱（ FQDN ）、連接埠和憑證。

確認 **ILM** 儲存池組態

如果您最初安裝的是 StorageGRID 11.6 或更早版本、則表示您已設定要使用的儲存池。一般而言、您應該為將用於儲存 ONTAP 資料的每個 StorageGRID 站台建立儲存池。

> 如果您最初安裝的是 StorageGRID 11.7 或 11.8 、則不適用此先決條件。當您最初安裝其中任一版本時、系統會自動為每個站台建立儲存資源池。

ONTAP 與 **StorageGRID** 雲端層之間的關係

FabricPool 精靈會引導您完成建立單一 StorageGRID 雲端層的程序、其中包括一個 StorageGRID 租戶、一組存取金鑰和一個 StorageGRID 貯體。您可以將此 StorageGRID 雲端層附加到一或多個 ONTAP 本機層。

將單一雲端層附加到叢集中的多個本機層是一般最佳實務做法。不過、視您的需求而定、您可能會想要在單一叢集中的本機層使用多個貯體、甚至多個 StorageGRID 租戶。使用不同的貯體和租戶、可讓您隔離 ONTAP 本機層之間的資料和資料存取、但設定和管理的複雜度較高。

NetApp 不建議將單一雲端層附加到多個叢集中的本機層。

> 有關將 StorageGRID 與 NetApp MetroCluster ™和 FabricPool 鏡像配合使用的最佳做法，請參閱 "TR-4598 ： ONTAP 中的 FabricPool 最佳實務做法"。

選用：為每個本機層使用不同的貯體

若要在 ONTAP 叢集中的本機階層使用多個儲存區、請在 ONTAP 中新增多個 StorageGRID 雲端層。每個雲端層都共用相同的 HA 群組、負載平衡器端點、租戶和存取金鑰、但使用不同的容器（ StorageGRID 貯體）。請遵循下列一般步驟：

1. 在 StorageGRID Grid Manager 中、完成第一個雲端層的 FabricPool 設定精靈。
2. 從 ONTAP 系統管理員新增雲端層、並使用您從 StorageGRID 下載的檔案來提供必要的值。
3. 從 StorageGRID 租戶管理員登入精靈所建立的租戶、然後建立第二個貯體。
4. 再次完成 FabricPool 精靈。選取現有的 HA 群組、負載平衡器端點和租戶。然後、選取您手動建立的新貯體。為新的貯體建立新的 ILM 規則、並啟動 ILM 原則以納入該規則。
5. 從 ONTAP 新增第二個雲端層、但提供新的儲存區名稱。

選用：為每個本機層使用不同的租戶和貯體

若要為 ONTAP 叢集中的本機層使用多個租戶和不同的存取金鑰集、請在 ONTAP 中新增多個 StorageGRID 雲端層。每個雲端層共用相同的 HA 群組、負載平衡器端點、但使用不同的租戶、存取金鑰和容器（ StorageGRID 貯體）。請遵循下列一般步驟：

1. 在 StorageGRID Grid Manager 中、完成第一個雲端層的 FabricPool 設定精靈。
2. 從 ONTAP 系統管理員新增雲端層、並使用您從 StorageGRID 下載的檔案來提供必要的值。
3. 再次完成 FabricPool 精靈。選取現有的 HA 群組和負載平衡器端點。建立新的租戶和貯體。為新的貯體建立新的 ILM 規則、並啟動 ILM 原則以納入該規則。

4. 從 ONTAP 新增第二層雲端、但提供新的存取金鑰、秘密金鑰和儲存庫名稱。

存取並完成 **StorageGRID FabricPool** 設定精靈

您可以使用 FabricPool 設定精靈、將 StorageGRID 設定為 FabricPool 雲端層的物件儲存系統。

開始之前

- 您已檢閱"考量與要求"以使用 FabricPool 安裝精靈。

> 如果您想將 StorageGRID 設定為與任何其他 S3 用戶端應用程式搭配使用"使用 S3 設定精靈"、請前往。

- 您有"root 存取權限"。

存取精靈

您可以在開始使用 StorageGRID Grid Manager 時完成 FabricPool 設定精靈、也可以在任何時候存取並完成精靈。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 如果儀表板上出現「* FabricPool and S3 設定精靈*」橫幅，請選擇橫幅中的連結。如果橫幅不再顯示，請從 Grid Manager 的標題列中選擇說明圖示 ，然後選擇「* FabricPool and S3 設定精靈*」。
3. 在 FabricPool and S3 設定精靈頁面的 FabricPool 區段中、選取 * 立即設定 * 。
   - 步驟 1 （共 9 步）：出現 Configure HA group* （配置 HA 組 * ）。

步驟 **9** 之 **1** ：設定 **HA** 群組

高可用度（ HA ）群組是每個節點包含 StorageGRID 負載平衡器服務的集合。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用 HA 群組來協助保持 FabricPool 資料連線可用。HA 群組使用虛擬 IP 位址（ VIP ）來提供高可用度的負載平衡器服務存取權。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、對 FabricPool 作業的影響微乎其微

有關此任務的詳細信息，請參閱"管理高可用度群組"和"高可用度群組的最佳實務做法"。

步驟

1. 如果您打算使用外部負載平衡器、則不需要建立 HA 群組。選擇 * 跳過此步驟 * 並轉至步驟 2 、共 9 步：設定負載平衡器端點。
2. 若要使用 StorageGRID 負載平衡器、請建立新的 HA 群組或使用現有的 HA 群組。

建立**HA**群組

a. 若要建立新的 HA 群組、請選取 * 建立 HA 群組 * 。

b. 如需 * 輸入詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
HA 群組名稱	此 HA 群組的唯一顯示名稱。
說明（選用）	此 HA 群組的描述。

c. 在 * 新增介面 * 步驟中、選取您要在此 HA 群組中使用的節點介面。

使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。

您可以選取一或多個節點、但每個節點只能選取一個介面。

d. 對於「介面優先順序」步驟、請判斷此 HA 群組的主要介面和任何備份介面。

拖曳列以變更 * 優先順序 * 欄中的值。

清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。

如果 HA 群組包含多個介面、且作用中介面故障、則虛擬 IP （ VIP ）位址會依照優先順序移至第一個備份介面。如果該介面故障、VIP位址會移至下一個備份介面、依此類推。解決故障時、VIP位址會移回可用的最高優先順序介面。

e. 在 * 輸入 IP 位址 * 步驟中、請填寫下列欄位。

欄位	說明
子網路 CIDR	以 CIDR 表示法表示的 VIP 子網路位址和 #8212 ； IPv4 位址後面接著斜線和子網路長度（ 0-32 ）。 網路位址不得設定任何主機位元。例如 `192.16.0.0/22`：。
閘道 IP 位址（選用）	選用。如果用於存取 StorageGRID 的 ONTAP IP 位址與 StorageGRID VIP 位址不在同一子網路上、請輸入 StorageGRID VIP 本機閘道 IP 位址。本機閘道IP位址必須位於VIP子網路內。
虛擬 IP 位址	為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內、而且所有位址都會同時在作用中介面上作用。 至少一個位址必須是 IPv4 。您也可以指定其他的IPv6位址。

f. 選取 * 建立 HA 群組 * 、然後選取 * 完成 * 以返回 FabricPool 設定精靈。

g. 選取 * 繼續 * 以移至負載平衡器步驟。

使用現有 **HA** 群組

a. 若要使用現有的 HA 群組、請從 * 選取 HA 群組 * 下拉式清單中選取 HA 群組名稱。

b. 選取 * 繼續 * 以移至負載平衡器步驟。

步驟 **2** 、共 **9** 步：設定負載平衡器端點

StorageGRID 使用負載平衡器來管理用戶端應用程式（例如 FabricPool ）的工作負載。負載平衡可將多個儲存節點的速度和連線容量最大化。

您可以使用 StorageGRID 負載平衡器服務（存在於所有閘道和管理節點上）、也可以連線至外部（第三方）負載平衡器。建議使用 StorageGRID 負載平衡器。

如需此工作的詳細資訊，請參閱一般"負載平衡考量"和"FabricPool 負載平衡的最佳實務做法"。

步驟

1. 選取或建立 StorageGRID 負載平衡器端點、或使用外部負載平衡器。

建立端點

a. 選取*建立端點*。

b. 如需 * 輸入端點詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
名稱	端點的描述性名稱。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為您建立的第一個端點為 10433 、但您可以輸入任何未使用的外部連接埠。如果您輸入 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。 • 注意： * 不允許其他網格服務使用的連接埠。請參閱"網路連接埠參考"。
用戶端類型	必須是 *S3 * 。
網路傳輸協定	選擇* HTTPS *。 • 注意 * ：支援與 StorageGRID 通訊、但不建議使用 TLS 加密。

c. 對於 *Select 綁定模式 * 步驟，請指定綁定模式。繫結模式可控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

模式	說明
全域（預設）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。

d. 對於 * 租戶存取 * 步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。 • 「允許所有租戶」 * 幾乎永遠是 FabricPool 所使用的負載平衡器端點的適當選項。 如果您使用 FabricPool 安裝精靈來安裝新的 StorageGRID 系統、但尚未建立任何租戶帳戶、則必須選取此選項。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

e. 對於 * 附加憑證 * 步驟、請選取下列其中一項：

欄位	說明
上傳憑證（建議）	使用此選項可上傳 CA 簽署的伺服器憑證、憑證私密金鑰及選用的 CA 套件組合。
產生憑證	使用此選項可產生自我簽署的憑證。如需詳細的輸入內容、請參閱"設定負載平衡器端點"。
使用 StorageGRID S3 憑證	只有在您已上傳或產生 StorageGRID 通用憑證的自訂版本時、才能使用此選項。如需詳細資訊、請參閱 "設定 S3 API 憑證" 。

f. 選擇 * 完成 * 返回 FabricPool 設定精靈。

g. 選擇 * 繼續 * 以前往租戶和貯體步驟。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

使用現有負載平衡器端點

a. 從 * 選取負載平衡器端點 * 下拉式清單中選取現有端點的名稱。

b. 選擇 * 繼續 * 以前往租戶和貯體步驟。

使用外部負載平衡器

a. 請填寫下列外部負載平衡器欄位。

欄位	說明
FQDN	外部負載平衡器的完整網域名稱（ FQDN ）。
連接埠	FabricPool 用來連線至外部負載平衡器的連接埠號碼。

欄位	說明
憑證	複製外部負載平衡器的伺服器憑證、然後貼到此欄位。

b. 選擇 * 繼續 * 以前往租戶和貯體步驟。

步驟 **3** 、共 **9** 步：租戶和貯體

租戶是可以使用 S3 應用程式在 StorageGRID 中儲存及擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、貯體、物件和一組特定功能。您必須先建立 StorageGRID 租戶、才能建立 FabricPool 將使用的貯體。

貯體是用來儲存租戶物件和物件中繼資料的容器。雖然有些租戶可能有許多貯體、但精靈可讓您一次只建立或選取一個租戶和一個貯體。您可以稍後使用租戶管理器來新增任何您需要的額外貯體。

您可以建立新的租戶和貯體以供 FabricPool 使用、也可以選取現有的租戶和貯體。如果您建立新的租戶、系統會自動為租戶的根使用者建立存取金鑰 ID 和秘密存取金鑰。

有關此任務的詳細信息，請參閱"建立一個客戶帳戶FabricPool 以供使用"和"建立S3儲存區並取得存取金鑰"。

步驟

建立新的租戶和貯體、或選擇現有的租戶。

新租戶和貯體

1. 若要建立新的租戶和貯體、請輸入 * 租戶名稱 * 。例如 `FabricPool tenant`：。
2. 根據您的StorageGRID系統是否使用，定義租用戶帳戶的根存取權限"身分識別聯盟"，"單一登入（ SSO ）"，或兩者兼而有之。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

3. 對於 * 儲存庫名稱 * 、請輸入儲存 ONTAP 資料時 FabricPool 將使用的儲存庫名稱。例如 `fabricpool-bucket`：。

   您無法在建立貯體之後變更貯體名稱。

4. 為此貯體選取 * 區域 * 。

   使用預設區域(`us-east-1`）、除非您預期未來會使用 ILM 來根據貯體的區域篩選物件。

5. 選取 * 建立並繼續 * 以建立租戶和貯體、並前往下載資料步驟

選擇租戶和貯體

現有的租戶帳戶必須至少有一個未啟用版本設定的貯體。如果該租戶不存在任何貯體、則無法選取現有租戶帳戶。

1. 從 * 浮動授權名稱 * 下拉式清單中選取現有的浮動授權。
2. 從 * 貯體名稱 * 下拉式清單中選取現有貯體。

   FabricPool 不支援物件版本設定、因此不會顯示啟用版本設定的儲存區。

   請勿選擇已啟用 S3 物件鎖定的貯體來搭配 FabricPool 使用。

3. 選取 * 繼續 * 以前往下載資料步驟。

步驟 **4 / 9** ：下載 **ONTAP** 設定

在此步驟中、您可以下載檔案、以便在 ONTAP 系統管理員中輸入值。

步驟

1. （可選）選擇複製圖示（ ）將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。

   這些值會包含在下載檔案中、但您可能想要個別儲存。

2. 選取 * 下載 ONTAP 設定 * 下載包含您目前所輸入值的文字檔。

   此 `ONTAP_FabricPool_settings_*bucketname*.txt`檔案包含將 StorageGRID 設定為 FabricPool 雲端層的物件儲存系統所需的資訊、包括：

   - 負載平衡器連線詳細資料、包括伺服器名稱（ FQDN ）、連接埠和憑證
   - 儲存區名稱
   - 存取租戶帳戶根使用者的金鑰 ID 和秘密存取金鑰

3. 將複製的金鑰和下載的檔案儲存到安全的位置。

   在複製兩個存取金鑰、下載 ONTAP 設定或兩者之前、請勿關閉此頁面。關閉此頁面後、金鑰將無法使用。請務必將此資訊儲存在安全的位置、因為此資訊可用於從 StorageGRID 系統取得資料。

4. 選取核取方塊以確認您已下載或複製存取金鑰 ID 和秘密存取金鑰。
5. 選取 * 繼續 * 以移至 ILM 儲存資源池步驟。

步驟 **5** （共 **9** 步）：選擇一個儲存池

儲存池是一組儲存節點。當您選取儲存池時、您會決定 StorageGRID 將使用哪些節點來儲存從 ONTAP 分層的資料。

如需此步驟的詳細資訊，請參閱"建立儲存資源池"。

步驟

1. 從 * 站台 * 下拉式清單中、選取您要用於從 ONTAP 分層資料的 StorageGRID 站台。
2. 從 * 儲存池 * 下拉式清單中、選取該站台的儲存池。

   站台的儲存池包含該站台的所有儲存節點。

3. 選取 * 繼續 * 以移至 ILM 規則步驟。

第 **6** 步、共 **9** 步：檢閱 **FabricPool** 的 **ILM** 規則

資訊生命週期管理（ ILM ）規則可控制 StorageGRID 系統中所有物件的放置、持續時間和擷取行為。

FabricPool 安裝精靈會自動建立建議的 ILM 規則以供 FabricPool 使用。此規則僅適用於您指定的貯體。它在單一站台使用 2+1 銷毀編碼來儲存從 ONTAP 分層的資料。

有關此步驟的詳細信息，請參閱"建立ILM規則"和"搭配 FabricPool 資料使用 ILM 的最佳實務做法"。

步驟

1. 檢閱規則詳細資料。

欄位	說明
規則名稱	自動產生且無法變更
說明	自動產生且無法變更
篩選器	貯體名稱 此規則僅適用於儲存在您指定的貯體中的物件。
參考時間	擷取時間 放置指示會在物件最初儲存至貯體時開始。
放置指示	使用 2+1 銷毀編碼

2. 依 * 時段 * 和 * 儲存池 * 排序保留圖、以確認放置指示。
   - 規則的 * 時段 * 是 * 天 0 - 永遠 * 。* 第 0 天 * 表示當資料從 ONTAP 分層時會套用規則。* Forever * 表示 StorageGRID ILM 不會刪除已從 ONTAP 分層的資料。
   - 規則的 * 儲存池 * 是您選取的儲存池。* EC 2+1 * 表示資料將使用 2+1 銷毀編碼來儲存。每個物件都會儲存為兩個資料片段和一個同位元檢查片段。每個物件的三個片段將儲存至單一站台的不同儲存節點。
3. 選取 * 建立並繼續 * 以建立此規則、並前往 ILM 原則步驟。

第 **7** 步、共有 **9** 步：審查並啟動 **ILM** 原則

在 FabricPool 安裝精靈建立 ILM 規則以供 FabricPool 使用之後，它會建立 ILM 原則。您必須先仔細模擬並檢閱此原則、然後再加以啟動。

有關此步驟的詳細信息，請參閱"建立ILM原則"和"搭配 FabricPool 資料使用 ILM 的最佳實務做法"。

當您啟動新的 ILM 原則時、 StorageGRID 會使用該原則來管理網格中所有物件（包括現有物件和新擷取的物件）的放置、持續時間和資料保護。在某些情況下、啟動新原則可能會導致現有物件移至新位置。

為了避免資料遺失、請勿使用會過期或刪除 FabricPool 雲端層資料的 ILM 規則。將保留期間設為 * 永遠 * 、以確保 FabricPool 物件不會被 StorageGRID ILM 刪除。

步驟

1. （可選）更新系統生成的 * 策略名稱 * 。根據預設、系統會將「 + FabricPool 」附加至作用中或非作用中原則的名稱、但您可以提供自己的名稱。
2. 檢閱非作用中原則中的規則清單。
   - 如果您的網格沒有非作用中的 ILM 原則、精靈會複製作用中原則並將新規則新增至頂端、藉此建立非作用中原則。
   - 如果您的網格已有非作用中的 ILM 原則、且該原則使用與作用中 ILM 原則相同的規則和順序、則精靈會將新規則新增至非作用中原則的頂端。

◦ 如果非作用中原則包含不同的規則或不同於作用中原則的順序、則精靈會複製作用中原則並將新規則新增至最上方、藉此建立新的非作用中原則。

3. 檢閱新非作用中原則中的規則順序。

   因為 FabricPool 規則是第一個規則、所以在評估原則中的其他規則之前、會先放置 FabricPool 儲存庫中的任何物件。任何其他儲存區中的物件都會依後續規則置於原則中。

4. 檢閱保留圖表、瞭解如何保留不同的物件。

   a. 選取 * 全部展開 * 以查看非作用中原則中每個規則的保留圖表。

   b. 選取 * 時段 * 和 * 儲存池 * 以檢閱保留圖表。確認適用於 FabricPool 貯體或租戶的任何規則都會保留物件 * 永遠 * 。

5. 檢閱非作用中原則後、請選取 * 啟動並繼續 * 來啟動原則、然後前往流量分類步驟。

   ILM 原則中的錯誤可能導致無法修復的資料遺失。在啟動之前、請先仔細檢閱原則。

步驟 **8** （共 **9** 步）：建立流量分類原則

FabricPool 設定精靈可選擇建立流量分類原則、以用於監控 FabricPool 工作負載。系統建立的原則會使用相符的規則來識別與您建立的貯體相關的所有網路流量。此原則僅監控流量、不會限制 FabricPool 或任何其他用戶端的流量。

如需此步驟的詳細資訊，請參閱"建立FabricPool 一套適用於此功能的流量分類原則"。

步驟

1. 檢閱原則。
2. 如果要建立此流量分類原則、請選取 * 建立並繼續 * 。

   一旦 FabricPool 開始將資料分層至 StorageGRID 、您就可以前往「流量分類原則」頁面、檢視此原則的網路流量計量。之後、您也可以新增規則來限制其他工作負載、並確保 FabricPool 工作負載擁有大部分的頻寬。

3. 否則、請選取 * 略過此步驟 * 。

步驟 **9** 之 **9** ：檢視摘要

此摘要提供您設定項目的詳細資料、包括負載平衡器、租戶和貯體的名稱、流量分類原則、以及作用中的 ILM 原則、

步驟

1. 檢閱摘要。
2. 選擇*完成*。

後續步驟

完成 FabricPool 精靈後、請執行這些額外步驟。

步驟

1. 移至"設定 ONTAP 系統管理員"以輸入儲存的值、並完成連線的 ONTAP 端。您必須將 StorageGRID 新增為

雲端層、將雲端層附加至本機層以建立 FabricPool 、並設定磁碟區分層原則。

2. 前往"設定 DNS 伺服器"並確定 DNS 包含一筆記錄、可將 StorageGRID 伺服器名稱（完整網域名稱）與您將使用的每個 StorageGRID IP 位址建立關聯。
3. 請移至"其他關於功能與功能的最佳實務做法StorageGRID FabricPool"以瞭解 StorageGRID 稽核記錄和其他全域組態選項的最佳實務做法。

手動設定 StorageGRID

在 StorageGRID 中為 FabricPool 建立高可用性（HA）群組

設定StorageGRID 使用FabricPool 搭配使用的功能時、您可以選擇性地建立一或多個高可用度（HA）群組。HA 群組是每個節點包含 StorageGRID 負載平衡器服務的集合。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用 HA 群組來協助保持 FabricPool 資料連線可用。HA 群組使用虛擬 IP 位址（ VIP ）來提供高可用度的負載平衡器服務存取權。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、對 FabricPool 作業的影響微乎其微。

如需此工作的詳細資訊，請參閱"管理高可用度群組"。要使用 FabricPool 安裝嚮導完成此任務，請轉至"存取並完成 FabricPool 設定精靈"。

開始之前

- 您已檢閱"適用於高可用度群組的最佳實務做法"。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 如果您打算使用VLAN、則已建立VLAN介面。請參閱。 "設定VLAN介面"

步驟

1. 選擇*設定* > 網路 > 高可用性群組。
2. 選擇* Create （建立）。
3. 如需 * 輸入詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
HA 群組名稱	此 HA 群組的唯一顯示名稱。
說明（選用）	此 HA 群組的描述。

4. 在 * 新增介面 * 步驟中、選取您要在此 HA 群組中使用的節點介面。

   使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。

   您可以選取一或多個節點、但每個節點只能選取一個介面。

5. 對於「介面優先順序」步驟、請判斷此 HA 群組的主要介面和任何備份介面。

拖曳列以變更 * 優先順序 * 欄中的值。

清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。

如果 HA 群組包含多個介面、且作用中介面故障、則虛擬 IP （ VIP ）位址會依照優先順序移至第一個備份介面。如果該介面故障、VIP位址會移至下一個備份介面、依此類推。解決故障時、VIP位址會移回可用的最高優先順序介面。

6. 在 * 輸入 IP 位址 * 步驟中、請填寫下列欄位。

欄位	說明
子網路 CIDR	以 CIDR 表示法表示的 VIP 子網路位址和 #8212 ； IPv4 位址後面接著斜線和子網路長度（ 0-32 ）。 網路位址不得設定任何主機位元。例如 `192.16.0.0/22` ：。
閘道 IP 位址（選用）	選用。如果用於存取 StorageGRID 的 ONTAP IP 位址與 StorageGRID VIP 位址不在同一子網路上、請輸入 StorageGRID VIP 本機閘道 IP 位址。本機閘道IP位址必須位於VIP子網路內。
虛擬 IP 位址	為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內。 至少一個位址必須是 IPv4 。您也可以指定其他的IPv6位址。

7. 選擇* Create HA group（建立HA群組）、然後選取 Finish（完成）*。

在 **StorageGRID** 中為 **FabricPool** 建立負載平衡器端點

StorageGRID 使用負載平衡器來管理用戶端應用程式（例如 FabricPool ）的工作負載。負載平衡可將多個儲存節點的速度和連線容量最大化。

設定 StorageGRID 搭配 FabricPool 使用時、您必須設定負載平衡器端點、然後上傳或產生負載平衡器端點憑證、以保護 ONTAP 和 StorageGRID 之間的連線。

要使用 FabricPool 安裝嚮導完成此任務，請轉至"存取並完成 FabricPool 設定精靈"。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。
- 您已經檢閱了一般"負載平衡考量" "FabricPool 負載平衡的最佳實務做法"資訊以及。

步驟

1. 選擇*設定* > 網路 > 負載平衡器端點。
2. 選擇* Create （建立）。
3. 如需 * 輸入端點詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
名稱	端點的描述性名稱。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為您建立的第一個端點為 10433 、但您可以輸入任何未使用的外部連接埠。如果您輸入 80 或 443 、則端點只能在 Gateway Node 上設定。這些連接埠保留在管理節點上。 • 注意： * 不允許其他網格服務使用的連接埠。請參閱"網路連接埠參考"。 當您將 StorageGRID 附加為 FabricPool 雲端層時、您會將此號碼提供給 ONTAP 。
用戶端類型	選擇* S三*。
網路傳輸協定	選擇* HTTPS *。 • 注意 * ：支援與 StorageGRID 通訊、但不建議使用 TLS 加密。

4. 對於 *Select 綁定模式 * 步驟，請指定綁定模式。繫結模式可控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

模式	說明
全域（預設）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。

5. 對於 * 租戶存取 * 步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。 • 「允許所有租戶」 * 幾乎永遠是 FabricPool 所使用的負載平衡器端點的適當選項。 如果您尚未建立任何租戶帳戶、則必須選取此選項。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

6. 對於 * 附加憑證 * 步驟、請選取下列其中一項：

欄位	說明
上傳憑證（建議）	使用此選項可上傳 CA 簽署的伺服器憑證、憑證私密金鑰及選用的 CA 套件組合。
產生憑證	使用此選項可產生自我簽署的憑證。如需詳細的輸入內容、請參閱"設定負載平衡器端點"。
使用 StorageGRID S3 憑證	只有在您已上傳或產生 StorageGRID 通用憑證的自訂版本時、才能使用此選項。如需詳細資訊、請參閱 "設定 S3 API 憑證" 。

7. 選擇* Create （建立）。

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。

在 **StorageGRID** 中為 **FabricPool** 建立租戶帳戶

您必須在Grid Manager中建立租戶帳戶FabricPool 、以供使用。

租戶帳戶可讓用戶端應用程式將物件儲存及擷取StorageGRID 到靜止不動的地方。每個租戶帳戶都有自己的帳戶ID、授權群組和使用者、庫位和物件。

如需此工作的詳細資訊，請參閱"建立租戶帳戶"。要使用 FabricPool 安裝嚮導完成此任務，請轉至"存取並完成 FabricPool 設定精靈"。

開始之前

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

步驟

1. 選擇*租戶*。

2. 選擇* Create （建立）。
3. 如需輸入詳細資料步驟、請輸入下列資訊。

欄位	說明
名稱	租戶帳戶的名稱。租戶名稱不一定是唯一的。建立租戶帳戶時、會收到唯一的數字帳戶ID。
說明（選用）	協助識別租戶的說明。
用戶端類型	必須是 **S2** （用於 FabricPool ）。
儲存配額（選用）	將此欄位保留空白以供 FabricPool 使用。

4. 對於 Select 權限步驟：
   a. 請勿選取 * 允許平台服務 * 。

      FabricPool 租戶通常不需要使用平台服務、例如 CloudMirror 複寫。

   b. 您也可以選擇 * 使用自己的身分識別來源 * 。
   c. 請勿選取 * 允許 S3 選取 * 。

      FabricPool 租戶通常不需要使用 S3 Select 。

   d. （可選）選取「使用網格聯合連線」，以允許租戶使用 "網格同盟連線" 進行帳戶同步和跨網格複寫。然後，選取要使用的網格聯合連線。
5. 對於定義根存取權限步驟，根據您的StorageGRID系統是否使用"身分識別聯盟"，"單一登入（ SSO ）"，或兩者兼而有之。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

6. 選取*建立租戶*。

在 **StorageGRID** 中為 **FabricPool** 建立 **S3** 儲存貯體並取得存取金鑰

在將StorageGRID 支援FabricPool 功能與功能性工作負載一起使用之前、您必須先建立S3儲存庫來儲存FabricPool 您的功能性資料。您也需要取得將用於FabricPool 執行此功能的

租戶帳戶的存取金鑰和秘密存取金鑰。

有關此任務的詳細信息，請參閱"建立S3儲存區"和"建立自己的S3存取金鑰"。要使用 FabricPool 安裝嚮導完成此任務，請轉至"存取並完成 FabricPool 設定精靈"。

開始之前

- 您已建立一個可供FabricPool 使用的租戶帳戶。
- 您擁有租戶帳戶的「根目錄」存取權。

步驟

1. 登入租戶管理程式。

   您可以執行下列其中一項：

   - 在Grid Manager的「租戶帳戶」頁面中、選取租戶的*登入*連結、然後輸入您的認證資料。
   - 在網頁瀏覽器中輸入租戶帳戶的URL、然後輸入您的認證資料。

2. 建立S3儲存庫以供FabricPool 資料使用。

   您必須為ONTAP 計畫使用的每個叢集建立獨特的儲存庫。

   a. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   b. 選取*建立桶*。

   c. 輸入您要搭配 FabricPool 使用的 StorageGRID 貯體名稱。例如 `fabricpool-bucket` ：。

      您無法在建立貯體之後變更貯體名稱。

   d. 選取此儲存區的區域。

      預設情況下，所有儲存桶均在 `us-east-1`地區。如果預設區域配置為 `us-east-1`，該其他區域最初是在下拉式選單中選擇的。

   e. 選擇*繼續*。

   f. 選取*建立桶*。

      請勿為 FabricPool 貯體選取 * 啟用物件版本管理 * 。同樣地、請勿編輯 FabricPool 儲存庫以使用 * 可用 * 或非預設一致性。FabricPool 儲存區的建議儲存區一致性為 * 新寫入後讀取 * 、這是新儲存區的預設一致性。

3. 建立存取金鑰和秘密存取金鑰。

   a. 選擇*儲存設備（S3）>*我的存取金鑰。

   b. 選取*建立金鑰*。

   c. 選取*建立存取金鑰*。

   d. 將存取金鑰ID和秘密存取金鑰複製到安全位置、或選取*下載.csv*以儲存內含存取金鑰ID和秘密存取金鑰的試算表檔案。

當您將「靜態」設定為「雲端層」時、將會在ONTAP 「靜態」中輸入這些值StorageGRID 。FabricPool

如果您未來在 StorageGRID 中產生新的存取金鑰和秘密存取金鑰、請先在 ONTAP 中輸入新金鑰、然後再從 StorageGRID 刪除舊值。否則、 ONTAP 可能會暫時失去對 StorageGRID 的存取權。

配置 **StorageGRID ILM** 以進行 **FabricPool** 數據

您可以使用這個簡單的範例原則做為自己 ILM 規則和原則的起點。

本範例假設您正在為StorageGRID 位於科羅拉多州丹佛的單一資料中心、擁有四個儲存節點的一套系統設計ILM規則和ILM原則。本範例中的 FabricPool 資料使用名為的貯體 `fabricpool-bucket`。

下列ILM規則和原則僅為範例。有許多方法可以設定ILM規則。在啟動新原則之前、請先進行模擬、確認其運作方式符合保護內容免於遺失的目的。若要深入瞭解"使用ILM管理物件"、請參閱。

為了避免資料遺失、請勿使用會過期或刪除 FabricPool 雲端層資料的 ILM 規則。將保留期間設為 * 永遠 * 、以確保 FabricPool 物件不會被 StorageGRID ILM 刪除。

開始之前

- 您已檢閱"搭配 FabricPool 資料使用 ILM 的最佳實務做法"。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"ILM 或 Root 存取權限"。
- 如果您是從早於 StorageGRID 11.7 的版本升級至 StorageGRID 12.1，則您已設定了要使用的儲存資源池。通常，您應該為每個用於儲存資料的 StorageGRID 站台建立一個儲存資源池。（從 11.7 版開始，系統會自動為每個站台建立儲存資源池。）

如果您最初安裝的是 StorageGRID 11.7 或 11.8 、則不適用此先決條件。當您最初安裝其中任一版本時、系統會自動為每個站台建立儲存資源池。

步驟

1. 建立僅適用於中資料的 ILM 規則 `fabricpool-bucket`。此範例規則會建立銷毀編碼複本。

規則定義	範例值
規則名稱	FabricPool 資料的 2+1 銷毀編碼
儲存區名稱	`fabricpool-bucket` 您也可以篩選FabricPool 出這個帳戶。

規則定義	範例值
進階篩選器	物件大小大於 0.2 MB 。 • 注意： * FabricPool 只寫入 4 MB 物件、但您必須新增物件大小篩選器、因為此規則使用銷毀編碼。
參考時間	擷取時間
時間週期和刊登位置	從第 0 天起、永遠儲存 在丹佛使用 2+1 EC 配置來銷毀編碼來儲存物件、並將這些物件永遠保留在 StorageGRID 中。 為了避免資料遺失、請勿使用會過期或刪除 FabricPool 雲端層資料的 ILM 規則。
擷取行為	平衡

2. 建立預設的 ILM 規則、為第一個規則不相符的任何物件建立兩個複寫複本。請勿選擇基本篩選條件（租戶帳戶或貯體名稱）或任何進階篩選條件。

規則定義	範例值
規則名稱	兩個複寫複本
儲存區名稱	無
進階篩選器	無
參考時間	擷取時間
時間週期和刊登位置	從第 0 天起、永遠儲存 在丹佛複製 2 份複本以儲存物件。
擷取行為	平衡

3. 建立 ILM 原則並選取兩個規則。由於複寫規則不使用任何篩選器、因此它可以是原則的預設（最後）規則。
4. 將測試物件擷取至網格。
5. 使用測試物件模擬原則、以驗證行為。
6. 啟動原則。

啟用此原則StorageGRID 時、將物件資料放置如下：

- 從中的 FabricPool 階層式資料 `fabricpool-bucket`將使用 2+1 銷毀編碼方案進行銷毀編碼。兩個資料片段和一個同位元檢查片段將放置在三個不同的儲存節點上。
- 所有其他儲存區中的所有物件都會複寫。將會建立兩個複本、並放置在兩個不同的儲存節點上。
- 這些複本將永遠保留在 StorageGRID 中。StorageGRID ILM 不會刪除這些物件。

在 **StorageGRID** 中為 **FabricPool** 建立流量分類原則

您可以選擇性地設計StorageGRID 一套「動態流量分類」原則、以最佳化FabricPool 針對該工作負載的服務品質。

如需此工作的詳細資訊，請參閱"管理流量分類原則"。要使用 FabricPool 安裝嚮導完成此任務，請轉至"存取並完成 FabricPool 設定精靈"。

開始之前

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

關於這項工作

建立FabricPool 適用於功能的流量分類原則的最佳實務做法取決於工作負載、如下所示：

- 如果您計畫將 FabricPool 主要工作負載資料分層至 StorageGRID 、則應確保 FabricPool 工作負載擁有大部分的頻寬。您可以建立流量分類原則、以限制所有其他工作負載。

  一般FabricPool 而言、將不區分寫入作業的優先順序、改為執行不必要的讀取作業。

  例如、如果其他S3用戶端使用StorageGRID 此功能、您應該建立流量分類原則。您可以限制其他儲存區、租戶、IP子網路或負載平衡器端點的網路流量。

- 一般而言、您不應對任何 FabricPool 工作負載施加服務品質限制、而應僅限制其他工作負載。
- 對其他工作負載的限制、應考慮到這些工作負載的行為。所規定的限制也會因網格的規模和功能、以及預期的使用量而有所不同。

步驟

1. 選擇*配置* > 網路 > 流量分類。
2. 選擇* Create （建立）。
3. 輸入原則的名稱和說明（選用）、然後選取 * 繼續 * 。
4. 針對 [新增符合的規則] 步驟，至少新增一個規則。
   a. 選取 * 新增規則 *
   b. 針對類型、選取 * 負載平衡器端點 * 、然後選取您為 FabricPool 建立的負載平衡器端點。

      您也可以選取FabricPool 「綁定帳戶」或「桶」。

   c. 如果您想要此流量原則限制其他端點的流量、請選取 * 逆向比對 * 。
5. 您也可以新增一或多個限制、以控制符合規則的網路流量。

StorageGRID 會收集指標、即使您沒有新增任何限制、也能瞭解流量趨勢。

a. 選取 * 新增限制 * 。

b. 選取您要限制的流量類型和要套用的限制。

6. 選擇*繼續*。

7. 閱讀並檢閱流量分類原則。使用 * 上一頁 * 按鈕返回並視需要進行變更。當您對原則感到滿意時、請選取 * 儲存並繼續 * 。

完成後

"檢視網路流量指標"驗證原則是否強制執行您預期的流量限制。

配置 ONTAP System Manager，將 StorageGRID 新增為 FabricPool 雲端層

取得必要的 StorageGRID 資訊之後、您可以前往 ONTAP 將 StorageGRID 新增為雲端層。

開始之前

- 如果您已完成 FabricPool 安裝精靈、表示您已 `ONTAP_FabricPool_settings_*bucketname*.txt`下載檔案。
- 如果您手動設定 StorageGRID 、您會擁有 StorageGRID 所使用的完整網域名稱（ FQDN ）、或 StorageGRID HA 群組的虛擬 IP （ VIP ）位址、負載平衡器端點的連接埠編號、負載平衡器憑證、 租戶帳戶根使用者的存取金鑰 ID 和秘密金鑰、以及貯體 ONTAP 在該租戶中使用的名稱。

存取 ONTAP 系統管理員

這些指示說明如何使用 ONTAP 系統管理員將 StorageGRID 新增為雲端層。您可以使用 ONTAP CLI 完成相同的組態。如需相關指示、請前往 "適用於 FabricPool 的 ONTAP 文件"。

步驟

1. 存取要分層至 StorageGRID 之 ONTAP 叢集的系統管理員。
2. 以叢集管理員身分登入。
3. 瀏覽 * 儲存 * > * 階層 * > * 新增雲端階層 * 。
4. 從物件存放區提供者清單中選取 * StorageGRID * 。

輸入 StorageGRID 值

如需詳細資訊、請參閱 "適用於 FabricPool 的 ONTAP 文件" 。

步驟

1. 使用您手動取得的檔案或值、填寫「新增雲端層」表單 `ONTAP_FabricPool_settings_*bucketname*.txt`。

欄位	說明
名稱	輸入此雲端層的唯一名稱。您可以接受預設值。

欄位	說明
URL 樣式	如果是"已設定 S3 端點網域名稱"，請選擇「虛擬託管式 URL」。 **Path-Style URL** 是 ONTAP 的預設值，但建議 StorageGRID 使用虛擬託管式請求。如果您在「伺服器名稱 （FQDN）」欄位中提供的是 IP 位址而不是網域名稱，則必須使用 **Path-Style URL**。
伺服器名稱（ FQDN ）	輸入您用於 StorageGRID 的完整網域名稱（ FQDN ）、或 StorageGRID HA 群組的虛擬 IP （ VIP ）位址。例如 `s3.storagegrid.company.com`：。 請注意下列事項： • 您在此處指定的 IP 位址或網域名稱必須符合您上傳或為 StorageGRID 負載平衡器端點產生的憑證。 • 如果您提供網域名稱、則 DNS 記錄必須對應至您要用來連線至 StorageGRID 的每個 IP 位址。請參閱。 "設定 DNS 伺服器"
SSL	啟用（預設）。
物件存放區憑證	貼上您用於 StorageGRID 負載平衡器端點的憑證 PEM 、包括：`-----BEGIN CERTIFICATE-----`和 `-----END CERTIFICATE-----`。 *附註：*如果中介CA核發StorageGRID 了此功能驗證、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。
連接埠	輸入 StorageGRID 負載平衡器端點使用的連接埠。ONTAP 會在連線至 StorageGRID 時使用此連接埠。例如 10433 。
存取金鑰和秘密金鑰	輸入 StorageGRID 租戶帳戶根使用者的存取金鑰 ID 和秘密存取金鑰。 • 提示 * ：如果您在未來在 StorageGRID 中產生新的存取金鑰和秘密存取金鑰、請在 ONTAP 中輸入新金鑰、然後再從 StorageGRID 刪除舊值。否則、 ONTAP 可能會暫時失去對 StorageGRID 的存取權。
容器名稱	輸入您建立用於此 ONTAP 層的 StorageGRID 貯體名稱。

2. 在 ONTAP 中完成最終的 FabricPool 組態。
   a. 將一或多個集合體附加至雲端層。
   b. 您也可以建立磁碟區分層原則。

使用 **FabricPool** 為 **StorageGRID** 配置 **DNS** 伺服器項目

設定高可用度群組、負載平衡器端點和 S3 端點網域名稱之後、您必須確保 DNS 包含 StorageGRID 所需的項目。您必須在安全性憑證中為每個名稱以及您可能使用的每個 IP 位址加入 DNS 項目。

請參閱。 "負載平衡考量"

StorageGRID 伺服器名稱的 DNS 項目

新增 DNS 項目、將 StorageGRID 伺服器名稱（完整網域名稱）與您將使用的每個 StorageGRID IP 位址建立關聯。您在 DNS 中輸入的 IP 位址取決於您是否使用 HA 群組的負載平衡節點：

- 如果您已設定 HA 群組、 ONTAP 將會連線至該 HA 群組的虛擬 IP 位址。
- 如果您不使用 HA 群組、 ONTAP 可以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。
- 如果伺服器名稱解析為多個 IP 位址、則 ONTAP 會與所有 IP 位址建立用戶端連線（最多 16 個 IP 位址）。建立連線時、會以循環配置資源的方式來取用IP位址。

虛擬主機式請求的 DNS 項目

如果您已定義"S3 端點網域名稱"並將使用虛擬託管風格的請求，請為所有必要的 S3 端點網域名稱新增 DNS 條目，包括任何萬用字元名稱。

適用於 FabricPool 的 StorageGRID 最佳實務做法

StorageGRID 高可用性（HA）群組搭配 FabricPool 的最佳實務做法

在將 StorageGRID 附加為 FabricPool 雲端層之前、請先瞭解 StorageGRID 高可用度（ HA ）群組、並檢閱將 HA 群組與 FabricPool 搭配使用的最佳實務做法。

什麼是HA群組？

高可用度（ HA ）群組是來自多個 StorageGRID 閘道節點、管理節點或兩者的介面集合。HA 群組有助於保持用戶端資料連線可用。如果 HA 群組中的作用中介面故障、備份介面可以管理工作負載、而對 FabricPool 作業的影響微乎其微。

每個HA群組都提供高可用度的存取權限、可存取相關節點上的共享服務。例如、僅由閘道節點或管理節點和閘道節點上的介面組成的HA群組、可提供對共享負載平衡器服務的高可用度存取。

若要深入瞭解高可用度群組、請參閱"管理高可用度（ HA ）群組"。

使用 HA 群組

為 FabricPool 建立 StorageGRID HA 群組的最佳實務做法取決於工作負載。

- 如果您計畫將 FabricPool 與主要工作負載資料搭配使用、則必須建立至少包含兩個負載平衡節點的 HA 群組、以避免資料擷取中斷。
- 如果您計畫使用FabricPool 僅供Snapshot使用的磁碟區分層原則或非主要的本機效能層（例如災難恢復位置或NetApp SnapMirror®目的地）、則只能設定一個節點的HA群組。

這些指示說明如何設定主動備份HA的HA群組（一個節點為作用中、一個節點為備份）。不過、您可能偏好使用DNS循環配置資源或主動式HA。若要瞭解其他 HA 組態的優點、請參閱"HA群組的組態選項"。

在將 StorageGRID 附加為 FabricPool 雲端層之前、請先檢閱搭配 FabricPool 使用負載平衡器的最佳實務做法。

若要深入瞭解 StorageGRID 負載平衡器和負載平衡器憑證的一般資訊，請參閱"負載平衡考量"。

租戶存取用於 FabricPool 的負載平衡器端點的最佳實務做法

您可以控制哪些租戶可以使用特定負載平衡器端點來存取其貯體。您可以允許所有租戶、允許某些租戶、或封鎖某些租戶。建立 FabricPool 使用的負載平衡端點時、請選取 * 允許所有租戶 * 。ONTAP 會加密放置在 StorageGRID 儲存區中的資料、因此這種額外的安全層幾乎不會提供額外的安全性。

安全性憑證的最佳實務做法

當您建立用於 FabricPool 的 StorageGRID 負載平衡器端點時、您會提供安全性憑證、讓 ONTAP 能夠使用 StorageGRID 進行驗證。

在大多數情況下、 ONTAP 和 StorageGRID 之間的連線應該使用傳輸層安全性（ TLS ）加密。支援不使用 TLS 加密的 FabricPool 、但不建議使用。當您選取 StorageGRID 負載平衡器端點的網路傳輸協定時、請選取 **HTTPS** 。然後提供安全性憑證、允許 ONTAP 驗證 StorageGRID 。

若要深入瞭解負載平衡端點的伺服器憑證：

- "管理安全性憑證"
- "負載平衡考量"
- "伺服器憑證的強化準則"

將憑證新增至 ONTAP

當您將 StorageGRID 新增為 FabricPool 雲端層時、必須在 ONTAP 叢集上安裝相同的憑證、包括根憑證和任何次級憑證授權單位（ CA ）憑證。

管理憑證過期

如果用於保護 ONTAP 與 StorageGRID 之間連線的憑證過期、 FabricPool 將暫時停止運作、 ONTAP 將暫時失去對 StorageGRID 階層資料的存取權。

若要避免憑證過期問題、請遵循下列最佳實務做法：

- 請仔細監控任何警告即將到期的憑證、例如 * 負載平衡器端點憑證到期 * 和 * S3 API* 警示的通用伺服器憑證到期日。
- 請務必保持憑證的 StorageGRID 和 ONTAP 版本同步。如果您更換或續約用於負載平衡器端點的憑證、則必須更換或續約 ONTAP 用於雲端層的同等憑證。
- 使用公開簽署的 CA 憑證。如果您使用 CA 簽署的憑證、則可以使用 Grid Management API 來自動化憑證輪換。這可讓您在不中斷營運的情況下、更換即將到期的憑證。
- 如果您已產生自我簽署的 StorageGRID 憑證、且該憑證即將過期、則必須在現有憑證過期之前、手動在 StorageGRID 和 ONTAP 中置換憑證。如果自我簽署的憑證已經過期、請在 ONTAP 中關閉憑證驗證、以防止存取遺失。

如需相關指示、請參閱 "NetApp 知識庫：如何在現有的 ONTAP FabricPool 部署上設定新的 StorageGRID 自我簽署伺服器憑證"。

搭配 **FabricPool** 資料使用 **StorageGRID ILM** 的最佳實務做法

如果您使用 FabricPool 將資料分層至 StorageGRID 、則必須瞭解使用 StorageGRID 資訊生命週期管理（ ILM ）搭配 FabricPool 資料的需求。

不知道什麼是無法理解的ILM規則或原則。FabricPool StorageGRID如果無法設定不正確的ILM原則、就可能發生資料遺失StorageGRID 。如需詳細資訊、請參閱"使用 ILM 規則來管理物件"和"建立 ILM 原則"。

搭配 **FabricPool** 使用 **ILM** 的準則

當您使用 FabricPool 設定精靈時、精靈會自動為您建立的每個 S3 儲存區建立新的 ILM 規則、並將該規則新增至非作用中原則。系統會提示您啟動原則。自動建立的規則遵循建議的最佳實務做法：在單一站台使用 2+1 銷毀編碼。

如果您是手動設定 StorageGRID 、而不是使用 FabricPool 設定精靈、請檢閱這些準則、確保您的 ILM 規則和 ILM 原則適合 FabricPool 資料和業務需求。您可能需要建立新規則並更新使用中的 ILM 原則、才能符合這些準則。

- 您可以使用複寫和銷毀編碼規則的任何組合來保護雲端層資料。

  建議的最佳實務做法是在站台內使用2+1銷毀編碼、以達到具成本效益的資料保護。銷毀編碼使用的CPU較多、但儲存容量卻遠低於複寫。4+1和6+1方案使用的容量比2+1方案少。不過、如果您需要在網格擴充期間新增儲存節點、4+1和6+1配置的彈性會較低。如需詳細資訊、請參閱 "新增銷毀編碼物件的儲存容量"。

- 套用至FabricPool 資料的每個規則都必須使用銷毀編碼、否則必須至少建立兩個複製複本。

  ILM規則只會在任何時間段建立一個複寫複本、使資料有永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

- 如果您需要"從 StorageGRID 移除 FabricPool 資料"、請使用 ONTAP 擷取 FabricPool Volume 的所有資料、並將其提升至效能層。

  為了避免資料遺失、請勿使用會過期或刪除 FabricPool 雲端層資料的 ILM 規則。將每個 ILM 規則的保留期間設定為 * 永遠 * 、以確保 FabricPool 物件不會被 StorageGRID ILM 刪除。

- 請勿建立將 FabricPool 雲端層資料從儲存庫移出至其他位置的規則。您無法使用雲端儲存池將 FabricPool 資料移至其他物件存放區。

  由於從雲端儲存資源池目標擷取物件的延遲增加、因此不支援使用FabricPool 含有支援功能的雲端儲存資源池。

- 從功能完善的9.8開始ONTAP 、您可以選擇性地建立物件標記、以協助分類及排序階層式資料、以便更輕鬆地進行管理。例如、您只能在FabricPool 附加StorageGRID 到該功能的不含資料的地方設定標籤。然後、當您在StorageGRID 物件標籤進階篩選器中建立ILM規則時、可以使用物件標籤進階篩選器來選取及放置此資料。

StorageGRID 全域設定搭配 **FabricPool** 的最佳實務做法

設定 StorageGRID 系統搭配 FabricPool 使用時、您可能需要變更其他 StorageGRID 選項。變更通用設定之前、請先考慮變更對其他 S3 應用程式的影響。

稽核訊息和記錄目的地

FabricPool 工作負載的讀取作業率通常很高、可能會產生大量的稽核訊息。

- 如果您不需要記錄FabricPool或任何其他 S3 應用程式的用戶端讀取操作，則可以選擇前往 設定 > 監控 > 稽核和系統日誌伺服器。將 用戶端讀取 設定變更為 錯誤 以減少稽核日誌中記錄的稽核訊息數量。看"設定日誌管理和外部系統日誌伺服器"了解詳情。
- 如果您有大型網格、請使用多種類型的 S3 應用程式、或是想要保留所有稽核資料、請設定外部 Syslog 伺服器、並遠端儲存稽核資訊。使用外部伺服器可將稽核訊息記錄的效能影響降至最低、而不會降低稽核資料的完整性。如需詳細資訊、請參閱 "外部syslog伺服器的考量" 。

物件加密

設定 StorageGRID 時、您可以選擇性地啟用"儲存物件加密的全域選項"、以瞭解是否需要其他 StorageGRID 用戶端的資料加密。從FabricPool 「支援」層級到StorageGRID 「支援」層級的資料已經加密、因此StorageGRID 不需要啟用「支援」功能。用戶端加密金鑰歸ONTAP 靜止所有。

物件壓縮

設定 StorageGRID 時、請勿啟用"用於壓縮儲存物件的全域選項"。從FabricPool 功能到StorageGRID 功能的分層資料已經被壓縮。使用 StorageGRID 選項不會進一步縮小物件的大小。

S3物件鎖定

如果您的StorageGRID系統啟用了全域 S3 物件鎖定設置，請不要啟用"S3物件鎖定"當您建立FabricPool儲存桶。 FabricPool儲存桶不支援 S3 物件鎖定。

貯體一致性

對於 FabricPool 貯體、建議的貯體一致性為 * 新寫入後讀取 * 、這是新貯體的預設一致性。請勿編輯 FabricPool 儲存庫以使用 * 可用 * 或 * 強式站台 * 。

分層**FabricPool**

如果 StorageGRID 節點使用從 NetApp ONTAP 系統指派的儲存設備、請確認該磁碟區未啟用 FabricPool 分層原則。例如、如果StorageGRID VMware主機上正在執行某個節點、請確保支援StorageGRID 該節點之資料存放區的磁碟區FabricPool 未啟用「分層原則」。停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

切勿使用FabricPool 無法將StorageGRID 任何與還原StorageGRID 本身相關的資料分層。將StorageGRID 資料分層還原StorageGRID 至物件、可增加疑難排解和作業複雜度。

從 **StorageGRID** 移除 **FabricPool** 資料

如果您需要移除目前儲存在 StorageGRID 中的 FabricPool 資料、則必須使用 ONTAP 來擷取 FabricPool Volume 的所有資料、並將其提升至效能層級。

開始之前

- 您已檢閱中的指示與考量事項 "將資料提升至效能層級"。
- 您使用的是 ONTAP 9.8 或更新版本。
- 您使用的是"支援的網頁瀏覽器"。
- 您屬於具有的 FabricPool 租戶帳戶的 StorageGRID 使用者群組"管理所有貯體或根目錄存取權限"。

關於這項工作

這些指示說明如何將資料從 StorageGRID 移回 FabricPool 。您可以使用 ONTAP 和 StorageGRID 租戶管理員來執行此程序。

步驟

1. 從 ONTAP 發出 `volume modify`命令。

   設 `tiering-policy`為 `none`以停止新的分層、並設 `cloud-retrieval-policy`為 `promote`以傳回先前分層至 StorageGRID 的所有資料。

   請參閱。 "將FabricPool 所有資料從一個數據區提升至效能層"

2. 等待作業完成。

   您可以將命令與選項 "檢查效能層級促銷的狀態"一起 `tiering`使用 `volume object-store`。

3. 升級作業完成後、請登入 FabricPool 租戶帳戶的 StorageGRID 租戶管理員。
4. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
5. 確認 FabricPool 貯體現在已空。
6. 如果貯體是空的、"刪除貯體"。

完成後

當您刪除貯體時、從 FabricPool 分層至 StorageGRID 的作業將無法繼續。然而、由於本機層仍附加至 StorageGRID 雲端層、 ONTAP 系統管理員將傳回錯誤訊息、指出儲存區無法存取。

若要避免出現這些錯誤訊息、請執行下列其中一項：

- 使用 FabricPool 鏡射將不同的雲端層附加到集合體。
- 將資料從 FabricPool Aggregate 移至非 FabricPool Aggregate 、然後刪除未使用的 Aggregate 。

如需相關指示、請參閱 "適用於 FabricPool 的 ONTAP 文件"。

使用 StorageGRID 租戶和用戶端

使用租戶帳戶

使用StorageGRID 綁定帳戶

租戶帳戶可讓您使用簡易儲存服務（ S3 ） REST API 來儲存及擷取 StorageGRID 系統中的物件。

什麼是租戶帳戶？

每個租戶帳戶都有自己的同盟或本機群組、使用者、 S3 貯體和物件。

租戶帳戶可用來分隔不同實體所儲存的物件。例如、多個租戶帳戶可用於下列任一使用案例：

- 企業使用案例： StorageGRID 如果在企業內部使用此功能、則網格的物件儲存設備可能會由組織內的不同部門加以分隔。例如、行銷部門、客戶支援部門、人力資源部門等可能有租戶帳戶。

  > 如果您使用 S3 用戶端協議，您也可以使用 S3 儲存桶和儲存桶策略在企業各部門之間隔離物件。您不需要建立單獨的租用戶帳戶。請參閱實施說明"S3 貯體和貯體原則"了解更多。

- 服務供應商使用案例： StorageGRID 如果服務供應商正在使用此功能、則網格的物件儲存設備可能會由租用儲存設備的不同實體加以分隔。例如、公司A、公司B、公司C等可能有租戶帳戶。

如何建立租戶帳戶

租戶帳戶是由建立"使用Grid Manager的網格管理員StorageGRID"的。建立租戶帳戶時、網格管理員會指定下列項目：

- 基本資訊、包括租戶名稱、用戶端類型（ S3 ）和選用的儲存配額。
- 租戶帳戶的權限、例如租戶帳戶是否可以使用 S3 平台服務、設定自己的身分識別來源、使用 S3 Select 或使用網格同盟連線。
- 租戶的初始根存取權、取決於 StorageGRID 系統是使用本機群組和使用者、身分識別聯盟或單一登入（ SSO ）。

此外、如果StorageGRID S3租戶帳戶需要符合法規要求、網格管理員也可以針對該系統啟用S3物件鎖定設定。啟用S3物件鎖定時、所有S3租戶帳戶都能建立及管理相容的儲存區。

設定S3租戶

之後"S3租戶帳戶已建立"、您可以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）
- 管理群組和使用者
- 使用網格聯合進行帳戶同步和跨網格複寫
- 管理S3存取金鑰

- 建立及管理 S3 儲存區
- 使用 S3 平台服務
- 使用S3 Select
- 監控儲存使用量

雖然您可以使用租戶管理程式來建立和管理 S3 貯體、但您必須使用"S3用戶端"或"S3 主控台"來擷取和管理物件。

如何登入及登出

Sign in 至 StorageGRID 租戶管理器

您可以在的網址列中輸入租戶的 URL 來存取租戶管理員"支援的網頁瀏覽器"。

開始之前

- 您擁有登入認證資料。
- 您可以使用網格管理員提供的 URL 來存取租戶管理程式。此URL的範例如下所示：

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  URL 一律包含完整網域名稱（ FQDN ）、管理節點的 IP 位址、或管理節點 HA 群組的虛擬 IP 位址。也可能包括連接埠號碼、 20 位數的租戶帳戶 ID 、或兩者。

- 如果 URL 不包含租戶的 20 位數帳戶 ID 、則您擁有此帳戶 ID 。
- 您使用的是"支援的網頁瀏覽器"。
- Cookie會在您的網頁瀏覽器中啟用。
- 您屬於具有"特定存取權限"的使用者群組。

步驟

1. 啟動。"支援的網頁瀏覽器"
2. 在瀏覽器的網址列中、輸入存取租戶管理程式的URL。
3. 如果系統提示您輸入安全性警示、請使用瀏覽器的安裝精靈來安裝憑證。
4. 登入租戶管理程式。

   顯示的登入畫面取決於您輸入的 URL 、以及是否已針對 StorageGRID 設定單一登入（ SSO ）。

未使用 **SSO**

如果 StorageGRID 未使用 SSO 、則會出現下列其中一個畫面：

- Grid Manager登入頁面。選取 * 租戶登入 * 連結。
- 租戶管理器登入頁面。 *帳戶*欄位可能已經填寫完畢。
  i. 如果租戶的20位數帳戶ID未顯示、請選取租戶帳戶名稱（如果出現在最近帳戶清單中）、或輸入帳戶ID。
  ii. 輸入您的使用者名稱和密碼。
  iii. 選擇*登入*。

  租戶管理器儀表板即會出現。

  iv. 如果您收到其他人的初始密碼、請選擇 * _ 使用者名稱 _ * > * 變更密碼 * 來保護您的帳戶安全。

使用 **SSO**

如果 StorageGRID 使用 SSO 、則會出現下列其中一個畫面：

- 您組織的 SSO 頁面。

  輸入您的標準 SSO 認證、然後選取 * 登入 * 。

- 租戶管理程式SSO登入頁面。
  i. 如果租戶的20位數帳戶ID未顯示、請選取租戶帳戶名稱（如果出現在最近帳戶清單中）、或輸入帳戶ID。
  ii. 選擇*登入*。
  iii. 在組織的SSO登入頁面上、以標準SSO認證登入。

  租戶管理器儀表板即會出現。

登出 **StorageGRID Tenant Manager**

完成租戶管理程式的使用後、您必須登出、以確保未經授權的使用者無法存取 StorageGRID 系統。根據瀏覽器Cookie設定、關閉瀏覽器可能不會將您登出系統。

步驟

1. 在使用者介面的右上角找到使用者名稱下拉式清單。
2. 選取使用者名稱、然後選取 * 登出 * 。

   - 如果未使用SSO：

     您已登出管理節點。隨即顯示「租戶管理程式」登入頁面。

     如果您登入多個管理節點、則必須登出每個節點。

◦ 如果啟用SSO：

您已登出您正在存取的所有管理節點。畫面會顯示「此功能的登入」頁面。StorageGRID您剛存取的租戶帳戶名稱會在「最近的帳戶」下拉式清單中列為預設名稱、並顯示租戶的*帳戶ID*。

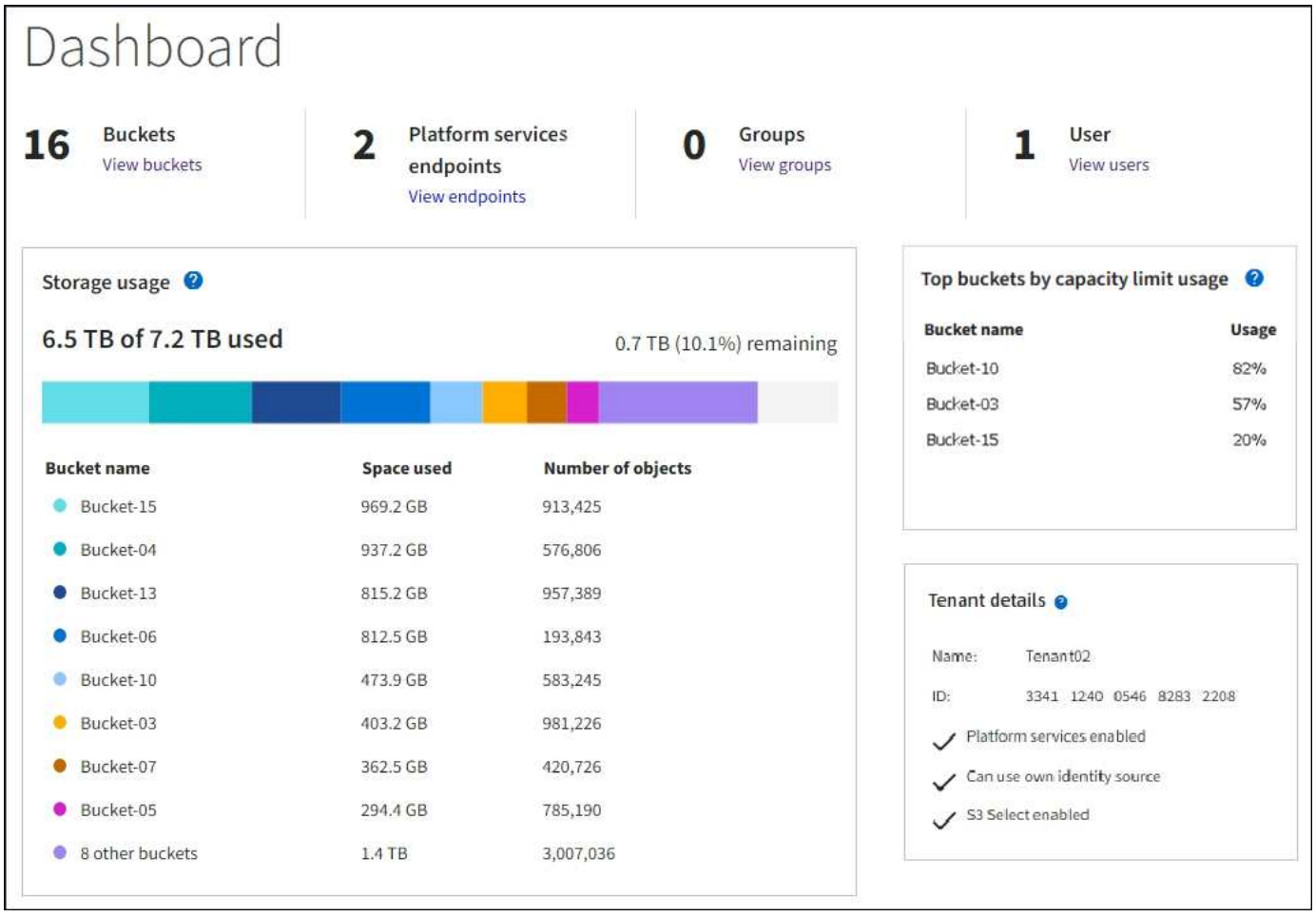
如果已啟用SSO、而且您也已登入Grid Manager、您也必須登出Grid Manager以登出SSO。

StorageGRID 中的租戶管理器儀表板

租用戶管理器儀表板概述了租用戶帳戶的配置以及租用戶 S3 儲存桶中物件使用的空間量。如果租戶有配額，儀表板會顯示已使用的配額量以及剩餘的配額量。如果存在與租用戶帳戶相關的任何錯誤，則錯誤將顯示在儀表板上。

屬於該租戶的所有物件的邏輯大小包括未完成和正在進行的分段上傳。此大小不包括用於 ILM 策略的額外實體空間。已用空間值是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。

物件上傳後、儀表板看起來像以下範例：



租戶帳戶資訊

儀表板頂端會顯示已設定的貯體或容器、群組和使用者數目。如果已設定任何平台服務端點、也會顯示其數量。

選取連結以檢視詳細資料。

視您擁有的和您設定的選項而定"租戶管理權限"、儀表板的其餘部分會顯示各種指南、儲存使用量、物件資訊和租戶詳細資料的組合。

儲存設備與配額使用量

「儲存設備」使用面板包含下列資訊：

- 租戶的物件資料量。

  此值表示上傳的物件資料總數量、不代表用來儲存這些物件複本及其中繼資料的空間。

- 如果已設定配額、則為物件資料可用的空間總量、以及剩餘空間的數量和百分比。配額會限制可擷取的物件資料量。

  > 配額使用量是根據內部預估、在某些情況下可能會超過。例如StorageGRID 、當租戶開始上傳物件時、會檢查配額、如果租戶超過配額、則會拒絕新的擷取。不過StorageGRID 、判斷是否超過配額時、不考慮目前上傳的大小。如果刪除物件、可能會暫時禁止租戶上傳新物件、直到重新計算配額使用量為止。配額使用量計算可能需要 10 分鐘或更長時間。

- 代表最大桶或容器之相對大小的長條圖。

  您可以將游標放在任何圖表區段上、以檢視該區段或容器所耗用的總空間。

- 若要對應長條圖、請列出最大的貯體或容器清單、包括物件資料的總數量、以及每個貯體或容器的物件數目。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

如果租戶擁有超過九個貯體或容器、則所有其他貯體或容器都會合併成清單底部的單一項目。

若要變更租戶管理程式中顯示的儲存值單位、請選取租戶管理程式右上角的使用者下拉式清單、然後選取 * 使用者偏好 * 。

配額使用量警示

如果 Grid Manager 已啟用配額使用量警示、則當配額不足或超過時、這些警示會顯示在租戶管理程式中、如下所示：

- 如果已使用90%以上的租戶配額、則會觸發*租戶配額使用量高*警示。

  請考慮要求網格管理員增加配額。

- 如果您超過配額、會有通知告訴您無法上傳新物件。

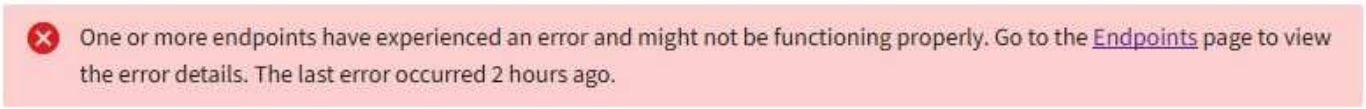
容量限制使用

如果您已為貯體設定容量限制、租戶管理器儀表板會依容量限制使用量顯示最大貯體清單。

如果沒有設定貯體限制、則其容量是無限的。不過、如果您的租戶帳戶有總儲存配額、而且達到該配額、則無論貯體的剩餘容量限制為何、您都無法擷取更多物件。

端點錯誤

如果您使用 Grid Manager 來設定一個或多個端點以搭配平台服務使用、租戶管理程式儀表板會在過去七天內發生任何端點錯誤時、顯示警示。



若要查看有關的詳細資料"平台服務端點錯誤"、請選取 * 端點 * 以顯示端點頁面。

租戶管理API

了解 StorageGRID Tenant Management API

您可以使用租戶管理REST API（而非租戶管理程式使用者介面）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。

租戶管理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與API互動。Swagger使用者介面提供每個API作業的完整詳細資料和文件。
- 用途"支援不中斷營運升級的版本管理"。

若要存取租戶管理API的Swagger文件：

1. 登入租戶管理程式。
2. 從租戶管理器的頂端、選取說明圖示、然後選取 * API 文件 * 。

API 作業

租戶管理API會將可用的API作業組織成下列區段：

- * 帳戶 * ：目前租戶帳戶的作業、包括取得儲存使用資訊。
- * 驗證 * ：執行使用者工作階段驗證的作業。

  租戶管理API支援承載權杖驗證方案。對於租戶登入、您可以在驗證要求的 JSON 本文中提供使用者名稱、密碼和帳戶 ID （即 `POST /api/v3/authorize`）。如果使用者已成功驗證、則會傳回安全性權杖。此權杖必須在後續API要求（「授權：承載權杖」）的標頭中提供。

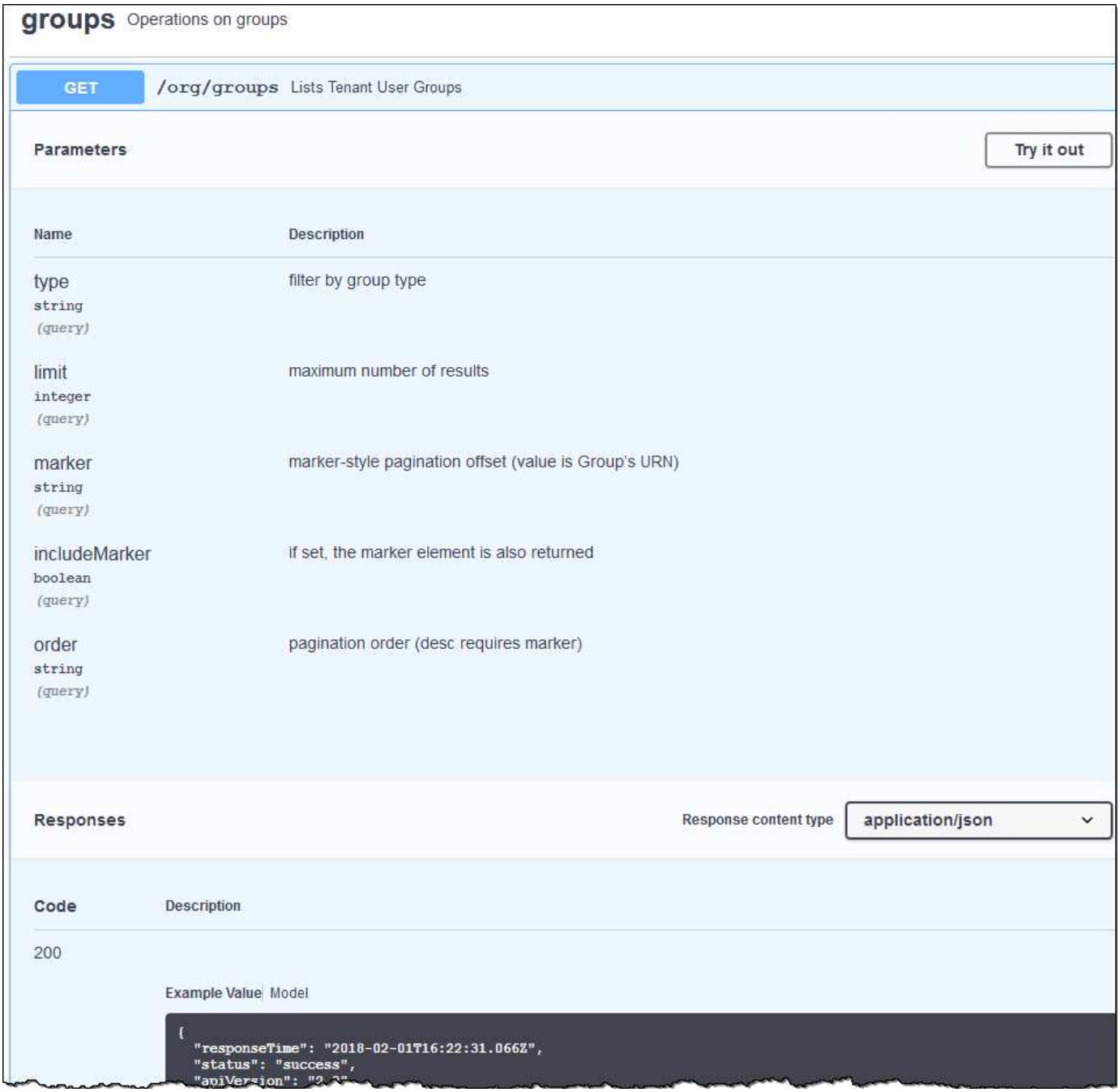
  如需改善驗證安全性的相關資訊，請參閱"防止跨網站要求偽造"。

  > 如果StorageGRID 啟用了單一登入（SSO）功能、您必須執行不同的驗證步驟。請參閱"網格管理API的使用說明"。

- * 組態 * ：與租戶管理 API 產品版本和版本相關的作業。您可以列出該版本所支援的產品版本和主要API版本。
- 容器：對 S3 儲存桶的操作。
- * 停用功能 * ：檢視可能已停用功能的作業。
- * 端點 * ：管理端點的作業。端點可讓S3儲存區使用外部服務StorageGRID 來進行CloudMirror複寫、通知或搜尋整合。
- * 網格聯合連線 * ：網格聯合連線和跨網格複寫的作業。
- * 群組 * ：管理本機租戶群組及從外部身分識別來源擷取同盟租戶群組的作業。
- * 身分識別來源 * ：設定外部身分識別來源及手動同步同盟群組與使用者資訊的作業。
- * ILM * ：資訊生命週期管理（ ILM ）設定的作業。
- * 地區 * ：用於確定已爲 StorageGRID 系統配置哪些區域的操作。
- **S1** ：管理租戶使用者 S3 存取金鑰的作業。
- **s3-configurations**：擷取 S3 全域配置的操作。
- **S3-object-lock** ：在全域 S3 物件鎖定設定上的作業、用於支援法規遵循。
- * 使用者 * ：檢視及管理租戶使用者的作業。

營運詳細資料

展開每個API作業時、您可以看到其HTTP動作、端點URL、任何必要或選用參數的清單、要求本文的範例（視需要）、以及可能的回應。



發出**API**要求

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. 選取HTTP動作以查看要求詳細資料。
2. 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。
3. 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。
4. 選擇*試用*。

5. 提供任何必要的參數、或視需要修改申請本文。
6. 選擇*執行*。
7. 檢閱回應代碼以判斷要求是否成功。

StorageGRID 租戶管理 API 版本控制

租戶管理API使用版本管理來支援不中斷營運的升級。

例如、此 Request URL 會指定 API 的版本 4 。

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

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

下列範例說明如何根據所做的變更類型來提高API版本。

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

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

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

過時的要求會以下列方式標示為已過時：

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

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

判斷目前版本支援哪些API版本

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

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

指定要求的**API**版本

您可以使用路徑參數(`/api/v4`（）或標頭(`Api-Version: 4`（）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/v4/grid/accounts

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

防止 **StorageGRID** 中的跨網站請求偽造

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、請在驗證期間將參數設 `csrfToken`為 `true`。預設值為 `false`。

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

如果為 True 、則 `GridCsrfToken`會以隨機值設定 Cookie 來登入 Grid Manager 、並以隨機值

`AccountCsrfToken`將 Cookie 設定為登入 Tenant Manager 。

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、標頭的值設為 CSRF Token Cookie 的值。
- 對於接受表單編碼實體的端點： `csrfToken`表單編碼的要求本文參數。

若要設定 CSRF 保護、請使用"網格管理API"或"租戶管理API"。

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

使用網格同盟連線

同步 **StorageGRID** 中的租戶群組和使用者

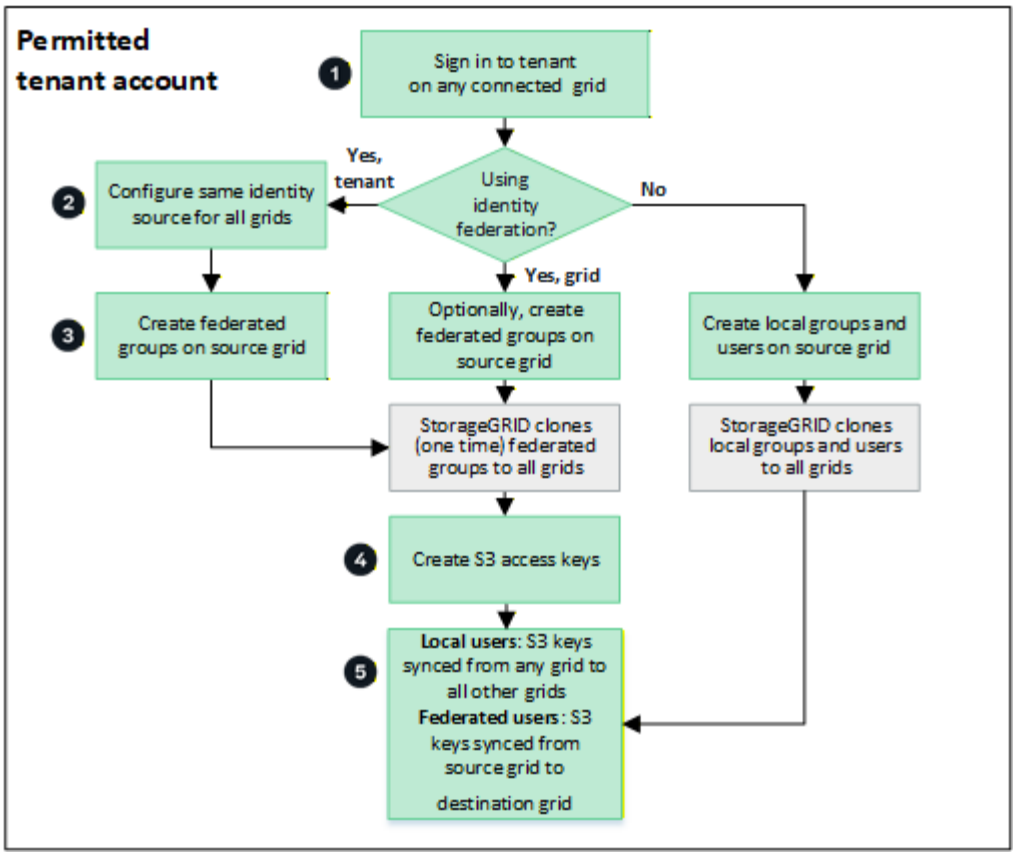
如果建立或編輯租戶時啟用了網格聯合連線，則該租戶會從一個 StorageGRID 系統（來源租戶）複寫到所有其他已連線的 StorageGRID 系統（複本租戶）。租戶複寫完成後，租戶群組、使用者和 S3 存取金鑰會在已連線的網格之間同步。

租戶最初建立的 StorageGRID 系統是該租戶的來源網格。租戶會複製到一個或多個目的地網格。所有已連接網格上的租戶帳戶具有相同的帳戶 ID、名稱、執行摘要、儲存配額、已指派的權限和 root 使用者密碼。如需詳細資訊，請參閱 "了解網格聯盟的帳戶同步" 和 "管理允許的租戶"。

同步租戶帳戶資訊是"跨網格複寫"儲存桶物件的必要條件。在所有網格上使用相同的租戶群組和使用者，可確保您能在任何已連線的網格上存取對應的儲存桶和物件。

租戶帳戶同步工作流程

如果您的租戶帳戶具有「使用網格聯合連線」權限，請審查工作流程圖，以了解同步群組、使用者和 S3 存取金鑰的步驟。



以下是工作流程的主要步驟：

1 登入租戶

在任何已連接的網格登入租戶帳戶。

2 您也可以選擇設定身分識別聯盟

如果您的租戶帳戶擁有 **Use own identity source** 權限以使用聯合群組和使用者，請為來源和一個或多個目的地租戶帳戶設定相同的身分來源（使用相同的設定）。聯合群組在建立時進行 Clone，聯合使用者在建立金鑰時進行 Clone。若要進行 Clone，必須在所有網格上設定相同的身分來源。如需相關指示，請參閱 "使用身分識別聯盟"。

3 建立群組和使用者

您可以從任何已連接的網格建立群組和使用者。當新增本機群組時，StorageGRID 會自動將其同步到所有已連接的網格。對本機群組的變更（編輯、刪除）也會持續同步。聯合群組在建立時會 Clone 一次。

- 如果身分識別同盟是針對整個 StorageGRID 系統或租戶帳戶而設定、請"建立新的租戶群組"從身分識別來源匯入同盟群組。
- 如果您不使用身份聯合，"建立新的本機群組"進而"建立本機使用者"。

4 建立 **S3** 存取金鑰

您可以"建立您自己的存取金鑰"或"建立其他使用者的存取金鑰"在任何網格上，以存取所有已連接網格上的儲存桶。

5 同步 S3 存取金鑰

如果您需要在所有網格中使用相同的存取金鑰存取儲存桶，請在其中一個網格上建立存取金鑰。對於本機使用者，存取金鑰預設會自動同步。對於聯合使用者，您必須在來源網格上建立 S3 存取金鑰，並選取 **Enable access key sync**，才能將金鑰同步到所有目的地網格。

群組、使用者和 S3 存取金鑰是如何同步的？

請審查本節內容，以了解如何在連接的網格之間同步群組、使用者和 S3 存取金鑰。

本機群組持續同步

租戶帳戶建立並複製到目的地網格後，StorageGRID 會持續同步所有已連接網格之間的本機群組。在任何網格上對本機群組所做的所有變更（包括建立、編輯和刪除操作）都會自動複製到所有其他已連接的網格。

原始群組及其同步副本具有相同的存取模式、群組權限和 S3 群組原則。有關說明，請參閱"為S3租戶建立群組"。

本機使用者會持續同步

當您在任何已連接的網格上建立新的本機使用者時，StorageGRID 會自動將該使用者同步到所有其他已連接的網格。後續的變更（包括編輯、刪除和密碼重設）也會持續同步。原始使用者及其同步副本具有相同的完整名稱、使用者名稱和 **Deny access** 設定。每個網格上的相同使用者也屬於相同的群組。如需相關指示，請參閱 "管理使用者"。

聯合群組在建立時同步一次。

假設使用帳戶同步搭配 "單一登入" 和 "身分識別聯盟" 的要求已滿足，則您為網格上的租戶建立（匯入）的聯合群組會自動同步到所有其他已連線網格上的租戶。

兩個群組具有相同的存取模式、群組權限和 S3 群組原則。

在為來源租戶建立聯合群組並將其同步到其他網格後，聯合使用者可以在任何已連接的網格上登入該租戶。之後對聯合群組的變更不會自動跨網格同步。

S3 存取金鑰可以自動同步，也可以手動同步。

預設情況下，StorageGRID 會自動同步 S3 存取金鑰。為了安全性，您可以為每個租戶停用 S3 存取金鑰的自動同步，並為每個網格上的每個租戶使用不同的金鑰。

若要管理聯網網格上的存取金鑰，您可以執行下列任一操作：

- 如果不需要在每個網格中使用相同的金鑰，則可以停用自動存取金鑰同步，並在每個網格上 "建立您自己的存取金鑰" 或 "建立其他使用者的存取金鑰"。

> ⓘ 當您為聯合使用者同步 S3 存取金鑰時，使用者和 S3 存取金鑰都會同步到目的地租戶。

本機使用者擁有的 S3 存取金鑰會在連接的網格之間持續同步，包括金鑰遭到刪除時。聯合使用者擁有的 S3 存取金鑰僅在建立時同步一次；後續變更（包括刪除）不會複寫。您可以為每個租戶連線啟用或停用存取金鑰同步。

新增至目的地網格的群組和使用者已同步

在任何已連接的網格上所做的變更，包括建立或匯入本機群組和使用者，都會自動同步到所有其他已連接的網格。

已編輯或刪除的本機群組、使用者和存取金鑰會同步。

本機群組、本機使用者以及本機使用者擁有的 S3 存取金鑰的變更會在所有連線的網格之間持續同步。同步操作包括編輯、刪除和密碼重設。

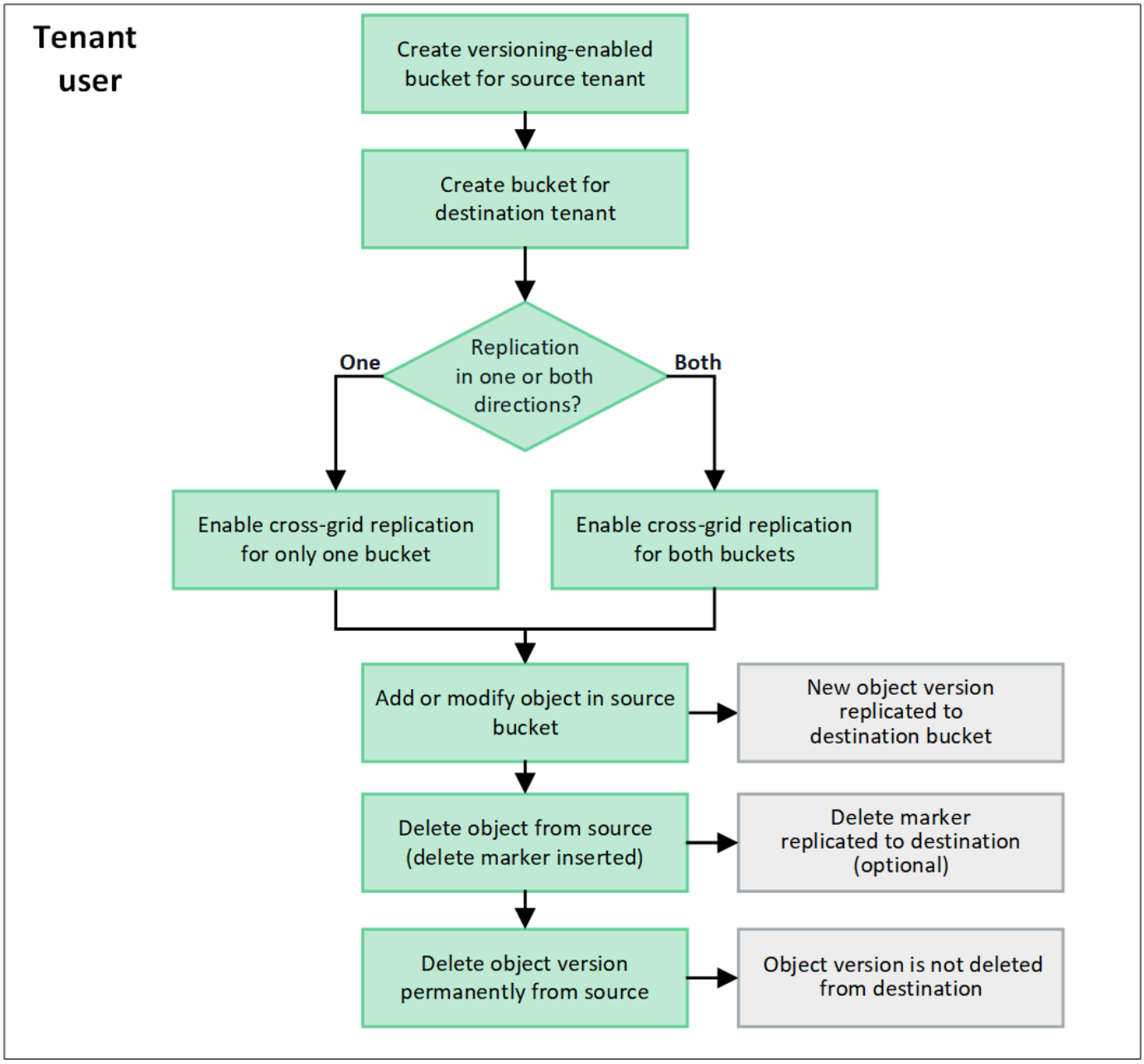
聯合群組和聯合使用者擁有的 S3 存取金鑰的變更在初始建立後不會同步。

在 **StorageGRID** 中管理跨網格複寫

如果您的租戶帳戶在建立時已獲指派 * 使用網格同盟連線 * 權限、您可以使用跨網格複寫、在租戶來源網格上的貯體和租戶目的地網格上的貯體之間自動複寫物件。跨網格複寫可在一個或兩個方向進行。

跨網格複寫的工作流程

工作流程圖總結了配置兩個網格上的儲存桶之間的跨網格複製所執行的步驟。圖表下方對這些步驟進行了更詳細的描述。



設定跨網格複寫

在使用跨網格複製之前，您必須登入每個網格上對應的租用戶帳戶並建立兩個儲存桶。然後，您可以在一個或兩個儲存桶上啟用跨網格複製。

開始之前

- 您已經查看了跨網格複製的要求。請參閱"什麼是跨網格複寫" 。
- 您正在使用"支援的網頁瀏覽器"。
- 租用戶帳戶具有*使用網格聯合連線*權限，且兩個網格上都存在相同的租用戶帳戶。請參閱"管理網格同盟連線的允許租戶" 。
- 您登入的租戶使用者已存在於兩個網格中，並且屬於具有"root 存取權限"。
- 如果您以本機使用者身分登入租用戶的目標網格，則租用戶帳戶的根使用者已為您在該網格上的使用者帳戶設定了密碼。

建立兩個儲存桶

第一步，登入每個網格上對應的租戶帳戶，並在每個網格上建立一個儲存桶。

步驟

1. 從網格聯盟連線的任一網格開始、建立新的儲存格：
   a. 使用位於兩個網格上的租戶使用者身分證明登入租戶帳戶。

      如果您無法以本機使用者身分登入租用戶的目標網格，請確認租用戶帳戶的根用戶已為您的使用者帳戶設定密碼。

   b. 按照的說明進行操作"建立 S3 儲存貯體"。

      每個網格上的儲存桶名稱和區域可以不同。

   c. 在 * 管理物件設定 * 索引標籤上、選取 * 啟用物件版本設定 * 。
   d. 如果您的StorageGRID系統啟用了 S3 物件鎖定，請參閱"使用 S3 物件鎖定進行跨網格複製"。
   e. 選取*建立桶*。
   f. 選擇*完成*。
2. 重複這些步驟，在網格聯合連接中的另一個網格上為相同租用戶帳戶建立儲存桶。

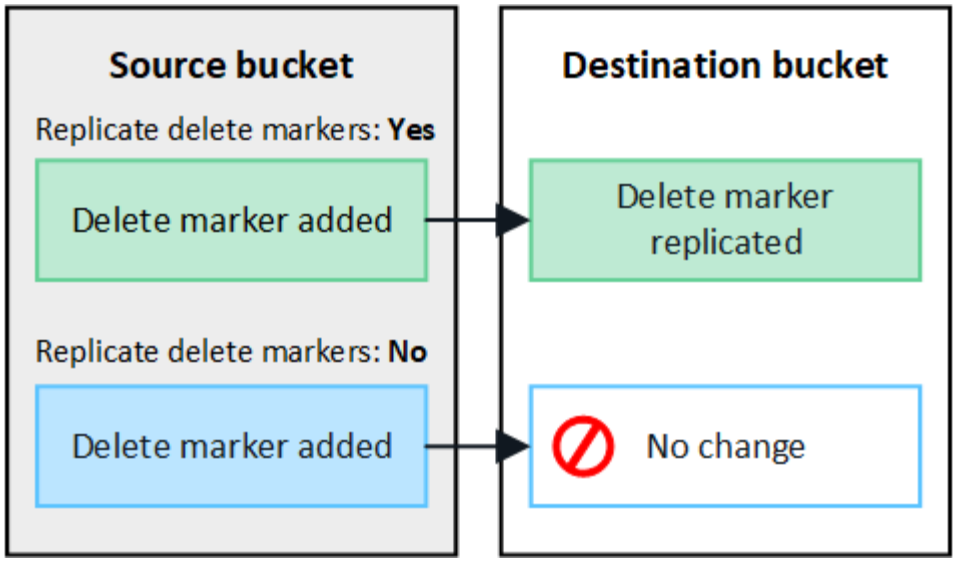
   根據需要、每個貯體可以使用不同的區域。

啟用跨網格複寫

步驟

1. 從您要複寫物件的網格開始、啟用"單向跨網格複寫"：
   a. 登入貯體的租戶帳戶。
   b. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
   c. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
   d. 選取 * 跨網格複寫 * 標籤。
   e. 選取 * 啟用 * 、然後檢閱要求清單。
   f. 如果符合所有需求、請選取您要使用的網格同盟連線。
   g. 您也可以變更 * 複寫刪除標記 * 的設定、以判斷如果 S3 用戶端向不含版本 ID 的來源網格發出刪除要求、目的地網格上會發生什麼情況：

      - * 是 * （預設）：刪除標記會新增至來源貯體、並複寫至目的地貯體。
      - 否：刪除標記已新增至來源儲存桶，但未複製到目標儲存桶。



如果刪除請求包含版本 ID，則該物件版本將從來源儲存桶中永久刪除。 StorageGRID不會複製包含版本 ID 的刪除要求，因此相同的物件版本不會從目標中刪除。

參考"什麼是跨網格複寫"了解詳情。

a. 您也可以變更 * 跨網格複寫 * 稽核類別的設定、以管理稽核訊息的數量：
   - * 錯誤 *（預設）：稽核輸出中僅包含失敗的跨網格複寫要求。
   - * 正常 *：包含所有跨網格複寫要求、大幅增加稽核輸出的容量。

b. 選取 * 啟用和測試 * 。

   片刻之後，會出現成功訊息。新增至此儲存桶的物件現在會自動複製到另一個網格。 *跨網格複製*在儲存桶詳細資料頁面上顯示為已啟用的功能。

2. 或者"雙向啟用跨網格複寫"、前往其他網格和上的對應儲存格。

測試網格之間的複寫

如果已為貯體啟用跨網格複寫、您可能需要驗證連線和跨網格複寫是否正常運作、以及來源和目的地貯體是否仍符合所有需求（例如、版本設定仍為啟用狀態）。

開始之前

- 您正在使用"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。

步驟

1. 登入貯體的租戶帳戶。
2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
3. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
4. 選取 * 跨網格複寫 * 標籤。
5. 選擇*測試連線*。

如果連接正常，則會出現成功橫幅。否則，會出現一條錯誤訊息，您和網格管理員可以使用它來解決問題。有關詳細信息，請參閱"疑難排解網格同盟錯誤"。

6. 如果跨網格複寫設定為雙向進行、請前往另一個網格上的對應儲存格、然後選取 * 測試連線 * 、確認跨網格複寫在另一個方向上運作。

停用跨網格複寫

如果您不想再將物件複製到其他網格、可以永久停止跨網格複寫。

停用跨網格複寫之前、請注意下列事項：

- 停用跨網格複製不會刪除任何已在網格之間複製的物件。例如， `my-bucket`網格 1 上已複製到 `my-bucket` 如果您停用該儲存桶的跨網格複製，則網格 2 上的資料不會被刪除。如果要刪除這些對象，則必須手動將其刪除。
- 如果已為每個貯體啟用跨網格複寫（也就是說、如果雙向進行複寫）、您可以停用其中一個或兩個貯體的跨網格複寫。例如、您可能想要停用從「在網格 1 」複寫物件 `my-bucket`至 `my-bucket`「在網格 2 」、同時繼續將物件從「在網格 2 」複寫 `my-bucket`至 `my-bucket`「在網格 1 」。
- 您必須先停用跨網格複製，然後才能刪除租用戶使用網格聯合連線的權限。請參閱"管理允許的租戶" 。

開始之前

- 您正在使用"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。

步驟

1. 從您不再想複寫物件的網格開始、停止貯體的跨網格複寫：
   a. 登入貯體的租戶帳戶。
   b. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
   c. 從表格中選取貯體名稱、以存取貯體詳細資料頁面。
   d. 選取 * 跨網格複寫 * 標籤。
   e. 選取 * 停用複寫 * 。
   f. 如果您確定要停用此儲存桶的跨網格複製，請在文字方塊中鍵入*是*，然後選擇*停用*。

      稍後會出現成功訊息。新增至此貯體的物件無法再自動複寫到其他網格。* 跨網格複寫 * 不再顯示為「已啟用」功能。

2. 如果跨網格複寫設定為雙向進行、請移至另一個網格上的對應儲存格、並在另一個方向停止跨網格複寫。

在 **StorageGRID** 中檢視網格聯盟連線

如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、您可以檢視允許的連線。

開始之前

- 租戶帳戶具有 * 使用網格同盟連線 * 權限。
- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。

- 您屬於具有的使用者群組"root 存取權限"。

步驟

1. 選擇 * 儲存設備（ S3 ） * > * 網格聯盟連線 * 。

   此時會出現 Grid Federation 連線頁面、其中包含摘要下列資訊的表格：

欄位	說明
連線名稱	此租用戶有權使用的網格同盟連線。
具有跨網格複寫的貯體	對於每個網格同盟連線、已啟用跨網格複寫的租戶區。新增至這些貯體的物件將會複寫至連線中的其他網格。
上次錯誤	對於每個網格聯盟連線、資料複寫到其他網格時、最新發生的錯誤（如果有）。請參閱。 清除最後一個錯誤

2. 您也可以選擇儲存區名稱至"檢視貯體詳細資料"。

[[Clear-last 錯誤 **]]** 清除最後一個錯誤

下列其中一個原因可能會在 * 最後一個錯誤 * 欄中出現錯誤：

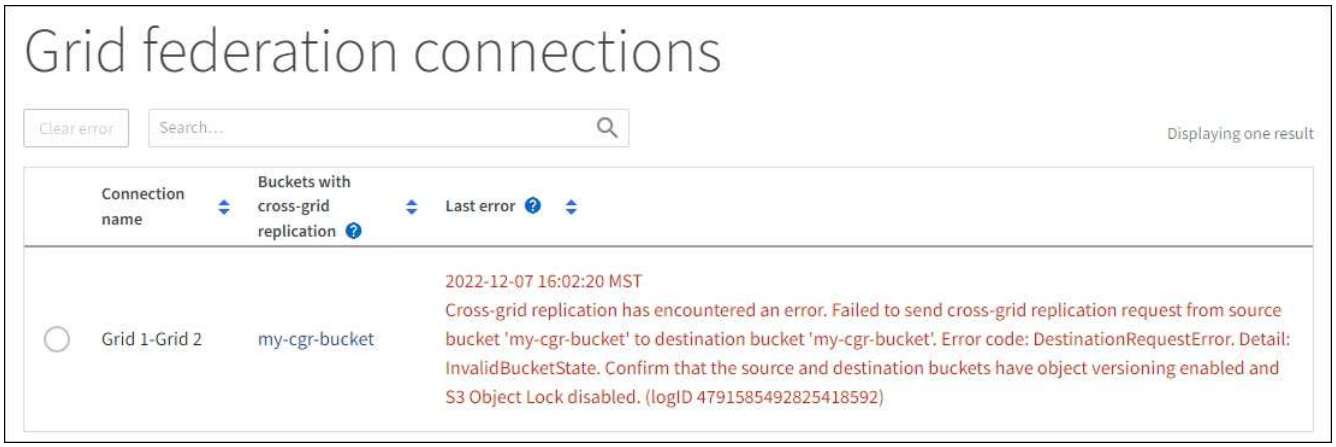
- 找不到來源物件版本。
- 找不到來源貯體。
- 目的地貯體已刪除。
- 目的地貯體是由不同的帳戶重新建立。
- 目的地貯體已暫停版本設定。
- 目的地貯體是由相同的帳戶重新建立、但現在已取消版本管理。

此欄只會顯示最後發生的跨網格複寫錯誤、不會顯示先前可能發生的錯誤。

步驟

1. 如果訊息出現在 * 最後一個錯誤 * 欄中、請檢視訊息文字。

   例如、此錯誤表示跨網格複寫的目的地儲存格處於無效狀態、可能是因為版本設定已暫停或啟用 S3 物件鎖定。



2. 執行任何建議的動作。例如、如果目的地貯體上的版本設定已暫停進行跨網格複寫、請重新啟用該貯體的版本設定。
3. 從表格中選取連線。
4. 選取 * 清除錯誤 * 。
5. 選擇 * 是 * 以清除訊息並更新系統狀態。
6. 等待 5-6 分鐘、然後將新物件擷取到貯體中。確認錯誤訊息不會再次出現。

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

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

管理群組和使用者

在 **StorageGRID** 中使用身分識別聯盟

使用身分識別聯盟可更快設定租戶群組和使用者、並可讓租戶使用者使用熟悉的認證登入租戶帳戶。

設定租戶管理程式的身分識別聯盟

如果您希望在另一個系統（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server ）中管理租用戶群組和用戶，則可以為租用戶管理器設定身分聯合。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作為身分識別提供者。

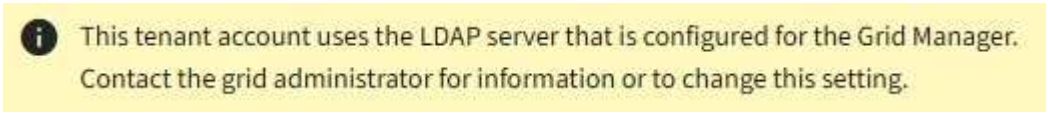
  如果您想使用未列出的 LDAP v3 服務，請聯絡技術支援。

- 如果您打算使用OpenLDAP、則必須設定OpenLDAP伺服器。請參閱。 設定OpenLDAP伺服器的準則
- 如果您打算使用傳輸層安全性（TLS）與LDAP伺服器進行通訊、則身分識別供應商必須使用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

您是否可以為租戶設定身分識別聯盟服務、取決於租戶帳戶的設定方式。您的租戶可能會共用為Grid Manager設定的身分識別聯盟服務。如果您在存取「身分識別聯盟」頁面時看到此訊息、則無法為此租用戶設定個別的同盟身分識別來源。

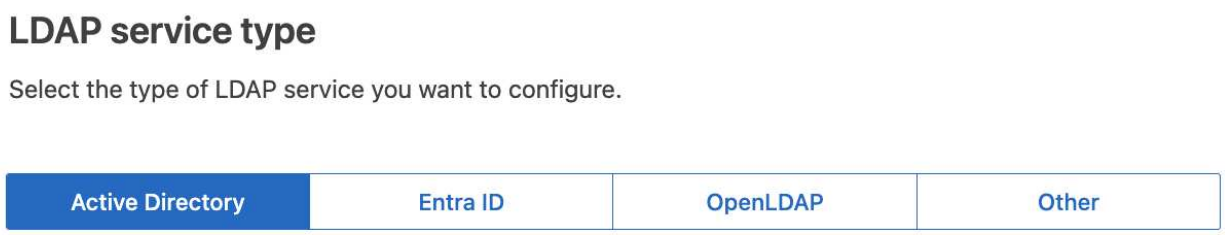


輸入組態

當您設定識別聯盟時、您會提供 StorageGRID 連線至 LDAP 服務所需的值。

步驟

1. 選擇*存取管理* > 身分聯合。
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：包含 LDAP 使用者唯一識別碼的屬性名稱。此屬性相當於 `sAMAccountName`對於 `Active Directory` 和 `uid`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `uid`。
   - 使用者 **UUID**：包含 LDAP 使用者的永久唯一識別碼的屬性名稱。此屬性相當於 `objectGUID`對於 `Active Directory` 和 `entryUUID`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `nsuniqueid`。每個使用者的指定屬性值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。
   - 群組唯一名稱：包含 LDAP 群組唯一識別碼的屬性的名稱。此屬性相當於 `sAMAccountName`對於 `Active Directory` 和 `cn`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `cn`。
   - 群組 **UUID**：包含 LDAP 群組的永久唯一識別碼的屬性的名稱。此屬性相當於 `objectGUID`對於 `Active Directory` 和 `entryUUID`對於 `OpenLDAP`。如果您正在設定 `Oracle Directory Server`，請輸入 `nsuniqueid`。每個群組的指定屬性的值必須是 16 位元組或字串格式的 32 位元十六進位數，其中連字元將被忽略。

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

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

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

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

     指定的使用者必須擁有列出群組和使用者的權限、並可存取下列屬性：

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

   - 密碼：與使用者名稱相關的密碼。

     如果您在未來變更密碼、您必須在此頁面上更新密碼。

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

     「群組唯一名稱*」值必須在所屬的*群組基礎DN*中是唯一的。

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

     *使用者唯一名稱*值必須在其所屬的*使用者基礎DN*內是唯一的。

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

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

     輸入下列其中一種模式：

     - **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
     - 下級登入名稱模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
     - * 辨別名稱模式 * ： `CN=[USERNAME],CN=Users,DC=example,DC=com`

請準確附上所寫的*（使用者名稱）*。

6. 在傳輸層安全性（TLS）區段中、選取安全性設定。
   - 使用 **STARTTLS**：使用 STARTTLS 確保與 LDAP 伺服器的通訊安全。這是 Active Directory 、OpenLDAP 或其他的建議選項，但 Microsoft Entra ID 不支援此選項。
   - 使用 **LDAPS**：LDAPS（透過 SSL 的 LDAP）選項使用 TLS 建立與 LDAP 伺服器的連線。您必須為 Microsoft Entra ID 選擇此選項。
   - 請勿使用 **TLS**： StorageGRID系統和 LDAP 伺服器之間的網路流量將不安全。 Microsoft Entra ID 不支援此選項。

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

7. 如果您選取了ARTTLS或LDAPS、請選擇用來保護連線安全的憑證。
   - 使用作業系統**CA**憑證：使用作業系統上安裝的預設Grid CA憑證來保護連線安全。
   - 使用自訂**CA**憑證：使用自訂安全性憑證。

     如果選取此設定、請將自訂安全性憑證複製並貼到CA憑證文字方塊中。

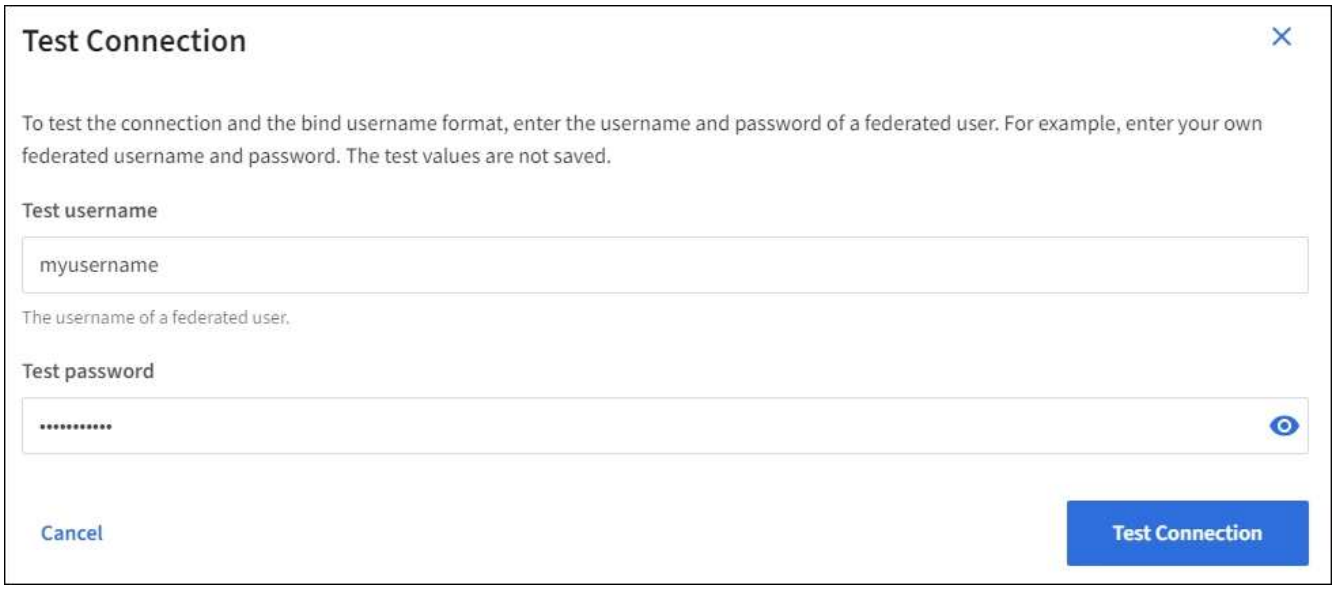
測試連線並儲存組態

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

步驟

1. 選擇*測試連線*。
2. 如果您沒有提供綁定使用者名稱格式：
   - 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（儲存）」*以儲存組態。
   - 如果連線設定無效、就會出現「無法建立測試連線」訊息。選擇*關閉*。然後、解決所有問題、並再次測試連線。
3. 如果您提供連結使用者名稱格式、請輸入有效同盟使用者的使用者名稱和密碼。

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



- 如果連線設定有效、就會出現「測試連線成功」訊息。選取*「Save（儲存）」*以儲存組態。
- 如果連線設定、連結使用者名稱格式或測試使用者名稱和密碼無效、則會出現錯誤訊息。解決所有問題、然後再次測試連線。

強制與身分識別來源同步

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

步驟

1. 前往「身分識別聯盟」頁面。
2. 選取頁面頂端的*同步伺服器*。

   視您的環境而定、同步處理程序可能需要一些時間。

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

停用身分識別聯盟

您可以暫時或永久停用群組和使用者的身份聯合。當身分聯合被停用時， StorageGRID和身分來源之間就沒有通訊。但是，您配置的任何設定都會保留，以便您將來可以輕鬆地重新啟用身份聯合。

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。
- StorageGRID系統和身分來源之間不會發生同步，並且不會對尚未同步的帳戶發出警報。
- 如果單一登入 (SSO) 狀態為 已啟用 或 沙盒模式，則 啟用身分聯合 核取方塊將會停用。在停用身分聯合之

前，單一登入頁面上的 SSO 狀態必須為 已停用。看"停用單一登入" 。

步驟

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

設定**OpenLDAP**伺服器的準則

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

> 對於非 Active Directory 或 Microsoft Entra ID 的識別來源， StorageGRID不會自動阻止外部停用的使用者存取 S3。若要封鎖 S3 訪問，請刪除使用者的所有 S3 金鑰或從所有群組中刪除該使用者。

memberOf和**refert**覆疊

應啟用memberof和refert覆疊。如需詳細資訊，請參閱中的反向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。

請參閱中有關反向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"^]。

管理租戶群組

在 **StorageGRID** 中為 **S3** 租戶建立群組

您可以匯入同盟群組或建立本機群組、來管理S3使用者群組的權限。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。
- 如果您計畫匯入同盟群組、則您擁有"已設定的身分識別聯盟"、且同盟群組已存在於已設定的身分識別來源中。
- 如果您的租戶帳戶具有「使用網格聯合連線」權限，您已審查工作流程和注意事項（適用於 "同步租戶群組和使用者"），並且您已登入租戶的來源網格。

存取建立群組精靈

第一步是存取「建立群組」精靈。

步驟

1. 選擇“存取管理”>“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。

步驟

1. 選取*本機群組*索引標籤以建立本機群組、或選取*聯盟群組*索引標籤、從先前設定的身分識別來源匯入群組。

   如果StorageGRID 您的系統啟用單一登入（SSO）、屬於本機群組的使用者將無法登入租戶管理程式、不過他們可以根據群組權限、使用用戶端應用程式來管理租戶的資源。

2. 輸入群組名稱。
   - 本機群組：輸入顯示名稱和唯一名稱。您可以稍後再編輯顯示名稱。

     如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 唯一名稱 * 、就會發生複製錯誤。

   - 聯盟群組：輸入唯一名稱。對於 Active Directory 、唯一名稱是與屬性相關的名稱 `sAMAccountName`。對於 OpenLDAP 、唯一名稱是與屬性相關聯的名稱 `uid`。
3. 選擇*繼續*。

管理群組權限

群組權限可控制使用者可在租戶管理器和租戶管理 API 中執行的工作。

步驟

1. 對於 * 存取模式 * 、請選取下列其中一項：
   - * 讀寫 *（預設）：使用者可以登入租戶管理員並管理租戶組態。
   - 唯讀：使用者只能檢視設定和功能。他們無法在租戶管理員或租戶管理 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. 為此群組選取一或多個權限。

   請參閱。 "租戶管理權限"

3. 選擇*繼續*。

設定 **S3** 群組原則

群組原則決定使用者將擁有哪些 S3 存取權限。

步驟

1. 選取您要用於此群組的原則。

群組原則	說明
無 S3 存取權	預設。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
唯讀存取	此群組中的使用者擁有 S3 資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
完整存取	此群組中的使用者可完全存取 S3 資源、包括貯體。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
勒索軟體緩解	此原則範例適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。 擁有「 * 管理所有儲存區 * 」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（ MFA ）。
自訂	群組中的使用者會獲得您在文字方塊中指定的權限。

2. 如果您選取*自訂*、請輸入群組原則。每個群組原則的大小上限為5、120位元組。您必須輸入有效的Json格式字串。

   如需群組原則的詳細資訊，包括語言語法和範例，請參閱"群組原則範例"。

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）

您可以儲存群組而不新增使用者、也可以選擇性地新增已存在的任何本機使用者。

步驟

1. 您也可以為此群組選取一或多個本機使用者。
2. 選擇* Create group（創建組）和 Finish（完成）*。

   您建立的群組會出現在群組清單中。

   如果您的租戶帳戶擁有 **Use grid federation connection** 權限，且您位於租戶的來源網格上，則新群組將同步至租戶的目的地網格。**Succeeded** 將顯示為群組詳細資料頁面「概覽」區段中的同步狀態。

建立租戶群組之前、請先考量您要指派給該群組的權限。租戶管理權限可決定使用者可以使用租戶管理程式或租戶管理API執行哪些工作。使用者可以屬於一或多個群組。如果使用者屬於多個群組、則權限是累積性的。

若要登入租戶管理程式或使用租戶管理API、使用者必須屬於至少擁有一項權限的群組。所有可以登入的使用者都可以執行下列工作：

- 檢視儀表板
- 變更自己的密碼（適用於本機使用者）

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、或是只能檢視相關設定和功能。

> 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。

您可以為群組指派以下權限。

權限	說明	詳細資料
root存取權	提供租戶管理程式和租戶管理API的完整存取權限。	
管理您自己的S3 認證	可讓使用者建立及移除自己的S3存取金鑰。	沒有此權限的使用者不會看到 * 儲存設備（ S3 ） * > * My S3 存取鍵 * 功能表選項。
檢視所有貯體	允許使用者查看所有儲存桶和儲存桶配置。	沒有「檢視所有貯體」或「管理所有貯體」權限的使用者、將不會看到「 *buckets 」功能表選項。 此權限已被「管理所有儲存桶」權限取代。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。
管理所有貯體	允許使用者使用租用戶管理器和租用戶管理 API 建立和刪除 S3 儲存桶並管理租用戶帳戶中所有 S3 儲存桶的設置，而無需考慮 S3 儲存桶或群組原則。	沒有「檢視所有貯體」或「管理所有貯體」權限的使用者、將不會看到「 *buckets 」功能表選項。 此權限取代了查看所有儲存桶的權限。它不會影響 S3 用戶端或 S3 控制台使用的 S3 儲存桶或群組原則。
管理端點	可讓使用者使用租戶管理器或租戶管理 API 來建立或編輯平台服務端點、這些端點是 StorageGRID 平台服務的目的地。	沒有此權限的使用者不會看到 * 平台服務端點 * 功能表選項。

權限	說明	詳細資料
使用 S3 Console 標籤	與「檢視所有貯體」或「管理所有貯體」權限結合使用時、可讓使用者從儲存庫詳細資料頁面上的「 S3 主控台」索引標籤檢視及管理物件。	

管理 **StorageGRID** 租戶群組

視需要管理租戶群組、以檢視、編輯或複製群組等項目。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。

檢視或編輯群組

您可以檢視和編輯每個群組的基本資訊和詳細資料。

步驟

1. 選擇“存取管理”>“群組”。
2. 檢閱「群組」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟群組的基本資訊。

   如果租戶帳戶具有 * 使用網格同盟連線 * 權限、且您正在租戶來源網格上檢視群組：

   - 如果任何群組未同步至目的地網格上的租戶，請依照下列步驟操作 重試群組同步。
3. 如果您要變更群組名稱：
   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 *
4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：
   - 選取群組名稱。
   - 選取群組的核取方塊、然後選取 * 動作 * > * 檢視群組詳細資料 * 。
5. 檢閱「總覽」一節、其中顯示每個群組的下列資訊：
   - 顯示名稱
   - 唯一名稱
   - 類型
   - 存取模式
   - 權限
   - S3 原則

- 此群組中的使用者數目
- 如果租戶帳戶具有「 * 使用網格同盟連線 * 」權限、且您正在租戶來源網格上檢視群組、則會顯示其他欄位：
  - 同步狀態，**Succeeded** 或 **Failed**
  - 對於聯合群組，藍色橫幅表示，如果您編輯或刪除此群組，您的變更將不會同步到另一個網格。

6. 根據需要編輯群組設定。參考"為S3租戶建立群組"了解輸入內容的詳細資訊。
   a. 在「概覽」部分，選擇名稱或編輯圖示 即可變更顯示名稱。
   b. 在 * 群組權限 * 索引標籤上、更新權限、然後選取 * 儲存變更 * 。
   c. 在 * 群組原則 * 索引標籤上、進行任何變更、然後選取 * 儲存變更 * 。

      根據需要選擇不同的 S3 組策略或輸入自訂策略的 JSON 字串。

7. 若要將一或多個現有的本機使用者新增至群組：
   a. 選取使用者索引標籤。

   b. 選取 * 新增使用者 * 。
   c. 選取您要新增的現有使用者、然後選取 * 新增使用者 * 。

      右上角會出現成功訊息。

8. 若要從群組中移除本機使用者：
   a. 選取使用者索引標籤。
   b. 選取 * 移除使用者 * 。
   c. 選取您要移除的使用者、然後選取 * 移除使用者 * 。

      右上角會出現成功訊息。

9. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

複製群組

您可以複製現有群組、以更快建立新群組。

如果您的租戶帳戶具有「使用網格聯合連線」權限，並且您從租戶的來源網格複製群組，則複製的群組將同步至租戶的目的地網格。

步驟

1. 選擇“存取管理”>“群組”。
2. 選取您要複製之群組的核取方塊。
3. 選取*「動作*」>*「重複群組*」。
4. 看"為S3租戶建立群組"了解輸入內容的詳細資訊。
5. 選取*建立群組*。

重試群組同步

如果任何群組同步失敗，則該群組的「同步狀態」欄位中會顯示「Failed」。表格上方會顯示橫幅，指示一個或多個群組同步失敗。

步驟

要重試同步：

1. 在橫幅上，選擇 **Retry sync**。此操作將重試所有同步失敗的群組的同步。
2. 若要重試同步某個群組，請選擇群組名稱。在群組詳細資料頁面上，選擇 **Retry sync**。
3. 從您正在同步的每個群組的詳細資訊頁面檢視同步作業的狀態。

如果重試成功，每個已成功同步的群組的「同步狀態」欄中將顯示「成功」，且橫幅會消失。

如需更多資訊，請參閱"同步租戶群組和使用者"。

刪除一或多個群組

您可以刪除一或多個群組。只屬於已刪除群組的任何使用者將無法再登入租戶管理員或使用租戶帳戶。

步驟

1. 選擇“存取管理”>“群組”。
2. 選取您要刪除的每個群組的核取方塊。
3. 選擇 * 行動 * > * 刪除群組 * 或 * 行動 * > * 刪除群組 * 。

   隨即顯示確認對話方塊。

4. 選取 * 刪除群組 * 或 * 刪除群組 * 。

設定 **AssumeRole**

開始之前

您必須是管理員才能設定 AssumeRole。

關於這項工作

若要設定 AssumeRole，請建立要假定的目標群組（如果該群組尚不存在）。編輯該組的 S3 策略以指定假設該組允許的操作。編輯群組的 S3 信任策略以指定允許使用 AssumeRole API 承擔該群組的可信任使用者。

假設該群組建立的臨時安全憑證在有限的時間內有效。會話時長為15分鐘到12小時，預設會話時長為1小時。當您從群組的 S3 信任原則中刪除使用者時，該使用者將無法再承擔該群組。

步驟

1. 選擇“存取管理”>“群組”。
2. 選取群組名稱。
3. 選擇“**S3** 信任策略”標籤。
4. 新增您的 S3 信任策略，包括可以執行 AssumeRole 的使用者清單。
5. 選取*儲存變更*。
6. 選擇“**S3** 群組原則”標籤。
7. 編輯 S3 策略以僅為該群組的 S3 信任策略中新增的受信任使用者指定所需的 S3 操作。
8. 選取*儲存變更*。

AssumeRole S3 信任策略範例

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

主體：

- `"Principal": "*"`符合所有請求，包括匿名（未簽署）請求。
- `"Principal": { "AWS": "*" }` 符合任何已驗證的身分或使用者（不符合匿名請求）
- 僅適用於儲存桶原則
- 主體是指被授予或拒絕權限的帳戶/使用者。

配置完成後，S3 信任策略中列出的使用者可以執行 AssumeRole 並接收憑證。最終的權限由群組原則、bucket策略、session策略決定。有關更多信息，請參閱"使用存取策略" 。

管理 **StorageGRID** 租戶使用者

您可以建立本機使用者並將其指派到本機群組，以確定這些使用者可以存取哪些功能。您也可以匯入聯合使用者。Tenant Manager 包含一個名為 *root* 的預先定義本機使用者。雖然您可以新增和移除本機使用者，但無法移除 root 使用者。

如果您的 StorageGRID 系統啟用了單一登入 （SSO），則本機使用者將無法登入 Tenant Manager 或 Tenant Management API，但他們可以根據群組權限使用用戶端應用程式存取租戶的資源。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。
- 如果您的租戶帳戶具有「使用網格聯合連線」權限，您已審查工作流程和注意事項（適用於 "同步租戶群組和使用者"），並且您已登入租戶的來源網格。

建立本機使用者

您可以建立本機使用者並將其指派給一或多個本機群組、以控制其存取權限。

不屬於任何群組的 S3 使用者沒有管理權限或 S3 群組原則套用到他們。這些使用者可能會透過儲存區原則授予S3儲存區存取權。

存取建立使用者精靈

步驟

1. 選擇“存取管理”>“使用者”。
2. 選取*建立使用者*。

輸入認證

步驟

1. 對於 * 輸入使用者認證 * 步驟、請填寫下列欄位。

欄位	說明
全名	此使用者的全名、例如人員的名字和姓氏、或應用程式的名稱。
使用者名稱	此使用者將用來登入的名稱。使用者名稱必須是唯一的、而且無法變更。 • 附註 * ：如果您的租戶帳戶具有 * 使用網格同盟連線 * 權限、則如果目的地網格上的租戶已經存在相同的 * 使用者名稱 * 、就會發生複製錯誤。
密碼和確認密碼	使用者在登入時最初使用的密碼。
拒絕存取	選取 * 是 * 可防止此使用者登入租戶帳戶、即使他們仍屬於一個或多個群組。 例如、選取 * 是 * 可暫時暫停使用者登入的能力。

2. 選擇*繼續*。

指派給群組

步驟

1. 將使用者指派給一或多個本機群組、以判斷他們可以執行哪些工作。

   將使用者指派給群組是選擇性的。如果您願意、可以在建立或編輯群組時選取使用者。

   不屬於任何群組的使用者將沒有管理權限。權限是累積性的。使用者將擁有所屬所有群組的所有權限。請參閱。 "租戶管理權限"

2. 選取*建立使用者*。

   如果您的租戶帳戶擁有 **Use grid federation connection** 權限，且您位於租戶的來源網格上，則新的本機使用者將同步到租戶的目的地網格。**Succeeded** 會顯示為使用者詳細資料頁面「概覽」部分中的 **Sync status**。

3. 選擇 * 完成 * 返回「使用者」頁面。

檢視或編輯本機使用者

步驟

1. 選擇“存取管理”>“使用者”。
2. 檢閱「使用者」頁面上提供的資訊、其中列出此租戶帳戶所有本機和同盟使用者的基本資訊。
3. 若要變更使用者的全名：
   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 *
4. 如果您想要檢視更多詳細資料或進行其他編輯、請執行下列其中一項：
   - 選取使用者名稱。
   - 選取使用者的核取方塊、然後選取 * 動作 * > * 檢視使用者詳細資料 * 。
5. 檢閱「總覽」一節、其中顯示每位使用者的下列資訊：
   - 全名
   - 使用者名稱
   - 使用者類型
   - 拒絕存取
   - 存取模式
   - 群組成員資格
6. 視需要編輯使用者設定。如需輸入內容的詳細資訊、請參閱建立本機使用者。
   a. 在「概覽」部分，選擇名稱或編輯圖示 即可變更全名。

      您無法變更使用者名稱。

b. 在 * 密碼 * 標籤上、變更使用者的密碼、然後選取 * 儲存變更 * 。

c. 在 * 存取 * 索引標籤上、選取 * 否 * 以允許使用者登入、或選取 * 是 * 以防止使用者登入。然後、選取 * 儲存變更 * 。

d. 在 * 存取鍵 * 索引標籤上、選取 * 建立鍵 * "建立其他使用者的 S3 存取金鑰"、然後依照的指示進行。

e. 在 * 群組 * 索引標籤上、選取 * 編輯群組 * 、將使用者新增至群組或從群組中移除使用者。然後選取 * 儲存變更 * 。

7. 確認您為變更的每個區段選擇了 * 儲存變更 * 。

導入聯合用戶

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

步驟

1. 選擇“存取管理”>“使用者”。
2. 選擇*導入聯合用戶*。
3. 輸入一個或多個聯合使用者的 UUID 或使用者名稱。

   對於多個條目，請在新行上新增每個 UUID 或使用者名稱。

4. 選擇*導入*。

   如果將一個或多個使用者匯入「使用者」欄位失敗，請執行下列步驟：

   a. 展開*未匯入的使用者*並選擇*複製使用者*。

   b. 透過選擇「上一個」並將複製的使用者貼上到「匯入聯合使用者」對話方塊中，重新嘗試匯入。

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

重複的本機使用者

您可以複製本機使用者、以更快建立新使用者。

> 如果您的租戶帳戶具有「使用網格聯合連線」權限，且您從租戶的來源網格複製使用者，則複製的使用者將同步到租戶的目的地網格。

步驟

1. 選擇“存取管理”>“使用者”。
2. 選取您要複製之使用者的核取方塊。
3. 選取*「動作*」>*「重複使用者*」。
4. 如需輸入內容的詳細資訊、請參閱建立本機使用者。
5. 選取*建立使用者*。

重試使用者同步

如果任何使用者同步失敗，則該使用者的「同步狀態」欄位中會顯示「Failed」。表格上方會顯示橫幅，指示一個或多個使用者同步失敗。

步驟

要重試同步：

1. 在橫幅上，選取 **Retry sync**。此操作會重試所有同步失敗的使用者的同步。
2. 若要重試同步個別使用者，請選擇使用者名稱。在使用者詳細資料頁面上，選擇 **Retry sync**。
3. 從每個正在同步的使用者的詳細資料頁面檢視同步作業的狀態。

如果重試成功，每個已成功同步的使用者的「同步狀態」欄中將顯示「成功」，且橫幅會消失。

如需更多資訊，請參閱"同步租戶群組和使用者"。

刪除一或多個本機使用者

您可以永久刪除不再需要存取 StorageGRID 租戶帳戶的一或多個本機使用者。

> 如果您的租戶帳戶擁有*使用網格聯合連線*權限，且您刪除了本機使用者，StorageGRID 將會刪除連線中其他網格上的對應使用者，除非該使用者是目標網格上的聯合使用者。您必須使用聯合身分識別來源來刪除聯合使用者。

步驟

1. 選擇“存取管理”>“使用者”。
2. 選取您要刪除的每個使用者的核取方塊。
3. 選擇 * 行動 * > * 刪除使用者 * 或 * 行動 * > * 刪除使用者 * 。

   隨即顯示確認對話方塊。

4. 選取 * 刪除使用者 * 或 * 刪除使用者 * 。

管理S3存取金鑰

在 **StorageGRID** 中管理 **S3** 存取金鑰

S3租戶帳戶的每位使用者都必須擁有存取金鑰、才能在StorageGRID 這個系統中儲存及擷取物件。存取金鑰包含存取金鑰ID和秘密存取金鑰。

S3存取金鑰的管理方式如下：

- 擁有 * 管理您自己的 S3 認證 * 權限的使用者可以建立或移除自己的 S3 存取金鑰。
- 擁有 * 根存取 * 權限的使用者可以管理 S3 根帳戶和所有其他使用者的存取金鑰。根存取金鑰可讓租戶完整存取所有的貯體和物件、除非已明確停用貯體原則。

支援簽名版本2和簽名版本4驗證。StorageGRID除非庫位原則明確啟用、否則不允許跨帳戶存取。

在 **StorageGRID** 中建立您自己的 **S3** 存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以建立自己的S3存取金鑰。您必須擁有存取金鑰才能存取您的貯體和物件。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理您自己的 S3 認證或根存取權限"。

關於這項工作

您可以建立一或多個S3存取金鑰、以便為租戶帳戶建立及管理貯體。建立新的存取金鑰之後、請使用新的存取金鑰ID和秘密存取金鑰來更新應用程式。為了安全起見、請勿建立超出您所需的金鑰、並刪除您未使用的金鑰。如果您只有一個金鑰即將過期、請在舊金鑰過期之前建立新金鑰、然後刪除舊金鑰。

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

- 設定金鑰的到期時間、將存取限制在特定時間段內。如果您的存取金鑰ID和秘密存取金鑰意外暴露、設定短的到期時間有助於降低風險。過期的金鑰會自動移除。
- 如果環境中的安全風險較低、而且您不需要定期建立新金鑰、就不需要設定金鑰的到期時間。如果您決定稍後再建立新金鑰、請手動刪除舊金鑰。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。

   「我的存取金鑰」頁面隨即出現、並列出任何現有的存取金鑰。

2. 選取*建立金鑰*。
3. 執行下列其中一項：
   - 選取*不要設定到期時間*以建立不會過期的金鑰。（預設）
   - 選取*設定到期時間*、然後設定到期日和時間。

     > 到期日最長可為從目前日期算起的五年。到期時間最短可從目前時間開始一分鐘。

4. 選取*建立存取金鑰*。

   此時會出現「下載存取金鑰」對話方塊、列出您的存取金鑰ID和秘密存取金鑰。

5. 將存取金鑰ID和秘密存取金鑰複製到安全位置、或選取*下載.csv*以儲存內含存取金鑰ID和秘密存取金鑰的試算表檔案。

   > 在複製或下載此資訊之前、請勿關閉此對話方塊。對話方塊關閉後、您無法複製或下載金鑰。

6. 選擇*完成*。

   新金鑰會列在「我的存取金鑰」頁面上。

在 StorageGRID 中檢視您的 S3 存取金鑰

如果您使用的是 S3 租戶且擁有、"適當的權限"則可以檢視 S3 存取金鑰清單。您可以依到期時間排序清單、以便判斷哪些金鑰即將到期。視需要、您可以"建立新金鑰"或"刪除金鑰"不再使用。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於擁有管理您自己的 S3 認證"權限"的使用者群組。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。
2. 從「我的存取金鑰」頁面、依 * 到期時間 * 或 * 存取金鑰 ID* 來排序任何現有的存取金鑰。
3. 視需要建立新金鑰或刪除不再使用的任何金鑰。

   如果您在現有金鑰過期之前建立新金鑰、您可以開始使用新金鑰、而不會暫時失去帳戶中物件的存取權。

   過期的金鑰會自動移除。

在 StorageGRID 中刪除您自己的 S3 存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以刪除自己的S3存取金鑰。刪除存取金鑰之後、就無法再使用它來存取租戶帳戶中的物件和儲存區。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您有"管理您自己的 S3 認證權限"。

> 您可以使用租戶管理程式中顯示的帳戶存取金鑰ID和秘密存取金鑰、來存取屬於您帳戶的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇*儲存設備（S3）>*我的存取金鑰。
2. 從「我的存取金鑰」頁面、選取您要移除的每個存取金鑰核取方塊。
3. 選取*刪除機碼*。
4. 從確認對話方塊中、選取 * 刪除機碼 * 。

   頁面右上角會出現確認訊息。

在 **StorageGRID** 中建立其他使用者的 **S3** 存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以為其他使用者建立S3存取金鑰、例如需要存取儲存區和物件的應用程式。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。

關於這項工作

您可以為其他使用者建立一或多個S3存取金鑰、以便他們為租戶帳戶建立及管理貯體。建立新的存取金鑰之後、請使用新的存取金鑰ID和秘密存取金鑰來更新應用程式。為了安全起見、請勿建立超出使用者需求的金鑰、並刪除未使用的金鑰。如果您只有一個金鑰即將過期、請在舊金鑰過期之前建立新金鑰、然後刪除舊金鑰。

每個金鑰都可以有特定的到期時間、或是沒有到期時間。請遵循下列到期時間準則：

- 設定金鑰的到期時間、以限制使用者存取特定時間段。如果存取金鑰ID和秘密存取金鑰意外暴露、設定短的過期時間有助於降低風險。過期的金鑰會自動移除。
- 如果環境中的安全風險較低、而且您不需要定期建立新金鑰、就不需要設定金鑰的到期時間。如果您決定稍後再建立新金鑰、請手動刪除舊金鑰。

> 您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇“存取管理”>“使用者”。
2. 選取您要管理其S3存取金鑰的使用者。

   使用者詳細資料頁面隨即出現。

3. 選取*存取金鑰*、然後選取*建立金鑰*。
4. 執行下列其中一項：
   - 選取 * 不要設定到期時間 * 來建立不會過期的金鑰。（預設）
   - 選取*設定到期時間*、然後設定到期日和時間。

     > 到期日最長可為從目前日期算起的五年。到期時間最短可從目前時間開始一分鐘。

5. 選取*建立存取金鑰*。

   此時會出現「下載存取金鑰」對話方塊、列出存取金鑰ID和秘密存取金鑰。

6. 將存取金鑰ID和秘密存取金鑰複製到安全位置、或選取*下載.csv*以儲存內含存取金鑰ID和秘密存取金鑰的試算表檔案。

   > 在複製或下載此資訊之前、請勿關閉此對話方塊。對話方塊關閉後、您無法複製或下載金鑰。

7. 選擇*完成*。

   新金鑰會列在使用者詳細資料頁面的「存取金鑰」索引標籤上。

在 StorageGRID 中檢視其他使用者的 S3 存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以檢視其他使用者的S3存取金鑰。您可以依到期時間排序清單、以便判斷哪些金鑰即將到期。您可以視需要建立新的金鑰、並刪除不再使用的金鑰。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您有"root 存取權限"。

> 您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇“存取管理”>“使用者”。
2. 從「使用者」頁面中、選取您要檢視其 S3 存取金鑰的使用者。
3. 從「使用者詳細資料」頁面、選取 * 存取金鑰 * 。
4. 按*過期時間*或*存取金鑰ID*來排序金鑰。
5. 視需要建立新金鑰、並手動刪除不再使用的金鑰。

   如果您在現有金鑰過期之前建立新金鑰、使用者可以開始使用新金鑰、而不會暫時失去帳戶中物件的存取權。

   過期的金鑰會自動移除。

相關資訊

- "建立另一個使用者的S3存取金鑰"
- "刪除其他使用者的S3存取金鑰"

刪除 StorageGRID 中其他使用者的 S3 存取金鑰

如果您使用的是S3租戶、而且您擁有適當的權限、則可以刪除其他使用者的S3存取金鑰。刪除存取金鑰之後、就無法再使用它來存取租戶帳戶中的物件和儲存區。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您有"root 存取權限"。

您可以使用租戶管理程式中顯示的該使用者存取金鑰ID和秘密存取金鑰、來存取屬於該使用者的S3儲存區和物件。因此、請像保護密碼一樣保護存取金鑰。定期旋轉存取金鑰、從帳戶中移除任何未使用的金鑰、而且切勿與其他使用者共用。

步驟

1. 選擇“存取管理”>“使用者”。
2. 從「使用者」頁面中、選取您要管理其 S3 存取金鑰的使用者。
3. 從「使用者詳細資料」頁面選取 * 存取金鑰 * 、然後選取您要刪除的每個存取金鑰的核取方塊。
4. 選取*「動作*」>*「刪除選取的金鑰*」。
5. 從確認對話方塊中、選取 * 刪除機碼 * 。

   頁面右上角會出現確認訊息。

管理S3儲存區

建立 StorageGRID S3 儲存區

您可以使用租戶管理程式來建立S3儲存區以供物件資料使用。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有 root 存取權或管理所有儲存區的使用者群組"權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

  設定或修改儲存桶或物件的 S3 物件鎖定屬性的權限可以透過以下方式授予"庫位原則或群組原則"。

- 如果您計畫為貯體啟用 S3 物件鎖定、則網格管理員已為 StorageGRID 系統啟用全域 S3 物件鎖定設定、而且您已檢閱 S3 物件鎖定貯體和物件的需求。
- 如果多個租戶各自擁有最多 5,000 個儲存桶，則網格中的每個儲存節點至少需要 64 GB 的 RAM。

  StorageGRID 系統為每個 S3 租戶帳戶支援最多 20,000 個儲存桶。每個網格最多可以擁有 100,000 個儲存桶，包括 "分支桶"。此外，"分支桶深度" 也有數量限制。

存取精靈

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間 （ S3 ） * > * 鏟斗 * 。
2. 選取*建立桶*。

輸入詳細資料

步驟

1. 輸入貯體的詳細資料。

欄位	說明
儲存區名稱	符合以下規則的貯體名稱： • 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 • 必須符合DNS規範。 • 必須包含至少 3 個字元、不得超過 63 個字元。 • 每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 • 不得包含虛擬託管樣式要求的句點。期間會導致伺服器萬用字元憑證驗證發生問題。 如需更多資訊，請參閱 "Amazon Web Services（AWS）儲存區命名規則文件"。 • 附註 * ：建立貯體後、您無法變更貯體名稱。
區域	貯體的區域。 您的StorageGRID管理員管理可用區域。儲存桶的區域會影響應用於物件的資料保護策略。預設情況下，所有儲存桶均在 `us-east-1`地區。如果預設區域配置為 `us-east-1`，該其他區域最初是在下拉式選單中選擇的。 • 附註 * ：建立貯體後、您無法變更區域。

2. 選擇*繼續*。

管理設定

步驟

1. 或者、為儲存區啟用物件版本管理。

   如果您要儲存此儲存區中每個物件的每個版本、請啟用物件版本管理。然後您可以視需要擷取物件的舊版。

   如果出現以下情況，則必須啟用物件版本控制：

   ◦ 此儲存桶將用於跨網格複製。

   ◦ 你想創建一個"分支桶"從這個桶子裡。

2. 如果啟用全域 S3 物件鎖定設定、則可選擇性啟用儲存區的 S3 物件鎖定、以使用一次寫入多讀（ WORM ）模式來儲存物件。

   只有當您需要保留物件一段固定時間（例如、為了符合特定法規要求）時、才需要為貯體啟用 S3 物件鎖定。S3 物件鎖定是一項永久性設定、可協助您防止物件在固定的時間內或無限期地遭到刪除或覆寫。

   > 為貯體啟用 S3 物件鎖定設定之後、就無法停用該設定。擁有正確權限的任何人都可以將無法變更的物件新增至此貯體。您可能無法刪除這些物件或貯體本身。

如果您為儲存區啟用S3物件鎖定、則會自動啟用儲存區版本設定。

3. 如果您選取 * 啟用 S3 物件鎖定 * 、則可選擇性啟用此貯體的 * 預設保留 * 。

   您的網格管理員必須授予您權限"使用 S3 物件鎖定的特定功能"。

   啟用 * 預設保留 * 時、新增至貯體的新物件將會自動受到保護、不被刪除或覆寫。「 * 預設保留 * 」設定不會套用至具有其本身保留期間的物件。

   a. 如果啟用 * 預設保留 * 、請為貯體指定 * 預設保留模式 * 。

預設保留模式	說明
治理	• 擁有權限的使用者 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`要求標頭來略過保留設定。 • 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。 • 這些使用者可以增加、減少或移除物件的保留到目前為止。
法規遵循	• 直到達到物件的保留日期、才能刪除物件。 • 物件的保留日期可以增加、但不能減少。 • 直到達到該日期為止、才能移除物件的保留日期。 。注意 * ：您的網格管理員必須允許您使用法規遵循模式。

   b. 如果啟用 * 預設保留 * 、請指定貯體的 * 預設保留期間 * 。

      「 * 預設保留期間 * 」表示新增至此貯體的物件應保留多久、從擷取開始算起。指定小於或等於租用戶保留期間上限的值、如網格管理員所設定。

   網格管理員建立租戶時、會設定 _ 最大 _ 保留期間（可為 1 天至 100 年）。當您設定 *default* 保留期間時、其值不得超過保留期間上限的設定值。如有需要、請要求您的網格管理員增加或縮短最長保留期間。

4. 可選地，選擇*啟用容量限制*，輸入一個值，然後選擇容量單位。

   容量上限是此貯體物件可用的最大容量。此值代表邏輯數量（物件大小）、而非實體數量（磁碟大小）。

   如果未設定上限、則此貯體的容量是無限的。如需詳細資訊、請參閱 "容量限制使用率" 。

5. 可選地，選擇*啟用物件計數限制*。

   物件數量限制是此儲存桶可以包含的最大物件數量。該值代表邏輯數量（物件計數）。如果沒有設定限制，則物件數量不受限制。

6. 選取*建立桶*。

   此庫位會建立並新增至「庫位」頁面上的表格。

7. 您也可以選擇 * 移至貯體詳細資料頁面 * 、以"檢視貯體詳細資料"執行其他組態。

您還可以"建立分支儲存桶"根據需要。

在 StorageGRID 中檢視 S3 儲存貯體詳細資料

您可以檢視租戶帳戶中的貯體。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權、管理所有貯體、或檢視所有貯體權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會出現「鏟斗」頁面。

2. 檢視每個貯體的摘要表。

   視需要、您可以依任何欄排序資訊、也可以在清單中前後翻頁。

   > 顯示的物件計數、使用空間和使用率值為估計值。這些預估值會受到擷取時間、網路連線能力和節點狀態的影響。如果儲存區已啟用版本管理、則刪除的物件版本會包含在物件數中。

   名稱
   貯體的獨特名稱、無法變更。

   啟用的功能
   已啟用貯體功能的清單。

   S3物件鎖定
   儲存區是否啟用 S3 物件鎖定。

   只有在網格啟用 S3 物件鎖定時、才會顯示此欄。此欄也會顯示任何舊版相容桶的資訊。

   區域
   庫位的區域、無法變更。此欄預設為隱藏。

   物件數
   此貯體中的物件數目。如果已啟用版本設定功能、則此值會包含非目前物件版本。

   新增或刪除物件時、此值可能不會立即更新。

   已用空間
   貯體中所有物件的邏輯大小。邏輯大小不包含複寫或銷毀編碼複本或物件中繼資料所需的實際空間。

   此值最多可能需要 10 分鐘才能更新。

使用量

如果已設定容量上限、則為貯體容量上限的使用百分比。

使用率值是根據內部預估、在某些情況下可能會超出。例如、當租戶開始上傳物件時、 StorageGRID 會檢查容量限制（如果已設定）、如果租戶已超過容量限制、則會拒絕新的擷取到此貯體。不過、 StorageGRID 在判斷是否超過容量上限時、並未考慮目前上傳的大小。如果刪除物件、可能會暫時禁止租戶將新物件上傳至此貯體、直到重新計算容量限制使用量為止。計算可能需要 10 分鐘或更長時間。

此值表示邏輯大小、而非儲存物件及其中繼資料所需的實體大小。

容量

如果已設定、則為貯體的容量上限。

建立日期

建立庫位的日期與時間。此欄預設為隱藏。

3. 若要檢視特定貯體的詳細資料、請從表格中選取貯體名稱。
   a. 檢視網頁頂端的摘要資訊、以確認貯體的詳細資料、例如區域和物件計數。
   b. 查看容量限制使用情況和物件數量限制使用情況條。如果使用率達到或接近 100%，請考慮增加限製或刪除一些物件。
   c. 視需要選取 * 刪除貯體中的物件 * 和 * 刪除貯體 * 。

      請密切注意在您選取這些選項時所出現的注意事項。如需詳細資訊、請參閱：

      - "刪除貯體中的所有物件"
      - "刪除貯體"（貯體必須為空）

   d. 視需要檢視或變更每個標籤中的貯體設定。
      - *S3 控制檯 * ：查看桶的對象。如需詳細資訊、請 "使用 S3 Console"參閱。
      - * 鏟斗選項 * ：檢視或變更選項設定。建立貯體後、某些設定（例如 S3 物件鎖定）無法變更。
        - "管理貯體一致性"
        - "上次存取時間更新"
        - "容量限制"
        - "物件數量限制"
        - "物件版本管理"
        - "S3物件鎖定"
        - "預設貯體保留"
        - "管理跨網格複寫"（如果租戶允許）
      - * 平台服務 * ："管理平台服務"（如果租戶允許）
      - * 鏟斗存取 * ：檢視或變更選項設定。您必須擁有特定的存取權限。
        - 配置"儲存桶和物件的 CORS"因此其他網域中的 Web 應用程式可以存取該儲存桶和儲存桶中的物件。

- "控制使用者存取"適用於 S3 貯體和該貯體中的物件。
- 分支：查看儲存桶的分支儲存桶清單。"建立新的分支儲存桶或管理分支儲存桶" 。

了解 **StorageGRID** 分支儲存貯體

分支儲存桶提供對儲存桶中在特定時間存在的物件的存取。

您可以從現有儲存桶建立分支儲存桶。建立分支儲存桶後，建立該儲存桶的原始儲存桶稱為_基本儲存桶_。此外，您可以從另一個分支儲存桶建立一個分支儲存桶。

分支儲存桶提供對受保護資料的訪問，但不作為備份。若要繼續保護數據，請在基本儲存桶上使用這些功能：

- "S3物件鎖定"
- "跨網格複寫"用於基礎桶
- "儲存桶策略"用於版本化儲存桶，以清理舊物件版本

請注意分支桶的以下特徵：

- 您可以使用以下方式存取分支儲存桶中的對象"S3 控制台下載對象"。
- 當客戶端存取分支儲存桶中的物件時，該分支儲存桶的"訪問策略"，而不是基本儲存桶的策略，決定是否允許或拒絕存取。
- 在基礎儲存桶中建立的物件是根據"ILM規則"適用於底部鏟鬥。根據 ILM 規則如何應用於分支儲存桶來評估在分支儲存桶中建立的物件。
- 分支儲存桶不支援跨網格複製。
- 分支儲存桶不支援平台服務。

分支儲存桶使用範例

- 您可以使用分支儲存桶來刪除損壞的對象，方法是從損壞發生之前的時間點建立一個分支儲存桶，然後將應用程式指向該分支儲存桶而不是包含損壞對象的基本儲存桶。
- 您正在將資料保存在版本控制的儲存桶中。存在一個意外的漏洞，導致許多不需要的物件在時間_T_之後被攝取。您可以為先前時間值 *T* 建立一個分支儲存桶，並將用戶端操作重新導向至該分支儲存桶。然後，只有早於時間 *T* 攝取的物件才會暴露給客戶端。
- 您正在將資料儲存在版本化的儲存桶中。由於意外漏洞，導致在時間 *T1* 和 *T2* 之間擷取了許多不必要的物件。您可以為 *Exclude* 時間值 *T1* 和 *T2* 建立分支儲存桶，並將用戶端操作重新導向至該分支儲存桶。如此一來，用戶端只會看到在 *T1* 之前和 *T2* 之後擷取的物件。

對分支儲存桶中的物件進行操作

- 對分支儲存桶執行 PUT 物件操作會在分支中建立一個物件。
- 對分支儲存桶執行 GET 物件操作將從分支中檢索物件。如果分支儲存桶中不存在該對象，則從基本儲存桶中擷取該物件。
- 分支儲存桶中的物件刪除如下：

營運	目標	結果	基本儲存桶中的物件可見性	分支儲存桶中的物件可見性
刪除沒有版本 ID 的	基礎桶	僅為基本儲存桶建立刪除標記	HEAD/GET 傳回物件不存在，但特定版本仍可存取	HEAD/GET 傳回物件存在，且特定版本仍可存取 刪除標記將在分支儲存桶之後創建 `beforeTime`。
根據版本 ID 刪除	基礎桶	刪除了基本儲存桶和分支儲存桶的特定物件版本	HEAD/GET 回傳物件版本不存在	HEAD/GET 回傳物件版本不存在
刪除沒有版本 ID 的	分支桶	僅為分支儲存桶建立刪除標記	HEAD/GET 傳回物件（基本儲存桶物件不受影響）	HEAD/GET 回傳物件不存在
根據版本 ID 刪除	分支桶	僅刪除分支儲存桶的特定物件版本	HEAD/GET 傳回特定物件版本（基本儲存桶物件不受影響）	HEAD/GET 回傳物件版本不存在

另請參閱"如何刪除S3版本控制物件"。

管理 **StorageGRID** 分支儲存區

使用租戶管理器建立和查看分支儲存桶的詳細資訊。

開始之前

- 您已使用"支援的網頁瀏覽器"。
- 您屬於具有 Root 存取權限的使用者群組，或者"管理所有貯體權限"。這些權限將覆蓋群組或儲存桶策略中的權限設定。
- 您要從中建立分支的基本儲存桶具有"已啟用版本控制"。
- 您是基本儲存桶的擁有者。

關於這項工作

請注意分支儲存桶的以下資訊：

分支桶深度限制

一個分支桶最多可以包含 20 個基本桶。隨著分支桶深度的增加，S3 存取延遲可能會增加，尤其是在 ListObjectVersions 呼叫時。

- 如果您從一般基礎儲存桶（最初建立為基礎儲存桶的儲存桶）建立分支儲存桶，則新的分支儲存桶將有一個基礎儲存桶。
- 如果基礎儲存桶本身是分支儲存桶，則新的分支儲存桶將繼承該分支儲存桶的所有基礎儲存桶。使用者只需直接指定一個基礎儲存桶；繼承的基礎儲存桶為隱含存在。
- 基本儲存桶（明確和隱含）的總數不能超過 20。

例如，假設儲存桶 **A** 是一個啟用了版本控制的普通儲存桶：

- 分支桶 **B** 由 **A** 建立，有一個基本桶：**A**。
- 分支桶 **C** 由 **B** 建立，有兩個基本桶：**B**（明確）和 **A**（隱含）。
- 分支桶 **D** 由 **C** 建立，有三個基本桶：**C**（明確）、**B**（隱含）和 **A**（隱含）。
- 這種模式會持續到最大深度達到 20 個基礎儲存桶為止。

S3 物件鎖定權限

可以透過以下方式授予設定儲存桶或物件的 S3 Object Lock 屬性的權限"庫位原則或群組原則"。

暫停版本控制

如果您暫停對基本儲存桶進行版本控制，則基本儲存桶的內容將不再在其分支儲存桶中可見。

配置並建立分支儲存桶後，您無法變更該配置。

建立分支儲存桶

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 選擇要從中建立分支的儲存桶（「基本儲存桶」）。
3. 在儲存桶詳情頁面，選擇*分支* > 建立分支儲存桶。

   如果基本儲存桶未啟用版本控制，則「建立分支儲存桶」按鈕將會停用。

輸入詳細資料

步驟

1. 輸入分支儲存桶的詳細資訊。

欄位	說明
分支儲存桶名稱	符合以下規則的分支儲存桶的名稱： • 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 • 必須符合DNS規範。 • 必須包含至少 3 個字元、不得超過 63 個字元。 • 每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 • 不得包含虛擬託管樣式要求的句點。期間會導致伺服器萬用字元憑證驗證發生問題。 如需詳細資訊，請參閱 "Amazon Web Services（AWS）儲存區命名規則文件"。 注意：建立分支儲存桶後，您無法變更名稱。
區域（無法修改分支儲存桶）	分支儲存桶的區域。 分支儲存桶的區域必須與基本儲存桶的區域匹配，因此此欄位對於分支儲存桶是停用的。
分支桶類型	• 讀寫：您可以在分支儲存桶中新增或刪除物件或物件版本。 • 只讀：您不能修改分支儲存桶中的物件。 注意：僅當分支儲存桶為空時，您才可以將分支儲存桶類型設定為唯讀。如果現有分支儲存桶的類型設定為讀寫，而您尚未寫入，則可以將類型變更為唯讀。

2. 選擇*繼續*。

時間過濾器

選擇要包含基礎儲存桶中物件版本的時間範圍。對於任何時間篩選器，請選擇以下範圍內的任何日期：

- 最短日期：2010 年 1 月 1 日（UTC）
- 最長期限：自今日（UTC）起五年

之前
: 分支儲存桶提供對早於 *Before* 時間建立的物件版本的存取。

之後
: 分支儲存桶提供對晚於 *After* 時間所建立之物件版本的存取。

之間
: 分支儲存桶提供對在 *From* 和 *To* 時間之間建立的物件版本的存取。

排除

分支儲存桶不提供對在 *Exclude from* 和 *Exclude to* 時間之間建立的物件版本的存取。

管理對象設定（可選）

分支儲存桶的物件設定不會影響基礎儲存桶中的物件版本。

步驟

1. 如果啟用了全域 S3 物件鎖定設置，則可以選擇為分支儲存桶啟用 S3 物件鎖定。若要啟用 S3 物件鎖，分支儲存桶必須是讀寫儲存桶。

   只有當您需要將物件保留一段固定的時間（例如，為了滿足某些監管要求）時，才為分支儲存桶啟用 S3 物件鎖定。 S3 物件鎖定是一種永久性設置，可協助您防止物件在固定時間內或無限期內被刪除或覆蓋。

   > 一旦為儲存桶啟用 S3 物件鎖定設置，就無法停用它。任何擁有正確權限的人都可以將物件新增到無法更改的分支儲存桶中。您可能無法刪除這些物件或分支儲存桶本身。

2. 如果您選擇了“啟用 S3 物件鎖定”，則可以選擇為分支儲存桶啟用“預設保留”。

   > 您的網格管理員必須授予您權限"使用 S3 物件鎖定的特定功能"。

   當啟用*預設保留*時，新增至分支儲存桶的新物件將自動受到保護，免遭刪除或覆蓋。 *預設保留*設定不適用於具有自己的保留期的物件。

   a. 如果啟用了*預設保留*，請為分支儲存桶指定*預設保留模式*。

預設保留模式	說明
治理	• 擁有權限的使用者 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`要求標頭來略過保留設定。 • 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。 • 這些使用者可以增加、減少或移除物件的保留到目前為止。
法規遵循	• 直到達到物件的保留日期、才能刪除物件。 • 物件的保留日期可以增加、但不能減少。 • 直到達到該日期為止、才能移除物件的保留日期。 。注意 * ：您的網格管理員必須允許您使用法規遵循模式。

   b. 如果啟用了*預設保留*，請指定分支儲存桶的*預設保留期*。

      *預設保留期*表示從提取新物件開始，新增至分支儲存桶中的新物件應保留多長時間。指定一個小於或等於網格管理員設定的租用戶最大保留期的值。

網格管理員建立租戶時、會設定 _ 最大 _ 保留期間（可為 1 天至 100 年）。當您設定 *default* 保留期間時、其值不得超過保留期間上限的設定值。如有需要、請要求您的網格管理員增加或縮短最長保留期間。

3. 或者，選擇“啟用容量限制”。

   容量限制是分支桶可用的最大容量。該值代表邏輯量（物件大小），而不是物理量（磁碟上的大小）。

   如果沒有設定限制，則分支桶的容量是無限的。請參閱"容量限制使用率"了解更多。

   > 此設定僅適用於直接提取到分支儲存桶中的對象，而不適用於透過分支儲存桶從基礎儲存桶中可見的對象。

4. 或者，選擇“啟用物件計數限制”。

   物件計數限制是分支儲存桶可以包含的最大物件數。該值代表邏輯數量（物件計數）。如果沒有設定限制，則物件數量不受限制。

   > 此設定僅適用於直接提取到分支儲存桶中的對象，而不適用於透過分支儲存桶從基礎儲存桶中可見的對象。

5. 選取*建立桶*。

   分支儲存桶已建立並新增至「儲存桶」頁面上的表格中。

6. 或者，選擇“前往儲存桶詳細資料頁面”"查看分支存儲桶詳細信息"並執行額外的配置。

   在 Bucket 詳情頁面，對於唯讀 Bucket，一些與修改物件相關的設定選項已停用。

將 **ILM** 策略標籤套用至 **StorageGRID** 儲存貯體

根據您的物件儲存需求、選擇要套用至儲存區的 ILM 原則標籤。

ILM 原則可控制物件資料的儲存位置、以及是否在一段時間後刪除。您的網格管理員會建立 ILM 原則、並在使用多個作用中原則時將其指派給 ILM 原則標籤。

> 避免經常重新指派貯體的原則標籤。否則可能會發生效能問題。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權、管理所有貯體、或檢視所有貯體權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會出現「鏟斗」頁面。視需要、您可以依任何欄排序資訊、也可以在清單中前後翻頁。

2. 選取您要指派 ILM 原則標籤的儲存區名稱。

   您也可以變更已指派標記之貯體的 ILM 原則標記指派。

所顯示的「物件數」和「已用空間」值為預估值。這些預估值會受到擷取時間、網路連線能力和節點狀態的影響。如果儲存區已啟用版本管理、則刪除的物件版本會包含在物件數中。

3. 在「 Bucket 選項」索引標籤中、展開 ILM 原則標籤折疊式。只有當您的網格管理員已啟用使用自訂原則標籤時、才會出現此折疊面板。
4. 請閱讀每個原則標籤的說明、以判斷應將哪個標籤套用至貯體。

變更貯體的 ILM 原則標籤將會觸發 ILM 重新評估貯體中的所有物件。如果新原則保留物件的時間有限、舊物件將會刪除。

5. 針對您要指派給貯體的標記、選取選項按鈕。
6. 選取*儲存變更*。新的 S3 儲存貯體標籤將會在儲存貯體上設定、並提供 ILM 原則標籤名稱的金鑰 `NTAP-SG-ILM-BUCKET-TAG`和值。

確保 S3 應用程式不會意外置換或刪除新的 Bucket 標記。如果在將新的 TagSet 套用至貯體時省略此標記、則貯體中的物件會還原為根據預設的 ILM 原則進行評估。

僅使用通過 ILM 原則標籤驗證的租戶管理員或租戶管理器 API 來設定及修改 ILM 原則標籤。請勿使用 S3 PuttBucketTaggingTaggingAPI 或 S3 DeletBucketaggingTaggingAPI 來修改 `NTAP-SG-ILM-BUCKET-TAG` ILM 原則標籤。

變更指派給貯體的原則標籤會暫時影響效能、同時使用新的 ILM 原則重新評估物件。

管理 **StorageGRID** 儲存貯體原則

您可以控制 S3 貯體和該貯體中物件的使用者存取。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。「檢視所有貯體」和「管理所有貯體」權限僅允許檢視。
- 您已確認所需的儲存節點和站台數量可用。如果任一站台內沒有兩個以上的儲存節點、或站台無法使用、則這些設定的變更可能無法使用。

步驟

1. 選擇 * 鏟斗 * 、然後選擇您要管理的鏟斗。
2. 在貯體詳細資料頁面上、選取 * 貯體存取 * > * 貯體原則 * 。
3. 執行下列其中一項：
   - 選取「 * 啟用原則 * 」核取方塊以輸入貯體原則。然後輸入有效的 JSON 格式字串。

     每個儲存區原則的大小上限為 20 、 480 位元組。

   - 編輯字串以修改現有原則。
   - 取消選取 * 啟用原則 * 以停用原則。

如需有關儲存庫原則的詳細資訊、包括語言語法和範例"貯體原則範例"、請參閱。

管理 **StorageGRID** 儲存貯體一致性

一致性值可用來指定儲存區設定變更的可用度、並在儲存節點和站台之間的物件可用度與這些物件一致性之間取得平衡。您可以將一致性值變更為不同於預設值、讓用戶端應用程式能夠滿足其作業需求。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

貯體一致性準則

貯體一致性用於判斷影響該 S3 貯體內物件的用戶端應用程式一致性。一般而言、您應該為儲存區使用 * 讀取 - 新寫入 * 一致性。

[[change-bucker-consistency （變更貯體一致性） **]** 變更貯體一致性

如果 **Read-after new-write** 的一致性不符合用戶端應用程式的要求、您可以透過設定貯體一致性或使用標頭來變更一致性 `Consistency-Control`。 `Consistency-Control`標頭會取代貯體一致性。

> 當您變更貯體的一致性時、只有在變更後擷取的物件才保證符合修訂的設定。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 ** 折疊式。
4. 針對此貯體中的物件所執行的作業、選取一致性。
   - * 全部 * ：提供最高等級的一致性。所有節點都會立即接收資料、否則要求將會失敗。
   - **Strong-globall** ：保證所有網站上所有用戶端要求的寫入後讀取一致性。
   - **Strong-site** ：保證網站內所有用戶端要求的寫入後讀取一致性。
   - * 新寫入後讀取 * （預設）：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
   - * 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。
5. 選取*儲存變更*。

變更貯體設定時會發生什麼情況

貯體有多個設定會影響貯體和這些貯體內物件的行為。

下列貯體設定預設使用 * 強 * 一致性。如果任一站台內沒有兩個以上的儲存節點、或站台無法使用、則這些設定的任何變更可能無法使用。

- "背景空白貯體刪除"
- "上次存取時間"
- "生命週期"
- "貯體原則"
- "貯體標記"
- "貯體版本管理"
- "S3物件鎖定"
- "貯體加密"

貯體版本管理、 S3 物件鎖定和貯體加密的一致性值無法設定為不太一致的值。

下列貯體設定不使用強而一致的特性、而且變更的可用度也較高。變更這些設定可能需要一些時間才能生效。

- "平台服務組態：通知、複寫或搜尋整合"
- "為儲存桶和物件配置StorageGRID CORS"
- 變更貯體一致性

如果變更貯體設定時所使用的預設一致性不符合用戶端應用程式的需求、您可以使用或 `force`的標頭"S3 REST API"來變更一致性、 `Consistency-Control`或使用中的或 `reducedConsistency`選項"租戶管理API"。

啟用或停用 **StorageGRID** 中的上次存取時間更新

當網格管理員為StorageGRID 某個系統建立資訊生命週期管理（ILM）規則時、他們可以選擇性地指定物件的上次存取時間、以決定是否要將該物件移到不同的儲存位置。如果您使用的是S3租戶、您可以針對S3儲存區中的物件啟用上次存取時間更新、藉此充分利用這類規則。

這些指示僅適用於至少包含一個 ILM 規則的 StorageGRID 系統、該規則使用 * 上次存取時間 * 選項作為進階篩選器或參考時間。如果您的支援系統不包含此類規則、您可以忽略這些指示StorageGRID 。如需詳細資訊、請參閱 "在 ILM 規則中使用上次存取時間" 。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。

關於這項工作

- 上次存取時間 * 是 ILM 規則的 * 參考時間 * 放置指示可用的選項之一。將規則的參考時間設為上次存取時間、可讓網格管理員根據上次擷取（讀取或檢視）物件的時間、指定物件放置在特定儲存位置。

例如、為了確保最近檢視的物件仍保留在較快的儲存空間、網格管理員可以建立ILM規則、指定下列項目：

- 過去一個月擷取的物件應保留在本機儲存節點上。
- 過去一個月未擷取的物件應移至異地位置。

根據預設、上次存取時間的更新會停用。如果您的 StorageGRID 系統包含使用 * 上次存取時間 * 選項的 ILM 規則、且您想要將此選項套用至此儲存庫中的物件、則必須針對該規則中指定的 S3 儲存區、啟用更新至上次存取時間。

更新上次擷取物件的存取時間、可能會降低StorageGRID 功能性、尤其是小型物件的效能。

上次存取時間更新會影響效能、因為StorageGRID 每次擷取物件時、VMware都必須執行下列額外步驟：

- 使用新的時間戳記更新物件
- 將物件新增至ILM佇列、以便根據目前的ILM規則和原則重新評估

下表摘要說明上次存取時間停用或啟用時、套用至儲存區中所有物件的行為。

申請類型	停用上次存取時間時的行為（預設）		啟用上次存取時間時的行為	
	上次存取時間已更新？	新增至ILM評估佇列的物件？	上次存取時間已更新？	新增至ILM評估佇列的物件？
發出 HEAD 操作時請求擷取物件的元數據	否	否	否	否
要求擷取物件、其存取控制清單或其中繼資料	否	否	是的	是的
要求更新物件的中繼資料	是的	是的	是的	是的
要求列出物件或物件版本	否	否	否	否
要求將物件從一個儲存區複製到另一個儲存區	• 否、來源複本 • 是、適用於目的地複本	• 否、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本	• 是、來源複本 • 是、適用於目的地複本
要求完成多部分上傳	是的、適用於組裝好的物件	是的、適用於組裝好的物件	是的、適用於組裝好的物件	是的、適用於組裝好的物件

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 * 上次存取時間更新 * 手風琴。
4. 啟用或停用上次存取時間更新。
5. 選取*儲存變更*。

變更 **StorageGRID** 中 **S3** 儲存貯體的物件版本管理

如果您使用的是 S3 租戶、則可以變更 S3 儲存區的版本設定狀態。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- 您已確認所需的儲存節點和站台數量可用。如果任一站台內沒有兩個以上的儲存節點、或站台無法使用、則這些設定的變更可能無法使用。

關於這項工作

您可以啟用或暫停儲存區的物件版本管理。在您啟用貯體的版本設定之後、它就無法恢復至未版本化狀態。不過、您可以暫停儲存區的版本管理。

- 停用：從未啟用版本管理
- 已啟用：已啟用版本管理
- 已暫停：先前已啟用版本管理、並已暫停

如需詳細資訊、請參閱下列內容：

- "物件版本管理"
- "S3版本化物件的ILM規則和原則（範例4）"
- "如何刪除物件"

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。
3. 從 * 儲存庫選項 * 標籤中、選取 * 物件版本設定 * 折疊器。
4. 選取此儲存區中物件的版本管理狀態。

   物件版本設定功能必須保持啟用、才能用於跨網格複寫的儲存區。如果啟用S3物件鎖定或舊版規範、則會停用*物件版本管理*選項。

選項	說明
啟用版本管理	如果您要儲存此儲存區中每個物件的每個版本、請啟用物件版本管理。然後您可以視需要擷取物件的舊版。 使用者修改儲存庫中已有的物件時、將會對其進行版本控制。
暫停版本管理	如果您不想再建立新的物件版本、請暫停物件版本管理。您仍然可以擷取任何現有的物件版本。

5. 選取*儲存變更*。

使用 **S3** 物件鎖定來保留 **StorageGRID** 中的物件

如果貯體和物件必須符合保留法規要求、您可以使用 S3 物件鎖定。

您的網格管理員必須授予您使用 S3 物件鎖定特定功能的權限。

什麼是**S3**物件鎖定？

「物件鎖定」功能是物件保護解決方案、StorageGRID 相當於Amazon Simple Storage Service（Amazon S3）中的S3物件鎖定。

當 StorageGRID 系統啟用全域 S3 物件鎖定設定後，S3 租戶帳戶可以建立啟用或未啟用 S3 物件鎖定的儲存桶。當啟用「允許對現有儲存桶啟用 S3 物件鎖定」設定後，S3 租戶帳戶可以為現有儲存桶啟用 S3 物件鎖定。如果儲存桶啟用了 S3 物件鎖定，則必須啟用儲存桶版本控制，且版本控制會自動啟用。S3 租戶帳戶為新建或現有儲存桶啟用 S3 物件鎖定後，將無法停用此功能。

- 沒有 S3 物件鎖定 * 的貯體只能有未指定保留設定的物件。任何擷取的物件都不會有保留設定。
- 具有 S3 物件鎖定 * 的儲存貯體可以有物件、無論是否有 S3 用戶端應用程式指定的保留設定。某些擷取的物件會有保留設定。
- 已設定 S3 物件鎖定和預設保留 * 的貯體、可以使用指定的保留設定來上傳物件、也可以不保留設定來上傳新物件。新物件會使用預設設定、因為尚未在物件層級設定保留設定。

有效地說、所有新擷取的物件在設定預設保留時都會有保留設定。沒有物件保留設定的現有物件不會受到影響。

保留模式

StorageGRID S3 物件鎖定功能支援兩種保留模式、可將不同層級的保護套用至物件。這些模式相當於 Amazon S3 保留模式。

- 在法規遵循模式中：
  - 直到達到物件的保留日期、才能刪除物件。
  - 物件的保留日期可以增加、但不能減少。
  - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
  - 具有特殊權限的使用者可以在修改特定保留設定的要求中使用略過標頭。

- 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
- 這些使用者可以增加、減少或移除物件的保留到目前為止。

物件版本的保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以使用 S3 用戶端應用程式、針對新增至貯體的每個物件、選擇性地指定下列保留設定：

- * 保留模式 * ：法規遵循或治理。
- * 保留至日期 * ：如果物件版本的保留至未來日期、則可以擷取物件、但無法刪除。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。合法持有不受保留至日期的限制。

> ⓘ 如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

有關物件設定的詳細資訊，請參閱"使用 S3 REST API 來設定 S3 物件鎖定"。

貯體的預設保留設定

如果在啟用 S3 物件鎖定的情況下建立貯體、使用者可以選擇性地指定貯體的下列預設設定：

- * 預設保留模式 * ：法規遵循或治理。
- * 預設保留期間 * ：新增至此貯體的物件版本應保留多久、從新增物件之日起算。

預設的貯體設定僅適用於沒有自己保留設定的新物件。當您新增或變更這些預設設定時、現有的貯體物件不會受到影響。

請參閱 "建立S3儲存區" 和 "更新 S3 物件鎖定預設保留"。

S3 物件鎖定工作

下列網格管理員和租戶使用者清單包含使用 S3 物件鎖定功能的高階工作。

網格管理員

- 為整個 StorageGRID 系統啟用全域 S3 物件鎖定設定。
- 允許使用者為現有儲存桶啟用 S3 物件鎖定。
- 確保資訊生命週期管理（ ILM ）原則符合 _ 標準 _ "啟用 S3 物件鎖定的貯體需求"、亦即符合。
- 視需要、允許租戶使用「法規遵循」做為保留模式。否則、只允許使用監管模式。
- 視需要為租戶設定最長保留期間。

租戶使用者

- 檢閱 S3 物件鎖定的貯體和物件考量事項。
- 如有需要，請聯絡網格系統管理員啟用以下設定之一：
  - 全域 S3 物件鎖定

- 允許為現有儲存桶啟用 S3 物件鎖定

- 建立啟用 S3 物件鎖定的貯體。
- 對現有儲存桶啟用 S3 物件鎖定。
- 您也可以選擇設定貯體的預設保留設定：
  - 預設保留模式：監管或法規遵循（如果網格管理員允許）。
  - 預設保留期間：必須小於或等於網格管理員設定的最大保留期間。
- 使用 S3 用戶端應用程式來新增物件、並選擇性地設定物件特定的保留：
  - 保留模式。監管或法規遵循、如果網格管理員允許的話。
  - 保留截止日期：必須小於或等於網格管理員設定的保留期間上限所允許的值。

啟用**S3**物件鎖定的儲存區需求

- 如果StorageGRID 已針對整個S3物件鎖定設定啟用for the S廳 系統、您可以使用租戶管理程式、租戶管理API或S3 REST API來建立啟用S3物件鎖定的儲存區。
- 當「S3物件鎖定」已啟用時、StorageGRID 即可自動啟用該儲存區的版本管理功能。您無法停用儲存區的 S3 物件鎖定或暫停版本設定。
- 您也可以選擇使用租戶管理員、租戶管理 API 或 S3 REST API 、為每個貯體指定預設保留模式和保留期間。貯體的預設保留設定僅適用於新增至貯體但沒有其本身保留設定的新物件。您可以指定保留模式來覆寫這些預設設定、並在上傳每個物件版本時保留至日期。
- 啟用 S3 物件鎖定的貯體支援貯體生命週期組態。

啟用**S3**物件鎖定之儲存區中的物件需求

- 若要保護物件版本、您可以指定貯體的預設保留設定、或是指定每個物件版本的保留設定。可以使用 S3 用戶端應用程式或 S3 REST API 來指定物件層級保留設定。
- 保留設定適用於個別物件版本。物件版本可以同時具有「保留直到日期」和「合法保留」設定、但不能有另一個設定、或兩者都沒有。指定物件的保留截止日期或合法保留設定、只會保護要求中指定的版本。您可以建立物件的新版本、而舊版物件仍會保持鎖定狀態。

啟用**S3**物件鎖定的儲存區物件生命週期

儲存在已啟用 S3 物件鎖定的儲存貯體中的每個物件都會經過下列階段：

1. 物件擷取

   當物件版本新增至啟用 S3 物件鎖定的儲存區時、保留設定會套用如下：

   - 如果為物件指定保留設定、則會套用物件層級的設定。任何預設貯體設定都會被忽略。
   - 如果未指定物件的保留設定、則會套用預設貯體設定（如果存在）。
   - 如果未指定物件或貯體的保留設定、則 S3 物件鎖定不會保護該物件。

   如果套用保留設定、則物件和任何 S3 使用者定義的中繼資料都會受到保護。

2. * 物件保留與刪除 *

   StorageGRID 會在指定的保留期間內儲存每個受保護物件的多個複本。物件複本和儲存位置的確切數量和類

型取決於主動式 ILM 原則中的相容規則。受保護物件是否能在達到保留截止日期之前刪除、取決於其保留模式。

- 如果物件處於合法保留狀態、則無論物件的保留模式為何、任何人都無法刪除該物件。

我是否仍能管理舊有的法規遵循貯體？

S3物件鎖定功能取代先前StorageGRID 版本的Compliance功能。如果您使用StorageGRID 舊版的《不規則》建立了相容的儲存桶、您可以繼續管理這些儲存桶的設定、但是您無法再建立新的相容儲存桶。有關說明，請參閱https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"^]。

相關資訊

瞭解 "S3 物件鎖定要求"

更新 **StorageGRID** 中的 **S3 Object Lock** 預設保留

如果您在建立貯體時啟用 S3 物件鎖定、則可以編輯貯體以變更預設保留設定。您可以啟用（或停用）預設保留、並設定預設保留模式和保留期間。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- S3 物件鎖定已在 StorageGRID 系統中全域啟用、您在建立儲存貯體時啟用 S3 物件鎖定。請參閱。 "使用 S3 物件鎖定來保留物件"

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
2. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

3. 從 **Bucket options** 標籤中、選取 **S3 Object Lock** 折疊式。
4. 或者、啟用或停用此貯體的 * 預設保留 * 。

   對此設定所做的變更不適用於已在貯體中的物件、也不適用於可能有其本身保留期間的任何物件。

5. 如果啟用 * 預設保留 * 、請為貯體指定 * 預設保留模式 * 。

預設保留模式	說明
治理	• 擁有權限的使用者 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`要求標頭來略過保留設定。 • 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。 • 這些使用者可以增加、減少或移除物件的保留到目前為止。
法規遵循	• 直到達到物件的保留日期、才能刪除物件。 • 物件的保留日期可以增加、但不能減少。 • 直到達到該日期為止、才能移除物件的保留日期。 。注意 * ：您的網格管理員必須允許您使用法規遵循模式。

6. 如果啟用 * 預設保留 * 、請指定貯體的 * 預設保留期間 * 。

   「 * 預設保留期間 * 」表示新增至此貯體的物件應保留多久、從擷取開始算起。指定小於或等於租用戶保留期間上限的值、如網格管理員所設定。

   網格管理員建立租戶時、會設定 _ 最大 _ 保留期間（可為 1 天至 100 年）。當您設定 *default* 保留期間時、其值不得超過保留期間上限的設定值。如有需要、請要求您的網格管理員增加或縮短最長保留期間。

7. 選取*儲存變更*。

在 StorageGRID 中設定 S3 儲存貯體的 CORS

如果您想讓其他網域中的 Web 應用程式能夠存取 S3 貯體中的貯體和物件、則可以為 S3 貯體設定跨來源資源共享（ CORS ）。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 對於 Get CORS 組態要求、您屬於具有的使用者群組"管理所有貯體或檢視所有貯體權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- 對於 Put CORS 組態要求、您屬於具有的使用者群組"管理所有貯體權限"。此權限會覆寫群組或儲存區原則中的權限設定。
- "root 存取權限"可存取所有 CORS 組態要求。

關於這項工作

跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的 S3 儲存區 `Images`來儲存圖形。透過設定貯體的 `CORS` `Images` 、您可以允許該貯體中的影像顯示在網站上 `http://www.example.com`。

為貯體啟用 CORS

步驟

1. 使用文字編輯器建立必要的 XML 。此範例顯示用於啟用S3儲存區的CORS的XML。具體而言：

- 允許任何網域將 GET 要求傳送至貯體
- 僅允許 `http://www.example.com`網域傳送 GET 、 POST 和 DELETE 要求
- 允許所有要求標頭

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

如需 CORS 組態 XML 的詳細資訊、請參閱 "Amazon Web Services （ AWS ）說明文件： Amazon Simple Storage Service 使用者指南"。

2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
3. 從表格中選取貯體名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 從 **Bucket access** （庫存取 * ）標籤中、選取 * 跨來源資源共用（ CORS ） * 折疊。
5. 選中 * 啓用 CORS* 複選框。
6. 將 CORS 組態 XML 貼到文字方塊中。
7. 選取*儲存變更*。

修改 **CORS** 設定

步驟

1. 在文字方塊中更新 CORS 組態 XML 、或選取 * 清除 * 重新開始。
2. 選取*儲存變更*。

停用 **CORS** 設定

步驟

1. 清除 **Enable CORS** （啓用 CORS* ）複選框。
2. 選取*儲存變更*。

相關資訊

"為管理介面配置StorageGRID CORS"

從 **StorageGRID S3** 儲存貯體中刪除物件

您可以使用 Tenant Manager 刪除一個或多個貯體中的物件。

考量與要求

執行這些步驟之前、請注意下列事項：

- 當您刪除貯體中的物件時、 StorageGRID 會從 StorageGRID 系統中的所有節點和站台、永久移除每個所選貯體中的所有物件和所有物件版本。StorageGRID 也會移除任何相關的物件中繼資料。您將無法恢復此資訊。
- 根據物件數量、物件複本和並行作業、刪除貯體中的所有物件可能需要數分鐘、數天甚至數週的時間。
- 如果某個貯體有"S3 物件鎖定已啟用"、它可能會保留在 * 刪除物件：唯讀 * 狀態、時間 _ 年 _ 。

