StorageGRID 解決方案與資源

StorageGRID solutions and resources

NetApp
December 12, 2025

目錄

StorageGRID 解決方案與資源

存取 StorageGRID 評估軟體的步驟

本指示適用於與 NetApp 合作的 NetApp 銷售人員、合作夥伴和潛在客戶。

註冊帳戶

1. 使用您的企業電子郵件在上註冊帳戶 "NetApp 支援網站" 。
   a. 請確定您未使用新建立的帳戶登入。
   b. 如果您已經有帳戶，請確定您尚未登入，然後繼續下一步。
2. 建立非技術支援案例、將存取層級提升至「潛在客戶」。若要這麼做、請按一下 ""回報問題"網站頁尾中的「」連結。
3. 選擇「註冊問題」作為意見回饋類別。
4. 在「意見」區段中，寫下：「我的帳戶電子郵件地址是 _ 您的電子郵件地址 _ 。我想讓潛在客戶存取下載 StorageGRID 評估軟體。」
   a. 提及 NetApp 內部人員的姓名、該人員建議您存取潛在客戶。

下載 StorageGRID

1. 在您的支援案例經過審查與核准之後、 NetApp 支援人員將透過電子郵件通知您您帳戶已獲授予潛在客戶存取權。
2. 下載 "StorageGRID 評估軟體"。

試用版授權檔案位於 zip 檔案中。檔案解壓縮後即為 StorageGRID-Webscale 、 <version> 、 vSphere\NLF000000.txt 。

下載軟體是一種程序、需要採取貿易法規遵循措施、以符合法律要求。為了確保法規遵循、使用者必須先建立帳戶並開啟支援案例、才能取得存取權。這項程序有助於我們維持適當的控制與文件記錄、同時為潛在客戶提供他們所需的正式作業軟體。

我們提供「正式作業就緒」版本的 StorageGRID 、這不是開放原始碼或替代版本。請務必注意、 * 除非潛在客戶升級至正式作業授權、否則不提供 * 支援 * 。

如有上述步驟的任何問題、請聯絡 StorageGRID.Feedback@netapp.com 。

已驗證的協力廠商解決方案

已驗證的協力廠商解決方案：總覽

NetApp與我們的合作夥伴合作、已驗證這些解決方案可搭配StorageGRID 使用。請檢閱本節中的資訊、瞭解哪些解決方案已通過驗證、並在適用的情況下取得其他指示。

與NetApp聯手加速產品組合創新、提高市場知名度、並在您建立經過測試、同級最佳的NetApp解決方案時提高銷售量。 "立即成為聯盟合作夥伴"。

StorageGRID 12.0 經過驗證的第三方解決方案

以下第三方解決方案已驗證可與StorageGRID 12.0 搭配使用。 + 如果您要尋找的解決方案未列出，請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Alluxio
- Apache Kafka
- AWS 安裝點
- Bridgestor
- Cantemo
- Citrix內容協同作業
- Collibra （ Collibra 資料品質最低版本 2024.02 ）
- CommVault 11.
- Couchbase 企業分析 2.0
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- 磁碟移轉資料
- 夢中
- 彈性搜尋快照（包括凍結層）
- Emam
- Fujifilm物件歸檔
- GitHub企業伺服器

- IBM FileNet
- IBM 儲存保護
- Interica
- Komprise
- Microsoft SQL Server巨量資料叢集
- 模型9.
- Modzy
- Moonwalk通用
- 很好
- Nasuni
- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- PixitMedia ngenea
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveville v10 build 220706或更新版本
- RRubrik CDM
- s3a
- 訊號
- 雪片
- SPECtra Logic on 一 Prem Glacier
- Splunk Smartstore
- Starburst
- 輕鬆儲存
- Trino
- Varish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本
- Vertica 10.x
- 維地松

- Virtalica StorageFabric
- Weka v3.10或更新版本

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- CommVault 11功能版本26
- IBM FileNet
- IBM 儲存保護
- OpenText文件21.4
- Rukrik
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 支援的關鍵管理程式

這些解決方案已通過測試。

- Entrust 加密安全平台 v10.4.5
- Entrust KeyControl 10.2.
- Hashicorp Vault 1.20.2
- 泰雷茲密碼信任管理器 2.20

StorageGRID 11.9 驗證的協力廠商解決方案

下列協力廠商解決方案已通過驗證、可搭配 StorageGRID 11.9 使用。+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Alluxio
- Apache Kafka
- AWS 安裝點
- Bridgestor
- Cantemo
- Citrix內容協同作業
- Collibra （ Collibra 資料品質最低版本 2024.02 ）
- CommVault 11.
- Couchbase 企業分析 2.0
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- 磁碟移轉資料
- 夢中
- 彈性搜尋快照（包括凍結層）
- Emam
- Fujifilm物件歸檔
- GitHub企業伺服器

- IBM FileNet
- IBM 儲存保護
- Interica
- Komprise
- Microsoft SQL Server巨量資料叢集
- 模型9.
- Modzy
- Moonwalk通用
- 很好
- Nasuni
- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- PixitMedia ngenea
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveville v10 build 220706或更新版本
- RRubrik CDM
- s3a
- 訊號
- 雪片
- SPECtra Logic on 一 Prem Glacier
- Splunk Smartstore
- Starburst
- 輕鬆儲存
- Trino
- Varish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本
- Vertica 10.x
- 維地松

- Virtalica StorageFabric
- Weka v3.10或更新版本

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- CommVault 11功能版本26
- IBM FileNet
- IBM 儲存保護
- OpenText文件21.4
- Rukrik
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 支援的關鍵管理程式

這些解決方案已通過測試。

- Entrust 加密安全平台 v10.4.5
- Entrust KeyControl 10.2.
- Hashicorp Vault 1.15.0
- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1.
- Thales CipherTrust Manager 2.2.
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4.
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9.
- Thales CipherTrust Manager 2.10
- Thales CipherTrust Manager 2.11.
- Thales CipherTrust Manager 2.12.
- Thales CipherTrust Manager 2.13
- Thales CipherTrust Manager 2.14
- Thales CipherTrust Manager 2.15
- Thales CipherTrust Manager 2.16
- 泰雷茲密碼信任管理器 2.20

StorageGRID 11.8 驗證的協力廠商解決方案

下列協力廠商解決方案已通過驗證、可搭配 StorageGRID 11.8 使用。+
如果未列出您要尋找的解決方案、請聯絡您的 NetApp 客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Alluxio
- Apache Kafka
- AWS 安裝點
- Bridgestor
- Cantemo
- Citrix內容協同作業
- Collibra （ Collibra 資料品質最低版本 2024.02 ）

- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- 磁碟移轉資料
- 夢中
- 彈性搜尋快照（包括凍結層）
- Emam
- Fujifilm物件歸檔
- GitHub企業伺服器
- IBM FileNet
- IBM 儲存保護
- Interica
- Komprise
- Microsoft SQL Server巨量資料叢集
- 模型9.
- Modzy
- Moonwalk通用
- 很好
- Nasuni
- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- PixitMedia ngenea
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveville v10 build 220706或更新版本
- RRubrik CDM
- s3a
- 訊號

- 雪片
- SPECtra Logic on － Prem Glacier
- Splunk Smartstore
- Starburst
- 輕鬆儲存
- Trino
- Varish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本
- Vertica 10.x
- 維地松
- Virtalica StorageFabric
- Weka v3.10或更新版本

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- CommVault 11功能版本26
- IBM FileNet
- IBM 儲存保護
- OpenText文件21.4
- Rukrik
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更新版本

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔

- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 支援的關鍵管理程式

這些解決方案已通過測試。

- Entrust KeyControl 10.2.
- Hashicorp Vault 1.15.0
- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1.
- Thales CipherTrust Manager 2.2.
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4.
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9.
- Thales CipherTrust Manager 2.10
- Thales CipherTrust Manager 2.11.
- Thales CipherTrust Manager 2.12.
- Thales CipherTrust Manager 2.13
- Thales CipherTrust Manager 2.14

StorageGRID 11.7 驗證的協力廠商解決方案

下列協力廠商解決方案已通過驗證、可搭配 StorageGRID 11.7 使用。+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動

- Alluxio
- Apache Kafka
- AWS 安裝點
- Bridgestor
- Cantemo
- Citrix內容協同作業
- Collibra （ Collibra 資料品質最低版本 2024.02 ）
- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- 磁碟移轉資料
- 夢中
- 彈性搜尋快照（包括凍結層）
- Emam
- Fujifilm物件歸檔
- GitHub企業伺服器
- IBM FileNet
- IBM Spectrum Protect Plus
- IBM 儲存保護
- Interica
- Komprise
- Microsoft SQL Server巨量資料叢集
- 模型9.
- Modzy
- Moonwalk通用
- 很好
- Nasuni
- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- PixitMedia ngenea

- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveville v10 build 220706或更新版本
- RRubrik CDM
- s3a
- 訊號
- 雪片
- SPECtra Logic on 一 Prem Glacier
- Splunk Smartstore
- 輕鬆儲存
- Trino
- Varish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1及更新版本
- Vertica 10.x
- 維地松
- Virtalica StorageFabric
- Weka v3.10或更新版本

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- CommVault 11功能版本26
- IBM FileNet
- IBM 儲存保護
- OpenText文件21.4
- Rukrik
- Veeam 12.
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1及更新版本

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 支援的關鍵管理程式

這些解決方案已通過測試。

- Thales CipherTrust Manager 2.0
- Thales CipherTrust Manager 2.1.
- Thales CipherTrust Manager 2.2.
- Thales CipherTrust Manager 2.3
- Thales CipherTrust Manager 2.4.
- Thales CipherTrust Manager 2.8
- Thales CipherTrust Manager 2.9.

通過驗證的第三方解決方案StorageGRID

下列第三方解決方案已通過驗證、可搭配StorageGRID 使用。+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Alluxio
- Apache Kafka
- Bridgestor
- Cantemo
- Citrix內容協同作業
- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- 磁碟移轉資料
- 夢中
- Emam
- Fujifilm物件歸檔
- GitHub企業伺服器
- IBM FileNet
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server巨量資料叢集
- 模型9.
- Modzy
- Moonwalk通用
- 很好
- Nasuni
- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- PixitMedia ngenea
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream

- Quantum StorNext 5.4.0.1
- Reveville v10 build 220706或更新版本
- RRubrik CDM
- s3a
- 訊號
- 雪片
- SPECtra Logic on 一 Prem Glacier
- Splunk Smartstore
- 輕鬆儲存
- Trino
- Varish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x
- 維地松
- Virtalica StorageFabric
- Weka v3.10或更新版本

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- CommVault 11功能版本26
- IBM FileNet
- OpenText文件21.4
- Veeam 12.
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1及更新版本

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台

- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

通過驗證的第三方解決方案StorageGRID

下列第三方解決方案已通過驗證、可搭配StorageGRID 使用+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Alluxio
- Bridgestor
- Cantemo
- Citrix內容協同作業
- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- Interica
- Komprise
- Moonwalk通用
- 很好
- Nasuni

- OpenText文件16.4
- OpenText文件21.4
- OpenText InfoArchive 16 EP7
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- RRubrik CDM
- s3a
- 訊號
- Splunk Smartstore
- Trino
- Varish Enterprise 6.0.4
- Veeam 11.
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- 維地松
- Virtalica StorageFabric

第三方解決方案已通過**StorageGRID** 物件鎖定驗證、可在不含物件鎖的情況下在

這些解決方案已與相關合作夥伴共同測試。

- OpenText文件21.4
- Veeam 11.

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台

- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

通過驗證的第三方解決方案StorageGRID

下列第三方解決方案已通過驗證、可搭配StorageGRID 使用+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Bridgestor
- Cantemo
- Citrix內容協同作業
- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文件16.4
- OpenText InfoArchive 16 EP7

- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- RRubrik CDM
- 訊號
- Splunk Smartstore
- Varish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- 維地松

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

通過驗證的第三方解決方案StorageGRID

下列第三方解決方案已通過驗證、可與StorageGRID NetApp 11.3搭配使用。+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Bridgestor
- Cantemo
- Citrix內容協同作業
- CommVault 11.
- CTera Portal 6.
- Dalet
- Datadobi
- Data Dynamics StorageX
- 定義
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文件16.4
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- RRubrik CDM 5.0.1 P1-1342
- 訊號
- Splunk Smartstore
- Varish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0

- 維地松

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

通過驗證的第三方解決方案StorageGRID

下列第三方解決方案已通過驗證、可搭配StorageGRID 使用+如果您要尋找的解決方案未列出、請聯絡您的NetApp客戶代表。

第三方解決方案已在StorageGRID NetApp上驗證

這些解決方案已與相關合作夥伴共同測試。

- 活動
- Bridgestor
- Cantemo
- Citrix內容協同作業
- CommVault 11.
- CTera Portal 6.
- Dalet

- Datadobi
- Data Dynamics StorageX
- 定義
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文件16.4
- 使用CyanGate Cloud進行OpenText媒體管理16.5%
- 泛祖拉
- 點歸檔閘道2.0
- Point Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- RRubrik CDM 5.0.1 P1-1342
- 訊號
- Splunk Smartstore
- Varish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- 維地松

StorageGRID 支援的協力廠商解決方案

這些解決方案已通過測試。

- 歸檔軟體
- Axis 通訊
- 一致性 360
- DataFrameworks
- EcoDigital Diva 平台
- Encoding.com
- Fujifilm物件歸檔
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera

- 里程碑系統
- OnSSI
- REACH 引擎
- SilverTrak
- SoftNAS
- QStar
- Velasea

產品功能指南

使用 StorageGRID 實現零 RPO ：完整的多站台複寫指南

本技術報告全面指導如何實施StorageGRID複製策略，以在站點發生故障時實現復原點目標 (RPO) 為零。該文件詳細介紹了StorageGRID的各種部署選項，包括多站點同步複製和多網格非同步複製。它解釋如何設定StorageGRID資訊生命週期管理 (ILM) 策略，以確保跨多個位置的資料持久性和可用性。此外，該報告還涵蓋了效能考量、故障場景和恢復流程，以維持不間斷的客戶營運。本文檔的目標是提供相關信息，以確保即使在站點完全發生故障的情況下，數據仍然可訪問且一致，方法是利用同步和異步複製技術。

StorageGRID 總覽

NetApp StorageGRID 是物件型儲存系統，支援業界標準的 Amazon Simple Storage Service （ Amazon S3 ） API 。

StorageGRID 在多個位置提供單一命名空間，並根據資訊生命週期管理原則（ ILM ）提供不同的服務層級。透過這些生命週期策略，您可以優化資料在整個生命週期中的儲存位置。

StorageGRID 提供可設定的耐用度，以及您在本機和地理區域分散式解決方案中資料的可用度。無論您的資料是在本地還是在公有雲中，整合的混合雲工作流程都允許您的企業利用雲端服務，例如 Amazon Simple Notification Service (Amazon SNS)、Google Cloud、Microsoft Azure Blob、Amazon S3 Glacier 、Elasticsearch 等。

StorageGRID 擴充

最小的StorageGRID部署包括一個管理節點和 3 個儲存節點，位於同一個站點內。單一網格最多可以發展到 220 個節點。StorageGRID可以部署為單一站點，也可以擴展到 16 個站點。

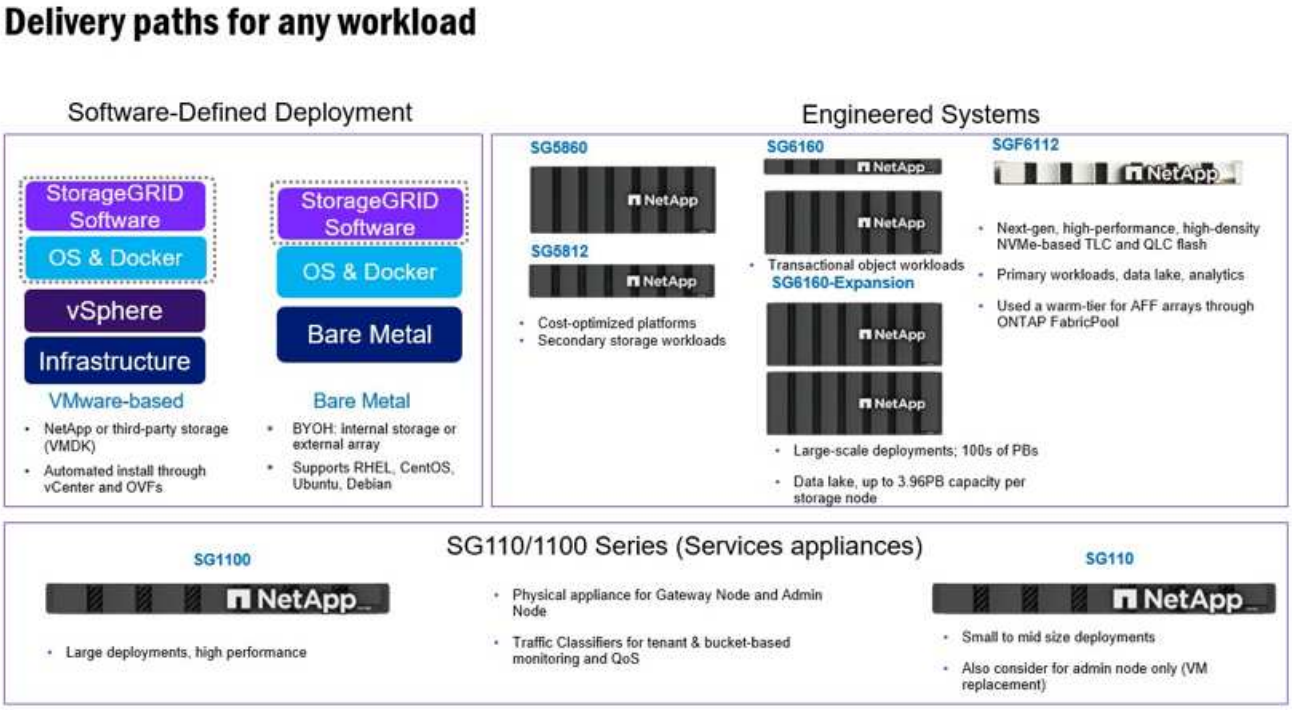
管理節點包含管理介面、指標和日誌記錄的中心點，並維護StorageGRID元件的配置。管理節點還包含用於 S3 API 存取的整合負載平衡器。

StorageGRID可部署為純軟體、VMware 虛擬機器設備或專用設備。

儲存節點可以部署為：

- 僅元資料節點最大化物件數量
- 僅儲存物件的節點，最大化物件空間
- 組合元資料和物件儲存節點，新增物件計數和物件空間

每個儲存節點都可以擴展到多 PB 容量，用於物件存儲，從而允許單一命名空間擁有數百 PB 的容量。StorageGRID也為 S3 API 操作提供了一個稱為網關節點的整合式負載平衡器。



StorageGRID由放置在站點拓撲中的節點集合組成。 StorageGRID中的站點可以是唯一的實體位置，也可以作為邏輯結構與網格中的其他站點位於共用的實體位置。 StorageGRID站點不應跨越多個實體位置。站點代表共用的區域網路 (LAN) 基礎架構和故障域。

StorageGRID 和故障網域

StorageGRID 包含多層故障網域，可用於決定如何建構解決方案，如何儲存資料，以及應將資料儲存在何處，以降低故障風險。

- 網格層級：由多個站台組成的網格可能會發生站台故障或隔離，而可存取的站台可以繼續作為網格運作。
- 站台層級：站台內的故障可能會影響該站台的作業，但不會影響網格的其餘部分。
- 節點層級：節點故障不會影響站台的運作。
- 磁碟層級：磁碟故障不會影響節點的運作。

物件資料和中繼資料

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。

- 物件數據代表實際的基礎數據，例如照片、影片或醫療記錄。
- 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：

- 系統元數據，包括每個物件的唯一 ID、物件名稱、S3 儲存桶的名稱、租用戶帳戶名稱或 ID、物件的邏輯大小、物件首次建立的日期和時間以及物件最後修改的日期和時間。
- 每個物件的副本或糾刪碼片段的目前儲存位置。
- 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，任何與物件相關的物件標籤金鑰值配對
- 對於分段對象和多部分對象，段標識符和資料大小。

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，請前往 "管理物件中繼資料儲存"。

StorageGRID 的資訊生命週期管理（ ILM ）系統用於協調 StorageGRID 系統中所有物件資料的放置，持續時間和擷取行為。ILM 規則決定 StorageGRID 如何使用物件的複本來儲存物件，或是在節點和站台之間對物件進行銷毀編碼。此 ILM 系統負責在網格內保持物件資料一致性。

銷毀編碼

StorageGRID提供在節點層級和磁碟機層級擦除程式碼資料的能力。使用StorageGRID設備，我們對每個節點上儲存在該節點內所有磁碟機上的資料進行擦除編碼，從而提供本機保護，防止多個磁碟故障導致資料遺失或中斷。驅動器故障的重建在節點本地進行，不需要透過網路複製資料。

此外， StorageGRID設備使用擦除編碼方案將物件資料儲存在站點內的節點上，或分佈在StorageGRID系統中的 3 個或更多站點上，儘管 StorageGRID 的 ILM 規則可防止節點故障。

糾刪碼提供了一種儲存佈局，該佈局能夠抵禦節點和站點故障，並且開銷比複製更低。只要滿足儲存資料區塊所需的最小節點數，所有StorageGRID糾刪碼方案都可以在單一網站中部署。這意味著對於 4+2 的 EC 方案，至少需要 6 個節點來接收資料。

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

中繼資料一致性

在 StorageGRID 中，中繼資料通常會每個站台儲存三個複本，以確保一致性和可用度。這種備援功能有助於維持資料完整性和存取能力，即使發生故障也沒問題。

預設一致性是在全網格層級定義。使用者可以隨時變更貯體層級的一致性。

StorageGRID 提供的貯體一致性選項包括：

- * 全部 * ：提供最高等級的一致性。網格中的所有節點都會立即接收資料，否則要求將會失敗。
- 強全球化：
  - **Legacy Strong Global**：確保所有網站上所有用戶端要求的讀寫一致性。
    - 對於所有從 11.9 或更早版本升級到 12.0 且未手動更改為新的 Quorum Strong Global 的系統，這是預設行為。
  - **Quorum Strong-global**：保證所有網站上所有客戶端請求的讀寫一致性。如果可以實現元資料副本仲裁，則可以為多個節點甚至站點故障提供一致性。
    - 這是所有新安裝的 12.0 或更高版本系統的預設行為。
    - QUORUM 一致性定義為儲存節點元資料副本的仲裁，其中每個站點有 3 個元資料副本。計算方法如下：1+((N*3)/2)，其中 N 為站點總數
    - 例如，3 站點網格必須至少製作 5 個副本，每個站點最多可製作 3 個副本。
- **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。

物件資料一致性

雖然中繼資料會在站台內及站台之間自動複寫，但物件資料儲存位置的決策取決於您。物件資料可以儲存在站台內和跨站台的複本中，在站台內或跨站台進行銷毀編碼，或是組合或複本，以及銷毀編碼儲存配置。ILM 規則可套用至所有物件，或僅篩選至特定物件，貯體或租戶。ILM 規則定義物件的儲存方式，複本和 / 或銷毀編碼，物件在這些位置儲存的時間，複本或銷毀編碼配置的數量應變更，或位置應隨著時間而變更。

每個 ILM 規則都會設定三種擷取行為之一來保護物件：雙重認可，平衡或嚴格。

雙重提交選項會立即在網格中的任兩個不同的儲存節點上建立兩個副本，並將請求成功傳回給客戶端。節點選擇將首先在請求站點內進行，但在某些情況下可能會使用其他站點的節點。該物件被添加到 ILM 隊列中，以便根據 ILM 規則進行評估和放置。

平衡選項會立即根據 ILM 策略評估對象，並在向客戶端返回請求成功之前同步放置對象。如果由於故障或儲存空間不足而無法立即滿足放置要求，則將改用雙重提交。問題解決後，ILM 將根據定義的規則自動放置物件。

嚴格選項會立即根據 ILM 策略評估對象，並在向客戶端返回請求成功之前同步放置對象。如果由於中斷或儲存空間不足而無法立即滿足 ILM 規則，則請求將失敗，用戶端需要重試。

負載平衡

StorageGRID 可透過整合式閘道節點，外部 3rd 協力廠商負載平衡器， DNS 循環配置資源，或直接部署至儲存節點，以進行用戶端存取。您可以在站台中部署多個閘道節點，並在高可用度群組中進行設定，以在閘道節點中斷時提供自動容錯移轉和容錯回復。您可以在解決方案中結合負載平衡方法，為解決方案中的所有站台提供單一存取點。

預設情況下，網關節點將平衡其所在站點內各個儲存節點之間的負載。StorageGRID可以設定為允許網關節點使用來自多個站點的節點來平衡負載。這種配置會將這些站點之間的延遲添加到客戶端請求的回應延遲中。只有當客戶可以接受總延遲時，才應進行此配置。

透過本地和全域負載平衡相結合，可以確保 RTO 為零。確保客戶端不間斷存取需要對客戶端請求進行負載平衡。StorageGRID解決方案可在每個站點包含多個網關節點和高可用性群組。為了確保即使在站點發生故障的情況下，客戶端也能在任何站點獲得不間斷的訪問，您應該配置外部負載平衡解決方案，並將其與StorageGRID網關節點結合使用。設定網關高可用性群組，以管理每個站點內的負載，並使用外部負載平衡器在高可用性群組之間平衡負載。必須設定外部負載平衡器以執行健康檢查，以確保請求僅傳送到正在執行的網站。有關使用StorageGRID進行負載平衡的更多信息，請參閱 "StorageGRID 負載平衡器技術報告"。

StorageGRID的零 RPO 要求

若要在物件儲存系統中實現零恢復點目標（ RPO ），在故障發生時必須：

- 中繼資料和物件內容都同步，而且被視為一致的
- 即使發生故障，物件內容仍可存取。

對於多站點部署，Quorum Strong Global 是首選的一致性模型，可確保元資料在所有站點之間同步，這對於滿足零 RPO 要求至關重要。

儲存系統中的物件是根據資訊生命週期管理 (ILM) 規則進行儲存的，這些規則規定了資料在其整個生命週期中如何以及在哪裡儲存。對於同步複製，可以考慮嚴格執行或平衡執行。

- 零 RPO 必須嚴格執行這些 ILM 規則，因為它能確保物件置於定義的位置，不會有任何延遲或後退，維持資料可用度和一致性。
- StorageGRID 的 ILM Balance 擷取行為可在高可用度與恢復能力之間取得平衡，讓使用者即使在站台發生故障時也能繼續擷取資料。

跨多個站台進行同步部署

多站點解決方案： StorageGRID可讓您在網格內的多個站點之間同步複製物件。透過設定具有平衡或嚴格行為的資訊生命週期管理 (ILM) 規則，物件會立即放置在指定位置。將儲存桶一致性等級配置為 Quorum Strong Global 也將確保同步元資料複製。 StorageGRID使用單一全域命名空間，將物件放置位置儲存為元數據，因此每個節點都知道所有副本或擦除編碼片段的位置。如果無法從發出請求的站點檢索對象，則將自動從遠端站點檢索該對象，而無需故障轉移程序。

一旦故障解決，就不需要手動進行容錯回復。複寫效能取決於網路處理量最低，延遲最高，效能最低的站台。站台效能是根據節點數量， CPU 核心數和速度，記憶體，磁碟機數量和磁碟機類型而定。

- 多網格解決方案： * StorageGRID 可以使用跨網格複寫（ CGR ），在多個 StorageGRID 系統之間複寫租戶，使用者和貯體。CGR 可將選取的資料延伸至超過 16 個站台，增加物件儲存區的可用容量，並提供災難恢復。使用 CGR 複寫貯體包括物件，物件版本和中繼資料，可以是雙向或單向的。恢復點目標（ RPO ）取決於每個 StorageGRID 系統的效能，以及它們之間的網路連線。

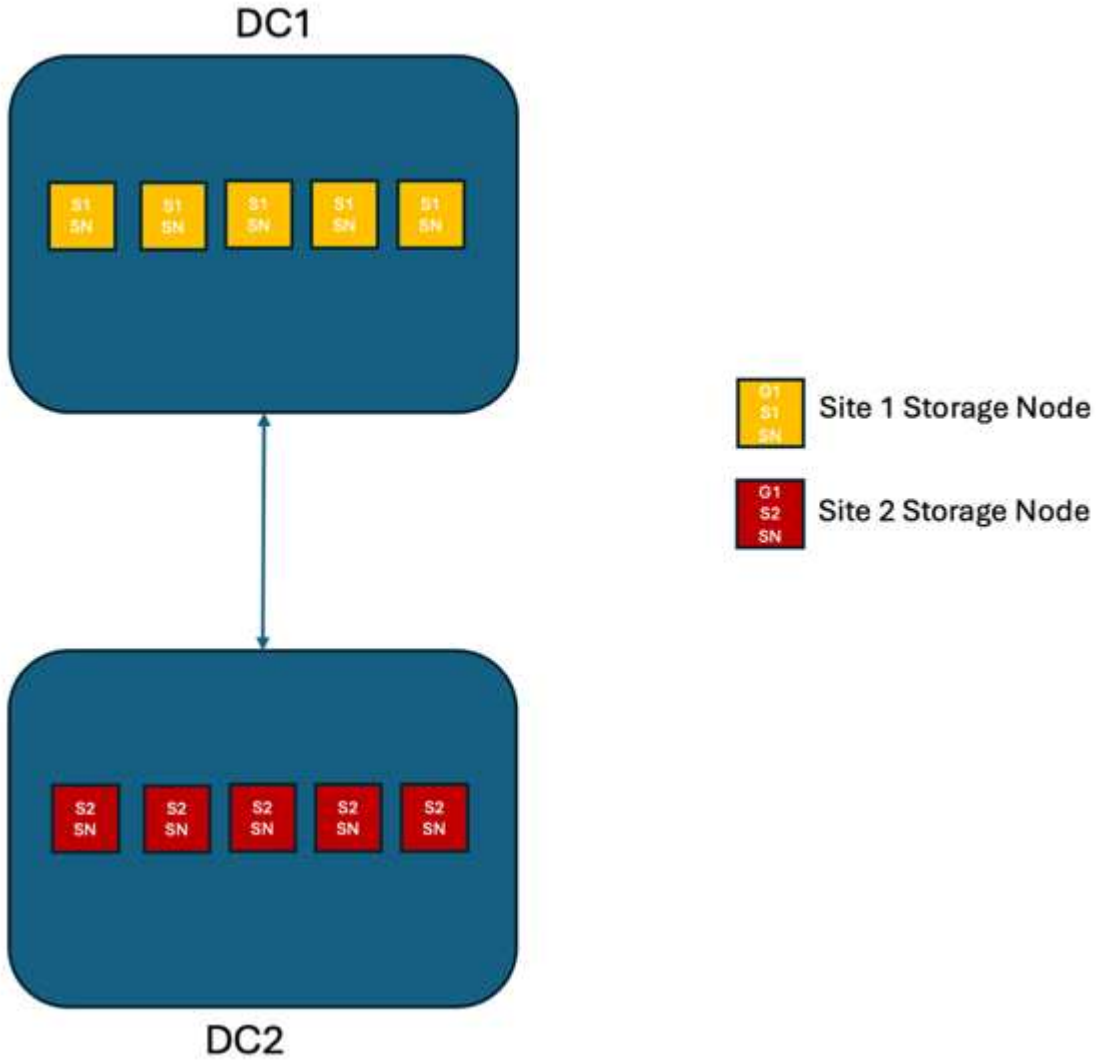
- 摘要： *
- 網格內複寫包括同步和非同步複寫，可透過 ILM 擷取行為和中繼資料一致性控制進行設定。
- 網格間複寫僅為非同步複寫。

單一網格多站台部署

在下列場景中， StorageGRID解決方案配置了一個可選的外部負載平衡器，用於管理整合負載平衡器高可用性群組的請求。這將實現零 RTO 和零 RPO。ILM 配置了平衡攝取保護，用於同步放置。每個儲存桶都配置了適用於 3 個或更多網站的網格的 Quorum 版本的強全域一致性模型，以及適用於 2 個網站的 Legacy 版本的強全域一致性模型。

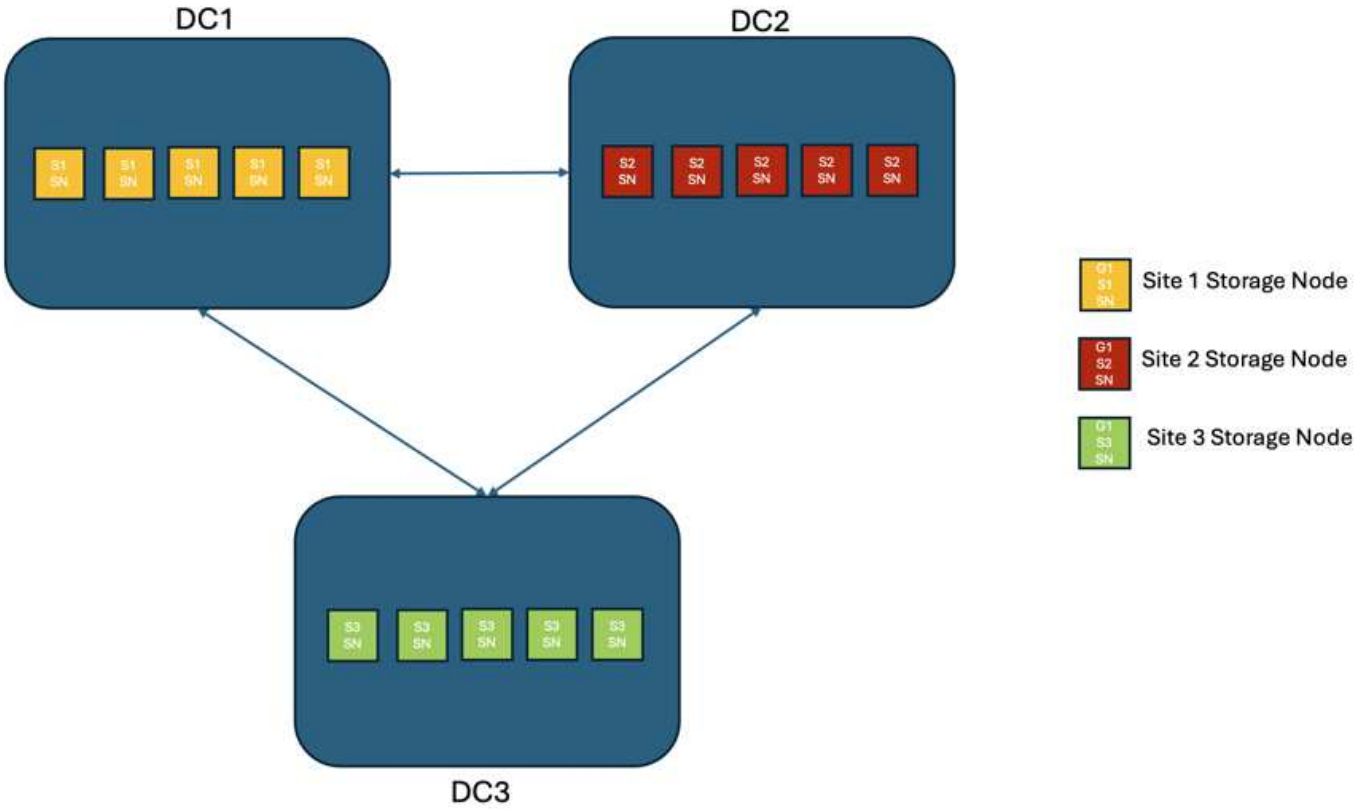
情境一：

在雙站點StorageGRID解決方案中，每個物件至少有兩個副本，所有元資料至少有 6 個副本。故障復原後，中斷期間的更新將自動同步到已復原的網站/節點。只有 2 個站點，在站點完全遺失以外的故障情況下，不太可能實現零 RPO。