> 使用 S3 物件鎖定的貯體將保留在 * 刪除物件：唯讀 * 狀態、直到達到所有物件的保留日期、並移除任何合法保留為止。

- 刪除物件時、貯體的狀態為 * 刪除物件：唯讀 * 。在此狀態下、您無法將新物件新增至貯體。
- 刪除所有物件後、貯體仍保持唯讀狀態。您可以執行下列其中一項：
  - 將貯體恢復為寫入模式、並將其重複用於新物件
  - 刪除貯體
  - 將貯體保持在唯讀模式、以保留其名稱供未來使用
- 如果貯體已啟用物件版本設定、則可使用刪除貯體作業中的物件來移除在 StorageGRID 11.8 或更新版本中建立的標記。
- 如果某個貯體已啟用物件版本設定、則刪除物件作業將不會移除在 StorageGRID 11.7 或更早版本中建立的刪除標記。請參閱中有關刪除貯體中物件"如何刪除S3版本控制物件"的資訊。
- 如果您使用"跨網格複寫"、請注意下列事項：
  - 使用此選項不會刪除其他網格上的貯體中的任何物件。
  - 如果您為來源貯體選取此選項、當您將物件新增至其他網格上的目的地貯體時、就會觸發 * 跨網格複寫失敗 * 警示。如果您無法保證、在刪除所有貯體物件之前、沒有人會將物件新增至另一個網格的貯體"停用跨網格複寫"。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"root 存取權限"。此權限會覆寫群組或儲存區原則中的權限設定。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。

2. 使用 * 動作 * 功能表或特定儲存庫的詳細資料頁面。

「行動」功能表

a. 選取您要從中刪除物件的每個貯體的核取方塊。

b. 選取 * 動作 * > * 刪除貯體中的物件 * 。

詳細資料頁面

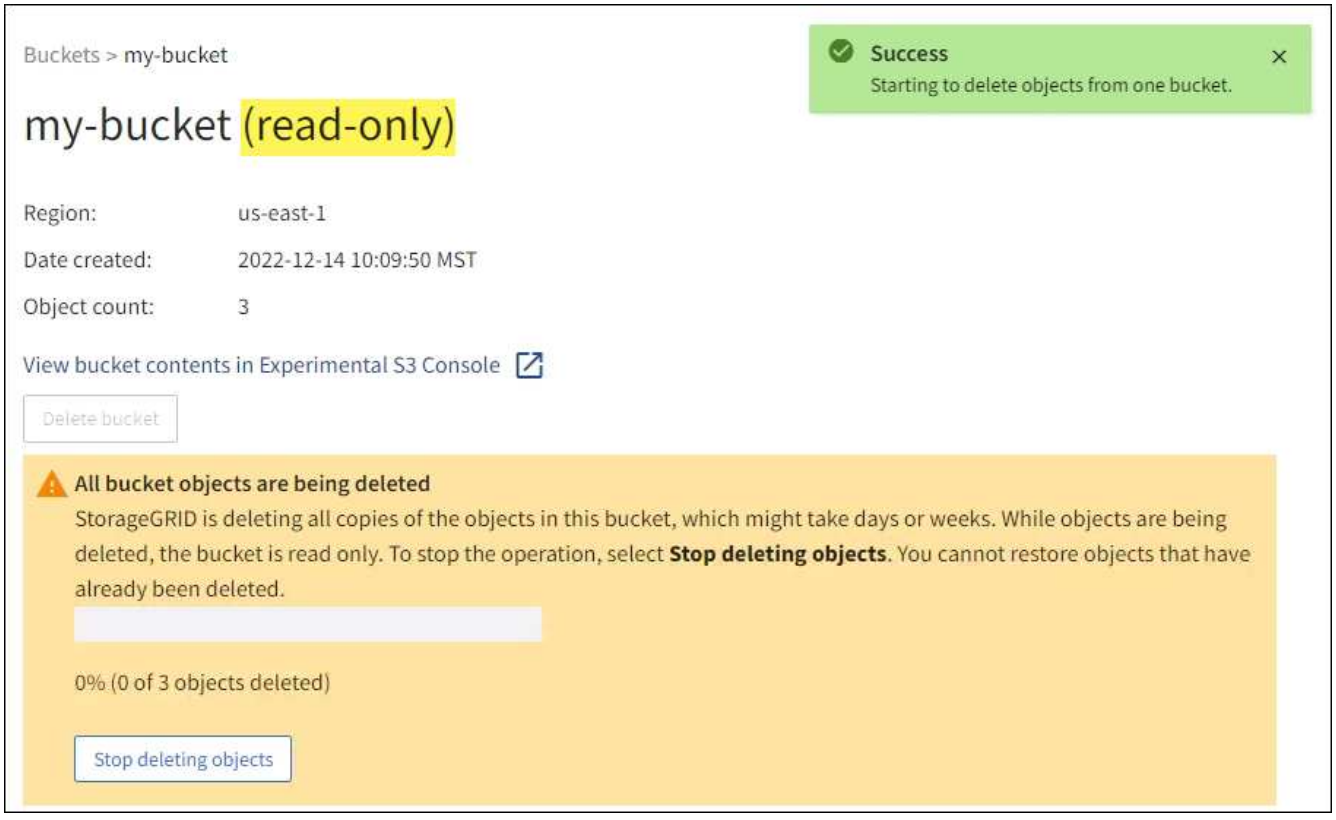
a. 選取貯體名稱以顯示其詳細資料。

b. 選取 * 刪除貯體中的物件 * 。

3. 當確認對話方塊出現時、請檢閱詳細資料、輸入 * 是 * 、然後選取 * 確定 * 。
4. 等待刪除作業開始。

   幾分鐘後：

   - 貯體詳細資料頁面上會出現黃色狀態橫幅。進度列代表已刪除物件的百分比。
   - * （唯讀） * 會出現在貯體詳細資料頁面上的貯體名稱之後。
   - * （刪除物件：唯讀） * 會出現在「 Bucket 」頁面上的 Bucket 名稱旁邊。

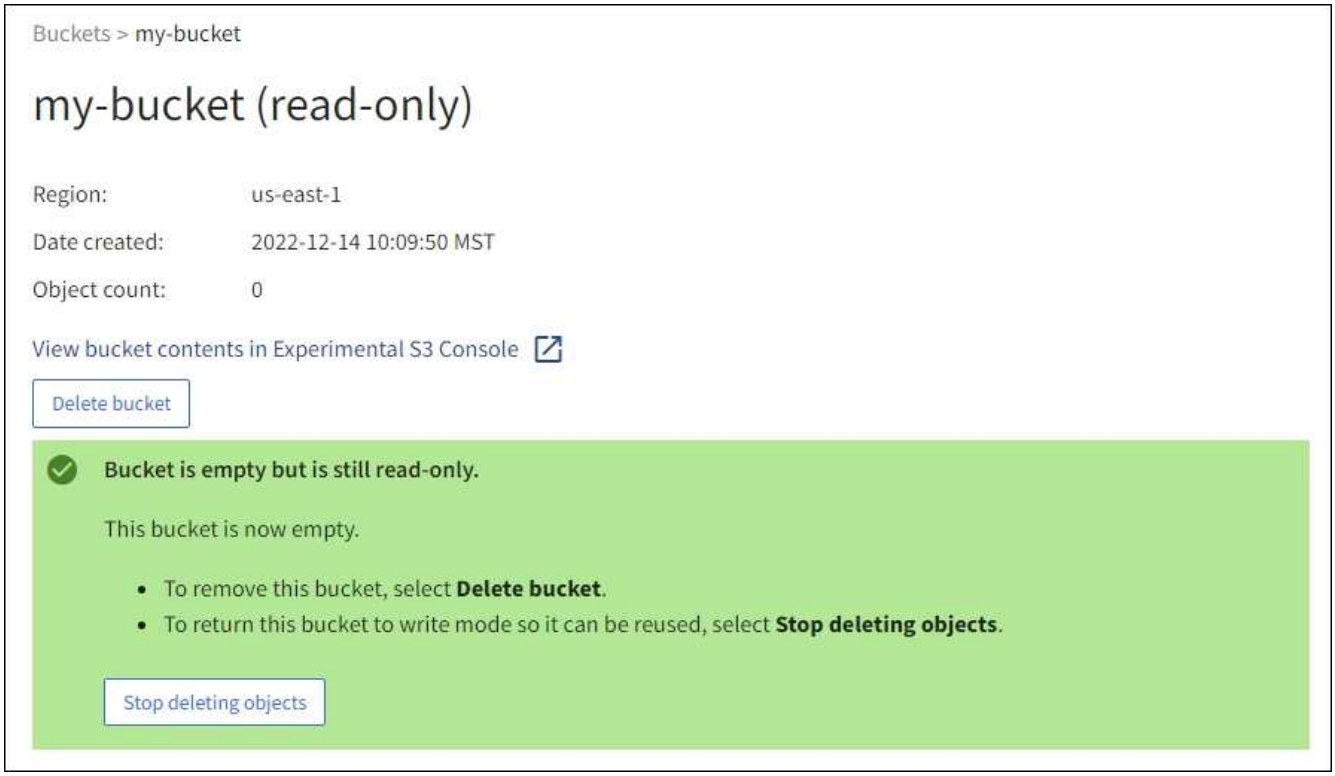


5. 在作業執行時視需要選取 * 停止刪除物件 * 以停止處理程序。然後、您也可以選擇 * 刪除貯體中的物件 * 來恢復處理程序。

   當您選取 * 停止刪除物件 * 時、貯體會返回寫入模式、但您無法存取或還原任何已刪除的物件。

6. 等待作業完成。

當貯體為空時、狀態橫幅會更新、但貯體仍為唯讀。



7. 執行下列其中一項：
   - 離開頁面以保持貯體處於唯讀模式。例如、您可以將空貯體保留為唯讀模式、以保留貯體名稱供未來使用。
   - 刪除儲存庫。您可以選擇 * 刪除貯體 * 來刪除單一貯體、或是退回 " 鏟斗 " 頁面、然後選取 * 動作 * > * 刪除 * 貯體來移除多個貯體。

     如果在刪除所有物件之後、無法刪除版本化的貯體、則刪除標記可能會保留。若要刪除貯體、您必須移除所有剩餘的刪除標記。

   - 將貯體恢復為寫入模式、並選擇性地將其重複用於新物件。您可以選擇 * 停止刪除單一貯體的物件 * 、或返回至鏟斗頁面、然後針對多個貯體選取 * 操作 * > * 停止刪除物件 * 。

刪除 **StorageGRID S3** 儲存貯體

您可以使用租戶管理程式刪除一或多個空的S3儲存區。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會覆寫群組或儲存區原則中的權限設定。
- 您要刪除的儲存區是空的。如果您要刪除的貯體不是空的，"刪除貯體中的物件"。

關於這項工作

這些指示說明如何使用租戶管理程式刪除S3儲存區。您也可以使用或刪除 S3 儲存區"租戶管理API""S3 REST API"。

如果 S3 儲存區包含物件、非目前物件版本或刪除標記、則無法刪除該儲存區。如需如何刪除 S3 版本化物件的相關資訊，請參閱"如何刪除物件"。

步驟

1. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。

   此時會顯示「庫位」頁面、並顯示所有現有的S3庫位。

2. 使用 * 動作 * 功能表或特定儲存庫的詳細資料頁面。

   「行動」功能表

   a. 選取您要刪除的每個貯體的核取方塊。

   b. 選取 * 動作 * > * 刪除儲存區 * 。

   詳細資料頁面

   a. 選取貯體名稱以顯示其詳細資料。

   b. 選取 * 刪除儲存庫 * 。

3. 當確認對話方塊出現時、請選取 * 是 * 。

   確認每個儲存區都是空的、然後刪除每個儲存區。StorageGRID此作業可能需要幾分鐘的時間。

   如果儲存區不是空的、就會出現錯誤訊息。您必須"刪除貯體中的所有物件和任何刪除標記"先刪除貯體、才能刪除該貯體。

在 **StorageGRID** 中使用 **S3 Console**

您可以使用 S3 Console 來檢視和管理 S3 儲存區中的物件。

S3 主控台可讓您：

- 上傳、下載、重新命名、複製、移動、 並刪除物件
- 檢視、還原、下載及刪除物件版本
- 依字首搜尋物件
- 管理物件標記
- 檢視物件中繼資料
- 檢視、建立、重新命名、複製、移動、 並刪除資料夾

> S3 主控台可改善最常見的使用者體驗。並非設計用來取代所有情況下的 CLI 或 API 作業。
>
> 如果使用 S3 Console 導致作業耗時過長（例如、分鐘或小時）、請考慮：
>
> - 減少所選物件的數量
> - 使用非圖形化（ API 或 CLI ）方法存取資料

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 如果您想要管理物件、則屬於具有「根」存取權限的使用者群組。或者、您屬於具有「使用 S3 主控台標籤」權限、以及「檢視所有貯體」權限或「管理所有貯體」權限的使用者群組。請參閱。 "租戶管理權限"
- 已為使用者配置 S3 群組或儲存桶策略。看"使用貯體和群組存取原則" 。
- 您知道使用者的存取金鑰ID和秘密存取金鑰。您也可以選擇 `.csv`包含此資訊的檔案。請參閱"建立存取金鑰的說明"。

步驟

1. 選擇 儲存 > 儲存桶 > 儲存桶名稱。
2. 選取 S3 主控台索引標籤。
3. 將存取金鑰 ID 和秘密存取金鑰貼到欄位中。否則、請選取 * 上傳存取金鑰 * 、然後選取您的 `.csv`檔案。
4. 選擇*登入*。
5. 此時會出現貯體物件的表格。您可以視需要管理物件。

其他資訊

- * 依字首搜尋 * ：字首搜尋功能只會搜尋以目前資料夾相關特定字詞開頭的物件。搜尋不會包含其他地方包含該字詞的物件。此規則也適用於資料夾內的物件。例如、搜尋 `folder1/folder2/somefile-`會傳回資料夾內的物件 `folder1/folder2/`、並以字詞開頭 `somefile-`。
- * 拖放 * ：您可以將檔案從電腦的檔案管理員拖放到 S3 主控台。不過、您無法上傳資料夾。
- * 資料夾作業 * ：當您移動、複製或重新命名資料夾時、資料夾中的所有物件都會一次更新一個、可能需要一段時間。
- * 停用貯體版本設定時的永久刪除 * ：當您覆寫或刪除儲存區中停用版本設定的物件時、該作業是永久性的。請參閱。 "變更儲存區的物件版本設定"

管理S3平台服務

S3平台服務

了解 StorageGRID 的平台服務

在實作平台服務之前、請先檢閱使用這些服務的總覽和考量事項。

如需 S3 的相關資訊"使用S3 REST API"、請參閱。

平台服務總覽

StorageGRID 平台服務可讓您將 S3 物件和物件中繼資料的事件通知和複本傳送至外部目的地、協助您實作混合雲策略。

由於平台服務的目標位置通常是StorageGRID 不受您的支援、因此平台服務可讓您靈活運用外部儲存資源、通知服務、以及搜尋或分析資料服務。

您可以為單一 S3 儲存桶設定任意平台服務組合。例如，您可以在 StorageGRID S3 儲存桶上同時設定 "CloudMirror 服務" 和 "通知"，以便將特定物件鏡射到 Amazon Simple Storage Service (S3)，同時將每個此類

物件的通知傳送到第三方監控應用程式，協助您追蹤 AWS 費用。

每個租戶帳戶必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務的使用。

平台服務的設定方式

平台服務與您使用設定的外部端點進行通信"租戶管理程式"或"租戶管理API"。每個端點代表一個外部目標，例如StorageGRID S3 儲存桶、Amazon Web Services 儲存桶、Amazon SNS 主題、webhook 端點或在本地端、AWS 或其他地方託管的 Elasticsearch 叢集。

建立外部端點之後、您可以將 XML 組態新增至貯體、為某個貯體啟用平台服務。XML組態可識別儲存區應執行的物件、儲存區應採取的動作、以及儲存區應用於服務的端點。

您必須為每個要設定的平台服務新增個別的XML組態。例如：

- 如果您想要將金鑰開頭的所有物件 `/images`複寫到 Amazon S3 儲存區、則必須將複寫組態新增到來源儲存區。
- 如果您也想要在這些物件儲存至儲存區時傳送通知、則必須新增通知組態。
- 如果您要為這些物件的中繼資料建立索引、則必須新增中繼資料通知組態、以實作搜尋整合。

組態XML的格式受用於實作StorageGRID 支援功能的S3 REST API所規範：

平台服務	**S3 REST API**	請參閱
CloudMirror複寫	• GetBucketReplication • PutBucketReplication	• "CloudMirror複寫" • "在貯體上作業"
通知	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "通知" • "在貯體上作業"
搜尋整合	• 取得Bucket中繼資料通知組態 • 放置時段中繼資料通知組態	• "搜尋整合" • "StorageGRID 自訂作業"

使用平台服務的考量

考量	詳細資料
目的地端點監控	您必須監控每個目的地端點的可用度。如果連線到目的地端點的時間過長、而且有大量的要求待處理、那麼額外的用戶端要求StorageGRID （例如提出要求）將會失敗。當端點可連線時、您必須重試這些失敗的要求。

考量	詳細資料
目的地端點節流	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。
訂購保證	可保證站台內物件的作業順序。StorageGRID只要物件的所有作業都在同一個站台內、最終的物件狀態（用於複寫）就會永遠等於StorageGRID 該站台的狀態。 在整個景點進行作業時、盡力訂購申請。StorageGRID StorageGRID例如、如果您一開始將物件寫入站台A、然後在站台B覆寫相同的物件、則CloudMirror複寫到目的地儲存區的最終物件將無法保證為較新的物件。
ILM導向物件刪除	為了符合 AWS CRR 和 Amazon Simple Notification Service 的刪除行為、當來源儲存庫中的物件因 StorageGRID ILM 規則而遭到刪除時、 CloudMirror 和事件通知要求不會傳送。例如、如果ILM規則在14天後刪除物件、則不會傳送CloudMirror或事件通知要求。 相反地、因為ILM而刪除物件時、會傳送搜尋整合要求。
使用 Kafka 端點	Kafka 端點的驗證使用下列驗證類型。這些類型與用於驗證其他端點（例如 Amazon SNS ）的類型不同、需要使用者名稱和密碼認證。 • SLS/PLAIN • SLS/SCRAM-SHA-256 • SLS/SCRAM-SHA-512 • 注意： * 設定的儲存 Proxy 設定不適用於 Kafka 平台服務端點。

使用**CloudMirror**複寫服務的考量

考量	詳細資料
複寫狀態	StorageGRID 不支援 `x-amz-replication-status`標頭。
物件大小	CloudMirror複寫服務可複寫至目的地儲存區的物件大小上限為5 TiB、與最大_supported物件大小相同。 • 注意 * ：單一 PutObject 作業的最大建議大小為 5 GiB （ 5 、 368,709,120 位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

考量	詳細資料
儲存區版本管理和版本ID	如果StorageGRID 支援版本管理功能的來源S3儲存區、您也應該啟用目的地儲存區的版本管理功能。 使用版本控制時，請附註，由於 S3 協定的限制，目的地儲存桶中物件版本的順序是盡力而為的，CloudMirror 服務無法保證其完全一致。此外，目的地儲存桶會維護自身的設定，且可能不提供版本控制功能。 • 附註 * ： StorageGRID 中來源貯體的版本 ID 與目的地貯體的版本 ID 無關。
標記物件版本	由於 S3 傳輸協定的限制、 CloudMirror 服務不會複寫任何提供版本 ID 的 PuttObjectTaggingor DeleteObjectTaggings 要求。由於來源和目的地的版本識別碼不相關、因此無法確保將標記更新複寫到特定版本識別碼。 相反地、 CloudMirror 服務會複寫未指定版本 ID 的 PutObjectTaggings 或 DeleteObjectTaggings 要求。這些要求會更新最新金鑰的標記（如果儲存庫版本已有版本、則會更新最新版本）。也會複寫含有標記的一般擷取（非標記更新）。
多部分上傳和 `ETag`價值	鏡射使用多重上傳的物件時、CloudMirror服務不會保留這些部分。因此、 `ETag` 鏡射物件的值將與原始物件的值不同 `ETag`。
使用SSE-C加密的物件（使用客戶提供的金鑰進行伺服器端加密）	CloudMirror 服務不支援使用 SSE-C 加密的物件。如果您嘗試將物件擷取至 CloudMirror 複寫的來源貯體、而要求包含 SSE-C 要求標頭、則作業會失敗。
啟用S3物件鎖定的儲存區	如果 StorageGRID 中的來源 S3 儲存桶已啟用 S3 Object Lock，則也應為已設定預設保留的目的地儲存桶啟用 S3 Object Lock。 啟用 S3 Object Lock 後，來源桶和目的地桶均支援_物件資料_的複寫。但是，目的地桶會維護自身的物件保留設定，且可能無法提供法規遵循或版本控制。

了解 **StorageGRID CloudMirror** 複製服務

如果您想要 StorageGRID 將新增至儲存區的指定物件複寫至一或多個外部目的地儲存區、則可以為 S3 儲存區啟用 CloudMirror 複寫功能。

例如、您可以使用CloudMirror複寫將特定的客戶記錄鏡射到Amazon S3、然後利用AWS服務對資料執行分析。

CloudMirror 複寫僅在來源儲存桶已啟用 S3 物件鎖定且端點為 Amazon 或 StorageGRID S3 儲存桶時才受支援。物件鎖定設定不會複寫至儲存桶端點。

CloudMirror 和 ILM

CloudMirror 複寫作業不受網格的主動式 ILM 原則所影響。CloudMirror服務會在物件儲存到來源儲存區時複寫物件、並盡快將物件傳送到目的地儲存區。物件擷取成功時、會觸發複寫物件的交付。

CloudMirror 和跨網格複寫

CloudMirror 複寫與跨網格複寫功能有重要的相似之處和差異。請參閱 "比較跨網格複寫和 CloudMirror 複寫"。

CloudMirror 和 S3 儲存區

CloudMirror複寫通常設定為使用外部S3儲存區作為目的地。不過、您也可以將複寫設定為使用其他StorageGRID 的支援功能或任何S3相容服務。

現有的貯體

當您為現有儲存區啟用 CloudMirror 複寫時、只會複寫新增至該儲存區的新物件。貯體中的任何現有物件都不會複寫。若要強制複寫現有物件、您可以執行物件複本來更新現有物件的中繼資料。

> 如果您使用 CloudMirror 複寫功能將物件複製到 Amazon S3 目的地、請注意 Amazon S3 會將每個 Put 要求標頭內使用者定義的中繼資料大小限制在 2 KB 。如果物件的使用者定義中繼資料大於2 KB、則不會複寫該物件。

多個目的地貯體

若要將單一貯體中的物件複寫到多個目的地貯體、請在複寫組態 XML 中指定每個規則的目的地。您無法同時將物件複寫到多個儲存庫。

版本化或無版本化的貯體

您可以在版本控制或未版本控制的貯體上設定 CloudMirror 複寫。目的地貯體可以是版本化或非版本化的。您可以使用任何版本控制和未版本控制的儲存區組合。例如、您可以將版本控制的儲存區指定為未版本化來源儲存區的目的地、反之亦然。您也可以在未版本化的儲存區之間進行複寫。

刪除、複寫迴圈和事件

刪除行為

與 Amazon S3 服務跨區域複寫（ CRR ）的刪除行為相同。刪除來源貯體中的物件時、絕不會刪除目的地中的複寫物件。如果來源和目的地儲存區都有版本、則會複寫刪除標記。如果目的地貯體沒有版本化、則刪除來源貯體中的物件並不會將刪除標記複寫到目的地貯體、也不會刪除目的地物件。

防止複寫迴圈

當物件複寫到目的地儲存區時、 StorageGRID 會將其標示為「複本」。目的地 StorageGRID 貯體不會再次複寫標示為複本的物件、可保護您不受意外複寫迴圈的影響。此複本標記是 StorageGRID 內部的、並不會阻止您在使用 Amazon S3 儲存區作為目的地時使用 AWS CRR 。

> 用於標記複本的自訂標頭為 `x-ntap-sg-replica`。此標記可防止串聯鏡射。StorageGRID 確實支援兩個網格之間的雙向 CloudMirror 。

目的地貯體中的事件

目的地貯體中事件的獨特性和順序不受保證。為了保證交付成功、可能會將多個相同的來源物件複本傳送至目的地。在極少數情況下、當同一個物件同時從兩StorageGRID 個或更多不同的站台更新時、目的地庫位上的作業順序可能與來源庫位上的事件順序不符。

了解 StorageGRID 針對 S3 儲存區的事件通知

如果您希望StorageGRID將有關指定事件的通知傳送至目標 Kafka 叢集、webhook 端點或 Amazon Simple Notification Service，則可以為 S3 儲存桶啟用事件通知。

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。

事件通知會在通知組態中指定的來源儲存區建立、並傳送至目的地。如果與物件相關聯的事件成功、就會建立該事件的通知並排入傳送佇列。

無法保證通知的唯一性和順序。由於為了確保交付成功而採取的作業、可能會將多個事件通知傳送到目的地。由於交付方式非同步、因此無法保證目的地的通知時間順序與來源庫位事件的順序相符、尤其是來自不同StorageGRID 的站台的作業。您可以使用 `sequencer`事件訊息中的金鑰來判斷特定物件的事件順序、如Amazon S3 文件所述。

StorageGRID 事件通知會遵循 Amazon S3 API 、但有一些限制。

- 支援下列事件類型：
  - S3 ： ObjectCreated ：
  - S3 ： ObjectCreated ： Put
  - S3 ： ObjectCreated ： Post
  - S3 ： ObjectCreated ：複製
  - S3 ： ObjectCreated ： CompleteMultpartUpload
  - S3 ： ObjectRemoved ：
  - S3:ObjectRemoved ：刪除
  - S3 ： ObjectRemoved ：刪除 MarkerCreated
  - S3 ： ObjectRestore ： Post
- 從 StorageGRID 傳送的事件通知使用標準 JSON 格式、但不包含某些金鑰、也不為其他金鑰使用特定值、如下表所示：

金鑰名稱	價值**StorageGRID**
事件來源	`sgws:s3`
awsRegion	_ 不包括 _
X-amz-id-2	_ 不包括 _
不需要	`urn:sgws:s3:::bucket_name`

了解 **StorageGRID** 搜尋整合服務

如果您想要使用外部搜尋與資料分析服務來取得物件中繼資料、可以啟用S3儲存區的搜尋整合。

搜尋整合服務是一項自訂的 StorageGRID 服務、可在建立或刪除物件、或更新其中繼資料或標記時、自動且非同步地將 S3 物件中繼資料傳送至目的地端點。然後、您可以使用目的地服務所提供的精密搜尋、資料分析、視覺化或機器學習工具、來搜尋、分析物件資料、並從中獲得深入見解。

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。

雖然彈性搜尋整合功能可在啟用 S3 物件鎖定的儲存貯體上設定、但傳送至彈性搜尋的中繼資料中不會包含物件的 S3 物件鎖定中繼資料（包括「保留截止日期」和「合法保留」狀態）。

> 由於搜尋整合服務會將物件中繼資料傳送至目的地、因此其組態 XML 稱為「 *meta* 資料 _ 通知組態 *XML* 」。此組態 *XML* 與用於啟用 *_event* 通知的「通知組態 XML 」不同。

搜尋整合與 **S3** 儲存區

您可以針對任何版本控制或未版本控制的儲存區啟用搜尋整合服務。搜尋整合是透過將中繼資料通知組態XML與儲存區建立關聯來設定、此儲存區會指定要在哪些物件上執行動作、以及物件中繼資料的目的地。

中繼資料通知會以 JSON 文件的形式產生、名稱為貯體名稱、物件名稱和版本 ID （如果有）。每個中繼資料通知都包含物件的標準系統中繼資料集、以及物件的所有標記和使用者中繼資料。

> 針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

搜尋通知

在下列情況下、會產生中繼資料通知並排入佇列以供交付：

- 隨即建立物件。
- 刪除物件、包括因網格ILM原則運作而刪除物件的時間。
- 物件中繼資料或標記會新增、更新或刪除。一律會在更新時傳送完整的中繼資料和標記集、而不只是變更的值。

將中繼資料通知組態XML新增至儲存區之後、系統會針對您所建立的任何新物件、以及您透過更新其資料、使用者中繼資料或標記來修改的任何物件、傳送通知。然而、對於已在貯體中的任何物件、則不會傳送通知。若要確保儲存區中所有物件的物件中繼資料都會傳送到目的地、您應該執行下列其中一項：

- 在建立儲存區之後、以及新增任何物件之前、請立即設定搜尋整合服務。
- 對儲存庫中已有的所有物件執行動作、以觸發將中繼資料通知訊息傳送至目的地。

搜尋整合服務和彈性搜尋

支援以Elasticsearch叢集作為目的地的支援。StorageGRID如同其他平台服務、目的地是在端點中指定、而其URN則用於服務的組態XML中。使用 "NetApp 互通性對照表工具"來決定 Elasticsearch 支援的版本。

管理平台服務端點

在 **StorageGRID** 中設定平台服務端點

您必須先將至少一個端點設定為平台服務的目的地、才能為某個服務區段設定平台服務。

平台服務的存取是StorageGRID 由NetApp管理員以每個租戶為單位來啟用。若要建立或使用平台服務端點、您

必須是具有管理端點或根存取權限的租戶使用者、位於網路已設定為允許儲存節點存取外部端點資源的網格中。對於單一租戶、您最多可設定 500 個平台服務端點。如StorageGRID 需詳細資訊、請聯絡您的管理員。

什麼是平台服務端點？

平台服務端點會指定 StorageGRID 存取外部目的地所需的資訊。

例如、如果您想要將物件從 StorageGRID 儲存庫複寫到 Amazon S3 儲存區、您可以建立平台服務端點、其中包含 StorageGRID 存取 Amazon 上目的地儲存區所需的資訊和認證。

每種類型的平台服務都需要自己的端點、因此您必須為每個打算使用的平台服務至少設定一個端點。在定義平台服務端點之後、您可以在用來啟用服務的組態XML中、使用端點的URN作為目的地。

您可以將同一個端點作為多個來源儲存區的目的地。例如、您可以設定多個來源儲存區、將物件中繼資料傳送至同一個搜尋整合端點、以便在多個儲存區之間執行搜尋。您也可以將來源貯體設定為使用多個端點做為目標、讓您能夠執行像是將物件建立通知傳送至單一 Amazon Simple Notification Service （ Amazon SNS ） 主題、以及將物件刪除通知傳送至第二個 Amazon SNS 主題等作業。

用於**CloudMirror**複寫的端點

支援代表S3儲存區的複寫端點。StorageGRID這些儲存庫可能託管在Amazon Web Services、相同或遠端StorageGRID 的功能或其他服務上。

通知的端點

StorageGRID支援 Amazon SNS、Kafka 和 webhook 端點。不支援簡單佇列服務 (SQS) 和 AWS Lambda 端點。

搜尋整合服務的端點

支援代表Elasticsearch叢集的搜尋整合端點。StorageGRID這些彈性搜尋叢集可以位於本機資料中心、也可以存放在 AWS 雲端或其他地方。

搜尋整合端點是指特定的彈性搜尋索引和類型。您必須先在Elasticsearch中建立索引、才能在StorageGRID 其中建立端點、否則端點建立將會失敗。建立端點之前、您不需要建立類型。如果需要、當將物件中繼資料傳送至端點時、將會建立類型。StorageGRID

相關資訊

"管理StorageGRID"

為 **StorageGRID** 平台服務端點指定 **URN**

當您建立平台服務端點時、必須指定唯一的資源名稱（URN）。當您為平台服務建立組態 XML 時、您將使用 URN 來參考端點。每個端點的URN必須是唯一的。

當您建立平台服務端點時、此功能會驗證它們。StorageGRID在建立平台服務端點之前、請先確認端點中指定的資源是否存在、以及是否可以到達該端點。

urnElements

平台服務端點的 URN 必須以或 `urn:mysite`開頭 `arn:aws`、如下所示：

- 如果服務是在 Amazon Web Services （ AWS ）上代管、請使用 `arn:aws`
- 如果服務是在 Google Cloud Platform （ GCP ）上代管、請使用 `arn:aws`
- 如果服務是在本機代管、請使用 `urn:mysite`

例如、如果您要為 StorageGRID 上託管的 CloudMirror 端點指定 URN 、則 URN 可能會以開頭 `urn:sgws`。

URN的下一個元素會指定平台服務的類型、如下所示：

服務	類型
CloudMirror複寫	`s3`
通知	`sns`， `kafka` ， 或者 `webhook`
搜尋整合	`es`

例如、若要繼續指定 StorageGRID 上所託管之 CloudMirror 端點的 URN 、您可以新增 `s3`至 `GET `urn:sgws:s3`。

對於大多數端點來說，URN 的最後一個元素標識目標 URI 處的特定目標資源，例如， `sns-topic-name` 。

對於 webhook 端點，目標資源就是目標 URI 本身。

服務	特定資源
CloudMirror複寫	`bucket-name`
通知	`sns-topic-name`或 `kafka-topic-name` *注意：*對於 webhook 端點，URN 的最後一個元素可以是任何字串，只要端點的 URN 是唯一的。
搜尋整合	`domain-name/index-name/type-name` *注意：*如果Elasticsearch叢集*未*設定為自動建立索引、則必須在建立端點之前手動建立索引。

提供**AWS**和**GCP**上的服務

對於AWS和GCP實體而言、完整的URN是有效的AWS ARN。例如：

- CloudMirror複寫：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 搜尋整合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> 對於 AWS 搜尋整合端點、 `domain-name`必須包含文字字串 `domain/`、如下所示。

適用於本機代管服務

使用本機代管服務而非雲端服務時、只要URN在第三和最後的位置中包含必要的元素、您就可以以任何方式指定URN、以建立有效且獨特的URN。您可以將選用的元素保留空白、也可以以任何方式指定這些元素、協助您識別資源並使URN成為唯一的。例如：

- CloudMirror複寫：

```
urn:mysite:s3:::bucket-name
```

對於託管在 StorageGRID 上的 CloudMirror 端點、您可以指定以下列開頭的有效 URN `urn:sgws` ：

```
urn:sgws:s3:::bucket-name
```

- 通知：

指定 Amazon Simple Notification Service 端點：

```
urn:aws:sns:region:account-id:sns-topic-name
```

指定 Kafka 端點：

```
urn::kafka:::kafka-topic-name
```

> 您可以選擇性地在指定 Kafka 端點時包含 `mysite`： `urn:mysite:kafka:::kafka-topic-name`

指定 webhook 端點：

```
urn:mysite:webhook:::webhook-name
```

- 搜尋整合：

```
urn:mysite:es:::domain-name/index-name/type-name
```

> 對於本地託管的搜尋整合端點、 `domain-name`只要端點的 URN 是唯一的、元素就可以是任何字串。

建立 **StorageGRID** 平台服務端點

您必須至少建立一個正確類型的端點、才能啟用平台服務。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您屬於具有的使用者群組"管理端點或根存取權限"。
- 平台服務端點所引用的資源已建立：
  - CloudMirror複寫：S3儲存區
  - 事件通知：Amazon Simple Notification Service (Amazon SNS) 主題、Kafka 主題或 Webhook 終端節點
  - 搜尋通知：Elasticsearch 索引，如果目標群集未配置為自動建立索引。
- 您有關於目的地資源的資訊：
  - 統一資源識別元（URI）的主機和連接埠

    > 如果您計畫將裝載在StorageGRID 某個SnapMirror系統上的儲存庫當作CloudMirror複寫的端點、請聯絡網格管理員、以判斷您需要輸入的值。

  - 獨特資源名稱（URN）

    "指定平台服務端點的URN"

  - 驗證認證資料（若有需要）：

搜尋整合端點

對於搜尋整合端點、您可以使用下列認證：

- 存取金鑰：存取金鑰ID和秘密存取金鑰
- 基本HTTP：使用者名稱和密碼

CloudMirror 複寫端點

對於 CloudMirror 複寫端點、您可以使用下列認證：

- 存取金鑰：存取金鑰ID和秘密存取金鑰
- CAP（C2S存取入口網站）：暫用認證URL、伺服器與用戶端認證、用戶端金鑰、以及選用的用戶端私密金鑰複雜密碼。

Amazon SNS 端點

對於 Amazon SNS 端點、您可以使用下列認證：

- 存取金鑰：存取金鑰ID和秘密存取金鑰

Kafka 端點

對於 Kafka 端點、您可以使用下列認證：

- SLS/PLAIN ：使用者名稱和密碼
- SLS/SCRAM-SHA-256 ：使用者名稱和密碼
- SLS/SCRAM-SHA-512 ：使用者名稱和密碼

  - 安全性憑證（如果需要憑證驗證）

- 如果啟用彈性搜尋安全功能、您就擁有監控叢集權限來進行連線測試、以及寫入索引權限、或是索引和刪除文件更新的索引權限。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。「平台服務端點」頁面隨即出現。
2. 選取*建立端點*。
3. 輸入顯示名稱、簡短說明端點及其用途。

   當端點在「端點」頁面上列出時，端點支援的平台服務類型會顯示在端點名稱旁邊，因此您不需要在名稱中包含該資訊。

4. 在「* URI *」欄位中、指定端點的唯一資源識別元（URI）。

   請使用下列其中一種格式：

```
https://host:port
http://host:port
```

如果您未指定連接埠、則會使用下列預設連接埠：

- HTTPS URI 連接埠 443 、 HTTP URI 連接埠 80 （大多數端點）
- 連接埠 9092 適用於 HTTPS 和 HTTP URI （僅限 Kafka 端點）

例如StorageGRID 、裝載於列舉在整個基礎上的儲存區的URI可能是：

```
https://s3.example.com:10443
```

在此範例中 `s3.example.com`、代表 StorageGRID 高可用度（ HA ）群組虛擬 IP （ VIP ）的 DNS 項目、並 `10443`代表負載平衡器端點中定義的連接埠。

> 您應該盡可能連線到 HA 群組的負載平衡節點、以避免單點故障。

同樣地、AWS上裝載的儲存區URI可能是：

```
https://s3-aws-region.amazonaws.com
```

> 如果端點用於 CloudMirror 複寫服務、請勿在 URI 中包含貯體名稱。您可以在「* URN*」欄位中加入貯體名稱。

5. 輸入端點的唯一資源名稱（URN）。

> 建立端點後、您無法變更端點的 URN 。

6. 選擇*繼續*。
7. 選擇 * 驗證類型 * 的值。

> 如果您需要對 webhook 端點進行身份驗證，請在步驟9。

搜尋整合端點

輸入或上傳搜尋整合端點的認證。

您提供的認證必須具有目的地資源的寫入權限。

驗證類型	說明	認證資料
匿名	提供對目的地的匿名存取。僅適用於停用安全性的端點。	無驗證。
存取金鑰	使用AWS型認證來驗證與目的地的連線。	• 存取金鑰ID • 機密存取金鑰
基本HTTP	使用使用者名稱和密碼來驗證目的地的連線。	• 使用者名稱 • 密碼

CloudMirror 複寫端點

輸入或上傳 CloudMirror 複寫端點的認證。

您提供的認證必須具有目的地資源的寫入權限。

驗證類型	說明	認證資料
匿名	提供對目的地的匿名存取。僅適用於停用安全性的端點。	無驗證。
存取金鑰	使用AWS型認證來驗證與目的地的連線。	• 存取金鑰ID • 機密存取金鑰
CAP（C2S存取入口網站）	使用憑證和金鑰來驗證與目的地的連線。	• 暫用認證URL • 伺服器CA憑證（PEE檔案上傳） • 用戶端憑證（PEE檔案上傳） • 用戶端私密金鑰（上傳PEE檔案、OpenSSL加密格式或未加密的私密金鑰格式） • 用戶端私密金鑰複雜密碼（選用）

Amazon SNS 端點

輸入或上傳 Amazon SNS 端點的認證。

您提供的認證必須具有目的地資源的寫入權限。

驗證類型	說明	認證資料
匿名	提供對目的地的匿名存取。僅適用於停用安全性的端點。	無驗證。
存取金鑰	使用AWS型認證來驗證與目的地的連線。	• 存取金鑰ID • 機密存取金鑰

Kafka 端點

輸入或上傳 Kafka 端點的認證。

您提供的認證必須具有目的地資源的寫入權限。

驗證類型	說明	認證資料
匿名	提供對目的地的匿名存取。僅適用於停用安全性的端點。	無驗證。
SLS/PLAIN	使用含有純文字的使用者名稱和密碼來驗證目的地的連線。	• 使用者名稱 • 密碼
SLS/SCRAM-SHA-256	使用使用挑戰回應通訊協定和 SHA-256 雜湊的使用者名稱和密碼來驗證目的地的連線。	• 使用者名稱 • 密碼
SLS/SCRAM-SHA-512	使用使用挑戰回應通訊協定和 SHA-512 雜湊的使用者名稱和密碼來驗證目的地的連線。	• 使用者名稱 • 密碼

如果使用者名稱和密碼來自從 Kafka 叢集取得的委派權杖、請選取 * 使用委派驗證 * 。

8. 選擇*繼續*。
9. 選擇*驗證憑證*單選按鈕來選擇如何驗證與端點的 TLS 連線。

大多數端點

驗證搜尋整合、CloudMirror 複製、Amazon SNS 或 Kafka 端點的 TLS 連線。

憑證驗證類型	說明
TLS	驗證與端點資源的 TLS 連線的伺服器憑證。
已停用	證書驗證已停用。此選項不安全。
使用自訂CA憑證	自訂 CA 憑證用於在連接到端點時驗證伺服器的身份。
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。

Webhook 和 **Kafka** 端點

驗證 webhook 或 Kafka 端點的 TLS 連線。

憑證驗證類型	說明
TLS	驗證與端點資源的 TLS 連線的伺服器憑證。
移動TLS	驗證與端點資源的相互 TLS 連線的用戶端和伺服器憑證。
已停用	證書驗證已停用。此選項不安全。
使用自訂CA憑證	自訂 CA 憑證用於在連接到端點時驗證伺服器的身份。
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。 附註：Webhook 端點沒有此選項。

當您選擇 **mTLS** 時，這些選項會變成可用。

憑證驗證類型	說明
不驗證伺服器憑證	禁用伺服器憑證驗證，這表示伺服器的身份未經驗證。此選項不安全。
用戶端憑證	客戶端憑證用於在連接到端點時驗證客戶端的身份。
客戶端私鑰	客戶端憑證的私鑰。如果加密，則必須使用傳統格式 PKCS #1（不支援 PKCS #8 格式）。
客戶端私鑰密碼	用於解密客戶端私鑰的密碼。如果私鑰未加密，請將此處留空。

10. 選擇*測試並建立端點*。
    - 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點驗證。
    - 當端點驗證失敗時、會出現錯誤訊息。如果您需要修改端點以修正錯誤、請選取*返回端點詳細資料*並更新資訊。然後選取*測試並建立端點*。

> 如果您的租戶帳戶未啟用平台服務、端點建立將會失敗。請聯絡StorageGRID 您的系統管理員。

設定端點之後、您可以使用其URN來設定平台服務。

相關資訊

- "指定平台服務端點的URN"
- "設定CloudMirror複寫"
- "設定事件通知"
- "設定搜尋整合服務"
- "用於外部通訊的連接埠"

測試 **StorageGRID** 平台服務端點的連線

如果平台服務的連線已變更、您可以測試端點的連線、以驗證目的地資源是否存在、以及是否可以使用您指定的認證來連線。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理端點或根存取權限"。

關於這項工作

無法驗證認證資料是否擁有正確的權限。StorageGRID

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。

2. 選取您要測試其連線的端點。

   端點詳細資料頁面隨即出現。

3. 選擇*測試連線*。
    - 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點驗證。
    - 當端點驗證失敗時、會出現錯誤訊息。如果您需要修改端點以修正錯誤、請選取*組態*並更新資訊。然後選取*測試並儲存變更*。

在 **StorageGRID** 中編輯平台服務端點

您可以編輯平台服務端點的組態、以變更其名稱、URI或其他詳細資料。例如、您可能需要更新過期的認證資料、或是變更URI以指向備份Elasticsearch索引以進行容錯移轉。您無法變更平台服務端點的 URN 。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理端點或根存取權限"。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。

2. 選取您要編輯的端點。

   端點詳細資料頁面隨即出現。

3. 選擇*組態*。
4. 視需要變更端點的組態。

   建立端點後、您無法變更端點的 URN 。

   a. 若要變更端點的顯示名稱，請選擇編輯圖示 。
   b. 視需要變更URI。
   c. 視需要變更驗證類型。
      - 若要進行存取金鑰驗證、請視需要變更金鑰、方法是選取*編輯S3金鑰*、然後貼上新的存取金鑰ID和秘密存取金鑰。如果您需要取消變更、請選取*恢復S3金鑰編輯*。
      - 若要進行CAP（C2S存取入口網站）驗證、請變更暫用認證URL或選用的用戶端私密金鑰通關密碼、並視需要上傳新的憑證和金鑰檔案。

        用戶端私密金鑰必須為OpenSSL加密格式或未加密的私密金鑰格式。

   d. 根據需要，變更驗證證書的方法。
5. 選擇*測試並儲存變更*。
   - 如果可以使用指定的認證資料來連線至端點、則會出現一則成功訊息。端點的連線會從每個站台的一個節點進行驗證。
   - 當端點驗證失敗時、會出現錯誤訊息。修改端點以修正錯誤、然後選取*測試並儲存變更*。

刪除 **StorageGRID** 平台服務端點

如果您不想再使用相關的平台服務、可以刪除端點。

開始之前

- 您可以使用登入租戶管理程式"支援的網頁瀏覽器"。
- 您屬於具有的使用者群組"管理端點或根存取權限"。

步驟

1. 選擇*儲存設備（S3）>*平台服務端點。

   「平台服務端點」頁面隨即出現、並顯示已設定的平台服務端點清單。

2. 選取您要刪除的每個端點的核取方塊。

   如果您刪除使用中的平台服務端點、則使用端點的任何貯體都會停用相關的平台服務。任何尚未完成的要求都會被捨棄。在您將庫位組態變更為不再參照已刪除的URN之前、將會繼續產生任何新的要求。將這些要求報告為不可恢復的錯誤。StorageGRID

3. 選取*「動作*」>*「刪除端點*」。

   隨即顯示確認訊息。

4. 選擇*刪除端點*。

疑難排解 **StorageGRID** 平台服務端點錯誤

如果 StorageGRID 嘗試與平台服務端點通訊時發生錯誤、儀表板上會顯示訊息。在「Platform Services Endives」（平台服務端點）頁面上、最後一個錯誤欄位會指出錯誤發生的時間已過多久。如果端點認證的相關權限不正確、則不會顯示錯誤。

判斷是否發生錯誤

如果過去 7 天內發生任何平台服務端點錯誤、租戶管理器儀表板會顯示警示訊息。您可以移至「平台服務端點」頁面、查看錯誤的詳細資料。

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.

儀表板上出現的相同錯誤也會出現在「平台服務端點」頁面頂端。若要檢視更詳細的錯誤訊息：

步驟

1. 從端點清單中、選取有錯誤的端點。
2. 在端點詳細資料頁面上，選擇 **Connection**。此標籤僅顯示端點的最新錯誤，並指示錯誤發生的時間。帶有紅色 X 圖示的錯誤 表示過去 7 天內發生的錯誤。

檢查錯誤是否仍為最新狀態

有些錯誤可能會繼續顯示在「最後一個錯誤」欄中、即使這些錯誤已解決。若要查看錯誤是否為目前錯誤、或強制從表格中移除已解決的錯誤：

步驟

1. 選取端點。

   端點詳細資料頁面隨即出現。

2. 選擇*連線*>*測試連線*。

選擇*測試連線*會使StorageGRID Sexing驗證平台服務端點是否存在、以及是否能以目前的認證資料來連線。端點的連線會從每個站台的一個節點驗證。

解決端點錯誤

您可以使用端點詳細資料頁面上的*上次錯誤*訊息來協助判斷造成錯誤的原因。有些錯誤可能需要您編輯端點才能解決問題。例如StorageGRID 、如果由於沒有正確的存取權限或存取金鑰已過期、所以無法存取目的地S3儲存區、就會發生CloudMirroring錯誤。訊息為「需要更新端點認證或目的地存取」、詳細資料為「 AccessDenied 」或「 InvalidAccessKeyId 」。

如果您需要編輯端點來解決錯誤、請選取*測試並儲存變更*、以StorageGRID 驗證更新的端點、並確認可以使用目前的認證來達到該端點。端點的連線會從每個站台的一個節點驗證。

步驟

1. 選取端點。
2. 在端點詳細資料頁面上、選取*組態*。
3. 視需要編輯端點組態。
4. 選擇*連線*>*測試連線*。

權限不足的端點認證

當驗證平台服務端點時、會確認端點的認證資料可用於聯絡目的地資源、並執行基本權限檢查。StorageGRID不過StorageGRID 、不驗證特定平台服務作業所需的所有權限。因此、如果您在嘗試使用平台服務時收到錯誤訊息（例如「 403 禁止」）、請檢查與端點認證相關的權限。

相關資訊

- 管理 **StorageGRID** › 疑難排解平台服務
- "建立平台服務端點"
- "測試平台服務端點的連線"
- "編輯平台服務端點"

在 **StorageGRID** 中設定 **CloudMirror** 複寫

若要為某個貯體啟用 CloudMirror 複寫、您需要建立並套用有效的貯體複寫組態 XML 。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已建立一個儲存區作為複寫來源。
- 您打算用作 CloudMirror 複寫目的地的端點已經存在、而且您有它的 URN 。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區

時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

CloudMirror複寫會將物件從來源儲存區複製到端點中指定的目的地儲存區。

有關貯體複寫及如何設定的一般資訊，請參閱 "Amazon Simple Storage Service （ S3 ）文件：複寫物件"。如需 StorageGRID 如何實作 GetBucketReplication 、 DeleteBucketReplication 和 PuttBucketReplication 的相關資訊，請參閱"在貯體上作業"。

> CloudMirror 複寫與跨網格複寫功能有重要的相似之處和差異。若要深入瞭解"比較跨網格複寫和 CloudMirror 複寫"、請參閱。

設定 CloudMirror 複寫時、請注意下列需求和特性：

- 當您建立並套用有效的貯體複寫組態 XML 時、它必須為每個目的地使用 S3 貯體端點的 URN 。
- 只有當來源桶或目的地桶啟用了 S3 物件鎖定功能時，才支援 Amazon S3 或 StorageGRID S3 儲存桶的複寫。物件鎖定標頭不會複寫到目的地物件。
- 如果您在包含物件的貯體上啟用 CloudMirror 複寫、則會複寫新增至該貯體的物件、但不會複寫該貯體中的現有物件。您必須更新現有物件、才能觸發複寫。
- 如果在設定 CloudMirror 複寫之後對目的地儲存桶啟用 S3 Object Lock，則可能需要"重新儲存端點"以允許複寫繼續。
- 如果您在複寫組態XML中指定儲存類別、StorageGRID 則當針對目的地S3端點執行作業時、會使用該類別。目的地端點也必須支援指定的儲存類別。請務必遵循目的地系統廠商所提供的任何建議。

步驟

1. 啟用來源儲存區的複寫：
   - 使用文字編輯器建立所需的複寫組態XML、以啟用S3複寫API中指定的複寫。
   - 設定XML時：
     - 請注意StorageGRID 、僅支援V1複寫組態。這表示 StorageGRID 不支援將元素用於規則、也不支援 `Filter`刪除物件版本的 V1 慣例。如需詳細資訊、請參閱Amazon複寫組態文件。
     - 使用S3貯體端點的URN作為目的地。
     - 選擇性地新增 `<StorageClass>`元素、並指定下列其中一項：
       - `STANDARD`：預設儲存類別。如果上傳物件時未指定儲存類別、則會使用儲存類別 `STANDARD`。
       - `STANDARD_IA`：（標準 - 不常存取。）使用此儲存類別來存取較不頻繁的資料、但仍需要在需要時快速存取。
       - `REDUCED_REDUNDANCY`：使用此儲存類別來儲存非關鍵且可重現的資料、其備援性比儲存類別低 `STANDARD`。
     - 如果您在組態 XML 中指定 `Role`、則會忽略。此值不供StorageGRID 下列項目使用：

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 從儀表板選取 * 檢視貯體 * 、或選取 * 儲存空間（ S3 ） * > * 鏟斗 * 。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*複寫*。
5. 選中 * 啓用複製 * 複選框。
6. 將複寫組態XML貼到文字方塊中、然後選取*儲存變更*。

   每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認複寫設定正確：
   a. 將符合複寫組態中所指定之複寫需求的物件新增至來源儲存區。

      在前面所示的範例中、會複寫符合前置字元「 2020 」的物件。

   b. 確認物件已複寫至目的地儲存區。

      對於小型物件、複寫作業很快就會完成。

相關資訊

"建立平台服務端點"

在 **StorageGRID** 中設定事件通知

您可以建立通知組態 XML 、並使用 Tenant Manager 將 XML 套用至貯體、以啟用貯體的通知。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已建立一個儲存庫做為通知來源。

- 您打算用作事件通知目的地的端點已經存在、而且您擁有它的 URN 。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

您可以將通知配置 XML 與來源儲存桶關聯來設定事件通知。通知配置 XML 遵循 S3 約定來配置儲存桶通知，並將目標 Amazon SNS 主題、Kafka 主題或 webhook 端點指定為端點的 URN。

如需事件通知及如何設定的一般資訊，請參閱 "Amazon 文件"。如需 StorageGRID 如何實作 S3 儲存區通知組態 API 的相關資訊"實作S3用戶端應用程式的指示"、請參閱。

為貯體設定事件通知時、請注意下列需求和特性：

- 當您建立並套用有效的通知組態 XML 時、它必須針對每個目的地使用事件通知端點的 URN 。
- 雖然可以在啟用 S3 物件鎖定的儲存貯體上設定事件通知、但通知訊息中不會包含物件的 S3 物件鎖定中繼資料（包括保留截止日期和合法保留狀態）。
- 配置事件通知後，每當來源儲存桶中的物件發生指定事件時，都會產生通知並將其傳送至用作目標的 Amazon SNS 主題、Kafka 主題或 webhook 終端節點。
- 如果您為包含物件的儲存區啟用事件通知、則通知僅會針對儲存通知組態後所執行的動作傳送。

步驟

1. 啟用來源儲存區的通知：
   - 使用文字編輯器建立啟用事件通知所需的通知組態XML、如S3通知API所指定。
   - 設定XML時、請使用事件通知端點的URN作為目的地主題。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 在租戶管理程式中、選取*儲存設備（S3）>*桶。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*事件通知*。
5. 選中 * 啓用事件通知 * 複選框。
6. 將通知組態XML貼到文字方塊中、然後選取*儲存變更*。

> 每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Grid Management API的管理員啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認事件通知設定正確：
   a. 對來源儲存區中符合觸發通知要求的物件執行動作、如組態XML中所設定。

      在範例中、每當使用前置碼建立物件時、就會傳送事件通知 `images/`。

   b. 確認通知已傳送至目標 Amazon SNS 主題、Kafka 主題或 webhook 終端節點。

      例如、如果您的目的地主題是在 Amazon SNS 上代管、您可以設定服務、以便在傳送通知時傳送電子郵件給您。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+
如果在目的地主題收到通知、表示您已成功設定來源庫位以供StorageGRID 發出資訊通知。

相關資訊

- "瞭解庫存箱通知"
- "使用S3 REST API"
- "建立平台服務端點"

在 **StorageGRID** 中設定搜尋整合服務

您可以建立搜尋整合 XML 、並使用 Tenant Manager 將 XML 套用至貯體、以啟用貯體的搜尋整合。

開始之前

- StorageGRID 管理員已為您的租戶帳戶啟用平台服務。
- 您已經建立了要索引其內容的 S3 儲存貯體。
- 您打算用作搜尋整合服務目的地的端點已經存在、而且您有其 URN 。
- 您屬於具有的使用者群組"管理所有貯體或根目錄存取權限"。這些權限會在使用租戶管理程式設定儲存區時、覆寫群組或儲存區原則中的權限設定。

關於這項工作

在您設定來源儲存區的搜尋整合服務之後、建立物件或更新物件的中繼資料或標記、會觸發物件中繼資料傳送到目的地端點。

如果您為已包含物件的貯體啟用搜尋整合服務、則不會自動傳送現有物件的中繼資料通知。更新這些現有物件、確保其中繼資料已新增至目的地搜尋索引。

步驟

1. 啟用貯體的搜尋整合：
   - 使用文字編輯器建立啟用搜尋整合所需的中繼資料通知XML。
   - 設定XML時、請使用搜尋整合端點的URN作為目的地。

     物件可依物件名稱的前置詞進行篩選。例如、您可以將具有前置詞的物件中繼資料傳送至一個目的地、並將具有前置詞的物件中繼資料傳送 `images`至另一個目的地 `videos`。有重疊前置字元的組態無效、提交時會遭到拒絕。例如、不允許針對具有前置字元的物件、包含一條規則的組態 `test`、以及針對具有前置字元的物件的第二條規則 `test2`。

     如有需要中繼資料組態 XML 的範例、請參閱。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

     中繼資料通知組態 XML 中的元素：

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的

名稱	說明	必要
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es`必須是第三個元素。 • URN 必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

2. 在租戶管理程式中、選取*儲存設備（S3）>*桶。
3. 選取來源儲存區的名稱。

   此時會顯示「庫位詳細資料」頁面。

4. 選擇*平台服務*>*搜尋整合*
5. 選中 * 啓用搜索集成 * 複選框。
6. 將中繼資料通知組態貼到文字方塊中、然後選取*儲存變更*。

   每個租戶帳戶都必須由StorageGRID 使用Grid Manager或Management API的管理員為其啟用平台服務。如果您儲存組態XML時發生錯誤、請聯絡StorageGRID 您的管理員。

7. 確認搜尋整合服務的設定正確：
   a. 將符合觸發組態XML中指定中繼資料通知要求的物件新增至來源儲存區。

      在先前所示的範例中、新增至儲存區的所有物件都會觸發中繼資料通知。

   b. 確認包含物件中繼資料和標記的Json文件已新增至端點中指定的搜尋索引。

完成後

如有必要、您可以使用下列任一方法來停用儲存區的搜尋整合：

- 選取 * 儲存（ S3 ） * > * 儲存容量 * 、然後清除 * 啟用搜尋整合 * 核取方塊。
- 如果您直接使用S3 API、請使用刪除時段中繼資料通知要求。請參閱實作S3用戶端應用程式的指示。

範例：適用於所有物件的中繼資料通知組態

在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

範例：中繼資料通知組態有兩個規則

在此範例中、符合前置碼之物件的物件中繼資料 `/images`會傳送至一個目的地、而符合前置碼之物件的物件中繼資料 `/videos`則會傳送至第二個目的地。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

中繼資料通知格式

當您啟用儲存區的搜尋整合服務時、每次新增、更新或刪除物件中繼資料或標記時、都會產生Json文件並傳送至目的地端點。

此範例顯示在名為的儲存格中建立 `test`具有金鑰的物件時、可能會產生的 `JSON` 範例 `SGWS/Tagging.txt`。 `test`貯體未版本化、因此 `versionId`標記為空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

JSON 文件中包含的欄位

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

儲存區和物件資訊

`bucket`：貯體名稱

`key`：物件金鑰名稱

`versionID`：對象版本，用於版本控制桶中的對象

`region`例如：鏟斗區域 `us-east-1`

系統中繼資料

`size`： HTTP 客戶端可見的對象大小（以字節爲單位）

`md5`：物件雜湊

使用者中繼資料

`metadata`：對象的所有用戶元數據，作爲鍵值對

`key:value`

標記

`tags`：爲對象定義的所有對象標記，作爲鍵值對

`key:value`

如何在彈性搜尋中檢視結果

針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。設定搜尋整合服務之前、請先啟用索引上的動態欄位對應。建立文件索引後、您就無法編輯索引中文件的欄位類型。

使用S3 REST API

StorageGRID S3 REST API 支援的版本和更新

支援簡單儲存服務（S3）API、此API是以代表狀態傳輸（REST）網路服務的形式實作。StorageGRID

S3 REST API 的支援可讓您將專為 S3 Web 服務開發的服務導向應用程式、與使用 StorageGRID 系統的內部部署物件儲存設備連線。用戶端應用程式目前使用 S3 REST API 呼叫的變更最少。

支援的版本

StorageGRID支援以下特定版本的 STS、S3 和 HTTP：

項目	版本
STS AssumeRole API 規範	"Amazon Web Services (AWS) 文件：Amazon Assumerole API 參考" 有關 AssumeRole 的更多信息，請參閱"設定 AssumeRole"。
S3 API 規格	"AWS 文件：Amazon Simple Storage Service API 參考"
HTTP	1.1 如需HTTP的詳細資訊、請參閱HTTP / 1.1（RFC 7230-35）。 "IETF RFC 2616：超文字傳輸傳輸協定（HTTP / 1.1）" 附註 StorageGRID ：不支援HTTP / 1.1鋪管。

S3 REST API 支援的更新

版本	註解
12.1.0	• `If-Match` The `If-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。 • `If-None-Match` The `If-None-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-None-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。 • 為以下請求和支援的標頭新增了對預先計算 Checksum 值的支援： ◦ CompleteMultipartUpload： `x-amz-checksum-crc32`， `x-amz-checksum-crc32c`，和 `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload： `CRC32`， `CRC32C`，以及 `CRC64NVME`，適用於 `x-amz-checksum-algorithm` ◦ CopyObject： `CRC32`， `CRC32C`， `CRC64NVME`，以及 `SHA256`（適用於 `x-amz-checksum-algorithm`） ◦ PutObject： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ UploadPart： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` • 新增了對 `x-amz-checksum-type` 的支援，適用於 CreateMultipartUpload 和 CompleteMultipartUpload。 • 增加了對 `s3:x-amz-copy-source`原則條件索引鍵的支援。 • 允許在現有儲存桶上啟用 S3 物件鎖定。
12.0	• 增加了對管理介面的跨域資源共用 (CORS) 支持，允許另一個網域使用管理 API 存取StorageGRID中的資料。"深入瞭解" 。 • 新增對 STS AssumeRole 和工作階段原則的支援。請參閱 "會話策略範例"。您可以在租戶群組下設定 AssumeRole。

版本	註解
11.9	• 新增下列要求和支援標頭的預先計算 SHA-256 檢查值支援。您可以使用此功能來驗證上傳物件的完整性： ◦ CompleteMultpartUpload ： `x-amz-checksum-sha256` ◦ CreateMultpartUpload ： `x-amz-checksum-algorithm` ◦ GetObject ： `x-amz-checksum-mode` ◦ 標題物件： `x-amz-checksum-mode` ◦ 清單零件 ◦ PutObject ： `x-amz-checksum-sha256` ◦ 上傳部分： `x-amz-checksum-sha256` • 新增網格管理員控制租戶層級保留和法規遵循設定的功能。這些設定會影響 S3 物件鎖定設定。 ◦ 貯體預設保留模式和物件保留模式：監管或法規遵循（如果網格管理員允許）。 ◦ 貯體預設保留期間和物件保留截止日期：必須小於或等於網格管理員所設定的保留期間上限所允許的值。 • 改善內容編碼與串流 `x-amz-content-sha256`值的支援 `aws-chunked`。限制： ◦ 如果存在、 `chunk-signature`則為選用且未驗證 ◦ 如果存在、 `x-amz-trailer`內容會被忽略
11.8	更新 S3 作業的名稱，以符合中使用的名稱 "Amazon Web Services（AWS）文件：Amazon Simple Storage Service API Reference"。
11.7	• 已新增"快速參考：支援的 S3 API 要求"。 • 新增對使用 S3 物件鎖定的治理模式的支援。 • 新增「取得物件」和「標頭物件」要求的 StorageGRID 特定回應標頭支援 `x-ntap-sg-cgr-replication-status`。此標頭提供物件的跨網格複寫狀態。 • SelectObjectContent 要求現在支援 Parquet 物件。
11.6	• 新增支援、可在「取得物件」和「標題物件要求」中使用 `partNumber`要求參數。 • 新增S3物件鎖定的預設保留模式支援、以及儲存區層級的預設保留期間。 • 新增對原則條件金鑰的支援 `s3:object-lock-remaining-retention-days`、可設定物件的允許保留期間範圍。 • 將單一「放置物件」作業的最大大小 _ 建議 _ 變更為 5 GiB （ 5 、 368,709,120 位元組）。如果您的物件大於5 GiB、請改用多部份上傳。

版本	註解
11.5	• 新增對管理儲存區加密的支援。 • 新增了對S3物件鎖定和過時舊版規範要求的支援。 • 新增使用刪除版本型儲存區上的多個物件的支援。 • `Content-MD5`現在已正確支援要求標頭。
11.4.11.4	• 新增刪除庫位標記、取得庫位標記及置入庫位標記的支援。不支援成本分攤標記。 • 對於StorageGRID 在VMware 11.4中建立的儲存區、不再需要限制物件金鑰名稱以符合效能最佳實務做法。 • 新增對活動類型的儲存庫通知的支援 `s3:ObjectRestore:Post`。 • 現在已強制多部分零件的AWS大小限制。多部分上傳中的每個部分必須介於5個mib和5 GiB之間。最後一個部分可能小於5個mib。 • 新增 TLS 1.3 支援
11.3	• 新增支援使用客戶提供的金鑰（SSE-C）進行物件資料的伺服器端加密。 • 新增刪除、取得及放置 Bucket 生命週期作業（僅限到期動作）及回應標頭的支援 `x-amz-expiration`。 • 更新的「放置物件」、「放置物件」-「複製」和「多重成分上傳」、說明ILM規則在擷取時使用同步放置的影響。 • 不再支援TLS 1.1密碼。
11.2	新增後物件還原支援、可搭配雲端儲存資源池使用。新增了使用AWS語法的支援、可用於ARN、原則條件金鑰、以及群組和儲存區原則中的原則變數。我們StorageGRID 將繼續支援使用此功能的現有群組和儲存區原則。 *附註：*在其他組態JSON/XML中使用ARN/URN StorageGRID （包括用於自訂的版本功能）並未變更。
11.1	新增支援跨來源資源共享（ CORS ）、 HTTP for S3 用戶端連線至網格節點、以及儲存區的法規遵循設定。
11.0	新增支援、可設定適用於儲存區的平台服務（CloudMirror複寫、通知及Elasticsearch整合）。此外、也新增對貯體物件標記位置限制的支援、以及可用的一致性。
10.4	新增對ILM掃描版本設定、端點網域名稱頁面更新、原則、原則範例及PuttoverwriteObject權限中的條件和變數的支援。
10.3	新增版本管理支援。
10.2	新增對群組和庫位存取原則的支援、以及多部份複本（上傳零件-複本）的支援。

版本	註解
10.1	新增對多部分上傳、虛擬主機式請求和 v4 驗證的支援。
10.0	StorageGRID系統初步支援 S3 REST API。 _簡單儲存服務 API 參考_目前支援的版本是 2006-03-01。

StorageGRID 中支援的 S3 API 要求

本頁概述 StorageGRID 如何支援 Amazon Simple Storage Service （ S3 ） API 。

本頁僅包含 StorageGRID 支援的 S3 操作。任何未列出的 S3 操作都可能傳回 `501 Not Implemented`或導致意外行為。

若要查看每項作業的 AWS 文件、請選取標題中的連結。

通用 **URI** 查詢參數和要求標頭

除非另有說明、否則支援下列常見的 URI 查詢參數：

- `versionId`（視物件作業需求而定）

除非另有說明、否則支援下列常見的要求標頭：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

相關資訊

- "S3 REST API 實作詳細資料"
- "Amazon Simple Storage Service API 參考：一般要求標頭"

"AbortMultiPart上 傳"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的全部通用參數和標頭功能、加上此額外的 URI 查詢參數：

- `uploadId`

申請本文

無

本文檔**StorageGRID**

"多部份上傳作業"

"完成多個部分上傳"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的全部通用參數和標頭功能、加上此額外的 URI 查詢參數：

- `uploadId`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-checksum-type`
- `x-amz-storage-class`

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `ChecksumCRC32`
- `ChecksumCRC32C`
- `ChecksumCRC64NVME`
- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

本文檔**StorageGRID**

"完成多個部分上傳"

"CopyObject"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外標頭：

- `x-amz-checksum-algorithm`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`

- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

申請本文

無

本文檔**StorageGRID**

"CopyObject"

"建立庫位"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外標頭：

- `x-amz-bucket-object-lock-enabled`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"建立多個部分上傳"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-checksum-type`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

申請本文

無

本文檔**StorageGRID**

"建立多個部分上傳"

"刪除**Bucket**"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

本文檔**StorageGRID**

"在貯體上作業"

"刪除 **BucketCors**"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"刪除 BucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"刪除 BucketLifecycle"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

- "在貯體上作業"
- "建立S3生命週期組態"

"刪除BucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"刪除 BucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"刪除 Bucketagging"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"刪除物件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

無

本文檔StorageGRID

"物件上的作業"

"刪除物件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及此額外的要求標頭：

- `x-amz-bypass-governance-retention`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔StorageGRID

"物件上的作業"

"刪除ObjectTagging"

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔StorageGRID

"物件上的作業"

"GetBucketAcl"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

- "在貯體上作業"
- "建立S3生命週期組態"

"GetBucketLocation"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"GetObject"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列其他 URI 查詢參數：

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

以及這些額外的要求標頭：

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

申請本文

無

本文檔**StorageGRID**

"GetObject"

"GetObjectAcl"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"GetObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"GetObjectTagging"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"物件上的作業"

"標題庫"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"標題物件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外標頭：

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

申請本文

無

本文檔**StorageGRID**

"標題物件"

"列表桶"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

無

本文檔**StorageGRID**

服務 › **ListB**桶 的操作

"ListMultipartUploads"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外參數：

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

申請本文

無

本文檔**StorageGRID**

"ListMultipartUploads"

"清單物件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外參數：

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

申請本文

無

本文檔**StorageGRID**

"在貯體上作業"

"清單對象V2."

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外參數：

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"ListObjectVerions"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外參數：

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

申請本文

無

本文檔StorageGRID

"在貯體上作業"

"清單零件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外參數：

- max-parts

- `part-number-marker`
- `uploadId`

申請本文

無

本文檔**StorageGRID**

"ListMultipartUploads"

"PuttBucketCors"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketEncryption"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketLifecycleConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- `And`
- `Days`

- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

本文檔**StorageGRID**

- "在貯體上作業"
- "建立S3生命週期組態"

"PutBucketNotificationConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

要求內文 **XML** 標記

StorageGRID 支援這些要求本文 XML 標記：

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration

- `Value`

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketPolicy"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

有關支援的 JSON 主體欄位的詳細信息，請參閱"使用貯體和群組存取原則"。

"PutBucketReplication"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

要求內文 **XML** 標記

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketTagging"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"在貯體上作業"

"PuttBucketVersion"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

要求主體參數

StorageGRID 支援下列要求主體參數：

- `VersioningConfiguration`
- `Status`

本文檔**StorageGRID**

"在貯體上作業"

"PuttObject"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列額外標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

申請本文

- 物件的二進位資料

本文檔**StorageGRID**

"PuttObject"

"PutObjectLegalHold"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectLockConfiguration"

URI 查詢參數和要求標頭

StorageGRID 支援此請求的 大多數 通用參數和標頭。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時定義的_大多數_請求本文參數，但下列情況除外：

除非您的網格系統管理員已授予權限，否則您無法使用 PutObjectLockConfiguration 在現有儲存桶上啟用 S3 物件鎖定。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PutObjectRetention"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、加上此額外標頭：

- `x-amz-bypass-governance-retention`

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"使用 S3 REST API 來設定 S3 物件鎖定"

"PuttObjectTagging"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

StorageGRID 支援 Amazon S3 REST API 在實作時所定義的所有要求主體參數。

本文檔**StorageGRID**

"物件上的作業"

"RestoreObject"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

如需有關支援的實體欄位的詳細資訊"RestoreObject"、請參閱。

"選取物件內容"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能。

申請本文

如需受支援實體欄位的詳細資訊、請參閱下列內容：

- "使用S3 Select"
- "選取物件內容"

"上傳零件"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列其他 URI 查詢參數：

- `partNumber`
- `uploadId`

以及這些額外的要求標頭：

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

申請本文

- 零件的二進位資料

本文檔**StorageGRID**

"上傳零件"

"上傳PartCopy"

URI 查詢參數和要求標頭

StorageGRID 支援此要求的所有通用參數和標頭功能、以及下列其他 URI 查詢參數：

- `partNumber`
- `uploadId`

以及這些額外的要求標頭：

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

申請本文

無

本文檔**StorageGRID**

"上傳PartCopy"

測試 **StorageGRID S3 REST API** 組態

您可以使用 Amazon Web Services 命令列介面（ AWS CLI ）來測試與系統的連線、並驗證您是否可以讀寫物件。

開始之前

- 您已從下載並安裝 AWS CLI "aws.amazon.com/cli" 。
- 您也可以選擇"已建立負載平衡器端點"使用。否則、您就知道要連線的儲存節點 IP 位址、以及要使用的連接埠號碼。請參閱。 "用戶端連線的 IP 位址和連接埠"
- 您有 "已建立 S3 租戶帳戶"。
- 您已登入租戶和"已建立存取金鑰"。

如需這些步驟的詳細"設定用戶端連線"資訊，請參閱。

步驟

1. 設定 AWS CLI 設定以使用您在 StorageGRID 系統中建立的帳戶：
   a. 進入組態模式： `aws configure`
   b. 輸入您所建立帳戶的存取金鑰 ID 。
   c. 輸入您所建立帳戶的秘密存取金鑰。
   d. 輸入要使用的預設區域。例如 `us-east-1` ：。
   e. 輸入要使用的預設輸出格式、或按* Enter *選取Json。
2. 建立儲存庫。

   本範例假設您已將負載平衡器端點設定為使用 IP 位址 10.96.101.17 和連接埠 10443 。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   如果成功建立了儲存區、則會傳回儲存區的位置、如下列範例所示：

   ```
   "Location": "/testbucket"
   ```

3. 上傳物件。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   如果物件上傳成功、則會傳回Etag、這是物件資料的雜湊。

4. 列出儲存區的內容、以驗證物件是否已上傳。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   list-objects --bucket testbucket
   ```

5. 刪除物件。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   delete-object --bucket testbucket --key s3.pdf
   ```

6. 刪除儲存庫。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

如何實作S3 REST API StorageGRID

StorageGRID S3 REST API 如何解決衝突的用戶端請求

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。

「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

StorageGRID S3 REST API 如何平衡可用性和一致性

一致性可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。您可以根據應用程式的需求變更一致性。

預設情況下， StorageGRID保證新建立物件的讀寫一致性。成功完成 PUT 之後的任何 GET 都將能夠讀取新寫入的資料。現有物件的覆蓋、元資料更新和刪除最終是一致的。

如果您想要以不同的一致性執行物件作業、您可以：

- 指定一致性每個貯體。
- 指定的一致性每項 API 作業。
- 執行下列其中一項工作、變更預設的全網格一致性：
  - 在網格管理員中，前往*配置* > 系統 > 儲存設定 > 預設儲存桶一致性。
  - 。。

> 對全網格一致性所做的變更僅適用於變更設定後所建立的貯體。若要判斷變更的詳細資料、請參閱位於的稽核記錄 `/var/local/log`（搜尋 * 一致性層級 * ）。

一致性值

一致性會影響StorageGRID用於追蹤物件的元資料在節點之間的分佈方式。一致性影響物件對於客戶端請求的可用性。

您可以將貯體或 API 作業的一致性設定為下列其中一個值：

- * 全部 * ：所有節點都會立即接收物件中繼資料、否則要求將會失敗。
- 強全域：保證所有網站上所有客戶端請求的讀寫一致性。配置 Quorum 語意時，將套用下列行為：
  - 當網格具有三個或更多站點時，允許對客戶端請求進行站點故障容忍。雙站點電網不具備站點故障容忍能力。
  - 如果一個站點發生故障，以下 S3 操作將無法成功：

- 刪除 BucketEncryption
- PutBucketBranch
- PuttBucketEncryption
- PuttBucketVersion
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObjectRetention

如果需要的話，你可以 "配置StorageGRID Quorum 語意以實現強全域一致性"。

- **Strong-site** ：物件中繼資料會立即散佈到站台上的其他節點。保證站台內所有用戶端要求的寫入後讀取一致性。
- * 新寫入後讀 * ：提供新物件的寫入後讀取一致性、以及物件更新的最終一致性。提供高可用度與資料保護保證。建議大多數情況下使用。
- * 可用 * ：提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

使用「讀取後新寫入」和「可用」一致性

當標頭或 GET 作業使用「讀取後新寫入」一致性時、 StorageGRID 會以多個步驟執行查詢、如下所示：

- 它會先使用低一致性來查詢物件。
- 如果該查詢失敗、它會在下一個一致性值重複查詢、直到達到等同於 Strong-global 行為的一致性為止。

如果 HEAD 或 GET 作業使用「讀取後新寫入」一致性、但物件不存在、則物件查詢一律會達到等同於 Strong-global 行為的一致性。由於這種一致性需要在每個站台上提供多個物件中繼資料複本、因此如果同一個站台上有兩個或多個儲存節點無法使用、您可能會收到大量 500 個內部伺服器錯誤。

除非您需要與 Amazon S3 類似的一致性保證、否則您可以將一致性設定為「可用」、以防止這些錯誤發生在 HEAD 和 GET 作業中。當前端或 GET 作業使用「可用」一致性時、 StorageGRID 僅提供最終一致性。它不會在增加一致性時重試失敗的作業、因此不需要物件中繼資料的多個複本。

[[API- 作業 **-** 一致性控制 **]]** 指定 **API** 作業的一致性

若要設定個別 API 作業的一致性、作業必須支援一致性值、而且您必須在要求標頭中指定一致性。此範例會將 GetObject 作業的一致性設定為「 Strong-site 」。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

PutObject 和 GetObject 作業必須使用相同的一致性。

指定 **bucket** 的一致性

若要設定貯體的一致性、您可以使用 StorageGRID "實現庫位一致性"要求。或者、您也可以"改變貯體的一致性"從租戶管理程式中執行。

設定貯體的一致性時、請注意下列事項：

- 設定貯體的一致性、可決定用於在貯體或貯體組態中的物件上執行 S3 作業的一致性。它不會影響儲存庫本身的作業。
- 個別 API 作業的一致性會覆寫貯體的一致性。
- 一般而言、貯體應使用預設的一致性「讀取後新寫入」。如果要求無法正常運作、請盡可能變更應用程式用戶端行為。或者、設定用戶端以指定每個 API 要求的一致性。將貯體層級的一致性設為最後的方法。

一致性和 **ILM** 規則如何相互作用以影響資料保護

您選擇的一致性和 ILM 規則都會影響物件的保護方式。這些設定可以互動。

例如、儲存物件時所使用的一致性會影響物件中繼資料的初始放置位置、而為 ILM 規則選取的擷取行為則會影響物件複本的初始放置位置。由於 StorageGRID 需要同時存取物件的中繼資料及其資料、才能滿足用戶端要求、因此針對一致性和擷取行為選擇符合的保護層級、可以提供更好的初始資料保護、以及更可預測的系統回應。

ILM 規則適用下列"擷取選項"項目：

雙重承諾
: StorageGRID 會立即製作物件的臨時複本、並將成功傳回給用戶端。在ILM規則中指定的複本會盡可能製作。

嚴格
: 在 ILM 規則中指定的所有複本都必須在成功傳回用戶端之前製作。

平衡
: StorageGRID 會嘗試在擷取時製作 ILM 規則中指定的所有複本；如果不可能、則會製作過渡複本、並將成功傳回用戶端。ILM規則中指定的複本會盡可能製作。

一致性與 **ILM** 規則如何互動的範例

假設您有一個三站點網格，具有以下 ILM 規則和以下一致性：

- **ILM** 規則：建立三個物件副本，一個在本機站點，另一個在每個遠端站點。使用嚴格的攝取行為。
- 一致性：強全域（物件元資料立即分發到多個站點）。

當客戶端將物件儲存到網格時， StorageGRID會複製所有三個物件並將元資料分發到多個站點，然後再將成功返回給客戶端。

在接收成功訊息時，物件將受到完全保護，不會遺失。例如，如果本機站點在攝取後不久遺失，則物件資料和物件元資料的副本仍然存在於遠端站點。該物件可以從其他站點完全檢索。

如果您使用相同的 ILM 規則和強站點一致性，則用戶端可能會在物件資料複製到遠端站點之後但在物件元資料分發到那裡之前收到成功訊息。在這種情況下，物件元資料的保護等級與物件資料的保護等級不符。如果本地站點在攝取後不久遺失，則物件元資料就會遺失。無法檢索該物件。

一致性與 ILM 規則之間的相互關係可能很複雜。如需協助、請聯絡 NetApp 。

StorageGRID 如何使用物件版本控制

如果您要保留每個物件的多個版本、可以設定貯體的版本設定狀態。啟用貯體版本設定有助於防止意外刪除物件、並可讓您擷取及還原物件的舊版。

支援大部分功能的支援功能、以及部分限制、可讓整個系統執行版本管理。StorageGRIDStorageGRID 最多支援每個物件的 10 、 000 個版本。

物件版本管理可與StorageGRID 資訊的生命週期管理（ILM）或S3生命週期組態結合使用。您必須明確啟用每個儲存區的版本設定。當貯體啟用版本設定時、新增至貯體的每個物件都會指派版本 ID 、由 StorageGRID 系統產生。

不支援使用MFA（多因素驗證）刪除。

> ⓘ 版本管理只能在StorageGRID 以不含更新版本的版本資訊版本10.3所建立的儲存庫上啟用。

ILM與版本管理

ILM原則會套用至物件的每個版本。ILM掃描程序會持續掃描所有物件、並根據目前的ILM原則重新評估這些物件。您對ILM原則所做的任何變更、都會套用至所有先前擷取的物件。如果啟用版本管理、則包括先前擷取的版本。ILM掃描會將新的ILM變更套用至先前擷取的物件。

對於啟用版本設定的儲存區中的 S3 物件、版本設定支援可讓您建立使用「非目前時間」做為參考時間的 ILM 規則（請針對中的「僅將此規則套用至舊版物件？」問題選取 * 是 * "建立 ILM 規則精靈的步驟 1"）。更新物件時、其舊版本會變成非最新版本。使用「非目前時間」篩選器可讓您建立原則、以減少舊版物件的儲存影響。

> ⓘ 當您使用多部分上傳作業上傳物件的新版本時、原始版本物件的非目前時間會反映新版本的多部分上傳時間、而非多部分上傳完成時。在有限的情況下、原始版本的非目前時間可能比目前版本的時間早上幾小時或幾天。

相關資訊

- "如何刪除S3版本控制物件"
- "S3版本化物件的ILM規則和原則（範例4）"。

使用 S3 REST API 設定 StorageGRID S3 Object Lock

如果 StorageGRID 系統已啟用全域 S3 物件鎖定設定、您可以在啟用 S3 物件鎖定的情況下建立儲存區。您可以針對每個物件版本、指定每個儲存區或保留設定的預設保留。

> ⓘ StorageGRID 不支援 `x-amz-sdk-checksum-algorithm`請求標頭。

如何為貯體啟用 S3 物件鎖定

如果StorageGRID 您的整個S3物件鎖定設定已啟用、則您可以在建立每個儲存區時、選擇性地啟用S3物件鎖定。

S3 物件鎖定是永久性設定、只有在建立貯體時才能啟用。建立貯體後、您無法新增或停用 S3 物件鎖定。

若要為儲存桶啟用 S3 物件鎖定，請使用下列方法之一：

- 使用租戶管理程式建立桶。請參閱。 "建立S3儲存區"
- 使用具有要求標頭的 CreateBucket 要求建立貯體 `x-amz-bucket-object-lock-enabled`。請參閱。 "在貯體上作業"
- 從租戶管理器管理儲存桶設定。請參閱"更新 S3 物件鎖定預設保留"。

S3 物件鎖定需要儲存區版本設定、此功能會在建立儲存區時自動啟用。您無法暫停儲存區的版本設定。請參閱。 "物件版本管理"

貯體的預設保留設定

為貯體啟用 S3 物件鎖定時、您可以選擇性地啟用貯體的預設保留、並指定預設保留模式和預設保留期間。

預設保留模式

- 在法規遵循模式中：
  - 直到達到物件的保留日期、才能刪除物件。
  - 物件的保留日期可以增加、但不能減少。
  - 直到達到該日期為止、才能移除物件的保留日期。
- 在治理模式中：
  - 擁有權限的使用者 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`要求標頭來略過保留設定。
  - 這些使用者可以在達到物件版本的保留截止日期之前刪除物件版本。
  - 這些使用者可以增加、減少或移除物件的保留到目前為止。

預設保留期間

每個貯體都可以有一段以年或日為單位指定的預設保留期間。

如何設定貯體的預設保留

若要設定貯體的預設保留、請使用下列其中一種方法：

- 從 Tenant Manager 管理貯體設定。請參閱"建立S3儲存區"和"更新 S3 物件鎖定預設保留"。
- 針對貯體發出 PutObjectLockConfiguration 要求、以指定預設模式和預設天數或年數。

PutObjectLockConfiguration

PutObjectLockConfiguration 要求可讓您設定及修改已啟用 S3 物件鎖定的儲存區的預設保留模式和預設保留期間。您也可以移除先前設定的預設保留設定。

當新物件版本被擷取至儲存桶時，如果未指定 `x-amz-object-lock-mode`和 `x-amz-object-lock-retain-until-date`，則套用預設保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，則使用預設保留期間來計算保留至日期。

如果在擷取物件版本後修改了預設保留期間，則物件版本的保留截止日期保持不變，不會使用新的預設保留期間

重新計算。

您必須具有 `s3:PutBucketObjectLockConfiguration`權限或是帳戶根目錄、才能完成此作業。

您必須在 PutObjectLockConfiguration 要求中指定以下要求標頭之一：

```
Content-MD5
x-amz-checksum-*
```

StorageGRID 不會驗證此操作的 x-amz-checksum-* 標頭內容。

申請範例

此範例為儲存桶啟用 S3 Object Lock（如果您的網格系統管理員已授予權限），並將預設保留模式設為 COMPLIANCE，預設保留期間設為 6 年。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

如何決定貯體的預設保留

若要判斷儲存區是否啟用 S3 物件鎖定、並查看預設保留模式和保留期間、請使用下列其中一種方法：

- 在租戶管理器中檢視貯體。請參閱。 "檢視 S3 儲存區"
- 發出 GetObjectLockConfiguration 要求。

GetObjectLockConfiguration

GetObjectLockConfiguration 要求可讓您判斷儲存區是否已啟用 S3 物件鎖定、如果已啟用、請查看儲存區是否已設定預設保留模式和保留期間。

當新物件版本擷取至儲存桶時，如果未指定 `x-amz-object-lock-mode`，則套用預設保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，則使用預設保留期間來計算保留截止日期。

您必須具有 `s3:GetBucketObjectLockConfiguration`權限或是帳戶根目錄、才能完成此作業。

申請範例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

回應範例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

啟用 S3 物件鎖定的貯體可包含物件組合、並具有或不含 S3 物件鎖定保留設定。

物件層級保留設定是使用 S3 REST API 指定的。物件的保留設定會覆寫貯體的任何預設保留設定。

您可以為每個物件指定下列設定：

- * 保留模式 * ：法規遵循或治理。
- * 截止日期 * ：指定 StorageGRID 必須保留物件版本多久的日期。
  - 在規範模式中、如果保留截止日期是未來、則可以擷取物件、但無法修改或刪除物件。保留截止日期可以增加、但無法減少或移除此日期。
  - 在治理模式中、具有特殊權限的使用者可以略過保留到最新的設定。他們可以在物件版本的保留期間結束之前刪除物件版本。他們也可以增加、減少或甚至移除截止日期的保留。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。

  物件的合法保留設定不受保留模式和保留截止日期的影響。如果物件版本處於合法保留狀態、則沒有人可以刪除該版本。

若要在將物件版本新增至貯體時指定 S3 物件鎖定設定"PuttObject"、請發出、"CopyObject"或"建立多個部分上傳"要求。

您可以使用下列項目：

- `x-amz-object-lock-mode`，可以是法規遵循或治理（區分大小寫）。

  > 如果指定 `x-amz-object-lock-mode`，則還必須指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
  - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
  - 保留截止日期必須為未來日期。
- `x-amz-object-lock-legal-hold`

  如果已開啟合法持有（區分大小寫）、則物件將置於合法持有之下。如果法律保留已關閉、則不會保留任何合法的保留。任何其他值都會導致400個錯誤要求（InvalidArgument）錯誤。

如果您使用上述任一要求標頭、請注意下列限制：

- 如果 PutObject 請求中存在任何 x-amz-object-lock-* 請求標頭，則必須包含下列其中一個請求標頭：

```
Content-MD5
x-amz-checksum-*
```

這些標頭對於 CopyObject 或 CreateMultipartUpload 並非必要。

- 如果儲存桶未啟用 S3 物件鎖定，且存在 x-amz-object-lock-* 請求標頭，則會傳回 400 Bad Request （InvalidRequest） 錯誤。
- PutObject 要求支援使用 `x-amz-storage-class: REDUCED_REDUNDANCY`以符合 AWS 行為。然而、當物件被擷取至啟用S3物件鎖定的儲存區時StorageGRID 、則會一律執行雙重認可擷取。
- 後續的 Get 或 HeadObject 版本回應將包括標頭 `x-amz-object-lock-mode`、和 `x-amz-object-lock-legal-hold`（如果已設定）、 `x-amz-object-lock-retain-until-date`以及要求寄件者是否擁有正確的 `s3:Get*`權限。

您可以使用 `s3:object-lock-remaining-retention-days`原則條件金鑰來限制物件的最小和最大允許保留期間。

如何更新物件的保留設定

如果您需要更新現有物件版本的合法保留或保留設定、可以執行下列物件子資源作業：

- `PutObjectLegalHold`

  如果新的合法持有值已開啟、則物件將置於合法持有之下。如果合法持有值為「關」、則合法持有將被解除。

- `PutObjectRetention`
  - 模式值可以是法規遵循或治理（區分大小寫）。
  - 保留截止日期值必須採用格式 `2020-08-10T21:46:00Z`。允許分數秒、但只保留3個小數位數（毫秒精度）。不允許其他 ISO 8601 格式。
  - 如果物件版本有現有的截至日期保留、您只能增加。新的價值必須是未來的價值。

您必須在請求中指定以下請求標頭之一：

```
Content-MD5
x-amz-checksum-*
```

StorageGRID 不會驗證這些操作中 x-amz-checksum-* 標頭的內容。

如何使用治理模式

擁有權限的使用者 `s3:BypassGovernanceRetention`可以略過使用治理模式之物件的作用中保留設定。任何刪除或 PutObjectRetention 作業都必須包含 `x-amz-bypass-governance-retention:true`要求標頭。這些使用者可以執行這些額外作業：

- 執行 DeleteObject 或 DeleteObjects 作業、以在物件版本的保留期間結束之前刪除物件版本。

  合法持有的物件無法刪除。合法持有必須關閉。

  此 `x-amz-bypass-governance-retention`標頭對沒有 S3 Object Lock 的物件無效。

- 在物件的保留期間結束之前、執行 PutObjectRetention 作業、將物件版本的模式從治理模式變更為法規遵循模式。

永遠不允許將模式從法規遵循變更為治理。

- 執行 PutObjectRetention 作業以增加、減少或移除物件版本的保留期間。

相關資訊

- "使用S3物件鎖定來管理物件"
- "使用 S3 物件鎖定來保留物件"
- "Amazon Simple Storage Service 使用者指南：鎖定物件"

了解 **StorageGRID** 的 **S3** 生命週期組態

您可以建立S3生命週期組態、以控制何時從StorageGRID 作業系統刪除特定物件。

本節中的簡單範例說明如何透過 S3 生命週期組態來控制何時從特定的 S3 儲存桶中刪除（過期）某些物件。本節中的範例僅用於說明目的。如需建立 S3 生命週期組態的完整詳細資訊，請參閱 "Amazon Simple Storage Service 使用者指南：管理物件的生命週期"。請注意，StorageGRID 僅支援 Expiration 動作，不支援 Transition 動作。

什麼是生命週期組態

生命週期組態是套用至特定S3儲存區中物件的一組規則。每個規則都會指定受影響的物件、以及這些物件何時到期（在特定日期或幾天之後）。

在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素：

- 過期：在達到指定日期或達到指定天數時刪除物件、從擷取物件開始算起。
- 非目前版本過期：在達到指定天數時刪除物件、從物件變成非目前的開始算起。
- 篩選器（前置、標記）
- 狀態
- ID

每個物件都遵循 S3 儲存區生命週期或 ILM 原則的保留設定。當 S3 貯體生命週期設定完成時、生命週期到期動作會覆寫符合貯體生命週期篩選器之物件的 ILM 原則。不符合貯體生命週期篩選器的物件、會使用 ILM 原則的保留設定。如果物件符合貯體生命週期篩選器、且未明確指定到期動作、則不會使用 ILM 原則的保留設定、而且會暗示物件版本會永遠保留。請參閱。 "S3 儲存區生命週期和 ILM 原則的優先順序範例"

因此、即使ILM規則中的放置指示仍套用至物件、也可能從網格中移除物件。或者、即使物件的任何ILM放置指示失效、物件仍可能保留在網格上。如需詳細資訊、請參閱 "ILM在物件生命週期內的運作方式"。

> 庫位生命週期組態可搭配已啟用S3物件鎖定的庫位使用、但庫位生命週期組態不支援舊型符合標準的庫位。

支援使用下列庫位作業來管理生命週期組態：StorageGRID

- 刪除 BucketLifecycle
- GetBucketLifecycleConfiguration
- PuttBucketLifecycleConfiguration

建立生命週期組態的第一步、就是建立一個包含一或多個規則的Json檔案。例如、此Json檔案包含三個規則、如下所示：

1. 規則 1 僅適用於符合前置碼/ 且 `key2`值為 `tag2`的物件 `category1`。此 `Expiration`參數指定符合篩選條件的物件將於 2020 年 8 月 22 日午夜到期。
2. 規則 2 僅適用於符合前置碼/ 的物件 `category2`。此 `Expiration`參數指定符合篩選條件的物件將在擷取後 100 天過期。

   > 指定天數的規則是相對於擷取物件的時間。如果目前日期超過擷取日期加上天數、則在套用生命週期組態後、部分物件可能會立即從儲存庫中移除。

3. 規則 3 僅適用於符合前置/ 的物件 `category3`。此 `Expiration`參數會指定任何非目前版本的相符物件會在非目前版本之後 50 天過期。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

將生命週期組態套用至貯體

建立生命週期組態檔案之後、您可以發出 PuttBucketLifecycleConfiguration 要求、將其套用至儲存庫。

此要求會將範例檔案中的生命週期組態套用至名為的貯體中的物件 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

若要驗證已成功將生命週期組態套用至貯體、請發出 GetBucketLifecycleConfiguration 要求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功的回應會列出您剛套用的生命週期組態。

驗證目標是否適用庫位生命週期到期

您可以在發出 PutObject 、 HeadObject 或 GetObject 要求時、判斷生命週期組態中的到期規則是否適用於特定物件。如果套用規則、回應會包含一個 `Expiration`參數、指出物件何時過期、以及相符的到期規則。

> 由於貯體生命週期會覆寫 ILM 、因此 `expiry-date`所顯示的是物件將被刪除的實際日期。如需詳細資訊、請參閱 "如何判斷物件保留"。

例如、本 PutObject 申請於 2020 年 6 月 22 日發出、並在貯體中放置物件 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功回應表示物件將在100天（2020年10月1日）後過期、且符合生命週期組態的規則2。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如、此 HeadObject 要求用於取得 testBucket 儲存區中相同物件的中繼資料。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功回應包括物件的中繼資料、指出物件將在100天內過期、且符合規則2。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

對於啟用版本控制的儲存區、 `x-amz-expiration`回應標頭僅適用於物件的目前版本。

使用 **StorageGRID** 實作 **S3 REST API** 的建議

實作S3 REST API以搭配StorageGRID 使用時、請遵循以下建議。

針對不存在物件的使用者提出建議

如果您的應用程式定期檢查某個物件是否存在於您認為該物件實際上不存在的路徑中，則應使用“可用”"一致性"。例如，如果您的應用程式在 PUT 之前 HEAD 某個位置，則您應該使用「可用」一致性。

否則、如果前端作業找不到物件、如果同一站台上有兩個或多個儲存節點無法使用、或遠端站台無法連線、您可能會收到大量 500 個內部伺服器錯誤。

您可以使用要求為每個貯體設定「可用」一致性"實現庫位一致性"、或是在個別 API 作業的要求標頭中指定一致性。

物件金鑰建議

請根據第一次建立貯體的時間、遵循下列物件金鑰名稱建議。

在 **StorageGRID 11.4** 或更早版本中建立的貯體

- 請勿使用隨機值做為物件金鑰的前四個字元。這與前AWS關於金鑰前置碼的建議不同。請改用非隨機、非唯一的前置字元、例如 `image`。
- 如果您遵循前 AWS 的建議、在金鑰首碼中使用隨機和唯一字元、請在物件金鑰前加上目錄名稱。也就是使用此格式：

  `mybucket/mydir/f8e3-image3132.jpg`

  而非此格式：

```
mybucket/f8e3-image3132.jpg
```

在 **StorageGRID 11.4** 或更新版本中建立的貯體

不需要限制物件金鑰名稱以符合效能最佳實務做法。在大多數情況下、您可以對物件金鑰名稱的前四個字元使用隨機值。

S3 工作負載的例外情況是、它會在一段短時間後持續移除所有物件。為了將此使用案例的效能影響降至最低、請將金鑰名稱的前置部分變更為每數千個物件、例如日期。例如、假設 S3 用戶端通常每秒寫入 2 、 000 個物件、而 ILM 或儲存庫生命週期原則則會在三天後移除所有物件。若要將效能影響降至最低、您可以使用如下模式命名金鑰： `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

「範圍讀取」建議

如果"用於壓縮儲存物件的全域選項"啟用、 S3 用戶端應用程式應避免執行 GetObject 作業、以指定傳回位元組範圍。這些「範圍讀取」作業效率不彰、因為 StorageGRID 必須有效地解壓縮物件以存取要求的位元組。從非常大的物件要求少量位元組的 GetObject 作業尤其缺乏效率、例如從 50 GB 壓縮物件讀取 10 MB 範圍是效率不彰的。

如果從壓縮物件讀取範圍、用戶端要求可能會逾時。

如果您需要壓縮物件、而用戶端應用程式必須使用範圍讀取、請增加應用程式的讀取逾時。

支援 Amazon S3 REST API

StorageGRID 中支援的 **S3 REST API** 作業和限制

此系統實作簡單儲存服務API（API版本2002-03）、支援大部分作業、並有一些限制。StorageGRID整合S3 REST API用戶端應用程式時、您必須瞭解實作詳細資料。

StorageGRID 系統同時支援虛擬託管式請求和路徑式請求。

日期處理

S3 REST API的支援僅支援有效的HTTP日期格式。StorageGRID

支援此功能的僅支援接受日期值的任何標頭的有效HTTP日期格式。StorageGRID日期的時間部分可以格林尼治標準時間（GMT）格式指定、或以通用協調時間（UTC）格式指定、且無時區偏移（必須指定+0000）。如果您在要求中包含 `x-amz-date`標頭、則它會覆寫在「日期要求」標頭中指定的任何值。使用 AWS 簽名版本 4 時、`x-amz-date`由於日期標頭不受支援、因此標頭必須存在於簽署的要求中。

一般要求標頭

StorageGRID 系統支援由定義的一般要求標頭 "Amazon Simple Storage Service API 參考：一般要求標頭"、但有一個例外。

要求標頭	實作
授權	完整支援AWS簽名版本2 支援AWS簽名版本4、但有下列例外： • 當您在中提供實際有效負載 Checksum 值時 `x-amz-content-sha256`、該值會在未驗證的情況下被接受、就好像已為標頭提供該值一樣 `UNSIGNED-PAYLOAD`。當您提供 `x-amz-content-sha256`**表示串流的標頭值** `aws-chunked`（例如串流 -AWS4 -HMAC-SHA256 有效負載）時、不會根據區塊資料驗證區塊簽章。

通用回應標頭

支援所有由_Simple Storage Service API Reference（簡易儲存服務API參考）定義的通用回應標頭、但有一項例外。StorageGRID

回應標頭	實作
X-amz-id-2	未使用

StorageGRID S3 REST API 如何驗證請求

支援使用S3 API驗證和匿名存取物件的功能。StorageGRID

S3 API支援驗證S3 API要求的簽名版本2和簽名版本4。

驗證的要求必須使用您的存取金鑰ID和秘密存取金鑰來簽署。

StorageGRID 系統支援兩種驗證方法： HTTP `Authorization` 標頭和使用查詢參數。

使用**HTTP**授權標頭

除了 Bucket 原則允許的匿名要求外、所有 S3 API 作業都會使用 HTTP `Authorization` 標頭。`Authorization`標頭包含驗證要求所需的所有簽署資訊。

使用查詢參數

您可以使用查詢參數將驗證資訊新增至URL。這稱為URL預先簽署、可用來授予特定資源的暫時存取權。具有預先簽署 URL 的使用者不需要知道密碼存取金鑰即可存取資源、這可讓您提供第三方受限存取資源。

StorageGRID 中支援的服務作業

支援下列服務作業的支援。StorageGRID

營運	實作
列表桶 （先前命名的 Get Service ）	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
取得儲存使用量	StorageGRID "取得儲存使用量"要求會告訴您帳戶使用的儲存空間總量、以及與帳戶相關的每個儲存區。這是服務上的一項作業、其路徑為 / (`?x-ntap-sg-usage`、並新增自訂查詢參數）。
選項/	用戶端應用程式可以向儲存節點上的 S3 連接埠發出 `OPTIONS /`要求、而無需提供 S3 驗證認證、以判斷儲存節點是否可用。您可以使用此要求進行監控、或允許外部負載平衡器識別儲存節點何時當機。

StorageGRID 中的 **S3** 儲存貯體作業和實作詳細資料

StorageGRID 系統為每個 S3 租戶帳戶支援最多 20,000 個儲存桶。

每個網格最多可有 100,000 個貯體。

如果多個租戶各自擁有最多 5,000 個儲存桶，則網格中的每個 Storage Node 必須至少有 64 GB 的 RAM。

儲存桶名稱限制遵循 AWS 美國標準區域限制，但為了支援 S3 虛擬託管式請求，您應該進一步將其限制為 DNS 命名慣例。

更多資訊請參考以下內容：

- "Amazon Simple Storage Service 使用者指南：貯體配額、限制和限制"
- "設定 S3 端點網域名稱"

ListObjects（取得 Bucket）和 ListObjectVersions（取得 Bucket 物件版本）操作支援StorageGRID"一致性值"。

您可以檢查是否已為各個儲存桶啟用或停用上次存取時間更新。請參閱"取得時段上次存取時間"。

下表說明StorageGRID 了為什麼由Ss哪些 人執行S3 REST API貯體作業。若要執行上述任何作業、必須為帳戶提供必要的存取認證資料。

營運	實作
建立庫位	建立新的貯體。建立貯體後、您就成為了貯體的擁有者。 注意：不支援 S3 目錄儲存桶。 • 庫位名稱必須符合下列規則： ◦ 必須在各個StorageGRID 方面都是獨一無二的（不只是租戶帳戶內的獨特功能）。 ◦ 必須符合DNS規範。 ◦ 必須包含至少 3 個字元、不得超過 63 個字元。 ◦ 可以是一或多個標籤的系列、相鄰的標籤以句點分隔。每個標籤都必須以英文字母或數字開頭和結尾、而且只能使用英文字母、數字和連字號。 ◦ 不得看起來像是文字格式的IP位址。 ◦ 不應在虛擬託管樣式要求中使用期間。期間會導致伺服器萬用字元憑證驗證發生問題。 • 根據預設、會在區域中建立貯 `us-east-1`體；不過、您可以使用 `LocationConstraint`要求主體中的 `request` 元素來指定不同的區域。使用該元素時 `LocationConstraint`、您必須指定使用 Grid Manager 或 Grid Management API 定義的確切區域名稱。如果您不知道應該使用的地區名稱、請聯絡您的系統管理員。 注意：如果您的 CreateBucket 要求使用了 StorageGRID 中未定義的區域，則會發生錯誤。 • 您可以透過新增 `x-amz-bucket-object-lock-enabled`請求標頭來建立啟用了 S3 物件鎖定的儲存桶。請參閱"使用 S3 REST API 來設定 S3 物件鎖定"。 S3 Object Lock 需要儲存桶版本控制，當您建立啟用了 S3 Object Lock 的儲存桶時，此功能會自動啟用。 您可以在建立儲存桶時或稍後啟用 S3 物件鎖定。
刪除Bucket	刪除貯體。
刪除 BucketCors	刪除貯體的 CORS 組態。
刪除 BucketEncryption	刪除儲存區中的預設加密。現有的加密物件會保持加密狀態、但新增至儲存庫的任何新物件都不會加密。
刪除 BucketLifecycle	從儲存桶中刪除生命週期組態。請參閱"建立S3生命週期組態"。
刪除BucketPolicy	刪除附加至貯體的原則。
刪除 BucketReplication	刪除附加至貯體的複寫組態。

營運	實作
刪除 Bucketagging	使用 `tagging`子資源從貯體中移除所有標記。 注意：如果此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤並已賦值。如果存在 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤，請勿發出 DeleteBucketTagging 要求。而應發出僅包含 `NTAP-SG-ILM-BUCKET-TAG`標籤及其賦值的 PutBucketTagging 要求，以移除儲存桶中的所有其他標籤。請勿修改或移除 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤。
GetBucketAcl	傳回正面回應、以及貯體擁有者的 ID 、 DisplayName 和權限、表示擁有者擁有該貯體的完整存取權。
GetBucketCors	傳回 `cors`貯體的組態。
GetBucketEncryption	傳回儲存區的預設加密組態。
GetBucketLifecycleConfiguration （先前命名的 Get Bucket 生命週期）	傳回儲存桶的生命週期組態。請參閱"建立S3生命週期組態"。
GetBucketLocation	傳回使用 `LocationConstraint` 元素在 CreateBucket 請求中設定的區域。如果儲存桶的區域為 `us-east-1`（預設值），則會傳回 `LocationConstraint` 的空值。
GetBucketNotificationConfiguration （先前命名的 Get Bucket 通知）	傳回附加至貯體的通知組態。
GetBucketPolicy	傳回附加至貯體的原則。
GetBucketReplication	傳回附加至貯體的複寫組態。
GetBucketTagging	使用 `tagging`子資源傳回貯體的所有標記。 注意：如果為此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤被賦予一個值。請勿修改或移除此標籤。
GetBucketVersion	此實作使用 `versioning`子資源傳回貯體的版本設定狀態。 • _ 空白 _ ：版本設定從未啟用（儲存庫「未版本化」） • 已啟用：已啟用版本管理 • 已暫停：先前已啟用版本管理、並已暫停

營運	實作
GetObjectLockConfiguration	如果已設定、則會傳回儲存區預設保留模式和預設保留期間。 請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。
標題庫	決定貯體是否存在、且您有存取權限。 此作業會傳回： • `x-ntap-sg-bucket-id`： UUID 格式的儲存區 UUID 。 • `x-ntap-sg-trace-id`：關聯請求的唯一跟蹤 ID 。
ListObjects 和 ListObjectsV2 （先前命名的 GET Bucket ）	傳回貯體中的部分或全部物件（最多 1 、 000 個物件）。物件的儲存類別可以有兩個值、即使物件是使用儲存類別選項擷取 `REDUCED_REDUNDANCY`： • `STANDARD`，表示物件儲存在由儲存節點組成的儲存資源池中。 • `GLACIER`、表示物件已移至 Cloud Storage Pool 指定的外部儲存區。 如果貯體包含大量具有相同首碼的刪除金鑰、回應可能會包含一些不包含金鑰的金鑰 `CommonPrefixes`。 對於 HeadObject 和 ListObject 請求， StorageGRID傳回具有不同精確度的 LastModified 時間戳，而 AWS 傳回具有相同精確度的時間戳，如以下範例所示： • StorageGRID HeadObject：“LastModified”：“2024-09-26T16：43：24 + 00：00” • StorageGRID ListObject：“LastModified”：“2024-09-26T16：43：24.931000 + 00：00” • AWS HeadObject：“LastModified”：“2023-10-17T00：19：54 + 00：00” • AWS ListObject：「LastModified」：「2023-10-17T00：19：54 + 00：00”
ListObjectVerions （先前命名的 Get Bucket 物件版本）	在貯體上具有讀取存取權、將此作業與子資源一起使用會 `versions`列出貯體中所有物件版本的中繼資料。
PuttBucketCors	設定貯體的 CORS 組態、以便該貯體能夠處理跨來源要求。跨來源資源共用（CORS）是一種安全機制、可讓單一網域中的用戶端Web應用程式存取不同網域中的資源。例如、假設您使用名為的 S3 儲存區 `images`來儲存圖形。透過設定貯體的 `CORS` 組態 `images`、您可以允許該貯體中的影像顯示在網站上 `http://www.example.com`。

營運	實作
PuttBucketEncryption	設定現有儲存區的預設加密狀態。啟用桶層級加密時、任何新增至桶的新物件都會加密。StorageGRID支援使用StorageGRID管理的金鑰進行伺服器端加密。指定伺服器端加密組態規則時，請將參數設定 `SSEAlgorithm`為 `AES256`，而不要使用 `KMSMasterKeyID`參數。 如果物件上傳要求已指定加密（亦即、如果要求包含要求標頭）、則會忽略貯體預設加密組態 `x-amz-server-side-encryption-*`。
PuttBucketLifecycleConfiguration （先前命名的 Put Bucket 生命週期）	為貯體建立新的生命週期組態、或取代現有的生命週期組態。在生命週期組態中、支援多達1、000個生命週期規則。StorageGRID每個規則可包含下列XML元素： • 到期（天數、日期、 ExpiredObjectDeleteMarker ） • 非目前版本到期（ NewerNoncurrentVerions 、 NoncurrentDays ） • 篩選器（前置、標記） • 狀態 • ID 不支援下列動作：StorageGRID • AbortIncompleteMultiPart上 傳 • 移轉 請參閱"建立S3生命週期組態"。若要了解儲存桶生命週期中的到期行動如何與 ILM 放置指令互動，請參閱"ILM如何在整個物件生命週期內運作"。 附註：鏟斗生命週期組態可搭配已啟用S3物件鎖定的鏟斗使用、但舊型符合標準的鏟斗不支援鏟斗生命週期組態。

營運	實作

PutBucketNotificationConfiguration
 	
（先前命名的 Put Bucket 通知）
	使用要求主體中的通知組態 XML 來設定貯體通知。您應該瞭解下列實作詳細資料：
	
	• StorageGRID支援 Amazon Simple Notification Service (Amazon SNS) 主題、Kafka 主題或 webhook 端點作為目的地。不支援簡單佇列服務 (SQS) 或 AWS Lambda 端點。
	• 通知的目的地必須指定為StorageGRID 一個端點的URN。端點可以使用租戶管理程式或租戶管理API來建立。
	
	端點必須存在、通知組態才能成功。如果端點不存在， `400 Bad Request` 則會傳回錯誤代碼 `InvalidArgument`。
	
	• 您無法設定下列事件類型的通知。這些事件類型*不支援*。
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• 從 StorageGRID 傳送的事件通知使用標準 JSON 格式、但不包含某些金鑰、也不為其他金鑰使用特定值、如下表所示：
	◦ 事件來源
	
	`sgws:s3`
	
	◦ * awsRegion *
	
	不含
	
	◦ * X-amz-id-2*
	
	不含
	
	◦ * arn*
	
	`urn:sgws:s3:::bucket_name`

PuttBucketPolicy	設定附加到儲存桶的原則。請參閱"使用貯體和群組存取原則"。

營運	實作
PutBucketReplication	使用要求主體中提供的複寫組態 XML 來設定"StorageGRID CloudMirror 複寫"貯體。對於CloudMirror複寫、您應該瞭解下列實作詳細資料： • StorageGRID 僅支援複寫組態的 V1 版本。這表示 StorageGRID 不支援在規則中使用 `Filter`元素，並遵循 V1 慣例來刪除物件版本。如需詳細資訊、請參閱 "Amazon Simple Storage Service 使用者指南：複寫組態"。 • 儲存區複寫可在版本控制或未版本控制的儲存區上進行設定。 • 您可以在複寫組態XML的每個規則中指定不同的目的地儲存區。來源儲存區可複寫至多個目的地儲存區。 • 目的地儲存桶必須指定為租戶管理器或租戶管理 API 中指定的 StorageGRID 端點的 URN。請參閱"設定CloudMirror複寫"。 複寫組態必須存在端點才能成功。如果端點不存在、則要求會以失敗的方式失敗 `400 Bad Request`。錯誤訊息指出：`Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • 您不需要在組態 XML 中指定 `Role`。此值不供StorageGRID Some使用、如果提交、將會忽略此值。 • 如果您省略組態 XML 中的儲存類別、則 StorageGRID 預設會使用 `STANDARD`儲存類別。 • 如果您從來源儲存區刪除物件、或是刪除來源儲存區本身、跨區域複寫行為如下： ◦ 如果您在物件或貯體複寫之前刪除該物件或貯體、則不會複寫該物件 / 貯體、也不會通知您。 ◦ 如果您在複寫物件或儲存區之後將其刪除、StorageGRID 則針對跨區域複寫的V1、執行標準Amazon S3刪除行為。
PuttBucketTagging	使用 `tagging`子資源來新增或更新貯體的一組標記。新增庫位標記時、請注意下列限制： • 支援每個儲存區最多50個標籤的支援功能包括：StorageGRID • 與庫位關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元。 • 標記值長度最多可達256個UNICODE字元。 • 金鑰和值區分大小寫。 注意：如果為此儲存桶設定了非預設的 ILM 原則標籤，則會有一個 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤及其賦值。請確保在所有 PutBucketTagging 請求中包含 `NTAP-SG-ILM-BUCKET-TAG`儲存桶標籤及其賦值。請勿修改或移除此標籤。 • 附註 * ：此作業將覆寫貯體已有的任何目前標籤。如果集合中遺漏任何現有標記、則會移除該貯體的這些標記。

營運	實作
PuttBucketVersion	使用 `versioning`子資源來設定現有儲存區的版本設定狀態。您可以使用下列其中一個值來設定版本設定狀態： • 已啟用：啟用儲存區中物件的版本管理。新增至儲存庫的所有物件都會收到唯一的版本ID。 • 暫停：停用儲存區中物件的版本設定。添加到桶中的所有對象都將接收版本 ID `null`。
PutObjectLockConfiguration	• 設定或移除貯體預設保留模式和預設保留期間。 • 如果網格系統管理員已授予權限，則對現有儲存桶啟用 S3 物件鎖定。 如果修改預設保留期間，現有物件版本的保留截止日期保持不變，不會使用新的預設保留期間重新計算。 詳細資訊請參閱 "使用 S3 REST API 來設定 S3 物件鎖定"。

物件上的作業

StorageGRID 如何實作物件的 **S3 REST API** 作業

本節說明StorageGRID 此「物件」的「物件」功能如何執行S3 REST API作業。

下列條件適用於所有物件作業：

- StorageGRID"一致性值"所有物件操作均支持，但以下操作除外：
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - 選取物件內容
- 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。
- 所有物件均由庫位擁有者擁有、包括匿名使用者或其他帳戶所建立的物件。StorageGRID

下表說明StorageGRID 了Ss哪些 物件是由S3 REST API物件執行。

營運	實作
刪除物件	處理 DeleteObject 要求時、 StorageGRID 會嘗試立即從所有儲存位置移除物件的所有複本。如果成功、StorageGRID 則會立即將回應傳回給用戶端。如果無法在 30 秒內移除所有複本（例如、因為某個位置暫時無法使用）、 StorageGRID 會將複本排入佇列以供移除、然後表示用戶端成功。 限制 • 不支援多因素驗證（ MFA ）和回應標頭 `x-amz-mfa`。 • `If-Match` 和 `If-None-Match` 標頭的行為會因 StorageGRID 組態而有所不同。提供這些標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match` 或 `If-None-Match` 標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。 此 `x-amz-bypass-governance-retention`標頭對沒有 S3 Object Lock 的物件無效。 版本管理 若要移除特定版本、申請者必須是貯體擁有者、並使用 `versionId`子資源。使用此子資源會永久刪除版本。如果與刪除標記相對應、則 `versionId`回應標頭 `x-amz-delete-marker`會設為 `true`。 • 如果在已啟用版本設定的貯體上刪除物件而不使用子資源、則 `versionId`會產生刪除標記。 `versionId`刪除標記的會使用回應標頭傳回 `x-amz-version-id`、 `x-amz-delete-marker`回應標頭會設為 `true`。 • 如果刪除物件時、儲存庫中的子資源並已暫停版本設定、則 `versionId`會永久刪除已存在的「 `null` 」版本或「 `null` 」刪除標記、並產生新的「 `null` 」刪除標記。 `x-amz-delete-marker`回應標頭會傳回設定為 `true`。 附註：在某些情況下、物件可能會有多個刪除標記。 請參閱"使用 S3 REST API 來設定 S3 物件鎖定"以瞭解如何在治理模式中刪除物件版本。
刪除物件 （先前命名的刪除多個物件）	不支援多因素驗證（ MFA ）和回應標頭 `x-amz-mfa`。 您可以在同一個要求訊息中刪除多個物件。 此 `x-amz-bypass-governance-retention`標頭對沒有 S3 Object Lock 的物件無效。 請參閱"使用 S3 REST API 來設定 S3 物件鎖定"以瞭解如何在治理模式中刪除物件版本。

營運	實作
刪除ObjectTagging	使用 `tagging` SubResource 從物件移除所有標記。 版本管理 如果 `versionId`在要求中未指定查詢參數、則作業會從版本控制儲存區中最新版本的物件中刪除所有標記。如果物件的目前版本是刪除標記、則會傳回「 `MethodNotAllowed` 」狀態、並 `x-amz-delete-marker`將回應標頭設為 `true`。
GetObject	"GetObject"
GetObjectAcl	如果提供帳戶所需的存取認證資料、則作業會傳回正面回應、並傳回物件擁有者的ID、顯示名稱和權限、表示擁有者擁有物件的完整存取權。
GetObjectLegalHold	"使用 S3 REST API 來設定 S3 物件鎖定"
GetObjectRetention	"使用 S3 REST API 來設定 S3 物件鎖定"
GetObjectTagging	使用 `tagging` SubResource 傳回物件的所有標記。 版本管理 如果 `versionId`在要求中未指定查詢參數、則作業會傳回版本控制儲存區中物件最新版本的所有標記。如果物件的目前版本是刪除標記、則會傳回「 `MethodNotAllowed` 」狀態、並 `x-amz-delete-marker`將回應標頭設為 `true`。
標題物件	"標題物件"
RestoreObject	"RestoreObject"
PuttObject	"PuttObject"
CopyObject （先前命名的「 Put 物件 - 複本」）	"CopyObject"
PutObjectLegalHold	"使用 S3 REST API 來設定 S3 物件鎖定"
PutObjectRetention	"使用 S3 REST API 來設定 S3 物件鎖定"

營運	實作
PuttObjectTagging	使用 `tagging`子資源將一組標記新增至現有物件。 物件標籤限制 您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。 標記更新和擷取行為 當您使用 PuttObjectTagging 更新物件的標記時、 StorageGRID 不會重新擷取物件。這表示不會使用相符ILM規則中指定的擷取行為選項。當ILM由正常背景ILM程序重新評估時、會對更新所觸發的物件放置位置進行任何變更。 這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。 解決衝突 衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。 版本管理 如果 `versionId`在要求中未指定查詢參數、則作業會將標記新增至版本化儲存區中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「 `MethodNotAllowed` 」狀態、並 `x-amz-delete-marker`將回應標頭設為 `true`。
選取物件內容	"選取物件內容"

StorageGRID 中支援的 **Amazon S3 Select** 作業

StorageGRID 支援下列的 Amazon S3 Select 子句、資料類型和運算子"SelectObjectContent命令"。

不支援任何未列出的項目。

有關語法，請參閱"選取物件內容"。如需 S3 Select 的詳細資訊，請參閱 "S3 Select的AWS文件"。

只有啟用S3 Select的租戶帳戶才能發出SelectObjectContent查詢。請參閱"使用S3 Select的考量與要求"。

條款

- 選取清單

- from子句
- where子句
- 限制條款

資料類型

- 布爾
- 整數
- 字串
- 浮動
- 十進位、數字
- 時間戳記

運算子

邏輯運算子

- 和
- 不是
- 或

比較運算子

- <
- >
- &lt ； =
- >=
- =
- =
- <>
- ！=
- 兩者之間
- 在中

模式比對運算子

- 喜歡
- _
- %

單一運算子

- 為空值
- 不是空值

數學運算子

- +
- -
- *
- /
- %

StorageGRID 遵循 Amazon S3 Select 運算子的優先順序。

Aggregate函數

- 平均（）
- 計數（*）
- 最大（）
- 最小（）
- 總計（）

條件式函數

- 案例
- 合併
- NULLIF

轉換功能

- CAST（適用於支援的資料類型）

日期函數

- 日期新增
- 日期_差異
- 擷取
- 至字串
- 目標時間戳記
- UTCNOW

字串函數

- char_length、字元長度
- 降低
- 子字串
- 修剪
- 上

StorageGRID 如何使用伺服器端加密

伺服器端加密可讓您保護閒置的物件資料。當資料寫入物件時、系統會加密資料、並在您存取物件時解密資料。StorageGRID

如果您想要使用伺服器端加密、您可以根據加密金鑰的管理方式、選擇兩個互不相容的選項之一：

- * SSE（使用StorageGRID管理金鑰的伺服器端加密）*：當您發出S3要求以儲存物件時StorageGRID 、用唯一的金鑰來加密物件。當您發出S3要求以擷取物件時StorageGRID 、則會使用儲存的金鑰來解密物件。
- * SSE-C（使用客戶提供的金鑰進行伺服器端加密）*：當您發出S3要求以儲存物件時、您會提供自己的加密金鑰。擷取物件時、您提供的加密金鑰與要求的一部分相同。如果兩個加密金鑰相符、則會解密物件並傳回物件資料。

  雖然此功能可管理所有物件加密與解密作業、但您必須管理所提供的加密金鑰。StorageGRID

  您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

  如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

使用**SS**

若要使用StorageGRID 由支援此功能的唯一金鑰來加密物件、請使用下列要求標頭：

```
x-amz-server-side-encryption
```

下列物件作業可支援SSe要求標頭：

- "PuttObject"
- "CopyObject"
- "建立多個部分上傳"

使用**SSE-C**

若要使用您管理的唯一金鑰來加密物件、請使用三個要求標頭：

要求標頭	說明
`x-amz-server-side-encryption-customer-algorithm`	指定加密演算法。標頭值必須是 `AES256`。
`x-amz-server-side-encryption-customer-key`	指定將用於加密或解密物件的加密金鑰。金鑰的值必須是256位元、已編碼的base64。
`x-amz-server-side-encryption-customer-key-MD5`	根據RFC 1321指定加密金鑰的md5摘要、以確保傳輸加密金鑰時不會發生錯誤。md5摘要的值必須是以64編碼的128位元。

下列物件作業可支援SSE-C要求標頭：

- "GetObject"
- "標題物件"
- "PuttObject"
- "CopyObject"
- "建立多個部分上傳"
- "上傳零件"
- "上傳PartCopy"

使用伺服器端加密搭配客戶提供的金鑰（**SSE-C**）時的考量

使用SSE-C之前、請注意下列考量事項：

- 您必須使用https。

> StorageGRID 會拒絕在使用 SSE-C 時透過 http 提出的任何要求。基於安全考量、您應該考慮使用 http 意外傳送的任何金鑰是否遭到入侵。捨棄按鍵、然後視需要旋轉。

- 回應中的ETag不是物件資料的MD5。
- 您必須管理加密金鑰與物件之間的對應關係。不儲存加密金鑰。StorageGRID您必須負責追蹤為每個物件提供的加密金鑰。
- 如果您的儲存區已啟用版本管理功能、則每個物件版本都應該擁有自己的加密金鑰。您負責追蹤每個物件版本所使用的加密金鑰。
- 由於您管理用戶端的加密金鑰、因此也必須管理用戶端上的任何其他安全防護措施、例如金鑰輪替。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。

- 如果為貯體設定了跨網格複寫或 CloudMirror 複寫、您就無法擷取 SSE-C 物件。擷取作業將會失敗。

相關資訊

"Amazon S3 使用者指南：使用伺服器端加密搭配客戶提供的金鑰（ SSE-C ）"

您可以使用 S3 CopyObject 要求來建立已儲存在 S3 中的物件複本。CopyObject 作業與執行 GetObject 之後的 PutObject 相同。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一 PutObject 作業的最大大小 _ 建議 _ 為 5 GiB （ 5 、 368 、 709 、 120 位元組）。如果物件大於 5 GiB 、請改用"多部分上傳"。

單一 PutObject 作業的最大 _ 支援 _ 大小為 5 TiB （ 5 、 497 、 558 、 138 、 880 位元組）。

> 如果您從 StorageGRID 11.6 或更早版本升級、當您嘗試上傳超過 5 GiB 的物件時、會觸發 S3 「將物件大小設得太大」警示。如果您有新的 StorageGRID 11.7 或 11.8 安裝、在這種情況下不會觸發警示。不過、為了符合 AWS S3 標準、未來的 StorageGRID 版本不支援上傳大於 5 GiB 的物件。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

StorageGRID 不會解析或解釋使用者自訂中繼資料鍵名或值中包含的轉義 UTF-8 字元。轉義 UTF-8 字元將被視為 ASCII 字元：

- 如果使用者定義的中繼資料包含轉義的utf-8字元、則要求會成功。
- 如果鍵名或值的解釋值包含不可列印字元，StorageGRID 不會傳回 `x-amz-missing-meta`標頭。

支援的要求標頭

支援下列要求標頭：

- `Content-Type`
- `x-amz-checksum-algorithm`：指定 `CRC32`、 `CRC32C`、 `CRC64NVME`或 `SHA256`

  複製物件時，如果來源物件具有 `checksum`或包含 `x-amz-checksum-algorithm`，則複製的物件具有 FULL_OBJECT Checksum。

  如果來源物件具有 Checksum，但請求中未包含 `x-amz-checksum-algorithm`或使用了不支援的 Checksum 值，則複製的物件將具有與來源物件相同類型的 Checksum。StorageGRID 會忽略無效或不支援的 `x-amz-checksum-algorithm`值。

  如果來源物件沒有 Checksum，或不包含 `x-amz-checksum-algorithm`，或使用了不支援的 Checksum 值，則複製的物件也沒有 Checksum。

如果 CopyObject 請求未指定 Checksum，且來源物件沒有 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對
- `x-amz-metadata-directive`：預設值為 `COPY`，可讓您複製物件及相關的中繼資料。

  您可以指定 `REPLACE`在複製物件時覆寫現有的中繼資料、或是更新物件中繼資料。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：預設值為 `COPY`，可讓您複製物件和所有標籤。

  您可以指定 `REPLACE`在複製物件時覆寫現有的標記、或是更新標記。

- S3物件鎖定要求標頭：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱。 "使用 S3 REST API 來設定 S3 物件鎖定"

- SSe要求標頭：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `If-Match`

  The `If-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- `If-None-Match`

  The `If-None-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-None-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- `x-amz-website-redirect-location`

儲存類別選項

`x-amz-storage-class`如果匹配的 ILM 規則使用雙提交或平衡，則會支持請求標頭link:../ilm/data-protection-options-for-ingest.html["擷取選項"]，並影響 StorageGRID 創建的對象複製數量。

- `STANDARD`

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- `REDUCED_REDUNDANCY`

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

  如果您在啟用 S3 物件鎖定的情況下、將物件擷取至貯體、則會忽略此 `REDUCED_REDUNDANCY`選項。如果您正在將物件擷取至舊版的「符合標準」貯體、`REDUCED_REDUNDANCY`則選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

在 **CopyObject** 中使用 **x-amz-copy-source**

如果在標頭中指定的來源貯體和金鑰與目的地貯體和金鑰不同、則 `x-amz-copy-source`會將來源物件資料的複本寫入目的地。

如果來源和目的地相符，且 `x-amz-metadata-directive`標頭指定為 `REPLACE`，則物件的中繼資料將使用請求中提供的中繼資料值進行更新。在這種情況下，StorageGRID 不會重新擷取物件。這會產生兩個重要後果：

- 您無法使用 CopyObject 來加密現有物件、或變更現有物件的加密。如果您提供 `x-amz-server-side-encryption`標頭或 `x-amz-server-side-encryption-customer-algorithm`標頭、 StorageGRID 會拒絕要求並傳回 `XNotImplemented`。
- 符合的 ILM 規則中指定的「擷取行為」選項不會被使用。由更新觸發的任何物件放置變更，都會在正常的背景 ILM 程序重新評估 ILM 時生效。

  這表示、如果 ILM 規則使用嚴格選項來擷取行為、則無法在無法進行所需物件放置時（例如、因為新要求的位置無法使用）、就不會採取任何行動。更新後的物件會保留其目前的放置位置、直到能夠放置所需的位置為止。

要求伺服器端加密的標頭

如果"使用伺服器端加密"是、您提供的要求標頭取決於來源物件是否已加密、以及您是否打算加密目標物件。

- 如果來源物件是使用客戶提供的金鑰（ SSE-C ）加密、則必須在 CopyObject 要求中包含下列三個標頭、以便將物件解密後再複製：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-copy-source-server-side-encryption-customer-key`：指定創建源對象時提供的加密密鑰。
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的 MD5 摘要。
- 如果您要使用您提供及管理的唯一金鑰來加密目標物件（複本）、請包含下列三個標頭：
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：爲目標對象指定新的加密密鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新加密金鑰的 MD5 摘要。

  > 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱的考量事項"使用伺服器端加密"。

- 如果您要使用由 StorageGRID （ SSE ）管理的唯一金鑰來加密目標物件（複本）、請在 CopyObject 要求中加入此標頭：
  - `x-amz-server-side-encryption`

  > `server-side-encryption`物件的值無法更新。相反，請使用以下命令以新值 `x-amz-metadata-directive`複製副本 `server-side-encryption`： `REPLACE`。

版本管理

如果來源貯體已版本化、您可以使用 `x-amz-copy-source`標頭來複製物件的最新版本。若要複製物件的特定版本、您必須使用 `SubResource` 明確指定要複製的版本 `versionId`。如果目的地貯體已版本化、則會在回應標頭中傳回產生的版本 `x-amz-version-id`。如果目標貯體的版本設定已暫停、則 `x-amz-version-id`會傳回「 null 」值。

您可以使用 S3 GetObject 要求、從 S3 貯體擷取物件。

GetObject 和多部分物件

您可以使用 `partNumber` request 參數擷取多部分或分割物件的特定部分。 `x-amz-mp-parts-count`回應元素會指出物件有多少部分。

您可以針對分割 / 多部分物件和非分割 / 非多部分物件、將其設 `partNumber`為 1 ；不過、 `x-amz-mp-parts-count`只有分割或多部分物件才會傳回回應元素。

使用者中繼資料中的**UTF-8**字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID如果金鑰名稱或值包含不可列印的字元、則取得使用者定義中繼資料中含有轉義式 UTF-8 字元的物件要求時、不會傳回 `x-amz-missing-meta`標頭。

支援的要求標頭

支援下列要求標頭：

- `Accept-Encoding`

  當物件沒有儲存的 `Content-Encoding`時，帶有 `Accept-Encoding: gzip`的 `GET` 請求會對回應進行動態壓縮。只有 `gzip`會影響 `GET` 回應的編碼； `deflate`、 `br`和 `identity`則不會。對於已儲存 `Content-Encoding`的物件，StorageGRID 會傳回儲存的編碼，且不會根據 `Accept-Encoding`套用額外的動態壓縮。StorageGRID 不支援帶有 `Accept-Encoding: gzip`的 GET 請求的範圍讀取操作。

- `x-amz-checksum-mode`：具體說明 `ENABLED`

  > `Range`GetObject 不支援標頭 `x-amz-checksum-mode`。當您在啟用的要求 `x-amz-checksum-mode`中加入 `Range`時、 StorageGRID 不會傳回回應中的 `Checksum` 值。

不支援的要求標頭

不支援下列要求標頭並傳回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本管理

如果 `versionId`未指定子資源、則作業會擷取版本控制庫中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態、回應標頭會 `x-amz-delete-marker`設為 `true`。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件是以您提供的唯一金鑰加密、請使用所有三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定對象的加密密鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定對象加密密鑰的 MD5 摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱中的考量事項"使用伺服器端加密"。

GetObject for Cloud Storage Pool 物件的行為

如果物件已儲存在"雲端儲存資源池"中、 GetObject 要求的行為將取決於物件的狀態。如需詳細資訊、請參閱"標題物件"。

> 如果某個物件儲存在雲端儲存池中、且該物件的一個或多個複本也存在於網格上、則 GetObject 要求會嘗試從網格擷取資料、然後再從雲端儲存池擷取資料。

物件狀態	**GetObject** 的行為
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK` 系統會擷取物件複本。
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK` 系統會擷取物件複本。
物件移轉至無法擷取的狀態	`403 Forbidden`、 `InvalidObjectState` 使用"RestoreObject"要求將物件還原至可擷取的狀態。
正在從無法擷取的狀態還原的物件	`403 Forbidden`、 `InvalidObjectState` 等待 RestoreObject 要求完成。
物件已完全還原至雲端儲存資源池	`200 OK` 系統會擷取物件複本。

雲端儲存資源池中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、當物件的某些部分已經轉換為無法擷取的狀態、或物件的某些部分尚未還原時、 GetObject 要求可能會錯誤傳回 `200 OK`。

在這些情況下：

- GetObject 要求可能會傳回一些資料、但中途停止傳輸。

- 隨後的 GetObject 要求可能會傳回 `403 Forbidden`。

GetObject 和跨網格複寫

如果您正在使用"網格同盟"並"跨網格複寫"已啟用貯體、則 S3 用戶端可藉由發出 GetObject 要求來驗證物件的複寫狀態。回應包含 StorageGRID 專屬回應標頭、其中包含 `x-ntap-sg-cgr-replication-status`下列其中一個值：

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

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

使用 **S3 HeadObject** 請求從 **StorageGRID** 中的物件擷取中繼資料

您可以使用 S3 HeadObject 要求、從物件擷取中繼資料、而無需傳回物件本身。如果物件儲存在雲端儲存池中、您可以使用 HeadObject 來判斷物件的轉換狀態。

HeadObject 和多個零件物件

您可以使用 `partNumber` request 參數擷取多部分或分割物件特定部分的中繼資料。 `x-amz-mp-parts-count`回應元素會指出物件有多少部分。

您可以針對分割 / 多部分物件和非分割 / 非多部分物件、將其設 `partNumber`為 1 ；不過、 `x-amz-mp-parts-count`只有分割或多部分物件才會傳回回應元素。

使用者中繼資料中的UTF-8字元

在使用者定義的中繼資料中、無法剖析或解譯轉義的utf-8字元。StorageGRID如果金鑰名稱或值包含不可列印的字元、則使用者定義中繼資料中的轉義式 UTF-8 字元之物件的標頭要求不會傳回 `x-amz-missing-meta`標頭。

支援的要求標頭

支援下列要求標頭：

- `x-amz-checksum-mode`

> `partNumber`HeadObject 不支援參數和 `Range`標頭 `x-amz-checksum-mode`。當您在啟用的要求中加入這些項目 `x-amz-checksum-mode`時、 StorageGRID 不會傳回回應中的 `Checksum` 值。

不支援的要求標頭

不支援下列要求標頭並傳回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本管理

如果 `versionId`未指定子資源、則作業會擷取版本控制庫中物件的最新版本。如果物件的目前版本是刪除標記、則會傳回「找不到」狀態、回應標頭會 `x-amz-delete-marker`設為 `true`。

使用客戶提供的加密金鑰（**SSE-C**）要求伺服器端加密標頭

如果物件使用您提供的唯一金鑰加密、請使用這三個標頭。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定對象的加密密鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定對象加密密鑰的 MD5 摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱中的考量事項"使用伺服器端加密"。

Cloud Storage Pool 物件的 **HeadObject** 回應

如果物件儲存在"雲端儲存資源池"中、則會傳回下列回應標頭：

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

回應標頭會提供物件移至雲端儲存集區時的狀態資訊、並選擇性地移轉至無法擷取的狀態、然後還原。

物件狀態	對 **HeadObject** 的回應
物件擷取到StorageGRID 不經ILM評估、或儲存在傳統儲存資源池中的物件、或使用銷毀編碼	`200 OK`（不會傳回任何特殊回應標頭。）

Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	在物件轉換為無法擷取的狀態之前、的值 `expiry-date`會設定為未來的某段時間。確切的轉換時間不受StorageGRID 此功能的控制。

物件狀態	對 **HeadObject** 的回應

物件已轉換為無法擷取的狀態、但網格上至少也有一個複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	的值 `expiry-date`設定為未來的某段時間。
	
	• 注意 * ：如果網格上的複本無法使用（例如儲存節點停機）、您必須發出"RestoreObject"要求、要求從雲端儲存池還原複本、才能成功擷取物件。

物件移轉至無法擷取的狀態、而且網格上不存在複本	`200 OK`
	
	`x-amz-storage-class: GLACIER`

正在從無法擷取的狀態還原的物件	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

物件已完全還原至雲端儲存資源池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	`expiry-date`表示何時會將 `Cloud Storage Pool` 中的物件恢復為不可擷取的狀態。

Cloud Storage Pool中的多部份或分段物件

如果您上傳了多個部分的物件、或StorageGRID 是將一個大型物件分割成多個區段、StorageGRID 則透過取樣物件的一部分或區段、決定該物件是否可在Cloud Storage Pool中使用。在某些情況下、當物件的某些部分已經轉換為無法擷取的狀態、或物件的某些部分尚未還原時、 HeadObject 要求可能會錯誤傳回 `x-amz-restore: ongoing-request="false"`。

HeadObject 和跨網格複寫

如果您正在使用"網格同盟"並"跨網格複寫"已啟用貯體、則 S3 用戶端可以發出 HeadObject 要求、以驗證物件的

複寫狀態。回應包含 StorageGRID 專屬回應標頭、其中包含 `x-ntap-sg-cgr-replication-status`下列其中一個值：

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

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

使用 **S3 PutObject** 請求將物件新增至 **StorageGRID** 中的儲存區

您可以使用 S3 PuttObject 要求、將物件新增至貯體。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

物件大小

單一 PutObject 作業的最大大小 _ 建議 _ 為 5 GiB （ 5 、 368 、 709 、 120 位元組）。如果物件大於 5 GiB 、請改用"多部分上傳"。

單一 PutObject 作業的最大 _ 支援 _ 大小為 5 TiB （ 5 、 497 、 558 、 138 、 880 位元組）。

如果您從 StorageGRID 11.6 或更早版本升級、當您嘗試上傳超過 5 GiB 的物件時、會觸發 S3 「將物件大小設得太大」警示。如果您有新的 StorageGRID 11.7 或 11.8 安裝、在這種情況下不會觸發警示。不過、為了符合 AWS S3 標準、未來的 StorageGRID 版本不支援上傳大於 5 GiB 的物件。

使用者中繼資料大小

Amazon S3會將每個PUT要求標頭內使用者定義的中繼資料大小限制為2 KB。支援範圍將使用者中繼資料限制為24 KiB。StorageGRID使用者定義的中繼資料大小是以每個金鑰和值的utf-8編碼方式、計算出位元組數的總和。

使用者中繼資料中的**UTF-8**字元

如果要求在使用者定義的中繼資料金鑰名稱或值中包含（未轉義）utf-8值、StorageGRID 則無法定義任何不正常的行為。

不剖析或解譯使用者定義之中繼資料的金鑰名稱或值中包含的轉義式utf-8字元。StorageGRID轉義的UTF-8字元會視為Ascii字元：

- 如果使用者定義的中繼資料包含轉義式 UTF-8 字元、則 PutObject 、 CopyObject 、 GetObject 和

HeadObject 要求會成功。

- 如果金鑰名稱或值的解譯值包含不可列印字元、則 StorageGRID 不會傳回 `x-amz-missing-meta`標頭。

物件標籤限制

您可以在上傳新物件時新增標記、也可以將標記新增至現有物件。每個物件最多可支援10個標記的支援功能。StorageGRID與物件相關聯的標記必須具有唯一的標記金鑰。標籤金鑰長度最多可達128個UNICODE字元、標籤值長度最多可達256個UNICODE字元。金鑰和值區分大小寫。

物件擁有權

在功能區中StorageGRID 、所有物件均歸庫位擁有者帳戶所有、包括非擁有者帳戶或匿名使用者所建立的物件。

支援的要求標頭

支援下列要求標頭：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  當您指定 `aws-chunked`for `Content-Encoding`時，StorageGRID 不會驗證下列項目：

  - StorageGRID 不會針對資料區塊驗證 `chunk-signature`。
  - StorageGRID 不會驗證您提供的值 `x-amz-decoded-content-length`是否與物件相符。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  如果同時使用有效負載簽署、則支援分區傳輸編碼 `aws-chunked`。

- Checksum 請求標頭：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

> ⓘ 如果 PutObject 請求未指定 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。

- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對。

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

  ```
  x-amz-meta-name: value
  ```

  如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須使用 `creation-time`做為物件建立時所記錄的中繼資料名稱。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  的值 `creation-time`會從 1970 年 1 月 1 日起計算為秒數。

  > ILM 規則不能同時使用 * 使用者定義的建立時間 * 作為參考時間、也不能同時使用平衡或嚴格擷取選項。建立ILM規則時會傳回錯誤。

- `x-amz-tagging`
- S3物件鎖定要求標頭
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果要求是在沒有這些標頭的情況下提出、則貯體預設保留設定會用於計算物件版本模式並保留至最新日期。請參閱。 "使用 S3 REST API 來設定 S3 物件鎖定"

- SSe要求標頭：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    請參閱 [要求伺服器端加密的標頭]

不支援的要求標頭

不支援下列要求標頭：

- `If-Match`

  The `If-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- If-None-Match

  The `If-None-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-None-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- x-amz-acl
- x-amz-checksum-md5
- x-amz-checksum-sha1
- x-amz-checksum-sha512
- x-amz-checksum-xxhash3
- x-amz-checksum-xxhash64
- x-amz-checksum-xxhash128
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

  `x-amz-website-redirect-location`報頭返回 `XNotImplemented`。

儲存類別選項

`x-amz-storage-class`支援要求標頭。提交的值 `x-amz-storage-class`會影響 StorageGRID 在擷取期間保護物件資料的方式、而不會影響儲存在 StorageGRID 系統中的物件持續複本數量（由 ILM 決定）。

如果符合擷取物件的 ILM 規則使用嚴格擷取選項、則 `x-amz-storage-class`標頭不會生效。

下列值可用於 x-amz-storage-class：

- STANDARD（預設）
  - 雙重提交：如果ILM規則指定「內嵌行為」的「雙重提交」選項、則只要物件擷取到另一個物件複本、就會建立該物件的第二個複本、並將其分散到不同的儲存節點（雙重提交）。評估 ILM 時、 StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、 StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

    如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件複本（同步放置）、則 `x-amz-storage-class`標頭不會生效。

- REDUCED_REDUNDANCY

- 雙重提交：如果ILM規則指定擷取行為的雙重提交選項、StorageGRID 則會在擷取物件時建立單一的過渡複本（單一提交）。
- *Balanced * ：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID `REDUCED_REDUNDANCY`當符合物件的 ILM 規則建立單一複寫複本時、最好使用此選項。在這種情況下、使用 `REDUCED_REDUNDANCY`可避免在每次擷取作業中不必要地建立和刪除額外的物件複本。

在其他情況下不建議使用此 `REDUCED_REDUNDANCY`選項。 `REDUCED_REDUNDANCY`增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

> 在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 `REDUCED_REDUNDANCY`僅會影響首次擷取物件時所建立的複本數量。它不會影響使用中 ILM 原則評估物件時所製作的物件複本數量、也不會導致資料儲存在 StorageGRID 系統中較低的備援層級。

> 如果您在啟用 S3 物件鎖定的情況下、將物件擷取至貯體、則會忽略此 `REDUCED_REDUNDANCY`選項。如果您正在將物件擷取至舊版的「符合標準」貯體、 `REDUCED_REDUNDANCY`則選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密物件。「SSE」和「SSE-C」選項互不相關。

- * SSE-*：如果您想使用StorageGRID 由支援的唯一金鑰來加密物件、請使用下列標頭。
  - `x-amz-server-side-encryption`

    如果 `x-amz-server-side-encryption` PuttObject 要求中未包含標頭、則 PuttObject 回應中會省略網格範圍"儲存的物件加密設定"。
- * SSE-C*：如果您想使用您提供及管理的唯一金鑰來加密物件、請使用這三個標頭。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的 MD5 摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱的考量事項"使用伺服器端加密"。

> 如果物件是以SSE或SSE-C加密、則會忽略任何儲存區層級或網格層級的加密設定。

版本管理

如果已啟用貯體的版本設定功能、則會針對儲存的物件版本自動產生唯一的 `versionId`版本。這

`versionId`也會在回應中使用回應標頭傳回 `x-amz-version-id。

如果版本控制暫停、物件版本會以 null 儲存 versionId、如果空版本已經存在、則會覆寫該版本。

授權標頭的簽名計算

使用 `Authorization`標頭驗證要求時、 StorageGRID 與 AWS 的差異如下：

- StorageGRID 不需要 host`在中包含標頭 `CanonicalHeaders。
- StorageGRID 不需要 `Content-Type`包含在 `CanonicalHeaders`中。
- StorageGRID 不需要 x-amz-*`在中包含標頭 `CanonicalHeaders。

> 一般最佳實務做法是、務必在中加入這些標頭 CanonicalHeaders、以確保其已通過驗證；不過、如果您排除這些標頭、 StorageGRID 不會傳回錯誤。

如需詳細資訊、請 "授權標頭的簽名計算：在單一區塊中傳輸有效負載（AWS 簽名版本 4）"參閱。

相關資訊

- "使用ILM管理物件"
- "Amazon Simple Storage Service API 參考資料： PutObject"

使用 **S3 RestoreObject** 請求在 **StorageGRID** 中還原物件

您可以使用 S3 RestoreObject 要求來還原儲存在雲端儲存池中的物件。

支援的要求類型

StorageGRID 僅支援還原物件的 RestoreObject 要求。它不支援 SELECT`還原類型。選擇要求退貨 `XNotImplemented。

版本管理

您也可以選擇指定 versionId`還原版本控制儲存區中物件的特定版本。如果未指定 `versionId，則會還原物件的最新版本

Cloud Storage Pool 物件上的 **RestoreObject** 行為

如果對象已儲存"雲端儲存資源池"在中，則根據對象的狀態， RestoreObject 請求具有以下行爲。如需詳細資訊、請參閱"標題物件"。

> 如果物件儲存在雲端儲存池中、且網格上也有一個或多個物件複本、則無需透過發出 RestoreObject 要求來還原物件。而是可以使用 GetObject 要求直接擷取本機複本。

物件狀態	**RestoreObject** 的行為
物件擷取至StorageGRID 不受ILM評估、或物件不在雲端儲存資源池中	403 Forbidden、 InvalidObjectState

物件狀態	**RestoreObject** 的行為
Cloud Storage Pool中的物件、但尚未轉換為無法擷取的狀態	`200 OK`不做任何變更。 • 注意 * ：在物件轉換為不可擷取的狀態之前、您無法變更其 `expiry-date`。
物件移轉至無法擷取的狀態	`202 Accepted`將物件的可擷取複本還原至 Cloud Storage Pool 、直到在要求本文中指定的天數。在此期間結束時、物件會返回無法擷取的狀態。 （可選）使用 `Tier` request 元素來確定恢復作業完成(`Expedited`、`Standard`或所 `Bulk`需的時間。如果未指定 `Tier`，則使用該 `Standard`層。 重要事項：如果物件已移轉至 S3 Glacier Deep Archive 或雲端儲存池使用 Azure Blob Storage，則無法使用 `Expedited`分層還原物件。系統將傳回下列錯誤 `403 Forbidden，InvalidTier：Retrieval option is not supported by this storage class`。
正在從無法擷取的狀態還原的物件	`409 Conflict`、`RestoreAlreadyInProgress`
物件已完全還原至雲端儲存資源池	`200 OK` • 注意：* 如果物件已還原為可擷取的狀態、您可以重新核發具有新值的 RestoreObject 要求來變更 `expiry-date`物件 `Days`。還原日期會根據申請時間而更新。

使用 **S3 SelectObjectContent** 請求在 **StorageGRID** 中篩選物件資料

您可以使用S3 SelectObjectContent要求、根據簡單的SQL陳述來篩選S3物件的內容。

如需更多資訊、請參閱 "Amazon Simple Storage Service API 參考資料： SelectObjectContent"。

開始之前

- 租戶帳戶具有S3 Select權限。
- 您有 `s3:GetObject`查詢物件的權限。
- 您要查詢的物件必須採用下列其中一種格式：
  - * CSV* 。可依原樣使用、也可壓縮至 GZIP 或 bzip2 歸檔。
  - * 硬地板 * 。硬地板物件的其他需求：
    - S3 Select 僅支援使用 GZIP 或 Snappy 進行柱式壓縮。S3 Select 不支援 Parquet 物件的全物件壓縮。
    - S3 Select 不支援硬地板輸出。您必須將輸出格式指定為 CSV 或 JSON 。
    - 最大未壓縮列群組大小為 512 MB 。
    - 您必須使用物件架構中指定的資料類型。
    - 您無法使用時間間隔、 JSON 、清單、時間或 UUID 邏輯類型。

- SQL運算式的最大長度為256 KB。
- 輸入或結果中的任何記錄最大長度為1個mib。

CSV 要求語法範例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

拼花地板要求語法範例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL查詢範例

此查詢會取得州名、2010年人口、2015年估計人口、以及美國統計資料的變更百分比。檔案中非狀態的記錄會被忽略。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

要查詢的檔案的前幾行 `SUB-EST2020_ALL.csv`、如下所示：

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI 使用範例（ CSV ）

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

輸出文件的前幾行 `changes.csv`如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS-CLI 使用範例（ Parquet ）

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

輸出檔案的前幾行： changes .csv 、如下所示：

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

多部份上傳作業

StorageGRID 中支援的多部分上傳作業

本節說明StorageGRID 此功能如何支援多部份上傳作業。

下列條件與附註適用於所有多重部分上傳作業：

- 您不應超過 1 、 000 次同時上傳多個部分至單一儲存庫、因為該儲存庫的 ListMultipartuploADS 查詢結果可能會傳回不完整的結果。
- 針對多個零件執行AWS大小限制。StorageGRIDS3用戶端必須遵循下列準則：
  - 多部份上傳的每個部分必須介於5個mib（5、242,880位元組）和5 GiB（5、368,709,120位元組）之間。
  - 最後一部分可小於5個mib（5、242,880位元組）。
  - 一般而言、零件尺寸應盡量大。例如、對於100 GiB物件使用5 GiB的零件大小。因為每個零件都被視為唯一的物件、所以使用較大的零件大小可降低 StorageGRID 中繼資料的負荷。
  - 對於小於5 GiB的物件、請考慮改用非多部份上傳。
- 如果 ILM 規則使用平衡或嚴格"擷取選項"、則會在擷取時評估多部分物件的每個部分、以及在多部分上傳完成時評估整個物件的 ILM 。您應該瞭解這會如何影響物件和零件放置：
  - 如果在 S3 多部分上傳進行期間 ILM 有所變更、則當多部分上傳完成時、物件的某些部分可能不符合目前的 ILM 需求。未正確放置的任何零件都會排入 ILM 重新評估的佇列、稍後移至正確位置。
  - 評估零件的ILM時StorageGRID 、會根據零件大小而非物件大小來篩選。這表示物件的部分可以儲存在不符合整體物件 ILM 需求的位置。例如、如果規則指定所有 10 GB 或更大的物件都儲存在 DC1 、而所有較小的物件都儲存在 DC2 、則 10 部分多部分上傳的每 1 GB 部分都會儲存在 DC2 的擷取位置。不過、評估整體物件的 ILM 時、物件的所有部分都會移至 DC1 。

- 所有分段上傳操作都支援StorageGRID"一致性值" 。
- 當使用多部分上傳擷取物件時、"物件分割臨界值（ 1 GiB ）"不會套用。
- 視需要、您可以使用"伺服器端加密"多部分上傳。若要使用 SSE （伺服器端加密搭配 StorageGRID 託管金鑰）、請僅在 CreateMultpartUpload 要求中加入 `x-amz-server-side-encryption`要求標頭。若要使用 SSE-C （伺服器端加密搭配客戶提供的金鑰）、您可以在 CreateMultpartUpload 要求和每個後續的 UploPart 要求中指定相同的三個加密金鑰要求標頭。
- 多部分上傳物件是否包含在 "分支桶" 中，取決於發起擷取的時間和分支儲存桶的時間篩選器：
  - 之前。如果擷取是在分支儲存桶的 *Before* 時間戳記之前啟動，則無論上傳何時完成，都會包含多部分上傳的物件。
  - 之後。如果擷取是在分支儲存桶的 *After* 時間戳記之後發起的，則會包含多部分上傳的物件。
  - *介於*之間。如果擷取是在分支儲存桶的 *From* 和 *To* 時間戳記之間啟動，則無論上傳何時完成，都會包含多部分上傳的物件。
  - 排除。如果擷取是在分支儲存桶的 *Exclude from* 時間之前或 *Exclude to* 時間之後發起的，則多部分上傳的物件將包含在內。

營運	實作
AbortMultiPart上 傳	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
完成多個部分上傳	請參閱 "完成多個部分上傳"
建立多個部分上傳 （先前命名的「 Initiate Multifart Upload 」	請參閱 "建立多個部分上傳"
ListMultipartUploads	請參閱 "ListMultipartUploads"
清單零件	以所有Amazon S3 REST API行為來實作。如有變更、恕不另行通知。
上傳零件	請參閱 "上傳零件"
上傳PartCopy	請參閱 "上傳PartCopy"

StorageGRID S3 REST API 如何完成多部分上傳

「 CompleteMultpartUpload 」（ CompleteMultpartupload ）作業可組合先前上傳的零件、完成物件的多部分上傳。

> StorageGRID 透過 CompleteMultpartUpload 以遞增順序支援要求參數的非連續值 `partNumber`。此參數可以從任何值開始。

解決衝突

衝突的用戶端要求（例如兩個寫入同一個金鑰的用戶端）會以「最新致勝」的方式解決。「最新致勝」評估的時間取決於StorageGRID 何時由VMware系統完成指定的要求、而非S3用戶端開始作業的時間。

支援的要求標頭

支援下列要求標頭：

- Checksum 請求標頭：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`
  - `x-amz-checksum-type`

> 如果 CreateMultipartUpload 請求未指定 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。

- `x-amz-storage-class`

> `x-amz-storage-class`如果相符的 `ILM` 規則指定，則標頭會影響 `StorageGRID` 建立的物件複本數量`link:../ilm/data-protection-options-for-ingest.html["雙重認可或平衡擷取選項"]`。

- `STANDARD`

  （預設）當ILM規則使用雙重提交選項、或平衡選項回到建立臨時複本時、指定雙重提交擷取作業。

- `REDUCED_REDUNDANCY`

  當ILM規則使用雙重提交選項、或平衡選項回到建立過渡複本時、指定單一提交擷取作業。

> 如果您在啟用 S3 物件鎖定的情況下、將物件擷取至貯體、則會忽略此 `REDUCED_REDUNDANCY`選項。如果您正在將物件擷取至舊版的「符合標準」貯體、`REDUCED_REDUNDANCY`則選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

> 如果多部分上傳未在15天內完成、則該作業會標示為非作用中、且所有相關資料都會從系統中刪除。

> `ETag`傳回的值不是資料的 MD5 總和、而是依照 Amazon S3 API 實作的 `ETag`多部分物件值。

不支援的要求標頭

不支援下列要求標頭：

- `If-Match`

  The `If-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- `If-None-Match`

  The `If-None-Match`標頭的行為會根據您的 StorageGRID 組態而有所不同。提供此標頭可能會傳回錯誤訊息（501 Not Implemented）。如果 `If-None-Match`標頭被接受但無法運作，則可能會觸發警示，其中包含有關啟用更嚴格的 501 Not Implemented 錯誤行為的說明。

- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

版本管理

此作業會完成多部份上傳。如果已啟用貯體的版本設定功能、則物件版本會在完成多重部分上傳後建立。

如果已啟用貯體的版本設定功能、則會針對儲存的物件版本自動產生唯一的 `versionId`版本。這 `versionId`也會在回應中使用回應標頭傳回 `x-amz-version-id`。

如果版本控制暫停、物件版本會以 null 儲存 `versionId`、如果空版本已經存在、則會覆寫該版本。

> 當某個儲存區啟用版本管理時、完成多部份上傳會一律建立新版本、即使在同一個物件金鑰上同時完成多部份上傳也一樣。如果未針對某個儲存區啟用版本管理、則可以啟動多重部分上傳、然後在同一個物件金鑰上啟動並完成另一個多重部分上傳。在非版本的儲存區上、完成最後一次的多部分上傳優先。

複寫失敗、通知或中繼資料通知

如果平台服務已設定多重零件上傳的儲存區、即使相關的複寫或通知動作失敗、多重零件上傳仍會成功。

租戶可透過更新物件的中繼資料或標記來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。

請參閱 "疑難排解平台服務"。

StorageGRID 中的 S3 CreateMultipartUpload 請求標頭和選項

CreateMultpartupload （先前命名為「 Initiate Multifart Upload 」（起始多重部分上傳）

）作業會啟動物件的多重部分上傳、並傳回上傳 ID 。

`x-amz-storage-class`支援要求標頭。提交的值 `x-amz-storage-class`會影響 StorageGRID 在擷取期間保護物件資料的方式、而不會影響儲存在 StorageGRID 系統中的物件持續複本數量（由 ILM 決定）。

如果匹配已擷取物件的 ILM 規則使用 Strict "擷取選項"、則 `x-amz-storage-class`標頭不會生效。

下列值可用於 x-amz-storage-class：

- STANDARD（預設）
  - * 雙重認可 * ：如果 ILM 規則指定「雙重認可擷取」選項、則只要物件擷取第二個物件複本、就會建立並發佈至不同的儲存節點（雙重認可）。評估 ILM 時、 StorageGRID 會判斷這些初始過渡複本是否符合規則中的放置指示。如果沒有、則可能需要在不同位置製作新的物件複本、而且可能需要刪除初始過渡複本。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、而 StorageGRID 無法立即製作規則中指定的所有複本、 StorageGRID 會在不同的儲存節點上製作兩個臨時複本。

    如果 StorageGRID 可以立即建立 ILM 規則中指定的所有物件複本（同步放置）、則 `x-amz-storage-class`標頭不會生效。
- REDUCED_REDUNDANCY
  - * 雙重認可 * ：如果 ILM 規則指定雙重認可選項、 StorageGRID 會在擷取物件時（單一認可）建立單一的臨時複本。
  - *Balanced * ：如果 ILM 規則指定 Balanced 選項、則 StorageGRID 只會在系統無法立即製作規則中指定的所有複本時、才製作單一的臨時複本。如果能夠執行同步放置、則此標頭不會有任何影響。StorageGRID `REDUCED_REDUNDANCY`當符合物件的 ILM 規則建立單一複寫複本時、最好使用此選項。在這種情況下、使用 `REDUCED_REDUNDANCY`可避免在每次擷取作業中不必要地建立和刪除額外的物件複本。

  在其他情況下不建議使用此 `REDUCED_REDUNDANCY`選項。 `REDUCED_REDUNDANCY`增加擷取期間物件資料遺失的風險。例如、如果單一複本一開始儲存在無法進行ILM評估的儲存節點上、則可能會遺失資料。

> 在任何時間段只複寫一個複本、會使資料面臨永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

指定 `REDUCED_REDUNDANCY`僅會影響首次擷取物件時所建立的複本數量。它不會影響使用中 ILM 原則評估物件時所製作的物件複本數量、也不會導致資料儲存在 StorageGRID 系統中較低的備援層級。

> 如果您在啟用 S3 物件鎖定的情況下、將物件擷取至貯體、則會忽略此 `REDUCED_REDUNDANCY`選項。如果您正在將物件擷取至舊版的「符合標準」貯體、 `REDUCED_REDUNDANCY`則選項會傳回錯誤。執行「雙重承諾」的程序時、務必確保符合法規遵循要求。StorageGRID

支援的要求標頭

支援下列要求標頭：

- `Content-Type`
- `x-amz-checksum-algorithm`：指定 `CRC32`、 `CRC32C`、 `CRC64NVME`或 `SHA256`

> 如果 CreateMultipartUpload 請求未指定 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。StorageGRID 會忽略無效或不支援的 `x-amz-checksum-algorithm`值。

- `x-amz-checksum-type`
- `x-amz-meta-`，然後是包含使用者定義中繼資料的名稱值配對

  為使用者定義的中繼資料指定名稱值配對時、請使用以下一般格式：

  ```
  x-amz-meta-_name_: `value`
  ```

  如果您要使用 * 使用者定義的建立時間 * 選項做為 ILM 規則的參考時間、則必須使用 `creation-time`做為物件建立時所記錄的中繼資料名稱。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  的值 `creation-time`會從 1970 年 1 月 1 日起計算為秒數。

> 如果您要將物件新增至已啟用舊版規範的儲存區、則不允許新增 `creation-time`為使用者定義的中繼資料。將傳回錯誤。

- S3物件鎖定要求標頭：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果提出的要求沒有這些標頭、則會使用儲存庫預設保留設定來計算物件版本的保留日期。

  "使用 S3 REST API 來設定 S3 物件鎖定"

- SSe要求標頭：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

[要求伺服器端加密的標頭]

有關 StorageGRID 如何處理 UTF-8 字元的資訊、請參閱"PuttObject"。

要求伺服器端加密的標頭

您可以使用下列要求標頭、以伺服器端加密來加密多部份物件。「SSE」和「SSE-C」選項互不相關。

- *SSE * ：如果您想使用由 StorageGRID 管理的唯一金鑰來加密物件、請在 CreateMultpartUpload 要求中使用下列標頭。請勿在任何上傳組件要求中指定此標頭。
  - `x-amz-server-side-encryption`
- **SSE-C** ：如果您想要使用您提供和管理的唯一金鑰來加密物件、請在 CreateMultpartUpload 要求（以及每個後續的 UploadPart 要求）中使用這三個標頭。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新物件的加密金鑰。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新對象加密密鑰的 MD5 摘要。

您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱的考量事項"使用伺服器端加密"。

不支援的要求標頭

不支援下列要求標頭：

- `x-amz-website-redirect-location`

  `x-amz-website-redirect-location`報頭返回 `XNotImplemented`。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「 CompleteMultpartUpload 」（ CompleteMultpartUpload ）作業時、即會建立物件（並在適用的情況下進行版本控制）。

S3 ListMultipartUploads 操作和 **StorageGRID** 中支援的參數

ListMultipartuploADS 作業會列出某個儲存庫的進行中多個部分上傳。

支援下列要求參數：

- `encoding-type`
- `key-marker`
- `max-uploads`

- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「 CompleteMultpartUpload 」（ CompleteMultpartUpload ）作業時、即會建立物件（並在適用的情況下進行版本控制）。

StorageGRID 中 S3 UploadPart 作業支援和不支援的要求標頭

上傳 Part 作業會上傳物件的多部分上傳中的某個零件。

支援的要求標頭

支援下列要求標頭：

- Checksum 請求標頭：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

  如果您在 CreateMultipartUpload 請求期間指定了 CRC-32、CRC-32C、CRC-64/NVME 或 SHA-256 Checksum，則也必須在每個 UploadPart 請求中包含 Checksum 請求標頭。

  > 如果 CreateMultipartUpload 請求未指定 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。

- `Content-Length`
- `Content-MD5`

要求伺服器端加密的標頭

如果您為 CreateMultpartUpload 要求指定了 SSE-C 加密、則每個 UploadPart 要求中也必須包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定您在 CreateMultpartUpload 要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 CreateMultpartUpload 要求中提供的相同 MD5 摘要。

您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱中的考量事項"使用伺服器端加密"。

不支援的要求標頭

不支援下列要求標頭：

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「 CompleteMultpartUpload 」（ CompleteMultpartUpload ）作業時、即會建立物件（並在適用的情況下進行版本控制）。

使用 **S3 UploadPartCopy** 操作將物件的一部分上傳到 **StorageGRID**

上傳 PartCopy 作業會將現有物件的資料複製為資料來源、以上傳物件的一部分。

所有 Amazon S3 REST API 行為都會實作上傳 PartCopy 作業。如有變更、恕不另行通知。

此要求會讀寫 StorageGRID 系統內指定的物件資料 `x-amz-copy-source-range`。

支援的要求標頭

支援下列要求標頭：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

要求伺服器端加密的標頭

如果您為 CreateMultpartUpload 要求指定了 SSE-C 加密、則每個 UploadPartCopy 要求中也必須包含下列要求標頭：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。

- `x-amz-server-side-encryption-customer-key`：指定您在 CreateMultpartUpload 要求中提供的相同加密金鑰。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 CreateMultpartUpload 要求中提供的相同 MD5 摘要。

如果來源物件是使用客戶提供的金鑰（ SSE-C ）加密、則必須在上傳 PartCopy 要求中包含下列三個標頭、以便將物件解密後再複製：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定創建源對象時提供的加密密鑰。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在創建源對象時提供的 MD5 摘要。

> 您提供的加密金鑰永遠不會儲存。如果您遺失加密金鑰、就會遺失對應的物件。在使用客戶提供的金鑰來保護物件資料之前，請先檢閱中的考量事項"使用伺服器端加密"。

版本管理

多部分上傳包含不同的作業、可用於初始化上傳、列出上傳內容、上傳零件、組裝上傳的零件、以及完成上傳。執行「 CompleteMultpartUpload 」（ CompleteMultpartUpload ）作業時、即會建立物件（並在適用的情況下進行版本控制）。

S3 Checksum 支援

StorageGRID 會自動偵測 CreateMultipartUpload 請求中是否指定了 Checksum，並在 UploadPartCopy 操作中使用此 Checksum。您無需在 UploadPartCopy 請求中指定 Checksum。如果 CreateMultipartUpload 請求未指定 Checksum，StorageGRID 不會為物件計算預設的 CRC-64/NVME Checksum。當 CreateMultipartUpload 未指定 Checksum 時，StorageGRID 不會為複製的部分包含 Checksum。

StorageGRID S3 REST API 錯誤回應

支援所有適用的標準S3 REST API錯誤回應。StorageGRID此外、此功能還會加入數個自訂回應。StorageGRID

支援的**S3 API**錯誤代碼

名稱	**HTTP** 狀態
ACCESSDENIED	403禁止
《標誌摘要》	400個錯誤要求
BuckketAlreadyEx分子	衝突
BucketNotEmpty	衝突

名稱	**HTTP** 狀態
不完整正文	400個錯誤要求
內部錯誤	500內部伺服器錯誤
InvalidAccessKeyId	403禁止
InvalidArgument	400個錯誤要求
InvalidBucketName	400個錯誤要求
InvalidBucketState	衝突
InvalidDigest	400個錯誤要求
InvalidEncryptionAlgorithm錯誤	400個錯誤要求
InvalidPart	400個錯誤要求
InvalidPartOrder	400個錯誤要求
InvalidRang	無法滿足416個要求的範圍
InvalidRequest	400個錯誤要求
InvalidStorageClass	400個錯誤要求
InvalidTag	400個錯誤要求
InvalidURI	400個錯誤要求
KeyTooLong	400個錯誤要求
MalformedXML	400個錯誤要求
Metadata TooLarg	400個錯誤要求
方法未允許	不允許使用405方法
內容長度	需要411長度
MissingRequestBodyError	400個錯誤要求

名稱	**HTTP** 狀態
MISingSecurityHeader	400個錯誤要求
NoSuchBucket	找不到404
NoSuchKey	找不到404
NoSuchUpload	找不到404
未實作	501未實作
NoSuchBucketPolicy	找不到404
ObjectLockConfiguration未找到錯誤	找不到404
預先條件失敗	412先決條件失敗
要求時間TooSkewed	403禁止
服務無法使用	503服務無法使用
簽名DoesNotMatch	403禁止
TooManyboo	400個錯誤要求
使用者KeyMustBeSpecified	400個錯誤要求

零點自訂錯誤代碼**StorageGRID**

名稱	說明	**HTTP** 狀態
XBucketLifecycleNotSupported	不允許在符合舊版規範的儲存庫中進行貯體生命週期組態	400個錯誤要求
XBucketPolicyParseException	無法剖析收到的儲存區原則Json。	400個錯誤要求
XComplianceConflict	因為舊版規範設定而拒絕作業。	403禁止
XComplianceReducedRedundancyForbidd	舊型符合標準的儲存區不允許減少備援	400個錯誤要求
XMaxBucketPolicyLengthExceed	您的原則超過允許的儲存區原則長度上限。	400個錯誤要求

名稱	說明	HTTP 狀態
XMissingInternalRequestHeader	缺少內部要求的標頭。	400個錯誤要求
XNoSuchBucketCompliance	指定的儲存庫未啟用舊版法規遵循。	找不到404
XNotAcceptable	要求包含一或多個無法滿足的Accept標頭。	無法接受的406
XNotImplemed	您提供的要求暗示功能尚未實作。	501未實作

StorageGRID 自訂作業

StorageGRID 中支援的自訂儲存貯體作業

StorageGRID 系統支援新增至 S3 REST API 的自訂作業。

下表列出 StorageGRID 支援的自訂作業。

營運	說明
"取得庫位一致性"	傳回套用至特定儲存區的一致性。
"實現庫位一致性"	設定套用至特定貯體的一致性。
"取得時段上次存取時間"	傳回是否為特定儲存區啟用或停用上次存取時間更新。
"將資源桶放在最後存取時間"	可讓您啟用或停用特定儲存區的上次存取時間更新。
"刪除時段中繼資料通知組態"	刪除與特定儲存區相關聯的中繼資料通知組態XML。
"取得Bucket中繼資料通知組態"	傳回與特定儲存區相關聯的中繼資料通知組態XML。
"放置時段中繼資料通知組態"	設定區段的中繼資料通知服務。
"取得儲存使用量"	告訴您帳戶使用的儲存空間總量、以及與帳戶相關的每個儲存區。
"已過時：具有規範設定的 CreateBucket"	已過時且不受支援：您無法再建立啟用「符合性」的新儲存區。
"已過時：取得 Bucket 法規遵循"	已過時但受支援：傳回現有舊版相容儲存區目前有效的法規遵循設定。
"已過時：符合 Put Bucket 規範"	已過時但受支援：可讓您修改現有舊版相容儲存區的法規遵循設定。

使用 **GET Bucket consistency** 請求在 **StorageGRID** 中檢索儲存桶一致性層級

「取得貯體一致性」要求可讓您判斷套用至特定貯體的一致性。

預設一致性設定為保證新建立物件的寫入後讀取。

您必須具有S3：GetBucketConsistency權限或帳戶根權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

在回應 XML 中、 `<Consistency>`會傳回下列其中一個值：

一致性	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

回應範例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相關資訊

"一致性"

使用 **PUT Bucket** 一致性請求在 **StorageGRID** 中指定一致性層級

「放置貯體一致性」要求可讓您指定套用至在貯體上執行之作業的一致性。

預設一致性設定為保證新建立物件的寫入後讀取。

開始之前

您必須具有S3：PuttBucketConsistency權限或帳戶root權限、才能完成此作業。

申請

`x-ntap-sg-consistency`參數必須包含下列其中一個值：

一致性	說明
全部	所有節點都會立即接收資料、否則要求將會失敗。
強大的全球化技術	保證所有站台所有用戶端要求的寫入後讀取一致性。
強式網站	保證站台內所有用戶端要求的寫入後讀取一致性。
全新寫入後讀取	（預設）為新物件提供寫入後讀取一致性、並最終確保物件更新一致。提供高可用度與資料保護保證。建議大多數情況下使用。
可用	提供新物件和物件更新的最終一致性。對於 S3 貯體、請僅視需要使用（例如、包含很少讀取的記錄值之貯體、或用於對不存在的金鑰執行 head 或 Get 作業）。S3 FabricPool 儲存區不支援。

- 注意： * 一般而言、您應該使用「新寫入後讀取」的一致性。如果要求無法正常運作、請盡可能變更應用程

式用戶端行為。或者、設定用戶端以指定每個 API 要求的一致性。將貯體層級的一致性設為最後的方法。

申請範例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相關資訊

"一致性"

使用 **GET Bucket last access time** 請求從 **StorageGRID** 中擷取儲存區的最後存取時間狀態

「取得時段上次存取時間」要求可讓您決定是否為個別的時區啟用或停用上次存取時間更新。

您必須具有S3：GetBucketLastAccessTime權限或帳戶根權限、才能完成此作業。

申請範例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示已針對儲存庫啟用上次存取時間更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

使用 **PUT Bucket last access time** 請求在 **StorageGRID** 中啟用和停用最後存取時間更新

「放置時段上次存取時間」要求可讓您針對個別的時段啟用或停用上次存取時間更新。停用上次存取時間更新可改善效能、是所有以10.3.0版或更新版本建立之儲存區的預設設定。

您必須擁有儲存區的S3：PuttBucketLastAccessTime權限、或是帳戶root權限、才能完成此作業。

> 從版本10.3開始StorageGRID 、所有新的儲存庫預設都會停用上次存取時間的更新。如果您有使用StorageGRID 舊版的更新程式建立的儲存區、而且想要符合新的預設行為、則必須明確停用這些舊版儲存區的上次存取時間更新。您可以使用 Put Bucket 上次存取時間要求、或從租戶管理器中的儲存區詳細資料頁面、啟用或停用上次存取時間的更新。請參閱。 "啟用或停用上次存取時間更新"

如果某個儲存區的上次存取時間更新已停用、則會將下列行為套用至儲存區上的作業：

- GetObject 、 GetObjectAcl 、 GetObjectTagging, 和 HeadObject 要求不會更新上次存取時間。不會將物件新增至佇列、以進行資訊生命週期管理（ILM）評估。
- 僅更新中繼資料的 CopyObject 和 PutObjectTaggings 要求也會更新上次存取時間。物件會新增至佇列以進行ILM評估。
- 如果來源貯體的上次存取時間更新已停用、則 CopyObject 要求不會更新來源貯體的上次存取時間。複製的物件不會新增至來源儲存區的ILM評估佇列。不過、對於目的地、 CopyObject 要求一律會更新上次存取時間。物件複本會新增至佇列以進行ILM評估。
- CompleteMultpartUpload 要求上次更新存取時間。完成的物件會新增至佇列以進行ILM評估。

申請範例

此範例可讓儲存區的上次存取時間達到。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此範例會停用儲存區的上次存取時間。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

使用 **StorageGRID** 中的 **DELETE Bucket** 中繼資料通知組態要求停用搜尋整合服務

刪除庫位中繼資料通知組態要求可讓您刪除組態XML、以停用個別庫位的搜尋整合服務。

您必須擁有儲存區的S3：刪除BucketMetadata通知權限、或是帳戶根權限、才能完成此作業。

申請範例

此範例顯示停用區段的搜尋整合服務。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

使用 **GET Bucket** 元資料通知組態要求在 **StorageGRID** 中設定搜尋整合

「Get Bucket中繼資料」通知組態要求可讓您擷取組態XML、以設定個別儲存區的搜尋整合。

您必須具有S3：GetBucketMetadata通知權限、或是帳戶root、才能完成此作業。

申請範例

此要求會擷取名為的貯體之中繼資料通知組態 `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應

回應本文包含儲存區的中繼資料通知組態。中繼資料通知組態可讓您決定儲存區的搜尋整合設定方式。也就是、它可讓您決定要建立索引的物件、以及要將物件中繼資料傳送至哪個端點。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

每個中繼資料通知組態都包含一或多個規則。每個規則都會指定套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。目的地必須使用StorageGRID 不實端點的URN來指定。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es`必須是第三個元素。 • URN 必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

回應範例

標籤之間的 XML `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`顯示如何為貯體設定與搜尋整合端點的整合。在此範例中、物件中繼資料會傳送至名為的 `Elasticsearch` 索引 `current`、並輸入位於名為的 AWS 網域中的 `records`名稱 `2017`。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相關資訊

"使用租戶帳戶"

使用 **PUT Bucket** 元資料通知設定請求在 **StorageGRID** 中啟用搜尋整合服務

「置入庫位元資料」通知組態要求可讓您針對個別的庫位啟用搜尋整合服務。您在要求本文中提供的中繼資料通知組態XML、會指定將中繼資料傳送至目的地搜尋索引的物件。

您必須擁有儲存區的S3：PuttBucketMetadata通知權限、或是帳戶根權限、才能完成此作業。

申請

要求必須在要求本文中包含中繼資料通知組態。每個中繼資料通知組態都包含一或多個規則。每個規則都會指定要套用的物件、StorageGRID 以及應將物件中繼資料傳送到哪個目的地。

物件可依物件名稱的前置詞進行篩選。例如、您可以將字首為物件的中繼資料傳送至一個目的地、而將字首為另一個目的地的物件傳送 `/images`至另一個目的地 `/videos`。

有重疊前置字元的組態無效、提交時會遭到拒絕。例如、不允許為具有前置碼的物件加入一個規則、並為具有前置碼的物件加入第二個規則 `test2`的組態 `test`。

目的地必須使用StorageGRID 不實端點的URN來指定。提交中繼資料通知組態時、端點必須存在、否則要求會以失敗的方式失敗 `400 Bad Request`。錯誤訊息指出： `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表說明中繼資料通知組態XML中的元素。