情境二：

在擁有三個或更多站點的StorageGRID解決方案中，每個物件至少有 3 個副本或 3 個 EC 區塊，所有元資料至少有 9 個副本。故障復原後，中斷期間的更新將自動同步到已復原的網站/節點。如果擁有三個或更多站點，則有可能實現零 RPO。



多站台故障案例

故障	雙站點成果 + 傳承強大的全球	3 個或更多站點結果 + 法定人數強全球
單節點磁碟機故障	每個應用裝置使用多個磁碟群組，每個群組至少可維持 1 個磁碟機故障，而不會中斷或遺失資料。	每個應用裝置使用多個磁碟群組，每個群組至少可維持 1 個磁碟機故障，而不會中斷或遺失資料。
單一站台發生單一節點故障	不中斷營運或資料遺失。	不中斷營運或資料遺失。
單一站台發生多個節點故障	中斷客戶端對此站點的操作，但不會丟失任何數據。 導向至另一個站台的作業會保持不中斷，且不會遺失資料。	作業會導向所有其他站台，並保持不中斷且不會遺失資料。

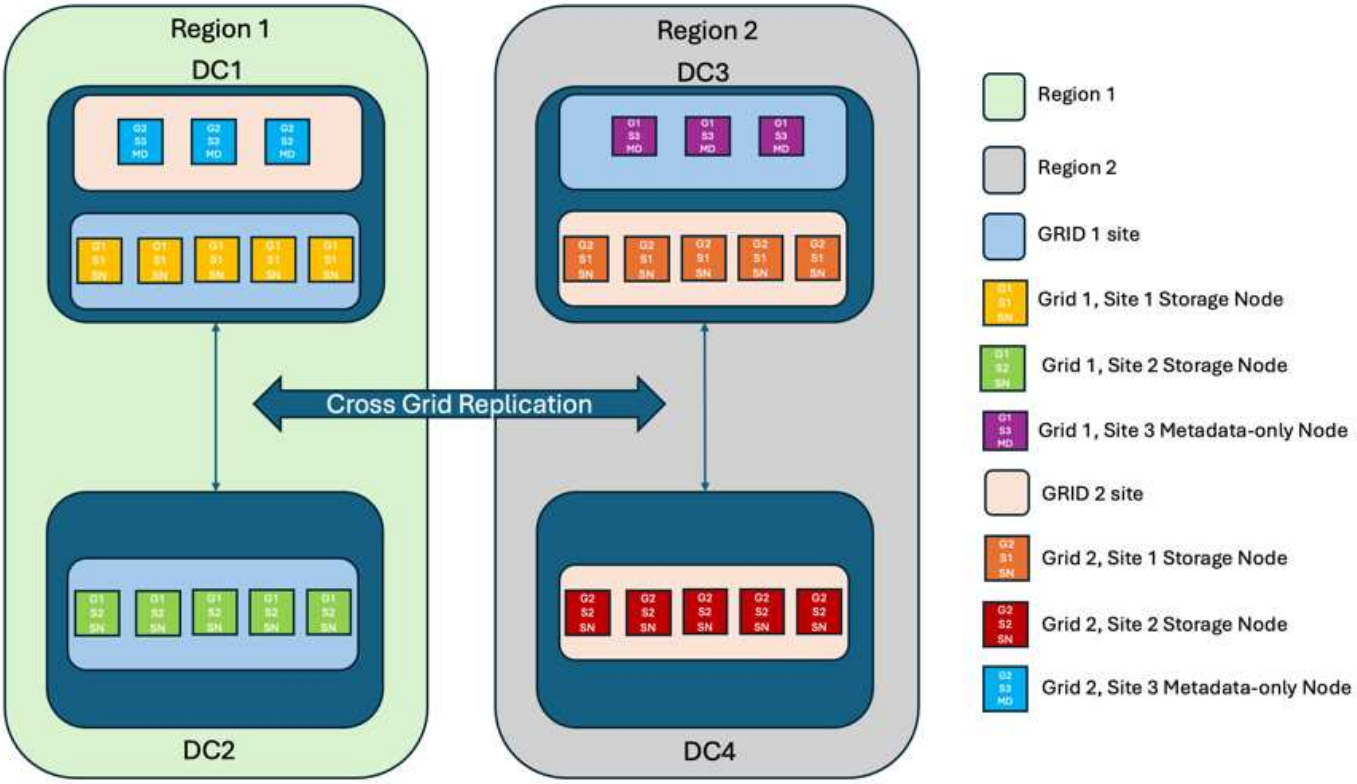
故障	雙站點成果 + 傳承強大的全球	3 個或更多站點結果 + 法定人數強全球
在多個站台發生單一節點故障	在下列情況下不會中斷或遺失資料： • 網格中至少存在一個副本。 • 網格中有足夠的 EC 區塊 若發生下列情況，作業中斷及資料遺失風險： • 沒有副本 • EC Chucks 不足	在下列情況下不會中斷或遺失資料： • 網格中至少存在一個副本。 • 網格中有足夠的 EC 區塊 若發生下列情況，作業中斷及資料遺失風險： • 沒有副本 • 沒有足夠的 EC Chucks 來擷取物件
單一站台故障	部分客戶端操作將會中斷，直到故障解決。GET 和 HEAD 操作將繼續進行，不會中斷。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。	不中斷營運或資料遺失。
單一站台加上單一節點故障	部分客戶端操作將會中斷，直到故障解決為止。HEAD 的運作將持續進行，不會中斷。如果存在副本或足夠的 EC 資料塊，GET 操作將繼續進行，不會中斷。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。	營運未中斷，資料未遺失。根據副本數量，可能出現資料遺失。局部糾刪碼可以防止資料遺失。
單一站台加上每個剩餘站台的節點	只有兩個網站。請參閱：單站點加單節點。	如果元資料副本法定人數無法滿足要求，則營運將會中斷。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。根據副本數量，永久性故障可能導致資料遺失。局部糾刪碼可以防止資料遺失。
多站台故障	所有營運場所均已關閉。如果至少一個站點無法完全恢復，則資料將會遺失。	如果元資料副本法定人數無法滿足要求，則營運將會中斷。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。如果剩餘的糾刪碼區塊不足，則可能導致永久性故障，造成資料遺失。本機糾刪碼或資料複製可以防止資料遺失。

故障	雙站點成果 + 傳承強大的全球	**3** 個或更多站點結果 + 法定人數強全球
站台的網路隔離	客戶端操作將中斷，直到故障解決為止。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。無資料遺失	該孤立站點的運作將受到影響，但不會出現資料遺失。在此故障狀態下，將儲存桶一致性降低到新寫入後讀取或更低，以繼續不間斷地執行操作。其餘站點的營運未受影響，數據也未遺失。

多站台多網格部署

為了新增額外的冗餘層，此場景將採用兩個StorageGRID叢集並使用跨網格複製來保持它們同步。對於此解決方案，每個StorageGRID叢集將有三個站點。兩個站點將用於物件儲存和元數據，而第三個站點將僅用於元數據。兩個系統都將配置平衡的 ILM 規則，以使用擦除編碼在兩個資料站點中同步儲存物件。儲存桶將採用 Quorum Strong Global 一致性模型進行設定。每個網格將在每個儲存桶上配置雙向跨網格複製。這提供了區域之間的非同步複製。可以選擇實作全域負載平衡器來管理兩個StorageGRID系統的整合負載平衡器高可用性群組的請求，以實現零 RPO。

此解決方案將使用四個位置，分為兩個區域。區域 1 將包含網格 1 的 2 個儲存網站，做為區域的主要網格，以及網格 2 的中繼資料網站。區域 2 將包含網格 2 的 2 個儲存網站，做為區域的主要網格，以及網格 1 的中繼資料網站。在每個區域中，相同的位置可以容納該區域主要網格的儲存網站，以及其他區域網格的中繼資料唯一網站。只使用中繼資料節點做為第三個站台，可提供中繼資料所需的一致性，而不會複製該位置中物件的儲存。



此解決方案具有四個獨立位置，可提供兩個獨立 StorageGRID 系統的完整備援，維護 0 的 RPO ，並同時使用多站台同步複寫和多網格非同步複寫。任何單一站台都可能發生故障，同時在兩個 StorageGRID 系統上維持不中斷的用戶端作業。

在本解決方案中，每個物件有四個銷毀編碼複本，所有中繼資料有 18 個複本。如此一來，就能在不影響用戶端

作業的情況下執行多種故障案例。當故障恢復時，系統會自動將故障的站台 / 節點同步更新。

多站台，多網格故障案例

故障	結果
單節點磁碟機故障	每個應用裝置使用多個磁碟群組，每個群組至少可維持 1 個磁碟機故障，而不會中斷或遺失資料。
網格中的一個站台發生單一節點故障	不中斷營運或資料遺失。
每個網格中的一個站台發生單一節點故障	不中斷營運或資料遺失。
網格中的一個站台發生多個節點故障	不中斷營運或資料遺失。
每個網格中的一個站台發生多個節點故障	不中斷營運或資料遺失。
在網格中的多個站台發生單一節點故障	不中斷營運或資料遺失。
每個網格中的多個站台發生單一節點故障	不中斷營運或資料遺失。
網格中的單一站台故障	不中斷營運或資料遺失。
每個網格中都有單一站台故障	不中斷營運或資料遺失。
網格中的單一站台加上單一節點故障	不中斷營運或資料遺失。
單一站台加上單一網格中每個剩餘站台的節點	不中斷營運或資料遺失。
單一位置故障	不中斷營運或資料遺失。
每個網格 DC1 和 DC3 中的單一位置故障	作業將中斷，直到故障解決或鏟斗一致性降低為止；每個網格遺失 2 個站台 所有資料仍存在於 2 個位置
每個網格 DC1 和 DC4 或 DC2 和 DC3 中的單一位置故障	不中斷營運或資料遺失。
每個網格 DC2 和 DC4 中的單一位置故障	不中斷營運或資料遺失。
站台的網路隔離	隔離站台的作業將會中斷，但不會遺失任何資料 不會中斷其餘站台的營運，也不會遺失資料。

結論

使用 StorageGRID 達成零恢復點目標（ RPO ）是確保資料在站台發生故障時的持久性和可用度的關鍵目標。透過運用 StorageGRID 強大的複寫策略，包括多站台同步複寫和多網格非同步複寫，組織可以維持不中斷的用戶端作業，並確保多個位置的資料一致性。資訊生命週期管理（ ILM ）原則的實作以及僅中繼資料節點的使用，進一步增強了系統的恢復能力和效能。有了 StorageGRID ，企業就能安心管理資料，因為即使面對複雜的故障情況，資料仍可存取且一致。這種資料管理與複寫的全方位方法，突顯了精密規劃與執行的重要性，使零 RPO 達到零，並保護寶貴資訊。

為AWS或Google Cloud建立雲端儲存資源池

如果您想要將StorageGRID 物件移到外部S3儲存區、可以使用Cloud Storage Pool。外部儲存庫可以屬於Amazon S3（AWS）或Google Cloud。

您需要的產品

- 已設定好整套功能。StorageGRID
- 您已在AWS或Google Cloud上設定外部S3儲存區。

步驟

1. 在Grid Manager中、瀏覽至* ILM > Storage Pools*。
2. 在頁面的「Cloud Storage Pools（雲端儲存池）」區段中、選取*「Create*（建立*）」。

   「Create Cloud Storage Pool（建立雲端儲存池）」快顯視窗隨即出現。

3. 輸入顯示名稱。
4. 從「提供者類型」下拉式清單中選取「* Amazon S3 *」。

   此供應商類型適用於AWS S3或Google Cloud。

5. 輸入用於雲端儲存池的S3儲存區URI。

   允許使用兩種格式：

   https://host:port`

   http://host:port`

6. 輸入S3儲存區名稱。

   您指定的名稱必須與S3儲存區名稱完全相符、否則建立雲端儲存池會失敗。儲存雲端儲存資源池後、您無法變更此值。

7. 或者、輸入存取金鑰ID和秘密存取金鑰。
8. 從下拉列表中選擇* Do Not Verify Certificate （不驗證證書）。
9. 按一下「 * 儲存 * 」。

預期結果

確認已為Amazon S3或Google Cloud建立雲端儲存資源池。

_ 作者： Jonathan Wong _

為Azure Blob Storage建立雲端儲存資源池

如果您想要將StorageGRID 物件移至外部Azure容器、可以使用Cloud Storage Pool。

您需要的產品

- 已設定好整套功能。StorageGRID
- 您已設定外部Azure容器。

步驟

1. 在Grid Manager中、瀏覽至* ILM > Storage Pools*。
2. 在頁面的「Cloud Storage Pools（雲端儲存池）」區段中、選取*「Create*（建立*）」。

   「Create Cloud Storage Pool（建立雲端儲存池）」快顯視窗隨即出現。

3. 輸入顯示名稱。
4. 從「供應商類型」下拉式清單中選取「* Azure Blob Storage*」。
5. 輸入用於雲端儲存池的S3儲存區URI。

   允許使用兩種格式：

   https://host:port`

   http://host:port`

6. 輸入Azure容器名稱。

   您指定的名稱必須與Azure容器名稱完全相符、否則建立Cloud Storage Pool將會失敗。儲存雲端儲存資源池後、您無法變更此值。

7. 或者、輸入Azure容器的相關帳戶名稱和帳戶金鑰以進行驗證。
8. 從下拉列表中選擇* Do Not Verify Certificate （不驗證證書）。
9. 按一下「 * 儲存 * 」。

預期結果

確認已為Azure Blob Storage建立雲端儲存資源池。

_ 作者： Jonathan Wong _

使用雲端儲存資源池進行備份

您可以建立ILM規則、將物件移入雲端儲存池進行備份。

您需要的產品

- 已設定好整套功能。StorageGRID
- 您已設定外部Azure容器。

步驟

1. 在Grid Manager中、瀏覽至* ILM > Rules > Create*。
2. 輸入說明。
3. 輸入條件以觸發規則。

4. 單擊 * 下一步 * 。
5. 將物件複寫到儲存節點。
6. 新增放置規則。
7. 將物件複寫至雲端儲存池
8. 單擊 * 下一步 * 。
9. 按一下「 * 儲存 * 」 。

預期結果

確認保留圖顯示儲存在StorageGRID 本機的物件、以及儲存在雲端儲存池中進行備份的物件。

確認在觸發ILM規則時、Cloud Storage Pool中會存在複本、而且您可以在本機擷取物件、而無需進行物件還原。

_ 作者： Jonathan Wong _

設定StorageGRID 搜尋整合服務

本指南提供使用 Amazon OpenSearch 服務或內部部署 Elasticsearch 來設定 NetApp StorageGRID 搜尋整合服務的詳細說明。

簡介

支援三種平台服務。StorageGRID

- 《**CloudMirror**複寫》 。StorageGRID將StorageGRID 特定物件從靜止庫鏡射到指定的外部目的地。
- 通知。每個儲存區事件通知、可將針對物件執行的特定動作通知傳送至指定的外部Amazon Simple Notification Service（Amazon SNS） 。
- 搜尋整合服務。將Simple Storage Service（S3）物件中繼資料傳送至指定的Elasticsearch索引、您可以在其中使用外部服務來搜尋或分析中繼資料。

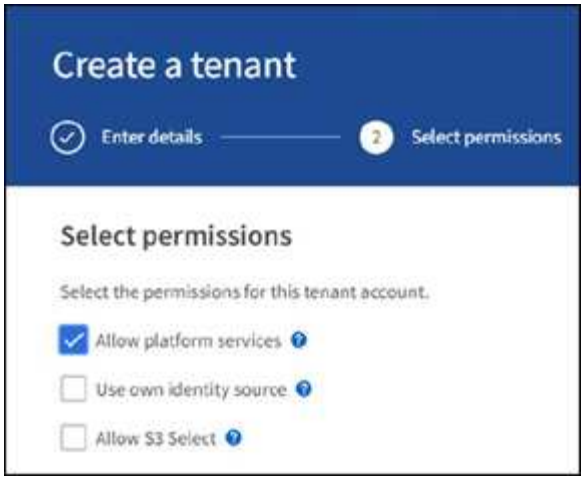
平台服務是由S3租戶透過租戶管理程式UI進行設定。如需詳細資訊、請參閱 "使用平台服務的考量"。

本文件為的補充說明 "《英文》《英文》（英文）StorageGRID" 並提供搜尋整合服務的端點和庫位組態逐步指示和範例。此處包含的Amazon Web Services（AWS）或內部部署彈性搜尋設定說明僅供基本測試或示範用途。

對象應熟悉Grid Manager、租戶管理程式、並能存取S3瀏覽器、執行StorageGRID 基本上傳（PUT）和下載（Get）作業、以利進行資訊搜尋整合測試。

建立租戶並啟用平台服務

1. 使用Grid Manager建立S3租戶、輸入顯示名稱、然後選取S3傳輸協定。
2. 在「權限」頁面上、選取「允許平台服務」選項。如有必要、也可選擇其他權限。



3. 設定租戶root使用者初始密碼、或者如果已在網格上啟用識別聯盟、請選取哪個聯盟群組具有root存取權限來設定租戶帳戶。
4. 按一下「以root登入」、然後選取「Bucket：Create and Manage Bucket」。

   這會帶您前往「租戶管理程式」頁面。

5. 從「租戶管理程式」中、選取「我的存取金鑰」以建立及下載S3存取金鑰、以便日後進行測試。

使用Amazon OpenSearch搜尋整合服務

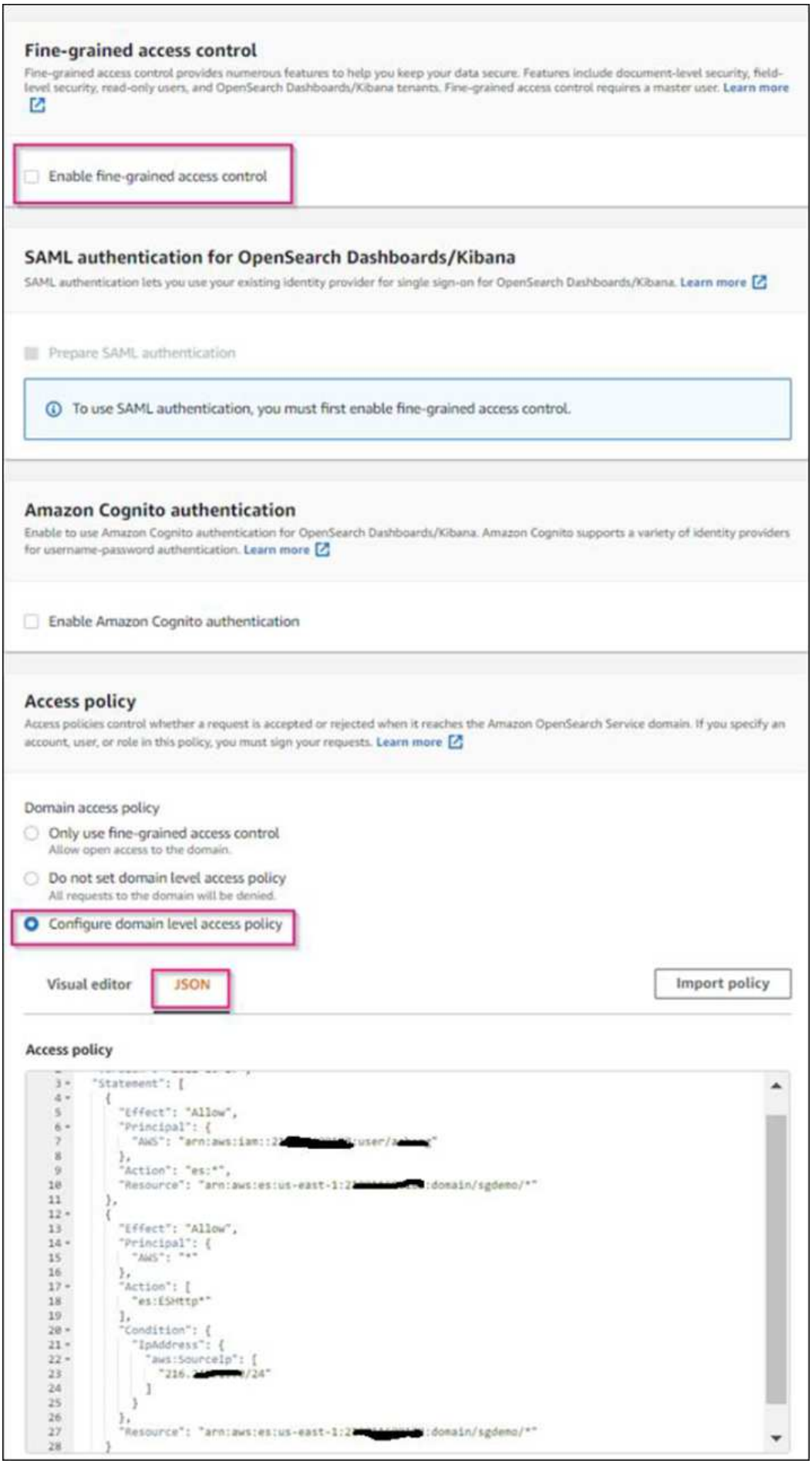
Amazon OpenSearch（前身為Elasticsearch）服務設定

使用此程序可快速且簡單地設定OpenSearch服務、僅供測試/示範之用。如果您使用內部部署Elasticsearch來搜尋整合服務、請參閱一節 搜尋整合服務與內部部署彈性搜尋。

> 您必須擁有有效的AWS主控台登入、存取金鑰、秘密存取金鑰、以及訂閱OpenSearch服務的權限。

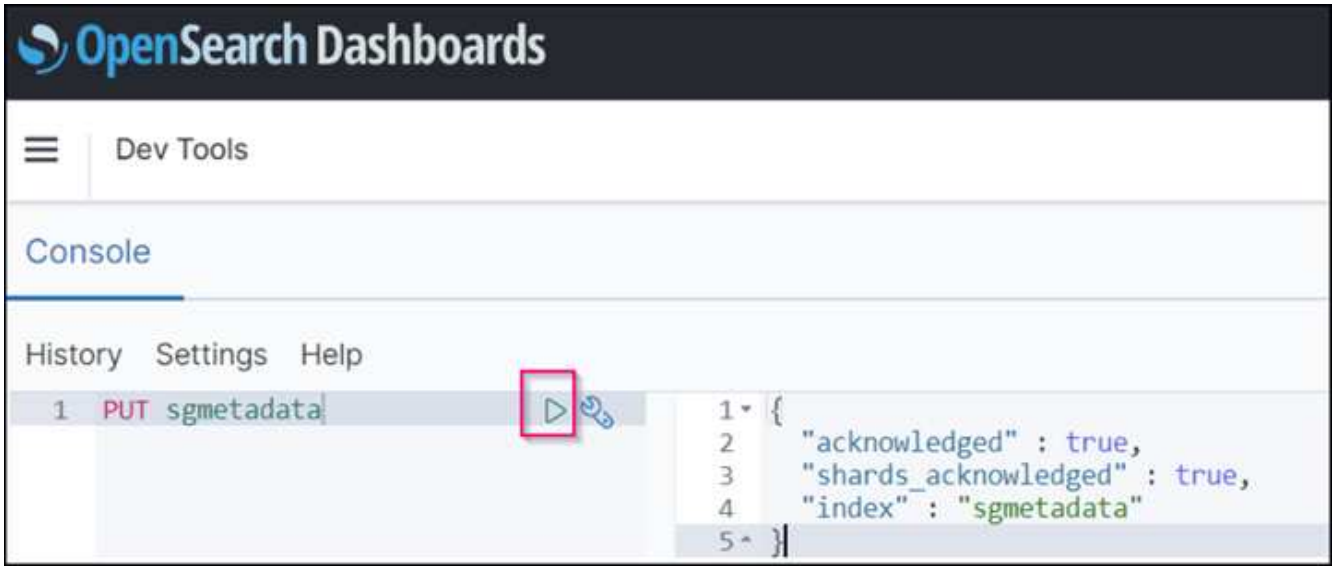
1. 依照中的指示建立新網域 "AWS OpenSearch Service入門"（以下項目除外）：
   - 步驟4.網域名稱：sgdemo
   - 步驟10：精細存取控制：取消選取「啟用精細存取控制」選項。
   - 步驟12.存取原則：選取「Configure Level Access Policy（設定層級存取原則）」、選取「Json」索引標籤以使用下列範例修改存取原則：
     - 以您自己的AWS身分識別與存取管理（IAM）ID和使用者名稱取代反白顯示的文字。
     - 將反白顯示的文字（IP位址）取代為您用來存取AWS主控台的本機電腦公用IP位址。
     - 開啟瀏覽器索引標籤 "https://checkip.amazonaws.com" 尋找您的公有IP。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal":
        {"AWS": "arn:aws:iam:: nnnnnn:user/xyzabc"},
        "Action": "es:*",
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        },
        {
        "Effect": "Allow",
        "Principal": {"AWS": "*"},
        "Action": [
        "es:ESHttp*"
                ],
        "Condition": {
            "IpAddress": {
                "aws:SourceIp": [ "nnn.nnn.nn.n/nn"
                    ]
                }
        },
        "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
        }
    ]
}
```

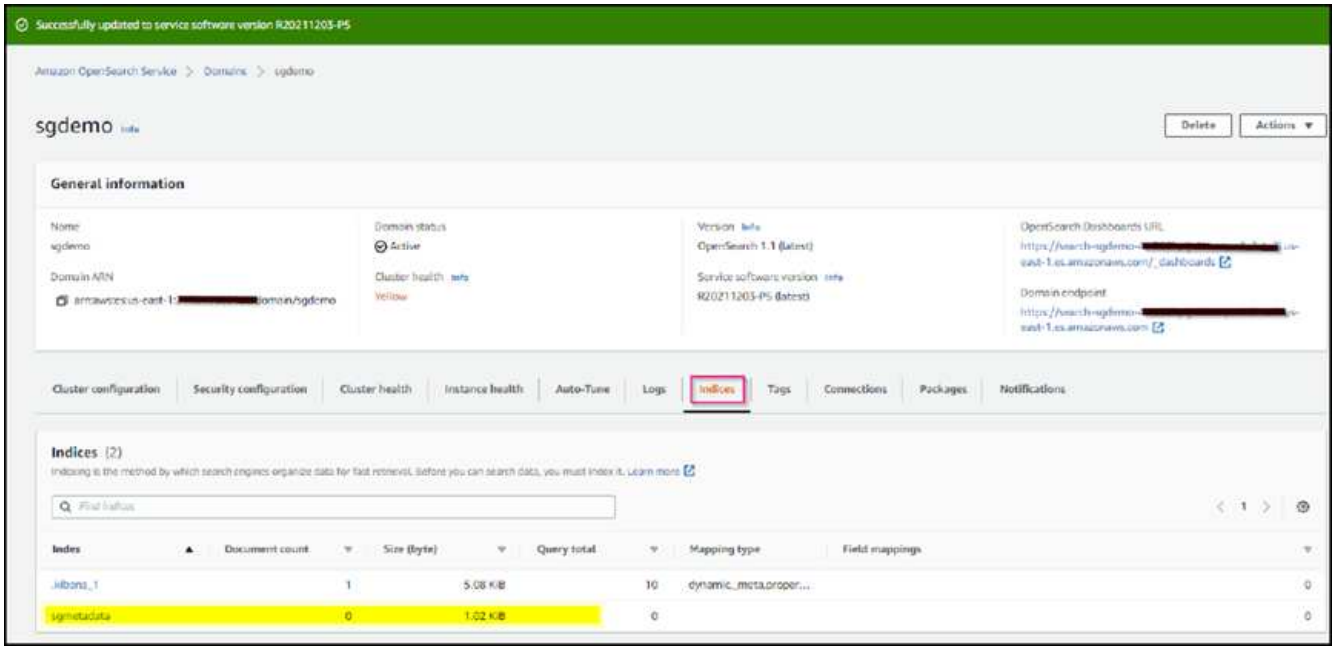

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
Enable fine-grained access control
SAML authentication for OpenSearch Dashboards/Kibana
SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. Learn more
Prepare SAML authentication
To use SAML authentication, you must first enable fine-grained access control.
Amazon Cognito authentication
Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more
Enable Amazon Cognito authentication
Access policy
Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. Learn more
Domain access policy
Only use fine-grained access control
Allow open access to the domain.
Do not set domain level access policy
All requests to the domain will be denied.
Configure domain level access policy
Visual editor
JSON
Import policy
Access policy
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::2[redacted]:user/A[redacted]"
},
"Action": "es:*",
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
},
{
"Effect": "Allow",
"Principal": {
"AWS": "*"
},
"Action": [
"es:ESHttp*"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": [
"216.[redacted]/24"
]
}
},
"Resource": "arn:aws:es:us-east-1:2[redacted]:domain/sgdemo/*"
}

2. 等待15到20分鐘、讓網域變成作用中狀態。

3. 按一下OpenSearch儀表板URL、在新索引標籤中開啟網域以存取儀表板。如果發生存取遭拒錯誤、請確認存取原則來源IP位址已正確設定為電腦的公用IP、以允許存取網域儀表板。
4. 在儀表板歡迎頁面上、選取「自行瀏覽」。從功能表移至「Management（管理）」→「Dev Tools（開發工具）」
5. 在「Dev Tools（開發工具）」→「Console（主控台）」下、輸入「PUT <index>'（放置<index>'）」、您可以在其中使用索引來儲存StorageGRID 物件中繼資料。我們在下列範例中使用索引名稱「gmeta資料」。按一下小三角符號以執行PUT命令。預期結果會顯示在右側面板上、如下列範例擷取畫面所示。



6. 確認索引可從sgdomain>索引下的Amazon OpenSearch UI中看到。

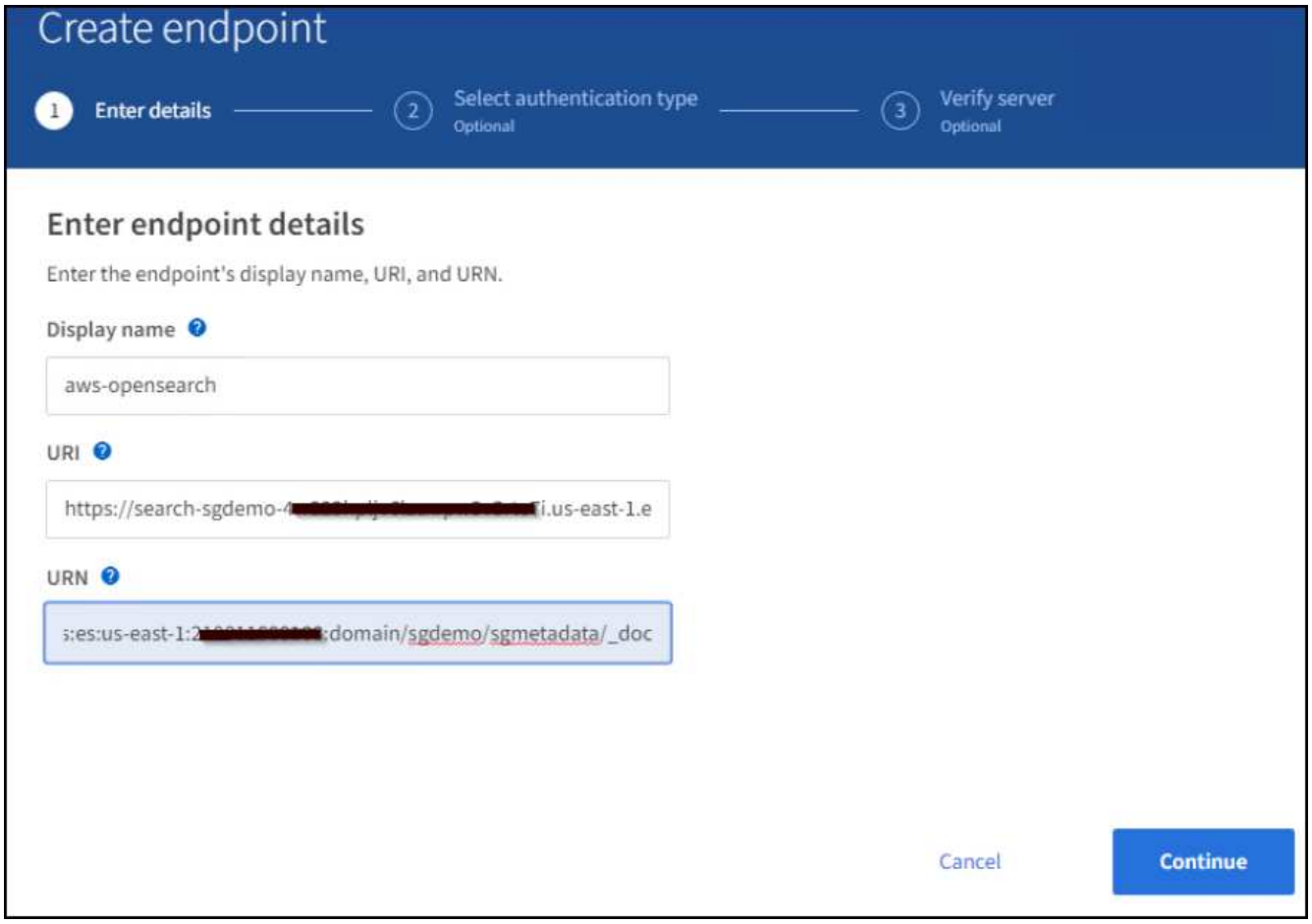


平台服務端點組態

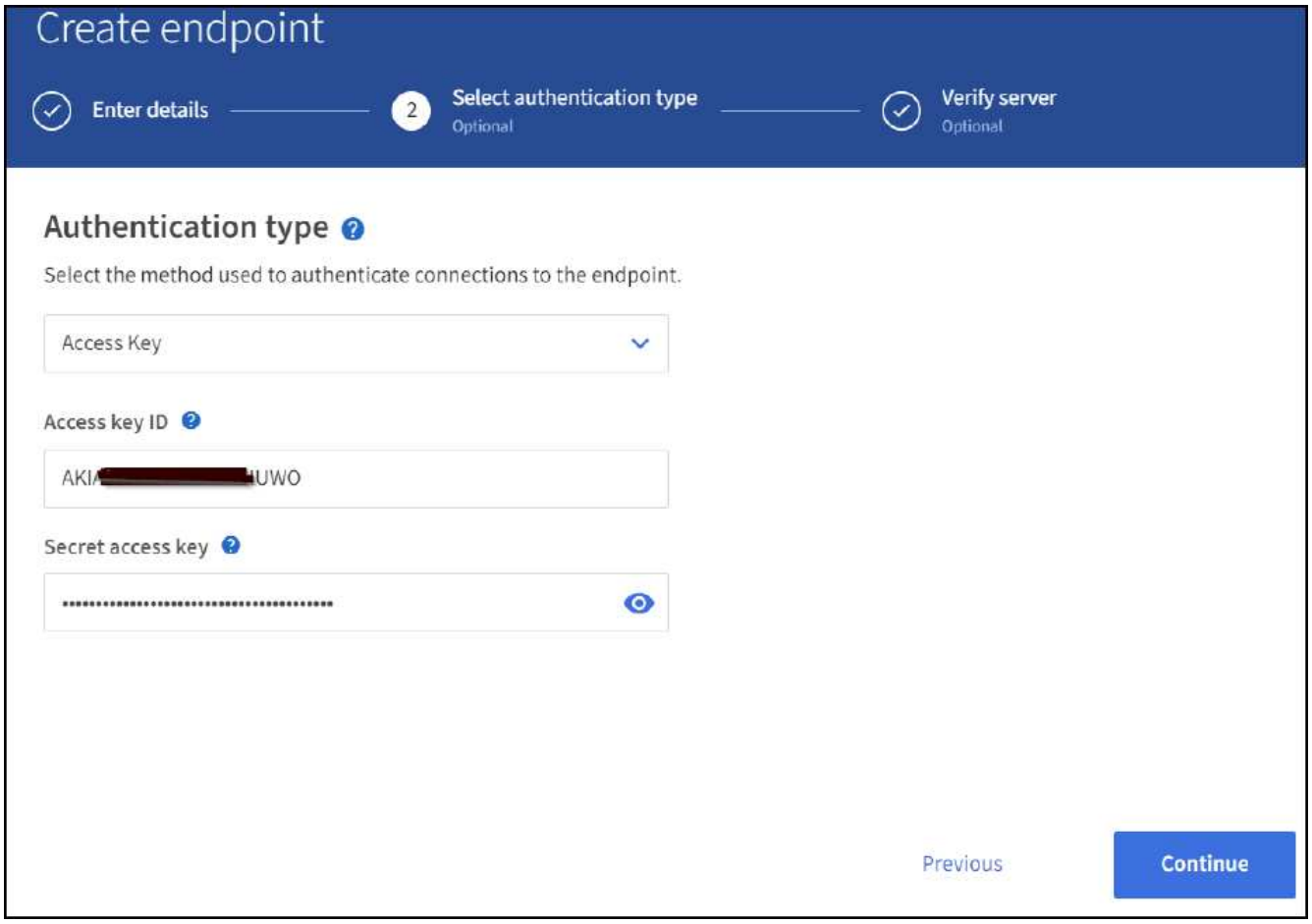
若要設定平台服務端點、請遵循下列步驟：

1. 在租戶管理程式中、前往儲存設備（S3）>平台服務端點。
2. 按一下「Create Endpoint（建立端點）」、輸入下列內容、然後按一下「Continue（繼續）」
   - 顯示名稱範例「AWS/OpenSearch」
   - 「URI」欄位中前面程序步驟2下範例快照中的網域端點。
   - 在之前的程序步驟2中、在「URN」欄位中使用的網域ARN、並在ARN結尾加上「/<index>//_doc'」。

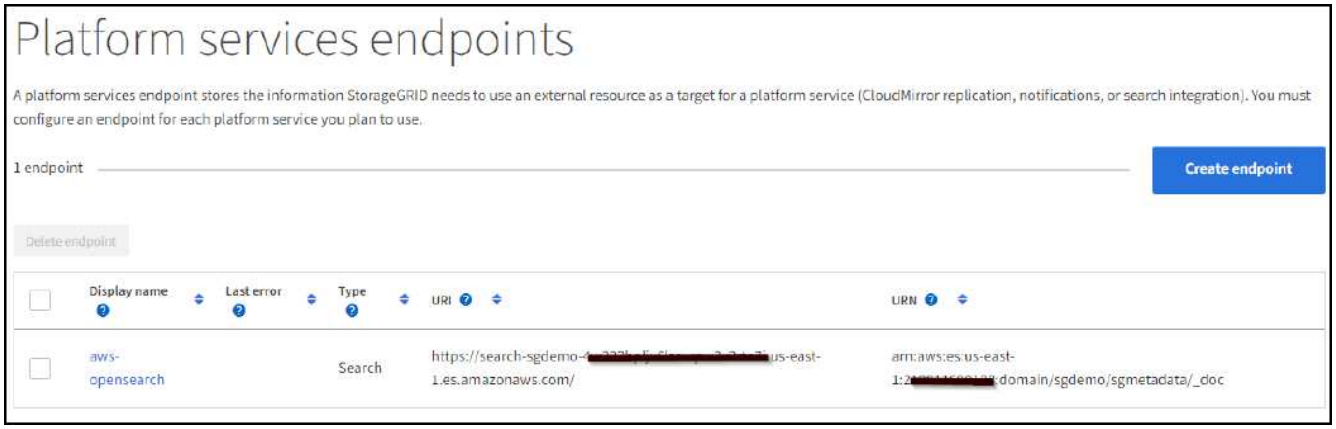
     在此範例中、URN會變成「arn:AWS：es：us-east-1:211234567890：domain/sgdemo /sgmeydata//_doc'。



3. 若要存取Amazon OpenSearch sgDomain、請選擇「存取金鑰」作為驗證類型、然後輸入Amazon S3存取金鑰和秘密金鑰。若要進入下一頁、請按一下「Continue（繼續）」。



4. 若要驗證端點、請選取「使用作業系統CA憑證並測試及建立端點」。如果驗證成功、則會顯示類似下圖的端點畫面。如果驗證失敗、請確認路徑結尾處的URN包含「/<index>//_doc'、而且AWS存取金鑰和秘密金鑰都正確無誤。



搜尋整合服務與內部部署彈性搜尋

內部部署彈性搜尋設定

此程序僅供快速設定內部部署Elasticsearch和Kibana Using Docker、僅供測試之用。如果Elasticsearch和Kibana伺服器已經存在、請前往步驟5。

1. 請遵循此步驟 "Docker安裝程序" 以安裝Docker。我們使用 "CentOS Docker安裝程序" 在此設定中。

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

- 若要在重新開機後啟動Docker、請輸入下列命令：

```
sudo systemctl enable docker
```

- 將「VM.max.map_count'」值設為262144：

```
sysctl -w vm.max_map_count=262144
```

- 若要在重新開機後保留設定、請輸入下列命令：

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. 請依照 "彈性搜尋快速入門指南" 自我管理區段、用於安裝及執行Elasticsearch和Kibana泊塢視窗。在此範例中、我們安裝了8.1版。

記下Elasticsearch所建立的使用者名稱/密碼和權杖、您需要這些資訊來啟動Kibana UI和StorageGRID Esplan端點驗證。

Elasticsearch Service | Self-managed

Install and run Elasticsearch

1. Install and start Docker Desktop.
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- Certificates and keys are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.

NOTE You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.

NOTE If you need to reset the password for the `elastic` user or other built-in users, run the `elasticsearch-reset-password` tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the `elasticsearch-create-enrollment-token` tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

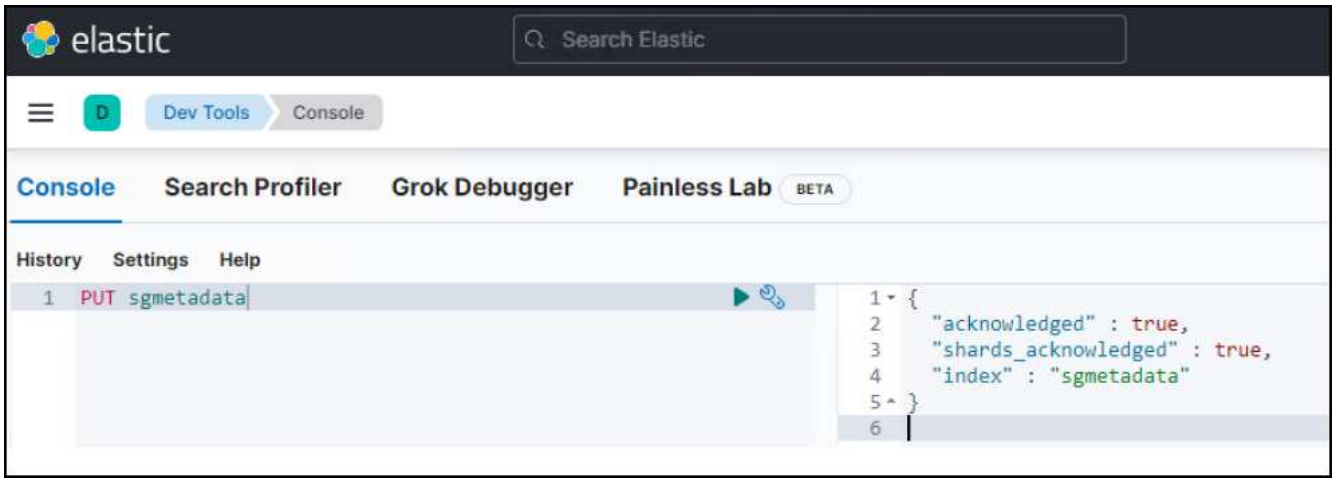
1. In a new terminal session, run:

```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/ki
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.
   a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
   b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

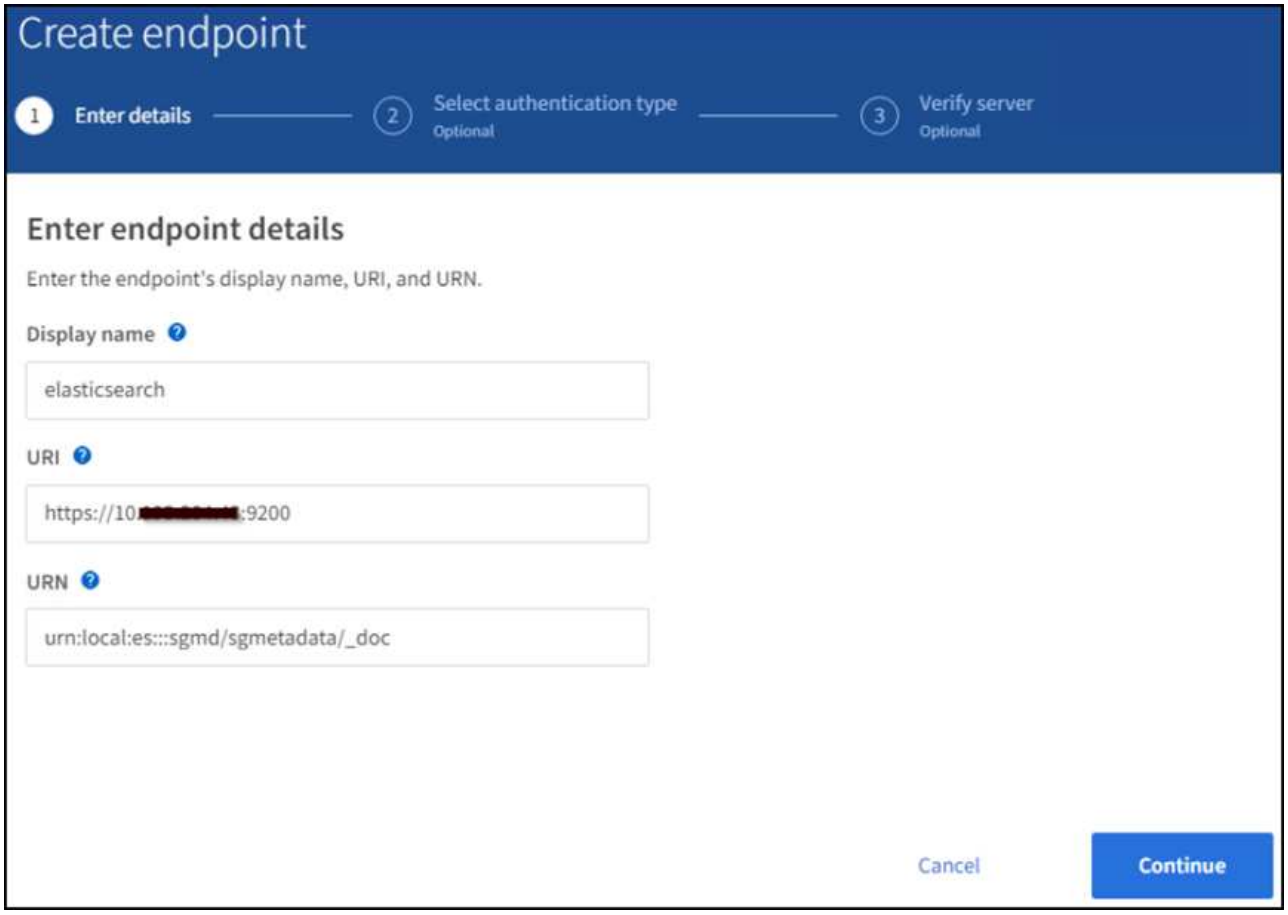
3. Kibana Docker容器啟動後、主控台會顯示URL連結「\https://0.0.0.0:5601`」。以URL中的伺服器IP位址取代0：0：0：0。
4. 使用使用者名稱「Elastic」和Elastic在前一個步驟中產生的密碼登入Kibana UI。
5. 首次登入時、請在儀表板歡迎頁面上、選取「自行瀏覽」。從功能表中、選取管理>開發工具。
6. 在Dev Tools Console（開發工具主控台）畫面上、輸入「放置<index>'」、您可以在其中使用此索引來儲存StorageGRID 物件中繼資料。在此範例中、我們使用索引名稱「shgmeta資料」。按一下小三角符號以執行PUT命令。預期結果會顯示在右側面板上、如下列範例擷取畫面所示。



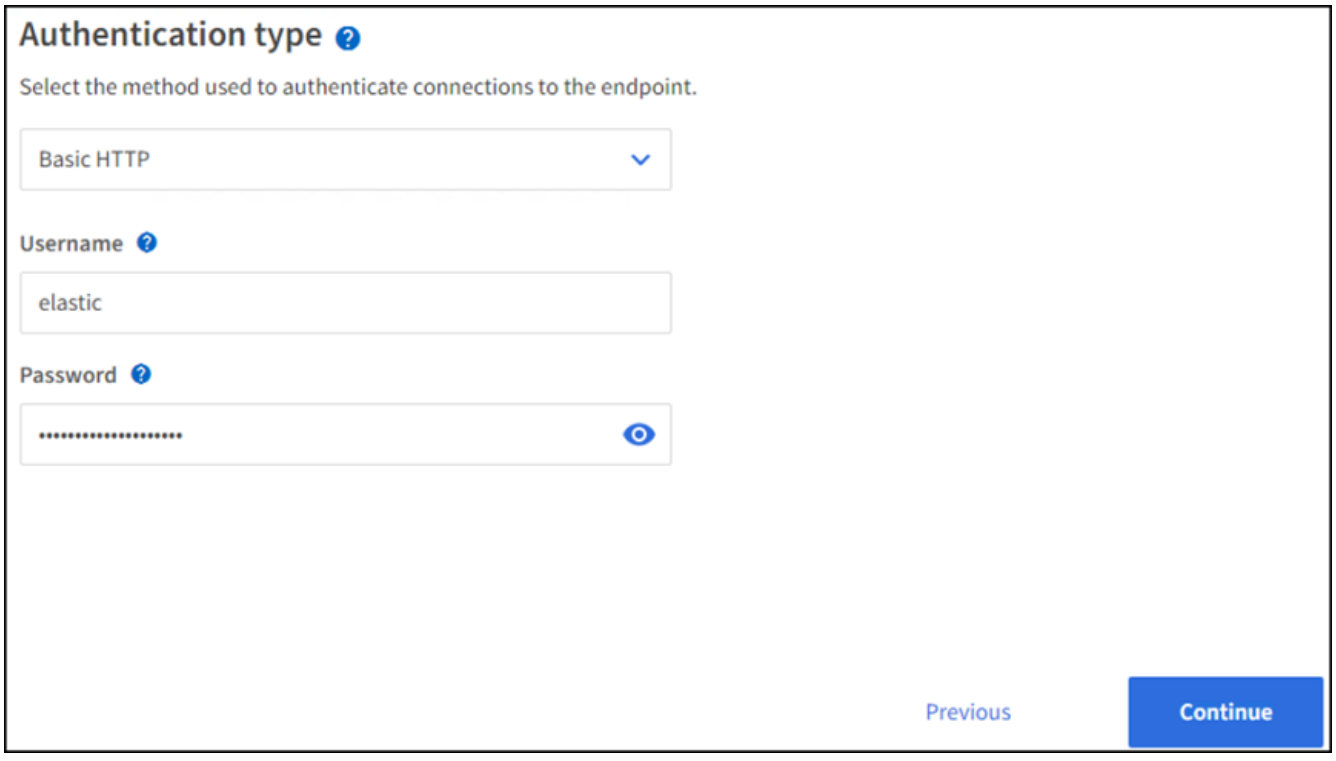
平台服務端點組態

若要設定平台服務的端點、請遵循下列步驟：

1. 在租戶管理程式中、前往儲存設備（S3）>平台服務端點
2. 按一下「Create Endpoint（建立端點）」、輸入下列內容、然後按一下「Continue（繼續）」
   - 顯示名稱範例：「彈性搜尋」
   - URI：https://<elasticsearch-server-ip或hostname>:9200'
   - urn:「urn:<soes>:es::::<se-unibe-text>/<index-name>//_doc'、其中index-name是您在Kibana主控台使用的名稱。範例：「urn:local:es：：sgmm/sgmadm/_do'

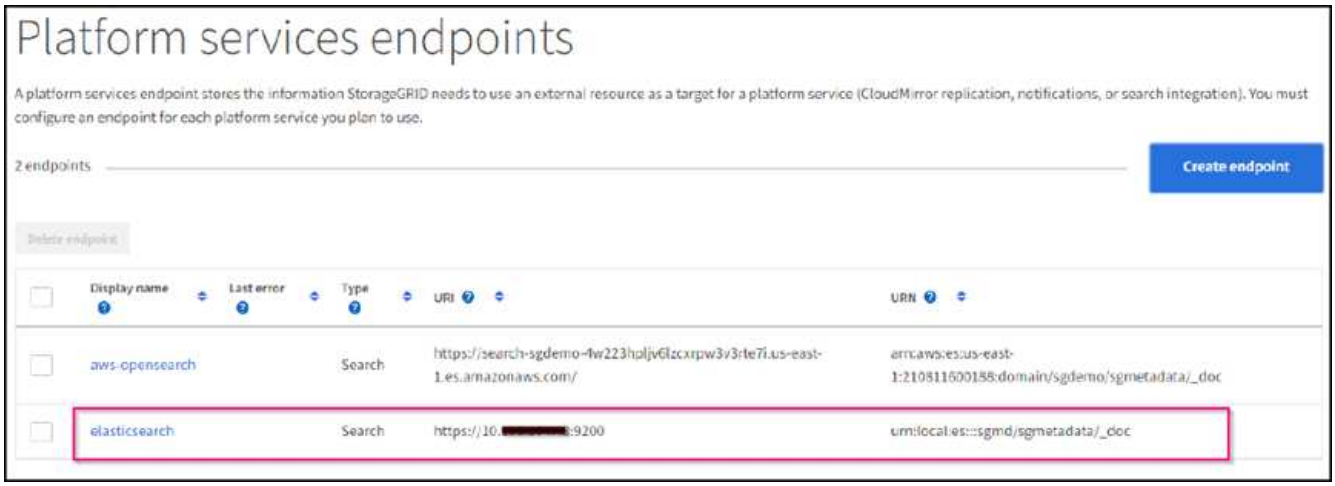


3. 選取基本HTTP作為驗證類型、輸入使用者名稱「elastic」和Elasticsearch安裝程序產生的密碼。若要前往下一頁、請按一下「Continue（繼續）」。



4. 選取「Do Not Verify Certificate and Test and Create Endpoint（不驗證憑證和測試並建立端點）」以驗證端

點。如果驗證成功、則會顯示類似下列螢幕快照的端點畫面。如果驗證失敗、請確認URN、URI和使用者名稱/密碼項目正確無誤。



Bucket搜尋整合服務組態

建立平台服務端點之後、下一步是在資源庫層級設定此服務、以便在物件建立、刪除或更新中繼資料或標記時、將物件中繼資料傳送至定義的端點。

您可以使用Tenant Manager將自訂StorageGRID 的功能XML套用至儲存庫、以設定搜尋整合、如下所示：

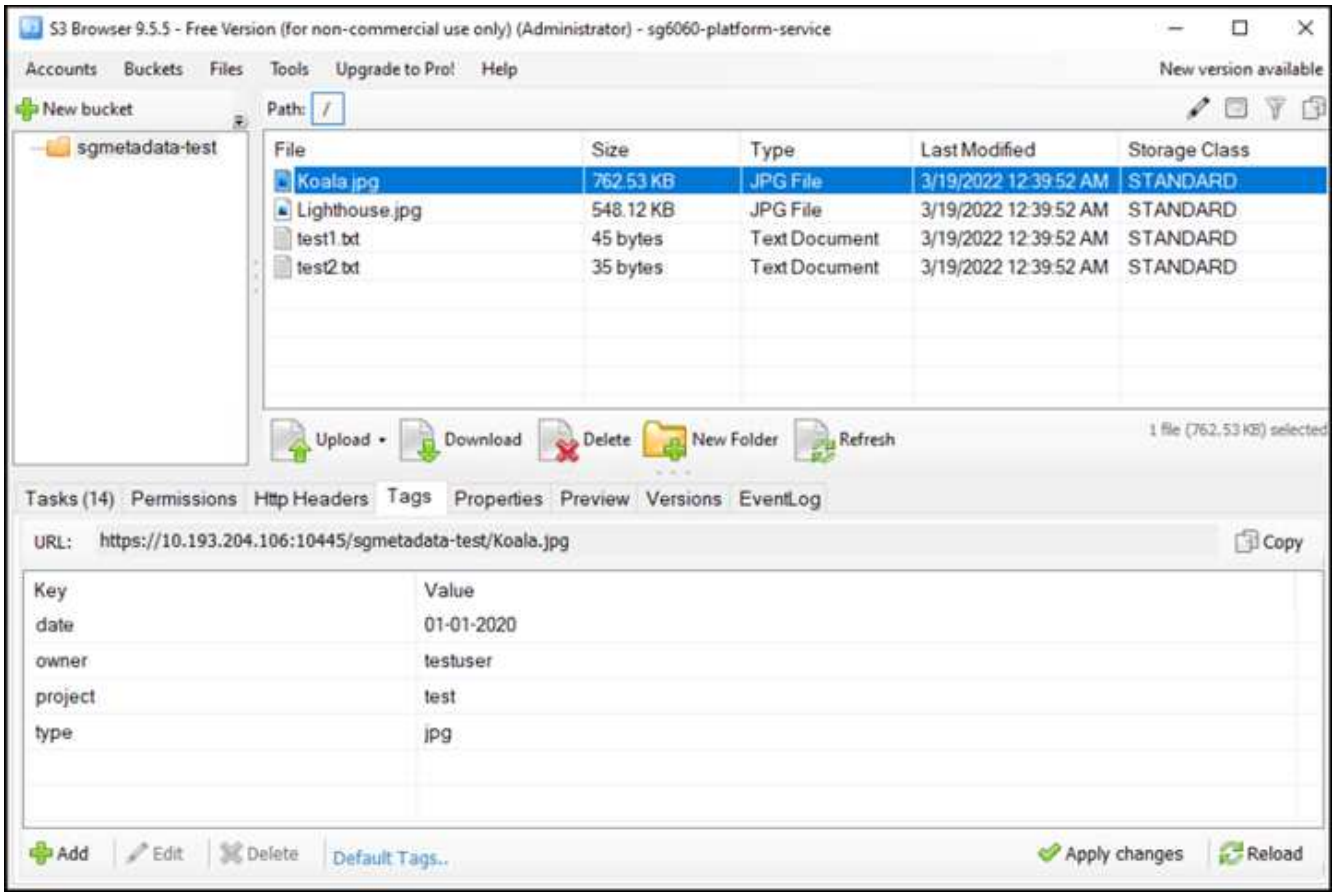
1. 在租戶管理程式中、前往儲存設備（S3）>儲存設備
2. 按一下「Create Bucket（建立儲存區）」、輸入儲存區名稱（例如「shgmadmadgtest-test」）、然後接受預設的「us-east-1」區域。
3. 按一下「繼續」>「建立工作區」。
4. 若要顯示「Bucket Overview」（庫位總覽）頁面、請按一下庫位名稱、然後選取「Platform Services」（平台服務）。
5. 選取「啟用搜尋整合」對話方塊。在提供的XML方塊中、使用此語法輸入組態XML。

   強調顯示的URN必須符合您所定義的平台服務端點。您可以開啟另一個瀏覽器索引標籤、以存取租戶管理程式、並從定義的平台服務端點複製URN。

   在此範例中、我們沒有使用前置詞、表示此儲存區中每個物件的中繼資料都會傳送到先前定義的Elasticsearch端點。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

6. 使用S3瀏覽器以StorageGRID 租戶存取/秘密金鑰連線至功能區、將測試物件上傳至「實元資料測試」儲存區、並將標記或自訂中繼資料新增至物件。



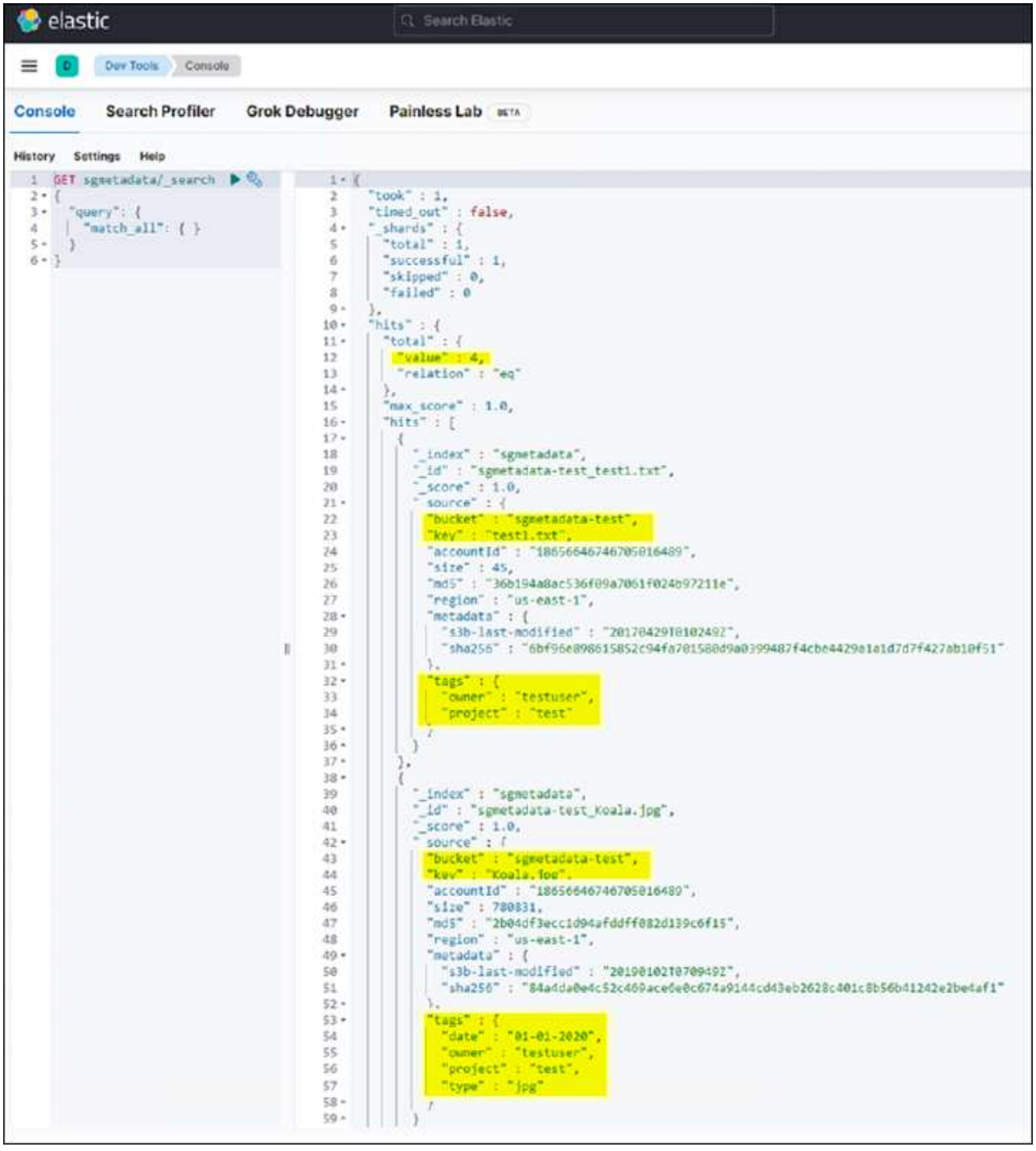
7. 使用Kibana UI來驗證物件中繼資料是否已載入sgmeta的索引。

   a. 從功能表中、選取管理>開發工具。

   b. 將範例查詢貼到左側的主控台面板、然後按一下三角符號以執行查詢。

      下列範例擷取畫面中的查詢1範例結果顯示四筆記錄。這與儲存區中的物件數量相符。

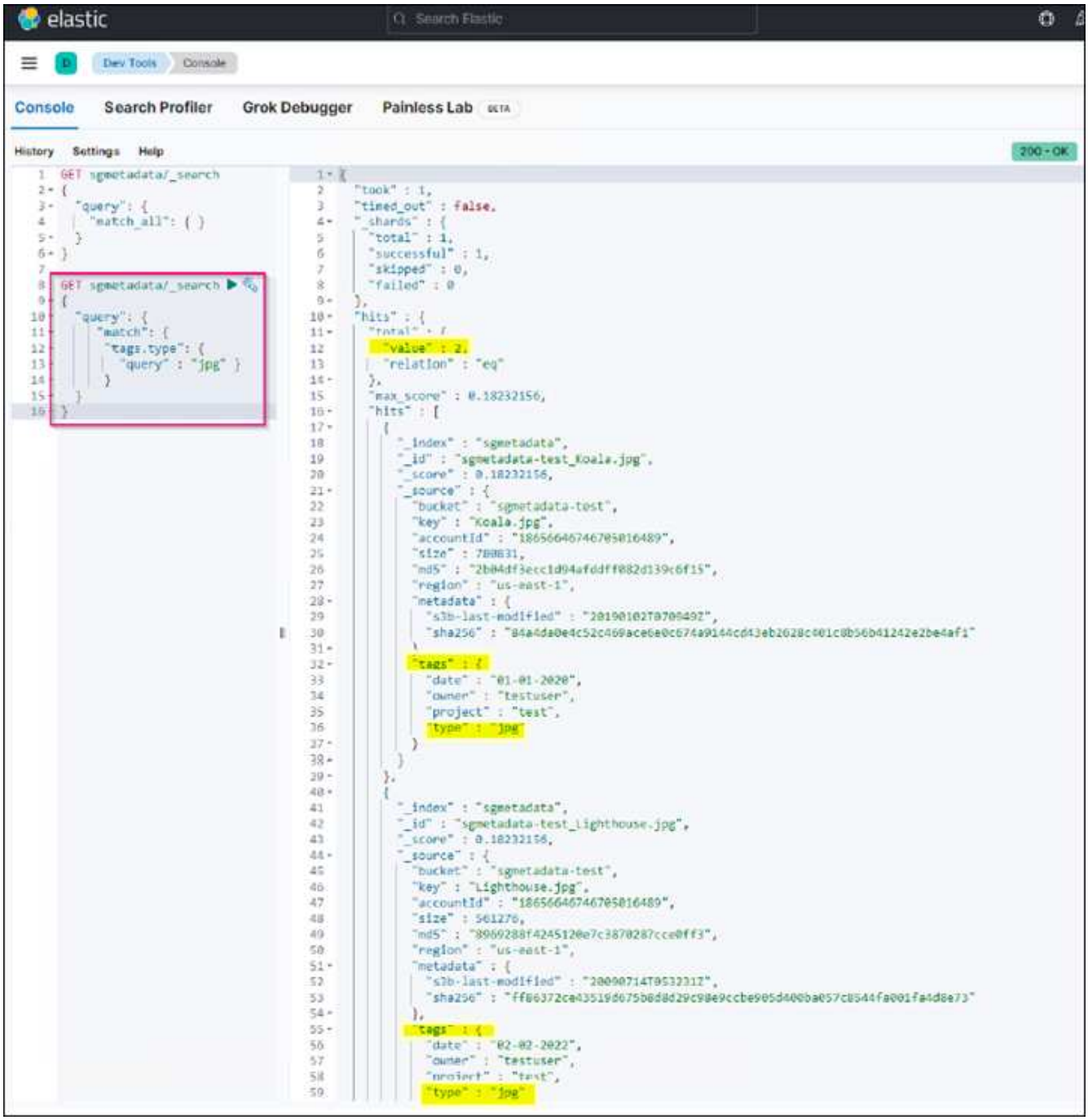
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



下列螢幕擷取畫面中的查詢2範例結果顯示兩筆標記類型為「jpg」的記錄。

```
GET sgmetadata/_search
{
    "query": {
        "match": {
            "tags.type": {
                "query" : "jpg" }
                }
            }
}
```

+



何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- "什麼是平台服務"
- "供應資料StorageGRID"

_ 作者： Angela Cheng _

節點複製

節點複製考量與效能。

節點複製考量

節點複製是取代現有應用裝置節點以進行技術更新、增加容量或提升StorageGRID 效能的更快方法。節點複製也有助於使用KMS轉換為節點加密、或將儲存節點從DDP8變更為DDP16。

- 來源節點的已用容量與完成複製程序所需的時間無關。節點複製是節點的完整複本、包括節點中的可用空間。
- 來源和目的地應用裝置必須使用相同的PGE版本
- 目的地節點的容量必須永遠大於來源
  - 請確定新的目的地應用裝置的磁碟機大小大於來源
  - 如果目的地應用裝置具有相同大小的磁碟機、且已針對DDP8進行設定、您可以設定DDP16的目的地。如果已針對DDP16設定來源、則無法進行節點複製。
  - 從SG5660或SG5760應用裝置改用SG6060應用裝置時、請注意SG5X60有60個容量磁碟機、SG6060只有58個容量磁碟機。
- 在複製程序期間、節點複製程序要求來源節點離線至網格。如果在此期間有其他節點離線、用戶端服務可能會受到影響。
- 11.8 和低：儲存節點只能離線 15 天。如果複製程序預估接近15天或超過15天、請使用擴充與取消委任程序。
  - 11.9 ： 15 天期限已移除。
- 若為具有擴充架的 SG6060 或 SG6160 、您需要將適當機櫃磁碟機大小的時間加入基本應用裝置時間、以獲得完整複製時間。
- 目標儲存設備中的磁碟區數量必須大於或等於來源節點中的磁碟區數量。即使目標應用裝置的容量大於來源節點、您也無法將具有 16 個物件儲存區（ rangedb ）的來源節點複製到具有 12 個物件儲存區的目標儲存應用裝置。除了 SFF6112 儲存設備只有 12 個物件儲存磁碟區之外、大部分的儲存設備都有 16 個物件儲存磁碟區。例如、您無法從 SG5760 複製到 SGF6112 。

節點複製效能預估

下表包含節點複製期間的計算預估值。條件各異、*粗體*中的項目可能會超過節點停機的15天上限。

DDP8.