名稱	說明	必要
Metadata NotifyationConfiguration	用於指定中繼資料通知物件和目的地之規則的容器標籤。 包含一或多個規則元素。	是的
規則	規則的容器標記、用於識別應將中繼資料新增至指定索引的物件。 會拒絕具有重疊前置碼的規則。 包括在Metadata NotifyationConfiguration元素中。	是的
ID	規則的唯一識別碼。 包含在Rule元素中。	否
狀態	狀態可以是「已啟用」或「已停用」。不針對停用的規則採取任何行動。 包含在Rule元素中。	是的

名稱	說明	必要
前置碼	符合前置碼的物件會受到規則影響、其中繼資料會傳送到指定的目的地。 若要符合所有物件、請指定一個空白首碼。 包含在Rule元素中。	是的
目的地	規則目的地的容器標記。 包含在Rule元素中。	是的
urn	傳送物件中繼資料的目的地之一。必須是StorageGRID 具有下列屬性的不景端點的URN： • `es`必須是第三個元素。 • URN 必須以索引結尾、並在表單中輸入中繼資料的儲存位置 `domain-name/myindex/mytype`。 端點是使用租戶管理程式或租戶管理API來設定。它們採用下列形式： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 端點必須在提交組態XML之前進行設定、否則組態將會失敗並顯示404錯誤。 目標元素中包含urn.	是的

申請範例

此範例顯示啟用儲存庫的搜尋整合功能。在此範例中、所有物件的物件中繼資料都會傳送到相同的目的地。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

在此範例中、符合前置碼之物件的物件中繼資料 `/images`會傳送至一個目的地、而符合前置碼之物件的物件中繼資料 `/videos`則會傳送至第二個目的地。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

由搜尋整合服務產生的**JSON**

當您啟用儲存區的搜尋整合服務時、每次新增、更新或刪除物件中繼資料或標記時、都會產生Json文件並傳送至目的地端點。

此範例顯示在名為的儲存格中建立 `test`具有金鑰的物件時、可能會產生的 `JSON` 範例 `SGWS/Tagging.txt`。 `test`貯體未版本化、因此 `versionId`標記為空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

中繼資料通知中包含的物件中繼資料

此表格列出JSON文件中所有欄位、這些欄位會在啟用搜尋整合時傳送至目的地端點。

文件名稱包含儲存區名稱、物件名稱及版本ID（若有）。

類型	項目名稱	說明
儲存區和物件資訊	鏟斗	庫位名稱
儲存區和物件資訊	金鑰	物件金鑰名稱
儲存區和物件資訊	版本ID	物件版本、適用於版本控制的儲存區中的物件
儲存區和物件資訊	區域	例如、貯體區域 `us-east-1`
系統中繼資料	尺寸	HTTP用戶端可見的物件大小（以位元組為單位）
系統中繼資料	md5	物件雜湊

類型	項目名稱	說明
使用者中繼資料	中繼資料 *key:value*	物件的所有使用者中繼資料、做為金鑰值配對
標記	標籤 *key:value*	為物件定義的所有物件標記、做為金鑰值配對

針對標記和使用者中繼資料StorageGRID 、將日期和數字以字串或S3事件通知的形式傳送至Elasticsearch。若要設定Elasticsearch將這些字串解譯為日期或數字、請遵循Elasticsearch指示進行動態欄位對應、以及對應日期格式。您必須先在索引上啟用動態欄位對應、才能設定搜尋整合服務。建立文件索引後、您就無法編輯索引中文件的欄位類型。

相關資訊

"使用租戶帳戶"

使用 **GET Storage Usage** 請求擷取 **StorageGRID** 中的帳戶和儲存桶儲存使用量

「Get Storage使用量」要求會告訴您某個帳戶所使用的總儲存容量、以及與該帳戶相關聯的每個儲存區容量。

帳戶及其貯體所使用的儲存容量、可透過修改後的 Listbuckets 要求和查詢參數來取得 `x-ntap-sg-usage`。儲存區的使用量會與系統處理的PUT和DELETE要求分開追蹤。使用值可能會在處理要求時延遲、使其符合預期值、尤其是系統負載過重時。

根據預設StorageGRID 、功能區會嘗試使用強大的全域一致性來擷取使用資訊。如果無法達成強大的全球一致性、 StorageGRID 會嘗試以強大的站台一致性來擷取使用資訊。

您必須具有S3：listAllMyb桶 權限、或是帳戶root、才能完成此作業。

申請範例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

此範例顯示一個帳戶、其中兩個儲存區中有四個物件和12個位元組的資料。每個儲存區包含兩個物件和六個位元組的資料。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本管理

儲存的每個物件版本都會影響 `ObjectCount`回應中的和 `DataBytes`值。刪除標記不會新增至 `ObjectCount`總計。

相關資訊

"一致性"

已過時的資源桶要求、適用於舊版法規遵循

已棄用的儲存區請求（針對舊版 **StorageGRID** 法規遵循）

您可能需要使用StorageGRID Sfs3 REST API來管理使用舊版Compliance功能所建立的儲存區。

法規遵循功能已過時

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID

如果您先前已啟用「全域符合性」設定、StorageGRID 則會在「支援物件鎖定」中啟用「全域S3物件鎖定」設定。您不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、您可以視需要使用StorageGRID 「S3 REST API」來管理任何現有的符合舊規範的儲存庫。

- "使用 S3 REST API 來設定 S3 物件鎖定"
- "使用ILM管理物件"
- "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

過時的法規遵循要求：

- "已過時-將資源桶要求修改以符合法規要求"

  SGCompliance XML元素已過時。先前、您可以將StorageGRID 此等不必要的自訂元素納入可選的XML要求內容中、以建立符合法規的儲存庫要求。

- "已過時 - 取得 Bucket 法規遵循"

  Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

- "已過時 - 符合 Put Bucket 規範"

  「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

StorageGRID 中已棄用的 **SGCompliance** 元素

SGCompliance XML元素已過時。以前、您可以將此 StorageGRID 自訂元素納入 CreateBucket 要求的選用 XML 要求本文、以建立符合法規的儲存區。

> 先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：
>
> - "使用 S3 REST API 來設定 S3 物件鎖定"
> - "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您無法再建立啟用「法規遵循」的新庫位。如果您嘗試使用 CreateBucket 要求修改來建立新的相容貯體、則會傳回下列錯誤訊息：

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

StorageGRID 中已棄用的 **GET Bucket compliance** 請求

Get Bucket法規遵循要求已過時。不過、您可以繼續使用此要求來判斷現有舊版相容儲存區目前有效的法規遵循設定。

先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：

- "使用 S3 REST API 來設定 S3 物件鎖定"
- "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您必須具有S3：GetBucketCompliance權限、或是帳戶root、才能完成此作業。

申請範例

此範例要求可讓您決定名為的貯體的符合性設定 `mybucket`。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

回應範例

在回應 XML 中、 `<SGCompliance>`列出有效的符合性設定。此回應範例顯示儲存區的法規遵循設定、其中每個物件將保留一年（525600分鐘）、從物件擷取到網格開始算起。此庫位目前沒有合法持有。每個物件將在一年後自動刪除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。

名稱	說明
LegalHold	• 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

錯誤回應

如果建立的貯體不符合標準、則回應的 HTTP 狀態代碼為、 S3 錯誤代碼 `XNoSuchBucketCompliance`為 `404 Not Found`。

StorageGRID 中已棄用的 **PUT Bucket** 合規性要求

「放入時段」法規遵循要求已過時。不過、您可以繼續使用此要求來修改現有舊版相容桶的法規遵循設定。例如、您可以將現有的貯體置於合法持有狀態、或是延長保留期間。

> 先前版本的不支援《支援不符合要求》功能、現已由S3物件鎖定取代。StorageGRID StorageGRID如需詳細資訊、請參閱下列內容：
>
> • "使用 S3 REST API 來設定 S3 物件鎖定"
>
> • "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"

您必須具有S3：PuttBucketCompliance權限、或是帳戶root、才能完成此作業。

在發出「放入庫位」法規遵循要求時、您必須為法規遵循設定的每個欄位指定一個值。

申請範例

此範例要求會修改名為的貯體的符合性設定 `mybucket`。在此範例中、從物件擷取到網格開始、中的物件 `mybucket`現在會保留兩年（ 1 、 051,200 分鐘）、而不是一年。此庫位沒有合法持有。每個物件將在兩年後自動刪除。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名稱	說明
RetentionPeriodMinutes	新增至此儲存區之物件的保留期間長度（以分鐘為單位）。保留期間是從物件擷取至網格時開始。 • 重要 * 為 RetentionPeriodMinutes 指定新值時、您必須指定一個值、該值等於或大於該貯體目前的保留期間。設定貯體保留期間之後、您就無法減少該值、只能增加該值。
LegalHold	• 是：此儲存庫目前處於合法持有狀態。除非取消合法保留、否則無法刪除此貯體中的物件、即使保留期間已過期。 • 假：此庫位目前未合法持有。此儲存區中的物件可在保留期間到期時刪除。
自動刪除	• 是：此儲存區中的物件會在保留期間到期時自動刪除、除非儲存區處於合法持有狀態。 • 否：保留期間到期時、此儲存區中的物件不會自動刪除。如果需要刪除這些物件、您必須手動刪除這些物件。

法規遵循設定的一致性

當您更新S3儲存區的法規遵循設定、並提出「置放儲存區法規遵循」要求時StorageGRID 、即可嘗試更新整個網格的儲存區中繼資料。根據預設、 StorageGRID 會使用 * 強式全域 * 一致性來保證所有資料中心站台和所有包含儲存區中繼資料的儲存節點、對於變更的法規遵循設定、都具有寫入後讀取一致性。

如果 StorageGRID 因為某個站台的資料中心站台或多個儲存節點無法使用而無法達到 * 強式全域 * 一致性、則回應的 HTTP 狀態代碼為 `503 Service Unavailable.`

如果您收到此回應、則必須聯絡網格管理員、以確保所需的儲存服務能夠儘快提供。如果網格管理員無法在每個網站上提供足夠的儲存節點、技術支援可能會強制使用 **Strong-site** 一致性、引導您重試失敗的要求。

除非技術支援人員指示您遵守、否則切勿強迫 * 強式站台 * 一致性、除非您瞭解使用此層級的潛在後果。

當一致性降至 * 強式站台 * 時、 StorageGRID 保證更新的法規遵循設定只會對站台內的用戶端要求具有讀寫後一致性。這表示StorageGRID 在所有站台和儲存節點都可用之前、此儲存區的設定可能會暫時有多個不一致的設定。不一致的設定可能會導致非預期和非預期的行為。例如、如果您將貯體置於合法保留之下、而您強制降低一致性、則貯體先前的法規遵循設定（即合法保留）可能會繼續在某些資料中心站台生效。因此、您認為合法保留的物件、可能會在保留期間到期時遭到刪除、使用者或自動刪除（如果已啟用）。

若要強制使用 **Strong-site** 一致性、請重新發出 Put Bucket 符合性要求、並加入 `Consistency-Control` HTTP 要求標頭、如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

錯誤回應

- 如果儲存區不是為了符合法規要求而建立、則回應的 HTTP 狀態代碼為 `404 Not Found`。
- 如果在要求中小於貯體目前的保留期間、則 `RetentionPeriodMinutes` HTTP 狀態代碼為 `400 Bad Request`。

相關資訊

"已過時：將資源桶要求修改以符合法規要求"

管理存取策略

StorageGRID 如何使用 **AWS** 原則來控制對 **S3** 儲存貯體和物件的存取

支援使用Amazon Web Services（AWS）原則語言、讓S3租戶能夠控制對這些儲存區內的儲存區和物件的存取。StorageGRID此系統實作S3 REST API原則語言的子集。StorageGRIDS3 API的存取原則是以Json撰寫。

存取原則總覽

StorageGRID支援三種存取策略：

- * Bucket Policies * 、使用 GetBucketPolicy 、 PuttBucketPolicy 及 DeleteBucketPolicy S3 API 作業或 Tenant Manager 或 Tenant Management API 來管理。庫位原則會附加至庫位、因此這些原則可設定為控制庫位擁有者帳戶或其他帳戶中的使用者對庫位及其中物件的存取。庫位原則僅適用於一個庫位、可能也適用於多個群組。
- 群組原則、使用租戶管理程式或租戶管理API進行設定。群組原則會附加至帳戶中的群組、因此這些原則會設定為允許該群組存取該帳戶所擁有的特定資源。群組原則僅適用於一個群組、可能也適用於多個儲存區。
- 會話策略，包含在 AssumeRole 請求中。會話策略僅適用於給定的會話，進一步定義使用者除了群組和儲存桶策略授予的權限之外還擁有的權限。

群組、桶和會話策略之間的優先順序沒有區別。

根據Amazon定義的特定語法、執行庫位和群組原則。StorageGRID每個原則內部都有一組原則聲明、每個陳述都包含下列元素：

- 對帳單ID（Sid）（選用）
- 效果
- 委託人/未委託人
- 資源/未資源
- 行動/未行動
- 條件（選用）

原則陳述是使用此結構來指定權限：在套用<condition>時，授與<effect>允許/拒絕<Principe>執行<Action"。

每個原則元素都用於特定功能：

元素	說明
SID	Sid元素為選用項目。Sid僅供使用者說明使用。它會儲存、但StorageGRID 不會被作業系統解讀。
效果	使用effect元素來確定是否允許或拒絕指定的作業。您必須使用支援的Action元素關鍵字、識別您允許（或拒絕）的貯體或物件作業。
委託人/未委託人	您可以允許使用者、群組和帳戶存取特定資源並執行特定動作。如果要求中未包含S3簽名、則可指定萬用字元（*）做為主體、以匿名存取。根據預設、只有root帳戶可以存取該帳戶擁有的資源。 主體： • `"Principal": "*"`符合所有請求，包括匿名（未簽署）請求。 • `"Principal": { "AWS": "*" }` 符合任何已驗證的身分或使用者（不符合匿名請求） • 僅適用於儲存桶原則 • 主體是指被授予或拒絕權限的帳戶/使用者。 您只需要在庫位原則中指定主要元素。對於群組原則而言、附加原則的群組是內含的主體元素。
資源/未資源	資源元素可識別儲存區和物件。您可以使用Amazon資源名稱（ARN）來允許或拒絕貯體和物件的權限、以識別資源。
行動/未行動	「行動」和「效果」元素是權限的兩個元件。當群組要求資源時、系統會將資源的存取權限授予或拒絕。除非您特別指派權限、否則存取會遭拒、但您可以使用明確拒絕來覆寫其他原則所授予的權限。
條件	條件元素為選用項目。條件可讓您建置運算式、以判斷何時應套用原則。

在Action元素中、您可以使用萬用字元（*）來指定所有作業或作業子集。例如、此動作會比對S3：GetObject、S3：PuttObject和S3：Delete物件等權限。

```
s3:*Object
```

在資源元素中、您可以使用萬用字元（*）和（？）。星號（*）與0個以上的字元相符、但問號（？） 符合任何單一字元。

在 Principal 元素中、除了設定匿名存取外、不支援萬用字元、這會將權限授予每個人。例如、您將萬用字元（*）設為主要值。

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

在下列範例中、陳述式使用的是「效果」、「主要」、「行動」和「資源」元素。此範例顯示完整的庫位原則聲明、使用「允許」效果授予主體、管理群組 `federated-group/admin`和財務群組 `federated-group/finance`、對該庫位 `mybucket`內所有物件執行「動作」的 `s3:GetObject`權限、以及對該庫位內所有物件執行「動作」的權限 `s3:ListBucket`。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

儲存區原則的大小上限為20、480個位元組、而且群組原則的大小上限為5、120個位元組。

原則的一致性

根據預設、您對群組原則所做的任何更新最終都是一致的。當群組原則變得一致時、由於原則快取、變更可能需要額外 15 分鐘才能生效。根據預設、您對儲存庫原則所做的任何更新都是非常一致的。

您可以視需要變更庫位原則更新的一致性保證。例如、您可能想要在站台中斷期間變更貯體原則。

在這種情況下、您可以在 PuttBucketPolicy 要求中設定 `Consistency-Control`標頭、也可以使用 Put Bucket 一致性要求。當貯體原則變得一致時、由於原則快取、變更可能需要額外 8 秒的時間才能生效。

如果您將一致性設定為不同的值來因應暫時情況、請務必在完成時將貯體層級設定恢復為原始值。否則、所有未來的貯體要求都會使用修改後的設定。

什麼是會話策略？

會話策略是一種存取策略，它暫時限制特定會話期間可用的權限，例如當使用者加入某個群組時。會話策略只能允許一部分權限，且不能授予額外的權限。該群組本身可能擁有更廣泛的權限。

在原則聲明中使用**ARN**

在原則聲明中、ARN用於主要和資源元素。

- 使用此語法來指定S3資源ARN：

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 使用此語法來指定身分識別資源ARN（使用者和群組）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他考量事項：

- 您可以使用星號（*）做為萬用字元、以比對物件金鑰內的零個或多個字元。
- 物件鍵中可指定的國際字元應使用 JSON UTF-8 編碼或使用 JSON \u 轉義序列進行編碼。不支援百分比編碼。

  "RFC 2141 URN語法"

  PuttBucketPolicy 作業的 HTTP 要求主體必須以 charset=UTF-8 編碼。

在原則中指定資源

在原則聲明中、您可以使用資源元素來指定允許或拒絕權限的儲存區或物件。

- 每個原則聲明都需要資源元素。在原則中、資源會以元素表示、或是以排除方式 `NotResource`表示 `Resource`。
- 您可以使用S3資源ARN來指定資源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以在物件機碼內使用原則變數。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 資源值可以指定在建立群組原則時尚不存在的儲存桶。

在原則中指定主體

使用主體元素來識別原則聲明允許/拒絕存取資源的使用者、群組或租戶帳戶。

- 庫位原則中的每個原則聲明都必須包含主要元素。群組原則中的原則聲明不需要 Principal 元素、因為群組被理解為主體。
- 在原則中、主體會以元素「 Principal 」表示、或是以「 NotPrincipal 」表示排除。
- 帳戶型身分識別必須使用ID或ARN來指定：

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 此範例使用租戶帳戶ID 27233906934684427525、其中包含帳戶root和帳戶中的所有使用者：

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 您只能指定帳戶根目錄：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定特定的聯盟使用者（「Alex」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 您可以指定特定的聯盟群組（「經理」）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers"  }
```

- 您可以指定匿名主體：

```
"Principal": "*"
```

- 為了避免混淆、您可以使用使用者UUID、而非使用者名稱：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

例如、假設 Alex 離開組織並刪除使用者名稱 `Alex`。如果有新的 Alex 加入組織並指派相同的 `Alex`使用者名稱、新使用者可能會不小心繼承授予原始使用者的權限。

- 主值可以指定在建立儲存桶原則時尚不存在的群組/使用者名稱。

在原則中指定權限

在原則中、會使用Action元素來允許/拒絕資源的權限。您可以在原則中指定一組權限、以元素「Action」表示、或是以「NotAction」表示排除權限。每個元素都對應到特定的S3 REST API作業。

這些表格列出套用至儲存區的權限、以及套用至物件的權限。

Amazon S3 現在會針對 PuttBucketReplication 和 DeleteBucketReplication 動作使用 S3:PutReplicationConfiguration 權限。針對每個行動使用不同的權限、這與原始的Amazon S3規格相符。StorageGRID

使用 Put 覆寫現有值時會執行刪除。

套用至貯體的權限

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：建立桶	建立庫位	是的。 • 附註 * ：僅用於群組原則。
S3：刪除資源桶	刪除Bucket	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：刪除BucketMetadata通知	刪除時段中繼資料通知組態	是的
S3：刪除BucketPolicy	刪除BucketPolicy	
S3：刪除複製組態	刪除 BucketReplication	是、請分別授予和刪除權限
S3：GetBucketAcl	GetBucketAcl	
S3：GetBucketCompliance	取得資源桶法規遵循（已過時）	是的
S3：GetBucketConsistency	取得庫位一致性	是的
S3：GetBucketCORS	GetBucketCors	
S3：GetEncryptionConfiguration	GetBucketEncryption	
S3：GetBucketLastAccessTime	取得時段上次存取時間	是的
S3：GetBucketLocation	GetBucketLocation	
S3：GetBucketMetadata通知	取得Bucket中繼資料通知組態	是的
S3：GetBucketNotification	GetBucketNotificationConfiguration	
S3：GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3：GetBucketPolicy	GetBucketPolicy	
S3：GetBucketting	GetBucketTagging	
S3：GetBucketVersion	GetBucketVersion	
S3：Get生命 週期組態	GetBucketLifecycleConfiguration	
S3：GetReplicationConfiguration	GetBucketReplication	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：ListAllMyb桶	• 列表桶 • 取得儲存使用量	是的、用於取得儲存使用量。 • 附註 * ：僅用於群組原則。
S3：清單庫	• GetObject • 標題庫 • 標題物件 • 清單物件	
S3：listBucketMultiPartUploads	• ListMultipartUploads	
S3：listBucketVerions	取得Bucket版本	
S3：PuttBucketCompliance	符合資源桶規範（已過時）	是的
S3：PuttBucketConsistency	實現庫位一致性	是的
S3：PuttBucketCORS	• 刪除 BucketCors † • PuttBucketCors	
S3：PuttEncryptionConfiguration	• 刪除 BucketEncryption • PuttBucketEncryption	
S3：PuttBucketLastAccessTime	將資源桶放在最後存取時間	是的
S3：PuttBucketMetadata通知	放置時段中繼資料通知組態	是的
S3：PuttBucketNotification	PutBucketNotificationConfiguration	
S3：PuttBucketObjectLockConfiguration	• 具有要求標頭的 CreateBucket `x-amz-bucket-object-lock-enabled: true` （也需要 S3:CreateBucket 權限） • PutObjectLockConfiguration	
S3：PuttBucketPolicy	PuttBucketPolicy	

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：PuttBucketting	• 刪除標籤† • PuttBucketTagging	
S3：PuttBucketVersion	PuttBucketVersion	
S3：Putt升降 器組態	• 刪除 BucketLifecycle † • PuttBucketLifecycleConfiguration	
S3：PuttReplicationConfiguration	PutBucketReplication	是、請分別授予和刪除權限

套用至物件的權限

權限	S3 REST API作業	客製StorageGRID化以供選擇
S3：中止多重角色上傳	• AbortMultiPart上 傳	
S3：BypassGovernanceRetention	• 刪除物件 • 刪除物件 • PutObjectRetention	
S3：刪除物件	• 刪除物件 • 刪除物件	
S3：刪除ObjectTagging	刪除ObjectTagging	
S3：刪除ObjectVersion標記	刪除物件標籤（物件的特定版本）	
S3：刪除ObjectVersion	DeleteObject （物件的特定版本）	
S3：GetObject	• GetObject • 標題物件 • 選取物件內容	
S3：GetObjectAcl	GetObjectAcl	
S3：GetObjectLegalHold	GetObjectLegalHold	

權限	**S3 REST API**作業	客製**StorageGRID**化以供選擇
S3：GetObjectRetention	GetObjectRetention	
S3：GetObjectTagging	GetObjectTagging	
S3：GetObjectVersion標記	GetObjectTagging(物件的特定版本)	
S3：GetObjectVersion	GetObject （物件的特定版本）	
S3：列出多個零件上傳零件	清單零件	
S3：PuttObject	• CopyObject • 完成多個部分上傳 • 建立多個部分上傳 • PuttObject • 上傳零件 • 上傳PartCopy	
S3：PuttObjectLegalHold	PutObjectLegalHold	
S3：PuttObjectRetention	PutObjectRetention	
S3：PuttObjectTagging	PuttObjectTagging	
S3：PuttObjectVersion標記	PutObjectTagging(物件的特定版本)	
S3：PuttOverwriteObject	• 完成多個部分上傳 • CopyObject • 刪除ObjectTagging • PuttObject • PuttObjectTagging	是的
S3：恢復物件	RestoreObject	

使用 **PutOverwriteObject** 權限

S3：PuttOverwriteObject權限是套StorageGRID 用至建立或更新物件之作業的自訂功能。此權限的設定決定用戶端是否可以覆寫物件的資料、使用者定義的中繼資料或S3物件標記。

此權限的可能設定包括：

- 允許：用戶端可以覆寫物件。這是預設設定。
- * 拒絕 * ：用戶端無法覆寫物件。設為「拒絕」時、PuttOverwriteObject權限的運作方式如下：
  - 如果在同一路徑找到現有物件：
    - 物件的資料、使用者定義的中繼資料或 S3 物件標記無法覆寫。
    - 任何進行中的擷取作業都會取消、並傳回錯誤。
    - 如果啟用 S3 版本設定、則「拒絕」設定會防止 PutObjectTagging 或 DeleteObjectTagging 作業修改物件及其非目前版本的 TagSet 。
  - 如果找不到現有物件，則此權限無效。
- 如果此權限不存在，則效果與設定了「允許」權限相同。

> 如果目前 S3 策略允許覆蓋，且 PutOverwriteObject 權限設定為 Deny，則用戶端無法覆寫物件的資料、使用者定義的元資料或物件標記。此外，如果勾選「防止用戶端修改」複選框（配置 > 安全設定 > 網路和物件），則該設定將覆蓋 PutOverwriteObject 權限的設定。

在原則中指定條件

條件會定義原則的生效時間。條件包括運算子和金鑰值配對。

條件使用金鑰值配對進行評估。條件元素可以包含多個條件、而且每個條件可以包含多個金鑰值配對。條件區塊使用下列格式：

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

在下列範例中、ipAddress條件使用SourceIp條件金鑰。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

支援的條件運算子

條件運算子的分類如下：

- 字串
- 數字
- 布林值
- IP 位址

- null檢查

條件運算子	說明
擷取等量資料	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。
擷取NotEquals	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。
StringEqualsIgnoreCase	根據完全相符的結果（忽略大小寫）、將金鑰與字串值進行比較。
StringNotEqualsIgnoreCase	根據否定比對（忽略大小寫）、將金鑰與字串值進行比較。
StringLike	根據完全相符（區分大小寫）、將金鑰與字串值進行比較。可以包含 * 和 ? 萬用字元。
StringNotLike	根據否定比對（區分大小寫）、將金鑰與字串值進行比較。可以包含 * 和 ? 萬用字元。
分子等量	根據完全相符的結果、將金鑰與數值進行比較。
NumericNotEquals	根據已否定的比對、將金鑰與數值進行比較。
數值資料	根據「大於」比對、將金鑰與數值進行比較。
NumericGreaterThang Equals	根據「大於或等於」比對、將金鑰與數值進行比較。
數字LessThan	根據「小於」比對、將金鑰與數值進行比較。
NumericLessThang Equals	根據「小於或等於」比對、將金鑰與數值進行比較。
布爾	根據 "TRUE 或 FALSE" 比對、將金鑰與布林值進行比較。
IP地址	比較金鑰與IP位址或IP位址範圍。
NotIppAddress	根據已否定的比對、將金鑰與IP位址或IP位址範圍進行比較。
null	檢查條件金鑰是否存在於目前的要求內容中。
如果存在	附加到除 Null 條件之外的任何條件運算子，以檢查該條件索引鍵是否不存在。如果條件索引鍵不存在，則傳回 TRUE。

支援的條件金鑰

條件金鑰	行動	說明
AWS：來源Ip	IP營運者	與傳送請求的 IP 位址進行比較。可用於儲存桶或物件操作。 *注意：*如果 S3 請求是透過管理節點和閘道節點上的負載平衡器服務發送的，則此請求將與負載平衡器服務的上游 IP 位址進行比較。 注意：如果使用第三方非透明負載平衡器，則會與該負載平衡器的 IP 位址進行比較。任何 `X-Forwarded-For`標頭都將被忽略，因為無法確定其有效性。
AWS：使用者名稱	資源/身分識別	與傳送請求的傳送者使用者名稱進行比較。可用於儲存桶或物件操作。
S3：分隔符號	S3：清單儲存庫和 S3：listBucketVerions權限	與 ListObjects 或 ListObjectVersions 請求中指定的分隔符號參數進行比較。
S3 ： <tag-key>	S3：刪除ObjectTagging S3：刪除ObjectVersion標記 S3：GetObject S3：GetObjectAcl 3 ： GetObjectTagging S3：GetObjectVersion S3：GetObjectVerionAcl S3：GetObjectVersion標記 S3 ： PutObjectAcl S3：PuttObjectTagging S3 ： PutObjectVersionAcl S3：PuttObjectVersion標記	要求現有物件具有特定的標籤鍵和值。

條件金鑰	行動	說明
S3：金鑰上限	S3：清單儲存庫和 S3：listBucketVerions權限	與 ListObjects 或 ListObjectVersions 請求中指定的 max-keys 參數進行比較。
s3：物件鎖定模式	S3：PuttObject	相比 `object-lock-mode`從PutObject、CopyObject、CreateMultipartUpload請求中的請求頭展開。
s3：物件鎖定模式	S3：PuttObjectRetention	相比 `object-lock-mode`從 PutObjectRetention 請求中的 XML 主體擴展而來。
S3：物件鎖定剩餘保留天數	S3：PuttObject	與要求標頭中指定的保留截止日期比較 `x-amz-object-lock-retain-until-date`、或是根據貯體預設保留期間計算、以確保這些值在下列要求的允許範圍內： • PuttObject • CopyObject • 建立多個部分上傳
S3：物件鎖定剩餘保留天數	S3：PuttObjectRetention	與 PutObjectRetention 要求中指定的保留截止日期進行比較、以確保其在允許範圍內。
S3：前置碼	S3：清單儲存庫和 S3：listBucketVerions權限	與 ListObjects 或 ListObjectVersions 請求中指定的前綴參數，或為 GetObject 或 HeadObject 指定的金鑰進行比較。
<tag-key>	S3：PuttObject S3：PuttObjectTagging S3：PuttObjectVersion標記	當物件請求包含標籤時，需要特定的標籤索引鍵和值。
s3:x-amz-copy-source	S3：PuttObject	與 PutObject 和 UploadPartCopy 請求標頭中展開的 x-amz-copy-source 進行比較。
s3:x-amz-伺服器端加密客戶演算法	S3：PuttObject	相比 `sse-customer-algorithm`或 `copy-source-sse-customer-algorithm`從 PutObject、CopyObject、CreateMultipartUpload、UploadPart、UploadPartCopy、CompleteMultipartUpload 請求中的請求頭展開。

在原則中指定變數

您可以在原則中使用變數、在原則可用時填入原則資訊。您可以在元素中使用原則變數、也可以在元素中使用 `Resource`字串比較 `Condition`。

在此範例中、變數 `${aws:username}`是 Resource 元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在此範例中、變數 `${aws:username}`是條件區塊中條件值的一部分：

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

變動	說明
`${aws:SourceIp}`	使用來源Ip金鑰作為提供的變數。
`${aws:username}`	使用UserName金鑰做為提供的變數。
`${s3:prefix}`	使用服務專屬的前置碼作為提供的變數。
`${s3:max-keys}`	使用服務專屬的最大金鑰作為提供的變數。
`${*}`	特殊字元。使用字元做為文字*字元。
`${?}`	特殊字元。使用字元做為文字字元。
`${$}`	特殊字元。使用字元做為文字$字元。

建立需要特殊處理的原則

有時候原則可能會授與安全性危險或危險的權限、以便繼續執行作業、例如封鎖帳戶的root使用者。在原則驗證期間、不像Amazon、StorageGRID 執行「支援S3 REST API」的限制較少、但在原則評估期間同樣嚴格。

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕root帳戶的任何權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同

原則說明	原則類型	**Amazon**行為	運作方式**StorageGRID**
拒絕對使用者/群組擁有任何權限	群組	有效且強制	相同
允許外部帳戶群組擁有任何權限	鏟斗	無效的主體	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤
允許外部帳戶root或使用者擁有任何權限	鏟斗	有效、但原則允許時、所有S3儲存區原則作業的權限都會傳回「不允許使用405方法」錯誤	相同
允許每個人都有權執行所有動作	鏟斗	有效、但所有S3儲存區原則作業的權限都會傳回異帳戶根目錄和使用者不允許的「405方法」錯誤	相同
拒絕所有人對所有動作的權限	鏟斗	有效且強制、但root使用者帳戶保留所有S3儲存區原則作業的權限	相同
主體是不存在的使用者或群組	鏟斗	無效的主體	有效
資源是不存在的S3儲存區	群組	有效	相同
主體是本機群組	鏟斗	無效的主體	有效
原則會授與非擁有者帳戶（包括匿名帳戶）權限、以放置物件。	鏟斗	有效。物件歸建立者帳戶所有，儲存桶原則不適用。建立者帳戶必須使用物件 ACL 授予物件的存取權限。	有效。物件由庫位擁有者帳戶擁有。適用庫位政策。

一次寫入多讀（**WORM**）保護

您可以建立一次寫入多次讀取（WORM）儲存區、以保護資料、使用者定義的物件中繼資料、以及S3物件標記。您可以設定WORM儲存區、以允許建立新物件、並防止覆寫或刪除現有內容。請使用本文所述的其中一種方法。

為了確保覆寫永遠被拒絕、您可以：

- 從網格管理員中，前往*配置* > 安全性 > 安全設定 > 網路和物件，然後選擇*防止客戶端修改*複選框。
- 套用下列規則和S3原則：
  - 將PuttOverwriteObject拒絕作業新增至S3原則。
  - 將刪除物件拒絕作業新增至S3原則。

。將 PutObject 允許作業新增至 S3 原則。

> 在 S3 原則中將 DeleteObject 設定為 DENY，並不能防止 ILM 在存在「30 天後零複本」之類的規則時刪除物件。

> 即使套用了所有這些規則和原則、也無法防範並行寫入（請參閱情況 A ）。它們確實能防止連續完成的覆寫（請參閱情況B）。

情況**A**：並行寫入（不受保護）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

情況**B**：連續完成覆寫（防範）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

相關資訊

- "如何利用ILM規則來管理物件StorageGRID"
- "貯體原則範例"
- "群組原則範例"
- "會話策略範例"
- "使用ILM管理物件"
- "使用租戶帳戶"

StorageGRID S3 REST API 工作階段原則範例

使用以下範例建立StorageGRID會話策略。

範例：設定允許物件檢索的會話策略

在本例中，工作階段的主體僅被允許從 bucket1 擷取物件。所有其他動作均被隱含拒絕，但 StorageGRID 特有的動作（例如使用 "S3：PuttOverwriteObject" 權限）除外。工作階段原則可以在呼叫 AssumeRole API 時以 JSON 檔案的形式提供。

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

StorageGRID S3 REST API 儲存區原則範例

使用本節中的範例、為貯體建立 StorageGRID 存取原則。

儲存區原則會指定原則附加的儲存區存取權限。您可以透過下列其中一個工具、使用 S3 PuttBucketPolicy API 來設定貯體原則：

- "租戶管理程式"。
- AWS CLI 使用此命令（請參閱"在貯體上作業"）：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

在 StorageGRID 中，主體：

- `"Principal": "*"`符合所有請求，包括匿名（未簽署）請求。
- `"Principal": { "AWS": "*" }` 符合任何已驗證的身分或使用者（不符合匿名請求）
- 僅適用於儲存桶原則
- 主體是指被授予或拒絕權限的帳戶/使用者。

範例：允許每個人只讀存取儲存區

在此範例中、每個人（包括匿名）都可以列出貯體中的物件、並對貯體中的所有物件執行 GetObject 作業。所有其他作業都將遭拒。請注意、這項原則可能並不特別有用、因為除了帳戶根目錄之外、沒有其他人擁有寫入貯體的權限。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

範例：允許同一個帳戶中的每個人都擁有完整存取權、以及其他帳戶中的每個人只讀存取庫位

在此範例中、指定帳戶中的每個人都可以完全存取貯體、而另一個指定帳戶中的每個人只能列出該貯體、並以物件金鑰首碼開頭、對貯體中的物件執行 GetObject 作業 `shared/`。

> 在功能區中StorageGRID 、非擁有者帳戶所建立的物件（包括匿名帳戶）、均由庫位擁有者帳戶擁有。庫位原則適用於這些物件。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

範例：允許每個人只讀存取儲存區、並由指定群組進行完整存取

在此範例中、包括匿名在內的每個人都可以列出貯體、並對貯體中的所有物件執行 GetObject 作業、而只有屬於指定帳戶中群組的使用者才可以擁有 `Marketing`完整存取權。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

範例：如果用戶端位於**IP**範圍、則允許每個人讀取及寫入儲存區的存取權

在此範例中、每個人（包括匿名）都可以列出儲存區、並在儲存區中的所有物件上執行任何物件作業、前提是要求來自指定的IP範圍（54.240.143.0至54.240.143.255、但54.240.143.188除外）。所有其他作業都會遭到拒絕、而且IP範圍以外的所有要求都會遭到拒絕。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

範例：允許特定同盟使用者專屬完整存取儲存區

在此範例中、同盟使用者 Alex 可完全存取 `examplebucket`貯體及其物件。所有其他使用者、包括「root」、都會明確拒絕所有作業。不過請注意、「root」永遠不會被拒絕存取權限來放置/取得/刪除BucketPolicy。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

範例：**PuttOverwriteObject**權限

在此範例中、 `Deny` PutOverwriteObject 和 DeleteObject 的效果可確保任何人都無法覆寫或刪除物件的資料、使用者定義的中繼資料和 S3 物件標記。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

StorageGRID S3 REST API 群組原則範例

使用本節中的範例、為群組建置 StorageGRID 存取原則。

群組原則會指定原則所附加之群組的存取權限。原則中沒有任何 `Principal`元素、因為它是隱含的。群組原則是使用租戶管理程式或API來設定。

範例：使用租戶管理程式設定群組原則

當您在租戶管理器中新增或編輯群組時、可以選取群組原則、以判斷此群組成員將擁有哪些 S3 存取權限。請參閱。 "為S3租戶建立群組"

- 無**S3**存取：預設選項。此群組中的使用者無法存取 S3 資源、除非已透過貯體原則授予存取權限。如果選取此選項、預設只有root使用者可以存取S3資源。
- 唯讀存取：此群組中的使用者擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。選取此選項時、唯讀群組原則的Json字串會出現在文字方塊中。您無法編輯此字串。
- 完整存取：此群組中的使用者可完整存取S3資源、包括儲存區。選取此選項時、會在文字方塊中顯示完整存取群組原則的Json字串。您無法編輯此字串。
- * 勒索軟體緩解 * ：此範例原則適用於此租戶的所有貯體。此群組中的使用者可以執行一般動作、但無法從已啟用物件版本設定的儲存區中永久刪除物件。

  擁有「管理所有貯體」權限的租戶管理員使用者可以覆寫此群組原則。將「管理所有貯體」權限限制於信任的使用者、並在可行的情況下使用「多因素驗證」（ MFA ）。

- 自訂：群組中的使用者會被授予您在文字方塊中指定的權限。

範例：允許群組完整存取所有儲存區

在此範例中、除非庫位原則明確拒絕、否則群組的所有成員都可以完整存取租戶帳戶擁有的所有庫位。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組唯讀存取所有儲存區

在此範例中、除非資源庫原則明確拒絕、否則群組的所有成員都擁有S3資源的唯讀存取權。例如、此群組中的使用者可以列出物件並讀取物件資料、中繼資料和標記。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

範例：允許群組成員完全存取儲存庫中的「資料夾」

在此範例中、群組成員只能在指定的儲存區中列出及存取其特定資料夾（金鑰首碼）。請注意、在決定這些資料夾的隱私權時、應考慮其他群組原則和儲存區原則的存取權限。

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

StorageGRID 稽核日誌中追蹤的 S3 操作

稽核訊息是StorageGRID 由支援服務產生、並儲存在文字記錄檔中。您可以在稽核記錄中檢閱 S3 特定的稽核訊息、以取得有關貯體和物件作業的詳細資料。

稽核記錄中追蹤的庫位作業

- 建立庫位
- 刪除Bucket
- 刪除BucketPolicy
- 刪除 Bucketagging
- 刪除物件
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketTagging
- 標題庫
- 清單物件
- ListObjectVerions
- 符合資源需求

- PuttBucketLifecycleConfiguration
- PuttBucketPolicy
- PuttBucketTagging
- PuttBucketVersion

稽核記錄中追蹤的物件作業

- 完成多個部分上傳
- CopyObject
- 刪除物件
- GetObject
- 標題物件
- PuttObject
- RestoreObject
- SelectObject
- 上傳組件（當 ILM 規則使用平衡或嚴格擷取時）
- 上傳 PartCopy （當 ILM 規則使用平衡或嚴格擷取時）

相關資訊

- "存取稽核記錄檔"
- "用戶端寫入稽核訊息"
- "用戶端讀取稽核訊息"

使用 **Swift REST API** （生命週期結束）

StorageGRID 中的 **Swift REST API** 支援

Swift API 的支援已達到使用期限、將於未來版本中移除。

Swift 詳細資料已從此文件網站版本中移除。請參閱。 "StorageGRID 11.8 ：使用 Swift REST API"

監控 StorageGRID 系統並進行疑難排解

監控 StorageGRID 系統

使用AutoSupport

了解 AutoSupport 在 StorageGRID 中的應用

AutoSupport 功能可讓 StorageGRID 將健全狀況和狀態套件傳送至 NetApp 技術支援。

使用AutoSupport有助於更快地解決問題。技術支援可以監控您系統的儲存需求並協助確定是否需要新增節點或網站。或者， AutoSupport可以將軟體包傳送到另一個目的地。

StorageGRID 有兩種類型的 AutoSupport ：

- * StorageGRID AutoSupport * 回報 StorageGRID 軟體問題。在您第一次安裝 StorageGRID 時、預設為啟用。如有需要、您可以"變更預設的 AutoSupport 組態"。

> 如果未啟用StorageGRID AutoSupport ，則網格管理器儀表板上會出現一則訊息。該訊息包含指向AutoSupport設定頁面的連結。如果您關閉該訊息，即使AutoSupport保持停用狀態，它也不會再次出現，直到您的瀏覽器快取已清除。

- * 設備硬體 AutoSupport * 回報 StorageGRID 應用裝置問題。您必須"在每個應用裝置上設定硬體 AutoSupport"。

什麼是 Digital Advisor？

Active IQ Digital Advisor （也稱為 Digital Advisor）是雲端型，它利用了 NetApp 安裝基礎使用者的預測分析和社群智慧。其持續的風險評估、預測警報、指導性建議和自動化操作可協助您在問題發生之前就加以預防，進而提高系統健全狀況和系統可用度。

如果您想要在 NetApp 支援網站上使用 Digital Advisor 儀表板和功能，則必須啟用 AutoSupport。

"Digital Advisor 文件"

AutoSupport 套件中包含的資訊

AutoSupport 套件包含下列檔案和詳細資料。

檔案名稱	欄位	說明
AutoSupport 歷史記錄 .xml	AutoSupport 序號 + 此 AutoSupport 的目的地 + 交付狀態 + 交付嘗試 + AutoSupport 主旨 + 交付 URI + 上次錯誤 + AutoSupport Put 檔案名稱 + 產生時間 + AutoSupport 壓縮大小 + AutoSupport 解壓縮大小 + 總收集時間（毫秒）	AutoSupport 歷程檔案。
AutoSupport .xml	節點 + 通訊協定：聯絡支援 + 支援網址（ HTTP/HTTPS ） + 支援位址 + AutoSupport 隨選狀態 + AutoSupport 隨選伺服器 URL + AutoSupport 隨選輪詢間隔	AutoSupport 狀態檔案。提供使用的通訊協定、技術支援 URL 和位址、輪詢間隔、以及啟用或停用的隨選 AutoSupport 等詳細資料。
buckets 。 xml	貯體 ID + 帳戶 ID + 建置版本 + 位置限制組態 + 啟用法規遵循組態 + 啟用 S3 物件鎖定 + S3 物件鎖定組態 + 一致性組態 + 啟用 CORS 組態 + 啟用上次存取時間 + 啟用原則組態 + 啟用通知 + 啟用通知組態 + 啟用雲端鏡射組態 + 啟用搜尋組態標記 + 啟用貯體組態版本設定	提供貯體層級的組態詳細資料和統計資料。貯體組態範例包括平台服務、法規遵循及貯體一致性。
GRID 組態 .xml	屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	全網格組態資訊檔案。包含有關網格憑證、中繼資料保留空間、網格範圍組態設定（符合性、 S3 物件鎖定、物件壓縮、警示、系統記錄和 ILM 組態）、銷毀編碼設定檔詳細資料、 DNS 名稱和"NMS 名稱"的資訊。
GRE-SPEC.xml	網格規格、原始 XML	用於設定及部署 StorageGRID 。包含網格規格、 NTP 伺服器 IP 、 DNS 伺服器 IP 、網路拓撲和節點的硬體設定檔。
GRID 工作 .xml	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	網格工作（維護程序）狀態檔案。提供網格作用中、終止、完成、失敗及擱置工作的詳細資料。
GRB.JSON	Grid + Revision + 軟體版本 + 說明 + 授權 + 密碼 + DNS + NTP + 站台 + 節點	網格資訊。
ILM 組態 .xml	屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	ILM 組態的屬性清單。

檔案名稱	欄位	說明
ILM-STATUS.xml	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	ILM 計量資訊檔案。包含每個節點的 ILM 評估率、以及全網格的計量。
ILM 。 xml	ILM 原始 XML	ILM 作用中原則檔案。包含使用中 ILM 原則的詳細資料、例如儲存池 ID 、擷取行為、篩選器、規則和說明。
log.Tgz	*n*	可下載的記錄檔。包含 `bycast-err.log`和 `servermanager.log`來自每個節點。
Manifest.xml	此資料的收集順序 + AutoSupport 內容檔名 + 此資料項目的說明 + 收集的位元組數 + 收集時間 + 此資料項目的狀態 + 此資料的錯誤說明 + AutoSupport 內容類型 +	包含 AutoSupport 中繼資料及所有 AutoSupport 檔案的簡短說明。
NMS-Entitys.xml	屬性索引 + 實體 OID + 節點 ID + 裝置型號 ID + 裝置機型版本 + 實體名稱	中的群組和服務實體"NMS 樹狀結構"。提供網格拓撲詳細資料。節點可根據節點上執行的服務來決定。
objectS-status.xml	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	物件狀態、包括背景掃描狀態、作用中傳輸、傳輸率、總傳輸率、刪除率、毀損的片段、遺失物件、遺失物件、嘗試修復、掃描速度、預估掃描期間、以及修復完成狀態。
Server-status.xml	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	伺服器組態。包含每個節點的下列詳細資料：平台類型、作業系統、安裝的記憶體、可用記憶體、儲存設備連線、儲存設備機箱序號、儲存控制器故障磁碟機數、運算控制器機箱溫度、運算硬體、運算控制器序號、電源供應器、磁碟機大小和磁碟機類型。
service-status.xml	節點 + 服務路徑 + 屬性 ID + 屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	服務節點資訊檔案。包含詳細資料、例如分配的表格空間、可用的表格空間、資料庫的 Reaper 指標、區段修復持續時間、修復工作持續時間、自動重新啟動工作、以及自動終止工作。
儲存等級 .xml	儲存等級 ID + 儲存等級名稱 + 儲存節點 ID + 儲存節點路徑	每個儲存節點的儲存等級定義檔。

檔案名稱	欄位	說明
摘要屬性 .xml	群組 OID + 群組路徑 + 摘要屬性 ID + 摘要屬性名稱 + 值 + 索引 + 表格 ID + 表格名稱	彙總 StorageGRID 使用資訊的高階系統狀態資料。提供詳細資料、例如網格名稱、網站名稱、每個網格和每個網站的儲存節點數量、授權類型、授權容量和使用量、軟體支援條款、以及 S3 作業的詳細資料。
system-alerts.xml	名稱 + 嚴重性 + 節點名稱 + 警示狀態 + 站台名稱 + 警示觸發時間 + 警示解決時間 + 規則 ID + 節點 ID + 站台 ID + 靜音 + 其他附註 + 其他標籤	指出 StorageGRID 系統中潛在問題的目前系統警示。
USERAGENTS.xml	使用者代理程式 + 天數 + HTTP 要求總計 + 擷取的總位元組 + 擷取的總位元組 + 放置要求 + 取得要求 + 刪除要求 + 前端要求 + 後端要求 + 選項要求 + 平均要求時間（毫秒） + 平均擱置要求時間（毫秒） + 平均要求後時間（毫秒） + 平均要求時間（毫秒） + 平均要求時間（毫秒）選項	以應用程式使用者代理程式為基礎的統計資料。例如、每個使用者代理程式的放置 / 取得 / 刪除 / 顯示頭作業數、以及每項作業的總位元組大小。
X-header-data	NetApp asup-General-on + NetApp asup-hostname + NetApp asup-OS 版本 + NetApp asup-SERIAL -num + NetApp asup-Subject + NetApp asup-system-id + NetApp asup-model 名稱 +	AutoSupport 標頭資料。

在 **StorageGRID** 中設定 **AutoSupport**

此 AutoSupport 功能可讓您的 StorageGRID 系統定期和根據事件向技術支援傳送運作健全狀況和狀態訊息，從而實現主動式監控和疑難排解。StorageGRID AutoSupport 也支援使用 Digital Advisor 進行預測性建議。

預設情況下，當您首次安裝 StorageGRID 時，基於軟體的 StorageGRID 系統會啟用每週和事件觸發的 AutoSupport 功能。但是，您必須在每個應用裝置上設定硬體 AutoSupport。如有需要，您可以變更 AutoSupport 組態。

如果要變更 StorageGRID AutoSupport 的組態，請僅在主要管理節點上進行變更。

開始之前

- 您已使用 "支援的網頁瀏覽器" 登入主要管理節點上的 Grid Manager。
- 您有"root 存取權限"。

- 如果您使用 HTTPS 傳送 AutoSupport 套件，則您已向主要管理節點提供傳出網際網路存取，可以直接提供，也可以透過其他方式 "使用 Proxy 伺服器" 提供（不需要傳入連線）。
- 如果在 StorageGRID AutoSupport 頁面上選擇了 HTTP，則必須"已設定 Proxy 伺服器"以 HTTPS 方式轉送 AutoSupport 套件。NetApp 的 AutoSupport 伺服器將拒絕使用 HTTP 傳送的套件。
- 如果您使用 SMTP 作為 AutoSupport 套件的傳輸協定，您將擁有"已設定電子郵件伺服器"。

關於這項工作

您可以使用下列任一選項組合、將 AutoSupport 套件傳送至技術支援：

- * 每週 * ：每週自動傳送一次 AutoSupport 套件。預設設定：已啟用。
- * 事件觸發 * ：每小時或發生重大系統事件時自動傳送 AutoSupport 套件。預設設定：已啟用。
- * 隨選 * ：允許技術支援人員要求您的 StorageGRID 系統自動傳送 AutoSupport 套件、這在他們主動處理問題時很有用（需要 HTTPS AutoSupport 傳輸協定）。預設設定：停用。
- * 使用者觸發 * ：隨時手動傳送 AutoSupport 套件。
- 日誌收集："手動收集日誌檔案和系統資料並發送AutoSupport套件" 。

設定 **AutoSupport**

若要變更 AutoSupport 的安裝預設組態，或在每個 StorageGRID 應用裝置上設定硬體 AutoSupport：

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選取您要用來傳送 AutoSupport 套件的傳輸協定。

   - * HTTPS *：這是新安裝的預設及建議設定。此通訊協定使用連接埠 443 。如果您想要啟用 AutoSupport on Demand 功能、則必須使用 HTTPS 。
   - **HTTP**：如果您選擇 HTTP，則必須"設定 Proxy 伺服器"將 AutoSupport 封包轉送為 HTTPS。NetApp 的 AutoSupport 伺服器會拒絕使用 HTTP 傳送的封包。此協定使用 80 連接埠。
   - **SMTP**：如果您希望透過電子郵件傳送 AutoSupport 套裝組合，請使用此選項。您必須先"設定電子郵件伺服器"。

   您設定的協定用於傳送所有 AutoSupport 套件，但 AutoSupport on Demand 除外，該功能需要使用 HTTPS 協定。

3. 如果您選取 **HTTPS** 、請選取是否要使用 NetApp 支援憑證（ TLS 憑證）來保護連線至技術支援伺服器的安全。

   - * 驗證憑證 *（預設）：確保 AutoSupport 套件的傳輸安全無虞。NetApp支援證書已隨StorageGRID 支援軟體一起安裝。
   - 不驗證憑證：只有在有充分理由不使用憑證驗證時（例如憑證暫時有問題時）、才選取此選項。

4. 如果您選擇了 **SMTP**，請使用 **Sender** 欄位輸入您先前設定的電子郵件伺服器位址。
5. 選擇*保存*。所有每週、使用者觸發和事件觸發的套件都會使用選取的傳輸協定來傳送。

停用每週 **AutoSupport**

根據預設、 StorageGRID 系統會設定為每週傳送一次 AutoSupport 套件給技術支援。

若要判斷每週 AutoSupport 套件的傳送時間、請前往 * AutoSupport * > * 結果 * 標籤。在 * 每週 AutoSupport * 區段中、查看 * 下一個排程時間 * 的值。

您可以隨時停用每週 AutoSupport 套件的自動傳送功能。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除 * 啟用每週 AutoSupport * 核取方塊。
3. 選擇*保存*。

停用事件觸發的 **AutoSupport**

根據預設、 StorageGRID 系統會設定為每小時傳送一次 AutoSupport 套件給技術支援。

您可以隨時停用事件觸發的 AutoSupport 。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除 * 啟用事件觸發的 AutoSupport * 核取方塊。
3. 選擇*保存*。

啟用**AutoSupport** 隨需功能

根據需求提供支援、協助您解決技術支援部門正在積極處理的問題。AutoSupport

根據預設、AutoSupport 會停用隨需功能。啟用此功能可讓技術支援部門要求您的 StorageGRID 系統自動傳送 AutoSupport 套件。技術支援部門也可以設定AutoSupport 「根據需求進行查詢」的輪詢時間間隔。

技術支援無法啟用或停用 AutoSupport on Demand 。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選取* HTTPS *作為傳輸協定。
3. 選中 *Enable Weekly AutoSupport （每週啓用） * 複選框。
4. 選中 **Enable AutoSupport on Demand** 複選框。
5. 選擇*保存*。

   支援隨需提供支援、技術支援人員可將「根據需求提出的要求」傳送至AutoSupport AutoSupport StorageGRID

停用軟體更新檢查

根據預設、StorageGRID 此功能會聯絡NetApp以判斷您的系統是否有可用的軟體更新。如果StorageGRID 有可用的更新版本或更新版本、則StorageGRID 更新版本會顯示在「更新版」頁面上。

視需要、您可以選擇停用軟體更新檢查。例如、如果您的系統沒有WAN存取、您應該停用檢查、以避免下載錯誤。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 清除 * 檢查軟體更新 * 核取方塊。
3. 選擇*保存*。

新增**AutoSupport** 其他的目的地

啟用 AutoSupport 時、 heath 和 status 套件會傳送至技術支援。您可以為所有 AutoSupport 套件指定一個額外目的地。

若要驗證或變更用於傳送 AutoSupport 套件的通訊協定，請參閱以下說明 設定 AutoSupport。

您無法使用 SMTP 傳輸協定將 AutoSupport 套件傳送至其他目的地。

步驟

1. 選擇 支援 > 工具 > **AutoSupport** > 設定。
2. 選取 * 啟用其他 AutoSupport 目的地 * 。
3. 指定下列項目：

主機名稱

其他 AutoSupport 目的地伺服器的伺服器主機名稱或 IP 位址。

您只能輸入一個額外的目的地。

連接埠

用於連接至其他 AutoSupport 目的地伺服器的連接埠。預設為 HTTP 連接埠 80 或 HTTPS 連接埠 443 。

憑證驗證

是否使用 TLS 憑證來保護連線至其他目的地的安全。

- 選取 * 驗證憑證 * 以使用憑證驗證。
- 選取 * 不驗證憑證 * 、即可在沒有憑證驗證的情況下傳送 AutoSupport 套件。

  只有當您有充分理由不使用憑證驗證時（例如憑證暫時有問題時）、才選取此選項。

4. 如果您選取 * 驗證憑證 * 、請執行下列步驟：
   a. 瀏覽至 CA 憑證的位置。
   b. 上傳 CA 憑證檔案。

   CA 憑證中繼資料即會出現。
5. 選擇*保存*。

所有未來的每週、事件觸發及使用者觸發 AutoSupport 套件都會傳送至其他目的地。

[[autosup-for -ariance]] 設定應用裝置的 **AutoSupport**

AutoSupport for Appliance 回報 StorageGRID 硬體問題、而 StorageGRID AutoSupport 回報 StorageGRID 軟體問題、但有一個例外：對於 SGF6112 、 StorageGRID AutoSupport 同時報告硬體和軟體問題。您必須在每個應用裝置上設定 AutoSupport 、 SGF6112 除外、因為 SGF6112 不需要額外的組態。AutoSupport 在服務應用裝置和儲存設備上的實作方式有所不同。

您可以使用 SANtricity 為每個儲存設備啟用 AutoSupport 。您可以在初始應用裝置設定期間或安裝應用裝置之後、設定 SANtricity AutoSupport ：

- 對於 SG6000 和 SG5700 應用裝置、 "在 SANtricity 系統管理員中設定 AutoSupport"

如果您在 "系統管理程式SANtricity" 中設定透過 Proxy 傳遞 AutoSupport，即可將來自 E 系列應用裝置的 AutoSupport 套件包含在 StorageGRID AutoSupport 中。

StorageGRID AutoSupport 不會回報硬體問題、例如 DIMM 或主機介面卡（ HIC ）故障。但是，某些組件故障可能會觸發"硬體警示"。對於配備主機板管理控制器（ BMC ）的 StorageGRID 應用裝置、您可以設定電子郵件和 SNMP 設陷來回報硬體故障：

- "設定 BMC 警示的電子郵件通知"
- "設定 BMC 的 SNMP 設定"

相關資訊

- "用於外部通訊的連接埠"
- "NetApp支援"

手動觸發 **StorageGRID** 中的 **AutoSupport** 套件

為了協助技術支援人員疑難排解 StorageGRID 系統的問題、您可以手動觸發要傳送的 AutoSupport 套件。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您具有 Root 存取權限或其他網格配置權限。

步驟

1. 選擇 支援 > 工具 > **AutoSupport**。
2. 在 * 動作 * 索引標籤上、選取 * 傳送使用者觸發的 AutoSupport * 。

   StorageGRID嘗試將AutoSupport套件傳送到NetApp支援站點。如果嘗試成功，則*結果*標籤上的*最近結果*和*上次成功時間*值將會更新。如果出現問題，*最新結果*值將更新為“失敗”，且StorageGRID不會再次嘗試傳送AutoSupport套件。

3. 1 分鐘後，刷新瀏覽器中的AutoSupport頁面以存取最新結果。

此外，您還可以"收集更廣泛的日誌檔案和系統數據"並將它們發送至NetApp支援站點。

StorageGRID 如何處理 AutoSupport 套件故障

查看 StorageGRID 在嘗試傳送 AutoSupport 套件失敗時所採取的動作清單。

StorageGRID 會根據 AutoSupport 套件類型採取不同的動作。您可以選取 **Support** > **Tools** > **AutoSupport** > **Results**，以查看 AutoSupport 套件的狀態。

當 AutoSupport 套件無法傳送時、「失敗」會出現在 * AutoSupport * 頁面的 * 結果 * 索引標籤上。

> 如果您設定了 Proxy 伺服器將 AutoSupport 套件轉送到 NetApp，"確認 Proxy 伺服器組態設定正確無誤"。

每週 AutoSupport 套件故障

如果每週 AutoSupport 套件無法傳送、 StorageGRID 系統會採取下列動作：

1. 將最新的結果屬性更新為「Retrying（重新執行）」。
2. 每四分鐘嘗試重新傳送 AutoSupport 套件 15 次、持續一小時。
3. 傳送失敗一小時後、將最近的「結果」屬性更新為「失敗」。
4. 嘗試在下一次排程時間再次傳送 AutoSupport 套件。
5. 如果套件因為 NMS 服務無法使用而失敗、且套件在七天內傳送、則會維持正常的 AutoSupport 排程。
6. 當 NMS 服務再次可用時、如果一個套件尚未傳送超過七天、就會立即傳送 AutoSupport 套件。

使用者觸發或事件觸發的 AutoSupport 套件故障

如果使用者觸發或事件觸發的 AutoSupport 套件無法傳送、 StorageGRID 系統會採取下列動作：

1. 如果已知錯誤、則顯示錯誤訊息。例如、如果使用者選取 SMTP 傳輸協定而未提供正確的電子郵件組態設定、則會顯示下列錯誤： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不會再次嘗試傳送套件。
3. 將錯誤記錄在中 `nms.log`。

如果發生故障且所選協定為 SMTP，則 AutoSupport 頁面上可能會出現下列錯誤訊息： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

瞭解如何"設定電子郵件伺服器設定"。

修正 AutoSupport 套件故障

如果發生故障且所選協定為 SMTP，請驗證 StorageGRID 系統的郵件伺服器設定是否正確，以及您的郵件伺服器是否正在運作。以下錯誤訊息可能會顯示在 AutoSupport 頁面上：由於郵件伺服器頁面上的設定不正確，無法使用 SMTP 協定傳送 AutoSupport 套件。

透過 StorageGRID 傳送 E 系列 AutoSupport 套件

您可以透過 StorageGRID 管理節點、而非儲存設備管理連接埠、將 E 系列 SANtricity 系

統管理員 AutoSupport 套件傳送給技術支援。

如需搭配 E 系列應用裝置使用 AutoSupport 的詳細資訊、請參閱 "E 系列硬體 AutoSupport"。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"儲存設備管理員或根存取權限"。
- 您已設定 SANtricity AutoSupport ：
  - 對於 SG6000 和 SG5700 應用裝置、 "在 SANtricity 系統管理員中設定 AutoSupport"

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

關於這項工作

E 系列 AutoSupport 套件包含儲存硬體的詳細資料、比 StorageGRID 系統傳送的其他 AutoSupport 套件更為具體。

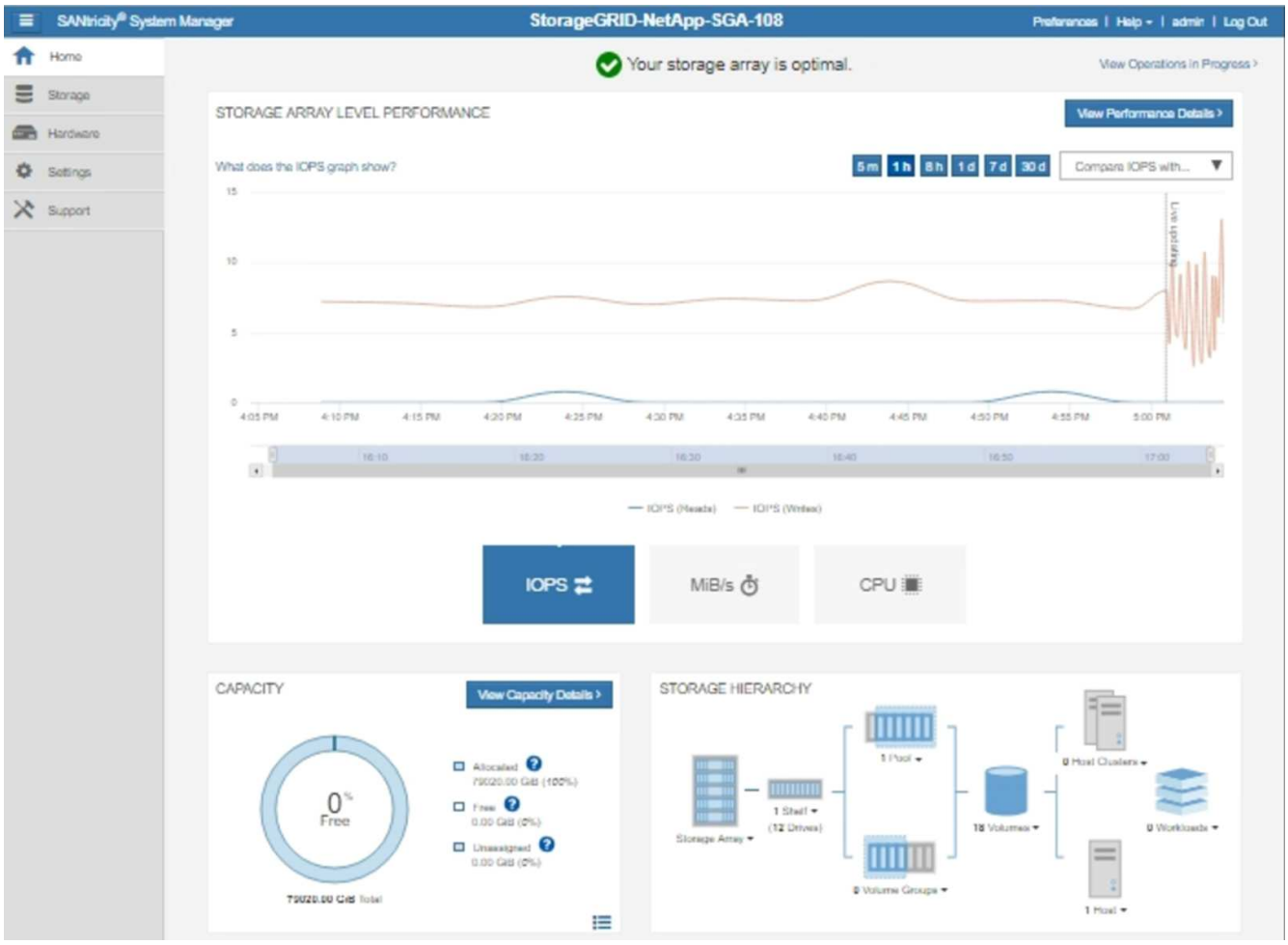
您可以在 SANtricity 系統管理員中設定特殊的 Proxy 伺服器位址、以便透過 StorageGRID 管理節點傳輸 AutoSupport 套件、而無需使用應用裝置的管理連接埠。以這種方式傳輸的 AutoSupport 套件會由傳送"偏好的寄件者管理節點"、而且會使用在 Grid Manager 中設定的任何"管理 Proxy 設定"套件。

> 此程序僅適用於設定 E 系列 AutoSupport 套件的 StorageGRID Proxy 伺服器。如需 E 系列 AutoSupport 組態的詳細資訊，請參閱 "NetApp E系列與SANtricity VMware文檔"。

步驟

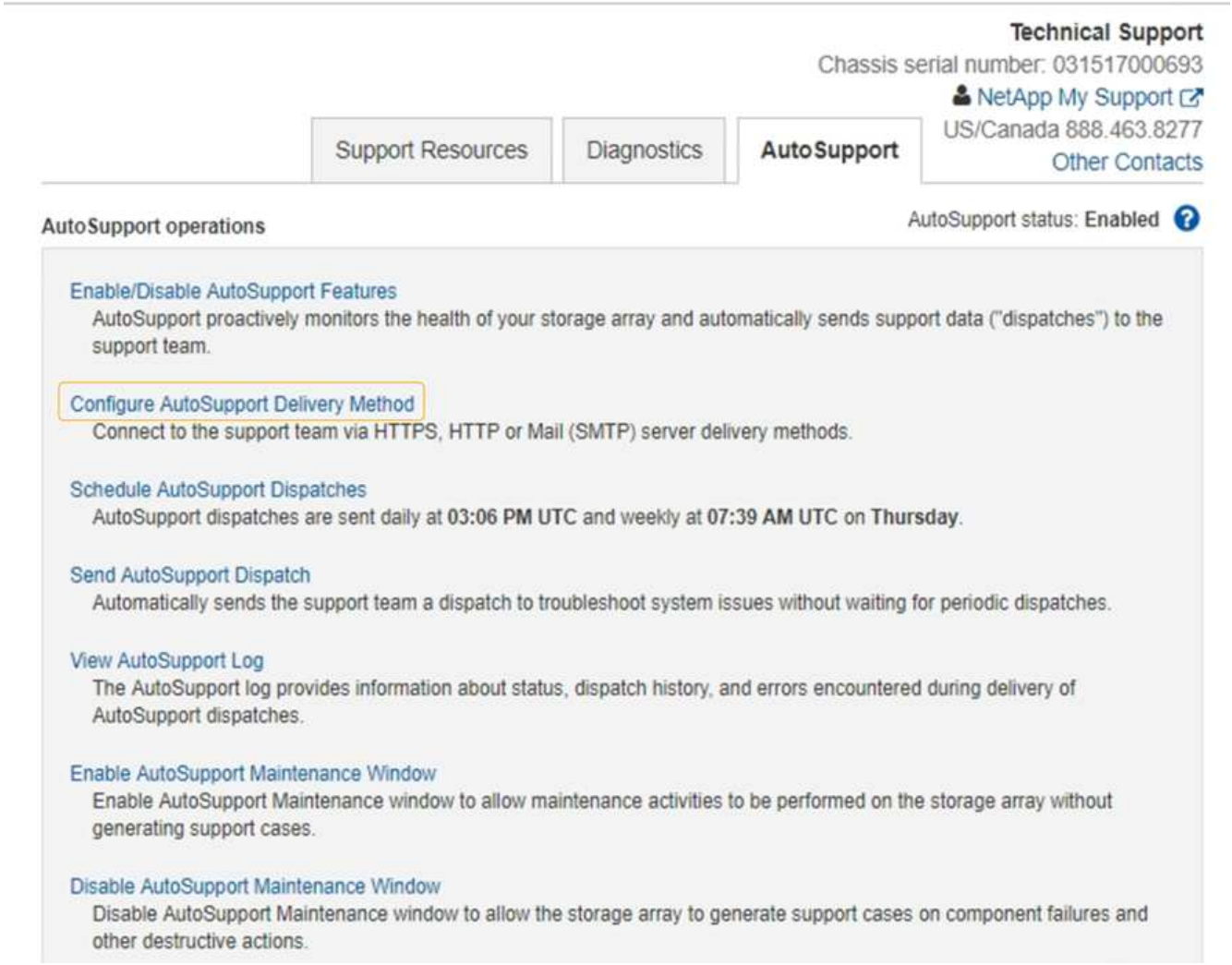
1. 在網格管理器中，選擇*節點*。
2. 從左側節點清單中、選取您要設定的儲存應用裝置節點。
3. 選擇* SANtricity 《系統管理程式》*。

   出現「系統管理程式」首頁。SANtricity



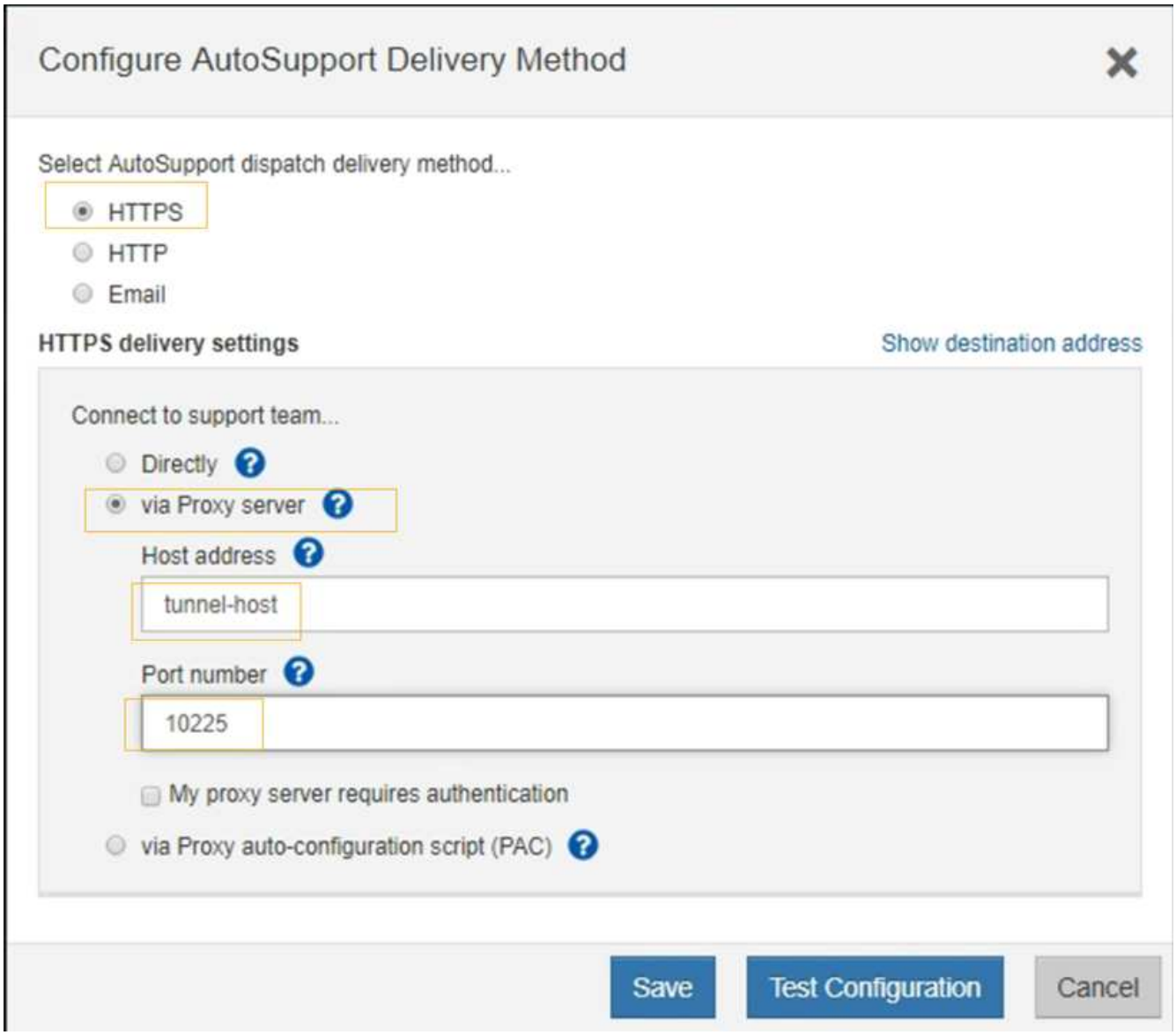
4. 選擇*支援* > 支援中心 > **AutoSupport**。

   畫面上會出現「介紹操作」頁面。AutoSupport



5. 選擇*設定AutoSupport 「供應方法」*。

   此時會出現「設定AutoSupport 供應方法」頁面。



6. 選擇* HTTPS *作為交付方法。

   已預先安裝啟用 HTTPS 的憑證。

7. 選擇*透過Proxy伺服器*。
8. 輸入 `tunnel-host` * 主機位址 * 。

   `tunnel-host`是使用管理節點傳送 E 系列 AutoSupport 套件的特殊位址。

9. 輸入 `10225` * 連接埠號碼 * 。

   `10225`是 StorageGRID Proxy 伺服器上的連接埠編號、可從應用裝置的 E 系列控制器接收 AutoSupport 套件。

10. 選擇*測試組態*來測試AutoSupport 您的Proxy伺服器的路由和組態。

    如果正確、綠色橫幅中會出現訊息：「您的 AutoSupport 組態已通過驗證。」

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

11. 選擇*保存*。

    隨即儲存組態、並顯示確認訊息：「 AutoSupport 傳遞方法已設定。」

監控StorageGRID 一個系統

定期監控您的 StorageGRID 系統、以確保其正常運作。

開始之前

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

> 若要變更 Grid Manager 中顯示的儲存值單位、請選取 Grid Manager 右上角的使用者下拉式選單、然後選取 * 使用者偏好 * 。

關於這項工作

這些指示說明如何：

- "檢視及管理儀表板"
- "檢視「節點」頁面"
- "定期監控系統的這些層面："
  - "系統健全狀況"
  - "儲存容量"
  - "資訊生命週期管理"
  - "網路與系統資源"
  - "租戶活動"
  - "負載平衡作業"
  - "網格同盟連線"
- "管理警示"
- "檢視記錄檔"
- "設定日誌管理和外部系統日誌伺服器"
- "使用外部syslog伺服器"以收集稽核資訊
- "使用 SNMP 進行監控"
- "更改 I/O 優先權"改變 I/O 操作的相對優先權

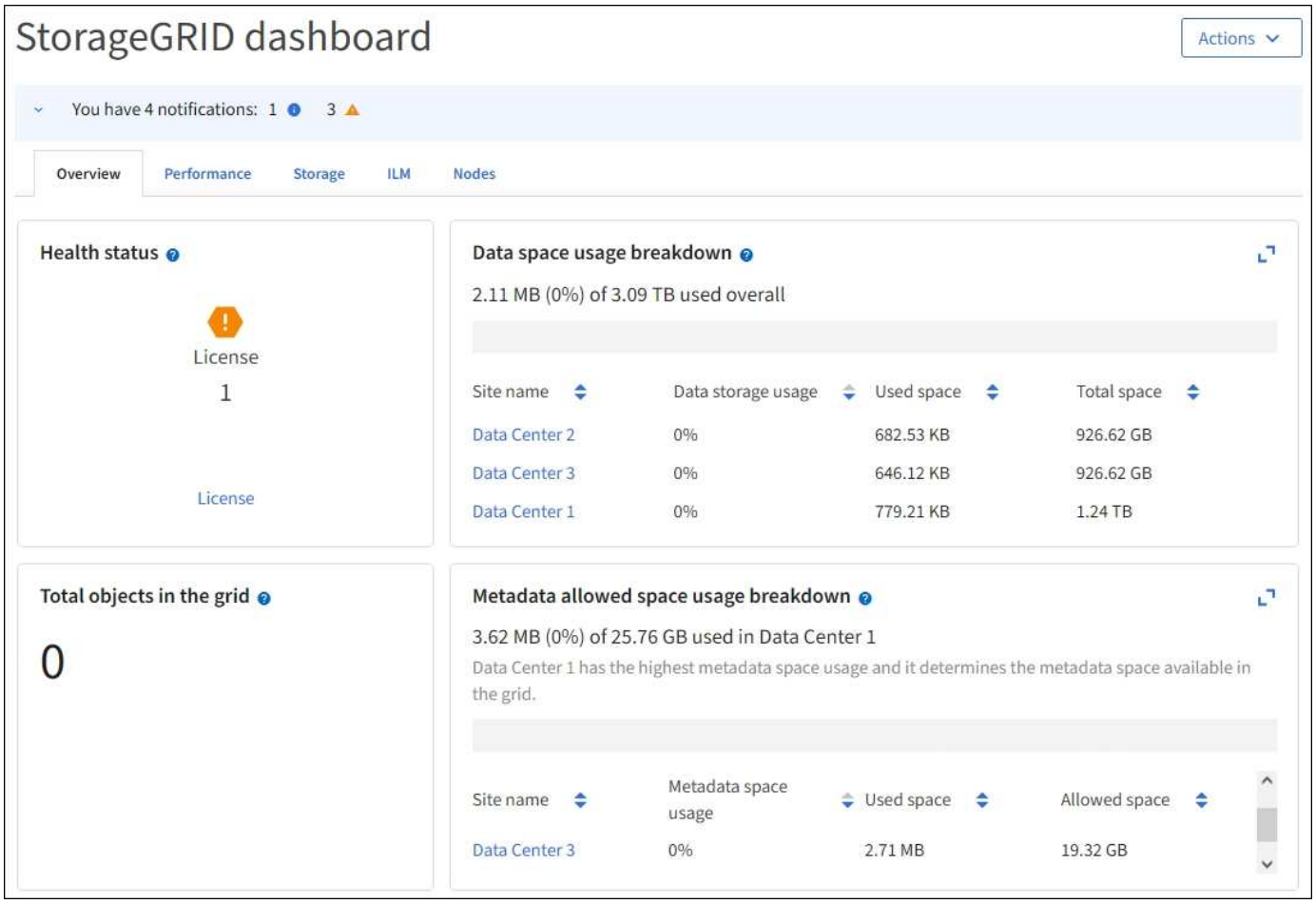
在 StorageGRID 中檢視及管理儀表板

您可以使用儀表板一眼就能監控系統活動。您可以建立自訂儀表板來監控 StorageGRID 的

實作。

若要變更 Grid Manager 中顯示的儲存值單位、請選取 Grid Manager 右上角的使用者下拉式選單、然後選取 * 使用者偏好 * 。

您的儀表板可能會因系統組態而異。



檢視儀表板

儀表板由包含 StorageGRID 系統特定資訊的索引標籤所組成。每個索引標籤都包含顯示在卡片上的資訊類別。

您可以使用系統提供的儀表板。此外、您也可以建立自訂儀表板、只包含與監控 StorageGRID 實作相關的標籤和卡片。

系統提供的儀表板索引標籤包含下列資訊類型的卡片：

系統所提供儀表板上的索引標籤	包含
總覽	網格的一般資訊、例如作用中警示、空間使用量、以及網格中的物件總數。
效能	空間使用量、長期使用的儲存設備、 S3 作業、要求持續時間、錯誤率。

系統所提供儀表板上的索引標籤	包含
儲存設備	租戶配額使用量和邏輯空間使用量。預測使用者資料和中繼資料的空間使用量。
ILM	資訊生命週期管理佇列與評估率。
節點	CPU 、資料和記憶體使用量、依節點而定。S3 依節點執行作業。節點對站台發佈。

部分卡片可以最大化以便更清晰地查看。選擇卡片右上角的最大化圖示 。若要關閉已最大化的卡片，請選擇最小化圖示 或選取 **Close**。

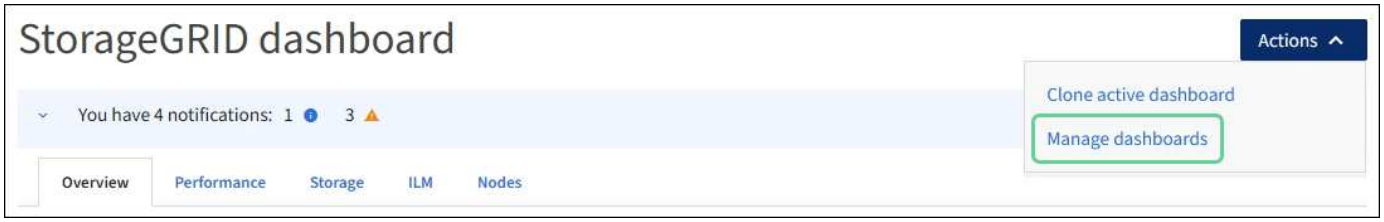
管理儀表板

如果您擁有 root 存取權（請參閱"管理群組權限"）、您可以針對儀表板執行下列管理工作：

- 從頭建立自訂儀表板。您可以使用自訂儀表板來控制要顯示哪些 StorageGRID 資訊、以及該資訊的組織方式。
- 複製儀表板以建立自訂儀表板。
- 設定使用者的作用中儀表板。作用中儀表板可以是系統提供的儀表板或自訂儀表板。
- 設定預設儀表板、這是所有使用者除非啟動自己的儀表板、否則會看到的內容。
- 編輯儀表板名稱。
- 編輯儀表板以新增或移除索引標籤和卡片。您可以有至少 1 個索引標籤、最多 20 個索引標籤。
- 移除儀表板。

如果您除了「根目錄」存取權限之外、還擁有其他任何權限、則只能設定作用中的儀表板。

若要管理儀表板、請選取 * 動作 * > * 管理儀表板 * 。



設定儀表板

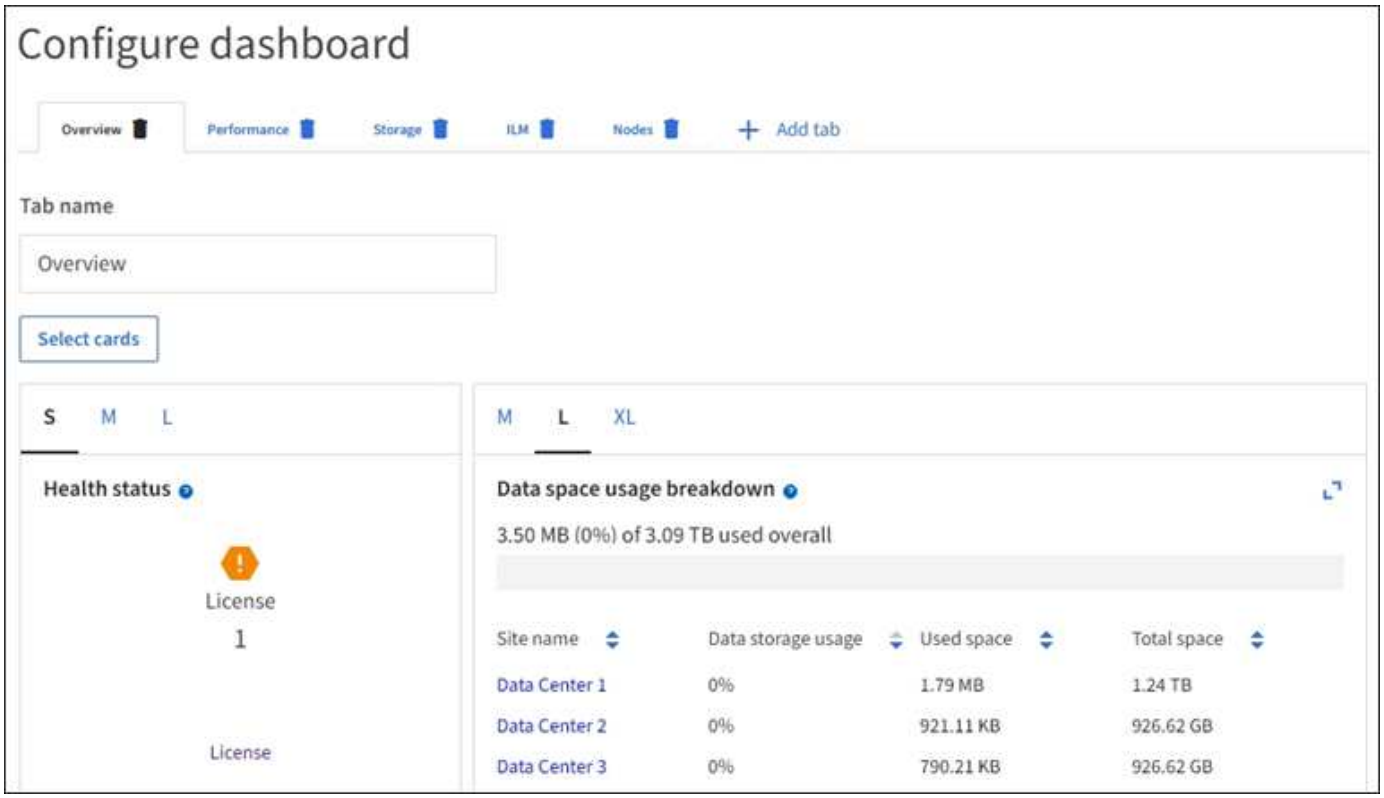
若要透過複製作用中儀表板來建立新的儀表板、請選取 * 動作 * > * 複製作用中儀表板 * 。

若要編輯或複製現有的儀表板、請選取 * 動作 * > * 管理儀表板 * 。

系統提供的儀表板無法編輯或移除。

設定儀表板時、您可以：

- 新增或移除索引標籤
- 重新命名索引標籤、並為新的索引標籤命名唯一的名稱
- 為每個索引標籤新增、移除或重新排列（拖曳）卡片
- 選取卡片頂端的 * S* 、 * M* 、 * L* 或 * XL* 、以選取個別卡片的大小



檢視「節點」頁面

檢視 **StorageGRID Nodes** 頁面

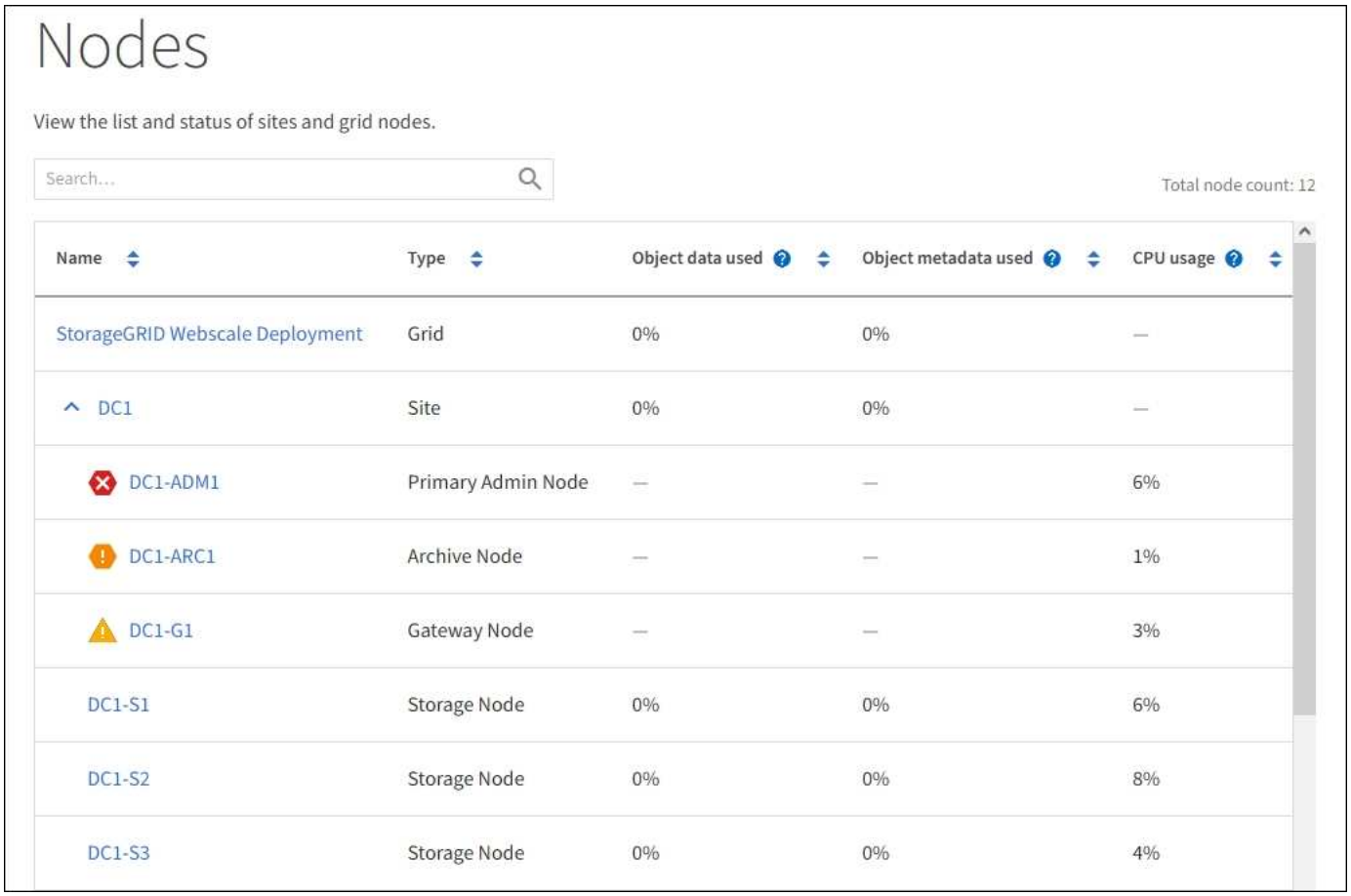
當您需要比儀表板更詳細的 StorageGRID 系統資訊時、可以使用「節點」頁面來檢視整個網格、網格中的每個站台、以及站台上的每個節點的度量。

「節點」表格會列出整個網格、每個站台及每個節點的摘要資訊。如果節點中斷連線或有作用中警示、節點名稱旁會出現圖示。如果節點已連線且沒有作用中的警示、則不會顯示任何圖示。

當節點未連線至網格時、例如在升級期間或中斷連線狀態時、某些度量可能無法使用或排除在站台和網格總計之外。節點重新連線至網格之後、請等待數分鐘、讓值穩定下來。

若要變更 Grid Manager 中顯示的儲存值單位、請選取 Grid Manager 右上角的使用者下拉式選單、然後選取 * 使用者偏好 * 。

所示的螢幕擷取畫面為範例。您的結果可能會因 StorageGRID 版本而異。



連線狀態圖示

如果節點與網格中斷連線、下列任一圖示會出現在節點名稱旁。

圖示	說明	需要採取行動
	未連線-未知 由於不明原因、節點中斷連線或節點上的服務意外停機。例如、節點上的服務可能會停止、或是節點因為停電或非預期的停電而失去網路連線。 也可能會觸發*無法與node*通訊警示。其他警示也可能處於作用中狀態。	需要立即注意。"選取每個警示"並遵循建議的行動。 例如、您可能需要重新啟動已停止或重新啟動節點主機的服務。 • 注意 * ：在託管關機作業期間、節點可能會顯示為「未知」。在這些情況下、您可以忽略「未知」狀態。

圖示	說明	需要採取行動
	未連線-管理性關機 由於預期的原因、節點未連線至網格。 例如、節點或節點上的服務已正常關機、節點正在重新開機、或軟體正在升級。一個或多個警示也可能處於作用中狀態。 根據基礎問題、這些節點通常會在不需介入的情況下重新上線。	判斷是否有任何警示影響此節點。 如果有一個或多個警示處於作用中"選取每個警示"狀態、請遵循建議的動作。

如果節點與網格中斷連線、可能會有基礎警示、但只會顯示「未連線」圖示。若要查看節點的作用中警示、請選取節點。

警示圖示

如果節點有作用中警示、節點名稱旁會出現下列其中一個圖示：

Critical：StorageGRID 節點或服務出現異常情況，導致其正常運作停止。您必須立即解決根本問題。如果問題無法解決，可能會導致服務中斷和資料遺失。

Major：存在異常情況，該情況正在影響目前作業或接近嚴重警示的臨界值。您應調查重大警示並解決任何根本問題，以確保異常情況不會停止 StorageGRID 節點或服務的正常運作。

Minor：系統目前運作正常，但有異常情況，如果持續下去可能會影響系統運作。您應監控並解決不會自行消失的輕微警報，以確保它們不會導致更嚴重的問題。

檢視系統、站台或節點的詳細資料

若要篩選「節點」表格中顯示的資訊、請在「 * 搜尋 * 」欄位中輸入搜尋字串。您可以依系統名稱、顯示名稱或類型進行搜尋（例如、輸入 * gat* 以快速找到所有閘道節點）。

若要檢視網格、站台或節點的資訊：

- 選取網格名稱、即可查看整個StorageGRID 作業系統統計資料的彙總摘要。
- 選取特定的資料中心站台、即可查看該站台所有節點統計資料的彙總摘要。
- 選取特定節點以檢視該節點的詳細資訊。

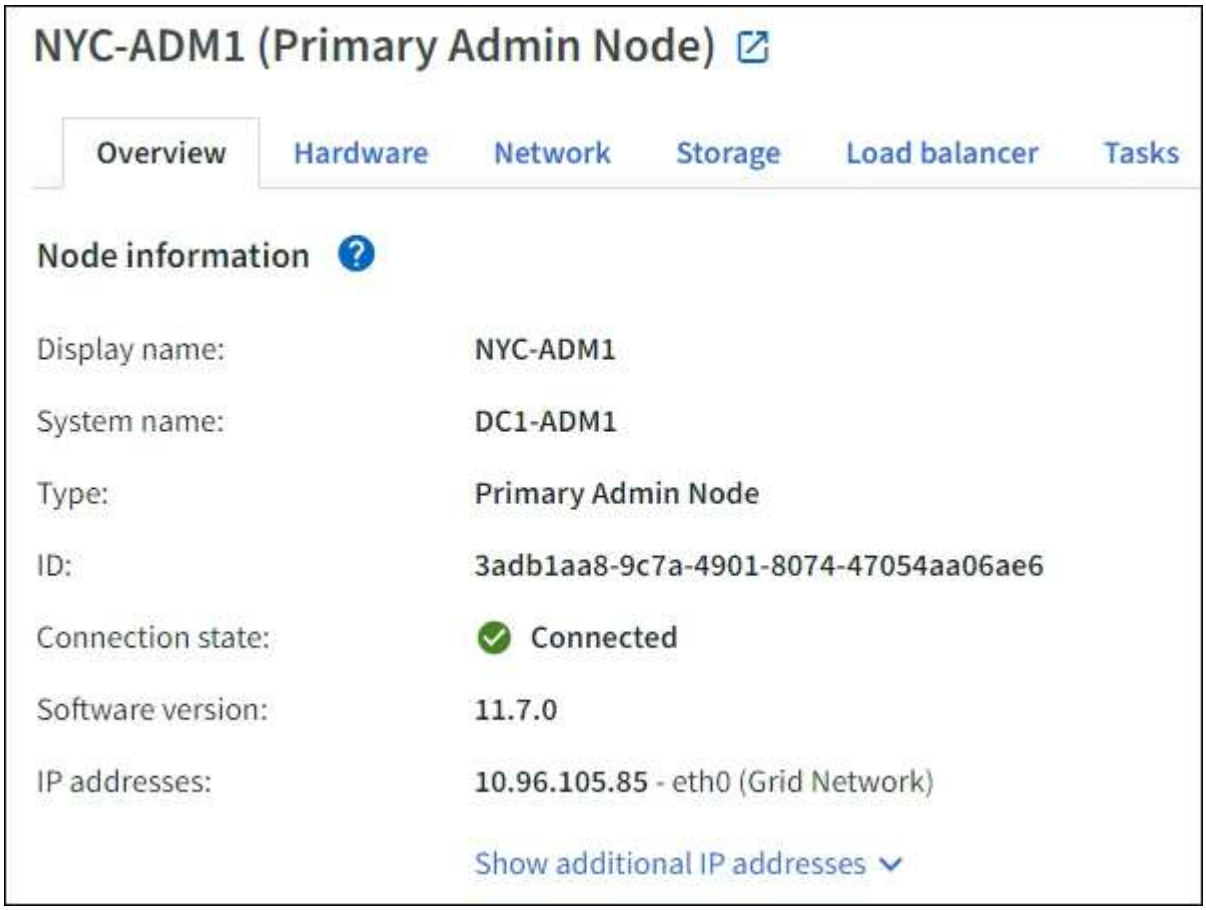
檢視 **StorageGRID** 概覽標籤

「總覽」索引標籤提供每個節點的基本資訊。也會顯示目前影響節點的任何警示。

「總覽」索引標籤會顯示所有節點。

節點資訊

「概觀」索引標籤的「節點資訊」區段會列出有關節點的基本資訊。



節點的總覽資訊包括下列項目：

- * 顯示名稱 * （僅當節點已重新命名時顯示）：節點的目前顯示名稱。請使用"重新命名網格、站台和節點"程序來更新此值。
- * 系統名稱 * ：您在安裝期間為節點輸入的名稱。系統名稱用於內部 StorageGRID 作業、無法變更。
- * 類型 * ：節點類型 - 管理節點、主要管理節點、儲存節點或閘道節點。
- * ID*：節點的唯一識別碼、也稱為UUID。
- 連線狀態：三種狀態之一。此時會顯示最嚴重狀態的圖示。
  - 未知：由於未知原因，節點未連接到網格，或一項或多項服務意外中斷。例如，節點間的網路連線中斷、斷電或某項服務中斷。此時可能還會觸發 無法與節點通訊 警報。此外，可能還有其他警報。這種情況需要立即處理。

    在託管關機作業期間、節點可能會顯示為「未知」。在這些情況下、您可以忽略「未知」狀態。

  - **Administratively down**：節點因預期原因未連接至網格。例如，節點或其上的服務已正常關閉、節點正在重新開機，或軟體正在升級。也可能有一個或多個警示處於作用中狀態。
  - 已連接：節點已連接至網格。
- 使用的儲存設備：僅適用於儲存節點。
  - 物件資料：儲存節點上已使用之物件資料的可用空間總計百分比。

◦ 物件中繼資料：儲存節點上已使用之物件中繼資料的總允許空間百分比。

- 軟體版本：StorageGRID 安裝在節點上的版本。
- * HA Groups *：僅適用於管理節點和閘道節點。顯示節點上的網路介面是否包含在高可用度群組中、以及該介面是否為主要介面。
- **IP** 位址：節點的 IP 位址。選擇 顯示其他 **IP** 位址 可檢視節點的 IPv4 和 IPv6 位址以及介面對映。

警示

Overview （概述）選項卡的 Alerts "目前影響此節點且尚未靜音的警示"（警報）部分列出了任何。選取警示名稱以檢視其他詳細資料和建議的動作。

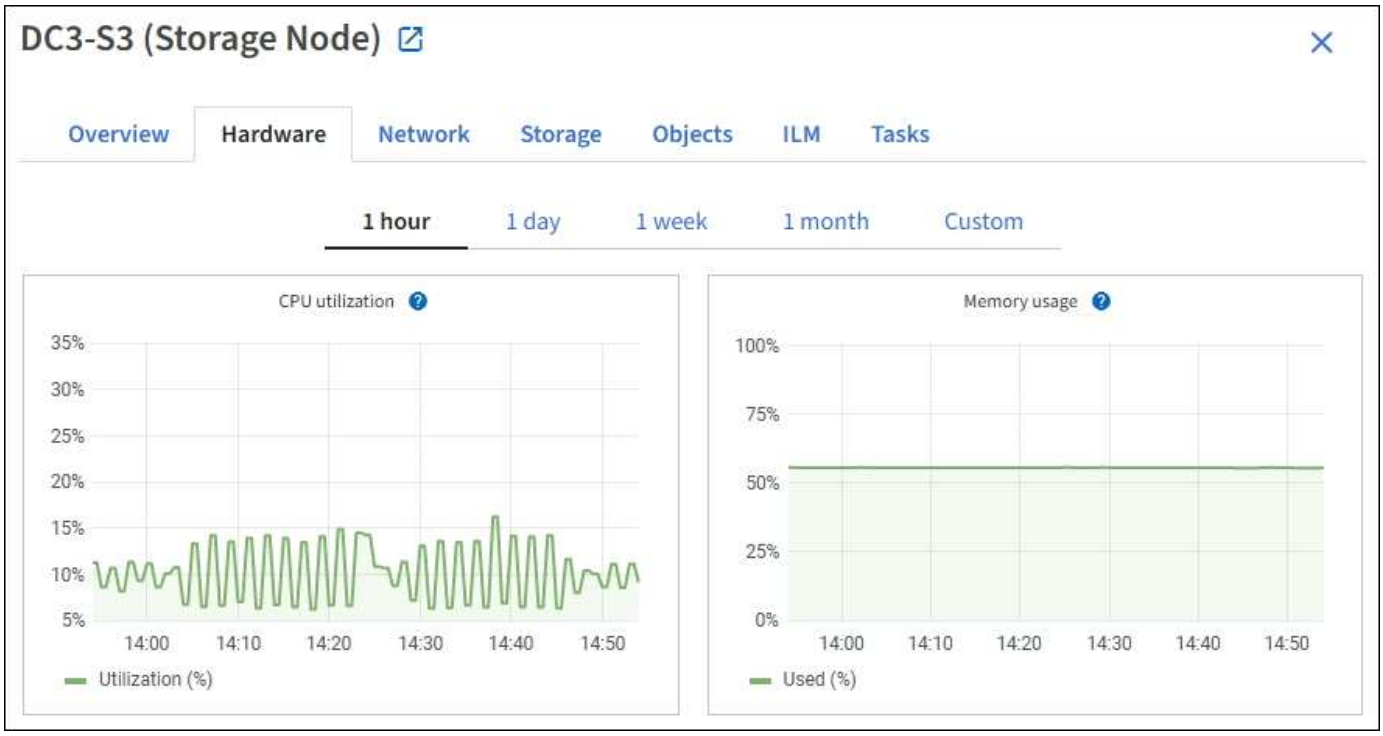
也包含的警示"節點連線狀態"。

檢視 **StorageGRID** 硬體索引標籤

「硬體」索引標籤會顯示每個節點的CPU使用率和記憶體使用量、以及裝置的其他硬體資訊。

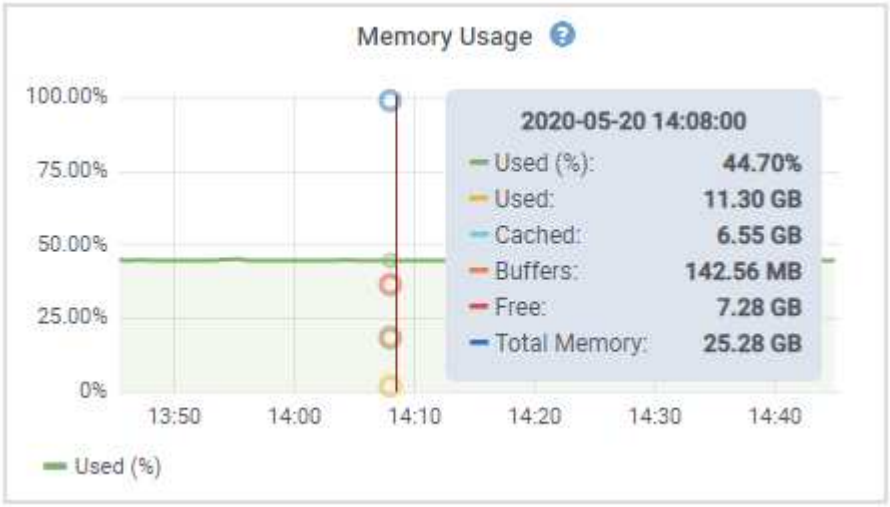
Grid Manager 會隨每個版本一起更新、可能與此頁面上的範例螢幕擷取畫面不符。

顯示所有節點的Hardware（硬體）索引標籤。



若要顯示不同的時間間隔、請選取圖表或圖表上方的其中一個控制項。您可以顯示1小時、1天、1週或1個月的可用時間間隔資訊。您也可以設定自訂時間間隔、以便指定日期和時間範圍。

若要查看 CPU 使用率和記憶體使用率的詳細資料、請將游標放在每個圖表上。



如果節點是應用裝置節點、此索引標籤也會包含一節、其中包含應用裝置硬體的詳細資訊。

檢視應用裝置儲存節點的相關資訊

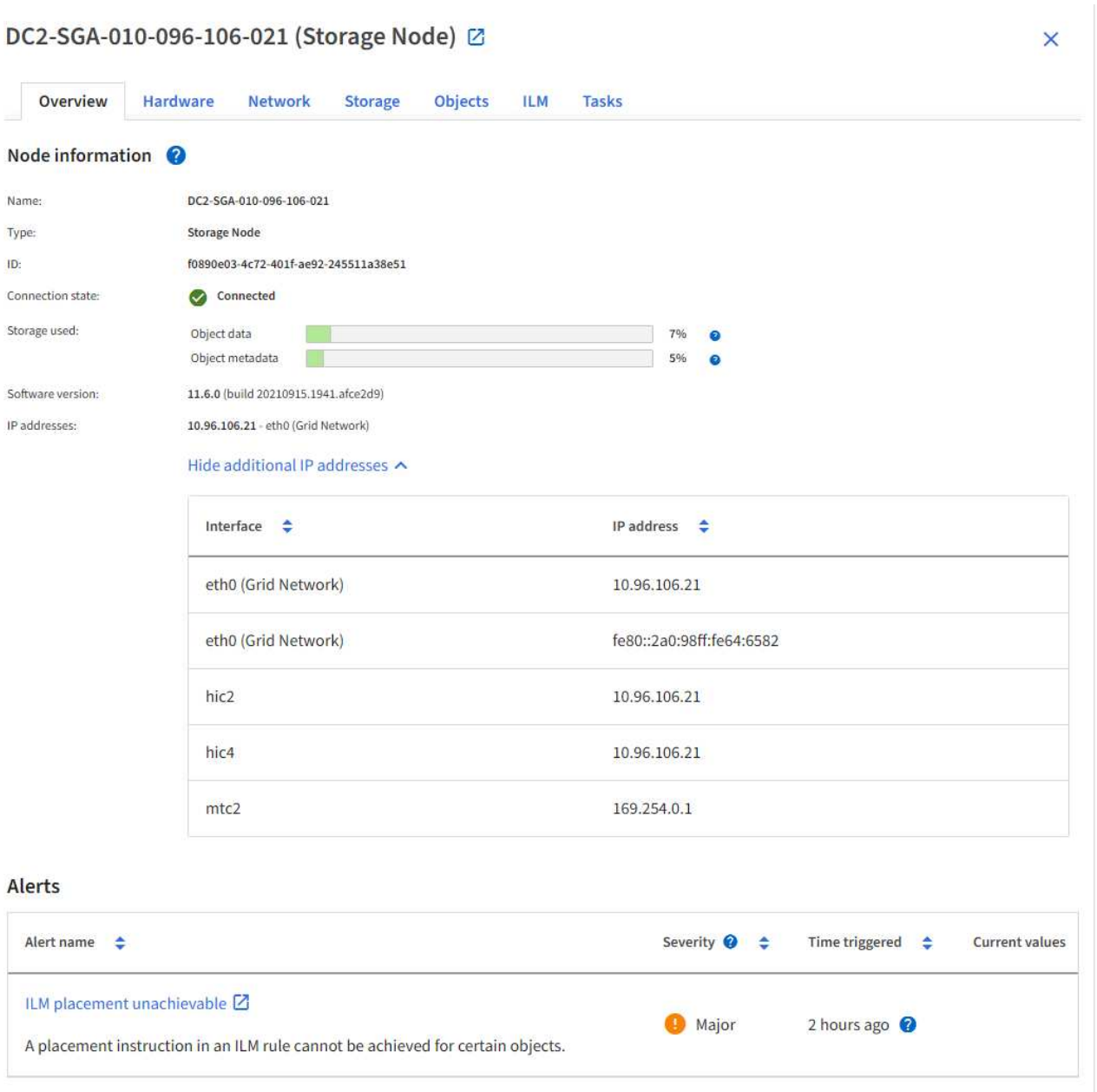
「節點」頁面會列出每個應用裝置儲存節點的服務健全狀況及所有運算、磁碟設備和網路資源相關資訊。您也可以看到記憶體、儲存硬體、控制器韌體版本、網路資源、網路介面、 網路位址、以及接收和傳輸資料。

步驟

1. 從「節點」頁面、選取應用裝置儲存節點。
2. 選擇*總覽*。

「概觀」索引標籤的「節點資訊」區段會顯示節點的摘要資訊、例如節點的名稱、類型、ID和連線狀態。IP位址清單包含每個位址的介面名稱、如下所示：

- * eth*：網格網路、管理網路或用戶端網路。
- * hic*：設備上的實體10、25或100 GbE連接埠之一。這些連接埠可連結在一起、並連接StorageGRID至「資訊網」（eth0）和「用戶端網路」（eth2）。
- * MTC*：設備上實體1 GbE連接埠之一。一個或多個MTC介面會連結、形成StorageGRID 「支援支援者支援者網路介面」（eth1）。您可以保留其他MTC介面、讓資料中心的技術人員暫時在本機連線。

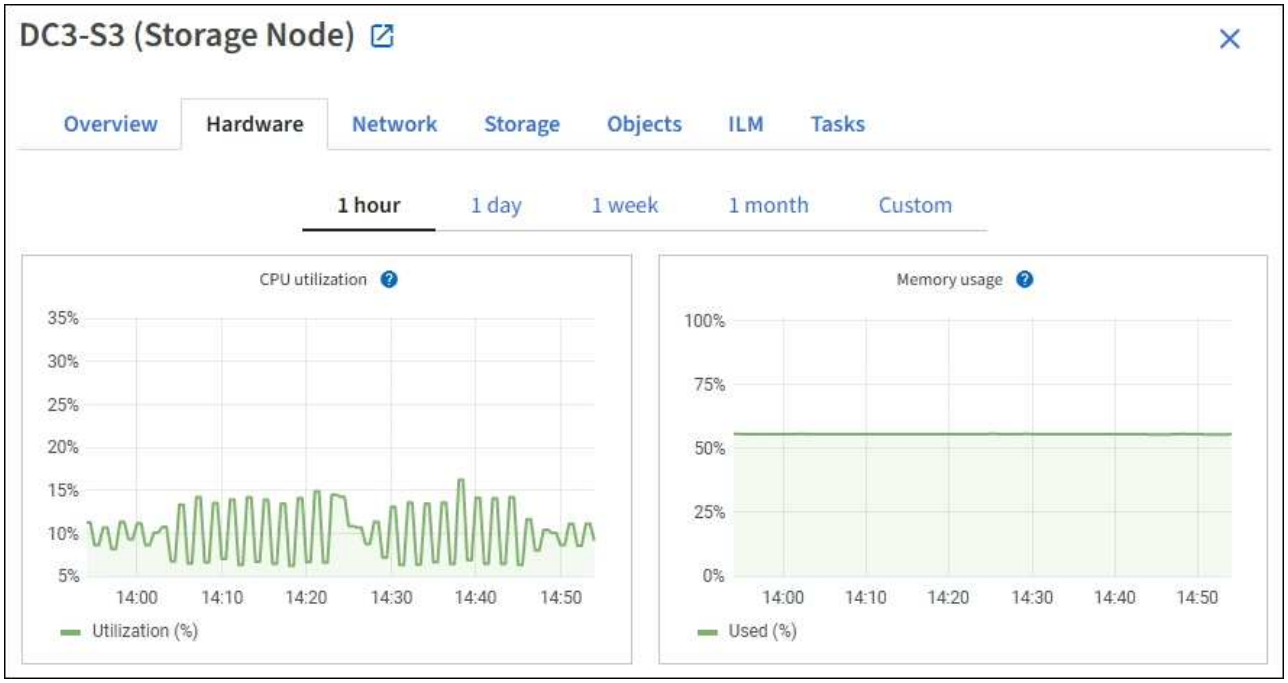


「概觀」索引標籤的「警示」區段會顯示節點的任何作用中警示。

3. 選取*硬體*以查看有關應用裝置的詳細資訊。

   a. 查看 CPU 使用率和記憶體使用率圖表，以了解 CPU 和記憶體容量使用率隨時間變化的百分比。若要顯示不同的時間間隔，請選擇圖表上方的其中一個控制項。您可以顯示 1 小時、1 天、1 週或 1 個月的時

間間隔內的資訊。您也可以設定自訂時間間隔，指定日期和時間範圍。



b. 向下捲動以檢視應用裝置的元件表。此表包含應用裝置的機型名稱、控制器名稱、序號和IP位址、以及每個元件的狀態等資訊。

某些欄位（例如運算控制器BMC IP和運算硬體）僅會針對具有該功能的應用裝置顯示。

儲存櫃和擴充櫃的元件（如果是安裝的一部分）會顯示在應用裝置表格下方的獨立表格中。

欄位	說明
應用裝置機型	此 StorageGRID 應用裝置的型號如 SANtricity OS 所示。
儲存控制器名稱	SANtricity OS 中顯示的此 StorageGRID 應用裝置名稱。
儲存控制器A管理IP	儲存控制器 A 上管理連接埠 1 的 IP 位址。您可以使用此 IP 來存取 SANtricity OS 來疑難排解儲存問題。
儲存控制器B管理IP	儲存控制器 B 上管理連接埠 1 的 IP 位址。您可以使用此 IP 來存取 SANtricity OS 來疑難排解儲存問題。 部分應用裝置機型沒有儲存控制器 B
儲存控制器WWID	SANtricity OS 中顯示的儲存控制器全球識別碼。
儲存應用裝置機箱序號	應用裝置的機箱序號。
儲存控制器韌體版本	此應用裝置儲存控制器上的韌體版本。

欄位	說明
儲存控制器 SANtricity OS 版本	儲存控制器 A 的 SANtricity OS 版本
儲存控制器 NVSRAM 版本	SANtricity 系統管理員報告的儲存控制器 NVSRAM 版本。 對於 SG6060 和 SG6160 、如果兩個控制器之間的 NVSRAM 版本不相符、則會顯示控制器 A 的版本。如果控制器 A 未安裝或無法運作、則會顯示控制器 B 的版本。
儲存硬體	儲存控制器硬體的整體狀態。如果「系統管理程式」報告儲存硬體的需求注意狀態、則該系統也會報告此值。SANtricity StorageGRID 如果狀態為「需要注意」、請先使用 SANtricity OS 檢查儲存控制器。然後、請確定不存在其他適用於運算控制器的警示。
儲存控制器故障磁碟機數	不是最佳的磁碟機數量。
儲存控制器A	儲存控制器A的狀態
儲存控制器B	儲存控制器 B 的狀態。部分應用裝置機型沒有儲存控制器 B
儲存控制器電源供應器A	儲存控制器的電源供應器A狀態。
儲存控制器電源供應器B	儲存控制器的電源供應器B狀態。
儲存資料磁碟機類型	應用裝置中的磁碟機類型、例如 HDD （硬碟）或 SSD （固態硬碟）。
儲存資料磁碟機大小	一個資料磁碟機的有效大小。 SG6160 也會顯示快取磁碟機的大小。 • 附註 * ：對於有擴充機櫃的節點、請改用每個機櫃的資料磁碟機大小。有效磁碟機大小可能因機櫃而異。
儲存RAID模式	為應用裝置設定的RAID模式。
儲存連線能力	儲存連線狀態。
整體電源供應器	產品所有電源供應器的狀態。
運算控制器BMC IP	運算控制器中基礎板管理控制器（BMC）連接埠的IP位址。您可以使用此IP連線至BMC介面、以監控及診斷應用裝置硬體。 對於不含 BMC 的應用裝置機型、不會顯示此欄位。

欄位	說明
運算控制器序號	運算控制器的序號。
運算硬體	運算控制器硬體的狀態。如果應用裝置機型沒有獨立的運算硬體和儲存硬體、則不會顯示此欄位。
運算控制器CPU溫度	運算控制器CPU的溫度狀態。
運算控制器機箱溫度	運算控制器的溫度狀態。
運算控制器電源供應 A	運算控制器電源供應 A 的狀態。
運算控制器電源供應 B	運算控制器電源供應 B 的狀態。

+

儲存櫃表格中的欄	說明
機櫃機箱序號	儲存櫃機箱的序號。
機櫃ID	儲存櫃的數字識別碼。 • 99：儲存控制器機櫃 • 0：第一個擴充櫃 • 1：第二個擴充櫃 ◦ 附註： * 擴充機櫃僅適用於 SG6060 和 SG6160 。
機櫃狀態	儲存櫃的整體狀態。
IOM 狀態	任何擴充櫃中的輸入/輸出模組（IOM）狀態。不適用（如果不是擴充櫃）。
電源供應器狀態	儲存櫃電源供應器的整體狀態。
藥櫃狀態	儲存櫃中的藥櫃狀態。不適用如果機櫃不含藥櫃。
風扇狀態	儲存櫃中冷卻風扇的整體狀態。
磁碟機插槽	儲存櫃中的磁碟機插槽總數。
資料磁碟機	儲存櫃中用於資料儲存的磁碟機數量。

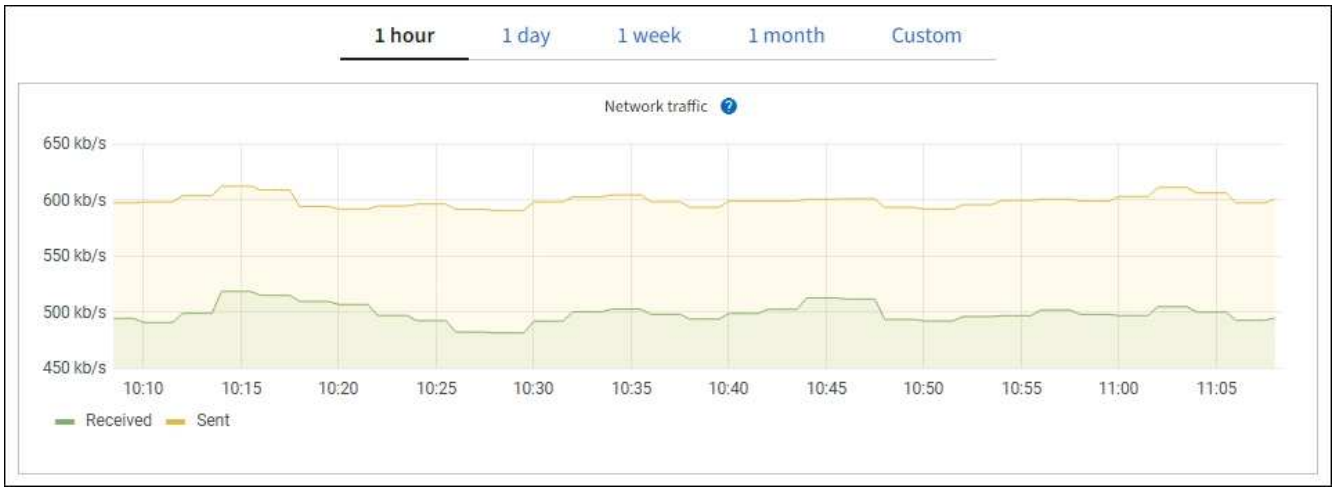
儲存櫃表格中的欄	說明
資料磁碟機大小	儲存櫃中一個資料磁碟機的有效大小。
快取磁碟機	儲存櫃中用於快取的磁碟機數量。
快取磁碟機大小	儲存櫃中最小快取磁碟機的大小。一般而言、快取磁碟機的大小都相同。
組態狀態	儲存櫃的組態狀態。

a. 確認所有狀態均為「標稱」。

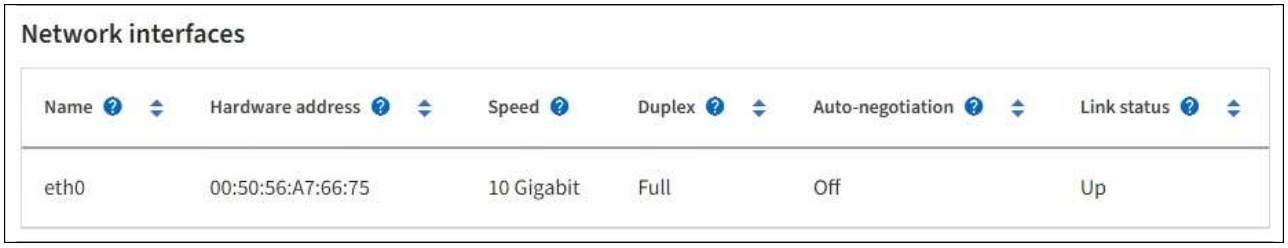
如果狀態不是「標稱」、請檢閱任何目前的警示。您也可以使用SANtricity 「功能變數系統管理程式」來深入瞭解這些硬體價值。請參閱安裝與維護應用裝置的說明。

4. 選取*網路*以檢視每個網路的資訊。

網路流量圖表提供整體網路流量的摘要。



a. 請查看「網路介面」部分。



使用下表以及網路介面表中「速度」欄中的值，確定應用裝置上的 10/25-GbE 網路連接埠是否已設定為使用主動/備份模式或 LACP 模式。

表中顯示的值假設使用了全部四個連結。

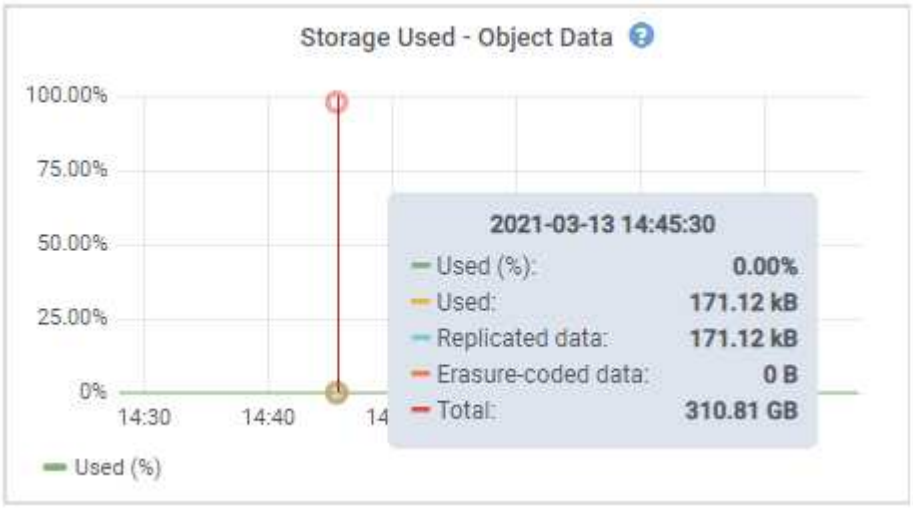
連結模式	債券模式	個別**HIC**連結速度（**hic1**、**hic2**、**hic3**、**hic4**）	預期網格/用戶端網路速度（**eth0**、**eth2**）
Aggregate	LACP	25	100
固定	LACP	25	50
固定	使用中/備份	25	25
Aggregate	LACP	10	40
固定	LACP	10	20
固定	使用中/備份	10	10

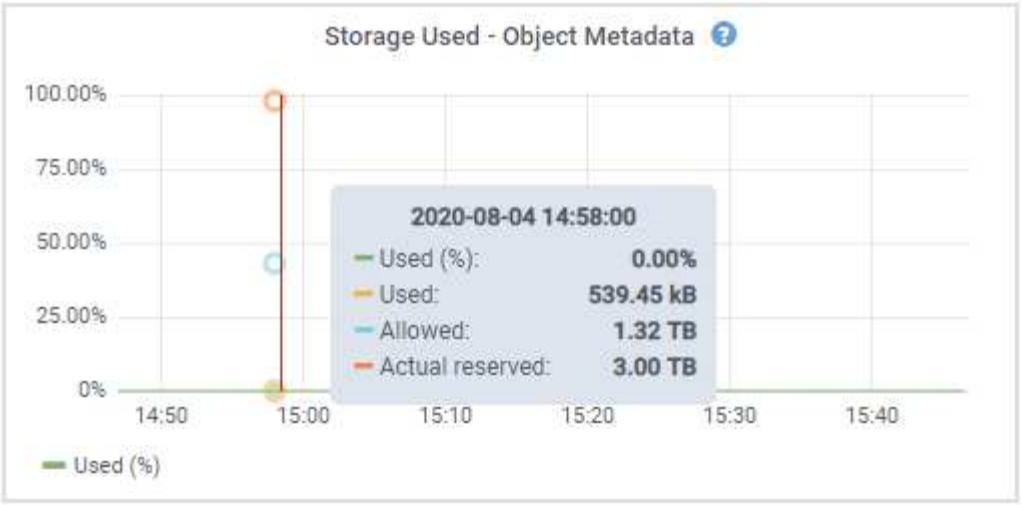
+
如需設定 10/25-GbE 連接埠的詳細資訊、請參閱 "設定網路連結"。

a. 請查看「網路通訊」部分。

「接收和傳輸」表格顯示已在每個網路上接收和傳送多少位元組和封包、以及其他接收和傳輸度量。

5. 選取「儲存設備」可檢視圖表、以顯示物件資料和物件中繼資料隨時間使用的儲存設備百分比、以及磁碟裝置、磁碟區和物件存放區的相關資訊。





a. 向下捲動以檢視每個Volume和物件存放區的可用儲存容量。

每個磁碟的全球名稱都符合在 SANtricity OS 中檢視標準 Volume 內容（連接至應用裝置儲存控制器的管理軟體）時所顯示的全域 Volume 識別碼（ WWID ）。

為了協助您解讀磁碟讀取及寫入與磁碟區掛載點相關的統計資料、「磁碟裝置」表格*名稱*欄（即_sdc_、*sdd*、_sde_等）中顯示的名稱第一部分、會與「磁碟區」表格*「裝置*」欄中顯示的值相符。

檢視應用裝置管理節點和閘道節點的相關資訊

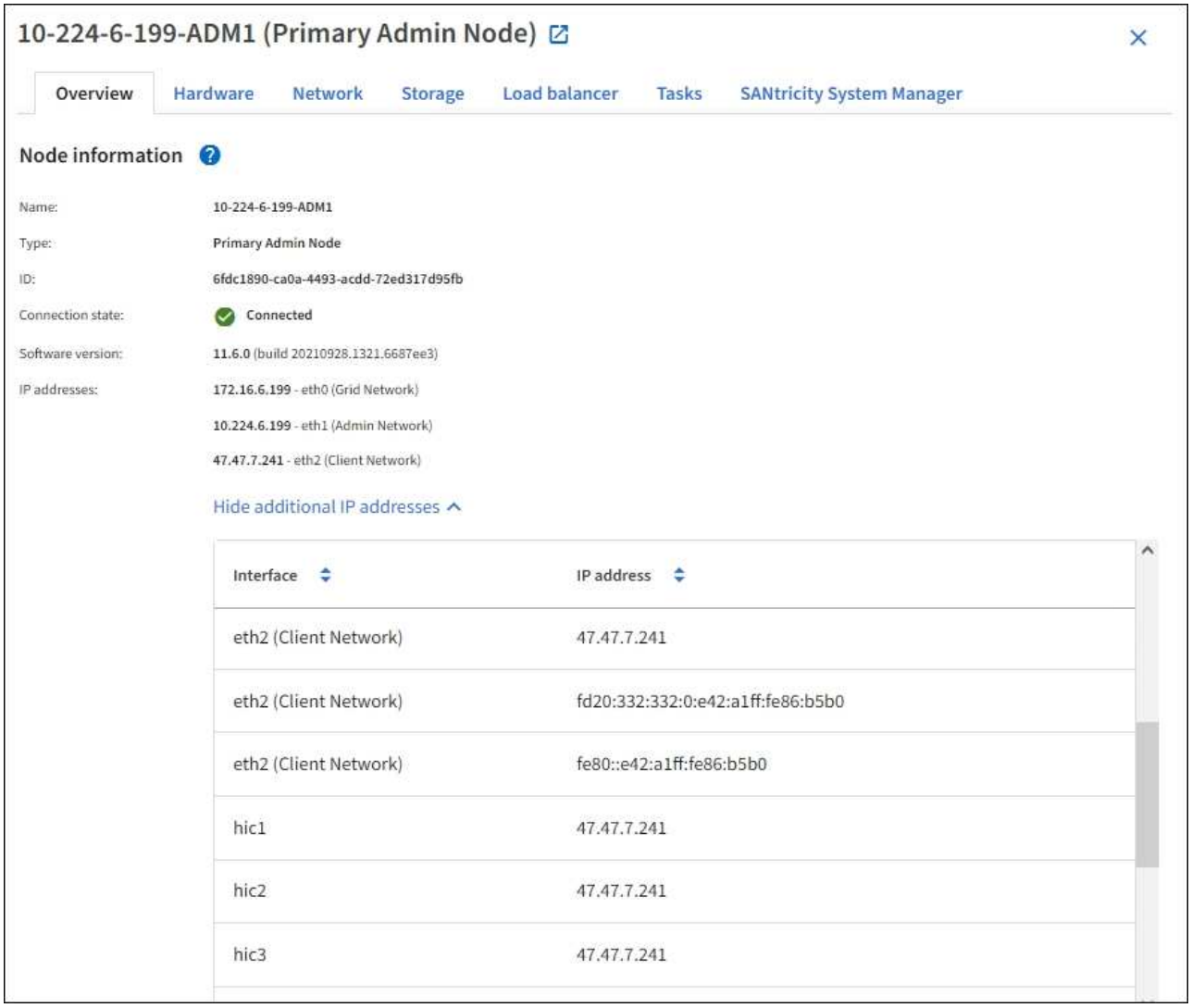
「節點」頁面會列出服務健全狀況的相關資訊、以及每個作為管理節點或閘道節點之服務應用裝置的所有運算、磁碟裝置和網路資源。您也可以看到記憶體、儲存硬體、網路資源、網路介面、網路位址、 以及接收和傳輸資料。

步驟

1. 從「節點」頁面、選取應用裝置管理節點或應用裝置閘道節點。
2. 選擇* Overview（概述）*選項卡。

「概觀」索引標籤的「節點資訊」區段會顯示節點的摘要資訊、例如節點的名稱、類型、ID和連線狀態。IP位址清單包含每個位址的介面名稱、如下所示：

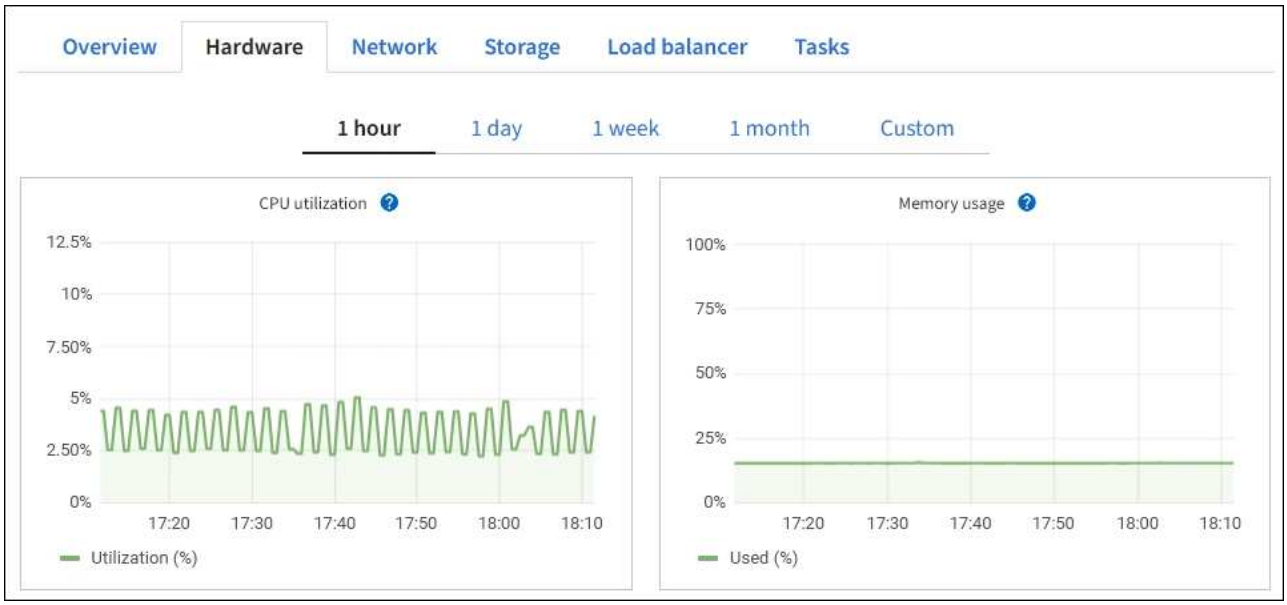
- * adllb*和* adlli*：顯示管理網路介面是否使用主動/備份連結
- * eth*：網格網路、管理網路或用戶端網路。
- * hic*：設備上的實體10、25或100 GbE連接埠之一。這些連接埠可連結在一起、並連接StorageGRID至「資訊網」（eth0）和「用戶端網路」（eth2）。
- * MTC*：應用裝置上的實體1-GbE連接埠之一。一個或多個MTC介面已繫結、以形成管理網路介面（eth1）。您可以保留其他MTC介面、讓資料中心的技術人員暫時在本機連線。



「概觀」索引標籤的「警示」區段會顯示節點的任何作用中警示。

3. 選取*硬體*索引標籤，以查看有關此應用裝置的更多資訊。

   a. 檢視CPU使用率和記憶體圖表、以判斷CPU和記憶體使用率的百分比。若要顯示不同的時間間隔、請選取圖表或圖表上方的其中一個控制項。您可以顯示1小時、1天、1週或1個月的可用時間間隔資訊。您也可以設定自訂時間間隔、以便指定日期和時間範圍。



b. 向下捲動以檢視應用裝置的組件表。此表包含型號名稱、序號、控制器韌體版本以及每個組件的狀態等資訊。

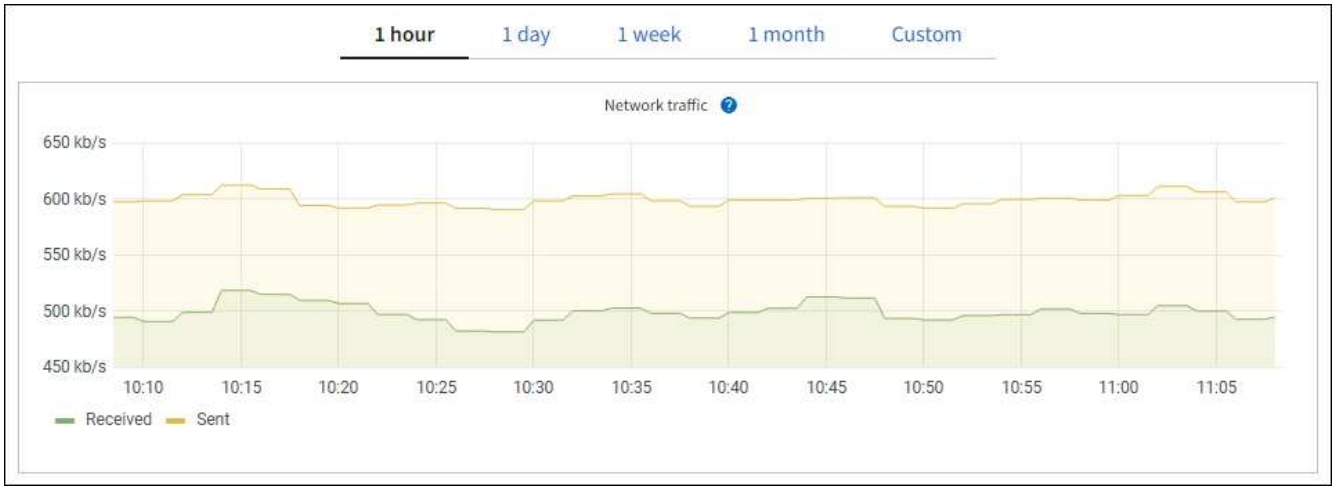
欄位	說明
應用裝置機型	此產品的型號StorageGRID 。
儲存控制器故障磁碟機數	不是最佳的磁碟機數量。
儲存資料磁碟機類型	應用裝置中的磁碟機類型、例如 HDD （硬碟）或 SSD （固態硬碟）。
儲存資料磁碟機大小	一個資料磁碟機的有效大小。
儲存RAID模式	應用裝置的RAID模式。
整體電源供應器	產品中所有電源供應器的狀態。
運算控制器BMC IP	運算控制器中基礎板管理控制器（BMC）連接埠的IP位址。您可以使用此IP連線至BMC介面、以監控及診斷應用裝置硬體。 對於不含 BMC 的應用裝置機型、不會顯示此欄位。
運算控制器序號	運算控制器的序號。
運算硬體	運算控制器硬體的狀態。
運算控制器CPU溫度	運算控制器CPU的溫度狀態。
運算控制器機箱溫度	運算控制器的溫度狀態。

c. 確認所有狀態均為「標稱」。

如果狀態不是「標稱」、請檢閱任何目前的警示。

4. 選擇 **Network** 索引標籤以檢視每個網路的資訊。

網路流量圖表提供整體網路流量的摘要。



a. 請查看「網路介面」部分。

使用下表以及網路介面表中「速度」欄中的值，確定應用裝置上的四個 40/100-GbE 網路連接埠是否已設定為使用主動/備份模式或 LACP 模式。

表中顯示的值假設使用了全部四個連結。

連結模式	債券模式	個別**HIC**連結速度（**hic1**、**hic2**、**hic3**、**hic4**）	預期網格/用戶端網路速度（**eth0**、**eth2**）
Aggregate	LACP	100	400
固定	LACP	100	200
固定	使用中/備份	100	100
Aggregate	LACP	40	160
固定	LACP	40	80
固定	使用中/備份	40	40

a. 請查看「網路通訊」部分。

「接收和傳輸」表格顯示已在每個網路上接收和傳送多少位元組和封包、以及其他接收和傳輸度量。

5. 選擇 **Storage** 索引標籤，以檢視服務應用裝置上磁碟設備和 Volume 的相關資訊。

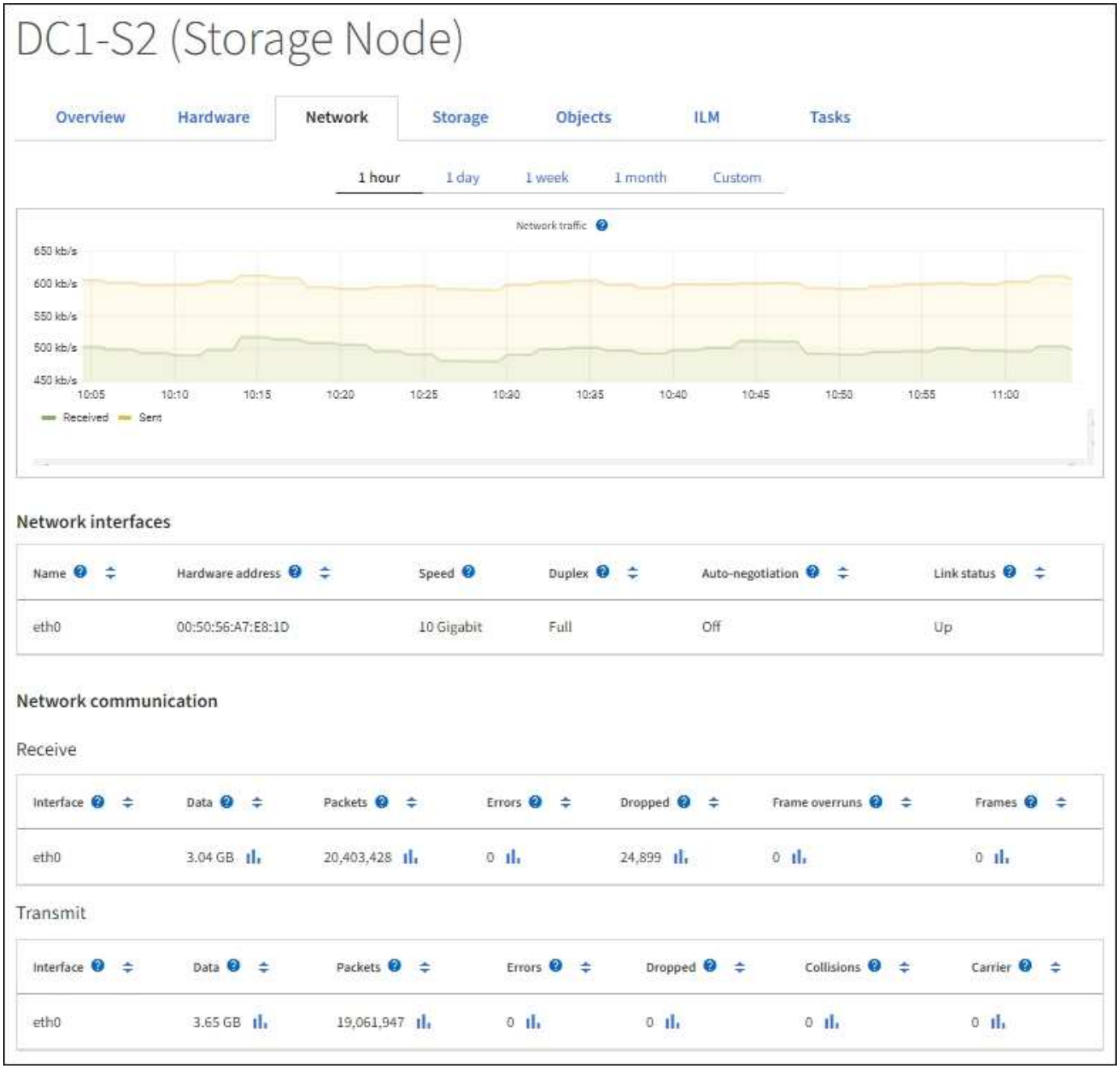
檢視 **StorageGRID** 網路標籤

「網路」索引標籤會顯示圖表、顯示在節點、站台或網格上所有網路介面上接收和傳送的網路流量。

「網路」索引標籤會顯示所有節點、每個站台及整個網格。

若要顯示不同的時間間隔、請選取圖表或圖表上方的其中一個控制項。您可以顯示1小時、1天、1週或1個月的可用時間間隔資訊。您也可以設定自訂時間間隔、以便指定日期和時間範圍。

對於節點、「網路介面」表提供每個節點實體網路連接埠的相關資訊。網路通訊表提供每個節點的接收和傳輸作業、以及任何驅動程式回報的故障計數器的詳細資料。



相關資訊

"監控網路連線與效能"

檢視 **StorageGRID** 儲存選項卡

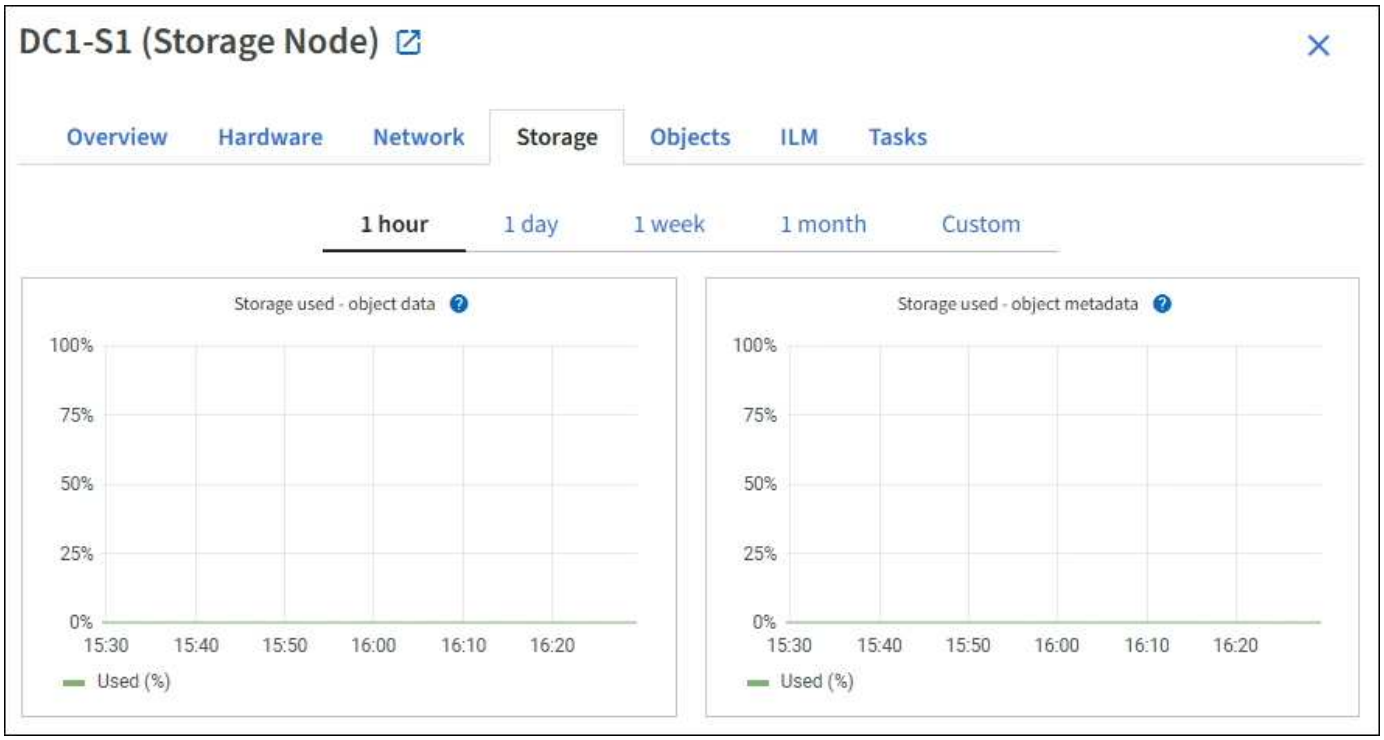
「Storage（儲存設備）」索引標籤摘要說明儲存可用度和其他儲存指標。

「儲存」標籤會顯示所有節點、每個站台以及整個網格的資訊。此索引標籤包含以下資訊：

儲存使用的圖表

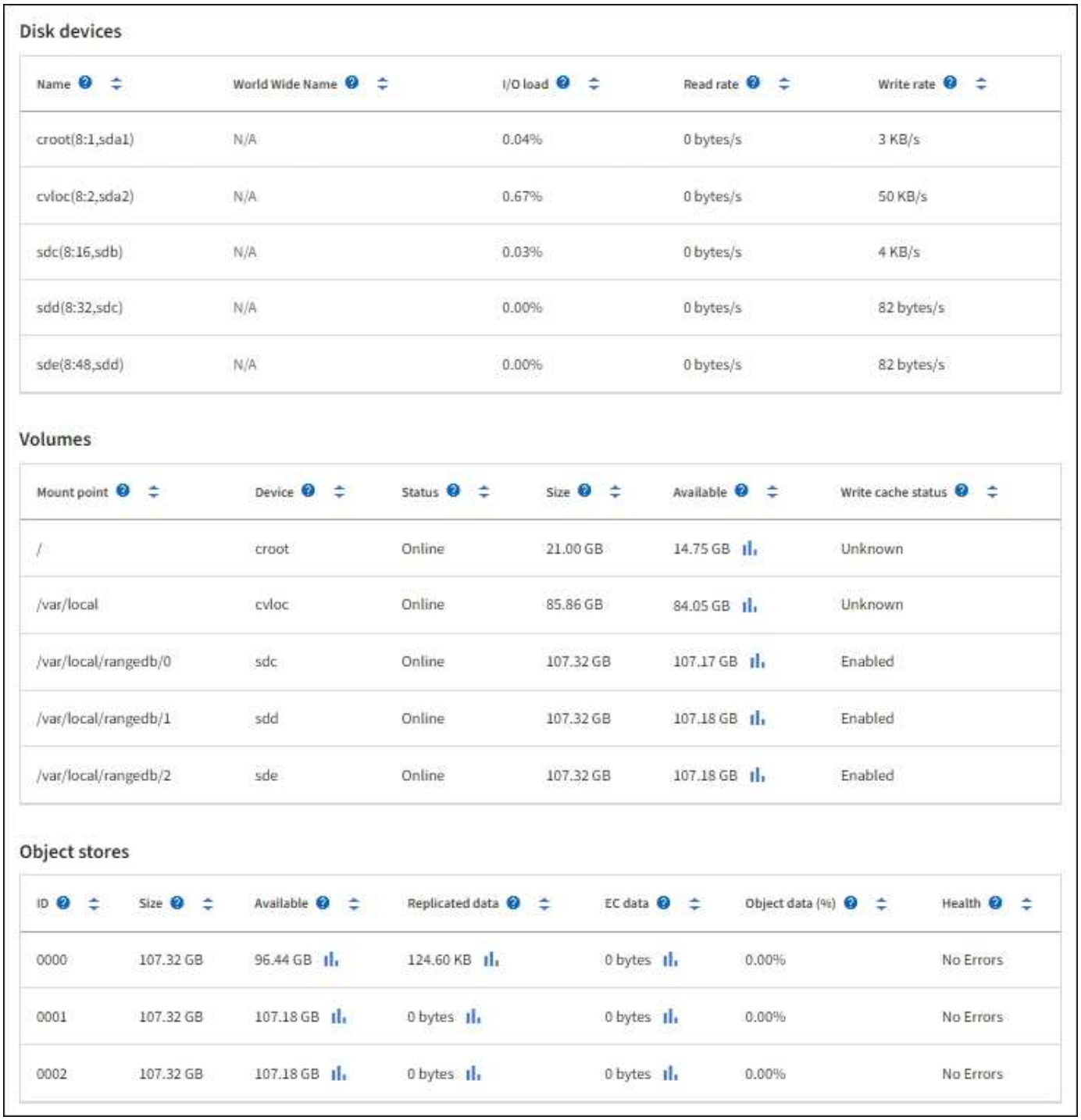
對於儲存節點、每個站台及整個網格、「儲存」索引標籤會顯示物件資料和物件中繼資料一段時間以來使用的儲存容量圖表。

當節點未連線至網格時、例如在升級期間或中斷連線狀態時、某些度量可能無法使用或排除在站台和網格總計之外。節點重新連線至網格之後、請等待數分鐘、讓值穩定下來。



磁碟裝置、磁碟區和物件會儲存資料表

對於所有節點、「Storage（儲存）」索引標籤包含節點上磁碟裝置和磁碟區的詳細資料。對於儲存節點、「物件存放區」表格提供每個儲存磁碟區的相關資訊。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

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

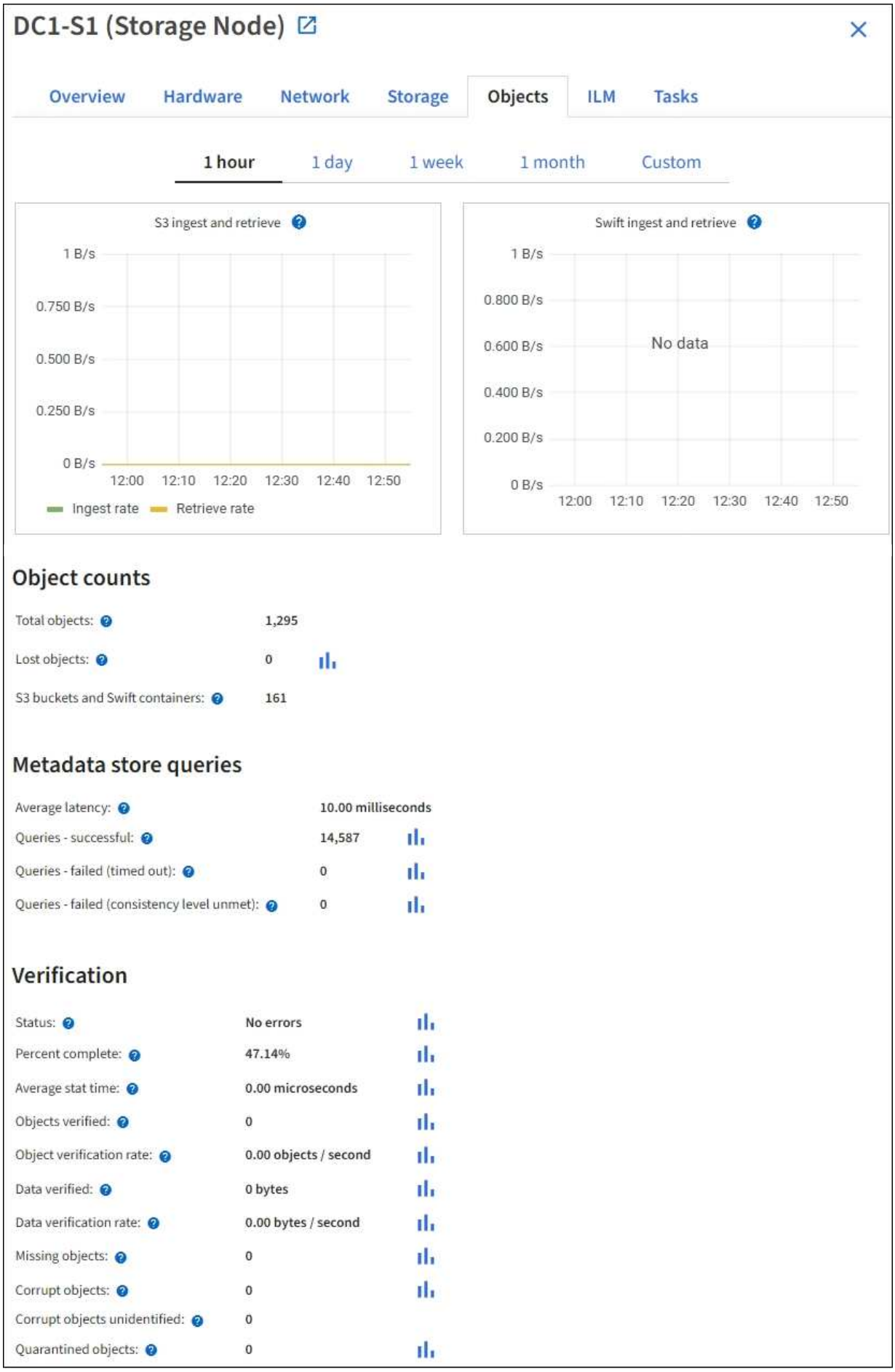
相關資訊

"監控儲存容量"

檢視 **StorageGRID Objects** 標籤

Objects （對象）選項卡提供了有關的信息"S3 擷取和擷取速率"。

每個儲存節點、每個站台及整個網格都會顯示物件索引標籤。對於儲存節點、「物件」索引標籤也會提供有關中繼資料查詢和背景驗證的物件計數和資訊。

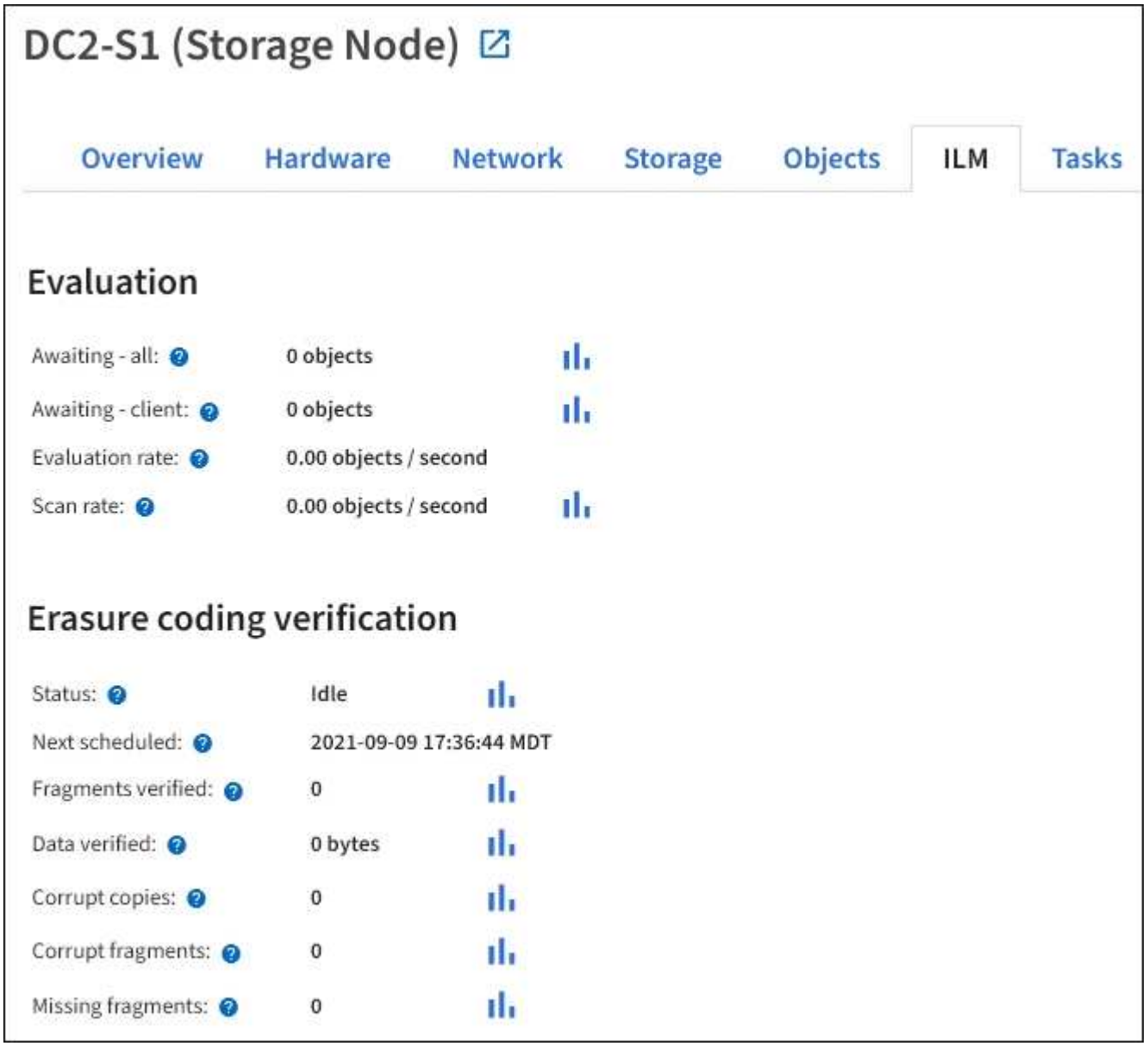

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

檢視 **StorageGRID ILM** 索引標籤

ILM 索引標籤提供資訊生命週期管理（ ILM ）作業的相關資訊。

此時會顯示每個儲存節點、每個站台及整個網格的ILM索引標籤。針對每個站台和網格、ILM索引標籤會顯示一段時間內ILM佇列的圖表。對於網格、此索引標籤也提供完成所有物件完整ILM掃描的預估時間。

對於儲存節點、 ILM 索引標籤會提供有關 ILM 評估和背景驗證的詳細資料、以用於銷毀編碼物件。



相關資訊

- "監控資訊生命週期管理"
- "管理StorageGRID"

使用 **StorageGRID Tasks** 標籤

所有節點均顯示「任務」標籤。您可以使用此標籤重新命名或重新啟動節點，或將設備節

點置於維護模式。對於儲存節點，您可以設定儲存狀態。

如需此索引標籤上每個選項的完整需求和指示、請參閱下列內容：

- "重新命名網格、站台和節點"
- "重新開機網格節點"
- "將應用裝置置於維護模式"
- 在將直接連接或 SAN 磁碟區新增至儲存節點後，或在復原儲存節點後，您可以驗證或設定儲存節點的儲存狀態。這些說明可以在描述這些任務的主題中找到。

檢視 **StorageGRID** 負載平衡器索引標籤

負載平衡器索引標籤包含與負載平衡器服務作業相關的效能和診斷圖表。

「負載平衡器」索引標籤會顯示為管理節點和閘道節點、每個站台及整個網格。對於每個站台、負載平衡器索引標籤會提供該站台所有節點統計資料的彙總摘要。在整個網格中、負載平衡器索引標籤會提供所有站台統計資料的彙總摘要。

如果沒有透過負載平衡器服務執行 I/O 、或未設定負載平衡器、則圖表會顯示「無資料」。

要求流量

此圖表提供負載平衡器端點與發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。

此值會在每個要求完成時更新。因此、此值可能與低要求率或極長時間要求的即時處理量有所不同。您可以查看「網路」索引標籤、以更真實地檢視目前的網路行為。

傳入要求率

此圖表提供每秒新要求數的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。

平均要求持續時間（非錯誤）

此圖表提供3分鐘的平均移動要求持續時間、並依申請類型（Get、PUT、HEAD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。

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。

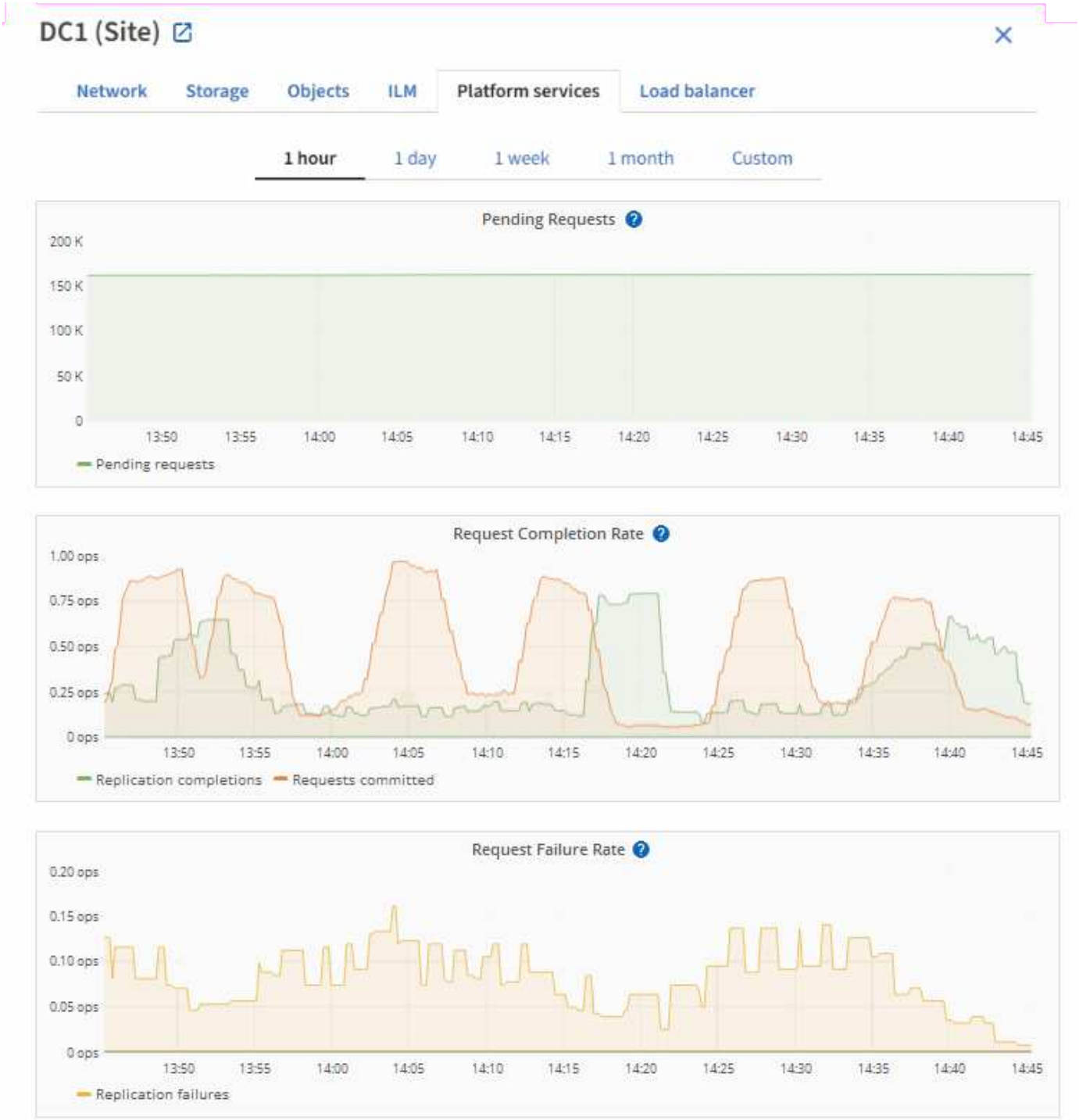
相關資訊

- "監控負載平衡作業"
- "管理StorageGRID"

檢視 **StorageGRID** 平台服務標籤

Platform Services（平台服務）索引標籤提供站台上任何S3平台服務作業的相關資訊。

每個站台都會顯示「平台服務」索引標籤。此索引標籤提供S3平台服務的相關資訊、例如CloudMirror複寫和搜尋整合服務。此索引標籤上的圖表會顯示待處理要求數、要求完成率及要求失敗率等指標。



如需 S3 平台服務的詳細資訊，包括疑難排解詳細資料"關於管理StorageGRID 功能的說明"，請參閱。

檢視 **StorageGRID** 管理磁碟機標籤

「管理磁碟機」索引標籤可讓您存取詳細資料、並在支援此功能的應用裝置中執行磁碟機的疑難排解和維護工作。

使用「管理磁碟機」索引標籤、您可以執行下列動作：

- 檢視應用裝置中資料儲存磁碟機的配置

- 檢視列出每個磁碟機位置、類型、狀態、韌體版本和序號的表格
- 在每個磁碟機上執行疑難排解和維護功能

若要存取「管理磁碟機」標籤、您必須擁有"儲存設備管理員或根存取權限"。

如需使用 [管理磁碟機] 索引標籤的相關資訊，請參閱 "使用管理磁碟機索引標籤"。

檢視 **StorageGRID SANtricity System Manager** 標籤

「支援系統管理程式」索引標籤可讓您存取《支援系統管理程式》、而無需設定或連接儲存應用裝置的管理連接埠。SANtricity SANtricity您可以使用此索引標籤來檢閱硬體診斷與環境資訊、以及與磁碟機相關的問題。

從SANtricity Grid Manager存取「支援系統管理程式」通常只是為了監控應用裝置硬體、以及設定E系列AutoSupport 的功能。SANtricity 系統管理員中的許多功能和作業（例如升級韌體）不適用於監控 StorageGRID 應用裝置。為避免發生問題、請務必遵循設備的硬體維護指示。若要升級 SANtricity 韌體、請參閱 "維護組態程序"儲存設備的。

只有使用 E 系列硬體的儲存設備節點才會顯示 SANtricity 系統管理員標籤。

使用「系統管理程式」、您可以執行下列動作：SANtricity

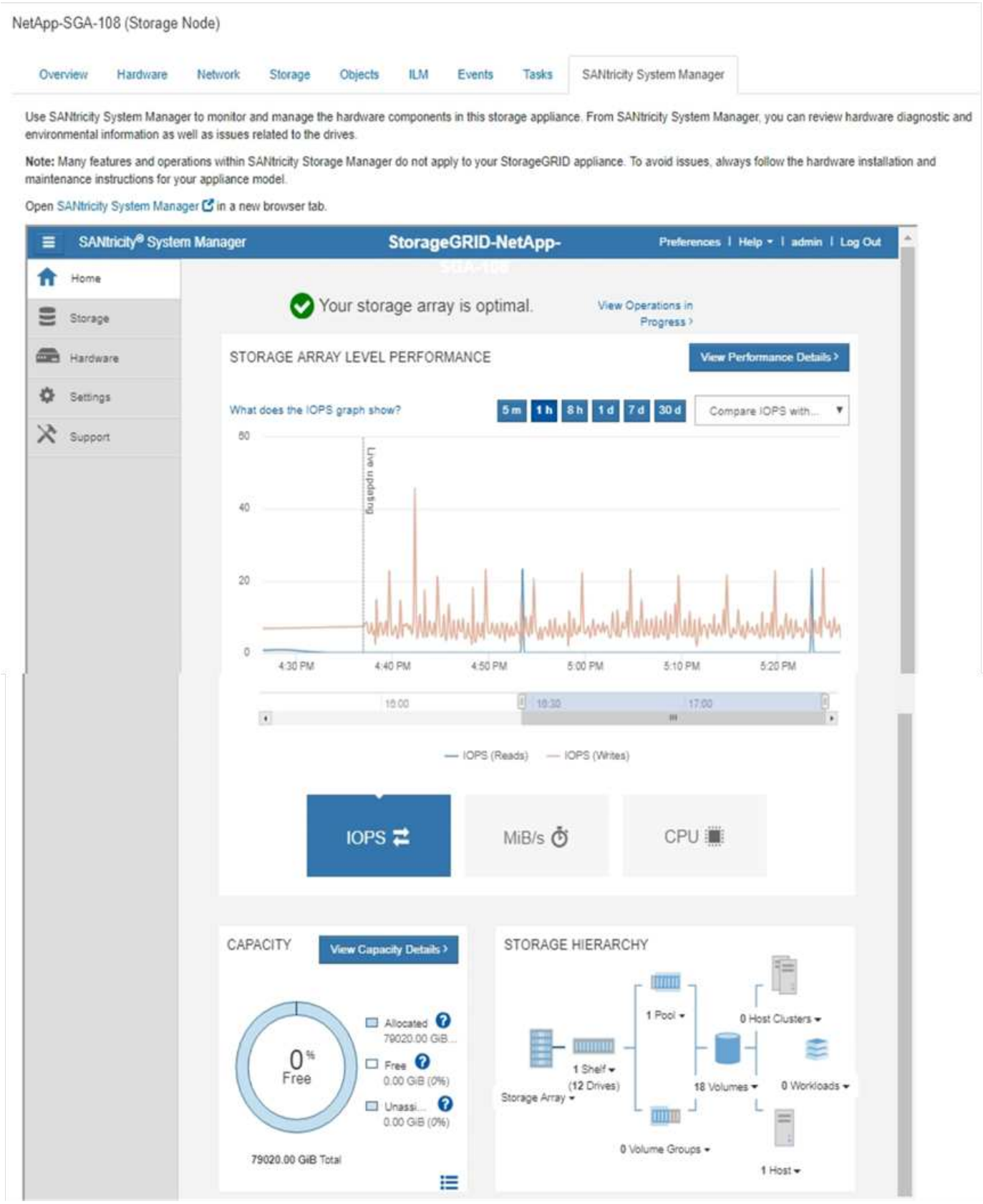
- 檢視儲存陣列層級效能、 I/O 延遲、儲存控制器 CPU 使用率和處理量等效能資料。
- 檢查硬體元件狀態。
- 執行支援功能、包括檢視診斷資料和設定 E 系列 AutoSupport 。

若要使用 SANtricity System Manager 為 E 系列 AutoSupport 設定 Proxy，請參閱"透過 StorageGRID 傳送 E 系列 AutoSupport 套件"。

若要透過 Grid Manager 存取 SANtricity 系統管理員、您必須擁有"儲存設備管理員或根存取權限"。

您必須擁有SANtricity 更新版本的韌體8.70才能SANtricity 使用Grid Manager存取《系統管理程式》。

索引標籤會顯示SANtricity 「系統管理程式」的首頁。



您可以使用SANtricity 「更新系統管理程式」連結、在SANtricity 新的瀏覽器視窗中開啟「更新系統管理程式」、以便更輕鬆地檢視。

若要查看儲存陣列層級效能和容量使用量的詳細資料、請將游標放在每個圖表上方。

如需更多有關檢視可從 SANtricity 系統管理員標籤存取之資訊的詳細資訊，請參閱 "NetApp E系列與SANtricity不完整的文件"。

定期監控的資訊

在 **StorageGRID** 中監控什麼和何時監控

即使 StorageGRID 系統在發生錯誤或網格的某些部分無法使用時仍可繼續運作、您仍應在潛在問題影響網格效率或可用度之前進行監控和解決。

開始之前

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

關於監控工作

忙碌的系統會產生大量資訊。下列清單提供持續監控最重要資訊的指引。

監控內容	頻率
"系統健全狀況"	每日
使用率"儲存節點物件和中繼資料容量"	每週
"資訊生命週期管理作業"	每週
"網路與系統資源"	每週
"租戶活動"	每週
"S3 用戶端作業"	每週
"負載平衡作業"	在初始組態之後以及任何組態變更之後
"網格同盟連線"	每週

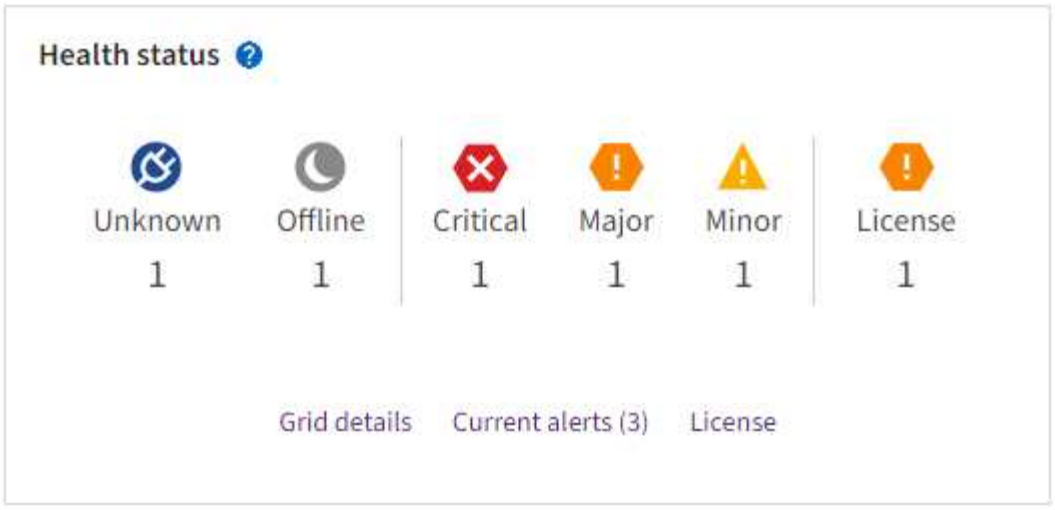
監控 **StorageGRID** 中的系統健全狀況

每天監控 StorageGRID 系統的整體健全狀況。

關於這項工作

當網格的某些部分無法使用時、 StorageGRID 系統仍可繼續運作。警示所指出的潛在問題不一定是系統作業的問題。調查 Grid Manager 儀表板健全狀況狀態卡上摘要的問題。

若要在警示觸發"設定 SNMP 設陷"時立即收到通知、您可以 "設定警示的電子郵件通知"或。



當問題存在時、會出現連結、讓您檢視其他詳細資料：

連結	出現時間 ...
網格詳細資料	任何節點都會中斷連線（連線狀態為「未知」或「管理性關閉」）。
目前警示（重大、重大、次要）	警示為目前使用中。
最近解決的警示	上週觸發現已解決的警示。
授權	此 StorageGRID 系統的軟體授權有問題。您可以"視需要更新授權資訊"。

監控節點連線狀態

如果一個或多個節點與網格中斷連線、關鍵StorageGRID 的功能不正常運作可能會受到影響。監控節點連線狀態、並立即解決任何問題。

圖示	說明	需要採取行動
	未連線-未知 由於不明原因、節點中斷連線或節點上的服務意外停機。例如、節點上的服務可能會停止、或是節點因為停電或非預期的停電而失去網路連線。 也可能會觸發*無法與node*通訊警示。其他警示也可能處於作用中狀態。	需要立即注意。選取每個警示並遵循建議的行動。 例如、您可能需要重新啟動已停止或重新啟動節點主機的服務。 • 注意 * ：在託管關機作業期間、節點可能會顯示為「未知」。在這些情況下、您可以忽略「未知」狀態。

圖示	說明	需要採取行動
	未連線-管理性關機 由於預期的原因、節點未連線至網格。 例如、節點或節點上的服務已正常關機、節點正在重新開機、或軟體正在升級。一個或多個警示也可能處於作用中狀態。 根據基礎問題、這些節點通常會在不需介入的情況下重新上線。	判斷是否有任何警示影響此節點。 如果有一個或多個警示處於作用中選取每個警示狀態、請遵循建議的動作。
	已連線 節點已連線至網格。	無需採取任何行動。

檢視目前和已解決的警示

- 目前警示 * ：觸發警示時、儀表板上會顯示警示圖示。節點的「節點」頁面上也會顯示警示圖示。如果"已設定警示電子郵件通知"是、除非警示已靜音、否則也會傳送電子郵件通知。
- 已解決的警示 * ：您可以搜尋並檢視已解決的警示記錄。

或者，您已經觀看了影片：

警報概述

下表說明 Grid Manager 中顯示的目前和已解決警示資訊。

欄標題	說明
名稱或職稱	警示名稱及其說明。
嚴重性	警示的嚴重性。對於目前警示、如果將多個警示分組、標題列會顯示每個嚴重性發生多少個警示執行個體。 **Critical**：StorageGRID 節點或服務出現異常情況，導致其正常運作停止。您必須立即解決根本問題。如果問題無法解決，可能會導致服務中斷和資料遺失。 **Major**：存在異常情況，該情況正在影響目前作業或接近嚴重警示的臨界值。您應調查重大警示並解決任何根本問題，以確保異常情況不會停止 StorageGRID 節點或服務的正常運作。 **Minor**：系統目前運作正常，但有異常情況，如果持續下去可能會影響系統運作。您應監控並解決不會自行消失的輕微警報，以確保它們不會導致更嚴重的問題。

欄標題	說明
觸發時間	• 目前警示 * ：警示在您當地時間和 UTC 中觸發的日期和時間。如果群組多個警示、標題列會顯示警示最近執行個體（_new）和警示最舊執行個體（_*OLDEST*）的時間。 • 已解決的警示 * ：多久前觸發警示。
站台/節點	發生或發生警示的站台和節點名稱。
狀態	警示為作用中、已靜音或已解決。如果群組多個警示、並在下拉式清單中選取*所有警示*、標題列會顯示該警示的作用中執行個體數目、以及已將多少個執行個體設為靜音。
已解決時間（僅限已解決的警示）	警示已解決多久。
目前值或 _data 值 _	導致觸發警示的度量值。有些警示會顯示其他值、以協助您瞭解及調查警示。例如、*低物件資料儲存*警示所顯示的值、包括使用的磁碟空間百分比、磁碟空間總量、以及使用的磁碟空間量。 • 附註： * 如果將多個目前警示分組、則目前的值不會顯示在標題列中。
觸發的值（僅限已解決的警示）	導致觸發警示的度量值。有些警示會顯示其他值、以協助您瞭解及調查警示。例如、*低物件資料儲存*警示所顯示的值、包括使用的磁碟空間百分比、磁碟空間總量、以及使用的磁碟空間量。

步驟

1. 選取 * 目前警示 * 或 * 已解決的警示 * 連結、即可檢視這些類別中的警示清單。您也可以選取 * 節點 * > ***node*** > * 總覽 * 、然後從警示表中選取警示、以檢視警示的詳細資料。

   依預設、目前警示顯示如下：

   ◦ 最新觸發的警示會先顯示。
   ◦ 相同類型的多個警示會顯示為群組。
   ◦ 未顯示已靜音的警示。
   ◦ 對於特定節點上的特定警示、如果達到超過一個嚴重性的臨界值、則只會顯示最嚴重的警示。也就是、如果次要、主要和關鍵嚴重性達到警示臨界值、則只會顯示嚴重警示。

   目前警示頁面每兩分鐘會重新整理一次。

2. 若要展開警報組，請選擇向下插入號 ⌄。若要折疊群組中的單一警報，請選擇向上插入號 ⌃，或選擇群組的名稱。
3. 若要顯示個別警示而非警示群組、請清除 * 群組警示 * 核取方塊。
4. 若要對目前警報或警報群組進行排序，請選擇每列標題中的向上/向下箭頭 ⇅。

   ◦ 選取*群組警示*時、會同時排序警示群組和每個群組內的個別警示。例如、您可能想要依*觸發時間*排序群組中的警示、以找出特定警示的最新執行個體。

- 當 * 群組警示 * 被清除時、警示的完整清單會被排序。例如、您可能想要依*節點/站台*排序所有警示、以查看影響特定節點的所有警示。

5. 若要依狀態（ * 所有警示 * 、 * 作用中 * 或 * 靜音 * ）篩選目前警示、請使用表格頂端的下拉式功能表。

   請參閱。 "靜音警示通知"

6. 若要排序已解決的警示：
   - 從「 * 觸發時 * 」下拉式功能表中選取時間週期。
   - 從 * 嚴重性 * 下拉式功能表中選取一或多個嚴重性。
   - 從*警示規則*下拉式功能表中選取一或多個預設或自訂警示規則、以篩選與特定警示規則相關的已解決警示。
   - 從「節點」下拉式功能表中選取一或多個節點、以篩選與特定節點相關的已解決警示。
7. 若要檢視特定警示的詳細資料、請選取該警示。對話方塊會提供您所選警示的詳細資料和建議動作。
8. （選用）針對特定警示、請選取將此警示設為靜音、以將觸發此警示的警示規則設為靜音。

   您必須有"管理警示或根目錄存取權限"才能將警示規則設為靜音。

   > 決定將警示規則設為靜音時請務必小心。如果警示規則設為靜音、您可能無法偵測潛在問題、直到無法完成關鍵作業為止。

9. 若要檢視警示規則的目前條件：
   a. 從警示詳細資料中、選取 * 檢視條件 * 。

      隨即出現快顯視窗、列出每個已定義嚴重性的Prometheus運算式。

   b. 若要關閉彈出視窗，請選擇彈出視窗以外的任意位置。
10. 您也可以選擇 * 編輯規則 * 來編輯導致觸發此警示的警示規則。

    您必須具有"管理警示或根目錄存取權限"才能編輯警示規則。

    > 決定編輯警示規則時請務必小心。如果您變更觸發值、則在無法完成關鍵作業之前、可能無法偵測潛在問題。

11. 若要關閉警示詳細資料、請選取 * 關閉 * 。

監控 **StorageGRID** 中的儲存容量

監控可用空間總量、確保StorageGRID 不讓物件或物件中繼資料的儲存空間耗盡。

物件資料和物件中繼資料會分開儲存、並針對包含物件中繼資料的分散式Cassandra資料庫保留特定空間量。StorageGRID監控物件和物件中繼資料所耗用的空間總量、以及各物件所耗用空間量的趨勢。這可讓您預先規劃新增節點、避免任何服務中斷。

您可以"檢視儲存容量資訊"針對整個網格、每個網站、以及 StorageGRID 系統中的每個儲存節點、進行設定。

監控網格的整體儲存容量、確保物件資料和物件中繼資料有足夠的可用空間。瞭解隨著時間而改變的儲存容量、有助於您在使用網格的可用儲存容量之前、計畫新增儲存節點或儲存磁碟區。

Grid Manager 儀表板可讓您快速評估整個網格和每個資料中心有多少可用儲存空間。「節點」頁面提供更詳細的物件資料和物件中繼資料值。

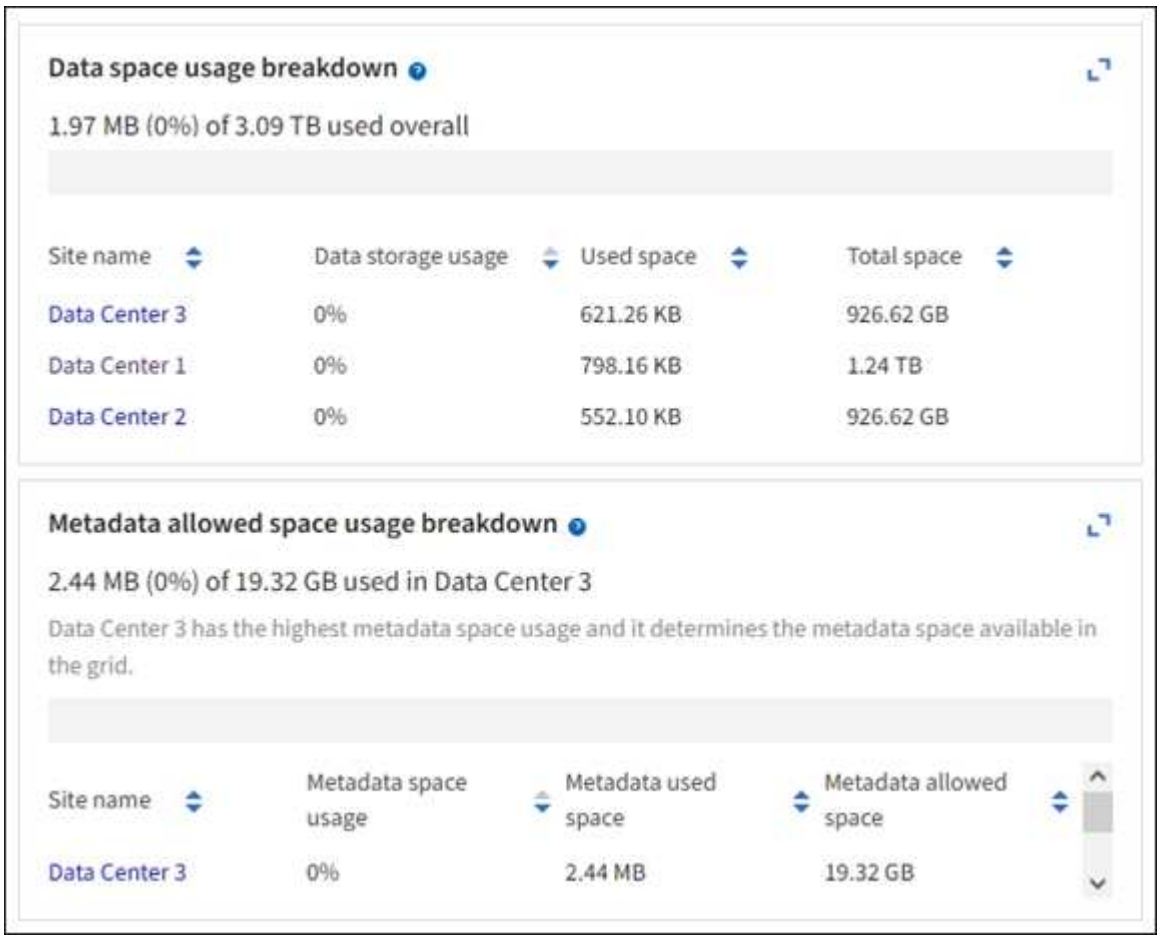
步驟

1. 評估整個網格和每個資料中心可用的儲存容量。

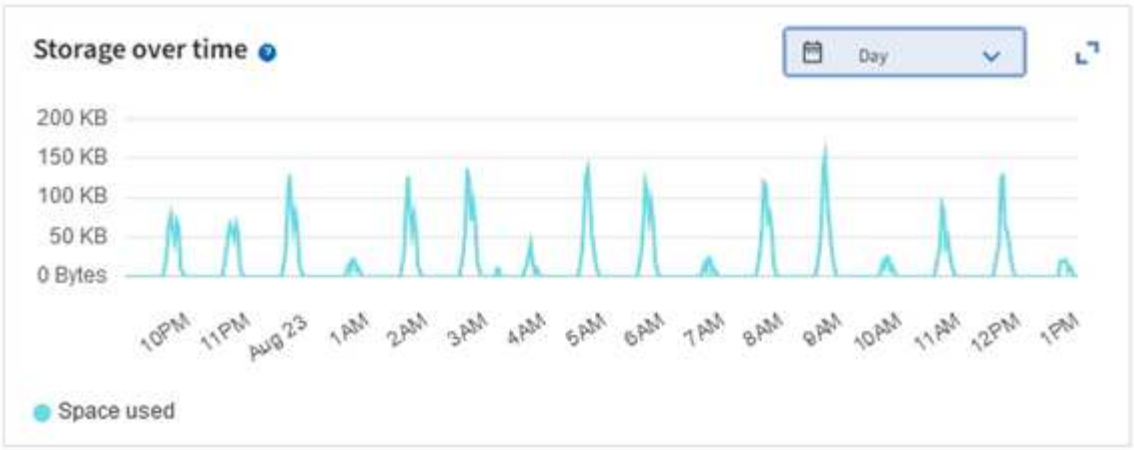
   a. 選取 * 儀表板 > 總覽 * 。

   b. 請注意「資料空間使用量明細」和「中繼資料允許空間使用量明細」卡上的值。每張卡片都會列出儲存使用率的百分比、已用空間的容量、以及站台可用或允許的總空間。

      摘要不包括歸檔媒體。



   a. 記下儲存設備隨時間卡上的圖表。使用「時間週期」下拉式清單、協助您判斷儲存設備的使用速度。



2. 請使用「節點」頁面、進一步瞭解已使用的儲存空間量、以及在網格上可用於物件資料和物件中繼資料的儲存空間量。

   a. 選擇*節點*。

   b. 選擇「網格_>*儲存設備*」。

   c. 將游標放在 * 已使用的儲存空間 - 物件資料 * 和 * 已使用的儲存空間 - 物件中繼資料 * 圖表上、以查看整個網格有多少物件儲存空間和物件中繼資料儲存空間可供使用、以及一段時間內已使用的容量。

   站台或網格的總值不包括至少五分鐘未報告度量的節點、例如離線節點。

3. 計畫在使用網格可用儲存容量之前、先執行擴充以新增儲存節點或儲存磁碟區。

   規劃擴充的時間時、請考量購買和安裝額外儲存設備所需的時間。

如果您的ILM原則使用銷毀編碼、當現有的儲存節點已滿約70%時、您可能會偏好擴充、以減少必須新增的節點數量。

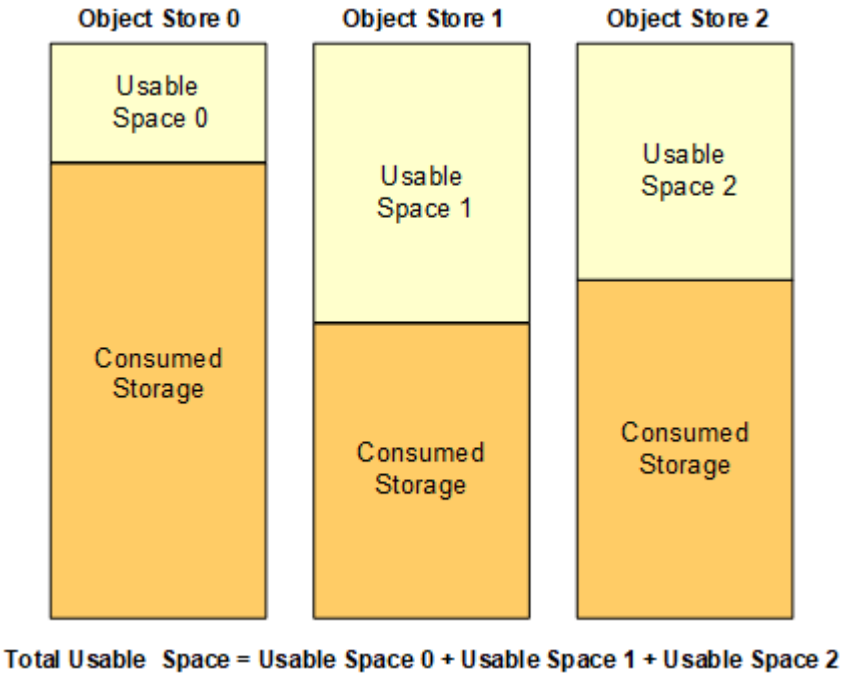
如需規劃儲存擴充的詳細資訊，請參閱"擴充StorageGRID 功能說明"。

監控每個儲存節點的儲存容量

監控每個儲存節點的總可用空間、確保節點有足夠空間容納新的物件資料。

關於這項工作

可用空間是儲存物件可用的儲存空間量。儲存節點的總可用空間是透過將節點內所有物件存放區的可用空間一起新增來計算。



步驟

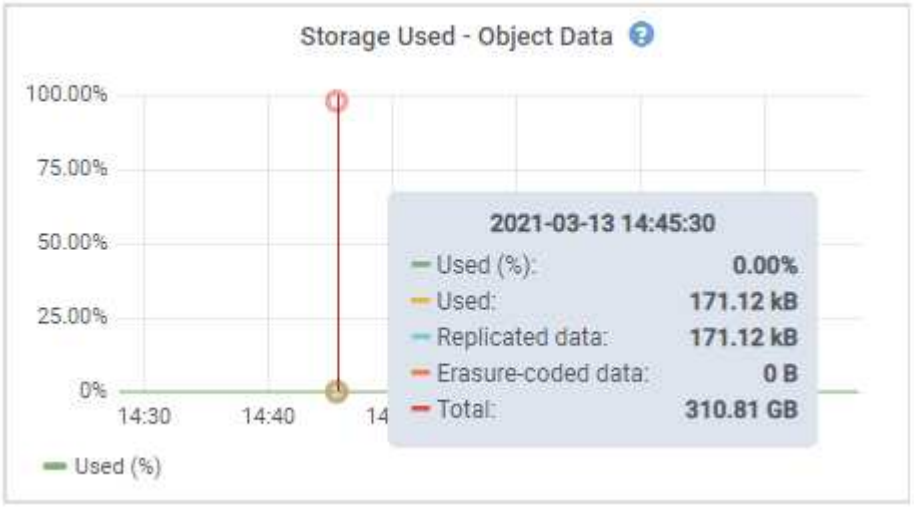
1. 選擇*節點* > 儲存節點 > 儲存。

   此時會顯示節點的圖形和表格。

2. 將游標放在「已使用的儲存空間 - 物件資料」圖表上。

   顯示下列值：

   - 已用（**%**）：已用於物件資料的總可用空間百分比。
   - 已用：用於物件資料的總可用空間量。
   - 複寫資料：此節點、站台或網格上的複寫物件資料量預估。
   - 銷毀編碼資料：此節點、站台或網格上的銷毀編碼物件資料量預估。
   - 總計：此節點、站台或網格上的可用空間總量。使用的值為 `storagegrid_storage_utilization_data_bytes`度量。



3. 檢閱「Volumes and Object Stores」（磁碟區和物件儲存區）表格中的可用值、圖表下方。

   若要檢視這些值的圖表，請選取「可用欄」中的圖表圖示。

4. 監控一段時間內的值、以預估可用儲存空間的使用率。
5. 若要維持正常的系統作業、請先新增儲存節點、新增儲存磁碟區或歸檔物件資料、然後再使用可用空間。

   規劃擴充的時間時、請考量購買和安裝額外儲存設備所需的時間。

   如果您的ILM原則使用銷毀編碼、當現有的儲存節點已滿約70%時、您可能會偏好擴充、以減少必須新增的節點數量。

   如需規劃儲存擴充的詳細資訊，請參閱"擴充StorageGRID 功能說明"。

   "低物件資料儲存"當在儲存節點上儲存物件資料的空間不足時、就會觸發警示。

監控每個儲存節點的物件中繼資料容量

監控每個儲存節點的中繼資料使用量、確保有足夠的空間可供重要的資料庫作業使用。在物件中繼資料超過允許的100%中繼資料空間之前、您必須在每個站台新增儲存節點。

關於這項工作

支援在每個站台維護三份物件中繼資料複本、以提供備援功能、並保護物件中繼資料免於遺失。StorageGRID這三個複本會使用保留給每個儲存節點之儲存Volume 0上的中繼資料的空間、平均分散於每個站台的所有儲存節點。

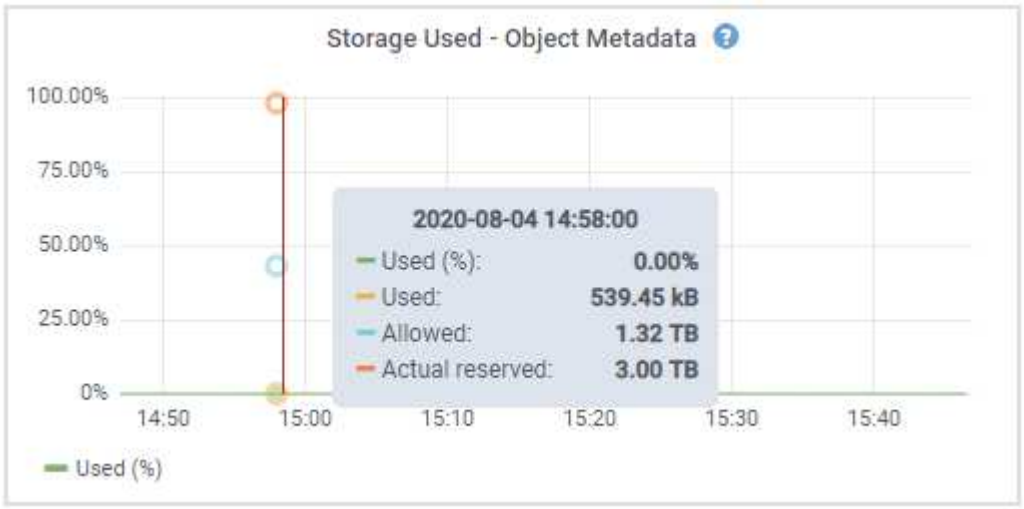
在某些情況下、網格的物件中繼資料容量使用速度可能比物件儲存容量快。例如、如果您通常會擷取大量的小型物件、則可能需要新增儲存節點來增加中繼資料容量、即使物件儲存容量仍足夠。

可增加中繼資料使用量的部分因素包括使用者中繼資料和標記的大小和數量、多重內容上傳的零件總數、以及ILM儲存位置變更的頻率。

步驟

1. 選擇*節點* > 儲存節點 > 儲存。

2. 將游標放在「已使用的儲存空間 - 物件中繼資料」圖表上、即可查看特定時間的值。



已用（%）

此儲存節點上已使用之允許中繼資料空間的百分比。

Prometheus 指標： `storagegrid_storage_utilization_metadata_bytes`和 `storagegrid_storage_utilization_metadata_allowed_bytes`

已使用

此儲存節點上已使用之允許中繼資料空間的位元組。

Prometheus 公制： `storagegrid_storage_utilization_metadata_bytes`

允許

此儲存節點上允許用於物件中繼資料的空間。要了解如何確定每個 Storage Node 的此值，請參閱"允許中繼資料空間的完整說明"。

Prometheus 公制： `storagegrid_storage_utilization_metadata_allowed_bytes`

實際保留

保留給此儲存節點上中繼資料的實際空間。包括允許的空間及必要的中繼資料作業空間。若要瞭解如何為每個儲存節點計算此值，請參閱"中繼資料的實際保留空間完整說明"。

未來版本將新增 _Prometheus 指標。 _

站台或網格的總值不包括至少五分鐘未報告度量的節點、例如離線節點。

3. 如果*已用（%）*值為70%或更高、請StorageGRID 在每個站台新增儲存節點來擴充您的系統。

當*已用（%）*值達到特定臨界值時、會觸發*低中繼資料儲存*警示。如果物件中繼資料使用超過100%的允許空間、可能會產生不理想的結果。

新增節點時、系統會自動在站台內的所有儲存節點之間重新平衡物件中繼資料。請參閱"擴充StorageGRID功能的說明"。

監控空間使用量預測

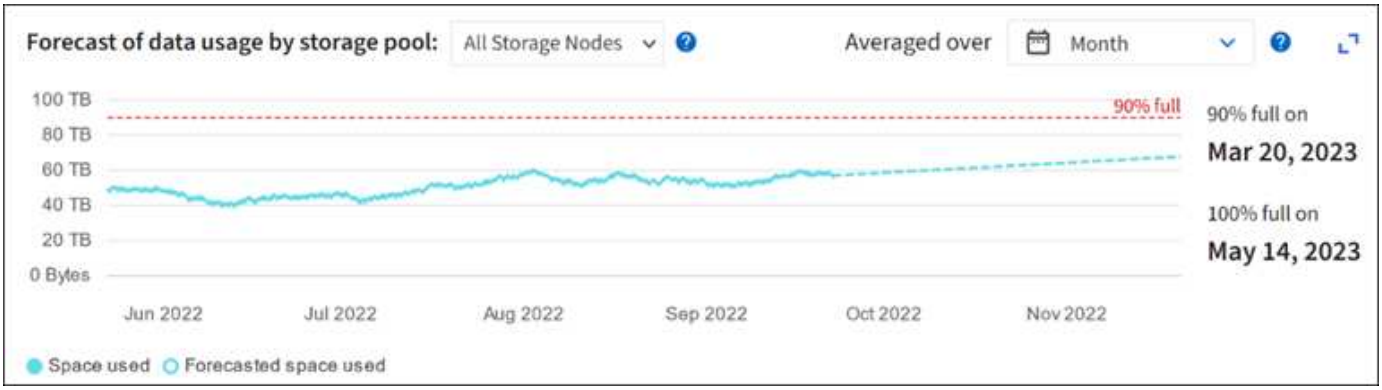
監控使用者資料和中繼資料的空間使用量預測"展開網格"、以預估何時需要。

如果您注意到使用率隨著時間變化、請從 * 平均過 * 下拉式清單中選取較短的範圍、以僅反映最近的擷取模式。如果您注意到季節性模式、請選擇較長的範圍。

如果您有新的 StorageGRID 安裝、請在評估空間使用量預測之前、先允許資料和中繼資料累積。

步驟

1. 在儀表板上、選取 * 儲存 * 。
2. 檢視儀表板卡、依儲存池預測資料使用量、以及依站台預測中繼資料使用量。
3. 使用這些值來估計何時需要新增資料和中繼資料儲存的儲存節點。



監控 **StorageGRID** 中的資訊生命週期管理

資訊生命週期管理（ILM）系統可為儲存在網格上的所有物件提供資料管理。您必須監控 ILM 作業、以瞭解網格是否能處理目前負載、或是否需要更多資源。

關於這項工作

StorageGRID 系統會套用主動式 ILM 原則來管理物件。ILM 原則和相關的 ILM 規則決定製作多少份複本、建立的複本類型、放置複本的位置、以及每份複本的保留時間長度。

物件擷取和其他物件相關活動可能會超過 StorageGRID 評估 ILM 的速度、導致系統將無法即時完成 ILM 放置指示的物件排入佇列。您應該監控 StorageGRID 是否與用戶端動作保持一致。

使用 **Grid Manager** 儀表板索引標籤

步驟

使用 Grid Manager 儀表板上的 ILM 索引標籤來監控 ILM 作業：

1. 登入Grid Manager。
2. 從儀表板選取 ILM 索引標籤、並記下 ILM 佇列（物件）卡和 ILM 評估率卡上的值。

   儀表板上的 ILM 佇列（物件）卡可能會暫時尖峰。但是如果佇列持續增加且永不減少、則網格需要更多資源才能有效運作：增加儲存節點、或是 ILM 原則將物件置於遠端位置、則需要更多網路頻寬。

使用節點頁面

步驟

此外，使用「節點」頁面調查 ILM 佇列：

在未來的StorageGRID版本中，*節點*頁面上的圖表將被對應的儀表闆卡取代。

1. 選擇*節點*。
2. 選擇*網格名稱_*>* ILM *。
3. 將游標放在 ILM 佇列圖形上、即可在指定時間點查看下列屬性的值：
   - 排入佇列的物件（來自用戶端作業）：因為用戶端作業（例如擷取）而等待ILM評估的物件總數。
   - 排入佇列的物件（來自所有作業）：等待ILM評估的物件總數。
   - 掃描速率（物件數/秒）：網格中的物件在ILM中掃描並排入佇列的速率。
   - 評估率（物件數/秒）：根據網格中的ILM原則評估物件的目前速度。

   ILM 佇列區段僅適用於網格。此資訊不會顯示在站台或儲存節點的ILM索引標籤上。
4. 在「ILM佇列」區段中、查看下列屬性。
   - * 掃描週期 - 預估 * ：完成所有物件完整 ILM 掃描的預估時間。

     完整掃描並不保證ILM已套用至所有物件。
   - * 嘗試的修復 * ：已嘗試複寫資料的物件修復作業總數。每次儲存節點嘗試修復高風險物件時、此計數就會遞增。如果網格忙碌、高風險的ILM修復會優先處理。

     如果修復後複製失敗，則相同物件修復可能會再次增加。 + 當您監控儲存節點磁碟區復原的進度時，這些屬性非常有用。如果嘗試修復的次數停止增加並且完整掃描已完成，則修復可能已完成。
5. 或者，提交 Prometheus 查詢 `storagegrid_ilm_scan_period_estimated_minutes`和 `storagegrid_ilm_repairs_attempted`。

監控 **StorageGRID** 中的網路和系統資源

節點和站台之間的網路完整性和頻寬、以及個別網格節點的資源使用量、都是有效作業的關鍵。

監控網路連線與效能

如果您的資訊生命週期管理（ILM）原則使用提供站台遺失保護的方案、在站台之間複製複寫的物件、或是儲存以銷毀編碼的物件、那麼網路連線能力和頻寬就特別重要。如果站台之間的網路無法使用、網路延遲太高、或網路頻寬不足、則部分ILM規則可能無法將物件放置在預期位置。這可能會導致擷取失敗（若為 ILM 規則選取嚴格擷取選項）、或是擷取效能和 ILM 待處理記錄不佳。

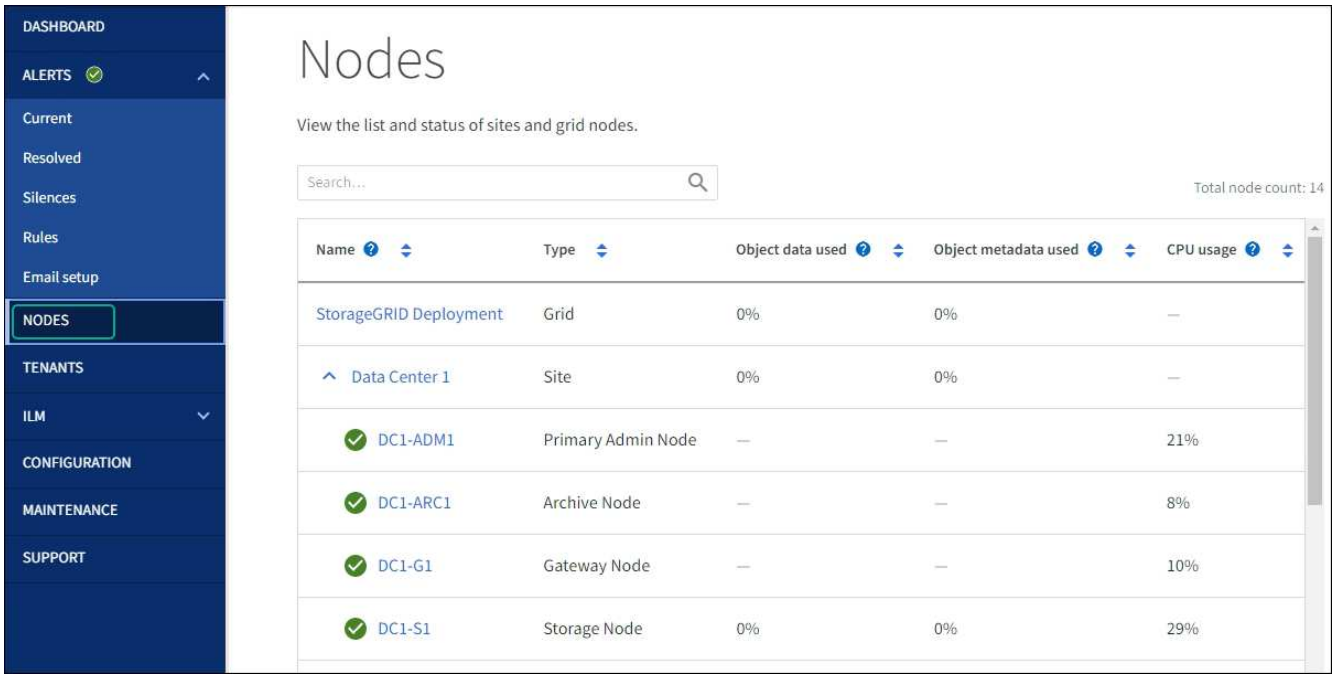
使用 Grid Manager 來監控連線能力和網路效能、以便您迅速解決任何問題。

此外、請考慮"建立網路流量分類原則"監控與特定租戶、貯體、子網路或負載平衡器端點相關的流量。您可以視需要設定流量限制原則。

步驟

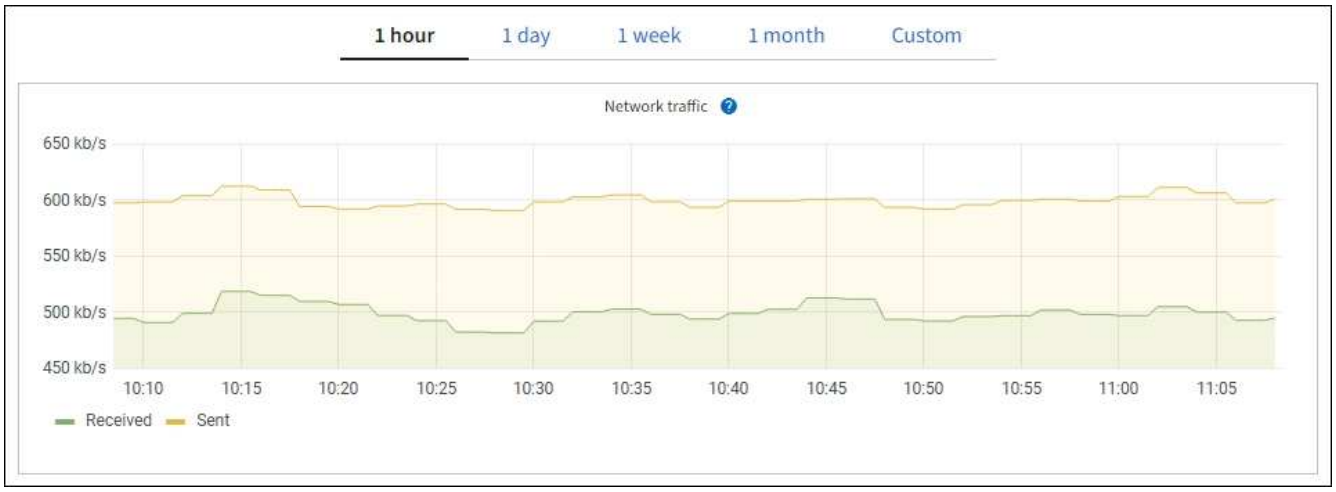
1. 選擇*節點*。

   此時會出現「節點」頁面。網格中的每個節點都會以表格格式列出。

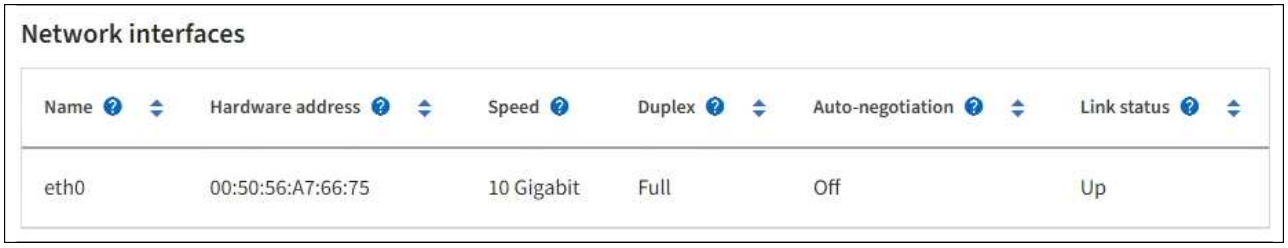


2. 選取網格名稱、特定資料中心站台或網格節點、然後選取*網路*索引標籤。

   網路流量圖表提供整個網格、資料中心站台或節點的整體網路流量摘要。



   a. 如果您選取了網格節點、請向下捲動以檢閱頁面的「網路介面」區段。



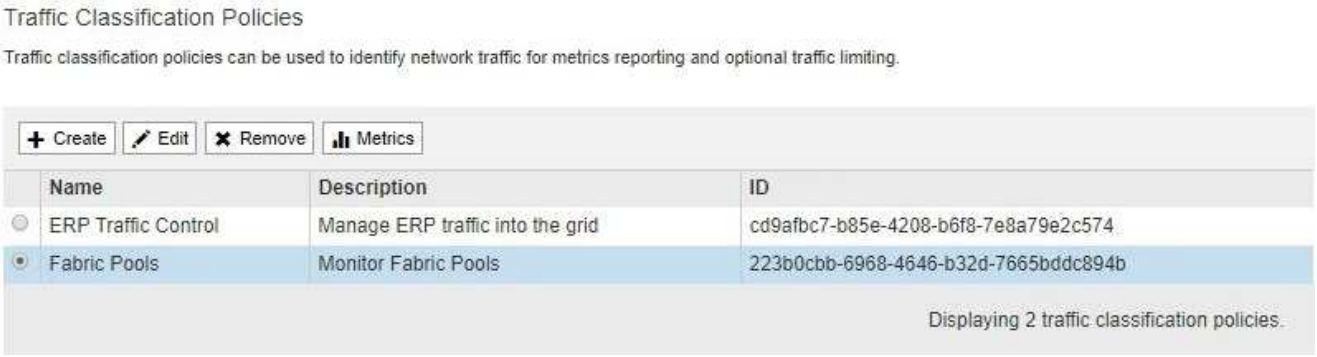
b. 對於網格節點、請向下捲動以檢閱頁面的「網路通訊」區段。

「接收和傳輸」表格顯示已在每個網路上接收和傳送多少位元組和封包、以及其他接收和傳輸度量。

3. 使用與流量分類原則相關的度量來監控網路流量。

a. 選擇*配置* > 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。



a. 若要檢視顯示與原則關聯的連網計量的圖表，請選擇原則左側的單選按鈕，然後選擇 **Metrics**。

b. 檢閱圖表以瞭解與原則相關的網路流量。

如果流量分類原則是設計用來限制網路流量、請分析流量受限的頻率、並決定原則是否持續符合您的需求。不時地"視需要調整每個流量分類原則"、

相關資訊

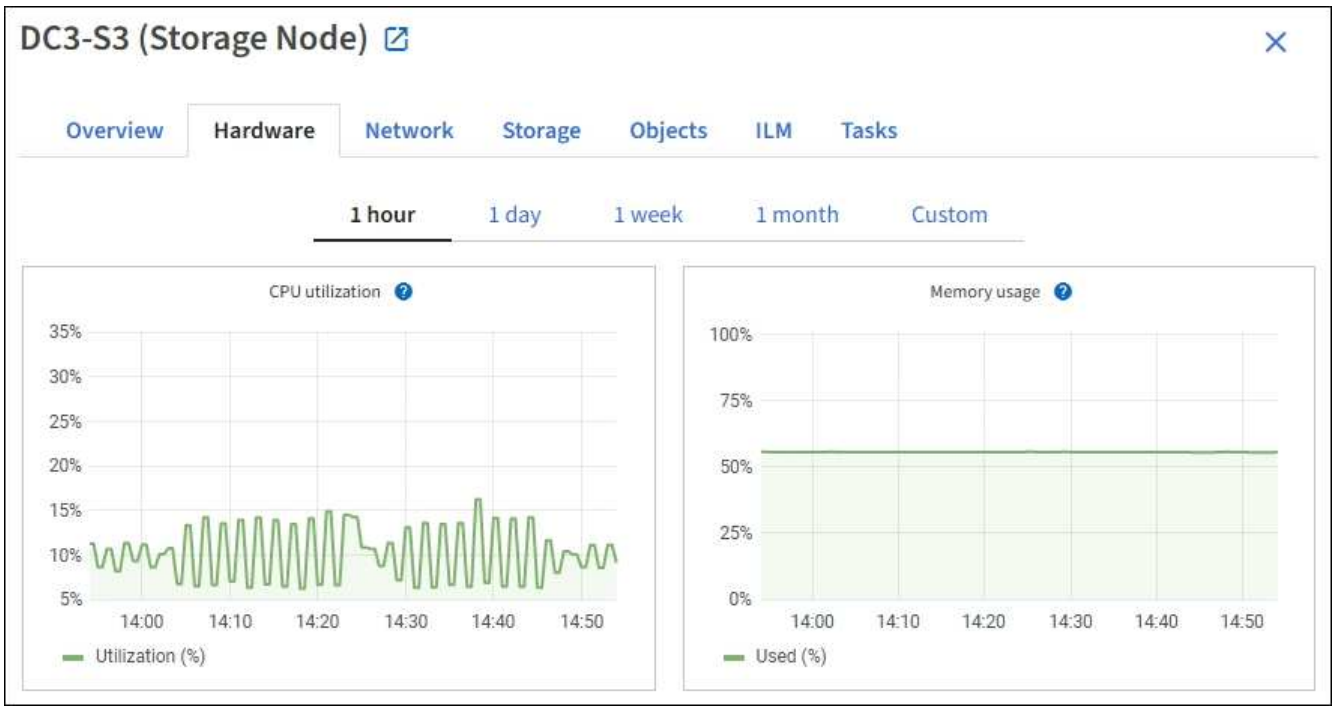
- "檢視「網路」索引標籤"
- "監控節點連線狀態"

監控節點層級資源

監控個別網格節點、以檢查其資源使用量。如果節點持續過載、則可能需要更多節點才能有效運作。

步驟

1. 從*節點*頁面中選擇節點。
2. 選取「硬體」索引標籤以顯示CPU使用率和記憶體使用率的圖表。



3. 若要顯示不同的時間間隔、請選取圖表或圖表上方的其中一個控制項。您可以顯示1小時、1天、1週或1個月的可用時間間隔資訊。您也可以設定自訂時間間隔、以便指定日期和時間範圍。
4. 如果節點裝載在儲存設備或服務應用裝置上、請向下捲動以檢視元件表。所有元件的狀態應為「標稱」。調查其他狀態的元件。

相關資訊

- "檢視應用裝置儲存節點的相關資訊"
- "檢視應用裝置管理節點和閘道節點的相關資訊"

監控 **StorageGRID** 中的租戶活動

所有 S3 用戶端活動都與 StorageGRID 租戶帳戶相關聯。您可以使用 Grid Manager 來監控所有租戶或特定租戶的儲存使用量或網路流量。您可以使用稽核記錄或 Grafana 儀表板來收集租戶如何使用 StorageGRID 的詳細資訊。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權或 Tenant 帳戶權限"。

檢視所有租戶

租戶頁面會顯示所有目前租戶帳戶的基本資訊。

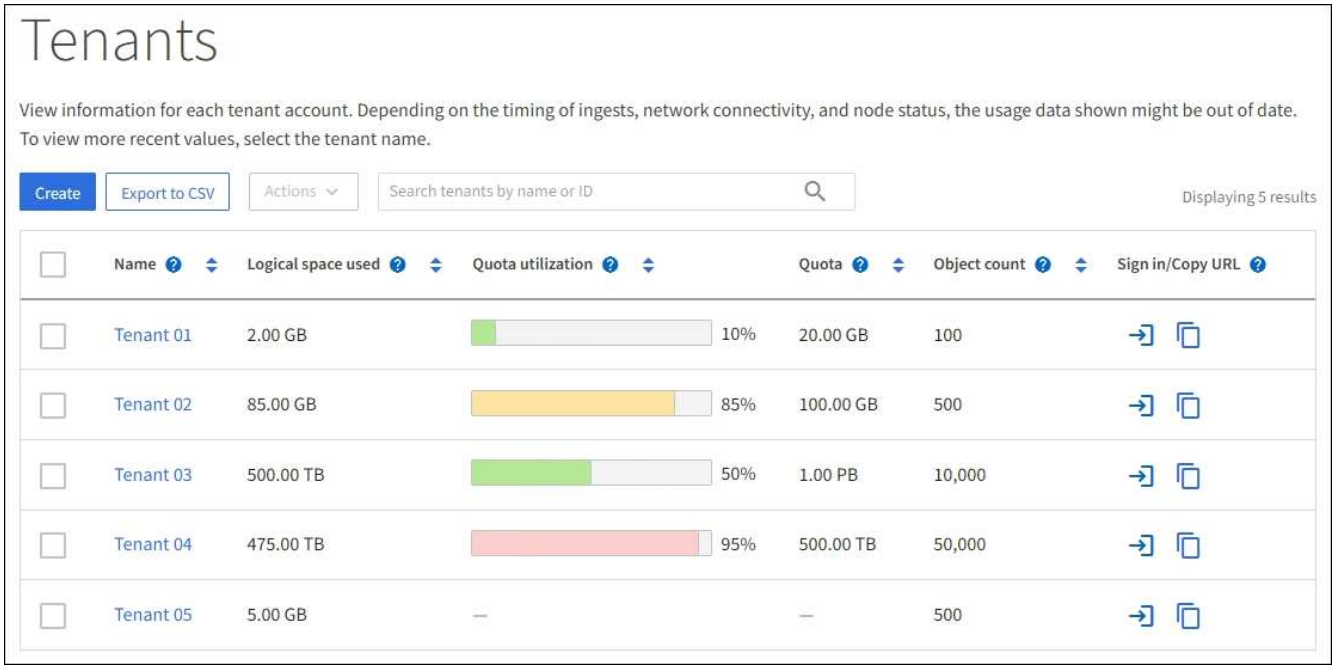
步驟

1. 選擇*租戶*。
2. 檢閱租戶頁面上顯示的資訊。

   每個租戶都會列出「已使用的邏輯空間」、「配額使用量」、「配額」和「物件」計數。如果未為租戶設定

配額、「配額使用量」和「配額」欄位會包含破折號（ &#8212 ；）。

> 屬於該租戶的所有物件的邏輯大小包括未完成和正在進行的分段上傳。此大小不包括用於 ILM 策略的額外實體空間。已用空間值是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。



3. （可選）透過選擇 **Sign in/Copy URL** 欄中的登入連結 登入租用戶帳戶。
4. （可選）在 **Sign in/Copy URL** 欄中選取複製 URL 連結 ，以複製租用戶登入頁面的 URL。
5. 您也可以選擇 * 匯出至 CSV* 來檢視和匯出 `.csv`包含所有租戶使用值的檔案。

   系統會提示您開啟或儲存 `.csv`檔案。

   檔案內容 `.csv`如下所示：

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   您可以在試算表應用程式中開啟 `.csv`檔案、或在自動化中使用。

6. 如果沒有列出任何物件、請選擇性地選取 * 動作 * > * 刪除 * 來移除一或多個租戶。請參閱。 "刪除租戶帳戶"

   如果帳戶包含任何貯體或容器、則無法移除租戶帳戶。

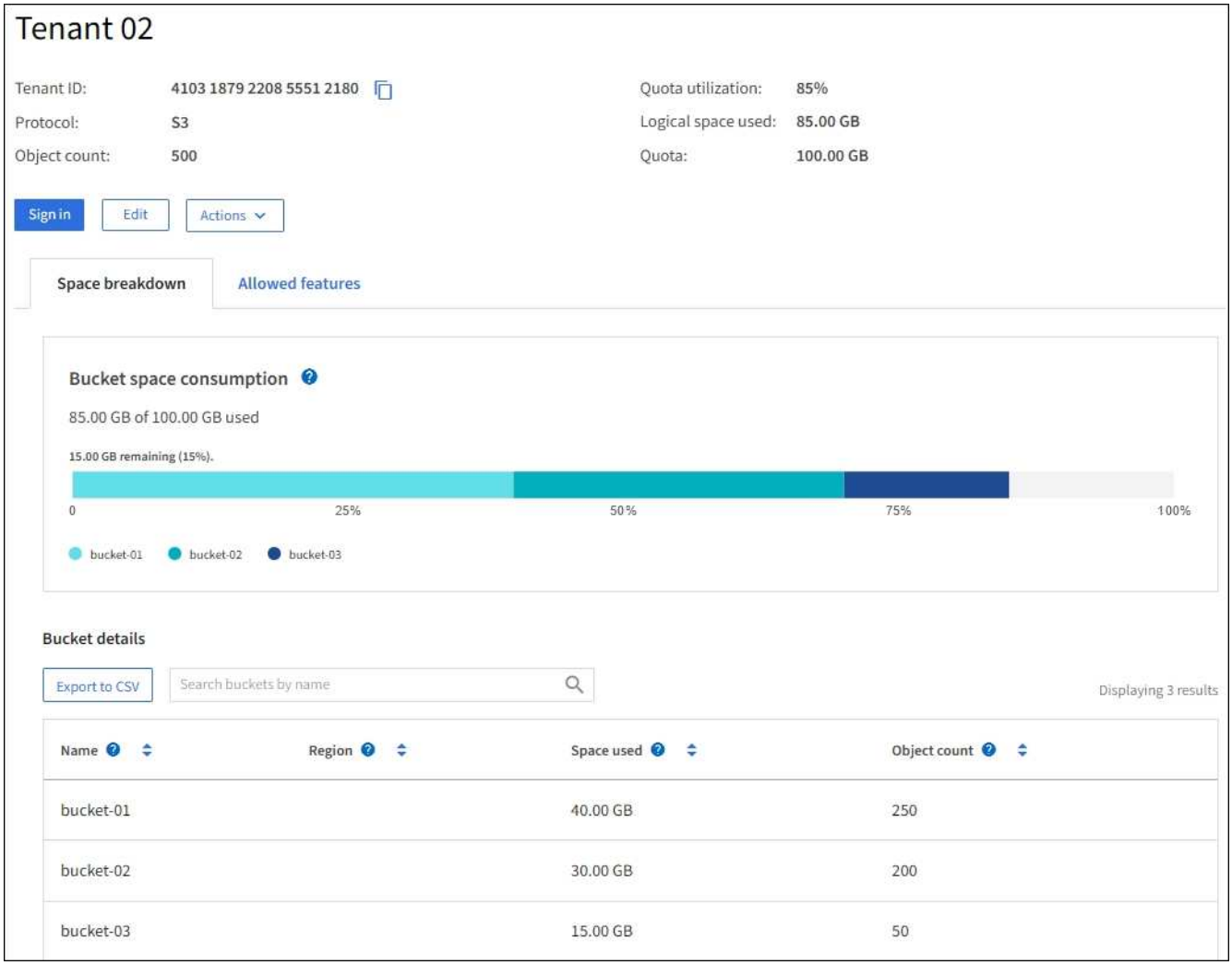
檢視特定租戶

您可以檢視特定租戶的詳細資料。

步驟

1. 從「租戶」頁面中選取租戶名稱。

   此時會顯示租戶詳細資料頁面。



2. 檢閱頁面頂端的租戶總覽。

   詳細資料頁面的這個區段提供租戶的摘要資訊、包括租戶的物件數、配額使用量、使用的邏輯空間和配額設定。

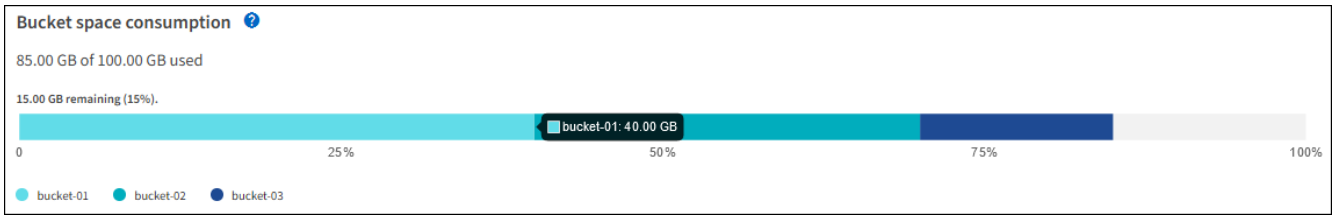
   > 屬於該租戶的所有物件的邏輯大小包括未完成和正在進行的分段上傳。此大小不包括用於 ILM 策略的額外實體空間。已用空間值是估計值。這些估計值受到攝取時間、網路連接和節點狀態的影響。

3. 從 * 空間分解 * 索引標籤、檢閱 * 空間消耗 * 圖表。

   此圖表顯示所有租戶 S3 貯體的總空間使用量。

   如果爲此租戶設置了配額，則使用的配額量和剩餘的配額將以文本形式顯示（例如 `85.00 GB of 100 GB used`）。如果未設定配額、則租戶具有無限配額、且文字僅包含已使用的空間量（例如 `85.00 GB used`）。長條圖會顯示每個儲存區或容器中的配額百分比。如果租戶超過儲存配額1%以上、而且至少1 GB、則圖表會顯示總配額和超額金額。

您可以將游標放在橫條圖上、以查看每個儲存桶或容器所使用的儲存設備。您可以將游標放在可用空間區段上、以查看剩餘的儲存配額量。



配額使用量是根據內部預估、在某些情況下可能會超過。例如StorageGRID 、當租戶開始上傳物件時、會檢查配額、如果租戶超過配額、則會拒絕新的擷取。不過StorageGRID 、判斷是否超過配額時、不考慮目前上傳的大小。如果刪除物件、可能會暫時禁止租戶上傳新物件、直到重新計算配額使用量為止。配額使用量計算可能需要 10 分鐘或更長時間。

租戶的配額使用量會指出租戶已上傳至 StorageGRID 的物件資料總量（邏輯大小）。配額使用量並不代表用來儲存這些物件及其中繼資料複本（實體大小）的空間。

您可以啟用 * 租戶配額使用量高 * 警示規則、以判斷租戶是否正在使用其配額。如果啟用、當租戶使用90%的配額時、就會觸發此警示。有關說明，請參閱"編輯警示規則"。

4. 從 * 空間分解 * 索引標籤、檢閱 * 庫位詳細資料 * 。

   此表列出租戶的 S3 儲存區。「已用空間」是指儲存區或容器中的物件資料總量。此值不代表ILM複本和物件中繼資料所需的儲存空間。

5. （可選）選擇*匯出至CSV*以檢視及匯出內含每個儲存區或容器使用值的.csv*檔案。

   個別 S3 租戶檔案的內容 `.csv`如下所示：

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   您可以在試算表應用程式中開啟 `.csv`檔案、或在自動化中使用。

6. 您也可以選擇 * 允許的功能 * 索引標籤、查看已啟用租戶的權限和功能清單。查看"編輯租戶帳戶"您是否需要變更這些設定。
7. 如果租戶具有 * 使用網格同盟連線 * 權限、請選擇性地選取 * 網格同盟 * 索引標籤、以深入瞭解連線。

   請參閱"什麼是網格同盟？"和"管理 Grid Federation 的允許租戶"。

檢視網路流量

如果租戶已制定流量分類原則、請檢閱該租戶的網路流量。

步驟

1. 選擇*配置* > 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. 檢閱原則清單、找出適用於特定租戶的原則。
3. 若要檢視與原則相關的度量、請選取原則左側的選項按鈕、然後選取 * 度量 * 。
4. 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。

如需詳細資訊、請參閱 "管理流量分類原則" 。

使用稽核記錄

您也可以選擇使用稽核記錄來更精細地監控租戶的活動。

例如、您可以監控下列類型的資訊：

- 特定的用戶端作業、例如PUT、Get或DELETE
- 物件大小
- 套用至物件的ILM規則
- 用戶端要求的來源IP

稽核記錄會寫入文字檔、您可以使用所選的記錄分析工具進行分析。這可讓您更深入瞭解客戶活動、或實作精密的計費與計費模式。

如需詳細資訊、請參閱 "檢閱稽核記錄" 。

使用 **Prometheus** 指標

您也可以選擇使用 Prometheus 指標來報告租戶活動。

- 在網格管理員中，選擇*支援* > 工具 > 指標。您可以使用現有的儀表板（例如 S3 概覽）來查看客戶活動。

> 「指標」頁面上提供的工具主要供技術支援使用。這些工具中的某些功能和功能表項目是刻意無法運作的。

- 從 Grid Manager 頂端選取說明圖示、然後選取 * API 文件 * 。您可以使用Grid Management API的「度量」區段中的度量、為租戶活動建立自訂警示規則和儀表板。

如需詳細資訊、請參閱 "檢視支援指標" 。

監控 **StorageGRID** 中的 **S3** 用戶端作業

您可以監控物件擷取和擷取速率、以及物件計數、查詢和驗證的度量。您可以檢視用戶端應用程式在StorageGRID 讀取、寫入及修改物件時、成功和失敗的嘗試次數。

開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

步驟

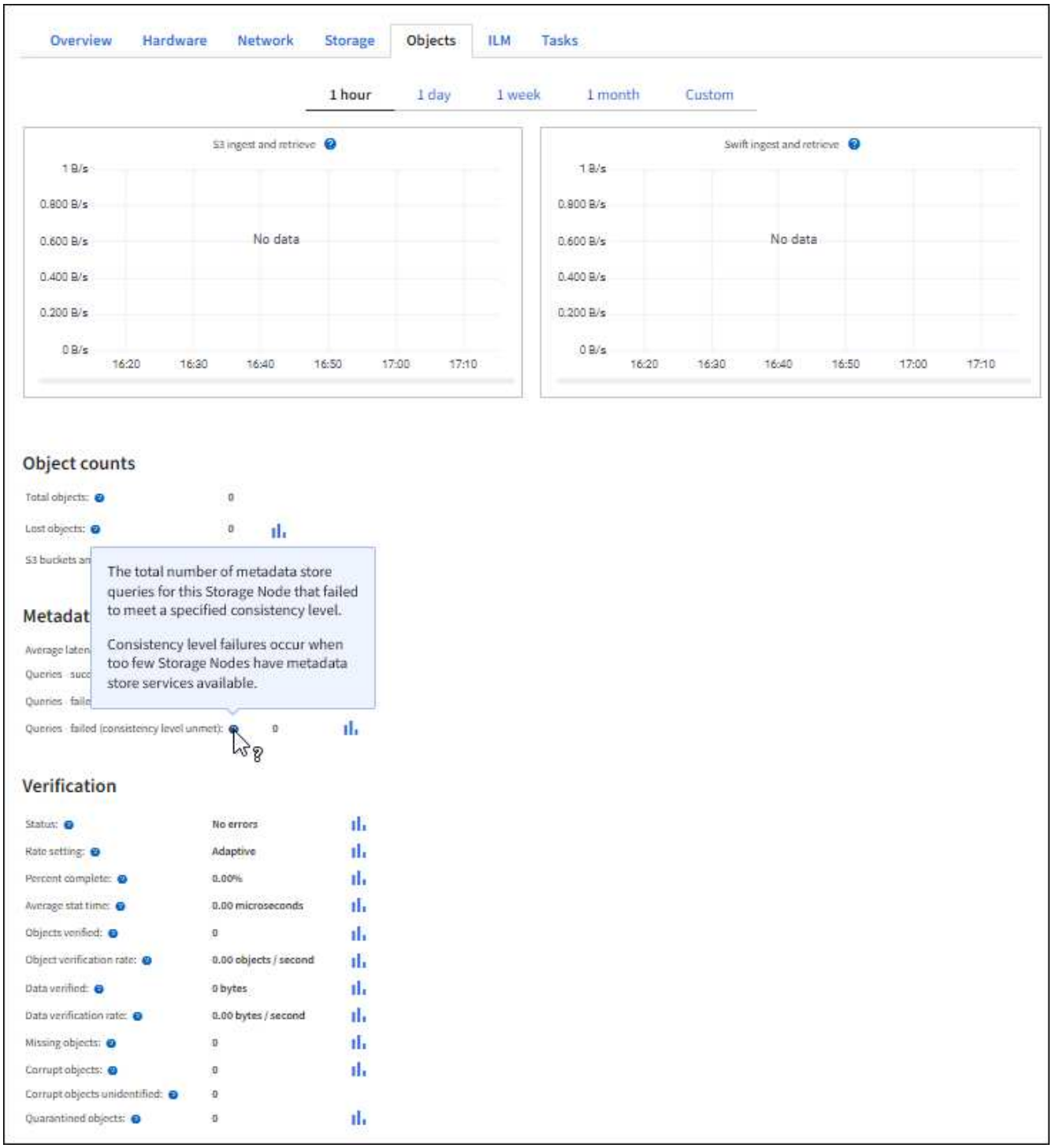
1. 從儀表板選取 * 效能 * 索引標籤。

2. 請參閱 S3 圖表、其中摘要說明儲存節點執行的用戶端作業數、以及儲存節點在所選時間範圍內接收的 API 要求數。
3. 選擇“節點”以存取“節點”頁面。
4. 從節點首頁（網格層級）選取 * 物件 * 索引標籤。

   此圖表顯示整個 StorageGRID 系統的 S3 擷取和擷取速率、單位為每秒位元組數、以及擷取或擷取的資料量。您可以選擇時間間隔或套用自訂時間間隔。

5. 若要查看特定儲存節點的資訊、請從左側清單中選取節點、然後選取 * 物件 * 索引標籤。

   圖表顯示節點的擷取和擷取速率。索引標籤也包含物件計數、中繼資料查詢和驗證作業的度量。



監控 **StorageGRID** 中的負載平衡作業

如果您使用負載平衡器來管理用戶端與StorageGRID VMware的連線、則應先設定系統、然後在進行任何組態變更或執行擴充之後、監控負載平衡作業。

關於這項工作

您可以使用管理節點或閘道節點上的負載平衡器服務、或外部協力廠商負載平衡器、將用戶端要求分散到多個儲存節點上。

設定負載平衡之後、您應該確認物件擷取和擷取作業在儲存節點之間平均分散。平均分散的要求可確

保StorageGRID 在負載下、不影響到客戶要求的回應能力、並有助於維持用戶端效能。

如果您在主動備份模式中設定了閘道節點或管理節點的高可用度（HA）群組、則群組中只有一個節點會主動散佈用戶端要求。

如需更多資訊、請參閱 "設定 S3 用戶端連線"。

步驟

1. 如果 S3 用戶端使用負載平衡器服務進行連線、請檢查管理節點或閘道節點是否正在依您預期的方式主動分配流量：
   a. 選擇*節點*。
   b. 選取閘道節點或管理節點。
   c. 在 * 概述 * 標籤上、檢查節點介面是否位於 HA 群組中、以及節點介面是否具有「主要」角色。

      具有「主要」角色的節點和不在 HA 群組中的節點應主動將要求發佈給用戶端。

   d. 對於每個應該主動分配用戶端要求的節點，請選取"負載平衡器索引標籤"。
   e. 檢閱上週的負載平衡器要求流量圖表、確保節點已主動散佈要求。

      主動備份HA群組中的節點可能會不時扮演備份角色。在此期間、節點不會散佈用戶端要求。

   f. 檢閱上週負載平衡器傳入要求率圖表、以檢閱節點的物件處理量。
   g. 對StorageGRID 整個系統中的每個管理節點或閘道節點重複這些步驟。
   h. 或者、您也可以使用流量分類原則來檢視負載平衡器服務所提供流量的更詳細分析。
2. 請確認這些要求平均分散到儲存節點。
   a. 選擇「儲存節點_」>「* LdR*」>「* HTTP *」。
   b. 檢閱*目前建立的傳入工作階段數目*。
   c. 針對網格中的每個儲存節點重複上述步驟。

      所有儲存節點之間的工作階段數量應大致相同。

監控 **StorageGRID** 網格聯盟連線

您可以監控關於所有"網格同盟連線"的基本資訊、特定連線的詳細資訊、或是關於跨網格複寫作業的 Prometheus 指標。您可以從任一網格監控連線。

開始之前

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

檢視所有連線

「 Grid Federation 」頁面會顯示所有網格同盟連線的基本資訊、以及所有允許使用網格同盟連線的租戶帳戶。

步驟

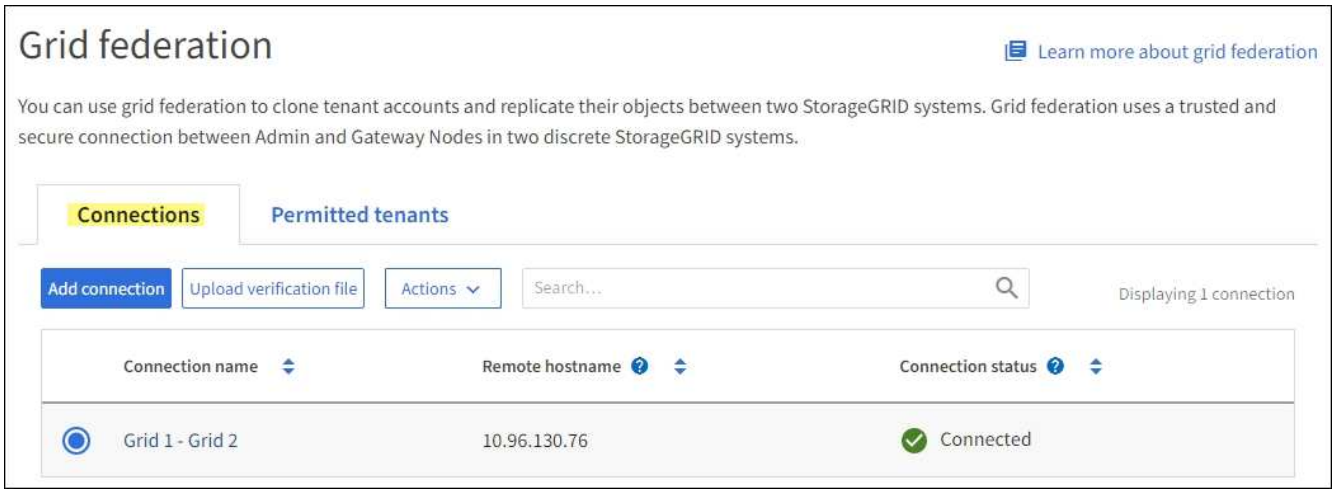
1. 選擇*配置* > 系統 > 網格聯合。

   「 Grid Federation 」頁面隨即出現。

2. 若要查看此網格上所有連線的基本資訊、請選取 * 連線 * 索引標籤。

   您可以從這個索引標籤：

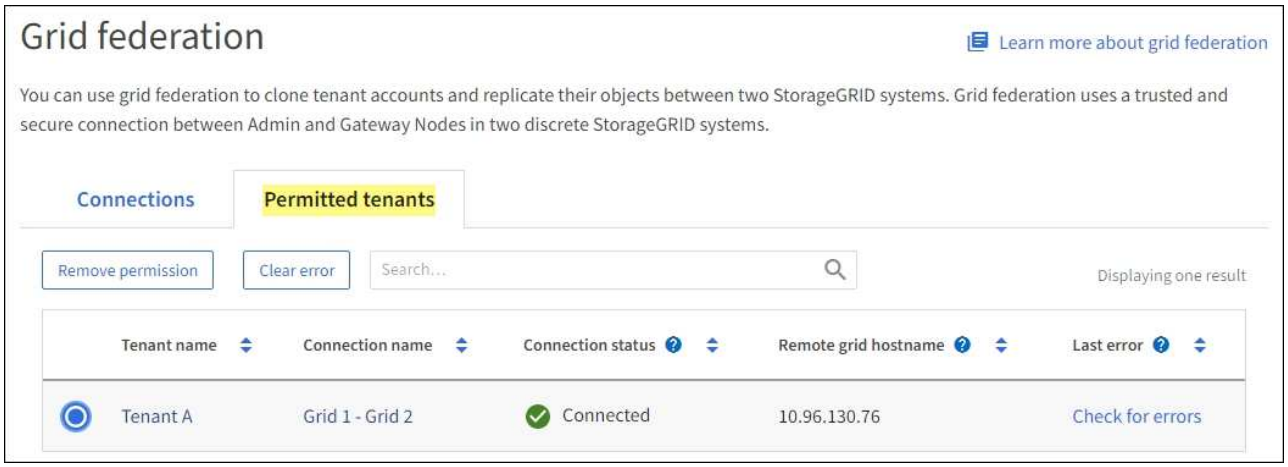
   - "建立新連線"。
   - 選擇與的現有連線"編輯或測試"。



3. 若要查看此網格上具有「 * 使用網格同盟連線 * 」權限的所有租戶帳戶的基本資訊、請選取 * 允許租戶 * 索引標籤。

   您可以從這個索引標籤：

   - "檢視每個允許租戶的詳細資料頁面"。
   - 檢視每個連線的詳細資料頁面。請參閱。 檢視特定連線
   - 選擇允許的租戶，然後選擇"移除權限"。
   - 檢查跨網格複寫錯誤、並清除最後一個錯誤（如果有）。請參閱。 "疑難排解網格同盟錯誤"



[[view-specific 連線]] 檢視特定連線

您可以檢視特定網格同盟連線的詳細資料。

步驟

1. 從「 Grid Federation 」頁面中選取任一索引標籤、然後從表格中選取連線名稱。

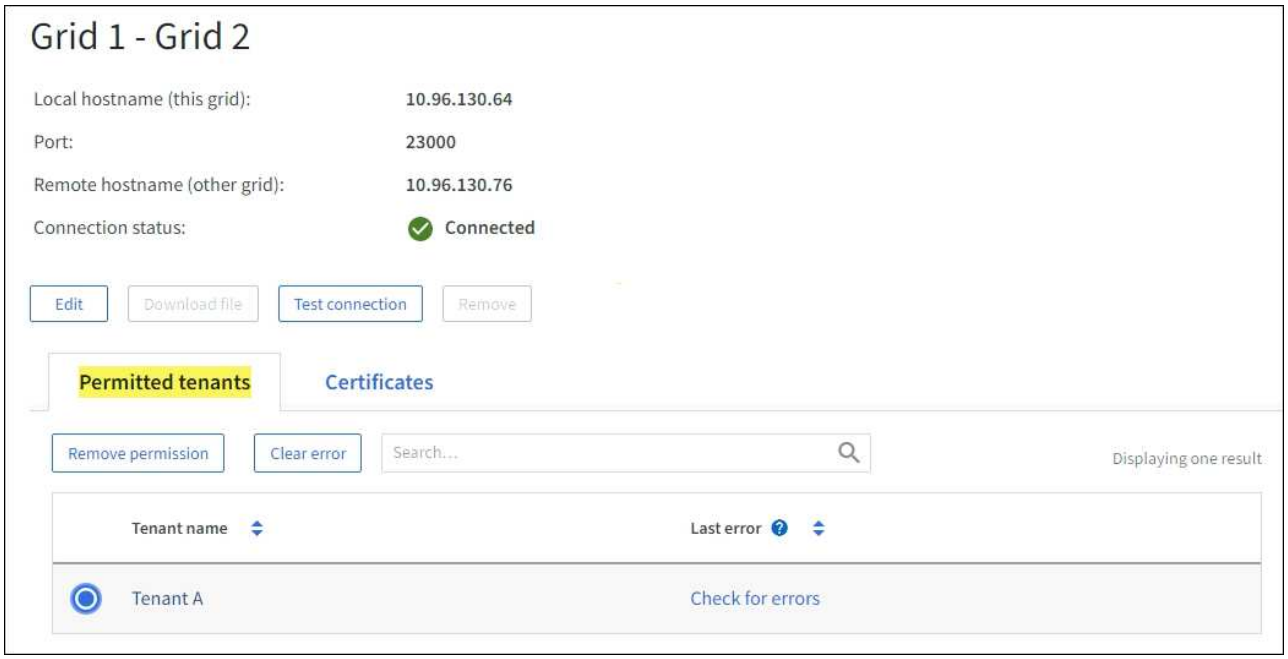
   從連線的詳細資料頁面、您可以：

   - 查看連線的基本狀態資訊、包括本機和遠端主機名稱、連接埠和連線狀態。
   - 選擇與的連線"編輯、測試或移除"。

2. 檢視特定連線時、請選取 * 允許的租戶 * 索引標籤、以檢視連線允許租戶的詳細資料。

   您可以從這個索引標籤：

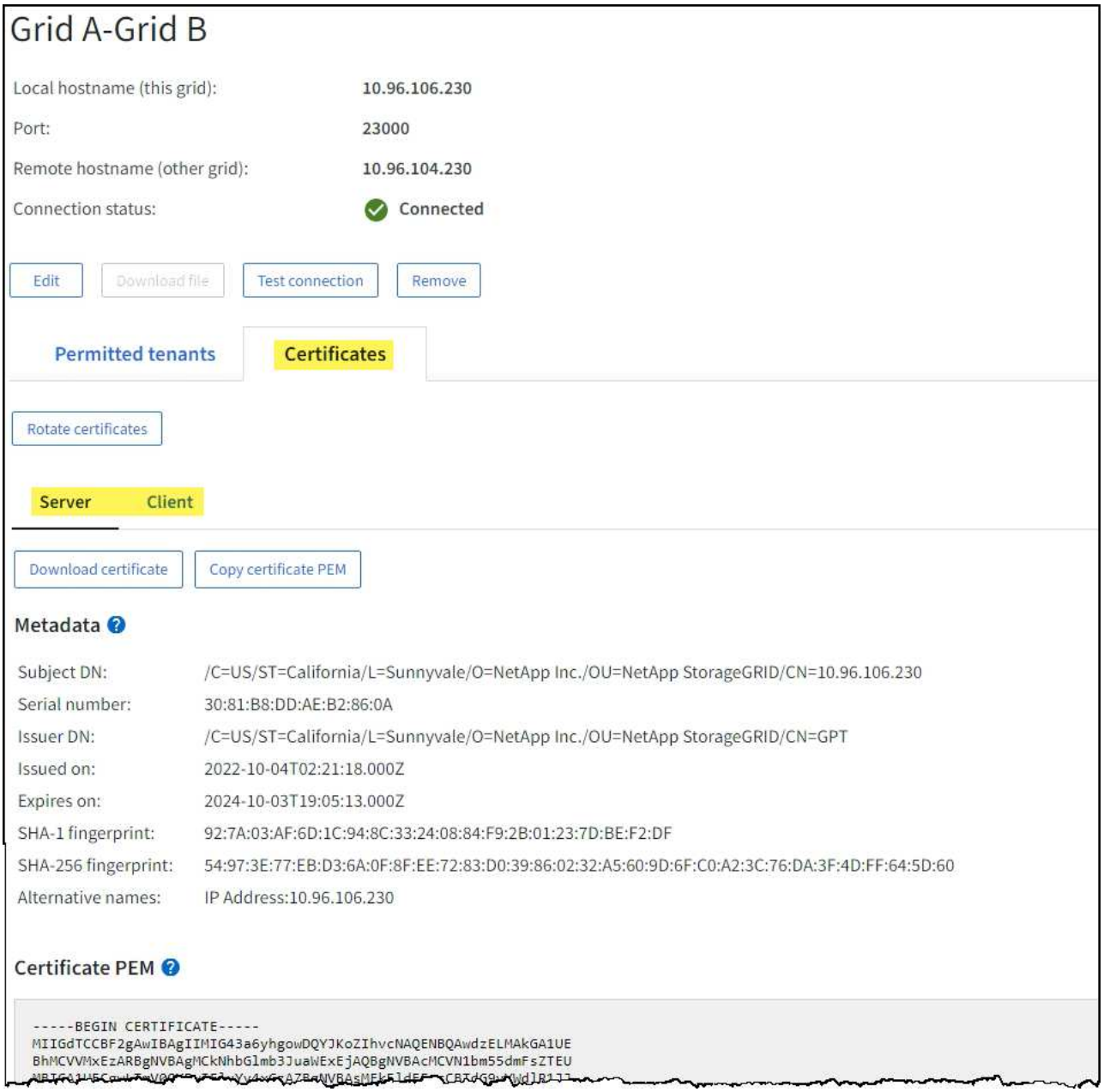
   - "檢視每個允許租戶的詳細資料頁面"。
   - "移除租戶權限"以使用連線。
   - 檢查跨網格複寫錯誤、並清除最後一個錯誤。請參閱。 "疑難排解網格同盟錯誤"



3. 檢視特定連線時、請選取 * 憑證 * 索引標籤、以檢視此連線的系統產生伺服器和用戶端憑證。

   您可以從這個索引標籤：

   - "旋轉連線憑證"。
   - 選取 * 伺服器 * 或 * 用戶端 * 以檢視或下載相關的憑證、或複製憑證 PEM 。



檢閱跨網格複寫指標

您可以使用 Grafana 中的跨網格複寫儀表板來檢視 Prometheus 在您網格上跨網格複寫作業的計量。

步驟

1. 從網格管理器中，選擇*支援* > 工具 > 指標。

   「指標」頁面上提供的工具僅供技術支援使用。這些工具中的某些功能和功能表項目會刻意無法運作、而且可能會有所變更。請參閱清單"常用的Prometheus指標"。

2. 在頁面的 Grafana 區段中、選取 * 跨網格複寫 * 。

   有關詳細說明，請參閱"檢視支援指標"。

3. 若要重試複寫無法複寫的物件、請參閱"識別並重試失敗的複寫作業"。

管理警示

管理 StorageGRID 中的警示

警示系統提供易於使用的介面、可偵測、評估及解決StorageGRID 在執行過程中可能發生的問題。

當警示規則條件評估為真時、警示會以特定的嚴重性層級觸發。觸發警示時、會發生下列動作：

- Grid Manager 的儀表板上會顯示警示嚴重性圖示、目前警示的數量也會增加。
- 警報顯示在 **Nodes** 摘要頁面和 **Nodes** > ***node*** > **Overview** 標籤上。
- 系統會傳送電子郵件通知、前提是您已設定一個SMTP伺服器、並提供收件者的電子郵件地址。
- 假設您已設定StorageGRID 好Sing SNMP代理程式、系統就會傳送簡單網路管理傳輸協定（SNMP）通知。

您可以建立自訂警示、編輯或停用警示、以及管理警示通知。

若要深入瞭解：

- 回顧影片：

  警報概述

  自訂警報

- 請參閱"警示參考資料"。

檢視 StorageGRID 警示規則

警示規則定義觸發"特定警示"的條件。包含一組預設警示規則、您可以使用或修改這些規則、也可以建立自訂警示規則。StorageGRID

您可以檢視所有預設和自訂警示規則的清單、以瞭解哪些條件會觸發每個警示、並查看是否已停用任何警示。

開始之前

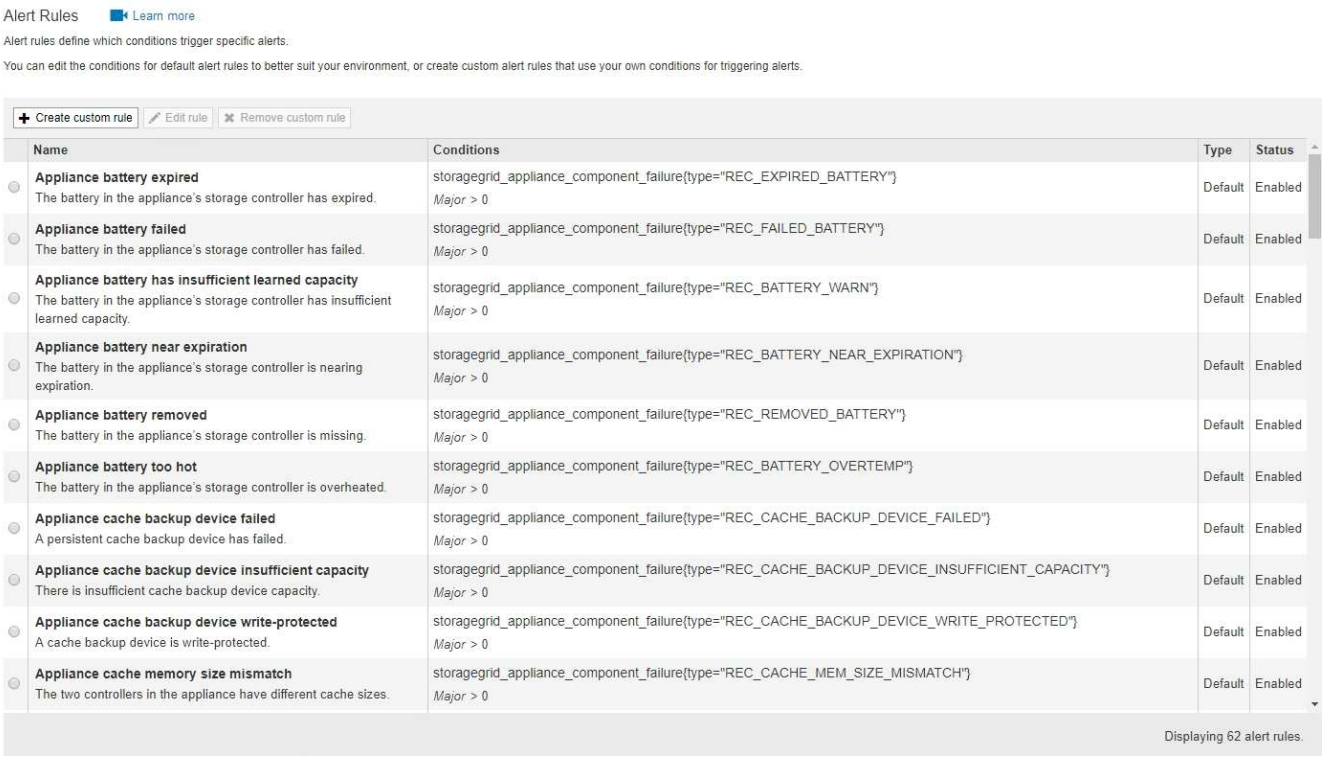
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。
- 或者，您已經觀看了影片：

  警報概述

步驟

1. 選擇*警報* > 規則。

   此時會出現警示規則頁面。



2. 檢閱警示規則表中的資訊：

欄標題	說明
名稱	警示規則的唯一名稱和說明。自訂警示規則會先列出、然後依循預設警示規則。警示規則名稱是電子郵件通知的主旨。
條件	判斷何時觸發此警示的Prometheus運算式。警示可在下列一個或多個嚴重性層級觸發、但不需要每個嚴重性層級的條件。 • **Critical** ：StorageGRID 節點或服務出現異常情況，導致其正常運作停止。您必須立即解決根本問題。如果問題無法解決，可能會導致服務中斷和資料遺失。 • 重大 ：存在異常情況，該情況正在影響目前作業或接近嚴重警示的閾值。您應調查重大警示並解決任何潛在問題，以確保異常情況不會停止 StorageGRID 節點或服務的正常運作。 • 輕微 ：系統目前運作正常，但有異常情況，如果持續下去可能會影響系統運作。您應監控並解決不會自行消失的輕微警示，以確保它們不會導致更嚴重的問題。

欄標題	說明
類型	警示規則類型： • 預設：系統隨附的警示規則。您可以停用預設警示規則、或編輯預設警示規則的條件和持續時間。您無法移除預設的警示規則。 • 預設：包含編輯條件或持續時間的預設警示規則。視需要、您可以輕鬆地將修改後的條件還原為原始預設值。 • 自訂：您建立的警示規則。您可以停用、編輯及移除自訂警示規則。
狀態	此警示規則目前是否已啟用或停用。停用的警示規則條件不會受到評估、因此不會觸發警示。

在 **StorageGRID** 中建立自訂警示規則

您可以建立自訂警示規則、以定義自己觸發警示的條件。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。
- 您熟悉"常用的Prometheus指標"。
- 您瞭解 "Prometheus查詢的語法"。
- 或者，您已經觀看了影片：

  自訂警報

關於這項工作

無法驗證自訂警示。StorageGRID如果您決定建立自訂警示規則、請遵循下列一般準則：

- 查看預設警示規則的條件、並將其做為自訂警示規則的範例。
- 如果您為警示規則定義多個條件、請針對所有條件使用相同的運算式。然後變更每個條件的臨界值。
- 仔細檢查每個條件是否有錯字和邏輯錯誤。
- 僅使用Grid Management API中列出的度量。
- 使用 Grid Management API 測試運算式時、請注意「成功」回應可能是空的回應主體（未觸發警示）。若要查看警示是否實際觸發、您可以暫時將臨界值設定為目前預期為真的值。

  例如、若要測試運算式 `node_memory_MemTotal_bytes < 24000000000`、請先執行、`node_memory_MemTotal_bytes >= 0`並確保您獲得預期的結果（所有節點都會傳回值）。接著、將運算子和臨界值變更回預期值、然後再次執行。沒有任何結果表示此運算式目前沒有警示。

- 除非您已驗證警示會在預期時觸發、否則請勿假設自訂警示正常運作。

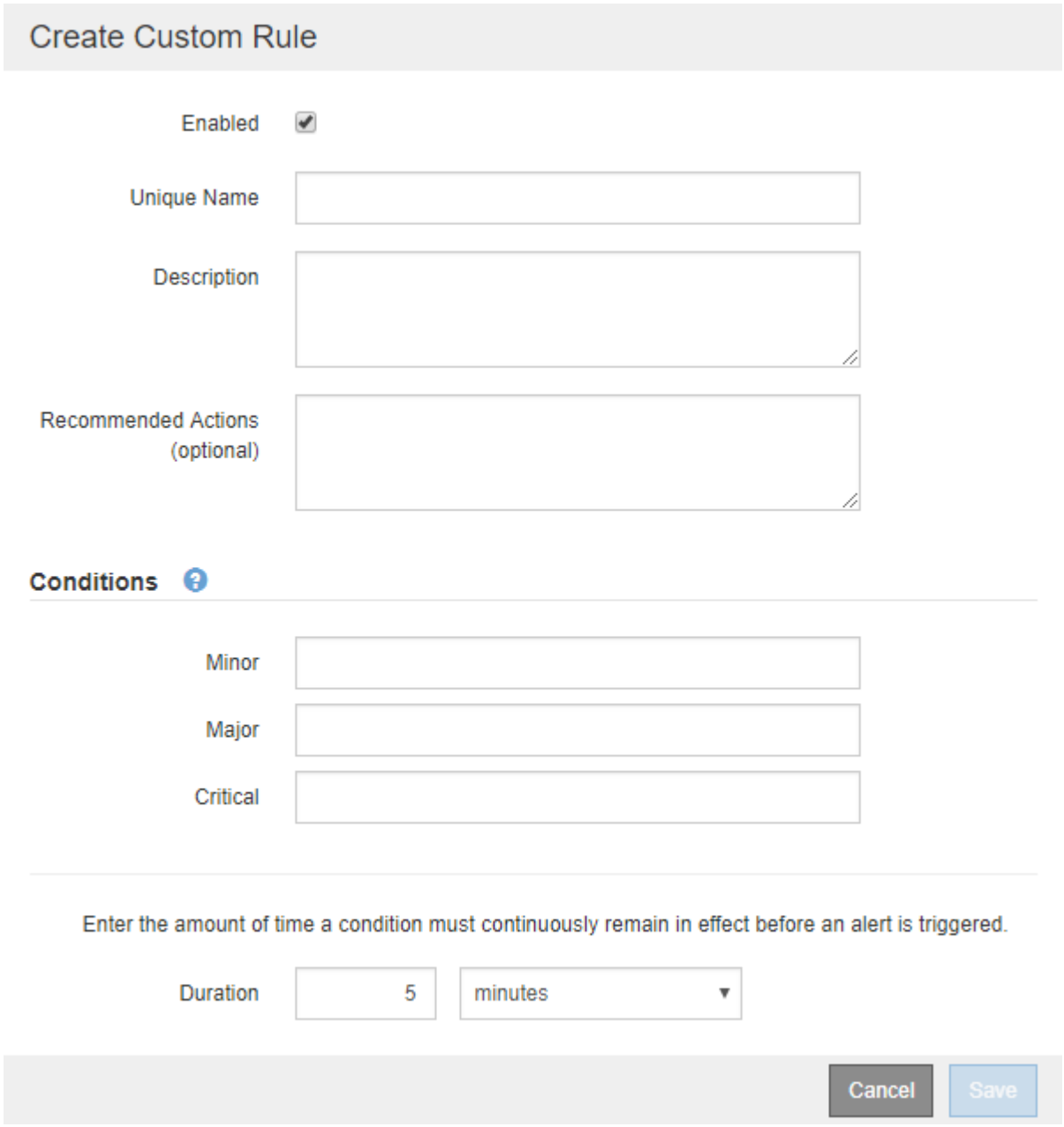
步驟

1. 選擇*警報* > 規則。

此時會出現警示規則頁面。

2. 選取*建立自訂規則*。

「建立自訂規則」對話方塊隨即出現。



3. 選取或清除 **Enabled** 核取方塊、以判斷目前是否啟用此警示規則。

如果停用警示規則、則不會評估其運算式、也不會觸發警示。

4. 輸入下列資訊：

欄位	說明
唯一名稱	此規則的唯一名稱。警示規則名稱會顯示在「警示」頁面上、也是電子郵件通知的主旨。警示規則的名稱可以介於1到64個字元之間。
說明	所發生問題的說明。說明是警示訊息、顯示在「警示」頁面和電子郵件通知中。警示規則的說明可介於1到128個字元之間。
建議行動	也可以選擇觸發此警示時要採取的建議行動。以純文字輸入建議的動作（無格式化代碼）。警示規則的建議動作可介於0到1,024個字元之間。

5. 在「條件」區段中、輸入一或多個警示嚴重性層級的Prometheus運算式。

   基本運算式通常採用以下形式：

   ```
   [metric] [operator] [value]
   ```

   運算式可以是任何長度、但會出現在使用者介面的單行上。至少需要一個運算式。

   如果節點安裝的RAM容量少於24、000、000、000位元組（24 GB）、則會觸發警示。

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   若要查看可用指標並測試 Prometheus 運算式，請選擇說明圖示 並點擊連結進入 Grid Management API 的 Metrics 區段。

6. 在*持續時間*欄位中、輸入觸發警示之前條件必須持續有效的時間量、然後選取時間單位。

   要在條件變爲true時立即觸發警報，請輸入*0*。請增加此值、以防止暫時性情況觸發警示。

   預設值為 5 分鐘。

7. 選擇*保存*。

   對話方塊隨即關閉、新的自訂警示規則會出現在警示規則表格中。

在 **StorageGRID** 中編輯警示規則

您可以編輯警示規則來變更觸發條件、針對自訂警示規則、也可以更新規則名稱、說明及建議的動作。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。

關於這項工作

當您編輯預設警示規則時、可以變更次要、主要和關鍵警示的條件、以及持續時間。當您編輯自訂警示規則時、也可以編輯規則的名稱、說明和建議的動作。

決定編輯警示規則時請務必小心。如果您變更觸發值、則在無法完成關鍵作業之前、可能無法偵測潛在問題。

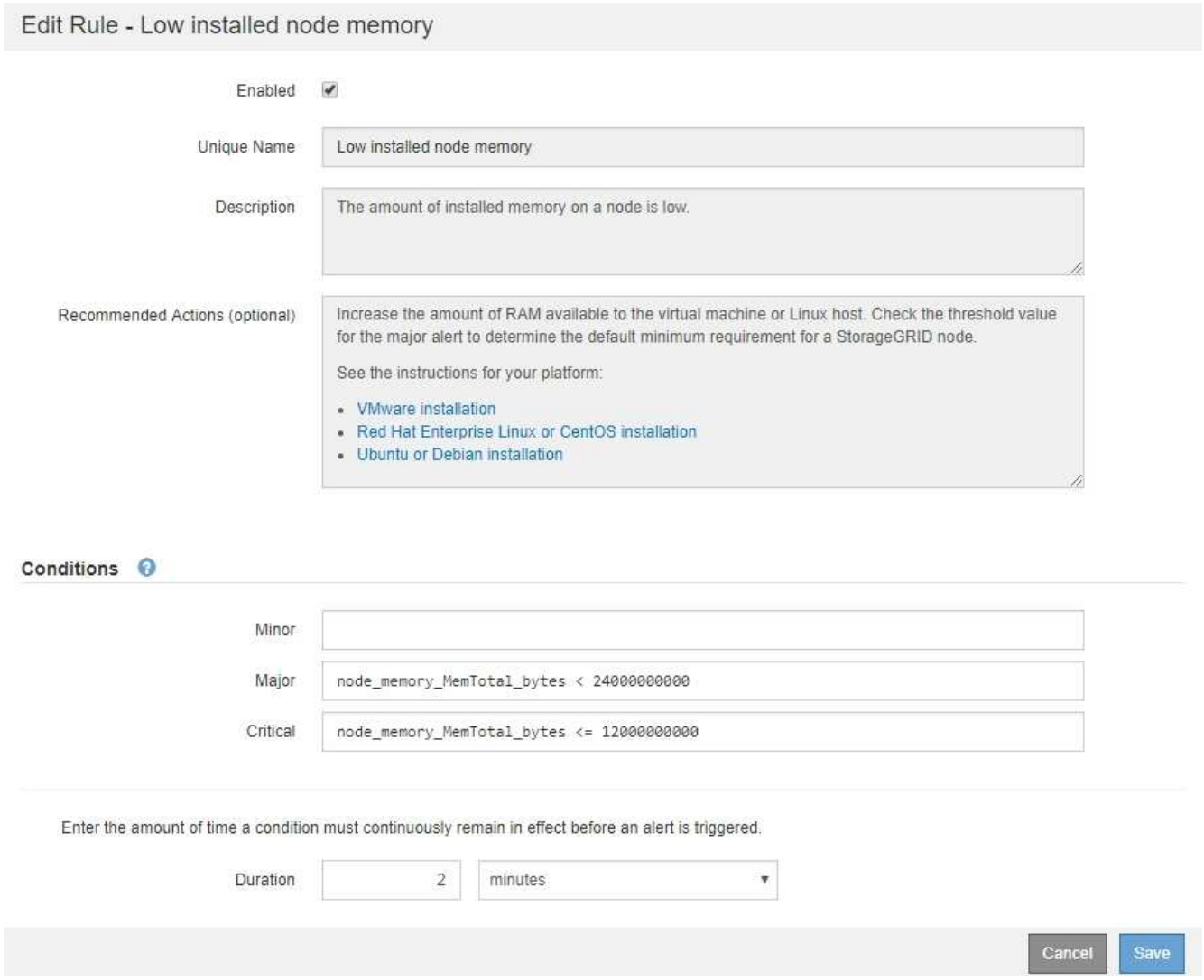
步驟

1. 選擇*警報* > 規則。

   此時會出現警示規則頁面。

2. 選取您要編輯之警示規則的選項按鈕。
3. 選擇*編輯規則*。

   「編輯規則」對話方塊隨即出現。此範例顯示預設警示規則、「唯一名稱」、「說明」和「建議動作」欄位已停用、無法編輯。



4. 選取或清除 **Enabled** 核取方塊、以判斷目前是否啟用此警示規則。

   如果停用警示規則、則不會評估其運算式、也不會觸發警示。

   如果停用目前警示的警示規則、您必須等待數分鐘、使警示不再顯示為作用中警示。

一般而言、不建議停用預設警示規則。如果警示規則已停用、則在無法完成關鍵作業之前、您可能不會偵測到潛在問題。

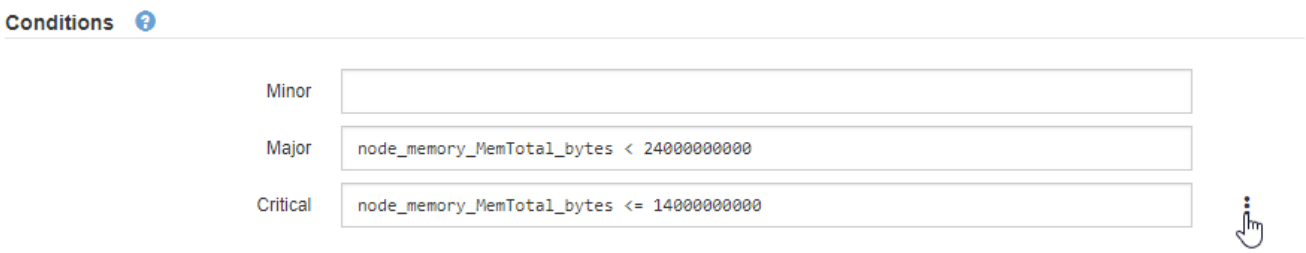
5. 如需自訂警示規則、請視需要更新下列資訊。

您無法編輯預設警示規則的此資訊。

欄位	說明
唯一名稱	此規則的唯一名稱。警示規則名稱會顯示在「警示」頁面上、也是電子郵件通知的主旨。警示規則的名稱可以介於1到64個字元之間。
說明	所發生問題的說明。說明是警示訊息、顯示在「警示」頁面和電子郵件通知中。警示規則的說明可介於1到128個字元之間。
建議行動	也可以選擇觸發此警示時要採取的建議行動。以純文字輸入建議的動作（無格式化代碼）。警示規則的建議動作可介於0到1,024個字元之間。

6. 在「條件」區段中、輸入或更新一或多個警示嚴重性層級的Prometheus運算式。

如果您想要將已編輯的預設警示規則的條件還原回原始值、請選取修改條件右側的三個點。



如果您更新目前警示的條件、則在解決先前的條件之前、您的變更可能不會實作。下次符合規則的其中一個條件時、警示將會反映更新的值。

基本運算式通常採用以下形式：