SG5612/SG5712/SG5812 → 任何

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	1天	2天	2.5天	3天	4天	4.5天	5.5天
25GB	1天	2天	2.5天	3天	4天	4.5天	5.5天

SG5660 → SG5760/SG5860

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	3.5天	7天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*
25GB	3.5天	7天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*

SG5660 → SG6060/SG6160

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	2.5天	4.5天	5.5天	6.5天	9天	10天	• 12天*
25GB	2天	4天	5天	6天	8天	9天	10天

SG5760/SG5860 → SG5760/SG5860

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	3.5天	7天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*
25GB	3.5天	7天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*

SG5760/SG5860 → SG6060/SG6160

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	2.5天	4.5天	5.5天	6.5天	9天	10天	• 12天*

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
25GB	2天	3.5天	4.5天	5.5天	7天	8天	9.5天

SG6060/SG6160 → SG6060/SG6160

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	2.5天	4.5天	5.5天	6.5天	8.5天	9.5天	11.5天
25GB	2天	3天	4天	4.5天	6天	7天	8.5天

DDP16

SG5760/SG5860 → SG5760/SG5860

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	3.5天	6.5天	8天	9.5天	• 12.5天*	• 14天*	• 17天*
25GB	3.5天	6.5天	8天	9.5天	• 12.5天*	• 14天*	• 17天*

SG5760/SG5860 → SG6060/SG6160

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	2.5天	5天	6天	7.5天	10天	11天	• 13天*
25GB	2天	3.5天	4天	5天	6.5天	7天	8.5天

SG6060/SG6160 → SG6060/SG6160

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	3天	5天	6天	7天	9.5天	10.5天	• 13天*
25GB	2天	3.5天	4.5天	5天	7天	7.5天	9天

擴充機櫃（針對來源應用裝置上的每個機櫃、新增到 **SG6060/SG6160** 以上）

網路介面速度	**4TB**磁碟機大小	**8TB**磁碟機大小	**10TB**磁碟機大小	**12TB**磁碟機大小	**16TB**磁碟機大小	**18TB**磁碟機大小	**22TB**磁碟機大小
10Gb	3.5天	5天	6天	7天	9.5天	10.5天	• 12天*
25GB	2天	3天	4天	4.5天	6天	7天	8.5天

_ 作者： Aron Klein_

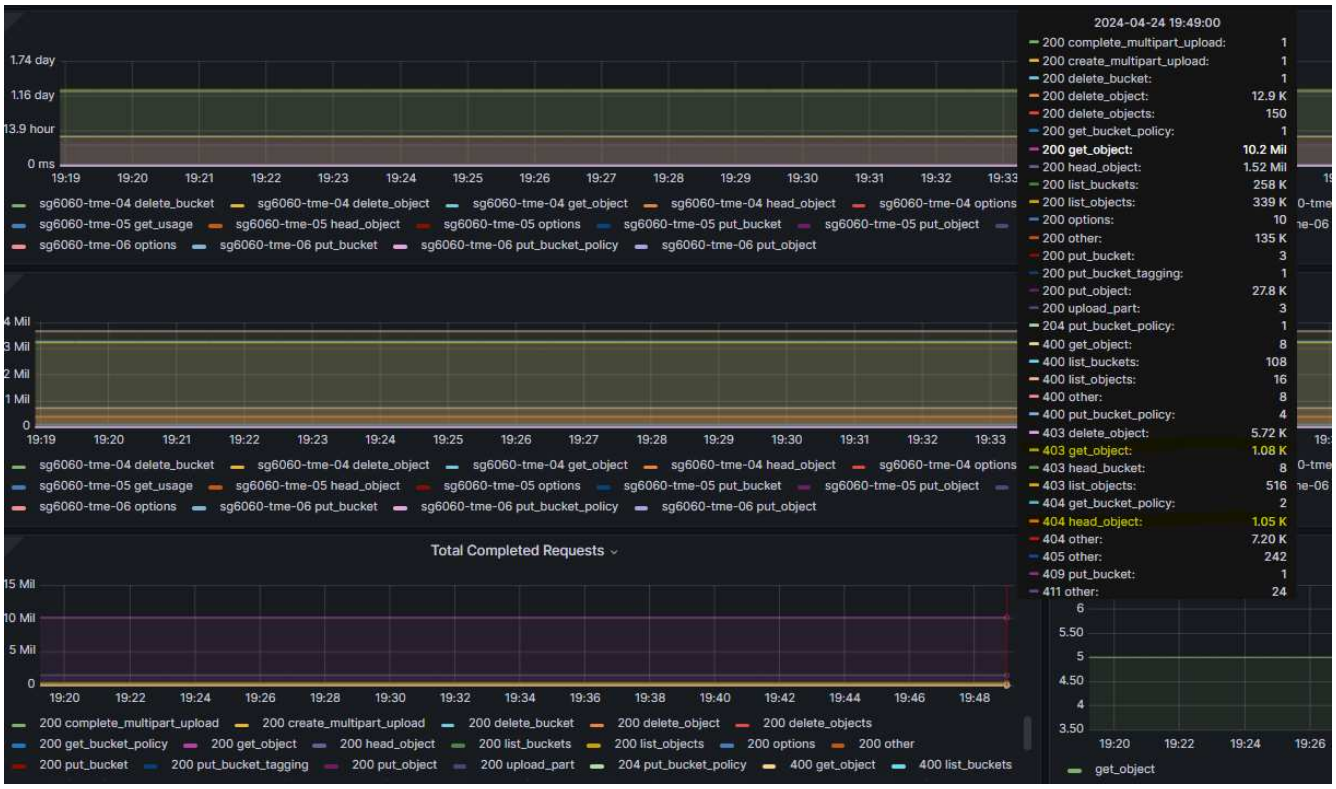
網格站台重新配置和站台範圍的網路變更程序

本指南說明在多站台網格中重新定位 StorageGRID 站台的準備和程序。您應完全瞭解此程序、並事先規劃、以確保程序順暢、並將客戶中斷的情形降至最低。

如果您需要變更整個 Grid 的 Grid 網路、請參閱
"變更網格中所有節點的IP位址"。

重新部署站台前的考量事項

- 應完成站台移動、所有節點應在 15 天內上線、以避免 Cassandra 資料庫重建。
"將儲存節點還原至停機時間超過15天"
- 如果主動式原則中有任何 ILM 規則使用嚴格的擷取行為、如果客戶想要在站台重新定位期間繼續將物件放入 Grid 、請考慮將其變更為平衡或雙重認可。
- 若為具有 60 個以上磁碟機的儲存設備、切勿在安裝磁碟機的情況下移動機櫃。 標記每個磁碟機、並在包裝 / 搬移之前將其從儲存機櫃中移除。
- 變更 StorageGRID 應用裝置網格網路 VLAN 可透過管理網路或用戶端網路從遠端執行。 或是計畫到現場、在重新安置之前或之後執行變更。
- 在放置之前、請檢查客戶應用程式是否使用 head 或取得不存在的物件。如果是、請將貯體一致性變更為 Strong-site 、以避免 HTTP 500 錯誤。 如果您不確定、請查看 S3 概述 Grafana 圖表 * Grid Manager > Support > Metrics * 、將滑鼠移到「完成的申請總數」圖表上。 如果「 Get Object 」（取得物件）或「 404 head 物件」（ 404 頭物件）的數量非常高、則可能有一或多個應用程式使用 head 或 Get non生存 物件。這是累積次數、將滑鼠移到不同的時間軸上以查看差異。



站台重新定位前變更 **Grid IP** 位址的程序

步驟

1. 如果在新位置使用新的 Grid 網路子網路、 "將子網路新增至 Grid 網路子網路清單"
2. 登入主要管理節點、使用 change-ip 進行 Grid IP 變更、必須 * 登入 * 登入 * 變更才能關閉節點以進行重新定位。
   a. 選擇 2 、然後選擇 1 進行網格 IP 變更

```
Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP/mask [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP/mask [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP/mask [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP/mask [     10.45.74.18/26 ]: 10.45.74.28/26
================================================================================
LONDON-ADM1 Grid    Gateway [         10.45.74.1 ]:
LONDON-S1   Grid    Gateway [         10.45.74.1 ]:
LONDON-S2   Grid    Gateway [         10.45.74.1 ]:
LONDON-S3   Grid    Gateway [         10.45.74.1 ]:
================================================================================
================================================================================
Site: OXFORD
================================================================================
OXFORD-ADM1 Grid    IP/mask [     10.45.75.14/26 ]:
OXFORD-S1   Grid    IP/mask [     10.45.75.16/26 ]:
OXFORD-S2   Grid    IP/mask [     10.45.75.17/26 ]:
OXFORD-S3   Grid    IP/mask [     10.45.75.18/26 ]:
================================================================================
OXFORD-ADM1 Grid    Gateway [         10.45.75.1 ]:
OXFORD-S1   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S2   Grid    Gateway [         10.45.75.1 ]:
OXFORD-S3   Grid    Gateway [         10.45.75.1 ]:
================================================================================
Finished editing. Press Enter to return to menu.
```

b. 選取 5 以顯示變更

```
================================================================================
Site: LONDON
================================================================================
LONDON-ADM1 Grid    IP      [     10.45.74.14/26 ]: 10.45.74.24/26
LONDON-S1   Grid    IP      [     10.45.74.16/26 ]: 10.45.74.26/26
LONDON-S2   Grid    IP      [     10.45.74.17/26 ]: 10.45.74.27/26
LONDON-S3   Grid    IP      [     10.45.74.18/26 ]: 10.45.74.28/26
Press Enter to continue
```

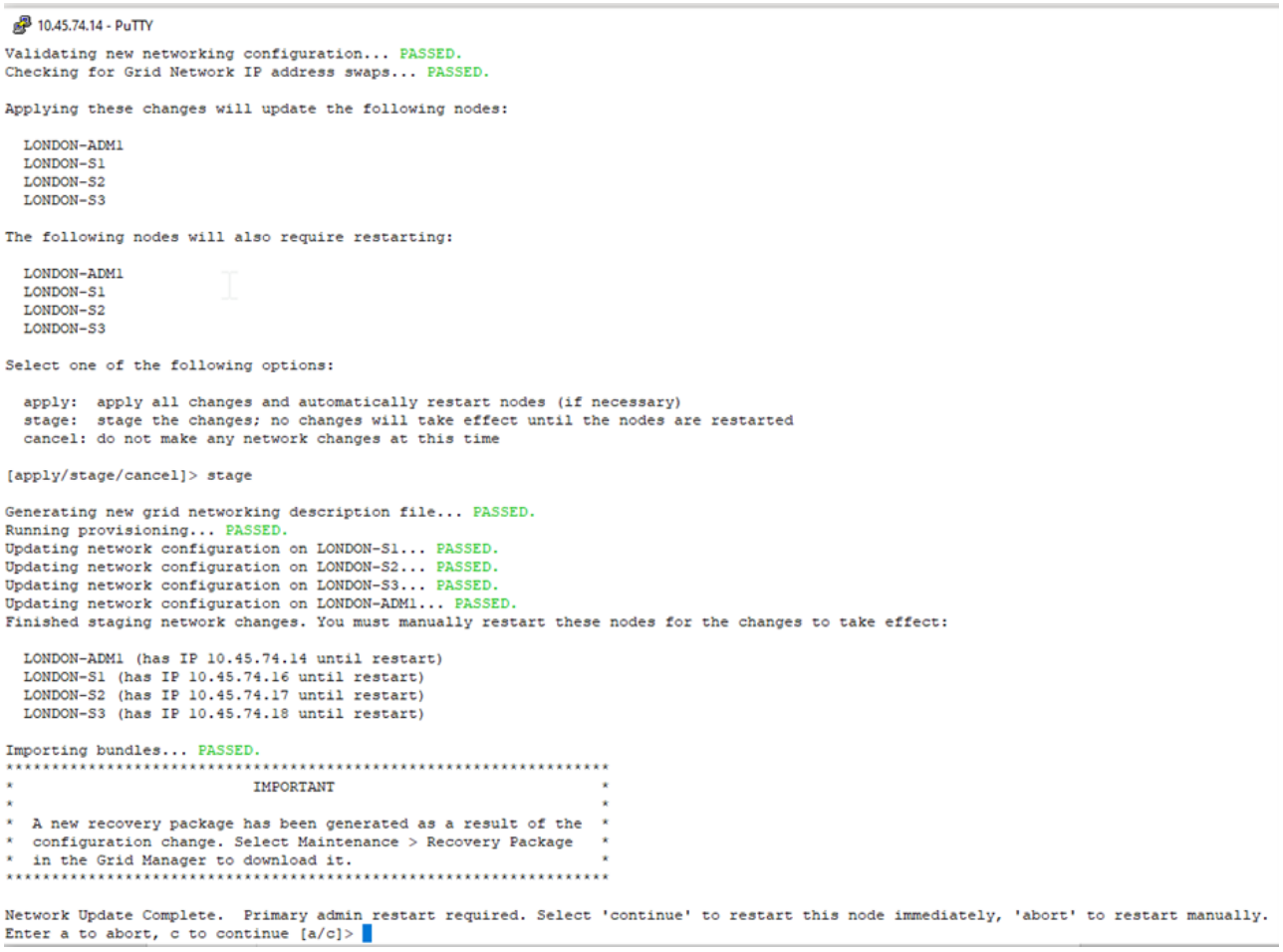
c. 選取 10 以驗證及套用變更。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
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: 10
```

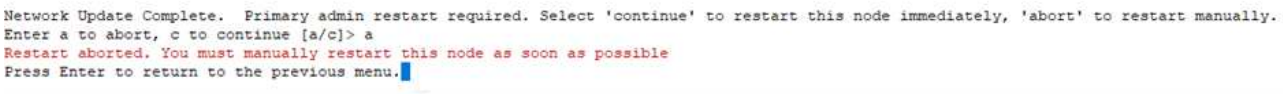
d. 必須在此步驟中選擇 * 階段 * 。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

The following nodes will also require restarting:

  LONDON-ADM1
  LONDON-S1
  LONDON-S2
  LONDON-S3

Select one of the following options:

  apply:  apply all changes and automatically restart nodes (if necessary)
  stage:  stage the changes; no changes will take effect until the nodes are restarted
  cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. 如果上述變更中包含主要管理節點、請輸入 *'A' 以手動重新啟動主要管理節點 *



f. 按 ENTER 鍵返回上一個功能表、然後結束 change-IP 介面。



3. 從 Grid Manager 下載新的恢復套件。* Grid manager* > * Maintenance * > * Recovery package*
4. 如果 StorageGRID 應用裝置需要變更 VLAN 、請參閱一節 應用裝置 VLAN 變更。
5. 關閉站台上的所有節點和 / 或應用裝置、必要時標記 / 移除磁碟機、卸載、包裝和移動。
6. 如果您計畫變更管理網路 IP 和 / 或用戶端 VLAN 和 IP 位址、您可以在重新配置後執行變更。

應用裝置 **VLAN** 變更

下列程序假設您可以遠端存取 StorageGRID 應用裝置的管理員或用戶端網路、以便從遠端執行變更。

步驟

1. 關閉應用裝置之前、
"將產品置於維護模式"。
2. 使用瀏覽器存取 StorageGRID 應用裝置安裝程式 GUI https://<admin-or-client-network-ip>:8443。 一旦設備開機進入維護模式、就無法使用 Grid IP 做為已就緒的新 Grid IP 。
3. 變更 Grid 網路的 VLAN 。 如果您是透過用戶端網路存取應用裝置、目前無法變更用戶端 VLAN 、您可以在移動後變更。

4. SSH 至應用裝置、並使用「 hutdoown -h now 」關閉節點
5. 在新網站上準備好應用裝置之後、請使用存取 StorageGRID 應用裝置安裝程式 GUI https://<grid-network-ip>:8443。 使用 GUI 中的 ping/nmap 工具、確認儲存設備處於最佳狀態、並與其他網格節點進行網路連線。
6. 如果計畫變更用戶端網路 IP 、您可以在此階段變更用戶端 VLAN 。 用戶端網路尚未就緒、除非您在稍後的步驟中使用 change-ip 工具更新用戶端網路 IP 。
7. 結束維護模式。從「the Some Appliance Installer」StorageGRID 選取「進階>*重新開機控制器*」、然後選取「*重新開機至StorageGRID *」。
8. 當所有節點都正常運作且 Grid 沒有連線問題時、如有必要、請使用 change-ip 來更新應用裝置管理網路和用戶端網路。

將物件型儲存設備從 **ONTAP S3** 移轉至 **StorageGRID**

透過將物件型儲存設備從 **ONTAP S3** 順暢移轉至 **StorageGRID** 、實現企業級 **S3**

透過將物件型儲存設備從 ONTAP S3 順暢移轉至 StorageGRID 、實現企業級 S3

移轉示範

這是將使用者和貯體從 ONTAP S3 移轉至 StorageGRID 的示範。

透過將物件型儲存設備從 **ONTAP S3** 順暢移轉至 **StorageGRID** 、實現企業級 **S3**

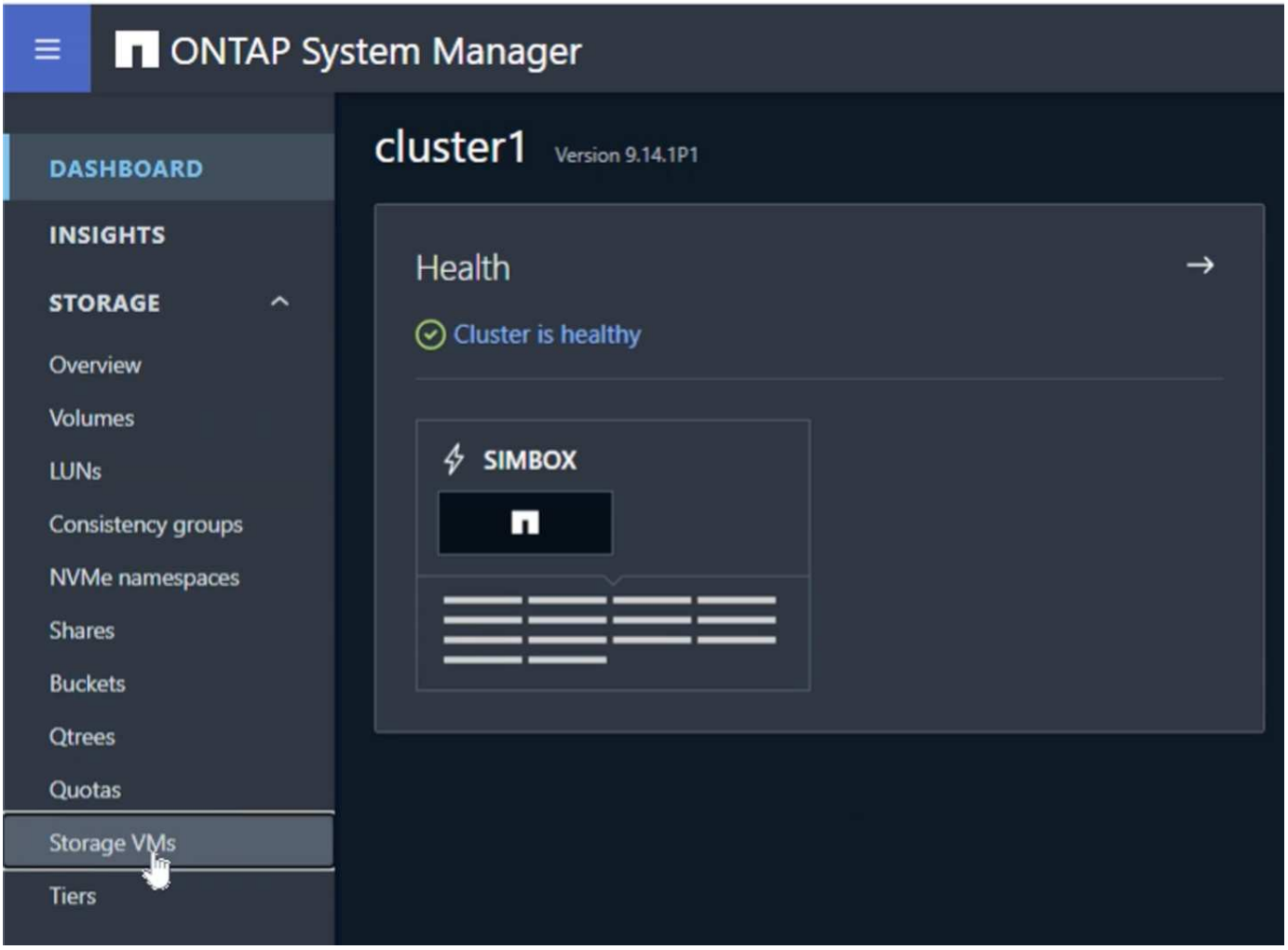
透過將物件型儲存設備從 ONTAP S3 順暢移轉至 StorageGRID 、實現企業級 S3

準備 **ONTAP**

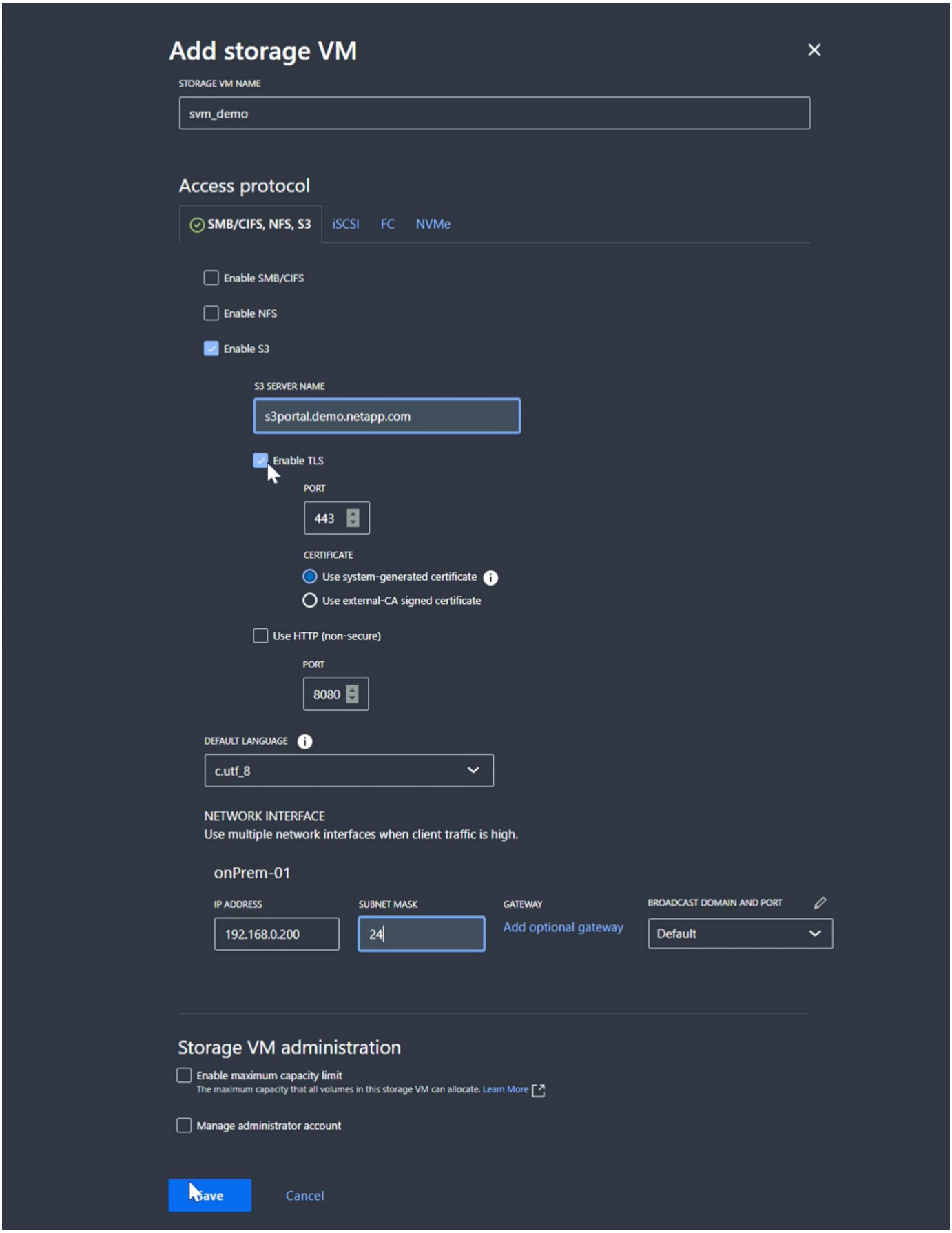
為了展示用途、我們將建立 SVM 物件儲存區伺服器、使用者、群組、群組原則和儲存區。

建立儲存虛擬機器