```
[metric] [operator] [value]
```

運算式可以是任何長度、但會出現在使用者介面的單行上。至少需要一個運算式。

如果節點安裝的RAM容量少於24、000、000、000位元組（24 GB）、則會觸發警示。

```
node_memory_MemTotal_bytes < 24000000000
```

7. 在*持續時間*欄位中、輸入觸發警示之前條件必須持續保持有效的時間量、然後選取時間單位。

要在條件變爲true時立即觸發警報，請輸入*0*。請增加此值、以防止暫時性情況觸發警示。

預設值為 5 分鐘。

8. 選擇*保存*。

   如果您編輯了預設警示規則、*預設*會出現在類型欄中。如果您停用預設或自訂警示規則、*停用*會出現在*狀態*欄中。

停用 StorageGRID 中的警示規則

您可以變更預設或自訂警示規則的啟用/停用狀態。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。

關於這項工作

停用警示規則時、不會評估其運算式、也不會觸發警示。

> 一般而言、不建議停用預設警示規則。如果警示規則已停用、則在無法完成關鍵作業之前、您可能不會偵測到潛在問題。

步驟

1. 選擇*警報* > 規則。

   此時會出現警示規則頁面。

2. 選取您要停用或啟用之警示規則的選項按鈕。
3. 選擇*編輯規則*。

   「編輯規則」對話方塊隨即出現。

4. 選取或清除 **Enabled** 核取方塊、以判斷目前是否啟用此警示規則。

   如果停用警示規則、則不會評估其運算式、也不會觸發警示。

   > 如果停用目前警示的警示規則、您必須等待數分鐘、讓警示不再顯示為作用中警示。

5. 選擇*保存*。

   *停用*會出現在*狀態*欄中。

移除 StorageGRID 中的自訂警示規則

如果您不想再使用自訂警示規則、可以將其移除。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。

- 您有"管理警示或根目錄存取權限"。

步驟

1. 選擇*警報* > 規則。

   此時會出現警示規則頁面。

2. 選取您要移除之自訂警示規則的選項按鈕。

   您無法移除預設的警示規則。

3. 選取*移除自訂規則*。

   隨即顯示確認對話方塊。

4. 選擇*確定*以移除警示規則。

   警示的任何作用中執行個體都會在10分鐘內解決。

管理警示通知

設定 **StorageGRID** 警示的 **SNMP** 通知

如果您想StorageGRID 要在警示發生時傳送SNMP通知、您必須啟用StorageGRID 此功能、並設定一個或多個設陷目的地。

您可以使用網格管理器中的 配置 > 監控 > **SNMP** 代理 選項或網格管理 API 的 SNMP 端點來啟用和設定StorageGRID SNMP 代理程式。 SNMP 代理程式支援 SNMP 協定的所有三個版本。

若要瞭解如何設定 SNMP 代理程式，請參閱"使用SNMP監控"。

設定StorageGRID 完SURE SNMP代理程式後、即可傳送兩種事件導向通知：

- 設陷是 SNMP 代理程式傳送的通知、不需要管理系統的認可。陷阱可讓管理系統知道StorageGRID 在某些情況下發生、例如觸發警示。SNMP的所有三個版本均支援陷阱。
- 通知類似於陷阱、但需要管理系統確認。如果SNMP代理程式在一定時間內未收到確認訊息、則會重新傳送通知、直到收到確認訊息或達到最大重試值為止。在SNMPv2c和v3中支援通知。

在任何嚴重性層級觸發預設或自訂警示時、都會傳送陷阱和通知。若要隱藏警示的SNMP通知、您必須設定警示的靜音。請參閱。 "靜音警示通知"

如果您的 StorageGRID 部署包含多個管理節點、則主要管理節點是警示通知、 AutoSupport 套件和 SNMP 設陷及通知的慣用寄件者。如果主要管理節點無法使用、則其他管理節點會暫時傳送通知。請參閱。 "什麼是管理節點？"

設定 **StorageGRID** 警示的電子郵件通知

如果您想要在警示發生時傳送電子郵件通知、您必須提供有關您的SMTP伺服器的資訊。您也必須輸入警示通知收件者的電子郵件地址。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。
- 您有"已設定電子郵件伺服器"。

關於這項工作

如果您的 StorageGRID 部署包含多個管理節點、則主要管理節點是警示通知、 AutoSupport 套件和 SNMP 設陷及通知的慣用寄件者。如果主要管理節點無法使用、則其他管理節點會暫時傳送通知。請參閱。 "什麼是管理節點？"

步驟

1. 選擇 **Alerts** > **Alerts email**。

   顯示「提醒郵件」頁面。

2. 勾選「啟用電子郵件提醒」核取方塊，表示您希望在警示達到已設定的閾值時傳送通知電子郵件。
3. 在「以嚴重程度接收電子郵件」部分，選取表示您希望收到通知的警示類型的選項按鈕。
4. 在「寄件者」部分，指定一個有效的電子郵件地址，用作警報通知的「寄件者」地址。

   例如： `storagegrid-alerts@example.com`

   a. 在「收件者」區段中、輸入每個電子郵件清單的電子郵件地址、或在發生警示時應接收電子郵件的人員。

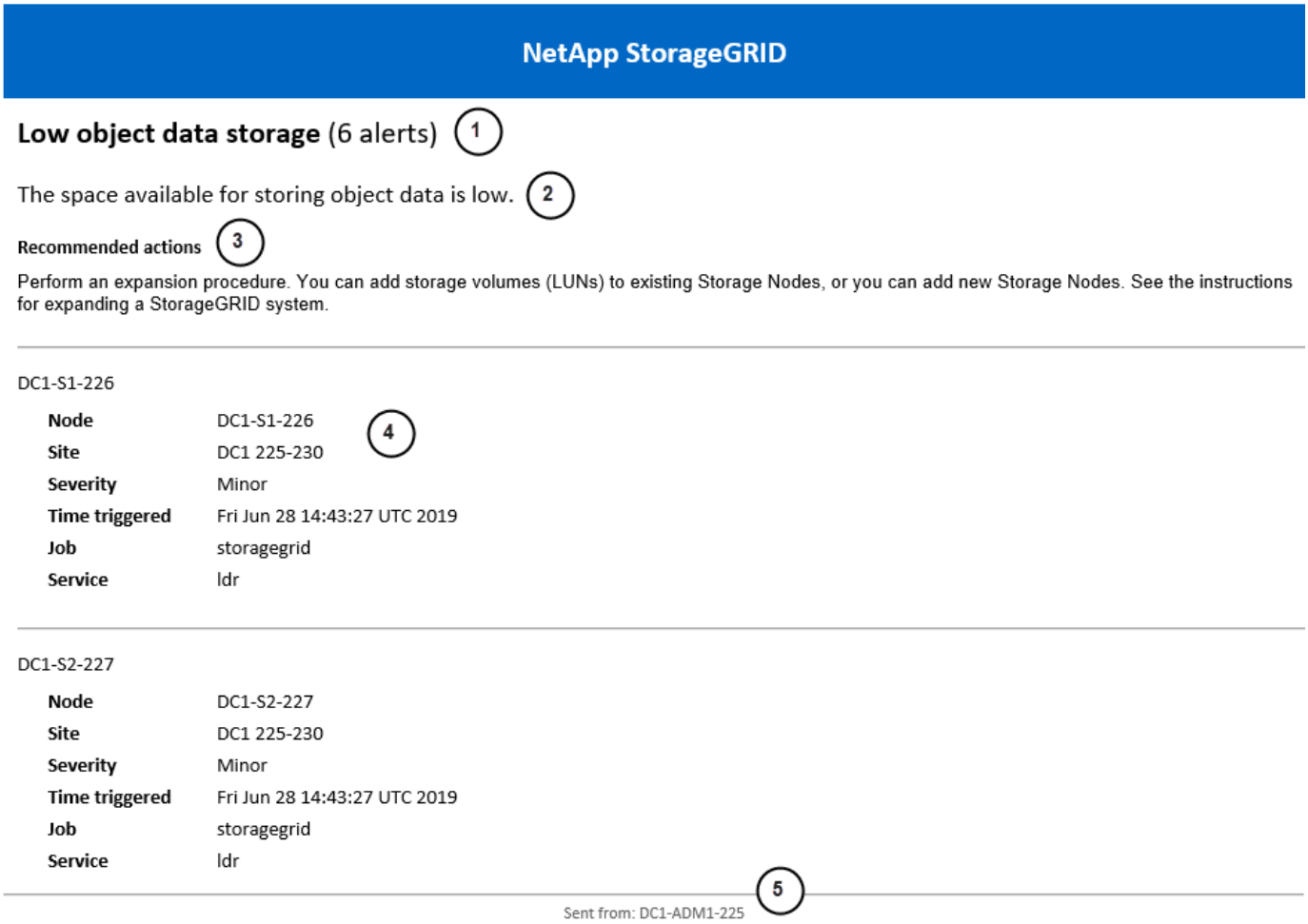
      選擇「新增收件者」以新增收件者。

5. 選擇*保存*。

警示電子郵件通知中包含的資訊

設定郵件伺服器並啟用郵件警報後，除非警報規則被靜默抑制，否則當觸發警報時，系統會向指定的收件者發送電子郵件通知。請參閱 "靜音警示通知"。

電子郵件通知包含下列資訊：



標註	說明
1	警示名稱、後面接著此警示的作用中執行個體數目。
2	警示的說明。
3	針對此警報的建議操作。
4	每個警示作用中執行個體的詳細資料、包括受影響的節點和站台、警示嚴重性、觸發警示規則的UTC時間、以及受影響工作和服務的名稱。
5	傳送通知的管理節點主機名稱。

警示的分組方式

為了避免在觸發警示時傳送過多的電子郵件通知、StorageGRID 所以當同一通知中、我們會嘗試將多個警示分組。

請參閱下表、瞭解StorageGRID 有關如何在電子郵件通知中將多個警示分組的範例。

行為	範例
每個警示通知僅適用於名稱相同的警示。如果同時觸發兩個名稱不同的警示、則會傳送兩個電子郵件通知。	• 同時在兩個節點上觸發警示A。只會傳送一則通知。 • 警示A會在節點1上觸發、而警示B會同時在節點2上觸發。會傳送兩個通知、每個警示各一個。
對於特定節點的特定警示、如果達到超過一個嚴重性的臨界值、則只會針對最嚴重的警示傳送通知。	• 警示A會觸發、並達到次要、主要和關鍵警示臨界值。系統會針對嚴重警示傳送一則通知。
第一次觸發警示時StorageGRID 、不知何時會先等待2分鐘再傳送通知。如果在此期間觸發其他名稱相同的警示、StorageGRID 則會將初始通知中的所有警示分組	1. 警示 A 會在節點 1 的 08:00 觸發。不會傳送通知。 2. 警示 A 會在節點 2 上於 08-01 觸發。不會傳送通知。 3. 在 08 ： 02 時、系統會傳送通知、以回報警示的兩個執行個體。
如果觸發另一個名稱相同的警示、StorageGRID 則在傳送新通知之前、將等候10分鐘。新通知會報告所有作用中的警示（目前尚未靜音的警示）、即使這些警示先前已報告。	1. 警示 A 會在節點 1 的 08:00 觸發。通知會在 08 ： 02 傳送。 2. 警示 A 會於 08 ： 05 在節點 2 上觸發。第二則通知會在 08 ： 15 （ 10 分鐘後）傳送。兩個節點都會報告。
如果有多個目前警示具有相同名稱、且其中一個警示已解決、則在警示已解決的節點上重新出現警示時、不會傳送新的通知。	1. 觸發節點 1 的警示 A 。系統會傳送通知。 2. 觸發節點 2 的警示 A 。第二次通知即會傳送。 3. 節點2的警示A已解決、但節點1的警示A仍為作用中狀態。 4. 再次觸發節點2的警示A。由於節點1的警示仍在作用中、因此不會傳送新通知。
在解決所有警示執行個體或將警示規則設為靜音之前、系統會每7天繼續傳送一次電子郵件通知。StorageGRID	1. 3月8日觸發節點1的警示A。系統會傳送通知。 2. 警示A未解析或靜音。其他通知將於3月15日、3月22日、3月29日等時間傳送。

疑難排解警示電子郵件通知

如果觸發了電子郵件通知故障警報且您未收到郵件，請按照以下步驟調查並解決問題：

- 測試郵件伺服器通知
- StorageGRID 警報郵件
- 多重管理員驗證 (MAV) 電子郵件

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。

- 您擁有"root 存取權限"。如果您擁有管理警報權限，則可以檢視電子郵件伺服器組態，但不能編輯。

步驟

1. 請確認您的警示電子郵件設定。
   a. 確認您已為收件者指定有效的電子郵件地址。
   b. 選擇 **Configuration** > **Email server**，並確認電子郵件（SMTP）伺服器設定是否正確。
2. 檢查垃圾郵件篩選器、確定電子郵件未傳送至垃圾郵件資料夾。
3. 請要求您的電子郵件管理員確認寄件者地址的電子郵件並未遭到封鎖。
4. 請檢查以下與電子郵件傳輸相關的項目：
   a. 郵件伺服器日誌監控：查看 StorageGRID 所使用的郵件伺服器的日誌（設定 > 郵件伺服器）。尋找與 StorageGRID 嘗試傳送電子郵件時間相符的轉送錯誤、驗證錯誤和其他故障。
   b. 未送達報告（退信）：如果郵件未收到且 StorageGRID 未報告故障，則問題可能是退信。將「寄件者」地址設定為有效的電子郵件地址，即可查看這些退信回覆郵件。
5. 收集傳送電子郵件之管理節點的日誌檔案。檢閱 /var/local/log/prometheus.log 和 /var/local/log/nms.log 檔案，找出可能可以修正的明顯問題。如果無法解決問題，請聯絡技術支援。

   技術支援人員可以使用記錄中的資訊來協助判斷發生問題的原因。例如、prometheus.log檔案在連線至您指定的伺服器時可能會顯示錯誤。

   請參閱 "收集記錄檔和系統資料"。

在 **StorageGRID** 中靜音警示通知

或者、您可以設定靜音、以暫時抑制警示通知。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"管理警示或根目錄存取權限"。

關於這項工作

您可以將整個網格、單一站台或單一節點以及一個或多個嚴重性的警示規則設為靜音。每次靜音都會禁止單一警示規則或所有警示規則的所有通知。

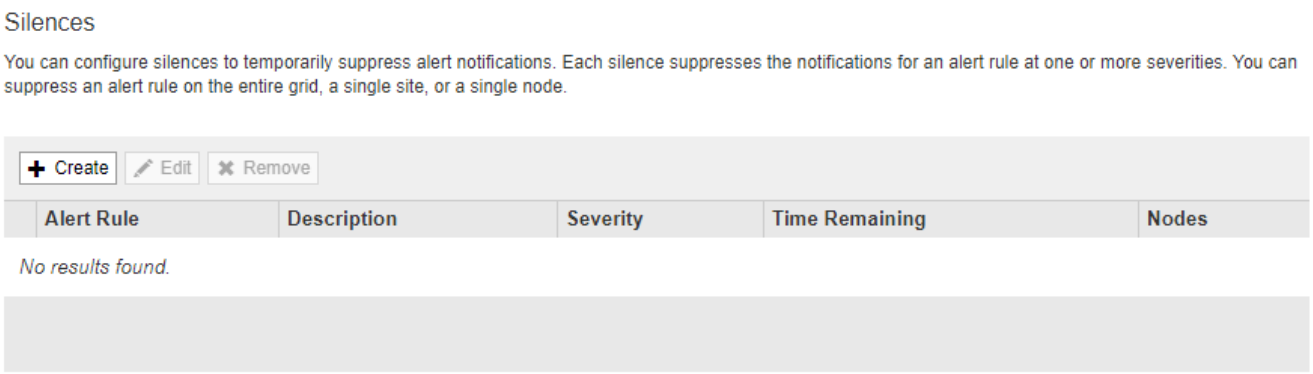
如果您已啟用SNMP代理程式、靜音功能也會抑制SNMP設陷並通知。

> 決定將警示規則設為靜音時請務必小心。如果您將警示設為靜音、則在無法完成關鍵作業之前、可能無法偵測潛在問題。

步驟

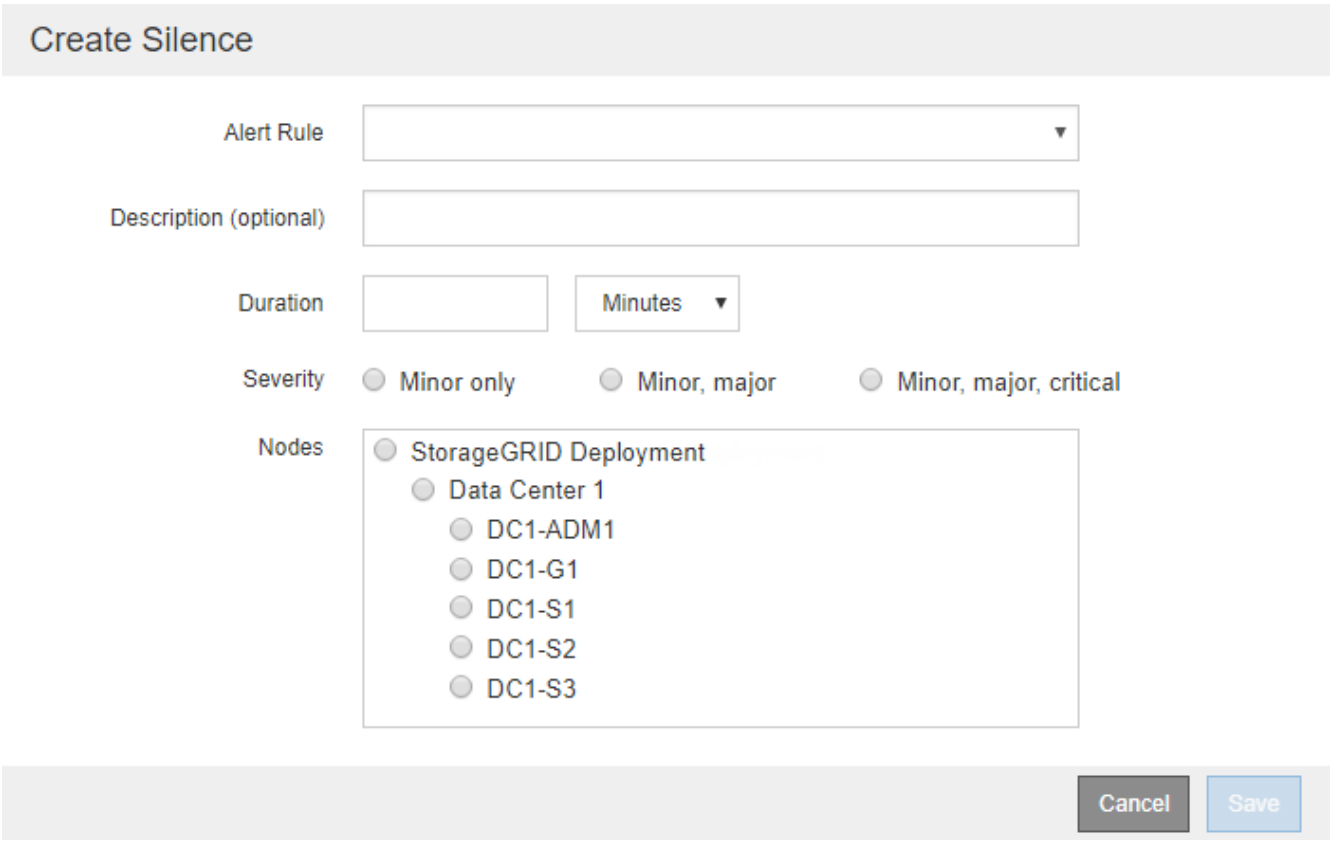
1. 選擇*警報* > 靜音。

   「靜音」頁面隨即出現。



2. 選擇* Create （建立）。

「建立靜音」對話方塊隨即出現。



3. 選取或輸入下列資訊：

欄位	說明
警示規則	您要靜音的警示規則名稱。您可以選取任何預設或自訂警示規則、即使警示規則已停用。 附註：*如果您要使用此對話方塊中指定的準則將所有警示規則設為靜音、請選取*所有規則。
說明	選擇性地說明靜音。例如、說明此靜音的目的。

欄位	說明
持續時間	您希望此靜音保持有效的時間（以分鐘、小時或天為單位）。靜音的生效時間為5分鐘至1、825天（5年）。 *附註：*您不應將警示規則靜音一段較長的時間。如果警示規則設為靜音、您可能無法偵測潛在問題、直到無法完成關鍵作業為止。但是、如果特定的刻意組態觸發警示、例如*服務應用裝置連結向下*警示和*儲存應用裝置連結向下*警示、您可能需要使用延長的靜音。
嚴重性	應將哪些警示嚴重性或嚴重性設為靜音。如果警示是在選取的嚴重性之一觸發、則不會傳送任何通知。
節點	您想要將此靜音套用至哪個節點。您可以隱藏整個網格、單一站台或單一節點上的警示規則或所有規則。如果您選取整個網格、則靜音會套用至所有站台和所有節點。如果您選取站台、則靜音僅適用於該站台的節點。 • 附註： * 您無法為每個靜音選取多個節點或多個站台。如果您想要同時在多個節點或多個站台上隱藏相同的警示規則、則必須建立額外的靜音。

4. 選擇*保存*。
5. 如果您想要在靜音過期之前修改或結束、可以編輯或移除它。

選項	說明
編輯靜音	a. 選擇*警報* > 靜音。 b. 從表格中、選取您要編輯的靜音選項按鈕。 c. 選擇*編輯*。 d. 變更說明、剩餘時間量、選取的嚴重性或受影響的節點。 e. 選擇*保存*。
消除靜音	a. 選擇*警報* > 靜音。 b. 從表格中、選取您要移除的靜音選項按鈕。 c. 選擇*移除*。 d. 選擇*確定*以確認您要移除此靜音。 附註：觸發此警示時、系統會立即傳送通知（除非被另一個靜音所抑制）。如果目前觸發此警示、可能需要幾分鐘的時間才能傳送電子郵件或SNMP通知、以及更新「警示」頁面。

相關資訊

"設定SNMP代理程式"

此參考會列出出現在 Grid Manager 中的預設警示。建議的動作會顯示在您收到的警示訊息中。

您可以視需要建立自訂警示規則、以符合系統管理方法。

某些預設警示"Prometheus指標"會使用。

應用裝置警示

警示名稱	說明
應用裝置電池已過期	應用裝置儲存控制器中的電池已過期。
應用裝置電池故障	應用裝置儲存控制器中的電池故障。
應用裝置電池記憶體容量不足	應用裝置儲存控制器中的電池記憶容量不足。
應用裝置電池即將過期	產品儲存控制器中的電池即將過期。
已取出應用裝置電池	產品儲存控制器中的電池遺失。
應用裝置電池過熱	產品儲存控制器中的電池過熱。
應用裝置BMC通訊錯誤	與基板管理控制器（BMC）的通訊中斷。
偵測到設備開機裝置故障	偵測到裝置中的開機裝置有問題。
應用裝置快取備份裝置故障	持續快取備份裝置故障。
應用裝置快取備份裝置容量不足	快取備份裝置容量不足。
應用裝置快取備份裝置具有寫入保護	快取備份裝置具有寫入保護。
應用裝置快取記憶體大小不相符	應用裝置中的兩個控制器具有不同的快取大小。
應用裝置 CMOS 電池故障	偵測到應用裝置中的 CMOS 電池存在問題。
應用裝置運算控制器機箱溫度過高	在一個應用不支援的應用環境中、StorageGRID 運算控制器的溫度已超過一個標稱臨界值。
應用裝置運算控制器CPU溫度過高	在一個應用程式中、運算控制器中的CPU溫度StorageGRID 已超過正常臨界值。

警示名稱	說明
應用裝置運算控制器需要注意	在應用程式的運算控制器中偵測到硬體故障StorageGRID 。
應用裝置運算控制器電源供應器A發生問題	運算控制器中的電源供應器 A 發生問題。
應用裝置運算控制器電源供應器B發生問題	運算控制器的電源供應器B發生問題。
應用裝置運算硬體監控服務停止	監控儲存硬體狀態的服務已停止。
設備 DAS 磁碟機每天寫入資料的數量超過上限	每天都會將過多的資料寫入磁碟機、這可能會使其保固失效。
偵測到設備 DAS 磁碟機故障	偵測到設備中的直接附加儲存（ DAS ）磁碟機有問題。
設備 DAS 驅動器位於錯誤的插槽或節點	直接連接儲存 (DAS) 磁碟機位於錯誤的插槽或節點
應用裝置 DAS 磁碟機定位器指示燈亮起	應用裝置儲存節點中一或多個直接附加儲存（ DAS ）磁碟機的磁碟機定位指示燈亮起。
設備 DAS 磁碟機重建	直接附加儲存（ DAS ）磁碟機正在重建中。如果最近更換或移除 / 重新插入、則預期會出現此情況。
偵測到應用裝置風扇故障	偵測到產品中的風扇裝置有問題。
偵測到應用裝置光纖通道故障	偵測到應用裝置儲存控制器與運算控制器之間的光纖通道連結問題
應用裝置Fibre Channel HBA連接埠故障	Fibre Channel HBA連接埠故障或故障。
應用裝置快閃快取磁碟機非最佳化	用於SSD快取的磁碟機並非最佳。
已移除應用裝置互連/電池箱	互連/電池箱遺失。
設備LACP連接埠遺失	一個連接埠StorageGRID 位於一個不屬於LACP連結的應用裝置上。
偵測到應用裝置 NIC 故障	偵測到應用裝置中的網路介面卡（ NIC ）問題。
應用裝置整體電源供應器降級	不推薦的操作電壓已偏離了產品的功能StorageGRID 。
需要設備SANtricity OS 軟體更新	SANtricity軟體版本低於此StorageGRID版本的建議最低版本。

警示名稱	說明
偵測到應用裝置 SFP 故障	StorageGRID 應用裝置運算控制器中偵測到 SFP 故障。
應用裝置 SSD 嚴重警告	應用裝置 SSD 回報嚴重警告。
應用裝置儲存控制器A故障	儲存控制器A StorageGRID 在一個應用程式中故障。
應用裝置儲存控制器B故障	無法在應用程式中使用StorageGRID 儲存控制器B。
應用裝置儲存控制器磁碟機故障	一個或多個StorageGRID 驅動器在一個應用程式中故障或不是最佳的。
應用裝置儲存控制器硬體問題	該軟件報告說某個元件「需要注意」在一個應用程式中。SANtricity StorageGRID
應用裝置儲存控制器電源供應器故障	供應器A StorageGRID 的電源供應器已偏離建議的操作電壓。
應用裝置儲存控制器電源供應器B故障	供應器B StorageGRID 的電源供應器已偏離建議的操作電壓。
應用裝置儲存硬體監控服務停止	監控儲存硬體狀態的服務已停止。
應用裝置儲存櫃降級	儲存設備儲存櫃中其中一個元件的狀態會降級。
應用裝置溫度超過上限	產品儲存控制器的名義或最高溫度已超過上限。
已移除應用裝置溫度感測器	已移除溫度感測器。
應用裝置 UEFI 安全開機錯誤	應用裝置尚未安全開機。
磁碟I/O非常緩慢	非常緩慢的磁碟 I/O 可能會影響網格效能。
偵測到儲存設備風扇故障	偵測到產品儲存控制器中的風扇單元有問題。
儲存應用裝置儲存設備連線能力降級	運算控制器與儲存控制器之間的一或多個連線發生問題。
儲存設備無法存取	無法存取儲存設備。

稽核與系統記錄警示

警示名稱	說明
稽核記錄正在新增至記憶體內的佇列	節點無法將記錄傳送至本機syslog伺服器、而且記憶體內的佇列已滿。
外部syslog伺服器轉送錯誤	節點無法將記錄轉送至外部syslog伺服器。
大型稽核佇列	審計訊息的磁碟佇列已滿。如果不解決此問題，S3 操作可能會失敗。
正在將記錄新增至磁碟上佇列	節點無法將記錄轉送至外部syslog伺服器、而且磁碟上的佇列已滿。

貯體警示

警示名稱	說明
FabricPool 貯體具有不受支援的貯體一致性設定	FabricPool 貯體使用不支援的可用或強式站台一致性層級。
FabricPool 貯體具有不受支援的版本設定	FabricPool 貯體已啟用版本設定或 S3 物件鎖定、但不支援。
ListBucket 已停用 Get/Head 物件的權限檢查	ListBucket 對不存在的金鑰執行 GetObject/HeadObject 的權限檢查已停用。

Cassandra 警示

警示名稱	說明
Cassandra自動執行元件錯誤	Cassandra自動執行元件發生錯誤。
Cassandra自動執行元件度量資料已過期	介紹Cassandra自動執行元件的指標已過時。
Cassandra通訊錯誤	執行Cassandra服務的節點無法彼此通訊。
Cassandra相容性過載	Cassandra壓縮程序過載。
Cassandra 超大寫入錯誤	內部 StorageGRID 程序傳送寫入要求給 Cassandra 、要求太大。
Cassandra修復指標已過期	說明Cassandra修復工作的指標已過時。
Cassandra修復進度緩慢	Cassandra資料庫修復的進度緩慢。
Cassandra修復服務無法使用	Cassandra修復服務無法使用。

警示名稱	說明
Cassandra表格毀損	Cassandra偵測到表格毀損。如果Cassandra偵測到表格毀損、就會自動重新啟動。

雲端儲存池警示

警示名稱	說明
雲端儲存資源池連線錯誤	Cloud Storage Pool的健全狀況檢查偵測到一或多個新錯誤。
IAM 角色 Anywhere 終端實體認證到期	IAM 角色 Anywhere 終端實體憑證即將過期。

跨網格複寫警示

警示名稱	說明
跨網格複寫永久失敗	發生跨網格複寫錯誤、需要使用者介入才能解決。
無法使用跨網格複寫資源	由於資源無法使用、因此跨網格複寫要求擱置中。

DHCP 警示

警示名稱	說明
DHCP租用已過期	網路介面上的DHCP租用已過期。
DHCP租約即將到期	網路介面上的DHCP租用即將到期。
DHCP伺服器無法使用	DHCP伺服器無法使用。

偵錯與追蹤警示

警示名稱	說明
偵錯效能影響	啟用偵錯模式時、系統效能可能會受到負面影響。
追蹤組態已啟用	啟用追蹤組態時、系統效能可能會受到負面影響。

電子郵件和 **AutoSupport** 警示

警示名稱	說明
AutoSupport 訊息無法傳送	最近的 AutoSupport 訊息無法傳送。

警示名稱	說明
網域名稱解析失敗	StorageGRID 節點無法解析網域名稱。
電子郵件通知失敗	無法傳送警示的電子郵件通知。
未找到日誌歸檔目標儲存桶	缺少日誌歸檔目標儲存桶，導致日誌無法歸檔到目標儲存桶。
SNMP 通知錯誤	將 SNMP 通知通知傳送至設陷目的地時發生錯誤。
已啟用 SSH 外部存取	SSH 外部存取已啟用超過 24 小時。
偵測到 SSH 或主控台登入	在過去 24 小時內、使用者已使用 Web Console 或 SSH 登入。

銷毀編碼（ **EC** ）警示

警示名稱	說明
Chunk 服務高 goroutine 數量	chunk 服務具有異常高的 goroutine 數量，這可能表示存在死鎖或資源洩漏。
EC重新平衡故障	EC 重新平衡程序失敗或已停止。
EC修復失敗	EC 資料的修復工作已失敗或已停止。
EC修復停止	EC 資料的修復工作已停止。
銷毀編碼片段驗證錯誤	無法再驗證銷毀編碼的片段。毀損的片段可能無法修復。
處於「需要修復」狀態的糾刪碼群組	當沒有正在進行的銷毀編碼資料修理時，一個或多個銷毀編碼群組處於「需要修理」狀態。

憑證警示過期

警示名稱	說明
管理 Proxy CA 憑證過期	管理 Proxy 伺服器 CA 套件中的一或多個憑證即將過期。
用戶端憑證過期	一或多個用戶端憑證即將過期。
S3 的全域伺服器憑證到期	S3 的全球伺服器憑證即將過期。
負載平衡器端點憑證過期	一個或多個負載平衡器端點憑證即將過期。

警示名稱	說明
管理介面的伺服器憑證過期	用於管理介面的伺服器憑證即將過期。
外部syslog CA憑證過期	用於簽署外部syslog伺服器憑證的憑證授權單位（CA）憑證即將過期。
外部syslog用戶端憑證過期	外部syslog伺服器的用戶端憑證即將過期。
外部syslog伺服器憑證過期	外部syslog伺服器提供的伺服器憑證即將過期。

Grid Network 警示

警示名稱	說明
Grid Network MTU不符	網格網路介面（ eth0 ）的 MTU 設定在網格中的各個節點之間有顯著差異。

網格同盟警示

警示名稱	說明
Grid Federation 憑證過期	一或多個網格同盟憑證即將過期。
Grid Federation 連線失敗	本機和遠端網格之間的網格同盟連線無法運作。

高使用率或高延遲警示

警示名稱	說明
中繼資料查詢的高延遲	Cassandra中繼資料查詢的平均時間過長。

身分識別聯盟警示

警示名稱	說明
身分識別聯盟同步失敗	無法同步處理來自身分識別來源的聯盟群組和使用者。
租戶的身分識別聯盟同步處理失敗	無法從租戶設定的身分識別來源同步處理聯盟群組和使用者。

資訊生命週期管理（ **ILM** ）警示

警示名稱	說明
ILM放置無法實現	ILM規則中的放置指示無法針對特定物件執行。

警示名稱	說明
ILM掃描率過低	ILM掃描速率設定為每秒不到100個物件。

金鑰管理伺服器（ **KMS** ）警示

警示名稱	說明
KMS CA憑證過期	用於簽署金鑰管理伺服器（KMS）憑證的憑證授權單位（CA）憑證即將過期。
KMS用戶端憑證過期	金鑰管理伺服器的用戶端憑證即將過期
無法載入kms組態	金鑰管理伺服器的組態存在、但無法載入。
KMS連線錯誤	應用裝置節點無法連線至其站台的金鑰管理伺服器。
找不到kms加密金鑰名稱	設定的金鑰管理伺服器沒有符合所提供名稱的加密金鑰。
KMS加密金鑰旋轉失敗	已成功解密所有應用裝置磁碟區、但一個或多個磁碟區無法旋轉至最新的金鑰。
未設定公里	此站台不存在金鑰管理伺服器。
KMS金鑰無法解密應用裝置磁碟區	裝置上啟用節點加密的一或多個磁碟區無法使用目前的KMS金鑰解密。
KMS伺服器憑證過期	金鑰管理伺服器（KMS）所使用的伺服器憑證即將過期。
KMS 伺服器連線失敗	應用裝置節點無法連線至其站台的金鑰管理伺服器叢集中的一或多個伺服器。

負載平衡器警示

警示名稱	說明
提高零要求負載平衡器連線	在未執行要求的情況下、中斷連線至負載平衡器端點的連線百分比提高。

本機時鐘偏移警示

警示名稱	說明
本機時鐘大時間偏移	本機時鐘與網路時間傳輸協定（ NTP ）時間之間的偏移量太大。

記憶體不足或空間不足警示

警示名稱	說明
稽核記錄磁碟容量過低	審計日誌的可用空間不足。如果不解決此問題，S3 操作可能會失敗。
可用節點記憶體不足	節點上可用的RAM量很低。
儲存資源池可用空間不足	儲存節點中可用於儲存物件資料的空間不足。
安裝的節點記憶體不足	節點上安裝的記憶體容量過低。
低中繼資料儲存	用於儲存物件中繼資料的空間不足。
低度量磁碟容量	度量資料庫可用空間不足。
低物件資料儲存	用於儲存物件資料的空間不足。
低唯讀浮水印會置換	儲存 Volume 軟式唯讀浮水印覆寫低於儲存節點最佳化的最低浮水印。
低根磁碟容量	根磁碟上的可用空間不足。
低系統資料容量	/var/local 的可用空間不足。如果不解決此問題，S3 操作可能會失敗。
低溫度目錄可用空間	/tmp目錄中的可用空間不足。

節點或節點網路警示

警示名稱	說明
ADC 法定人數未達	具有 ADC 服務的儲存節點處於離線狀態。在 ADC 仲裁恢復之前，擴展和退役操作將被阻止。
管理網路接收使用量	管理網路上的接收使用率很高。
管理網路傳輸使用量	管理網路上的傳輸使用率很高。
防火牆組態失敗	無法套用防火牆組態。
以後援模式管理介面端點	所有管理介面端點都已回復為預設連接埠太久。
節點網路連線錯誤	在節點之間傳輸資料時發生錯誤。
節點網路接收框架錯誤	節點接收到的網路框架有很大比例發生錯誤。

警示名稱	說明
節點未與NTP伺服器同步	節點未與網路時間傳輸協定（ NTP ）伺服器同步。
節點未被NTP伺服器鎖定	節點未鎖定至網路時間傳輸協定（NTP）伺服器。
非應用裝置節點網路中斷	一或多個網路裝置當機或中斷連線。
管理網路上的服務應用裝置連結中斷	管理網路（ eth1 ）的應用裝置介面已關閉或中斷連線。
管理網路連接埠1上的服務應用裝置連結中斷	應用裝置上的管理網路連接埠1已關閉或中斷連線。
客戶端網路上的服務應用裝置連結中斷	用戶端網路（ eth2 ）的應用裝置介面已關閉或中斷連線。
服務應用裝置在網路連接埠 1 上連結中斷	裝置上的網路連接埠 1 已關閉或中斷連線。
服務應用裝置在網路連接埠 2 上連結中斷	裝置上的網路連接埠 2 已關閉或中斷連線。
服務應用裝置在網路連接埠 3 上連結中斷	裝置上的網路連接埠 3 已關閉或中斷連線。
服務應用裝置在網路連接埠 4 上連結中斷	裝置上的網路連接埠 4 已關閉或中斷連線。
管理網路上的儲存設備連結中斷	管理網路（ eth1 ）的應用裝置介面已關閉或中斷連線。
儲存應用裝置連結至管理網路連接埠1	應用裝置上的管理網路連接埠1已關閉或中斷連線。
儲存設備在用戶端網路上連結中斷	用戶端網路（ eth2 ）的應用裝置介面已關閉或中斷連線。
儲存設備在網路連接埠 1 上向下連結	裝置上的網路連接埠 1 已關閉或中斷連線。
儲存設備在網路連接埠 2 上向下連結	裝置上的網路連接埠 2 已關閉或中斷連線。
儲存設備在網路連接埠 3 上向下連結	裝置上的網路連接埠 3 已關閉或中斷連線。

警示名稱	說明
儲存設備在網路連接埠 4 上向下連結	裝置上的網路連接埠 4 已關閉或中斷連線。
儲存節點未處於所需的儲存狀態	儲存節點上的 LDR 服務因為內部錯誤或與磁碟區相關的問題而無法轉換至所需的狀態
TCP 連線使用量	此節點上的 TCP 連線數量接近可追蹤的最大數量。
無法與節點通訊	一個或多個服務沒有回應、或無法連線至節點。
非預期的節點重新開機	節點在過去24小時內意外重新開機。

物件警示

警示名稱	說明
物件存在檢查失敗	物件存在檢查工作失敗。
物件存在檢查停止	物件存在檢查工作已停止。
可能遺失的物品	網格中可能會遺失一個或多個物件。
偵測到孤立對象	已偵測到孤立物件。
S3 多部分上傳部分大小過大	用戶端正在嘗試執行多部分上傳操作，但該操作超過了各部分的大小限制。
S3 將物件大小放得太大	用戶端嘗試的「放置物件」作業超過 S3 大小限制。
使用不支援的條件標頭的 S3 請求	S3 用戶端在對某些操作使用不受支援的條件標頭（If-Match 或 If-None-Match）。
啟用全域命名空間後，S3 請求使用了錯誤的區域	S3 用戶端使用了錯誤的簽章區域來存取此網格的儲存桶。
偵測到不明毀損的物件	在複寫的物件儲存設備中找到無法識別為複寫物件的檔案。

物件損壞警報

警示名稱	說明
物件尺寸不匹配	在物件存在性檢查過程中偵測到意外的物件大小。

平台服務警示

警示名稱	說明
平台服務擱置要求容量不足	平台服務擱置要求的數量即將接近容量。
平台服務無法使用	有太少的儲存節點與站台上正在執行或可用的RSM服務。

儲存磁碟區警示

警示名稱	說明
儲存磁碟區需要注意	儲存磁碟區離線、需要注意。
儲存磁碟區需要還原	儲存磁碟區已恢復、需要還原。
儲存磁碟區離線	儲存磁碟區已離線超過 5 分鐘。
已嘗試重新掛載儲存磁碟區	儲存磁碟區已離線並觸發自動重新掛載。這可能表示磁碟機問題或檔案系統錯誤。
Volume 還原無法開始複寫資料修復	無法自動啟動已修復磁碟區的複寫資料修復。

StorageGRID 服務警示

警示名稱	說明
使用備份組態的 Nginx 服務	Nginx 服務的組態無效。現在正在使用先前的組態。
使用備份組態的 Nginx) 服務	Nginx) 服務的組態無效。現在正在使用先前的組態。
需要重新開機才能停用 FIPS	安全性原則不需要 FIPS 模式，但正在使用 FIPS 模組。
需要重新開機才能啟用 FIPS	安全性原則需要 FIPS 模式，但未使用 FIPS 模組。
使用備份組態的 SSH 服務	SSH 服務的組態無效。現在正在使用先前的組態。

租戶警示

警示名稱	說明
租戶配額使用量高	使用的配額空間百分比很高。此規則預設為停用、因為它可能導致通知太多。

StorageGRID 中常用的 Prometheus 指標

請參閱這份常用的 Prometheus 指標清單、以更深入瞭解預設警示規則中的條件、或建構自訂警示規則的條件。

您也可以取得所有指標的完整清單。

有關 Prometheus 查詢語法的詳細資訊，請參閱 "查詢基礎知識"。

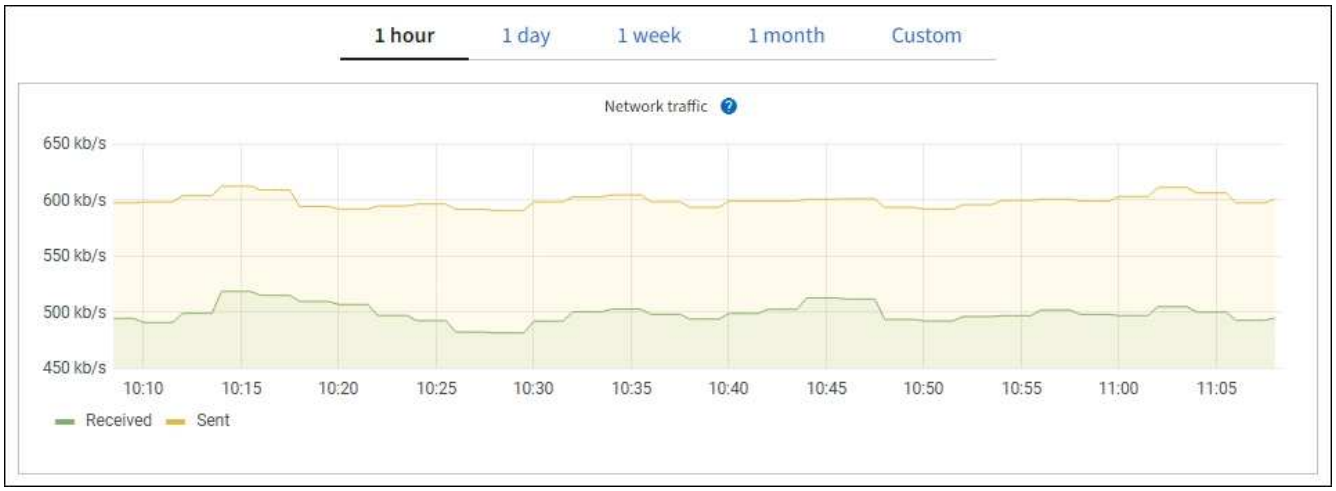
什麼是 Prometheus 指標？

Prometheus 指標是時間系列測量。管理節點上的 Prometheus 服務會從所有節點上的服務收集這些度量。度量會儲存在每個管理節點上、直到保留給Prometheus資料的空間已滿為止。當 `/var/local/mysql_ibdata/`磁碟區達到容量時、會先刪除最舊的度量。

Prometheus 指標在哪裡使用？

Prometheus 所收集的指標會在 Grid Manager 的多個位置使用：

- 節點頁面：節點頁面上可用索引標籤上的圖表使用Grafana視覺化工具來顯示Prometheus所收集的時間序列指標。Grafana以圖表和圖表格式顯示時間序列資料、而Prometheus則是後端資料來源。



- 警示：當使用Prometheus度量的警示規則條件評估為真時、警示會在特定嚴重性層級觸發。
- * Grid Management API*：您可以在自訂警示規則中使用Prometheus指標、或搭配外部自動化工具來監控StorageGRID 您的VMware系統。您可從Grid Management API取得Prometheus指標的完整清單。（從 Grid Manager 頂端選取說明圖示、然後選取 * API 說明文件 * > * 規格 * 。）雖然有超過一千種指標可供使用、但監控最關鍵StorageGRID 的功能只需要相對較少的數量。

> 名稱中包含_Private的指標僅供內部使用、StorageGRID 可能會在不另行通知的情況下於各個版本之間變更。

- 支援 > 工具 > 診斷*頁面和*支援 > 工具 > *指標*頁面：這些頁面主要供技術支援使用，提供了使用 Prometheus 指標值的多種工具和圖表。

> 「指標」頁面中的某些功能和功能表項目會刻意無法運作、而且可能會有所變更。

下列清單包含最常用的 Prometheus 指標。

> 名稱中包含 _private 的計量僅供內部使用、且可能會在 StorageGRID 版本之間變更、恕不另行通知。

alertmanager_notifications失敗總計

失敗警示通知的總數。

node_filesystem_可用 字節

非 root 使用者可用的檔案系統空間量（位元組）。

node_memory_MemAvailable_bytes

記憶體資訊欄位Mem可用 位元組。

node_network_carrier_

的載體值 `/sys/class/net/iface`。

node_network_receip_errs_total

網路裝置統計 `receive_errs`資料。

node_network_Transmim_errs_total

網路裝置統計 `transmit_errs`資料。

storagegRid_管理 性關機

由於預期原因、節點未連線至網格。例如、節點或節點上的服務已正常關機、節點正在重新開機、或軟體正在升級。

storagegRid_applie_compute控制器硬體狀態

應用裝置中的運算控制器硬體狀態。

storagegRid_applie_fred_disks

對於應用裝置中的儲存控制器而言、磁碟機數量並不理想。

儲存格**RID_applie_storage_控制 器硬體狀態**

設備中儲存控制器硬體的整體狀態。

storagegRid_content_bucks_and容器

此儲存節點已知的 S3 儲存桶總數。

storagegRid_content_objects

此儲存節點已知的 S3 資料物件總數。計數僅對透過 S3 與系統互動的客戶端應用程式所建立的資料物件有效。

storagegRid_content_objects_lost

此服務偵測到StorageGRID 的物件總數在整個系統中遺失。應採取行動來判斷損失原因、以及是否有可能恢復。

"疑難排解遺失和遺失的物件資料"

storagegRid_http工作階段傳入嘗試

嘗試存取儲存節點的HTTP工作階段總數。

storagegRid_http工作階段傳入的**_current_Estimated**

儲存節點上目前作用中（開啟）的HTTP工作階段數目。

storagegRid_htt_sessions_incoming_f失敗

由於HTTP要求格式錯誤或處理作業失敗而無法成功完成的HTTP工作階段總數。

storagegRid_htt_sesss_incoming_Successful

已成功完成的HTTP工作階段總數。

儲存格**RID_ILM_waiting**背景物件

此節點上等待掃描進行ILM評估的物件總數。

儲存格**RID_ILM_waiting**用戶端評估物件數**_per**秒

根據此節點上的ILM原則評估物件的目前速度。

儲存格**RID_ILM_waiting**用戶端物件

此節點上等待用戶端作業（例如擷取）ILM評估的物件總數。

storagegRid_lm_waiding_total_objects

等待ILM評估的物件總數。

儲存格**RID_ILM_SCAN_objects_per**秒

此節點擁有的物件掃描並佇列ILM的速度。

儲存格**RID_ILM**掃描_期間_預估_分鐘

完成此節點上完整ILM掃描的預估時間。

*附註：*完整掃描並不保證ILM已套用至此節點擁有的所有物件。

storagegRid_load_平衡 器端點**_cert**過期時間

負載平衡器端點憑證的到期時間、從上一時期開始算起的秒數。

storagegRid_meta數據查詢**_average_dimetime_m**毫秒

透過此服務針對中繼資料儲存區執行查詢所需的平均時間。

storagegRid_network_receiped_bytes

自安裝以來接收的資料總量。

storagegrid網路傳輸的位元組

安裝後傳送的資料總量。

儲存格**RID_node_cpo_utilation_Percentage**

此服務目前使用的可用CPU時間百分比。指出服務的忙碌程度。可用的CPU時間量取決於伺服器的CPU數量。

儲存格**RID_NTP_chosed_time_source_offset_**毫秒

系統化地抵銷所選時間來源所提供的時間。當到達時間來源的延遲與時間來源到達NTP用戶端所需的時間不一致時、便會採用偏移。

儲存格**RID_NTP_Locked**

節點未鎖定至網路時間傳輸協定（ NTP ）伺服器。

storagegrid_s3_data_transfers_bytes_ingested

自上次重設屬性以來、從S3用戶端擷取至此儲存節點的資料總量。

storagegrid_s3_data_transfers_bytes_retrieved

自上次重設屬性以來、S3用戶端從此儲存節點擷取的資料總量。

storagegrid_s3_operations_failed

S3作業失敗的總數（HTTP狀態代碼4xx和5xx）、不包括由S3授權失敗所造成的作業。

storagegrid_s3_operations_successful

成功S3作業的總數（HTTP狀態代碼2xx）。

storagegrid_s3_operations_unauthorized

因授權失敗而失敗的S3作業總數。

storagegRid_servercert_management介面**_cert_expire_days**

管理介面憑證過期的天數。

storagegRid_servercert_storage_API_Enders_cert_expiry_days

物件儲存API憑證過期的天數。

storagegRid_service_cpo_seconds

自安裝以來、此服務已使用CPU的累計時間量。

storagegRid_service_memory_usage_bytes

此服務目前使用的記憶體容量（RAM）。此值與Linux Top公用程式顯示的RES.

storagegRid_service_network_receiped_bytes

自安裝以來、此服務所接收的資料總量。

storagegRid_service_network_forted_bytes

此服務傳送的資料總量。

storagegRid_service_restarts

服務重新啟動的總次數。

storagegrid_service_rid_seconds

安裝後服務執行的總時間。

storagegRid_service_upde_seconds

自上次重新啟動服務以來、服務一直在執行的總時間。

storagegRid_storage_ista_current

儲存服務的目前狀態。屬性值包括：

- 10 =離線
- 15 =維護
- 20 =唯讀
- 30 =線上

storagegRid_storage_STATUS

儲存服務的目前狀態。屬性值包括：

- 0 =無錯誤
- 10 =轉換中
- 20 =可用空間不足
- 30 = Volume不可用
- 40 =錯誤

storagegRid_storage_utilization_data_bytes

儲存節點上複寫和刪除編碼物件資料的總大小估計值。

storagegRid_storage_utilation_maddenta_allowed_bytes

每個儲存節點的Volume 0上允許用於物件中繼資料的總空間。此值一律低於節點上為中繼資料保留的實際空間、因為必要的資料庫作業（例如壓縮和修復）以及未來的硬體和軟體升級需要一部分保留空間。物件中繼資料所允許的空間可控制整體物件容量。

storagegRid_storage_utilation_madda_bytes

儲存Volume 0上的物件中繼資料量、以位元組為單位。

storagegRid_storage_utilation_total_space_bytes

分配給所有物件存放區的儲存空間總量。

storagegRid_storage_utilation_可用 空間位元組

物件儲存空間的總剩餘量。計算方法是將儲存節點上所有物件存放區的可用空間量一併新增。

storagegRid_enture_usage_data_bytes

租戶所有物件的邏輯大小。

storagegRid_enture_usage_object_count

租戶的物件數目。

storagegRid_enture_usage_quota位元組

租戶物件可用的最大邏輯空間量。如果未提供配額度量、則可用空間不限。

取得所有指標清單

[[Obele-all-argems] 若要取得完整的計量清單、請使用 Grid Management API 。

步驟

1. 從 Grid Manager 頂端選取說明圖示、然後選取 * API 文件 * 。
2. 找出*指標*作業。
3. 執行 `GET /grid/metric-names`作業。
4. 下載結果。

記錄檔參考

StorageGRID 日誌檔案

提供記錄、可用來擷取事件、診斷訊息和錯誤狀況。StorageGRID系統可能會要求您收集記錄檔、並將其轉送至技術支援部門、以協助進行疑難排解。

記錄的分類如下：

- "軟體記錄StorageGRID"
- "部署與維護記錄"
- "關於bycast.log"

> 每種記錄類型的詳細資料僅供參考。這些記錄可由技術支援人員進行進階疑難排解。使用稽核記錄和應用程式記錄檔來重新建構問題歷程記錄的進階技術、已超出本指示的範圍。

存取記錄

要存取日誌，您可以"收集記錄檔和系統資料"來自一個或多個節點作為單一日誌檔案存檔。或者，您可以如下存取每個網格節點的單獨日誌檔案：

步驟

1. 輸入下列命令： `ssh admin@grid_node_IP`
2. 輸入檔案中列出的密碼 `Passwords.txt`。
3. 輸入以下命令切換到 root ： `su -`
4. 輸入檔案中列出的密碼 `Passwords.txt`。

將記錄匯出至 **Syslog** 伺服器

將記錄匯出至 Syslog 伺服器可提供下列功能：

- 除了 S3 請求之外，還接收所有網格管理器和租用戶管理器請求的清單。
- 更清楚地瞭解傳回錯誤的 S3 要求、而不會受到稽核記錄方法所造成的效能影響。
- 存取容易剖析的 HTTP 層要求和錯誤代碼。
- 對於負載平衡器上的流量分類器所封鎖的要求、可提供更好的可見度。

若要匯出日誌，請參閱"設定日誌管理和外部系統日誌伺服器"。

包含針對每個類別所描述的記錄檔、以及包含度量和偵錯命令輸出的其他檔案。StorageGRID

歸檔位置	說明
acct-tunnel.log	與負載平衡器搭配使用的帳戶通道協助程式記錄。
稽核	稽核在正常系統作業期間所產生的訊息。
基礎作業系統記錄	基本作業系統資訊、包括StorageGRID 不含影像版本的資訊。
套裝組合	全域組態資訊（套裝組合）。
快取服務	快取服務日誌（僅在網關節點上）。
Cassandra	Cassandra資料庫資訊和Reaper修復記錄。
EC	VCSs 有關目前節點和 EC 群組資訊的資訊（依設定檔 ID ）。
網格	一般網格記錄(`bycast.log`、包括除錯）和 `servermanager`記錄。
GRB.json	所有節點共用的網格組態檔。此外、 `node.json`也專屬於目前節點。
還價	高可用度群組指標與記錄。
安裝	`Gdu-server`並安裝記錄檔。
internal-access.log	內部 HTTP Proxy 流量記錄。
Lambda-仲裁 人	與S3 Select Proxy要求相關的記錄。
洩漏	來自 leakd 服務的日誌。
lumberjack.log	偵錯與記錄收集相關的訊息。
manage-audit.log	`mgmt-api`存取稽核日誌。
指標	Grafana、Jaeger、節點輸出程式和Prometheus的服務記錄。
誤用	Miscd存取與錯誤記錄。
MySQL	MariaDB資料庫組態及相關記錄。

歸檔位置	說明
網路	由網路相關指令碼和Dynip服務所產生的記錄。
恩靈思	負載平衡器和網格同盟組態檔案和記錄。也包括Grid Manager和Tenant Manager流量記錄。
恩靈思- GW	• `access.log`： Grid Manager 和 Tenant Manager 會要求記錄訊息。 ◦ 使用 Syslog 匯出時、這些訊息會以前置 `mgmt:`方式顯示。 ◦ 這些記錄訊息的格式為 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`：傳入的跨網格複寫要求。 ◦ 使用 Syslog 匯出時、這些訊息會以前置 `cgr:`方式顯示。 ◦ 這些記錄訊息的格式為 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`：S3 請求負載平衡器端點。 ◦ 使用 Syslog 匯出時、這些訊息會以前置 `endpoint:`方式顯示。 ◦ 這些記錄訊息的格式為 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`：與新的 DNS 檢查警示有關。 • stream-access.log：流區塊的 TCP/TLS 流（第 4 階層）Proxy 工作階段。 注意：這不是 HTTP 請求日誌。
NTP	NTP組態檔案和記錄。
孤立物件	與孤立物件相關的記錄。
作業系統	節點和網格狀態文件，包括服務 `pid`。
其他	其他資料夾中未收集的記錄檔 `/var/local/log`。
效能	CPU、網路和磁碟I/O的效能資訊
Prometheus-data	目前的Prometheus指標（如果記錄收集包含Prometheus資料）。
資源配置	與網格資源配置程序相關的記錄。

歸檔位置	說明
漂流	平台服務所用的來自於raft叢集的記錄。
revision_history.json	修訂歷史。
routed-s3-access.log.gz	存取日誌用於記錄透過 S3（全域命名空間/聯盟 URL）路由的網格聯盟流量。
SSH	與 SSH 組態和服務相關的記錄。
SNMP	用於傳送 SNMP 通知的 SNMP 代理程式組態。
套接字資料	用於網路偵錯的通訊端資料。
system-bucket.log	`update-system-bucket-configuration.log`：系統儲存桶日誌。
system-commands.txt	輸出示例容器命令。StorageGRID包含系統資訊、例如網路和磁碟使用量。
Synchrone-recovery 套件	與維護託管 ADC 服務的所有管理節點和儲存節點上最新恢復包的一致性有關。
update-cipher-configurations.log	`update-cors-configurations.log`：追蹤與 TLS/密碼和 CORS 變更相關的記錄。
update-leakd-configurations.log	孤立偵測組態記錄。

軟體記錄**StorageGRID**

您可以使用StorageGRID 資訊檔來疑難排解問題。

如果您想要將日誌傳送到外部系統日誌伺服器或變更稽核資訊的目的地，例如 `bycast.log`和 `nms.log`，看"設定日誌管理"。

一般**StorageGRID** 資訊記錄

檔案名稱	附註	找到
/var/local/log/bycast.log	主要的StorageGRID故障排除檔。	所有節點
/var/local/log/bycast-err.log	包含一個子集 `bycast.log`（嚴重性為 ERROR 和 CRITICAL 的訊息）。系統中也會顯示嚴重訊息。	所有節點

檔案名稱	附註	找到
/var/local/core	包含在程式異常終止時所建立的任何核心傾印檔案。可能的原因包括聲明失敗、違規或執行緒逾時。 • 附註 * ：檔案 ``/var/local/core/kexec_cmd`通常存在於應用裝置節點上、並不表示發生錯誤。	所有節點

密碼相關記錄

檔案名稱	附註	找到
/var/local/log/ssh-config-generation.log	包含與產生 SSH 組態和重新載入 SSH 服務相關的記錄。	所有節點
/var/local/log/Ngins/config-generation.log	包含與產生 Nginx 組態及重新載入 Nginx 服務相關的記錄。	所有節點
/var/local/log/Nginx) config-generation.log	包含與產生 Nginx) 組態（以及重新載入 Nginx) 相關的記錄檔。	管理和閘道節點
/var/local/log/update-cipher-configurations.log	包含與設定 TLS 和 SSH 原則相關的記錄。	所有節點

網格同盟記錄

檔案名稱	附註	找到
/var/local/log/update_grid_federation_config.log	包含與產生網格同盟連線的 Nginx 和 Nginx) 組態相關的記錄。	所有節點

NMS記錄

檔案名稱	附註	找到
/var/local/log/nms.log	• 從Grid Manager和Tenant Manager擷取通知。 • 擷取與 NMS 服務運作相關的事件。例如、電子郵件通知和組態變更。 • 包含因系統中所做的組態變更而產生的XML套裝組合更新。 • 包含一天執行一次屬性降級取樣的相關錯誤訊息。 • 包含Java Web伺服器錯誤訊息、例如頁面產生錯誤和HTTP狀態500錯誤。 • 包含與 AutoSupport 相關的日誌。	管理節點
/var/local/log/nms.errlog	包含與MySQL資料庫升級相關的錯誤訊息。 包含對應服務的標準錯誤（stderr）串流。每個服務有一個記錄檔。除非服務有問題、否則這些檔案通常是空的。	管理節點
/var/local/log/nms.requestlog	包含有關從管理API傳出連線至內部StorageGRID 支援服務的資訊。	管理節點

伺服器管理員記錄

檔案名稱	附註	找到
/var/local/log/servermanager.log	伺服器管理程式應用程式的記錄檔。	所有節點
/var/local/log/GridstatBackend.errlog	伺服器管理員GUI後端應用程式的記錄檔。	所有節點
/var/local/log/gratstat.errlog	伺服器管理員GUI的記錄檔。	所有節點

StorageGRID 服務記錄

檔案名稱	附註	找到
/var/local/log/acct.errlog		執行ADC服務的儲存節點
/var/local/log/ADC.errlog	包含對應服務的標準錯誤（stderr）串流。每個服務有一個記錄檔。除非服務有問題、否則這些檔案通常是空的。	執行ADC服務的儲存節點

檔案名稱	附註	找到
/var/local/log/AMS		管理節點
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	快取服務日誌。	閘道節點
/var/local/log/cassandra / system.log	當新增儲存節點時發生問題、或當節點修復工作停止時、可使用的中繼資料存放區（Cassandra資料庫）資訊。	儲存節點
/var/local/log/cassandra-reaper.log	Cassandra Reaper服務的相關資訊、可用來修復Cassandra資料庫中的資料。	儲存節點
/var/local/log/cassandra － reaper.errlog	Cassandra Reaper服務的錯誤資訊。	儲存節點
/var/local/log/cchk.errlog		儲存節點
/var/local/log/CMN.errlog		管理節點
/var/local/log/cms.errlog	此記錄檔可能存在於已從StorageGRID舊版的更新版本的系統上。其中包含舊有資訊。	儲存節點
/var/local/log/Ds.errlog		儲存節點
/var/local/log/DMV.errlog		儲存節點
/var/local/log/Dynip*	包含與dynip服務相關的記錄、該服務會監控網格是否有動態IP變更及更新本機組態。	所有節點
/var/local/log/grafana.log	與Grafana服務相關的記錄、用於Grid Manager中的度量視覺化。	管理節點
/var/local/log/hagroups.log	與高可用度群組相關的記錄。	管理節點和閘道節點
/var/local/log/hagroups_events.log	追蹤狀態變更、例如從備份轉換為主要或故障。	管理節點和閘道節點
/var/local/log/idnt.errlog		執行ADC服務的儲存節點
/var/local/log/jaeger.log	與用於追蹤收集的jaeger服務相關聯的記錄。	所有節點

檔案名稱	附註	找到
/var/local/log/kstn.errlog		執行ADC服務的儲存節點
/var/local/log/lambda*	包含S3 Select服務的記錄。	管理和閘道節點 只有特定的管理節點和閘道節點包含此記錄。請參閱"S3選取管理和閘道節點的需求和限制"。
/var/local/log/LDR.errlog		儲存節點
/var/local/log/miscd/*.log	包含MISCd服務（Information Service Control Daemon）的記錄、此服務提供介面、可用於查詢及管理其他節點上的服務、以及管理節點上的環境組態、例如查詢其他節點上執行的服務狀態。	所有節點
/var/local/log/Ngins/*.log	包含用於Nginx服務的記錄、可做為各種網格服務（例如Prometheus和Dynip）的驗證與安全通訊機制、以便透過HTTPS API與其他節點上的服務進行交談。	所有節點
/var/local/log/Nginx)	包含與 Nginx) -GW 服務相關的一般記錄、包括錯誤記錄、以及管理節點上受限管理連接埠的記錄。	管理節點和閘道節點
/var/local/log/Nginx) cgr-access.log.gz	包含與跨網格複寫流量相關的存取記錄。	管理節點、閘道節點、或兩者、以網格同盟組態為基礎。只能在目標網格上找到用於跨網格複寫的資料。
/var/local/log/Nginx) endpoint-access.log.gz	包含負載平衡器服務的存取記錄、可提供從用戶端到儲存節點的 S3 流量負載平衡。	管理節點和閘道節點
/var/local/log/persistent*	包含「持續性」服務的記錄、此服務會管理根磁碟上需要在重新開機後持續存在的檔案。	所有節點
/var/local/log/prometheus.log	針對所有節點、包含節點資料輸出器服務記錄和AD-Exporter度量服務記錄。 對於管理節點、也包含Prometheus和Alert Manager服務的記錄。	所有節點

檔案名稱	附註	找到
/var/local/log/raft.log	包含RSM服務 用於raft傳輸協定的程式庫輸出。	儲存節點搭配RSM服務
/var/local/log/rms.errlog	包含用於S3平台服務的複寫狀態機器服務（RSM）服務記錄。	儲存節點搭配RSM服務
/var/local/log/sm.errlog		所有節點
/var/local/log/update-s3vs-domains.log	包含處理S3虛擬託管網域名稱組態更新的相關記錄。請參閱實作S3用戶端應用程式的指示。	管理和閘道節點
/var/local/log/update-snmp-firewall.*	包含與SNMP管理的防火牆連接埠相關的記錄。	所有節點
/var/local/log/update-sysl.log	包含與系統syslog組態變更相關的記錄。	所有節點
/var/local/log/update-traffic-classes.log	包含與流量分類器組態變更相關的記錄。	管理和閘道節點
/var/local/log/update-utcn.log	包含與此節點上不受信任的用戶端網路模式相關的記錄。	所有節點

相關資訊

- "關於bycast.log"
- "使用S3 REST API"

StorageGRID 中的部署和維護日誌

您可以使用部署和維護記錄來疑難排解問題。

檔案名稱	附註	找到
/var/local/log/install.log	在軟體安裝期間建立。包含安裝事件的記錄。	所有節點
/var/local/log/expansion-progress.log	在擴充作業期間建立。包含擴充事件的記錄。	儲存節點
/var/local/log/pa-move.log	執行指令碼時建立 `pa-move.sh`。	主要管理節點
/var/local/log/pa-move-new_pa.log	執行指令碼時建立 `pa-move.sh`。	主要管理節點

檔案名稱	附註	找到
/var/local/log/pa-move-old_pa.log	執行指令碼時建立 `pa-move.sh`。	主要管理節點
/var/local/log/gdu-server.log	由GDU服務建立。包含與主管理節點管理的資源配置和維護程序相關的事件。	管理節點
/var/local/log/send_admin_hw.log	安裝期間建立。包含與節點與主要管理節點通訊相關的偵錯資訊。	所有節點
/var/local/log/upgrade.log	在軟體升級期間建立。包含軟體更新事件的記錄。	所有節點

了解 **StorageGRID bycast.log**

檔案 `/var/local/log/bycast.log`是 StorageGRID 軟體的主要疑難排解檔案。每個網格節點都有一個 `bycast.log`檔案。檔案包含該網格節點的特定訊息。

檔案 `/var/local/log/bycast-err.log`是的子集 `bycast.log`。其中包含嚴重性錯誤和嚴重的訊息。

或者，您可以變更稽核日誌的目標並將稽核資訊傳送至外部系統日誌伺服器。當設定外部系統日誌伺服器時，將繼續產生和儲存稽核記錄的本機日誌。看"設定日誌管理和外部系統日誌伺服器" 。

bycast.log的檔案旋轉

當檔案達到 1 GB 時 `bycast.log`、會儲存現有檔案、並啟動新的記錄檔。

保存的文件將被重命名，新文件將被 `bycast.log.1`命名爲 `bycast.log`。當新的容量達到 1 GB `bycast.log.1` 時， `bycast.log`會重新命名並壓縮成 `bycast.log.2.gz`，並 `bycast.log`重新命名 `bycast.log.1`。

的旋轉限制 `bycast.log`為 21 個檔案。建立第 22 版 `bycast.log`檔案時、會刪除最舊的檔案。

的旋轉限制 `bycast-err.log`為七個檔案。

> 如果記錄檔已壓縮、則不得將其解壓縮至寫入的相同位置。將檔案解壓縮到相同位置可能會干擾記錄檔的旋轉指令碼。

或者，您可以變更稽核日誌的目標並將稽核資訊傳送至外部系統日誌伺服器。當設定外部系統日誌伺服器時，將繼續產生和儲存稽核記錄的本機日誌。看"設定日誌管理和外部系統日誌伺服器" 。

相關資訊

"收集記錄檔和系統資料"

bycast.log中的訊息

中的訊息 `bycast.log`是由 ADE （非同步分散式環境）所寫入。ade是每個網格節點服務所使用的執行時間環境。

ADE訊息範例：

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ade訊息包含下列資訊：

訊息區段	範例中的值
節點 ID	12455685
ade程序ID	0357819531
模組名稱	SVMR
訊息識別碼	EVHR
UTC系統時間	2019 年 5 月 5 日 T27T17 ： 10 ： 29.784677 （ YYYY-MM-DDTHH ： MM ： SS.uuuuuu ）
嚴重性等級	錯誤
內部追蹤編號	0906
訊息	SVMR：磁碟區3的健全狀況檢查失敗、原因為「tout」

bycast.log中的訊息嚴重性

中的訊息 `bycast.log`會指派嚴重性等級。

例如：

- 通知：應記錄的事件已發生。大多數記錄訊息都屬於此層級。
- 警告：發生非預期的情況。
- 錯誤：發生重大錯誤、會影響作業。
- 臨界：發生異常狀況、停止正常作業。您應該立即解決基本條件。

中的錯誤代碼 `bycast.log`

中的大多數錯誤訊息都 `bycast.log`包含錯誤代碼。

下表列出中常見的非數字代碼 `bycast.log`。非數字代碼的確切含義取決於報告它的環境。

錯誤代碼	意義
SUCS	無錯誤
GERR	不明
取消	已取消
ABRT	已中止
宣傳	逾時
INVI	無效
NFND	找不到
版本	版本
會議	組態
失敗	失敗
ICPL	不完整
完成	完成
SUN駒 方案	服務無法使用

下表列出中的數值錯誤代碼 `bycast.log`。

錯誤編號	錯誤代碼	意義
001	EPERM	不允許操作
002	ENOENT	無此類檔案或目錄
003	ESRCH	沒有這種程序
004	EINTR	系統通話中斷
005	EIO	I/O錯誤
006	ENXIO	無此類裝置或位址

錯誤編號	錯誤代碼	意義
007	E2BIG	引數清單太長
008	ENOEXEC	執行格式錯誤
009	EBADF	錯誤的檔案編號
010	ECHILD	無子程序
011	EAGAIN	請再試一次
012	ENOMEM	記憶體不足
013	EACCES	權限遭拒
014	預設	地址錯誤
015	ENOTBK	需要區塊裝置
016	EBUSY	裝置或資源忙碌中
017	EEXIST	檔案存在
018	EXDEV	跨裝置連結
019	ENODEV	無此類裝置
020	ENOTDIR	不是目錄
021	EISDIR	是目錄
022	EINVAL	無效的引數
023	ENFILE	檔案表溢位
024	EMFILE	開啟的檔案太多
025	ENOTY	不是打字機
026	ETXTBSY	文字檔忙碌中
027	EFBIG	檔案太大

錯誤編號	錯誤代碼	意義
028	ENOSPC	裝置上沒有剩餘空間
029	EIPE	非法搜尋
030	EROFS	唯讀檔案系統
031	EMLINK	連結過多
032	EPIPE	管路毀損
033	益登	數學引數超出func網域
034	ERANGE	無法呈現數學結果
035	EDEADLK	將會發生資源死鎖
036	ENAMETOOLON	檔案名稱太長
037	ENOLCK	沒有可用的記錄鎖定
038	ENOSYS	功能未實作
039	ENOTEMPTY	目錄不是空的
040	ELOOP	遇到過多符號連結
041		
042	ENOMSG	無所需類型的訊息
043	EIDRM	已移除識別碼
044	ECHRNG	通道號碼超出範圍
045	EL2NSYNC	第2級未同步
046	EL3HLT	層級 3 停止
047	EL3RST	第3級重設
048	ELNRNG	連結號碼超出範圍

錯誤編號	錯誤代碼	意義
049	EUNATCH	未附加傳輸協定驅動程式
050	ENOCI	無可用的csi架構
051	EL2HLT	層級 2 停止
052	EBADE	無效的交換
053	EBADR	無效的要求描述元
054	非常棒	Exchange已滿
055	ENOANO	無陽極
056	EBADRQc	申請代碼無效
057	EBADSLT-	無效插槽
058		
059	EBFONT	字型檔案格式錯誤
060	ENOSTR	裝置不是串流
061	ENODATA	無可用資料
062	電子時間	定時器已過期
063	ENOSR	資料流不足資源
064	ENONET	機器不在網路上
065	ENOPKG	未安裝套件
066	EREMOTE	物件是遠端的
067	ENOLINK	連結已中斷
068	EADV	通告錯誤
069	ESRMNT	Srsmount錯誤

錯誤編號	錯誤代碼	意義
070	EComm	傳送時發生通訊錯誤
071	EPROTO	傳輸協定錯誤
072	EMULOTIHOP	已嘗試多跳
073	EDOTDOT	RFS特定錯誤
074	EBADMSG	不是資料訊息
075	EOVERFLOW	對於已定義的資料類型、值太大
076	ENOTUNIQ	名稱在網路上不是唯一的
077	EBADFD	檔案描述元處於錯誤狀態
078	EREMCHG	遠端位址已變更
079	ELIBAC	無法存取所需的共用程式庫
080	ELIBBAD	存取毀損的共用程式庫
081	ELIBSCN	
082	ELIBMAX	嘗試連結過多的共用程式庫
083	ELIB執行	無法直接執行共用程式庫
084	EILSEQ	不合法的位元組順序
085	ERESTART	中斷的系統通話應重新啟動
086	ESTRPIPE	串流管道錯誤
087	EUSER	使用者過多
088	ENOTSOCK-	插槽在非插槽上運作
089	EDESTADDRREQ	目的地位址為必填
090	EMSGSIZ	訊息太長

錯誤編號	錯誤代碼	意義
091	EPROTOTYPE	套接字的傳輸協定類型錯誤
092	ENOPROTOOPT	傳輸協定無法使用
093	EPROTONOSUPPORT	不支援傳輸協定
094	ESOSKTNOSOUPPORT	不支援套接字類型
095	EOPNOT支持	傳輸端點不支援作業
096	EPFNOSOUPPORT	不支援傳輸協定系列
097	EAFFNOSOUPPORT	通訊協定不支援的位址系列
098	EADDRINUSE	位址已在使用中
099	EADDRNOTAVAIL	無法指派要求的位址
100	ENETDOWN	網路中斷
101	ENETUNREACH	無法連線至網路
102	ENETRESET	網路因為重設而中斷連線
103	ECONNABORTED	軟體導致連線終止
104	ECONNRESET	由對等端點重設連線
105	ENOBEufs	無可用的緩衝區空間
106	EISCONN	傳輸端點已連線
107	ENOTCONN	傳輸端點未連線
108	ESHUTDOWN	傳輸端點關機後無法傳送
109	ETOOMANYREFS	參考過多：無法接合
110	ETIMEDOUT	連線逾時
111	ECONNREFUSED	連線遭拒

錯誤編號	錯誤代碼	意義
112	EHOSTDOWN	主機當機
113	EHOSTUNREACH	沒有通往主機的路由
114	EALREADY	作業已在進行中
115	EINPROGRESS	目前正在運作中
116		
117	EUCULEAN	結構需要清理
118	ENOTNAM	不是Xenix命名類型檔案
119	ENAVAIL	沒有Xenix半馬
120	EISNAM	為命名類型檔案
121	EREMOTEIO	遠端I/O錯誤
122	EDCOT	已超過配額
123	ENOMEDIUM	找不到媒體
124	EMEDIUMTYPE	錯誤的媒體類型
125	ECANCELED	作業已取消
126	ENOKEY	所需的金鑰無法使用
127	EKEYEXPIRED	金鑰已過期
128	EKEYREVOKED	金鑰已撤銷
129	EKEYREJECTED	金鑰已遭服務拒絕
130	EOWNERDEAD	若需健全的互鎖：擁有者已死亡
131	ENOTRECOVERABE	對於強大的互鎖：狀態不可恢復

設定日誌管理和外部系統日誌伺服器

StorageGRID 中的外部 syslog 伺服器

外部syslog伺服器是StorageGRID 指不屬於功能區的伺服器、可用來在單一位置收集系統稽核資訊。使用外部 Syslog 伺服器可減少管理節點上的網路流量、並更有效率地管理資訊。對於 StorageGRID 、輸出系統記錄訊息封包格式符合 RFC 3164 。

您可以傳送至外部syslog伺服器的稽核資訊類型包括：

- 稽核日誌包含正常系統作業期間所產生的稽核訊息
- 安全性相關事件、例如登入和升級至root
- 如果需要開啟支援案例來疑難排解您遇到的問題、可能會要求的應用程式記錄

何時使用外部 Syslog 伺服器

如果您有大型網格、使用多種 S3 應用程式、或想要保留所有稽核資料、外部 Syslog 伺服器就特別有用。將稽核資訊傳送至外部syslog伺服器、可讓您：

- 更有效率地收集和管理稽核資訊、例如稽核訊息、應用程式記錄和安全事件。
- 減少管理節點上的網路流量、因為稽核資訊會直接從各種儲存節點傳輸到外部 Syslog 伺服器、而無需透過管理節點。

> 當記錄傳送至外部 Syslog 伺服器時、訊息結尾處會截斷大於 8 、 192 位元組的單一記錄、以符合外部 Syslog 伺服器實作的一般限制。

> 為了在外部 Syslog 伺服器發生故障時最大化完整資料恢復選項、(`localaudit.log`每個節點最多可保留 20 GB 的本機稽核記錄記錄。

如何設定外部 Syslog 伺服器

若要了解如何設定外部 syslog 伺服器，請參閱"設定日誌管理和外部系統日誌伺服器"。

如果您打算設定使用 TLS 或 RELP/TLS 通訊協定、則必須擁有下列憑證：

- * 伺服器 CA 憑證 * ：一或多個信任的 CA 憑證、用於驗證以 PEM 編碼的外部 Syslog 伺服器。如果省略、則會使用預設的Grid CA憑證。
- * 用戶端憑證 * ：用戶端憑證、用於以 PEM 編碼驗證外部 Syslog 伺服器。
- * 用戶端私密金鑰 * ：用戶端憑證的私密金鑰、採用 PEM 編碼。

> 如果您使用用戶端憑證、也必須使用用戶端私密金鑰。如果您提供加密的私密金鑰、也必須提供密碼。使用加密的私密金鑰並無顯著的安全效益、因為必須儲存金鑰和通關密碼；建議使用未加密的私密金鑰（若有）、以簡化操作。

一般而言、網格的大小可達到所需的處理量、定義為每秒S3作業量或每秒位元組數。例如、您可能需要網格處理每秒1、000次S3作業、或每秒2、000 MB的物件擷取和擷取作業。您應該根據網格的資料需求來調整外部syslog伺服器的大小。

本節提供一些啟發式公式、可協助您預估外部syslog伺服器需要處理的各種類型的記錄訊息速率和平均大小、以網格的已知或所需效能特性表示（每秒S3作業數）。

在預估公式中使用**S3**作業/秒

如果網格的處理量大小是以每秒位元組數表示、您必須將此規模轉換為每秒S3作業、才能使用估計公式。若要轉換網格處理量、您必須先判斷平均物件大小、以便使用現有稽核記錄和指標（如果有）中的資訊、或是運用您對StorageGRID 使用物件的應用程式所擁有的知識。例如、如果您的網格大小達到每秒2、000 MB的處理量、而且平均物件大小為2 MB、那麼您的網格大小就能處理每秒1、000次S3作業（2、000 MB / 2 MB）。

> 下列各節中的外部syslog伺服器規模調整公式提供一般案例預估（而非最糟案例預估）。視組態和工作負載而定、系統記錄訊息或系統記錄資料量的速率可能高於或低於公式所預測的速率。公式只能用作準則。

稽核記錄的估計公式

如果您沒有S3工作負載的相關資訊、而非預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的稽核記錄數量： 假設您將「稽核層級」設為預設值（所有類別均設為「正常」、但「儲存設備」設為「錯誤」除外）：

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒2、000個syslog訊息、而且應能以每秒1.6 MB的速率接收（及儲存）稽核記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。對於稽核記錄、最重要的其他變數是 S3 作業放置（相對於 GETs ）的百分比、以及下列 S3 欄位（表格中使用的 4 個字元縮寫為稽核記錄欄位名稱）的平均大小（以位元組為單位）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 貯體	S3儲存區名稱。
S3KY	S3 金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

讓我們使用P來表示S3作業所佔的百分比、其中0≤P≤1（因此、對於100%負載工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓我們使用 K 來代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以使用下列公式預估外部syslog伺服器需要處理的稽核記錄數量、前提是您將稽核層級設為預設值（所有類別均設為「正常」、儲存除外、 設定為「錯誤」）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則您的工作負載為50%、您的S3帳戶名稱、儲存區名稱、 而且物件名稱平均為90位元組、外部syslog伺服器的大小應可支援每秒1、500則syslog訊息、而且應能以每秒約1 MB的速率接收（及儲存）稽核記錄資料。

非預設稽核層級的估計公式

提供給稽核記錄的公式會假設使用預設的稽核層級設定（所有類別均設定為「正常」、但儲存區設為「錯誤」除外）。對於非預設稽核層級設定、無法使用估算稽核訊息速率和平均大小的詳細公式。不過、下表可用於粗略估計費率； 您可以使用提供給稽核記錄的平均大小公式、但請注意、這可能會導致預估過度、因為「額外」稽核訊息平均比預設稽核訊息小。

條件	公式
複寫：稽核層級全部設為「偵錯」或「正常」	稽核記錄速率 = 8 x S3 作業率
銷毀編碼：稽核層級全部設為「除錯」或「正常」	使用與預設設定相同的公式

安全性事件的估計公式

安全事件與 S3 作業無關、通常會產生可忽略的記錄和資料量。因此、我們不會提供任何預估公式。

應用程式記錄的估計公式

如果您沒有S3工作負載的相關資訊、而不是預期網格支援的每秒S3作業數量、您可以使用下列公式來預估外部syslog伺服器需要處理的應用程式記錄數量：

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、則外部syslog伺服器的大小應可支援每秒3、300個應用程式記錄、並能以每秒1.2 MB的速率接收（及儲存）應用程式記錄資料。

如果您對工作負載有更深入的瞭解、就有可能進行更精確的評估。對於應用程式記錄、最重要的其他變數是資料保護策略（複寫與刪除編碼）、 S3 作業放置（相對於取得 / 其他）的百分比、以及下列 S3 欄位的平均大小（以位元組為單位）（表格中使用的 4 個字元縮寫為稽核記錄欄位名稱）：

程式碼	欄位	說明
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
S3BK	S3 貯體	S3儲存區名稱。
S3KY	S3 金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。

規模估算範例

本節說明如何使用下列資料保護方法來使用網格的估計公式範例：

- 複寫
- 銷毀編碼

如果您使用複寫來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓 K 代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

例如、如果您的網格大小為每秒1、000次S3作業、工作負載為50%、S3帳戶名稱、儲存區名稱及物件名稱平均為90個位元組、則外部syslog伺服器的大小應可支援每秒1800個應用程式記錄、 並以每秒0.5 MB的速率接收（通常是儲存）應用程式資料。

如果您使用銷毀編碼來保護資料

讓P代表S3作業所放置的百分比、其中0≤P≤1（因此、對於100%投入工作負載、P = 1、對於100%取得工作負載、P = 0）。

讓 K 代表 S3 帳戶名稱、 S3 儲存區和 S3 金鑰的平均大小。假設S3帳戶名稱一律為my-S3帳戶（13位元組）、儲存區具有固定長度的名稱、例如/my/application/bucke-12345（28位元組）、而且物件具有固定長度的金鑰、例如5733a5d7-f069-41ef-8fbd-13247494c69c（36位元組）。然後K值為90（13 + 13 + 28 + 36）。

如果您可以判斷P和K的值、您可以預估外部syslog伺服器必須使用下列公式才能處理的應用程式記錄數量。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

舉例來說、如果您的網格大小為每秒 1 、 000 次 S3 作業、則您的工作負載為 50% 、而您的 S3 帳戶名稱、貯體名稱、 物件名稱平均 90 個位元組、外部 Syslog 伺服器的大小應可支援每秒 2 、 250 個應用程式記錄檔、而且應能以每秒 0.6 MB 的速度接收（通常是儲存）應用程式資料。

在 **StorageGRID** 中設定記錄管理

根據需要設定稽核等級、協定標頭、稽核訊息和日誌的位置以及日誌保留。

所有StorageGRID節點都會產生稽核訊息和日誌來追蹤系統活動和事件。審計訊息和日誌是監控和故障排除的重要工具。

您也可以"設定外部系統日誌伺服器"選擇將稽核資訊遠端儲存。使用外部伺服器可以最大限度地降低稽核訊息記錄的效能影響，同時又不降低稽核資料的完整性。如果您擁有大型網格、使用多種類型的 S3 應用程式或希望保留所有稽核資料，則外部 syslog 伺服器尤其有用。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 如果您打算設定外部系統日誌伺服器，則您已閱讀並遵循"使用外部 Syslog 伺服器的考量事項"。
- 如果您打算使用 TLS 或 RELP/TLS 通訊協定來設定外部 Syslog 伺服器、則您擁有所需的伺服器 CA 和用戶端憑證、以及用戶端私密金鑰。

變更稽核訊息層級

您可以在稽核日誌中針對下列每個類別的訊息設定不同的稽核層級：

稽核類別	預設設定	更多資訊
系統	正常	"系統稽核訊息"
儲存設備	錯誤	"物件儲存稽核訊息"
管理	正常	"管理稽核訊息"
用戶端讀取	正常	"用戶端讀取稽核訊息"
用戶端寫入	正常	"用戶端寫入稽核訊息"
ILM	正常	"ILM 稽核訊息"

稽核類別	預設設定	更多資訊
跨網格複寫	錯誤	"CGRR ：跨網格複寫要求"

升級期間，審計等級配置不會立即生效。

步驟

1. 選擇*設定* > 監控 > 日誌管理。
2. 針對每個稽核訊息類別、從下拉式清單中選取稽核層級：

稽核層級	說明
關	不會記錄任何類別的稽核訊息。
錯誤	僅記錄錯誤訊息－結果代碼不「成功」（SUCS）的稽核訊息。
正常	記錄標準交易訊息：此類別的說明中所列訊息。
偵錯	已過時。此層級的行為與正常稽核層級相同。

針對任何特定層級所包含的訊息、包括將記錄在較高層級的訊息。例如、「正常」層級包含所有的錯誤訊息。

如果您不需要 S3 應用程式的用戶端讀取操作的詳細記錄，則可以選擇將 用戶端讀取 設定變更為 錯誤 以減少稽核日誌中記錄的稽核訊息數量。

3. 選擇*保存*。

定義 **HTTP** 要求標頭

您可以選擇定義要包含在客戶端讀寫審計訊息中的任何 HTTP 請求標頭。

步驟

1. 在「 * 稽核通訊協定標頭 * 」區段中、定義您要包含在用戶端讀寫稽核訊息中的 HTTP 要求標頭。

   使用星號（*）做為萬用字元、以符合零個或多個字元。使用轉義順序（*）來符合文字星號。

2. 如有需要、請選取*新增其他標頭*以建立其他標頭。

   當 StorageGRID 在請求中發現 HTTP 標頭時，它會將這些標頭包含在稽核訊息的 HTRH 欄位中。

   只有當「用戶端讀取」或「用戶端寫入」的稽核等級不是「關閉*」時，才會記錄稽核協定請求標頭。

3. 選擇*保存*

預設情況下，稽核訊息和日誌會儲存在產生它們的節點上。StorageGRID 會定期輪替並最終刪除稽核訊息和日誌，以防止佔用過多磁碟空間。若要將稽核訊息和部分日誌儲存到外部，使用外部系統日誌伺服器。

如果要在內部儲存日誌文件，請選擇用於日誌儲存的租用戶和儲存桶並啟用日誌存檔。

[[use-external -syslog-server]] 使用外部 **Syslog** 伺服器

您可以選擇性地設定外部 Syslog 伺服器、將稽核記錄、應用程式記錄和安全性事件記錄儲存到網格外的位置。

如果您不想使用外部系統日誌伺服器，請跳過此步驟並轉到選擇日誌位置。

如果本程序中可用的組態選項不夠靈活、無法滿足您的需求、則可使用端點套用其他組態選項 `audit-destinations`、端點位於的「私有 API 」區段中"網格管理API"。例如、如果您想要將不同的 Syslog 伺服器用於不同的節點群組、可以使用 API 。

輸入系統記錄資訊

存取「設定外部系統記錄伺服器」精靈、並提供 StorageGRID 存取外部系統記錄伺服器所需的資訊。

步驟

1. 從本機節點和外部伺服器標籤中，選擇*設定外部系統日誌伺服器*。或者，如果您之前設定了外部系統日誌伺服器，請選擇*編輯外部系統日誌伺服器*。

   此時將顯示 Configure external Syslog server （配置外部系統日誌服務器）

2. 在嚮導的 * 輸入系統日誌 info* 步驟中，在 * 主機 * 字段中輸入外部系統日誌服務器的有效完全限定域名或 IPv4 或 IPv6 地址。
3. 輸入外部syslog伺服器上的目的地連接埠（必須是介於1和6555之間的整數）。預設連接埠為 514 。
4. 選取用於傳送稽核資訊至外部syslog伺服器的傳輸協定。

   建議使用 **TLS** 或 **RELP/TLS** 。您必須上傳伺服器憑證、才能使用上述任一選項。使用憑證有助於保護網格與外部syslog伺服器之間的連線。如需更多資訊、請參閱 "管理安全性憑證"。

   所有的傳輸協定選項都需要外部syslog伺服器的支援和組態。您必須選擇與外部syslog伺服器相容的選項。

   可靠的事件記錄傳輸協定（RELP）可延伸系統記錄傳輸協定的功能、以提供可靠的事件訊息傳輸。如果您的外部syslog伺服器必須重新啟動、使用RELP有助於防止稽核資訊遺失。

5. 選擇*繼續*。
6. [[attach 憑證]] 如果您選取 **TLS** 或 **RELP/TLS** 、請上傳伺服器 CA 憑證、用戶端憑證和用戶端私密金鑰。
   a. 選取*瀏覽*以取得您要使用的憑證或金鑰。
   b. 選取憑證或金鑰檔案。
   c. 選取*「Open*（開啟*）」上傳檔案。

      憑證或金鑰檔名稱旁會出現綠色勾號、通知您已成功上傳。

7. 選擇*繼續*。

管理系統記錄內容

您可以選取要傳送至外部 Syslog 伺服器的資訊。

步驟

1. 針對精靈的 * 管理系統記錄內容 * 步驟、選取您要傳送至外部系統記錄伺服器的每種稽核資訊類型。
   - * 傳送稽核記錄 * ：傳送 StorageGRID 事件和系統活動
   - * 傳送安全性事件 * ：傳送安全性事件，例如未獲授權的使用者嘗試登入或使用者以 root 身分登入
   - * 傳送應用程式記錄 * ：傳送"StorageGRID 軟體記錄檔"有助於疑難排解的項目、包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`（僅限管理節點）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - * 傳送存取記錄 * ：將外部要求的 HTTP 存取記錄傳送至 Grid Manager 、 Tenant Manger 、設定的負載平衡器端點、以及來自遠端系統的網格同盟要求。
2. 使用下拉式功能表為您要傳送的每個稽核資訊類別選取嚴重性和醫事機構（訊息類型）。

   設定嚴重性和設施值可協助您以可自訂的方式來彙總記錄、以便更輕鬆地進行分析。

   a. 對於 * 嚴重性 * 、請選取 * Passthrough * 、或選取介於 0 和 7 之間的嚴重性值。

      如果選擇一個值，StorageGRID 會將所選值套用至所有此類訊息。如果使用固定值置換嚴重性設定，則會遺失有關不同嚴重性的詳細資訊。

嚴重性	說明
Passthrough	傳送至外部 Syslog 的每則訊息、其嚴重性值與本機登入節點時相同： • 對於稽核記錄、嚴重性為「資訊」。 • 對於安全事件、嚴重性值是由節點上的 Linux 發佈所產生。 • 對於應用程式記錄、「資訊」和「通知」之間的嚴重性會因問題而異。例如、新增 NTP 伺服器並設定 HA 群組會提供「 info 」的值、而刻意停止 SSM 或 RSM 服務則會提供「 notice 」的值。 • 對於存取記錄、嚴重性為「資訊」。
0	緊急：系統無法使用

嚴重性	說明
1	警示：必須立即採取行動
2	關鍵：關鍵條件
3	錯誤：錯誤情況
4	警告：警告條件
5	注意：正常但重要的情況
6	資訊：資訊訊息
7	偵錯：偵錯層級的訊息

b. 對於 * 設施 * 、請選取 * Passthrough * 、或選取介於 0 和 23 之間的設施值。

如果您選取一個值、它會套用至所有此類型的訊息。如果您以固定值覆寫醫事機構、則會遺失有關不同醫事機構的資訊。

設施	說明
Passthrough	傳送至外部 Syslog 的每則訊息、其設施值與本機登入節點時相同： • 對於稽核記錄、傳送至外部 Syslog 伺服器的設施為「 local7 」。 • 對於安全事件、設施值是由節點上的 Linux 套裝作業系統所產生。 • 對於應用程式記錄、傳送至外部 Syslog 伺服器的應用程式記錄具有下列設施值： ◦ `bycast.log`：用戶或守護程序 ◦ `bycast-err.log`：用戶、守護程序、 local3 或 local4 ◦ `jaeger.log`： local2. ◦ `nms.log`： local3. ◦ `prometheus.log`： local4. ◦ `raft.log`： local5. ◦ `hagroups.log`： local6. • 對於存取記錄、傳送至外部 Syslog 伺服器的設施為「 local0 」。
0	KERN（核心訊息）
1	使用者（使用者層級訊息）

設施	說明
2	郵件
3	精靈（系統精靈）
4	驗證（安全性/授權訊息）
5	系統記錄（系統記錄所產生的訊息）
6	LPR（線路印表機子系統）
7	新聞（網路新聞子系統）
8	uucp
9	cron（時鐘精靈）
10	安全性（安全性/授權訊息）
11	FTP
12	NTP
13	記錄稽核（記錄稽核）
14	記錄警示（記錄警示）
15	時鐘（時鐘精靈）
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6

設施	說明
23	local7

3. 選擇*繼續*。

傳送測試訊息

在使用外部 syslog 伺服器之前，請要求網格中的所有節點向該外部 syslog 伺服器傳送測試訊息。這些測試訊息有助於您在將資料傳送至外部 syslog 伺服器之前，驗證整個記錄收集基礎架構。

請勿使用外部 Syslog 伺服器組態、除非您確認外部 Syslog 伺服器收到來自網格中每個節點的測試訊息、且訊息已如預期般處理。

步驟

1. 如果您不想傳送測試訊息、因為您確定已正確設定外部 Syslog 伺服器、而且可以從網格中的所有節點接收稽核資訊、請選取 * 略過並完成 * 。

   綠色橫幅表示已儲存組態。

2. 否則、請選取 * 傳送測試訊息 * （建議）。

   測試結果會持續顯示在頁面上、直到您停止測試為止。測試進行中時、您的稽核訊息會繼續傳送至先前設定的目的地。

3. 如果您在 syslog 伺服器設定期間或執行時收到任何錯誤，請修正它們並再次選擇*傳送測試訊息*。

   請參閱"排除外部syslog伺服器的故障"以協助您解決任何錯誤。

4. 請等到看到綠色橫幅、表示所有節點都已通過測試。
5. 請檢查您的syslog伺服器、確定是否收到測試訊息、並按照預期處理。

   如果您使用 UDP，請檢查整個日誌收集基礎架構。 UDP 協定不像其他協定那樣允許嚴格的錯誤檢測。

6. 選擇*停止並結束*。

   您將返回到* Audit和syslog server*頁面。綠色橫幅表示系統記錄伺服器組態已儲存。

   直到您選擇包含外部系統日誌伺服器的目標時， StorageGRID稽核資訊才會傳送至外部系統日誌伺服器。

選擇日誌位置

您可以指定稽核日誌、安全事件日誌、"StorageGRID應用程式日誌" ，並發送訪問日誌。

StorageGRID 預設為本機節點稽核目的地、並將稽核資訊儲存在 `/var/local/log/localaudit.log` 中。

使用 `/var/local/log/localaudit.log`時、 `Grid Manager` 和 `Tenant Manager` 稽核記錄項目可能會傳送至儲存節點。您可以使用命令來尋找哪些節點具有最近的項目 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`。

某些目的地只有在您已設定外部 Syslog 伺服器時才可使用。

步驟

1. 選擇*日誌位置* > 本機節點和外部伺服器。
2. 若要變更日誌類型的日誌位置，請選擇其他選項。

* 僅限本機節點 * 和 * 外部系統記錄伺服器 * 通常可提供更好的效能。

選項	說明
僅限本機節點（預設）	稽核訊息、安全事件日誌和應用程式日誌不會傳送到管理節點。相反，它們僅保存在生成它們的節點（“本地節點”）上。每個本地節點產生的審計資訊儲存在 `/var/local/log/localaudit.log`。 注意： StorageGRID會定期刪除本機日誌以釋放空間。當節點的日誌檔案達到 1 GB 時，將儲存現有檔案並啟動新的日誌檔案。日誌的輪換限制為 21 個檔案。當建立第 22 個版本的日誌檔案時，最舊的日誌檔案將被刪除。每個節點平均儲存約 20 GB 的日誌資料。為了長期保存日誌，使用租戶和存儲桶進行日誌存儲 。
管理節點 / 本機節點	稽核訊息會傳送至管理節點上的稽核記錄、安全性事件記錄和應用程式記錄會儲存在產生這些記錄的節點上。稽核資訊會儲存在下列檔案中： • 管理節點（主要和非主要）： `/var/local/audit/export/audit.log` • 所有節點： `/var/local/log/localaudit.log`檔案通常是空的或遺失的。它可能包含次要資訊、例如某些訊息的額外複本。
外部syslog伺服器	審計資訊被傳送到外部系統日誌伺服器並保存在本地節點上 (`/var/local/log/localaudit.log`) 。傳送的訊息類型取決於您如何設定外部系統日誌伺服器。此選項僅在您設定外部系統日誌伺服器。
管理節點和外部系統日誌伺服器	審計訊息被傳送到審計日誌 (`/var/local/audit/export/audit.log`)，並將稽核資訊傳送至外部系統日誌伺服器並保存在本機節點上 (`/var/local/log/localaudit.log`) 。傳送的訊息類型取決於您如何設定外部系統日誌伺服器。此選項僅在您設定外部系統日誌伺服器。

3. 選擇*保存*。

   出現警告訊息。

4. 選取 * 確定 * 以確認您要變更稽核資訊的目的地。

   新記錄會傳送至您選取的目的地。現有記錄仍會保留在目前位置。

使用儲存桶

日誌會定期輪換。使用同一網格中的 S3 儲存桶來長期儲存日誌。

1. 選擇*日誌位置* > 使用儲存桶。
2. 選取“啟用存檔日誌”複選框。
3. 如果列出的租戶和儲存桶不是您想要使用的，請選擇*更改租戶和儲存桶*，然後選擇*建立租戶和儲存桶*或*選擇租戶和儲存桶*。

   建立租戶和儲存桶

   a. 輸入新的租戶名稱。
   b. 輸入並確認新租戶的密碼。
   c. 輸入新的儲存桶名稱。
   d. 選擇*建立並啟用*。

   選擇租戶和貯體

   a. 從下拉式選單中選擇租戶名稱。
   b. 從下拉式選單中選擇一個儲存桶。
   c. 選擇*選擇並啟用*。

4. 選擇*保存*。

   日誌將儲存在您指定的租用戶和儲存桶中。日誌的物件鍵名稱採用以下格式：

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   例如：

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```

管理記錄保留

您可以透過建立 ILM 規則或設定 S3 儲存桶生命週期原則來管理 StorageGRID 保留記錄的時間。

ILM 規則

為儲存桶建立 ILM 規則，並將此規則新增至作用中的 ILM 原則。

步驟

1. 選擇* ILM > Rules *。
2. 選擇 **Create**。"步驟 1 （輸入詳細資料）" 「建立 ILM 規則精靈」隨即出現：
   a. 請為該規則輸入唯一名稱。例如：ILM Rule for archived logs。
   b. 選擇日誌歸檔 S3 租戶帳戶。
   c. 指定日誌歸檔的 S3 儲存桶。
3. 繼續"步驟 2 （定義放置位置）"並定義歸檔日誌規則的存放位置。例如，ILM 規則在第一年於站台 1 和站台 2 各儲存一份複本。一年後，產生一份 2+1 的銷除編碼複本，並僅儲存在一個站台。
4. 建立規則後，將其新增至作用中的 ILM 原則。

S3 bucket 生命週期

在日誌歸檔 S3 儲存桶上設定 S3 儲存桶生命週期原則：