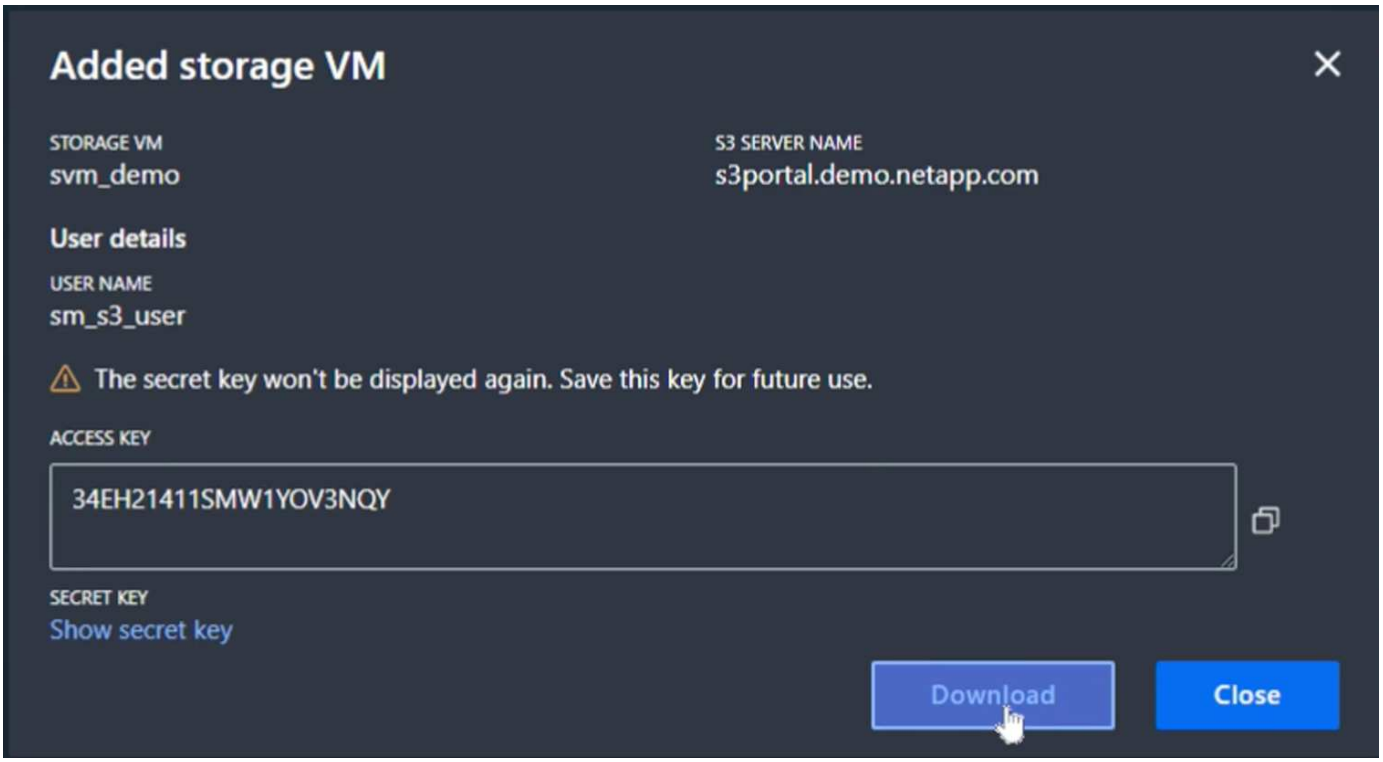
在 ONTAP System Manager 中、瀏覽至儲存 VM 、然後新增儲存 VM 。



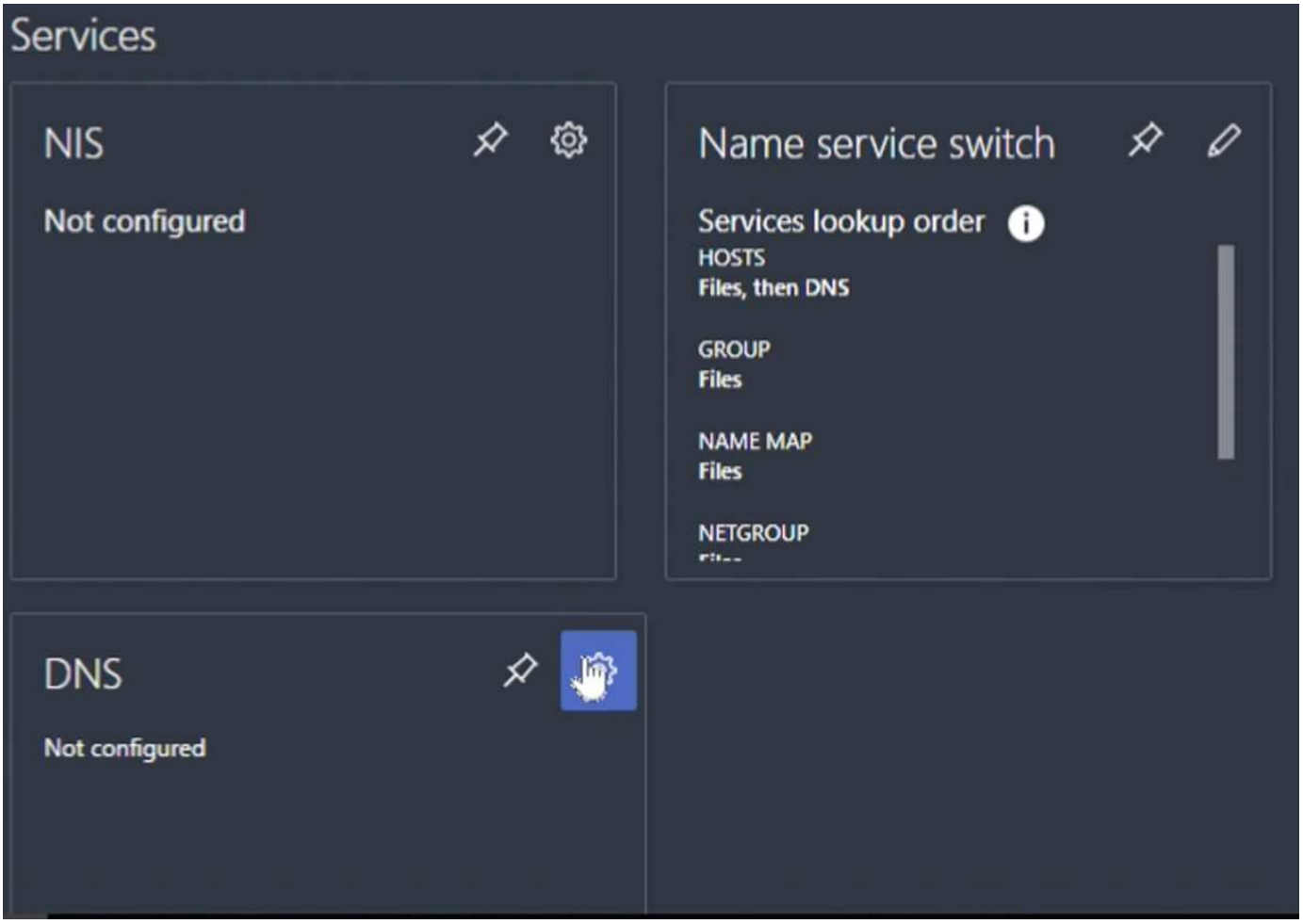
選取「啟用 S3 」和「啟用 TLS 」核取方塊、然後設定 HTTP （ S ）連接埠。定義 IP 、子網路遮罩、並定義閘道和廣播網域（如果您的環境中未使用預設或必要）。



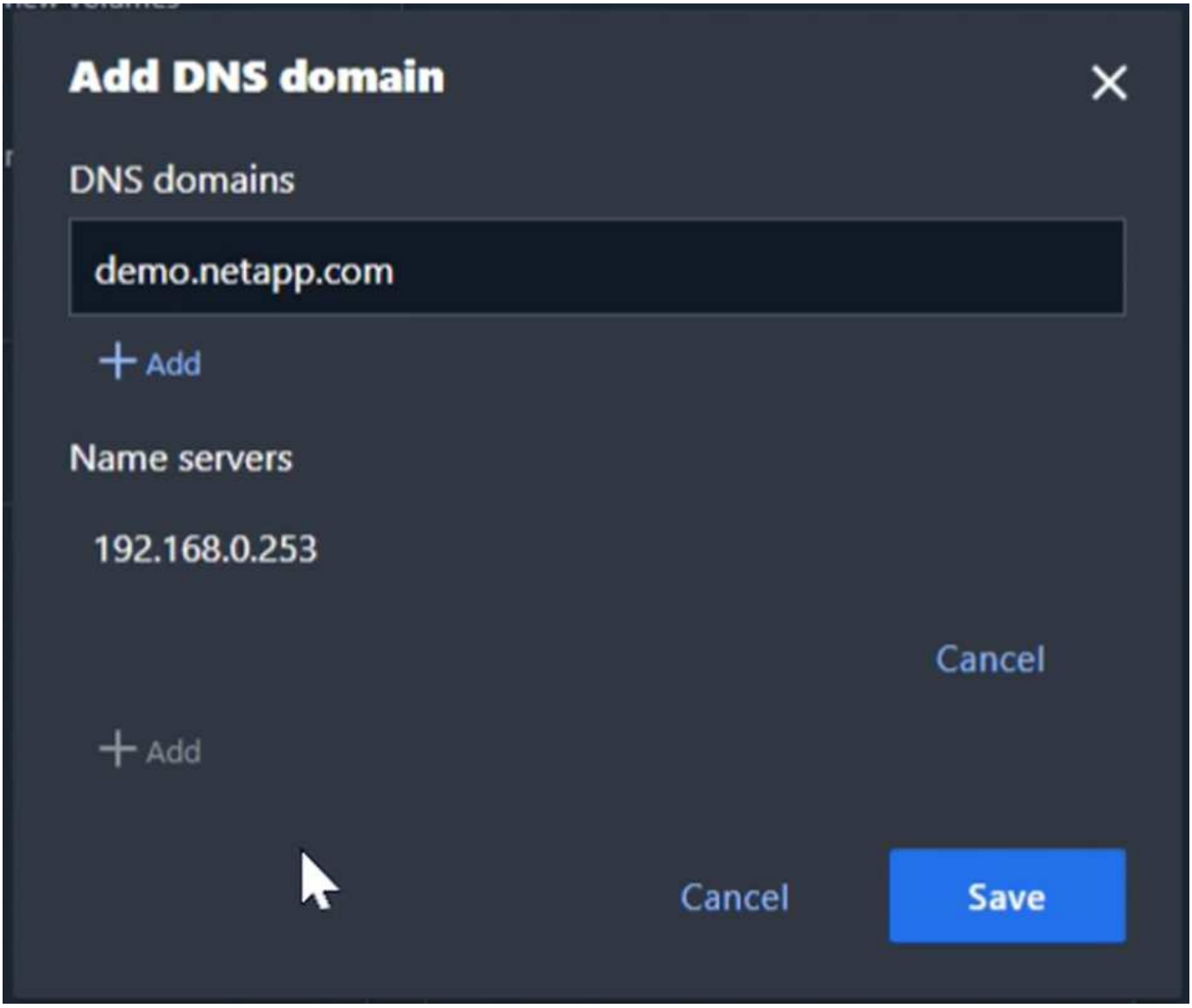
在建立 SVM 的過程中、將會建立使用者。下載此使用者的 S3 金鑰並關閉視窗。



建立 SVM 之後、請編輯 SVM 並新增 DNS 設定。

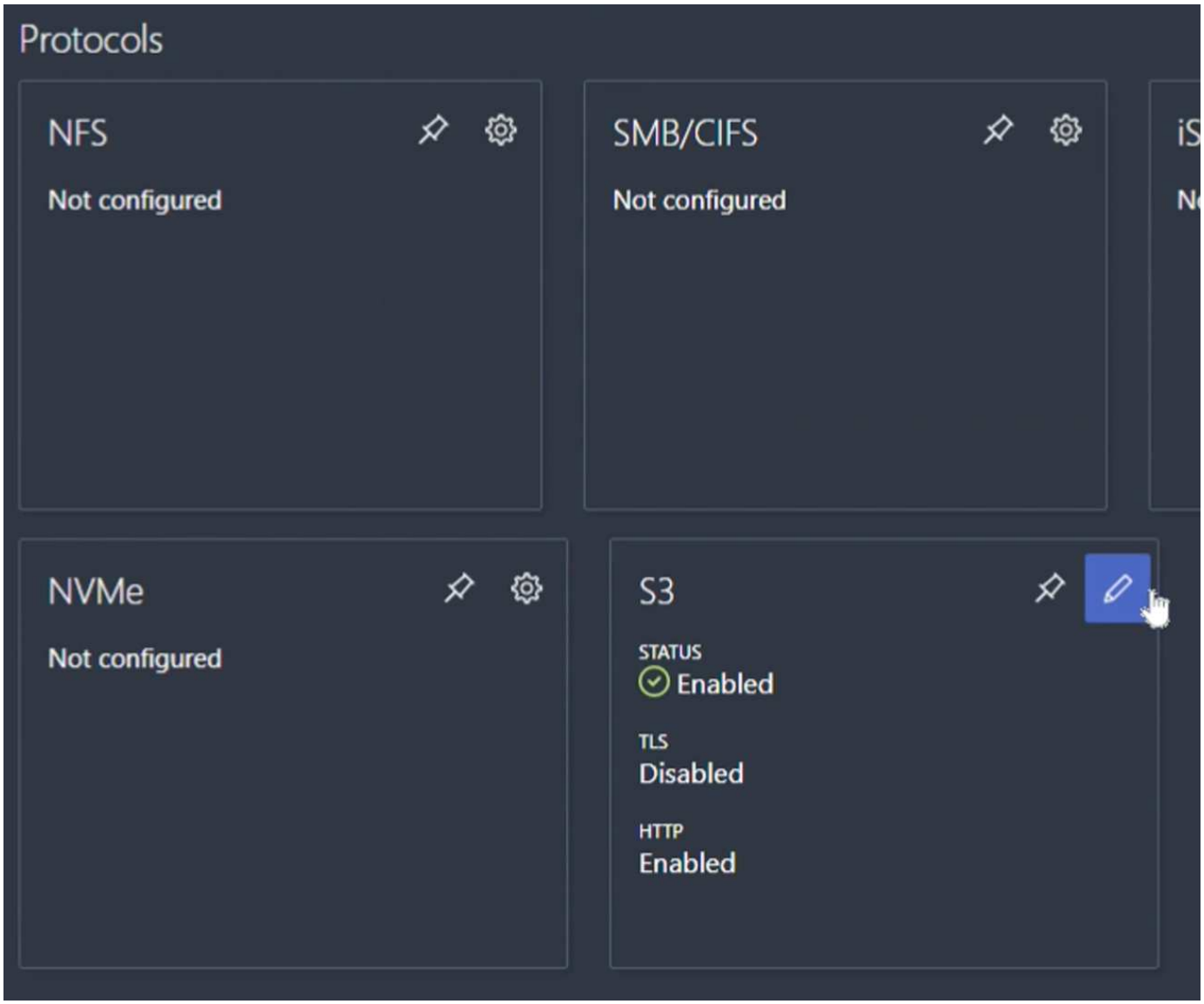


定義 DNS 名稱和 IP 。

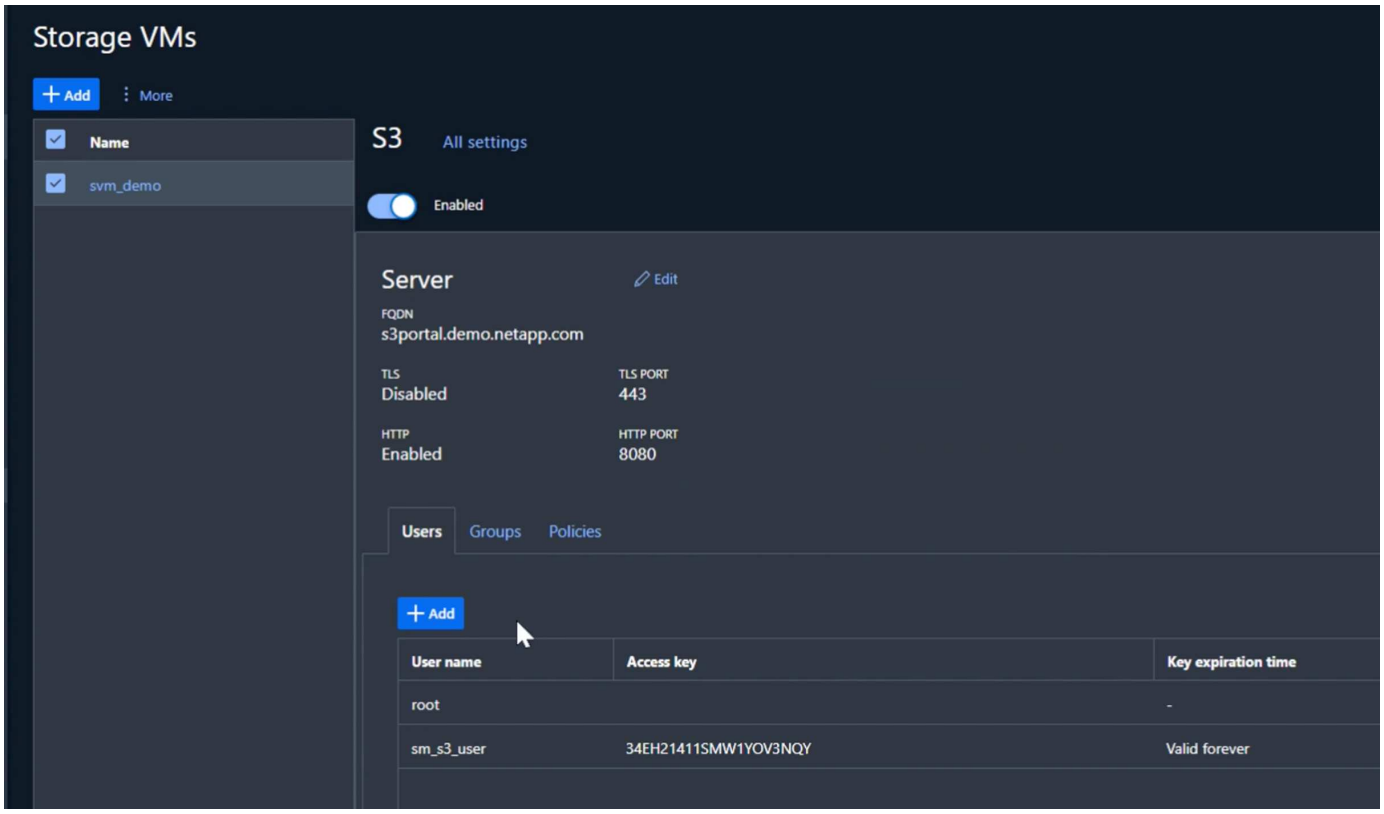


建立 **SVM S3** 使用者

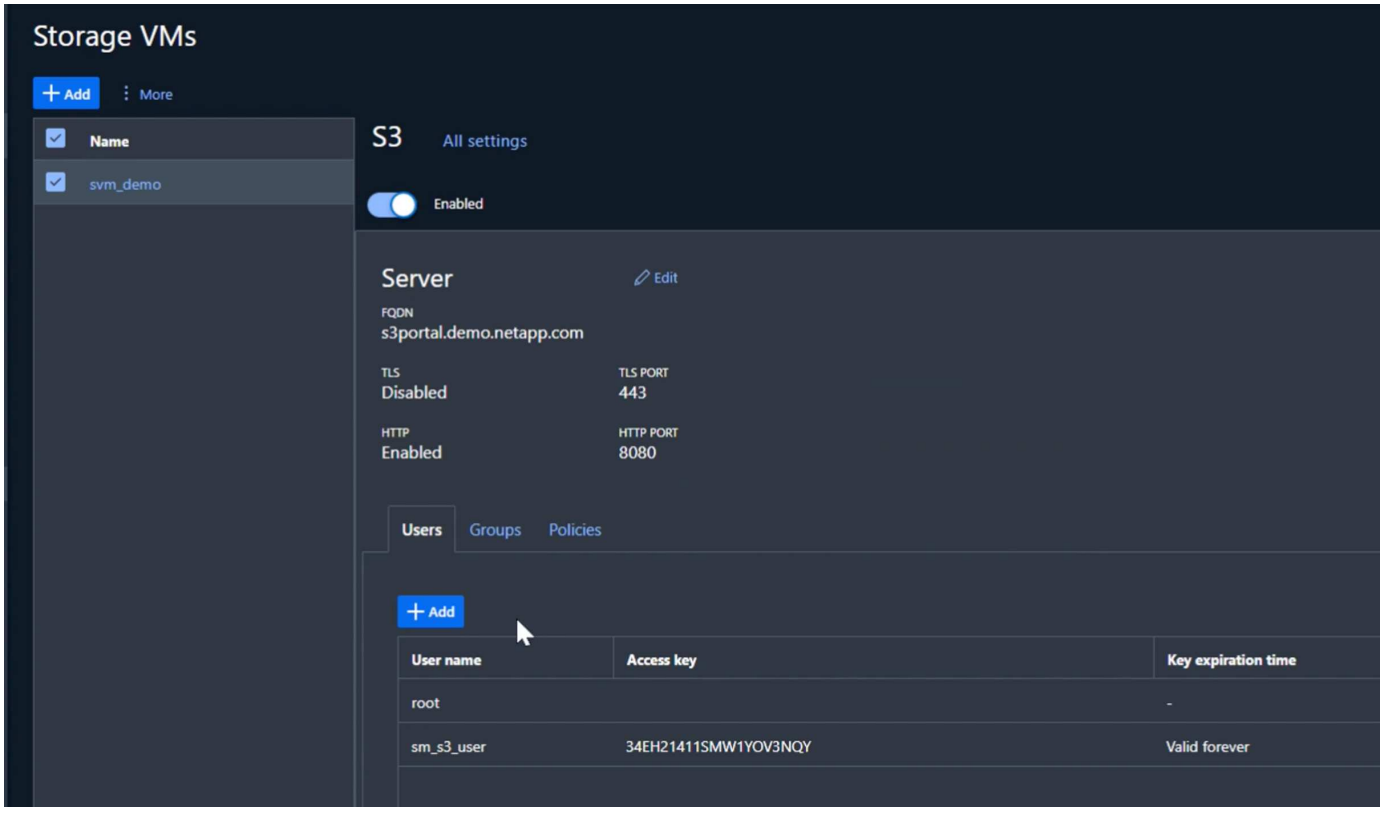
現在我們可以設定 S3 使用者和群組。編輯 S3 設定。


Protocols
NFS
Not configured
SMB/CIFS
Not configured
NVMe
Not configured
S3
STATUS
Enabled
TLS
Disabled
HTTP
Enabled

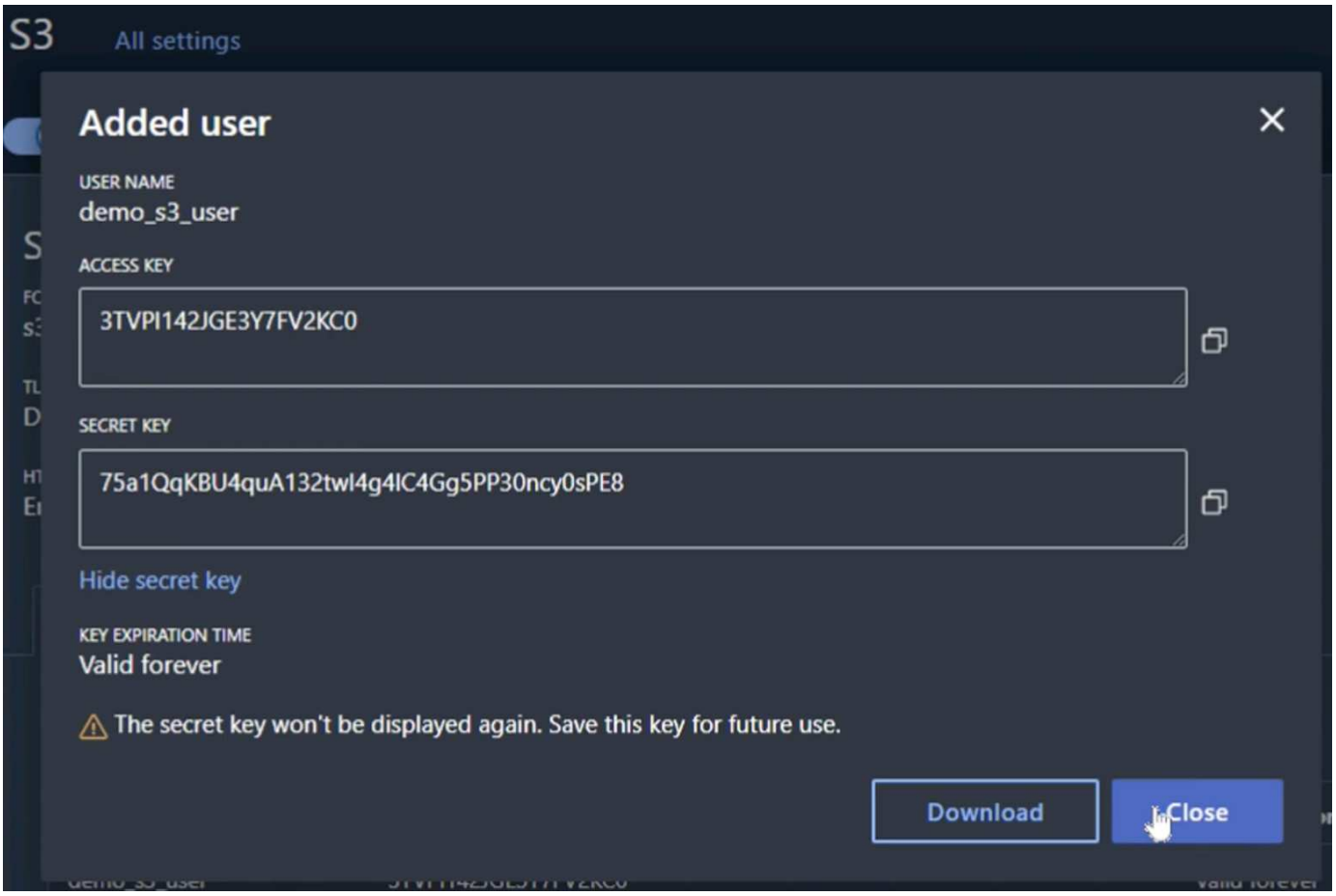
新增使用者。



輸入使用者名稱和金鑰到期日。

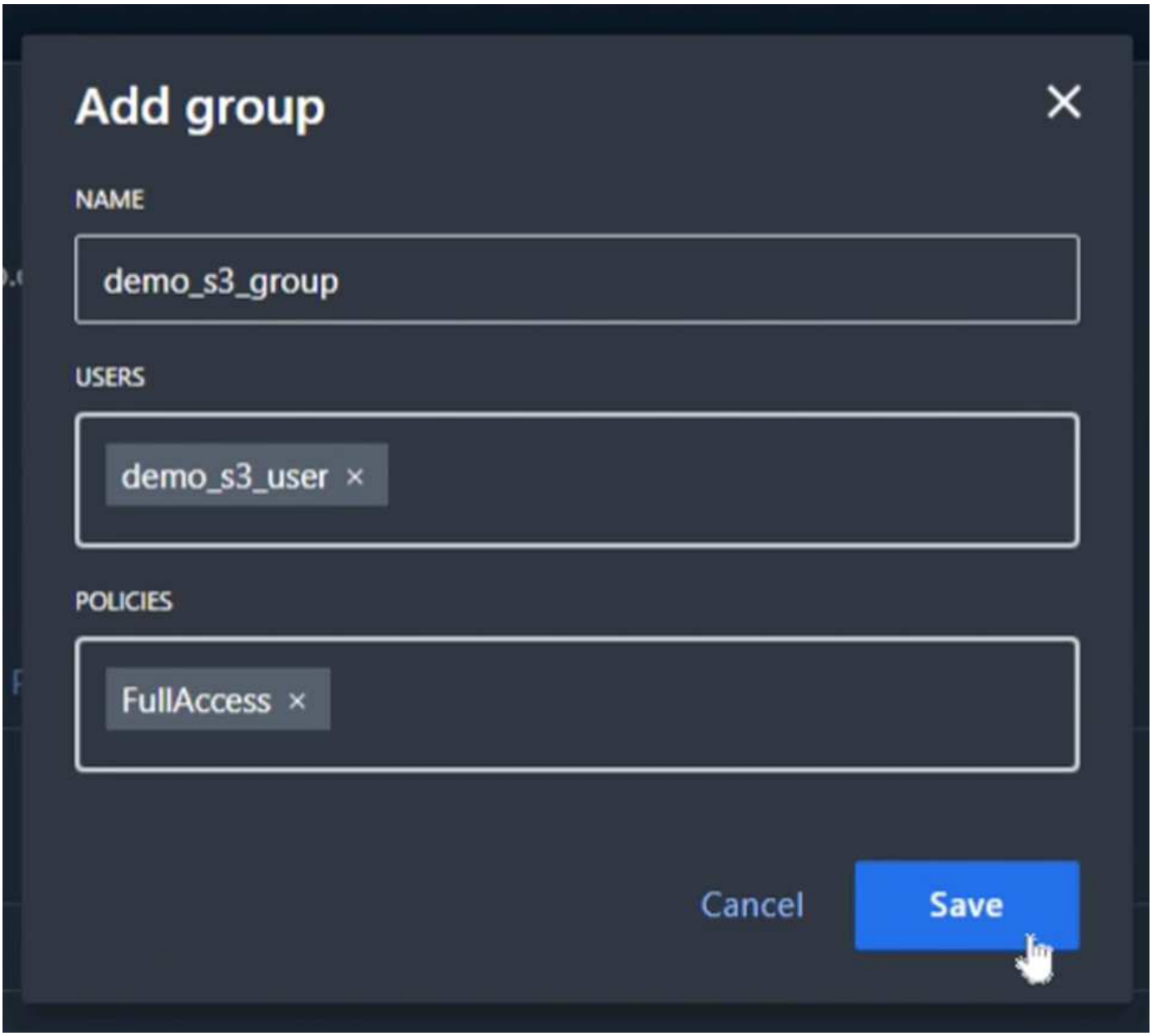


下載適用於新使用者的 S3 金鑰。



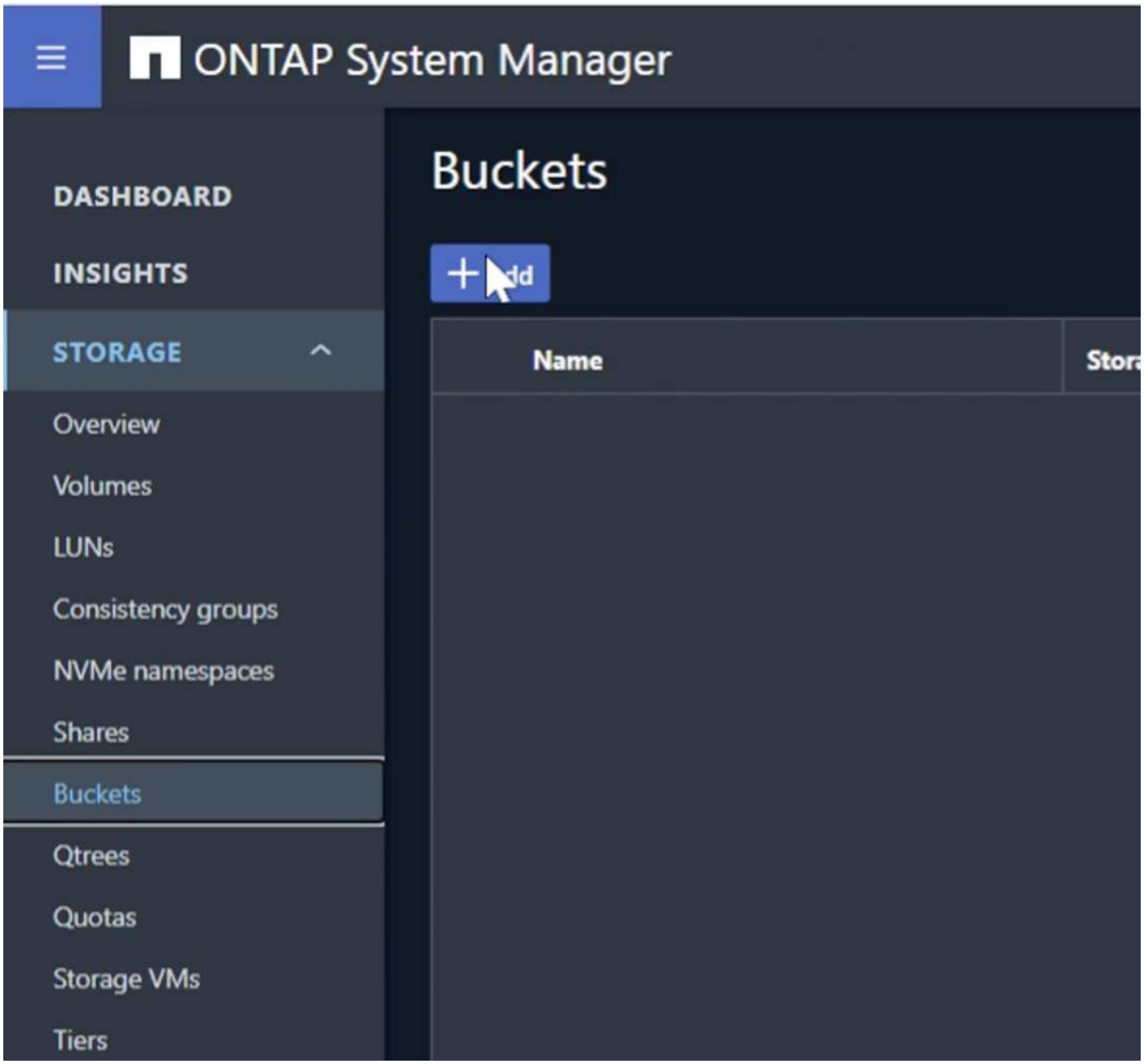
建立 **SVM S3** 群組

在 SVM S3 設定的「群組」索引標籤上、新增具有上述建立之使用者和「完整存取」權限的新群組。

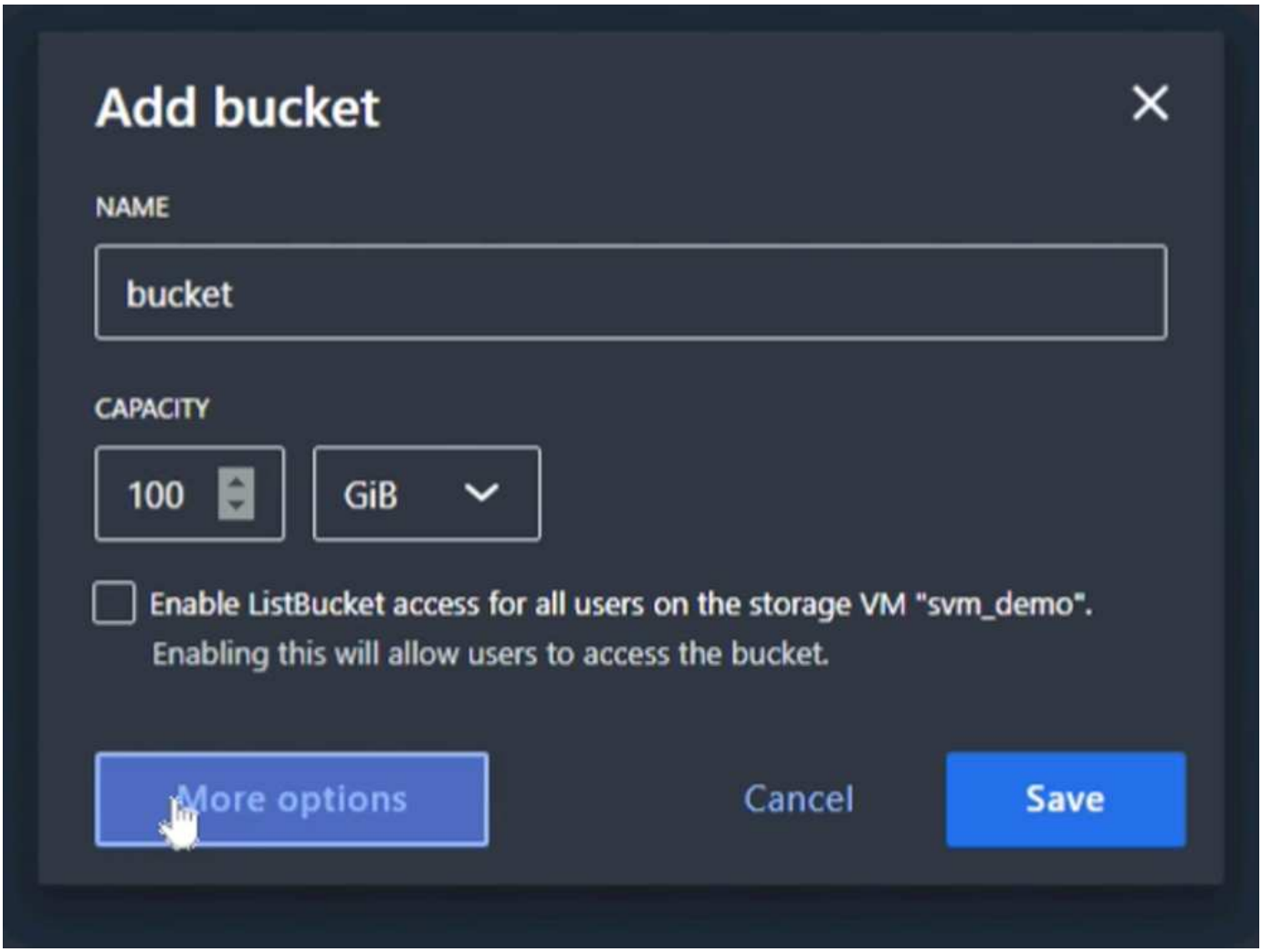


建立 **SVM S3** 儲存區

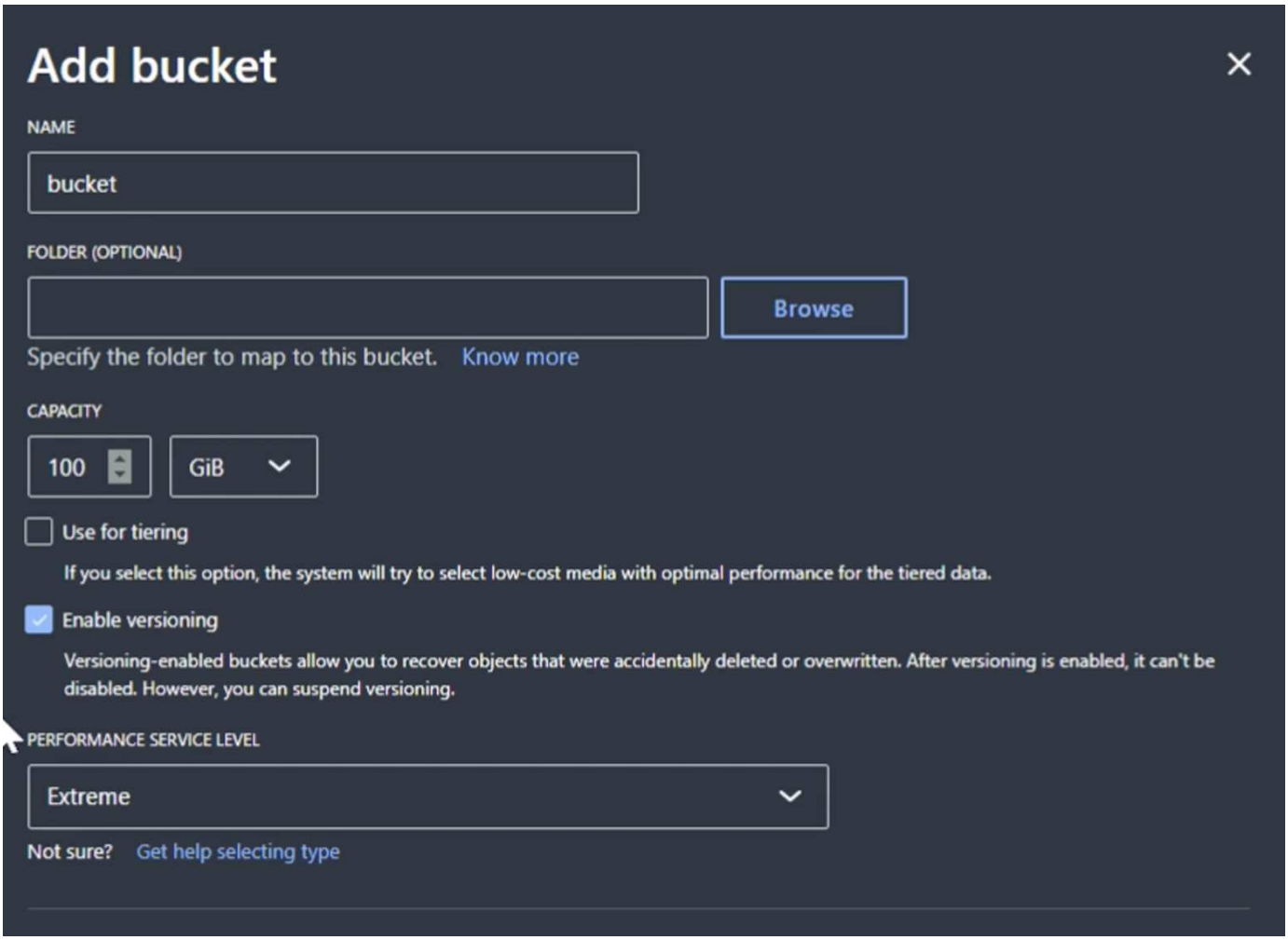
瀏覽至「鏟斗」區段、然後按一下「 + 新增」按鈕。



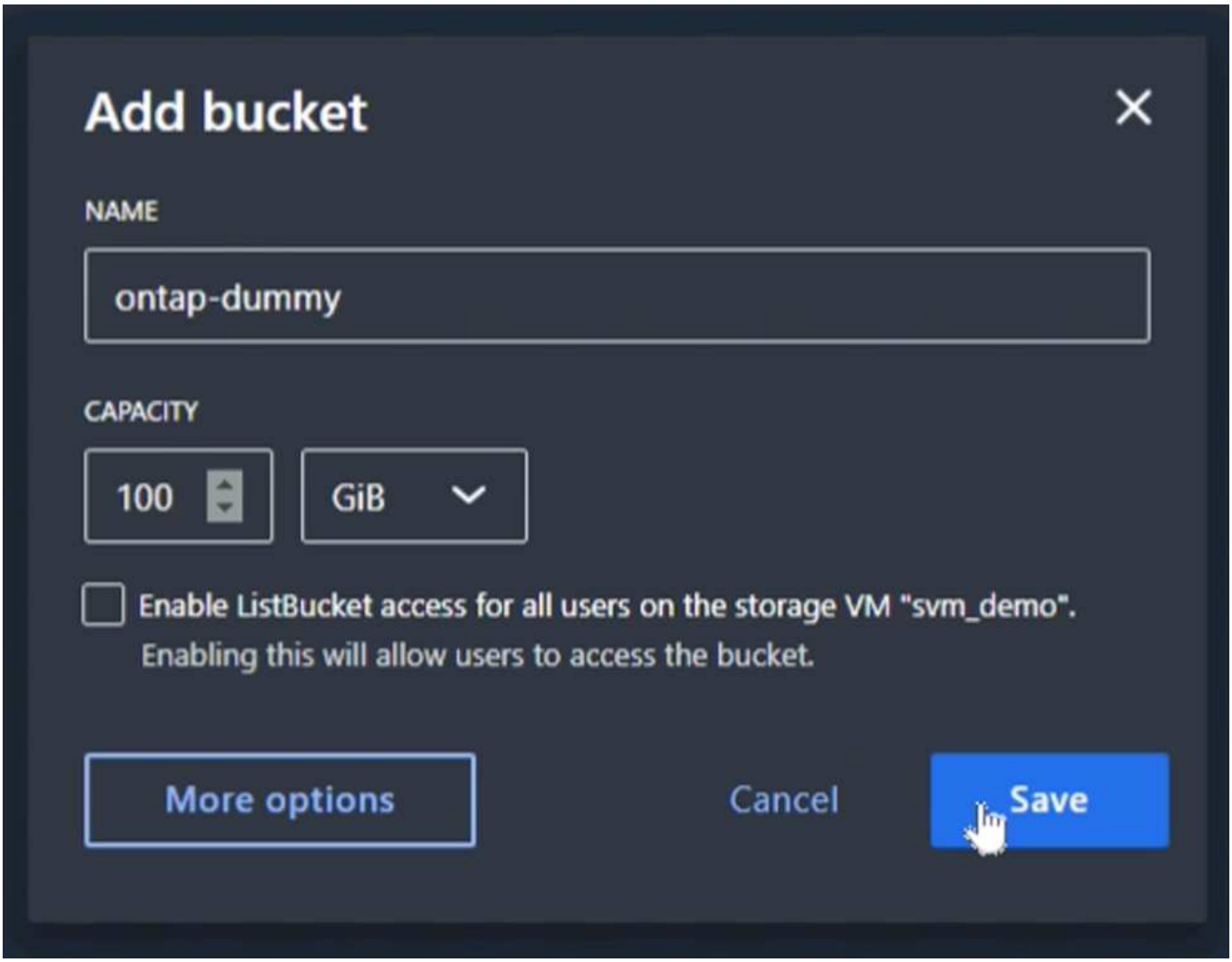
輸入名稱、容量、並取消選取「啟用清單儲存庫存取 … 」核取方塊、然後按一下「更多選項」按鈕。



在「更多選項」區段中、選取「啟用版本設定」核取方塊、然後按一下「儲存」按鈕。



重複此程序並建立第二個儲存區、但不啟用版本設定。輸入名稱、與貯體 1 的容量相同、並取消選取「啟用 ListBucket 存取 … 」核取方塊、然後按一下「儲存」按鈕。



_ 作者： Rafael Guedes 和 Aron Klein_

透過將物件型儲存設備從 **ONTAP S3** 順暢移轉至 **StorageGRID** 、實現企業級 **S3**

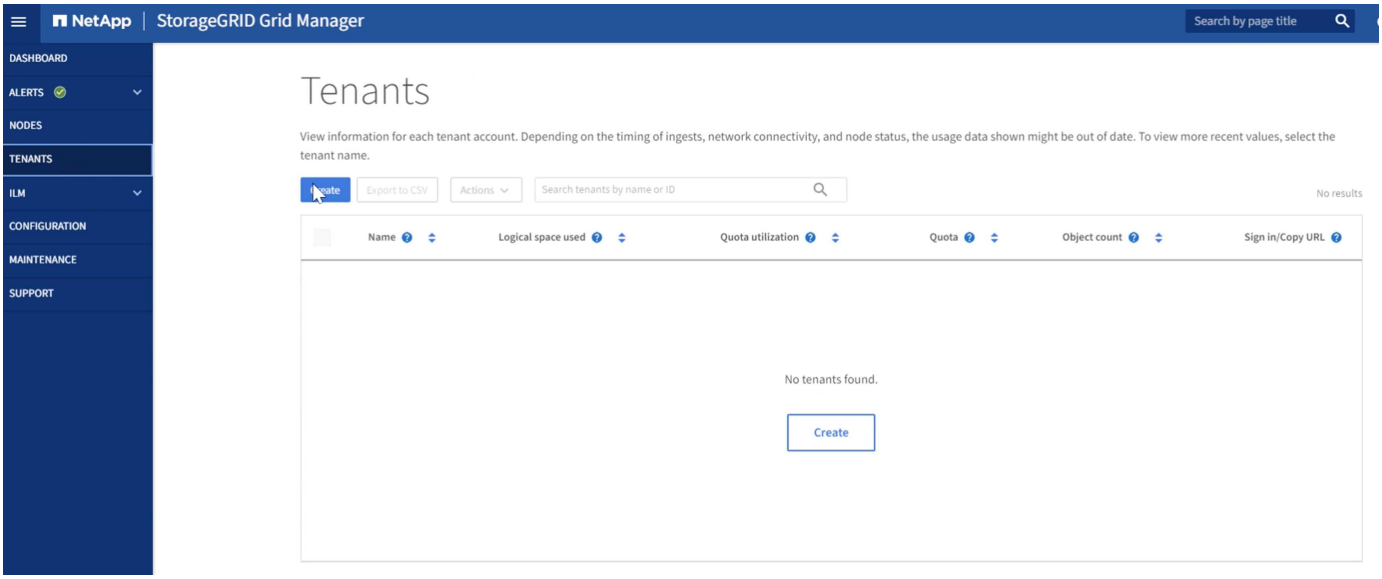
透過將物件型儲存設備從 ONTAP S3 順暢移轉至 StorageGRID 、實現企業級 S3

準備 **StorageGRID**

繼續進行此示範的組態、我們將建立租戶、使用者、安全群組、群組原則和貯體。

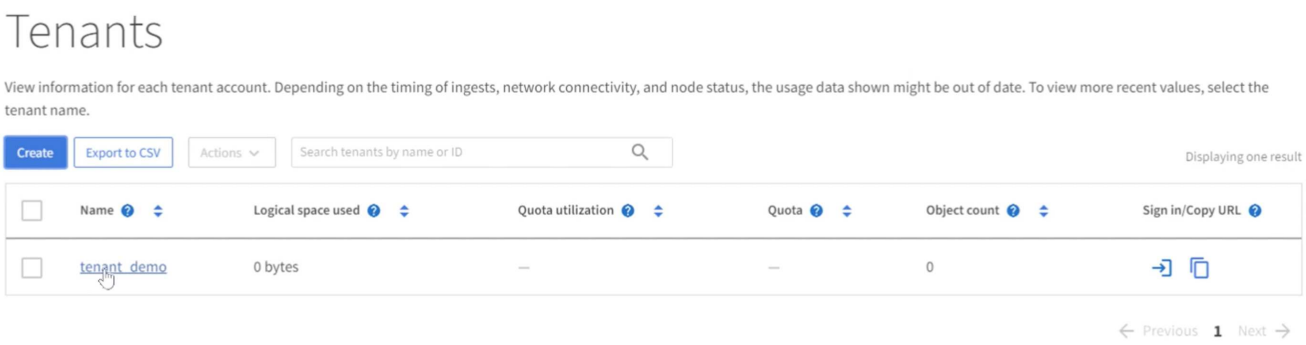
建立租戶

瀏覽至「租戶」標籤、然後按一下「建立」按鈕

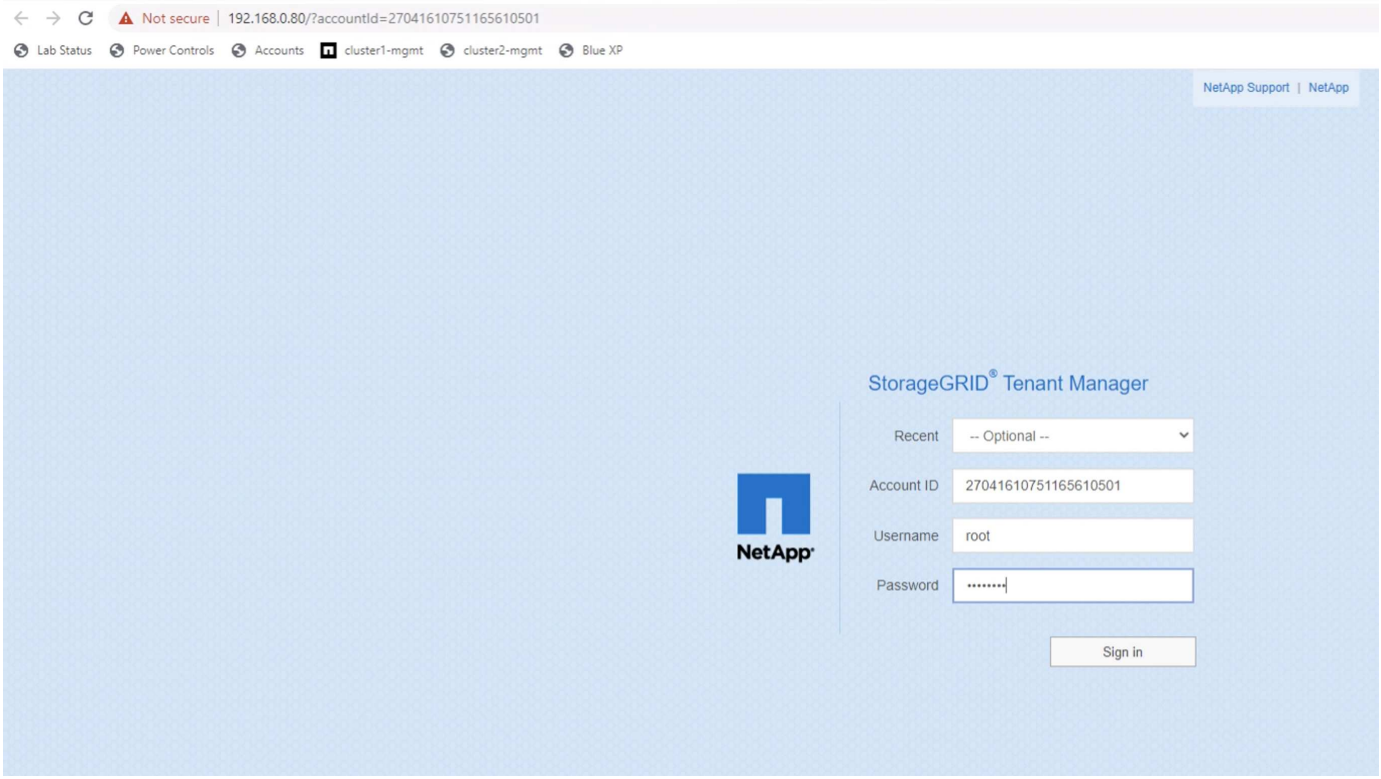


填寫租戶提供租戶名稱的詳細資料、選取 S3 作為用戶端類型、不需要配額。無需選取平台服務或允許 S3 選取。您可以選擇使用自己的身分識別來源。設定 root 密碼、然後按一下完成按鈕。

按一下租戶名稱以檢視租戶詳細資料。* 您稍後需要租戶 ID 、請將其複製到 * 。按一下「登入」按鈕。這會將您帶到租戶入口網站登入。儲存 URL 以供未來使用。

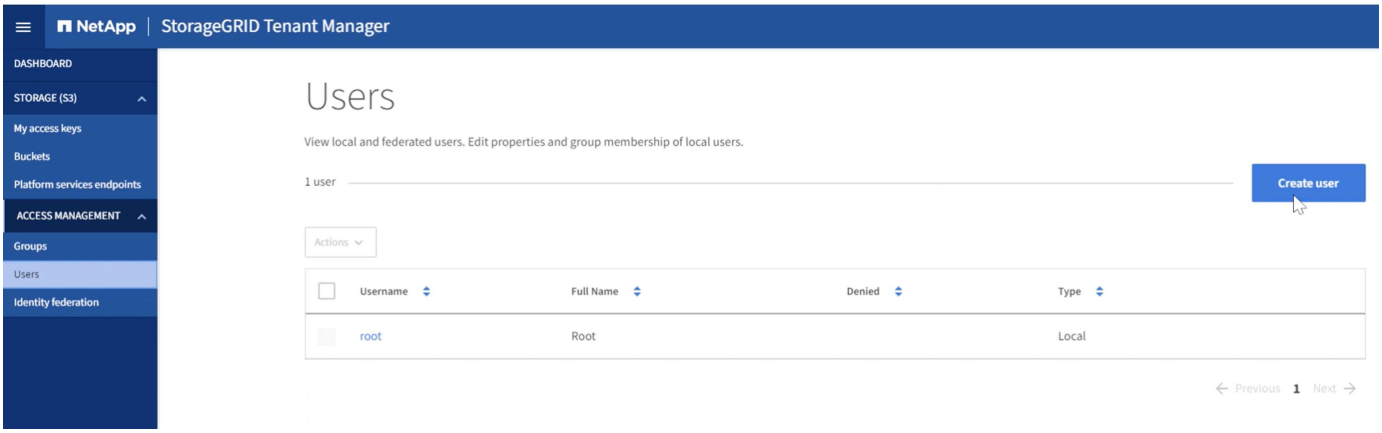


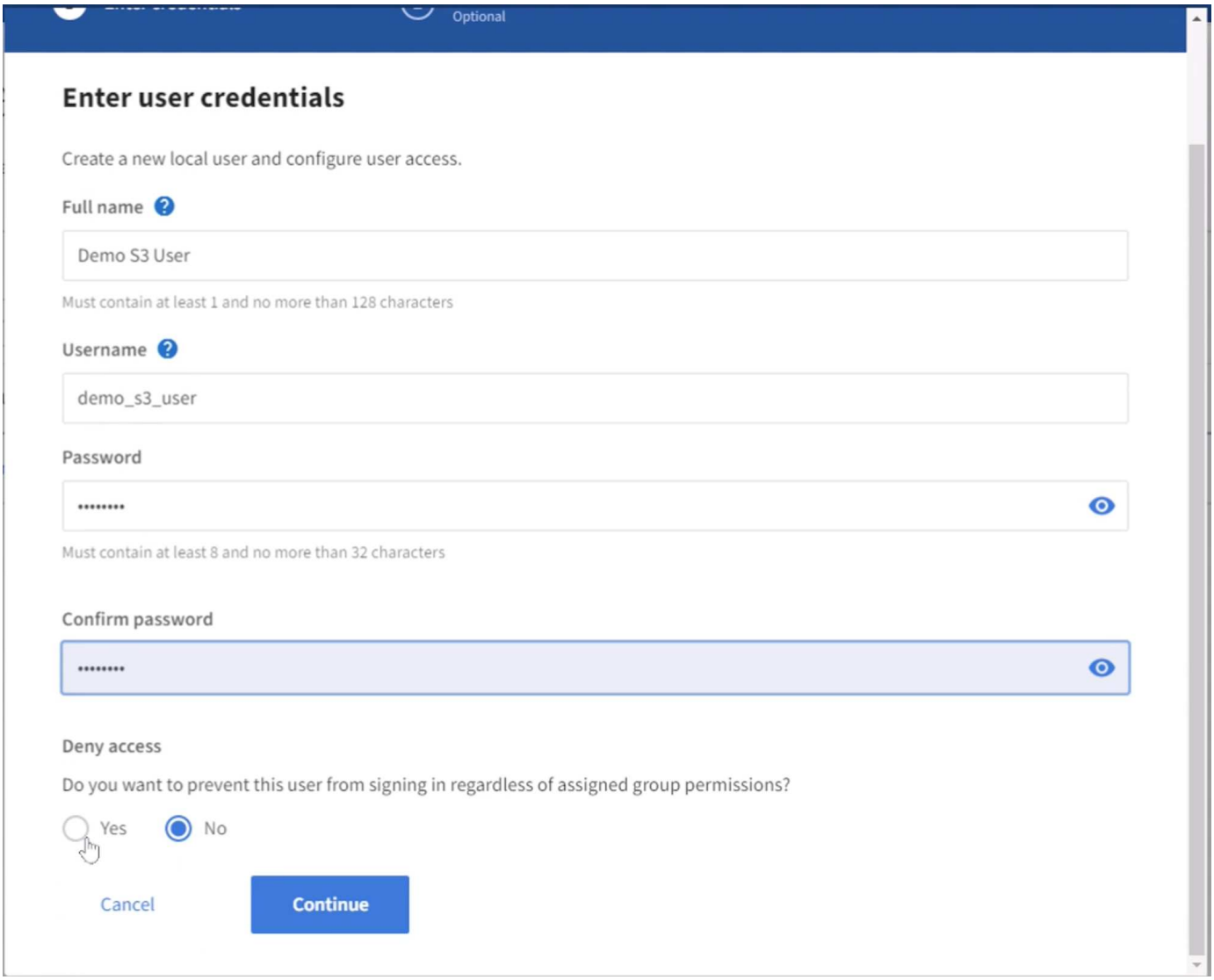
這會將您帶到租戶入口網站登入。儲存 URL 以供未來使用、然後輸入 root 使用者認證。



建立使用者

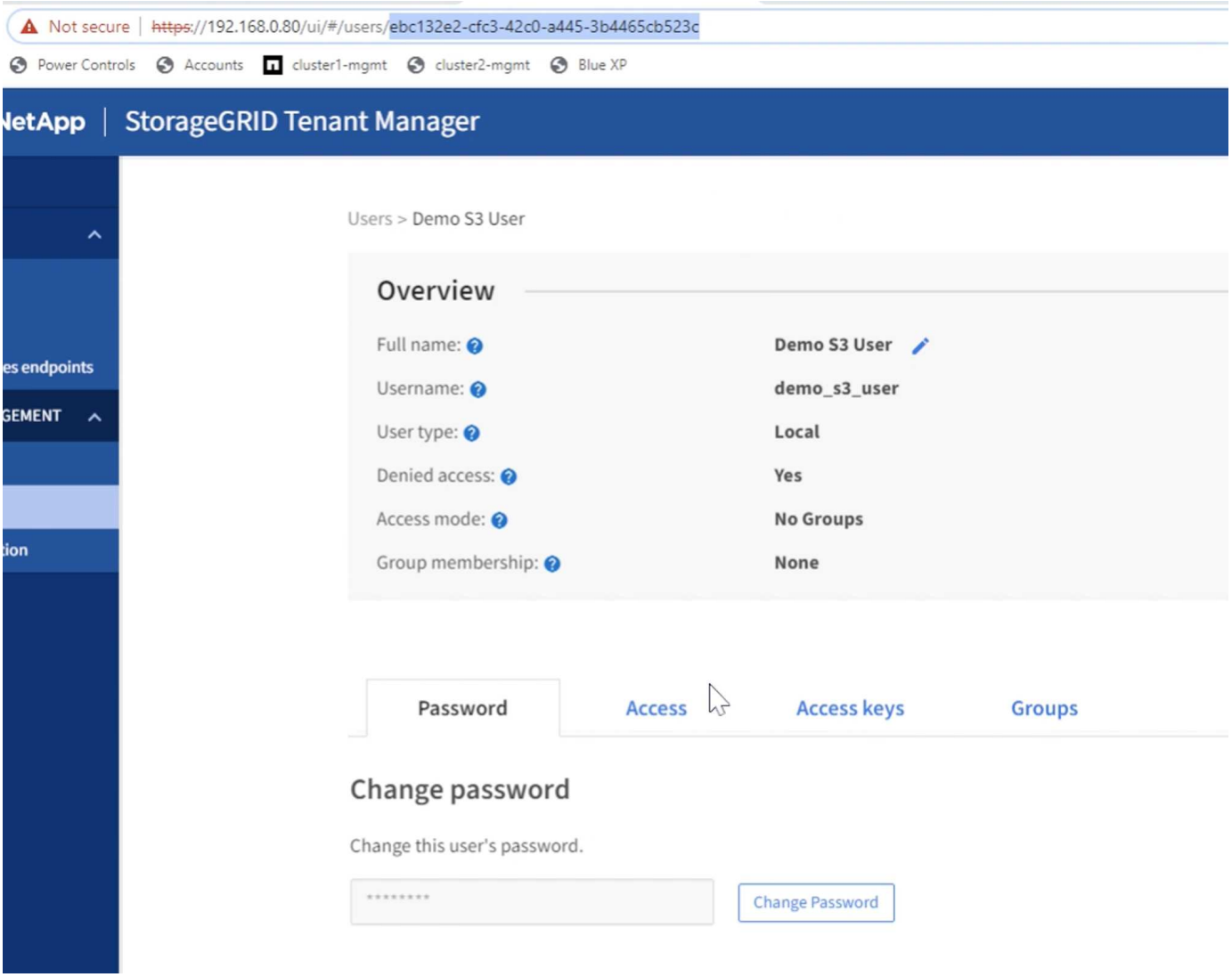
瀏覽至「使用者」標籤並建立新使用者。



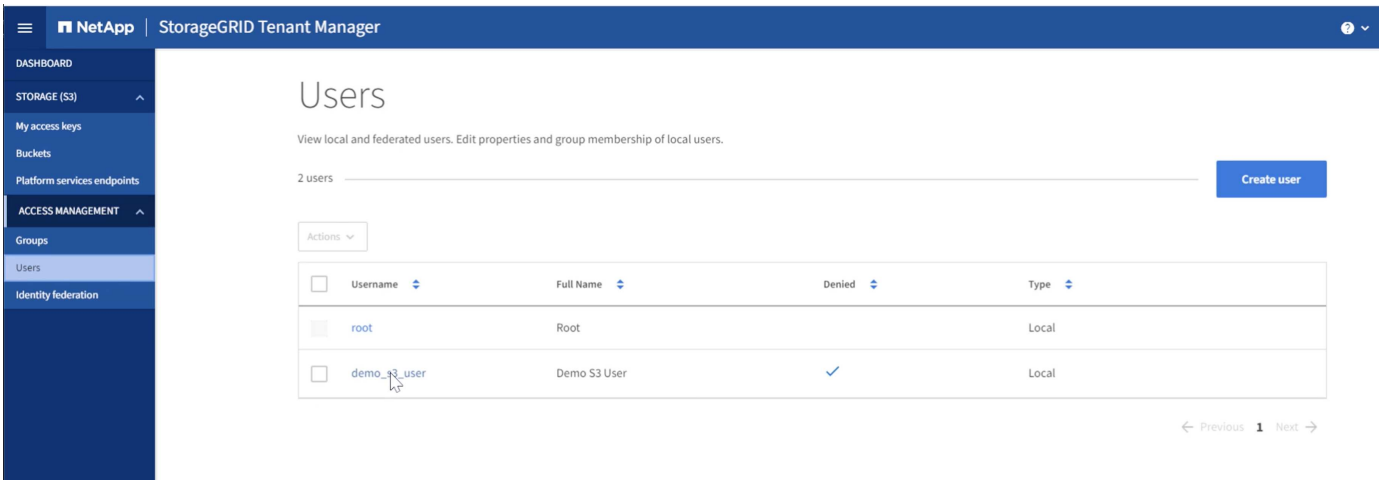


建立新使用者之後、請按一下使用者名稱以開啟使用者的詳細資料。

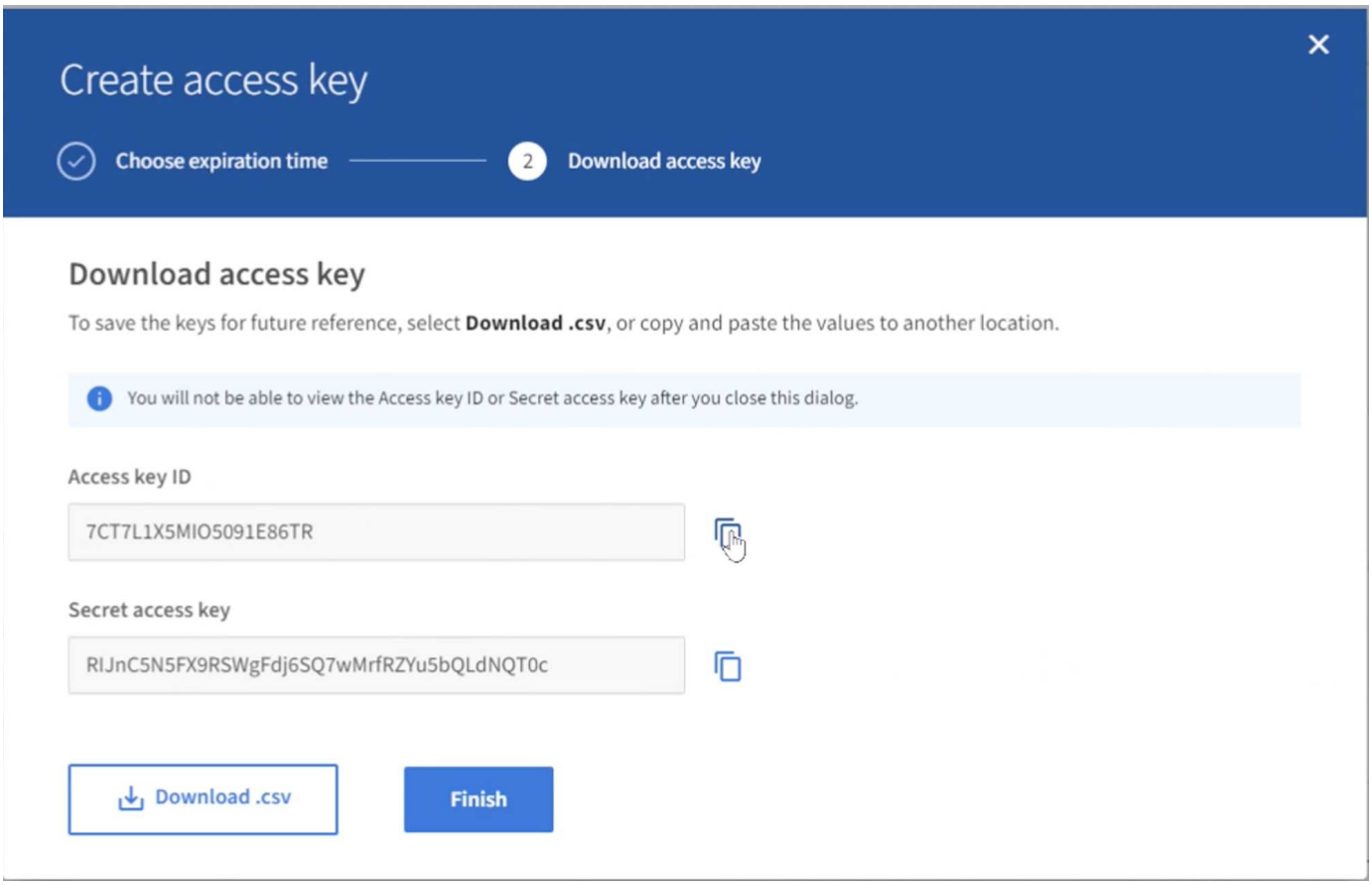
從稍後要使用的 URL 複製使用者 ID 。



若要建立 S3 金鑰、請按一下使用者名稱。

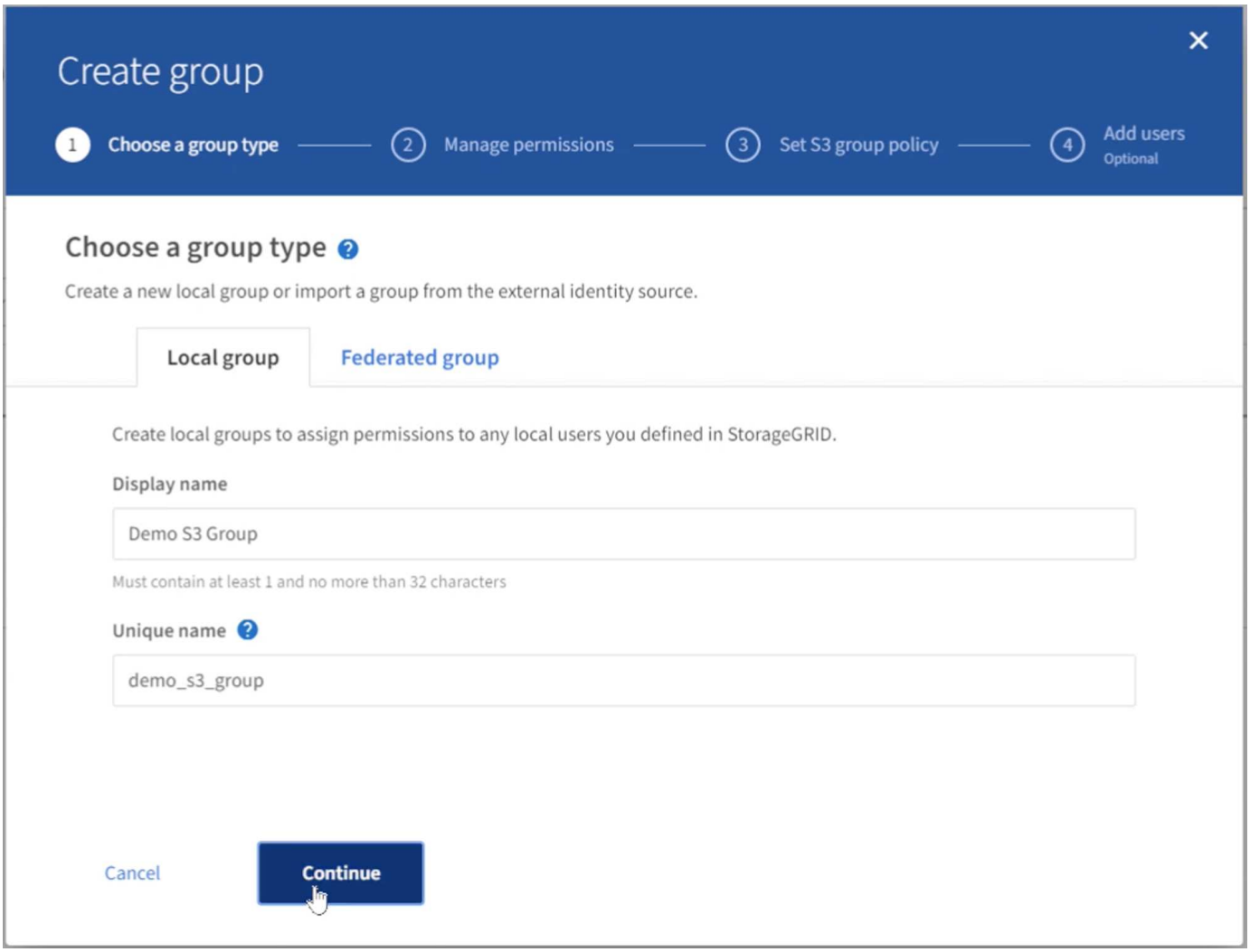