```
{
      "Rules": [
        {
           "ID": "Retain logs forever",
           "Filter": {},
           "Status": "Enabled"，
           "Expiration": {}
        }
      ]
}
```

在日誌歸檔 S3 儲存桶上設定 S3 儲存桶生命週期原則時，對於符合儲存桶生命週期篩選器的物件，生命週期過期作業會置換 ILM 原則。不符合儲存桶生命週期篩選器的物件將使用 ILM 原則的保留設定。如果物件符合儲存桶生命週期篩選器，但未明確指定過期作業，則不會使用 ILM 原則的保留設定，並隱含表示物件版本將永久保留。

設定郵件伺服器

身為 StorageGRID 系統管理員，您需要設定電子郵件伺服器，以便從 StorageGRID 警示和監控系統傳送通知，告知您、其他系統管理員及技術支援有關系統事件和問題的資訊。

StorageGRID 使用郵件伺服器進行通知的功能包括警報、AutoSupport 和多重管理員驗證 (MAV)。您可以使用同一個郵件伺服器來傳送所有通知。

開始之前

- 您有"root 存取權限"。

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。

步驟

1. 選擇 組態 > 監控 > 電子郵件伺服器。

   顯示電子郵件伺服器頁面。

2. 選擇下拉式選單「檢視可能需要電子郵件伺服器的功能」。如果您想檢視設定某項功能的電子郵件通知的詳細資訊和所需資訊，請選擇「檢視」。

   您將被引導至 Grid Manager 中該功能的組態頁面。每個功能的組態頁面都包含一則通知，提示您需要一個郵件伺服器才能傳送電子郵件通知。

3. 若要從「電子郵件伺服器」頁面設定電子郵件伺服器：
   a. 請輸入郵件伺服器的 IP 位址或 FQDN。
   b. 選擇郵件伺服器使用的連接埠號碼。預設值為 25。
   c. 若要啟用驗證，請選擇 **Use authentication** ，然後輸入使用者名稱和密碼。
   d. 若要要求驗證 SMTP 伺服器的身份，請選擇「使用傳輸層安全性協定 (TLS)」。然後：
      i. 提供 CA 憑證套裝組合。
      ii. 如果 SMTP 郵件伺服器要求郵件寄件者提供用戶端憑證進行驗證，請選擇 **Send client certificate**。然後提供用戶端憑證和私鑰。
   e. 為確保您的電子郵件設定正確，請輸入寄件者和收件者資訊以傳送測試電子郵件。選取 * 傳送 *。

      隨即顯示確認訊息、表示已傳送測試電子郵件。

   f. 勾選所有電子郵件收件者的收件匣、確認已收到測試電子郵件。

      如果幾分鐘內未收到電子郵件、或觸發*電子郵件通知失敗*警示、請檢查您的設定、然後再試一次。

   g. 登入任何其他管理節點、然後傳送測試電子郵件以驗證所有站台的連線能力。

      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。這與測試 AutoSupport 套件形成對照、其中所有管理節點都會傳送測試電子郵件。

4. 選擇*保存*。

   發送測試郵件不會儲存您的設定。您必須選擇 **Save**。

   電子郵件設定即會儲存。

5. 前往使用電子郵件伺服器的功能的組態頁面，並完成電子郵件通知設定。
   - "警示"。對於警示，您也可以 "設定 SNMP 通知"。
   - "AutoSupport".您可以透過電子郵件、HTTPS 或 HTTP 傳送 AutoSupport 套件（不建議使用 HTTP）。
   - "多重管理員驗證 (MAV)"。

使用SNMP監控

在 StorageGRID 中使用 SNMP 監控

如果您想StorageGRID 要使用簡單網路管理傳輸協定（SNMP）監控效能、您必須設定StorageGRID 包含在資訊區中的SNMP代理程式。

- "設定SNMP代理程式"
- "更新SNMP代理程式"

功能

每個 StorageGRID 節點都會執行 SNMP 代理程式或常駐程式、提供 MIB 。StorageGRID MIB 包含警示的表格和通知定義。此外、也包含系統說明資訊、例如每個節點的平台和型號。每StorageGRID 個支援MIB-II物件的子集。

查看"存取 MIB 檔案"是否要在網格節點上下載 MIB 檔案。

一開始、所有節點上的SNMP都會停用。當您設定SNMP代理程式時、所有StorageGRID 的Sing節點都會收到相同的組態。

支援所有三種版本的SNMP傳輸協定的Sof SNMP代理程式。StorageGRID它可為查詢提供唯讀的MIB存取、並可將兩種事件導向通知傳送至管理系統：

陷阱

設陷是 SNMP 代理程式傳送的通知、不需要管理系統的認可。陷阱可讓管理系統知道StorageGRID 在某些情況下發生、例如觸發警示。

SNMP的所有三個版本均支援陷阱。

通知

通知類似於陷阱、但需要管理系統確認。如果 SNMP 代理程式在一定時間內未收到回應、它會重新傳送通知、直到收到回應或達到最大重試值為止。

在SNMPv2c和v3中支援通知。

在下列情況下會傳送陷阱和通知：

- 預設或自訂警示會在任何嚴重性層級觸發。若要隱藏警示的 SNMP 通知、您必須"設定靜音"發出警示。警示通知會由傳送"偏好的寄件者管理節點"。

  每個警示都會根據警示的嚴重性層級、對應到三種陷阱類型中的一種：activeMinorAlert、activeMajorAlert和activeCriticalAlert。如需觸發這些陷阱的警示清單，請參閱"警示參考資料"。

SNMP 版本支援

下表提供每個SNMP版本所支援項目的高層摘要。

	SNMPv1	SNMPv2c	SNMPv3
查詢 （ Get 和 GETNEXT ）	唯讀的mib查詢	唯讀的mib查詢	唯讀的mib查詢
查詢驗證	社群字串	社群字串	使用者型安全模式（USM）使用者
通知 （陷阱與通知）	僅設陷	擷取並通知	擷取並通知
通知驗證	每個陷阱目的地的預設陷阱社群或自訂社群字串	每個陷阱目的地的預設陷阱社群或自訂社群字串	每個陷阱目的地的USM使用者

限制

- 支援唯讀的mib存取。StorageGRID不支援讀寫存取。
- 網格中的所有節點都會收到相同的組態。
- v3：StorageGRID 不支援傳輸支援模式（TSM）。
- v3：唯一支援的驗證傳輸協定是SHa（HMAC - SHA-96）。
- v3：唯一支援的隱私權傳輸協定是AES。

在 **StorageGRID** 中設定 **SNMP** 代理程式

您可以將 StorageGRID SNMP 代理程式設定為使用協力廠商 SNMP 管理系統來進行唯讀 MIB 存取和通知。

開始之前

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

關於這項工作

StorageGRID SNMP 代理程式支援 SNMPv1 、 SNMPv2c 和 SNMPv3 。您可以為代理程式設定一或多個版本。對於 SNMPv3 、僅支援使用者安全模式（ USM ）驗證。

網格中的所有節點都使用相同的 SNMP 組態。

指定基本組態

首先、請啟用 StorageGRID SMNP 代理程式、並提供基本資訊。

步驟

1. 選擇*設定* > 監控 > **SNMP** 代理程式。

   此時將顯示 SNMP 代理程式頁面。

2. 若要在所有網格節點上啟用 SNMP 代理程式、請選取 * 啟用 SNMP* 核取方塊。
3. 在「基本組態」區段中輸入下列資訊。

欄位	說明
系統聯絡人	選用。StorageGRID 系統的主要聯絡人、會以系統聯絡人的形式在 SNMP 訊息中傳回。 系統聯絡人通常是電子郵件地址。此值適用於 StorageGRID 系統中的所有節點。* 系統連絡人 * 最多可有 255 個字元。
系統位置	選用。StorageGRID 系統的位置、會以 sysLocation 的形式在 SNMP 訊息中傳回。 系統位置可以是任何有助於識別 StorageGRID 系統所在位置的資訊。例如、您可以使用設施的街道地址。此值適用於 StorageGRID 系統中的所有節點。* 系統位置 * 最多可有 255 個字元。
啟用 SNMP 代理程式通知	• 如果選取此選項、 StorageGRID SNMP 代理程式會傳送設陷和通知通知。 • 如果未選取、則 SNMP 代理程式支援唯讀 MIB 存取、但不會傳送任何 SNMP 通知。
啟用驗證陷阱	如果選取此選項、 StorageGRID SNMP 代理程式會在收到驗證不正確的通訊協定訊息時傳送驗證陷阱。

輸入社群字串

如果您使用 SNMPv1 或 SNMPv2c 、請填寫社群字串一節。

當管理系統查詢StorageGRID 到這個功能時、它會傳送一個社群字串。如果社群字串符合此處指定的其中一個值、SNMP代理程式會傳送回應給管理系統。

步驟

1. 對於 * 唯讀社群 * 、可選擇性地輸入社群字串、以允許對 IPv4 和 IPv6 代理程式位址進行唯讀 MIB 存取。

   為了確保 StorageGRID 系統的安全性、請勿使用「 public 」作為社群字串。如果將此欄位保留空白、 SNMP 代理程式會使用 StorageGRID 系統的網格 ID 做為社群字串。

   每個社群字串最多可以有 32 個字元、而且不能包含空白字元。

2. 選取 * 新增其他社群字串 * 以新增其他字串。

   最多允許五個字串。

[[SELECT （選取） TRAP_DESTIN]：建立設陷目的地

使用「其他組態」區段中的「設陷目的地」索引標籤、可定義 StorageGRID 設陷或通知通知通知的一個或多個目的地。當您啟用 SNMP 代理程式並選取 * 儲存 * 時、 StorageGRID 會在觸發警示時、將通知傳送至每個定義的目的地。也會針對支援的MIB-II實體（例如ifdown和coldStart）傳送標準通知。

步驟

1. 在 * 預設設陷社群 * 欄位中、選擇性地輸入您要用於 SNMPv1 或 SNMPv2 設陷目的地的預設社群字串。

   根據需要、您可以在定義特定陷阱目的地時、提供不同的（「自訂」）社群字串。

   ◦ 預設設陷社群 * 最多可有 32 個字元、且不可包含空格字元。

2. 若要新增設陷目的地、請選取 * 建立 * 。
3. 選取要用於此設陷目的地的 SNMP 版本。
4. 針對您選取的版本填寫「建立設陷目的地」表單。

SNMPv1

如果您選取的是 SNMPv1 版本、請填寫這些欄位。

欄位	說明
類型	必須是 SNMPv1 的陷阱。
主機	用於接收陷阱的 IPv4 或 IPv6 位址或完整網域名稱（ FQDN ）。
連接埠	使用 162 、這是 SNMP 設陷的標準連接埠、除非您必須使用其他值。
傳輸協定	除非您需要使用 TCP 、否則請使用標準 SNMP 設陷傳輸協定的 UDP 。
社群字串	如果指定了預設陷阱社群、請使用該陷阱社群、或為此陷阱目的地輸入自訂社群字串。 自訂社群字串最多可以有 32 個字元、而且不能包含空格。

SNMPv2c

如果您選取的是 SNMPv2c 版本、請填寫這些欄位。

欄位	說明
類型	目的地將用於陷阱還是通知。
主機	接收陷阱的 IPv4 或 IPv6 位址或 FQDN 。
連接埠	使用 162 、這是 SNMP 設陷的標準連接埠、除非您必須使用其他值。
傳輸協定	除非您需要使用 TCP 、否則請使用標準 SNMP 設陷傳輸協定的 UDP 。
社群字串	如果指定了預設陷阱社群、請使用該陷阱社群、或為此陷阱目的地輸入自訂社群字串。 自訂社群字串最多可以有 32 個字元、而且不能包含空格。

SNMPv3

如果您選取的是 SNMPv3 版本、請填寫這些欄位。

欄位	說明
類型	目的地將用於陷阱還是通知。

欄位	說明
主機	接收陷阱的 IPv4 或 IPv6 位址或 FQDN 。
連接埠	使用 162 、這是 SNMP 設陷的標準連接埠、除非您必須使用其他值。
傳輸協定	除非您需要使用 TCP 、否則請使用標準 SNMP 設陷傳輸協定的 UDP 。
USM使用者	將用於驗證的 USM 使用者。 • 如果您選取* Trap *、則只會顯示沒有授權引擎ID的USM使用者。 • 如果您選取* INFUS*、則只會顯示具有驗證引擎ID的USM使用者。 • 如果沒有顯示使用者： i. 建立並儲存設陷目的地。 ii. 前往建立 USM 使用者並建立使用者。 iii. 返回「設陷目的地」標籤、從表格中選取儲存的目的地、然後選取 * 編輯 * 。 iv. 選取使用者。

5. 選擇* Create （建立）。

   陷阱目的地隨即建立並新增至表格。

建立代理程式位址

或者、您也可以使用「其他組態」區段中的「值機員位址」標籤來指定一或多個「接聽位址」。這些是 SNMP 代理程式可以接收查詢的 StorageGRID 位址。

如果您未設定代理程式位址、則所有 StorageGRID 網路上的預設聆聽位址為 UDP 連接埠 161 。

步驟

1. 選擇* Create （建立）。
2. 輸入下列資訊。

欄位	說明
網際網路傳輸協定	此位址是使用 IPv4 還是 IPv6 。 依預設、SNMP使用的是IPV4。

欄位	說明
傳輸傳輸傳輸協定	此位址是使用 UDP 還是 TCP 。 依預設、SNMP使用的是udp。
StorageGRID 網路	代理程式將接聽的 StorageGRID 網路。 • 網格、管理和用戶端網路： SNMP 代理程式會在所有三個網路上接聽查詢。 • 網格網路 • 管理網路 • 用戶端網路 ◦ 注意 * ：如果您使用 Client Network 取得不安全的資料、並為 Client Network 建立代理程式位址、請注意、 SNMP 流量也不安全。
連接埠	（可選） SNMP 代理應偵聽的端口號。 SNMP代理程式的預設udp連接埠為161、但您可以輸入任何未使用的連接埠號碼。 • 注意 * ：儲存 SNMP 代理程式時、 StorageGRID 會自動開啟內部防火牆上的代理程式位址連接埠。您必須確保任何外部防火牆都允許存取這些連接埠。

3. 選擇* Create （建立）。

   代理程式位址隨即建立並新增至表格。

建立 **USM** 使用者

如果您使用的是 SNMPv3 、請使用「其他組態」區段中的 USM 使用者索引標籤、定義授權查詢 MIB 或接收設陷並通知的 USM 使用者。

> 對於 SNMPv3 *trap* 目的地，建議為每個管理節點建立一個 USM 使用者。如果每個管理節點都沒有 USM 用戶，當主管理節點發生故障時，您的管理系統可能會停止接收通知。

> SNMPv3 通知目的地必須有具有引擎 ID 的使用者。SNMPv3 _trap 目的地無法擁有具有引擎 ID 的使用者。

如果您只使用 SNMPv1 或 SNMPv2c 、則不適用這些步驟。

步驟

1. 選擇* Create （建立）。
2. 輸入下列資訊。

欄位	說明
使用者名稱	此 USM 使用者的唯一名稱。 使用者名稱最多可以有 32 個字元、而且不能包含空格字元。建立使用者後、無法變更使用者名稱。
唯讀 MIB 存取	如果選取此選項、則此使用者應擁有 MIB 的唯讀存取權。
授權引擎 ID	如果此使用者將用於通知目的地、則為此使用者的授權引擎 ID 。 輸入 10 至 64 個十六進位字元（ 5 至 32 位元組）、不含空格。此值是 USM 使用者所需的、將會在陷阱目的地中選取以通知。將在陷阱目的地中選取的 USM 使用者不允許使用此值。 • 注意 * ：如果您選取 * 唯讀 MIB 存取 * 、則不會顯示此欄位、因為擁有唯讀 MIB 存取權的 USM 使用者無法擁有引擎 ID 。
安全性層級	USM 使用者的安全層級： • 驗證權限：此使用者與驗證和隱私權（加密）通訊。您必須指定驗證傳輸協定和密碼、以及隱私權傳輸協定和密碼。 • 驗證**NoPrimv**：此使用者可與驗證通訊、且無隱私權（無加密）。您必須指定驗證傳輸協定和密碼。
驗證傳輸協定	請務必設定為 SHA 、這是唯一支援的傳輸協定（ HMAC-SHA-96 ）。
密碼	此使用者將用於驗證的密碼。
隱私權傳輸協定	僅當您選擇 **authPrimv** 並始終設置爲 AES 時顯示，這是唯一支持的隱私協議。
密碼	僅當您選擇了 **authPrimv** 時才顯示。此使用者將用於隱私的密碼。

3. 選擇* Create （建立）。

   系統會建立USM使用者並將其新增至表格。

4. 完成 SNMP 代理程式組態後、請選取 * 儲存 * 。

   新的SNMP代理程式組態會變成作用中狀態。

相關資訊

"用於外部通訊的連接埠"

更新 **StorageGRID SNMP** 代理程式

您可以停用 SNMP 通知、更新社群字串、或新增或移除代理程式位址、 USM 使用者和設陷目的地。

開始之前

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

關於這項工作

如需 SNMP 代理程式頁面上每個欄位的詳細資訊、請參閱"設定SNMP代理程式"。您必須在頁面底部選取 * 儲存 * 、以提交您在每個標籤上所做的任何變更。

步驟

1. 選擇*設定* > 監控 > **SNMP** 代理程式。

   此時將顯示 SNMP 代理程式頁面。

2. 若要停用所有網格節點上的 SNMP 代理程式、請清除 * 啟用 SNMP* 核取方塊、然後選取 * 儲存 * 。

   如果重新啟用 SNMP 代理程式、則會保留任何先前的 SNMP 組態設定。

3. 您也可以選擇更新基本組態區段中的資訊：

   a. 視需要更新 * 系統聯絡人 * 和 * 系統位置 * 。

   b. 或者、選取或清除 * 啟用 SNMP 代理程式通知 * 核取方塊、以控制 StorageGRID SNMP 代理程式是否傳送陷阱和通知通知。

      清除此核取方塊時、 SNMP 代理程式支援唯讀 MIB 存取、但不會傳送 SNMP 通知。

   c. 或者、選取或清除 * 啟用驗證設陷 * 核取方塊、以控制 StorageGRID SNMP 代理程式是否在收到驗證不當的傳輸協定訊息時傳送驗證設陷。

4. 如果您使用 SNMPv1 或 SNMPv2c 、請選擇性地在社群字串區段中更新或新增 * 唯讀社群 * 。

5. 若要更新設陷目的地、請選取「其他組態」區段中的「設陷目的地」索引標籤。

   使用此索引標籤可定義 StorageGRID 設陷或通知通知的一或多個目的地。當您啟用 SNMP 代理程式並選取 * 儲存 * 時、 StorageGRID 會在觸發警示時、將通知傳送至每個定義的目的地。也會針對支援的MIB-II實體（例如ifdown和coldStart）傳送標準通知。

   如需輸入內容的詳細資訊，請參閱"建立設陷目的地"。

   - 您也可以更新或移除預設的設陷社群。

     如果您移除預設的陷阱社群、則必須先確定任何現有的陷阱目的地都使用自訂社群字串。

   - 若要新增設陷目的地、請選取 * 建立 * 。
   - 若要編輯設陷目的地、請選取選項按鈕、然後選取 * 編輯 * 。
   - 若要移除設陷目的地、請選取選項按鈕、然後選取 * 移除 * 。

- 若要提交變更、請選取頁面底部的 * 儲存 * 。

6. 若要更新代理程式位址、請選取「其他組態」區段中的「代理程式位址」標籤。

   使用此索引標籤可指定一或多個「聆聽地址」。這些是 SNMP 代理程式可以接收查詢的 StorageGRID 位址。

   如需輸入內容的詳細資訊，請參閱"建立代理程式位址"。

   - 若要新增代理程式位址、請選取 * 建立 * 。
   - 若要編輯值機員地址、請選取選項按鈕、然後選取 * 編輯 * 。
   - 若要移除代理程式位址、請選取選項按鈕、然後選取 * 移除 * 。
   - 若要提交變更、請選取頁面底部的 * 儲存 * 。

7. 若要更新 USM 使用者、請選取「其他組態」區段中的 USM 使用者標籤。

   使用此索引標籤可定義有權查詢mib或接收陷阱和通知的USM使用者。

   如需輸入內容的詳細資訊，請參閱"建立 USM 使用者"。

   - 若要新增 USM 使用者、請選取 * 建立 * 。
   - 若要編輯 USM 使用者、請選取選項按鈕、然後選取 * 編輯 * 。

     無法變更現有 USM 使用者的使用者名稱。如果您需要變更使用者名稱、則必須移除使用者並建立新的使用者名稱。

     > 如果您新增或移除使用者的授權引擎 ID 、且目前已為目的地選取該使用者、則必須編輯或移除目的地。否則、當您儲存SNMP代理程式組態時、就會發生驗證錯誤。

   - 若要移除 USM 使用者、請選取選項按鈕、然後選取 * 移除 * 。

     > 如果您移除的使用者目前已選取作為設陷目的地、您必須編輯或移除目的地。否則、當您儲存SNMP代理程式組態時、就會發生驗證錯誤。

   - 若要提交變更、請選取頁面底部的 * 儲存 * 。

8. 更新 SNMP 代理程式組態後、請選取 * 儲存 * 。

存取 **StorageGRID MIB** 檔案

MIB 檔案包含有關網格中節點的受管理資源和服務內容的定義和資訊。您可以存取定義 StorageGRID 物件和通知的 MIB 檔案。這些檔案可用於監控您的網格。

如需 SNMP 和 MIB 檔案的詳細資訊、請參閱"使用SNMP監控"。

存取 **MIB** 檔案

請依照下列步驟存取 MIB 檔案。

步驟

1. 選擇*設定* > 監控 > **SNMP** 代理程式。
2. 在 SNMP 代理程式頁面上、選取您要下載的檔案：
   - **NetApp-STORAGEGRID-MIB.txt** ：定義可在所有管理節點上存取的警示表和通知（陷阱）。
   - **ES-NetApp-06-MIB.mIB** ：定義 E 系列應用裝置的物件和通知。
   - **MIB_1_10.zip** ：定義具有 BMC 介面的應用裝置物件和通知。

   您也可以在任何 StorageGRID 節點上的下列位置存取 MIB 檔案：`/usr/share/snmp/mibs`

3. 若要從 MIB 檔案擷取 StorageGRID OID ：
   a. 取得 StorageGRID MIB 根目錄的 OID ：

      ```
      root@user-adm1:~ # snmptranslate -On -IR storagegrid
      ```

      結果： `.1.3.6.1.4.1.789.28669` (`28669`永遠是 StorageGRID 的 oID ）

   b. 在整個樹狀結構中的 StorageGRID OID （ `paste`用於連接線）：

      ```
      root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
      ```

      此 `snmptranslate`命令有許多選項可用於探索 MIB 。此命令可在任何 StorageGRID 節點上使用。

MIB 檔案內容

所有物件都位於 StorageGRID OID 之下。

物件名稱	物件 **ID** （ **OID** ）	說明
	1.3.6.1.4.1.789.28669	NetApp StorageGRID 實體的 MIB 模組。

MIB 物件

物件名稱	物件 **ID** （ **OID** ）	類型	使用權	**MIB** 模組	說明
activeAlertCount	1.3.6.1.4.1.+789.28669.1.3	Integer32	只讀	NETAPP-STORAGEGRID-MIB	activeAlertTable 中作用中警示的數量。
activeAlertTable	1.3.6.1.4.1.+789.28669.1.4	ActiveAlertEntry 的序列	不可訪問	NETAPP-STORAGEGRID-MIB	StorageGRID 中作用中警示的表格。

物件名稱	物件 **ID** （ **OID** ）	類型	使用權	**MIB** 模組	說明
活動警報條目		順序	不可訪問	NETAPP-STORAGEGRID-MIB	單一StorageGRID警報，按警報 ID 索引。
activeAlertId	1.3.6.1.4.1.+789.28669.1.4.1.1	八位元位元組串	只讀	NETAPP-STORAGEGRID-MIB	警示的 ID 。僅在目前的一組作用中警示中是唯一的。
activeAlertName	1.3.6.1.4.1.+789.28669.1.4.1.2	八位元位元組串	只讀	NETAPP-STORAGEGRID-MIB	警示的名稱。
activeAlertInstance	1.3.6.1.4.1.+789.28669.1.4.1.3	八位元位元組串	只讀	NETAPP-STORAGEGRID-MIB	產生警示的實體名稱、通常是節點名稱。
行動警示嚴重性	1.3.6.1.4.1.+789.28669.1.4.1.4	八位元位元組串	只讀	NETAPP-STORAGEGRID-MIB	警示的嚴重性。
activeAlertStartTime	1.3.6.1.4.1.+789.28669.1.4.1.5	日期和時間	只讀	NETAPP-STORAGEGRID-MIB	觸發警報的時間。

收集其他**StorageGRID** 的資料

監控 **StorageGRID** 中的 **PUT** 和 **GET** 效能

您可以監控特定作業（例如物件存放區和擷取）的效能、以協助識別可能需要進一步調查的變更。

關於這項工作

若要監控 Put 並取得效能、您可以直接從工作站或使用開放原始碼 S3tester 應用程式來執行 S3 命令。使用這些方法可讓您獨立評估StorageGRID 不受支援的因素效能、例如用戶端應用程式問題或外部網路問題。

執行PUT與Get作業測試時、請遵循下列準則：

- 使用與一般擷取至網格的物件類似的物件大小。
- 針對本機和遠端站台執行作業。

中的訊息"稽核日誌"指出執行特定作業所需的總時間。例如、若要判斷S3 Get要求的總處理時間、您可以檢閱SGET稽核訊息中Time屬性的值。您也可以在稽核訊息中找到下列 S3 作業的時間屬性：刪除、取得、標題、中繼資料更新、張貼、放置

分析結果時、請查看滿足要求所需的平均時間、以及您可以達到的整體處理量。定期重複相同的測試並記錄結果、以便識別可能需要調查的趨勢。

- 您可以 "從GitHub下載S3tester"。

監控 **StorageGRID** 中的物件驗證作業

這個支援系統可驗證儲存節點上物件資料的完整性、同時檢查毀損和遺失的物件。StorageGRID

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。

關於這項工作

兩個"驗證程序"共同作業以確保資料完整性：

- *背景驗證*會自動執行、持續檢查物件資料的正確性。

  背景驗證會自動持續檢查所有儲存節點、以判斷複寫和銷毀編碼物件資料是否有毀損的複本。如果發現問題、StorageGRID 則此現象系統會自動嘗試從儲存在系統其他位置的複本中、更換毀損的物件資料。背景驗證不會在 Cloud Storage Pool 中的物件上執行。

  > 如果系統偵測到無法自動修正的毀損物件、就會觸發 * 未識別的毀損物件 * 警示。

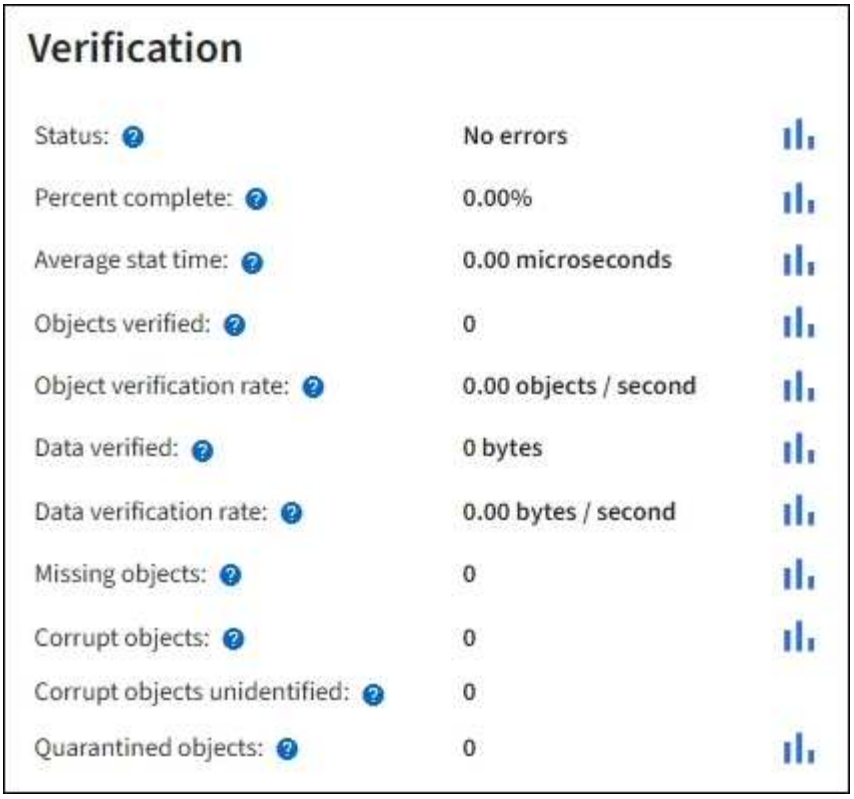
- *物件存在檢查*可由使用者觸發、以更快速地驗證物件資料的存在（雖然不正確）。

  物件存在檢查可驗證儲存節點上是否存在所有預期的物件複本和銷毀編碼片段。物件存在檢查提供驗證儲存裝置完整性的方法、尤其是最近發生的硬體問題可能會影響資料完整性時。

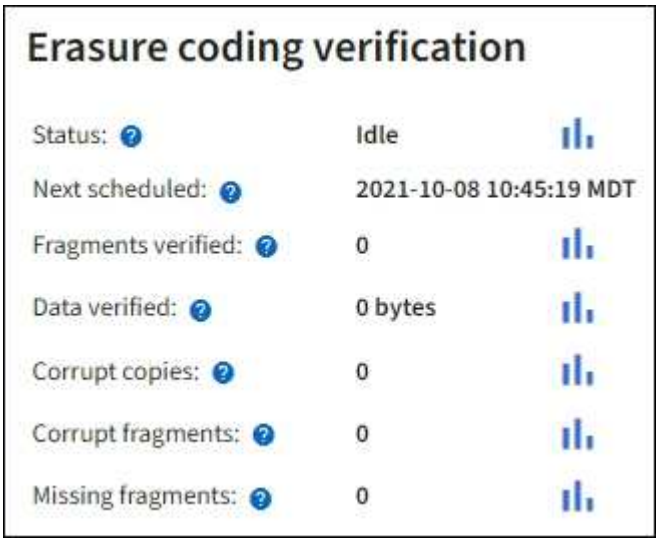
您應該定期檢閱背景驗證和物件存在檢查的結果。立即調查任何毀損或遺失物件資料的執行個體、以判斷根本原因。

步驟

1. 檢閱背景驗證的結果：
   a. 選擇*節點* > 儲存節點 > 物件。
   b. 檢查驗證結果：
      - 若要檢查複寫的物件資料驗證、請查看「驗證」區段中的屬性。

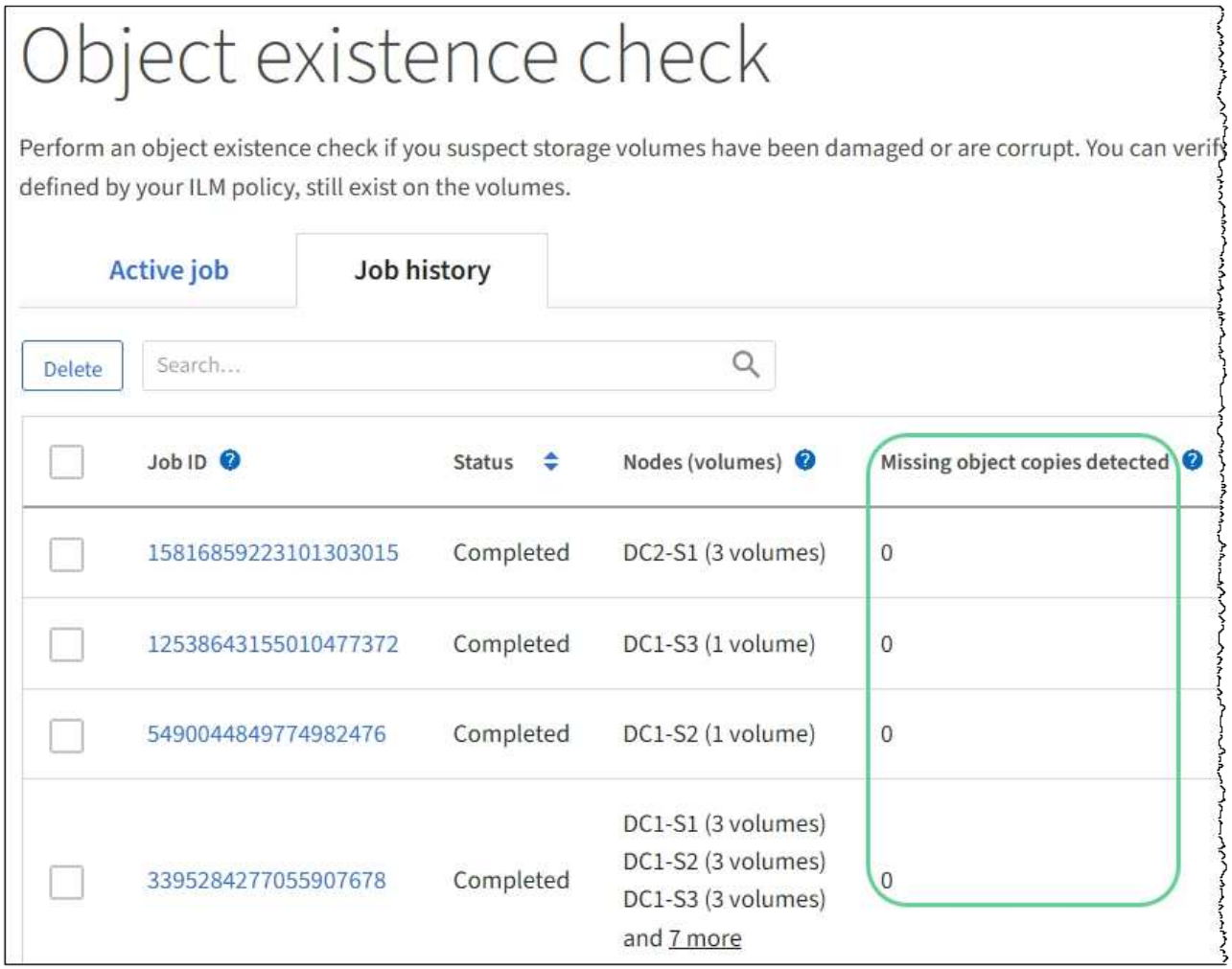


- 若要檢查以銷毀編碼的片段驗證、請選取「儲存節點_>* ILM *」、然後查看「刪除編碼驗證」區段中的屬性。



選擇屬性名稱旁的問號 (?) 即可顯示說明文字。

2. 檢閱物件存在檢查工作的結果：
   a. 選擇*維護* > 物件存在檢查 > 作業記錄。
   b. 掃描偵測到的缺失物件副本列。如果任何作業導致 100 個或更多物件副本遺失，並且觸發了「物件可能遺失」警報，請聯絡技術支援。



檢閱 **StorageGRID** 稽核訊息

稽核訊息可協助您更深入瞭解StorageGRID 您的作業系統的詳細操作。您可以使用稽核記錄來疑難排解問題、並評估效能。

在正常系統運作期間、所有StorageGRID 的支援服務都會產生稽核訊息、如下所示：

- 系統稽核訊息與稽核系統本身、網格節點狀態、全系統工作活動及服務備份作業有關。
- 物件儲存稽核訊息與StorageGRID 儲存及管理物件相關、包括物件儲存與擷取、網格節點對網格節點的傳輸及驗證。
- S3 用戶端應用程式要求建立、修改或擷取物件時、會記錄用戶端讀寫稽核訊息。
- 管理稽核訊息會記錄使用者對管理API的要求。

每個管理節點都會將稽核訊息儲存在文字檔中。稽核共用區包含使用中檔案（稽核記錄）、以及前幾天的壓縮稽核記錄。網格中的每個節點也會儲存節點上產生的稽核資訊複本。

您可以直接從管理節點的命令列存取稽核記錄檔。

StorageGRID 預設可以傳送稽核資訊、也可以變更目的地：

- StorageGRID 預設為本機節點稽核目的地。

- Grid Manager 和 Tenant Manager 稽核記錄項目可能會傳送至儲存節點。
- 您也可以變更稽核記錄的目的地、並將稽核資訊傳送至外部syslog伺服器。設定外部syslog伺服器時、仍會繼續產生及儲存稽核記錄的本機記錄。
- "了解有關配置日誌管理的信息" 。

如需稽核記錄檔、稽核訊息格式、稽核訊息類型及分析稽核訊息可用工具的詳細資訊，請參閱"檢閱稽核記錄"。

收集 **StorageGRID** 日誌檔案和系統資料

您可以檢索StorageGRID日誌檔案和系統資料（包括設定資料），並將其傳送給技術支援。

開始之前

- 您已使用任意管理節點登入網格管理器"支援的網頁瀏覽器"。
- 您有 "特定存取權限"。

關於這項工作

使用網格管理器來收集"記錄檔"、系統資料和來自任何網格節點的您選擇的時間段的配置資料。資料被收集並歸檔在 `.tar.gz`然後您可以將其下載到本機電腦或傳送給技術支援。

或者，您可以變更稽核日誌的目標並將稽核資訊傳送至外部系統日誌伺服器。當設定外部系統日誌伺服器時，將繼續產生和儲存稽核記錄的本機日誌。看"設定日誌管理和外部系統日誌伺服器" 。

如果用於啟動記錄收集的管理節點在記錄收集過程中離線，StorageGRID 將不會保留收集結果。您需要重新開機該節點，並在重新開機完成後重新啟動記錄收集。

步驟

1. 選擇*支援* > 工具 > 日誌收集。顯示節點表。
2. 選取您要收集記錄檔的網格節點。

   您可以按節點名稱、網站和節點類型進行排序。站點和節點類型列包含按單一站點和節點類型選擇的篩選器。

3. 選擇*繼續*。
4. 選擇要包含在日誌檔案中的資料的日期和時間範圍。

   如果您選擇很長的時間段或從大型網格中的所有節點收集日誌，則日誌存檔可能會變得太大而無法儲存在節點上，或者太大而無法由管理節點收集進行下載。如果發生任何一種情況，請使用較小的資料集重新開始日誌收集。

5. 選取您要收集的記錄類型。
   - 應用程式日誌：技術支援最常用於故障排除的應用程式特定日誌。收集的日誌是可用應用程式日誌的子集。
   - 稽核日誌：包含系統正常運作期間產生的稽核訊息的日誌。
   - 網路追蹤：用於網路偵錯的日誌。
   - **Prometheus** 資料庫：來自所有節點上的服務的時間序列指標。

6. 或者，使用 **Notes** 文字方塊輸入有關您正在收集的日誌檔案的註解。

   您可以使用這些附註、提供有關問題的技術支援資訊、以提示您收集記錄檔。您的筆記會新增至名為的檔案 `info.txt`、以及其他有關記錄檔集合的資訊。 `info.txt`檔案會儲存在記錄檔歸檔套件中。

7. 選擇*收集日誌*。

   您可以使用日誌收集頁面來監控每個網格節點的日誌檔案收集進度。

   如果您收到記錄大小的錯誤訊息、請嘗試收集較短時間內的記錄、或是收集較少節點的記錄。

8. 如果日誌收集失敗：

   - 如果出現「日誌收集失敗」訊息，您可以重試日誌收集或完成會話而無需重試。
   - 如果出現「日誌收集部分失敗」訊息，您可以重試日誌收集、完成會話、下載部分日誌檔案或將部分日誌檔案傳送至AutoSupport。

   > 您可以選擇將 Provisioning 密碼欄位留空以進行標準重試，或者輸入密碼以使用 SSH 進行重試。

9. 當日誌檔案收集完成：

   - 選擇*下載*下載 `.tar.gz`文件。
   - 選擇“發送至AutoSupport”以發送 `.tar.gz`文件發送給技術支援。

     這 `.tar.gz`檔案包含所有成功收集日誌的網格節點的所有日誌檔案。合併後的 `.tar.gz`檔案包含每個網格節點的一個日誌檔案存檔。

   AutoSupport軟體套件的主題是 `USER_TRIGGERED_SUPPORT_BUNDLE`。

10. 選擇*完成*。

    > 這 `.tar.gz`當您選擇*完成*時，檔案將被刪除。請確保您先下載或傳送該檔案。

檢閱 **StorageGRID** 支援指標

疑難排解問題時、您可以與技術支援部門合作、檢閱StorageGRID 有關您的整套系統的詳細指標和圖表。

開始之前

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

關於這項工作

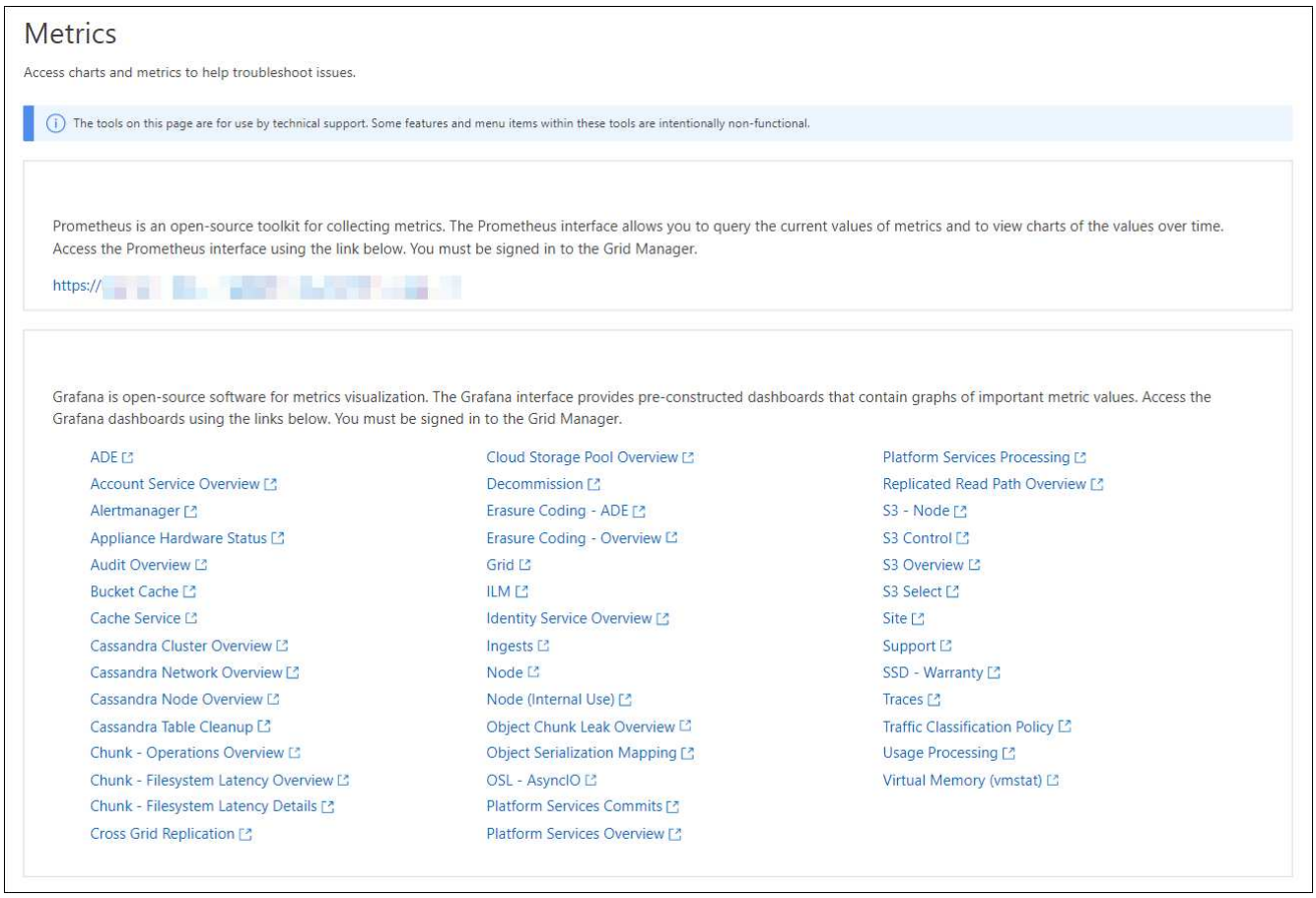
「指標」頁面可讓您存取Prometheus和Grafana使用者介面。Prometheus是開放原始碼軟體、可用來收集指標。Grafana是開放原始碼軟體、可用於指標視覺化。

「指標」頁面上提供的工具僅供技術支援使用。這些工具中的某些功能和功能表項目會刻意無法運作、而且可能會有所變更。請參閱清單"常用的Prometheus指標"。

步驟

1. 依照技術支援的指示，選擇 支援 > 工具 > 指標。

   此處顯示「指標」頁面的範例：



2. 若要查詢 StorageGRID 計量的目前值並檢視這些值隨時間變化的圖表，請選擇 Prometheus 部分中的連結。

   隨即顯示Prometheus介面。您可以使用此介面來執行有關可用StorageGRID 的版本資訊指標的查詢、StorageGRID 並在一段時間內繪製各種版本的資訊。

   名稱中包含_Private的指標僅供內部使用、StorageGRID 可能會在不另行通知的情況下於各個版本之間變更。

3. 若要存取包含 StorageGRID 計量隨時間變化圖表的預先建置儀表板，請選擇 Grafana 區段中的連結。

   此時會出現所選連結的Grafana介面。

變更 **StorageGRID** 中的 **I/O** 優先順序

輸入/輸出 (I/O) 優先權可讓您變更網格上 I/O 操作的相對優先權。

預設情況下，客戶端 PUT 和 GET I/O 流量比清除擦除編碼 (EC) 資料和 EC 修復等後台活動具有最高優先權。透過提高清除擦除編碼 (EC) 資料和 EC 修復活動的優先級，這些任務可能會更快完成。 I/O 優先權變更的有效性受到客戶端請求率、網路流量波動和其他正在進行的網路任務的影響。

開始之前

- 查看 I/O 優先頁面，確定哪些選項可能會影響您的網格。
- 評估正在進行的客戶端流量是否可以安全地處理更長的等待時間或客戶端逾時。
- 準備好監控優先順序變化的影響並根據需要進行調整。這些變化實施得很快，但其效果可能需要幾個小時才能顯現。

步驟

1. 選擇*支援* > **I/O** 優先權。

2. （可選）將清除 EC 資料的後台操作的 EC 清除和修復優先順序從其預設值變更。

   對於具有基於 RAID 的節點的網格，使用預設的低 EC 清除和修復優先權。

3. 選擇*保存*。
4. 監控"指標"評估優先順序變化的影響。

在 **StorageGRID** 中執行診斷

疑難排解問題時、您可以與技術支援部門合作、在StorageGRID 您的故障排除系統上執行診斷、並檢閱結果。

- "檢視支援指標"
- "常用的Prometheus指標"

開始之前

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

關於這項工作

「診斷」頁面會針對網格的目前狀態執行一組診斷檢查。每項診斷檢查都有三種狀態之一：

- **Normal**：所有數值均在正常範圍內。
- **Attention**：一個或多個數值超出正常範圍。
- **Caution**：其中一個或多個數值明顯超出正常範圍。

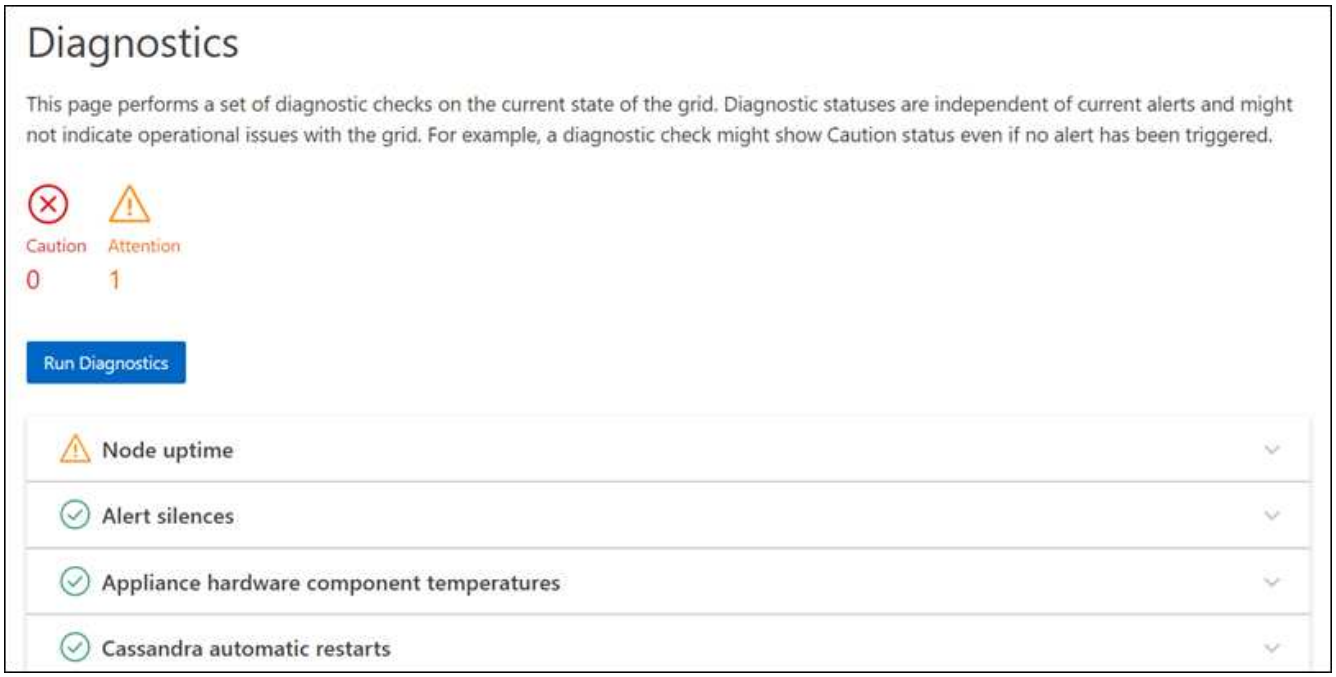
診斷狀態與目前警示無關、可能無法指出網格的作業問題。例如、即使未觸發警示、診斷檢查仍可能顯示「警示」狀態。

步驟

1. 選擇*支援* > 工具 > 診斷。

   「診斷」頁面隨即出現、並列出每項診斷檢查的結果。結果依嚴重性排序（注意、注意、然後正常）。在每個嚴重性範圍內、結果會依字母順序排序。

   在此範例中，一個診斷具有「注意」狀態，三個診斷具有「正常」狀態。



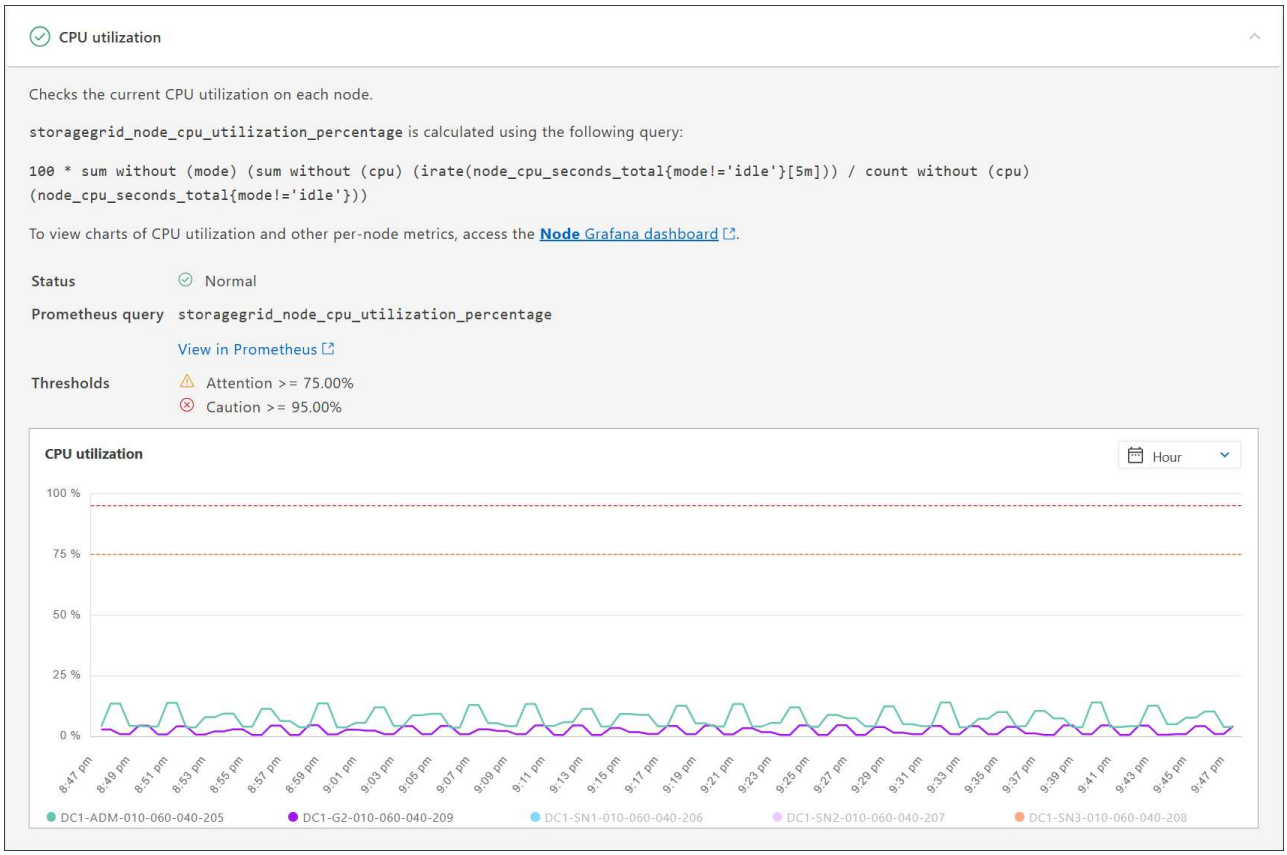
2. 若要深入瞭解特定診斷，請選取該列。

   將顯示診斷及其目前結果的詳細資料。下列為詳細資料：

   - 狀態：此診斷的目前狀態：正常、注意或注意。
   - * Prometheus query*：如果用於診斷、則用於產生狀態值的Prometheus運算式。（並非所有診斷都使用Prometheus運算式。）
   - 臨界值：如果可用於診斷、則每個異常診斷狀態的系統定義臨界值。（臨界值並非用於所有診斷。）

     您無法變更這些臨界值。

   - 狀態值：圖形和表格（螢幕截圖中未顯示表格）顯示整個StorageGRID系統的診斷狀態和值。在此範例中，顯示了StorageGRID系統中每個節點的目前 CPU 使用率。所有節點值均低於注意和警告閾值，因此診斷的整體狀態為正常。



3. 可選：若要查看與此診斷相關的 Grafana 圖表，請選擇 **Grafana** 儀表板。

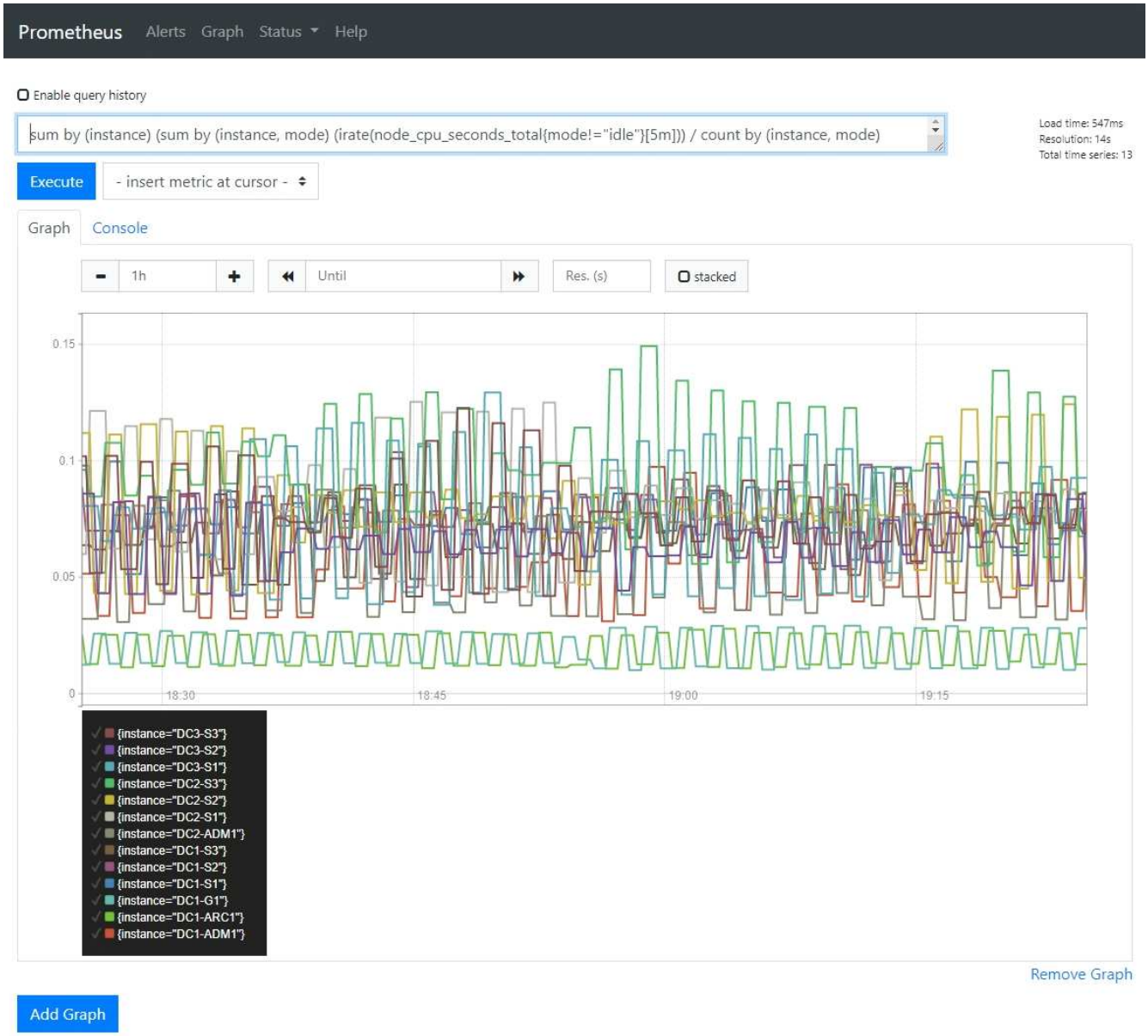
   並非所有診斷都會顯示此連結。

   出現相關的 Grafana 儀表板。在此範例中，節點儀表板顯示該節點隨時間變化的 CPU 使用率以及該節點的其他 Grafana 圖表。

   > 您也可以從 支援 > 工具 > 指標 頁面的 Grafana 部分存取預先建立的 Grafana 儀表板。

4. 選用：若要查看 Prometheus 表示式隨時間變化的圖表，請選擇 **View in Prometheus**。

   隨即顯示診斷所使用之運算式的Prometheus圖表。



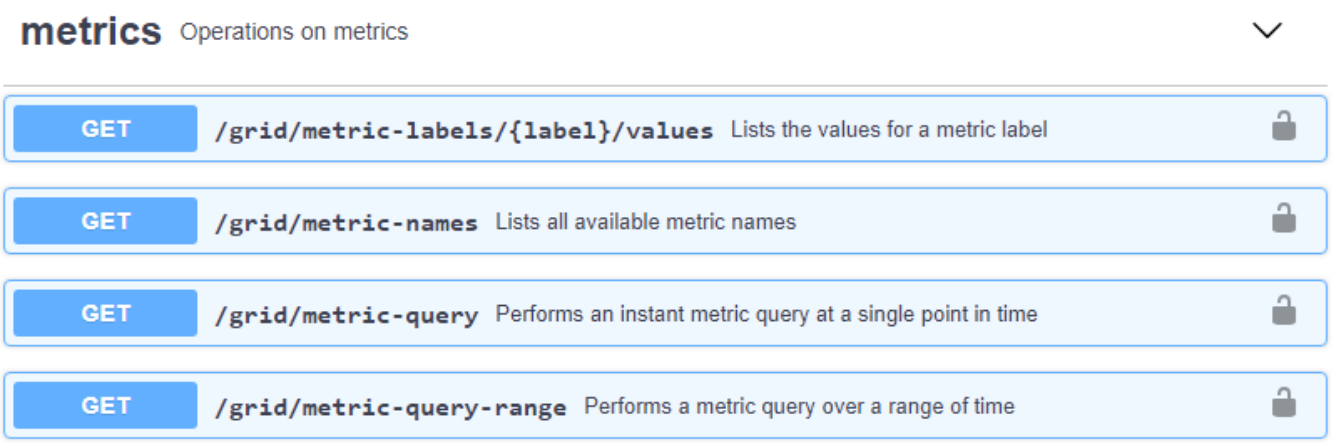
為 **StorageGRID** 建立自訂監控應用程式

您可以使用StorageGRID Grid Management API提供的功能表來建置自訂的監控應用程式和儀表板。

如果您想要監控 Grid Manager 現有頁面上未顯示的度量、或是想要為 StorageGRID 建立自訂儀表板、您可以使用 Grid Management API 來查詢 StorageGRID 度量。

您也可以使用外部監控工具（例如Grafana）直接存取Prometheus指標。使用外部工具時、您必須上傳或產生管理用戶端憑證StorageGRID 、才能讓驗證工具的安全性。請參閱"關於管理StorageGRID 功能的說明"。

若要查看指標 API 作業，包括可用指標的完整清單，請前往 Grid Manager。從頁面頂端選取說明圖示，然後選取 **API documentation** > **metrics**
。



如何實作自訂監控應用程式的詳細資料不在本文件的範圍之內。

疑難排解 StorageGRID 系統

疑難排解StorageGRID 作業系統

如果您在使用StorageGRID 無法修復的系統時遇到問題、請參閱本節中的秘訣與準則、以協助您判斷及解決問題。

您通常可以自行解決問題、但您可能需要將某些問題提報給技術支援部門。

定義問題

解決問題的第一步是清楚定義問題。

下表提供定義問題時可能收集的資訊類型範例：

問題	回應範例
什麼是不執行的功能？StorageGRID其症狀為何？	用戶端應用程式回報物件無法擷取至 StorageGRID 。
問題從何時開始？	在 2020 年 1 月 8 日約 14 ： 50 時、首次拒絕物件擷取。
您第一次注意到問題的方式為何？	用戶端應用程式通知。也收到警示電子郵件通知。
問題是否一致發生、或只是偶爾發生？	問題持續發生。
如果問題經常發生、會發生哪些步驟	每次用戶端嘗試擷取物件時都會發生問題。
如果問題間歇性發生、何時會發生？記錄您所察覺的每個事件的時間。	問題不是間歇性的。

問題	回應範例
您以前是否曾遇到過這個問題？您過去有多常發生此問題？	這是我第一次看到這個問題。

評估系統的風險與影響

在您定義問題之後、請評估問題對StorageGRID VMware系統的風險和影響。例如、關鍵警示的存在並不代表系統不提供核心服務。

下表摘要說明範例問題對系統作業的影響：

問題	回應範例
這個系統能否擷取內容？StorageGRID	不可以
用戶端應用程式可以擷取內容嗎？	有些物件可以擷取、有些則無法擷取。
資料是否有風險？	不可以
經營業務的能力是否受到嚴重影響？	是的、因為用戶端應用程式無法將物件儲存至StorageGRID 系統、因此無法一致地擷取資料。

收集資料

在您定義問題並評估其風險與影響之後、請收集資料以供分析。最適合收集的資料類型取決於問題的本質。

要收集的資料類型	為何要收集此資料	說明
建立最近變更的時間表	變更您的系統、其組態或環境可能會導致新的行為。StorageGRID	• 建立最近變更的時間表
檢閱警示	警示可針對可能造成問題的潛在問題提供重要線索、協助您快速判斷問題的根本原因。 檢閱目前警示清單、查看 StorageGRID 是否已識別出問題的根本原因。 檢閱過去觸發的警示、以取得更多洞見。	• "檢視目前和已解決的警示"
建立基準	收集各種作業值的正常層級資訊。這些基準值和偏離這些基準值、可提供寶貴的線索。	• 建立基準
執行擷取和擷取測試	若要疑難排解擷取和擷取的效能問題、請使用工作站來儲存和擷取物件。比較使用用戶端應用程式時的結果。	• "監控成效、獲得效能"

要收集的資料類型	為何要收集此資料	說明
檢閱稽核訊息	檢閱稽核訊息StorageGRID 以詳細追蹤各項功能。稽核訊息中的詳細資料可用於疑難排解許多類型的問題、包括效能問題。	• "檢閱稽核訊息"
檢查物件位置和儲存設備完整性	如果您遇到儲存問題、請確認物件放置在您預期的位置。檢查儲存節點上物件資料的完整性。	• "監控物件驗證作業" • "確認物件資料位置" • "驗證物件完整性"
收集技術支援資料	技術支援可能會要求您收集資料或檢閱特定資訊、以協助疑難排解問題。	• "收集記錄檔和系統資料" • "手動觸發 AutoSupport 套件" • "檢視支援指標"

建立最近變更的時間表

發生問題時、您應該考慮最近發生的變更、以及變更發生的時間。

- 變更您的系統、其組態或環境可能會導致新的行為。StorageGRID
- 變更時間表可協助您找出可能導致問題的變更、以及每項變更可能如何影響問題的開發。

建立系統最近變更的表格、其中包含每項變更發生時間的相關資訊、以及變更的相關詳細資料、例如變更進行期間發生的其他事項：

改變時間	變更類型	詳細資料
例如： • 您何時開始恢復節點？ • 軟體升級何時完成？ • 您是否中斷此程序？	發生什麼事了？您是做什麼工作？	記錄變更的相關詳細資料。例如： • 網路變更的詳細資料。 • 安裝了哪個修補程式。 • 用戶端工作負載的變更方式。 請務必注意、是否同時發生多項變更。例如、升級進行期間是否進行此變更？

最近重大變更的範例

以下是一些可能發生重大變更的範例：

- 最近是否安裝、擴充或恢復了這個功能？StorageGRID
- 系統最近是否已升級？是否套用了修補程式？
- 最近是否有任何硬體已修復或變更？
- ILM原則是否已更新？

- 用戶端工作負載是否已變更？
- 用戶端應用程式或其行為是否有所變更？
- 您是否已變更負載平衡器、或新增或移除管理節點或閘道節點的高可用度群組？
- 是否有任何可能需要很長時間才能完成的工作？範例包括：
  - 恢復故障的儲存節點
  - 儲存節點汰換
- 是否已對使用者驗證進行任何變更、例如新增租戶或變更LDAP組態？
- 資料移轉是否正在進行？
- 平台服務最近是否啟用或變更？
- 最近是否啟用法規遵循？
- 是否已新增或移除雲端儲存池？
- 儲存壓縮或加密是否有任何變更？
- 網路基礎架構是否有任何變更？例如、VLAN、路由器或DNS。
- NTP來源是否有任何變更？
- Grid、管理或用戶端網路介面是否有任何變更？
- 是否對StorageGRID 此系統或其環境進行任何其他變更？

建立基準

您可以記錄各種作業值的正常層級、為系統建立基準。未來您可以比較目前值與這些基準、以協助偵測並解決異常值。

屬性	價值	如何取得
平均儲存使用量	每天消耗GB 每日使用百分比	前往Grid Manager。在「節點」頁面上、選取整個網格或站台、然後前往「儲存」索引標籤。 在「使用的儲存設備-物件資料」圖表中、找出該行相當穩定的期間。將游標放在圖表上、以預估每天使用多少儲存設備 您可以針對整個系統或特定資料中心收集此資訊。
平均中繼資料使用量	每天消耗GB 每日使用百分比	前往Grid Manager。在「節點」頁面上、選取整個網格或站台、然後前往「儲存」索引標籤。 在「使用的儲存設備-物件中繼資料」圖表中、找出該行相當穩定的期間。將游標放在圖表上、以估計每天使用多少中繼資料儲存設備 您可以針對整個系統或特定資料中心收集此資訊。

屬性	價值	如何取得
S3 操作速率	作業/秒	在網格管理器儀表板上，選擇*效能*>*儲存節點的 S3 操作*。 若要查看特定網站或節點的擷取和檢索速率和計數，請選擇 **Nodes** > ***site*** 或 ***Storage Node*** > **Objects**。將遊標放在 S3 攝取和檢索圖表上。
ILM評估率	物件數/秒	從「節點」頁面選取「網格_>* ILM *」。 在ILM佇列圖表中、找出線路相當穩定的期間。將游標放在圖表上、以預估系統 * 評估率 * 的基準值。
ILM掃描率	物件數/秒	選擇 **Nodes** > ***grid*** > **ILM**。 在ILM佇列圖表中、找出線路相當穩定的期間。將游標放在圖表上、以預估系統 * 掃描速率 * 的基準值。
從用戶端作業排入佇列的物件	物件數/秒	選擇 **Nodes** > ***grid*** > **ILM**。 在ILM佇列圖表中、找出線路相當穩定的期間。將游標放在圖表上、以預估系統的 * 物件佇列（從用戶端作業） * 的基準值。
平均查詢延遲	毫秒	選擇*節點* > 儲存節點 > 物件。在查詢表中，查看平均延遲的值。

分析資料

請使用您收集的資訊來判斷問題的原因和可能的解決方案。

分析是問題相依的、但一般而言：

- 使用警示找出故障點和瓶頸。
- 使用警示記錄和圖表來重建問題歷程記錄。
- 使用圖表找出異常狀況、並將問題情況與正常作業進行比較。

提報資訊檢查清單

如果您無法自行解決問題、請聯絡技術支援部門。聯絡技術支援人員之前、請先收集下表所列的資訊、以利解決問題。

✔	項目	附註
	問題陳述	問題症狀為何？問題從何時開始？是否持續或間歇性發生？如果是間歇性的、發生的時間為何？ 定義問題
	影響評估	問題的嚴重性為何？對用戶端應用程式有何影響？ • 用戶端之前是否已成功連線？ • 用戶端是否可以擷取、擷取及刪除資料？
	系統ID StorageGRID	選擇*維護* > 系統 > 許可證。 StorageGRID系統 ID 顯示為目前授權的一部分。
	軟體版本	從Grid Manager頂端、選取說明圖示、然後選取*關於*以查看StorageGRID 此版本。
	自訂	概述StorageGRID 如何設定您的系統。例如、請列出下列項目： • 網格是否使用儲存壓縮、儲存加密或法規遵循？ • ILM 是否會建立複寫或刪除編碼的物件？ILM是否確保站台備援？ILM 規則是否使用平衡、嚴格或雙重承諾擷取行為？
	記錄檔和系統資料	收集系統的日誌檔案和系統資料。選擇*支援* > 工具 > 日誌收集。 您可以收集整個網格或所選節點的記錄。 如果您僅收集選定節點的日誌，請確保至少包含一個具有 ADC 服務的儲存節點。站點安裝的前三個儲存節點包括 ADC 服務。
	基礎資訊	收集有關擷取作業、擷取作業和儲存使用量的基礎資訊。 建立基準
	最近變更的時間表	建立時間軸、摘要說明系統或其環境最近的任何變更。 建立最近變更的時間表
	診斷問題的歷史記錄	如果您已自行診斷或疑難排解問題、請務必記錄您所採取的步驟和結果。

疑難排解物件和儲存問題

確認 StorageGRID 中的物件資料位置

視問題而定"確認物件資料的儲存位置"、您可能會想要。例如、您可能想要驗證ILM原則是否如預期般執行、而且物件資料是否儲存在預期的位置。

開始之前

- 您必須擁有物件識別碼、可以是：
  - * UUID *：物件的通用唯一識別碼。輸入全大寫的UUID。
  - * CBID*：StorageGRID 物件在功能區內的唯一識別碼。您可以從稽核記錄取得物件的CBID。輸入全大寫的CBID。
  - *S3 貯體與物件金鑰 * ：當物件透過擷取"S3 介面"時、用戶端應用程式會使用貯體與物件金鑰組合來儲存及識別物件。

步驟

1. 選取* ILM >*物件中繼資料查詢。
2. 在*識別碼*欄位中輸入物件的識別碼。

   您可以輸入 UUID、CBID 或 S3 bucket/object-key。

3. 如果您要查詢物件的特定版本、請輸入版本ID（選用）。

4. 選擇*查詢*。

   "物件中繼資料查詢結果"隨即出現。本頁列出下列資訊類型：

   - 系統中繼資料、包括物件ID（UUID）、版本ID（選用）、物件名稱、容器名稱、租戶帳戶名稱或ID、物件的邏輯大小、第一次建立物件的日期和時間、以及上次修改物件的日期和時間。
   - 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、包含區段識別碼和資料大小的物件區段清單。對於超過100個區段的物件、只會顯示前100個區段。
- 所有物件中繼資料均採用未處理的內部儲存格式。此原始中繼資料包含內部系統中繼資料、無法保證從發行到發行都會持續存在。

  下列範例顯示儲存為兩個複寫複本之S3測試物件的物件中繼資料查詢結果。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


了解 **StorageGRID** 中儲存磁碟區的物件存放區故障

儲存節點上的基礎儲存設備分為物件存放區。物件存放區也稱為儲存磁碟區。

您可以查看每個儲存節點的物件儲存資訊。選擇*節點* > 儲存節點 > 儲存。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	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
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

視故障的性質而定、儲存磁碟區的故障可能會反映在"儲存磁碟區警示"中。如果儲存磁碟區故障、您應該修復故障的儲存磁碟區、以便儘快將儲存節點還原為完整功能。如有必要、您可以移至 * 組態 * 索引標籤、"將儲存節點置於唯讀狀態"以便 StorageGRID 系統在準備伺服器的完整還原時、可以使用它來擷取資料。

驗證 **StorageGRID** 中物件資料的完整性

此系統可驗證儲存節點上物件資料的完整性、同時檢查毀損和遺失的物件。StorageGRID

驗證程序有兩種：背景驗證和物件存在檢查（先前稱為前景驗證）。他們共同合作、確保資料完整性。背景驗證會自動執行、並持續檢查物件資料的正確性。使用者可觸發物件存在檢查、以更快驗證物件的存在（雖然不正確）。

什麼是背景驗證？

背景驗證程序會自動持續檢查儲存節點是否有物件資料毀損的複本、並自動嘗試修復找到的任何問題。

背景驗證會檢查複寫物件和銷毀編碼物件的完整性、如下所示：

- 複寫物件：如果背景驗證程序找到毀損的複寫物件、則毀損的複本會從其位置移除、並隔離儲存節點上的其他位置。接著會產生新的未損毀複本、並將其放置在符合使用中 ILM 原則的位置。新複本可能不會放在原始複本所使用的儲存節點上。

  > 毀損的物件資料會被隔離、而非從系統中刪除、以便仍可存取。如需存取隔離物件資料的詳細資訊、請聯絡技術支援部門。

- 刪除編碼物件：如果背景驗證程序偵測到刪除編碼物件的片段毀損、StorageGRID 則會使用剩餘的資料和同位元檢查片段、自動嘗試在同一個儲存節點上重新建置遺失的片段。如果損壞的片段無法重建、則會嘗試擷取該物件的另一個複本。如果擷取成功、則會執行ILM評估、以建立銷毀編碼物件的替換複本。

  背景驗證程序僅會檢查儲存節點上的物件。它不會檢查 Cloud Storage Pool 中的物件。物件必須超過四天才能符合背景驗證資格。

背景驗證會以不干擾一般系統活動的持續速度執行。背景驗證無法停止。不過、您可以提高背景驗證率、以便在懷疑有問題時更快驗證儲存節點的內容。

與背景驗證相關的警示

如果系統偵測到毀損的物件無法自動修正（因為毀損會防止物件被識別）、就會觸發 * 未識別的毀損物件偵測 * 警示。

如果後台驗證無法取代損壞的對象，因為它無法找到另一個副本，則會觸發*對象可能會遺失*警報。

什麼是物件存在檢查？

物件存在檢查可驗證儲存節點上是否存在所有預期的物件複本和銷毀編碼片段。物件存在檢查不會驗證物件資料本身（背景驗證會驗證）、而是提供驗證儲存裝置完整性的方法、尤其是最近發生的硬體問題可能會影響資料完整性時。

與自動進行背景驗證不同、您必須手動啟動物件存在檢查工作。

物件存在檢查會讀取StorageGRID 儲存在物件中的每個物件的中繼資料、並驗證複寫的物件複本和銷毀編碼的物件片段是否存在。任何遺失的資料都會以下列方式處理：

- 複製的複本：如果缺少複製物件資料的複本、StorageGRID 則會自動嘗試從儲存在系統其他地方的複本中更換複本。儲存節點會透過ILM評估執行現有複本、以判斷此物件不再符合目前的ILM原則、因為缺少另一個複本。系統會產生並放置新的複本、以滿足系統的主動式 ILM 原則。此新複本可能不會放在儲存遺失複本的相同位置。
- 刪除編碼的片段：如果刪除編碼物件的片段遺失、StorageGRID 則會使用其餘的片段、自動嘗試在同一個儲存節點上重建遺失的片段。如果無法重建遺失的片段（因為遺失的片段太多）、 ILM 會嘗試尋找物件的另一個複本、以用於產生新的銷毀編碼片段。

執行物件存在檢查

您一次只能建立並執行一個物件存在檢查工作。當您建立工作時、請選取您要驗證的儲存節點和磁碟區。您也可以選取工作的一致性。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您已確保要檢查的儲存節點處於線上狀態。選擇*節點*來查看節點表。確保要檢查的節點的節點名稱旁邊沒有出現警報圖示。
- 您已確保下列程序*未*在您要檢查的節點上執行：
  - 網格擴充以新增儲存節點
  - 儲存節點取消委任
  - 恢復故障的儲存磁碟區
  - 恢復具有故障系統磁碟機的儲存節點
  - EC重新平衡
  - 應用裝置節點複製

物件存在檢查無法在這些程序進行期間提供實用資訊。

關於這項工作

根據網格中的物件數量、選取的儲存節點和磁碟區、以及選取的一致性、物件存在檢查工作可能需要數天或數週的時間才能完成。您一次只能執行一個工作、但可以同時選取多個儲存節點和磁碟區。

步驟

1. 選擇*維護* > 任務 > 物件存在檢查。
2. 選取*建立工作*。「建立物件存在檢查」工作精靈隨即出現。
3. 選取包含您要驗證之磁碟區的節點。若要選取所有線上節點、請選取欄標題中的 * 節點名稱 * 核取方塊。

   您可以依節點名稱或站台進行搜尋。

   您無法選取未連線至網格的節點。

4. 選擇*繼續*。
5. 為清單中的每個節點選取一或多個磁碟區。您可以使用儲存磁碟區編號或節點名稱來搜尋磁碟區。

   若要為您選取的每個節點選取所有磁碟區、請選取欄標題中的 * 儲存磁碟區 * 核取方塊。

6. 選擇*繼續*。
7. 選取工作的一致性。

   一致性決定物件中繼資料的複本數量、用於物件存在檢查。

   - * Strong站台*：單一站台的兩個中繼資料複本。
   - 強式全域：每個站台有兩份中繼資料複本。
   - * All（全部）*（預設）：每個站台的所有三個中繼資料複本。

     如需一致性的詳細資訊、請參閱精靈中的說明。

8. 選擇*繼續*。
9. 檢閱並驗證您的選擇。您可以選取*上一個*、移至精靈的上一個步驟、以更新您的選擇。

   物件存在檢查工作會產生並執行、直到發生下列其中一項：

   - 工作完成。
   - 您可以暫停或取消工作。您可以恢復已暫停的工作、但無法恢復已取消的工作。
   - 工作中斷。觸發*物件存在檢查已停止*警示。請遵循針對警示所指定的修正行動。
   - 工作失敗。觸發*物件存在檢查失敗*警示。請遵循針對警示所指定的修正行動。
   - 出現「服務無法使用」或「內部伺服器錯誤」訊息。一分鐘後、重新整理頁面以繼續監控工作。

     視需要、您可以離開「物件存在」檢查頁面、然後返回以繼續監控工作。

10. 當工作執行時、請檢視*作用中工作*索引標籤、並記下偵測到的遺失物件複本值。

    此值代表一或多個遺失片段的複寫物件和銷毀編碼物件的遺失複本總數。

    如果偵測到的遺失物件副本數量大於 100，則儲存節點的儲存可能有問題。

11. 工作完成後、請採取任何其他必要行動：
    - 如果偵測到的物件複本遺失為零、則找不到問題。無需採取任何行動。
    - 如果偵測到的遺失物件副本大於零且未觸發*物件可能遺失*警報，則系統已修正所有遺失的副本。驗證所有硬體問題是否都已修正，以防止將來對物件副本造成損壞。
    - 如果偵測到的遺失物件副本數大於零，並且觸發了*物件可能會遺失*警報，則資料完整性可能會受到影響。聯繫技術支援。
    - 您可以使用 grep 提取 LLST 審計訊息來調查可能遺失的物件副本： `grep LLST audit_file_name` 。

      此過程類似於"調查可能遺失的物品"，儘管你搜尋的是物件副本 `LLST`而不是 `OLST`。

12. 如果您為工作選擇了強式站台或強式全域一致性、請等待約三週的中繼資料一致性、然後再次在相同的磁碟區上重新執行工作。

    當執行此工作時、若有時間為工作中所含的節點和磁碟區達到中繼資料一致性、重新執行工作可能會清除錯誤回報的物件複本、或是在遺失時檢查其他物件複本。StorageGRID

a. 選擇*維護* > 物件存在檢查 > 作業記錄。
b. 判斷哪些工作已準備好要重新執行：
   i. 請查看*結束時間*欄、以判斷三週前執行的工作。
   ii. 對於這些工作、請掃描一致性控制欄、找出強站台或強全域。
c. 選中要重新運行的每個作業的複選框，然後選擇 **rerun** 。
d. 在重新執行工作精靈中、檢閱選取的節點和磁碟區、以及一致性。
e. 當您準備好重新執行工作時、請選取*重新執行*。

此時會出現作用中工作索引標籤。您選取的所有工作都會在強式站台的一致性上以單一工作的方式重新執行。「詳細資料」區段中的*相關工作*欄位會列出原始工作的工作ID。

解決 **StorageGRID** 中 **S3 PUT** 物件大小過大的警示

如果租戶嘗試執行超過 S3 大小上限 5 GiB 的非多部分 PutObject 作業、則會觸發 S3 「放置物件太大」警示。

開始之前

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

判斷哪些租戶使用大於 5 GiB 的物件、以便通知他們。

步驟

1. 前往*設定*>*監控*>*稽核和系統日誌伺服器*。
2. 如果用戶端寫入為正常、請存取稽核記錄：
   a. 輸入 `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
   e. 變更至稽核記錄所在的目錄。

      稽核記錄目錄和適用的節點取決於您的稽核目的地設定。

選項	目的地
本機節點（預設）	`/var/local/log/localaudit.log`

選項	目的地
管理節點 / 本機節點	• 管理節點（主要和非主要）：`/var/local/audit/export/audit.log` • 所有節點：`/var/local/log/localaudit.log`此模式中的檔案通常是空的或遺失的。
外部syslog伺服器	`/var/local/log/localaudit.log`

視稽核目的地設定而定，請輸入：`cd /var/local/log`或 `/var/local/audit/export/`

要了解更多信息，請參閱"選擇日誌位置"。

f. 識別哪些租戶使用的物件大於 5 GiB 。

i. 輸入 `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

ii. 針對結果中的每個稽核訊息、請查看 `S3AI`欄位以判斷租戶帳戶 ID 。使用訊息中的其他欄位來判斷用戶端、貯體和物件使用的 IP 位址：

程式碼	說明
SAIP	來源 IP
S3AI	租戶 ID
S3BK	鏟斗
S3KY	物件
CSIZ	大小（位元組）

▪ 稽核記錄結果範例 *

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):43332831798076591 19]]
```

3. 如果用戶端寫入不正常、請使用警示中的租戶 ID 來識別租戶：

   a. 前往*支援* > 工具 > 日誌收集。收集警報中儲存節點的應用程式日誌。指定警報前後 15 分鐘。請參閱"收集記錄檔和系統資料" 。

   b. 解壓縮檔案並移至 `bycast.log`：

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. 在記錄中搜尋 `method=PUT`、並在欄位中識別用戶端 `clientIP`。

      - 範例 bycast.log*

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. 告知租戶、 PutObject 的最大大小為 5 GiB 、並針對大於 5 GiB 的物件使用多部分上傳。
5. 如果應用程式已變更、請忽略警示一週。

疑難排解遺失和遺失的物件資料

了解 **StorageGRID** 中遺失和缺少的物件資料

物件可擷取的原因有多種、包括從用戶端應用程式讀取要求、複寫物件資料的背景驗證、ILM重新評估、以及在儲存節點還原期間還原物件資料。

StorageGRID系統使用物件元資料中的位置資訊來決定從哪個位置擷取物件。如果在預期位置未找到該物件的副本，系統將嘗試從系統的其他位置擷取該物件的另一個副本，假設 ILM 策略包含製作該物件的兩個或更多個副本的規則。

如果檢索成功， StorageGRID系統將取代該物件的遺失副本。否則，將觸發*物件可能遺失*警報，如下所示：

- 對於複寫的複本、如果無法擷取另一個複本、則物件會視為遺失、並觸發警示。
- 如果是以刪除方式編碼的複本、如果無法從預期位置擷取複本、則偵測到毀損的複本（ ECOR ）屬性會在嘗試從其他位置擷取複本之前遞增一次。如果找不到其他複本、則會觸發警示。

您應該立即調查所有*物件可能遺失*警報，以確定遺失的根本原因，並確定物件是否仍存在於離線或目前不可用的儲存節點中。看"調查可能遺失的物品" 。遺失物品警報可能會因謹慎而被錯誤觸發。

如果沒有副本的物件資料遺失，則沒有復原解決方案。但是，你必須"重置可能遺失的物件計數器"以防止已知遺失的物品掩蓋任何新的遺失物品。

解決 **StorageGRID** 中可能遺失物件的警示

當觸發「物體可能遺失」警報時，您必須立即進行調查。收集受影響對象的資訊並聯絡技術支援。

開始之前

- 您必須使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您必須擁有 `Passwords.txt`檔案。

關於這項工作

*物件可能遺失*警報表明，根據StorageGRID中的可用信息，網格中沒有物件的副本。資料可能已永久遺失。

立即調查遺失的物件警示。您可能需要採取行動、以避免進一步的資料遺失。在某些情況下、如果您採取提示行動、可能可以還原遺失的物件。

如果報告遺失的物品超過 10 件，請聯絡技術支援。請勿自行遵循此程序。

步驟

1. 選擇*節點*。
2. 選擇「儲存節點_>*物件*」。
3. 檢閱「物件數」表格中顯示的遺失物件數。

   此數字表示此網格節點偵測到整個StorageGRID 作業系統中遺失的物件總數。此值是在LDR和DDS服務中、資料儲存區元件遺失物件計數器的總和。

4. 從管理節點，"存取稽核記錄"確定觸發*物件可能遺失*警報的物件的唯一識別碼（UUID）：
   a. 登入網格節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。當您以 root 登入時、提示會從變更 `$`為 `#`。
   b. 變更至稽核記錄所在的目錄。

      稽核記錄目錄和適用的節點取決於您的稽核目的地設定。

選項	目的地
本機節點（預設）	`/var/local/log/localaudit.log`
管理節點 / 本機節點	• 管理節點（主要和非主要）： `/var/local/audit/export/audit.log` • 所有節點： `/var/local/log/localaudit.log`此模式中的檔案通常是空的或遺失的。
外部syslog伺服器	`/var/local/log/localaudit.log`

      視稽核目的地設定而定，請輸入： `cd /var/local/log`或 `/var/local/audit/export/`

要了解更多信息，請參閱"選擇日誌位置"。

c. 使用Grep擷取物件遺失（OLST）稽核訊息。輸入： `grep OLST audit_file_name`

d. 請注意訊息中包含的UUID值。

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. 使用 UUID 來查詢遺失物件的中繼資料：

a. 選取* ILM >*物件中繼資料查詢。

b. 輸入 UUID 、然後選取 * 查詢 * 。

c. 檢閱中繼資料中的位置、並採取適當的行動：

中繼資料	結論
找不到物件 <object_identifier>	如果未找到該對象，則傳回訊息「ERROR」：「」。 如果找不到該對象，重置可能遺失的物件計數器清除警報。缺少某個物件表示該物件被故意刪除。
位置> 0	如果輸出中列出了位置，則「物體可能遺失」警報可能是誤報。 確認物件存在。使用輸出中列出的節點ID和檔案路徑、確認物件檔案位於所列位置。 如果物體存在，重置可能遺失的物件計數器清除警報。
位置= 0	如果輸出中沒有列出位置，則該物件可能會遺失。聯繫技術支援。 技術支援可能會要求您確定是否存在正在進行的儲存設備恢復流程。請參閱： • "將物件資料還原至應用裝置的儲存磁碟區" • "將物件資料還原至系統磁碟機不受影響的儲存磁碟區" • "將物件資料還原至儲存磁碟區（系統磁碟機故障）"

6. 解決遺失物件問題後，請重設可能遺失的物件計數器，以確保警報不是誤報：

a. 選擇*節點*。

b. 選擇*_Storage Node_* > **Tasks**。

c. 在重置物件可能遺失計數器部分，選擇*重置*。

解決 **StorageGRID** 中的低物件資料儲存警示

「低物件資料儲存」警示會監控每個儲存節點上可用於儲存物件資料的空間。

開始之前

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

關於這項工作

當儲存節點上的複寫和刪除編碼物件資料總量符合警示規則中所設定的條件之一時、就會觸發 * 物件資料儲存不足 * 警示。

根據預設、當此條件評估為true時、會觸發重大警示：

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

在此情況下：

- `storagegrid_storage_utilization_data_bytes`是儲存節點複寫及刪除編碼物件資料總大小的估計值。
- `storagegrid_storage_utilization_usable_space_bytes`為儲存節點剩餘的物件儲存空間總量。

如果觸發重大或次要*低物件資料儲存*警示、您應該儘快執行擴充程序。

步驟

1. 選擇*警報* > 目前。

   「警示」頁面隨即出現。

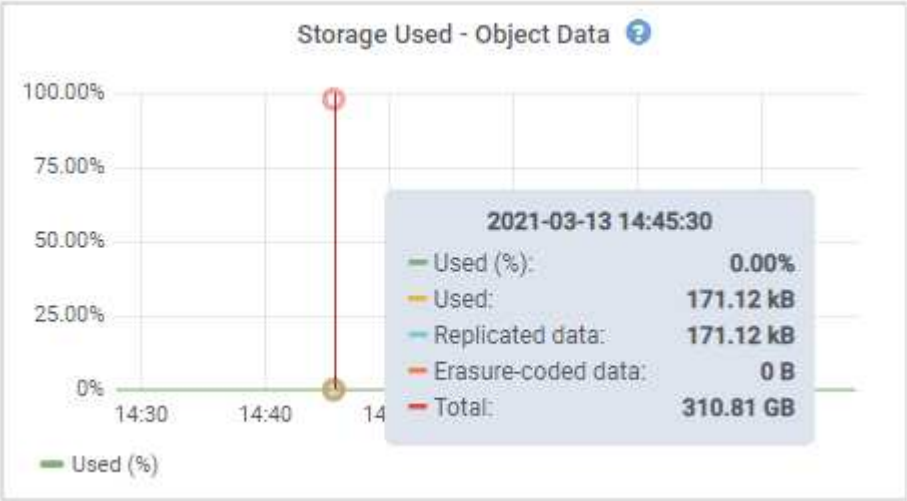
2. 從警示表中、展開*低物件資料儲存*警示群組（若有需要）、然後選取您要檢視的警示。

   選取警示、而非警示群組的標題。

3. 檢閱對話方塊中的詳細資料、並注意下列事項：
   - 觸發時間
   - 站台和節點的名稱
   - 此警示的度量目前值
4. 選擇 **Nodes** > ***Storage Node*** 或 ***Site*** > **Storage**。
5. 將游標放在「已使用的儲存空間 - 物件資料」圖表上。

顯示下列值：

- 已用（**%**）：已用於物件資料的總可用空間百分比。
- 已用：用於物件資料的總可用空間量。
- 複寫資料：此節點、站台或網格上的複寫物件資料量預估。
- 銷毀編碼資料：此節點、站台或網格上的銷毀編碼物件資料量預估。
- 總計：此節點、站台或網格上的可用空間總量。使用的值為 `storagegrid_storage_utilization_data_bytes`度量。



6. 選取圖表上方的時間控制項、以檢視不同時段的儲存使用情形。

   查看一段時間內的儲存使用情形、有助於瞭解警示觸發前後的儲存設備使用量、並可協助您預估節點剩餘空間可能需要多長時間才能充滿。

7. 請儘快"增加儲存容量"移至您的網格。

   您可以將儲存磁碟區（LUN）新增至現有的儲存節點、也可以新增儲存節點。

   如需更多資訊、請參閱 "管理完整儲存節點"。

解決 **StorageGRID** 中的浮水印覆寫警示

如果您使用儲存Volume浮點的自訂值、則可能需要解決*低唯讀浮點置換*警示。如果可能、您應該更新系統、以開始使用最佳化的值。

在之前的版本中、這三種"儲存Volume浮點"是通用設定和 #8212 ；同樣的值會套用至每個儲存節點上的每個儲存磁碟區。從供應到供應的供應功能中、軟體可根據儲存節點的大小和磁碟區的相對容量、針對每個儲存磁碟區最佳化這些浮點。StorageGRID

當您升級至 StorageGRID 11.6 或更高版本時、最佳化的唯讀和讀寫浮水印會自動套用至所有儲存磁碟區、除非下列任一項為真：

- 您的系統接近容量、如果套用最佳化的浮水印、就無法接受新資料。在此情況下、不會變更浮水印設定。StorageGRID

- 您先前已將任何儲存Volume浮點設為自訂值。無法使用最佳化的值覆寫自訂浮水印設定。StorageGRID不過、如果您的儲存 Volume 軟式唯讀浮水印自訂值太小、 StorageGRID 可能會觸發 * 低唯讀浮水印置換 * 警示。

瞭解警示

如果您將自訂值用於儲存Volume浮點、則可能會針對一個或多個儲存節點觸發*低唯讀浮點置換*警示。

警示的每個執行個體都表示儲存磁碟區軟式唯讀浮水印的自訂值小於該儲存節點的最小最佳化值。如果您繼續使用自訂設定、儲存節點可能會在極低的空間中執行、然後才能安全地轉換至唯讀狀態。當節點達到容量時、部分儲存磁碟區可能無法存取（自動卸載）。

例如、假設您先前已將儲存磁碟區的軟式唯讀浮水印設為 5 GB 。現在假設StorageGRID 、針對儲存節點A中的四個儲存磁碟區、已計算出下列最佳化值：

Volume 0.	12GB
Volume 1.	12GB
Volume 2.	11GB
Volume 3.	15GB

儲存節點A會觸發*低唯讀浮水印overroverride *警示、因為您的自訂浮水印（5 GB）小於該節點中所有磁碟區的最小最佳化值（11 GB）。如果您繼續使用自訂設定、節點可能會在極低的空間中執行、然後才能安全地轉換至唯讀狀態。

解決警示

如果觸發了一或多個*低唯讀浮水印置換*警示、請遵循下列步驟。如果您目前使用自訂浮水印設定、而且想要開始使用最佳化設定、即使沒有觸發警示、也可以使用這些指示。

開始之前

- 您已完成 StorageGRID 11.6 或更新版本的升級。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限"。

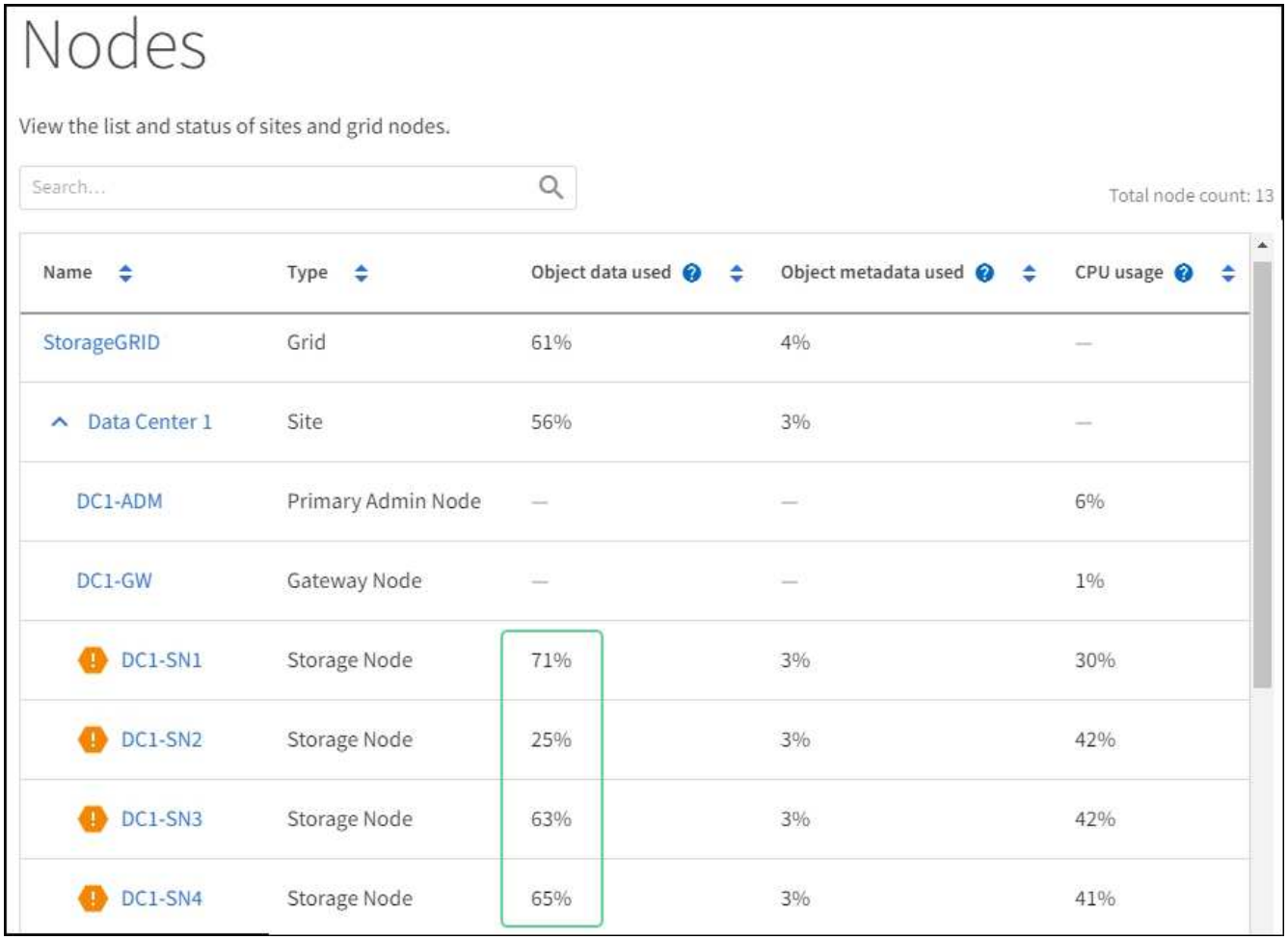
關於這項工作

您可以將自訂浮水印設定更新為新的浮水印覆寫、以解決*低唯讀浮水印覆寫*警示。不過、如果一或多個儲存節點接近完整容量、或是您有特殊的ILM需求、您應該先檢視最佳化的儲存浮水印、然後判斷使用它們是否安全。

評估整個網格的物件資料使用量

步驟

1. 選擇*節點*。
2. 針對網格中的每個站台、展開節點清單。
3. 檢閱每個站台之每個儲存節點的「物件資料已使用」欄中所顯示的百分比值。



4. 請遵循適當步驟：

   a. 如果所有的儲存節點都未接近完整（例如、所有*使用的物件資料*值都低於80%）、您可以開始使用置換設定。前往 使用最佳化的浮水印。

   b. 如果 ILM 規則使用嚴格的擷取行為、或是特定的儲存集區即將滿、請執行和中的步驟檢視最佳化的儲存浮水印判斷您是否可以使用最佳化的浮水印。

[[view-優 化浮水印]] 檢視最佳化的儲存浮水印

StorageGRID 使用兩個 Prometheus 指標來顯示其針對儲存 Volume 軟唯讀浮水印所計算的最佳化值。您可以檢視網格中每個儲存節點的最小和最大最佳化值。

步驟

1. 選擇*支援* > 工具 > 指標。
2. 在Prometheus區段中、選取連結以存取Prometheus使用者介面。
3. 若要查看建議的最小軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*執行*：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後一欄顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印最小最佳化值。如果此值大於儲存磁碟區軟唯讀浮水印的自訂設定、則會針對儲存節點觸發 * 低唯讀浮水印置換 * 警示。

4. 若要查看建議的最大軟式唯讀浮水印、請輸入下列Prometheus指標、然後選取*執行*：

`storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark`

最後一欄顯示每個儲存節點上所有儲存磁碟區的軟唯讀浮水印最大最佳化值。

5. [[maximized_value]請注意每個儲存節點的最大最佳化值。

[[determine 最佳化的浮水印 **]]** 判斷您是否可以使用最佳化的浮水印

步驟

1. 選擇*節點*。
2. 針對每個線上儲存節點重複這些步驟：
   a. 選擇「儲存節點_>*儲存設備*」。
   b. 向下捲動至物件存放區表格。
   c. 比較每個物件存放區（Volume）的*可用*值、以及您針對該儲存節點所記錄的最佳化浮水印上限。
3. 如果每個線上儲存節點上至少有一個磁碟區的可用空間超過該節點的最佳化浮水印上限、請前往使用最佳化的浮水印開始使用最佳化的浮水印。

   否則、請盡快展開網格。或"新增儲存磁碟區""新增儲存節點"移至現有節點或。然後、前往使用最佳化的浮水印更新浮水印設定。

4. 如果您需要繼續使用儲存 Volume 浮水印的自訂值、"靜音"或 "停用"* 低唯讀浮水印置換 * 警示。

> ⓘ 每個儲存節點上的每個儲存磁碟區都會套用相同的自訂浮水印值。如果將小於建議值的儲存Volume浮點用於儲存磁碟區、則當節點達到容量時、可能會導致部分儲存磁碟區無法存取（自動卸載）。

[[use-最佳 化浮水印 **]]** 使用最佳化的浮水印

步驟

1. 前往*支援* > 其他 > 儲存浮水印。
2. 選中 * 使用優化值 * 複選框。
3. 選擇*保存*。

根據儲存節點的大小和Volume的相對容量、每個儲存Volume的最佳化儲存Volume浮水印設定現在都有效。

疑難排解 StorageGRID 中的中繼資料問題

如果發生中繼資料問題、警示會通知您問題的來源、以及建議採取的行動。尤其是、如果觸發低中繼資料儲存警示、您必須新增儲存節點。

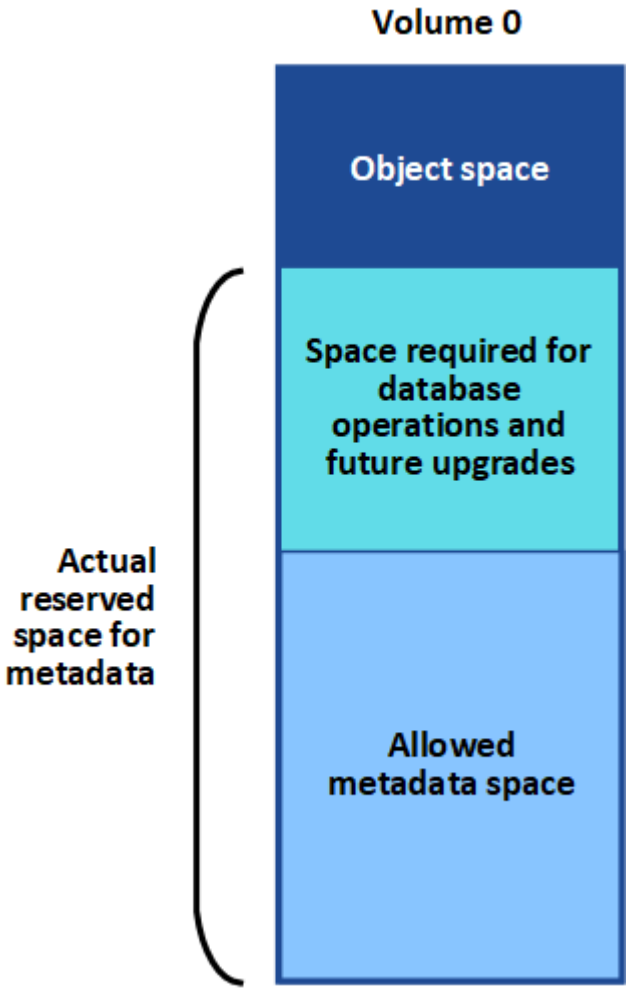
開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

關於這項工作

針對觸發的每個中繼資料相關警示、請遵循建議的動作。如果觸發*低中繼資料儲存*警示、您必須新增儲存節點。

針對物件中繼資料、在每個儲存節點的Volume 0上保留一定的空間量。StorageGRID此空間稱為 _ 實際保留空間 _ 、可細分為物件中繼資料（允許的中繼資料空間）所允許的空間、以及關鍵資料庫作業（例如壓縮和修復）所需的空間。允許的中繼資料空間可控制整體物件容量。



如果物件中繼資料佔用的空間超過中繼資料所允許的 100% 、資料庫作業就無法有效執行、而且會發生錯誤。

您可以"監控每個儲存節點的物件中繼資料容量"協助您預測錯誤、並在錯誤發生之前加以修正。

下列Prometheus指標可用來測量允許的中繼資料空間是否已滿：StorageGRID

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

當此Prometheus運算式達到特定臨界值時、會觸發*低中繼資料儲存*警示。

- 次要：物件中繼資料使用70%以上的中繼資料空間。您應該盡快新增儲存節點。
- 主要：物件中繼資料使用90%以上的允許中繼資料空間。您必須立即新增儲存節點。

> 當物件中繼資料使用 90% 以上的允許中繼資料空間時、儀表板上會出現警告。如果出現此警告、您必須立即新增儲存節點。您絕不能允許物件中繼資料使用超過100%的允許空間。

- 重大：物件中繼資料使用100%以上的允許中繼資料空間、開始耗用必要資料庫作業所需的空間。您必須停止擷取新物件、而且必須立即新增儲存節點。

> 如果Volume 0的大小小於中繼資料保留空間儲存選項（例如、在非正式作業環境中）、則*低中繼資料儲存*警示的計算可能不準確。

步驟

1. 選擇*警報* > 目前。
2. 如有需要、請從警示表中展開*低中繼資料儲存*警示群組、然後選取您要檢視的特定警示。
3. 檢閱警示對話方塊中的詳細資料。
4. 如果已觸發重大或重大*低中繼資料儲存*警示、請執行擴充以立即新增儲存節點。

> 由於整個網格的中繼資料容量受限於最小網站的中繼資料容量、因此整個網格的所有物件中繼資料複本都會保留在每個網站上。StorageGRID如果您需要將中繼資料容量新增至單一站台、則也應該"展開任何其他站台"使用相同數量的儲存節點。

執行擴充之後StorageGRID 、將現有的物件中繼資料重新散佈到新節點、以增加網格的整體中繼資料容量。不需要使用者採取任何行動。*低中繼資料儲存*警示已清除。

疑難排解 **StorageGRID** 中的憑證錯誤

當您嘗試使用網頁瀏覽器、 S3 用戶端或外部監控工具連線至 StorageGRID 時、如果發現安全性或憑證問題、您應該檢查憑證。

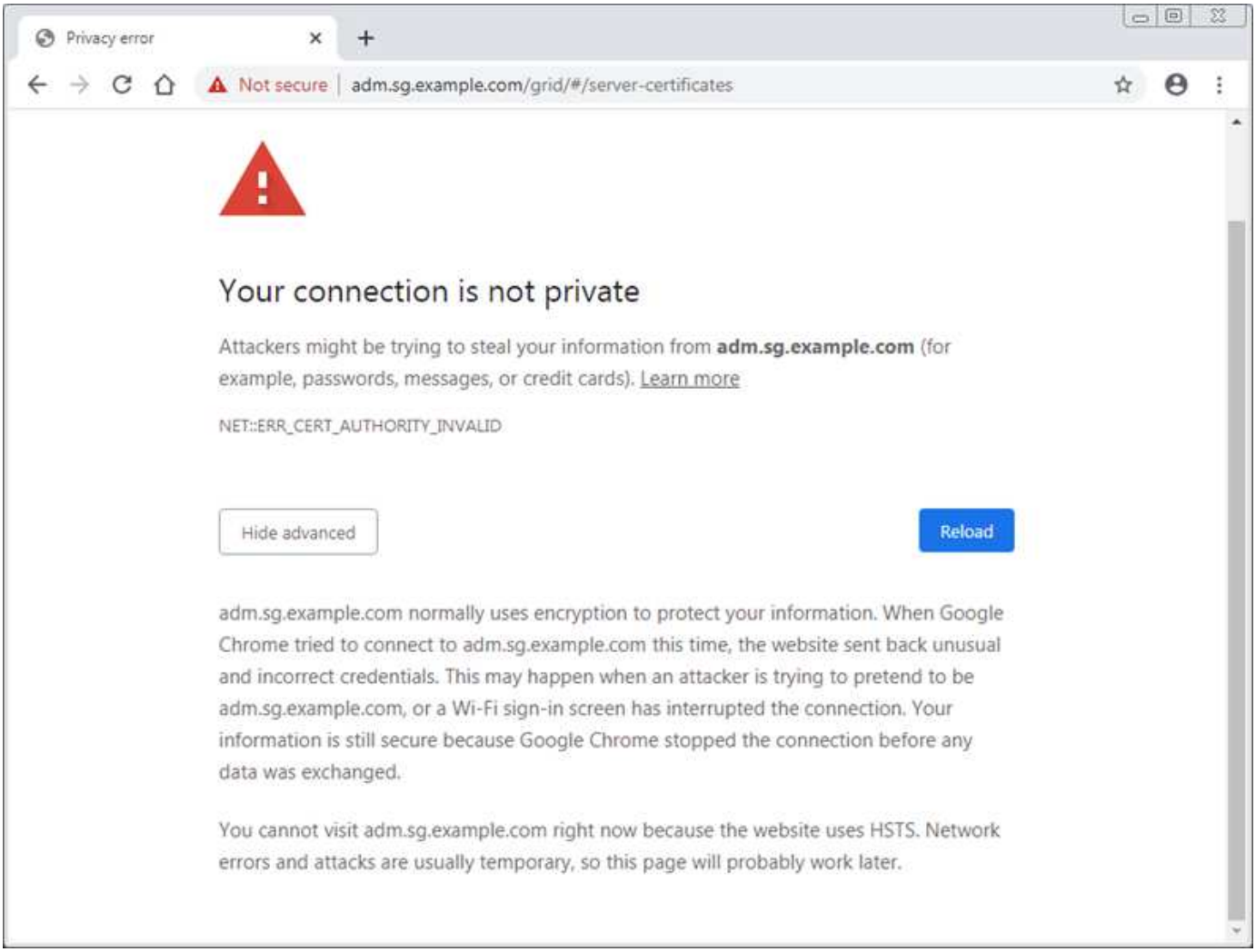
關於這項工作

當您嘗試StorageGRID 使用Grid Manager、Grid Management API、Tenant Manager或租戶管理API連線至功能時、憑證錯誤可能會造成問題。當您嘗試使用 S3 用戶端或外部監控工具連線時、也可能發生憑證錯誤。

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。
- 您可以從自訂管理介面憑證還原為預設的伺服器憑證。

下列範例顯示自訂管理介面憑證過期時的憑證錯誤：



為確保作業不會因伺服器憑證故障而中斷、當伺服器憑證即將過期時、就會觸發 * 管理介面伺服器憑證過期 * 警示。

當您使用用戶端憑證進行外部Prometheus整合時、憑證錯誤可能是StorageGRID 由該管理介面憑證或用戶端憑證所造成。用戶端憑證即將到期時、會觸發「憑證」頁面*警示上設定的用戶端憑證過期。

步驟

如果您收到有關證書過期的警報通知，請訪問證書詳細資訊：。選擇 設定 > 安全 > 憑證，然後"選取適當的憑證索引標籤"。

1. 檢查憑證的有效期間。+ 部分網頁瀏覽器和 S3 用戶端不接受有效期超過 398 天的憑證。
2. 如果憑證已過期或即將到期、請上傳或產生新的憑證。
   - 如需伺服器憑證，請參閱的步驟"為Grid Manager和Tenant Manager設定自訂伺服器憑證"。
   - 如需用戶端憑證，請參閱的步驟"設定用戶端憑證"。
3. 若為伺服器憑證錯誤、請嘗試下列任一或兩個選項：
   - 確認已填入憑證的主體替代名稱（SAN）、且SAN符合您要連線之節點的IP位址或主機名稱。
   - 如果您嘗試StorageGRID 使用網域名稱連線到IsName：
     i. 輸入管理節點的IP位址、而非網域名稱、以略過連線錯誤並存取Grid Manager。

ii. 從網格管理器中，選擇 配置 > 安全性 > 證書，然後"選取適當的憑證索引標籤"安裝新的自訂憑證或繼續使用預設憑證。

iii. 在管理 StorageGRID 的說明中，請參閱的步驟"為Grid Manager和Tenant Manager設定自訂伺服器憑證"。

疑難排解 **StorageGRID** 中的管理節點和使用者介面問題

您可以執行數項工作、以協助判斷與管理節點和 StorageGRID 使用者介面相關的問題來源。

管理節點登入錯誤

如果您在登入 StorageGRID 管理節點時遇到錯誤、系統可能會發生"網路"或 "硬體"問題、"管理節點服務"或是"Cassandra 資料庫問題"連線儲存節點上的問題。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有 `Passwords.txt`檔案。
- 您有 "特定存取權限"。

關於這項工作

如果您在嘗試登入管理節點時看到下列任一錯誤訊息、請使用這些疑難排解準則：

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

步驟

1. 等待10分鐘、然後再次嘗試登入。

   如果錯誤未自動解決、請前往下一步。

2. 如果您的 StorageGRID 系統有多個管理節點、請嘗試從另一個管理節點登入 Grid Manager 、以檢查無法使用的管理節點狀態。

   - 如果您能夠登錄，您可以使用*儀表板*、節點、*警報*和*支援*選項來協助確定錯誤的原因。
   - 如果您只有一個管理節點、或仍無法登入、請前往下一步。

3. 判斷節點的硬體是否離線。

4. 如果您的 StorageGRID 系統已啟用單一登入 （SSO），請參閱使用 "OIDC" 或 "SAML" 設定 SSO。

   您可能需要暫時停用單一管理節點並重新啟用SSO、才能解決任何問題。

5. 判斷您使用的帳戶是否屬於聯盟使用者。

如果同盟使用者帳戶無法運作、請嘗試以本機使用者身分（例如root）登入Grid Manager。

- 如果本機使用者可以登入：
  i. 檢閱警示。
  ii. 選擇*配置* > 存取控制 > 身份聯合。
  iii. 選擇「測試連線」以驗證 LDAP 伺服器的連線設定。
  iv. 如果測試失敗、請解決任何組態錯誤。
- 如果本機使用者無法登入、而且您確信認證正確無誤、請前往下一步。

6. 使用安全外殼協定 (SSH) 登入管理節點：
   a. 輸入下列命令： `ssh admin@Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

7. 檢視網格節點上執行的所有服務狀態： `storagegrid-status`

   請確定NMS、MI、Ngin像 及管理API服務都在執行中。

   如果服務狀態變更、則會立即更新輸出。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. 確認 Nginx) 服務正在執行中 `# service nginx-gw status`
9. [[use_lumbjack_to_collect_logs] 使用 Lumbjack 來收集記錄： `# /usr/local/sbin/lumberjack.rb`

   如果過去發生驗證失敗、您可以使用—start和—end Lumberjack指令碼選項來指定適當的時間範圍。如需這些選項的詳細資訊、請使用lumberjack -h。

   對終端機的輸出會指出記錄歸檔已複製到何處。

10. [[Review_logs、start=10]檢閱下列記錄：
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`

11. 如果您無法識別管理節點的任何問題、請發出下列任一命令、以判斷在您站台上執行ADC服務的三個儲存節點的IP位址。一般而言、這是站台上安裝的前三個儲存節點。

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

管理節點會在驗證程序期間使用ADC服務。

12. 從管理節點、使用 ssh 使用您識別的 IP 位址登入每個 ADC 儲存節點。
13. 檢視網格節點上執行的所有服務狀態： `storagegrid-status`

請確定idnt, acct, Ngin像 和cassandra服務都在執行中。

14. 重複步驟使用Lumberjack收集記錄和檢閱記錄、檢閱儲存節點上的記錄。
15. 如果您無法解決問題、請聯絡技術支援部門。

將收集到的記錄提供給技術支援人員。另請參閱"記錄檔參考"。

使用者介面問題

在 StorageGRID 軟體升級之後、 Grid Manager 或 Tenant Manager 的使用者介面可能無法如預期般回應。

步驟

1. 請確定您使用的"支援的網頁瀏覽器"是。
2. 清除網頁瀏覽器快取。

清除快取會移除舊版StorageGRID 的更新資源、並允許使用者介面再次正確運作。如需相關指示、請參閱網頁瀏覽器的說明文件。

疑難排解 **StorageGRID** 中的網路、硬體和平台問題

您可以執行多項工作、以協助判斷StorageGRID 與故障有關的問題來源。

[[422-unprocessable-entity-errors]]
== 「 422 ：無法處理的實體」錯誤

錯誤 422 ：無法處理的實體可能會因不同原因而發生。請查看錯誤訊息、以判斷您的問題是由何種原因造成的。

如果您看到列出的錯誤訊息之一、請採取建議的行動。

錯誤訊息	根本原因與修正行動

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	如果您在使用Windows Active Directory（AD）設定身分識別聯盟時、選取「傳輸層安全性（TLS）」「不要使用**TLS**」選項、就可能會出現此訊息。
	
	不支援使用*「不使用TLS*」選項來搭配執行LDAP簽署的AD伺服器使用。您必須選取*使用ARTTLS*選項或*使用LDAPS*選項來使用TLS。

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	如果您嘗試使用不受支援的密碼、將傳輸層安全性（TLS）連線從StorageGRID 支援的內部系統、連接到用於識別聯盟或雲端儲存資源池的外部系統、則會出現此訊息。
	
	檢查外部系統提供的密碼。系統必須使用其中一種"StorageGRID 支援的密碼"進行外寄 TLS 連線、如管理 StorageGRID 的指示所示。

[[troubleshoot _MTU _alert]] Grid Network MTU 不相符警示

當Grid Network介面（eth0）的最大傳輸單位（MTU）設定在網格中的各個節點之間大幅不同時、就會觸發* Grid Network MTU mismis*警示。

關於這項工作

MTU設定的差異可能代表部分（但並非全部）eth0網路已設定為使用巨型框架。MTU大小不相符的值大於1000、可能會導致網路效能問題。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 列出所有節點上eth0的MTU設定。
   - 使用Grid Manager中提供的查詢。
   - 瀏覽 *primary Admin Node IP address*`/metrics/graph`並輸入下列查詢：`node_network_mtu_bytes{device="eth0"}`
3. "修改MTU設定"為確保所有節點上的網格網路介面（ eth0 ）相同、請視需要加以確認。
   - 對於 Linux 和 VMware 型節點、請使用下列命令： `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`
     - 範例 * ： `change-ip.py -n node 1500 grid admin`
     - 注意 * ：在 Linux 型節點上、如果容器中網路所需的 MTU 值超過主機介面上已設定的值、則必須先將主機介面設定為具有所需的 MTU 值、然後使用 `change-ip.py`指令碼來變更容器中網路的 MTU 值。

     請使用下列引數來修改Linux或VMware節點上的MTU。

位置引數	說明
`mtu`	要設定的MTU。必須介於1280至9216之間。
`network`	要套用MTU的網路。包括下列一種或多種網路類型： • 網格 • 管理 • 用戶端

+

選用引數	說明
`-h, - help`	顯示說明訊息並結束。
`-n node, --node node`	節點。預設值為本機節點。

4. 如果您允許外部 SSH 訪問，"阻止訪問"當你完成任務時。

節點網路接收框架錯誤警示

- 節點網路接收框架錯誤 * 警示可能是 StorageGRID 與網路硬體之間的連線問題所造成。解決基礎問題後、此警示會自行清除。

關於這項工作

- 節點網路接收框架錯誤 * 警示可能是因為連線至 StorageGRID 的網路硬體發生下列問題：
- 需要轉送錯誤修正（FEC）、且不使用
- 交換器連接埠和NIC MTU不符
- 高連結錯誤率
- NIC環狀緩衝區溢位

步驟

1. 根據您的網路組態、請遵循疑難排解步驟、找出此警示的所有可能原因。
2. 視錯誤原因而定、請執行下列步驟：

FEC 不相符

這些步驟僅適用於 StorageGRID 應用裝置上 FEC 不相符所造成的 * 節點網路接收框架錯誤 * 警示。

a. 檢查連接StorageGRID 到您的產品的交換器連接埠的FEC狀態。

b. 檢查從設備到交換器的纜線實體完整性。

c. 如果您想要變更 FEC 設定以嘗試解決警示、請先確認在 StorageGRID 應用裝置安裝程式的「連結組態」頁面上、已將應用裝置設定為 * 自動 * 模式（請參閱應用裝置的說明：

   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 和 SG1100"
   - "SG100 和 SG1000"

d. 變更交換器連接埠上的 FEC 設定。如果可能、該產品連接埠會調整其FEC設定。StorageGRID

   您無法在 StorageGRID 應用裝置上設定 FEC 設定。相反地、應用裝置會嘗試探索並鏡射其所連接之交換器連接埠上的FEC設定。如果鏈路被迫達到25-GbE或100-GbE網路速度、交換器和NIC可能無法協調通用的FEC設定。如果沒有通用的 FEC 設定、網路就會恢復為「無 FEC 」模式。如果未啟用 FEC 、則連線更容易受到電子雜訊所造成的錯誤影響。

   StorageGRID 應用裝置支援 Firecode （ FC ）和 Reed Solomon （ RS ） FEC 、也不支援 FEC 。

交換器連接埠和**NIC MTU**不符

如果警示是由交換器連接埠和 NIC MTU 不符所造成、請檢查節點上設定的 MTU 大小是否與交換器連接埠的 MTU 設定相同。

節點上設定的MTU大小可能小於節點所連接之交換器連接埠上的設定。如果 StorageGRID 節點收到大於其 MTU 的乙太網路訊框（此組態可能會發生）、則可能會回報 * 節點網路接收訊框錯誤 * 警示。如果您認為這是發生的情況、請根據StorageGRID 端點對端點MTU的目標或需求、變更交換器連接埠的MTU以符合該網路介面MTU、或變更StorageGRID 該網路介面的MTU以符合交換器連接埠。

為獲得最佳網路效能、所有節點都應在其Grid Network介面上設定類似的MTU值。如果個別節點上Grid Network的MTU設定有顯著差異、則會觸發* Grid Network MTU mismis*警示。所有網路類型的 MTU 值都不一定相同。如需詳細資訊、請參閱 疑難排解Grid Network MTU不相符警示 。

另請參閱 "變更MTU設定"。

高連結錯誤率

a. 啟用FEC（若尚未啟用）。

b. 確認您的網路纜線品質良好、而且未損壞或連接不當。

c. 如果纜線似乎沒有問題、請聯絡技術支援部門。

> 您可能會注意到、在電子雜訊較高的環境中、錯誤率很高。

NIC環狀緩衝區溢位

如果錯誤是NIC環緩衝區溢位、請聯絡技術支援部門。

當無法及時處理網路事件時、當整個過程中出現過多的問題時、環狀緩衝區可能會發生溢位StorageGRID 。

3. 監控問題、如果警示無法解決、請聯絡技術支援部門。

時間同步錯誤

您可能會在網格中看到時間同步的問題。

如果您遇到時間同步問題、請確認您已指定至少四個外部NTP來源、每個來源都提供階層3或更好的參考資料、而且所有外部NTP來源都正常運作、StorageGRID 且可由您的支援節點存取。

> 若"指定外部 NTP 來源"為正式作業層級的 StorageGRID 安裝、請勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 時間（ W32Time ）服務。舊版Windows上的時間服務不夠準確、Microsoft不支援在StorageGRID 高準確度環境中使用、例如：

Linux：網路連線問題

您可能會發現在 Linux 主機上裝載的 StorageGRID 節點的網路連線問題。

MAC位址複製

在某些情況下，可以透過使用 MAC 位址克隆來解決網路問題。如果您使用虛擬主機，請在節點設定檔中將每個網路的 MAC 位址複製鍵的值設為「true」。此設定會導致StorageGRID容器的 MAC 位址使用主機的 MAC 位址。請參閱說明"建立節點設定檔"。

> 為 Linux 主機作業系統建立分隔的虛擬網路介面。如果 Linux 主機作業系統和 StorageGRID Container 使用相同的網路介面，可能會導致主機作業系統無法存取。

欲了解更多信息，請參閱"啟用 MAC 克隆"。

Linux ：節點狀態為「孤立」

處於孤立狀態的Linux節點通常表示StorageGRID 、控制StorageGRID 節點容器的孤立服務或是由節點監控的節點監控程式、會在非預期情況下死亡。

關於這項工作

如果Linux節點回報其處於孤立狀態、您應該：

- 檢查記錄中是否有錯誤和訊息。

- 嘗試重新啟動節點。
- 如有必要、請使用Container Engine命令來停止現有的節點容器。
- 重新啟動節點。

步驟

1. 檢查服務精靈和孤立節點的記錄、查看是否有明顯的錯誤或非預期結束的訊息。
2. 以root身分或使用具有Sudo權限的帳戶登入主機。
3. 執行下列命令、嘗試再次啟動節點： `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   如果節點是孤立的、則回應為

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. 從Linux停止Container引擎和任何控制的storagegrid節點程序。例如：`sudo docker stop --time secondscontainer-name`

   對於 `seconds`，輸入要等待容器停止的秒數（通常爲 15 分鐘或更短）。例如：

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. 重新啟動節點： `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux：疑難排解**IPv6**支援

如果您在StorageGRID Linux主機上安裝了支援IPv6的節點、而且您注意到IPv6位址尚未如預期指派給節點容器、則可能需要在核心中啟用IPv6支援。

關於這項工作

若要查看已指派給網格節點的 IPv6 位址：

1. 選擇*節點*並選擇節點。
2. 在「概述」標籤的 * IP 位址 * 旁、選取 * 顯示其他 IP 位址 * 。

如果未顯示IPv6位址、且節點已安裝在Linux主機上、請依照下列步驟在核心中啟用IPv6支援。

步驟

1. 以root身分或使用具有Sudo權限的帳戶登入主機。

2. 執行下列命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果應為 0 。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> 如果結果不是 0 、請參閱作業系統文件以變更 `sysctl`設定。然後、請先將值變更為0再繼續。

3. 輸入 StorageGRID 節點容器： `storagegrid node enter node-name`
4. 執行下列命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果應為 1 。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> 如果結果不是1、則此程序不適用。聯絡技術支援。

5. 結束容器： `exit`

```
root@DC1-S1:~ # exit
```

6. 以 root 用戶身份編輯以下文件 `/var/lib/storagegrid/settings/sysctl.d/net.conf`：。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 找出下列兩行、並移除註解標記。然後儲存並關閉檔案。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 執行下列命令以重新啟動StorageGRID 此資訊容器：

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

疑難排解 **StorageGRID** 的外部 **syslog** 伺服器錯誤訊息

下表說明可能與外部 Syslog 伺服器相關的錯誤訊息、並列出修正行動。

如果您在傳送測試訊息以驗證外部系統日誌伺服器是否正確設定時遇到問題，則設定外部系統日誌伺服器精靈會顯示這些錯誤。

運行時問題可能會由"外部syslog伺服器轉送錯誤"警報。如果您收到此警報，請按照警報中的指示重新發送測試訊息，以便您可以獲得詳細的錯誤訊息。

如需將稽核資訊傳送至外部 Syslog 伺服器的詳細資訊、請參閱：

- "使用外部 Syslog 伺服器的考量事項"
- "設定日誌管理和外部系統日誌伺服器"

錯誤訊息	說明與建議行動
無法解析主機名稱	您為syslog伺服器輸入的FQDN無法解析為IP位址。 1. 檢查您輸入的主機名稱。如果您輸入 IP 位址、請確定它是有效的 IP 位址、以 W.X.Y.Z （「點分十進制」）表示法表示。 2. 檢查DNS伺服器的設定是否正確。 3. 確認每個節點都可以存取DNS伺服器的IP位址。
連線遭拒	拒絕與syslog伺服器的TCP或TLS連線。主機的TCP或TLS連接埠可能沒有偵聽服務、或是防火牆可能封鎖存取。 1. 檢查您是否為syslog伺服器輸入正確的FQDN或IP位址、連接埠和傳輸協定。 2. 確認系統記錄服務的主機正在執行偵聽指定連接埠的系統記錄精靈。 3. 確認防火牆並未封鎖從節點到syslog伺服器IP和連接埠的TCP/IP連線存取。
無法連線至網路	syslog伺服器不在直接附加的子網路上。路由器傳回ICMP故障訊息、表示無法將測試訊息從列出的節點轉送到syslog伺服器。 1. 檢查您輸入的syslog伺服器FQDN或IP位址是否正確。 2. 針對列出的每個節點、檢查Grid Network Subnet List（網格網路子網路清單）、管理網路子網路清單和Client Network Gateways（用戶端網路閘道）。確認這些設定可透過預期的網路介面和閘道（Grid、Admin或Client）、將流量路由傳送至syslog伺服器。

錯誤訊息	說明與建議行動
主機無法連線	syslog伺服器位於直接附加的子網路（所列節點用於其Grid、Admin或Client IP位址的子網路）上。節點嘗試傳送測試訊息、但未收到針對syslog伺服器MAC位址的ARP要求回應。 1. 檢查您輸入的syslog伺服器FQDN或IP位址是否正確。 2. 檢查執行syslog服務的主機是否已啟動。
連線逾時	已嘗試進行TCP/IP連線、但系統記錄伺服器長時間未收到任何回應。可能是路由設定錯誤、或是防火牆在不傳送任何回應的情況下丟棄流量（通用組態）。 1. 檢查您輸入的syslog伺服器FQDN或IP位址是否正確。 2. 針對列出的每個節點、檢查Grid Network Subnet List（網格網路子網路清單）、管理網路子網路清單和Client Network Gateways（用戶端網路閘道）。確認這些設定是使用您預期可連線到 Syslog 伺服器的網路介面和閘道（ Grid 、 Admin 或 Client ）、將流量路由至 Syslog 伺服器。 3. 確認防火牆並未封鎖從所列節點存取到syslog伺服器IP和連接埠的TCP/IP連線。
合作夥伴已關閉連線	已成功建立與syslog伺服器的TCP連線、但後來關閉。原因可能包括： • 系統記錄伺服器可能已重新啟動或重新開機。 • 節點和syslog伺服器可能有不同的TCP/IP設定。 • 中間防火牆可能會關閉閒置的TCP連線。 • 偵聽syslog伺服器連接埠的非syslog伺服器可能已關閉連線。 若要解決此問題： 1. 檢查您是否為syslog伺服器輸入正確的FQDN或IP位址、連接埠和傳輸協定。 2. 如果您使用 TLS 、請確認 Syslog 伺服器也使用 TLS 。如果您使用 TCP 、請確認 Syslog 伺服器也使用 TCP 。 3. 檢查中繼防火牆是否未設定為關閉閒置的TCP連線。
TLS憑證錯誤	從syslog伺服器收到的伺服器憑證與您提供的CA憑證套件和用戶端憑證不相容。 1. 確認CA憑證套件組合和用戶端憑證（如果有）與syslog伺服器上的伺服器憑證相容。 2. 確認來自syslog伺服器之伺服器憑證中的身分識別包含預期的IP或FQDN值。
轉送已暫停	系統記錄不再轉送到系統記錄伺服器、StorageGRID 而且無法偵測原因。 檢閱此錯誤所提供的偵錯記錄、以嘗試判斷根本原因。

錯誤訊息	說明與建議行動
TLS工作階段已終止	syslog伺服器終止TLS工作階段、StorageGRID 且無法偵測原因。 1. 檢閱此錯誤所提供的偵錯記錄、以嘗試判斷根本原因。 2. 檢查您是否為syslog伺服器輸入正確的FQDN或IP位址、連接埠和傳輸協定。 3. 如果您使用 TLS 、請確認 Syslog 伺服器也使用 TLS 。如果您使用 TCP 、請確認 Syslog 伺服器也使用 TCP 。 4. 確認CA憑證套件組合和用戶端憑證（如果有）與來自syslog伺服器的伺服器憑證相容。 5. 確認來自syslog伺服器之伺服器憑證中的身分識別包含預期的IP或FQDN值。
結果查詢失敗	用於系統記錄伺服器組態和測試的管理節點無法從列出的節點要求測試結果。一個或多個節點可能當機。 1. 請遵循標準疑難排解步驟、確保節點處於線上狀態、而且所有預期的服務都在執行中。 2. 在列出的節點上重新啟動misd服務。

了解 **StorageGRID** 中的負載平衡器快取問題

了解負載平衡器快取可能存在的問題以及如何解決這些問題。

確定請求是否為快取命中

- X-Cache 標頭是在快取服務處理的請求的回應中設定的。可能的代碼：
  - `HIT`：該物件由快取提供
  - `PARTIAL-HIT`：儲存桶/鍵在快取中有記錄，但並非所有請求的範圍都能夠從快取中得到服務
  - `STALE`：儲存桶/鍵在快取中有一個記錄，但自上次從快取中提供該物件後，該物件已被更新。
  - `MISS`：該物件不在快取中
- 這 `nginx-gw/endpoint-access.log.gz`請求的記錄包括“unix:/run/cache-svc/cache-svc.sock”，用於快取處理的請求。
- 這 `cache-svc/cache-svc.log`報告諸如「請求 320390：成功完成（快取命中）」或「請求 320375：成功完成（快取未命中）」之類的訊息。透過搜尋具有相同「Request <*number*>」字串的其他記錄來尋找請求的路徑。

快取命中率低

- 當新增新的工作負載或工作負載存取的工作集發生變化時，可能會出現較低的快取命中率。在這些情況下，命中率預計會隨著時間的推移而增加。
- 如果多個工作負載正在使用緩存，請考慮新增流量分類策略來隔離由快取服務的工作負載部分。每個流量分類策略都有快取命中率指標。如果某些工作負載的快取命中率不高，請考慮將這些工作負載移至未啟用快取的其他端點。

- 評估快取驅逐率。如果快取太小而無法容納工作集，它將經歷高驅逐率並可能導致命中率降低。
- FPVR 下可能提供用於提高某些工作負載命中率的選項。

性能低下

- 評估緩存命中率。低緩存命中率會導致整體效能低下。
- 評估快取驅逐率。在驅逐期間，一些儲存資源用於從磁碟中刪除現有物件。如果驅逐過程跟不上新物件的訪問，系統可能會達到硬水印閾值並開始繞過快取。
- 使用「網路介面接收使用情況」和「網路介面傳輸使用情況」診斷檢查網路限制。

檢閱稽核記錄

稽核訊息和記錄

這些指示包含StorageGRID 有關不稽核訊息和稽核記錄的結構和內容資訊。您可以使用此資訊來讀取及分析系統活動的稽核記錄。

這些指示適用於負責製作系統活動和使用報告的系統管理員、這些報告需要分析StorageGRID 整個系統的稽核訊息。

若要使用文字記錄檔、您必須擁有管理節點上已設定之稽核共用的存取權。

有關配置審計訊息等級和使用外部系統日誌伺服器的信息，請參閱"設定日誌管理和外部系統日誌伺服器"。

稽核訊息如何透過 **StorageGRID** 系統傳輸到 **audit.log** 檔案以進行保留

所有StorageGRID 的支援服務都會在正常系統運作期間產生稽核訊息。您應該瞭解這些稽核訊息如何透過 StorageGRID 系統移至 `audit.log`檔案。

僅當為 管理節點/本機節點 或 管理節點和外部系統日誌伺服器 設定StorageGRID時，下列稽核訊息和稽核訊息保留工作流程才適用。如果StorageGRID配置為“僅本機節點”（預設）或“外部系統日誌伺服器”，則稽核訊息將保存在本機的每個節點上 `/var/local/log/localaudit.log`檔案並且無法由管理節點或儲存節點處理。

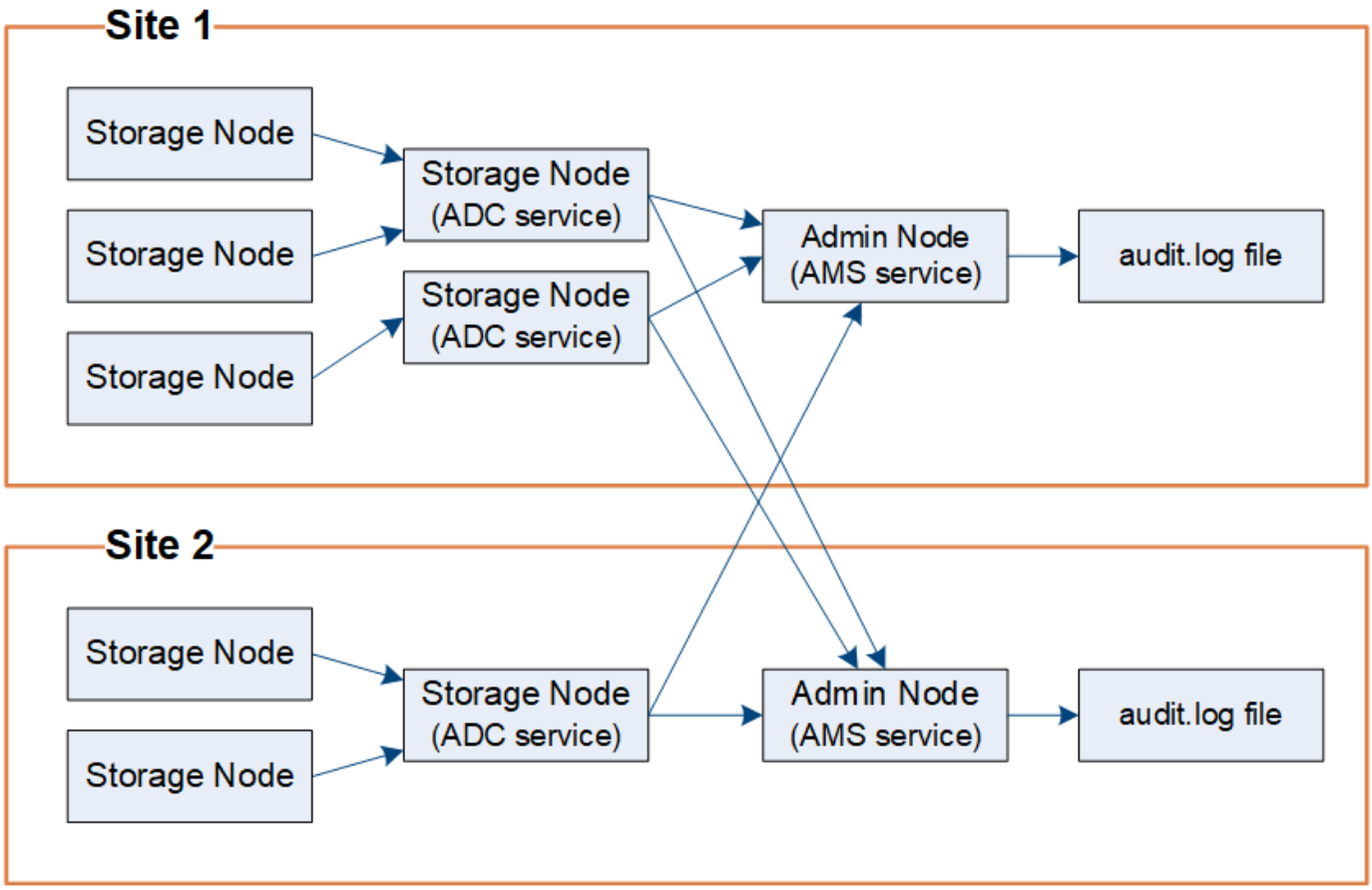
稽核訊息流程

當StorageGRID配置為 管理節點/本機節點 或 管理節點和外部系統日誌伺服器 時，稽核訊息由管理節點處理，並且由具有管理網域控制器 (ADC) 服務的儲存節點處理。

如稽核訊息流程圖所示、每StorageGRID 個節點都會將稽核訊息傳送至資料中心站台的其中一個ADC服務。每個站台上安裝的前三個儲存節點會自動啟用「ADC」服務。

接著、每個ADC服務會做為中繼、並將其稽核訊息集合傳送到StorageGRID 整個系統的每個管理節點、讓每個管理節點都能完整記錄系統活動。

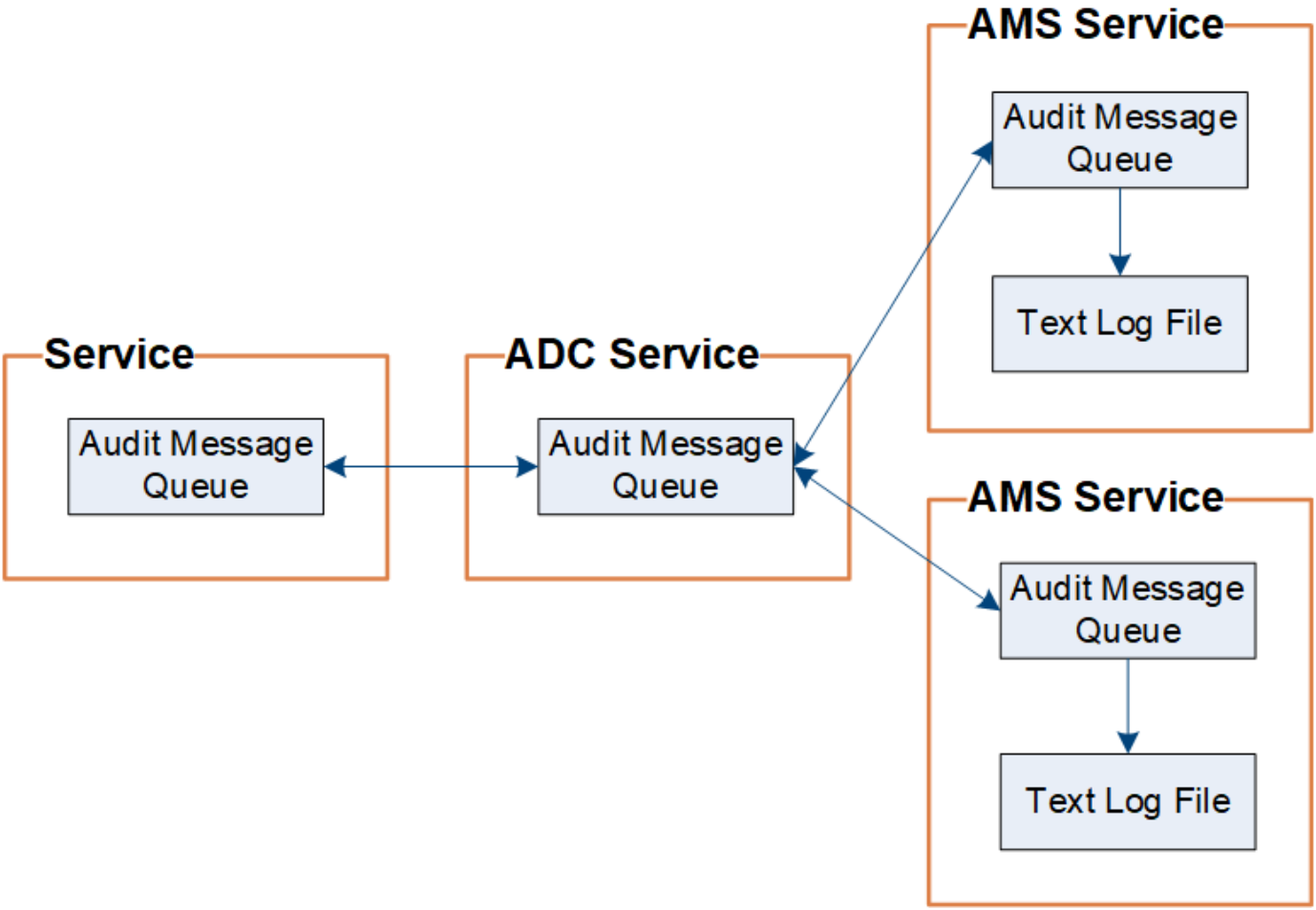
每個管理節點都會將稽核訊息儲存在文字記錄檔中；使用中的記錄檔會命名為 `audit.log`。



稽核訊息保留

使用複製與刪除程序、確保不會遺失任何稽核訊息、然後再寫入稽核記錄。StorageGRID

當節點產生或中繼稽核訊息時，該訊息將儲存在網格節點系統磁碟上的稽核訊息佇列中。訊息的副本始終保存在審計訊息佇列中，直到該訊息寫入管理節點的稽核日誌檔案為止 `/var/local/audit/export`目錄。這有助於防止審計訊息在傳輸過程中遺失。



由於網路連線問題或審計容量不足，審計訊息佇列可能會暫時增加。隨著佇列的增加，它們會消耗每個節點的更多可用空間 `/var/local/`目錄。如果問題仍然存在，並且節點的審計訊息目錄變得太滿，則各個節點將優先處理其積壓訊息，並暫時無法接收新訊息。

具體而言、您可能會看到下列行為：

- 如果 `/var/local/audit/export`管理節點使用的目錄已滿，管理節點將被標記為無法接收新的稽核訊息，直到目錄不再滿為止。 S3 客戶端請求不受影響。當審計儲存庫無法存取時，會觸發 XAMS（無法存取的審計儲存庫）警報。
- 如果 `/var/local/`當具有 ADC 服務的儲存節點所使用的目錄已滿 92% 時，該節點將被標記為不可用於審核訊息，直到目錄僅已滿 87% 為止。 S3 客戶端對其他節點的請求不受影響。當審計中繼無法存取時，會觸發 NRLY（可用審計中繼）警報。

> 如果 ADC 服務沒有可用的儲存節點、儲存節點會將稽核訊息儲存在本機檔案中 `/var/local/log/localaudit.log`。

- 如果 `/var/local/`當儲存節點使用的目錄已滿 `85%` 時，該節點開始拒絕 `S3` 用戶端請求 `503 Service Unavailable`。

下列類型的問題可能導致稽核訊息佇列變得非常龐大：

- 管理節點或儲存節點與ADC服務的中斷。如果其中一個系統節點當機、其餘節點可能會變成回溯記錄。
- 超過系統稽核容量的持續活動率。

- `/var/local/`由於與稽核訊息無關的原因、 ADC 儲存節點上的空間已滿。發生這種情況時、節點會停止接受新的稽核訊息、並優先處理其目前的待處理項目、這可能會導致其他節點發生待處理。

大型稽核佇列警示和稽核訊息佇列（**AMQS**）警示

為了協助您監控一段時間內稽核訊息佇列的大小、當儲存節點佇列或管理節點佇列中的訊息數目達到特定臨界值時、就會觸發*大型稽核佇列*警示和舊版AMQS警示。

如果觸發*大型稽核佇列*警示或舊版AMQS警示、請先檢查系統負載、如果最近發生大量交易、警示和警示應會隨著時間而解除、並可予以忽略。

如果警報或警告持續且嚴重程度增加，請查看佇列大小圖表。如果該數字在數小時或數天內穩定增加，則審計負載可能已經超出了系統的審計容量。透過將客戶端寫入和客戶端讀取的稽核等級變更為錯誤或關閉，降低客戶端操作率或減少記錄的稽核訊息數量。看"設定日誌管理和外部系統日誌伺服器" 。

重複的訊息

如果發生網路或節點故障、StorageGRID 那麼這個系統會採取保守的方法。因此、稽核記錄中可能會出現重複的訊息。

從 **StorageGRID** 管理節點命令列存取稽核記錄檔

稽核共用包含作用中 `audit.log`檔案和任何壓縮的稽核記錄檔。您可以直接從管理節點的命令列存取稽核記錄檔。

這 `audit.log`除非您為 管理節點/本機節點 或 管理節點和外部系統日誌伺服器 設定StorageGRID ，否則檔案保持為空。有關詳細信息，請參閱"選擇日誌位置" 。

開始之前

- 您有 "特定存取權限"。
- 您必須擁有 `Passwords.txt`檔案。
- 您必須知道管理節點的IP位址。

步驟

1. 登入管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 移至包含稽核記錄檔的目錄：

   ```
   cd /var/local/audit/export/
   ```
3. 視需要檢視目前或已儲存的稽核記錄檔。

了解 StorageGRID 中的稽核記錄檔輪替

如果StorageGRID配置為 管理節點/本機節點 或 管理節點和外部系統日誌伺服器，則稽核日誌檔案將會儲存到管理節點的 `/var/local/audit/export/`目錄。活動審計日誌檔案被命名為 `audit.log`。

> 或者，您可以變更稽核日誌的目標並將稽核資訊傳送至外部系統日誌伺服器。當設定外部系統日誌伺服器時，將繼續產生和儲存稽核記錄的本機日誌。請參閱"設定稽核訊息和外部 Syslog 伺服器"。

一天一次、作用中檔案就 `audit.log`會儲存、並啟動新 `audit.log`檔案。保存的文件的名稱以格式表示保存的時間 `*yyyy-mm-dd.txt*`。如果在一天內創建多個審計日誌，則文件名將使用保存文件的日期（以數字附加），格式爲 *`yyyy-mm-dd.txt.n`*。例如 `2018-04-15.txt`、和 `2018-04-15.txt.1`是在 2018 年 4 月 15 日建立及儲存的第一和第二個記錄檔。

一天后，已儲存的檔案被壓縮並重新命名，格式為 *`yyyy-mm-dd.txt.gz`*，保留原始日期。隨著時間的推移，分配給審計日誌的管理節點儲存空間將被消耗。腳本監控稽核日誌空間消耗，並根據需要刪除日誌檔案以釋放空間 `/var/local/audit/export/`目錄。審計日誌將根據其建立日期刪除。最舊的日誌將首先被刪除。您可以在以下文件中監視腳本的操作： `/var/local/log/manage-audit.log`。

此示例顯示了活動 `audit.log`文件、前一天的文件（`2018-04-14.txt.gz`）(`2018-04-15.txt`和前一天的壓縮文件）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

稽核記錄檔格式

了解 StorageGRID 中稽核記錄檔的格式

稽核記錄檔位於每個管理節點、並包含個別稽核訊息的集合。

每個稽核訊息都包含下列項目：

- 觸發ISO 8601格式稽核訊息（ATIM）的事件協調世界時間（UTC）、後面接著空格：

  `YYYY-MM-DDTHH:MM:SS.UUUUUU`，其中 *`UUUUUU`*是微秒。

- 稽核訊息本身，包含在方括號內，開頭為 `AUDT`。

下列範例顯示稽核記錄檔中的三個稽核訊息（換行符號會新增以方便閱讀）。當租戶建立S3儲存區並將兩個物件新增至該儲存區時、就會產生這些訊息。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

稽核記錄檔中的稽核訊息是預設格式、不易讀取或解讀。您可以使用"稽核說明工具"取得稽核記錄中稽核訊息的簡化摘要。您可以使用"稽核總和工具"來總結記錄的寫入、讀取和刪除作業數、以及這些作業所需的時間。

使用 **audit-explain** 工具翻譯 **StorageGRID** 稽核訊息

您可以使用此 `audit-explain`工具、將稽核記錄中的稽核訊息轉譯為易於讀取的格式。

開始之前

- 您有 "特定存取權限"。
- 您必須擁有 `Passwords.txt`檔案。
- 您必須知道主管理節點的IP位址。

關於這項工作

此 `audit-explain`工具可在主要管理節點上使用、可在稽核記錄中提供稽核訊息的簡化摘要。

> 此 `audit-explain`工具主要供技術支援人員在疑難排解作業期間使用。處理 `audit-explain`查詢可能會消耗大量 CPU 電力、這可能會影響 StorageGRID 作業。

此範例顯示工具的一般輸出 `audit-explain`。當 S3 租戶的帳戶 ID 為 92484777680322627870 、使用 S3 提交要求建立名為「 Bucket1 」的貯體、並將三個物件新增至該貯體時、就會產生這四個"SPUT"稽核訊息。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

此 `audit-explain`工具可執行下列動作：

- 處理純或壓縮的稽核記錄。例如：

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 同時處理多個檔案。例如：

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- 接受來自管道的輸入、可讓您使用命令或其他方法來篩選及預先處理輸入 `grep`。例如：

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

由於稽核記錄可能非常大且剖析速度緩慢、因此您可以篩選要查看的部分、並在零件上執行、而非整個檔案、以節省時間 `audit-explain`。

此 `audit-explain`工具不接受壓縮檔案作為管道輸入。若要處理壓縮檔案、請提供檔案名稱做為命令列引數、或使用工具先解壓縮 `zcat`檔案。例如：

```
zcat audit.log.gz | audit-explain
```

使用 `help (-h)`選項查看可用選項。例如：

```
$ audit-explain -h
```

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 輸入以下命令，其中 `/var/local/audit/export/audit.log`代表您要分析的檔案的名稱和位置：

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   此 `audit-explain`工具會列印指定檔案中所有訊息的人類可讀判讀。

   為了減少線條長度並協助閱讀、預設不會顯示時間戳記。如果您想查看時間戳記，請使用時間戳記(`-t`選項。

使用 **audit-sum** 工具彙總 **StorageGRID** 稽核訊息

您可以使用此 `audit-sum`工具來計算寫入、讀取、標頭及刪除稽核訊息、並查看每種作業類型的最小、最大及平均時間（或大小）。

開始之前

- 您有 "特定存取權限"。
- 您有 `Passwords.txt`檔案。
- 您知道主要管理節點的 IP 位址。

關於這項工作

`audit-sum`主要管理節點上提供的工具會摘要說明記錄的寫入、讀取和刪除作業數、以及這些作業所需的時間。

此 `audit-sum`工具主要供技術支援人員在疑難排解作業期間使用。處理 `audit-sum`查詢可能會消耗大量 CPU 電力、這可能會影響 StorageGRID 作業。

此範例顯示工具的一般輸出 `audit-sum`。此範例顯示傳輸協定作業所需的時間。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

這 `audit-sum`此工具為稽核日誌中的以下 S3 和 ILM 稽核訊息提供計數和時間。

由於功能已被棄用，因此審計代碼已從產品和文件中刪除。如果您遇到此處未列出的稽核程式碼，請檢查此主題的先前版本以了解較舊的StorageGRID版本。例如， "StorageGRID 11.8 使用稽核總和工具" 。

程式碼	說明	請參閱
理想	ILM初始化刪除：ILM開始刪除物件的程序時記錄。	"表意：ILM啟動刪除"
SDEL	S3刪除：記錄成功的交易以刪除物件或儲存區。	"SDEL：S3刪除"
SGET	S3 Get：記錄成功的交易、以擷取物件或列出儲存區中的物件。	"SGET：S3取得"
Shea	S3標頭：記錄成功的交易、以檢查物件或儲存區是否存在。	"Shea：S3負責人"
SPUT	S3 PUT：記錄成功的交易、以建立新的物件或儲存區。	"SPUT：S3"

此 `audit-sum`工具可執行下列動作：

- 處理純或壓縮的稽核記錄。例如：

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 同時處理多個檔案。例如：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- 接受來自管道的輸入、可讓您使用命令或其他方法來篩選及預先處理輸入 `grep`。例如：

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> 此工具不接受壓縮檔案作為管道輸入。若要處理壓縮文件，請將其檔案名稱作為命令列參數提供，或使用 `zcat`工具先解壓縮檔案。例如：
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

您可以使用命令列選項、將儲存區上的作業與物件上的作業分開彙總、或依儲存區名稱、時間期間或目標類型將訊息摘要分組。根據預設、摘要會顯示最小、最大和平均操作時間、但您可以使用 `size (-s)`選項來查看物件大小。

使用 `help (-h)`選項查看可用選項。例如：

```
$ audit-sum -h
```

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 如果您要分析與寫入、讀取、標頭及刪除作業相關的所有訊息、請依照下列步驟操作：
   a. 輸入以下命令，其中 `/var/local/audit/export/audit.log`代表您要分析的檔案的名稱和位置：

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      此範例顯示工具的一般輸出 `audit-sum`。此範例顯示傳輸協定作業所需的時間。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

在此範例中、SGET（S3 Get）作業平均速度最慢、僅1.13秒、但SGET和SPUT（S3 PUT）作業都顯示出約1、730秒的長時間最差時間。

b. 若要顯示最慢的 10 次擷取作業、請使用 Grep 命令僅選取 SGET 訊息、並新增長輸出選項(`-l`）以包含物件路徑：

```
grep SGET audit.log | audit-sum -l
```

結果包括類型（物件或儲存區）和路徑、可讓您為稽核日誌中與這些特定物件相關的其他訊息進行 Grep。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
在此範例輸出中、您可以看到三個最慢的S3「Get（取得）」要求是針對大小約5 GB的物件、比其他物件大得多。大容量則是最差擷取時間緩慢的問題。

3. 如果您想要確定要在網格中擷取和擷取的物件大小、請使用「大小(`-s`」選項）：

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

在此範例中、SPUT的平均物件大小低於2.5 MB、但SGET的平均大小卻大得多。SPUT訊息的數量遠高於SGET訊息的數量、表示大部分的物件永遠不會擷取。

4. 如果您想要判斷昨天擷取的速度是否緩慢：

   a. 在適當的稽核記錄上發出命令、並使用依時間分組選項(`-gt`）、接著輸入時間段（例如 15M 、 1H 、 10S ）：

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

這些結果表明，S3 GET 流量在 06:00 至 07:00 之間出現峰值。在此時間跨度內，最大時間和平均時間都相當高，而且它們並沒有隨著計數的增加而逐漸增加。這些指標顯示容量可能超出了範圍，可能是網路或電網處理請求的能力超出了範圍。

b. 要確定昨天每小時檢索的對象大小，請將 Size 選項(`-s`（大小選項）添加到命令中：

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group            count       min(B)          max(B)
average(B)
  =============            =====     ========        ========
============
  2019-09-05T00             7591        0.040        1481.867
1.976
  2019-09-05T01             4173        0.043        1740.290
2.062
  2019-09-05T02            20142        0.083        1274.961
2.303
  2019-09-05T03            57591        0.912        1383.867
1.182
  2019-09-05T04           124171        0.730        1740.290
1.528
  2019-09-05T05           420182        0.875        4274.511
2.398
  2019-09-05T06          1220371        0.691  5663711385.961
51.328
  2019-09-05T07           527142        0.130        1974.228
2.147
  2019-09-05T08           384173        0.625        1740.290
1.878
  2019-09-05T09            27591        0.689        1481.867
1.354
```

這些結果顯示、當整體擷取流量達到最大值時、會發生一些非常大的擷取。

c. 若要查看更多詳細資料、請使用"稽核說明工具"檢閱該時段內的所有 SGET 作業：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果 Grep 命令的輸出預期為多行、請新增命令、 `less`一次顯示一頁（一個畫面）的稽核記錄檔內容。

5. 如果您想要判斷儲存區上的SPUT作業是否比物件的SPUT作業慢：

a. 首先使用 `-go`選項、將訊息分別分組以進行物件和貯體作業：

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

結果顯示、適用於貯體的SPUT作業與物件的SPUT作業具有不同的效能特性。

b. 若要判斷哪些貯體具有最慢的 SPUT 作業、請使用 `-gb`選項、依貯體將訊息分組：

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 若要判斷哪些貯體具有最大的 SPUT 物件大小、請同時使用 `-gb`和 `-s`選項：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

稽核訊息格式

了解 **StorageGRID** 稽核訊息的結構

在這個系統內交換的稽核訊息StorageGRID 包括所有訊息通用的標準資訊、以及說明所報告事件或活動的特定內容。

如果和"稽核總和"工具提供的摘要資訊"稽核說明"不足、請參閱本節以瞭解所有稽核訊息的一般格式。

以下是稽核記錄檔中可能出現的稽核訊息範例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每個稽核訊息都包含一串屬性元素。整個字符串包含在方括號(`[ ]`中），字符串中的每個屬性元素具有以下特徵：

- 括在支架中 `[ ]`
- 由字串引入 `AUDT`、表示稽核訊息
- 不含分隔符號（不含逗號或空格）
- 以換行字元結束 `\n`

每個元素都包含屬性代碼、資料類型及以下列格式報告的值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

訊息中的屬性元素數目取決於訊息的事件類型。屬性元素不會以任何特定順序列出。

下列清單說明屬性元素：

- `ATTR`為所報告屬性的四個字元代碼。有些屬性是所有稽核訊息和其他特定事件的常見屬性。
- `type`為值之程式設計資料類型的四個字元識別碼、例如 UI64 、 FC32 等。該類型以括號括 `( )`住。
- `value`是屬性的內容、通常是數值或文字值。值始終以冒號 (:`結尾）。資料類型 CStr 的值會以雙引號 " " 括住。

StorageGRID 稽核訊息中的資料類型

不同的資料類型可用來將資訊儲存在稽核訊息中。

類型	說明
UI32	無符號長整數（32位元）；可儲存0至4、294、967、295的數字。
UI64	無符號雙長整數（64位元）；可儲存0至18、446,744,073,709,551615的數字。
FC32	四個字元常量； 32 位元無符號整數值、表示為四個 ASCII 字元、例如「 ABCD 」。
iPad	用於IP位址。
CStr	UTF-8 字元的可變長度陣列。可以使用下列慣例來轉義字元： • 反斜槓是\。 • 回車是\r • 雙引號是\ • 換行（新行）為 • 字元可以用其十六進位等效字元來取代（格式為\xhh、其中hh是代表字元的十六進位值）。

StorageGRID 稽核訊息中的事件特定資料

稽核日誌中的每個稽核訊息都會記錄特定於系統事件的資料。

在識別訊息本身的開啟容器之後 `[AUDT:`、下一組屬性會提供有關稽核訊息所描述的事件或動作的資訊。這些屬性會在下列範例中反白顯示：

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

`ATYP`元素（在範例中加上底線）會識別產生訊息的事件。此範例訊息包含link:shea-s3-head.html["Shea"]訊息代碼（ [ATYP(FC32):Shea ）、表示它是由成功的 S3 頭部要求所產生。

StorageGRID 稽核訊息中的常見元素

所有稽核訊息都包含通用元素。

程式碼	類型	說明
在	FC32	模組 ID ：產生訊息之模組 ID 的四個字元識別碼。這表示產生稽核訊息的程式碼區段。
ANID	UI32	節點ID：指派給產生訊息之服務的網格節點ID。每項服務在StorageGRID設定和安裝完整套系統時、都會分配一個唯一的識別碼。此 ID 無法變更。
。	UI64	稽核工作階段識別碼：在舊版中、此元素指出在服務啟動後、稽核系統初始化的時間。此時間值是以微秒為單位、自作業系統時代（ 1970 年 1 月 1 日為 00 ： 00 ： 00 UTC ）開始計算。 *注意：*此元素已過時、不再出現在稽核訊息中。
ASQN	UI64	連續數：在先前版本中、此計數器會針對網格節點（ANID）上每個產生的稽核訊息遞增、並在服務重新啟動時重設為零。 *注意：*此元素已過時、不再出現在稽核訊息中。
ATID	UI64	追蹤ID：由單一事件觸發的一組訊息所共用的識別碼。

程式碼	類型	說明
ATIM	UI64	時間戳記：觸發稽核訊息的事件產生時間、以微秒為單位測量、自作業系統時代（ 1970 年 1 月 1 日 00 ： 00 ： 00 UTC ）。請注意、將時間戳記轉換為本機日期和時間的大多數可用工具都是以毫秒為基礎。 可能需要捨入或捨去記錄的時間戳記。出現在檔案中稽核訊息開頭的人類可讀時間 `audit.log`是 `ISO 8601` 格式的 `ATIM` 屬性。日期和時間表示爲 `*YYYY-MMDDTHH:MM:SS.UUUUUU*`，其中 `T`是指示日期時間段開始的文字字符串字符。`*UUUUUU*`為微秒。
ATYP	FC32	事件類型：所記錄事件的四個字元識別碼。這會規範訊息的「有效負載」內容：包含的屬性。
離職者	UI32	版本：稽核訊息的版本。隨著更新版的支援軟體、新版的服務可能會在稽核報告中加入新功能。StorageGRID此欄位可在AMS服務中啟用向下相容性、以處理舊版服務的訊息。
RSRLT	FC32	結果：事件、程序或交易的結果。如果與訊息無關、則不會使用任何訊息、而不會使用SUCS、因此不會意外篩選訊息。

StorageGRID 稽核訊息格式和範例

您可以在每個稽核訊息中找到詳細資訊。所有稽核訊息都使用相同的格式。

以下是檔案中可能出現的稽核訊息範例 `audit.log`：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

稽核訊息包含所記錄事件的相關資訊、以及稽核訊息本身的相關資訊。

若要識別稽核訊息所記錄的事件、請尋找ATYP屬性（反白顯示如下）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP屬性的值為SPUT。"SPUT"代表 S3 Put 交易、將物件的擷取記錄到儲存區。

下列稽核訊息也會顯示物件關聯的儲存區：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

若要瞭解放置事件發生的時間、請在稽核訊息開頭記下通用協調時間（UTC）時間戳記。此值是稽核訊息本身的ATIM 屬性的人類可讀版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM會記錄UNIX時代開始以來的時間（以微秒為單位）。在此範例中、此值 `1405631878959669`會轉譯為2014 年 7 月 17 日星期四 21 ： 17 ： 59 UTC 。

稽核訊息和物件生命週期

當 StorageGRID 產生稽核訊息時

每次擷取、擷取或刪除物件時、都會產生稽核訊息。您可以找出 S3 API 特定稽核訊息、在稽核記錄中識別這些交易。

稽核訊息是透過每個傳輸協定的特定識別碼來連結。

傳輸協定	程式碼
連結S3作業	S3BK （貯體）、 S3KY （鑰匙）或兩者
連結內部營運	CBID （物件的內部識別碼）

稽核訊息的時間

由於網格節點之間的時間差異、物件大小和網路延遲等因素、不同服務所產生的稽核訊息順序可能與本節範例所示的順序不同。

StorageGRID 中物件擷取交易的稽核訊息

您可以找出 S3 API 特定稽核訊息、以識別稽核記錄中的用戶端擷取交易。

下表並未列出攝取事務期間產生的所有稽核訊息。僅包含追蹤攝取事務所需的訊息。

S3擷取最新稽核訊息

程式碼	名稱	說明	追蹤	請參閱
SPUT	S3投入交易	S3「投入」交易已成功完成。	CBID、S3BK、S3KY	"SPUT：S3"
ORLM	符合物件規則	此物件的ILM原則已獲滿足。	CBID	"ORLM：符合物件規則"

範例：**S3**物件擷取

以下一系列稽核訊息是S3用戶端將物件擷取至儲存節點（LMR服務）時、所產生並儲存至稽核記錄的稽核訊息範例。

在此範例中、主動式 ILM 原則包括製作 2 份 ILM 規則。

以下範例並未列出交易期間產生的所有稽核訊息。僅列出與S3擷取交易（SPUT）相關的項目。

此範例假設先前已建立S3儲存區。

SPUT：S3

產生SPUT訊息、表示已發出S3 PUT交易、以在特定的儲存桶中建立物件。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM：符合物件規則

ORLM訊息表示此物件已符合ILM原則。訊息包括物件的CBID和套用的ILM規則名稱。

對於複寫的物件、LOCS欄位包含物件位置的LMR節點ID和Volume ID。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

對於銷毀編碼物件、 LOCS 欄位包括銷毀編碼設定檔 ID 和銷毀編碼群組 ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

PATH 欄位包含 S3 儲存桶和金鑰資訊。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

StorageGRID 中物件刪除交易的稽核訊息

您可以找出 S3 API 特定稽核訊息、以識別稽核記錄中的物件刪除交易。

下表並未列出在刪除交易期間產生的所有稽核訊息。僅包含追蹤刪除交易所需的訊息。

S3刪除稽核訊息

程式碼	名稱	說明	追蹤	請參閱
SDEL	S3刪除	要求從儲存區刪除物件。	CBID、S3KY	"SDEL：S3刪除"

範例：**S3**物件刪除

當S3用戶端從儲存節點（LMR服務）刪除物件時、會產生稽核訊息並儲存至稽核記錄。

> 並非所有在刪除交易期間產生的稽核訊息都會列在下例中。僅列出與S3刪除交易（SDEL）相關的項目。

SDEL：**S3**刪除

當用戶端將 DeleteObject 要求傳送至 LDR 服務時、即會開始刪除物件。訊息包含用來刪除物件的儲存區、以及用來識別物件的S3金鑰。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

您可以找出 S3 API 專屬稽核訊息、以識別稽核記錄中的物件擷取交易。

下表並未列出檢索事務期間產生的所有稽核訊息。僅包含追蹤檢索交易所需的訊息。

S3擷取稽核訊息

程式碼	名稱	說明	追蹤	請參閱
SGET	S3取得	要求從儲存區擷取物件。	CBID、S3BK、S3KY	"SGET：S3取得"

範例：**S3**物件擷取

當S3用戶端從儲存節點（LMR服務）擷取物件時、會產生稽核訊息並儲存至稽核記錄。

請注意、下列範例並未列出交易期間產生的所有稽核訊息。僅列出與S3擷取交易（SGET）相關的項目。

SGET：S3取得

當用戶端將 GetObject 要求傳送至 LDR 服務時、就會開始物件擷取。訊息包含用來擷取物件的儲存區、以及用來識別物件的S3金鑰。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

如果儲存區原則允許、用戶端可以匿名擷取物件、或從不同租戶帳戶所擁有的儲存區擷取物件。稽核訊息包含有關庫位擁有者租戶帳戶的資訊、以便您追蹤這些匿名和跨帳戶的要求。

在下列範例訊息中、用戶端會傳送 GetObject 要求給儲存在他們不擁有的儲存區中的物件。SAI和Sbus的值會記錄庫位擁有者的租戶帳戶ID和名稱、這與S3AI和SACC中記錄的租戶帳戶ID和用戶端名稱不同。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

範例：在物件上選取**S3**

當S3用戶端對物件發出S3 Select查詢時、會產生稽核訊息並儲存至稽核記錄。

請注意、下列範例並未列出交易期間產生的所有稽核訊息。僅列出與S3 Select交易（SelectObjectContent）相關的交易。

每個查詢會產生兩個稽核訊息：一個執行 S3 Select 要求授權（ S3SR 欄位設定為「 SELECT 」）、另一個後續標準 GET 作業、可在處理期間從儲存設備擷取資料。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

StorageGRID 中 **S3** 物件中繼資料更新的稽核訊息

當S3用戶端更新物件的中繼資料時、就會產生稽核訊息。

S3中繼資料更新稽核訊息

程式碼	名稱	說明	追蹤	請參閱
SUPD	S3中繼資料已更新	當S3用戶端更新擷取物件的中繼資料時產生。	CBID、S3KY、HTRH	"SUBPD：S3中繼資料已更新"

範例：**S3**中繼資料更新

此範例顯示更新現有S3物件中繼資料的成功交易。

SUBPD：**S3**中繼資料更新

S3 用戶端發出請求 (SUPD) 以更新 S3 物件 (S3KY) 的指定中繼資料 (`x-amz-meta-*`。

在本例中，請求標頭包含在 HTRH 欄位中，因為它已設定為稽核協定標頭（組態 > 監控 > 稽核和 **syslog** 伺服器）。請參閱"設定日誌管理和外部系統日誌伺服器"。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

稽核訊息

了解 **StorageGRID** 中的稽核訊息類型和代碼

以下各節將詳細說明系統傳回的稽核訊息。每個稽核訊息都會先列在表格中、並依訊息所代表的活動類別來分組相關訊息。這些群組對於瞭解稽核的活動類型、以及選取所需的稽核訊息篩選類型都很有用。

稽核訊息也會依其四個字元的代碼的字母順序列出。此字母清單可讓您尋找特定訊息的相關資訊。

本章中使用的四個字元代碼為稽核訊息中的 ATYP 值、如下列範例訊息所示：

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

有關設定審計訊息等級、變更日誌目標以及使用外部系統日誌伺服器儲存稽核資訊的信息，請參閱"設定日誌管理和外部系統日誌伺服器"

稽核訊息類別

屬於系統稽核類別的稽核訊息用於與稽核系統本身、網格節點狀態、全系統工作活動（網格工作）和服務備份作業相關的事件。

程式碼	訊息標題與說明	請參閱
ECMC	遺失抹除編碼資料片段：表示偵測到遺失的銷毀編碼資料片段。	"ECMC ：遺失抹除編碼資料片段"
ECOC	毀損的刪除編碼資料片段：表示偵測到毀損的刪除編碼資料片段。	"ECOC ：毀損的刪除編碼資料片段"
ETAF	安全驗證失敗：使用傳輸層安全性（TLS）的連線嘗試失敗。	"ETAF：安全驗證失敗"
GNRG	GNDS登錄：一項服務、更新或註冊StorageGRID 了有關其本身在本系統中的資訊。	"GNRG：GNDS登錄"
GNur	GNDS取消登錄：服務已從StorageGRID 這個系統中取消登錄。	"GNur：GNDS取消登錄"
GTED	網格工作已結束：CMN服務已完成網格工作的處理。	"GTED：網格工作已結束"
GTSt	網格工作已開始：CMN服務已開始處理網格工作。	"GTST：網格工作已開始"
GTSU	已提交網格工作：已將網格工作提交至CMN服務。	"GTSU：已提交Grid工作"
LLST	位置遺失：此稽核訊息會在位置遺失時產生。	"LLST：位置遺失"
OLST	物件遺失：要求的物件無法位於StorageGRID 整個系統內。	"OLST：系統偵測到遺失物件"
Sadd	安全稽核停用：稽核訊息記錄已關閉。	"Sadd：停用安全性稽核"
SAade	啟用安全性稽核：稽核訊息記錄已還原。	"SAade：啟用安全性稽核"
SVRF	物件存放區驗證失敗：內容區塊驗證檢查失敗。	"SVRF：物件存放區驗證失敗"
SVRU	物件存放區驗證不明：在物件存放區中偵測到非預期的物件資料。	"SVRU：物件存放區驗證不明"
SYSD	節點停止：要求關機。	"SYSD：節點停止"

程式碼	訊息標題與說明	請參閱
系統	節點停止：服務啟動正常停止。	"Syst：節點停止"
SYSU	節點啟動：服務已啟動；先前關機的性質會在訊息中指出。	"SYSU：節點啟動"

StorageGRID 中物件儲存事件的稽核訊息

屬於物件儲存稽核類別的稽核訊息、用於與 StorageGRID 系統內物件的儲存和管理相關的事件。包括物件儲存與擷取、網格節點對網格節點傳輸及驗證。

稽核代碼會從產品和文件中移除、因為功能已過時。如果您遇到本文未列出的稽核程式碼、請查看本主題的舊版以瞭解較舊的 SG 版本。例如 "StorageGRID 11.8 物件儲存稽核訊息"：。

程式碼	說明	請參閱
BROR	貯體唯讀要求：已進入或退出唯讀模式的貯體。	"BROR ：貯體唯讀要求"
CBSE	物件傳送結束：來源實體已完成網格節點對網格節點的資料傳輸作業。	"CBSE：物件傳送結束"
CBRE	物件接收結束：目的地實體完成了網格節點對網格節點的資料傳輸作業。	"CBRE：物件接收結束"
CGRR	跨網格複寫要求： StorageGRID 嘗試跨網格複寫作業、以在網格同盟連線中的儲存區之間複寫物件。	"CGRR ：跨網格複寫要求"
EBDL	清空貯體刪除： ILM 掃描器刪除了某個貯體中正在刪除所有物件的物件（執行清空貯體作業）。	"EBDL ：清空庫位刪除"
EBKR	清空貯體申請：使用者傳送要求、要求開啟或關閉清空貯體（即刪除貯體物件或停止刪除物件）。	"EBKR ：清空庫位要求"
SCMT	物件存放區提交：內容區塊已完全儲存並驗證、現在可以申請。	"SCMT ：物件存放區提交要求"
Srem	物件存放區移除：內容區塊已從網格節點刪除、無法再直接要求。	"Srem：物件存放區移除"

StorageGRID 中用於用戶端讀取作業的稽核訊息

S3 用戶端應用程式要求擷取物件時、會記錄用戶端讀取稽核訊息。

程式碼	說明	使用者	請參閱
S3SL	S3 Select 要求：將 S3 Select 要求傳回用戶端後、記錄完成。S3SL 訊息可能包含錯誤訊息和錯誤代碼詳細資料。要求可能未成功。	S3用戶端	"S3SL ： S3 Select 要求"
SGET	S3 Get：記錄成功的交易、以擷取物件或列出儲存區中的物件。 *附註：*如果交易是在子資源上進行、則稽核訊息會包含S3SR欄位。	S3用戶端	"SGET：S3取得"
Shea	S3標頭：記錄成功的交易、以檢查物件或儲存區是否存在。	S3用戶端	"Shea：S3負責人"

StorageGRID 中用戶端寫入作業的稽核訊息

S3 用戶端應用程式要求建立或修改物件時、會記錄用戶端寫入稽核訊息。

程式碼	說明	使用者	請參閱
VW寫入	物件覆寫：記錄交易、以其他物件覆寫一個物件。	S3用戶端	"OW寫入：物件覆寫"
SDEL	S3刪除：記錄成功的交易以刪除物件或儲存區。 *附註：*如果交易是在子資源上進行、則稽核訊息會包含S3SR欄位。	S3用戶端	"SDEL：S3刪除"
SPOS	S3 POST：記錄成功的交易、將物件從AWS Glacier儲存設備還原至雲端儲存池。	S3用戶端	"SPOS：S3 POST"
SPUT	S3 PUT：記錄成功的交易、以建立新的物件或儲存區。 *附註：*如果交易是在子資源上進行、則稽核訊息會包含S3SR欄位。	S3用戶端	"SPUT：S3"
SUPD	S3中繼資料已更新：記錄成功的交易、以更新現有物件或儲存區的中繼資料。	S3用戶端	"SUBPD：S3中繼資料已更新"

StorageGRID 管理稽核訊息

「管理」類別會將使用者要求記錄至管理API。

程式碼	訊息標題與說明	請參閱
MGAU	管理API稽核訊息：使用者要求記錄。	"MGAU：管理稽核訊息"

StorageGRID ILM 稽核訊息

屬於 ILM 稽核類別的稽核訊息會用於與資訊生命週期管理 (ILM) 作業相關的事件。

程式碼	訊息標題與說明	請參閱
理想	ILM初始化刪除：此稽核訊息是在ILM開始刪除物件的程序時產生。	"表意：ILM啟動刪除"
LKCU	覆寫物件清除。此稽核訊息會在自動移除覆寫的物件以釋放儲存空間時產生。	"LKCU：覆寫物件清理"
ORLM	符合的物件規則：此稽核訊息會在物件資料依照 ILM 規則指定儲存時產生。	"ORLM：符合物件規則"

稽核訊息參考

StorageGRID 中儲存貯體唯讀要求的 BROR 稽核訊息

當貯體進入或退出唯讀模式時、 LDR 服務會產生此稽核訊息。例如、當刪除所有物件時、貯體會進入唯讀模式。

程式碼	欄位	說明
BKHD	貯體 UUID	貯體 ID 。
BROV	貯體唯讀要求值	儲存貯體是設為唯讀狀態、或是離開唯讀狀態（ 1 = 唯讀、 0 = 非唯讀）。
Bros	貯體唯讀原因	儲存貯體變成唯讀或離開唯讀狀態的原因。例如、 emptyBucket 。
S3AI	S3 租戶帳戶 ID	傳送要求的租戶帳戶 ID 。空白值表示匿名存取。
S3BK	S3 貯體	S3儲存區名稱。

StorageGRID 中物件接收開始的 CBRB 稽核訊息

在正常系統作業期間、內容區塊會在存取、複寫及保留資料時、在不同節點之間持續傳輸。當內容區塊從一個節點傳輸至另一個節點時、此訊息會由目的地實體發出。

程式碼	欄位	說明
CNID	連線識別碼	節點對節點工作階段/連線的唯一識別碼。
CBID	內容區塊識別碼	要傳輸之內容區塊的唯一識別碼。
CTDR	傳輸方向	表示CBID傳輸是推入初始化還是拉出初始化： 推送：傳送實體要求傳輸作業。 Pull：傳輸作業是由接收實體所要求。
CTSR	來源實體	CBID傳輸來源（傳送者）的節點ID。
CTD	目的地實體	CBID傳輸目的地（接收者）的節點ID。
CTSS	開始順序計數	表示所要求的第一個順序數。如果成功、傳輸會從這個順序數開始。
CTES	預期結束順序計數	表示上次要求的順序數。如果成功、則在收到此順序數後、傳輸即視為完成。
RSRLT	傳輸開始狀態	開始傳輸時的狀態： SUCS：傳輸已成功開始。

此稽核訊息表示節點對節點的資料傳輸作業是在單一內容上啟動、內容區塊識別碼可識別此作業。作業會要求從「開始順序計數」到「預期結束順序計數」的資料。傳送和接收節點會以其節點ID來識別。此資訊可用於追蹤系統資料流、並與儲存稽核訊息結合使用、以驗證複本數。

StorageGRID 中物件接收結束的 **CBRE** 稽核訊息

當內容區塊從一個節點傳輸至另一個節點時、此訊息會由目的地實體發出。

程式碼	欄位	說明
CNID	連線識別碼	節點對節點工作階段/連線的唯一識別碼。
CBID	內容區塊識別碼	要傳輸之內容區塊的唯一識別碼。
CTDR	傳輸方向	表示CBID傳輸是推入初始化還是拉出初始化： 推送：傳送實體要求傳輸作業。 Pull：傳輸作業是由接收實體所要求。
CTSR	來源實體	CBID傳輸來源（傳送者）的節點ID。

程式碼	欄位	說明
CTD	目的地實體	CBID傳輸目的地（接收者）的節點ID。
CTSS	開始順序計數	表示開始傳輸的順序數。
TA	實際結束順序計數	表示上次成功傳輸的順序數。如果實際結束順序計數與開始順序計數相同、且傳輸結果不成功、則不會交換任何資料。
RSRLT	傳輸結果	傳輸作業的結果（從傳送實體的觀點來看）： SUCS：傳輸成功完成；已傳送所有要求的順序計數。 COLL：傳輸期間連線中斷 CTMO：建立或傳輸期間連線逾時 UNDE：無法連線目的地節點ID CRPT ：由於接收到毀損或無效的資料、因此傳輸已結束

此稽核訊息表示節點對節點資料傳輸作業已完成。如果傳輸結果成功、則作業會將資料從「開始順序計數」傳輸至「實際結束順序計數」。傳送和接收節點會以其節點ID來識別。此資訊可用於追蹤系統資料流、以及找出、製表及分析錯誤。搭配儲存稽核訊息時、也可用來驗證複本數。

StorageGRID 中物件傳送開始的 **CBSB** 稽核訊息

在正常系統作業期間、內容區塊會在存取、複寫及保留資料時、在不同節點之間持續傳輸。當內容區塊從一個節點傳輸至另一個節點時、此訊息會由來源實體發出。

程式碼	欄位	說明
CNID	連線識別碼	節點對節點工作階段/連線的唯一識別碼。
CBID	內容區塊識別碼	要傳輸之內容區塊的唯一識別碼。
CTDR	傳輸方向	表示CBID傳輸是推入初始化還是拉出初始化： 推送：傳送實體要求傳輸作業。 Pull：傳輸作業是由接收實體所要求。
CTSR	來源實體	CBID傳輸來源（傳送者）的節點ID。
CTD	目的地實體	CBID傳輸目的地（接收者）的節點ID。
CTSS	開始順序計數	表示所要求的第一個順序數。如果成功、傳輸會從這個順序數開始。

程式碼	欄位	說明
CTES	預期結束順序計數	表示上次要求的順序數。如果成功、則在收到此順序數後、傳輸即視為完成。
RSRLT	傳輸開始狀態	開始傳輸時的狀態： SUCS：傳輸已成功開始。

此稽核訊息表示節點對節點的資料傳輸作業是在單一內容上啟動、內容區塊識別碼可識別此作業。作業會要求從「開始順序計數」到「預期結束順序計數」的資料。傳送和接收節點會以其節點ID來識別。此資訊可用於追蹤系統資料流、並與儲存稽核訊息結合使用、以驗證複本數。

StorageGRID 中物件傳送結束的 **CBSE** 稽核訊息

當內容區塊從一個節點傳輸至另一個節點時、此訊息會由來源實體發出。

程式碼	欄位	說明
CNID	連線識別碼	節點對節點工作階段/連線的唯一識別碼。
CBID	內容區塊識別碼	要傳輸之內容區塊的唯一識別碼。
CTDR	傳輸方向	表示CBID傳輸是推入初始化還是拉出初始化： 推送：傳送實體要求傳輸作業。 Pull：傳輸作業是由接收實體所要求。
CTSR	來源實體	CBID傳輸來源（傳送者）的節點ID。
CTD	目的地實體	CBID傳輸目的地（接收者）的節點ID。
CTSS	開始順序計數	表示開始傳輸的順序數。
TA	實際結束順序計數	表示上次成功傳輸的順序數。如果實際結束順序計數與開始順序計數相同、且傳輸結果不成功、則不會交換任何資料。

程式碼	欄位	說明
RSRLT	傳輸結果	傳輸作業的結果（從傳送實體的觀點來看）： SUCS：傳輸成功完成；已傳送所有要求的順序計數。 COLL：傳輸期間連線中斷 CTMO：建立或傳輸期間連線逾時 UNDE：無法連線目的地節點ID CRPT ：由於接收到毀損或無效的資料、因此傳輸已結束

此稽核訊息表示節點對節點資料傳輸作業已完成。如果傳輸結果成功、則作業會將資料從「開始順序計數」傳輸至「實際結束順序計數」。傳送和接收節點會以其節點ID來識別。此資訊可用於追蹤系統資料流、以及找出、製表及分析錯誤。搭配儲存稽核訊息時、也可用來驗證複本數。

StorageGRID 中跨網格複寫請求的 **CGRR** 稽核訊息

當 StorageGRID 嘗試跨網格複寫作業來複寫網格同盟連線中的資料桶之間的物件時、就會產生此訊息。

程式碼	欄位	說明
CSIZ	物件大小	物件大小（以位元組為單位）。 StorageGRID 11.8 引進了 CSEZ 屬性。因此、跨越 StorageGRID 11.7 至 11.8 升級的跨網格複寫要求、可能會有不正確的物件總大小。
S3AI	S3 租戶帳戶 ID	擁有要複寫物件之桶的租戶帳戶 ID 。
GFID	網格同盟連線 ID	用於跨網格複寫的網格同盟連線 ID 。
操作者	CGR 作業	嘗試的跨網格複寫作業類型： • 0 = 複寫物件 • 1 = 複寫多個部分物件 • 2 = 複寫刪除標記
S3BK	S3 貯體	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。
VSID	版本ID	正在複寫之物件之特定版本的版本 ID 。

程式碼	欄位	說明
RSRLT	結果代碼	傳回成功（ SUCS ）或一般錯誤（ GERR ）。

StorageGRID 中空白儲存貯體物件刪除的 **EBDL** 稽核訊息

ILM 掃描器刪除了儲存庫中刪除所有物件的物件（執行清空儲存庫作業）。

程式碼	欄位	說明
CSIZ	物件大小	物件大小（以位元組為單位）。
路徑	S3 鏟斗 / 金鑰	S3 貯體名稱和 S3 金鑰名稱。
SEGC	容器 UUID	分割物件容器的 UUID 。此值僅在物件分段時可用。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
RSRLT	刪除作業的結果	事件、程序或交易的結果。如果與訊息無關、則不會使用任何訊息、而不會使用SUCS、因此不會意外篩選訊息。

StorageGRID 中空白儲存貯體要求的 **EBKR** 稽核訊息

此訊息表示使用者已傳送開啟或關閉清空貯體（即刪除貯體物件或停止刪除物件）的要求。

程式碼	欄位	說明
BUID	貯體 UUID	貯體 ID 。
EBJS	清空 Bucket JSON 組態	包含代表目前空白 Bucket 組態的 JSON 。
S3AI	S3 租戶帳戶 ID	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。

StorageGRID 中遺失銷毀編碼資料的 **ECMC** 稽核訊息

此稽核訊息表示系統偵測到遺失的銷毀編碼資料片段。

程式碼	欄位	說明
VCMC	VCS ID	包含遺失區塊的VCS名稱。

程式碼	欄位	說明
MCID	區塊ID	遺失銷毀編碼片段的識別碼。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此特定訊息無關。使用「無」而非「UCS」、因此不會篩選此訊息。

StorageGRID 中毀損的抹除編碼資料的 **ECOC** 稽核訊息

此稽核訊息表示系統偵測到毀損的銷毀編碼資料片段。

程式碼	欄位	說明
VCCO	VCS ID	包含毀損區塊的VCS名稱。
VLID	Volume ID	包含毀損的銷毀編碼片段的R地理DB Volume。
CCID	區塊ID	毀損的銷毀編碼片段的識別碼。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此特定訊息無關。使用「無」而非「UCS」、因此不會篩選此訊息。

StorageGRID 中安全驗證失敗的 **ETAF** 稽核訊息

當使用傳輸層安全性（TLS）的連線嘗試失敗時、就會產生此訊息。

程式碼	欄位	說明
CNID	連線識別碼	驗證失敗之TCP/IP連線的唯一系統識別碼。
RUID	使用者身分識別	代表遠端使用者身分的服務相依識別碼。

程式碼	欄位	說明
RSRLT	原因代碼	故障原因： SCNI：安全連線建立失敗。 CERM：缺少憑證。 認證：認證無效。 cere：憑證已過期。 CERR：憑證已撤銷。 CSGN：憑證簽章無效。 CSGU：憑證簽署者不明。 UCRM：缺少使用者認證資料。 UCRI：使用者認證無效。 UCRU：不允許使用者認證。 Tout：驗證逾時。

建立連線至使用TLS的安全服務時、會使用TLS設定檔和服務內建的其他邏輯來驗證遠端實體的認證。如果此驗證因為無效、非預期或不允許的憑證或認證而失敗、則會記錄稽核訊息。如此可針對未獲授權的存取嘗試和其他與安全性相關的連線問題進行查詢。

此訊息可能是因為遠端實體的組態不正確、或是嘗試向系統提供無效或不允許的認證資料。應監控此稽核訊息、以偵測嘗試取得未獲授權的系統存取權。

StorageGRID 中 GNDS 註冊的 GNRG 稽核訊息

當服務已更新StorageGRID 或登錄有關自身的資訊、並將其登錄到該系統時、CMN服務會產生此稽核訊息。

程式碼	欄位	說明
RSRLT	結果	更新要求的結果： • SUCS：成功 • SUNVM：服務無法使用 • GERR:其他故障
GNID	節點 ID	啟動更新要求之服務的節點ID。
GNTP	裝置類型	網格節點的裝置類型（例如、用於LMR服務的BLDR）。

程式碼	欄位	說明
GNDV	裝置機型版本	在DMDL套裝組合中識別網格節點裝置型號版本的字串。
GNGP	群組	網格節點所屬的群組（在連結成本和服務查詢排名的內容中）。
GNIA	IP位址	網格節點的IP位址。

每當網格節點更新其在Grid Node產品組合中的項目時、就會產生此訊息。

StorageGRID 中 **GNDS** 取消註冊的 **GNUR** 稽核訊息

當服務從StorageGRID 該系統中取消登錄其本身的資訊時、CMN服務會產生此稽核訊息。

程式碼	欄位	說明
RSRLT	結果	更新要求的結果： • SUCS：成功 • SUNVM：服務無法使用 • GERR:其他故障
GNID	節點 ID	啟動更新要求之服務的節點ID。

StorageGRID 中已結束網格工作的 **GTED** 稽核訊息

此稽核訊息表示CMN服務已完成處理指定的網格工作、並已將工作移至「歷史」表格。如果結果為SUCS、ABRT或ROLf、則會出現對應的Grid工作已開始稽核訊息。其他結果則表示此網格工作的處理從未開始。

程式碼	欄位	說明
TSID	工作ID	此欄位可唯一識別所產生的網格工作、並可讓網格工作在其生命週期內進行管理。 *附註：*工作ID是在產生網格工作時指派、而非在提交時指派。指定的網格工作可以多次提交、在此情況下、「工作ID」欄位不足以唯一連結已提交、已啟動及已結束的稽核訊息。

程式碼	欄位	說明
RSRLT	結果	網格工作的最終狀態結果： • SUCS：已成功完成網格工作。 • ABRT ：網格工作已終止、沒有復原錯誤。 • Rolf ：網格工作已終止、無法完成復原程序。 • 取消：網格工作在啟動之前已由使用者取消。 • 支出：網格工作在開始之前即過期。 • IVLD：網格工作無效。 • 驗證：網格工作未獲授權。 • DUPL：網格工作遭拒為重複項目。

StorageGRID 中已啟動網格任務的 **GTST** 稽核訊息

此稽核訊息表示CMN服務已開始處理指定的網格工作。稽核訊息會緊接著Grid工作提交訊息、顯示內部Grid工作提交服務所啟動並選取自動啟動的網格工作。對於提交至「擱置」資料表的網格工作、此訊息會在使用者啟動網格工作時產生。

程式碼	欄位	說明
TSID	工作ID	此欄位可唯一識別所產生的網格工作、並允許在其生命週期內管理該工作。 *附註：*工作ID是在產生網格工作時指派、而非在提交時指派。指定的網格工作可以多次提交、在此情況下、「工作ID」欄位不足以唯一連結已提交、已啟動及已結束的稽核訊息。
RSRLT	結果	結果。此欄位只有一個值： • SUCS：已成功啟動網格工作。

StorageGRID 中已提交網格任務的 **GTSU** 稽核訊息

此稽核訊息表示已將網格工作提交至CMN服務。

程式碼	欄位	說明
TSID	工作ID	唯一識別產生的網格工作、並允許在工作生命週期內進行管理。 *附註：*工作ID是在產生網格工作時指派、而非在提交時指派。指定的網格工作可以多次提交、在此情況下、「工作ID」欄位不足以唯一連結已提交、已啟動及已結束的稽核訊息。
TTWYP	工作類型	網格工作類型。

程式碼	欄位	說明
TVER	工作版本	表示網格工作版本的數字。
TDSC	工作說明	人類可讀的網格工作說明。
Vat	時間戳記後有效	網格工作有效的最早時間（UINT64微秒、自1970年1月1日起- UNIX時間）。
VBTS	時間戳記前有效	網格工作有效的最新時間（UINT64微秒、自1970年1月1日起- UNIX時間）。
TSRC	來源	工作來源： • TXTB：網格工作是以StorageGRID 簽署的文字區塊形式透過申請表系統提交。 • 網格：網格工作是透過內部網格工作提交服務提交。
ACTV	啟動類型	啟動類型： • 自動：已提交網格工作以供自動啟動。 • PEND：網格工作已提交至擱置的資料表。這是唯一可用於TXTB來源的可能性。
RSRLT	結果	提交結果： • SUCS：已成功提交網格工作。 • 失敗：工作已直接移至歷史表格。

StorageGRID 中 **ILM** 啟動刪除的 **IDEL** 稽核訊息

此訊息是在ILM開始刪除物件的程序時產生。

idel訊息會在下列任一情況下產生：

- 對於相容**S3**儲存區中的物件：此訊息是在ILM啟動自動刪除物件的程序時產生、因為物件的保留期間已過期（假設已啟用自動刪除設定且合法保留已關閉）。
- * 適用於不相容 S3 儲存區中的物件 * 。此訊息是在 ILM 開始刪除物件的程序時產生、因為目前使用中 ILM 原則中沒有套用到物件的放置指示。

程式碼	欄位	說明
CBID	內容區塊識別碼	物件的CBID。
CMPa.	法規遵循：自動刪除	僅適用於相容S3儲存區中的物件。0（假）或1（真）、表示在保留期間結束時、是否應自動刪除相容物件、除非儲存區處於合法持有狀態。

程式碼	欄位	說明
Cmpl	法規遵循：合法持有	僅適用於相容S3儲存區中的物件。0（假）或1（真）、表示該儲存桶目前是否處於合法持有狀態。
CMPR	法規遵循：保留期間	僅適用於相容S3儲存區中的物件。物件保留期間的長度（以分鐘為單位）。
CTME	法規遵循：擷取時間	僅適用於相容S3儲存區中的物件。物件的擷取時間。您可以將保留期間（以分鐘為單位）新增至此值、以決定何時可從儲存區刪除物件。
DMRK	刪除標記版本ID	從版本控制的儲存區刪除物件時所建立的刪除標記版本ID。貯體的作業不包括此欄位。
CSIZ	內容大小	物件大小（以位元組為單位）。
LOCS	位置	物件資料在StorageGRID 整個作業系統中的儲存位置。如果物件沒有位置（例如、已刪除）、LOCS的值為「」。 CLEC ：對於銷毀編碼物件、抹除編碼設定檔 ID 、以及套用至物件資料的銷毀編碼群組 ID 。 CLDI：對於複寫的物件、則為該物件位置的LDR節點ID和Volume ID。 CLNL：物件資料歸檔時物件位置的旋轉節點ID。
路徑	S3 鏟斗 / 金鑰	S3 貯體名稱和 S3 金鑰名稱。
RSRLT	結果	ILM作業的結果。 SUCS：ILM作業成功。
規則	規則標籤	• 如果相容S3儲存區中的物件因為保留期間已過期而自動刪除、則此欄位為空白。 • 如果物件因為目前沒有更多套用至物件的放置指示而被刪除、此欄位會顯示套用至物件的上一個ILM規則的人類可讀取標籤。
SGRP	站台（群組）	如果存在、則會在指定的站台刪除物件、而非擷取物件的站台。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	已刪除物件的特定版本的版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中覆寫物件清理的 **LKCU** 稽核訊息

此訊息是在StorageGRID 將先前需要清除以釋放儲存空間的覆寫物件移除時產生。當 S3 用戶端將物件寫入已包含物件的路徑時、物件會被覆寫。移除程序會自動在背景執行。

程式碼	欄位	說明
CSIZ	內容大小	物件大小（以位元組為單位）。
LTYP	清理類型	僅限內部使用。
LUID	移除物件UUID	已移除物件的識別碼。
路徑	S3 鏟斗 / 金鑰	S3 貯體名稱和 S3 金鑰名稱。
SEGC	容器 UUID	分割物件容器的 UUID 。此值僅在物件分段時可用。
UUID	通用唯一識別碼	仍存在的物件識別碼。此值只有在物件尚未刪除時才能使用。

StorageGRID 中洩漏物件清理的 **LKDM** 稽核訊息

當清除或刪除外洩的區塊時、就會產生此訊息。區塊可以是複寫物件或抹除編碼物件的一部分。

程式碼	欄位	說明
CLOC	區塊位置	被刪除的外洩區塊的檔案路徑。

CTYP	區塊類型	區塊類型：
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

程式碼	欄位	說明

LTYP	洩漏類型	可偵測到的五種洩漏類型：
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	區塊建立時間	建立外洩區塊的時間。
UUID	通用唯一識別碼	區塊所屬物件的識別碼。
CBID	內容區塊識別碼	外洩區塊所屬物件的 CBID 。
CSIZ	內容大小	區塊大小（以位元組為單位）。

StorageGRID 中遺失物件複本位置的 **LLST** 稽核訊息

每當找不到物件複本（複寫或刪除編碼）的位置時、就會產生此訊息。

程式碼	欄位	說明
CBIL	CBID	受影響的CBID。
ECPR	銷毀編碼設定檔	用於以銷毀編碼的物件資料。使用的銷毀編碼設定檔 ID 。
LTYP	位置類型	CLDI（線上）：適用於複寫的物件資料 CLEC（線上）：用於以銷毀編碼的物件資料 CLNL（Nearline）：用於歸檔的複寫物件資料
NOID	來源節點ID	遺失位置的節點ID。

程式碼	欄位	說明
PCLD	複寫物件的路徑	通往遺失物件資料之磁碟位置的完整路徑。只有當LTYP的值為CLDI（即複寫物件）時才會傳回。 採取這種形式 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSRLT	結果	永遠無。RSRLT為必填訊息欄位、但與此訊息無關。使用「無」而非「無」、以不篩選此訊息。
TSRC	觸發來源	使用者：使用者觸發 Syst：系統觸發
UUID	通用唯一ID	受影響物件在StorageGRID 整個作業系統中的識別碼。

StorageGRID 中管理 **API** 請求的 **MGAU** 稽核訊息

「管理」類別會將使用者要求記錄至管理API。每個不是取得或發出有效 API URI 要求的 HTTP 要求、都會記錄一個回應、其中包含 API 的使用者名稱、 IP 和要求類型。不會記錄無效的 API URI （例如 /API/v3 授權）、以及對有效 API URI 的無效要求。

程式碼	欄位	說明
MDIP	目的地IP位址	伺服器（目的地）IP位址。
MDNA	網域名稱	主機網域名稱。
MPAT	要求路徑	要求路徑。
MPQP	要求查詢參數	要求的查詢參數。
MRBD	申請本文	申請本文的內容。當回應本文預設為記錄時、在某些情況下、當回應本文為空白時、會記錄要求本文。由於下列資訊無法在回應本文中取得、因此會從下列POST方法的要求本文中取得： • * POST授權*中的使用者名稱和帳戶ID • 在* POST / GRID / GRID網路/更新*中設定新的子網路 • 在* POST / GRID / NTP-伺服器/更新*中新增NTP伺服器 • 在* POST / GRID /伺服器/取消委任*中停用伺服器ID *附註：*敏感資訊會被刪除（例如S3存取金鑰）、或以星號（例如密碼）遮罩。

程式碼	欄位	說明
MRMD	申請方法	HTTP要求方法： • 貼文 • 放入 • 刪除 • 修補程式
MRSC	回應代碼	回應代碼。
MRSP	回應本文	預設會記錄回應內容（回應本文）。 *附註：*敏感資訊會被刪除（例如S3存取金鑰）、或以星號（例如密碼）遮罩。
MSIP	來源IP位址	用戶端（來源）IP位址。
多重複使用者	使用者URN	傳送要求之使用者的URN（統一資源名稱）。
RSRLT	結果	傳回成功（SUCS）或後端報告的錯誤。

StorageGRID 中系統偵測到遺失物件的 **OLST** 稽核訊息

當 DDS 服務找不到 StorageGRID 系統中物件的任何複本時、就會產生此訊息。

程式碼	欄位	說明
CBID	內容區塊識別碼	遺失物件的CBID。
NOID	節點 ID	如果可用、則為遺失物件的最後一個已知直接或近線位置。如果無法取得磁碟區資訊、則只能使用沒有Volume ID的節點ID。
路徑	S3 鏟斗 / 金鑰	S3 儲存區名稱和 S3 金鑰名稱（如果有）。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此訊息無關。使用「無」而非「無」、以不篩選此訊息。
UUID	通用唯一ID	在整個系統中遺失物件的識別碼StorageGRID 。
VOLI	Volume ID	如果可用、儲存節點的 Volume ID 會顯示遺失物件的最後已知位置。

此訊息是在物件依照ILM規則所指定的方式成功儲存及複製時產生。

如果原則中的另一個規則使用「物件大小」進階篩選器、則預設的「製作2份複本」規則會成功儲存物件時、不會產生ORLM訊息。

程式碼	欄位	說明
BUID	鏟斗接頭	「庫位ID」欄位。用於內部作業。僅當「立即給藥」為PRGD時才會顯示。
CBID	內容區塊識別碼	物件的CBID。
CSIZ	內容大小	物件大小（以位元組為單位）。
LOCS	位置	物件資料在StorageGRID 整個作業系統中的儲存位置。如果物件沒有位置（例如、已刪除）、LOCS的值為「」。 CLEC ：對於銷毀編碼物件、抹除編碼設定檔 ID 、以及套用至物件資料的銷毀編碼群組 ID 。 CLDI：對於複寫的物件、則為該物件位置的LDR節點ID和Volume ID。 CLNL：物件資料歸檔時物件位置的旋轉節點ID。
路徑	S3 鏟斗 / 金鑰	S3 貯體名稱和 S3 金鑰名稱。
RSRLT	結果	ILM作業的結果。 SUCS：ILM作業成功。
規則	規則標籤	套用至此物件之ILM規則的人工讀取標籤。
SEGC	容器 UUID	分割物件容器的 UUID 。此值僅在物件分段時可用。
SGCB	容器 CBID	分割物件容器的 CBID 。此值僅適用於分段和多部分物件。
立即	狀態	ILM作業的狀態。 完成：針對物件的ILM作業已完成。 DFER：此物件已標記為未來ILM重新評估。 PRGD：此物件已從StorageGRID 該系統中刪除。 NLOC：物件資料無法再在StorageGRID 整個系統中找到。此狀態可能表示物件資料的所有複本遺失或損壞。

程式碼	欄位	說明
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	在版本控制儲存區中建立的新物件版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

ORLM 稽核訊息可針對單一物件發出多次。例如、只要發生下列其中一項事件、就會發出此訊息：

- 物件的ILM規則永遠都能滿足。
- 在此時期、物件的ILM規則已符合要求。
- ILM規則已刪除物件。
- 背景驗證程序會偵測複寫物件資料的複本是否毀損。該系統會執行ILM評估、以取代毀損的物件。StorageGRID

相關資訊

- "物件擷取交易"
- "物件刪除交易"

StorageGRID 中物件覆寫的 OVWR 稽核訊息

當外部（用戶端要求）作業導致一個物件被另一個物件覆寫時、就會產生此訊息。

程式碼	欄位	說明
CBID	內容區塊識別碼（新增）	新物件的CBID。
CSIZ	上一個物件大小	被覆寫物件的大小（以位元組為單位）。
OCBD	內容區塊識別碼（上一頁）	前一個物件的CBID。
UUID	通用唯一ID（新）	更新物件的識別碼StorageGRID 。
OUID	通用唯一ID（先前）	在整個過程中、先前物件在StorageGRID 整個過程中的識別碼。
路徑	S3 物件路徑	S3 物件路徑同時用於上一個物件和新物件
RSRLT	結果代碼	物件覆寫交易的結果。結果永遠是： SUCS：成功

程式碼	欄位	說明
SGRP	站台（群組）	如果有覆寫的物件、則會在指定的站台刪除、而非擷取覆寫物件的站台。

StorageGRID 中 **S3 Select** 請求的 **S3SL** 稽核訊息

此訊息會在 S3 Select 要求傳回用戶端後記錄完成。S3SL 訊息可能包含錯誤訊息和錯誤代碼詳細資料。要求可能未成功。

程式碼	欄位	說明
BYSC	掃描的位元組數	從儲存節點掃描（接收）的位元組數。 如果物件經過壓縮、 BYSC 和 BYPR 可能會有所不同。如果物件經過壓縮、 BYSC 會有壓縮的位元組數、而 BYPR 會是解壓縮後的位元組數。
BYPR	已處理位元組	處理的位元組數。指出 S3 Select 工作實際處理或處理多少位元組的「掃描位元組」。
BYRT	傳回位元組	S3 Select 工作傳回用戶端的位元組數。
重新報告	已處理記錄	S3 Select 工作從儲存節點接收的記錄或資料列數。
RERT	已傳回記錄	S3 Select 工作傳回用戶端的記錄或列數。
JOFI	工作已完成	指出 S3 Select 工作是否已完成處理。如果這是錯誤的、則工作無法完成、而且錯誤欄位中可能有資料。用戶端可能已收到部分結果、或根本沒有結果。
Reid	申請 ID	S3 Select 要求的識別碼。
EXTM	執行時間	S3 Select 工作完成所需的時間（以秒為單位）。
ERMG	錯誤訊息	S3 Select 工作產生的錯誤訊息。
很不一樣	錯誤類型	S3 Select 工作產生的錯誤類型。
第	Stacktrace 錯誤	S3 Select 工作產生的錯誤堆疊追蹤。
S3BK	S3 貯體	S3儲存區名稱。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的 S3 存取金鑰 ID 。

程式碼	欄位	說明
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。

StorageGRID 中停用安全稽核的 SADD 稽核訊息

此訊息表示來源服務（節點 ID）已關閉稽核訊息日誌記錄。StorageGRID 不再收集或傳遞稽核訊息。

程式碼	欄位	說明
AeTM	啟用方法	用來停用稽核的方法。
AE	使用者名稱	執行命令以停用稽核記錄的使用者名稱。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此訊息無關。使用「無」而非「無」、以不篩選此訊息。

此訊息表示先前已啟用記錄、但現在已停用。這通常只會在大量擷取期間使用、以改善系統效能。在大量活動之後、系統會還原稽核（減量）、然後永久封鎖停用稽核的功能。

StorageGRID 中安全稽核啟用的 SADE 稽核訊息

此訊息表示來源服務（節點 ID）已還原稽核訊息日誌記錄。StorageGRID 再次收集和傳遞稽核訊息。

程式碼	欄位	說明
AeTM	啟用方法	用於啟用稽核的方法。
AE	使用者名稱	執行命令以啟用稽核記錄的使用者名稱。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此訊息無關。使用「無」而非「無」、以不篩選此訊息。

此訊息表示記錄先前已停用（SADD）、但現在已還原。這通常只會在大量擷取期間使用、以改善系統效能。在大量活動之後、系統會還原稽核、並永久封鎖停用稽核的功能。

StorageGRID 中物件存放區認可的 SCMT 稽核訊息

在提交網格內容之前、網格內容將無法使用或辨識為儲存內容（亦即持續儲存）。持續儲存的內容已完全寫入磁碟、並通過相關的完整性檢查。此訊息會在內容區塊提交至儲存設備時發出。

程式碼	欄位	說明
CBID	內容區塊識別碼	提交至永久儲存設備之內容區塊的唯一識別碼。
RSRLT	結果代碼	物件儲存至磁碟時的狀態： SUCS：物件已成功儲存。

此訊息表示指定的內容區塊已完全儲存並驗證、現在可以要求。它可用於追蹤系統內的資料流。

StorageGRID 中 **S3 DELETE** 交易的 **SDEL** 稽核訊息

當 S3 用戶端發出刪除交易時、系統會要求移除指定的物件或貯體、或移除貯體 / 物件子資源。如果交易成功、伺服器就會發出此訊息。

程式碼	欄位	說明
ASRS	假定角色工作階段 URN	所扮演角色工作階段的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
ASRU	假定角色 URN	所扮演角色的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。貯體的作業不包括此欄位。
CNCH	一致性控制標頭	一致性控制HTTP要求標頭的值（如果要求中有的話）。
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	刪除物件的大小（以位元組為單位）。貯體的作業不包括此欄位。
DMRK	刪除標記版本ID	從版本控制的儲存區刪除物件時所建立的刪除標記版本ID。貯體的作業不包括此欄位。
GFID	Grid Federation Connection ID	與跨網格複寫刪除要求相關聯的網格同盟連線連線 ID 。僅包含在目的地網格上的稽核記錄中。
GVSA	Grid Federation 來源帳戶 ID	跨網格複寫刪除要求之來源網格上租用戶的帳戶 ID 。僅包含在目的地網格上的稽核記錄中。

程式碼	欄位	說明
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。 `x-amz-bypass-governance-retention`會在申請中自動加入。
MTME	上次修改時間	Unix時間戳記（以微秒為單位）、表示上次修改物件的時間。
RSRLT	結果代碼	刪除交易的結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
S3SR	S3子資源	要操作的庫位或物件子資源（若適用）。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。
SGRP	站台（群組）	如果存在、則會在指定的站台刪除物件、而非擷取物件的站台。

程式碼	欄位	說明
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。
UUDM	刪除標記的通用唯一識別碼	刪除標記的識別碼。稽核記錄訊息會指定 UUDM 或 UUID 、其中 UUDM 表示因物件刪除要求而建立的刪除標記、 UUID 則表示物件。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	已刪除物件的特定版本的版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中 **S3 GET** 交易的 **SGET** 稽核訊息

當 S3 用戶端發出 GET 交易時、系統會要求擷取物件或列出貯體中的物件、或移除貯體 / 物件子資源。如果交易成功、伺服器就會發出此訊息。

程式碼	欄位	說明
ASRS	假定角色工作階段 URN	所扮演角色工作階段的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
ASRU	假定角色 URN	所扮演角色的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。貯體的作業不包括此欄位。
CNCH	一致性控制標頭	一致性控制HTTP要求標頭的值（如果要求中有的話）。
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	擷取物件的大小（以位元組為單位）。貯體的作業不包括此欄位。

程式碼	欄位	說明
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。
實用	清單對象V2.	已要求 _v2 格式 _ 回應。如需詳細資訊、請參閱 "AWS ListObjectsV2"。僅適用於取得貯體作業。
NCHD	子項目數	包含金鑰和通用首碼。僅適用於取得貯體作業。
振鈴	範圍讀取	僅適用於範圍讀取作業。指出此要求讀取的位元組範圍。斜槓（/）後面的值會顯示整個物件的大小。
RSRLT	結果代碼	Get交易的結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
S3SR	S3子資源	要操作的庫位或物件子資源（若適用）。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。

程式碼	欄位	說明
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。
TRNC	截斷或不截斷	如果傳回所有結果、請設為 False 。如果有更多結果可供傳回、請設為 true 。僅適用於取得貯體作業。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	所要求之物件的特定版本的版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中 **S3 HEAD** 操作的 **SHEA** 稽核訊息

當 S3 用戶端發出 HEAD 操作時，會發出請求來檢查物件或儲存桶是否存在並擷取有關物件的元資料。如果操作成功，伺服器將發出此訊息。

程式碼	欄位	說明
ASRS	假定角色工作階段 URN	所扮演角色工作階段的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
ASRU	假定角色 URN	所扮演角色的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。貯體的作業不包括此欄位。
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	已檢查物件的大小（以位元組為單位）。貯體的作業不包括此欄位。

程式碼	欄位	說明
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。
RSRLT	結果代碼	Get交易的結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。

程式碼	欄位	說明
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	所要求之物件的特定版本的版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中 **S3 POST** 交易的 **SPOS** 稽核訊息

當S3用戶端發出POST物件要求時、如果交易成功、伺服器就會發出此訊息。

程式碼	欄位	說明
ASRS	假定角色工作階段 URN	所扮演角色工作階段的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
ASRU	假定角色 URN	所扮演角色的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。
CNCH	一致性控制標頭	一致性控制HTTP要求標頭的值（如果要求中有的話）。
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	擷取物件的大小（以位元組為單位）。
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。 （不適用於 SPOS ）。
RSRLT	結果代碼	RestoreObject 要求的結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。

程式碼	欄位	說明
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
S3SR	S3子資源	要操作的庫位或物件子資源（若適用）。 將 S3 Select 作業設為「 SELECT 」。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。
SRCF	子資源組態	還原資訊：
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	所要求之物件的特定版本的版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中 **S3 PUT** 交易的 **SPUT** 稽核訊息

當 S3 用戶端發出 Put 交易時、系統會要求建立新的物件或儲存庫、或移除儲存庫 / 物件

子資源。如果交易成功、伺服器就會發出此訊息。

程式碼	欄位	說明
ASRS	假定角色工作階段 URN	所扮演角色工作階段的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
ASRU	假定角色 URN	所扮演角色的唯一識別碼。 只有當 S3 請求使用來自 AssumeRole 請求的臨時安全性憑證時才會出現。
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。貯體的作業不包括此欄位。
CMP	法規遵循設定	建立貯體時所使用的規範設定（如果存在於要求中）（被截斷為前 1024 個字元）。
CNCH	一致性控制標頭	一致性控制HTTP要求標頭的值（如果要求中有的話）。
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	擷取物件的大小（以位元組為單位）。貯體的作業不包括此欄位。
GFID	Grid Federation Connection ID	與跨網格複寫置入要求相關聯的網格同盟連線連線 ID 。僅包含在目的地網格上的稽核記錄中。
GVSA	Grid Federation 來源帳戶 ID	跨網格複寫置入要求來源網格上租用戶的帳戶 ID 。僅包含在目的地網格上的稽核記錄中。
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。 `x-amz-bypass-governance-retention`會在申請中自動加入。
LKEN	物件鎖定已啟用	請求標題的值 `x-amz-bucket-object-lock-enabled`（如果存在於請求中）。
LKLH	物件鎖定合法持有	請求標頭的值 `x-amz-object-lock-legal-hold`（如果 PuttObject 請求中存在）。

程式碼	欄位	說明
LKMD	物件鎖定保留模式	請求標頭的值 `x-amz-object-lock-mode`（如果 PuttObject 請求中存在）。
LKRU	物件鎖定保留至日期	請求標頭的值 `x-amz-object-lock-retain-until-date`（如果 PuttObject 請求中存在）。值限制在擷取物件的日期後 100 年內。
MTME	上次修改時間	Unix時間戳記（以微秒為單位）、表示上次修改物件的時間。
RSRLT	結果代碼	交易結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
S3SR	S3子資源	要操作的庫位或物件子資源（若適用）。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。
SRCF	子資源組態	新的子資源組態（截至前1024個字元）。
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。

程式碼	欄位	說明
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。
使用者ID	上傳ID	僅包含在用於 CompleteMultpartUpload 作業的 SPUT 訊息中。表示所有零件均已上傳和組裝。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	在版本控制儲存區中建立的新物件版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。
VSST	版本管理狀態	儲存區的新版本管理狀態。使用兩種狀態：「啟用」或「暫停」。物件上的作業不包含此欄位。

StorageGRID 中物件存放區移除的 **SREM** 稽核訊息

此訊息會在內容從持續儲存設備中移除時發出、而且無法再透過一般API存取。

程式碼	欄位	說明
CBID	內容區塊識別碼	從永久儲存設備刪除之內容區塊的唯一識別碼。
RSRLT	結果代碼	指出內容移除作業的結果。唯一定義的值是： SUCS：從持續儲存設備移除內容

此稽核訊息表示已從節點刪除指定的內容區塊、因此無法再直接要求。此訊息可用於追蹤系統中刪除內容的流程。

StorageGRID 中 **S3** 中繼資料更新的 **SUPD** 稽核訊息

當S3用戶端更新擷取物件的中繼資料時、此訊息會由S3 API產生。如果中繼資料更新成功、伺服器就會發出此訊息。

程式碼	欄位	說明
CBID	內容區塊識別碼	所要求內容區塊的唯一識別碼。如果CBID未知、此欄位會設定為0。貯體的作業不包括此欄位。
CNCH	一致性控制標頭	更新儲存區的法規遵循設定時、一致性控制HTTP要求標頭的值（若要求中有）。

程式碼	欄位	說明
CNID	連線識別碼	TCP/IP連線的唯一系統識別碼。
CSIZ	內容大小	擷取物件的大小（以位元組為單位）。貯體的作業不包括此欄位。
HTRH	HTTP要求標頭	設定期間選取的記錄HTTP要求標頭名稱和值清單。 `X-Forwarded-For`如果存在於要求中、且值與要求寄件者 IP 位址（ SAIP 稽核欄位）不同、則會自動納入 `X-Forwarded-For`。
RSRLT	結果代碼	Get交易的結果。結果永遠是： SUCS：成功
S3AI	S3租戶帳戶ID（要求寄件者）	傳送要求之使用者的租戶帳戶ID。空白值表示匿名存取。
S3AK	S3存取金鑰ID（要求傳送者）	傳送要求之使用者的雜湊S3存取金鑰ID。空白值表示匿名存取。
S3BK	S3時段	S3儲存區名稱。
S3KY	S3金鑰	S3金鑰名稱、不含儲存區名稱。貯體的作業不包括此欄位。
SACC	S3租戶帳戶名稱（要求寄件者）	傳送要求之使用者的租戶帳戶名稱。匿名要求為空白。
SAIP	IP位址（要求傳送者）	發出要求的用戶端應用程式IP位址。
小型企業	S3租戶帳戶名稱（庫位擁有者）	庫位擁有者的租戶帳戶名稱。用於識別跨帳戶或匿名存取。
SAI	S3租戶帳戶ID（貯體擁有者）	目標桶擁有者的租戶帳戶ID。用於識別跨帳戶或匿名存取。
SUSE	S3使用者URN（要求傳送者）	發出要求的使用者之租戶帳戶ID和使用者名稱。使用者可以是本機使用者或LDAP使用者。例如： `urn:sgws:identity::03393893651506583485:root` 匿名要求為空白。

程式碼	欄位	說明
時間	時間	申請的總處理時間（以微秒為單位）。
TLIP	信任的負載平衡器IP位址	如果要求是由信任的第7層負載平衡器路由、則為負載平衡器的IP位址。
UUID	通用唯一識別碼	物件在StorageGRID 整個系統內的識別碼。
VSID	版本ID	更新中繼資料之物件的特定版本ID。對非版本化貯體中的貯體和物件的作業不包括此欄位。

StorageGRID 中物件存放區驗證失敗的 **SVRF** 稽核訊息

每當內容區塊未通過驗證程序時、就會發出此訊息。每次從磁碟讀取或寫入複寫的物件資料時、都會執行數項驗證和完整性檢查、以確保傳送給要求使用者的資料與原先擷取到系統的資料相同。如果其中任何一項檢查失敗、系統會自動隔離毀損的複寫物件資料、以防止再次擷取。

程式碼	欄位	說明
CBID	內容區塊識別碼	驗證失敗之內容區塊的唯一識別碼。
RSRLT	結果代碼	驗證失敗類型： CRCF：循環備援檢查（crc）失敗。 HMAC：雜湊型訊息驗證碼（HMAC）檢查失敗。 EHSH：非預期的加密內容雜湊。 PHSH：非預期的原始內容雜湊。 SEQC：磁碟上的資料順序不正確。 PERR：磁碟檔案結構無效。 DERR：磁碟錯誤。 FNAM：錯誤的檔案名稱。

應密切監控此訊息。內容驗證失敗可能表示即將發生的硬體故障。

若要判斷觸發訊息的操作、請參閱「IDID（模組ID）」欄位的值。例如、SVFY值表示該訊息是由Storage Verifier模組產生、也就是背景驗證和儲存、表示該訊息是由內容擷取所觸發。

StorageGRID 中未知物件存放區內容的 **SVRU** 稽核訊息

LDR服務的儲存元件會持續掃描物件存放區中複寫物件資料的所有複本。當物件存放區偵測到複寫物件資料的未知或非預期複本、並將其移至隔離目錄時、就會發出此訊息。

程式碼	欄位	說明
FPTH	檔案路徑	非預期物件複本的檔案路徑。
RSRLT	結果	此欄位的值為「無」。RSRLT為必填訊息欄位、但與此訊息無關。使用「無」而非「UCS」、因此不會篩選此訊息。

應密切監控 SVRU ：物件存放區驗證未知稽核訊息。這表示在物件存放區中偵測到非預期的物件資料複本。應立即調查這種情況、以判斷這些複本的建立方式、因為這可能表示即將發生硬體故障。

StorageGRID 中正常節點停止的 **SYSD** 稽核訊息

正常停止服務時、會產生此訊息、表示已要求關機。通常只有在後續重新啟動之後才會傳送此訊息、因為稽核訊息佇列不會在關機之前清除。如果服務尚未重新啟動、請尋找在關機順序開頭傳送的SYST訊息。

程式碼	欄位	說明
RSRLT	乾淨關機	關機性質： SUCS：系統正常關機。

此訊息並不表示主機伺服器是否正在停止、僅表示報告服務。SYSD 的 RSLT 無法指示「不正常」關機、因為訊息只會由「乾淨」關機所產生。

StorageGRID 中節點停止的 **SYST** 稽核訊息

當服務正常停止時，會產生此訊息以表示已要求關閉服務，且該服務已啟動其關閉序列。SYST 可用於在服務重新啟動之前確定是否已要求關閉服務（與通常在服務重新啟動後發送的 SYSD 不同）。

程式碼	欄位	說明
RSRLT	乾淨關機	關機性質： SUCS：系統正常關機。

此訊息並不表示主機伺服器是否正在停止、僅表示報告服務。SYST 訊息的 RSLT 代碼無法表示「不正常」關機、因為訊息只會由「乾淨」關機所產生。

重新啟動服務時、會產生此訊息、指出先前的關機是否乾淨（命令）或不正常（非預期）。

程式碼	欄位	說明
RSRLT	乾淨關機	關機性質： SUCS：系統完全關機。 DSDN：系統並未完全關機。 VRGN：系統在伺服器安裝（或重新安裝）後第一次啟動。

此訊息並不表示主機伺服器是否已啟動、僅表示報告服務。此訊息可用於：

- 偵測稽核追蹤中的不連續性。
- 判斷服務是否在運作期間故障（StorageGRID 因為整個過程中、由於系統分散的特性可能會遮罩這些故障）。伺服器管理員會自動重新啟動失敗的服務。

擴充StorageGRID系統的容量或功能

了解如何擴充您的StorageGRID系統

了解如何擴充StorageGRID系統，以在不中斷運作的情況下增加容量或功能。您可以為現有儲存節點新增儲存卷，為現有網站新增新的網格節點，或新增網站。

在擴展網格節點之前，您必須確認沒有處於活動狀態的資料修復作業。如果任何修復失敗，則必須重新啟動它們並讓它們完成，然後再執行退役或擴充功能。請參閱"檢查資料修復工作" 。

StorageGRID 擴充功能可讓您新增：

- 儲存磁碟區至儲存節點
- 將新的網格節點移至現有站台
- 全新網站

您執行擴充的原因、決定您必須新增的每種類型新節點數量、以及這些新節點的位置。例如、如果您要執行擴充以增加儲存容量、新增中繼資料容量、或新增備援或新功能、則會有不同的節點需求。

請依照所執行擴充類型的步驟進行：

新增網格節點

1. 請依照的步驟"將網格節點新增至現有站台"進行。
2. "更新子網路"。
3. 部署網格節點：
   - "應用裝置"
   - "VMware"
   - "Linux"

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱"NetApp互通性對照表工具IMT （不含）"。

1. "執行擴充"。
2. "設定擴充系統"。

新增儲存磁碟區

請依照的步驟"將儲存磁碟區新增至儲存節點"進行。

新增網站

1. 請依照的步驟"新增站台"進行。
2. "更新子網路"。
3. 部署網格節點：
   - "應用裝置"
   - "VMware"
   - "Linux"

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱"NetApp互通性對照表工具IMT （不含）"。

1. "執行擴充"。
2. "設定擴充系統"。

擴張計劃

StorageGRID中複製資料的擴展規劃

如果您部署的資訊生命週期管理（ILM）原則包含建立物件複本的規則、您必須考量要新增多少儲存設備、以及新增儲存磁碟區或儲存節點的位置。

如需新增其他儲存設備的相關指引、請檢查建立複寫複本的ILM規則。如果ILM規則建立兩個以上的物件複本、請規劃在物件複本所在的每個位置新增儲存設備。簡單來說、如果您有兩個站台的網格和 ILM 規則、在每個站台建立一個物件複本、則您必須"新增儲存設備"前往每個站台、以增加網格的整體物件容量。如需物件複寫的相

關資訊，請參閱"什麼是複寫"。

基於效能考量、您應該嘗試在不同站台之間維持儲存容量和運算能力的平衡。因此、在此範例中、您應該將相同數量的儲存節點新增至每個站台、或是在每個站台新增額外的儲存磁碟區。

如果您有更複雜的ILM原則、其中包含根據儲存區名稱等準則將物件放置在不同位置的規則、或是隨著時間變更物件位置的規則、則您對擴充所需儲存區的分析將會類似、但會更為複雜。

記錄整體儲存容量的使用速度、有助於瞭解擴充所需的儲存容量、以及何時需要額外的儲存空間。您可以使用 Grid Manager 來"監控及記錄儲存容量"。

在規劃擴充時間時，請記住考慮採購和安裝額外儲存可能需要多長時間。為了簡化擴充規劃，當現有儲存節點達到 70% 容量時，請考慮新增儲存節點。

StorageGRID中糾刪碼（EC）資料的擴充規劃

如果您的ILM原則包含製作銷毀編碼複本的規則、您必須規劃新增儲存設備的位置、以及新增儲存設備的時間。您新增的儲存容量和新增的時間、可能會影響網格的可用儲存容量。

規劃儲存擴充的第一步是檢查ILM原則中建立銷毀編碼物件的規則。由於此功能可為每個銷毀編碼物件建立_k+m_片段、並將每個片段儲存在不同的儲存節點上、因此您必須確保擴充後至少有_k+m_儲存節點空間可容納新的銷毀編碼資料。StorageGRID如果銷毀編碼設定檔提供站台遺失保護、您必須將儲存設備新增至每個站台。如需銷毀編碼設定檔的相關資訊、請參閱"什麼是銷毀編碼方案"。

您需要新增的節點數量也取決於執行擴充時現有節點的完整程度。

新增銷毀編碼物件儲存容量的一般建議

如果您想要避免詳細計算、當現有儲存節點的容量達到70%時、您可以在每個站台新增兩個儲存節點。

這項一般建議針對單一站台網格和磁碟區編碼提供站台遺失保護的網格、提供廣泛的銷毀編碼方案合理的結果。

要更好地瞭解導致此建議的因素或爲您的站點制定更精確的計劃，請參閱"重新平衡銷毀編碼資料的考量事項"。如需針對您的情況最佳化的自訂建議、請聯絡您的 NetApp 專業服務顧問。

了解StorageGRID中擴充後的 EC 重新平衡

如果您正在執行擴充以新增儲存節點、並使用 ILM 規則來清除程式碼資料、則如果您無法新增足夠的儲存節點來執行銷毀編碼（ EC ）重新平衡程序、以供您使用的銷毀編碼配置使用。

檢閱這些考量之後、請執行擴充、然後前往"新增儲存節點後、重新平衡以銷毀編碼的資料"執行程序。

什麼是EC重新平衡？

EC重新平衡StorageGRID 是擴充儲存節點之後可能需要的一個過程。此程序會以命令列指令碼形式從主要管理節點執行。當您執行 EC 重新平衡程序時、 StorageGRID 會在站台的現有儲存節點和新新增的儲存節點之間重新分配銷毀編碼片段。

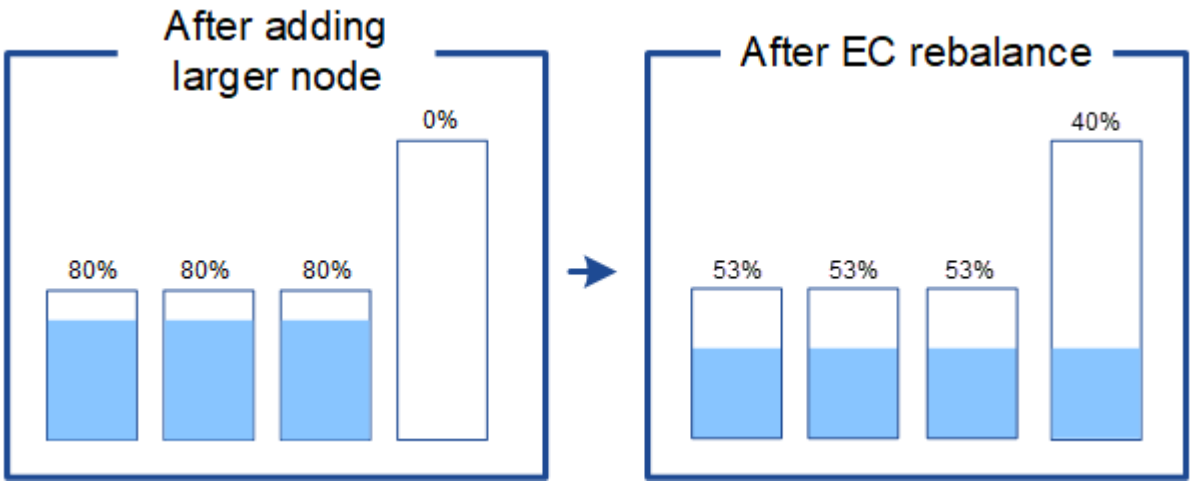
EC重新平衡程序：

- 僅移動以銷毀編碼的物件資料。它不會移動複寫的物件資料。
- 在站台內重新分配資料。它不會在站台之間移動資料。
- 在站台的所有儲存節點之間重新分配資料。它不會重新分配儲存磁碟區內的資料。
- 嘗試將資料位元組分配到每個節點，使每個節點擁有相同的可用空間。包含更多複寫資料的節點在重新平衡完成後可能儲存較少的銷除編碼資料。
- 在不考慮各節點相對容量的情況下，將可用空間平均分配到各個儲存節點。複寫資料也包含在計算中。
- 即使可用空間仍然分佈不均，如果無法再移動任何銷毀編碼資料，則視為重新平衡程序已完成。
- 不會將銷毀編碼資料分發到已使用率超過 80% 的 Storage Node 或僅中繼資料的 Storage Node。
- 執行 ILM 作業和 S3 用戶端作業時、可能會降低其效能？ #8212 ；需要額外資源來重新散佈銷毀編碼片段。

當EC重新平衡程序完成時：

- 銷毀編碼的資料將從可用空間較少的儲存節點移至可用空間較大的儲存節點。
- 銷毀編碼物件的資料保護將維持不變。
- 使用的（ % ）值可能因兩個原因而不同：
  - 複寫的物件複本將繼續佔用現有節點上的空間 #8212 ； EC 重新平衡程序不會移動複寫的資料。
  - 容量較大的節點可能比容量較小的節點相對較不滿，即使所有節點最終都會擁有大致相同數量的可用空間。

    例如，對於 2+1 糾刪碼方案，假設三個 200 TB 的節點都已使用 80%（每個節點 200 × 0.8 = 160 TB，整個站台共 480 TB）。如果新增一個 400 TB 的節點並執行重新平衡程序，所有舊節點現在將擁有大致相同數量的糾刪碼資料（106.66 TB，使用率 53%）。新節點將擁有（160 TB 的資料，使用率 40%）。在這種情況下，較大節點的已使用率（%）將低於較小節點的已使用率（%）。由於無法在不違反糾刪碼方案限制的情況下移動更多糾刪碼資料，因此重新平衡程序會在可用空間達到平衡之前完成。



何時重新平衡銷毀編碼資料

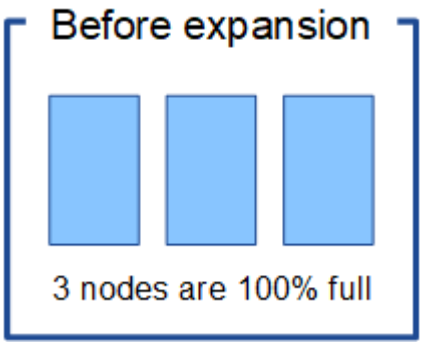
EC 重新平衡程序重新分配現有的擦除編碼數據，以確保節點不會變滿或保持滿狀態。該程序有助於確保 EC 編碼能夠在網站上繼續進行。

當網站上的資料分佈有令人擔憂的偏差且網站儲存大部分 EC 資料時（因為複製的資料無法透過重新平衡來移動

），請執行重新平衡程序。

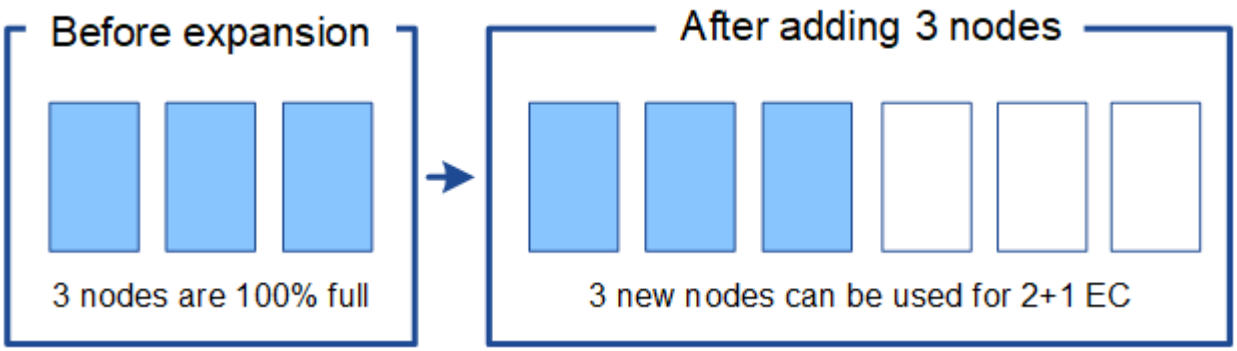
請考慮下列案例：

- 包含三個儲存節點的單一站台正在執行。StorageGRID
- ILM原則對所有大於1.0 MB的物件使用2+1銷毀編碼規則、而對較小的物件使用雙複製複寫規則。
- 所有儲存節點都已完全滿。在主要嚴重性層級觸發 * 物件儲存空間不足 * 警示。



如果新增足夠的節點，則無需重新平衡

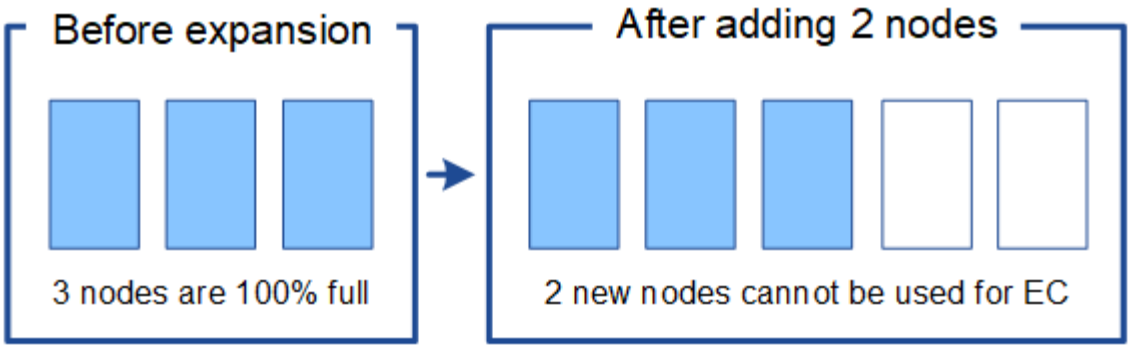
若要瞭解何時不需要 EC 重新平衡、請假設您新增了三個（或更多）新的儲存節點。在這種情況下、您不需要執行 EC 重新平衡。原始儲存節點將保持完整狀態、但新物件現在將使用三個新節點來進行 2+1 銷毀編碼和 #8212 ；兩個資料片段和一個同位元區隔片段都可以儲存在不同的節點上。



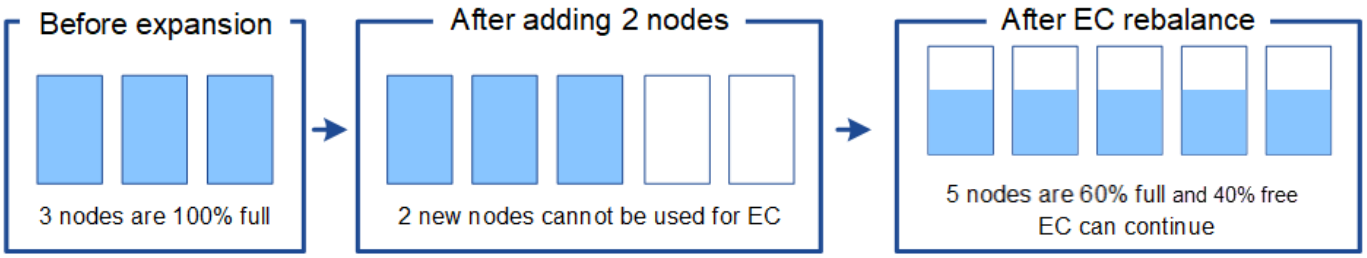
雖然您可以在此案例中執行 EC 重新平衡程序、但移動現有的銷毀編碼資料將會暫時降低網格的效能、這可能會影響用戶端作業。

如果您無法新增足夠的節點、則需要重新平衡

若要瞭解何時需要 EC 重新平衡、假設您只能新增兩個儲存節點、而不能新增三個。由於 2+1 配置需要至少三個儲存節點才能有可用空間、因此無法將空節點用於新的銷毀編碼資料。



要使用新的儲存節點，您應該執行 EC 重新平衡程序。執行此程序時，StorageGRID 會重新分配現有的糾刪碼資料和同位元檢查片段，使可用空間均勻分佈在站台上的所有儲存節點上。在本範例中，EC 重新平衡程序完成後，所有五個節點的已使用空間均為 60%，可用空間為 40%，物件可以繼續擷取至所有儲存節點上的 2+1 糾刪碼方案。



EC 重新平衡的建議

如果下列陳述中的所有陳述均正確、則 NetApp 需要 EC 重新平衡：

- 您使用銷毀編碼來處理物件資料。
- 站台上的一個或多個儲存節點已觸發*低物件儲存*警示、表示節點已滿80%以上。
- 您無法新增足夠的新儲存節點以供使用的銷毀編碼配置使用。請參閱。 "新增銷毀編碼物件的儲存容量"
- 在執行 EC 重新平衡程序時、 S3 用戶端可以容忍較低的寫入和讀取作業效能。

如果您偏好將儲存節點填滿至類似層級、而 S3 用戶端可以在執行 EC 重新平衡程序時、容忍其寫入和讀取作業的效能降低、則可以選擇性地執行 EC 重新平衡程序。

EC重新平衡程序如何與其他維護工作互動

您無法在執行 EC 重新平衡程序的同時執行某些維護程序。

程序	在**EC**重新平衡程序期間允許？
其他EC重新平衡程序	不可以 您一次只能執行一個EC重新平衡程序。

程序	在**EC**重新平衡程序期間允許？
取消委任程序 EC資料修復工作	不可以 • 在執行EC重新平衡程序時、您無法啟動取消委任程序或EC資料修復。 • 在執行儲存節點取消委任程序或EC資料修復時、您無法啟動EC重新平衡程序。
擴充程序	不可以 如果您需要在擴充中新增儲存節點、請在新增所有新節點之後執行 EC 重新平衡程序。
升級程序	不可以 如果您需要升級 StorageGRID 軟體、請在執行 EC 重新平衡程序之前或之後執行升級程序。您可以視需要終止EC重新平衡程序、以執行軟體升級。
應用裝置節點複製程序	不可以 如果您需要複製應用裝置儲存節點、請在新增節點之後執行 EC 重新平衡程序。
修復程序	是的。 您可以在StorageGRID 執行EC重新平衡程序時套用更新程式。
其他維護程序	不可以 在執行其他維護程序之前、您必須先終止EC重新平衡程序。

EC重新平衡程序如何與**ILM**互動

當EC重新平衡程序正在執行時、請避免變更ILM、以免變更現有銷毀編碼物件的位置。例如、請勿開始使用具有不同銷毀編碼設定檔的 ILM 規則。如果您需要進行此類 ILM 變更、您應該終止 EC 重新平衡程序。

擴充指南

StorageGRID中新增物件容量的指南

您可以StorageGRID 將儲存磁碟區新增至現有的儲存節點、或新增儲存節點至現有站台、以擴充您的物件儲存容量。您必須以符合資訊生命週期管理（ILM）原則要求的方式新增儲存容量。

新增儲存磁碟區的準則

在將儲存磁碟區新增至現有儲存節點之前、請先檢閱下列準則與限制：

- 您必須檢查目前的 ILM 規則、以決定在何處及何時"新增儲存磁碟區"增加或"銷毀編碼物件"的可用儲存空間"複寫物件"。
- 您無法透過新增儲存磁碟區來增加系統的中繼資料容量、因為物件中繼資料只會儲存在磁碟區 0 上。
- 每個軟體型儲存節點最多可支援48個儲存磁碟區。如果您需要新增容量、則必須新增儲存節點。
- 您可以在每個 SG6060 應用裝置上新增一或兩個擴充架。每個擴充機櫃都會新增 16 個儲存磁碟區。安裝兩個擴充機櫃後、 SG6060 可支援總共 48 個儲存磁碟區。
- 您可以在每個 SG6160 應用裝置上新增一或兩個擴充架。每個擴充機櫃都會新增 60 個儲存磁碟區。安裝兩個擴充機櫃後、 SG6160 可支援總共 180 個儲存磁碟區。
- 您無法將儲存磁碟區新增至任何其他儲存設備。
- 您無法增加現有儲存磁碟區的大小。
- 您無法在執行系統升級、恢復作業或其他擴充時、將儲存磁碟區新增至儲存節點。

決定新增儲存磁碟區並決定必須擴充哪些儲存節點以符合ILM原則之後、請依照您的儲存節點類型指示操作：

- 若要在 SG6060 儲存設備中新增一或兩個擴充櫃、請前往 "將擴充機櫃新增至部署的 SG6060"。
- 若要在 SG6160 儲存設備中新增一或兩個擴充櫃、請前往 "將擴充機櫃新增至部署的 SG6160"
- 對於軟體型節點、請遵循的指示"將儲存磁碟區新增至儲存節點"。

新增儲存節點的準則

在將儲存節點新增至現有站台之前、請先檢閱下列準則與限制：

- 您必須檢查目前的 ILM 規則、以決定在何處及何時新增儲存節點"銷毀編碼物件"、以增加或的可用儲存空間"複寫物件"。
- 在單一擴充程序中、不應新增超過10個儲存節點。
- 您可以在單一擴充程序中將儲存節點新增至多個站台。
- 您可以在單一擴充程序中新增儲存節點和其他類型的節點。
- 在開始擴充程序之前、您必須先確認在還原過程中執行的所有資料修復作業均已完成。請參閱。 "檢查資料修復工作"
- 如果您需要在執行擴充之前或之後移除儲存節點、則不應在單一取消配置節點程序中取消委任超過10個儲存節點。
- 增加足夠的儲存節點以維持底層儲存 I/O 效能。寫入操作將根據可用儲存容量在儲存節點之間分配。如果擴充的儲存節點具有更多可用儲存容量，則這些節點將接收更多的寫入。特別是，當現有的儲存節點幾乎已滿時，新的寫入將僅依賴擴充的儲存節點。讀取和刪除操作將根據您的特定工作負載來處理。

儲存節點上的**ADC**服務準則

設定擴充時、您必須選擇是否要在每個新的儲存節點上加入管理網域控制器（ADC）服務。ADC服務會追蹤網格服務的位置和可用度。

- 您可以"將 ADC 服務從一個儲存節點移至同一站點上的另一個儲存節點" 。

- StorageGRID 系統需要"ADC服務的仲裁數"在每個站台和任何時間都能使用。
- 每個站台至少必須有三個儲存節點包含ADC服務。
- 不建議將ADC服務新增至每個儲存節點。包含太多的ADC服務可能會因為節點之間的通訊量增加而導致速度變慢。
- 單一網格在使用ADC服務時、不得有超過48個儲存節點。這相當於16個站台、每個站台有三項ADC服務。
- 一般來說，當您為新節點選擇*ADC 服務*設定時，您應該選擇*自動*。僅當新節點將取代包含 ADC 服務的另一個儲存節點時才選擇*是*。由於如果剩餘的 ADC 服務太少，您就無法停用儲存節點，因此選擇「是」可確保在刪除舊服務之前有新的 ADC 服務可用。

StorageGRID元資料容量新增指南

為了確保物件中繼資料有足夠的可用空間、您可能需要執行擴充程序、以便在每個站台新增儲存節點。

此功能可在每個儲存節點的Volume 0上保留物件中繼資料的空間。StorageGRID每個站台都會維護三份所有物件中繼資料複本、並平均分散到所有儲存節點。

您可以使用Grid Manager來監控儲存節點的中繼資料容量、並預估中繼資料容量的使用速度。此外、當使用的中繼資料空間達到特定臨界值時、會針對儲存節點觸發*低中繼資料儲存*警示。

請注意、網格的物件中繼資料容量可能會比物件儲存容量消耗得更快、視您使用網格的方式而定。例如、如果您通常會擷取大量的小型物件、或是將大量的使用者中繼資料或標記新增至物件、則可能需要新增儲存節點、以增加中繼資料容量、即使物件儲存容量仍足夠。

如需詳細資訊、請參閱下列內容：

- "管理物件中繼資料儲存"
- "監控每個儲存節點的物件中繼資料容量"

增加中繼資料容量的準則

在新增儲存節點以增加中繼資料容量之前、請先檢閱下列準則與限制：

- 假設有足夠的物件儲存容量可用、則有更多空間可用於物件中繼資料、會增加StorageGRID 可儲存在您的物件系統中的物件數量。
- 您可以在每個站台新增一或多個儲存節點、以增加網格的中繼資料容量。
- 保留給定儲存節點上物件中繼資料的實際空間取決於中繼資料保留空間儲存選項（全系統設定）、分配給節點的RAM容量、以及節點Volume 0的大小。
- 您無法透過將儲存磁碟區新增至現有的儲存節點來增加中繼資料容量、因為中繼資料只會儲存在磁碟區 0 上。
- 您無法透過新增網站來增加中繼資料容量。
- 在每個站台保留三份所有物件中繼資料複本。StorageGRID因此、系統的中繼資料容量受限於最小站台的中繼資料容量。
- 新增中繼資料容量時、您應該將相同數量的儲存節點新增至每個站台。

純中繼資料儲存節點有特定的硬體需求：

- 使用 StorageGRID 應用裝置時，只能在具有十二個 1.9 TB 或十二個 3.8 TB 磁碟機的 SGF6112 應用裝置上設定純中繼資料節點。
- 使用軟體型節點時，純中繼資料節點資源必須符合現有的儲存節點資源。例如：
  - 如果現有的 StorageGRID 站台使用 SG6000 或 SG6100 應用裝置，則僅限軟體型中繼資料節點必須符合下列最低需求：
    - 128 GB RAM
    - 8 核心 CPU
    - 8 TB SSD 或與 Cassandra 資料庫相同的儲存設備（ rangedb/0 ）
  - 如果現有的StorageGRID站點使用具有 24 GB RAM、8 核心 CPU 和 3 TB 或 4TB 元資料儲存的虛擬儲存節點，則基於軟體的僅元資料節點應使用類似的資源（24 GB RAM、8 核心 CPU 和 4TB 元資料儲存（rangedb/0））。
- 新增 StorageGRID 站台時，新站台的中繼資料總容量至少應與現有的 StorageGRID 站台和新站台資源相符，且應與現有 StorageGRID 站台的儲存節點相符。

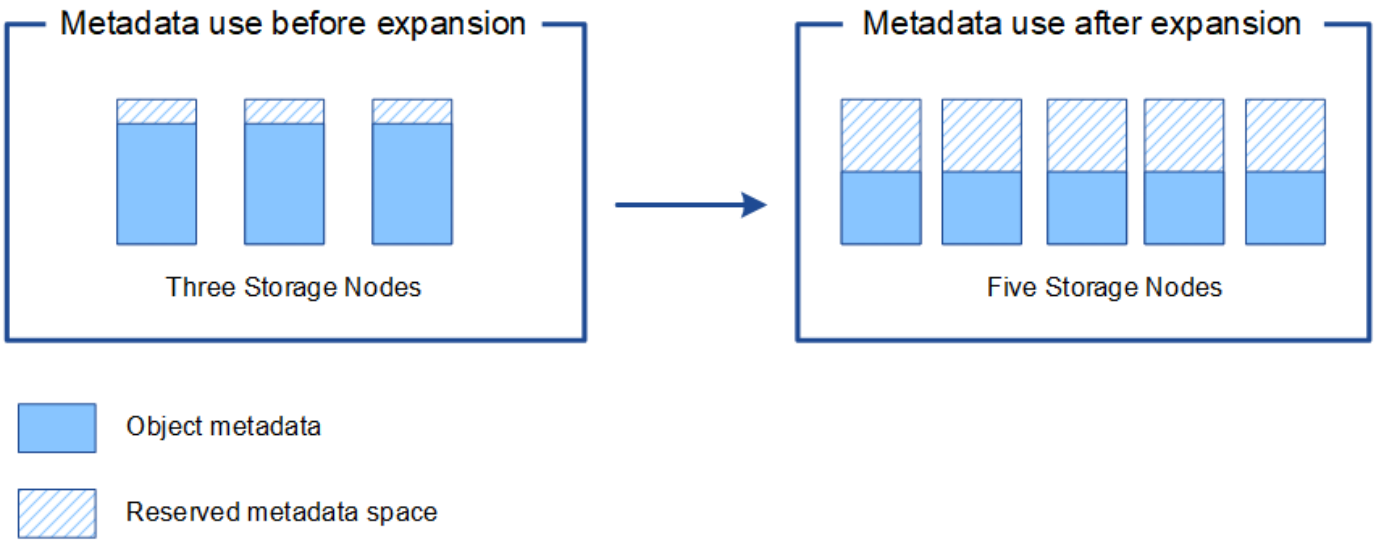
請參閱"中繼資料保留空間的說明"。

新增儲存節點時、中繼資料的重新分配方式

在擴充中新增儲存節點時StorageGRID 、功能區會將現有的物件中繼資料重新分配至每個站台的新節點、以增加網格的整體中繼資料容量。不需要使用者採取任何行動。

下圖顯示StorageGRID 當您在擴充中新增儲存節點時、功能區的功能如何重新發佈物件中繼資料。圖左方表示三個儲存節點的Volume 0（磁碟區0）、然後再進行擴充。中繼資料佔用每個節點可用中繼資料空間的相對較大部分、而且已觸發*低中繼資料儲存*警示。

右圖顯示在站台新增兩個儲存節點之後、如何重新分配現有的中繼資料。每個節點上的中繼資料量已減少、*低中繼資料儲存設備*警示不再觸發、而且中繼資料可用空間也已增加。



StorageGRID中新增網格節點的指南

您可以StorageGRID 新增新的網格節點至現有站台、以新增備援功能或其他功能至該系統。

例如、您可以選擇新增要用於高可用度（ HA ）群組的閘道節點、或是在遠端站台新增管理節點、以允許使用本機節點進行監控。

您可以在單一擴充作業中、將下列一種或多種類型的節點新增至一或多個現有站台：

- 非主要管理節點
- 儲存節點
- 閘道節點

準備新增網格節點時、請注意下列限制：

- 主管理節點會在初始安裝期間部署。您無法在擴充期間新增主要管理節點。
- 您可以在相同的擴充中新增儲存節點和其他類型的節點。
- 新增儲存節點時、您必須仔細規劃新節點的數量和位置。請參閱。 "新增物件容量的準則"
- 如果防火牆控制頁面上不受信任的用戶端網路標籤上的 設定新節點預設值 選項為 不受信任，則使用用戶端網路連線至擴充節點的用戶端應用程式必須使用負載平衡器端點連接埠進行連線（設定 > 安全 > 防火牆控制）。請參閱說明"變更新節點的安全性設定"以及"設定負載平衡器端點"。

StorageGRID新增網站的指南

您可以新增一個網站來擴充StorageGRID 您的功能。

新增站台的準則

在新增站台之前、請先檢閱下列需求與限制：

- 每個擴充作業只能新增一個站台。
- 您無法將網格節點新增至現有站台、做為相同擴充的一部分。
- 所有站台必須至少包含三個儲存節點。這些節點可以是組合式儲存節點和僅中繼資料儲存節點的任意組合。如果儲存節點超過三個，則可以是組合式儲存節點、僅中繼資料儲存節點和僅資料儲存節點的任意組合，前提是必須有三個 ADC 服務可用。如需更多資訊，請參閱 "每個網格和每個站點所需的儲存節點"。
- 新增網站時，可儲存的物件數量不會自動增加。網格的總物件容量取決於可用儲存設備空間、ILM 原則以及每個站點的中繼資料容量。
- 調整新網站規模時、您必須確保其中包含足夠的中繼資料容量。

  StorageGRID 會在每個站台保留所有物件中繼資料的複本。新增站台時，請確保其包含足夠的中繼資料容量，以因應現有物件中繼資料的需求，以及未來成長所需的容量。

  如需更多資訊，請參閱下列內容：

  - "管理物件中繼資料儲存"
  - "監控每個儲存節點的物件中繼資料容量"
- 您必須考量站台之間的可用網路頻寬、以及網路延遲的層級。即使所有物件只儲存在擷取的站台、也會在站台之間持續複寫中繼資料更新。

  為了避免因延遲而導致的效能下降：

- 對於延遲大於 100 毫秒的站台之間，不建議使用銷除編碼。
- StorageGRID 系統中的站點不應跨越過大的地理距離，例如跨越多個大洲。

- 由於StorageGRID 您的非功能性系統在擴充期間仍可運作、因此您必須先檢閱ILM規則、再開始擴充程序。在擴充程序完成之前、您必須確保物件複本不會儲存至新站台。

  例如，在開始擴充之前，請檢查是否有任何規則使用了預設儲存資源池（所有儲存節點）。如果有，請使用現有儲存節點建立一個新的儲存資源池，並更新您的 ILM 規則以使用新的儲存資源池。否則，一旦該站台的第一個節點啟動，物件就會立即複製到新站台。

  有關在新增網站時變更 ILM 原則的詳細資訊，請參閱"變更 ILM 原則的範例"。

準備擴展您的StorageGRID系統

在執行擴充作業之前、請先收集相關資料、然後安裝及設定任何新的硬體和網路。

項目	附註
安裝歸檔StorageGRID	如果您要新增網格節點或新網站、則必須下載StorageGRID 並擷取此安裝檔案。您必須使用目前在網格上執行的相同版本。 如需詳細資訊，請參閱的說明下載及解壓縮StorageGRID 安裝文件。 • 注意： * 如果您要將新的儲存磁碟區新增至現有的儲存節點或安裝新的 StorageGRID 應用裝置、則不需要下載檔案。
服務筆記型電腦	服務型筆記型電腦具備下列功能： • 網路連接埠 • SSH用戶端（例如Putty） • "支援的網頁瀏覽器"
`Passwords.txt`檔案	包含在命令列上存取網格節點所需的密碼。包含在恢復包中。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼不在 `Passwords.txt`檔案中。
本文檔StorageGRID	• "管理StorageGRID" • "版本資訊"。您必須登入現有 NetApp 帳戶或建立帳戶才能存取發行說明。 • "適用於您平台的安裝說明"
您平台的最新文件	如需支援的版本、請參閱 "互通性對照表工具IMT （不含）"。

下載並解壓縮StorageGRID 安裝檔案

[[download-and -extract -install-files]]

在新增網格節點或新網站之前、您必須先下載適當StorageGRID 的安裝檔案、然後擷取檔案。

關於這項工作

您必須使用StorageGRID 目前在網格上執行的版本的功能表來執行擴充作業。

步驟

1. 前往 "NetApp下載StorageGRID"。
2. 選取StorageGRID 目前在網格上執行的版本的功能。
3. 以您NetApp帳戶的使用者名稱和密碼登入。
4. 閱讀終端使用者授權合約、選取核取方塊、然後選取 * 接受並繼續 * 。
5. 在下載頁面的 * 安裝 StorageGRID * 欄中、選取 `.tgz`適用於您平台的或 `.zip`檔案。

   安裝歸檔檔檔案中顯示的版本必須符合目前安裝的軟體版本。

   如果您在服務筆記型電腦上執行 Windows 、請使用 `.zip`此檔案。

平台	安裝歸檔
紅帽企業版	`StorageGRID-Webscale-version-RPM-uniqueID.zip` `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
Ubuntu或DEBIANOR應用裝置	`StorageGRID-Webscale-version-DEB-uniqueID.zip` `StorageGRID-Webscale-version-DEB-uniqueID.tgz`
VMware	`StorageGRID-Webscale-version-VMware-uniqueID.zip` `StorageGRID-Webscale-version-VMware-uniqueID.tgz`
OpenStack /其他Hypervisor	若要在OpenStack上擴充現有部署、您必須部署執行上述其中一種支援Linux套裝作業系統的虛擬機器、並遵循適用於Linux的適當指示。

6. 下載並解壓縮歸檔檔案。
7. 請根據您的平台、規劃的網格拓撲、以及您將如何擴充StorageGRID 自己的系統、依照您平台的適當步驟來選擇所需的檔案。

   每個平台步驟中所列的路徑、都是相對於歸檔檔案所安裝的頂層目錄。

8. 如果您正在擴展 RHEL 系統，請選擇適當的檔案。

路徑和檔案名稱	說明
	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。

路徑和檔案名稱	說明
	不提供產品任何支援權利的免費授權。
	用於在 RHEL 主機上安裝 StorageGRID 節點映像的 RPM 套件。
	用於在 RHEL 主機上安裝 StorageGRID 主機服務的 RPM 套件。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行Ping 聯合整合。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	範例 Ansible 角色和教戰手冊、用於設定 StorageGRID 容器部署的 RHEL 主機。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

1. 如果您要擴充Ubuntu或Debian系統、請選取適當的檔案。

路徑和檔案名稱	說明
每個問題/讀我檔案	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	非正式作業的NetApp授權檔案、可用於測試及概念驗證部署。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝不含節點的映像。
	檔案的 MD5 Checksum `/debs/storagegrid-webscale-images-version-SHA.deb` 。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝支援功能主機服務。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行Ping 聯合整合。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。
/扣款/額外費用/可選	範例Ansible角色與方針、可用來設定Ubuntu或Debian主機以StorageGRID 進行列舉容器部署。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。

路徑和檔案名稱	說明
/debs/storagegRID -soaut-azure.js	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

1. 如果您要擴充VMware系統、請選取適當的檔案。

路徑和檔案名稱	說明
/vSphere/README	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	不提供產品任何支援權利的免費授權。
/vSphere/NetApp-SG-version -SHA-vmdk	用來做為建立網格節點虛擬機器範本的虛擬機器磁碟檔案。
/vSphere/vSphere-primer-admin.OVF ./vSphere/vSphere-prime-admin.mf	開放式虛擬化格式模板文件(`.mf`）(`.ovf`和清單文件），用於部署主管理節點。
/vSphere/vSphere-non-prime-admin.OVF ./vSphere/vSphere-non-prime-admin.mf	模板文件(`.mf`）(`.ovf`和清單文件），用於部署非主管理員節點。
/vSphere/vSphere-gateway.OVF ./vSphere/vSphere-gateway.mf	模板文件(`.mf`）(`.ovf`和清單文件），用於部署網關節點。
/vSphere/vSphere-storage。OVF ./vSphere/vSphere-storage	模板文件(`.mf`）(`.ovf`和清單文件），用於部署基於虛擬機的存儲節點。
部署指令碼工具	說明
	Bash Shell指令碼、用於自動化虛擬網格節點的部署。
	用於指令碼的範例組態檔 `deploy-vsphere-ovftool.sh`。
	Python指令碼、用於自動化StorageGRID 組態的功能。

路徑和檔案名稱	說明
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入（ SSO ）時、您可以使用 Python 指令碼範例登入 Grid Management API 。您也可以使用此指令碼來進行 Ping 聯合整合。
/vSphere/configure-storagegrid、same.json	用於指令碼的範例組態檔 `configure-storagegrid.py`。
/vSphere/configure-storagegrid、blank.json	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
/vSphere/Extras / API架構	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

1. 如果您要擴充StorageGRID 以應用程式為基礎的系統、請選取適當的檔案。

對於設備安裝，僅當您需要避免網路流量時才需要這些檔案。設備可以從您執行復原過程的管理節點下載所需的檔案。

路徑和檔案名稱	說明
	DEB套件可在StorageGRID 您的應用裝置上安裝不含節點的影像。
	檔案的 MD5 Checksum `/debs/storagegridwebscale-images-version-SHA.deb` 。

驗證硬體與網路

在開始擴充StorageGRID 您的作業系統之前、請先確認下列事項：

- 已安裝並設定支援新網格節點或新站台所需的硬體。
- 所有新節點都有通往所有現有節點和新節點的雙向通訊路徑（Grid Network的需求）。請特別確認您要新增至擴充節點和主要管理節點之間的下列 TCP 連接埠已開啟：
  - 1055
  - 7443
  - 8011
  - 10342

  請參閱。 "內部網格節點通訊"
- 主管理節點可與所有用於裝載StorageGRID 該系統的擴充伺服器進行通訊。
- 如果任何新節點在先前未使用的子網路上有 Grid Network IP 位址、您就已經"已新增子網路"進入 Grid Network 子網路清單。否則、您必須取消擴充、新增子網路、然後重新開始程序。
- 您並未在網格網路上的網格節點之間或 StorageGRID 站台之間使用網路位址轉譯（ NAT ）。當您將私有的IPv4位址用於Grid Network時、這些位址必須從每個站台的每個網格節點直接路由傳送。只有在使用對網格中所有節點透明的通道應用程式時、才支援使用NAT跨公共網路區段橋接網格網路、亦即網格節點不需要知道公有IP位址。

  此NAT限制僅適用於網格節點和網格網路。視需要、您可以在外部用戶端和網格節點之間使用NAT、例如為閘道節點提供公有IP位址。

新增網格節點或站台

在StorageGRID中新增網格節點或新站點的工作流程概述

請遵循此程序、將網格節點新增至現有站台或新增站台。一次只能執行一種擴充類型。

開始之前

- 您有"root 存取權或維護權限"。
- 網格中的所有現有節點都會在所有站台上啟動並執行。
- 任何先前的擴充、升級、汰換或還原程序均已完成。

> 當另一個擴充、升級、還原或作用中取消委任程序正在進行時、您將無法啟動擴充。不過、如有必要、您可以暫停取消委任程序以開始擴充。

步驟

1. "更新網格網路的子網"。
2. "部署新的網格節點"。
3. "執行擴充"。

在StorageGRID中新增或更新網格網路子網路以進行擴展

當您在擴充中新增網格節點或新站台時、可能需要更新或新增子網路至網格網路。

此技術可維護網格網路（eth0）上用於在網格節點之間進行通訊的網路子網路清單。StorageGRID這些項目包括StorageGRID 您的系統所在站台用於Grid Network的子網路、以及透過Grid Network閘道存取的NTP、DNS、LDAP或其他外部伺服器所使用的任何子網路。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您可以使用CIDR表示法來設定要設定的子網路位址。

關於這項工作

如果任何新節點在先前未使用的子網路上有Grid Network IP位址、則在開始擴充之前、您必須先將新的子網路新增至Grid Network子網路清單。否則、您必須取消擴充、新增子網路、然後重新開始程序。

任何節點的網格網路、管理網路或用戶端網路都不要使用包含下列 IPv4 位址的子網路：

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

例如，任何節點的網格網路、管理網路或用戶端網路都不要使用下列子網路範圍：

- 192.168.130.0/24，因為此子網路範圍包含 IP 位址 192.168.130.101 和 192.168.130.102
- 192.168.131.0/24，因為此子網路範圍包含 IP 位址 192.168.131.101 和 192.168.131.102
- 198.51.100.0/24，因為此子網路範圍包含 IP 位址 198.51.100.2 和 198.51.100.4

步驟

1. 選擇*維護* > 網路 > 電網。
2. 選取 * 新增其他子網路 * 、以 CIDR 表示法新增子網路。

   例如，輸入 `10.96.104.0/22`。

3. 輸入資源配置通關密碼、然後選取*「Save*（儲存*）」。

4. 等待更改套用完畢，然後下載新的恢復包。
   a. 選擇*維護* > 系統 > 恢復包。
   b. 請輸入*佈建密碼*。

> 復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。它也用於恢復主管理節點。

您指定的子網路會自動設定為StorageGRID 適用於您的整個系統。

在StorageGRID中部署新的網格節點

在擴充中部署新網格節點的步驟、與第一次安裝網格時所用的步驟相同。您必須先部署所有新的網格節點、才能執行擴充。

展開網格時、您新增的節點不必符合現有的節點類型。您可以新增VMware節點、Linux Container型節點或應用裝置節點。

VMware：部署網格節點

您必須在VMware vSphere中為要新增至擴充的每個VMware節點部署虛擬機器。

步驟

1. "將新節點部署為虛擬機器"並將其連接到一個或多個StorageGRID網路。

   部署節點時、您可以選擇重新對應節點連接埠、或增加CPU或記憶體設定。

2. 部署完所有新的 VMware 節點之後"執行擴充程序"，。

Linux：部署網格節點

您可以在新的Linux主機或現有的Linux主機上部署網格節點。如果您需要額外的Linux主機來支援StorageGRID您要新增至網格之支撐節點的CPU、RAM和儲存需求、請依照您第一次安裝主機時的準備方式來準備這些主機。然後、您可以依照安裝期間部署網格節點的相同方式來部署擴充節點。

開始之前

- 您已獲得針對您的 Linux 版本安裝StorageGRID 的說明，並且您已查看"硬體和儲存需求"。
- 如果您打算在現有主機上部署新的網格節點、則表示您已確認現有主機具有足夠的CPU、RAM和儲存容量、可用於其他節點。
- 您有計畫將故障網域降至最低。例如、您不應該在單一實體主機上部署所有閘道節點。

> 在正式作業部署中、請勿在單一實體或虛擬主機上執行多個儲存節點。使用每個儲存節點的專屬主機、可提供隔離的故障網域。

- 如果 StorageGRID 節點使用從 NetApp ONTAP 系統指派的儲存設備、請確認該磁碟區未啟用 FabricPool 分層原則。停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

步驟

1. 如果您要新增主機、請參閱部署StorageGRID 節點的安裝說明。
2. 若要部署新主機、請依照主機準備指示進行。
3. 若要建立節點組態檔案並驗證StorageGRID 此功能的組態、請遵循部署網格節點的指示。
4. 如果您要將節點新增至新的Linux主機、請啟動StorageGRID 「支援服務」。
5. 如果您要將節點新增至現有的 Linux 主機、請使用 StorageGRID 主機服務 CLI 啟動新節點：`sudo storagegrid node start [<node name\>]`

完成後

部署所有新的網格節點之後"執行擴充"、您可以。

設備：部署儲存設備、閘道或非主要管理節點

若要在StorageGRID 應用裝置節點上安裝此功能、請使用StorageGRID 產品隨附的《應用程式安裝程式（介紹）：在擴充過程中、每個儲存設備都會以單一儲存節點的形式運作、而每個服務應用裝置則會以單一閘道節點或非主要管理節點的形式運作。任何應用裝置都可以連線至Grid Network、管理網路和用戶端網路。

開始之前

- 設備已安裝在機架或機櫃中、並已連接至您的網路、並已開啟電源。
- 您已完成這些 "設定硬體"步驟。

  設定應用裝置硬體包括設定 StorageGRID 連線（網路連結和 IP 位址）所需的步驟、以及啟用節點加密、變更 RAID 模式和重新對應網路連接埠的選用步驟。

- 列出在《IP組態》頁面StorageGRID 上的所有Grid Network子網路、均已在主要管理節點的Grid Network Subnet List（網格網路子網路清單）中定義。
- 替換應用裝置上的《解決方法安裝程式韌體與目前在網格上執行的《解決方法與應用程式的更新版本相容。StorageGRID StorageGRID如果版本不相容、您必須升級 StorageGRID 應用裝置安裝程式韌體。
- 您的服務型筆記型電腦配備"支援的網頁瀏覽器"。
- 您知道指派給應用裝置運算控制器的其中一個IP位址。您可以將IP位址用於任何附加StorageGRID 的靜態網路。

關於這項工作

在StorageGRID 應用裝置節點上安裝過程有下列階段：

- 您可以指定或確認主要管理節點的IP位址、以及應用裝置節點的名稱。
- 您可以開始安裝、並在磁碟區已設定且已安裝軟體時等待。

  在執行設備安裝工作時、安裝會暫停。若要繼續安裝、請登入Grid Manager、核准所有網格節點、並完成StorageGRID 安裝程序。

> 如果您需要一次部署多個應用裝置節點、可以使用 Appliance 安裝指令碼來自動化安裝程序 `configure-sga.py`。

步驟

1. 開啟瀏覽器、然後輸入應用裝置運算控制器的其中一個IP位址。

   `https://Controller_IP:8443`

   畫面會出現「the不再安裝StorageGRID 程式」首頁。

2. 在「*主要管理節點*連線」區段中、判斷您是否需要指定主要管理節點的IP位址。

   如果您先前已在此資料中心安裝其他節點、StorageGRID 則當主管理節點或至少有一個已設定ADD_IP的其他網格節點出現在同一個子網路上時、即可自動探索此IP位址。

3. 如果未顯示此IP位址、或您需要變更它、請指定位址：

選項	說明
手動輸入IP	a. 清除 * 啟用管理節點探索 * 核取方塊。 b. 手動輸入IP位址。 c. 選擇*保存*。 d. 等待連線狀態、讓新的IP位址準備就緒。
自動探索所有連線的主要管理節點	a. 選中 * 啓用管理節點發現 * 複選框。 b. 等待顯示已發現的IP位址清單。 c. 選取要部署此應用裝置儲存節點的網格主要管理節點。 d. 選擇*保存*。 e. 等待連線狀態、讓新的IP位址準備就緒。

4. 在*節點名稱*欄位中、輸入您要用於此應用裝置節點的名稱、然後選取*儲存*。

   節點名稱會指派給StorageGRID 此應用裝置節點的功能。它會顯示在Grid Manager的節點頁面（總覽索引標籤）上。如果需要、您可以在核准節點時變更名稱。

5. 在 * 安裝 * 區段中、確認目前狀態為「準備好開始將節點名稱 _ 安裝至具有主要管理節點 *admin_ip* 的網格」、且 * 開始安裝 * 按鈕已啟用。

   如果*開始安裝*按鈕未啟用、您可能需要變更網路組態或連接埠設定。如需相關指示、請參閱產品的維護指示。

6. 從「the Some Appliance Installer」首頁選取「開始安裝」StorageGRID 。

   目前狀態變更為「Installation is in progress」，並顯示監控安裝頁面。

7. 如果您的擴充包含多個應用裝置節點、請針對每個應用裝置重複上述步驟。

   如果您需要一次部署多個應用裝置儲存節點、可以使用configure-sga.py應用裝置安裝指令碼來自動化安裝程序。

8. 如果需要手動存取監視器安裝頁面，請從功能表列中選擇「監視器安裝」。

Monitor 安裝頁面會顯示安裝進度。

藍色狀態列會指出目前正在進行的工作。綠色狀態列表示已成功完成的工作。

> 安裝程式可確保先前安裝中完成的工作不會重新執行。如果您正在重新執行安裝、任何不需要重新執行的工作都會顯示綠色狀態列和「略過」狀態。

9. 檢閱前兩個安裝階段的進度。

   1.設定應用裝置

   在此階段中、會發生下列其中一個程序：

   - 對於儲存設備、安裝程式會連線至儲存控制器、清除任何現有的組態、與 SANtricity OS 通訊以設定磁碟區、以及設定主機設定。
   - 對於服務應用裝置、安裝程式會從運算控制器中的磁碟機清除任何現有的組態、並設定主機設定。

   2.安裝作業系統

   在此階段、安裝程式會將基礎作業系統映像複製到StorageGRID 應用裝置中以供使用。

10. 繼續監控安裝進度、直到主控台視窗出現訊息、提示您使用Grid Manager核准節點。

> 請等到您在此擴充中新增的所有節點都已準備好核准、再前往Grid Manager核准節點。

執行StorageGRID擴展

當您執行擴充時、新的網格節點會新增至您現有StorageGRID 的功能介紹部署。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有資源配置通關密碼。
- 您已部署此擴充中要新增的所有網格節點。
- 您有"維護或根存取權限"。
- 如果您要新增儲存節點、表示您已確認在還原過程中執行的所有資料修復作業均已完成。請參閱。 "檢查資料修復工作"
- 如果您要新增儲存節點、而且想要將自訂儲存等級指派給這些節點、您已經擁有了"已建立自訂儲存等級"。您也擁有「根目錄」存取權限、或同時擁有「維護」和「 ILM 」權限。
- 如果您要新增網站、您已檢閱並更新 ILM 規則。您必須確保物件複本不會儲存到新站台、直到擴充完成為止。例如、如果規則使用預設儲存池（ * 所有儲存節點 * ）、則您必須"建立新的儲存池"只包含現有儲存節點和 ILM 原則、才能使用該新儲存"更新 ILM 規則"池。否則、只要該站台的第一個節點變成作用中、就會將物件複製到新站台。

關於這項工作

執行擴充包括下列主要使用者工作：

1. 設定擴充。
2. 開始擴充。
3. 下載新的復原包檔案。
4. 監控擴充步驟和階段、直到安裝和設定所有新節點、並啟動所有服務為止。

> 某些擴充步驟和階段可能需要大量時間才能在大型網格上執行。例如、如果Cassandra資料庫是空的、將Cassandra串流至新的儲存節點可能只需要幾分鐘的時間。不過、如果Cassandra資料庫包含大量的物件中繼資料、這個階段可能需要數小時或更長的時間。在「展開 Cassandra 叢集」或「啟動 Cassandra 和串流資料」階段期間、請勿重新啟動任何儲存節點。

步驟

1. 選擇 **Maintenance** > **Tasks** > **Grid expansion**。

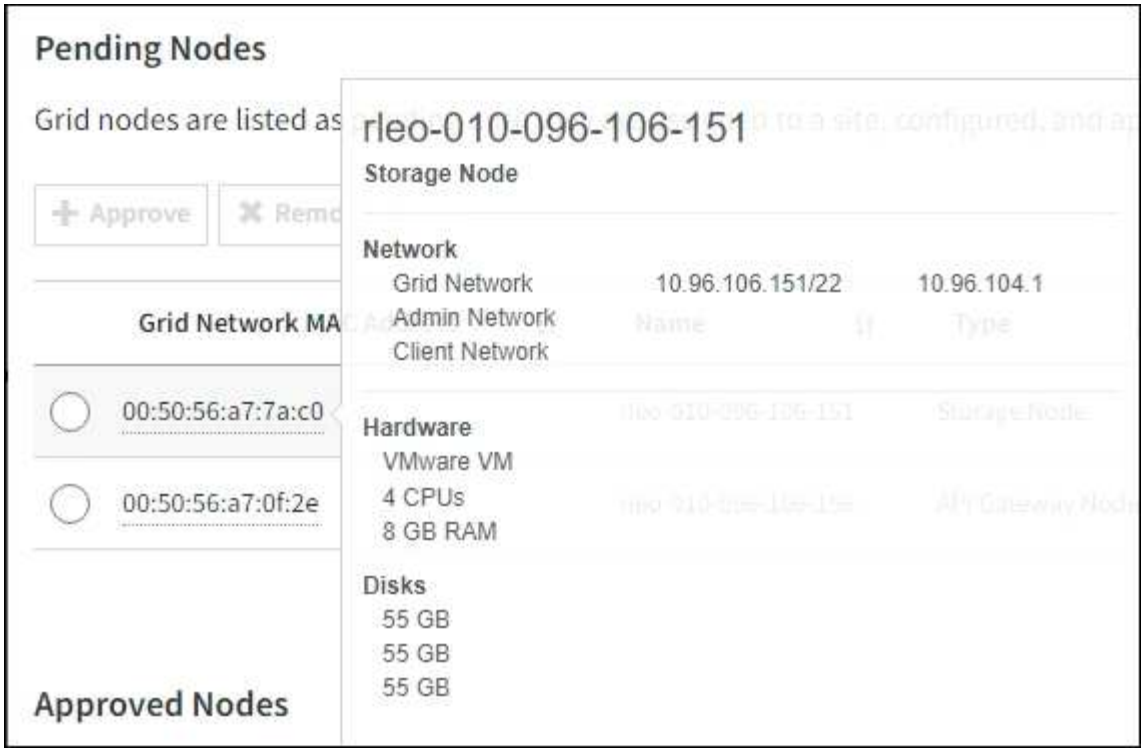
   網格擴充頁面隨即出現。「待新增節點」部分列出了可以新增的節點。

2. 選擇*組態擴充*。

   此時會出現站台選擇對話方塊。

3. 選取您要開始的擴充類型：
   - 如果您要新增站台、請選取*新增*、然後輸入新站台的名稱。
   - 如果您要將一個或多個節點新增至現有站台、請選取 * 現有 * 。
4. 選擇*保存*。
5. 檢閱「擱置節點」清單、並確認其顯示您部署的所有網格節點。

   視需要、您可以將游標放在節點的 * 網格網路 MAC 位址 * 上、以查看該節點的詳細資料。



如果節點遺失、請確認已成功部署。

6. 從擱置節點清單中、核准您要新增至此擴充項目的節點。
   a. 選取您要核准之第一個擱置的網格節點旁的選項按鈕。
   b. 選取*核准*。

      此時將出現網格節點組態表單。

   c. 視需要修改一般設定：

欄位	說明
網站	與網格節點相關聯的站台名稱。如果您要新增多個節點、請務必為每個節點選取正確的站台。如果您要新增站台、所有節點都會新增至新站台。
名稱	節點的系統名稱。內部 StorageGRID 作業需要系統名稱、因此無法變更。
儲存類型（僅限儲存節點）	• * 資料與中繼資料 * （「組合」）：物件資料與中繼資料儲存節點 • * 僅限資料 * ：僅包含物件資料的儲存節點（無中繼資料） • * 僅中繼資料 * ：僅包含中繼資料的儲存節點（無物件資料）

欄位	說明
NTP 角色	網格節點的網路時間傳輸協定（ NTP ）角色： • 選取 * 自動 *（預設）以自動指派 NTP 角色給節點。主要角色將指派給管理節點、具有 ADC 服務的儲存節點、閘道節點、以及任何具有非靜態 IP 位址的網格節點。用戶端角色將指派給所有其他網格節點。 • 選取 * 主要 * 以手動將主要 NTP 角色指派給節點。每個站台至少應有兩個節點具有「主要」角色、以提供對外部計時來源的備援系統存取。 • 選擇 * Client* 可手動將 Client NTP 角色指派給節點。
ADC 服務（組合式或純中繼資料儲存節點）	此儲存節點是否將執行管理網域控制器 (ADC) 服務。 ADC 服務追蹤電網服務的位置和可用性。每個站點至少有三個儲存節點必須包含 ADC 服務。 • 如果您要更換的儲存節點包括 ADC 服務，請選擇*是*。由於如果剩餘的 ADC 服務太少，您就無法停用儲存節點，因此此設定可確保在刪除舊服務之前有新的 ADC 服務可用。 • 你可以"將 ADC 服務移至同一網站上的另一個儲存節點"以確保滿足 ADC 服務法定人數。 • 選取 * 自動 * 讓系統判斷此節點是否需要 ADC 服務。 瞭解"ADC 仲裁"。
儲存等級（組合式或純資料儲存節點）	使用 * 預設 * 儲存等級、或選取您要指派給此新節點的自訂儲存等級。 儲存等級由 ILM 儲存資源池使用、因此您的選擇可能會影響將哪些物件放置在儲存節點上。

d. 視需要修改網格網路、管理網路和用戶端網路的設定。

- * IPV4位址（CIDR）*：網路介面的CIDR網路位址。例如： 172.16.10.100/24

> 如果您在核准節點時發現網格網路上的節點有重複的 IP 位址、則必須取消擴充、重新部署具有非重複 IP 的虛擬機器或應用裝置、然後重新啟動擴充。

- 閘道：網格節點的預設閘道。例如： 172.16.10.1
- 子網路（**CIDR**）：管理網路的一或多個子網路。

e. 選擇*保存*。

核准的網格節點會移至「核准的節點」清單。

- 若要修改已核准網格節點的內容、請選取其選項按鈕、然後選取*編輯*。
- 若要將已核准的網格節點移回「Pending Node」（擱置節點）清單、請選取其選項按鈕、然後選取* Reset*（重設*）。

- 若要永久移除已核准的網格節點、請關閉節點電源。然後選取其選項按鈕、並選取*移除*。

f. 針對您要核准的每個擱置的網格節點、重複這些步驟。

> 如有可能、您應核准所有待處理的網格備註、並執行單一擴充。如果您執行多項小型擴充、則需要更多時間。

7. 當您核准所有網格節點後，輸入*佈建複雜密碼*，然後選擇*展開*。

幾分鐘後、此頁面會更新以顯示擴充程序的狀態。當影響個別網格節點的工作正在進行中時、「網格節點狀態」區段會列出每個網格節點的目前狀態。

> 在新應用裝置的「安裝網格節點」步驟中、 StorageGRID 應用裝置安裝程式會顯示安裝從第 3 階段移至第 4 階段、完成安裝。當階段4完成時、控制器會重新開機。

> 站台擴充包括為新站台設定Cassandra的額外工作。

8. 一旦出現*下載恢復包*鏈接，請下載恢復包文件。

對StorageGRID系統進行網格拓撲變更後，您必須盡快下載復原套件檔案的更新副本。如果發生故障，恢復包檔案可讓您恢復系統。

a. 選取下載連結。

b. 輸入資源配置通關密碼、然後選取*開始下載*。

c. 下載完成後、請開啟 `.zip`檔案並確認您可以存取內容、包括 `Passwords.txt`檔案。

d. 複製下載的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

> 復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

9. 如果您要將儲存節點新增至現有站台或新增站台、請監控 Cassandra 階段、這些階段會在新的網格節點上啟動服務時發生。

> 在「展開 Cassandra 叢集」或「啟動 Cassandra 和串流資料」階段、請勿重新啟動任何儲存節點。每個新的儲存節點可能需要許多小時才能完成這些階段、尤其是現有的儲存節點包含大量的物件中繼資料時。

新增儲存節點

如果您要將儲存節點新增至現有站台、請檢閱「啟動 Cassandra 和串流資料」狀態訊息中顯示的百分比。

此百分比會根據可用的Cassandra資料總量和已寫入新節點的數量、來估計Cassandra串流作業的完成程度。

新增站台

如果您要新增站台、請使用 `nodetool status`監控 Cassandra 串流的進度、並查看在「擴充 Cassandra 叢集」階段中、已將多少中繼資料複製到新站台。新站台上的資料負載總計應在目前站台總數的20%之內。

10. 繼續監控擴充作業、直到所有工作都完成、且「組態擴充」按鈕再次出現。

完成後

視您新增的網格節點類型而定、請執行其他整合和組態步驟。請參閱。 "擴充後的組態步驟"

新增儲存磁碟區

在StorageGRID系統新增儲存磁碟區

您可以擴充低於最大支援磁碟區數的儲存節點的儲存容量。您可能需要將儲存磁碟區新增至多個儲存節點以滿足複製或擦除編碼副本的 ILM 要求。

開始之前

在新增儲存磁碟區之前、請先檢閱"新增物件容量的準則"、以確保您知道在何處新增磁碟區、以符合 ILM 原則的要求。

> 這些說明僅適用於軟體型儲存節點。請參閱 "將擴充機櫃新增至部署的 SG6060"或 "將擴充機櫃新增至部署的 SG6160"、瞭解如何安裝擴充機櫃、將儲存磁碟區新增至 SG6060 或 SG6160 。其他應用裝置儲存節點無法擴充。

關於這項工作

儲存節點的基礎儲存空間分為儲存磁碟區。儲存磁碟區是以區塊為基礎的儲存裝置、由StorageGRID 作業系統格式化並掛載以儲存物件。每個儲存節點最多可支援48個儲存磁碟區、在Grid Manager中稱為「物件存放區」。

> 物件中繼資料一律儲存在物件存放區0中。

每個物件存放區都會掛載到與其ID相對應的磁碟區上。例如、 ID 為 0000 的物件存放區對應於 `/var/local/rangedb/0`裝載點。

在新增儲存磁碟區之前、請使用Grid Manager來檢視每個儲存節點的目前物件存放區、以及對應的掛載點。您可以在新增儲存磁碟區時使用此資訊。

步驟

1. 選擇 節點 > 網站 > 儲存節點 > 儲存。
2. 向下捲動以檢視每個Volume和物件存放區的可用儲存容量。

   對於應用裝置儲存節點、每個磁碟的全球名稱會與您在 SANtricity OS （連接至應用裝置儲存控制器的管理軟體）中檢視標準 Volume 內容時所顯示的全域 Volume 識別碼（ WWID ）相符。

   為了協助您解讀磁碟讀取及寫入與磁碟區掛載點相關的統計資料、「磁碟裝置」表格*名稱*欄（即_sdc_、*sdd*、_sde_等）中顯示的名稱第一部分、會與「磁碟區」表格*「裝置*」欄中顯示的值相符。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	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
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. 依照平台的指示、將新的儲存磁碟區新增至儲存節點。
   - "VMware：將儲存磁碟區新增至儲存節點"
   - "Linux：將直接附加或SAN磁碟區新增至儲存節點"

在StorageGRID中為 VMware 儲存節點新增儲存磁碟區

如果儲存節點包含的儲存磁碟區少於 16 個，則可以使用 VMware vSphere 新增磁碟區來增加其容量。

開始之前

- 您可以訪問"為 VMware 部署安裝StorageGRID的說明"。
- 您有 `Passwords.txt`檔案。
- 您有 "特定存取權限"。

> 當軟體升級、還原程序或其他擴充程序處於作用中狀態時、請勿嘗試將儲存磁碟區新增至儲存節點。

關於這項工作

當您新增儲存磁碟區時、儲存節點會暫時無法使用。您應一次在一個儲存節點上執行此程序、以避免影響面向用戶端的網格服務。

步驟

1. 如有必要、請安裝新的儲存硬體並建立新的VMware資料存放區。
2. 將一或多個硬碟新增至虛擬機器、以做為儲存設備（物件存放區）。
   a. 開啟VMware vSphere Client。
   b. 編輯虛擬機器設定以新增一或多個額外的硬碟。

   硬碟通常設定為虛擬機器磁碟（VMDK）。VMDK 更常使用、更容易管理、而 RDM 則可為使用較大物件大小（例如大於 100 MB ）的工作負載提供更好的效能。如需將硬碟新增至虛擬機器的詳細資訊、請參閱VMware vSphere文件。
3. 使用 VMware vSphere Client 中的 * 重新啟動來賓作業系統 * 選項、或在連往虛擬機器的 ssh 工作階段中輸入下列命令、以重新啟動虛擬機器：`sudo reboot`

   > 請勿使用 * 關機 * 或 * 重設 * 來重新啟動虛擬機器。
4. 設定儲存節點使用的新儲存設備：
   a. 登入網格節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。當您以 root 登入時、提示會從變更 `$`為 `#`。

b. 設定新的儲存磁碟區：

```
sudo add_rangedbs.rb
```

此指令碼會尋找任何新的儲存磁碟區、並提示您進行格式化。

c. 輸入* y*以接受格式化。

d. 如果任何磁碟區先前已格式化、請決定是否要重新格式化。

- 輸入* y*重新格式化。
- 輸入* n*跳過重新格式化。

`setup_rangedbs.sh`指令碼會自動執行。

5. 檢查服務是否正確啟動：

a. 檢視伺服器上所有服務的狀態清單：

```
sudo storagegrid-status
```

狀態會自動更新。

a. 請等到所有服務都在執行或已驗證為止。

b. 結束狀態畫面：

```
Ctrl+C
```

6. 確認儲存節點已上線：

a. 使用登入 Grid Manager "支援的網頁瀏覽器"。

b. 選擇“節點”>“儲存節點”>“任務”。

c. 如果“儲存狀態”下拉清單設定為“唯讀”或“離線”，請選擇“線上”。

d. 選擇*保存*。

7. 若要查看新的物件存儲，請選擇*存儲*。

8. 查看*Volumes*表中的詳細資訊。

結果

您可以使用儲存節點的擴充容量來儲存物件資料。

在StorageGRID中為 Linux 儲存節點新增直連磁碟區或 SAN 卷

如果儲存節點包含少於48個儲存磁碟區、您可以新增區塊儲存設備、讓Linux主機看到這些儲存設備、並將新的區塊裝置對應新增至StorageGRID 用於儲存節點的更新組態檔、藉此增加容量。

開始之前

- 您可以訪問"StorageGRID安裝說明"適用於您的 Linux 平台。
- 您有 `Passwords.txt`檔案。
- 您有 "特定存取權限"。

> 當軟體升級、還原程序或其他擴充程序處於作用中狀態時、請勿嘗試將儲存磁碟區新增至儲存節點。

關於這項工作

當您新增儲存磁碟區時、儲存節點會暫時無法使用。您應一次在一個儲存節點上執行此程序、以避免影響面向用戶端的網格服務。

步驟

1. 安裝新的儲存硬體。

   如需詳細資訊、請參閱硬體廠商提供的文件。

2. 建立所需大小的新區塊儲存磁碟區。
   - 連接新磁碟機並視需要更新 RAID 控制器組態、或在共享儲存陣列上分配新的 SAN LUN 、並允許 Linux 主機存取這些 LUN 。
   - 使用與現有儲存節點上儲存磁碟區相同的持續命名方案。
   - 如果您使用StorageGRID 「物件節點移轉」功能、請將新的磁碟區顯示給其他Linux主機、這些主機是此儲存節點的移轉目標。如需更多資訊、請參閱Linux StorageGRID 平台的安裝資訊。
3. 以 root 或擁有 Sudo 權限的帳戶登入支援儲存節點的 Linux 主機。
4. 確認新的儲存磁碟區可在Linux主機上看到。

   您可能必須重新掃描裝置。

5. 執行下列命令、暫時停用儲存節點：

   ```
   sudo storagegrid node stop <node-name>
   ```

6. 使用 vim 或 pico 等文字編輯器、編輯儲存節點的節點組態檔案、可在中找到 `/etc/storagegrid/nodes/<node-name>.conf`。
7. 找出節點組態檔中包含現有物件儲存區塊裝置對應的區段。

   在範例中、 `BLOCK_DEVICE_RANGEDB_00`目標 `BLOCK_DEVICE_RANGEDB_03`是現有的物件儲存區塊裝置對應。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. 新增對應於您為此儲存節點新增之區塊儲存磁碟區的物件儲存區塊裝置對應。

   請務必從下一個開始 `BLOCK_DEVICE_RANGEDB_nn`。不要留下任何落差。

   - 根據上述範例，請從開始 `BLOCK_DEVICE_RANGEDB_04`。
   - 在以下範例中、已將四個新的區塊儲存磁碟區新增至節點： `BLOCK_DEVICE_RANGEDB_04`至 `BLOCK_DEVICE_RANGEDB_07`。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 執行下列命令、以驗證您對儲存節點節點組態檔所做的變更：

   ```
   sudo storagegrid node validate <node-name>
   ```

   在繼續下一步之前、請先解決任何錯誤或警告。

如果您觀察到類似下列的錯誤、表示節點組態檔案正嘗試將 for <PURPOSE> 所使用的區塊裝置對應至 Linux 檔案系統中的指定 <path-name>、但該位置沒有有效的區塊 `<node-name>`裝置特殊檔案（或區塊裝置特殊檔案的軟連結）。

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

驗證您輸入的是正確 `<path-name>`的。

10. 執行下列命令、以新的區塊裝置對應重新啟動節點：

```
sudo storagegrid node start <node-name>
```

11. 使用檔案中列出的密碼、以管理員身分登入儲存節點 Passwords.txt。
12. 檢查服務是否正確啟動：
    a. 檢視伺服器上所有服務的狀態清單：
    sudo storagegrid-status

    狀態會自動更新。

    b. 請等到所有服務都在執行或已驗證為止。
    c. 結束狀態畫面：

    Ctrl+C

13. 設定儲存節點使用的新儲存設備：
    a. 設定新的儲存磁碟區：

    sudo add_rangedbs.rb

    此指令碼會尋找任何新的儲存磁碟區、並提示您進行格式化。

    b. 輸入* y*格式化儲存磁碟區。
    c. 如果任何磁碟區先前已格式化、請決定是否要重新格式化。
        - 輸入* y*重新格式化。
        - 輸入* n*跳過重新格式化。

    `setup_rangedbs.sh`指令碼會自動執行。

14. 確認儲存節點的儲存狀態為線上：
    a. 使用登入 Grid Manager "支援的網頁瀏覽器"。
    b. 選擇“節點”>“儲存節點”>“任務”。

c. 如果“儲存狀態”下拉清單設定為“唯讀”或“離線”，請選擇“線上”。

d. 選擇*保存*。

15. 若要查看新的物件存儲，請選擇*存儲*。

16. 查看*Volumes*表中的詳細資訊。

結果

您現在可以使用儲存節點的擴充容量來儲存物件資料。

設定擴充系統

在StorageGRID中配置新新增的節點和站點

完成擴充之後、您必須執行其他整合與組態步驟。

關於這項工作

您必須完成以下所列的網格節點或擴充中新增的站台組態工作。某些工作可能是選擇性的、視安裝和管理系統時所選的選項、以及您想要如何設定擴充期間新增的節點和站台而定。

步驟

1. 如果您新增站台：

   - "建立儲存資源池"針對您為新的儲存節點所選擇的站台和每個儲存等級。
   - 確認 ILM 原則符合新要求。如果需要變更規則、"建立新規則"請"更新 ILM 原則"參閱和。如果規則已經正確、則不會變更任何規則、"啟動新原則"以確保 StorageGRID 使用新節點。
   - 確認可從該站台存取網路時間傳輸協定（ NTP ）伺服器。請參閱。 "管理NTP伺服器"

   > 請確定每個站台至少有兩個節點可以存取至少四個外部NTP來源。如果站台只有一個節點可以連線至NTP來源、則當該節點當機時、就會發生計時問題。此外、將每個站台的兩個節點指定為主要NTP來源、可確保站台與網格的其他部分隔離時、能確保準確的時間安排。

2. 如果您將一或多個儲存節點新增至現有站台：

   - "檢視儲存資源池詳細資料"確認您新增的每個節點都包含在預期的儲存資源池中、並用於預期的 ILM 規則。
   - 確認 ILM 原則符合新要求。如果需要變更規則、"建立新規則"請"更新 ILM 原則"參閱和。如果規則已經正確、則不會變更任何規則、"啟動新原則"以確保 StorageGRID 使用新節點。
   - "確認儲存節點處於作用中狀態"並能擷取物件。
   - 如果您無法新增建議的儲存節點數量、請重新平衡銷毀編碼資料。請參閱。 "新增儲存節點後、重新平衡以銷毀編碼的資料"

3. 如果您新增了閘道節點：

   - 如果用戶端連線使用高可用性 (HA) 群組，則可以選擇將網關節點新增至 HA 群組。選擇「設定」>「網路」>「高可用性群組」來查看現有 HA 群組的清單並新增節點。看"設定高可用度群組" 。

4. 如果您新增了管理節點：

a. 如果您的 StorageGRID 系統已啟用單一登入 （SSO），請為新的管理節點建立信賴方信任。在建立此信賴方信任之前，您無法登入該節點。請參閱使用 "OIDC" 或 "SAML" 設定 SSO。

b. 如果您打算在管理節點上使用負載平衡器服務，則可以選擇將新的管理節點新增至 HA 群組。選擇「設定」>「網路」>「高可用性群組」來查看現有 HA 群組的清單並新增節點。看"設定高可用度群組" 。

c. 或者、如果您想在每個管理節點上保持歷史數據一致、請將Prometheus資料庫從主要管理節點複製到擴充管理節點。請參閱。 "複製Prometheus指標"

d. 或者、如果您想要在每個管理節點上保持記錄資訊一致、請將現有的稽核記錄從主要管理節點複製到擴充管理節點。請參閱。 "複製稽核記錄"

5. 要檢查擴展節點是否添加了不受信任的客戶端網絡，或者要更改節點的客戶端網路是否不受信任或受信任，請前往*配置*>*安全*>*防火牆控制*。

   如果擴充節點上的用戶端網路不受信任、則必須使用負載平衡器端點連線至用戶端網路上的節點。請參閱"設定負載平衡器端點"和"管理防火牆控制"。

6. 設定 DNS 。

   如果您已分別為每個網格節點指定DNS設定、則必須為新節點新增自訂的每節點DNS設定。請參閱。 "修改單一網格節點的DNS組態"

若要確保正常運作、請指定兩或三個 DNS 伺服器。如果您指定超過三個、可能只會使用三個、因為某些平台的已知作業系統限制。如果您在環境中有路由限制、則可"自訂 DNS 伺服器清單"讓個別節點（通常是站台上的所有節點）使用最多三個 DNS 伺服器的不同組別。

如有可能、請使用每個站台都能在本機存取的 DNS 伺服器、以確保某個著陸站台可以解析外部目的地的 FQDN 。

在StorageGRID擴充後，驗證儲存節點是否處於活動狀態。

在新增儲存節點的擴充作業完成後、StorageGRID 該系統應自動開始使用新的儲存節點。您必須使用StorageGRID 此功能驗證新的儲存節點是否處於作用中狀態。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 選擇“節點”>“擴充儲存節點”>“儲存”。
3. 將游標放在 * 「已使用的儲存空間 - 物件資料 * 」圖形上方、即可檢視 * 已使用 * 的值、這是已用於物件資料的總可用空間量。
4. 將游標移到圖表右側時、請確認*已使用*的值正在增加。

將 Prometheus 指標複製到StorageGRID中的新管理節點

新增管理節點之後、您可以選擇性地將Prometheus維護的歷史指標、從主要管理節點複製到新的管理節點。複製度量可確保管理節點之間的歷史度量一致。

開始之前

- 新的管理節點已安裝並執行。
- 您有 `Passwords.txt`檔案。

- 您有資源配置通關密碼。

關於這項工作

新增管理節點時、軟體安裝程序會建立新的Prometheus資料庫。您可以將Prometheus資料庫從主要管理節點（_SOURUS管理節點）複製到新的管理節點、使節點之間的歷史指標保持一致。

> 複製Prometheus資料庫可能需要一小時以上的時間。當服務在來源管理節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。
2. 從來源管理節點停止 Prometheus 服務： `service prometheus stop`
3. 在新的管理節點上完成下列步驟：
   a. 登入新的管理節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。
   b. 停止 Prometheus 服務： `service prometheus stop`
   c. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`
   d. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。
   e. 將 Prometheus 資料庫從來源管理節點複製到新的管理節點：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出現提示時、請按* Enter *確認您要在新的管理節點上銷毀新的Prometheus資料庫。

      原始的Prometheus資料庫及其歷史資料會複製到新的管理節點。複製作業完成後、指令碼會啟動新的管理節點。此時會顯示下列狀態：

```
Database cloned, starting services
```

   a. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：