選取「存取金鑰」索引標籤、然後按一下「建立金鑰」按鈕。不需要設定到期時間。下載 S3 金鑰、因為一旦關閉視窗、就無法再次擷取這些金鑰。

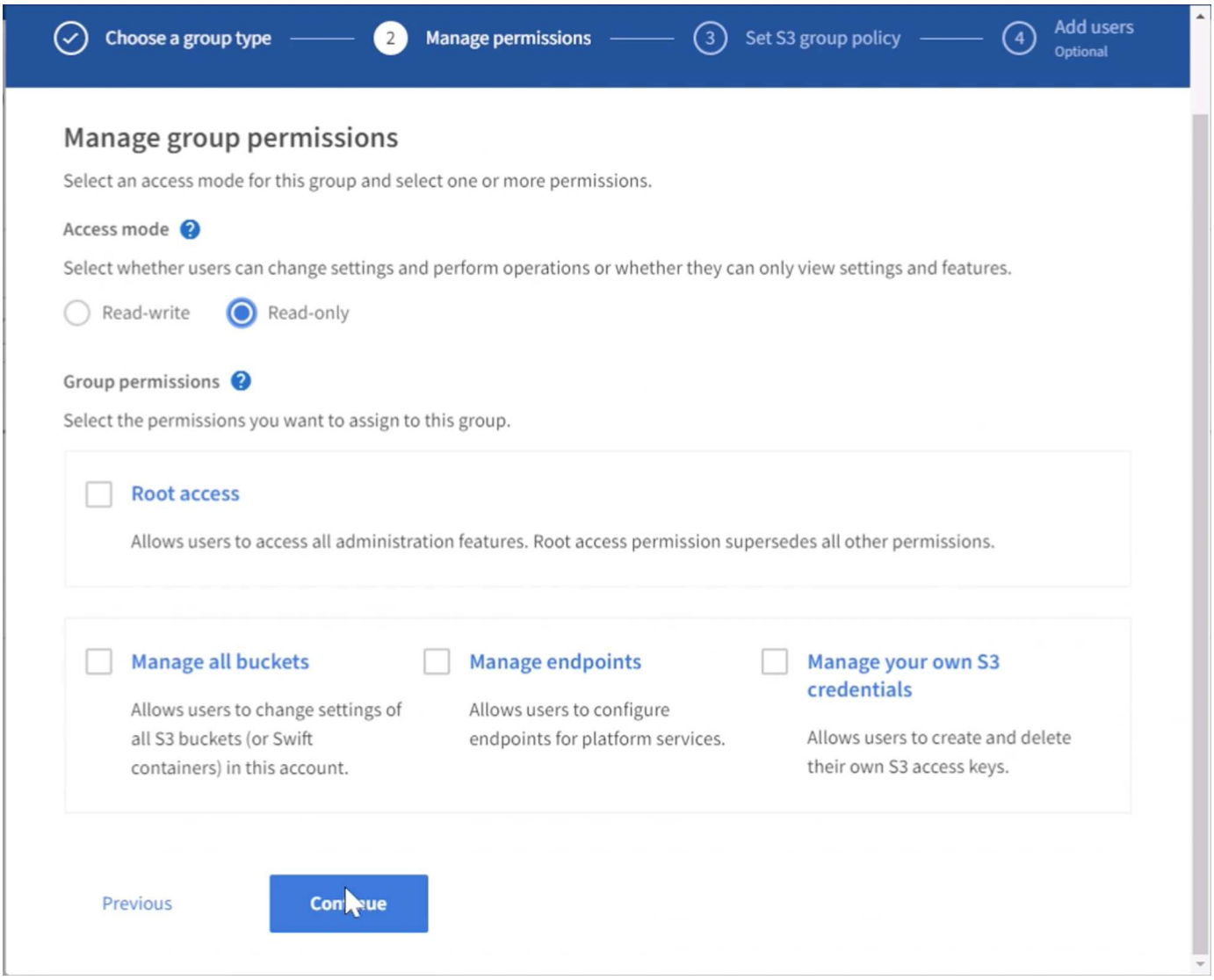


建立安全性群組

現在請移至「群組」頁面並建立新群組。

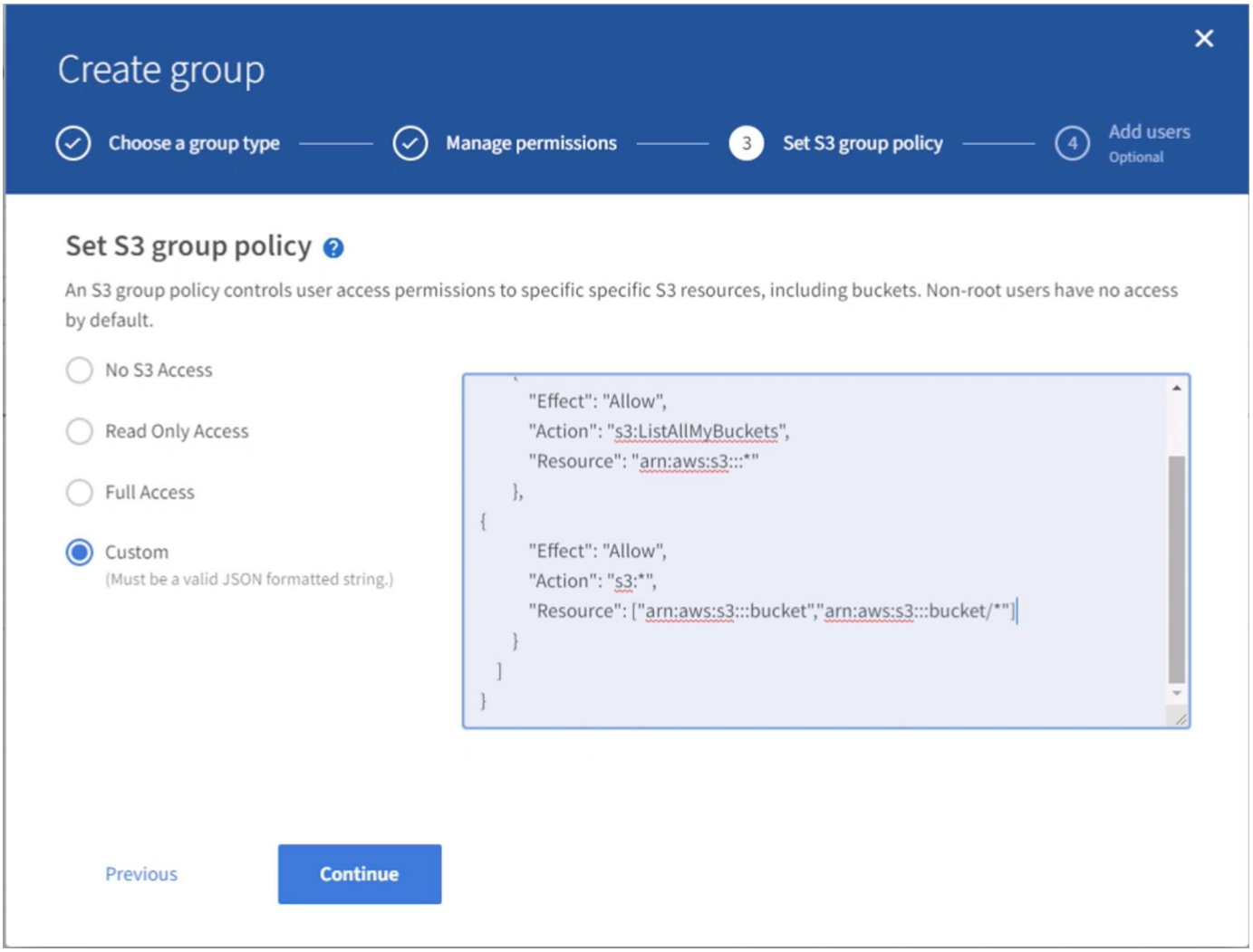


將群組權限設定為唯讀。這是租戶 UI 權限、而非 S3 權限。

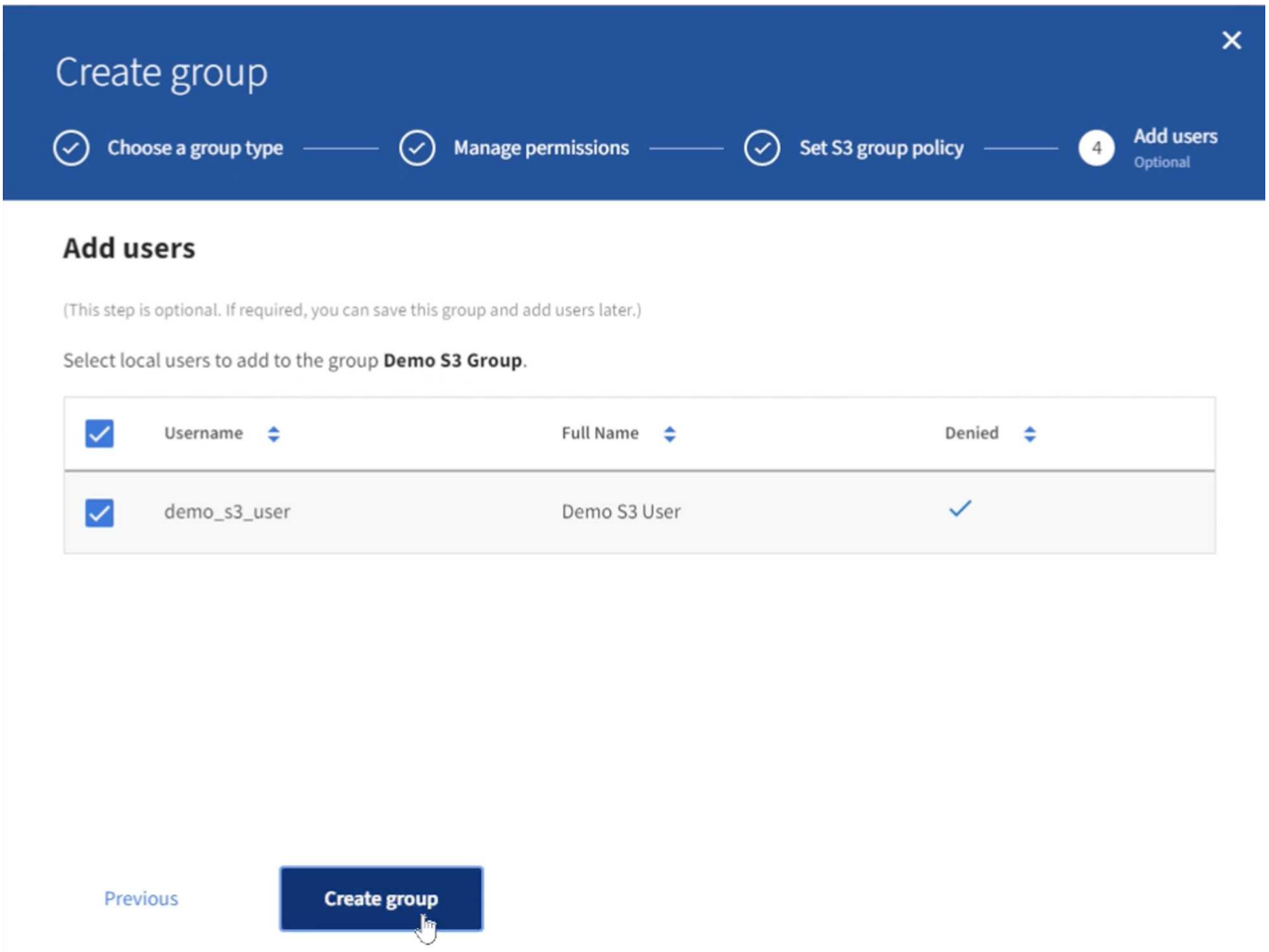


S3 權限由群組原則（ IAM 原則）控制。將群組原則設定為自訂、然後將 json 原則貼到方塊中。此原則可讓此群組的使用者列出租戶的貯體、並在名為「 Bucket 」的貯體或名為「 Bucket 」的子資料夾中執行任何 S3 作業。

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

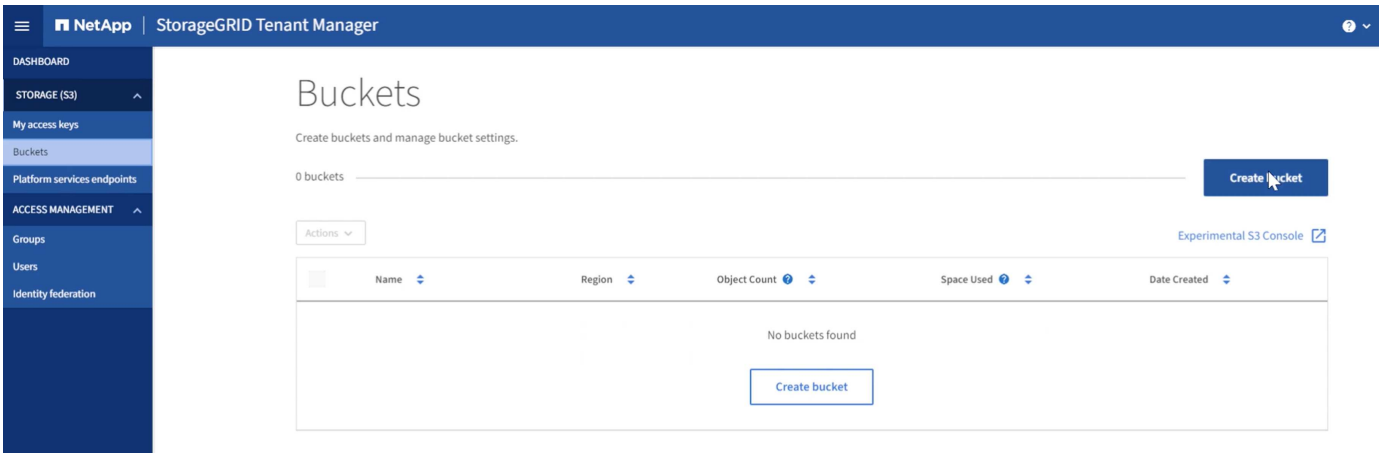


最後、將使用者新增至群組並完成。

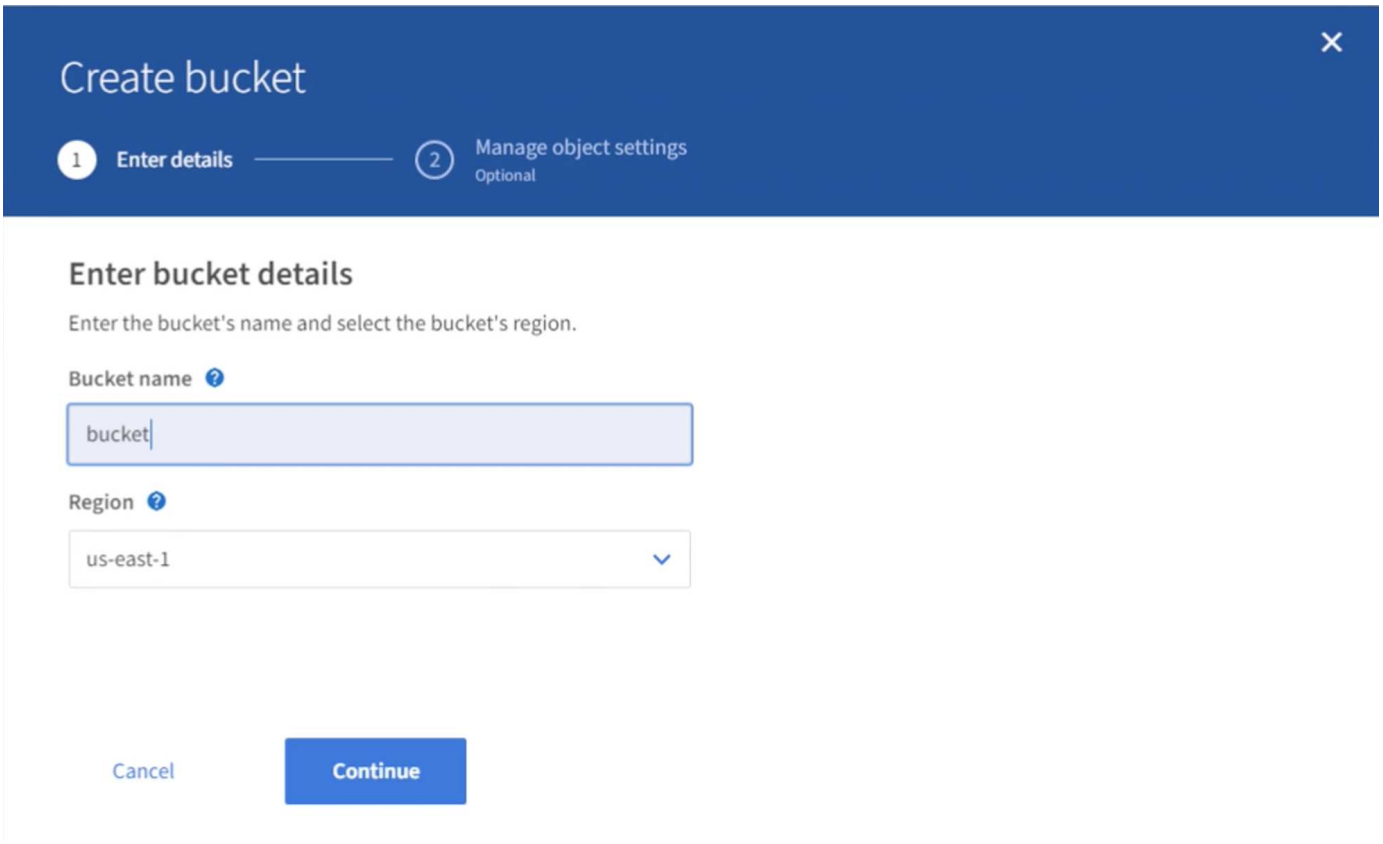


建立兩個貯體

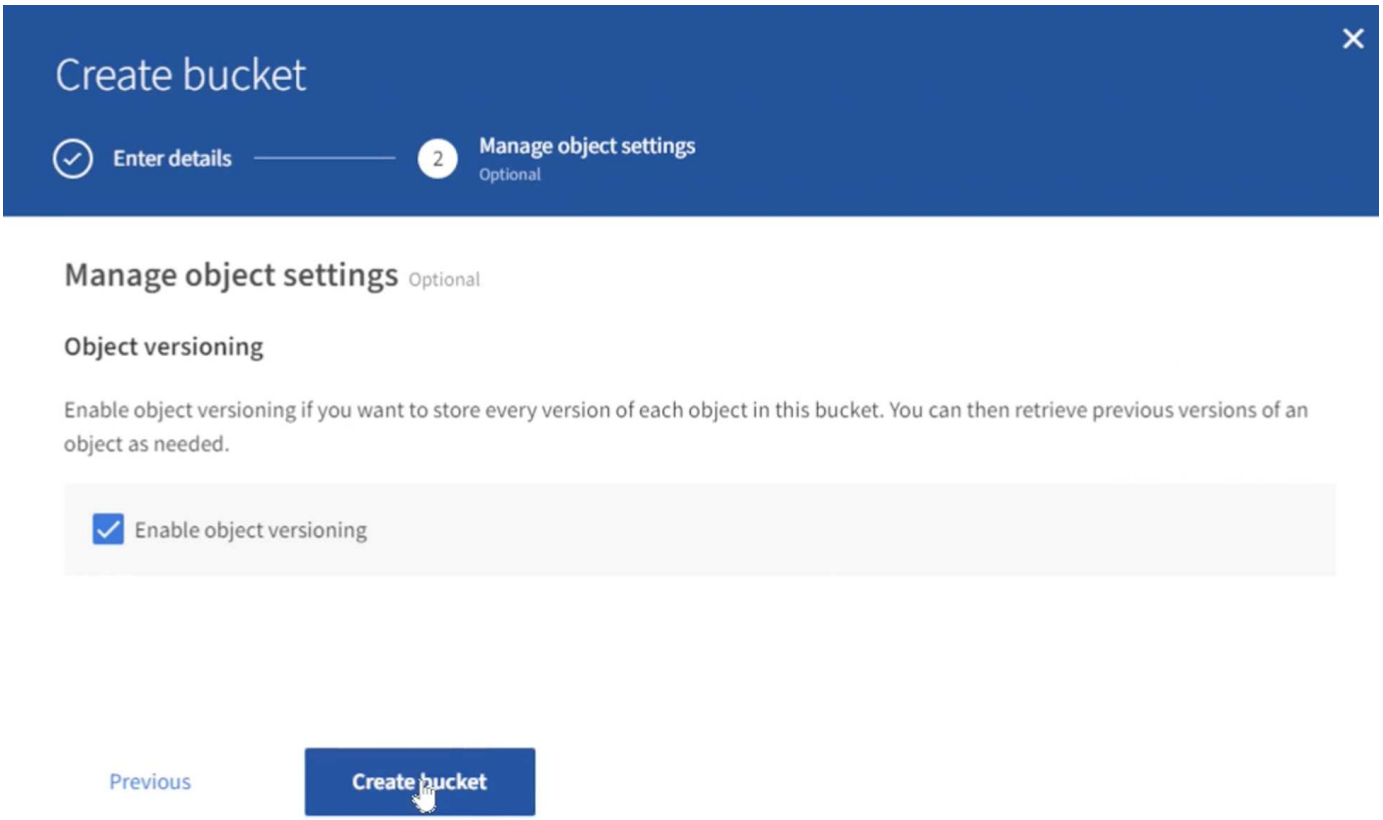
瀏覽至「貯體」標籤、然後按一下「建立貯體」按鈕。



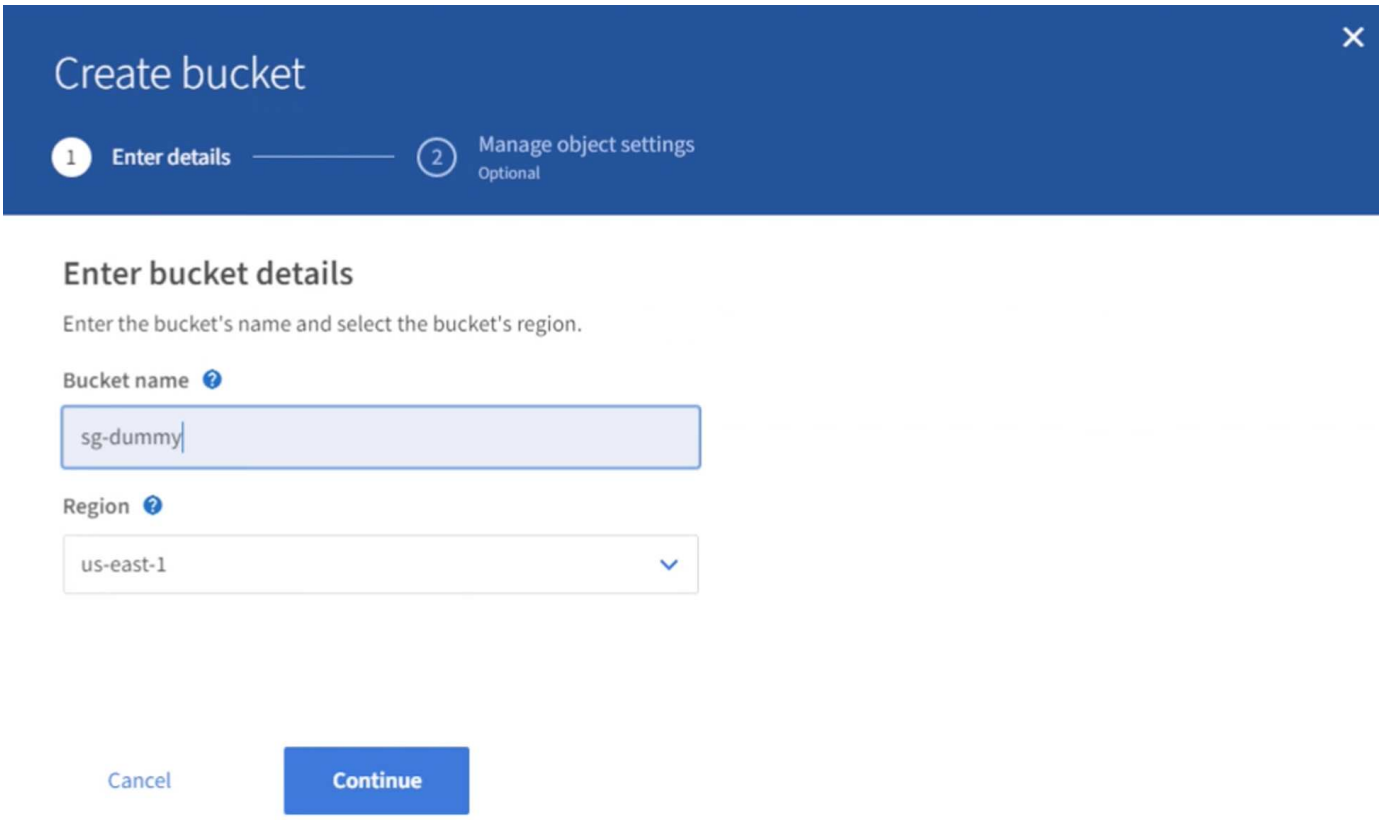
定義貯體名稱和區域。



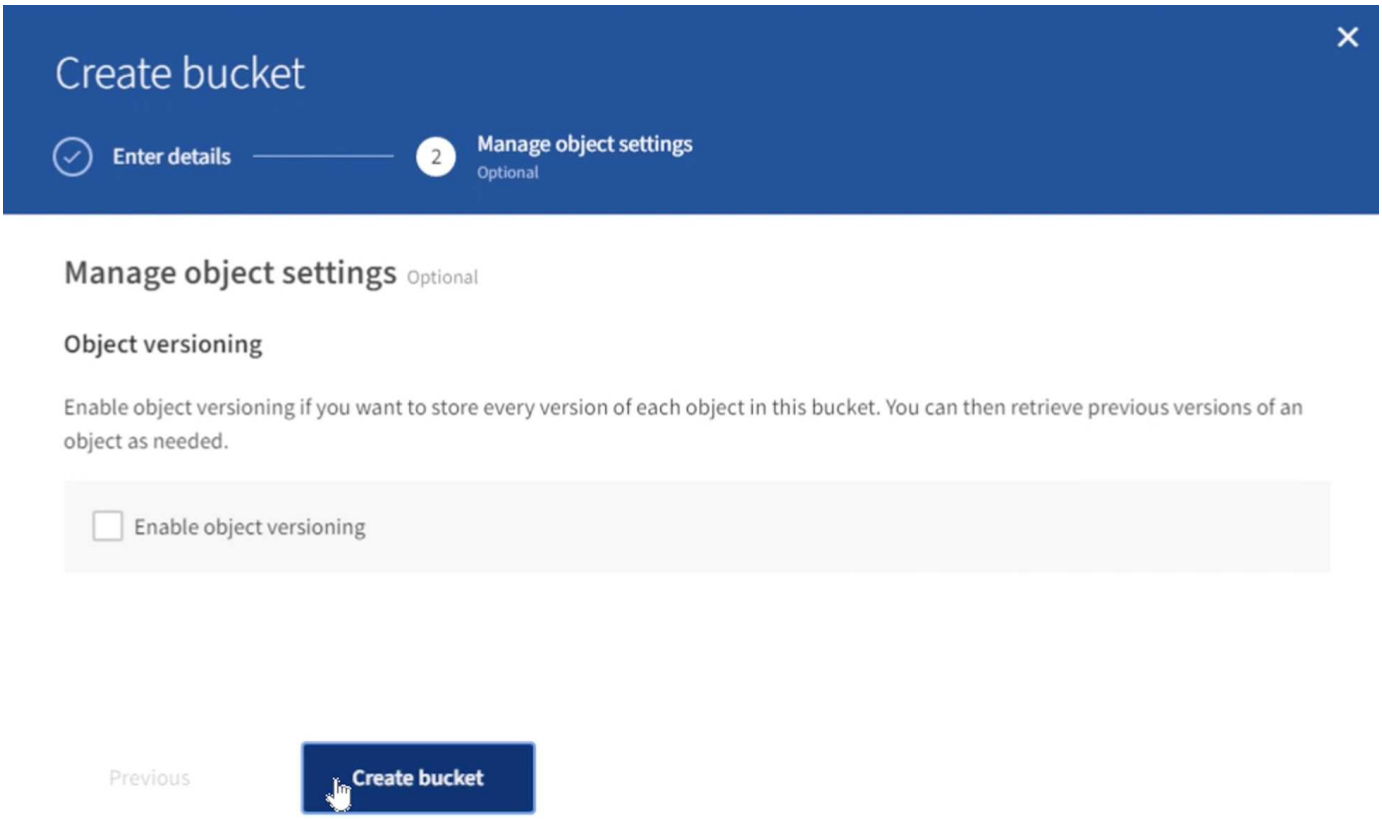
在此第一個儲存庫上啟用版本設定。



現在建立第二個儲存區、但未啟用版本設定功能。



請勿在此第二個儲存區上啟用版本設定。



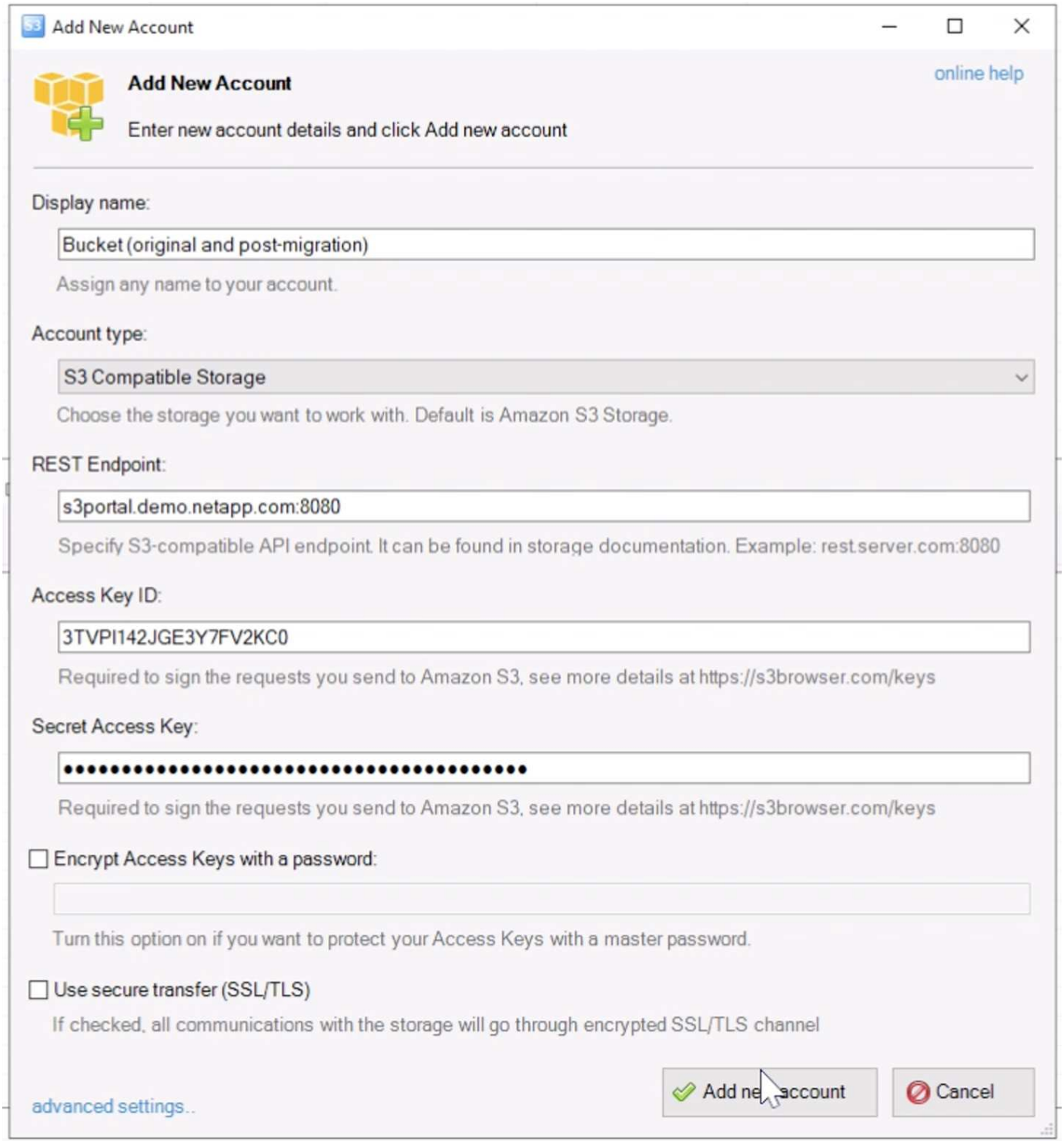
_ 作者： Rafael Guedes 和 Aron Klein_

透過將物件型儲存設備從 ONTAP S3 順暢移轉至 StorageGRID 、實現企業級 S3

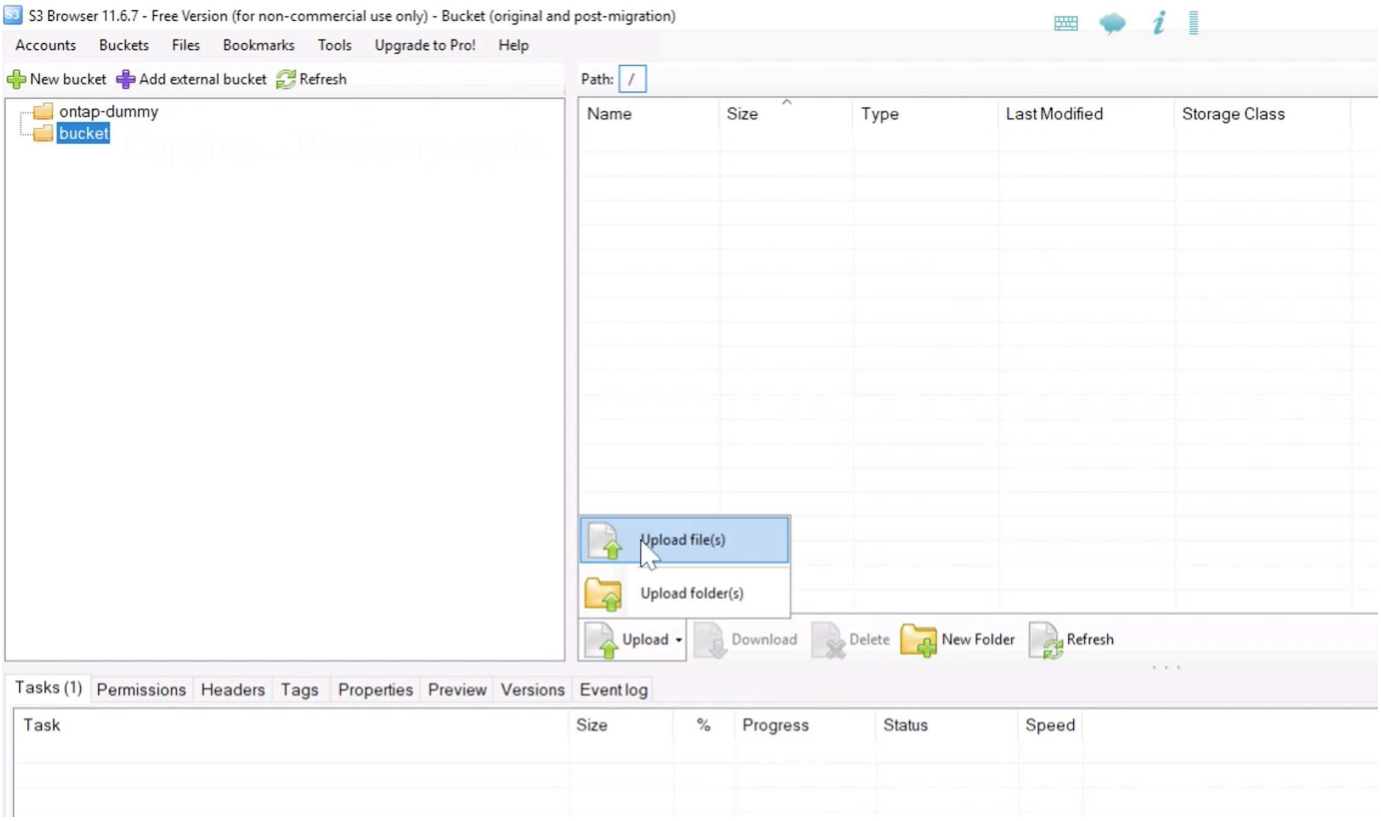
填入來源 **Bucket**

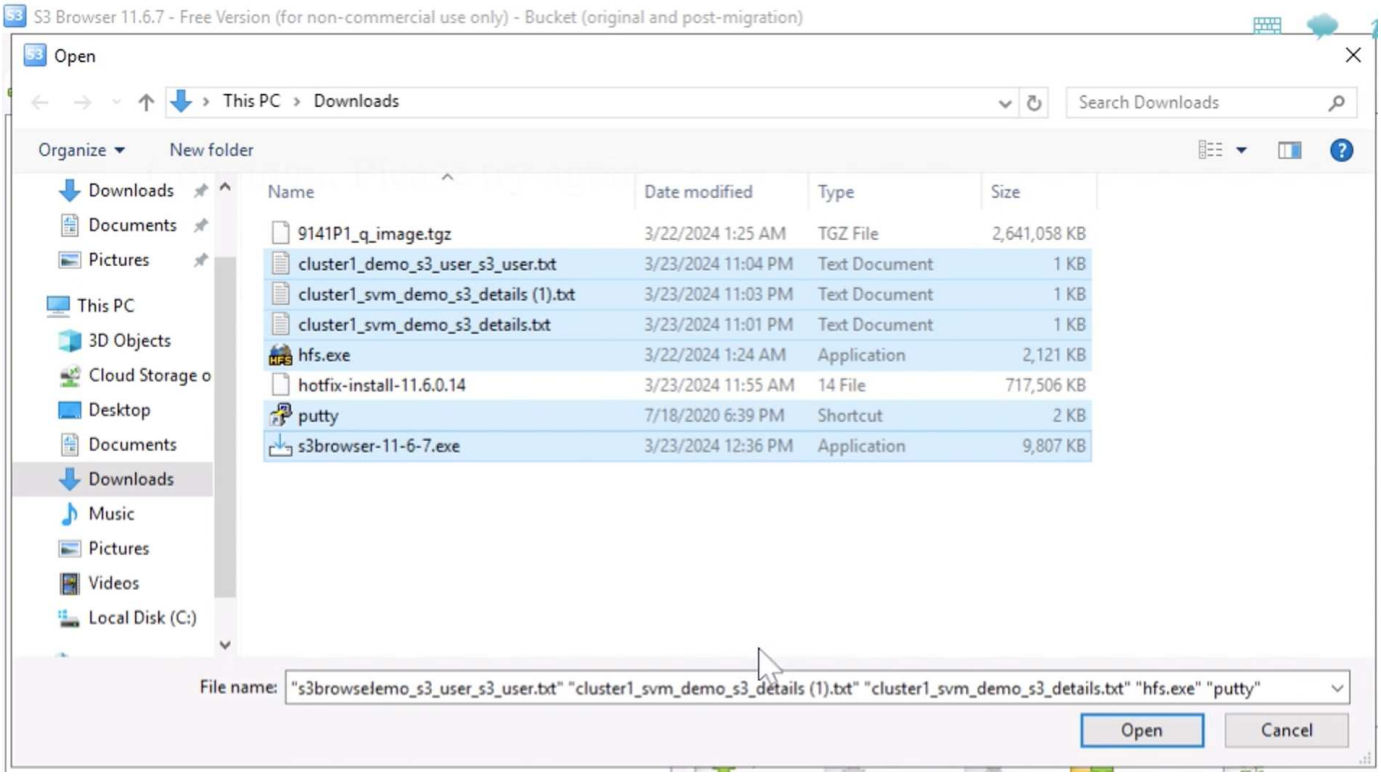
讓我們將一些物件放入來源 ONTAP 貯體中。我們將使用 S3 瀏覽器進行此示範、但您可以使用任何您熟悉的工具。

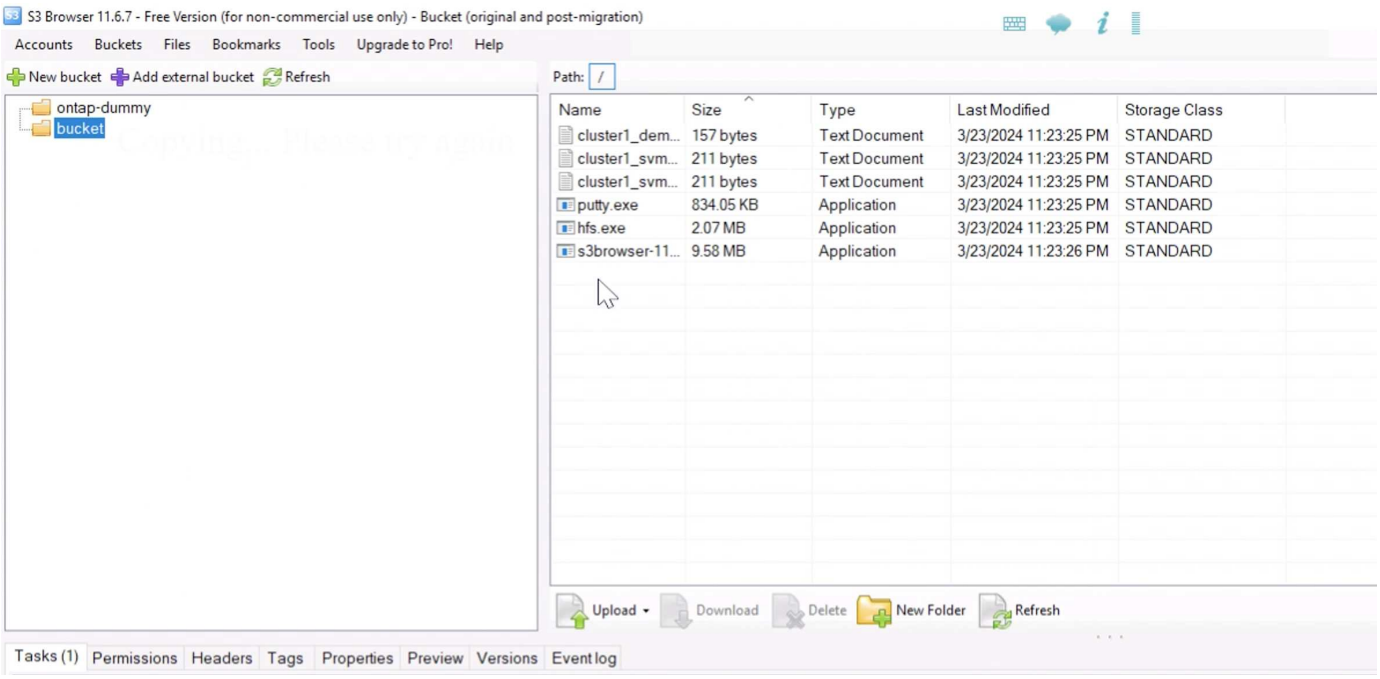
使用上述建立的 ONTAP 使用者 S3 金鑰、將 S3 瀏覽器設定為連線至 ONTAP 系統。



現在讓我們將一些檔案上傳至啟用版本控制的儲存庫。

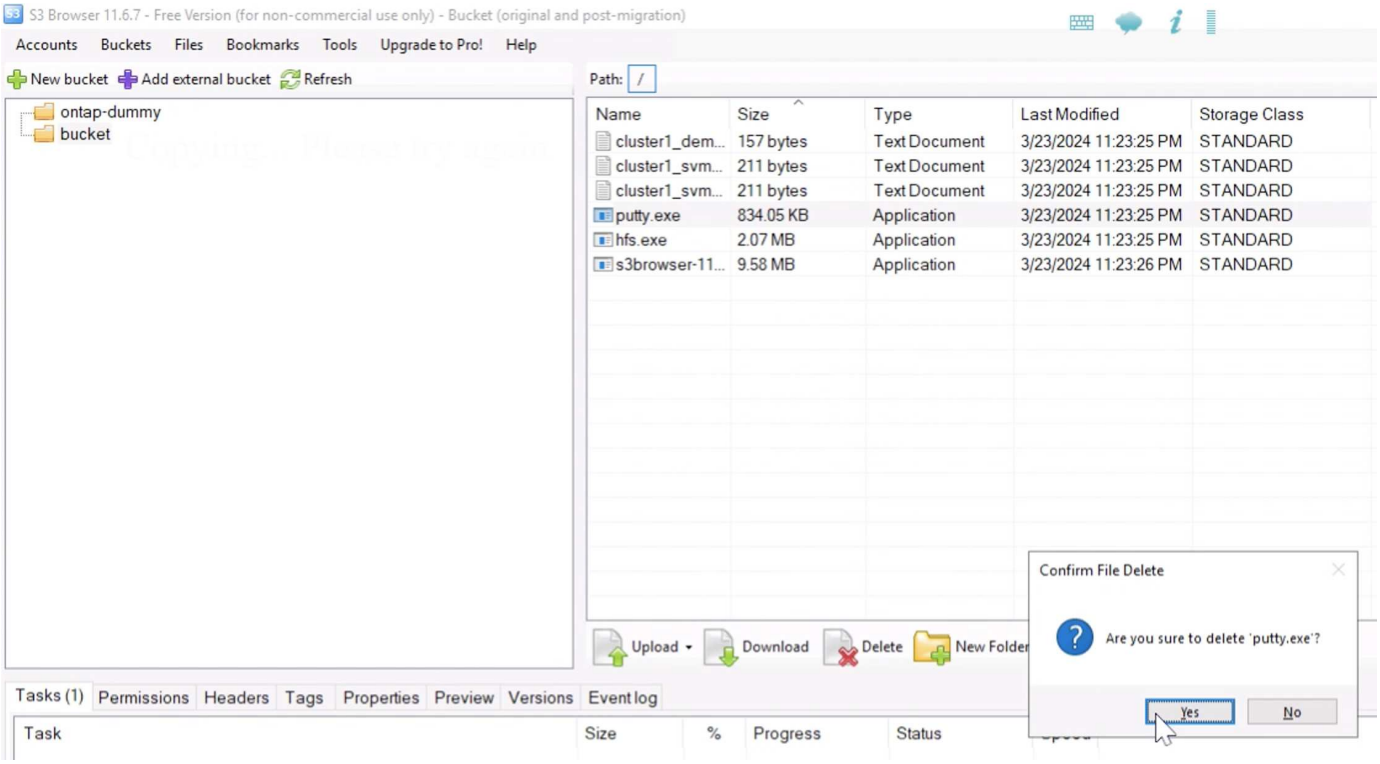




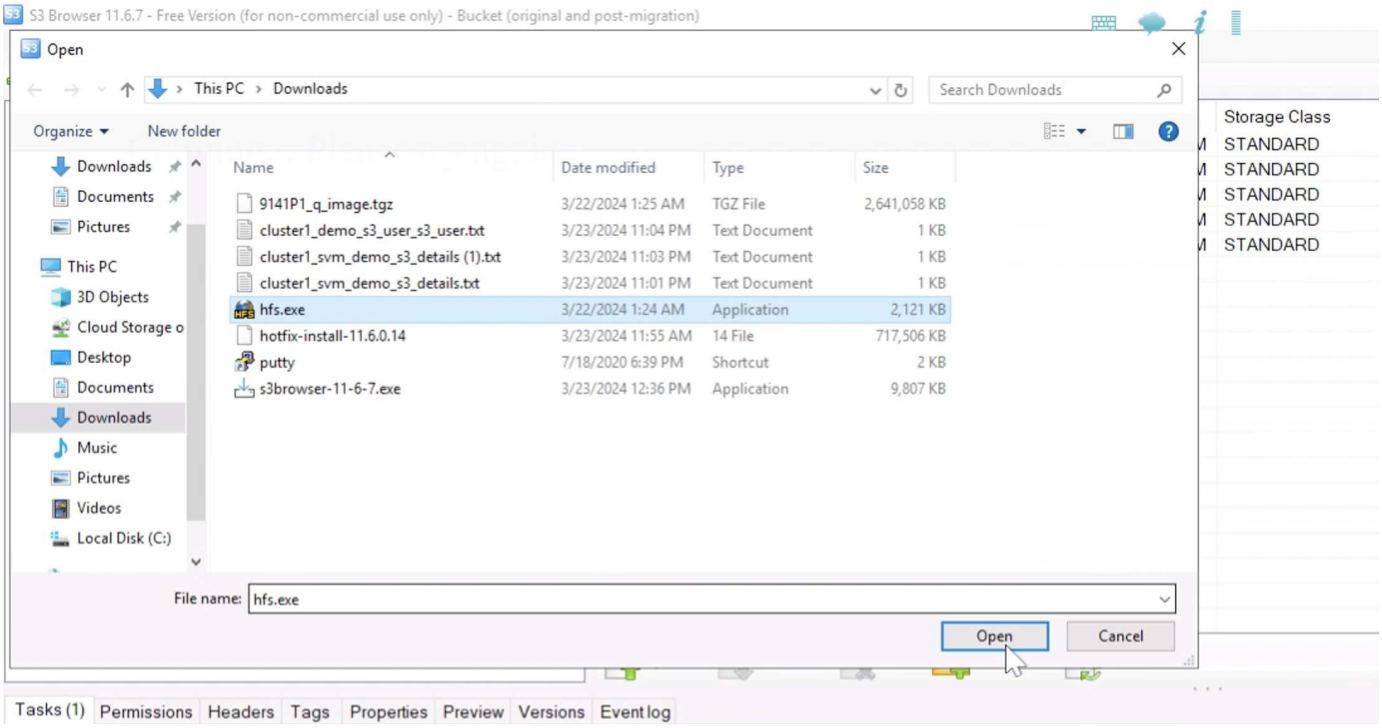


現在讓我們在貯體中建立一些物件版本。

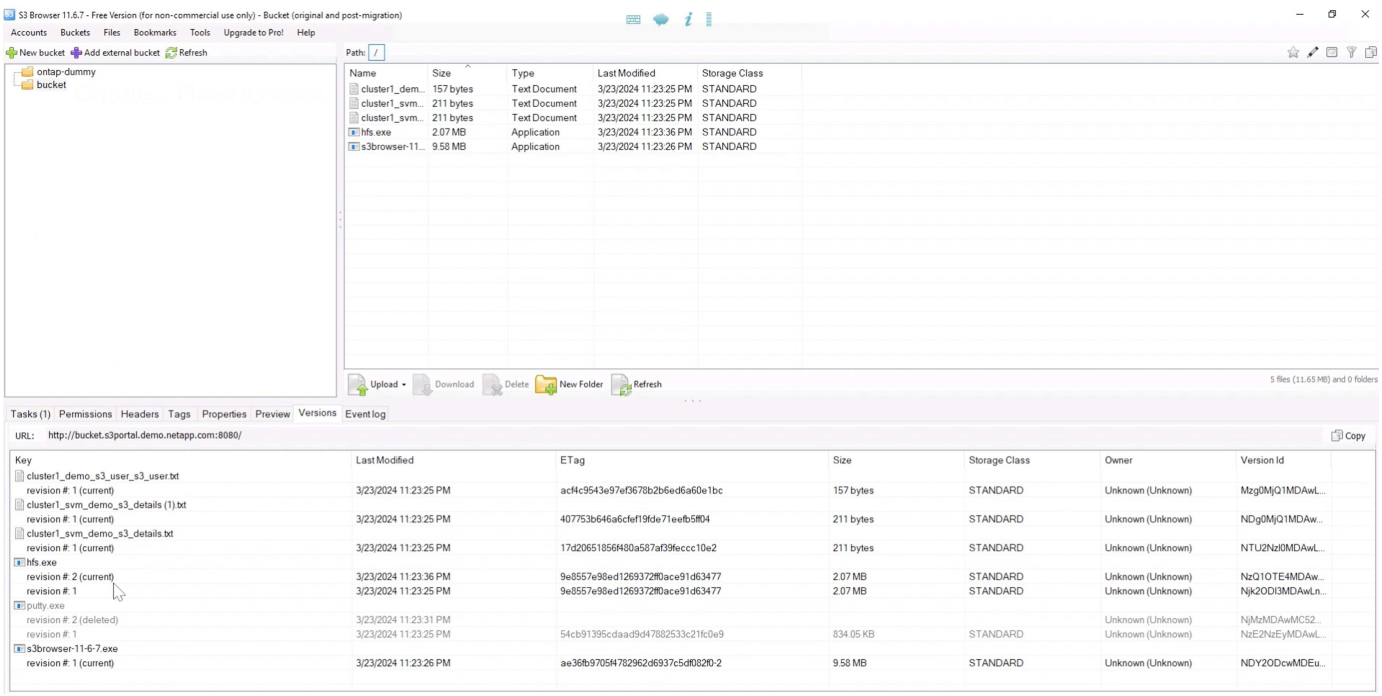
刪除檔案。



上傳已存在於貯體中的檔案、將檔案複製到其本身、然後建立新版本。



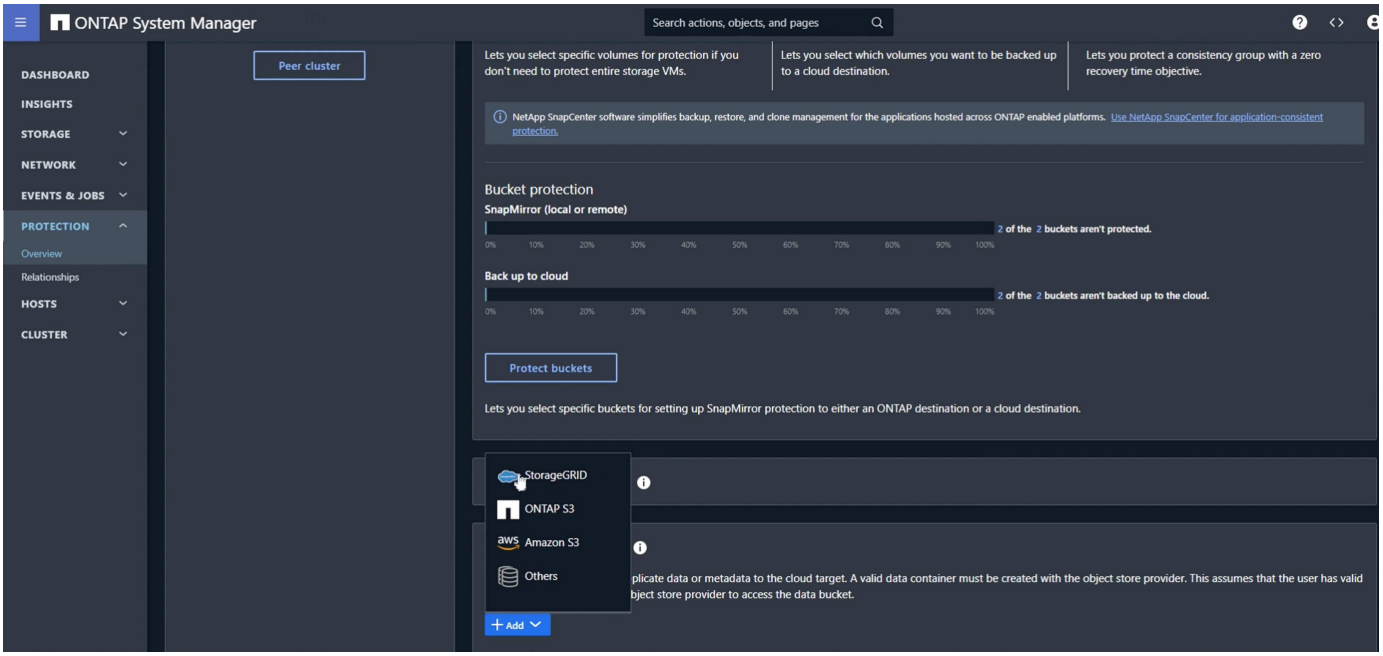
在 S3 瀏覽器中、我們可以檢視剛建立的物件版本。



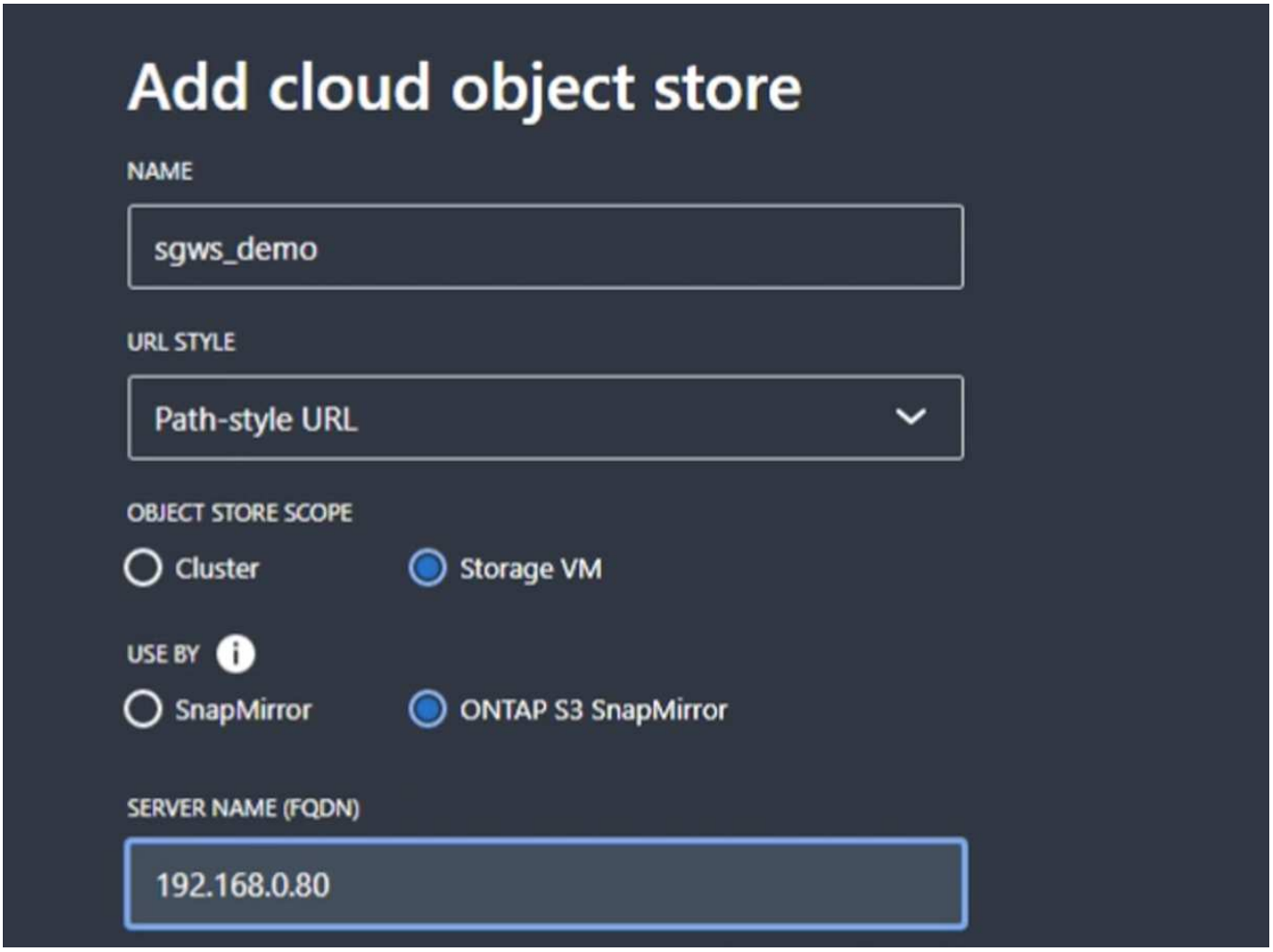
建立複寫關係

讓我們開始將資料從 ONTAP 傳送至 StorageGRID 。

在 ONTAP 系統管理員中、瀏覽至「保護 / 概述」。向下捲動至「雲端物件儲存區」、然後按一下「新增」按鈕並選取「 StorageGRID 」。



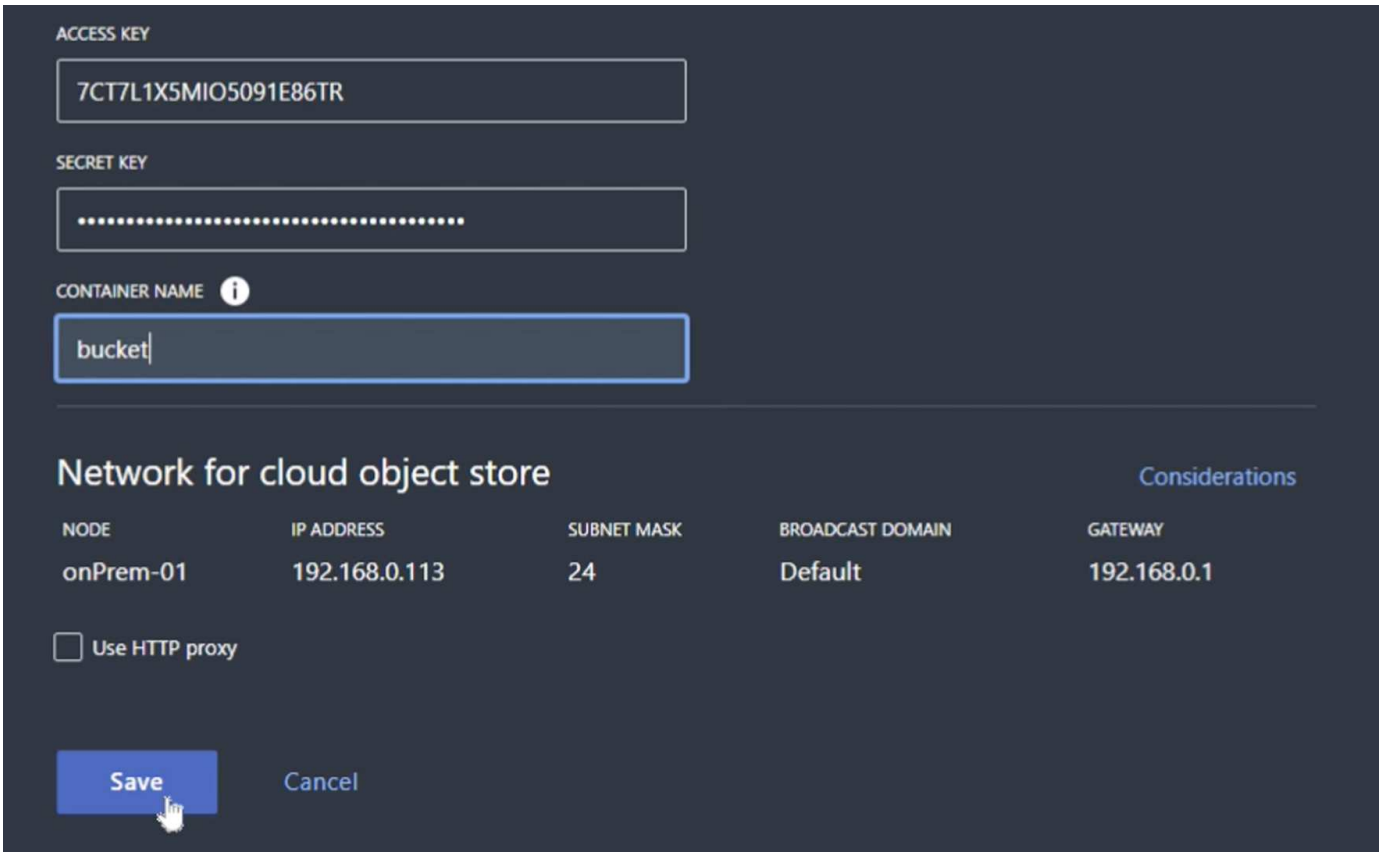
提供名稱和 URL 樣式來輸入 StorageGRID 資訊（本示範將使用 Path-styl URL ）。將物件存放區範圍設定為「 Storage VM 」。



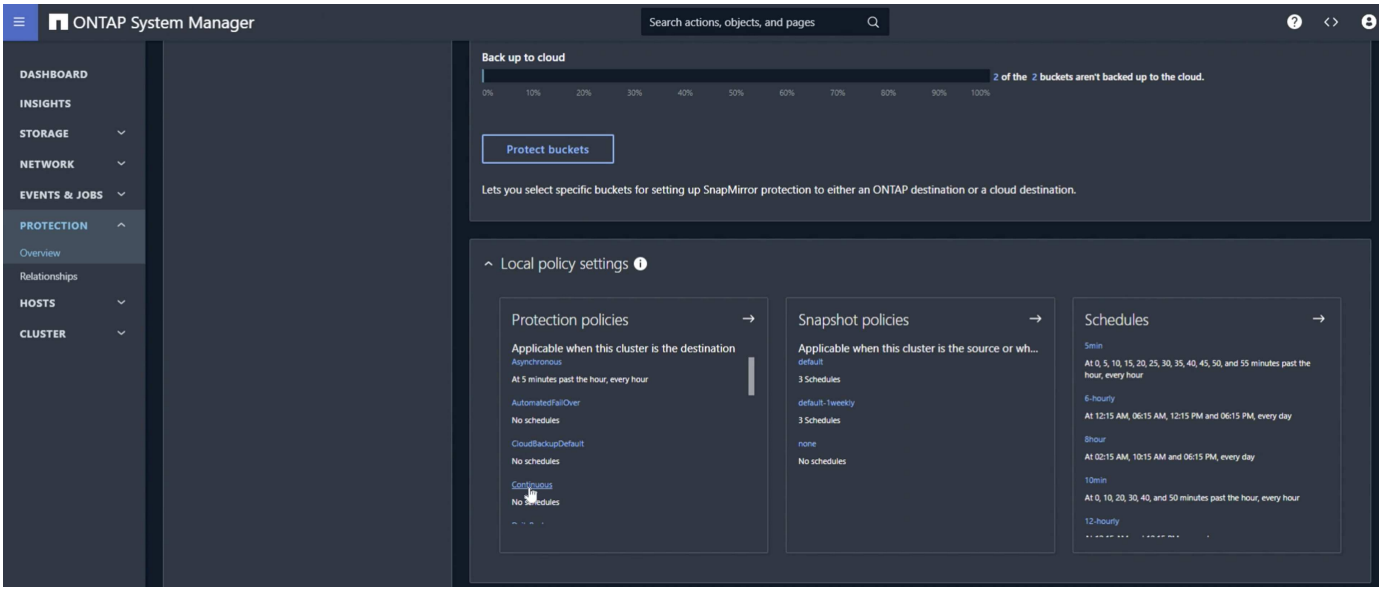
如果您使用的是 SSL 、請在此處設定負載平衡器端點連接埠、並在 StorageGRID 端點憑證中複製。否則、請取

消核取 SSL 方塊、然後在此輸入 HTTP 端點連接埠。

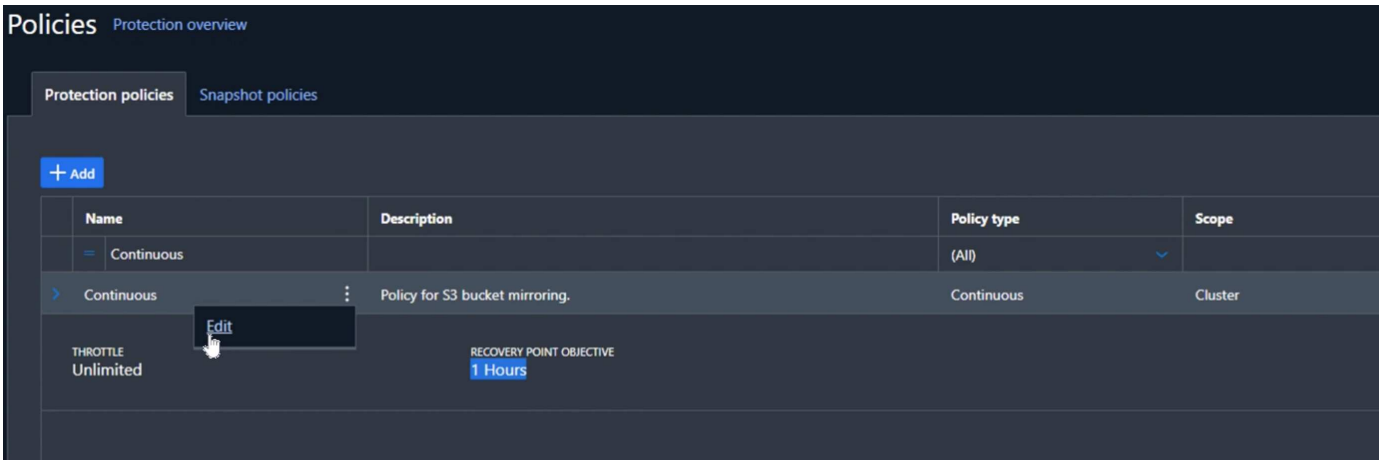
從上述目的地的 StorageGRID 組態輸入 StorageGRID 使用者 S3 金鑰和儲存格名稱。



現在已設定目的地目標、我們可以設定目標的原則設定。展開「本機原則設定」、然後選取「持續」。

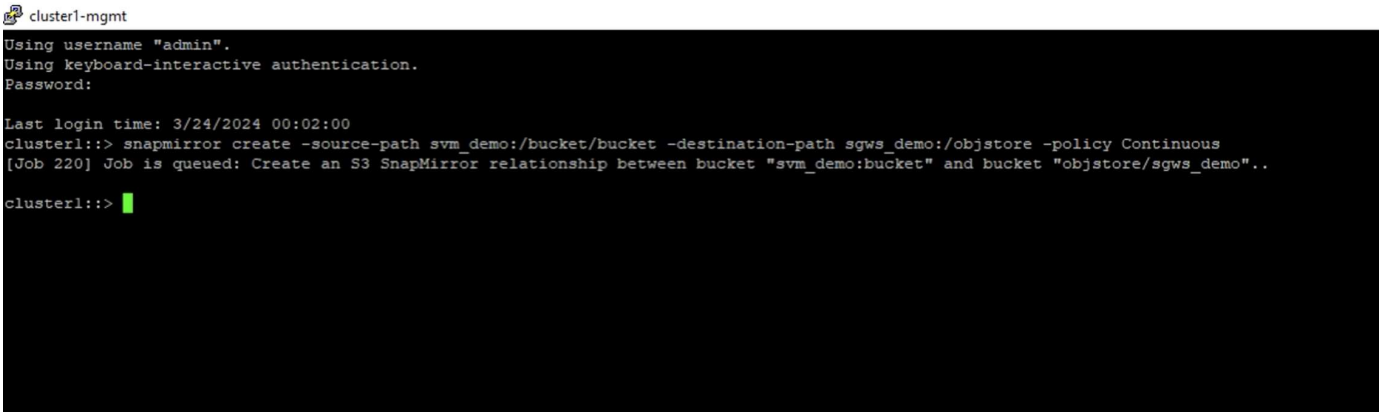


編輯持續原則、並將「恢復點目標」從「 1 小時」變更為「 3 秒」。



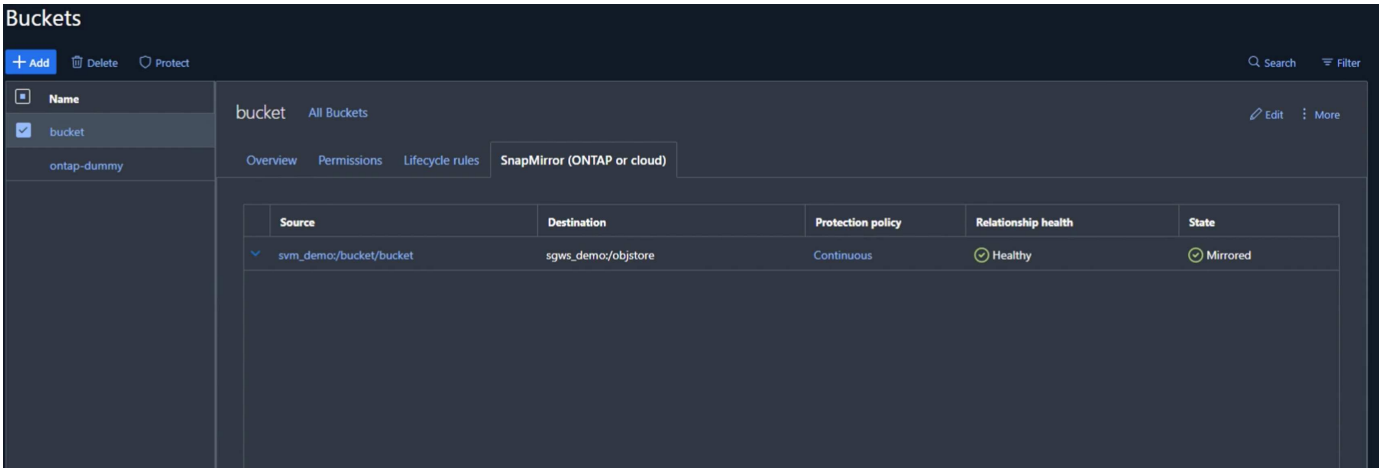
現在我們可以設定 SnapMirror 來複寫貯體。