```
ssh-add -D
```

4. 在來源管理節點上重新啟動Prometheus服務。

```
service prometheus start
```

將稽核日誌複製到StorageGRID中的新管理節點

當您透過擴充功能新增新的管理節點時，其 AMS 服務僅記錄其加入系統後發生的事件和操作。根據需要，您可以將稽核日誌從先前安裝的管理節點複製到新的擴充管理節點，以便它與StorageGRID系統的其餘部分同步。

開始之前

- 您已完成新增管理節點所需的擴充步驟。
- 您有 `Passwords.txt`檔案。

關於這項工作

若要在新的管理節點上提供歷史稽核訊息、您必須手動將稽核記錄檔從現有的管理節點複製到擴充管理節點。

> 預設情況下，審計資訊將發送到 `localaudit`登入每個節點。若要使用此流程，您必須已將管理節點配置為稽核目標，如下所示：
>
> - 您將 管理節點/本機節點 配置為日誌目標。
> - 您已將*管理節點和外部系統日誌伺服器*配置為日誌目標。
>
> 參考"設定稽核訊息和外部 Syslog 伺服器"了解詳情。

步驟

1. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@_primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 停止 AMS 服務以防止其建立新檔案： `service ams stop`
3. 瀏覽至稽核匯出目錄：

   ```
   cd /var/local/audit/export/
   ```

4. 重新命名來源 `audit.log`文件以確保它不會覆蓋您要將其複製到的擴充管理節點上的檔案：

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```

5. 將所有稽核記錄檔複製到擴充管理節點上的目的地位置：

   ```
   scp -p * IP_address:/var/local/audit/export/
   ```

6. 如果系統提示您輸入的密碼 `/root/.ssh/id_rsa`、請輸入檔案中所列主要管理節點的 SSH 存取密碼 `Passwords.txt`。
7. 還原原始 `audit.log`檔案：

   ```
   mv new_name.txt audit.log
   ```

8. 啟動AMS服務：

   ```
   service ams start
   ```

9. 從伺服器登出：

   ```
   exit
   ```

10. 登入擴充管理節點：
    a. 輸入下列命令： `ssh admin@expansion_Admin_Node_IP`
    b. 輸入檔案中列出的密碼 `Passwords.txt`。
    c. 輸入以下命令切換到 root ： `su -`
    d. 輸入檔案中列出的密碼 `Passwords.txt`。

       當您以 root 登入時、提示會從變更 `$`為 `#`。

11. 更新稽核記錄檔的使用者和群組設定：

    ```
    cd /var/local/audit/export/

    chown ams-user:bycast *
    ```

12. 從伺服器登出：

    ```
    exit
    ```

在StorageGRID系統新增節點後，重新平衡糾刪碼資料。

新增儲存節點之後、您可以使用抹除編碼（ EC ）重新平衡程序、在現有和新的儲存節點之間重新分配銷毀編碼片段。

開始之前

- 您已完成新增儲存節點的擴充步驟。
- 您已檢閱"重新平衡銷毀編碼資料的考量事項"。
- 您了解複製的物件資料不會被此過程移動，且 EC 重新平衡過程不會移動複製的資料。但是，在確定將 EC 資料移至何處時，會考慮複製資料。
- 您有 `Passwords.txt`檔案。

執行此程序時會發生什麼情況

開始程序之前、請注意下列事項：

- 如果一或多個磁碟區離線（未掛載）、或是它們在線上（掛載）但處於錯誤狀態、則 EC 重新平衡程序將不會啟動。
- EC重新平衡程序會暫時保留大量的儲存空間。儲存警示可能會觸發、但會在重新平衡完成時解決。如果保留空間不足、EC重新平衡程序將會失敗。無論程序失敗或成功、在EC重新平衡程序完成時、都會釋出儲存保留。
- 如果在 EC 重新平衡程序進行期間某個 Volume 離線、則重新平衡程序將會終止。已移動的任何資料片段都會保留在新位置、不會遺失任何資料。

  您可以在所有磁碟區重新上線後重新執行程序。

- 當執行 EC 重新平衡程序時、 ILM 作業和 S3 用戶端作業的效能可能會受到影響。

> 如果需要超過 24 小時才能完成、則上傳物件（或物件零件）的 S3 API 作業可能會在 EC 重新平衡程序期間失敗。如果適用的 ILM 規則在擷取上使用平衡或嚴格的放置方式、則長時間的放置作業將會失敗。將報告以下錯誤： `500 Internal Server Error`。

- * 工作完成條件 * 。當下列任一情況成立時、 EC 重新平衡程序即視為完成：
  - 它無法移動任何其他的銷毀編碼資料。
  - 所有節點中的資料與目標可用空間劃分的偏差均在 5% 以內。
  - 此程序已執行 30 天。

步驟

1. [[ree_object_storage]檢閱您計畫重新平衡之站台的目前物件儲存詳細資料。
   a. 選擇*節點*。
   b. 選取站台的第一個儲存節點。
   c. 選擇* Storage*（儲存設備）選項卡。
   d. 將游標放在「已使用的儲存空間 - 物件資料」圖表上、即可查看儲存節點上目前的複寫資料量和銷毀編碼資料量。
   e. 重複這些步驟、即可檢視站台上的其他儲存節點。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
3. 開始以下程序：

   ' 重新平衡資料開始 - 站台 "*side-name*"

   對於 "*side-name*" 、請指定您新增儲存節點或節點的第一個站台。請以引號括住 `site-name`。

EC重新平衡程序隨即開始、並傳回工作ID。

4. 複製工作ID。
5. 監控 EC 重新平衡程序的狀態。
   - 若要檢視單一EC重新平衡程序的狀態：

     ```
     rebalance-data status --job-id job-id
     ```

     對於 *job-id*，請指定在啓動過程時返回的 ID 。
   - 若要檢視目前EC重新平衡程序的狀態、以及任何先前完成的程序：

     ```
     rebalance-data status
     ```

     > 若要取得有關reBalance-data命令的說明：
     >
     > ```
     > rebalance-data --help
     > ```

6. 根據傳回的狀態執行其他步驟：
   - 如果 `State`為 `In progress`、則 EC 重新平衡作業仍在執行中。您應該定期監控程序、直到程序完成為止。

     前往節點頁面來評估網站中儲存節點的資料分佈。

   當所有節點中的可用空間與目標可用空間分割區之間的偏差在 5% 以內時，EC 重新平衡作業即被視為完成並停止。
   - 如果為 `Success`、則 `State`可選擇性地檢閱物件儲存查看網站的更新詳細資料。

     站台上各個儲存節點的可用空間現在應該更加均衡。
   - 如果 `State`是 `Failure`：
     i. 確認站台上的所有儲存節點均已連線至網格。
     ii. 檢查並解決可能影響這些儲存節點的任何警示。
     iii. 重新啟動 EC 重新平衡程序：

     ```
     rebalance-data start --job-id job-id
     ```

     iv. 檢視狀態的新程序。如果 `State`仍在 `Failure`、請聯絡技術支援部門。
7. 如果EC重新平衡程序產生過多負載（例如、擷取作業會受到影響）、請暫停程序。

   ```
   rebalance-data pause --job-id job-id
   ```

8. 如果您需要終止EC重新平衡程序（例如、您可以執行StorageGRID 更新版的程式碼）、請輸入下列命令：

   ```
   rebalance-data terminate --job-id job-id
   ```

當您終止 EC 重新平衡程序時、任何已移動的資料片段都會保留在新的位置。資料不會移回原始位置。

9. 如果您在多個站台使用銷毀編碼、請針對所有其他受影響的站台執行此程序。

排除StorageGRID中的擴充錯誤

如果您在網格擴充程序期間遇到無法解決的錯誤、或網格工作失敗、請收集記錄檔並聯絡技術支援部門。

聯絡技術支援人員之前、請先收集必要的記錄檔、以協助進行疑難排解。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 連線至發生故障的擴充節點：

   a. 請輸入以下命令： `ssh -p 8022 admin@grid_node_IP`

      連接埠8022是基礎作業系統的SSH連接埠、而連接埠22則是執行StorageGRID 支援的Container引擎SSH連接埠。

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   以 root 登入後、提示會從變更 `$`為 `#`。

3. 視安裝所到達的階段而定、擷取網格節點上可用的下列任何記錄：

平台	記錄
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf`（針對每個故障節點） • `/var/log/storagegrid/nodes/<node-name>.log`（對於每個故障節點、可能不存在）

4. 如果您允許外部 SSH 訪問，"阻止訪問"當你完成任務時。

維護 StorageGRID 系統

StorageGRID 網格維護

網格維護工作包括汰換節點或站台、重新命名網格、節點或站台、以及維護網路。您也可以執行主機和中介軟體程序、以及網格節點程序。

> 在這些說明中，「Linux」指的是 Red Hat® Enterprise Linux® (RHEL)、Ubuntu® 或 Debian® 部署。有關受支援版本的列表，請參閱 "NetApp 互通性對照表工具"。

開始之前

- 您對StorageGRID 此系統有廣泛的瞭解。
- 您已檢閱StorageGRID 過您的不全系統拓撲、並瞭解網格組態。
- 您瞭解必須確實遵循所有指示、並留意所有警告。
- 您瞭解不支援未說明的維護程序、或是需要服務參與。

設備的維護程序

有關硬體程序、請參閱 "StorageGRID 應用裝置的維護指示"。

下載 StorageGRID 恢復套件

如果發生故障，恢復包檔案可讓您恢復StorageGRID系統。

開始之前

- 從任何管理節點，您都可以使用"支援的網頁瀏覽器"。
- 您有資源配置通關密碼。
- 您有 "特定存取權限"。

在對StorageGRID系統進行網格拓撲變更或升級軟體之前，請下載目前的復原套件檔案。然後，在更改電網拓撲或升級軟體後下載恢復包的新副本。

步驟

1. 選擇*維護* > 系統 > 恢復包。
2. 輸入資源配置密碼、然後選取 * 開始下載 * 。

   下載隨即開始。

3. 下載完成後、請開啟 `.zip`檔案並確認您可以存取內容、包括 `Passwords.txt`檔案。
4. 複製下載的復原包文件(`.zip`）到兩個安全、可靠且獨立的地點。

復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

取消委任節點或站台

停用 StorageGRID 節點或站台

您可以執行取消委任程序、將網格節點或整個站台從StorageGRID 整套系統中永久移除。

若要移除網格節點或站台、請執行下列取消委任程序之一：

- 執行"網格節點取消委任"以移除一個或多個節點、這些節點可以位於一個或多個站台。您移除的節點可以連線至StorageGRID 線上、也可以離線或中斷連線。
- 執行"站台取消委任"以移除站台。如果所有節點都連接到 StorageGRID 、您就可以執行 * 已連線的站台取消委任 * 。如果所有節點都與 StorageGRID 中斷連線、您可以執行 * 中斷連線的站台取消委任 * 。如果站台混合了已連線和已中斷連線的節點、您必須將所有離線節點重新上線。

在執行中斷連線的站台取消委任之前、請聯絡您的 NetApp 客戶代表。NetApp將在取消委任網站精靈中啟用所有步驟之前、先審查您的需求。如果您認為可以從站台恢復或從站台恢復物件資料、則不應嘗試中斷站台的停用。

在退役網格節點之前，您必須確認沒有處於活動狀態的資料修復作業。如果任何修復失敗，則必須重新啟動它們並讓它們完成，然後再執行退役程序。請參閱"檢查資料修復工作" 。

取消委任節點

StorageGRID 網格節點汰除

您可以使用節點取消委任程序、在一或多個站台上移除一或多個網格節點。您無法取消委任主要管理節點。

何時取消委任節點

當下列任一情況成立時、請使用節點取消委任程序：

- 您在擴充中新增了較大的儲存節點、並想要移除一個或多個較小的儲存節點、同時保留物件。

如果您想要以較新的應用裝置來更換較舊的應用裝置、請考慮不要在擴充設備中新增新的應用裝置、然後將舊的應用裝置汰換 "複製應用裝置節點"。

- 您所需的總儲存容量較少。
- 您不再需要閘道節點。
- 您不再需要非主要管理節點。
- 您的網格包含一個中斷連線的節點、您無法恢復或恢復連線。
- 您的網格包含歸檔節點。

如何取消委任節點

您可以取消委任連接的網格節點或中斷連線的網格節點。

取消委任已連線的節點

一般來說，只有當網格節點連接到StorageGRID系統並且所有節點都處於正常狀態（在 節點 頁面和 退役節點 頁面上有綠色圖示）時，才應該退役網格節點。

有關說明，請參閱"取消委任連線的網格節點"。

取消委任中斷連線的節點

在某些情況下、您可能需要取消委任目前未連線至網格的網格節點（健全狀況為未知或管理性關閉的節點）。

有關說明，請參閱"取消委任中斷連線的網格節點"。

淘汰節點之前應考慮的事項

在執行任一程序之前、請先檢閱每種節點類型的考量事項：

- "管理或閘道節點取消委任的考量事項"
- "儲存節點取消委任的考量事項"

StorageGRID 管理或閘道節點取消委任考量

檢閱解除委任管理節點或閘道節點的考量事項。

管理節點的考量事項

- 您無法取消委任主要管理節點。
- 如果管理節點的其中一個網路介面是高可用度（ HA ）群組的一部分、則無法取消委任管理節點。您必須先從HA群組移除網路介面。請參閱的說明"管理 HA 群組"。
- 視需要、您可以在解除委任管理節點的同時、安全地變更 ILM 原則。
- 如果您取消委任管理節點、並啟用StorageGRID 單一登入（SSO）來啟用您的支援、您必須記得從Active Directory Federation Services（AD FS）移除節點的信賴方信任。
- 如果您使用"網格同盟"、請確定您要停用的節點的 IP 位址未指定給網格同盟連線。
- 當您取消委任已中斷連線的管理節點時、將會遺失該節點的稽核記錄；不過、這些記錄也應該存在於主要管理節點上。

閘道節點的考量事項

- 如果閘道節點的其中一個網路介面是高可用度（ HA ）群組的一部分、您就無法取消委任該節點。您必須先從HA群組移除網路介面。請參閱的說明"管理 HA 群組"。
- 視需要、您可以在解除委任閘道節點的同時、安全地變更 ILM 原則。
- 如果您使用"網格同盟"、請確定您要停用的節點的 IP 位址未指定給網格同盟連線。
- 您可以在閘道節點中斷連線時安全地取消委任。

StorageGRID 中的儲存節點汰換考量事項

在解除委任儲存節點之前、請考慮是否可以改為複製節點。然後、如果您決定取消委任節點、請檢閱 StorageGRID 在取消委任程序期間如何管理物件和中繼資料。

何時要複製節點而非將其停用

如果您想要以較新或較大的應用裝置來取代較舊的應用裝置儲存節點、請考慮複製應用裝置節點、而不要在擴充中新增新應用裝置、然後將舊應用裝置汰換。

設備節點複製功能可讓您在同一個 StorageGRID 站台上、使用相容的應用裝置輕鬆更換現有的應用裝置節點。複製程序會將所有資料傳輸到新應用裝置、將新應用裝置放置在服務中、並將舊應用裝置保留在預先安裝狀態。

如果需要：

- 請更換已達到使用壽命的產品。
- 升級現有節點、充分利用改良的應用裝置技術。
- 增加網格儲存容量、而不需變更StorageGRID 您的一套系統中的儲存節點數量。
- 改善儲存效率、例如變更 RAID 模式。

如需詳細資訊、請參閱 "應用裝置節點複製"。

連線儲存節點的考量事項

檢閱解除委任連線儲存節點的考量事項。

- 在單一取消委任節點程序中、您不應取消委任超過10個儲存節點。
- 系統必須始終包含足夠的儲存節點以滿足運作需求，包括 "ADC 仲裁" 和使用中的 "ILM原則"。如果退役作業會導致站台的 ADC 數量低於法定人數，StorageGRID 會自動將 ADC 服務移至同一站台上可用的非 ADC 儲存節點，以維持 ADC 法定人數。如果 ADC 服務無法自動移動，您可能需要先 "在擴充作業中新增儲存節點"，才能退役現有的儲存節點。

  在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

- 移除儲存節點時、會透過網路傳輸大量的物件資料。雖然這些傳輸不應影響正常的系統作業、但它們可能會影響 StorageGRID 系統所使用的網路頻寬總量。
- 與儲存節點解除委任相關的工作優先順序低於正常系統作業相關的工作。這表示汰換不會干擾StorageGRID正常的非功能性系統作業、也不需要排定系統閒置一段時間。由於汰換是在背景執行、因此很難預估完成程序所需的時間。一般而言、當系統處於靜止狀態時、或一次只移除一個儲存節點時、汰換作業會更快完成。
- 取消委任儲存節點可能需要數天或數週的時間。請據此規劃此程序。雖然取消委任程序的設計不會影響系統作業、但它可能會限制其他程序。一般而言、移除網格節點之前、您應該先執行任何計畫性的系統升級或擴充。
- 如果您需要在移除儲存節點時執行其他維護程序、則可以在其他程序完成後繼續執行"暫停取消委任程序"。

只有在達到ILM評估或銷毀編碼資料解除委任階段時、才會啟用*暫停*按鈕；不過、ILM評估（資料移轉）仍會在背景中繼續執行。

- 當取消委任工作正在執行時、您無法在任何網格節點上執行資料修復作業。
- 在解除委任儲存節點時、您不應對 ILM 原則進行任何變更。
- 若要永久且安全地移除資料、您必須在解除委任程序完成後、清除儲存節點的磁碟機。

中斷連線儲存節點的考量事項

檢閱解除委任中斷連線的儲存節點的考量事項。

- 除非您確定無法將中斷連線的節點上線或還原、否則請勿將其取消委任。

如果您認為可能可以從節點恢復物件資料、請勿執行此程序。請聯絡技術支援部門、以判斷是否可以恢復節點。

- 當您取消委任中斷連線的儲存節點時、 StorageGRID 會使用來自其他儲存節點的資料來重建中斷連線節點上的物件資料和中繼資料。
- 如果您取消委任多個中斷連線的儲存節點、可能會導致資料遺失。如果沒有足夠的物件複本、銷毀編碼的片段或物件中繼資料可供使用、系統可能無法重建資料。當在網格中停用儲存節點時、若只有軟體型中繼資料節點、則停用所有設定為同時儲存物件和中繼資料的節點、會從網格中移除所有物件儲存。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

如果您有多個無法恢復的已中斷連線儲存節點、請聯絡技術支援部門、以決定最佳的行動方針。

- 當您取消委任已中斷連線的儲存節點時、StorageGRID 在解除委任程序結束時、即可開始執行資料修復工作。這些工作會嘗試重建儲存在中斷連線節點上的物件資料和中繼資料。
- 當您取消委任已中斷連線的儲存節點時、取消委任程序相對較快完成。不過、資料修復工作可能需要數天或數週的時間才能執行、而且不會受到取消委任程序的監控。您必須手動監控這些工作、並視需要重新啟動。請參閱。 "檢查資料修復工作"
- 如果您取消委任包含物件唯一複本的已中斷連線儲存節點、該物件將會遺失。只有在目前連線的儲存節點上至少有一個複寫複本或有足夠的銷毀編碼片段存在時、資料修復工作才能重建及還原物件。

什麼是 **StorageGRID ADC** 仲裁？

ADC 仲裁機制可確保每個站點至少保留一定數量的管理網域控制站 （ADC） 服務可用。StorageGRID 在必要時會自動在退役期間移動 ADC 服務。

在某些儲存節點上找到的 ADC 服務可維護網格拓撲資訊、並為網格提供組態服務。這個支援系統要求每個站台及任何時間都能達到特定的ADC服務量。StorageGRID

如果移除節點會導致不再符合 ADC 仲裁、則無法取消委任儲存節點。為了在汰換期間滿足 ADC 仲裁、每個站台至少必須有三個儲存節點、才能使用 ADC 服務。如果站台有三個以上的儲存節點搭配 ADC 服務、則在汰換之後、這些節點中的大多數必須保持可用： `((0.5 * Storage Nodes with ADC) + 1)`

在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

例如、假設某個站台目前包含六個具有 ADC 服務的儲存節點、而您想要取消委任三個儲存節點。由於必須達到ADC仲裁要求、您必須完成下列兩個取消委任程序：

- 在第一次取消委任程序中、您必須確保具有 ADC 服務的四個儲存節點仍然可用 `((0.5 * 6) + 1)`：。這表示您一開始只能取消委任兩個儲存節點。
- 在第二個退役過程中，您可以刪除第三個儲存節點，因為 ADC 仲裁現在只需要三個 ADC 服務保持可用：`((0.5 * 4) + 1)` 。

當您退役一個提供 ADC 服務的儲存節點時，如果退役會導致網站的 ADC 數量低於法定數量，StorageGRID 會自動將 ADC 服務遷移到同一網站上的另一個儲存節點。自動遷移的前提是網格中的所有節點都已連線，且同一網站上存在可接收該服務的非 ADC 儲存節點。退役程序會確保每個網站至少保留三個 ADC 儲存節點。例如，如果您在一個網站上退役四個或六個 ADC 節點，假設同一網站上存在可用的非 ADC 節點，則程序結束後仍會保留三個 ADC 儲存節點。

如果 ADC 服務無法自動遷移，您可以"手動移動 ADC 服務"將其遷移到同一網站上的另一個儲存節點，或"在擴充中新增一個新的儲存節點"並指定該節點需要 ADC 服務。然後，您可以退役現有儲存節點，而不會影響仲裁。

檢閱 **StorageGRID ILM** 原則和儲存組態

如果您打算取消委任儲存節點、則在StorageGRID 開始解除委任程序之前、應先檢閱您的一套NetApp系統的ILM原則。

在汰換期間、所有物件資料都會從停用的儲存節點移轉至其他儲存節點。

您在取消委任期間擁有的ILM原則將是取消委任後使用的ILM原則。在開始取消委任之前及取消委任完成後、您都必須確保此原則符合您的資料需求。

您應該檢閱每個規則"主動式 ILM 原則"、以確保 StorageGRID 系統將繼續擁有足夠容量的正確類型和正確位置、以容納儲存節點的汰換。

請考慮下列事項：

- ILM評估服務是否能複製物件資料、以符合ILM規則？
- 當停用進行中的站台暫時無法使用時、會發生什麼情況？是否可以在其他位置製作其他複本？
- 汰換程序如何影響內容的最終發佈？如中所述"整合儲存節點"、您應該"新增儲存節點"在汰換舊的前置作業。如果您在解除委任較小的儲存節點之後新增較大的替換儲存節點、舊的儲存節點可能接近容量、而新的儲存節點幾乎沒有內容。新物件資料的大部分寫入作業會導向新的儲存節點、進而降低系統作業的整體效率。
- 系統是否會隨時包含足夠的儲存節點、以滿足使用中的 ILM 原則？

  無法滿足的 ILM 原則會導致待處理記錄和警示、並可能停止 StorageGRID 系統的運作。

評估表中列出的區域、確認解除委任程序所產生的建議拓撲符合 ILM 原則。

需要評估的領域	考量事項
可用容量	是否有足夠的儲存容量來容納儲存在 StorageGRID 系統中的所有物件資料、包括目前儲存在要停用的儲存節點上的物件資料永久複本？ 在完成停用後、是否有足夠的容量來處理預估的儲存物件資料成長時間、以達到合理的時間間隔？
儲存位置	如果StorageGRID 整個恆指系統仍有足夠的容量、那麼該容量是否位於適當位置、以滿足StorageGRID 該系統的業務規則？
儲存類型	取消委任完成後、是否會有足夠的適當類型儲存空間？ 例如、 ILM 規則可能會將內容從一種儲存設備移至另一種儲存設備、做為內容老化的方式。在這種情況下、您必須確保 StorageGRID 系統的最終組態中有足夠的適當類型儲存空間。

整合 **StorageGRID** 儲存節點

您可以整合儲存節點、以減少站台或部署的儲存節點數、同時增加儲存容量。

當您整合儲存節點時、您可以"展開 StorageGRID 系統"新增容量更大的新儲存節點、然後取消委任容量較小的舊儲存節點。在取消委任程序期間、物件會從舊的儲存節點移轉至新的儲存節點。

> 如果您要使用新機型或大容量設備來整合較舊和較小的設備、請考慮（如果您沒有進行一對一的更換、則可以 "複製應用裝置節點"使用設備節點複製和取消委任程序）。

例如、您可以新增兩個較大容量的新儲存節點、以取代三個較舊的儲存節點。您會先使用擴充程序來新增兩個較大的新儲存節點、然後使用取消委任程序來移除三個較小的舊儲存節點。

在移除現有的儲存節點之前新增容量、可確保在StorageGRID 整個整個作業系統之間更平衡地分配資料。您也可以降低現有儲存節點可能被推到儲存浮水印層級以外的可能性。

停用多個 **StorageGRID** 儲存節點

如果您需要移除多個儲存節點、可以依序或平行取消委任。

> 在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

- 如果您依序取消委任儲存節點、則必須等到第一個儲存節點完成解除委任之後、才能開始取消委任下一個儲存節點。
- 如果您平行取消委任儲存節點、則儲存節點會同時處理所有停用儲存節點的取消委任工作。這可能會導致檔案的所有永久複本都標示為「唯讀」、並在啟用此功能的網格中暫時停用刪除功能。

檢查 **StorageGRID** 中的資料修復工作

在退役或擴展網格節點之前，您必須確認沒有處於活動狀態的資料修復作業。如果任何修

復失敗，則必須重新啟動它們並讓它們完成，然後再執行退役程序。

- 參考"擴充類型"有關如何擴展網格節點的詳細資訊。
- 使用 Grid Manager 監控正在進行的恢復程序並顯示恢復歷史記錄。請參閱以下程序：
  - "將物件資料還原至應用裝置的儲存磁碟區"
  - "將物件資料還原至系統磁碟機不受影響的儲存磁碟區"
  - "將物件資料還原至儲存磁碟區（系統磁碟機故障）"

收集 StorageGRID 節點退役所需的材料

在執行網格節點取消委任之前、您必須先取得下列資訊。

項目	附註
恢復包 `.zip`文件	你必須"下載最新的復原包" `.zip`文件（`sgws-recovery-package-id-revision.zip`）。如果發生故障，您可以使用復原包檔案來復原系統。
`Passwords.txt`檔案	該檔案包含在命令列上存取網格節點所需的密碼，並包含在復原套件中。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼不在 `Passwords.txt`檔案中。
汰換之前、請先說明StorageGRID這個系統的拓撲	如有、請取得任何說明系統目前拓撲的文件。

相關資訊

"網頁瀏覽器需求"

存取 StorageGRID 中的解除委任節點頁面

當您存取Grid Manager中的「取消委任節點」頁面時、您可以一覽哪些節點可以停用。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。

> 在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

步驟

1. 選擇*維護* > 任務 > 退役。
2. 選取*取消委任節點*。

此時會出現「取消委任節點」頁面。在此頁面中、您可以：

- 判斷哪些網格節點目前可以停用。
- 查看所有網格節點的健全狀況
- 按*名稱*、站台、*類型*或*具有ADC/*的遞增或遞減順序排序清單。
- 輸入搜尋詞彙以快速尋找特定節點。

在此範例中、「可退役」欄中的綠色核取記號表示您可以退役 API Gateway 節點和僅含資料的儲存節點。其他節點因各種原因無法退役。例如、主要管理節點無法退役、因為不支援退役此類型的節點。僅含中繼資料的儲存節點無法退役、因為退役後站台將不再符合 "ADC 仲裁"。

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	⚠	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node (Metadata-only)	Yes	✓	No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S4	Data Center 1	Storage Node (Data-only)	No	✓	✓
DC2-ADM1	Data Center 2	Admin Node	-	✓	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC2-S1	Data Center 2	Storage Node	Yes	✓	No, site Data Center 2 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.

3. 檢閱您要取消委任之每個節點的*可能取消委任*欄。

如果可以取消委任網格節點、則此欄會包含綠色核取記號、左欄則會包含核取方塊。如果節點無法停用、此欄會說明問題。如果節點無法停用的原因不止一個、則會顯示最重要的原因。

取消委任可能原因	說明	解決步驟
否、不支援 _ 節點類型 _ 停用。	您無法取消委任主要管理節點。	無。
否、至少有一個網格節點已中斷連線。 注意：此訊息僅針對連接的網格節點顯示。	如果任何網格節點中斷連線、則無法取消委任已連線的網格節點。 「健全狀況」欄包含下列其中一個已中斷連線的網格節點圖示： • （灰色）：管理性關閉 • （藍色）：未知	您必須將所有中斷連線的節點重新上線、或在移除已連線"取消委任所有中斷連線的節點"的節點之前。 • 注意 * ：如果您的網格包含多個中斷連線的節點、軟體會要求您同時將它們全部取消委任、這會增加產生非預期結果的可能性。

取消委任可能原因	說明	解決步驟
否、目前有一或多個必要節點已中斷連線、必須加以恢復。 注意：此訊息僅針對斷開連接的網格節點顯示。	如果一或多個必要節點也中斷連線（例如、 ADC 仲裁所需的儲存節點）、則無法取消委任中斷連線的網格節點。	a. 檢閱所有中斷連線節點的取消委任可能訊息。 b. 判斷哪些節點因為需要而無法停用。 ◦ 如果所需節點的健全狀況為管理性關機、請將節點重新連線。 ◦ 如果所需節點的健全狀況為「未知」、請執行節點還原程序來恢復所需節點。
否，HA 組的成員：組名稱。在停用此節點之前，您必須將其從所有 HA 群組中刪除。	如果節點介面屬於高可用度（ HA ）群組、則無法取消委任管理節點或閘道節點。	編輯HA群組以移除節點的介面、或移除整個HA群組。請參閱。 "設定高可用度群組"
不，網站 *x* 至少需要 3 個具備 ADC 服務的儲存節點，或有可用的非 ADC 節點可供移轉 ADC 服務。如果任何節點離線，則無法退役 ADC 節點。	僅限儲存節點（包括組合儲存節點或僅儲存元資料的儲存節點）。如果站台中剩餘節點不足以支援 ADC 仲裁要求，且 ADC 服務無法自動移動，則無法退役儲存節點。自動移動需要網格中有兩個以上的 ADC 儲存節點處於線上狀態，且同一站台上有可用的非 ADC 儲存節點。	確保符合自動 ADC 服務移動的條件（請參閱 "ADC 仲裁"），或 "手動移動 ADC 服務" 至同一站台上的另一個儲存節點。您也可以透過向站台新增新的儲存節點並指定其應具有 ADC 服務來執行擴充。請參閱 "將網格節點新增至 StorageGRID 的工作流程概述"。

取消委任可能原因	說明	解決步驟
否、一或多個銷毀編碼設定檔至少需要 *n* 個儲存節點。如果ILM規則未使用設定檔、您可以停用該設定檔。	僅限儲存節點。除非為現有的擦除編碼設定檔保留足夠的節點，否則您無法停用儲存節點。 例如、如果存在用於 4+2 銷毀編碼的銷毀編碼設定檔、則至少必須保留 6 個儲存節點。	針對每個受影響的抹除編碼設定檔、根據設定檔的使用方式、執行下列其中一個步驟： • * 用於主動 ILM 原則 * ：執行擴充。新增足夠的新儲存節點、以便繼續進行銷毀編碼。請參閱的說明"擴充您的網格"。 • * 用於 ILM 規則、但不在使用中的 ILM 原則 * ：編輯或刪除規則、然後停用銷毀編碼設定檔。 • * 未用於任何 ILM 規則 * ：停用銷毀編碼設定檔。 ◦ 附註： * 如果您嘗試停用銷毀編碼設定檔、且物件資料仍與設定檔相關聯、則會出現錯誤訊息。您可能需要等待數週、才能再次嘗試停用程序。 瞭解 "停用銷毀編碼設定檔"。
否、除非節點中斷連線、否則您無法取消委任歸檔節點。	如果保存節點仍在連線、則無法將其移除。	• 附註 * ：已移除對歸檔節點的支援。如果您需要取消委任歸檔節點、請參閱 "Grid 節點汰換（ StorageGRID 11.8 doc 網站）"

停用已中斷連線的 **StorageGRID** 節點

您可能需要取消委任目前未連線至網格的節點（健全狀況為未知或管理性關閉的節點）。

開始之前

- 您瞭解停用的考量事項及停用"儲存節點"的考量"管理和閘道節點"事項。
- 您已取得所有必要項目。
- 您已確保沒有任何資料修復工作處於作用中狀態。請參閱。 "檢查資料修復工作"
- 您已確認儲存節點還原在網格中的任何位置均未進行。如果是、您必須等到恢復完成時執行任何Cassandra重新建置。然後您可以繼續解除委任。
- 您已確保在節點取消委任程序執行期間不會執行其他維護程序、除非節點取消委任程序暫停。
- 您要取消委任的中斷節點的*可能取消委任*欄會包含綠色核取符號。
- 您有資源配置通關密碼。

關於這項工作

您可以透過在 **Health** 欄中尋找藍色的「未知」圖示 或灰色的「管理關閉」圖示 來識別斷開連線的節點。

在解除委任任何中斷連線的節點之前、請注意下列事項：

- 此程序主要用於移除單一中斷連線的節點。如果您的網格包含多個中斷連線的節點、則軟體會要求您同時取消委任所有節點、進而增加意外結果的可能性。

  如果您一次取消委任多個中斷連線的儲存節點、可能會導致資料遺失。請參閱。 "中斷連線儲存節點的考量事項"

  在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

- 如果無法移除中斷連線的節點（例如、 ADC 仲裁所需的儲存節點）、則無法移除其他中斷連線的節點。

步驟

1. 除非您正在解除委任歸檔節點（必須中斷連線）、否則請嘗試將任何中斷連線的網格節點恢復上線或恢復。

   如需相關指示、請參閱 "網格節點還原程序" 。

2. 如果您無法恢復已中斷連線的網格節點、而且想要在中斷連線時將其取消委任、請選取該節點的核取方塊。

   如果您的網格包含多個中斷連線的節點、則軟體會要求您同時取消委任所有節點、進而增加意外結果的可能性。

   選擇一次取消委任多個中斷連線的網格節點時、請務必小心、尤其是當您選擇多個中斷連線的儲存節點時。如果您有多個無法恢復的已中斷連線儲存節點、請聯絡技術支援部門、以決定最佳的行動方針。

3. 輸入資源配置通關密碼。

   「開始取消委任」按鈕已啟用。

4. 選擇 **Start decommission**。

   此時會出現一則警告、指出您已選取中斷連線的節點、而且如果節點只有物件複本、該物件資料將會遺失。

5. 查看節點列表，然後選擇 **OK**。

   退役程序開始，並顯示每個節點的進度。在此過程中，將產生一個包含電網配置變更的新復原包。

6. 新的恢復套件可用後，選擇連結或選擇 **Maintenance** > **System** > **Recovery package** 以存取恢復套件頁面。然後，下載 `.zip` 檔案。

   請參閱說明"下載恢復包"。

盡快下載恢復包，以確保在退役過程中出現問題時可以恢復電網。

復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

7. 定期監控「取消委任」頁面、確保所有選取的節點都能順利停用。

   儲存節點可能需要數天或數週的時間才能取消委任。當所有工作都完成時、會重新顯示節點選擇清單、並顯示成功訊息。如果您停用中斷連線的儲存節點、會出現一則資訊訊息、指出修復工作已啟動。

8. 當節點在取消委任程序中自動關機之後、請移除任何其他與停用節點相關的虛擬機器或其他資源。

   在節點自動關機之前、請勿執行此步驟。

9. 如果您要退役儲存節點，請監控在退役過程中自動啟動的*複製資料*和*糾刪碼 (EC) 資料*修理作業的狀態。

複寫資料

- 若要判斷維修是否完成：
  i. 選擇 節點 > 正在修復的儲存節點 > **ILM**。
  ii. 檢閱「評估」區段中的屬性。當修復完成時、「等待-全部」屬性會指出0個物件。
- 若要更詳細地監控維修：
  i. 選擇*節點*。
  ii. 選擇*網格名稱_*>* ILM *。
  iii. 將遊標放在 ILM 佇列圖上，查看 掃描速率（物件/秒） 屬性的值，該值是網格中物件被掃描並排隊等待 ILM 的速率。
  iv. 在 ILM 佇列部分中，查看以下屬性：
    - * 掃描週期 - 預估 * ：完成所有物件完整 ILM 掃描的預估時間。

      全面掃描並不能保證 ILM 已套用於所有物件。

    - 嘗試修復：針對被視為高風險的複製資料嘗試的物件修復操作的總數。高風險對像是任何僅剩一個副本的對象，無論是由 ILM 策略指定的還是由於副本遺失造成的。每次儲存節點嘗試修復高風險物件時，此計數都會增加。如果電網變得繁忙，則優先進行高風險的 ILM 修復。

      如果修復後複製失敗，則相同物件修復可能會再次增加。 + 當您監控儲存節點磁碟區復原的進度時，這些屬性非常有用。如果嘗試修復的次數停止增加並且完整掃描已完成，則修復可能已完成。

  v. 或者，提交 Prometheus 查詢 `storagegrid_ilm_scan_period_estimated_minutes` 和 `storagegrid_ilm_repairs_attempted`。

銷毀編碼（ **EC** ）資料

若要監控糾刪碼資料的修理並重試任何可能失敗的請求，請選擇 **Support** > **Tools** > **Metrics**，檢視目前作業的預計完成時間和完成百分比。然後，在 Grafana 部分選擇 **EC Overview**。查看 **Grid EC Job Estimated Time to Completion** 和 **Grid EC Job Percentage Completed** 儀表板。

完成後

一旦中斷連線的節點已停用、而且所有資料修復工作都已完成、您就可以視需要取消委任任何已連線的網格節點。

然後在完成取消委任程序後、完成下列步驟：

- 請確保已淘汰的網格節點磁碟機已清除。使用市售的資料抹除工具或服務、永久且安全地移除磁碟機中的資料。
- 如果您停用了某個應用裝置節點、但設備上的資料是使用節點加密來保護、請使用StorageGRID 此應用裝置安裝程式來清除金鑰管理伺服器組態（清除KMS）。如果您要將應用裝置新增至其他網格、則必須清除KMS組態。有關說明，請參閱 "在維護模式中監控節點加密"。

停用已連線的 StorageGRID 節點

您可以取消委任並永久移除連接至網格的節點。

開始之前

- 您瞭解停用的考量事項及停用"儲存節點"的考量"管理和閘道節點"事項。
- 您已收集所有必要資料。
- 您已確保沒有任何資料修復工作處於作用中狀態。
- 您已確認儲存節點還原在網格中的任何位置均未進行。如果是、請等到任何 Cassandra 重建作業完成後再執行恢復。然後您可以繼續解除委任。
- 您已確保在節點取消委任程序執行期間不會執行其他維護程序、除非節點取消委任程序暫停。
- 您有資源配置通關密碼。
- 網格節點已連線。
- 要取消委任的節點的 * 取消委任可能 * 欄包含綠色核取標記。

  如果一個或多個磁碟區離線（未掛載）、或是它們在線上（掛載）但處於錯誤狀態、則無法啟動解除委任。

  如果一個或多個磁碟區在取消委任期間離線、則在這些磁碟區重新上線後、取消委任程序就會完成。

- 所有網格節點均顯示正常（綠色）狀態。如果在 **Health** 欄中看到以下圖示之一，則必須嘗試解決問題：

圖示	色彩	嚴重性
	黃色	注意
	淡橘色	次要
	暗橘色	主要
	紅色	關鍵

- 如果您先前已停用中斷連線的儲存節點、則資料修復工作都已成功完成。請參閱。 "檢查資料修復工作"

  請勿移除網格節點的虛擬機器或其他資源、直到本程序指示您移除這些資源為止。

  在包含僅軟體中繼資料節點的網格中取消委任儲存節點時、請務必謹慎。如果您取消委任所有設定為儲存物件和中繼資料的節點、則儲存物件的能力會從網格中移除。如需僅中繼資料儲存節點的詳細資訊、請參閱"儲存節點類型"。

關於這項工作

當節點停用時、其服務會停用、節點會自動關機。

步驟

1. 從「取消委任節點」頁面、選取您要取消委任的每個網格節點的核取方塊。
2. 輸入資源配置通關密碼。

   「開始取消委任」按鈕已啟用。

3. 選取 * 開始取消委任 * 。
4. 檢閱確認對話方塊中的節點清單、然後選取 * 確定 * 。

   節點取消委任程序隨即開始、並顯示每個節點的進度。

   取消委任程序開始後、請勿將儲存節點離線。變更狀態可能會導致部分內容無法複製到其他位置。

5. 一旦新的恢復包可用，請選擇橫幅中的恢復包連結或選擇*維護*>*系統*>*恢復包*以訪問恢復包頁面。然後，下載 `.zip`文件。

   看"下載恢復包" 。

   盡快下載恢復包，以確保在退役過程中出現問題時可以恢復電網。

6. 定期監控「取消委任節點」頁面、確保所有選取的節點都能順利停用。

   儲存節點可能需要數天或數週的時間才能取消委任。

   當所有工作都完成時、會重新顯示節點選擇清單、並顯示成功訊息。

完成後

完成節點取消委任程序後、請完成下列步驟：

1. 請依照您的平台所需的適當步驟進行。例如：
   - **Linux**：您可能想要分離磁碟區並刪除在安裝期間建立的節點設定檔。看"在基於軟體的節點上安裝StorageGRID" 。
   - * VMware* ：您可能想使用 vCenter 的「從磁碟刪除」選項來刪除虛擬機器。您可能還需要刪除任何獨立於虛擬機器的資料磁碟。
   - * StorageGRID 《》應用裝置：應用裝置節點會自動恢復為未部署狀態、您可在此存取StorageGRID 《應用程式安裝程式》。您可以關閉產品電源、或將其新增至StorageGRID 其他的系統。
2. 請確保已淘汰的網格節點磁碟機已清除。使用市售的資料抹除工具或服務、永久且安全地移除磁碟機中的資料。
3. 如果您停用了某個應用裝置節點、但設備上的資料是使用節點加密來保護、請使用StorageGRID 此應用裝置安裝程式來清除金鑰管理伺服器組態（清除KMS）。如果您要將應用裝置新增至其他網格、則必須清除KMS組態。有關說明，請參閱 "在維護模式中監控節點加密"。

如果您需要執行第二個維護程序、可以在特定階段暫停儲存節點的取消委任程序。完成其他程序之後、您就可以繼續解除委任。

只有在達到ILM評估或銷毀編碼資料解除委任階段時、才會啟用*暫停*按鈕；不過、ILM評估（資料移轉）仍會在背景中繼續執行。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。

步驟

1. 選擇*維護* > 任務 > 退役。

   此時會出現「取消委任」頁面。

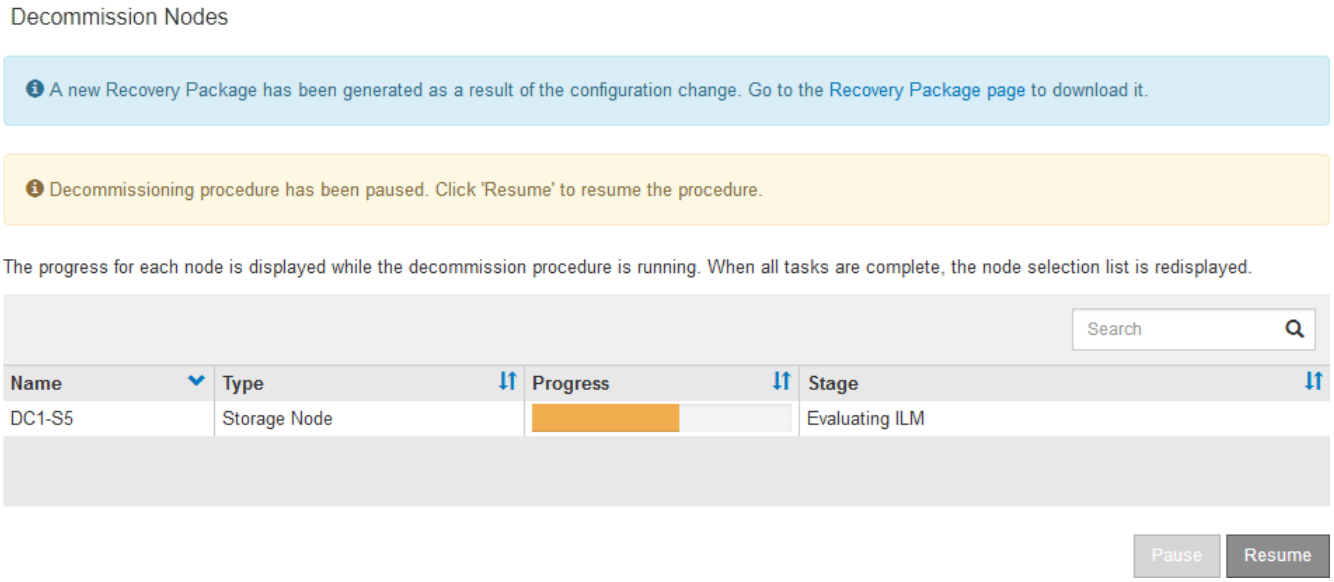
2. 選取*取消委任節點*。

   此時會出現「取消委任節點」頁面。當取消委任程序達到下列任一階段時、*暫停*按鈕就會啟用。

   - 評估ILM
   - 停用「刪除編碼資料」

3. 選取*暫停*以暫停程序。

   目前階段會暫停、並啟用*恢復*按鈕。



4. 完成其他維護程序之後、選取*恢復*以繼續取消委任。

取消委任網站

StorageGRID 中的站台停用考量

在使用站台取消委任程序移除站台之前、您必須先檢閱考量事項。

當您取消委任站台時會發生什麼事

當您取消對站台的委任時StorageGRID 、由站台上的所有節點和站台本身從StorageGRID 這個系統中永久移除。

當站台取消委任程序完成時：

- 您無法再使用StorageGRID 「畫面」來檢視或存取站台或站台上的任何節點。
- 您無法再使用任何參照到站台的儲存資源池或銷毀編碼設定檔。當 StorageGRID 取消委任站台時、它會自動移除這些儲存池、並停用這些銷毀編碼設定檔。

連線站台與中斷站台停用程序之間的差異

您可以使用站台取消委任程序來移除所有節點都連接StorageGRID 到該站台的站台（稱為「連線站台取消委任」）、或移除所有節點從StorageGRID 該站台中斷連線的站台（稱為「中斷連線的站台取消委任」）。開始之前、您必須先瞭解這些程序之間的差異。

如果一個站點包含已連接（）和已斷開連接的節點（或），則必須將所有離線節點重新上線。

- 連線站台取消委任可讓您從StorageGRID 作業系統中移除作業站台。例如、您可以執行連線站台取消委任、以移除功能正常但不再需要的站台。
- 當使用者移除連線的站台時、它會使用ILM來管理站台的物件資料。StorageGRID在開始連線站台取消委任之前、您必須先從所有ILM規則中移除站台、然後啟動新的ILM原則。ILM程序可同時移轉物件資料和移除站台的內部程序、但最佳做法是在開始實際的取消委任程序之前、先讓ILM步驟完成。
- 中斷連線的站台取消委任可讓您從StorageGRID 故障站台系統中移除故障站台。例如、您可以執行中斷連線的站台取消委任、以移除因火災或水災而毀損的站台。

  當用不到中斷連線的站台進行移除時、它會將所有節點視為不可恢復、而且不會嘗試保留資料。StorageGRID不過、在開始中斷連線的站台取消委任之前、您必須先從所有ILM規則中移除站台、然後啟動新的ILM原則。

在執行中斷連線的站台取消委任程序之前、您必須聯絡NetApp客戶代表。NetApp將在取消委任網站精靈中啟用所有步驟之前、先審查您的需求。如果您認為可以從站台恢復或從站台恢復物件資料、則不應嘗試中斷站台的停用。

移除已連線或已中斷連線站台的一般需求

在移除已連線或已中斷連線的站台之前、您必須瞭解下列需求：

- 您無法取消委任包含主要管理節點的網站。
- 如果任何節點都有屬於高可用度（ HA ）群組的介面、則無法取消委任站台。您必須編輯HA群組才能移除節點的介面、或移除整個HA群組。
- 如果站台包含已連線（）和已中斷連線（或）節點的混合情況，則無法將其取消委任。

- 如果任何其他站台上的任何節點已中斷連線（ 或 ），則無法取消委任站台。
- 如果正在進行 EC 節點修復作業、則無法啟動站台取消委任程序。請參閱"檢查資料修復工作"以追蹤銷毀編碼資料的修復。
- 當站台取消委任程序正在執行時：
  - 您無法建立 ILM 規則來參照要停用的網站。您也無法編輯現有的 ILM 規則來參照網站。
  - 您無法執行其他維護程序、例如擴充或升級。

    如果您需要在連線站台取消委任期間執行其他維護程序，您可以"在移除儲存節點時暫停程序"。只有在達到ILM評估或銷毀編碼資料解除委任階段時、才會啟用*暫停*按鈕；不過、ILM評估（資料移轉）仍會在背景中繼續執行。完成第二個維護程序之後、您就可以繼續解除委任。

  - 如果您在開始站台取消委任程序之後需要恢復任何節點、則必須聯絡支援部門。
- 您一次不能取消委任多個站台。
- 如果站台包含一或多個管理節點、且StorageGRID 您的系統已啟用單一登入（SSO）、則您必須從Active Directory Federation Services（AD FS）移除該站台的所有依賴方信任。

資訊生命週期管理（**ILM**）需求

在移除站台時、您必須更新ILM組態。取消委任網站精靈會引導您完成許多必要步驟、以確保達成下列目標：

- 任何 ILM 原則都不會參照此網站。如果是、您必須編輯原則、或使用新的 ILM 規則建立及啟動原則。
- 沒有 ILM 規則會參照網站、即使這些規則未用於任何原則。您必須刪除或編輯所有參照網站的規則。

當 StorageGRID 取消網站配置時、它會自動停用參照該網站的任何未使用的銷毀編碼設定檔、並自動刪除任何參照該網站的未使用儲存池。如果存在所有儲存節點儲存池（ StorageGRID 11.6 及更早版本）、則會移除該儲存池、因為它會使用所有站台。

您可能需要先建立新的ILM規則並啟動新的ILM原則、才能移除站台。這些指示假設您已充分瞭解 ILM 的運作方式、並且熟悉建立儲存資源池、銷毀編碼設定檔、 ILM 規則、以及模擬及啟動 ILM 原則。請參閱。 "使用ILM管理物件"

連接站台的物件資料考量

如果您要執行連線的站台取消委任、則必須在建立新的ILM規則和新的ILM原則時、決定該如何處理站台上的現有物件資料。您可以執行下列其中一項或兩項操作：

- 將物件資料從選取的站台移到網格中的一個或多個其他站台。

  *移動資料*範例：假設您想要取消委任羅利的站台、因為您在桑尼維爾新增了一個站台。在此範例中、您要將所有物件資料從舊站台移至新站台。在更新 ILM 規則和 ILM 原則之前、您必須檢閱兩個站台的容量。您必須確保Sunnyvale站台有足夠的容量來容納Raleigh站台的物件資料、而且Sunnyvale仍有足夠的容量可供未來成長使用。

  為了確保有足夠的容量可用、您可能需要"展開網格"在執行此程序之前、將儲存磁碟區或儲存節點新增至現有站台、或新增站台。

- 從選取的站台刪除物件複本。

  *刪除資料*範例：假設您目前使用3份ILM規則、在三個站台之間複寫物件資料。在解除委任站台之前、您可以建立對等的雙份複製ILM規則、以便只在兩個站台儲存資料。當您啟動使用雙份複本規則的新ILM原則時StorageGRID 、由於複本不再符合ILM需求、所以從第三個站台刪除複本。不過、物件資料仍會受到保護、其餘兩個站台的容量也會維持不變。

  > 切勿建立單一複本ILM規則來因應網站移除作業。ILM規則只會在任何時間段建立一個複寫複本、使資料有永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

連線站台取消委任的其他需求

在移除連線站台之前StorageGRID 、您必須先確認下列事項：

- StorageGRID 系統中的所有節點必須具有 **Connected** 連線狀態（）；但是，節點可以有活動警報。

  > 如果一個或多個節點中斷連線、您可以完成取消委任網站精靈的步驟1-4。不過、除非所有節點都已連線、否則您無法完成精靈的步驟 5 、以啟動取消委任程序。

- 如果您打算移除的站台包含用於負載平衡的閘道節點或管理節點、您可能需要"展開網格"在另一個站台新增對等的新節點。在開始站台取消委任程序之前、請確定用戶端可以連線至替換節點。
- 如果您要移除的站台包含高可用度（HA）群組中的任何閘道節點或管理節點、您可以完成「取消委任站台」精靈的步驟1-4。不過、您無法完成精靈的步驟 5 、這會啟動取消委任程序、直到您從所有 HA 群組中移除這些節點為止。如果現有用戶端連線至包含站台節點的HA群組、您必須確保StorageGRID 在站台移除後、它們仍可繼續連線至該站台。
- 如果用戶端直接連線至您打算移除的站台上的儲存節點、則必須先確認用戶端可連線至其他站台的儲存節點、然後再開始站台取消委任程序。
- 您必須在其餘站台上提供足夠的空間、以容納因任何主動 ILM 原則變更而將移動的任何物件資料。在某些情況下、您可能需要"展開網格"先新增儲存節點、儲存磁碟區或新站台、才能完成連線站台的取消委任。
- 您必須留出足夠的時間來完成取消委任程序。在停止使用站台之前、ILM程序可能需要數天、數週甚至數月的時間才能從站台移動或刪除物件資料。StorageGRID

  > 從站台移動或刪除物件資料可能需要數天、數週甚至數月的時間、視站台的資料量、系統負載、網路延遲及必要ILM變更的性質而定。

- 只要可能、您應該儘早完成「取消配置網站」精靈的步驟1-4。如果您允許在開始實際取消委任程序之前從站台移除資料（在精靈的步驟5中選取*啟動取消委任*）、則取消委任程序將會更快完成、並減少中斷和效能影響。

中斷站台停用的其他需求

在移除中斷連線的站台之前StorageGRID 、您必須先確認下列事項：

- 您已聯絡NetApp客戶代表。NetApp將在取消委任網站精靈中啟用所有步驟之前、先審查您的需求。

  > 如果您認為可以從站台恢復或從站台恢復任何物件資料、則不應嘗試中斷站台的停用。請參閱。 "技術支援如何恢復網站"

- 站台上的所有節點必須具有下列其中一種連線狀態：
  - 未知（）：由於未知原因，節點斷開連接或節點上的服務意外中斷。例如，節點上的某個服務可能已停止，或者節點可能因斷電或意外中斷而失去網路連線。
  - **Administratively Down**（）：節點因預期原因未連接到網格。例如，節點或節點上的服務已正常關閉。
- 所有其他站點的所有節點必須具有 已連接 的連接狀態（）；但是，這些其他節點可以有活動警報。
- 您必須瞭StorageGRID 解、您將不再能夠使用效益分析來檢視或擷取任何儲存在站台上的物件資料。執行此程序時、不會嘗試保留中斷連線站台的任何資料。StorageGRID

> 如果您的ILM規則和原則是設計用來防止單一站台遺失、則物件的複本仍會存在於其餘站台上。

- 您必須瞭解、如果網站包含唯一的物件複本、則物件會遺失且無法擷取。

移除網站時的一致性考量

S3 貯體的一致性決定 StorageGRID 是否在告知用戶端物件擷取成功之前、將物件中繼資料完全複寫至所有節點和站台。一致性可在物件的可用度與這些物件在不同儲存節點和站台之間的一致性之間取得平衡。

當執行此動作時、需要確保不會將任何資料寫入要移除的站台。StorageGRID因此、它會暫時覆寫每個貯體或容器的一致性。在您開始站台取消委任程序之後、StorageGRID 由於停止將物件中繼資料寫入要移除的站台、因此暫時性地使用強式站台一致性。

由於這項暫時性置換、請注意、如果其他站台有多個節點無法使用、站台取消委任期間發生的任何用戶端寫入、更新及刪除作業都可能失敗。

收集 **StorageGRID** 站台汰除所需的資料

在取消委任站台之前、您必須先取得下列資料。

項目	附註
恢復包 `.zip`文件	您必須下載最新的恢復包 `.zip`文件（`sgws-recovery-package-id-revision.zip`）。如果發生故障，您可以使用復原包檔案來復原系統。 "下載恢復包"
`Passwords.txt`檔案	該檔案包含在命令列上存取網格節點所需的密碼，並包含在復原套件中。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼不在 `Passwords.txt`檔案中。
汰換之前、請先說明StorageGRID 這個系統的拓撲	如有、請取得任何說明系統目前拓撲的文件。

相關資訊

"網頁瀏覽器需求"

在 **StorageGRID** 中選取要取消委任的站台

若要判斷某個網站是否可以停用、請從存取「取消委任網站」精靈開始。

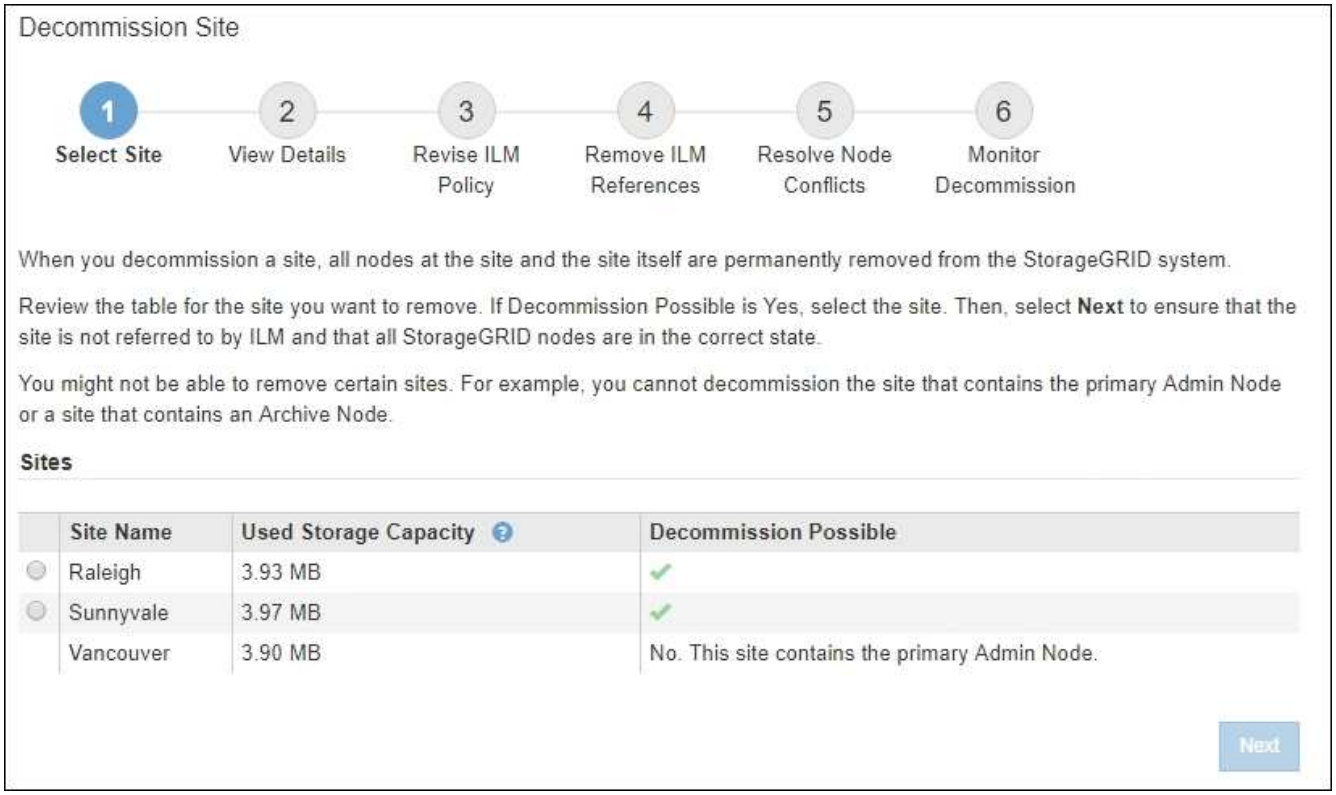
開始之前

- 您已取得所有必要資料。
- 您已檢閱移除網站的考量事項。
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"root 存取權限或維護與 ILM 權限"。

步驟

1. 選擇*維護* > 任務 > 退役。
2. 選取*取消委任站台*。

   此時會出現取消委任網站精靈的步驟1（選取網站）。此步驟包含StorageGRID 您的系統中站台的字母清單。



3. 檢視「已使用的儲存容量」欄中的值、以判斷每個站台目前使用多少儲存空間來處理物件資料。

   「已用儲存容量」是預估值。如果節點離線、「使用的儲存容量」是站台的最後已知值。

   - 對於連線的站台取消委任、此值表示在安全地取消委任此站台之前、需要將多少物件資料移至其他站台或由ILM刪除。
   - 對於中斷連線的站台取消委任、此值代表當您取消委任此站台時、系統的資料儲存空間將無法存取多

少。

如果您的ILM原則是設計用來防止單一站台遺失、則物件資料的複本仍應存在於其餘站台上。

4. 請檢閱「取消委任可能」欄中的理由、以判斷目前哪些站台可以停用。

如果網站無法停用的原因不止一個、則會顯示最重要的原因。

取消委任可能原因	說明	下一步
綠色對勾（）	您可以取消委任此站台。	前往 下一步。
否。此網站包含主要管理節點。	您無法取消委任包含主要管理節點的站台。	無。您無法執行此程序。
否。此網站包含一或多個歸檔節點。	您無法取消委任包含歸檔節點的站台。	無。您無法執行此程序。
否。此站台的所有節點都會中斷連線。請聯絡您的NetApp客戶代表。	除非站點中的每個節點都已連接，否則無法執行已連接站點的停用操作（）。	如果您想要執行中斷連線的站台取消委任、您必須聯絡NetApp客戶代表、由他檢閱您的需求、並啟用「取消委任站台」精靈的其餘部分。 重要：請勿讓線上節點離線、以便移除站台。您將遺失資料。

此範例展示了一個包含三個站點的 StorageGRID 系統。Raleigh 和 Sunnyvale 站點的綠色核取記號（）表示您可以取消委任這些站點。但是，您無法取消委任 Vancouver 站點，因為它包含主要管理節點。

1. 如果可以取消委任、請選取站台的選項按鈕。

*下一步*按鈕已啟用。

2. 選擇*下一步*。

步驟2（檢視詳細資料）隨即出現。

在 **StorageGRID** 中取消委任之前、請先檢閱站台詳細資料

從「取消委任網站」精靈的步驟2（檢視詳細資料）、您可以檢閱網站中包含哪些節點、查看每個儲存節點上已使用多少空間、以及評估網格中其他站台可用的空間。

開始之前

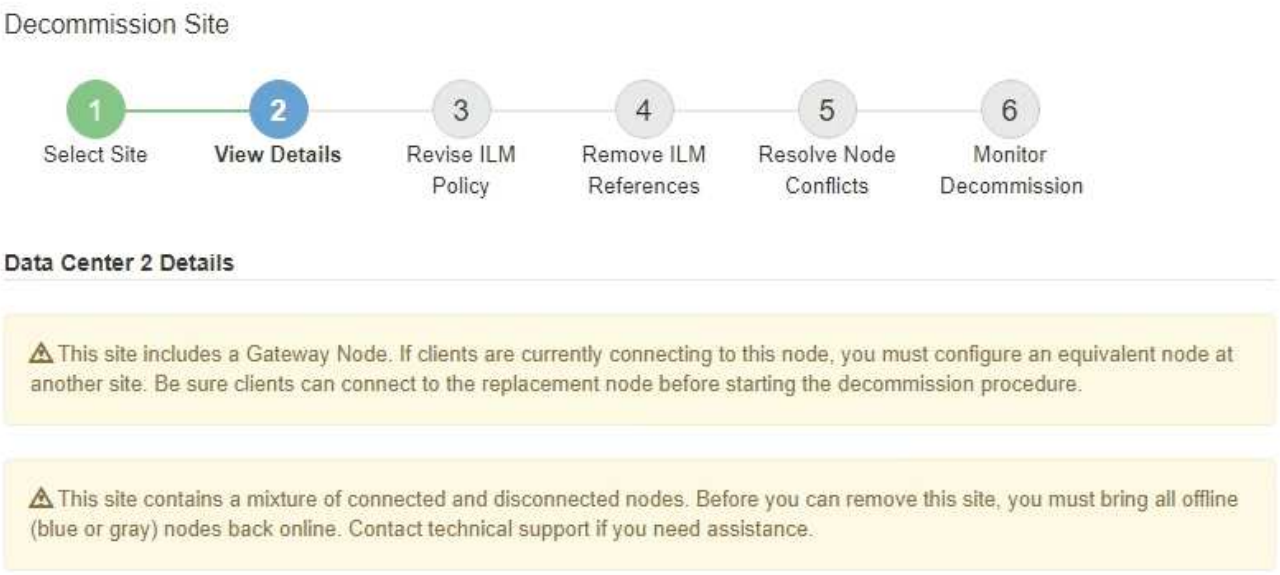
在解除委任站台之前、您必須先檢閱站台上存在多少物件資料。

- 如果您要執行連線站台取消委任、則必須先瞭解站台目前有多少物件資料存在、然後再更新ILM。根據站台容量和資料保護需求、您可以建立新的ILM規則、將資料移至其他站台、或從站台刪除物件資料。
- 如果可能、請先執行任何必要的儲存節點擴充、再開始取消委任程序。
- 如果您執行中斷連線的站台取消委任、則必須瞭解當您移除站台時、會永遠無法存取多少物件資料。

> 如果您正在執行中斷連線的站台解除委任、 ILM 將無法移動或刪除物件資料。保留在站台上的任何資料都會遺失。不過、如果您的ILM原則是設計來防止單一站台遺失、則物件資料的複本仍會存在於其餘站台上。請參閱。 "啟用站台遺失保護"

步驟

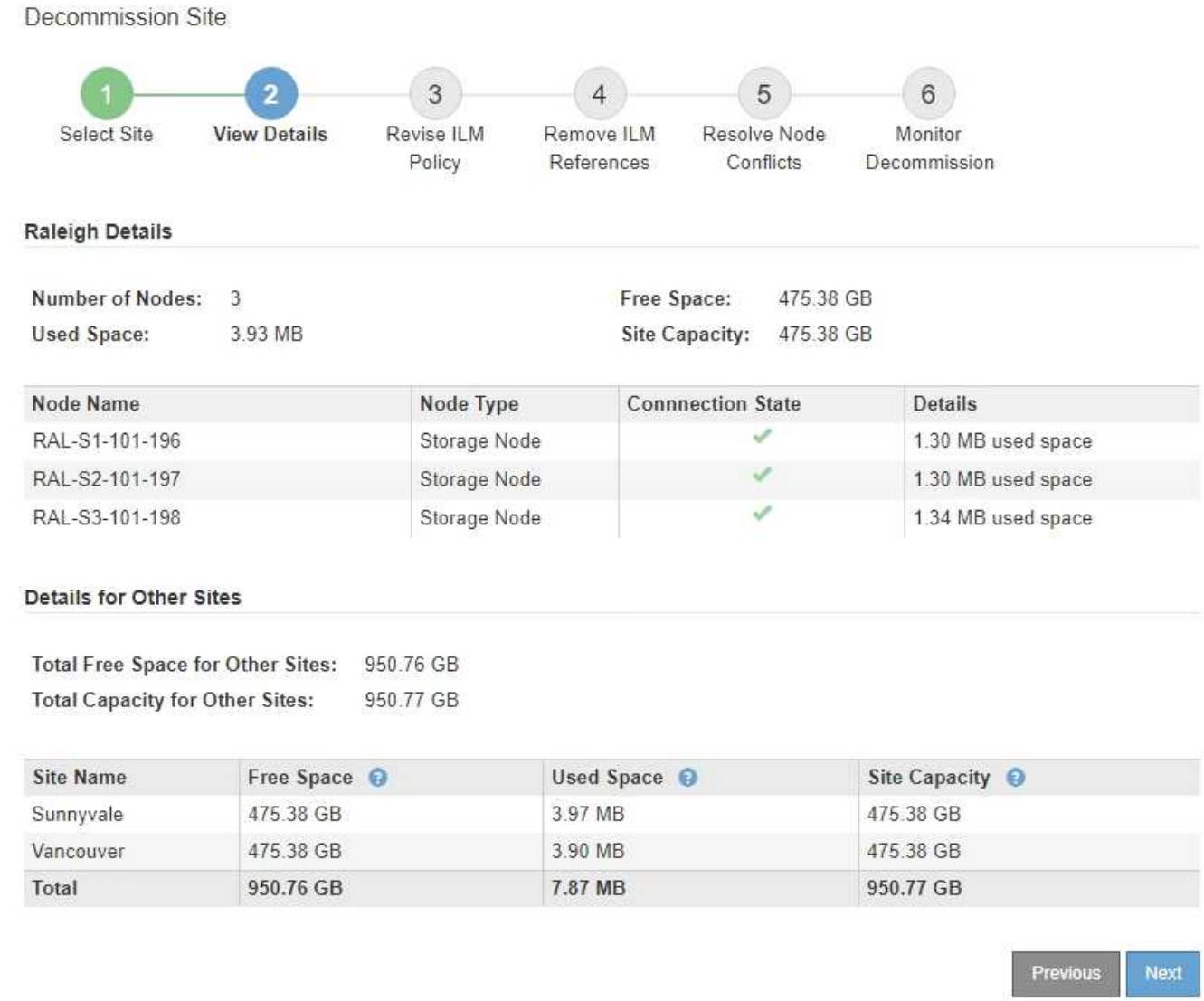
1. 在步驟2（檢視詳細資料）中、檢閱與您選取要移除之站台相關的任何警告。



在下列情況下會出現警告：

- 站台包括閘道節點。如果 S3 用戶端目前正在連線至此節點、您必須在另一個站台上設定對等節點。在繼續取消委任程序之前、請確定用戶端可以連線至更換節點。
- 該站點包含已連接（）和已斷開連接的節點（或）。在移除此站點之前，您必須先將所有離線節點重新上線。

2. 檢閱您選取要移除之網站的詳細資料。



所選網站包含下列資訊：

- 節點數
- 站台中所有儲存節點的已用空間、可用空間和容量總計。
  - 對於連線站台取消委任、*已用空間*值表示必須將多少物件資料移至其他站台、或是使用ILM刪除。
  - 對於中斷連線的站台取消委任、*已用空間*值會指出當您移除站台時、將無法存取多少物件資料。
- 節點名稱、類型和連線狀態：
  - （已連接）
  - （管理性關閉）
  - （未知）
- 每個節點的詳細資料：
  - 對於每個儲存節點、已用於物件資料的空間量。
  - 對於管理節點和閘道節點、該節點目前是否用於高可用度（HA）群組。您無法取消委任 HA 群組中

使用的管理節點或閘道節點。在您開始解除委任之前、請先編輯 HA 群組、以移除站台上的所有節點、如果 HA 群組只包含此站台的節點、請將其移除。有關說明，請參閱"管理高可用度（ HA ）群組"。

3. 在頁面的「其他站台的詳細資料」區段中、評估網格中其他站台的可用空間。

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

如果您正在執行連線站台取消委任、且計畫使用ILM從所選站台移除物件資料（而非僅刪除）、則必須確保其他站台有足夠的容量來容納已移動的資料、並確保仍有足夠的容量可供未來成長使用。

如果您要移除之站台的*已用空間*大於*其他站台的可用空間總計*、就會出現警告。為了確保在移除站台後仍有足夠的可用儲存容量、您可能需要先執行擴充、才能執行此程序。

4. 選擇*下一步*。

此時會出現步驟3（修訂ILM原則）。

修訂 **StorageGRID** 中站台停用的 **ILM** 原則

從「取消委任網站」精靈的步驟 3 （修訂 ILM 原則）開始、您可以判斷該網站是否由任何 ILM 原則參照。

開始之前

您對如何操作有很好的瞭解"使用 ILM 管理物件"。您熟悉建立儲存資源池和 ILM 規則、以及模擬和啟動 ILM 原則。

關於這項工作

如果任何原則（作用中或非作用中）中有任何 ILM 規則參照該站台、 StorageGRID 就無法取消委任該站台。

如果任何 ILM 原則參照您要取消委任的網站、您必須移除或編輯這些原則、使其符合下列要求：

- 完全保護所有物件資料。
- 請勿參閱您即將停用的網站。
- 請勿使用參照網站的儲存資源池、或使用「所有網站」選項。
- 請勿使用參照網站的銷毀編碼設定檔。
- 請勿使用 StorageGRID 11.6 或更早版本安裝的「複製 2 份複本」規則。

切勿建立單一複本ILM規則來因應網站移除作業。ILM規則只會在任何時間段建立一個複寫複本、使資料有永久遺失的風險。如果只有一個物件複寫複本存在、則當儲存節點故障或發生重大錯誤時、該物件就會遺失。在升級等維護程序期間、您也會暫時失去物件的存取權。

如果您正在執行 _Connected 站台取消委任 _ 、則必須考慮 StorageGRID 應如何管理您要移除之站台上目前的物件資料。根據您的資料保護需求、新規則可以將現有的物件資料移至不同的站台、也可以刪除不再需要的任何額外物件複本。

如果您需要協助設計新原則、請聯絡技術支援部門。

步驟

1. 從步驟 3 （修訂 ILM 原則）中、判斷是否有任何 ILM 原則參照到您選取要取消委任的站台。
2. 如果未列出策略，請選擇 **Next** 轉至"步驟4：移除ILM參考"。
3. 如果列出一或多個 *activity* ILM 原則、請複製每個現有原則、或建立不參照所停用站台的新原則：

   a. 在「原則名稱」欄中選取原則的連結。

      原則的 ILM 原則詳細資料頁面會顯示在新的瀏覽器索引標籤中。「取消委任網站」頁面仍會在「其他」索引標籤上保持開啟狀態。

   b. 視需要遵循以下準則和指示：

      - 使用 ILM 規則：
        - "建立一個或多個儲存資源池"這並不代表網站。
        - "編輯或取代規則"這是指網站。

          請勿選取 * 製作 2 份複本 * 規則、因為該規則使用 * 所有儲存節點 * 儲存池、這是不允許的。

      - 使用 ILM 原則：
        - "複製現有的 ILM 原則" 或 "建立新的 ILM 原則"。
        - 確保預設規則和其他規則不會參照網站。

          您必須確認ILM規則的順序正確。當原則啟動時、新物件和現有物件會依照列出的順序進行評估、從上方開始。

   c. 擷取測試物件並模擬原則、以確保套用正確的規則。

      ILM原則中的錯誤可能導致無法恢復的資料遺失。在啟動原則之前、請仔細檢閱並模擬原則、以確認其運作正常。

      當您啟動新的ILM原則時StorageGRID 、利用它來管理所有物件、包括現有物件和新擷取的物件。在啟動新的ILM原則之前、請先檢閱現有複寫和銷毀編碼物件放置位置的任何變更。變更現有物件的位置、可能會在評估和實作新放置位置時、導致暫時性資源問題。

   d. 啟動新原則、並確保舊原則現在處於非作用中狀態。

如果您想要啟動多個原則，"請依照步驟建立 ILM 原則標籤"。

如果您正在執行連線站台取消委任、StorageGRID 則只要啟動新的ILM原則、即可立即從所選站台移除物件資料。移動或刪除所有物件複本可能需要數週的時間。雖然您可以在站台上仍存在物件資料的情況下安全地啟動站台取消委任、但如果您允許在開始實際取消委任程序之前、從站台移除資料、則取消委任程序將會更快完成、並減少中斷和效能影響 （在精靈的步驟5中選取*開始取消委任*）。

4. 針對每個 _inactive 原則、請先選取前述步驟所述的每個原則連結、以進行編輯或移除。
   - "編輯原則"因此它並不代表要停用的網站。
   - "移除原則"。
5. 當您完成 ILM 規則和原則的變更時、步驟 3 （修訂 ILM 原則）中不應再列出原則。選擇*下一步*。

   此時會出現步驟4（移除ILM參考）。

移除 **StorageGRID** 中對站台的 **ILM** 參照

從「取消委任網站」精靈的步驟 4 （移除 ILM 參考）中、您必須刪除或編輯任何未使用的 ILM 規則、以參照該網站、即使這些規則未用於任何 ILM 原則。

步驟

1. 判斷是否有任何未使用的ILM規則是指該站台。

   如果列出任何 ILM 規則、這些規則仍會參照網站、但不會用於任何原則。

   > 當 StorageGRID 取消網站配置時、它會自動停用參照該網站的任何未使用的銷毀編碼設定檔、並自動刪除任何參照該網站的未使用儲存池。所有儲存節點儲存池（ StorageGRID 11.6 及更早版本）都會移除、因為它使用「 All Sites 」（所有站台）站台。

2. 編輯或刪除每個未使用的規則：
   - 若要編輯規則、請前往 ILM 規則頁面、並更新所有使用抹除編碼設定檔或參照網站的儲存池的放置位置。然後返回*步驟4（移除ILM參考）*。
   - 若要刪除規則，請選擇垃圾桶圖示 並選擇 **OK**。

     > 您必須先刪除 *Make 2 Copies （製作 2 份複本） * 規則、才能取消委任網站。

3. 確認沒有未使用的 ILM 規則會參照網站、且「 * 下一步 * 」按鈕已啟用。
4. 選擇*下一步*。

   > 移除站台時、任何其他參照站台的儲存資源池和銷毀編碼設定檔都將會失效。當 StorageGRID 取消網站配置時、它會自動停用參照該網站的任何未使用的銷毀編碼設定檔、並自動刪除任何參照該網站的未使用儲存池。所有儲存節點儲存池（ StorageGRID 11.6 及更早版本）都會移除、因為它使用「 All Sites 」（所有站台）站台。

   此時會出現步驟5（解決節點衝突）。

從「取消委任網站」精靈的步驟5（解決節點衝突）、您可以判斷StorageGRID 您的系統中是否有任何節點中斷連線、或所選網站上的任何節點是否屬於高可用度（HA）群組。解決任何節點衝突之後、請從本頁開始取消委任程序。

開始之前

您必須確保StorageGRID 您的整個作業系統中的所有節點都處於正確狀態、如下所示：

- StorageGRID 系統中的所有節點都必須連接（）。

  如果您執行中斷連線的站台取消委任、則您要移除站台的所有節點都必須中斷連線、而且所有其他站台的所有節點都必須連線。

  如果一個或多個磁碟區離線（未掛載）、或是它們在線上（掛載）但處於錯誤狀態、則無法啟動解除委任。

  如果一個或多個磁碟區在取消委任期間離線、則在這些磁碟區重新上線後、取消委任程序就會完成。

- 您要移除之站台的任何節點都無法擁有屬於高可用度（HA）群組的介面。

關於這項工作

如果在步驟5（解決節點衝突）中列出任何節點、您必須先修正問題、才能開始取消委任。

從本頁開始站台取消委任程序之前、請先檢閱下列考量事項：

- 您必須留出足夠的時間來完成取消委任程序。

  從站台移動或刪除物件資料可能需要數天、數週甚至數月的時間、視站台的資料量、系統負載、網路延遲及必要ILM變更的性質而定。

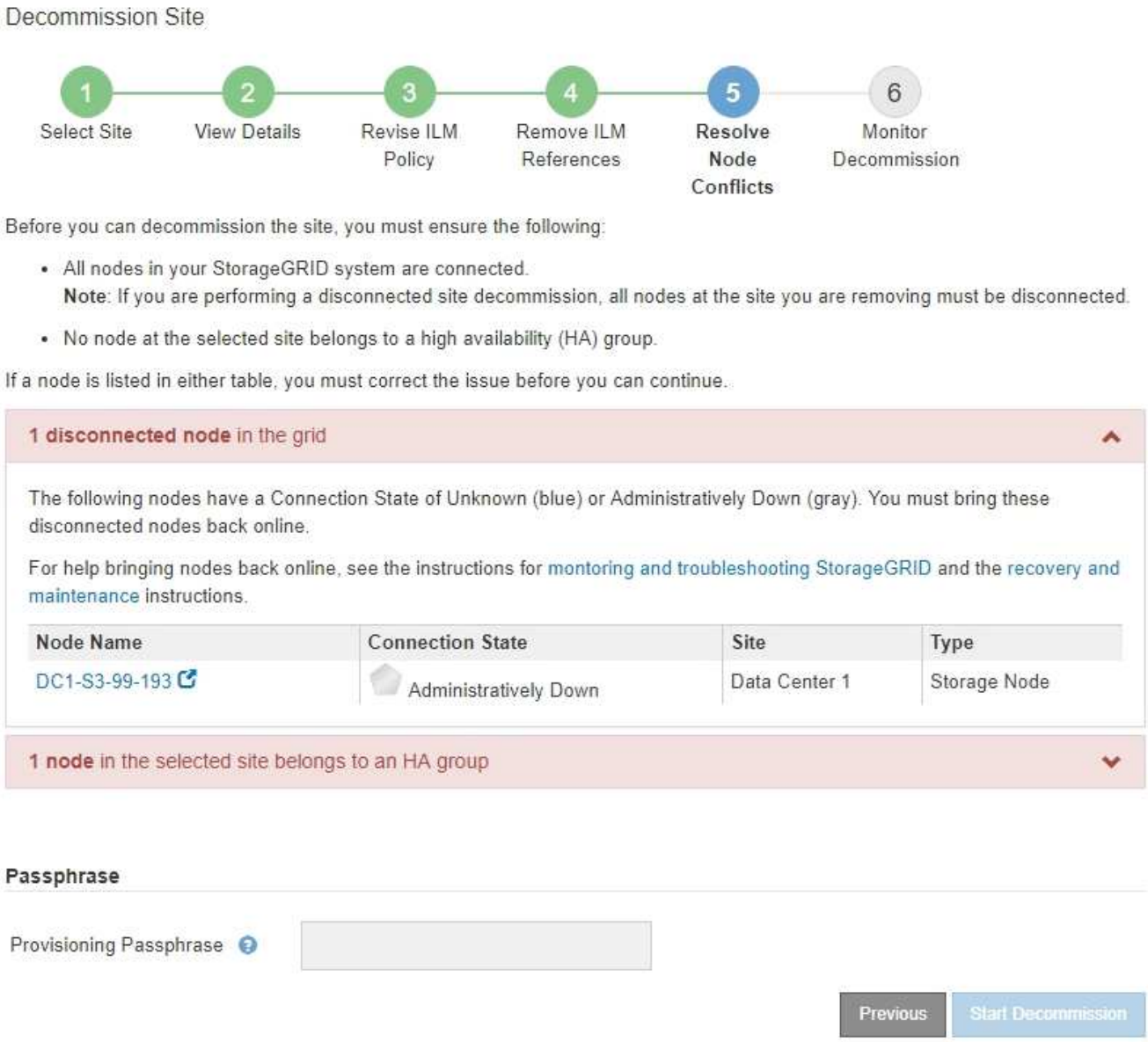
- 當站台取消委任程序正在執行時：
  - 您無法建立 ILM 規則來參照要停用的網站。您也無法編輯現有的 ILM 規則來參照網站。
  - 您無法執行其他維護程序、例如擴充或升級。

    如果您需要在連線站台取消委任期間執行其他維護程序、可以在移除儲存節點時暫停該程序。在「取消壓縮複製和刪除編碼資料」階段、 * 暫停 * 按鈕會啟用。

  - 如果您在開始站台取消委任程序之後需要恢復任何節點、則必須聯絡支援部門。

步驟

1. 檢視步驟 5（解決節點衝突）中斷開連接的節點部分，以確認 StorageGRID 系統中是否有任何節點的連線狀態為未知（）或管理關閉（）。

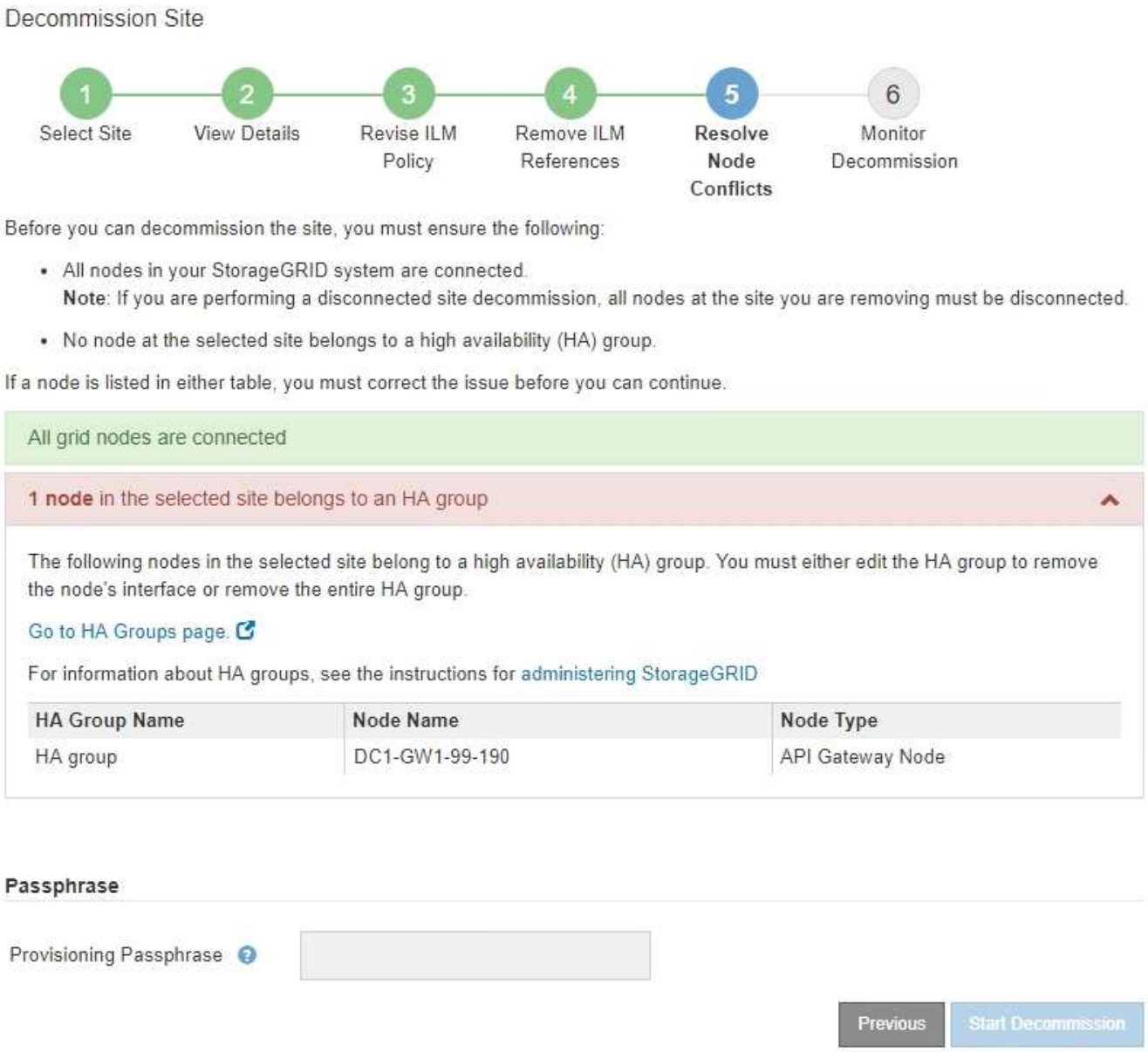


2. 如果有任何節點中斷連線、請將其重新連線。

   請參閱"節點程序"。如需協助、請聯絡技術支援。

3. 當所有已中斷連線的節點恢復上線時、請檢閱步驟5（解決節點衝突）的「HA Groups（HA群組）」區段。

   此表列出所選站台中屬於高可用度（HA）群組的任何節點。



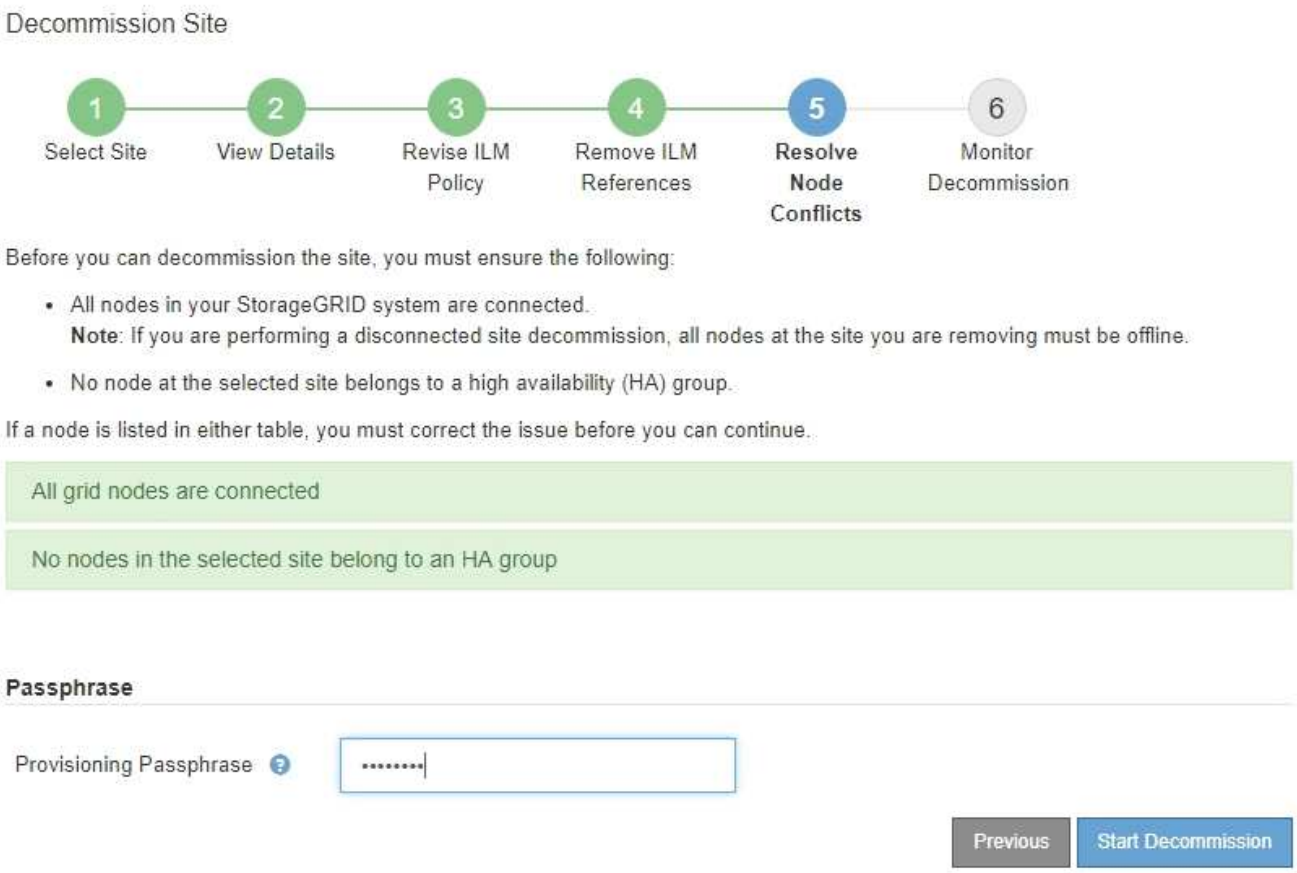
4. 如果列出任何節點、請執行下列其中一項：

   - 編輯每個受影響的HA群組以移除節點介面。
   - 移除此站台僅包含節點的HA群組。請參閱「管理StorageGRID 功能」的說明。

   如果所有節點都已連線，且所選站台中沒有節點用於 HA 群組，則會啟用 **Provisioning passphrase** 欄位。

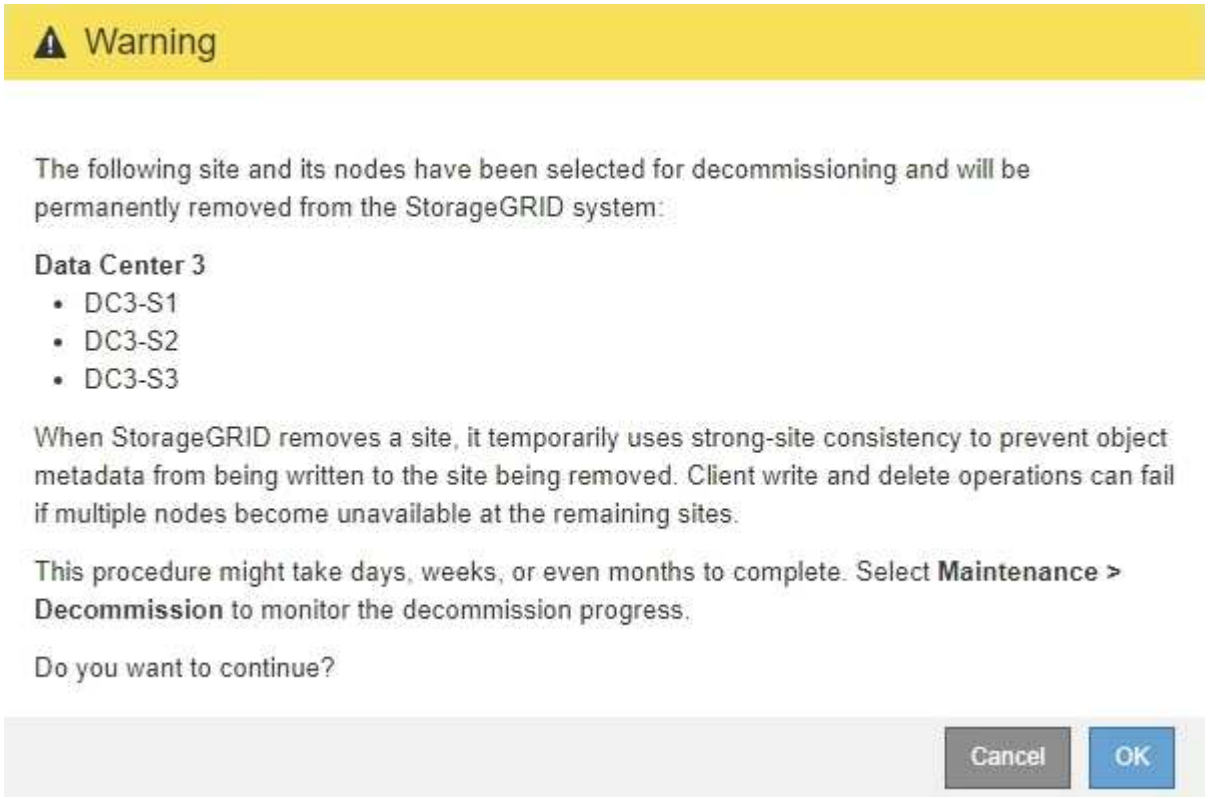
5. 輸入資源配置通關密碼。

   「開始取消配置」按鈕隨即啟用。



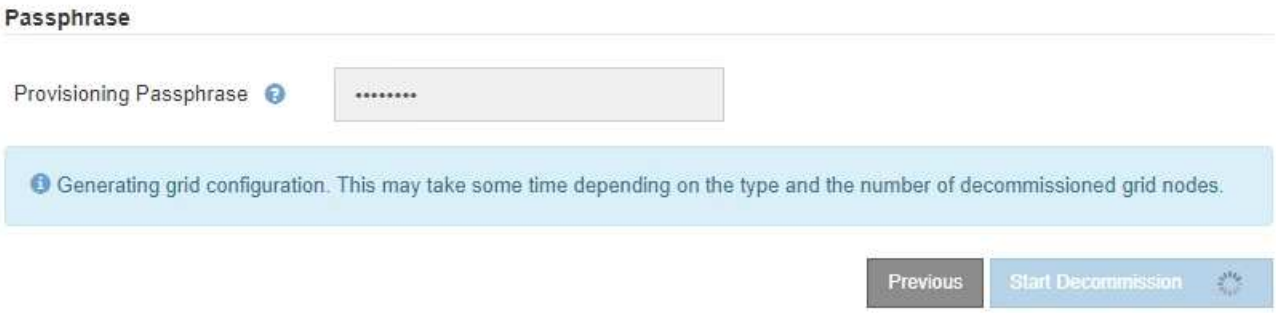
6. 如果您準備好開始站台取消委任程序、請選取*開始取消委任*。

警告會列出要移除的站台和節點。我們提醒您、完全移除網站可能需要數天、數週甚至數月的時間。



7. 檢閱警告。如果您準備好開始、請選取*確定*。

   產生新的網格組態時、會出現一則訊息。視停用的網格節點類型和數量而定、此程序可能需要一些時間。



   當產生新的網格組態時、會出現步驟6（監控取消配置）。

   在取消委任完成之前、*上一個*按鈕會保持停用狀態。

在 **StorageGRID** 中監控站台取消委任進度

從取消配置網站頁面精靈的步驟6（監控取消配置）、您可以在移除網站時監控進度。

關於這項工作

當執行此動作時、若從連線的站台移除節點、則會依照下列順序移除節點：StorageGRID

1. 閘道節點
2. 管理節點
3. 儲存節點

當用這個順序移除中斷連線的站台時、它會移除節點：StorageGRID

1. 閘道節點
2. 儲存節點
3. 管理節點

每個閘道節點或管理節點可能只需要幾分鐘或一小時即可移除、不過儲存節點可能需要數天或數週的時間。

步驟

1. 一旦產生新的恢復包，請下載該檔案。

盡快下載恢復包，以確保在退役過程中出現問題時可以恢復電網。

a. 選擇訊息中的鏈接，或選擇*維護* > 系統 > 恢復包。

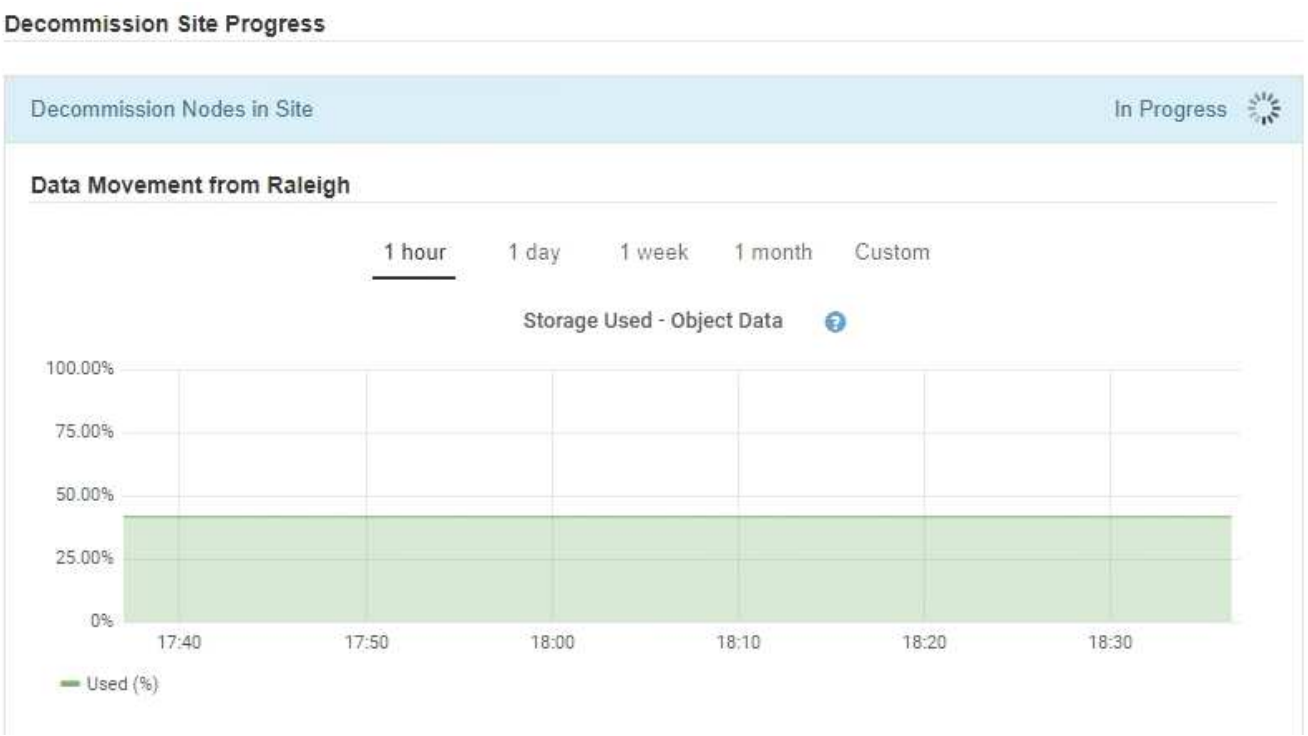
b. 下載 `.zip`檔案。

請參閱說明"下載恢復包"。

復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

2. 使用「資料移動」圖表、監控物件資料從此站台移至其他站台的移動。

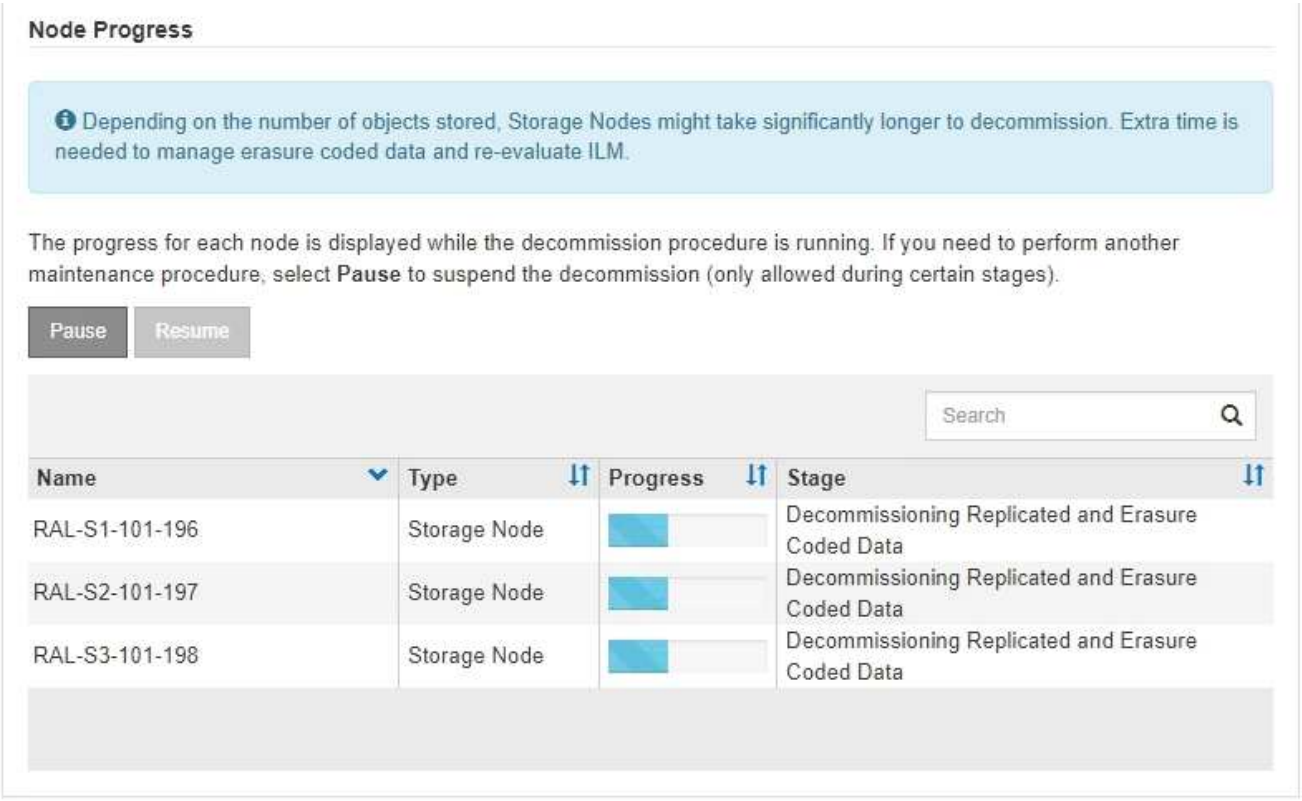
當您在步驟3中啟動新的ILM原則（修訂ILM原則）時、資料便會開始移動。資料會在整個取消委任程序期間移動。



3. 在頁面的「節點進度」區段中、監控節點移除時取消委任程序的進度。

移除儲存節點時、每個節點都會經歷一系列階段。雖然這些階段大多發生得很快、甚至難以察覺、但您可能

需要等待數天甚至數週、才能完成其他階段、視需要移動多少資料而定。需要更多時間來管理銷毀編碼資料並重新評估ILM。



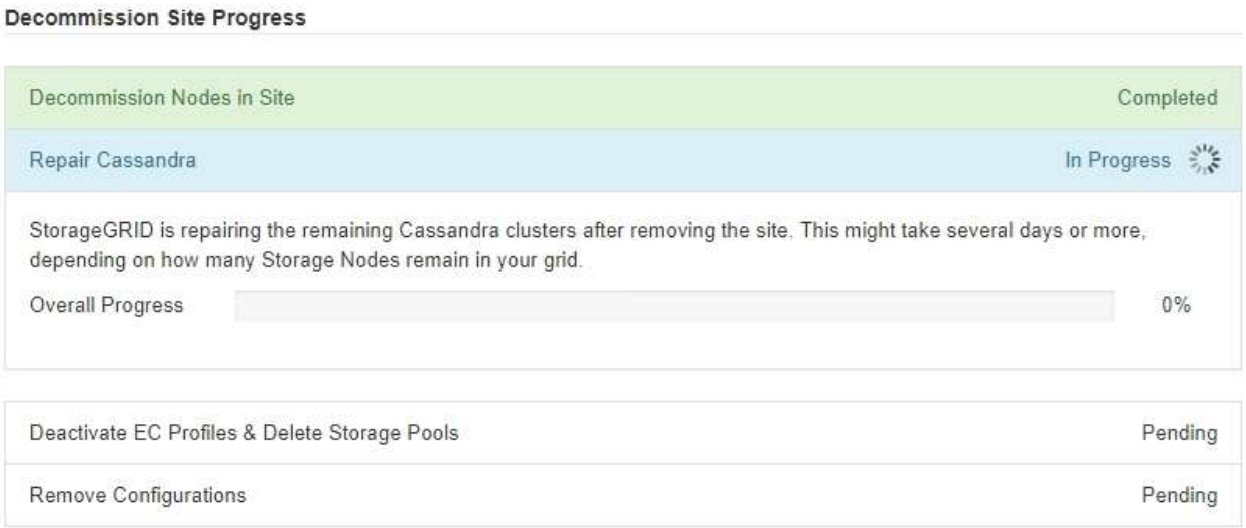
如果您正在監控連線站台取消委任的進度、請參閱下表以瞭解儲存節點的取消委任階段：

階段	預估持續時間
擱置中	分鐘或更短
等待鎖定	分鐘
準備工作	分鐘或更短
將LDR標記為已停用	分鐘
解除委任複寫和刪除編碼資料	小時、天或週、視資料量而定 附註：如果您需要執行其他維護活動、您可以在此階段暫停站台停用。
LMR設定狀態	分鐘
清除稽核佇列	根據訊息數量和網路延遲、從數分鐘到數小時。
完成	分鐘

如果您正在監控中斷站台取消委任的進度、請參閱下表以瞭解儲存節點的取消委任階段：

階段	預估持續時間
擱置中	分鐘或更短
等待鎖定	分鐘
準備工作	分鐘或更短
停用外部服務	分鐘
憑證撤銷	分鐘
節點取消登錄	分鐘
儲存分級取消註冊	分鐘
移除儲存群組	分鐘
實體移除	分鐘
完成	分鐘

4. 當所有節點都達到完整階段之後、請等待其餘站台取消委任作業完成。
   - 在*修復Cassandra *步驟中、StorageGRID 針對保留在網格中的Cassandra叢集進行必要的修復。視網格中剩餘的儲存節點數量而定、這些修復可能需要數天或更久的時間。



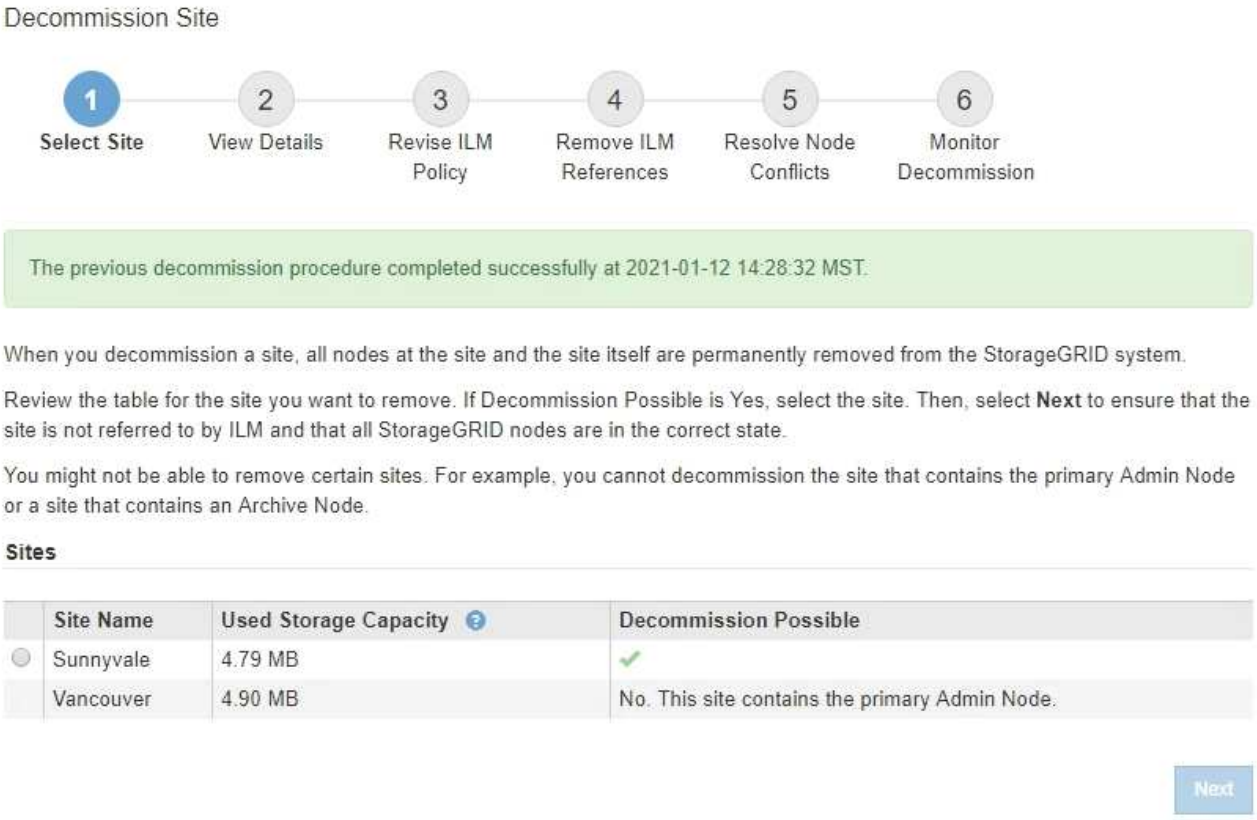
   - 在「停用**EC**設定檔與刪除儲存資源池」步驟中、會進行下列ILM變更：
     - 任何轉介至站台的銷毀編碼設定檔都會停用。

- 任何參照站台的儲存資源池都會刪除。

> 所有儲存節點儲存池（ StorageGRID 11.6 及更早版本）也會移除、因為它使用「 All Sites 」（所有站台）站台。

。最後、在「移除組態」步驟中、任何對站台及其節點的剩餘參照都會從網格的其餘部分移除。

5. 當取消委任程序完成時、取消委任網站頁面會顯示成功訊息、且移除的網站將不再顯示。



完成後

完成站台取消委任程序後、請完成下列工作：

- 確保已淘汰站台中所有儲存節點的磁碟機都已清除。使用市售的資料抹除工具或服務、永久且安全地移除磁碟機中的資料。
- 如果站台包含一或多個管理節點、且您StorageGRID 的作業系統已啟用單一登入（SSO）、請從Active Directory Federation Services（AD FS）移除該站台的所有依賴方信任。
- 在連接站台取消委任程序中自動關閉節點之後、請移除相關的虛擬機器。

重新命名網格、站台或節點

使用 **StorageGRID** 重新命名程序

您可以視需要變更整個網格管理程式、每個網站及每個節點的顯示名稱。您可以在需要時安全地更新顯示名稱。

什麼是重新命名程序？

一開始安裝 StorageGRID 時、您會為網格、每個站台及每個節點指定一個名稱。這些初始名稱稱為 _ 系統名稱 _、這些名稱最初會顯示在整個 StorageGRID 中。

內部 StorageGRID 作業需要系統名稱、因此無法變更。不過、您可以使用重新命名程序、為網格、每個站台及每個節點定義新的 _ 顯示名稱 _。這些顯示名稱會出現在不同的 StorageGRID 位置、而非（或在某些情況下、除了）基礎系統名稱。

使用重新命名程序來修正打字錯誤、實作不同的命名慣例、或表示站台及其所有節點已重新定位。與系統名稱不同、顯示名稱可在必要時更新、而不會影響 StorageGRID 作業。

系統名稱和顯示名稱出現在何處？

下表摘要說明系統名稱和顯示名稱在 StorageGRID 使用者介面和 StorageGRID 檔案中的顯示位置。

位置	系統名稱	顯示名稱
Grid Manager 頁面	除非項目已重新命名、否則會顯示	如果項目已重新命名、則會在下列位置顯示、而非顯示系統名稱： • 儀表板 • 節點頁面 • 高可用度群組、負載平衡器端點、 VLAN 介面、金鑰管理伺服器、網格密碼、 和防火牆控制 • 警示 • 儲存資源池定義 • 物件中繼資料查詢頁面 • 與維護程序相關的頁面、包括升級、 Hotfix 、 SANtricity OS 升級、取消委任、 擴充、恢復和物件存在檢查 • 支援頁面（記錄和診斷） • 單一登入頁面、位於管理節點詳細資料表格中的管理節點主機名稱旁
節點 > 節點的 概覽選項卡	永遠顯示	只有在項目重新命名時才會顯示
• 節點健全狀況 * API	一律歸還	只有在項目重新命名時才傳回

使用 SSH 存取節點時提示	除非項目已重新命名、否則會顯示為主要名稱：
	`admin@SYSTEM-NAME: ~ $`
	項目重新命名時會包含在括弧中：
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		項目重新命名時顯示為主要名稱：
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt`復原包中的文件	顯示為 `Server Name`	顯示為 `Display Name`

位置	系統名稱	顯示名稱
`/etc/hosts`所有節點上的檔案 例如： `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	一律顯示在第二欄中	項目重新命名時、會顯示在第四欄
`topology-display-names.json`，包含在 AutoSupport 資料中	不含	除非項目已重新命名、否則為空白；否則、會將網格、站台和節點 ID 對應至其顯示名稱。

顯示名稱需求

使用此程序之前、請先檢閱顯示名稱的需求。

節點的顯示名稱

節點的顯示名稱必須遵循下列規則：

- 在 StorageGRID 系統中必須是唯一的。
- 不得與 StorageGRID 系統中任何其他項目的系統名稱相同。
- 必須包含至少 1 個字元、不得超過 32 個字元。
- 可以包含數字、連字號（ - ）、大寫和小寫字母。
- 可以以字母或數字開頭或結尾、但不能以連字號開頭或結尾。
- 不能全部都是數字。
- 不區分大小寫。例如 `DC1-ADM`、和 `dc1-adm`被視為重複項目。

您可以使用先前由不同節點使用的顯示名稱來重新命名節點、只要重新命名不會產生重複的顯示名稱或系統名稱即可。

顯示網格和網站的名稱

網格和網站的顯示名稱遵循相同的規則、但這些例外情況除外：

- 可以包含空格。

- 可以包含以下特殊字元： = - _ : , . @ !
- 可以以特殊字元開始和結束、包括連字號。
- 可以是所有數字或特殊字元。

顯示名稱最佳實務做法

如果您打算重新命名多個項目、請在使用此程序之前記錄一般的命名方案。請準備一套系統、確保名稱獨一無二、一致且易於理解、一目瞭然。

您可以使用任何符合組織需求的命名慣例。請考慮以下基本建議、說明應包含哪些內容：

- * 站台指標 * ：如果您有多個站台、請在每個節點名稱中新增站台代碼。
- * 節點類型 * ：節點名稱通常表示節點的類型。您可以使用、 adm`和 `gw（儲存節點、管理節點和閘道節點）等縮寫 s。
- * 節點編號 * ：如果站台包含多種特定類型的節點、請在每個節點的名稱中新增唯一編號。

請三思、再將特定詳細資料新增至可能隨著時間而改變的名稱。例如、請勿在節點名稱中包含 IP 位址、因為這些位址可以變更。同樣地、如果您移動設備或升級硬體、機架位置或設備型號也可能會有所變更。

顯示名稱範例

假設您的 StorageGRID 系統有三個資料中心、每個資料中心都有不同類型的節點。您的顯示名稱可能與以下名稱一樣簡單：

- * 網格 * ： StorageGRID Deployment
- * 第一站 * ： Data Center 1
  - dc1-adm1
  - dc1-s1
  - dc1-s2
  - dc1-s3
  - dc1-gw1
- * 第二站 * ： Data Center 2
  - dc2-adm2
  - dc2-s1
  - dc2-s2
  - dc2-s3
- * 第三網站 * ： Data Center 3
  - dc3-s1
  - dc3-s2
  - dc3-s3

新增或更新 StorageGRID 顯示名稱

您可以使用此程序來新增或更新用於網格、站台和節點的顯示名稱。您可以同時重新命名單一項目、多個項目、甚至所有項目。定義或更新顯示名稱不會以任何方式影響 StorageGRID 作業。

開始之前

- 從任何管理節點，您都可以使用"支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您瞭解顯示器名稱的要求和最佳實務做法。請參閱。 "重新命名網格、站台和節點"

如何重新命名網格、站台或節點

您可以重新命名 StorageGRID 系統、一個或多個站台、或是一個或多個節點。

您可以使用先前由不同節點使用的顯示名稱、只要重新命名不會產生重複的顯示名稱或系統名稱。

選取要重新命名的項目

若要開始、請選取您要重新命名的項目。

步驟

1. 選擇*維護* > 任務 > 重新命名網格、網站和節點。
2. 在 * 選取名稱 * 步驟中、選取您要重新命名的項目。

要變更的項目	指示
系統中所有項目（或幾乎所有項目）的名稱	a. 選擇 * 全選 * 。 b. 您也可以清除任何不想重新命名的項目。
網格名稱	選取網格的核取方塊。
站台及其部分或全部節點的名稱	a. 選取網站表格標題中的核取方塊。 b. 或者、清除您不想重新命名的任何節點。
站台名稱	選取站台的核取方塊。
節點名稱	選取節點的核取方塊。

3. 選擇*繼續*。
4. 檢閱表格、其中包含您選取的項目。
    - 「 * 顯示名稱 * 」欄會顯示每個項目的目前名稱。如果項目從未重新命名、其顯示名稱會與系統名稱相同。

- * 系統名稱 * 欄會顯示您在安裝期間為每個項目輸入的名稱。系統名稱用於內部 StorageGRID 作業、無法變更。例如、節點的系統名稱可能是其主機名稱。
- 「 * 類型 * 」欄表示項目的類型：網格、站台或特定類型的節點。

提出新名稱

對於 * 建議新名稱 * 步驟、您可以分別為每個項目輸入顯示名稱、或是大量重新命名項目。

個別重新命名項目

請依照下列步驟、為您要重新命名的每個項目輸入顯示名稱。

步驟

1. 在 * 顯示名稱 * 欄位中、為清單中的每個項目輸入建議的顯示名稱。

   請參閱"重新命名網格、站台和節點"以瞭解命名要求。

2. 若要移除任何您不想重新命名的項目，請在「從清單中移除」欄中選取 ✕。

   如果您不建議項目的新名稱、則必須將其從表格中移除。

3. 當您為表格中的所有項目建議新名稱時、請選取 * 重新命名 * 。

   隨即顯示成功訊息。全新的顯示名稱現在會在整個 Grid Manager 中使用。

大量重新命名項目

如果品項名稱共用您要以不同字串取代的通用字串、請使用大量重新命名工具。

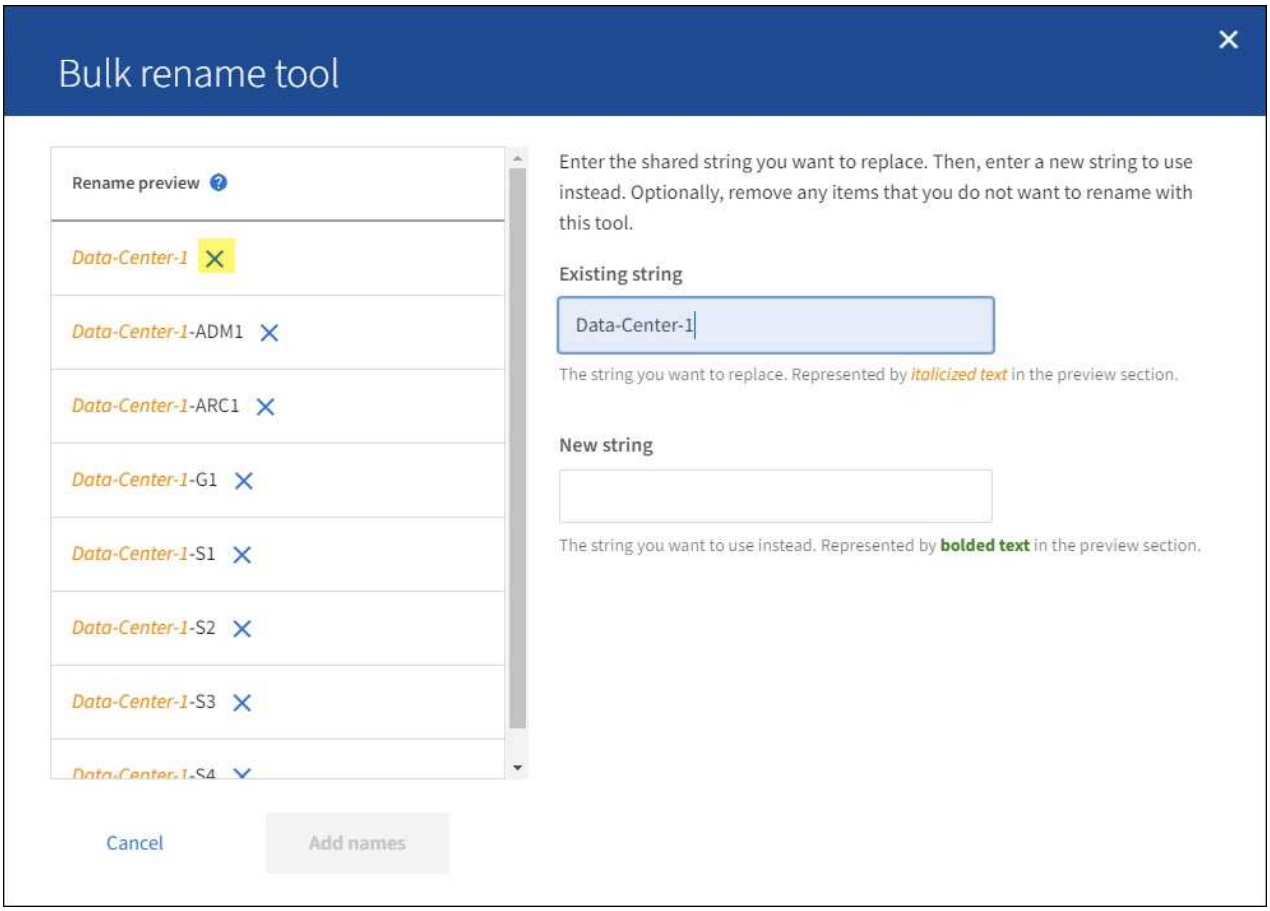
步驟

1. 對於 * 建議新名稱 * 步驟、請選取 * 使用大量重新命名工具 * 。
   - 重新命名預覽 * 包含 * 建議新名稱 * 步驟所顯示的所有項目。您可以使用預覽來查看取代共用字串後顯示名稱的外觀。
2. 在 * 現有字串 * 欄位中、輸入您要取代的共用字串。例如，如果要替換的字符串是 `Data-Center-1`，請輸入 **Data-Center-1** 。

   輸入時、您的文字會在左側名稱中的任何位置反白顯示。

3. 選擇 ✕ 以移除任何您不想使用此工具重新命名的項目。

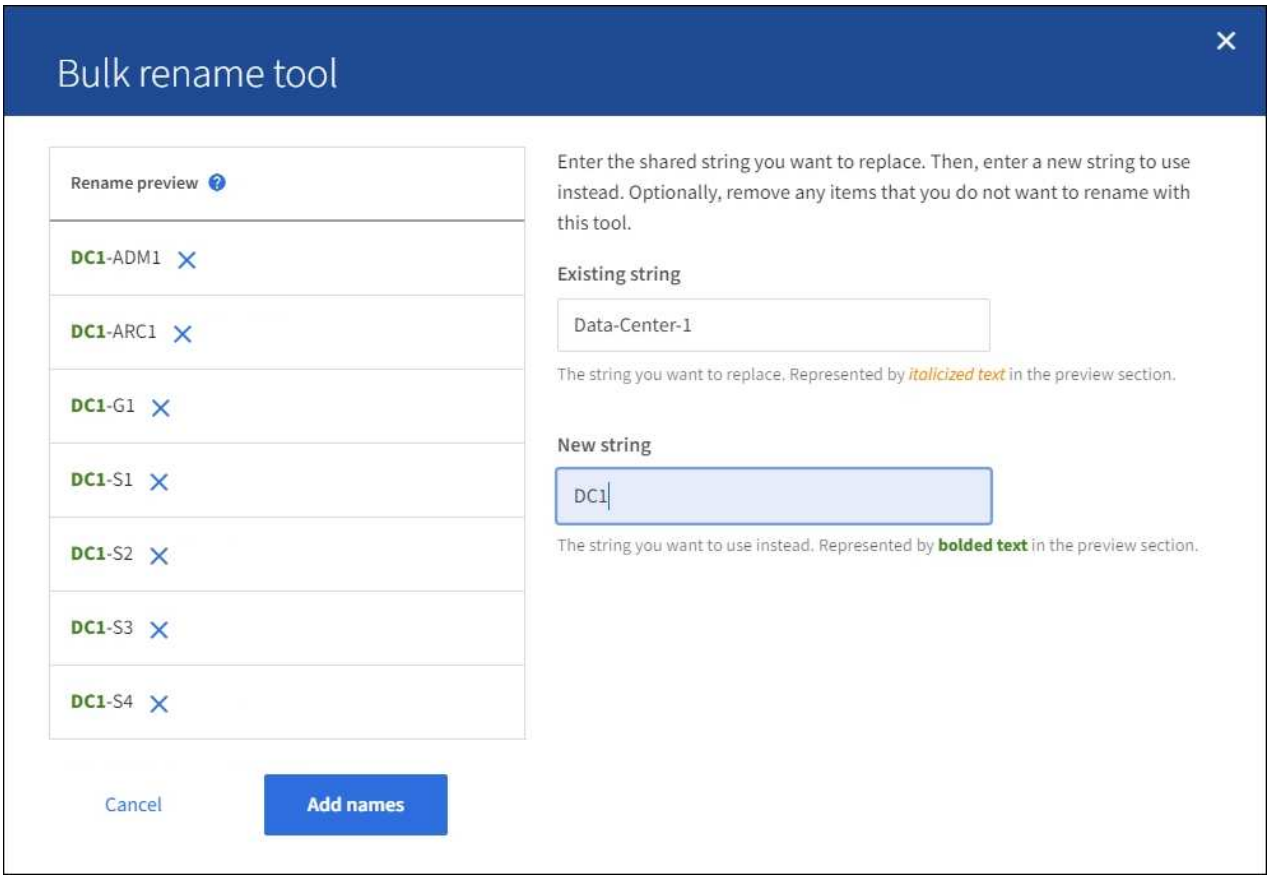
   例如，假設您想要重新命名所有包含字串 `Data-Center-1` 的節點，但不想重新命名 `Data-Center-1` 網站本身。選取 ✕ 可從重新命名預覽中移除網站。



4. 在 * 新字串 * 欄位中、輸入您要改用的替換字串。例如，輸入 **DC1** 。

   請參閱"重新命名網格、站台和節點"以瞭解命名要求。

   當您輸入替換字串時、左側的名稱會更新、以便您確認新名稱是否正確。



5. 當您對預覽中顯示的名稱感到滿意時、請選取 * 新增名稱 * 、將名稱新增至 * 建議新名稱 * 步驟的表格。
6. 進行任何其他必要的更改，或選擇 ✕ 以移除您不想重新命名的任何項目。
7. 當您準備好重新命名表格中的所有項目時、請選取 * 重新命名 * 。

   畫面會顯示成功訊息。全新的顯示名稱現在會在整個 Grid Manager 中使用。

下載復原包

完成重新命名專案後，下載並儲存新的復原包。您重新命名的項目的新顯示名稱包含在 `Passwords.txt`文件。

步驟

1. 輸入資源配置通關密碼。
2. 選擇*下載恢復套件*。

   下載隨即開始。

3. 下載完成後、開啟 `Passwords.txt`檔案以查看所有節點的伺服器名稱、以及任何重新命名節點的顯示名稱。
4. 將檔案複製 `sgws-recovery-package-*id-revision*.zip`到兩個安全且獨立的位置。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

5. 選擇 * 完成 * 返回第一步。

將顯示名稱回復為系統名稱

您可以將重新命名的網格、站台或節點還原為其原始系統名稱。當您將項目還原為其系統名稱時、 Grid Manager 頁面和其他 StorageGRID 位置不會再顯示該項目的 * 顯示名稱 * 。只會顯示項目的系統名稱。

步驟

1. 選擇*維護* > 任務 > 重新命名網格、網站和節點。
2. 對於 * 選取名稱 * 步驟、請選取您要回復為系統名稱的任何項目。
3. 選擇*繼續*。
4. 對於「 * 提出新名稱 * 」步驟、請將顯示名稱個別或大量還原回系統名稱。

   個別還原為系統名稱

   a. 複製每個項目的原始系統名稱並將其貼上到 顯示名稱 欄位中，或選擇 ✕ 以移除任何您不想還原的項目。

      若要回復顯示名稱、系統名稱必須顯示在 * 顯示名稱 * 欄位中、但名稱不區分大小寫。

   b. 選取*重新命名*。

      隨即顯示成功訊息。不再使用這些項目的顯示名稱。

   大量還原為系統名稱

   a. 對於 * 建議新名稱 * 步驟、請選取 * 使用大量重新命名工具 * 。
   b. 在 * 現有字串 * 欄位中、輸入您要取代的顯示名稱字串。
   c. 在 * 新字串 * 欄位中、輸入您要改用的系統名稱字串。
   d. 選取 * 新增名稱 * ，將名稱新增至 * 建議新名稱 * 步驟的表格。
   e. 確認「顯示名稱」欄位中的每個條目都與「系統名稱」欄位中的名稱一致。進行任何更改，或選擇 ✕ 以移除任何您不想還原的項目。

      若要回復顯示名稱、系統名稱必須顯示在 * 顯示名稱 * 欄位中、但名稱不區分大小寫。

   f. 選取*重新命名*。

      畫面會顯示成功訊息。不再使用這些項目的顯示名稱。

5. 下載並儲存新的復原包 。

   您還原項目的顯示名稱不再包含在檔案中 `Passwords.txt`。

節點程序

StorageGRID 節點維護程序

您可能需要執行與特定網格節點或節點服務相關的維護程序。

行動 **ADC**

這"ADC 服務"位於一些儲存節點上。在某些退役和節點轉換情況下，您需要將 ADC 服務移至同一站點上的另一個儲存節點。

將儲存節點轉換為僅資料節點

您可以將不包含 ADC 服務的儲存節點轉換為僅資料的儲存節點。

節點重啟、關閉和電源

您可以使用這些程序來重新開機一或多個節點、關閉和重新啟動節點、或關閉節點電源、然後重新開啟節點電源。

連接埠重映射

您可以使用連接埠重新對應程序、從節點移除連接埠重新對應、例如、如果您要使用先前重新對應的連接埠來設定負載平衡器端點。

伺服器管理員

伺服器管理程式會在每個網格節點上執行、以監督服務的啟動和停止、並確保服務順利加入StorageGRID 並離開此系統。伺服器管理員也會監控每個網格節點上的服務、並自動嘗試重新啟動任何報告故障的服務。

要執行伺服器管理器程序，通常需要存取節點的命令列。

只有在技術支援指示您存取伺服器管理程式時、您才應該存取伺服器管理程式。

在 StorageGRID 中移動 ADC 服務

您可以將 ADC 服務移至同一網站上的另一個儲存節點。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 你有"維護或根存取權限"。
- 源節點包含 ADC 服務。
- 目標節點不包含 ADC 服務。
- 目標節點是僅元資料節點或組合（元資料和物件資料）節點。
- 來源節點和目標節點位於同一站點。

關於這項工作

使用「移動 ADC」程序手動在儲存節點之間移動 ADC 服務。例如，您可能需要跨節點重新指派 ADC 服務，或將 ADC 服務移至效能較高的節點。

此程序將 ADC、IDNT、ACCT 和 RSM 服務從一個儲存節點移至同一站點上的另一個儲存節點。 RSM、IDNT 和 ACCT 服務依賴 ADC 服務，因此當 ADC 服務移動時，它們也會自動移動。

- 在 "將儲存節點轉換為僅資料節點" 或退役儲存節點之前，無需手動移動 ADC 服務。這些程序會在需要時自動移動 ADC 服務。有關要求的詳細資訊，請參閱 "ADC 仲裁數是多少？"。
- StorageGRID 會將 ADC 服務移至符合託管該服務要求的最新儲存節點。

步驟

1. 記錄源節點和目標節點的節點ID。

   在網格管理 API 中，來源節點 ID 被稱為 `sourceNodeId`。目標節點 ID 稱為 `targetNodeId`。

2. 從 Grid Manager 頂端選取說明圖示、然後選取 * API 文件 * 。
3. 選取 * 前往私有 API 文件 * 。
4. 選擇 `POST /private/move-adc/start`手術。請參閱"發出API要求"了解更多。

   在此過程中，兩個節點將依序重新啟動。來源節點首先重新啟動，然後是目標節點。

5. 您可以使用 `GET /private/move-adc`監控該過程。如果出現錯誤，請選擇 `POST /private/move-adc/retry`重試該過程。
6. "下載恢復包"完成此過程後。

將 StorageGRID Storage Node 轉換為僅資料節點

為了提高效能，您可以將較慢的非 ADC 儲存節點轉換為僅資料的儲存節點。

如果您的儲存節點具有不同的效能特性、則只使用儲存節點來處理資料可能是有意義的。例如、若要提高效能、您可以使用僅限資料的大容量旋轉磁碟儲存節點、以及僅限中繼資料的高效能儲存節點。

此外，您可以透過從 Cassandra 中刪除低 RAM 節點來獲得更多元資料容量，這會增加每個節點的元資料容量限制。請參閱"管理物件中繼資料儲存" 。

轉換僅資料節點時，每個站點的網格必須至少包含三個組合或僅元資料的儲存節點。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 儲存節點不是僅元資料節點或僅資料節點。
- 如果儲存節點包含 ADC 服務，則網格中有兩個以上的 ADC 儲存節點線上，並且同一站台上有非 ADC 儲存節點可用於主控 ADC 服務。
- 站點上其他節點上有足夠的元資料空間（或者您已經"擴大你的網格") 來容納將從您正在轉換的儲存節點遷移的元資料。

  - 如果遷移到同一站點上其他節點的元資料超出了"元資料保留空間"，電網就會變得不穩定。
  - 開始轉換後，您將無法擴展網格。

關於這項工作

使用此程序可將一個或多個組合儲存節點轉換為僅資料節點。如果儲存節點包含 ADC 服務，則在轉換過程中，該服務將自動移至同一站台上的另一個儲存節點。

除了轉換儲存節點之外，此過程還會從節點中退役 Cassandra。所有元資料將遷移到組合或僅元資料的儲存節點。根據需要遷移的元資料的數量，每個節點可能需要幾天的時間才能完成此過程。

通常，如果每個節點的元資料使用量小於 1 TB，則一次最多可以轉換 10 個節點。如果每個節點的元資料使用量超過 1 TB，則每個流程最多轉換 5 個節點。

StorageGRID 會將 ADC 服務移至符合託管該服務要求的最新儲存節點。

步驟

1. 記錄要轉換的非 ADC 儲存節點的節點 ID。
2. 從 Grid Manager 頂端選取說明圖示、然後選取 * API 文件 * 。
3. 選取 * 前往私有 API 文件 * 。
4. 選擇 `POST /private/convert-to-data-only-node/start`手術。請參閱"發出API要求"了解更多。

   在此過程中，每個節點都會重新啟動。

5. 您可以使用 `GET /private/convert-to-data-only-node`監控該過程。如果出現錯誤，請選擇 `POST /private/convert-to-data-only-node/retry`重試該過程。
6. "下載恢復包"完成此過程後。

重新開機、關機和電源程序

執行 **StorageGRID** 滾動重新開機

您可以執行滾動重新開機、以重新啟動多個網格節點、而不會造成服務中斷。

開始之前

- 您已登入主要管理節點上的 Grid Manager 、且使用的是"支援的網頁瀏覽器"。

  您必須登入主要管理節點才能執行此程序。

- 您有"維護或根存取權限"。

關於這項工作

如果您需要同時重新啟動多個節點、請使用此程序。例如，您可以在變更網格的 FIPS 模式之後使用此程序"TLS 和 SSH 安全性原則"。當 FIPS 模式變更時、您必須重新啟動所有節點、才能使變更生效。

如果您只需要重新啟動一個節點、您可以"從「工作」標籤重新啟動節點"。

StorageGRID 重新開機網格節點時、會在每個節點上發出 `reboot`命令、導致節點關機並重新啟動。所有服務都會自動重新啟動。

- 重新啟動 VMware 節點會重新啟動虛擬機器。

- 重新啟動 Linux 節點會重新啟動容器。
- 重新啟動 StorageGRID 應用裝置節點會重新啟動運算控制器。

滾動重新開機程序可同時重新啟動多個節點、但以下情況除外：

- 相同類型的兩個節點將不會同時重新開機。
- 閘道節點和管理節點不會同時重新開機。

相反地、這些節點會依序重新開機、以確保 HA 群組、物件資料和關鍵節點服務永遠保持可用。

當您重新啟動主要管理節點時、瀏覽器會暫時失去 Grid Manager 的存取權、因此您無法再監控程序。因此、主要管理節點會最後重新開機。

執行循環重新開機

您可以選取要重新開機的節點、檢閱您的選擇、啟動重新開機程序、以及監控進度。

選取節點

第一步是存取「循環重新開機」頁面、然後選取您要重新開機的節點。

步驟

1. 選擇*維護* > 任務 > 捲動重新啟動。
2. 檢閱 * 節點名稱 * 欄中的連線狀態和警示圖示。

   如果節點與網格斷開連接，則無法重新啟動該節點。帶有以下圖示的節點的核取方塊將被停用： 或 。

3. 如果有任何節點有作用中警示、請檢閱 * 警示摘要 * 欄中的警示清單。

   若要查看節點的所有目前警示、您也可以選取節點 › 概述索引標籤。

4. 您也可以執行建議的動作來解決任何目前的警示。
5. 或者、如果所有節點都已連線、而且您想要全部重新開機、請選取表格標題中的核取方塊、然後選取 * 全選 * 。否則、請選取您要重新開機的每個節點。

   您可以使用表格的篩選選項來檢視節點子集。例如、您只能檢視及選取特定站台上的儲存節點或所有節點。

6. 選取 * 檢閱選擇 * 。

檢閱選擇

在此步驟中、您可以判斷重新開機程序的總時間長度、並確認您選取了正確的節點。

1. 在「 Review Selection 」（檢閱選擇）頁面上、檢閱「 Summary 」（摘要）、指出將重新開機的節點數量、以及所有節點重新開機的預估總時間。
2. 或者、若要從重新開機清單中移除特定節點、請選取 * 移除 * 。

3. 或者、若要新增更多節點、請選取 * 上一步 * 、選取其他節點、然後選取 * 檢閱選取項目 * 。
4. 當您準備好開始所有選取節點的循環重新開機程序時、請選取 * 重新開機節點 * 。
5. 如果您選擇重新啟動主要管理節點、請閱讀資訊訊息、然後選取 * 是 * 。

> 主要管理節點將是最後一個重新開機節點。當此節點正在重新開機時、瀏覽器的連線將會中斷。當主管理節點再次可用時、您必須重新載入循環重新開機頁面。

監控循環重新開機

當循環重新開機程序正在執行時、您可以從主要管理節點監控。

步驟

1. 檢閱作業的整體進度、其中包括下列資訊：
   - 重新開機的節點數
   - 正在重新開機的節點數
   - 要重新開機的剩餘節點數
2. 檢閱每種節點類型的表格。

   這些表格提供每個節點上作業的進度列、並顯示該節點的重新開機階段、這可以是其中一項：

   - 正在等待重新開機
   - 停止服務
   - 重新啟動系統
   - 啟動服務
   - 重新開機完成

停止循環重新開機程序

您可以從主要管理節點停止循環重新開機程序。當您停止程序時、狀態為「停止服務」、「重新啟動系統」或「啟動服務」的任何節點都會完成重新開機作業。不過、這些節點將不再是程序的一部分。

步驟

1. 選擇*維護* > 任務 > 捲動重新啟動。
2. 在 * 監視器重新開機 * 步驟中、選取 * 停止重新開機程序 * 。

從「任務」標籤重新啟動 **StorageGRID** 節點

您可以從「節點」頁面上的「工作」索引標籤、重新啟動個別的網格節點。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。

- 如果您要重新啟動主要管理節點或任何儲存節點、您已檢閱下列考量事項：
  - 當您重新啟動主要管理節點時、瀏覽器會暫時失去對 Grid Manager 的存取權。
  - 如果您在指定站台重新啟動兩個以上的儲存節點、則在重新開機期間可能無法存取某些物件。如果任何 ILM 規則使用 *Dual Commit * 擷取選項（或規則指定 *Balanced * 、無法立即建立所有必要複本）、就可能發生此問題。在這種情況下、 StorageGRID 會將新擷取的物件提交至同一個站台上的兩個儲存節點、並於稍後評估 ILM 。
  - 為了確保您可以在儲存節點重新開機時存取所有物件、請先停止在站台上擷取物件約一小時、再重新啟動節點。

關於這項工作

StorageGRID 重新開機網格節點時、會在節點上發出 `reboot`命令、導致節點關機並重新啟動。所有服務都會自動重新啟動。

- 重新啟動 VMware 節點會重新啟動虛擬機器。
- 重新啟動 Linux 節點會重新啟動容器。
- 重新啟動 StorageGRID 應用裝置節點會重新啟動運算控制器。

如果您需要重新啟動多個節點、可以使用"循環重新開機程序"。

步驟

1. 選擇*節點*。
2. 選取您要重新開機的網格節點。
3. 選取*工作*索引標籤。
4. 選擇*重新開機*。

   隨即顯示確認對話方塊。如果您要重新開機主管理節點、確認對話方塊會提醒您、當服務停止時、瀏覽器與Grid Manager的連線將會暫時中斷。

5. 輸入資源配置通關密碼、然後選取*確定*。
6. 等待節點重新開機。

   服務可能需要一些時間才能關機。

   當節點重新開機時、節點頁面上的節點會出現灰色（管理性關閉）圖示。當所有服務重新啟動、且節點已成功連線至網格時、「節點」頁面應會顯示正常狀態（節點名稱左側沒有圖示）、表示沒有作用中警示、且節點已連線至網格。

從命令列重新啟動 **StorageGRID** 節點

如果您需要更密切地監控重新開機作業、或是無法存取 Grid Manager 、您可以登入網格節點、然後從命令 Shell 執行 Server Manager 重新開機命令。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 您也可以選擇停止服務： `service servermanager stop`

   停止服務是選用的步驟、但建議您採取此步驟。服務關機最多需要15分鐘、您可能想要遠端登入系統、以監控關機程序、然後再於下一步重新開機節點。

3. 重新啟動網格節點： `reboot`

4. 登出命令 Shell ： `exit`

關閉 **StorageGRID** 節點

您可以從節點的命令Shell關閉網格節點。

開始之前

- 您有 `Passwords.txt`檔案。

關於這項工作

執行此程序之前、請先檢閱下列考量事項：

- 一般而言、您不應一次關閉多個節點、以免發生中斷。
- 除非文件或技術支援明確指示、否則請勿在維護程序期間關閉節點。
- 關機程序取決於節點的安裝位置、如下所示：
  - 關閉VMware節點會關閉虛擬機器。
  - 關閉Linux節點會關閉容器。
  - 關閉StorageGRID 一個不中斷的應用程式節點會關閉運算控制器。
- 如果您打算在站台上關閉多個儲存節點、請在關閉節點之前、先停止在該站台上擷取物件約一小時。

  如果有任何 ILM 規則使用 * 雙重認可 * 擷取選項（或如果規則使用 * 平衡 * 選項、且無法立即建立所有必要的複本）、 StorageGRID 會立即將任何新擷取的物件提交至同一站台上的兩個儲存節點、並於稍後評估 ILM 。如果站台上有多個儲存節點已關機、則在關機期間、您可能無法存取新擷取的物件。如果站台上的儲存節點數量太少、寫入作業也可能會失敗。請參閱。 "使用ILM管理物件"

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 停止所有服務： `service servermanager stop`

服務關機最多需要15分鐘、您可能想要從遠端登入系統、以監控關機程序。

3. 如果節點是在 VMware 虛擬機器上執行、或是應用裝置節點、請發出關機命令： `shutdown -h now`

無論命令的結果為何、都請執行此步驟 `service servermanager stop`。

> 在應用裝置節點上發出命令後 `shutdown -h now`、您必須關閉設備電源再重新啟動、才能重新啟動節點。

對於應用裝置、此命令會關閉控制器、但應用裝置仍會開啟電源。您必須完成下一步。

4. 如果您要關閉應用裝置節點的電源、請遵循應用裝置的步驟。

SG6160

a. 關閉 SG6100-CN 儲存控制器的電源。

b. 等待 SG6100-CN 儲存控制器上的藍色電源 LED 熄滅。

SGF6112

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG6000

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、然後等待藍色電源LED燈關閉。

SG5800

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 從「SView System Manager」首頁SANtricity 選取*「View Operations in progress*」。

c. 請確認所有作業均已完成、然後再繼續下一步。

d. 關閉控制器機櫃上的兩個電源開關、並等待控制器機櫃上的所有 LED 燈熄滅。

SG5700

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、並等待所有LED和七段顯示活動停止。

SG100 或 **SG1000**

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

關閉 **StorageGRID** 主機

在關閉主機電源之前、您必須停止該主機上所有網格節點上的服務。

步驟

1. 登入網格節點：

a. 輸入下列命令： `ssh admin@grid_node_IP`

b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 停止在節點上執行的所有服務： `service servermanager stop`

服務關機最多需要15分鐘、您可能想要從遠端登入系統、以監控關機程序。

3. 針對主機上的每個節點重複步驟1和2。

4. 如果您有Linux主機：

a. 登入主機作業系統。

b. 停止節點： `storagegrid node stop`

c. 關閉主機作業系統。

5. 如果節點是在 VMware 虛擬機器上執行、或是應用裝置節點、請發出關機命令： `shutdown -h now`

無論命令的結果為何、都請執行此步驟 `service servermanager stop`。

> 在應用裝置節點上發出命令後 `shutdown -h now`、您必須關閉設備電源再重新啟動、才能重新啟動節點。

對於應用裝置、此命令會關閉控制器、但應用裝置仍會開啟電源。您必須完成下一步。

6. 如果您要關閉應用裝置節點的電源、請遵循應用裝置的步驟。

SG6160

a. 關閉 SG6100-CN 儲存控制器的電源。

b. 等待 SG6100-CN 儲存控制器上的藍色電源 LED 熄滅。

SGF6112

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG6000

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、然後等待藍色電源LED燈關閉。

SG5800

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 從「SView System Manager」首頁SANtricity 選取*「View Operations in progress*」。

c. 請確認所有作業均已完成、然後再繼續下一步。

d. 關閉控制器機櫃上的兩個電源開關、並等待控制器機櫃上的所有 LED 燈熄滅。

SG5700

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、並等待所有LED和七段顯示活動停止。

SG110 或 SG1100

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG100 或 SG1000

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

7. 登出命令 Shell ： `exit`

相關資訊

- "SGF6112 和 SG6160 儲存設備"
- "SG6000 儲存設備"

- "SG5700 儲存設備"
- "SG5800 儲存設備"
- "SG110 和 SG1100 服務應用裝置"
- "SG100 和 SG1000 服務應用裝置"

關閉並開啟所有 **StorageGRID** 節點

例如、如果您要搬移資料中心、可能需要關閉整個StorageGRID 的整套功能。這些步驟提供建議的執行管制關機和開機順序的高階概觀。

當您關閉網站或網格中的所有節點時，儲存節點離線期間您將無法存取已擷取的物件。

停止服務並關閉網格節點

在您關閉StorageGRID 某個VMware系統之前、您必須先停止每個網格節點上執行的所有服務、然後關閉所有VMware虛擬機器、Container引擎和StorageGRID VMware應用程式。

關於這項工作

首先停止管理節點和閘道節點上的服務，然後停止儲存節點上的服務。

此方法可讓您使用主要管理節點、盡可能長時間監控其他網格節點的狀態。

如果單一主機包含多個網格節點、請在停止該主機上的所有節點之前、不要關閉主機。如果主機包含主要管理節點、請最後關閉該主機。

如果需要、您可以"將節點從一個Linux主機移轉至另一個主機"執行主機維護、而不會影響網格的功能或可用度。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 停止所有用戶端應用程式存取網格。
3. [[log_in_to _GN]登入每個閘道節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。
4. 停止在節點上執行的所有服務： `service servermanager stop`

   服務關機最多需要15分鐘、您可能想要從遠端登入系統、以監控關機程序。
5. 重複上述兩個步驟、停止所有儲存節點和非主要管理節點上的服務。

您可以依任何順序停止這些節點上的服務。

> 如果您發出 `service servermanager stop`命令來停止應用裝置儲存節點上的服務、則必須關閉應用裝置電源再重新啟動節點。

6. 對於主管理節點，請重複和停止節點上的所有服務的步驟登入節點。
7. 對於在Linux主機上執行的節點：
   a. 登入主機作業系統。
   b. 停止節點： `storagegrid node stop`
   c. 關閉主機作業系統。
8. 對於在 VMware 虛擬機器和應用裝置儲存節點上執行的節點、請發出關機命令： `shutdown -h now`

   無論命令的結果為何、都請執行此步驟 `service servermanager stop`。

   對於應用裝置、此命令會關閉運算控制器、但應用裝置仍會開啟電源。您必須完成下一步。
9. 如果您有應用裝置節點、請依照應用裝置的步驟進行。

SG110 或 SG1100

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG100 或 SG1000

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG6160

a. 關閉 SG6100-CN 儲存控制器的電源。

b. 等待 SG6100-CN 儲存控制器上的藍色電源 LED 熄滅。

SGF6112

a. 關閉產品電源。

b. 等待藍色電源LED燈關閉。

SG6000

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、然後等待藍色電源LED燈關閉。

SG5800

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 從「SView System Manager」首頁SANtricity 選取*「View Operations in progress*」。

c. 請確認所有作業均已完成、然後再繼續下一步。

d. 關閉控制器機櫃上的兩個電源開關、並等待控制器機櫃上的所有 LED 燈熄滅。

SG5700

a. 等待儲存控制器背面的綠色快取作用中LED關閉。

當需要將快取的資料寫入磁碟機時、此LED會亮起。您必須等待此LED燈關閉、才能關閉電源。

b. 關閉產品電源、並等待所有LED和七段顯示活動停止。

10. 如有必要、請登出命令 Shell ： `exit`

此功能現已關閉。StorageGRID

11. 如果您允許外部 SSH 訪問，"阻止訪問"當您關閉完節點後。

啟動網格節點

如果可能、請依下列順序開啟網格節點：

- 先將電力套用至管理節點。
- 最後將電力套用至閘道節點。

如果主機包含多個網格節點，則在主機通電時，這些節點會自動重新上線。

步驟

1. 開啟主要管理節點和任何非主要管理節點的主機。

   在儲存節點重新啟動之前，您無法登入管理節點。

2. 開啟所有儲存節點的主機電源。

   您可以依任何順序開啟這些節點。

3. 開啟所有閘道節點的主機電源。
4. 登入Grid Manager。
5. 選擇*節點*並監控網格節點的狀態。驗證節點名稱旁邊沒有警報圖示。

相關資訊

- "SGF6112 和 SG6160 儲存設備"
- "SG110 和 SG1100 服務應用裝置"
- "SG100 和 SG1000 服務應用裝置"
- "SG6000 儲存設備"
- "SG5800 儲存設備"
- "SG5700 儲存設備"

連接埠重新對應程序

刪除**StorageGRID**設備上的連接埠重新映射

如果您想要設定負載平衡器服務的端點、而且想要使用已設定為連接埠重新對應對應對應對應對應對應對應對應對應對應對應的連接埠、則必須先移除現有的連接埠重新對應、否則端點將無法生效。您必須在每個具有衝突的重新對應連接埠的管理節點和閘道節點上執行指令碼、才能移除節點的所有連接埠重新對應。

關於這項工作

此程序會移除所有連接埠重新對應。如果您需要保留部分重新對應、請聯絡技術支援部門。

如需設定負載平衡器端點的相關資訊，請參閱"設定負載平衡器端點"。

如果連接埠重新對應提供用戶端存取、請將用戶端重新設定為使用不同的連接埠做為負載平衡器端點、以避免服務中斷。否則、移除連接埠對應將導致用戶端存取中斷、並應適當排程。

此程序不適用於StorageGRID 以容器形式部署在裸機主機上的作業系統。請參閱的說明"移除裸機主機上的連接埠重新對應"。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 登入節點。
   a. 輸入下列命令： `ssh -p 8022 admin@node_IP`

      連接埠8022是基礎作業系統的SSH連接埠、而連接埠22則是執行StorageGRID 支援的Container引擎SSH連接埠。

   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
3. 執行下列指令碼： `remove-port-remap.sh`
4. 重新啟動節點： `reboot`
5. 登出命令 Shell ： `exit`
6. 在每個重新對應連接埠發生衝突的管理節點和閘道節點上重複這些步驟。
7. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成刪除連接埠重新映射後。

相關資訊

- "用於外部通訊的連接埠"

移除裸機主機上的 **StorageGRID** 連接埠重新映射

如果您想要設定負載平衡器服務的端點、而且想要使用已設定為連接埠重新對應對應對應對應對應對應對應對應對應對應對應的連接埠、則必須先移除現有的連接埠重新對應、否則端點將無法生效。

關於這項工作

如果StorageGRID 您是在裸機主機上執行效能不全、請遵循此程序、而非移除連接埠重新對應的一般程序。您必須編輯每個管理節點和閘道節點的節點組態檔、這些節點具有衝突的重新對應連接埠、以移除節點的所有連接埠重新對應並重新啟動節點。

此程序會移除所有連接埠重新對應。如果您需要保留部分重新對應、請聯絡技術支援部門。

如需設定負載平衡器端點的相關資訊、請參閱《關於管理StorageGRID 》介紹。

此程序可能會在節點重新啟動時導致服務暫時中斷。

步驟

1. 登入支援節點的主機。以root或具有Sudo權限的帳戶登入。
2. 執行下列命令以暫時停用節點： `sudo storagegrid node stop node-name`
3. 使用vim或pico等文字編輯器、編輯節點的節點組態檔。

   節點組態檔位於 `/etc/storagegrid/nodes/node-name.conf`。

4. 找出節點組態檔中包含連接埠重新對應的區段。

   請參閱下列範例中的最後兩行。

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = DedicatedInterface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = DedicatedInterface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = DedicatedInterface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. 編輯port_remap和port_remap_inbound項目、以移除連接埠重新對應。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 執行下列命令、以驗證您對節點組態檔所做的變更：`sudo storagegrid node validate *node-name*`

   在繼續下一步之前、請先解決任何錯誤或警告。

7. 執行下列命令以重新啟動節點、而不重新對應連接埠： `sudo storagegrid node start *node-name*`
8. 使用檔案中列出的密碼、以 admin 身分登入節點 `Passwords.txt`。
9. 驗證服務是否正確啟動。
   a. 檢視伺服器上所有服務的狀態清單：`sudo storagegrid-status`

      狀態會自動更新。

   b. 等到所有服務的狀態都為「執行中」或「已驗證」。
   c. 結束狀態畫面：`Ctrl+C`
10. 在每個重新對應連接埠發生衝突的管理節點和閘道節點上重複這些步驟。

Server Manager 程序

檢視 **StorageGRID Server Manager** 狀態和版本

對於每個網格節點、您可以檢視該網格節點上執行的伺服器管理程式目前狀態和版本。您也可以取得在該網格節點上執行之所有服務的目前狀態。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：
   a. 輸入下列命令： `ssh admin@*grid_node_IP*`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 檢視網格節點上執行的 Server Manager 目前狀態： **`service servermanager status`**

   報告網格節點上執行的伺服器管理員目前狀態（執行中或非執行中）。如果 Server Manager 的狀態為 `running`、則會列出其自上次啟動以來的執行時間。例如：

```
servermanager running for 1d, 13h, 0m, 30s
```

3. 檢視網格節點上執行的 Server Manager 目前版本： **`service servermanager version`**

   列出目前的版本。例如：

```
11.1.0-20180425.1905.39c9493
```

4. 登出命令 Shell ： **`exit`**

查看所有 **StorageGRID** 服務的目前狀態

您可以隨時檢視在網格節點上執行的所有服務目前狀態。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

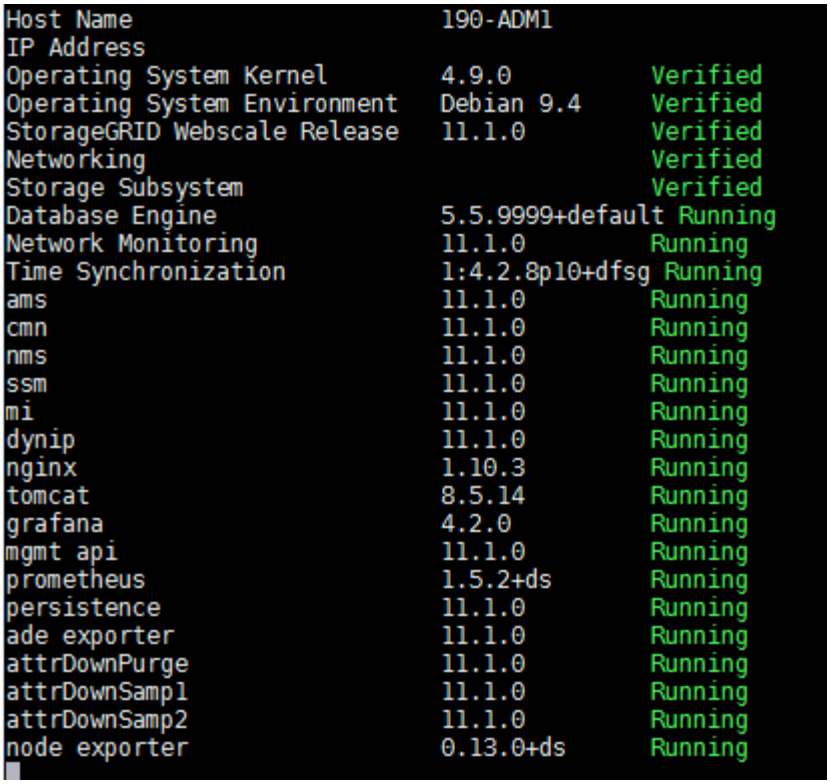
   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 檢視網格節點上執行的所有服務狀態： `storagegrid-status`

   例如、主管理節點的輸出會顯示AMS、CMN和NMS服務目前的執行狀態。如果服務狀態變更、則會立即更新此輸出。



3. 返回命令列、按* Ctrl-+* C*。
4. 或者、您也可以檢視網格節點上執行的所有服務的靜態報告：
   `/usr/local/servermanager/reader.rb`

   此報告包含的資訊與持續更新的報告相同、但如果服務狀態變更、則不會更新報告。

5. 登出命令 Shell ： `exit`

啟動 **StorageGRID Server Manager** 和所有服務

您可能需要啟動伺服器管理員、伺服器管理員也會啟動網格節點上的所有服務。

開始之前

您有 `Passwords.txt`檔案。

關於這項工作

在已執行伺服器管理程式的網格節點上啟動伺服器管理程式、將會重新啟動伺服器管理程式、並重新啟動網格節點上的所有服務。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 啟動 Server Manager ： `service servermanager start`
3. 登出命令 Shell ： `exit`

重新啟動 **StorageGRID Server Manager** 和所有服務

您可能需要重新啟動 Server Manager 以及網格節點上執行的所有服務。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 重新啟動伺服器管理員和網格節點上的所有服務： `service servermanager restart`

   伺服器管理員和網格節點上的所有服務都會停止、然後重新啟動。

   使用 `restart`命令與使用命令後面接著命令的 `start`方式相同 `stop`。

3. 登出命令 Shell ： `exit`

停止 **StorageGRID Server Manager** 和所有服務

伺服器管理程式可隨時執行、但您可能需要停止伺服器管理程式及在網格節點上執行的所有服務。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 停止伺服器管理程式和網格節點上執行的所有服務： `service servermanager stop`

   伺服器管理程式和在網格節點上執行的所有服務都會正常終止。關閉服務最多需要15分鐘。

3. 登出命令 Shell ： `exit`

查看 **StorageGRID** 服務的目前狀態

您可以隨時查看網格節點上執行的服務目前狀態。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 檢視在網格節點上執行的服務目前狀態：「*服務_servicename_狀態*報告在網格節點上執行的要求服務目前狀態（執行中或非執行中）。例如：

```
cmn running for 1d, 14h, 21m, 2s
```

3. 登出命令 Shell ： **`exit`**

停止 **StorageGRID** 服務

有些維護程序會要求您停止單一服務、同時讓網格節點上的其他服務保持執行狀態。只有在維護程序指示時、才會停止個別服務。

開始之前

您有 `Passwords.txt`檔案。

關於這項工作

當您使用這些步驟「管理性停止」服務時、伺服器管理員不會自動重新啟動服務。您必須手動啟動單一服務、或重新啟動伺服器管理員。

如果您需要停止儲存節點上的LDR服務、請注意、如果有作用中的連線、可能需要一段時間才能停止服務。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 停止個別服務： `service servicename stop`

   例如：

   ```
   service ldr stop
   ```

   > 服務最多可能需要11分鐘的時間才能停止。

3. 登出命令 Shell ： `exit`

相關資訊

"強制服務終止"

強制 StorageGRID 服務終止

如果您需要立即停止服務、可以使用 `force-stop`命令。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 手動強制服務終止： `service servicename force-stop`

   例如：

   ```
   service ldr force-stop
   ```

系統會在終止服務之前等待30秒。

3. 登出命令 Shell ： `exit`

啟動或重新啟動 **StorageGRID** 服務

您可能需要啟動已停止的服務、或是需要停止並重新啟動服務。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 根據服務目前正在執行或停止、決定要發出哪一個命令。

   - 如果服務目前已停止、請使用 `start`命令手動啟動服務： `service servicename start`

     例如：

     ```
     service ldr start
     ```

   - 如果服務目前正在執行中、請使用命令停止服務、 `restart`然後重新啟動： `service servicename restart`

     例如：

```
service ldr restart
```

+

> 使用 `restart`命令與使用命令後面接著命令的 `start`方式相同 `stop`。即使服務目前已停止、您仍可能發生問題 `restart`。

3. 登出命令 Shell ： `exit`

使用 **StorageGRID DoNotStart** 文件

如果您在技術支援的指導下執行各種維護或組態程序、可能會要求您使用DoNotStart檔案、以防止伺服器管理員啟動或重新啟動時啟動服務。

只有在技術支援人員指示您新增或移除DoNotStart檔案時、您才應該新增或移除該檔案。

若要防止服務啟動、請將DoNotStart檔案放在您要防止啟動的服務目錄中。在啟動時、伺服器管理員會尋找DoNotStart檔案。如果檔案存在、則服務（及其相依的任何服務）將無法啟動。當DoNotStart檔案移除時、先前停止的服務會在下一次啟動或重新啟動伺服器管理員時啟動。當 DoNotStart 檔案移除時、服務不會自動啟動。

防止所有服務重新啟動的最有效方法、是防止NTP服務啟動。所有服務均視 NTP 服務而定、如果 NTP 服務未執行、則無法執行。

新增服務的**DoNotStart**檔案

您可以將DoNotStart檔案新增至網格節點上的服務目錄、以防止個別服務啟動。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 新增 DoNotStart 檔案： `touch /etc/sv/service/DoNotStart`

   其中 `service`是要防止啟動的服務名稱。例如、

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   已建立DoNotStart檔案。不需要檔案內容。

   重新啟動伺服器管理員或網格節點時、伺服器管理員會重新啟動、但服務不會。
3. 登出命令 Shell ： `exit`

移除服務的**DoNotStart**檔案

當您移除導致服務無法啟動的DoNotStart檔案時、必須啟動該服務。

開始之前

您有 `Passwords.txt`檔案。

步驟

1. 登入網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 從服務目錄中移除 DoNotStart 檔案： `rm /etc/sv/service/DoNotStart`

   其中 `service`是服務的名稱。例如、

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. 啟動服務： `service servicename start`

4. 登出命令 Shell ： `exit`

疑難排解 **StorageGRID** 中的 **Server Manager**

如果使用伺服器管理員時發生問題、請檢查其記錄檔。

伺服器管理員記錄檔中會擷取與伺服器管理員相關的錯誤訊息、該檔案位於： `/var/local/log/servermanager.log`

請查看此檔案、以瞭解有關故障的錯誤訊息。如有需要、請將問題提報給技術支援部門。系統可能會要求您將記錄檔轉寄給技術支援部門。

具有錯誤狀態的服務

如果偵測到某項服務已進入錯誤狀態、請嘗試重新啟動該服務。

開始之前

您有 `Passwords.txt`檔案。

關於這項工作

伺服器管理程式會監控服務、並重新啟動任何非預期停止的服務。如果某項服務失敗、伺服器管理員會嘗試重新啟動該服務。如果在五分鐘內有三次嘗試啟動服務失敗、服務會進入錯誤狀態。伺服器管理程式不會嘗試重新啟動。

步驟

1. 登入網格節點：

a. 輸入下列命令： `ssh admin@grid_node_IP`

b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 確認服務的錯誤狀態： `service servicename status`

例如：

```
service ldr status
```

如果服務處於錯誤狀態，則會傳回下列訊息： `servicename in error state`。例如：

```
ldr in error state
```

如果服務狀態為 `disabled`，請參閱的說明"移除服務的DoNotStart檔案"。

3. 嘗試重新啟動服務以移除錯誤狀態： `service servicename restart`

如果服務無法重新啟動、請聯絡技術支援部門。

4. 登出命令 Shell ： `exit`

網路程序

更新 **StorageGRID Grid Network** 的子網路

此技術可維護網格網路（eth0）上用於在網格節點之間進行通訊的網路子網路清單。StorageGRID這些項目包括StorageGRID 您的系統所在站台用於Grid Network的子網路、以及透過Grid Network閘道存取的NTP、DNS、LDAP或其他外部伺服器所使用的任何子網路。當您在擴充中新增網格節點或新站台時、可能需要更新或新增子網路至網格網路。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您可以使用CIDR表示法來設定要設定的子網路位址。

關於這項工作

如果您執行的擴充活動包括新增子網路、則必須在開始擴充程序之前、將新的子網路新增至 Grid Network 子網路清單。否則、您必須取消擴充、新增子網路、然後重新開始擴充。

請勿對任何節點的網格網路、管理網路或用戶端網路使用包含下列 IPv4 位址的子網路：

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

例如，不要對任何節點的網格網路、管理網路或客戶端網路使用下列子網路範圍：

- 192.168.130.0/24，因為此子網路範圍包含 IP 位址 192.168.130.101 和 192.168.130.102
- 192.168.131.0/24，因為此子網路範圍包含 IP 位址 192.168.131.101 和 192.168.131.102
- 198.51.100.0/24，因為此子網路範圍包含 IP 位址 198.51.100.2 和 198.51.100.4

新增子網路

步驟

1. 選擇*維護* > 網路 > 電網。
2. 選取 * 新增其他子網路 * 、以 CIDR 表示法新增子網路。

   例如，輸入 `10.96.104.0/22`。

3. 輸入資源配置通關密碼、然後選取*「Save*（儲存*）」。
4. 等待更改套用完畢，然後下載新的恢復包。
   a. 選擇*維護* > 系統 > 恢復包。
   b. 請輸入*佈建密碼*。

   復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。它也用於恢復主管理節點。

您指定的子網路會自動設定為StorageGRID 適用於您的整個系統。

編輯子網路

步驟

1. 選擇*維護* > 網路 > 電網。
2. 選取您要編輯的子網路、然後進行必要的變更。
3. 輸入資源配置通關密碼、然後選取*「Save*（儲存*）」。
4. 在確認對話方塊中選取*是*。
5. 等待更改套用完畢，然後下載新的恢復包。
   a. 選擇*維護* > 系統 > 恢復包。
   b. 請輸入*佈建密碼*。

刪除子網路

步驟

1. 選擇*維護* > 網路 > 電網。
2. 選擇子網路旁的刪除圖示 ✕。
3. 輸入資源配置密碼短語、然後選取 * 儲存 * 。
4. 在確認對話方塊中選取*是*。
5. 等待更改套用完畢，然後下載新的恢復包。
   a. 選擇*維護* > 系統 > 恢復包。
   b. 請輸入*佈建密碼*。

設定IP位址

StorageGRID IP 位址準則

您可以使用變更IP工具來設定網格節點的IP位址、以執行網路組態。

您必須使用變更IP工具、對網格部署期間最初設定的網路組態進行大部分變更。使用標準Linux網路命令和檔案進行手動變更、可能不會傳播到所有StorageGRID 的支援服務、也不會在升級、重新開機或節點還原程序期間持續進行。

IP變更程序可能會造成中斷。在套用新組態之前、網格的某些部分可能無法使用。

如果您僅變更Grid Network Subnet List（網格網路子網路清單）、請使用Grid Manager新增或變更網路組態。否則、如果由於網路組態問題而無法存取Grid Manager、或者您同時執行Grid Network路由變更和其他網路變更、請使用變更IP工具。

如果您要變更網格中所有節點的網格網路 IP 位址、請使用"全網格變更的特殊程序"。

乙太網路介面

指派給eth0的IP位址永遠是網格節點的網格網路IP位址。指派給eth1的IP位址永遠是網格節點的管理網路IP位址。指派給eth2的IP位址永遠是網格節點的用戶端網路IP位址。

請注意、在StorageGRID 某些平台上、例如：功能完善的設備、eth0、eth1和eth2、可能是由附屬橋接器或實

體或VLAN介面的連結所組成的集合體介面。在這些平台上、* S要*>* Resources（資源）*索引標籤可能會顯示除了eth0、eth1或eth2之外、指派給其他介面的Grid（網格）、Admin（管理）和Client Network IP位址。

DHCP

您只能在部署階段設定DHCP。您無法在組態期間設定 DHCP 。如果您想要變更網格節點的IP位址、子網路遮罩和預設閘道、則必須使用IP位址變更程序。使用變更IP工具會使DHCP位址變成靜態。

高可用度（**HA**）群組

- 如果用戶端網路介面包含在 HA 群組中、您就無法將該介面的用戶端網路 IP 位址變更為 HA 群組所設定之子網路以外的位址。
- 您無法將用戶端網路 IP 位址變更為指派給用戶端網路介面上設定的 HA 群組的現有虛擬 IP 位址值。
- 如果 Grid 網路介面包含在 HA 群組中、您就無法將該介面的 Grid 網路 IP 位址變更為 HA 群組所設定之子網路以外的位址。
- 您無法將 Grid Network IP 位址變更為指派給 Grid Network 介面上設定的 HA 群組的現有虛擬 IP 位址值。

變更 **StorageGRID** 中的節點網路組態

您可以使用「變更 IP」工具變更一個或多個節點的網路組態。您可以變更網格網路的組態，也可以新增、變更或移除管理網路或用戶端網路。您也可以變更應用裝置節點 BMC 的 LAN IP 設定。

開始之前

您有 `Passwords.txt`檔案。

關於這項工作

*Linux：*如果您是第一次將網格節點新增至管理網路或用戶端網絡，且先前未在節點設定檔中設定 ADMIN_NETWORK_TARGET 或 CLIENT_NETWORK_TARGET，則必須現在這樣做。查看StorageGRID"安裝說明"適用於您的 Linux 作業系統。

- 應用裝置： * 在 StorageGRID 應用裝置上、如果在初始安裝期間未在 StorageGRID 應用裝置安裝程式中設定用戶端或管理網路、則無法僅使用變更 IP 工具來新增網路。首先、您必須 "將產品置於維護模式"設定連結、將應用裝置恢復為正常操作模式、然後使用變更 IP 工具來修改網路組態。請參閱 "設定網路連結的程序"。

您可以變更任何網路上一或多個節點的IP位址、子網路遮罩、閘道或MTU值。

您也可以從用戶端網路或管理網路新增或移除節點：

- 您可以將該網路上的IP位址/子網路遮罩新增至節點、將節點新增至用戶端網路或管理網路。
- 您可以刪除該網路上節點的IP位址/子網路遮罩、從用戶端網路或管理網路中移除節點。

  無法從 Grid Network 移除節點。

不允許 IP 位址交換。如果您必須在網格節點之間交換IP位址、則必須使用暫用的中繼IP位址。

如果您的 StorageGRID 系統已啟用單一登入 (SSO)，且您正在變更管理節點的 IP 位址，請注意，任何使用管理節點的 IP 位址（而非建議的完整網域名稱）設定的信賴方信任都將失效。您將無法再登入該節點。變更 IP 位址後，您必須立即使用新的 IP 位址在 Active Directory Federation Services (AD FS) 中更新或重新設定節點的信賴方信任。請參閱使用 "OIDC" 或 "SAML" 設定 SSO 的說明。

您使用變更IP工具對網路所做的任何變更、都會傳播至StorageGRID 安裝程式韌體、以供使用各種版本的應用裝置使用。如此一StorageGRID 來、如果在應用裝置上重新安裝了支援功能的軟體、或是將應用裝置置於維護模式、網路組態就會正確。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。
3. 輸入下列命令以啟動變更 IP 工具： `change-ip`
4. 在提示字元下輸入資源配置通關密碼。

   主功能表隨即出現。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. （可選）選擇* 1*以選擇要更新的節點。然後選取下列其中一個選項：
   - **1**：單一節點-依名稱選取
   - **2**：單一節點-依站台、然後依名稱選取
   - * 3*：單一節點-依目前IP選取
   - * 4 *：站台上的所有節點
   - **5**：網格中的所有節點

*附註：*如果您要更新所有節點、請允許「ALL」保持選取狀態。

選擇之後、主功能表隨即出現、*所選節點*欄位會更新以反映您的選擇。所有後續行動只會在顯示的節點上執行。

6. 在主功能表上、選取選項* 2*以編輯所選節點的IP/遮罩、閘道和MTU資訊。
   a. 選取您要變更的網路：
      - * 1 *：網格網路
      - * 2 *：管理網路
      - * 3 *：用戶端網路
      - **4** ：所有網路

      選擇之後、提示會顯示節點名稱、網路名稱（ Grid 、 Admin 或 Client ）、資料類型（ IP/ 遮罩、 閘道或 MTU ）、以及目前的值。

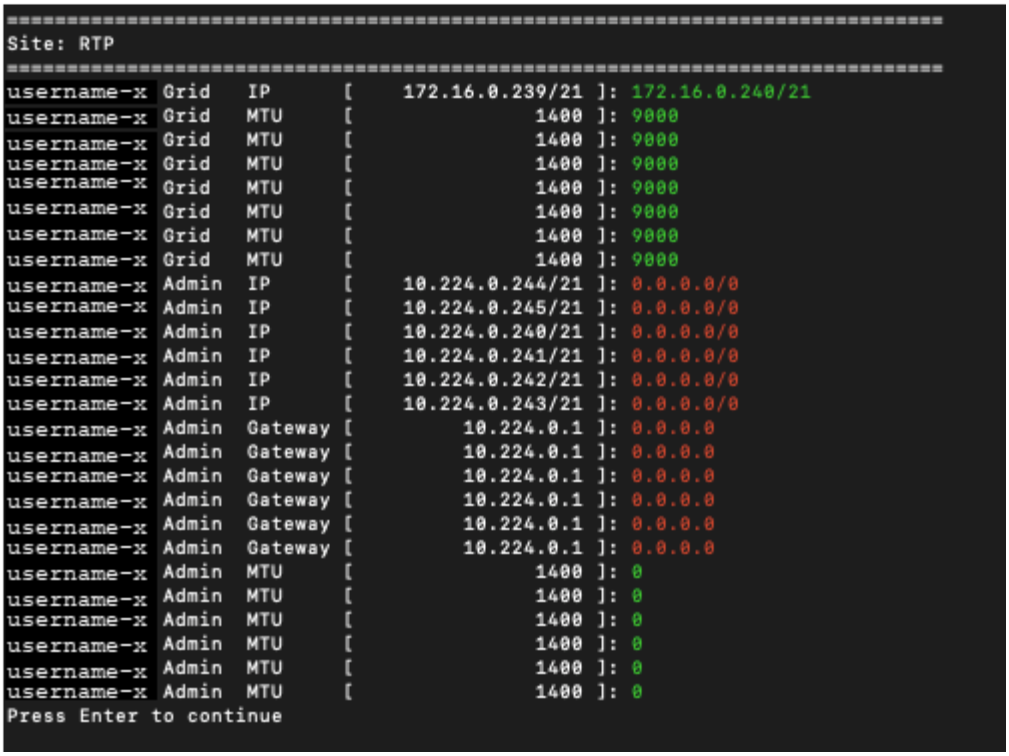
      編輯DHCP設定介面的IP位址、字首長度、閘道或MTU、將會將介面變更為靜態。當您選擇變更DHCP設定的介面時、會顯示警告、通知您介面將變更為靜態。

      設定為的介面 `fixed`無法編輯。

   b. 若要設定新值、請以目前值的顯示格式輸入。
   c. 若要保持目前值不變、請按* Enter *。
   d. 如果資料類型為 `IP/mask`、您可以輸入 * d* 或 * 0.0.0/0* 、從節點刪除管理或用戶端網路。
   e. 編輯完所有要變更的節點之後、輸入* q*即可返回主功能表。

      您的變更會保留到清除或套用為止。

7. 選取下列其中一個選項、以檢閱您的變更：
   - **5**：顯示輸出中的編輯內容、這些編輯內容被隔離、僅顯示變更的項目。變更會以綠色（新增）或紅色（刪除）強調顯示、如範例輸出所示：



。**6**：顯示輸出中顯示完整組態的編輯內容。變更會以綠色（新增）或紅色（刪除）強調顯示。

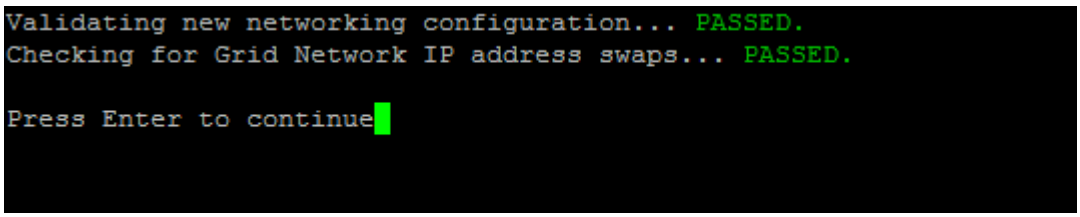
> 某些命令列介面可能會使用刪除線格式顯示新增和刪除內容。正確的顯示取決於您的終端用戶端是否支援必要的VT100轉義序列。

8. 選擇選項* 7*以驗證所有變更。

   這項驗證可確保 Grid 、 Admin 和 Client Networks 的規則（例如不使用重疊的子網路）不會受到違反。

   在此範例中、驗證傳回錯誤。

   在此範例中、驗證已通過。



9. 驗證通過後、請選擇下列其中一個選項：

- **8**：儲存未套用的變更。

  此選項可讓您結束變更IP工具、並在稍後重新啟動、而不會遺失任何未套用的變更。

- * 10*：套用新的網路組態。

10. 如果您選擇選項*10*、請選擇下列其中一個選項：

    - 套用：立即套用變更、必要時自動重新啟動每個節點。

      如果新的網路組態不需要任何實體網路變更、您可以選取*套用*來立即套用變更。必要時、節點會自動重新啟動。此時會顯示需要重新啟動的節點。

    - 階段：下次手動重新啟動節點時套用變更。

      如果您需要變更實體或虛擬網路組態以使新的網路組態正常運作、您必須使用*登臺*選項、關閉受影響的節點、進行必要的實體網路變更、然後重新啟動受影響的節點。如果您選擇*套用*而不先進行這些網路變更、變更通常會失敗。

      如果您使用* st段*選項、則必須在接移後盡快重新啟動節點、以將中斷情況降至最低。

    - * 取消 * ：目前請勿進行任何網路變更。

      如果您不知道所提議的變更需要重新啟動節點、您可以延後變更、將使用者影響降至最低。選取*取消*會返回主功能表、並保留您的變更、以便稍後套用。

      當您選取*套用*或*階段*時、會產生新的網路組態檔、執行資源配置、並以新的工作資訊更新節點。

      在資源配置期間、輸出會在套用更新時顯示狀態。

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

    套用或階段變更後，將根據網格配置變更產生新的復原包。

11. 如果您選擇*階段*、請在資源配置完成後遵循下列步驟：

    a. 進行所需的實體或虛擬網路變更。

       實體網路變更：進行必要的實體網路變更、必要時可安全關閉節點。

    Linux ：如果您是第一次將節點新增至管理網路或用戶端網路、請務必依照中所述新增介面"Linux：新增介面至現有節點"。

    a. 重新啟動受影響的節點。

12. 選取「* 0*」以在變更完成後結束「變更IP」工具。

13. 從網格管理器下載新的復原套件。
    a. 選擇*維護* > 系統 > 恢復包。
    b. 輸入資源配置通關密碼。
14. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成更改節點網路配置後。

暫時更改 **LACP PDU** 速率

若要對裝置中安裝的網路元件執行維護作業（例如昇級 NIC 韌體），您可以檢查目前 LACP PDU 速率設定是否符合 NIC 通訊時序要求。如果需要，您可以非持續地在快速（等待 1 秒）和慢速（等待 30 秒）之間切換 LACP PDU 速率。

> 若要永久變更 LACP PDU 速率，請參閱 "設定網路連結"。

開始之前

- 管理節點已安裝並正在運行。
- 您有 `Passwords.txt`檔案。

步驟

1. 登入主要管理節點：
    a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
    b. 輸入檔案中列出的密碼 `Passwords.txt`。
    c. 輸入以下命令切換到 root ： `su -`
    d. 輸入檔案中列出的密碼 `Passwords.txt`。

    當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 若要檢查目前 LACP PDU 速率設置，請輸入以下命令：

    ```
    run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
    ```
3. 若要暫時變更 LACP PDU 速率，請輸入以下命令：

    ```
    run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
    ```

    在哪裡 `<speed>`是 `fast`或者 `slow`。

下次設備重新啟動時，LACP PDU 速率將恢復到先前的設定。

更改應用裝置節點 **BMC LAN IP** 設定

您可以變更應用裝置節點 BMC 的 LAN IP 設定。

1. 在 Grid Manager 中，前往 節點 > ***grid node*** > **BMC** 設定。
2. 在 LAN IP 設定部分，選擇 靜態 或 **DHCP** 的 IP 指派類型。
3. 輸入 BMC 的 MAC 位址、IPv4 位址（CIDR）和預設閘道。

4. 選擇*保存*。

您也可以使用 `PUT /bmc-configuration/root-password`或 `GET /bmc-configuration/root-password` API 來變更或檢視 BMC LAN IP 設定。

在 StorageGRID 中新增或變更管理網路上的子網路清單

您可以在一或多個節點的管理網路子網路清單中新增、刪除或變更子網路。

開始之前

- 您有 `Passwords.txt`檔案。

您可以新增、刪除或變更子網路至管理網路子網路清單上的所有節點。

> 請勿對任何節點的網格網路、管理網路或用戶端網路使用包含下列 IPv4 位址的子網路：
>
> - 192,168,130,101
> - 192,168,130,121
> - 192,168,131,101
> - 192,168,131,121
> - 192,168,130,102
> - 192,168,130,122
> - 192,168,131,102
> - 192,168,131,122
> - 198.51.100.2
> - 198.51.100.4
>
> 例如，不要對任何節點的網格網路、管理網路或客戶端網路使用下列子網路範圍：
>
> - 192.168.130.0/24，因為此子網路範圍包含 IP 位址 192.168.130.101 和 192.168.130.102
> - 192.168.131.0/24，因為此子網路範圍包含 IP 位址 192.168.131.101 和 192.168.131.102
> - 198.51.100.0/24，因為此子網路範圍包含 IP 位址 198.51.100.2 和 198.51.100.4

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

3. 輸入下列命令以啟動變更 IP 工具： `change-ip`
4. 在提示字元下輸入資源配置通關密碼。

   主功能表隨即出現。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. （可選）限制執行操作的網路/節點。請選擇下列其中一項：
   - 如果您要篩選要執行作業的特定節點、請選擇* 1*來選取要編輯的節點。選取下列其中一個選項：
     - * 1*：單一節點（依名稱選取）
     - * 2 *：單一節點（依站台選取、然後依名稱選取）
     - * 3*：單一節點（依目前IP選取）
     - * 4 *：站台上的所有節點
     - **5**：網格中的所有節點
     - * 0*：返回
   - 允許「全部」保持選取狀態。選擇完成後、主功能表畫面會出現。「選取的節點」欄位會反映您的新選擇、現在所有選取的作業都只會在此項目上執行。
6. 在主功能表上、選取選項以編輯管理網路的子網路（選項* 3*）。
7. 請選擇下列其中一項：
   - 輸入以下命令新增子網路： `add CIDR`
   - 輸入以下命令刪除子網路： `del CIDR`
   - 輸入以下命令來設定子網路清單： `set CIDR`

   對於所有命令、您可以使用下列格式輸入多個位址： `add CIDR, CIDR`

   範例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   您可以使用「向上箭頭」將先前輸入的值重新叫用至目前的輸入提示、然後視需要編輯、以減少所需的輸入量。

   以下輸入範例顯示將子網路新增至管理網路子網路清單：

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

8. 準備好後、輸入* q*返回主功能表畫面。您的變更會保留到清除或套用為止。

> 如果您在步驟 3 中選擇了任何「全部」節點選擇模式，請按下 **Enter**（不含 **q**）以前往清單中的下一個節點。

9. 請選擇下列其中一項：

   - 選擇選項*5*可在隔離的輸出中顯示編輯內容、僅顯示變更的項目。變更會以綠色（新增）或紅色（刪除）反白顯示、如下面的範例輸出所示：

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - 選擇選項*6*可在顯示完整組態的輸出中顯示編輯內容。變更會以綠色（新增）或紅色（刪除）強調顯示。*附註：*某些終端模擬器可能會使用刪除線格式顯示新增和刪除內容。

     當您嘗試變更子網路清單時、會顯示下列訊息：

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

如果您未將NTP和DNS伺服器子網路明確指派給網路、StorageGRID 則會自動建立連線的主機路由（/32）。例如、如果您想要使用/16或/24路由進行DNS或NTP伺服器的傳出連線、您應該刪除自動建立的/32路由、然後新增所需的路由。如果您不刪除自動建立的主機路由、則會在您套用任何變更至子網路清單後保留該路由。

> 雖然您可以使用這些自動探索的主機路由、但一般而言、您應該手動設定DNS和NTP路由、以確保連線能力。

10. 選取選項* 7*以驗證所有階段變更。

    此驗證可確保遵循Grid、Admin和Client Networks的規則、例如使用重疊的子網路。

11. （可選）選擇選項*8*以保存所有分段更改並稍後返回以繼續進行更改。

    此選項可讓您結束變更IP工具、並在稍後重新啟動、而不會遺失任何未套用的變更。

12. 執行下列其中一項：
    - 如果您要清除所有變更而不儲存或套用新的網路組態、請選取選項* 9*。
    - 如果您準備好套用變更並配置新的網路組態、請選取選項* 10*。在資源配置期間、輸出會在套用更新時顯示狀態、如下列輸出範例所示：

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

13. 從網格管理器下載新的復原套件。
    a. 選擇*維護* > 系統 > 恢復包。
    b. 輸入資源配置通關密碼。
14. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成新增或變更子網路清單後。

在 **StorageGRID** 中新增或變更 **Grid Network** 上的子網路清單

您可以使用變更IP工具來新增或變更網格網路上的子網路。

開始之前

- 您有 `Passwords.txt`檔案。

您可以在Grid Network Subnet List（網格網路子網路清單）中新增、刪除或變更子網路。變更會影響網格中所有節點的路由傳送。

如果您僅變更Grid Network Subnet List（網格網路子網路清單）、請使用Grid Manager新增或變更網路組態。否則、如果由於網路組態問題而無法存取Grid Manager、或者您同時執行Grid Network路由變更和其他網路變更、請使用變更IP工具。

請勿對任何節點的網格網路、管理網路或用戶端網路使用包含下列 IPv4 位址的子網路：

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

例如，不要對任何節點的網格網路、管理網路或客戶端網路使用下列子網路範圍：

- 192.168.130.0/24，因為此子網路範圍包含 IP 位址 192.168.130.101 和 192.168.130.102
- 192.168.131.0/24，因為此子網路範圍包含 IP 位址 192.168.131.101 和 192.168.131.102
- 198.51.100.0/24，因為此子網路範圍包含 IP 位址 198.51.100.2 和 198.51.100.4

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

當您以 root 登入時、提示會從變更 `$`為 `#`。

3. 輸入下列命令以啟動變更 IP 工具： `change-ip`
4. 在提示字元下輸入資源配置通關密碼。

   主功能表隨即出現。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. 在主功能表上、選取編輯Grid Network子網路的選項（選項* 4*）。

   網格網路子網路清單的變更為全網格。

6. 請選擇下列其中一項：

   - 輸入以下命令新增子網路： `add CIDR`
   - 輸入以下命令刪除子網路： `del CIDR`
   - 輸入以下命令來設定子網路清單： `set CIDR`

   對於所有命令、您可以使用下列格式輸入多個位址： `add CIDR, CIDR`

   範例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   您可以使用「向上箭頭」將先前輸入的值重新叫用至目前的輸入提示、然後視需要編輯、以減少所需的輸入量。

   以下輸入範例顯示網格網路子網路清單的子網路設定：

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

7. 準備好後、輸入* q*返回主功能表畫面。您的變更會保留到清除或套用為止。
8. 請選擇下列其中一項：
   - 選擇選項*5*可在隔離的輸出中顯示編輯內容、僅顯示變更的項目。變更會以綠色（新增）或紅色（刪除）反白顯示、如下面的範例輸出所示：

```
Grid Network Subnet List (GNSL)

                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                                [      172.30.0.0/21 ]
                                [      172.31.0.0/21 ]
                                [     192.168.0.0/21 ]
Press Enter to continue
```

   - 選擇選項*6*可在顯示完整組態的輸出中顯示編輯內容。變更會以綠色（新增）或紅色（刪除）強調顯示。

     某些命令列介面可能會使用刪除線格式顯示新增和刪除內容。

9. 選取選項* 7*以驗證所有階段變更。

   此驗證可確保遵循Grid、Admin和Client Networks的規則、例如使用重疊的子網路。

10. （可選）選擇選項*8*以保存所有分段更改並稍後返回以繼續進行更改。

    此選項可讓您結束變更IP工具、並在稍後重新啟動、而不會遺失任何未套用的變更。

11. 執行下列其中一項：
    - 如果您要清除所有變更而不儲存或套用新的網路組態、請選取選項* 9*。
    - 如果您準備好套用變更並配置新的網路組態、請選取選項* 10*。在資源配置期間、輸出會在套用更新時顯示狀態、如下列輸出範例所示：

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. 如果您在變更Grid Network時選擇選項* 10*、請選取下列其中一個選項：

    - 套用：立即套用變更、必要時自動重新啟動每個節點。

      如果新的網路組態可與舊的網路組態同時運作、而無需任何外部變更、您可以使用* appli*選項來進行全自動組態變更。

    - 階段：下次重新啟動節點時套用變更。

      如果您需要變更實體或虛擬網路組態以使新的網路組態正常運作、您必須使用*登臺*選項、關閉受影響的節點、進行必要的實體網路變更、然後重新啟動受影響的節點。

      ⓘ 如果您使用 * 階段 * 選項、請在登臺後盡快重新啟動節點、以將中斷情形減至最低。

    - * 取消 * ：目前請勿進行任何網路變更。

      如果您不知道所提議的變更需要重新啟動節點、您可以延後變更、將使用者影響降至最低。選取*取消*會返回主功能表、並保留您的變更、以便稍後套用。

    套用或階段變更後，將根據網格配置變更產生新的復原包。

13. 如果組態因為錯誤而停止、則可使用下列選項：

    - 若要終止 IP 變更程序並返回主功能表、請輸入 **A** 。
    - 若要重試失敗的作業、請輸入* r*。
    - 若要繼續下一個作業、請輸入* c*。

      稍後可從主功能表選取選項* 10*（套用變更）、重試失敗的作業。在所有作業順利完成之前、IP變更程序將不會完成。

    - 如果您必須手動介入（例如重新開機節點）、並且確信工具認為失敗的動作確實成功完成、請輸入* f*將其標示為成功、然後移至下一個作業。

14. 從網格管理器下載新的復原套件。

    a. 選擇*維護* > 系統 > 恢復包。

    b. 輸入資源配置通關密碼。

    ⚠ 復原包檔案必須是安全的，因為它包含可用於從StorageGRID系統取得資料的加密金鑰和密碼。

15. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成新增或變更子網路清單後。

更改 **StorageGRID** 網格中所有節點的 **IP** 位址

如果您需要變更網格中所有節點的網格網路IP位址、則必須遵循此特殊程序。您無法使用變更個別節點的程序來變更全網格網路 IP 。

開始之前

- 您有 `Passwords.txt`檔案。

為了確保網格能順利啟動、您必須同時進行所有變更。

> 此程序僅適用於Grid Network。您無法使用此程序變更管理或用戶端網路上的 IP 位址。

如果您只想變更單一站台節點的 IP 位址和 MTU 、請遵循"變更節點網路組態"指示。

步驟

1. 事先規劃變更IP工具以外所需的變更、例如DNS或NTP的變更、以及單一登入（SSO）組態的變更（若有使用）。

   > 如果新IP位址上的網格無法存取現有的NTP伺服器、請在執行變更IP程序之前、先新增NTP伺服器。

   > 如果新IP位址上的網格無法存取現有的DNS伺服器、請在執行變更IP程序之前、先新增DNS伺服器。

   > 如果您的 StorageGRID 系統已啟用 SSO，且任何信賴方信任都是使用管理節點 IP 位址（而非建議的完整網域名稱）設定的，請在變更 IP 位址後，立即在 Active Directory Federation Services （AD FS） 中更新或重新設定這些信賴方信任。請參閱使用 "OIDC" 或 "SAML" 設定 SSO 的相關資訊。

   > 如有必要、請新增新IP位址的子網路。

2. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
3. 登入主要管理節點：

   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

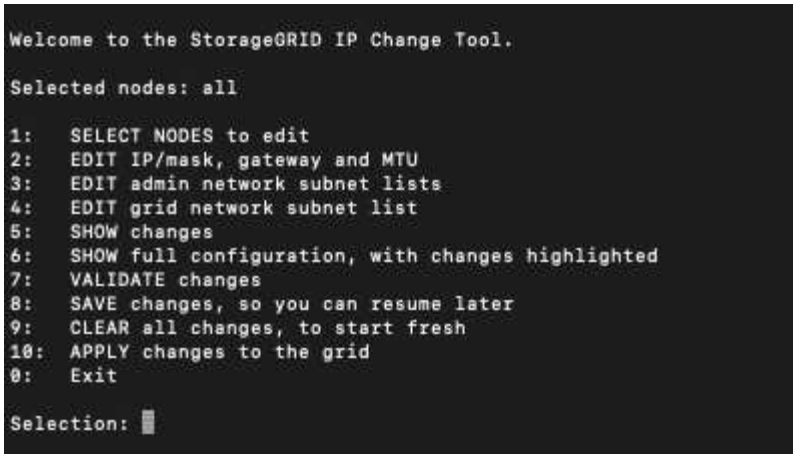
   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

4. 輸入下列命令以啟動變更 IP 工具： `change-ip`
5. 在提示字元下輸入資源配置通關密碼。

   主功能表隨即出現。根據預設， `Selected nodes`欄位設定為 `all`。



6. 在主功能表上、選取* 2*以編輯所有節點的IP/子網路遮罩、閘道和MTU資訊。

   a. 選取「* 1*」以變更「Grid Network（網格網路）」。

      選取之後、提示會顯示節點名稱、網格網路名稱、資料類型（IP/遮罩、閘道或MTU）、 和目前值。

      編輯DHCP設定介面的IP位址、字首長度、閘道或MTU、將會將介面變更為靜態。在DHCP設定的每個介面之前、都會顯示警告。

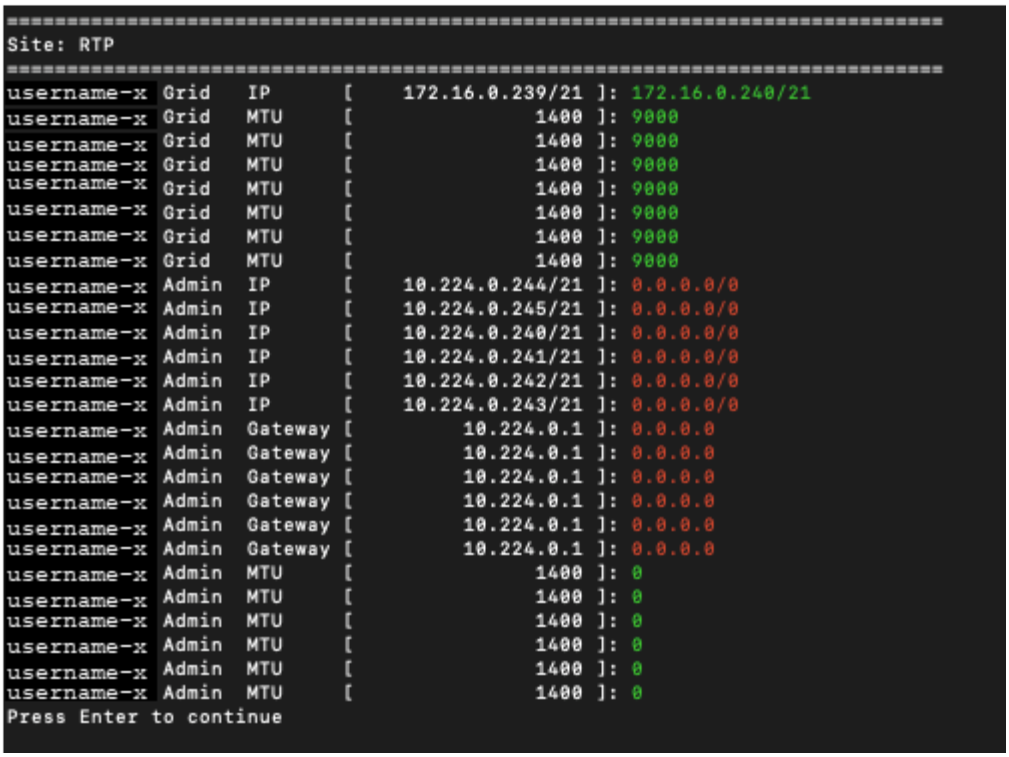
   設定為的介面 `fixed`無法編輯。

   a. 若要設定新值、請以目前值的顯示格式輸入。
   b. 編輯完所有要變更的節點之後、輸入* q*即可返回主功能表。

      您的變更會保留到清除或套用為止。

7. 選取下列其中一個選項、以檢閱您的變更：

   - **5**：顯示輸出中的編輯內容、這些編輯內容被隔離、僅顯示變更的項目。變更會以綠色（新增）或紅色（刪除）強調顯示、如範例輸出所示：



。**6**：顯示輸出中顯示完整組態的編輯內容。變更會以綠色（新增）或紅色（刪除）強調顯示。

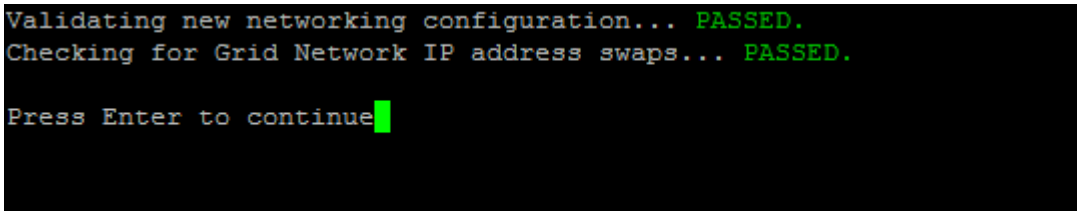
> 某些命令列介面可能會使用刪除線格式顯示新增和刪除內容。正確的顯示取決於您的終端用戶端是否支援必要的VT100轉義序列。

8. 選擇選項* 7*以驗證所有變更。

   這項驗證可確保 Grid Network 的規則（例如不使用重疊的子網路）不會受到違反。

   在此範例中、驗證傳回錯誤。

   在此範例中、驗證已通過。



9. 驗證通過後、請選取 **10** 以套用新的網路組態。

10. 選取*登臺*以在下次重新啟動節點時套用變更。

> 您必須選擇*階段*。請勿手動或選取 * 套用 * 而非 * 階段 * 來執行滾動重新啟動；網格將無法成功啟動。

11. 完成變更後、請選取* 0*以結束變更IP工具。
12. 同時關閉所有節點。

> 必須關閉整個網格、以便同時關閉所有節點。

13. 進行所需的實體或虛擬網路變更。
14. 確認所有網格節點都已關閉。
15. 開啟所有節點的電源。
16. 網格成功啟動後：
    a. 如果您新增了NTP伺服器、請刪除舊的NTP伺服器值。
    b. 如果您新增了DNS伺服器、請刪除舊的DNS伺服器值。
17. 從網格管理器下載新的復原套件。
    a. 選擇*維護* > 系統 > 恢復包。
    b. 輸入資源配置通關密碼。
18. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成更改 IP 位址後。

相關資訊

- "新增或變更Grid Network上的子網路清單"
- "關閉網格節點"

新增介面至現有節點

在 **StorageGRID** 中將管理或用戶端介面新增至 **Linux** 節點

請使用這些步驟、在安裝管理網路或用戶端網路之後、將介面新增至Linux節點。

如果在安裝期間未在 Linux 主機上的節點設定檔中設定 ADMIN_NETWORK_TARGET 或 CLIENT_NETWORK_TARGET，請使用此程序新增介面。有關節點配置文件的更多信息，請參閱"在基於軟體的節點上安裝StorageGRID"。

您可以在裝載需要新網路指派之節點的Linux伺服器上執行此程序、而非在節點內部執行。此程序僅會將介面新增至節點；如果您嘗試指定任何其他網路參數、則會發生驗證錯誤。

若要提供定址資訊、您必須使用變更IP工具。請參閱。 "變更節點網路組態"

步驟

1. 登入裝載節點的Linux伺服器。
2. 編輯節點組態檔案： `/etc/storagegrid/nodes/node-name.conf`。

請勿指定任何其他網路參數、否則將導致驗證錯誤。

a. 新增新網路目標的項目。例如：

```
CLIENT_NETWORK_TARGET = bond0.3206
```

b. 選用：新增MAC位址項目。例如：

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. 執行節點驗證命令：

```
sudo storagegrid node validate node-name
```

4. 解決所有驗證錯誤。
5. 執行節點重新載入命令：

```
sudo storagegrid node reload node-name
```

在 StorageGRID 中將主幹或存取介面新增至 Linux 節點

您可以在安裝Linux節點之後、將額外的主幹或存取介面新增至該節點。您新增的介面會顯示在「VLAN介面」頁面和「HA群組」頁面上。

開始之前

- 您可以訪問"StorageGRID安裝說明"在您的 Linux 平台上。
- 您有 `Passwords.txt`檔案。
- 您有 "特定存取權限"。

當軟體升級、還原程序或擴充程序作用中時、請勿嘗試將介面新增至節點。

關於這項工作

安裝節點之後、請使用這些步驟將一個或多個額外介面新增至Linux節點。例如、您可能想要將主幹介面新增至管理或閘道節點、以便使用VLAN介面來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、以便在高可用度（HA）群組中使用。

如果您新增主幹介面、則必須在StorageGRID 功能鏈路的資訊鏈路中設定VLAN介面。如果您新增存取介面、可以直接將介面新增至 HA 群組、而不需要設定 VLAN 介面。

當您新增介面時、節點會在短時間內無法使用。您應該一次在一個節點上執行此程序。

步驟

1. 登入裝載節點的Linux伺服器。
2. 使用vim或pico等文字編輯器、編輯節點組態檔案：

```
/etc/storagegrid/nodes/node-name.conf
```

3. 將項目新增至檔案、以指定您要新增至節點的每個額外介面名稱及說明（可選）。請使用此格式。

   `INTERFACE_TARGET_nnnn=value`

   針對 _nnnn 、為您要新增的每個項目指定唯一的編號 `INTERFACE_TARGET`。

   針對_value_、指定裸機主機上實體介面的名稱。接著、您可以選擇性地新增一個逗號、並提供介面說明、該介面會顯示在「VLAN介面」頁面和「HA群組」頁面上。

   例如：

   ```
   INTERFACE_TARGET_0001=ens256, Trunk
   ```

   請勿指定任何其他網路參數、否則將導致驗證錯誤。

4. 執行下列命令、驗證您對節點組態檔的變更：

   `sudo storagegrid node validate node-name`

   在繼續下一步之前、請先解決任何錯誤或警告。

5. 執行下列命令以更新節點的組態：

   `sudo storagegrid node reload node-name`

完成後

- 如果您新增了一或多個主幹介面、請前往"設定VLAN介面"為每個新的父介面設定一個或多個 VLAN 介面。
- 如果您新增一或多個存取介面、請前往"設定高可用度群組"、將新介面直接新增至 HA 群組。

在 **StorageGRID** 中新增主幹或存取介面至 **VMware** 節點

您可以在安裝節點之後、將主幹或存取介面新增至VM節點。您新增的介面會顯示在「VLAN介面」頁面和「HA群組」頁面上。

開始之前

- 您可以造訪以下說明"在 VMware 平台上安裝 StorageGRID"。
- 您擁有管理節點和閘道節點VMware虛擬機器。
- 您的網路子網路未被用作 Grid 、 Admin 或 Client Network 。
- 您有 `Passwords.txt`檔案。
- 您有 "特定存取權限"。

當軟體升級、還原程序或擴充程序作用中時、請勿嘗試將介面新增至節點。

關於這項工作

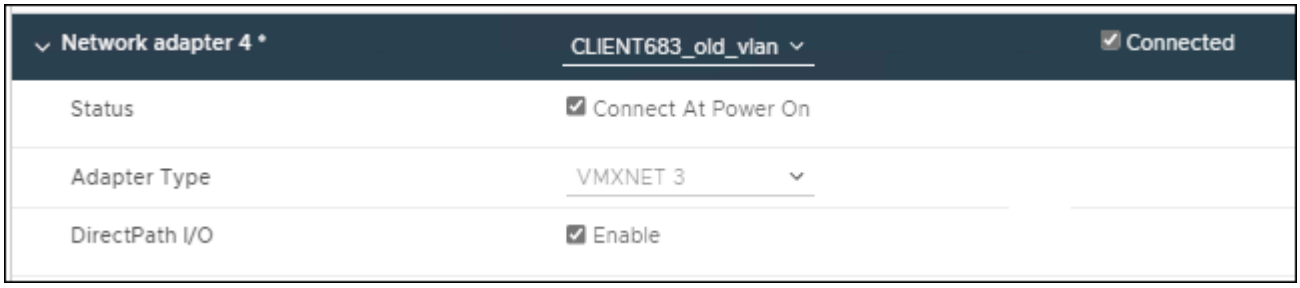
安裝節點之後、請使用這些步驟將一個或多個額外介面新增至VMware節點。例如、您可能想要將主幹介面新增至管理或閘道節點、以便使用VLAN介面來分隔屬於不同應用程式或租戶的流量。或者、您可能想要新增存取介面、以便在高可用度（HA）群組中使用。

如果您新增主幹介面、則必須在StorageGRID 功能鏈路的資訊鏈路中設定VLAN介面。如果您新增存取介面、可以直接將介面新增至 HA 群組、而不需要設定 VLAN 介面。

新增介面時、節點可能會暫時無法使用。

步驟

1. 在vCenter中、將新的網路介面卡（輸入VMXNET3）新增至管理節點和閘道節點VM。選中 * Connected *（已連接 * ）和 * Connect at Power On* （開機時連接）複選框。



2. 使用SSH登入管理節點或閘道節點。
3. 用於 `ip link show`確認偵測到新的網路介面 ens256 。

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

完成後

- 如果您新增了一或多個主幹介面、請前往"設定VLAN介面"為每個新的父介面設定一個或多個 VLAN 介面。
- 如果您新增一或多個存取介面、請前往"設定高可用度群組"、將新介面直接新增至 HA 群組。

在 StorageGRID 中設定 DNS 伺服器

您可以新增、更新及移除 DNS 伺服器、以便使用完整網域名稱（ FQDN ）主機名稱、而非 IP 位址。

若要在指定外部目的地的主機名稱時使用完整網域名稱（ FQDN ）而非 IP 位址、請指定您要使用的每個 DNS 伺服器的 IP 位址。這些項目用於 AutoSupport 、警示電子郵件、 SNMP 通知、平台服務端點、雲端儲存池、還有更多。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有要設定的 DNS 伺服器 IP 位址。

關於這項工作

若要確保正常運作、請指定兩或三個 DNS 伺服器。如果您指定超過三個、可能只會使用三個、因為某些平台的已知作業系統限制。如果您在環境中有路由限制、則可"自訂 DNS 伺服器清單"讓個別節點（通常是站台上的所有節點）使用最多三個 DNS 伺服器的不同組別。

如有可能、請使用每個站台都能在本機存取的 DNS 伺服器、以確保某個著陸站台可以解析外部目的地的 FQDN 。

新增 **DNS** 伺服器

請依照下列步驟新增 DNS 伺服器。

步驟

1. 選擇*維護* > 網路 > **DNS** 伺服器。
2. 選取 * 新增其他伺服器 * 以新增 DNS 伺服器。
3. 選擇*保存*。

修改 **DNS** 伺服器

請依照下列步驟修改 DNS 伺服器。

步驟

1. 選擇*維護* > 網路 > **DNS** 伺服器。
2. 選取您要編輯的伺服器名稱 IP 位址、然後進行必要的變更。
3. 選擇*保存*。

刪除 **DNS** 伺服器

請依照下列步驟刪除 DNS 伺服器的 IP 位址。

步驟

1. 選擇*維護* > 網路 > **DNS** 伺服器。
2. 選擇 IP 位址旁的刪除圖示 ✕。
3. 選擇*保存*。

修改單一 **StorageGRID** 節點的 **DNS** 組態

您可以執行指令碼、以不同方式為每個網格節點設定 DNS 、而不是針對整個部署進行全域 DNS 設定。

一般來說，您應該使用網格管理員上的 維護 > 網路 > **DNS** 伺服器 選項來設定 DNS 伺服器。僅當您需要為不同的網格節點使用不同的 DNS 伺服器時才使用下列腳本。

步驟

1. 預設情況下，外部 SSH 存取是被阻止的。如果需要，"暫時允許訪問" 。
2. 登入主要管理節點：
   a. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
   e. 將SSH私密金鑰新增至SSH代理程式。輸入： `ssh-add`
   f. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。
3. [[log_in_to 節點] 登入您要使用自訂 DNS 組態更新的節點： `ssh node_IP_address`
4. 執行 DNS 設定指令碼： `setup_resolv.rb.`

   指令碼會以支援的命令清單回應。

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

5. 新增為您的網路提供網域名稱服務的伺服器的 IPv4 位址： `add <nameserver IP_address>`
6. 重複此 `add nameserver`命令以新增名稱伺服器。
7. 請依照提示輸入其他命令的指示進行。
8. 儲存變更並結束應用程式： `save`
9. [[close （關閉） cmd ： shell ）] 關閉伺服器上的命令 Shell ： `exit`
10. 對於每個網格節點，重複從到關閉命令Shell的步驟登入節點。
11. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入： `ssh-add -D`

12. 如果您允許外部 SSH 訪問，"阻止訪問"當您完成修改 DNS 配置後。

在 **StorageGRID** 中管理 **NTP** 伺服器

您可以新增、更新或移除網路時間傳輸協定（ NTP ）伺服器、以確保資料在 StorageGRID 系統的網格節點之間準確同步。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您有要設定的 NTP 伺服器的 IPv4 位址。

StorageGRID 如何使用 **NTP**

StorageGRID 系統使用網路時間傳輸協定（ NTP ）來同步網格中所有網格節點之間的時間。

在每個站台StorageGRID 、至少有兩個節點被指派主要的NTP角色。它們會同步處理至建議的最少四個外部時間來源、最多六個外部時間來源、並彼此同步。非主要NTP節點的StorageGRID 每個節點都會做為NTP用戶端、並與這些主要NTP節點同步。

外部 NTP 伺服器會連線到先前指派主要 NTP 角色的節點。因此、建議至少指定兩個具有主要 NTP 角色的節點。

NTP 伺服器準則

請遵循以下準則、避免發生時間問題：

- 外部 NTP 伺服器會連線到先前指派主要 NTP 角色的節點。因此、建議至少指定兩個具有主要 NTP 角色的節點。
- 請確定每個站台至少有兩個節點可以存取至少四個外部 NTP 來源。如果站台只有一個節點可以連線至NTP來源、則當該節點當機時、就會發生計時問題。此外、將每個站台的兩個節點指定為主要NTP來源、可確保站台與網格的其他部分隔離時、能確保準確的時間安排。
- 指定的外部NTP伺服器必須使用NTP傳輸協定。您必須指定階層3或更高層級的NTP伺服器參考資料、以避免時間浪費問題。

> 為生產級 StorageGRID 安裝指定外部 NTP 來源時，請勿使用 Windows Server 2016 之前的 Windows 版本上的 Windows 時間 （W32Time） 服務。舊版 Windows 上的時間服務精確度不足，Microsoft 不支援在高精度環境（包括 StorageGRID）中使用該服務。如需詳細資訊，請參閱 "支援高精度時間的邊界"。

設定 **NTP** 伺服器

請依照下列步驟新增、更新或移除 NTP 伺服器。

步驟

1. 選擇*維護* > 網路 > **NTP** 伺服器。

2. 在「伺服器」區段中、視需要新增、更新或移除 NTP 伺服器項目。

   您至少應包含四部 NTP 伺服器、最多可指定六部伺服器。

3. 輸入 StorageGRID 系統的資源配置密碼、然後選取 * 儲存 * 。

   頁面會停用、直到組態更新完成為止。

   如果所有 NTP 伺服器在您儲存新的 NTP 伺服器之後都未通過連線測試、請勿繼續。聯絡技術支援。

解決 **NTP** 伺服器問題

如果您在安裝期間遇到最初指定NTP伺服器的穩定性或可用度問題、您可以StorageGRID 新增其他伺服器、或更新或移除現有伺服器、以更新該系統使用的外部NTP來源清單。

恢復隔離的 **StorageGRID** 節點的網路連線

在某些情況下、一或多個節點群組可能無法與網格的其他部分聯絡。例如、站台或網格範圍內的 IP 位址變更可能會導致隔離節點。

關於這項工作

節點隔離以下列方式表示：

- 警示、例如 * 無法與節點 * 通訊（ * 警示 * > * 目前 * ）
- 與連線相關的診斷（支援 > 工具 > 診斷）

隔離節點的部分後果包括：

- 如果隔離多個節點、您可能無法登入或存取Grid Manager。
- 如果隔離多個節點、則租戶管理程式儀表板上顯示的儲存使用量和配額值可能已過期。當網路連線恢復時、總計將會更新。

若要解決隔離問題、您可以在每個隔離節點或群組中的一個節點（子網路中不含主要管理節點的所有節點）上執行命令列公用程式、這些節點與網格隔離。公用程式會在網格中提供節點的非隔離節點IP位址、讓隔離的節點或節點群組能夠再次聯絡整個網格。

如果網路中停用多點傳送網域名稱系統（ mDNS ）、您可能必須在每個隔離節點上執行命令列公用程式。

步驟

只有部分服務離線或回報通訊錯誤時、此程序不適用。

1. 存取節點並檢查 `/var/local/log/dynip.log`隔離訊息。

   例如：

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

如果您使用的是VMware主控台、它會顯示一則訊息、指出該節點可能已隔離。

在 Linux 部署中、隔離訊息會出現在 `/var/log/storagegrid/node/<nodename>.log`檔案中。

2. 如果隔離訊息是重複且持續的、請執行下列命令：

   `add_node_ip.py <address>`

   其中 `<address>`是連線至網格的遠端節點的 IP 位址。

```
# /usr/sbin/add_node_ip.py  10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. 針對先前隔離的每個節點、驗證下列項目：
   - 節點的服務已啟動。
   - 執行命令後、動態 IP 服務的狀態為「執行中」 `storagegrid-status`。
   - 在「節點」頁面上、節點不再與網格的其他部分中斷連線。

如果執行 `add_node_ip.py`命令無法解決問題、可能還有其他網路問題需要解決。

主機和中介軟體程序

將 StorageGRID 節點遷移到新的 Linux 主機

您可以將一個或多個 StorageGRID 節點從一個 Linux 主機（ _ 來源主機 _ ）移轉到另一個 Linux 主機（ _ 目標主機 _ ）、以執行主機維護、而不會影響網格的功能或可用度。

例如、您可能想要移轉節點、以執行作業系統修補和重新開機。

開始之前

- 您計劃將StorageGRID部署包含遷移支援。看"節點容器移轉需求" 。
- 目標主機已準備好用於 StorageGRID 。
- 共享儲存設備用於所有的每節點儲存磁碟區
- 網路介面在主機之間具有一致的名稱。

在正式作業部署中、請勿在單一主機上執行多個儲存節點。使用每個儲存節點的專屬主機、可提供隔離的故障網域。

其他類型的節點（例如管理節點或閘道節點）可部署在同一部主機上。不過、如果您有多個相同類型的節點（例如兩個閘道節點）、請勿在同一部主機上安裝所有執行個體。

從來源主機匯出節點

首先、請關閉網格節點、然後從來源 Linux 主機匯出。

在 _ 來源主機 _ 上執行下列命令。

步驟

1. 取得目前在來源主機上執行的所有節點狀態。

   ```
   sudo storagegrid node status all
   ```

   輸出範例：

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. 識別您要移轉的節點名稱、並在其「執行狀態」執行時停止該節點。

   ```
   sudo storagegrid node stop DC1-S3
   ```

   輸出範例：

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. 從來源主機匯出節點。

   ```
   sudo storagegrid node export DC1-S3
   ```

   輸出範例：

   ```
   Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
   Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
   want to import it again.
   ```

4. 記下 `import`輸出中建議的命令。

   您將在下一步在目標主機上執行此命令。

在目標主機上匯入節點

從來源主機匯出節點之後、您將匯入並驗證目標主機上的節點。驗證可確認節點存取的區塊儲存設備和網路介面裝置與來源主機相同。

在 *target host* 上執行下列命令。

步驟

1. 匯入目標主機上的節點。

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   輸出範例：

   ```
   Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
   You should run 'storagegrid node validate DC1-S3'
   ```

2. 驗證新主機上的節點組態。

   ```
   sudo storagegrid node validate DC1-S3
   ```

   輸出範例：

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. 如果發生任何驗證錯誤、請在啟動移轉的節點之前先解決這些錯誤。

   有關故障排除信息，請參閱StorageGRID"安裝說明"適用於您的 Linux 作業系統。

啟動移轉的節點

驗證移轉的節點之後、您可以在 *target host* 上執行命令來啟動節點。

步驟

1. 在新主機上啟動節點。

   ```
   sudo storagegrid node start DC1-S3
   ```

2. 登入 Grid Manager 、確認節點狀態為綠色且無警示。

驗證節點狀態是否為綠色、可確保移轉的節點已完全重新啟動並重新加入網格。如果狀態不是綠色、請勿移轉任何其他節點、以免有多個節點無法運作。

3. 如果您無法存取Grid Manager、請等待10分鐘、然後執行下列命令：

   ```
   sudo storagegrid node status _node-name
   ```

   確認移轉節點的執行狀態為「執行中」。

在 **StorageGRID** 中配置 **VMware** 虛擬機器以自動重新啟動

如果虛擬機器在VMware vSphere Hypervisor重新啟動後未重新啟動、您可能需要設定虛擬機器以自動重新啟動。

如果您注意到在恢復網格節點或執行其他維護程序時、虛擬機器並未重新啟動、則應執行此程序。

步驟

1. 在VMware vSphere Client樹狀結構中、選取尚未啟動的虛擬機器。
2. 在虛擬機器上按一下滑鼠右鍵、然後選取*「Power On*（開機*）」。
3. 設定VMware vSphere Hypervisor以在未來自動重新啟動虛擬機器。

恢復或更換節點

StorageGRID 節點恢復的警告和注意事項

如果網格節點故障、您必須盡快恢復。開始之前、您必須檢閱所有節點還原的警告和考量事項。

由多個節點共同運作的分散式系統。StorageGRID請勿使用磁碟快照來還原網格節點。請參閱每種節點類型的恢復與維護程序。

如果整個StorageGRID站點發生故障，請聯絡技術支援。技術支援將與您合作制定並執行網站復原計劃，以最大限度地恢復資料量並滿足您的業務目標。請參閱"技術支援如何恢復網站" 。

儘快恢復故障網格節點的原因包括：

- 故障的網格節點可減少系統和物件資料的備援、讓您在其他節點故障時容易遭受永久性資料遺失的風險。
- 故障的網格節點可能會影響日常作業的效率。
- 故障的網格節點可能會降低監控系統作業的能力。
- 如果有嚴格的ILM規則、故障的網格節點可能會導致500個內部伺服器錯誤。
- 如果網格節點未立即恢復、恢復時間可能會增加。例如、可能需要先清除佇列、才能完成恢復。

請務必遵循所還原之特定類型網格節點的還原程序。主要或非主要管理節點、閘道節點、應用裝置節點和儲存節點的恢復程序各不相同。

恢復網格節點的先決條件

恢復網格節點時、會假設下列所有情況：

- 故障的實體或虛擬硬體已被更換及設定。
- 替換應用裝置上的 StorageGRID 應用裝置安裝程式版本與 StorageGRID 系統的軟體版本相符、如所述 "驗StorageGRID 證並升級版本的應用程式"。
- 如果您要恢復的網格節點不是主要管理節點，則正在恢復的網格節點與管理恢復程序的管理節點之間必須存在連線。
- 如果要恢復設備儲存節點，則必須在設備安裝期間指定與原始設備相同的儲存類型（組合、僅元資料或僅資料）。如果指定不同的儲存類型，復原將失敗，並且需要使用指定的正確儲存類型重新安裝裝置。

如果託管多個網格節點的伺服器故障、則節點恢復順序

如果託管多個網格節點的伺服器發生故障，您可以按任意順序恢復節點。但是，如果發生故障的伺服器託管著主要管理節點，且不存在非主要管理節點，則必須先恢復主要管理節點。

恢復節點的IP位址

請勿嘗試使用目前指派給任何其他節點的 IP 位址來恢復節點。部署新節點時、請使用故障節點的目前IP位址或未使用的IP位址。

如果您使用新的IP位址來部署新節點、然後恢復該節點、新的IP位址將繼續用於恢復的節點。如果您想要回復到原始IP位址、請在恢復完成後使用變更IP工具。

收集 StorageGRID 網格節點恢復所需的材料

在執行維護程序之前、您必須確保擁有必要的資料來恢復故障的網格節點。

項目	附註
安裝歸檔StorageGRID	如果您需要恢復網格節點、則需要下載StorageGRID 安裝文件針對您的平台進行。 • 注意： * 如果您要在儲存節點上恢復故障的儲存磁碟區、則不需要下載檔案。
服務筆記型電腦	服務型筆記型電腦必須具備下列項目： • 網路連接埠 • SSH用戶端（例如Putty） • "支援的網頁瀏覽器"
恢復包 `.zip`文件	取得最新恢復包的副本 `.zip`文件： `sgws-recovery-package-id-revision.zip` 的內容 `.zip`每次修改系統時都會更新檔案。進行此類變更後，您需要將最新版本的復原包儲存在安全的位置。使用最新的副本來恢復電網故障。 登入任何管理節點時，使用網格管理器下載復原包。選擇*維護* > 系統 > 恢復包。 如果您無法存取網格管理器，您可以在包含 ADC 服務的某些儲存節點上找到復原包的加密副本。在每個儲存節點上，檢查復原包的此位置：`/var/local/install/sgws-recovery-package-*grid-id-revision*.zip.gpg`使用修訂號最高的恢復包。
`Passwords.txt`檔案	包含在命令列上存取網格節點所需的密碼。包含在恢復包中。
資源配置通關密碼	當StorageGRID 首次安裝此功能時、系統會建立並記錄密碼。資源配置複雜密碼不在 `Passwords.txt`檔案中。
您平台的最新文件	如需文件、請前往平台廠商的網站。 如需目前支援的平台版本，請參閱 "NetApp 互通性對照表工具"。

下載並解壓縮StorageGRID 安裝檔案

[[download-and -Extract 安裝檔案 -recover]]

下載軟體並解壓縮檔案"在儲存節點上恢復故障的儲存磁碟區"、除非您是。

您必須使用StorageGRID 目前在網格上執行的版本。

步驟

1. 判斷目前安裝的軟體版本。從Grid Manager頂端、選取說明圖示、然後選取*關於*。
2. 前往 "NetApp下載頁StorageGRID 面"。
3. 選取StorageGRID 目前在網格上執行的版本的功能。

   StorageGRID 軟體版本的格式如下： `11.x.y`。

4. 以您NetApp帳戶的使用者名稱和密碼登入。
5. 閱讀終端使用者授權合約、選取核取方塊、然後選取 * 接受並繼續 * 。
6. 在下載頁面的 * 安裝 StorageGRID * 欄中、選取 `.tgz`適用於您平台的或 `.zip`檔案。

   安裝歸檔檔檔案中顯示的版本必須符合目前安裝的軟體版本。

   如果您執行的是 Windows 、請使用 `.zip`檔案。

平台	安裝歸檔
紅帽企業版	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu或DEBIANOR應用裝置	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. 下載並解壓縮歸檔檔案。
8. 根據您的平台和需要還原的網格節點，跳至適合您平台的部分來選擇您需要的檔案。

   每個平台步驟中所列的路徑、都是相對於歸檔檔案所安裝的頂層目錄。

9. 如果你正在恢復"基於軟體的節點"，選擇相應的文件：

紅帽企業版

路徑和檔案名稱	說明
	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	不提供產品任何支援權利的免費授權。
	用於在 RHEL 主機上安裝 StorageGRID 節點映像的 RPM 套件。
	用於在 RHEL 主機上安裝 StorageGRID 主機服務的 RPM 套件。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行 Ping 聯合整合。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	範例 Ansible 角色和教戰手冊、用於設定 StorageGRID 容器部署的 RHEL 主機。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。

路徑和檔案名稱	說明
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

Ubuntu或DEBIAN

路徑和檔案名稱	說明
每個問題/讀我檔案	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	非正式作業的NetApp授權檔案、可用於測試及概念驗證部署。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝不含節點的映像。
	檔案的 MD5 Checksum `/debs/storagegrid-webscale-images-version-SHA.deb` 。
	Deb套件、用於在StorageGRID Ubuntu或Debian主機上安裝支援功能主機服務。
部署指令碼工具	說明
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入時、您可用來登入Grid Management API的Python指令碼範例。您也可以使用此指令碼來進行 Ping 聯合整合。
	用於指令碼的範例組態檔 `configure-storagegrid.py`。
	用於指令碼的空白組態檔 `configure-storagegrid.py`。

路徑和檔案名稱	說明
/扣款/額外費用/可選	範例Ansible角色與方針、可用來設定Ubuntu或Debian主機以StorageGRID 進行列舉容器部署。您可以視需要自訂角色或方針。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
/debs/storagegRID -soaut-azure.js	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

VMware

路徑和檔案名稱	說明
/vSphere/README	說明StorageGRID 包含在更新檔中的所有檔案的文字檔。
	不提供產品任何支援權利的免費授權。
/vSphere/NetApp-SG-version -SHA-vmdk	用來做為建立網格節點虛擬機器範本的虛擬機器磁碟檔案。
/vSphere/vSphere-primer-admin.OVF ./vSphere/vSphere-prime-admin.mf	開放式虛擬化格式模板文件(`.mf`)（`.ovf`和清單文件），用於部署主管理節點。
/vSphere/vSphere-non-prime-admin.OVF ./vSphere/vSphere-non-prime-admin.mf	模板文件(`.mf`)（`.ovf`和清單文件），用於部署非主管理員節點。
/vSphere/vSphere-gateway.OVF ./vSphere/vSphere-gateway.mf	模板文件(`.mf`)（`.ovf`和清單文件），用於部署網關節點。
/vSphere/vSphere-storage。OVF ./vSphere/vSphere-storage	模板文件(`.mf`)（`.ovf`和清單文件），用於部署基於虛擬機的存儲節點。
部署指令碼工具	說明

路徑和檔案名稱	說明
	Bash Shell指令碼、用於自動化虛擬網格節點的部署。
	用於指令碼的範例組態檔 `deploy-vsphere-ovftool.sh`。
	Python指令碼、用於自動化StorageGRID 組態的功能。
	Python指令碼、用於自動化StorageGRID 設定不必要的應用程式。
	啟用單一登入（ SSO ）時、您可以使用 Python 指令碼範例登入 Grid Management API 。您也可以使用此指令碼來進行 Ping 聯合整合。
/vSphere/configure-storagegrid、same.json	用於指令碼的範例組態檔 `configure-storagegrid.py`。
/vSphere/configure-storagegrid、blank.json	用於指令碼的空白組態檔 `configure-storagegrid.py`。
	使用 Active Directory 或 Ping 聯合啟用單一登入（ SSO ）時、可以用來登入 Grid Management API 的 Python 指令碼範例。
	由搭配 Python 指令碼所呼叫的輔助程式指令碼 `storagegrid-ssoauth-azure.py`、用於執行與 Azure 的 SSO 互動。
/vSphere/Extras / API架構	API架構StorageGRID 。 • 注意 * ：在執行升級之前、如果您沒有非正式作業的 StorageGRID 環境來進行升級相容性測試、您可以使用這些架構來確認您為使用 StorageGRID 管理 API 所撰寫的任何程式碼、都與新的 StorageGRID 版本相容。

10. 如果您要還原StorageGRID 以應用程式為基礎的系統、請選取適當的檔案。

對於設備安裝，僅當您需要避免網路流量時才需要這些檔案。設備可以從您執行復原過程的管理節點下載所需的檔案。

路徑和檔案名稱	說明
	DEB套件可在StorageGRID 您的應用裝置上安裝不含節點的影像。
	檔案的 MD5 Checksum `/debs/storagegridwebscale-images-version-SHA.deb` 。

選擇 StorageGRID 節點還原程序

選擇與發生故障的節點類型相對應的正確恢復程序。

網格節點	恢復程序
儲存節點	儲存節點恢復程序取決於故障類型。 "從儲存節點故障中恢復"
管理節點	管理節點程序取決於您是否需要恢復主管理節點或非主管理節點。 "從管理節點故障中恢復"
閘道節點	"從閘道節點故障中恢復"
歸檔節點	"從歸檔節點故障中恢復（ StorageGRID 11.8 doc 網站）"

如果託管多個網格節點的伺服器發生故障，您可以以任意順序恢復這些節點。但是，如果發生故障的伺服器託管著主要管理節點，且不存在其他非主要管理節點，則必須先恢復主要管理節點。先恢復主要管理節點可防止其他節點的恢復因嘗試聯繫主要管理節點而停滯。如果存在非主要管理節點，您也可以使用它來恢復其他節點，使這些節點的恢復無需聯繫主要管理節點即可繼續進行。

從儲存節點故障中恢復

從 StorageGRID 儲存節點故障中恢復

恢復故障儲存節點的程序取決於故障類型和故障儲存節點的類型。

使用此表格選取故障儲存節點的恢復程序。

問題	行動	附註
多個儲存節點發生故障。	聯絡技術支援。	如果多個儲存節點發生故障，技術支援必須協助進行恢復，以防止 Cassandra 資料庫出現不一致，進而導致資料遺失。可能需要執行站台恢復程序。 技術支援可以確定何時可以安全地開始恢復第二個儲存節點。 注意：如果某個站台上有多個包含 ADC 服務的儲存節點發生故障，則該站台所有待處理的平台服務要求都將遺失。
站台上有多個儲存節點發生故障或整個站台發生故障。	聯絡技術支援。可能需要執行站台恢復程序。	技術支援人員將評估您的情況、並制定恢復計畫。請參閱。 "技術支援如何恢復網站"
應用裝置儲存節點故障。	"恢復應用裝置儲存節點"	應用裝置儲存節點的恢復程序與所有故障相同。
一或多個儲存磁碟區發生故障、但系統磁碟機仍未受損	"從系統磁碟機不受影響的儲存磁碟區故障中恢復"	此程序適用於軟體型儲存節點。
系統磁碟機故障。	"從系統磁碟機故障中恢復"	節點更換程序取決於部署平台、以及是否有任何儲存磁碟區也發生故障。

部分StorageGRID 還原程序會使用Reaper來處理Cassandra的修復作業。一旦相關或必要的服務開始、系統就會自動進行修復。您可能會注意到指令碼輸出中提到「 reaper 」或「 Cassandra repair 」。如果您看到指出修復失敗的錯誤訊息、請執行錯誤訊息中指出的命令。

恢復應用裝置儲存節點

恢復 **StorageGRID** 應用裝置儲存節點的警告

無論StorageGRID 是從系統磁碟機遺失或僅從儲存磁碟區遺失中恢復、恢復故障的故障的功能相同。

如果多個儲存節點發生故障（或離線），請聯絡技術支援。請勿執行以下恢復程序。可能會發生資料遺失。有關詳細信息，請參閱"技術支援如何恢復網站" 。

如果ILM規則設定為僅儲存一個複寫複本、且複本存在於故障的儲存磁碟區、您將無法恢復物件。

如需硬體維護程序（例如更換控制器或重新安裝 SANtricity OS 的說明），請參閱 "儲存設備的維護指示"。

準備 **StorageGRID** 應用裝置儲存節點以進行重新安裝

恢復應用裝置儲存節點時、您必須先準備好應用裝置以重新安裝StorageGRID 還原軟體。

步驟

1. 登入故障儲存節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 準備應用裝置儲存節點以安裝 StorageGRID 軟體。 `sgareinstall`
3. 當系統提示您繼續時、請輸入： `y`

   設備會重新開機、SSH工作階段也會結束。雖然有時您可能需要等待30分鐘、但使用起來通常需要5分鐘才能StorageGRID 使用《不知如何使用的應用程式」。

   請勿嘗試透過循環電源或以其他方式重設應用裝置來加速重新開機。您可能會中斷自動 BIOS 、 BMC 或其他韌體升級。

   將重設此功能、儲存節點上的資料將無法再存取。StorageGRID在原始安裝程序期間所設定的IP位址應保持不變；不過、建議您在程序完成時確認。

   執行命令後 `sgareinstall`、所有 StorageGRID 提供的帳戶、密碼和 SSH 金鑰都會移除、並產生新的主機金鑰。

開始**StorageGRID** 安裝應用程式

若要在StorageGRID 應用裝置儲存節點上安裝功能、請使用StorageGRID 產品隨附的《產品安裝程式》。

開始之前

- 應用裝置已安裝在機架中、連接至您的網路、並已開啟電源。
- 已使用StorageGRID 《整套應用程式安裝程式》為應用裝置設定網路連結和IP位址。
- 您知道以下其中一個管理節點的 IP 位址：
  - StorageGRID 網格的主要管理節點
  - 非主要管理節點（如果可用）
- 列出在《IP組態》頁面StorageGRID 上的所有Grid Network子網路、均已在主要管理節點的Grid Network Subnet List（網格網路子網路清單）中定義。

- 您已依照儲存設備的安裝指示完成這些必要工作。請參閱。 "硬體安裝快速入門"
- 您使用的是"支援的網頁瀏覽器"。
- 您知道指派給應用裝置中運算控制器的其中一個IP位址。您可以使用管理網路（控制器上的管理連接埠1）、網格網路或用戶端網路的IP位址。

關於這項工作

若要在StorageGRID 應用裝置儲存節點上安裝功能：

- 您需要指定主要管理節點的 IP 位址。如果主要管理節點無法使用，則需要指定非主要管理節點的 IP 位址（如果可用）。您還需要確認節點的主機名稱（系統名稱）。
- 您可以開始安裝、並在磁碟區已設定且已安裝軟體時等待。

> 恢復設備儲存節點時，使用與原始設備相同的儲存類型（組合、僅元資料或僅資料）重新安裝它。如果指定不同的儲存類型，復原將失敗，並且需要使用指定的正確儲存類型重新安裝裝置。

- 在整個過程中、安裝會暫停一段時間。若要繼續安裝、您必須登入Grid Manager、並將擱置的儲存節點設定為故障節點的替代項目。
- 設定節點之後、應用裝置安裝程序便會完成、應用裝置也會重新開機。

步驟

1. 開啟瀏覽器、然後輸入應用裝置中運算控制器的其中一個IP位址。

   `https://Controller_IP:8443`

   畫面會出現「the不再安裝StorageGRID 程式」首頁。

2. 在「主要管理節點連線」區段中、判斷是否需要指定主要管理節點的IP位址。

   如果主管理節點或至少有一個已設定ADD_IP的其他網格節點存在於同一個子網路中、則可使用此解決方案安裝程式自動探索此IP位址。StorageGRID

3. 如果未顯示此IP位址、或您需要變更它、請指定位址：

選項	步驟
手動輸入IP	a. 清除 * 啟用管理節點探索 * 核取方塊。 b. 手動輸入 IP 位址。 注意：對於安裝，請手動輸入要用於安裝節點的管理節點的 IP 位址。對於恢復，如果可用，請使用主管理節點的 IP；否則，使用非主管理節點的 IP。 a. 選擇*保存*。 b. 等待新 IP 位址的連線狀態變成「就緒」。

選項	步驟
自動探索所有連線的主要管理節點	a. 選中 * 啓用管理節點發現 * 複選框。 b. 從發現的 IP 位址清單中，選擇將部署此設備儲存節點的網格的管理節點。 注意：對於恢復，如果可用，請使用主管理節點的 IP；否則，使用非主管理節點的 IP。 a. 選擇*保存*。 b. 等待新 IP 位址的連線狀態變成「就緒」。

4. 在「節點名稱」欄位中，輸入與要恢復的節點相同的主機名稱（系統名稱），然後選擇「儲存」。
5. 在「安裝」部分，確認目前狀態為「準備開始將 *node name* 安裝到主要管理節點 *admin_ip* 的網格中」，且「開始安裝」按鈕已啟用。

   如果*開始安裝*按鈕未啟用、您可能需要變更網路組態或連接埠設定。如需相關指示、請參閱產品的維護指示。

6. 從 StorageGRID 應用裝置安裝程式首頁，選取 * 開始安裝 *。

   目前狀態變更為「Installation is in progress」，並顯示監控安裝頁面。

   如果需要手動存取 Monitor 安裝頁面，請從功能表列中選取 **Monitor installation**。參見 "監控應用裝置安裝"。

監控**StorageGRID** 產品安裝

直到安裝完成為止、才會StorageGRID 顯示此狀態。軟體安裝完成後、即會重新啟動應用裝置。

步驟

1. 若要監控安裝進度，請從功能表列中選擇 **Monitor installation**。

   Monitor 安裝頁面會顯示安裝進度。

   藍色狀態列會指出目前正在進行的工作。綠色狀態列表示已成功完成的工作。

   安裝程式可確保先前安裝中完成的工作不會重新執行。如果您正在重新執行安裝、任何不需要重新執行的工作都會顯示綠色狀態列和「略過」狀態。

2. 檢閱前兩個安裝階段的進度。

   - **1.**設定儲存設備

     在此階段、安裝程式會連線至儲存控制器、清除任何現有的組態、與 SANtricity OS 通訊以設定磁碟區、以及設定主機設定。

◦ **2.**安裝作業系統

在此階段、安裝程式會將基礎作業系統映像複製到StorageGRID 應用裝置中以供使用。

3. 繼續監控安裝進度、直到*安裝StorageGRID Sid*階段暫停、並在內嵌主控台顯示訊息、提示您使用Grid Manager在管理節點上核准此節點。
4. 前往 "選取「Start Recovery（開始恢復）」以設定應用裝置儲存節點"。

選擇 **Start Recovery** 以配置 **StorageGRID** 應用裝置儲存節點

您必須在Grid Manager中選取「Start Recovery」（開始還原）、才能將應用裝置儲存節點設定為故障節點的替換節點。

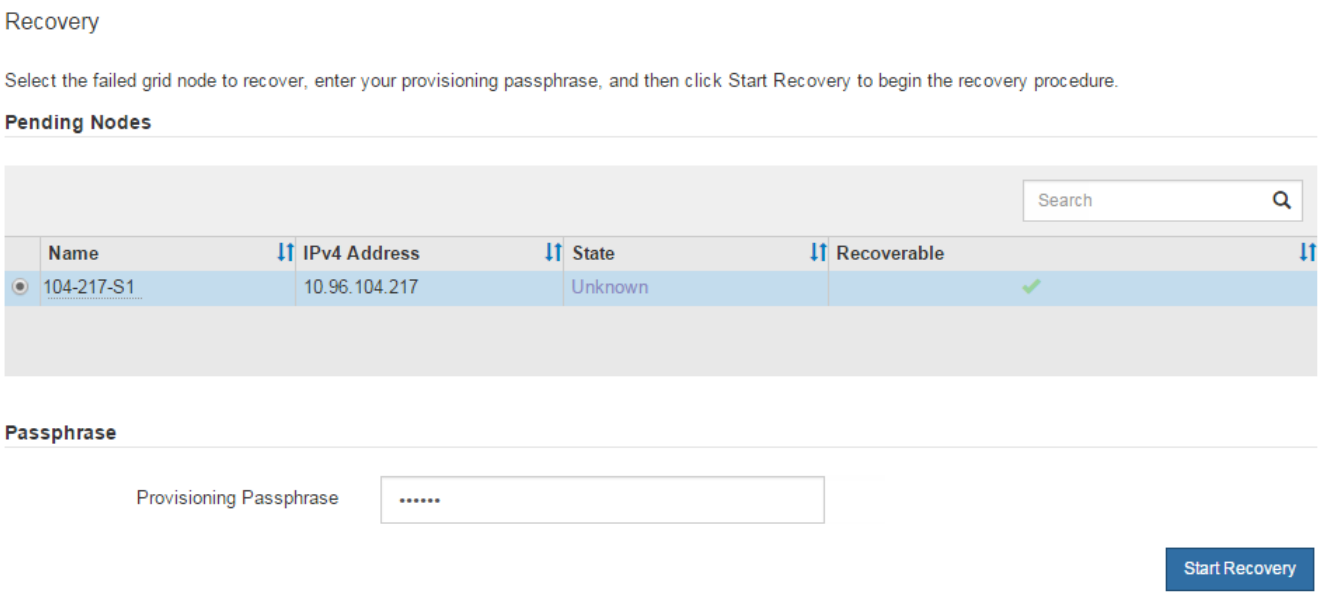
開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您已部署恢復設備儲存節點。
- 您擁有任何修復工作的開始日期、可用於銷毀編碼資料。

步驟

1. 從 Grid Manager 中，選擇 **Maintenance** > **Tasks** > **Node recovery**。
2. 在「Pending Node」（擱置節點）清單中選取您要恢復的網格節點。

   節點在故障後會出現在清單中、但您無法選取節點、直到節點重新安裝並準備好恢復為止。
3. 請輸入*佈建密碼*。
4. 選擇 **Start recovery**。



5. 監控恢復網格節點表格中的恢復進度。
   - 如果網格節點達到「等待手動步驟」階段，您必須"手動重新掛載並重新格式化應用裝置儲存設備磁碟區"。
   - 如果未出現「等待手動步驟」訊息，則表示儲存設備磁碟區已自動重新掛載和重新格式化，您可以"將物件資料還原到磁碟區中"。

> 在恢復過程中的任何階段，您都可以選擇 **Reset** 來開始新的恢復。此時會出現一個對話方塊，提示如果您重設程序，節點將處於不確定狀態。
>
> 如果您想在重設程序後重試恢復、則必須在節點上執行、將應用裝置節點還原為預先安裝的狀態 `sgareinstall`。

重新掛載並重新格式化 **StorageGRID** 應用裝置儲存磁碟區（手動步驟）

如果自動程式未能重新掛載已保留的儲存設備磁碟區並重新格式化故障的儲存設備磁碟區，則必須手動執行兩個指令碼來完成這些作業。第一個指令碼重新掛載已正確格式化為 StorageGRID 儲存設備磁碟區的磁碟區。第二個指令碼重新格式化所有未掛載的磁碟區，並在需要時重建 Cassandra 資料庫，然後啟動服務。

在 Storage Node 恢復期間，如果 Grid Manager 中出現「等待手動步驟」訊息，請依照下列步驟重新掛載和重新格式化儲存設備磁碟區。如果未看到此訊息，則重新掛載和重新格式化操作已自動完成，您可以跳過_此_程序"還原物件資料"。

開始之前

- 您已更換硬體、以更換已知需要更換的任何故障儲存磁碟區。

  執行 `sn-remount-volumes`指令碼可能有助於識別其他故障的儲存磁碟區。

- 您已檢查儲存節點退役未正在進行，或您已暫停節點退役程序。 （在網格管理員中，選擇*維護* > 任務 > 退役。）
- 您已檢查擴充功能是否尚未進行。 （在網格管理員中，選擇*維護* > 任務 > 擴充。）

> 如果多個儲存節點離線，請聯絡技術支援。不要運行 `sn-recovery-postinstall.sh`腳本。

關於這項工作

若要完成此程序、請執行下列高階工作：

- 登入恢復的儲存節點。
- 執行 `sn-remount-volumes`指令碼以重新掛載格式正確的儲存磁碟區。執行此指令碼時、會執行下列動作：
  - 掛載和卸載每個儲存磁碟區、以重新播放XFS日誌。
  - 執行XFS檔案一致性檢查。
  - 如果檔案系統一致、請判斷儲存磁碟區是否為格式正確StorageGRID 的等化儲存磁碟區。
  - 如果儲存磁碟區格式正確、請重新掛載儲存磁碟區。磁碟區上的任何現有資料均保持不變。
- 檢閱指令碼輸出並解決任何問題。

- 執行 `sn-recovery-postinstall.sh`指令碼。執行此指令碼時、會執行下列動作。

> 執行（步驟 4 ）之前、請勿在恢復期間重新開機儲存節點 `sn-recovery-postinstall.sh`、以重新格式化故障的儲存磁碟區並還原物件中繼資料。在完成前重新啟動儲存節點 `sn-recovery-postinstall.sh`會導致服務發生錯誤、導致 StorageGRID 應用裝置節點離開維護模式。

  - 重新格式化指令碼無法掛載或發現格式不正確的任何儲存磁碟區 `sn-remount-volumes`。

> 如果重新格式化儲存磁碟區、則該磁碟區上的任何資料都會遺失。您必須執行其他程序、從網格中的其他位置還原物件資料、前提是ILM規則已設定為儲存多個物件複本。

  - 視需要在節點上重新建置Cassandra資料庫。
  - 啟動儲存節點上的服務。

步驟

1. 登入恢復的儲存節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 執行第一個指令碼、重新掛載任何格式正確的儲存磁碟區。

> 如果所有的儲存磁碟區都是新的且需要格式化、或是所有的儲存磁碟區都失敗、您可以跳過此步驟並執行第二個指令碼、重新格式化所有未掛載的儲存磁碟區。

   a. 執行指令碼： `sn-remount-volumes`

      此指令碼可能需要數小時才能在含有資料的儲存磁碟區上執行。

   b. 指令碼執行時、請檢閱輸出並回答任何提示。

> 根據需要，您可以使用 `tail -f`命令來監控腳本日誌文件的內容 (/var/local/log/sn-remount-volumes.log`）。記錄檔包含的資訊比命令列輸出更詳細。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
```

```
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
```

```
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在範例輸出中、已成功重新掛載一個儲存磁碟區、三個儲存磁碟區發生錯誤。

- `/dev/sdb`通過 XFS 檔案系統一致性檢查、並具有有效的磁碟區結構、因此已成功重新掛載。由指令碼重新掛載的裝置上的資料會保留下來。
- `/dev/sdc`XFS 檔案系統一致性檢查失敗、因為儲存磁碟區是新的或毀損。
- `/dev/sdd`無法掛載、因為磁碟未初始化或磁碟的超級區塊毀損。當指令碼無法掛載儲存磁碟區時、它會詢問您是否要執行檔案系統一致性檢查。
  - 如果儲存磁碟區已附加至新磁碟、請在提示字元中回答* N*。您不需要檢查新磁碟上的檔案系統。
  - 如果儲存磁碟區已附加至現有磁碟、請在提示字元中回答* Y*。您可以使用檔案系統檢查的結果來判斷毀損的來源。結果會儲存在記錄檔中 `/var/local/log/sn-remount-volumes.log`。
- `/dev/sde`通過 `XFS` 檔案系統一致性檢查、並具有有效的 `Volume` 結構；不過、檔案中的 `LDR` 節點 `ID` `volID` 與此儲存節點的 ID 不符（`configured LDR noid`顯示於頂端）。此訊息表示此磁碟區屬於另一個儲存節點。

3. 檢閱指令碼輸出並解決任何問題。

> 如果儲存磁碟區未通過XFS檔案系統一致性檢查或無法掛載、請仔細檢閱輸出中的錯誤訊息。您必須瞭解在這些磁碟區上執行指令碼的影響 `sn-recovery-postinstall.sh`。

a. 檢查以確定結果包含您所預期所有磁碟區的項目。如果未列出任何磁碟區、請重新執行指令碼。

b. 檢閱所有掛載裝置的訊息。請確定沒有錯誤指出儲存磁碟區不屬於此儲存節點。

在範例中、dev/sde的輸出包含下列錯誤訊息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

如果儲存磁碟區被回報為屬於其他儲存節點、請聯絡技術支援部門。如果您執行 `sn-recovery-postinstall.sh`指令碼、儲存磁碟區將會重新格式化、這可能會導致資料遺失。

c. 如果無法掛載任何儲存裝置、請記下裝置名稱、然後修復或更換裝置。

您必須修復或更換任何無法掛載的儲存裝置。

d. 修復或更換所有無法掛載的裝置之後、請再次執行 `sn-remount-volumes`指令碼、確認所有可重新掛載的儲存磁碟區都已重新掛載。

如果儲存磁碟區無法掛載或格式化不當、而您繼續下一步、則磁碟區和磁碟區上的任何資料都會遭到刪除。如果您有兩份物件資料複本、則在完成下一個程序（還原物件資料）之前、只會有一份複本。

如果您認為故障儲存磁碟區上的剩餘資料無法從網格中的其他位置重建、請勿執行 `sn-recovery-postinstall.sh`指令碼（例如、如果您的 ILM 原則使用的規則只製作一份複本、或是如果磁碟區在多個節點上發生故障）。請聯絡技術支援部門、以決定如何恢復資料。

4. 執行 `sn-recovery-postinstall.sh`**指令碼：** `sn-recovery-postinstall.sh`

此指令碼會重新格式化任何無法掛載或被發現格式不正確的儲存磁碟區；如有需要、可在節點上重新建置Cassandra資料庫；並在儲存節點上啟動服務。

請注意下列事項：

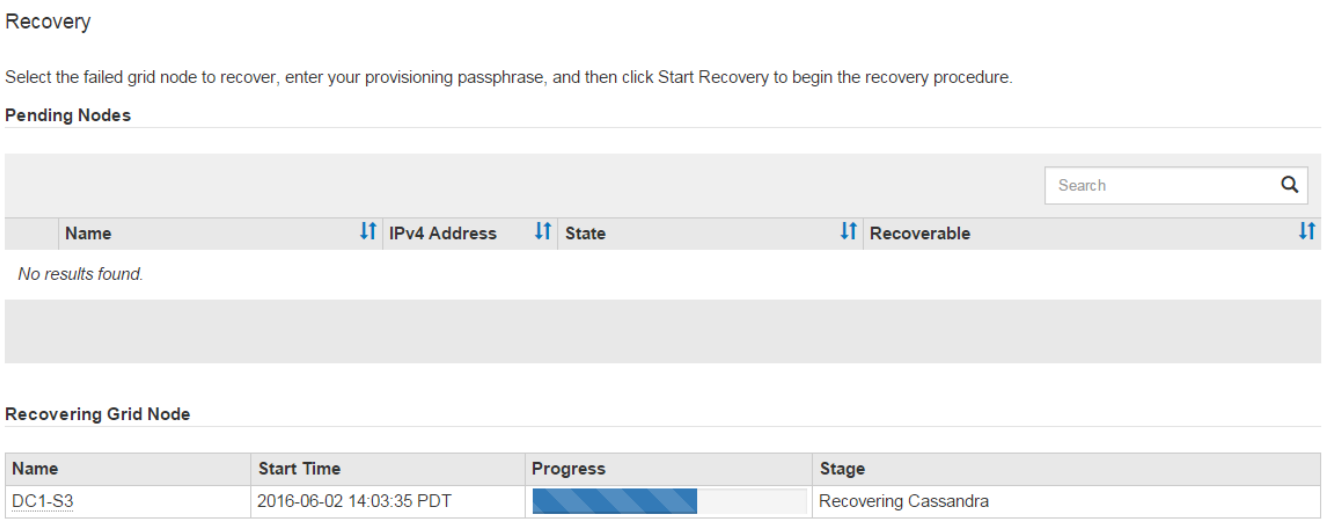
- 指令碼可能需要數小時才能執行。
- 一般而言、您應該在指令碼執行時、單獨保留SSH工作階段。
- SSH 工作階段作用中時、請勿按 * Ctrl+C* 。
- 如果發生網路中斷、指令碼會在背景執行、並終止SSH工作階段、但您可以從「恢復」頁面檢視進度。
- 如果儲存節點使用的是RSM服務、則當節點服務重新啟動時、指令碼可能會停滯5分鐘。每當首次啟動RSM服務時、預期會有5分鐘的延遲時間。

其中包含了ADC服務的儲存節點上有此RSM服務。

部分StorageGRID 還原程序會使用Reaper來處理Cassandra的修復作業。一旦相關或必要的服務開始、系統就會自動進行修復。您可能會注意到指令碼輸出中提到「 reaper 」或「 Cassandra repair 」。如果您看到指出修復失敗的錯誤訊息、請執行錯誤訊息中指出的命令。

5. 執行指令碼時 `sn-recovery-postinstall.sh`、請在 Grid Manager 中監控「恢復」頁面。

「恢復」頁面上的進度列和「階段」欄位可提供指令碼的高層級狀態 `sn-recovery-postinstall.sh`。



6. 指令碼在節點上啟動服務之後 `sn-recovery-postinstall.sh`、您可以將物件資料還原至指令碼格式化的任何儲存磁碟區。

   指令碼會詢問您是否要使用 Grid Manager Volume 還原程序來還原物件資料。

   - 大多數情況下，您應該"使用 Grid Manager 還原物件資料"。回答 `y`以使用 Grid Manager。
   - 在極少數情況下，例如當您知道替換節點可用於物件儲存的 Volume 比原始節點少時，請聯絡技術支援以手動還原物件資料。如果其中一種情況適用，請回答 `n`並按任意鍵返回命令列。

將物件資料還原至 **StorageGRID** 應用裝置的儲存磁碟區

為應用裝置儲存節點恢復儲存磁碟區之後、您可以還原儲存節點故障時遺失的複寫或刪除編碼物件資料。

開始之前

- 如果自動程序未能重新掛載已保留的儲存設備 Volume 並重新格式化失敗的儲存設備 Volume，則表示您已執行下列其中一項程序：
  - "重新掛載及重新格式化應用裝置儲存磁碟區（手動步驟）"
  - "重新掛載及重新格式化儲存磁碟區（手動步驟）"
- 您已確認，在 Grid Manager 的「節點」>「總覽」索引標籤中，您正在還原物件的儲存節點的連線狀態為「已連線」 。
- 您已確認以下內容：
  - 目前沒有進行增加儲存節點的網格擴充計畫。
  - 儲存節點退役作業未在進行中或未失敗。
  - 故障儲存設備 Volume 的恢復尚未進行中。
  - 具有故障系統磁碟機的儲存節點恢復程序尚未進行中。
  - EC 重新平衡工作未在進行中。
  - 設備節點複製尚未進行中。

關於這項工作

更換磁碟機並格式化 Volume 後，Grid Manager 會將這些 Volume 顯示為「維護」>「Volume 還原」>「要還原的節點」標籤上的還原候選物件。

盡可能使用 Grid Manager 中的 Volume 還原頁面還原物件資料。您可以啟用自動還原模式在磁碟區準備好還原時自動啟動磁碟區還原、或手動執行磁碟區還原是。請遵循以下準則：

- 如果磁碟區在 維護 > 磁碟區復原 > 要復原的節點 中列出，請依照下列步驟還原物件資料。如果滿足以下條件，則會列出卷數：
  - 節點中的部分儲存磁碟區（但並非全部）發生故障
  - 節點中的所有儲存磁碟區都發生故障、正在以相同數量的磁碟區或更多磁碟區取代

    Grid Manager 中的 Volume 還原頁面也可讓您執行監控磁碟區還原程序和檢視還原歷史記錄。

  如果恢復的儲存節點包含的 Volume 比它所替換的節點少，請聯絡技術支援尋求協助。

您可以還原兩種類型的物件資料：

- 複寫的資料物件會從其他位置還原、前提是已將網格的 ILM 規則設定為可提供物件複本。
  - 如果 ILM 規則設定為僅儲存一個複寫複本，而該複本存在於發生故障的儲存設備 Volume 上，則您將無法恢復該物件。
  - 如果物件的唯一剩餘複本位於Cloud Storage Pool中、StorageGRID 則必須向Cloud Storage Pool端點發出多個要求、才能還原物件資料。
- 重新組裝儲存的片段、即可還原銷毀編碼（ EC ）資料物件。毀損或遺失的片段會由銷毀編碼演算法從剩餘資料和同位元檢查片段重新建立。

  在某些儲存節點離線時、可以開始修復以銷毀編碼的資料。然而、如果無法計算所有銷毀編碼資料、則無法完成維修。所有節點都可用後、修復作業即告完成。

磁碟區還原視儲存物件複本的資源可用度而定。磁碟區還原的進度是非線性的、可能需要數天或數週才能完成。

[[enable 自動還原模式 **]]** 啟用自動還原模式

當您啟用自動還原模式時、當磁碟區準備好要還原時、磁碟區還原會自動啟動。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至啟用的位置。
3. 當確認對話方塊出現時、請檢閱詳細資料。

   - 您將無法在任何節點上手動啟動 Volume 還原作業。
   - 只有在沒有其他維護程序進行時、磁碟區還原才會自動開始。
   - 您可以從進度監控頁面監控工作的狀態。
   - StorageGRID 會自動重試無法啟動的磁碟區還原。

4. 當您瞭解啟用自動還原模式的結果時、請在確認對話方塊中選取 * 是 * 。

   您可以隨時停用自動還原模式。

[[manually -store] 手動還原故障的磁碟區或節點

請依照下列步驟還原故障的磁碟區或節點。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至停用位置。

   索引標籤上的數字表示需要還原磁碟區的節點數。

3. 展開每個節點、查看 IT 中需要還原的磁碟區及其狀態。
4. 修正任何妨礙還原每個磁碟區的問題。如果問題顯示為 Volume 狀態、則當您選取 * 等待手動步驟 * 時、就會指出問題。
5. 選取要還原的節點、其中所有磁碟區都會顯示「準備還原」狀態。

   您一次只能還原一個節點的磁碟區。

   節點中的每個 Volume 都必須表明它已準備好還原。

6. 選取 * 開始還原 * 。
7. 解決可能出現的任何警告、或選取 * 無論如何啟動 * 以忽略警告並開始還原。

當還原開始時、節點會從 * 節點移至還原 * 索引標籤、移至 * 還原進度 * 索引標籤。

如果無法啟動磁碟區還原、節點會返回 * 節點以還原 * 標籤。

檢視還原進度

「 * 還原進度 * 」標籤會顯示磁碟區還原程序的狀態、以及要還原節點的磁碟區相關資訊。

所有 Volume 中已複製和已糾刪碼物件的資料修理率是所有正在進行的還原作業的平均值。此外，還顯示了這些 Volume 中完整且無需還原的物件所佔的百分比。

> 複寫資料還原視儲存複寫複本的資源可用度而定。複寫資料還原的進度是非線性的、可能需要數天或數週才能完成。

還原工作區段會顯示從 Grid Manager 開始的磁碟區還原資訊。

- 「還原工作」區段標題中的編號會指出正在還原或排入佇列以進行還原的磁碟區數量。
- 此表顯示正在還原之節點中每個磁碟區的相關資訊及其進度。
  - 每個節點的進度會顯示每個工作的百分比。
  - 展開詳細資料欄以顯示還原開始時間和工作 ID 。
- 如果磁碟區還原失敗：

- Status （狀態）列表示 `failed (attempting retry)`，將自動重試。
- 如果多個還原工作失敗、則會先自動重試最近的工作。
- 如果重試繼續失敗、就會觸發 *EC 修復失敗 * 警示。請依照警示中的步驟來解決問題。

檢視還原歷史記錄

「 * 還原歷史記錄 * 」標籤會顯示已成功完成的所有磁碟區還原資訊。

大小不適用於複寫的物件、只會出現在包含抹除編碼（ EC ）資料物件的還原中。

恢復 **StorageGRID** 設備儲存節點後、檢查儲存狀態

恢復應用裝置儲存節點之後、您必須確認應用裝置儲存節點的所需狀態已設定為「線上」、並確保在重新啟動儲存節點伺服器時、狀態預設為「線上」。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 儲存節點已恢復、資料恢復完成。

步驟

1. 選擇“節點”>“儲存節點”>“任務”。
2. 如果“儲存狀態”下拉清單設定為“唯讀”或“離線”，請選擇“線上”。
3. 選擇*保存*。

從系統磁碟機不受影響的儲存磁碟區故障中恢復

StorageGRID 儲存磁碟區復原警告

在恢復儲存節點的故障儲存磁碟區之前、請先檢閱下列警告。

儲存節點中的儲存磁碟區（或rangedbs）會以稱為Volume ID的十六進位數字來識別。例如、0000是第一個Volume、000F是第16個Volume。每個儲存節點上的第一個物件存放區（Volume 0）會使用高達4 TB的空間進行物件中繼資料和Cassandra資料庫作業；該磁碟區上的任何剩餘空間都會用於物件資料。所有其他儲存磁碟區僅用於物件資料。

如果出現以下情況，則 Cassandra 資料庫可能會作為磁碟區復原過程的一部分進行重建：

- 卷 0 發生故障並已恢復。
- 系統磁碟機和一或多個儲存磁碟區故障並恢復。

當 Cassandra 重建時，系統使用來自其他儲存節點的資訊。如果 Cassandra 最近重建，Cassandra 資料可能在整個網格中尚不一致。如果太多儲存節點處於離線狀態：

- 某些 Cassandra 資料可能無法使用。
- 可能會發生資料遺失。

如果多個儲存節點發生故障（或離線），請聯絡技術支援。請勿執行以下恢復程序。可能會發生資料遺失。有關詳細信息，請參閱"技術支援如何恢復網站" 。

如果 ILM 規則配置為僅儲存複製副本，且該副本存在於發生故障的儲存磁碟區上，則您將無法復原該物件。

相關資訊

"網格節點還原的警告與考量"

識別並卸載 **StorageGRID** 中故障的儲存磁碟區

在恢復儲存磁碟區故障的儲存節點時、您必須識別並卸載故障的磁碟區。您必須確認只有故障的儲存磁碟區才會重新格式化為還原程序的一部分。

開始之前

您已使用登入 Grid Manager "支援的網頁瀏覽器"。

關於這項工作

您應該儘快恢復故障的儲存磁碟區。

恢復程序的第一步是偵測已分離、需要卸載或發生I/O錯誤的磁碟區。如果故障的磁碟區仍附加在磁碟區中、但檔案系統隨機毀損、則系統可能無法偵測到磁碟未使用或未分配的部分有任何毀損。

您必須先完成此程序、再執行手動步驟來恢復磁碟區、例如新增或重新連接磁碟、停止節點、啟動節點或重新開機。否則、當您執行指令碼時 `reformat_storage_block_devices.rb`、可能會遇到檔案系統錯誤、導致指令碼當機或失敗。

在執行命令之前、請先修復硬體並正確連接磁碟 `reboot`。

請仔細識別故障的儲存磁碟區。您將使用此資訊來驗證哪些磁碟區必須重新格式化。磁碟區重新格式化之後、磁碟區上的資料將無法還原。

若要復原故障儲存卷，您需要知道故障儲存卷的裝置名稱及其磁碟區 ID。

安裝時，每個儲存裝置都會指派一個檔案系統通用唯一識別碼 (UUID)，並使用該指派的檔案系統 UUID 安裝到儲存節點上的 rangedb 目錄。檔案系統 UUID 和 rangedb 目錄列在 `/etc/fstab`文件。網格管理員中顯示磁碟區的掛載點、裝置名稱和大小。

步驟

1. 完成下列步驟、記錄故障的儲存磁碟區及其裝置名稱：
   a. 選擇 節點 > 網站 > 故障儲存節點 > 儲存。
   b. 向下捲動以找到捲表和物件儲存表，並記錄每個狀態為未知或離線的磁碟區的以下資訊。
      - 從卷宗表中，記錄安裝點、設備和大小。
      - 從物件儲存表中，記錄 `object_store_ID`。

`object_store_ID`是故障儲存磁碟區的 ID 。例如、在命令中指定 `0` ID 為 0000 的物件存放區。

2. 登入故障儲存節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

3. 執行下列指令碼以卸載故障的儲存磁碟區：

```
sn-unmount-volume object_store_ID
```

4. 如果出現提示、請按 * y* 停止 Cassandra 服務、視儲存磁碟區 0 而定。

   如果 Cassandra 服務已停止、系統不會提示您。Cassandra服務僅針對Volume 0停止。

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

   幾秒鐘後、磁碟區就會卸載。畫面上會出現訊息、指出程序的每個步驟。最後一則訊息表示磁碟區已卸載。

5. 如果卸載因磁碟區忙碌而失敗、您可以使用下列選項強制卸載 `--use-umountof`：

   使用選項強制卸載 `--use-umountof`可能會導致使用磁碟區的處理程序或服務發生非預期的行為或當機。

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

您必須執行指令碼、重新格式化及重新掛載故障儲存磁碟區上的儲存設備、並在系統判斷有必要時、在儲存節點上重新建置Cassandra資料庫。

開始之前

- 您有 `Passwords.txt`檔案。
- 伺服器上的系統磁碟機完好無損。
- 故障原因已確定、必要時已取得更換儲存硬體。
- 更換儲存設備的總大小與原始儲存設備相同。
- 您已檢查儲存節點退役未正在進行，或您已暫停節點退役程序。 （在網格管理員中，選擇*維護* > 任務 > 退役。）
- 您已檢查擴充功能是否尚未進行。 （在網格管理員中，選擇*維護* > 任務 > 擴充。）
- 您有 "已查看有關儲存磁碟區恢復的警告"。

步驟

1. 視需要更換故障的實體或虛擬儲存設備、這些儲存設備與您先前識別並卸載的故障儲存磁碟區相關聯。

   請勿在此步驟中重新掛載磁碟區。儲存設備會在稍後的步驟中重新掛載並新增至 `/etc/fstab`。

2. 在網格管理器中，前往 節點 > **`appliance Storage Node`** > 硬體。在頁面的StorageGRID Appliance 部分中，驗證儲存 RAID 模式是否正常。

3. 登入故障儲存節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

4. 使用文字編輯器（ vi 或 vim ）刪除檔案中的失敗磁碟區 `/etc/fstab`、然後儲存檔案。

   > 在檔案中註解失敗的磁碟區 `/etc/fstab`不足。必須從刪除磁碟區 `fstab`、因為還原程序會驗證檔案中的所有行都 `fstab`與掛載的檔案系統相符。

5. 重新格式化任何故障的儲存磁碟區、並視需要重新建置Cassandra資料庫。輸入： `reformat_storage_block_devices.rb`

   - 卸載儲存磁碟區 0 時、會出現提示和訊息、指出 Cassandra 服務正在停止。
   - 如有必要、系統會提示您重新建置Cassandra資料庫。
     - 檢閱警告。如果沒有任何應用程式、請重新建置Cassandra資料庫。輸入：* y*
     - 如果多個儲存節點處於離線狀態。輸入：**n**

指令碼將會結束而不重建Cassandra。聯絡技術支援。

- 對於儲存節點上的每個 rangedb 磁碟機、當系統詢問您時： `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`、請輸入下列其中一個回應：
  - * y*重新格式化發生錯誤的磁碟機。這會重新格式化儲存磁碟區、並將重新格式化的儲存磁碟區新增至 `/etc/fstab`檔案。
  - **N** 如果磁碟機沒有錯誤、而且您不想重新格式化。

> ⓘ 選取* n*會結束指令碼。掛載磁碟機（如果您認為應該保留磁碟機上的資料、而且磁碟機發生錯誤、請將其卸載）或移除磁碟機。然後再次執行 `reformat_storage_block_devices.rb`命令。

> ⓘ 部分StorageGRID 還原程序會使用Reaper來處理Cassandra的修復作業。一旦相關或必要的服務開始、系統就會自動進行修復。您可能會注意到指令碼輸出中提到「 reaper 」或「 Cassandra repair 」。如果您看到指出修復失敗的錯誤訊息、請執行錯誤訊息中指出的命令。

在下列輸出範例中、必須重新格式化磁碟機 `/dev/sdf`、而且不需要重建 Cassandra ：

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

接下來呢？

儲存設備磁碟區重新格式化並重新掛載，必要的 Cassandra 操作完成後，您可以"使用 Grid Manager 還原物件資料"。

將物件資料還原至系統磁碟機完好的 **StorageGRID** 儲存磁碟區

在系統磁碟機完好無損的儲存節點上還原儲存磁碟區之後、您可以還原儲存磁碟區故障時遺失的複寫或刪除編碼物件資料。

開始之前

- 如果自動程序未能重新掛載已保留的儲存設備 Volume 並重新格式化失敗的儲存設備 Volume，則表示您已執行下列其中一項程序：
  - "重新掛載及重新格式化應用裝置儲存磁碟區（手動步驟）"
  - "重新掛載及重新格式化儲存磁碟區（手動步驟）"
- 您已確認，在 Grid Manager 的「節點」>「總覽」索引標籤中，您正在還原物件的儲存節點的連線狀態為「已連線」 。
- 您已確認以下內容：
  - 目前沒有進行增加儲存節點的網格擴充計畫。
  - 儲存節點退役作業未在進行中或未失敗。
  - 故障儲存設備 Volume 的恢復尚未進行中。
  - 具有故障系統磁碟機的儲存節點恢復程序尚未進行中。
  - EC 重新平衡工作未在進行中。
  - 設備節點複製尚未進行中。

關於這項工作

更換磁碟機並格式化 Volume 後，Grid Manager 會將這些 Volume 顯示為「維護」>「Volume 還原」>「要還原的節點」標籤上的還原候選物件。

盡可能使用 Grid Manager 中的 Volume 還原頁面還原物件資料。您可以啟用自動還原模式在磁碟區準備好還原時自動啟動磁碟區還原、或手動執行磁碟區還原是。請遵循以下準則：

- 如果磁碟區在 維護 > 磁碟區復原 > 要復原的節點 中列出，請依照下列步驟還原物件資料。如果滿足以下條件，則會列出卷數：
  - 節點中的部分儲存磁碟區（但並非全部）發生故障
  - 節點中的所有儲存磁碟區都發生故障、正在以相同數量的磁碟區或更多磁碟區取代

    Grid Manager 中的 Volume 還原頁面也可讓您執行監控磁碟區還原程序和檢視還原歷史記錄。

  如果恢復的儲存節點包含的 Volume 比它所替換的節點少，請聯絡技術支援尋求協助。

您可以還原兩種類型的物件資料：

- 複寫的資料物件會從其他位置還原、前提是已將網格的 ILM 規則設定為可提供物件複本。
  - 如果 ILM 規則設定為僅儲存一個複寫複本，而該複本存在於發生故障的儲存設備 Volume 上，則您將無法恢復該物件。
  - 如果物件的唯一剩餘複本位於Cloud Storage Pool中、StorageGRID 則必須向Cloud Storage Pool端點發出多個要求、才能還原物件資料。
- 重新組裝儲存的片段、即可還原銷毀編碼（ EC ）資料物件。毀損或遺失的片段會由銷毀編碼演算法從剩餘資料和同位元檢查片段重新建立。

  在某些儲存節點離線時、可以開始修復以銷毀編碼的資料。然而、如果無法計算所有銷毀編碼資料、則無法完成維修。所有節點都可用後、修復作業即告完成。

磁碟區還原視儲存物件複本的資源可用度而定。磁碟區還原的進度是非線性的、可能需要數天或數週才能完成。

[[enable 自動還原模式 **]]** 啟用自動還原模式

當您啟用自動還原模式時、當磁碟區準備好要還原時、磁碟區還原會自動啟動。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至啟用的位置。
3. 當確認對話方塊出現時、請檢閱詳細資料。

   - 您將無法在任何節點上手動啟動 Volume 還原作業。
   - 只有在沒有其他維護程序進行時、磁碟區還原才會自動開始。
   - 您可以從進度監控頁面監控工作的狀態。
   - StorageGRID 會自動重試無法啟動的磁碟區還原。

4. 當您瞭解啟用自動還原模式的結果時、請在確認對話方塊中選取 * 是 * 。

   您可以隨時停用自動還原模式。

[[manually -store] 手動還原故障的磁碟區或節點

請依照下列步驟還原故障的磁碟區或節點。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至停用位置。

   索引標籤上的數字表示需要還原磁碟區的節點數。

3. 展開每個節點、查看 IT 中需要還原的磁碟區及其狀態。
4. 修正任何妨礙還原每個磁碟區的問題。如果問題顯示為 Volume 狀態、則當您選取 * 等待手動步驟 * 時、就會指出問題。
5. 選取要還原的節點、其中所有磁碟區都會顯示「準備還原」狀態。

   您一次只能還原一個節點的磁碟區。

   節點中的每個 Volume 都必須表明它已準備好還原。

6. 選取 * 開始還原 * 。
7. 解決可能出現的任何警告、或選取 * 無論如何啟動 * 以忽略警告並開始還原。

當還原開始時、節點會從 * 節點移至還原 * 索引標籤、移至 * 還原進度 * 索引標籤。

如果無法啟動磁碟區還原、節點會返回 * 節點以還原 * 標籤。

檢視還原進度

「 * 還原進度 * 」標籤會顯示磁碟區還原程序的狀態、以及要還原節點的磁碟區相關資訊。

所有 Volume 中已複製和已糾刪碼物件的資料修理率是所有正在進行的還原作業的平均值。此外，還顯示了這些 Volume 中完整且無需還原的物件所佔的百分比。

> 複寫資料還原視儲存複寫複本的資源可用度而定。複寫資料還原的進度是非線性的、可能需要數天或數週才能完成。

還原工作區段會顯示從 Grid Manager 開始的磁碟區還原資訊。

- 「還原工作」區段標題中的編號會指出正在還原或排入佇列以進行還原的磁碟區數量。
- 此表顯示正在還原之節點中每個磁碟區的相關資訊及其進度。
  - 每個節點的進度會顯示每個工作的百分比。
  - 展開詳細資料欄以顯示還原開始時間和工作 ID 。
- 如果磁碟區還原失敗：
  - Status （狀態）列表示 `failed (attempting retry)`，將自動重試。
  - 如果多個還原工作失敗、則會先自動重試最近的工作。
  - 如果重試繼續失敗、就會觸發 *EC 修復失敗 * 警示。請依照警示中的步驟來解決問題。

檢視還原歷史記錄

「 * 還原歷史記錄 * 」標籤會顯示已成功完成的所有磁碟區還原資訊。

> 大小不適用於複寫的物件、只會出現在包含抹除編碼（ EC ）資料物件的還原中。

恢復 **StorageGRID** 儲存磁碟區後檢查儲存狀態

恢復儲存磁碟區之後、您必須確認儲存節點的所需狀態已設定為「線上」、並確保在重新啟動儲存節點伺服器時、狀態預設為「線上」。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 儲存節點已恢復、資料恢復完成。

步驟

1. 選擇“節點”>“儲存節點”>“任務”。
2. 如果“儲存狀態”下拉清單設定為“唯讀”或“離線”，請選擇“線上”。
3. 選擇*保存*。

從系統磁碟機故障中恢復

StorageGRID 儲存節點系統磁碟機復原警告

在恢復儲存節點的故障系統磁碟機之前、請先檢閱一般"網格節點恢復的警告和注意事項"和下列特定警告。

儲存節點有一個包含物件元資料的 Cassandra 資料庫。如果出現以下情況，則可能需要重建 Cassandra 資料庫：

- 儲存磁碟區發生故障並已復原。
- 系統磁碟機和一或多個儲存磁碟區故障並恢復。

當 Cassandra 重建時，系統使用來自其他儲存節點的資訊。如果 Cassandra 最近重建，Cassandra 資料可能在整個網格中尚不一致。如果太多儲存節點處於離線狀態：

- 某些 Cassandra 資料可能無法使用。
- 可能會發生資料遺失。

> 如果多個儲存節點發生故障（或離線），請聯絡技術支援。不要執行以下恢復程序。可能會發生資料遺失。有關詳細信息，請參閱"技術支援如何恢復網站"。

> 如果此儲存節點處於唯讀維護模式，以便其他儲存節點能夠從儲存磁碟區發生故障的儲存節點擷取物件，請先恢復儲存磁碟區發生故障的儲存節點上的磁碟區，再還原此故障儲存節點。請參閱相關說明 "從系統磁碟機完好無損的儲存磁碟區故障中恢復"。

> 如果ILM規則設定為僅儲存一個複寫複本、且複本存在於故障的儲存磁碟區、您將無法恢復物件。

更換 StorageGRID Storage Node

如果系統磁碟機故障、您必須先更換儲存節點。

您必須為平台選取節點更換程序。所有類型的網格節點、更換節點的步驟都相同。

> 此程序僅適用於軟體型儲存節點。您必須遵循不同的程序"恢復應用裝置儲存節點"。

- Linux ： * 如果您不確定系統磁碟機是否故障、請依照指示更換節點、以判斷需要哪些恢復步驟。

平台	程序
VMware	"更換VMware節點"
Linux	"更換Linux節點"
OpenStack	NetApp提供的OpenStack虛擬機器磁碟檔案和指令碼不再支援還原作業。如果您需要恢復在OpenStack部署中執行的節點、請下載適用於您Linux作業系統的檔案。然後，請遵循的程序"更換 Linux 節點"。

選擇 **Start Recovery** 以配置 **StorageGRID Storage Node**

更換儲存節點之後、您必須在Grid Manager中選取「Start Recovery」（開始還原）、將新節點設定為故障節點的替換節點。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您已部署並設定替換節點。
- 您擁有任何修復工作的開始日期、可用於銷毀編碼資料。

關於這項工作

如果儲存節點是以容器形式安裝在Linux主機上、則只有在下列其中一項為真時、才必須執行此步驟：

- 您必須使用 `--force`旗標來匯入節點、或是您已核發 `storagegrid node force-recovery *node-name*`
- 您必須重新安裝完整節點、或是需要還原/var/local。

步驟

1. 登入主要管理節點。如果主要管理節點無法使用，請使用非主要管理節點（如果存在）。
2. 從 Grid Manager 中，選擇 **Maintenance** > **Tasks** > **Node recovery**。
3. 在「Pending Node」（擱置節點）清單中選取您要恢復的網格節點。

   節點在故障後會出現在清單中、但您無法選取節點、直到節點重新安裝並準備好恢復為止。

4. 請輸入*佈建密碼*。
5. 點選 **Start recovery**。
6. 選取 **Maintenance** > **Tasks** > **Node recovery** 並檢視恢復進度，以監控恢復進度。
   - 如果網格節點達到「等待手動步驟」階段，您必須 "手動重新掛載並重新格式化儲存設備磁碟區"。完成手動步驟後，請繼續 "將物件資料還原到磁碟區中"。
   - 如果網格節點恢復已從「進行中」狀態轉換至「已恢復」狀態，而未經過「等待手動步驟」階段，則無需採取進一步行動。

> 在恢復過程中的任何階段，您都可以選擇 **Reset** 來開始新的恢復。此時會出現一個對話方塊，提示如果您重設程序，節點將處於不確定狀態。
>
> 如果您想在重置程式後重試恢復，則必須將應用裝置節點還原到預安裝狀態，如下所示：
>
> - * VMware*：刪除已部署的虛擬網格節點。然後、當您準備好重新啟動恢復時、請重新部署節點。
> - **Linux** ：在 Linux 主機上執行以下命令、重新啟動節點： `storagegrid node force-recovery *node-name*`

如果自動程式未能重新掛載已保留的儲存設備磁碟區並重新格式化故障的儲存設備磁碟區，則必須手動執行兩個指令碼來完成這些作業。第一個指令碼重新掛載已正確格式化為 StorageGRID 儲存設備磁碟區的磁碟區。第二個指令碼重新格式化所有未掛載的磁碟區，並在需要時重建 Cassandra 資料庫，然後啟動服務。

在儲存節點恢復期間，如果 Grid Manager 中出現「等待手動步驟」訊息，請依照下列步驟重新掛載和重新格式化儲存設備磁碟區。如果未看到此訊息，則重新掛載和重新格式化操作已自動完成，您可以跳過此程序並"還原物件資料"。

開始之前

- 您已更換硬體、以更換已知需要更換的任何故障儲存磁碟區。

  執行 `sn-remount-volumes`指令碼可能有助於識別其他故障的儲存磁碟區。

- 您已檢查儲存節點退役未正在進行，或您已暫停節點退役程序。 （在網格管理員中，選擇*維護* > 任務 > 退役。）
- 您已檢查擴充功能是否尚未進行。 （在網格管理員中，選擇*維護* > 任務 > 擴充。）
- 您有 "已查看Storage Node系統磁碟機恢復的警告"。

> 如果多個儲存節點離線，請聯絡技術支援。不要運行 `sn-recovery-postinstall.sh`腳本。

關於這項工作

若要完成此程序、請執行下列高階工作：

- 登入恢復的儲存節點。
- 執行 `sn-remount-volumes`指令碼以重新掛載格式正確的儲存磁碟區。執行此指令碼時、會執行下列動作：
  - 掛載和卸載每個儲存磁碟區、以重新播放XFS日誌。
  - 執行XFS檔案一致性檢查。
  - 如果檔案系統一致、請判斷儲存磁碟區是否為格式正確StorageGRID 的等化儲存磁碟區。
  - 如果儲存磁碟區格式正確、請重新掛載儲存磁碟區。磁碟區上的任何現有資料均保持不變。
- 檢閱指令碼輸出並解決任何問題。
- 執行 `sn-recovery-postinstall.sh`指令碼。執行此指令碼時、會執行下列動作。

> 執行之前、請勿在恢復期間重新開機儲存節點 `sn-recovery-postinstall.sh`、以重新格式化故障的儲存磁碟區並還原物件中繼資料。在完成前重新啟動儲存節點 `sn-recovery-postinstall.sh`會導致服務發生錯誤、導致 StorageGRID 應用裝置節點離開維護模式。請參閱的步驟安裝後指令碼。

  - 重新格式化指令碼無法掛載或發現格式不正確的任何儲存磁碟區 `sn-remount-volumes`。

> 如果重新格式化儲存磁碟區、則該磁碟區上的任何資料都會遺失。您必須執行其他程序、從網格中的其他位置還原物件資料、前提是ILM規則已設定為儲存多個物件複本。

- 視需要在節點上重新建置Cassandra資料庫。
- 啟動儲存節點上的服務。

步驟

1. 登入恢復的儲存節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 執行第一個指令碼、重新掛載任何格式正確的儲存磁碟區。

   如果所有的儲存磁碟區都是新的且需要格式化、或是所有的儲存磁碟區都失敗、您可以跳過此步驟並執行第二個指令碼、重新格式化所有未掛載的儲存磁碟區。

   a. 執行指令碼： `sn-remount-volumes`

      此指令碼可能需要數小時才能在含有資料的儲存磁碟區上執行。

   b. 指令碼執行時、請檢閱輸出並回答任何提示。

      根據需要，您可以使用 `tail -f`命令來監控腳本日誌文件的內容 (/var/local/log/sn-remount-volumes.log`）。記錄檔包含的資訊比命令列輸出更詳細。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
```

```
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
```

```
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在範例輸出中、已成功重新掛載一個儲存磁碟區、三個儲存磁碟區發生錯誤。

- `/dev/sdb`通過 XFS 檔案系統一致性檢查、並具有有效的磁碟區結構、因此已成功重新掛載。由指令碼重新掛載的裝置上的資料會保留下來。
- `/dev/sdc`XFS 檔案系統一致性檢查失敗、因為儲存磁碟區是新的或毀損。
- `/dev/sdd`無法掛載、因為磁碟未初始化或磁碟的超級區塊毀損。當指令碼無法掛載儲存磁碟區時、它會詢問您是否要執行檔案系統一致性檢查。
  - 如果儲存磁碟區已附加至新磁碟、請在提示字元中回答* N*。您不需要檢查新磁碟上的檔案系統。
  - 如果儲存磁碟區已附加至現有磁碟、請在提示字元中回答* Y*。您可以使用檔案系統檢查的結果來判斷毀損的來源。結果會儲存在記錄檔中 `/var/local/log/sn-remount-volumes.log`。
- `/dev/sde`通過 XFS 檔案系統一致性檢查、並具有有效的 Volume 結構；然而、 volID 檔案中的 LDR 節點 ID 與此儲存節點的 ID 不符（ `configured LDR noid`顯示於頂端）。此訊息表示此磁碟區屬於另一個儲存節點。

3. 檢閱指令碼輸出並解決任何問題。

> 如果儲存磁碟區未通過XFS檔案系統一致性檢查或無法掛載、請仔細檢閱輸出中的錯誤訊息。您必須瞭解在這些磁碟區上執行指令碼的影響 `sn-recovery-postinstall.sh`。

a. 檢查以確定結果包含您所預期所有磁碟區的項目。如果未列出任何磁碟區、請重新執行指令碼。

b. 檢閱所有掛載裝置的訊息。請確定沒有錯誤指出儲存磁碟區不屬於此儲存節點。

在範例中、的輸出 `/dev/sde`包含下列錯誤訊息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

如果儲存磁碟區被回報為屬於其他儲存節點、請聯絡技術支援部門。如果您執行 `sn-recovery-postinstall.sh`指令碼、儲存磁碟區將會重新格式化、這可能會導致資料遺失。

c. 如果無法掛載任何儲存裝置、請記下裝置名稱、然後修復或更換裝置。

您必須修復或更換任何無法掛載的儲存裝置。

d. 修復或更換所有無法掛載的裝置之後、請再次執行 `sn-remount-volumes`指令碼、確認所有可重新掛載的儲存磁碟區都已重新掛載。

如果儲存磁碟區無法掛載或格式化不當、而您繼續下一步、則磁碟區和磁碟區上的任何資料都會遭到刪除。如果您有兩份物件資料複本、則在完成下一個程序（還原物件資料）之前、只會有一份複本。

如果您認為故障儲存磁碟區上的剩餘資料無法從網格中的其他位置重建、請勿執行 `sn-recovery-postinstall.sh`指令碼（例如、如果您的 ILM 原則使用的規則只製作一份複本、或是如果磁碟區在多個節點上發生故障）。請聯絡技術支援部門、以決定如何恢復資料。

4. 執行 `sn-recovery-postinstall.sh`**指令碼：** `sn-recovery-postinstall.sh`

此指令碼會重新格式化任何無法掛載或被發現格式不正確的儲存磁碟區；如有需要、可在節點上重新建置Cassandra資料庫；並在儲存節點上啟動服務。

請注意下列事項：

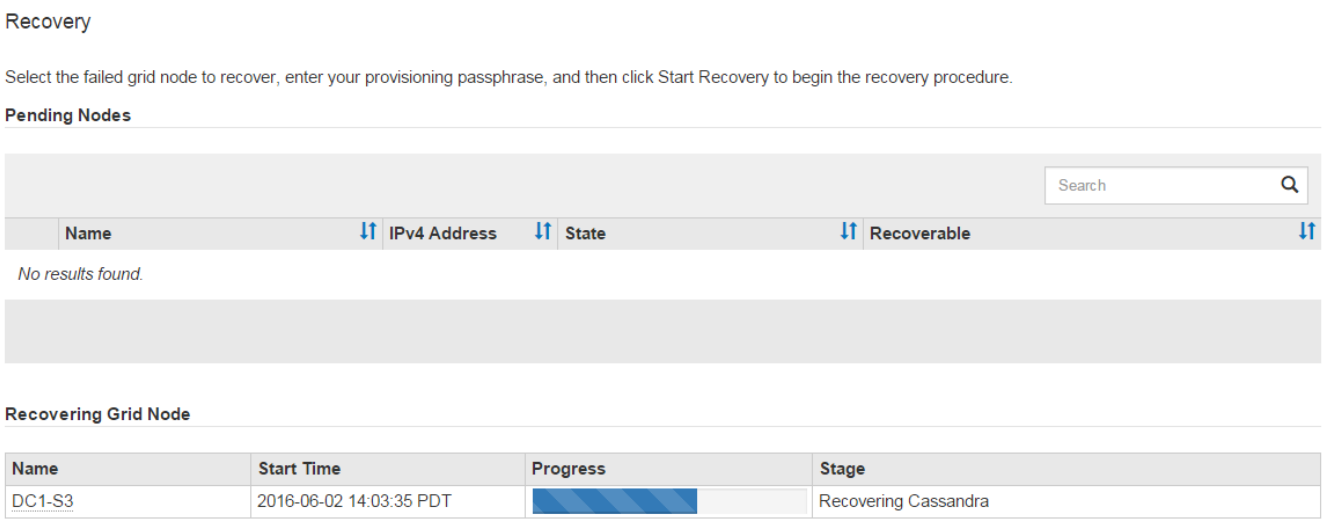
- 指令碼可能需要數小時才能執行。
- 一般而言、您應該在指令碼執行時、單獨保留SSH工作階段。
- SSH 工作階段作用中時、請勿按 * Ctrl+C* 。
- 如果發生網路中斷、指令碼會在背景執行、並終止SSH工作階段、但您可以從「恢復」頁面檢視進度。
- 如果儲存節點使用的是RSM服務、則當節點服務重新啟動時、指令碼可能會停滯5分鐘。每當首次啟動RSM服務時、預期會有5分鐘的延遲時間。

其中包含了ADC服務的儲存節點上有此RSM服務。

部分StorageGRID 還原程序會使用Reaper來處理Cassandra的修復作業。一旦相關或必要的服務開始、系統就會自動進行修復。您可能會注意到指令碼輸出中提到「 reaper 」或「 Cassandra repair 」。如果您看到指出修復失敗的錯誤訊息、請執行錯誤訊息中指出的命令。

5. 指令碼執行時 `sn-recovery-postinstall.sh`、請在 Grid Manager 中監控「恢復」頁面。

「恢復」頁面上的進度列和「階段」欄位可提供指令碼的高層級狀態 `sn-recovery-postinstall.sh`。



6. 指令碼在節點上啟動服務之後 `sn-recovery-postinstall.sh`、您可以將物件資料還原至指令碼格式化的任何儲存磁碟區。

   指令碼會詢問您是否要使用 Grid Manager Volume 還原程序。

   - 大多數情況下，您應該"使用 Grid Manager 還原物件資料"。回答 `y`以使用 Grid Manager。
   - 在極少數情況下，例如當您知道替換節點可用於物件儲存的 Volume 比原始節點少時，請聯絡技術支援以手動還原物件資料。如果其中一種情況適用，請回答 `n`並按任意鍵返回命令列。

將物件資料還原至 **StorageGRID** 儲存磁碟區（系統磁碟機故障）

在恢復非應用裝置儲存節點的儲存磁碟區之後、您可以還原儲存節點故障時遺失的複寫或刪除編碼物件資料。

開始之前

- 如果自動程序未能重新掛載已保留的儲存設備 Volume 並重新格式化失敗的儲存設備 Volume，則表示您已執行下列其中一項程序：
  - "重新掛載及重新格式化應用裝置儲存磁碟區（手動步驟）"
  - "重新掛載及重新格式化儲存磁碟區（手動步驟）"
- 您已確認，在 Grid Manager 的「節點」>「總覽」索引標籤中，您正在還原物件的儲存節點的連線狀態為「已連線」 。
- 您已確認以下內容：
  - 目前沒有進行增加儲存節點的網格擴充計畫。
  - 儲存節點退役作業未在進行中或未失敗。
  - 故障儲存設備 Volume 的恢復尚未進行中。
  - 具有故障系統磁碟機的儲存節點恢復程序尚未進行中。
  - EC 重新平衡工作未在進行中。
  - 設備節點複製尚未進行中。

關於這項工作

更換磁碟機並格式化 Volume 後，Grid Manager 會將這些 Volume 顯示為「維護」>「Volume 還原」>「要還原的節點」標籤上的還原候選物件。

盡可能使用 Grid Manager 中的 Volume 還原頁面還原物件資料。您可以啟用自動還原模式在磁碟區準備好還原時自動啟動磁碟區還原、或手動執行磁碟區還原是。請遵循以下準則：

- 如果磁碟區在 維護 > 磁碟區復原 > 要復原的節點 中列出，請依照下列步驟還原物件資料。如果滿足以下條件，則會列出卷數：
  - 節點中的部分儲存磁碟區（但並非全部）發生故障
  - 節點中的所有儲存磁碟區都發生故障、正在以相同數量的磁碟區或更多磁碟區取代

    Grid Manager 中的 Volume 還原頁面也可讓您執行監控磁碟區還原程序和檢視還原歷史記錄。

  如果恢復的儲存節點包含的 Volume 比它所替換的節點少，請聯絡技術支援尋求協助。

您可以還原兩種類型的物件資料：

- 複寫的資料物件會從其他位置還原、前提是已將網格的 ILM 規則設定為可提供物件複本。
  - 如果 ILM 規則設定為僅儲存一個複寫複本，而該複本存在於發生故障的儲存設備 Volume 上，則您將無法恢復該物件。
  - 如果物件的唯一剩餘複本位於Cloud Storage Pool中、StorageGRID 則必須向Cloud Storage Pool端點發出多個要求、才能還原物件資料。
- 重新組裝儲存的片段、即可還原銷毀編碼（ EC ）資料物件。毀損或遺失的片段會由銷毀編碼演算法從剩餘資料和同位元檢查片段重新建立。

  在某些儲存節點離線時、可以開始修復以銷毀編碼的資料。然而、如果無法計算所有銷毀編碼資料、則無法完成維修。所有節點都可用後、修復作業即告完成。

> ⓘ 磁碟區還原視儲存物件複本的資源可用度而定。磁碟區還原的進度是非線性的、可能需要數天或數週才能完成。

[[enable 自動還原模式 **]]** 啟用自動還原模式

當您啟用自動還原模式時、當磁碟區準備好要還原時、磁碟區還原會自動啟動。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至啟用的位置。
3. 當確認對話方塊出現時、請檢閱詳細資料。

> ⓘ
> - 您將無法在任何節點上手動啟動 Volume 還原作業。
> - 只有在沒有其他維護程序進行時、磁碟區還原才會自動開始。
> - 您可以從進度監控頁面監控工作的狀態。
> - StorageGRID 會自動重試無法啟動的磁碟區還原。

4. 當您瞭解啟用自動還原模式的結果時、請在確認對話方塊中選取 * 是 * 。

   您可以隨時停用自動還原模式。

[[manually -store] 手動還原故障的磁碟區或節點

請依照下列步驟還原故障的磁碟區或節點。

步驟

1. 在網格管理員中前往*維護*>*磁碟區復原*。
2. 選取 * 要還原的節點 * 標籤、然後將 * 自動還原模式 * 的切換滑至停用位置。

   索引標籤上的數字表示需要還原磁碟區的節點數。

3. 展開每個節點、查看 IT 中需要還原的磁碟區及其狀態。
4. 修正任何妨礙還原每個磁碟區的問題。如果問題顯示為 Volume 狀態、則當您選取 * 等待手動步驟 * 時、就會指出問題。
5. 選取要還原的節點、其中所有磁碟區都會顯示「準備還原」狀態。

   您一次只能還原一個節點的磁碟區。

   節點中的每個 Volume 都必須表明它已準備好還原。

6. 選取 * 開始還原 * 。
7. 解決可能出現的任何警告、或選取 * 無論如何啟動 * 以忽略警告並開始還原。

當還原開始時、節點會從 * 節點移至還原 * 索引標籤、移至 * 還原進度 * 索引標籤。

如果無法啟動磁碟區還原、節點會返回 * 節點以還原 * 標籤。

檢視還原進度

「 * 還原進度 * 」標籤會顯示磁碟區還原程序的狀態、以及要還原節點的磁碟區相關資訊。

所有 Volume 中已複製和已糾刪碼物件的資料修理率是所有正在進行的還原作業的平均值。此外，還顯示了這些 Volume 中完整且無需還原的物件所佔的百分比。

> 複寫資料還原視儲存複寫複本的資源可用度而定。複寫資料還原的進度是非線性的、可能需要數天或數週才能完成。

還原工作區段會顯示從 Grid Manager 開始的磁碟區還原資訊。

- 「還原工作」區段標題中的編號會指出正在還原或排入佇列以進行還原的磁碟區數量。
- 此表顯示正在還原之節點中每個磁碟區的相關資訊及其進度。
  - 每個節點的進度會顯示每個工作的百分比。
  - 展開詳細資料欄以顯示還原開始時間和工作 ID 。
- 如果磁碟區還原失敗：

- Status （狀態）列表示 `failed (attempting retry)`，將自動重試。
- 如果多個還原工作失敗、則會先自動重試最近的工作。
- 如果重試繼續失敗、就會觸發 *EC 修復失敗 * 警示。請依照警示中的步驟來解決問題。

檢視還原歷史記錄

「 * 還原歷史記錄 * 」標籤會顯示已成功完成的所有磁碟區還原資訊。

大小不適用於複寫的物件、只會出現在包含抹除編碼（ EC ）資料物件的還原中。

恢復 **StorageGRID** 儲存節點系統磁碟機後、檢查儲存狀態

恢復儲存節點的系統磁碟機後、您必須確認儲存節點的所需狀態已設定為「線上」、並確保在重新啟動儲存節點伺服器時、狀態預設為「線上」。

開始之前

- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 儲存節點已恢復、資料恢復完成。

步驟

1. 選擇“節點”>“儲存節點”>“任務”。
2. 如果“儲存狀態”下拉清單設定為“唯讀”或“離線”，請選擇“線上”。
3. 選擇*保存*。

從管理節點故障中恢復

StorageGRID 中的主要或非主要管理節點恢復

管理節點的還原程序取決於它是主要管理節點還是非主要管理節點。

恢復主管理節點或非主管理節點的高層步驟相同、不過步驟的詳細資料有所不同。

請務必針對您要恢復的管理節點、執行正確的還原程序。程序看起來大致相同、但細節卻不同。

選擇

- "使用同一個主要管理節點恢復主要管理節點"
- "使用非主要管理節點從主要管理節點故障中恢復"
- "從非主要管理節點故障中恢復"

使用同一個主要管理節點從主要管理節點故障中恢復

使用相同的主要管理節點恢復 **StorageGRID** 主要管理節點

您必須完成一組特定的工作、才能從主要管理節點故障中恢復。主管理節點裝載網格的組

態管理節點（CMN）服務。

> 您必須及時修復或更換故障的主要管理節點，否則可能無法執行某些維護程序。

請遵循下列高階步驟來恢復主要管理節點：

1. "從故障的主要管理節點複製稽核記錄"
2. "更換主管理節點"
3. "設定替換的主要管理節點"
4. "確定恢復的主管理節點是否需要修復程序"
5. "在恢復的主要管理節點上還原稽核記錄"
6. "還原主管理節點時、請還原管理節點資料庫"
7. "恢復主要管理節點時還原 Prometheus 指標"

從發生故障的 **StorageGRID** 主要管理節點複製稽核日誌

如果您能夠從故障的主要管理節點複製稽核記錄、則應保留這些記錄、以維護網格的系統活動和使用記錄。您可以在保留的稽核記錄啟動並執行後、將其還原至恢復的主要管理節點。

關於這項工作

此程序會將稽核記錄檔從故障的管理節點複製到個別網格節點上的暫用位置。然後、這些保留的稽核記錄就可以複製到替換的管理節點。稽核記錄不會自動複製到新的管理節點。

視故障類型而定、您可能無法從故障的管理節點複製稽核記錄。如果部署只有一個管理節點、則恢復的管理節點會在新的空白檔案中、開始將事件記錄到稽核記錄、而先前記錄的資料也會遺失。如果部署包含多個管理節點、您可以從另一個管理節點恢復稽核記錄。

> 如果現在無法在故障的管理節點上存取稽核記錄、您可能可以稍後存取這些記錄、例如在主機恢復之後。

步驟

1. 如果可能，請登入發生故障的主管理節點。否則，請登入任何可用的管理節點。
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 停止 AMS 服務以防止其建立新的記錄檔：`service ams stop`
3. 瀏覽至稽核匯出目錄：

   ```
   cd /var/local/audit/export
   ```

（或者 `cd /var/local/log`在早期系統上）

4. 將來源日誌檔案重新命名為唯一編號的檔案名稱。

   - 如果日誌檔案位於 `/var/local/audit/export`目錄，其名稱是 `audit.log`。
   - 如果日誌檔案位於 `/var/local/log`目錄，其名稱是 `localaudit.log`。

   例如，重新命名 `localaudit.log`文件到 `2025-10-22.txt.1`。

   ```
   ls -l
   mv localaudit.log 2025-10-22.txt.1
   ```

5. 重新啟動 AMS 服務： `service ams start`
6. 建立目錄、將所有稽核記錄檔複製到個別網格節點上的暫存位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出現提示時、輸入admin的密碼。

7. 將所有稽核記錄檔複製到暫存位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出現提示時、輸入admin的密碼。

8. 以 root 身分登出： `exit`

使用相同的主要管理節點取代 **StorageGRID** 主要管理節點

若要恢復主管理節點、您必須先更換實體或虛擬硬體。

若要恢復主管理節點、您必須先更換實體或虛擬硬體。

- 您可以將發生故障的主要管理節點替換為在同一平台上執行的主要管理節點。
- 您可以將執行在 VMware 或 Linux 主機上的主要管理節點取代為託管在 StorageGRID 服務應用裝置上的主要管理節點。
- 您可以將執行在 VMware 主機上的主要管理節點替換為 SG1000 或 SG100 服務應用裝置。

請使用符合您為節點所選替換平台的程序。完成節點更換程序（適用於所有節點類型）之後、該程序將引導您進行主要管理節點恢復的下一步。

替換平台	程序
VMware	"將 VMware 節點替換為恢復節點" "以 SG1000 或 SG100 取代 VMware 節點"
Linux	"更換Linux節點"

替換平台	程序
服務應用裝置	"更換服務應用裝置"
OpenStack	NetApp提供的OpenStack虛擬機器磁碟檔案和指令碼不再支援還原作業。如果您需要恢復在OpenStack部署中執行的節點、請下載適用於您Linux作業系統的檔案。然後，請遵循的程序"更換 Linux 節點"。

在 **StorageGRID** 中設定替換的主要管理節點

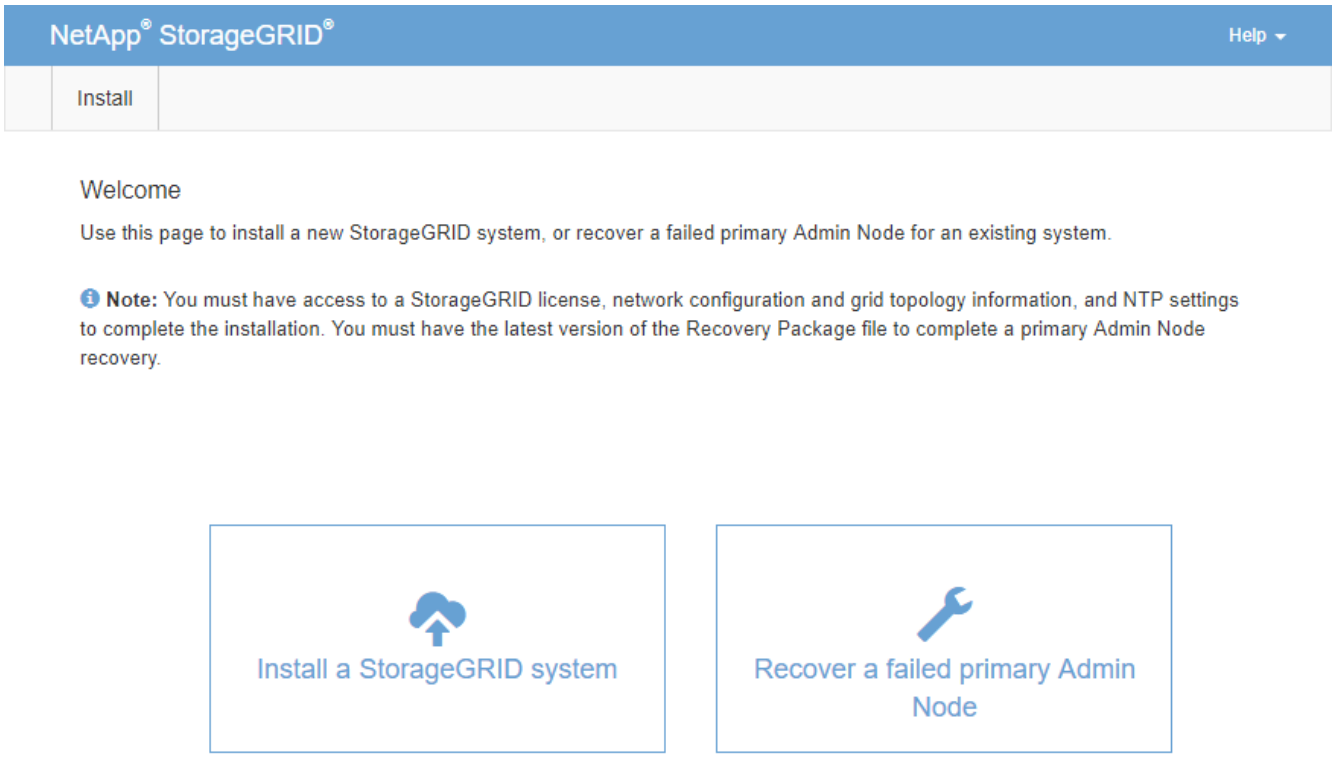
更換節點必須設定為StorageGRID 適用於您的整套系統的主要管理節點。

開始之前

- 對於虛擬機器上託管的主要管理節點、虛擬機器已部署、開機及初始化。
- 對於服務應用裝置上裝載的主要管理節點、您已更換應用裝置並安裝軟體。請參閱 "應用裝置的安裝指示"。
- 您有恢復包檔案的最新備份(`sgws-recovery-package-id-revision.zip`) 。
- 您有資源配置通關密碼。

步驟

1. 開啟網頁瀏覽器並瀏覽至 `https://primary_admin_node_ip`。
2. 視需要管理臨時安裝程式密碼：
   - 如果已使用下列其中一種方法設定密碼、請輸入密碼以繼續。
     - 使用者在先前存取安裝程式時設定密碼
     - 對於裸機系統、密碼會自動從位於的節點組態檔案匯入 `/etc/storagegrid/nodes/<node_name>.conf`
     - 對於 VM 、 SSH/ 主控台密碼會自動從 OVF 內容匯入
   - 如果尚未設定密碼、請選擇性地設定密碼以保護 StorageGRID 安裝程式。
3. 選擇 **Recover a failed primary Admin Node**。



4. 上傳恢復包的最新備份：
   a. 選擇*瀏覽*。
   b. 找到 StorageGRID 系統的最新恢復套件檔案，然後選擇 * 開啟 *。
5. 輸入資源配置通關密碼。
6. 選擇 **Start recovery**。

   恢復程序隨即開始。網格管理程式可能會在所需服務啟動後的數分鐘內無法使用。恢復完成後、會顯示登入頁面。

7. 如果StorageGRID 您的支援系統啟用單一登入（SSO）、且您所恢復之管理節點的依賴方信任已設定為使用預設管理介面憑證、請更新（或刪除及重新建立）節點在Active Directory Federation Services（AD FS）中的依賴方信任。使用在管理節點還原程序期間所產生的新預設伺服器憑證。

   若要設定信賴方信任，請參閱使用 "OIDC" 或 "SAML" 設定 SSO。若要存取預設伺服器憑證，請登入管理節點的命令 shell。前往 `/var/local/mgmt-api` 目錄，然後選取 `server.crt` 檔案。

在恢復主管理節點之後"判斷您是否需要套用 Hotfix"，。

確定 **StorageGRID** 中主要管理節點的 **Hotfix** 需求

在恢復主管理節點之後，確定是否需要應用修復程序。

開始之前

主要管理節點恢復已完成。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 選擇*節點*。
3. 從左側清單中選取主要管理節點。
4. 在「總覽」索引標籤上、記下「軟體版本」欄位中顯示的版本。
5. 選取任何其他網格節點。
6. 在「總覽」索引標籤上、記下「軟體版本」欄位中顯示的版本。
   - 如果 * 軟體版本 * 欄位中顯示的版本相同、您就不需要套用 Hotfix 。
   - 如果 * 軟體版本 * 欄位中顯示的版本不同、您必須"套用 Hotfix"將復原的主要管理節點更新為相同版本。

在已恢復的 **StorageGRID** 主要管理節點上還原稽核日誌

如果您能夠從故障的主要管理節點保留稽核記錄、則可以將其複製到您要恢復的主要管理節點。

開始之前

- 已安裝並執行復原的管理節點。
- 在原始管理節點失敗之後、您已將稽核記錄複製到其他位置。

關於這項工作

如果管理節點失敗、儲存至該管理節點的稽核記錄可能會遺失。您可以從故障的管理節點複製稽核記錄、然後將這些稽核記錄還原至恢復的管理節點、以避免資料遺失。視故障而定、可能無法從故障的管理節點複製稽核記錄。在這種情況下、如果部署有多個管理節點、您可以從另一個管理節點恢復稽核記錄、因為稽核記錄會複寫到所有管理節點。

如果只有一個管理節點、而且無法從故障節點複製稽核記錄、則復原的管理節點會開始將事件記錄到稽核記錄檔、就像是新安裝一樣。

您必須盡快恢復管理節點、才能還原記錄功能。

> 根據預設、稽核資訊會傳送至管理節點上的稽核記錄。如果下列任一項適用、您都可以跳過這些步驟：
>
> - 您已設定外部syslog伺服器、稽核記錄現在會傳送至syslog伺服器、而非管理節點。
> - 您明確指定稽核訊息只能儲存在產生這些訊息的本機節點上。
>
> 看"設定日誌管理和外部系統日誌伺服器"了解詳情。

步驟

1. 登入恢復的管理節點：
   a. 輸入下列命令： `ssh admin@recovery_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

以 root 登入後、提示會從變更 `$`為 `#`。

2. 檢查哪些審計文件已被儲存： `cd /var/local/audit/export`
3. 將保留的稽核記錄檔複製到復原的管理節點： `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   出現提示時、輸入admin的密碼。

4. 為了安全起見、請在確認已成功複製稽核記錄到恢復的管理節點之後、從故障的網格節點刪除這些記錄。
5. 更新已復原的管理節點上的稽核日誌檔案的使用者和群組設定： `chown ams-user:bycast *`
6. 以 root 身分登出： `exit`

復原主管理節點時，還原 **StorageGRID** 管理節點資料庫

如果您想要保留失敗的主要管理節點上的屬性和警示歷史資訊、可以還原管理節點資料庫。只有StorageGRID 當您的系統包含另一個管理節點時、才能還原此資料庫。

開始之前

- 已安裝並執行復原的管理節點。
- StorageGRID 系統至少包含兩個管理節點。
- 您有 `Passwords.txt`檔案。
- 您有資源配置通關密碼。

關於這項工作

如果管理節點故障、儲存在管理節點資料庫中的歷史資訊將會遺失。此資料庫包含下列資訊：

- 警示記錄
- 歷史屬性資料、用於節點頁面上的舊版樣式圖表

當您還原管理節點時、軟體安裝程序會在還原的節點上建立一個空白的管理節點資料庫。不過、新資料庫僅包含目前屬於系統一部分或稍後新增的伺服器和服務資訊。

如果您還原了主管理節點、StorageGRID 且您的系統有另一個管理節點、您可以將管理節點資料庫從非主管理節點（*SOUR*材料 管理節點）複製到恢復的主管理節點、以還原歷史資訊。如果您的系統只有主要管理節點、則無法還原管理節點資料庫。

> 複製管理節點資料庫可能需要數小時的時間。當服務在來源管理節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`

b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

2. 從來源管理節點停止 MI 服務： `service mi stop`

3. 從來源管理節點停止管理應用程式介面（ mgmt-API ）服務： `service mgmt-api stop`

4. 在恢復的管理節點上完成下列步驟：

a. 登入恢復的管理節點：

i. 輸入下列命令： `ssh admin@grid_node_IP`

ii. 輸入檔案中列出的密碼 `Passwords.txt`。

iii. 輸入以下命令切換到 root ： `su -`

iv. 輸入檔案中列出的密碼 `Passwords.txt`。

b. 停止 MI 服務： `service mi stop`

c. 停止 mgmt-API 服務： `service mgmt-api stop`

d. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`

e. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。

f. 出現提示時、請確認您要覆寫已恢復管理節點上的MI資料庫。

資料庫及其歷史資料會複製到恢復的管理節點。複製作業完成後、指令碼會啟動恢復的管理節點。

g. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：`ssh-add -D`

5. 在來源管理節點上重新啟動服務： `service servermanager start`

恢復 **StorageGRID** 主要管理節點時還原 **Prometheus** 計量

或者、您可以將Prometheus維護的歷史數據保留在失敗的主要管理節點上。只有StorageGRID 當您的系統包含另一個管理節點時、才能還原Prometheus指標。

開始之前

- 已安裝並執行復原的管理節點。
- StorageGRID 系統至少包含兩個管理節點。
- 您有 `Passwords.txt`檔案。
- 您有資源配置通關密碼。

關於這項工作

如果管理節點故障、管理節點上Prometheus資料庫中所維護的度量將會遺失。當您恢復管理節點時、軟體安裝程序會建立新的Prometheus資料庫。在恢復的管理節點啟動後、它會記錄指標、就像您已執行StorageGRID 全新的作業系統安裝一樣。

如果您還原了主管理節點、StorageGRID 且您的Estring系統有另一個管理節點、您可以將Prometheus資料庫從非主管理節點（_SOURUS管理節點）複製到恢復的主管理節點、以還原歷史指標。如果您的系統只有主要管理

節點、則無法還原 Prometheus 資料庫。

> 複製Prometheus資料庫可能需要一小時以上的時間。當服務在來源管理節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。
2. 從來源管理節點停止 Prometheus 服務： `service prometheus stop`
3. 在恢復的管理節點上完成下列步驟：
   a. 登入恢復的管理節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。
   b. 停止 Prometheus 服務： `service prometheus stop`
   c. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`
   d. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。
   e. 將 Prometheus 資料庫從來源管理節點複製到復原的管理節點： `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出現提示時、按* Enter *確認您要銷毀「恢復的管理節點」上的新Prometheus資料庫。

      原始的Prometheus資料庫及其歷史資料會複製到恢復的管理節點。複製作業完成後、指令碼會啟動恢復的管理節點。此時會顯示下列狀態：

   資料庫已複製、正在啟動服務

   a. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：`ssh-add -D`
4. 在來源管理節點上重新啟動 Prometheus 服務.`service prometheus start`

使用非主要管理節點從主要管理節點故障中恢復

使用非主要管理節點從 **StorageGRID** 主要管理節點故障中恢復

若要使用非主要管理節點從主要管理節點故障中恢復，您必須完成一組特定的任務。主要管理節點託管網格的組態管理節點 (CMN) 服務。

請依照以下高階步驟，使用非主要管理節點恢復主要管理節點：

1. "從故障的主要管理節點複製稽核記錄"
2. "取代主要管理節點"
3. "選擇「開始恢復」以設定主管理節點"
4. "判斷主要管理節點的 Hotfix 需求"
5. "在恢復的主要管理節點上還原稽核記錄"
6. "恢復主管理節點時、請還原Prometheus指標"

從發生故障的主要管理節點複製 **StorageGRID** 稽核日誌

如果您能夠從故障的主要管理節點複製稽核記錄、則應保留這些記錄、以維護網格的系統活動和使用記錄。您可以在保留的稽核記錄啟動並執行後、將其還原至恢復的主要管理節點。

關於這項工作

此程序會將稽核記錄檔從故障的管理節點複製到個別網格節點上的暫用位置。然後、這些保留的稽核記錄就可以複製到替換的管理節點。稽核記錄不會自動複製到新的管理節點。

視故障類型而定、您可能無法從故障的管理節點複製稽核記錄。如果部署只有一個管理節點、則恢復的管理節點會在新的空白檔案中、開始將事件記錄到稽核記錄、而先前記錄的資料也會遺失。如果部署包含多個管理節點、您可以從另一個管理節點恢復稽核記錄。

> 如果現在無法在故障的管理節點上存取稽核記錄、您可能可以稍後存取這些記錄、例如在主機恢復之後。

步驟

1. 如果可能，請登入發生故障的主管理節點。否則，請登入任何可用的管理節點。
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令以切換至 root 使用者帳戶： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

      當您以 root 登入時、提示會從變更 `$`為 `#`。
2. 停止 AMS 服務以防止其建立新的記錄檔：`service ams stop`
3. 瀏覽至稽核匯出目錄：

   ```
   cd /var/local/audit/export
   ```

   （或者 `cd /var/local/log`在早期系統上）
4. 將來源日誌檔案重新命名為唯一編號的檔案名稱。

- 如果日誌檔案位於 `/var/local/audit/export`目錄，其名稱是 `audit.log`。
- 如果日誌檔案位於 `/var/local/log`目錄，其名稱是 `localaudit.log`。

例如，重新命名 `localaudit.log`文件到 `2025-10-22.txt.1`。

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```

5. 重新啟動 AMS 服務： `service ams start`
6. 建立目錄、將所有稽核記錄檔複製到個別網格節點上的暫存位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出現提示時，輸入管理員使用者帳戶的密碼。

7. 將所有稽核記錄檔複製到暫存位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出現提示時，輸入管理員使用者帳戶的密碼。

8. 以 root 使用者身分登出： `exit`。

使用非主要管理節點取代 **StorageGRID** 主要管理節點

若要恢復主管理節點、您必須先更換實體或虛擬硬體。

- 您可以將發生故障的主要管理節點替換為在同一平台上執行的主要管理節點。
- 您可以將執行在 VMware 或 Linux 主機上的主要管理節點取代為託管在 StorageGRID 服務應用裝置上的主要管理節點。
- 您可以將執行在 VMware 主機上的主要管理節點替換為 SG1000 或 SG100 服務應用裝置。

請使用符合您為節點所選替換平台的程序。完成節點更換程序（適用於所有節點類型）之後、該程序將引導您進行主要管理節點恢復的下一步。

替換平台	程序
VMware	"將 VMware 節點替換為恢復節點" "將 VMware 節點替換為 SG1000 或 SG100 服務應用裝置"
Linux	"更換Linux節點"
服務應用裝置	"更換服務應用裝置"

替換平台	程序
OpenStack	NetApp提供的OpenStack虛擬機器磁碟檔案和指令碼不再支援還原作業。如果您需要恢復在OpenStack部署中執行的節點、請下載適用於您Linux作業系統的檔案。然後，請遵循的程序"更換 Linux 節點"。

選擇「開始恢復」以設定主要管理節點

更換主要管理節點後，必須在 Grid Manager 中選擇「開始恢復」，將新節點設定為故障節點的替換節點。

開始之前

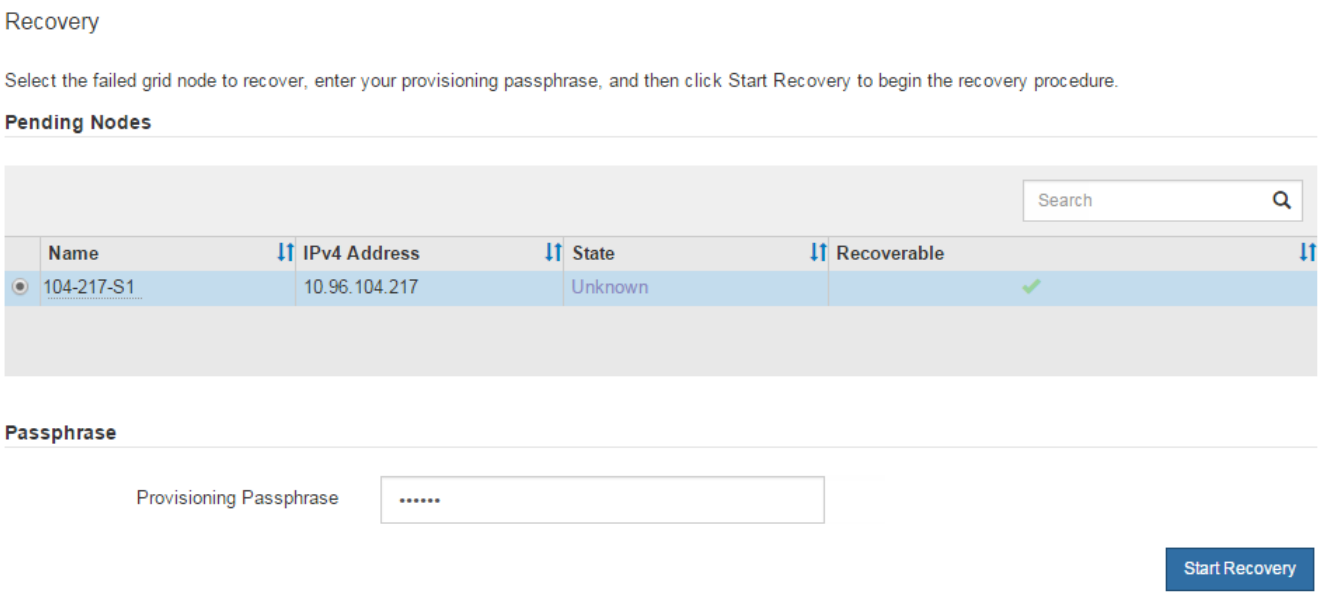
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您已部署並設定替換節點。

步驟

1. 從 Grid Manager 中，選擇 **Maintenance** > **Tasks** > **Node recovery**。
2. 在「Pending Node」（擱置節點）清單中選取您要恢復的網格節點。

   節點在故障後會出現在清單中、但您無法選取節點、直到節點重新安裝並準備好恢復為止。

3. 請輸入*佈建密碼*。
4. 選擇 **Start recovery**。



5. 監控恢復網格節點表格中的恢復進度。

恢復程序執行時，您可以選取 **Reset** 來啟動新的恢復。此時會出現一個對話方塊，提示若您重設程序，節點將處於不確定狀態。

如果您想在重設程序後重試恢復、則必須將節點還原至預先安裝的狀態、如下所示：

- * VMware*：刪除已部署的虛擬網格節點。然後、當您準備好重新啟動恢復時、請重新部署節點。
- **Linux** ：在 Linux 主機上執行以下命令、重新啟動節點： `storagegrid node force-recovery node-name`
- * 應用裝置 * ：如果您想在重設程序後重試恢復、您必須在節點上執行、將應用裝置節點還原為預先安裝的狀態 `sgareinstall`。請參閱。 "準備設備以重新安裝（僅限平台更換）"

6. 如果StorageGRID 您的支援系統啟用單一登入（SSO）、且您所恢復之管理節點的依賴方信任已設定為使用預設管理介面憑證、請更新（或刪除及重新建立）節點在Active Directory Federation Services（AD FS）中的依賴方信任。使用在管理節點還原程序期間所產生的新預設伺服器憑證。

若要配置信賴方信任，請參閱"設定單一登入"。若要存取預設伺服器證書，請登入管理節點的命令 shell。前往 `/var/local/mgmt-api`目錄，然後選擇 `server.crt`文件。

確定主要管理節點的 **StorageGRID Hotfix** 要求

恢復主要管理節點後，確定是否需要套用 Hotfix。

開始之前

主管理節點恢復已完成。

步驟

1. 使用登入 Grid Manager "支援的網頁瀏覽器"。
2. 選擇*節點*。
3. 從左側清單中選取主要管理節點。
4. 在「總覽」索引標籤上、記下「軟體版本」欄位中顯示的版本。
5. 選取任何其他網格節點。
6. 在「概覽」標籤上，記下「軟體版本」欄位中顯示的版本。
   - 如果 * 軟體版本 * 欄位中顯示的版本相同、您就不需要套用 Hotfix 。
   - 如果 * 軟體版本 * 欄位中顯示的版本不同、您必須"套用 Hotfix"將復原的主要管理節點更新為相同版本。

在已恢復的主要管理節點上還原 **StorageGRID** 稽核日誌

如果您能夠從故障的主要管理節點保留稽核記錄、則可以將其複製到您要恢復的主要管理節點。

開始之前

- 已安裝並執行復原的管理節點。
- 在原始管理節點失敗之後、您已將稽核記錄複製到其他位置。

關於這項工作

如果管理節點失敗、儲存至該管理節點的稽核記錄可能會遺失。您可以從故障的管理節點複製稽核記錄、然後將這些稽核記錄還原至恢復的管理節點、以避免資料遺失。視故障而定、可能無法從故障的管理節點複製稽核記錄。在這種情況下、如果部署有多個管理節點、您可以從另一個管理節點恢復稽核記錄、因為稽核記錄會複寫到所有管理節點。

如果只有一個管理節點、而且無法從故障節點複製稽核記錄、則復原的管理節點會開始將事件記錄到稽核記錄檔、就像是新安裝一樣。

您必須盡快恢復管理節點、才能還原記錄功能。

> 根據預設、稽核資訊會傳送至管理節點上的稽核記錄。如果下列任一項適用、您都可以跳過這些步驟：
>
> - 您已設定外部syslog伺服器、稽核記錄現在會傳送至syslog伺服器、而非管理節點。
> - 您明確指定稽核訊息只能儲存在產生這些訊息的本機節點上。
>
> 看"設定日誌管理和外部系統日誌伺服器"了解詳情。

步驟

1. 登入恢復的管理節點：
   a. 輸入下列命令： `ssh admin@recovery_Admin_Node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   以 root 登入後、提示會從變更 `$`為 `#`。
2. 檢查哪些審計文件已被儲存： `cd /var/local/audit/export`
3. 將保留的稽核記錄檔複製到復原的管理節點： `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   出現提示時、輸入admin的密碼。
4. 為了安全起見、請在確認已成功複製稽核記錄到恢復的管理節點之後、從故障的網格節點刪除這些記錄。
5. 更新已復原的管理節點上的稽核日誌檔案的使用者和群組設定： `chown ams-user:bycast *`
6. 以 root 身分登出： `exit`

恢復 **StorageGRID** 主要管理節點時還原 **Prometheus** 計量

或者、您可以將Prometheus維護的歷史數據保留在失敗的主要管理節點上。只有StorageGRID 當您的系統包含另一個管理節點時、才能還原Prometheus指標。

開始之前

- 已安裝並執行復原的管理節點。

- StorageGRID 系統至少包含兩個管理節點。
- 您有 `Passwords.txt`檔案。
- 您有資源配置通關密碼。

關於這項工作

如果管理節點故障、管理節點上Prometheus資料庫中所維護的度量將會遺失。當您恢復管理節點時、軟體安裝程序會建立新的Prometheus資料庫。在恢復的管理節點啟動後、它會記錄指標、就像您已執行StorageGRID 全新的作業系統安裝一樣。

如果您還原了主管理節點、StorageGRID 且您的Estring系統有另一個管理節點、您可以將Prometheus資料庫從非主管理節點（_SOURUS管理節點）複製到恢復的主管理節點、以還原歷史指標。如果您的系統只有主要管理節點、則無法還原 Prometheus 資料庫。

> 複製Prometheus資料庫可能需要一小時以上的時間。當服務在來源管理節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。
2. 從來源管理節點停止 Prometheus 服務： `service prometheus stop`
3. 在恢復的管理節點上完成下列步驟：
   a. 登入恢復的管理節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。
   b. 停止 Prometheus 服務： `service prometheus stop`
   c. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`
   d. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。
   e. 將 Prometheus 資料庫從來源管理節點複製到復原的管理節點：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出現提示時、按* Enter *確認您要銷毀「恢復的管理節點」上的新Prometheus資料庫。

      原始的Prometheus資料庫及其歷史資料會複製到恢復的管理節點。複製作業完成後、指令碼會啟動恢復的管理節點。此時會顯示下列狀態：

資料庫已複製、正在啟動服務

a. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：`ssh-add -D`

4. 在來源管理節點上重新啟動 Prometheus 服務.`service prometheus start`

從非主要管理節點故障中恢復

從 **StorageGRID** 非主要管理節點故障中恢復

您必須完成下列工作、才能從非主要管理節點故障中恢復。一個管理節點裝載組態管理節點（CMN）服務、稱為主要管理節點。雖然您可以擁有多個管理節點、但每StorageGRID個支援系統僅包含一個主要管理節點。所有其他管理節點均為非主要管理節點。

請遵循下列高階步驟來恢復非主要管理節點：

1. "從故障的非主要管理節點複製稽核記錄"
2. "更換非主要管理節點"
3. "選取「開始恢復」以設定非主要管理節點"
4. "在恢復的非主管理節點上還原稽核記錄"
5. "還原非主要管理節點時、請還原管理節點資料庫"
6. "還原非主要管理節點時的 Prometheus 指標"

從發生故障的 **StorageGRID** 非主要管理節點複製稽核日誌

如果您能夠從故障的管理節點複製稽核記錄、則應保留這些記錄、以維護網格的系統活動和使用記錄。您可以在已恢復的非主要管理節點啟動並執行之後、將保留的稽核記錄還原至該節點。

此程序會將稽核記錄檔從故障的管理節點複製到個別網格節點上的暫用位置。然後、這些保留的稽核記錄就可以複製到替換的管理節點。稽核記錄不會自動複製到新的管理節點。

視故障類型而定、您可能無法從故障的管理節點複製稽核記錄。如果部署只有一個管理節點、則恢復的管理節點會在新的空白檔案中、開始將事件記錄到稽核記錄、而先前記錄的資料也會遺失。如果部署包含多個管理節點、您可以從另一個管理節點恢復稽核記錄。

> 如果現在無法在故障的管理節點上存取稽核記錄、您可能可以稍後存取這些記錄、例如在主機恢復之後。

1. 如有可能、請登入故障的管理節點。否則、請登入主要管理節點或其他管理節點（若有）。
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 停止 AMS 服務以防止其建立新的記錄檔：`service ams stop`
3. 瀏覽至稽核匯出目錄：

   `cd /var/local/audit/export/`

4. 將來源 audit.log 檔案重新命名為唯一編號的檔案名稱。例如，將 audit.log 檔案重新命名為 `2023-10-25.txt.1`。

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. 重新啟動 AMS 服務：`service ams start`
6. 建立目錄、將所有稽核記錄檔複製到個別網格節點上的暫存位置：`ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出現提示時、輸入admin的密碼。

7. 將所有稽核記錄檔複製到暫存位置：`scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出現提示時、輸入admin的密碼。

8. 以 root 身分登出：`exit`

替換 **StorageGRID** 非主要管理節點

若要恢復非主要管理節點、您必須先更換實體或虛擬硬體。

您可以使用在同一個平台上執行的非主要管理節點來取代故障的非主要管理節點、也可以將在VMware上執行的非主要管理節點、或將Linux主機上裝載的非主要管理節點、替換成在服務應用裝置上的非主要管理節點。

請使用符合您為節點所選替換平台的程序。完成節點更換程序（適用於所有節點類型）之後、該程序將引導您進行非主要管理節點還原的下一步。

替換平台	程序
VMware	"更換VMware節點"
Linux	"更換Linux節點"
服務應用裝置	"更換服務應用裝置"
OpenStack	NetApp提供的OpenStack虛擬機器磁碟檔案和指令碼不再支援還原作業。如果您需要恢復在OpenStack部署中執行的節點、請下載適用於您Linux作業系統的檔案。然後，請遵循的程序"更換 Linux 節點"。

更換非主要管理節點之後、您必須在Grid Manager中選取「Start Recovery」（開始還原）、將新節點設定為故障節點的替換節點。

開始之前

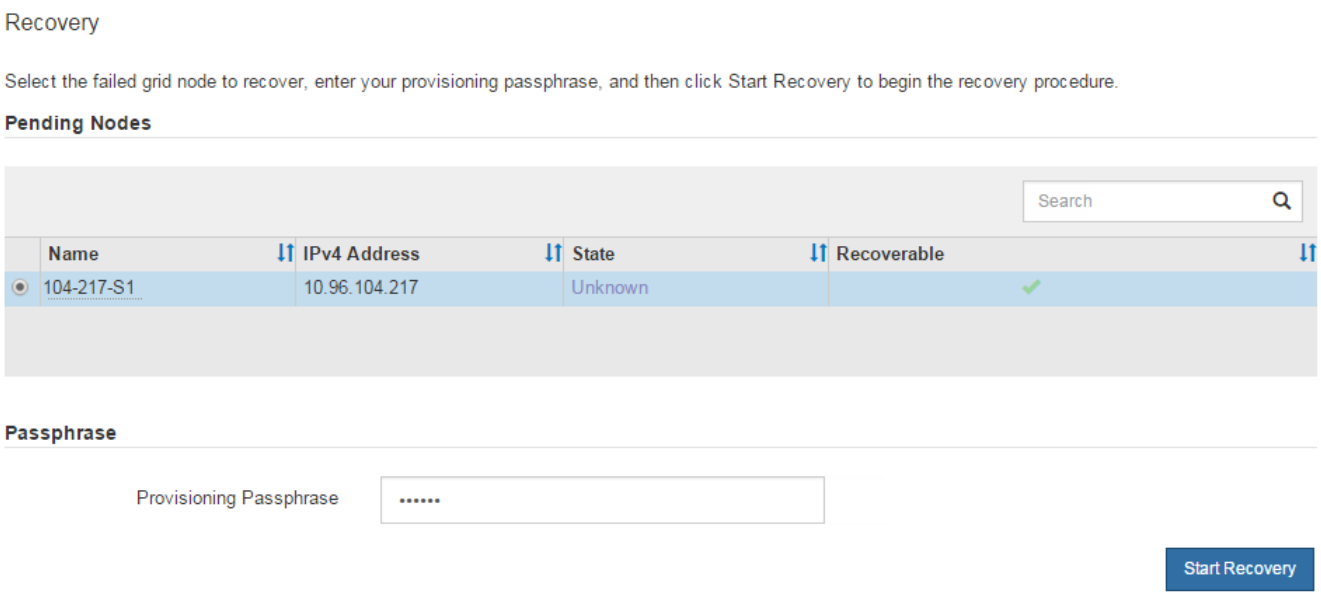
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您已部署並設定替換節點。

步驟

1. 從 Grid Manager 中，選擇 **Maintenance** > **Tasks** > **Node recovery**。
2. 在「Pending Node」（擱置節點）清單中選取您要恢復的網格節點。

   節點在故障後會出現在清單中、但您無法選取節點、直到節點重新安裝並準備好恢復為止。

3. 請輸入*佈建密碼*。
4. 選擇 **Start recovery**。



5. 監控恢復網格節點表格中的恢復進度。

   恢復程序執行時，您可以選取 **Reset** 來啟動新的恢復。此時會出現一個對話方塊，提示若您重設程序，節點將處於不確定狀態。

   如果您想在重設程序後重試恢復、則必須將節點還原至預先安裝的狀態、如下所示：

   - * VMware*：刪除已部署的虛擬網格節點。然後、當您準備好重新啟動恢復時、請重新部署節點。
   - **Linux** ：在 Linux 主機上執行以下命令、重新啟動節點： `storagegrid node force-recovery` *`node-name`*

◦ * 應用裝置 * ：如果您想在重設程序後重試恢復、您必須在節點上執行、將應用裝置節點還原為預先安裝的狀態 `sgareinstall`。請參閱。 "準備設備以重新安裝（僅限平台更換）"

6. 如果StorageGRID 您的支援系統啟用單一登入（SSO）、且您所恢復之管理節點的依賴方信任已設定為使用預設管理介面憑證、請更新（或刪除及重新建立）節點在Active Directory Federation Services（AD FS）中的依賴方信任。使用在管理節點還原程序期間所產生的新預設伺服器憑證。

若要配置信賴方信任，請參閱"設定單一登入"。若要存取預設伺服器證書，請登入管理節點的命令 shell。前往 `/var/local/mgmt-api`目錄，然後選擇 `server.crt`文件。

在已恢復的 **StorageGRID** 非主要管理節點上還原稽核日誌

如果您能夠從故障的非主要管理節點保留稽核記錄、以便保留歷史稽核記錄資訊、您可以將其複製到您要恢復的非主要管理節點。

開始之前

- 已安裝並執行復原的管理節點。
- 在原始管理節點失敗之後、您已將稽核記錄複製到其他位置。

關於這項工作

如果管理節點失敗、儲存至該管理節點的稽核記錄可能會遺失。您可以從故障的管理節點複製稽核記錄、然後將這些稽核記錄還原至恢復的管理節點、以避免資料遺失。視故障而定、可能無法從故障的管理節點複製稽核記錄。在這種情況下、如果部署有多個管理節點、您可以從另一個管理節點恢復稽核記錄、因為稽核記錄會複寫到所有管理節點。

如果只有一個管理節點、而且無法從故障節點複製稽核記錄、則復原的管理節點會開始將事件記錄到稽核記錄檔、就像是新安裝一樣。

您必須盡快恢復管理節點、才能還原記錄功能。

根據預設、稽核資訊會傳送至管理節點上的稽核記錄。如果下列任一項適用、您都可以跳過這些步驟：

- 您已設定外部syslog伺服器、稽核記錄現在會傳送至syslog伺服器、而非管理節點。
- 您明確指定稽核訊息只能儲存在產生這些訊息的本機節點上。

看"設定日誌管理和外部系統日誌伺服器"了解詳情。

步驟

1. 登入恢復的管理節點：

   a. 輸入下列命令：
   `ssh admin@recovery_Admin_Node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

以 root 登入後、提示會從變更 `$`為 `#`。

2. 檢查哪些稽核檔案已保留：

```
cd /var/local/log
```

3. 將保留的稽核記錄檔複製到恢復的管理節點：

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

出現提示時、輸入admin的密碼。

4. 為了安全起見、請在確認已成功複製稽核記錄到恢復的管理節點之後、從故障的網格節點刪除這些記錄。
5. 更新已恢復管理節點上稽核記錄檔的使用者和群組設定：

```
chown ams-user:bycast *
```

6. 以 root 身分登出： `exit`

復原非主要管理節點時還原 **StorageGRID** 管理節點資料庫

如果您想要保留失敗的非主要管理節點上的屬性和警示歷史資訊、可以從主要管理節點還原管理節點資料庫。

開始之前

- 已安裝並執行復原的管理節點。
- StorageGRID 系統至少包含兩個管理節點。
- 您有 `Passwords.txt`檔案。
- 您有資源配置通關密碼。

關於這項工作

如果管理節點故障、儲存在管理節點資料庫中的歷史資訊將會遺失。此資料庫包含下列資訊：

- 警示記錄
- 歷史屬性資料，用於節點頁面上的圖表。

當您還原管理節點時、軟體安裝程序會在還原的節點上建立一個空白的管理節點資料庫。不過、新資料庫僅包含目前屬於系統一部分或稍後新增的伺服器和服務資訊。

如果還原非主要管理節點、您可以將管理節點資料庫從主要管理節點（*SOURDE*管理節點）複製到還原節點、以還原歷史資訊。

> 複製管理節點資料庫可能需要數小時的時間。當服務在來源節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：

a. 輸入下列命令： `ssh admin@grid_node_IP`

b. 輸入檔案中列出的密碼 `Passwords.txt`。

c. 輸入以下命令切換到 root ： `su -`

d. 輸入檔案中列出的密碼 `Passwords.txt`。

2. 從來源管理節點執行下列命令。然後、在出現提示時輸入資源配置複雜密碼。 `recover-access-points`
3. 從來源管理節點停止 MI 服務： `service mi stop`
4. 從來源管理節點停止管理應用程式介面（ mgmt-API ）服務： `service mgmt-api stop`
5. 在恢復的管理節點上完成下列步驟：

a. 登入恢復的管理節點：

i. 輸入下列命令： `ssh admin@grid_node_IP`

ii. 輸入檔案中列出的密碼 `Passwords.txt`。

iii. 輸入以下命令切換到 root ： `su -`

iv. 輸入檔案中列出的密碼 `Passwords.txt`。

b. 停止 MI 服務： `service mi stop`

c. 停止 mgmt-API 服務： `service mgmt-api stop`

d. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`

e. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。

f. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：`ssh-add -D`

6. 在來源管理節點上重新啟動服務： `service servermanager start`

恢復 **StorageGRID** 非主要管理節點時還原 **Prometheus** 計量

或者、您可以將Prometheus維護的歷史數據保留在失敗的非主要管理節點上。

開始之前

- 已安裝並執行復原的管理節點。
- StorageGRID 系統至少包含兩個管理節點。
- 您有 `Passwords.txt`檔案。
- 您有資源配置通關密碼。

關於這項工作

如果管理節點故障、管理節點上Prometheus資料庫中所維護的度量將會遺失。當您恢復管理節點時、軟體安裝程序會建立新的Prometheus資料庫。在恢復的管理節點啟動後、它會記錄指標、就像您已執行StorageGRID 全新的作業系統安裝一樣。

如果還原非主要管理節點、您可以將Prometheus資料庫從主要管理節點（*SOURUS*管理節點）複製到恢復的管理節點、以還原歷史指標。

複製Prometheus資料庫可能需要一小時以上的時間。當服務在來源管理節點上停止時、部分Grid Manager功能將無法使用。

步驟

1. 登入來源管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 輸入以下命令切換到 root ： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。
2. 從來源管理節點停止 Prometheus 服務： `service prometheus stop`
3. 在恢復的管理節點上完成下列步驟：
   a. 登入恢復的管理節點：
      i. 輸入下列命令： `ssh admin@grid_node_IP`
      ii. 輸入檔案中列出的密碼 `Passwords.txt`。
      iii. 輸入以下命令切換到 root ： `su -`
      iv. 輸入檔案中列出的密碼 `Passwords.txt`。
   b. 停止 Prometheus 服務： `service prometheus stop`
   c. 將SSH私密金鑰新增至SSH代理程式。輸入：`ssh-add`
   d. 輸入檔案中列出的 SSH 存取密碼 `Passwords.txt`。
   e. 將 Prometheus 資料庫從來源管理節點複製到復原的管理節點：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出現提示時、按* Enter *確認您要銷毀「恢復的管理節點」上的新Prometheus資料庫。

      原始的Prometheus資料庫及其歷史資料會複製到恢復的管理節點。複製作業完成後、指令碼會啟動恢復的管理節點。此時會顯示下列狀態：

   資料庫已複製、正在啟動服務

   a. 當您不再需要無密碼存取其他伺服器時、請從SSH代理程式移除私密金鑰。輸入：`ssh-add -D`
4. 在來源管理節點上重新啟動 Prometheus 服務.`service prometheus start`

從閘道節點故障中恢復

替換 StorageGRID Gateway Node

您可以將故障的閘道節點更換為在相同實體或虛擬硬體上執行的閘道節點、或是將在VMware上執行的閘道節點或Linux主機替換為在服務應用裝置上裝載的閘道節點。

您必須遵循的節點更換程序取決於更換節點將使用哪個平台。完成節點更換程序（適用於所有節點類型）之後、

該程序將引導您進行閘道節點恢復的下一步。

替換平台	程序
VMware	"更換VMware節點"
Linux	"更換Linux節點"
服務應用裝置	"更換服務應用裝置"
OpenStack	NetApp提供的OpenStack虛擬機器磁碟檔案和指令碼不再支援還原作業。如果您需要恢復在OpenStack部署中執行的節點、請下載適用於您Linux作業系統的檔案。然後，請遵循的程序"更換 Linux 節點"。

選擇 **Start Recovery** 以設定 **StorageGRID Gateway Node**

更換閘道節點之後、您必須在Grid Manager中選取「Start Recovery」（開始還原）、將新節點設定為故障節點的替換節點。

開始之前

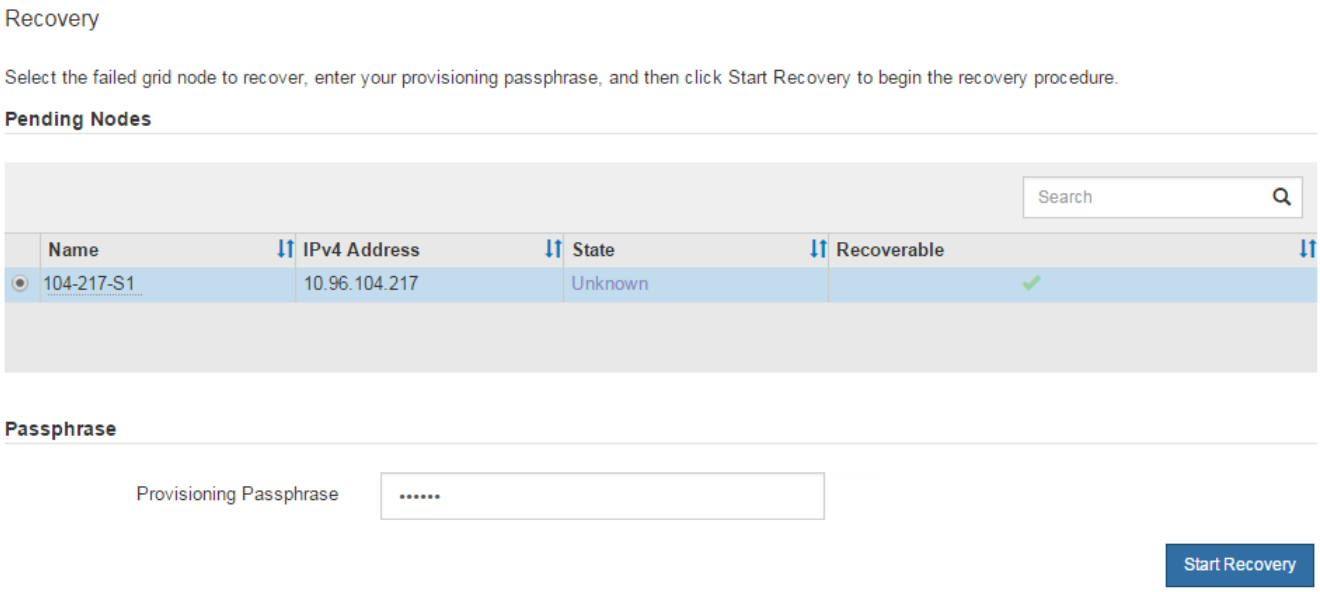
- 您已使用登入 Grid Manager "支援的網頁瀏覽器"。
- 您有"維護或根存取權限"。
- 您有資源配置通關密碼。
- 您已部署並設定替換節點。

步驟

1. 從 Grid Manager 中，選擇 **Maintenance** > **Tasks** > **Node recovery**。
2. 在「Pending Node」（擱置節點）清單中選取您要恢復的網格節點。

   節點在故障後會出現在清單中、但您無法選取節點、直到節點重新安裝並準備好恢復為止。

3. 請輸入*佈建密碼*。
4. 選擇 **Start recovery**。



5. 監控恢復網格節點表格中的恢復進度。

> 恢復程序執行時，您可以選取 **Reset** 來啟動新的恢復。此時會出現一個對話方塊，提示若您重設程序，節點將處於不確定狀態。

如果您想在重設程序後重試恢復、則必須將節點還原至預先安裝的狀態、如下所示：

- * VMware*：刪除已部署的虛擬網格節點。然後、當您準備好重新啟動恢復時、請重新部署節點。
- **Linux** ：在 Linux 主機上執行以下命令、重新啟動節點： `storagegrid node force-recovery node-name`
- * 應用裝置 * ：如果您想在重設程序後重試恢復、您必須在節點上執行、將應用裝置節點還原為預先安裝的狀態 `sgareinstall`。請參閱。 "準備設備以重新安裝（僅限平台更換）"

從歸檔節點故障中恢復

從 **StorageGRID** 歸檔節點故障中恢復

已移除對歸檔節點的支援。

有關恢復歸檔節點的信息，請參見 "從歸檔節點故障中恢復（ StorageGRID 11.8 doc 網站）"。

取代 **Linux** 節點

更換 **StorageGRID** 中的 **Linux** 節點

如果故障需要您部署一或多個新的實體或虛擬主機、或在現有主機上重新安裝 Linux 、請先部署並設定替換主機、然後才能恢復網格節點。此程序是所有類型網格節點的網格節點還原程序之一。

「Linux」指的是 Red Hat® Enterprise Linux® (RHEL)、Ubuntu® 或 Debian® 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

此程序只會在還原軟體型儲存節點、主要或非主要管理節點或閘道節點的程序中執行一步驟。無論您要恢復的網格節點類型為何、這些步驟都是相同的。

如果實體或虛擬 Linux 主機上託管了多個網格節點，您可以以任意順序恢復這些網格節點。但是，如果主要管理節點存在，則必須先恢復它，以避免其他網格節點在嘗試聯絡主要管理節點時阻塞恢復。如果您無法先恢復主要管理節點，但存在非主要管理節點，則可以使用該非主要管理節點以任意順序恢復節點。

為 StorageGRID 部署新的 Linux 主機

除了一些例外、您可以像在初始安裝程序中一樣、準備新的主機。

若要部署新的或重新安裝的實體或虛擬 Linux 主機，請依照適用於您的 Linux 作業系統的StorageGRID安裝說明中準備主機的步驟進行操作。看"安裝Linux" 。

> 「Linux」指的是 RHEL、Ubuntu 或 Debian 部署。有關受支援版本的列表，請參閱 "NetApp互通性對照表工具IMT （不含）"。

此程序包括完成下列工作的步驟：

1. 安裝Linux。
2. 設定主機網路。
3. 設定主機儲存設備。
4. 安裝Container引擎。
5. 安裝StorageGRID 支援服務。

> 完成安裝指示中的「安裝 StorageGRID 主機服務」工作後停止。請勿開始「部署網格節點」工作。

執行這些步驟時、請注意下列重要準則：

- 請務必使用與原始主機相同的主機介面名稱。
- 如果您使用共享儲存設備來支援 StorageGRID 節點、或是將部分或全部磁碟機或 SSD 從故障移至更換節點、則必須重新建立原始主機上的相同儲存對應。例如、如果您依照安裝指示中的建議使用 WWID 和別名、請務必在替換主機上使用 `/etc/multipath.conf`相同的別名 `/WWID` 配對 `/etc/multipath.conf`。
- 如果 StorageGRID 節點使用從 NetApp ONTAP 系統指派的儲存設備、請確認該磁碟區未啟用 FabricPool 分層原則。停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

> 切勿使用FabricPool 無法將StorageGRID 任何與還原StorageGRID 本身相關的資料分層。將StorageGRID 資料分層還原StorageGRID 至物件、可增加疑難排解和作業複雜度。

將 StorageGRID 節點還原至主機

若要將故障的網格節點還原至新的 Linux 主機、請執行下列步驟來還原節點組態檔案。

1. 還原並驗證節點還原節點組態檔案。對於新安裝、您可以為要安裝在主機上的每個網格節點建立節點組態檔案。將網格節點還原至替換主機時、您可以還原或取代任何故障網格節點的節點組態檔。
2. 啟動StorageGRID 「支援服務」 。
3. 如有需要復原無法啟動的任何節點、。

如果任何區塊儲存磁碟區是從先前的主機保留下來、您可能必須執行其他的還原程序。本節中的命令可協助您決定需要哪些額外程序。

還原及驗證網格節點

如果從非主要管理節點恢復節點，請將 ADMIN_IP 設定為該非主要管理節點的網格網路 IP 位址，以便恢復的節點向非主要管理節點註冊，而不是向主要管理節點註冊。若要檢視管理網路金鑰的規則，請參閱 "為 Linux 部署建立 StorageGRID 節點組態檔"。

您必須還原任何故障網格節點的網格組態檔、然後驗證網格組態檔並解決任何錯誤。

關於這項工作

您可以匯入任何應存在於主機上的網格節點、只要該節點的 `/var/local`磁碟區不會因前一主機故障而遺失。例如、 `/var/local`如果您將共用儲存設備用於 StorageGRID 系統資料磁碟區、則磁碟區可能仍存在、如適用於 Linux 作業系統的 StorageGRID 安裝指示所述。匯入節點會將其節點組態檔還原至主機。

如果無法匯入遺失的節點、您必須重新建立它們的網格組態檔案。

然後您必須驗證網格組態檔案、並解決任何可能發生的網路或儲存問題、才能繼續重新啟動StorageGRID 更新。當您重新建立節點的組態檔時、您必須使用與您要還原之節點相同的替換節點名稱。

查看"Linux 安裝說明"欲了解關於 `/var/local`節點的捲。

步驟

1. 在復原主機的命令列中、列出所有目前設定的 StorageGRID 節點：`sudo storagegrid node list`

   如果未設定任何網格節點、則不會有任何輸出。如果已設定某些網格節點、則預期輸出格式如下：

   ```
   Name               Metadata-Volume
   ============================================================
   dc1-adm1           /dev/mapper/sgws-adm1-var-local
   dc1-gw1            /dev/mapper/sgws-gw1-var-local
   dc1-sn1            /dev/mapper/sgws-sn1-var-local
   dc1-arc1           /dev/mapper/sgws-arc1-var-local
   ```

   如果未列出應在主機上設定的部分或全部網格節點、則需要還原遺失的網格節點。

2. 若要匯入具有磁碟區的網格節點 `/var/local`：

a. 針對您要匯入的每個節點執行下列命令：`sudo storagegrid node import node-var-local-volume-path`

> `storagegrid node import`只有當目標節點在上次執行的主機上正常關機時、命令才會成功。如果情況並非如此、您將會發現類似下列的錯誤：

```
This node (node-name) appears to be owned by another host (UUID host-uuid).

Use the --force flag if you are sure import is safe.
```

a. 如果您看到其他主機所擁有的節點發生錯誤、請再次執行命令並加上 `--force`旗標、以完成匯入：`sudo storagegrid --force node import node-var-local-volume-path`

> ⓘ 任何以旗標匯入的節點都 `--force`需要額外的恢復步驟、才能重新加入網格"接下來：視需要執行其他恢復步驟"、如所述。

3. 對於沒有 `/var/local`卷，重新建立節點的設定檔以將其恢復到主機。有關說明，請參閱"建立節點組態檔"。

> ⓘ 當您重新建立節點的組態檔時、您必須使用與您要還原之節點相同的替換節點名稱。對於Linux部署、請確定組態檔名稱包含節點名稱。您應該盡可能使用相同的網路介面、區塊裝置對應和IP位址。這種做法可將恢復期間需要複製到節點的資料量降至最低、這可能會使恢復速度大幅加快（在某些情況下、是幾分鐘而非數週）。

> ⓘ 如果您使用任何新的區塊裝置（ StorageGRID 節點先前未使用的裝置）做為任何組態變數的值、而這些設定變數是在重新建立節點的組態檔案時開始的 `BLOCK_DEVICE_`、請遵循中的準則修正遺失的區塊裝置錯誤。

4. 在恢復的主機上執行下列命令、列出所有StorageGRID 的支援節點。

```
sudo storagegrid node list
```

5. 驗證StorageGRID 每個網格節點的節點組態檔、其名稱會顯示在「節點清單」輸出中：

```
sudo storagegrid node validate node-name
```

您必須先解決任何錯誤或警告、才能開始StorageGRID 執行「支援服務」。以下各節將詳細說明在恢復期間可能具有特殊意義的錯誤。

修正遺失的網路介面錯誤

如果主機網路未正確設定或名稱拼錯、 StorageGRID 會在檢查檔案中指定的對應時發生錯誤 `/etc/storagegrid/nodes/node-name.conf`。

您可能會看到與此模式相符的錯誤或警告：

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

可能會針對Grid Network、管理網路或用戶端網路回報錯誤。此錯誤表示檔案會 `/etc/storagegrid/nodes/*node-name*.conf`將指定的 `StorageGRID` 網路對應到名為的主機介面、但目前主機上沒有使用該名稱的介面 `*host-interface-name*`。

如果收到此錯誤，請確認您已完成中的步驟"部署新的Linux主機"。對所有主機介面使用與原始主機相同的名稱。

如果無法命名主機介面以符合節點組態檔、您可以編輯節點組態檔、並變更GRID_NETWORD_target、ADD_NETWORD_target或用戶端網路目標的值、以符合現有的主機介面。

確定主機介面可存取適當的實體網路連接埠或VLAN、而且介面不會直接參照連結或橋接裝置。您必須在主機上的連結裝置上設定VLAN（或其他虛擬介面）、或使用橋接器和虛擬乙太網路（vith）配對。

修正遺失的區塊裝置錯誤

系統會檢查每個還原的節點是否對應到有效的區塊裝置特殊檔案、或是區塊裝置特殊檔案的有效軟體連結。如果StorageGRID 在檔案中找到無效的對應 `/etc/storagegrid/nodes/*node-name*.conf`、就會顯示遺失區塊裝置錯誤。

如果您發現與此模式相符的錯誤：

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

這表示會 `/etc/storagegrid/nodes/*node-name*.conf`將 *node-name* 使用的區塊裝置對應到 Linux 檔案系統中的指定路徑名稱、但該位置沒有有效的區塊 `PURPOSE`裝置特殊檔案或區塊裝置特殊檔案的軟連結。

確認您已完成中的步驟"部署新的Linux主機"。對所有區塊裝置使用與原始主機相同的持續裝置名稱。

如果您無法還原或重新建立遺失的區塊裝置特殊檔案、您可以分配適當大小和儲存類別的新區塊裝置、並編輯節點組態檔案、將值變更 `BLOCK_DEVICE_PURPOSE`為指向新區塊裝置特殊檔案。

使用 Linux 作業系統的表格確定適當的大小和儲存類別。看"儲存與效能需求" 。

查看以下建議"配置主機儲存"在繼續進行區塊設備替換之前。

> 如果您必須為任何組態檔案變數提供新的區塊儲存裝置、從開始、因為原始區塊裝置在發生故障的主機上遺失、請確保新的區 `BLOCK_DEVICE_`塊裝置未格式化、然後再嘗試進一步的恢復程序。如果您使用共享儲存設備並已建立新的Volume、則新的區塊裝置將不會格式化。如果您不確定、請針對任何新的區塊儲存設備特殊檔案執行下列命令。

僅針對新的區塊儲存裝置執行下列命令。如果您認為區塊儲存區仍包含要還原之節點的有效資料、請勿執行此命令、因為裝置上的任何資料都會遺失。

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

啟動StorageGRID 支援服務

若要啟動StorageGRID 您的支援節點、並確保在主機重新開機後重新啟動節點、您必須啟用StorageGRID 並啟動該支援中心服務。

步驟

1. 在每個主機上執行下列命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 執行下列命令以確保部署繼續進行：

```
sudo storagegrid node status node-name
```

3. 如果有任何節點傳回「未執行」或「已停止」的狀態、請執行下列命令：

```
sudo storagegrid node start node-name
```

4. 如果您先前已啟用並啟動StorageGRID 了「支援服務」（或如果您不確定服務是否已啟用並啟動）、請同時執行下列命令：

```
sudo systemctl reload-or-restart storagegrid
```

恢復無法正常啟動的節點

如果 StorageGRID 節點無法正常重新加入網格、且未顯示為可還原、則可能已毀損。您可以強制節點進入恢復模式。

步驟

1. 確認節點的網路組態正確無誤。

   由於網路介面對應不正確、或網格網路 IP 位址或閘道不正確、因此節點可能無法重新加入網格。

2. 如果網路組態正確、請發出 `force-recovery`命令：

   ```
   sudo storagegrid node force-recovery node-name
   ```

3. 執行節點的其他恢復步驟。請參閱。 "接下來：視需要執行其他恢復步驟"

執行額外的 StorageGRID 節點還原步驟

視您在StorageGRID 替換主機上執行的支援功能而定、您可能需要為每個節點執行額外的恢復步驟。

如果您在更換Linux主機或將故障的網格節點還原至新主機時、不需要採取任何修正行動、則節點還原即告完成。

修正行動與後續步驟

在節點更換期間、您可能需要採取下列其中一項修正行動：

- 您必須使用 `--force`旗標來匯入節點。
- 對於任何 `<PURPOSE>`、組態檔案變數的值 `BLOCK_DEVICE_<PURPOSE>`是指未包含與主機故障前相同資料的區塊裝置。
- 您已為節點發出 `storagegrid node force-recovery node-name`。
- 您已新增區塊裝置。

如果您採取*任何*這些修正行動、則必須執行其他恢復步驟。

恢復類型	下一步
主要管理節點	• "選擇「開始恢復」以設定主要管理節點" • "使用非主要管理節點恢復主要管理節點"
非主要管理節點	"選取「Start Recovery」（開始還原）以設定非主要管理節點"
閘道節點	"選取「Start Recovery（開始恢復）」以設定閘道節點"
儲存節點（軟體型）： • 如果您必須使用 `--force`旗標來匯入節點、或是您已核發 `storagegrid node force-recovery node-name` • 如果您必須重新安裝完整節點、或需要還原/var/local	"選取「Start Recovery（開始恢復）」以設定儲存節點"
儲存節點（軟體型）： • 如果您新增了區塊裝置。 • 如果 `<PURPOSE>`組態檔案變數的值 `BLOCK_DEVICE_<PURPOSE>`是指不包含與主機故障前相同資料的區塊裝置。	"從系統磁碟機不受影響的儲存磁碟區故障中恢復"

將 StorageGRID 中的 VMware 節點替換為恢復節點

當您恢復託管在 VMware 上的故障 StorageGRID 節點時、請移除故障節點並部署恢復節點。

開始之前

您已確定無法還原虛擬機器、因此必須更換該虛擬機器。

關於這項工作

您可以使用VMware vSphere Web Client、先移除與故障網格節點相關聯的虛擬機器。然後、您可以部署新的虛擬機器。

此程序只是網格節點還原程序的一個步驟。所有 VMware 節點（包括管理節點、儲存節點和閘道節點）的節點移除和部署程序都相同。

步驟

1. 登入VMware vSphere Web Client。
2. 瀏覽至故障的網格節點虛擬機器。
3. 記下部署恢復節點所需的所有資訊。
   a. 在虛擬機器上按一下滑鼠右鍵、選取*編輯設定*索引標籤、然後記下使用中的設定。
   b. 選取「* vApp選項*」索引標籤以檢視及記錄網格節點網路設定。
4. 如果故障的網格節點是儲存節點、請判斷用於資料儲存的任何虛擬硬碟是否未受損、並保留這些磁碟以重新附加至恢復的網格節點。
5. 關閉虛擬機器。
6. 選取*「動作*」>*「所有vCenter動作*」>*「從磁碟刪除*」以刪除虛擬機器。
7. 部署一個新的虛擬機器作為取代節點，並將其連接到一個或多個StorageGRID網路。有關說明，請參閱"將StorageGRID 節點部署為虛擬機器"。

   部署節點時、您可以選擇重新對應節點連接埠、或增加CPU或記憶體設定。

   部署新節點之後、您可以根據儲存需求新增虛擬磁碟、重新連接先前移除的故障網格節點所保留的任何虛擬硬碟、或兩者。

8. 根據您要恢復的節點類型、完成節點還原程序。

節點類型	前往
管理節點	"StorageGRID 中的主要或非主要管理節點恢復"
閘道節點	"選取「Start Recovery（開始恢復）」以設定閘道節點"
儲存節點	"選取「Start Recovery（開始恢復）」以設定儲存節點"

將 StorageGRID 中的 VMware 節點替換為 SG1000 或 SG100

如果主要管理節點以 VMware 節點執行，您可以將其替換為 SG1000 或 SG100 服務應用裝置。

> 完成並驗證節點替換後，必須刪除原有的 VMware 節點。如果舊節點保留在原地，一旦它重新上線，可能會導致嚴重的網格中斷。

開始之前

- 您已確定無法還原虛擬機器、因此必須更換該虛擬機器。
- 您已確認目前沒有正在進行的網格維護程序。
- 您已確認 SG1000 或 SG100 服務應用裝置上的 StorageGRID Appliance Installer 版本與您的 StorageGRID 系統軟體版本相符。
- 您擁有以下關於現有主管理節點的資訊：

  節點名稱：您必須使用與現有主要管理節點相同的節點名稱來安裝服務應用裝置。節點名稱即主機名稱（系統名稱）。

  IP 位址：您可以將服務應用裝置指派與現有主要管理節點相同的 IP 位址（建議），或者您可以為每個網路選擇一個新的未使用 IP 位址。

- 您有資源配置通關密碼。

步驟 1：替換 VMware 節點

首先，您需要在 Grid Manager 中移除現有的主管理節點。然後，使用 StorageGRID 應用裝置安裝程式將 SG1000 或 SG100 服務應用裝置安裝為新的主管理節點，並恢復該節點。如果您使用的是新的 IP 位址，則可以在移除現有主管理節點之前安裝服務應用裝置。

使用現有 **IP** 位址

使用現有主要管理節點 IP 位址取代主要管理節點。

步驟

1. 從 Grid Manager 下載恢復套件：
   a. 選擇 **Maintenance** > **Recovery package**。
   b. 輸入佈建密碼並下載套件。
2. 登入現有主管理節點：
   a. 輸入下列命令： `ssh admin@grid_node_IP`
   b. 輸入檔案中列出的密碼 `Passwords.txt`。
   c. 切換到根目錄： `su -`
   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。
3. "從現有主管理節點複製稽核日誌"。
4. 停止 Server Manager 和網格節點上的所有服務：

   ```
   shutdown -h now
   ```

   服務暫停最多需要 15 分鐘。
5. "安裝 SG1000 或 SG100 服務應用裝置"。
6. "部署 SG1000 或 SG100 服務應用裝置"。
7. 選擇 **Start installation** 後，大約需要十分鐘時間，安裝才能到達 **Load StorageGRID installer** 步驟。

   六到七分鐘後，瀏覽器會重新導向以開始恢復。
8. 檢查應用裝置的時鐘是否正確。
   a. 使用 SSH 連接到 8022 連接埠：
      i. 輸入命令： `ssh -p 8022 admin@grid_node_IP`。
      ii. 切換到根目錄： `su -`
      iii. 輸入 `netapp1!`。
   b. 請確認應用裝置時鐘與目前世界協調時 (UTC) 時間相差不超過幾分鐘。如有必要，請設定正確的日期和時間：

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```
9. 返回網頁瀏覽器並選擇 **Recover a failed primary Admin Node**。

10. 上傳您下載的恢復套件。
11. 輸入佈建密碼短語，然後選擇 **Start Recovery**。

    恢復進度列將顯示。請等待六到十分鐘，讓恢復程序完成並啟動服務。

12. 出現提示時，請登入 Grid Manager。

使用新的 **IP** 位址

使用新的 IP 位址取代主要管理節點。

步驟

1. "安裝 SG1000 或 SG100 服務應用裝置"。
2. 檢查應用裝置時鐘是否正確，以避免恢復期間出現 NTP 錯誤。
   a. 使用 SSH 連接到 8022 連接埠：
      i. 輸入命令： `ssh -p 8022 admin@grid_node_IP`。
      ii. 切換到根目錄： `su -`
      iii. 輸入 `netapp1!`。
   b. 請確認應用裝置時鐘與目前協調世界時 (UTC) 的誤差在幾分鐘以內。如有需要，請設定正確的日期和時間：

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```

3. 在 StorageGRID 應用裝置安裝程式中，前往 **Upload StorageGRID Software**，並檢查應用裝置上預先載入的軟體版本是否與網格上執行的 StorageGRID 版本相符。如果版本不符：
   a. 從 "NetApp 支援網站" 下載正確的 StorageGRID Debian 安裝套件。
   b. 選擇*移除*以移除安裝軟體。
   c. 上傳 `storagegrid-webscale-images-<sg-version>.deb`和 `storagegrid-webscale-images-<sgversion>.deb.md5`檔案。
4. 在 StorageGRID 應用裝置安裝程式的 Home 索引標籤上，選取 **Primary Admin (with Load Balancer)** 作為節點類型。
5. 請輸入節點名稱。節點名稱必須與現有主管理節點名稱一致。

   不要選擇 **Start Installation**。

6. 檢查新 IP 位址的子網路是否在網格網路中。如果新 IP 子網路不存在，請將其新增至網格網路：
   a. 在 Grid Manager 中，選擇 **Maintenance** > **Grid Network**。
   b. 輸入佈建密碼以更新子網路清單。
7. 從 Grid Manager 下載恢復套件：
   a. 選擇 **Maintenance** > **Recovery package**。
   b. 輸入佈建密碼，然後下載套件。

8. 登入現有主管理節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

9. "從現有主管理節點複製稽核日誌"。

10. 停止 Server Manager 和網格節點上的所有服務：

```
service servermanager stop
```

   服務暫停最多需要 15 分鐘。

11. 在 StorageGRID 應用裝置安裝程式主頁標籤上：

   a. 請驗證以下設定：

      - 節點類型設定為 **Primary Admin** （含負載平衡器）
      - 節點名稱與現有主要管理節點名稱相符

   b. 記錄新的 IP 位址。

12. 選擇 **Start Installation**。

   安裝大約需要 10 分鐘才能到達 載入 **StorageGRID** 安裝程式 步驟。

   六到七分鐘後，瀏覽器將會重新導向以開始恢復程式。

13. 檢查應用裝置的時鐘是否正確。

   a. 使用 SSH 連接到 8022 連接埠：

      i. 輸入命令： `ssh -p 8022 admin@grid_node_IP`。

      ii. 切換到根目錄： `su -`

      iii. 輸入 `netapp1!`。

   b. 請確認應用裝置時鐘與目前世界協調時 (UTC) 時間相差不超過幾分鐘。如有必要，請設定正確的日期和時間：

```
date -s "DD Mon YYYY HH:MM:SS"
```

14. 返回網頁瀏覽器，然後選擇 **Recover a failed primary Admin Node**。

15. 上傳您下載的恢復套件。

16. 輸入佈建密碼短語，然後選擇 **Start Recovery**。

主管理節點恢復頁面消失後又重新出現。如果再次選擇 **Start Recovery**， `500: Internal Server Error`則會出現，因為恢復已啟動，但無法將更新傳送至使用新 IP 位址的 Grid Manager。若要解決此問題，請更新 `/etc/hosts`檔案中的主管理節點 IP 位址：

a. 使用 SSH 連接到 8022 連接埠：

   i. 輸入命令： `ssh -p 8022 admin@grid_node_IP`。

   ii. 切換到根目錄： `su -`

   iii. 輸入檔案中列出的密碼 `Passwords.txt`。

b. 存取日誌：

```
tail /var/local/log/install.log
```

   您應該會重複看到以下錯誤： `curl: (7) Failed to connect to <primary_Admin_Node_name> port9999: No route to host`

   這是預期行為。StorageGRID 正在嘗試使用現有的主要管理節點 IP 位址、將更新傳送至主要管理節點。

c. 確認Container正在運作：

```
storagegrid node status
```

```
storagegrid node enter <primary_Admin_Node_name>
```

a. 在 Container 內的 `/etc/hosts`檔案中，將現有的主要管理節點 IP 位址替換為新的 IP 位址。

b. 儲存檔案。

c. 返回網頁瀏覽器。幾秒鐘後，恢復進度條將會出現。

   請等待六到十分鐘，以便恢復程序完成並啟動服務。

17. 出現提示時，請登入 Grid Manager。

18. 更新恢復套件：

a. 登入主要管理節點：

   i. 輸入下列命令： `ssh admin@primary_Admin_Node_IP`

   ii. 切換到根目錄： `su -`

   iii. 輸入以下命令： `change-ip`

b. 選擇選項 **3 –** 編輯管理網路子網路清單，然後新增子網路。

StorageGRID 會自動產生一個包含新主要管理節點 IP 位址的新恢復套件。

19. 從 Grid Manager 下載最新的恢復套件。

步驟 2：完成節點恢復

使用現有的非主要管理節點作為還原程序（稽核日誌、管理節點資料庫和 Prometheus 計量）的來源管理節點。如果網格沒有非主要管理節點，則可以使用要替換的原始 VMware 節點，前提是其執行的 IP 位址與已恢復的主要管理節點不同。

步驟

1. "還原稽核日誌"。
2. "還原管理節點資料庫"。
3. "還原 Prometheus 計量"。
4. 確認新的主管理節點運作正常。然後，立即刪除原有的虛擬機器節點或裸機 Container。

使用服務應用裝置來更換故障節點

使用服務應用裝置更換故障的 StorageGRID 節點

您可以使用服務應用裝置來復原故障的閘道節點、故障的非主要管理節點、或是位於 VMware 、 Linux 主機或服務應用裝置上的故障主要管理節點。此程序是網格節點還原程序的一個步驟。

開始之前

- 您已確定下列情況之一為真：
  - 無法還原主控節點的虛擬機器。
  - 網格節點的實體或虛擬Linux主機故障、必須更換。
  - 主控網格節點的服務應用裝置必須更換。
- 您已確認服務應用裝置上的 StorageGRID 應用裝置安裝程式版本與 StorageGRID 系統的軟體版本相符。請參閱。 "驗StorageGRID 證並升級版本的應用程式"

> 請勿在同一個站台同時部署 SG110 和 SG1100 服務應用裝置、或 SG100 和 SG1000 服務應用裝置。可能會導致無法預測的效能。

關於這項工作

在下列情況下、您可以使用服務應用裝置來恢復故障的網格節點：

- 故障節點託管在 VMware 或 Linux 上（"平台變更"）
- 故障節點託管在服務設備上（"平台更換"）

安裝 StorageGRID 服務應用裝置（僅限平台變更）

當您正在恢復 VMware 或 Linux 主機上託管的故障網格節點、並將服務應用裝置用於更換節點時、必須先使用與故障節點相同的節點名稱（系統名稱）來安裝新的應用裝置硬體。

開始之前

您有下列關於故障節點的資訊：

- 節點名稱：您必須使用與故障節點相同的節點名稱來安裝服務應用裝置。節點名稱為主機名稱（系統名稱）。
- * IP位址*：您可以為服務應用裝置指派與故障節點相同的IP位址（這是首選選選項）、也可以在每個網路上選取新的未使用IP位址。

關於這項工作

只有當您正在還原VMware或Linux上裝載的故障節點、並將其替換為服務應用裝置上裝載的節點時、才執行此程序。

步驟

1. 請依照指示安裝新的服務應用裝置。請參閱。 "硬體安裝快速入門"
2. 當系統提示您輸入節點名稱時、請使用故障節點的節點名稱。

準備 StorageGRID 設備以進行重新安裝 （僅限平台更換）

在恢復服務應用裝置上裝載的網格節點時、您必須先準備好應用裝置以重新安裝StorageGRID 該軟體。

只有在您要更換服務應用裝置上的故障節點時、才執行此程序。如果故障節點原本是託管在 VMware 或 Linux 主機上、請勿遵循這些步驟。

步驟

1. 登入故障的網格節點：

   a. 輸入下列命令： `ssh admin@grid_node_IP`

   b. 輸入檔案中列出的密碼 `Passwords.txt`。

   c. 輸入以下命令切換到 root ： `su -`

   d. 輸入檔案中列出的密碼 `Passwords.txt`。

   當您以 root 登入時、提示會從變更 `$`為 `#`。

2. 準備好產品以安裝StorageGRID 資訊軟體。輸入： `sgareinstall`
3. 當系統提示您繼續時、請輸入： `y`

   設備會重新開機、SSH工作階段也會結束。雖然有時您可能需要等待30分鐘、但使用起來通常需要5分鐘才能StorageGRID 使用《不知如何使用的應用程式」。

   服務應用裝置已重設、網格節點上的資料將無法再存取。在原始安裝程序期間所設定的IP位址應保持不變；不過、建議您在程序完成時確認。

   執行命令後 `sgareinstall`、所有 StorageGRID 提供的帳戶、密碼和 SSH 金鑰都會移除、並產生新的主機金鑰。

在服務設備上啟動 StorageGRID 軟體安裝

若要在服務應用裝置上安裝閘道節點或管理節點、請使用設備隨附的 StorageGRID 應用裝置安裝程式。

開始之前

- 此應用裝置安裝在機架中、連接至您的網路、並已開啟電源。
- 網路連結和 IP 位址是使用 StorageGRID 應用裝置安裝程式為應用裝置設定。
- 如果您要安裝 Gateway Node 或非主要 Admin Node，您需要知道以下任一 Admin Node 的 IP 位址：
  - StorageGRID 網格的主要管理節點
  - 如果存在非主要管理節點且該節點正用於恢復節點，則使用該非主要管理節點。
- 如果您使用非主要管理節點恢復節點（包括主要管理節點），則可以指定該管理節點的 IP 位址。
- StorageGRID 應用裝置安裝程式 IP 組態頁面上列出的所有網格網路子網路、都是在主要管理節點的網格網路子網路清單中定義。

  請參閱。 "硬體安裝快速入門"

- 您使用的是"支援的網頁瀏覽器"。
- 您已將其中一個 IP 位址指派給應用裝置。您可以使用管理網路、網格網路或用戶端網路的IP位址。
- 如果您安裝的是主管理節點、您可以StorageGRID 取得此版本的Ubuntu或DEBIANY安裝檔案。

> 製造過程中、服務應用裝置會預先載入最新版本StorageGRID 的支援軟體。如果預先載入的軟體版本與 StorageGRID 部署中使用的版本相符、則不需要安裝檔案。

關於這項工作

若要在服務應用裝置上安裝 StorageGRID 軟體：

- 對於主要管理節點，您需要指定節點名稱，然後上傳適當的軟體套件（如有需要）。如果您要還原主要管理節點，且您的網格中存在非主要管理節點，您可以選擇使用非主要管理節點還原節點並指定該管理節點的 IP 位址，或使用您目前的組態安裝或還原節點。
- 對於非主要管理節點或閘道節點、您可以指定或確認主要管理節點的IP位址和節點名稱。
- 您可以開始安裝、並在磁碟區已設定且已安裝軟體時等待。
- 在整個過程中、安裝會暫停一段時間。若要繼續安裝、您必須登入Grid Manager、並將擱置節點設定為故障節點的替代節點。
- 設定節點之後、應用裝置安裝程序便會完成、應用裝置也會重新開機。

步驟

1. 開啟瀏覽器、然後輸入服務應用裝置的其中一個 IP 位址。

   `https://Controller_IP:8443`

   畫面會出現「the不再安裝StorageGRID 程式」首頁。

2. 若要安裝主管理節點：
   a. 在「此節點」區段的「節點類型」中、選取「主要管理員」。
   b. 在「節點名稱」欄位中，輸入與要恢復的節點相同的名稱，然後選擇「儲存」。
   c. 請從「安裝模式」部分提供的兩種模式中選擇適當的模式。您可以選擇「Install a node or recover this node using current configuration」方法，也可以選擇「Recover this node using a non-primary Admin

Node」方法。

目前組態方法

使用目前組態安裝節點或恢復此節點。

i. 在「安裝」部分，檢查「目前狀態」下所列的軟體版本。如果準備安裝的軟體版本正確，請跳至 安裝步驟。

ii. 如果需要上傳其他版本的軟體，請在「進階」選單下選擇「上傳 StorageGRID 軟體」。此時將顯示「上傳 StorageGRID 軟體」頁面。

iii. 選擇 **Browse** 以上傳 StorageGRID 軟體的 **Software package** 和 **Checksum file**。選取檔案後，將自動上傳。

iv. 選擇 **Home** 以返回 StorageGRID Appliance Installer 首頁。

非主要管理節點方法

使用非主要管理節點恢復此節點。

i. 在非主要管理節點 IP 欄位中，輸入要用於恢復的非主要管理節點的網格網路 IP 位址，然後選擇 **Save**。

ii. 如果準備安裝的軟體版本正確，請跳至安裝步驟。

3. 若要安裝網關節點或非主管理節點：

a. 在「此節點」區段的「節點類型」中、根據您要還原的節點類型、選取「閘道」或「非主要管理員」。

b. 在「節點名稱」欄位中，輸入與要恢復的節點相同的名稱，然後選擇「儲存」。

c. 在「主要管理節點連線」區段中、判斷是否需要指定主要管理節點的IP位址。

如果主管理節點或至少有一個已設定ADD_IP的其他網格節點存在於同一個子網路中、則可使用此解決方案安裝程式自動探索此IP位址。StorageGRID

d. 如果未顯示此 IP 位址或您需要變更它，請指定位址：

選項	說明
手動輸入IP	a. 清除 * 啟用管理節點探索 * 核取方塊。 b. 手動輸入IP位址。 c. 選擇*保存*。 d. 等待新 IP 位址的連線狀態變成「就緒」。
自動探索所有連線的主要管理節點	a. 選中 * 啓用管理節點發現 * 複選框。 b. 從探索到的IP位址清單中、選取要部署此服務應用裝置之網格的主要管理節點。 c. 選擇*保存*。 d. 等待新 IP 位址的連線狀態變成「就緒」。

4. 在「安裝」區段中、確認目前狀態為「準備好開始安裝節點名稱」、且已啟用「開始安裝」按鈕。

   如果未啟用「開始安裝」按鈕，您可能需要變更網路設定或連接埠設定。請參閱您設備的維護說明。

5. 從 StorageGRID 應用裝置安裝程式首頁，選取 * 開始安裝 *。

   目前狀態變更為「Installation is in progress」，並顯示監控安裝頁面。

   如果需要手動存取 Monitor 安裝頁面，請從功能表列中選擇 **Monitor installation**。

監控 StorageGRID 服務應用裝置安裝

直到安裝完成為止、才會StorageGRID 顯示此狀態。軟體安裝完成後、即會重新啟動應用裝置。

步驟

1. 若要監控安裝進度，請從功能表列中選擇 **Monitor installation**。

   Monitor 安裝頁面會顯示安裝進度。

   藍色狀態列會指出目前正在進行的工作。綠色狀態列表示已成功完成的工作。

   安裝程式可確保先前安裝中完成的工作不會重新執行。如果您正在重新執行安裝、任何不需要重新執行的工作都會顯示綠色狀態列和「略過」狀態。

2. 檢閱前兩個安裝階段的進度。

   - **1.**設定儲存設備

     在此階段中、安裝程式會清除磁碟機的任何現有組態、並設定主機設定。

   - **2.**安裝作業系統

     在此階段、安裝程式會將基礎作業系統映像複製StorageGRID 到應用裝置、以供從主管理節點複製到應用裝置、或是從主要管理節點的安裝套件安裝基礎作業系統。

3. 繼續監控安裝進度、直到發生下列其中一項：

   - 若為應用裝置閘道節點或非主要應用裝置管理節點、則會StorageGRID 暫停「安裝**Sid**」階段、並在內嵌式主控台顯示訊息、提示您使用Grid Manager在管理節點上核准此節點。
   - 若為應用裝置主要管理節點StorageGRID 、則會出現第五階段（Load速度安裝程式）。如果第五階段進行超過10分鐘、請手動重新整理頁面。

4. 請前往您要還原之應用裝置網格節點類型的下一個還原程序步驟。

恢復類型	參考資料
閘道節點	"選取「Start Recovery（開始恢復）」以設定閘道節點"
非主要管理節點	"選取「Start Recovery」（開始還原）以設定非主要管理節點"

恢復類型	參考資料
主要管理節點	"設定替換的主要管理節點"

技術支援如何恢復 StorageGRID 站台

如果整個StorageGRID 站台故障或多個儲存節點故障、您必須聯絡技術支援部門。技術支援人員將評估您的情況、擬定恢復計畫、然後以符合業務目標的方式還原故障節點或站台、最佳化恢復時間、並防止不必要的資料遺失。

站台恢復只能由技術支援執行。

支援各種故障的支援能力強、您可以自行成功執行許多恢復與維護程序。StorageGRID不過、很難建立簡單、通用的站台還原程序、因為詳細步驟取決於您特定情況的因素。例如：

- 您的業務目標：StorageGRID 在完全失去一個景點之後、您應該評估如何最有效地達成您的業務目標。例如、您要就地重建遺失的站台嗎？您想要在StorageGRID 新位置更換遺失的景點嗎？每位客戶的情況都不同、您的恢復計畫必須針對您的優先事項而設計。
- * 故障的確切性質 * ：在開始站台恢復之前、請確定故障站台上的任何節點是否完整、或任何儲存節點是否包含可恢復的物件。如果您重新建置包含有效資料的節點或儲存磁碟區、可能會發生不必要的資料遺失。
- * 主動式 ILM 原則 * ：網格中物件複本的數量、類型和位置是由主動式 ILM 原則所控制。ILM 原則的細節可能會影響可恢復資料的數量、以及還原所需的特定技術。

  如果站台只包含物件的複本、且站台遺失、則物件會遺失。

- * 貯體（或容器）一致性 * ：套用至貯體（或容器）的一致性、會影響 StorageGRID 在告知用戶端物件擷取成功之前、是否將物件中繼資料完全複寫至所有節點和站台。如果一致性值允許最終一致性、則部分物件中繼資料可能會在站台故障中遺失。這可能會影響可恢復資料的數量、並可能影響恢復程序的詳細資料。
- * 最近變更的記錄 * ：還原程序的詳細資料可能會受到影響、因為故障發生時是否有任何維護程序正在進行、或是您的 ILM 原則是否有任何最近的變更。技術支援人員必須先評估網格的最新歷史記錄及目前狀況、然後才能開始站台恢復。

站台恢復只能由技術支援執行。

這是技術支援用於恢復故障站台的程序總覽：

1. 技術支援：
   a. 詳細評估故障。
   b. 與您一起檢視您的業務目標。
   c. 針對您的情況、擬定專屬的恢復計畫。
2. 如果主管理節點發生故障、技術支援會將其恢復。
3. 技術支援會依照以下概述、恢復所有儲存節點：
   a. 視需要更換儲存節點硬體或虛擬機器。

b. 將物件中繼資料還原至故障站台。

c. 將物件資料還原至恢復的儲存節點。

如果使用單一故障儲存節點的恢復程序、就會發生資料遺失。

當整個站台發生故障時、技術支援會使用特殊命令來成功還原物件和物件中繼資料。

4. 技術支援可恢復其他故障節點。

物件中繼資料和資料恢復後、技術支援會使用標準程序來恢復故障的閘道節點或非主要管理節點。

相關資訊

"站台取消委任"

StorageGRID解決方案和資源

前往 "StorageGRID解決方案和資源"了解如何在StorageGRID環境中測試和啟用應用程式。

如何使用NetApp控制台管理StorageGRID

前往 "使用NetApp控制台進行StorageGRID管理"了解如何使用 Grid Manager 從NetApp Console 管理您的StorageGRID系統，以及如何使用NetApp Console 的資料服務進行備份、資料分層等。

- BlueXP現在是NetApp控制台*

NetApp控制台建立在增強和重組的BlueXP基礎之上，可在企業級內部和雲端環境中集中管理NetApp儲存和NetApp資料服務，提供即時洞察、更快的工作流程和簡化的管理，並且高度安全且合規。

有關具體變更內容，請參閱... "NetApp控制台發行說明"。

法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp 、 Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

如需最新的 NetApp 擁有專利清單、請參閱：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

API許可證

本文檔不授予對StorageGRID S3 REST API 的任何授權或其他權利。使用或存取StorageGRID S3 REST API需要與NetApp簽訂單獨的授權協議，並且受該協議約束。

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

https://library.netapp.com/ecm/ecm_download_file/ECMLP3373066

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。