```
SnapMirror create -source-path SV_DEMO ： /bucket/bucket - destination-path sgws_demo ： /objstore -policy Continuous
```



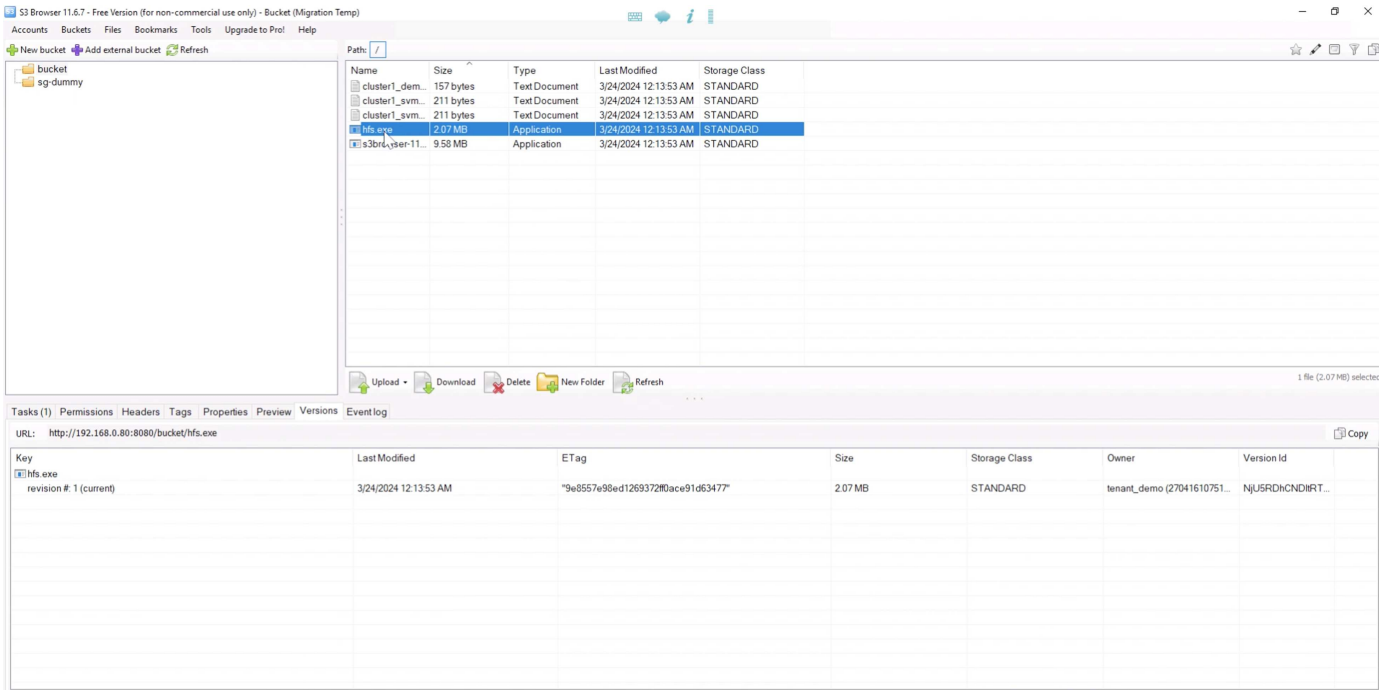
此時貯體將在保護的庫位清單中顯示雲端符號。

如果我們選取貯體並移至「 SnapMirror （ ONTAP 或雲端）」標籤、我們將會看到 SnapMirror 重新出貨狀態。

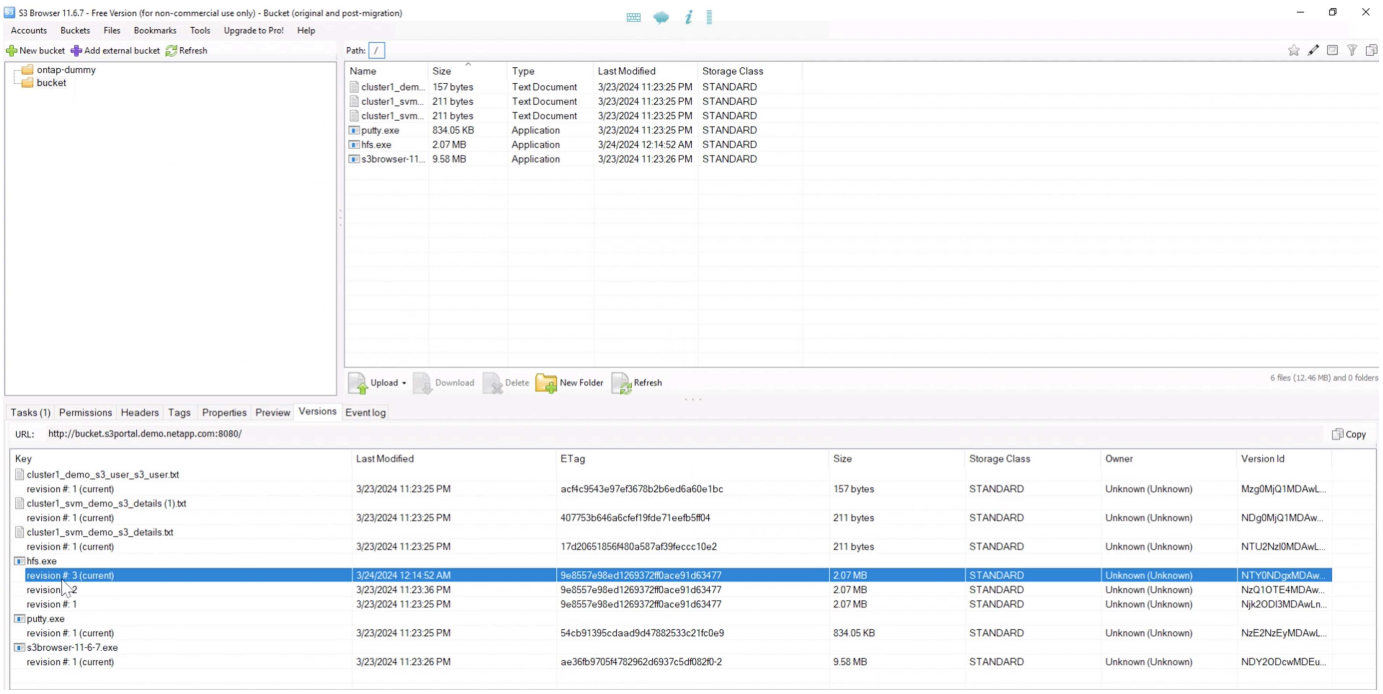


複寫詳細資料

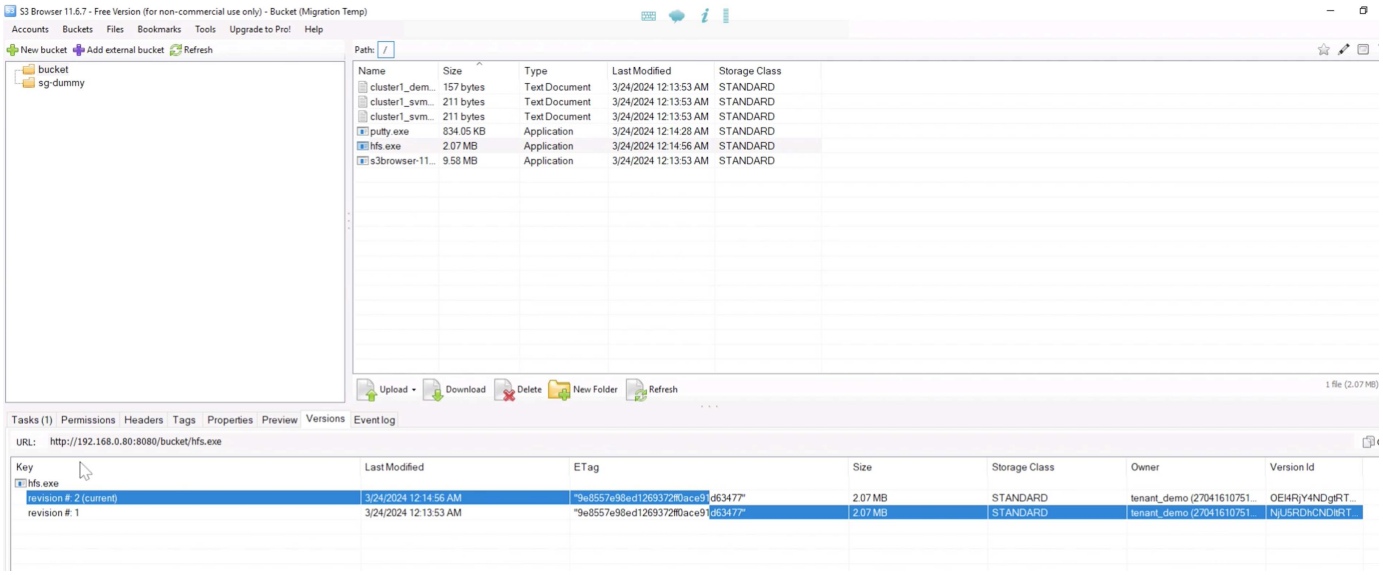
我們現在已成功將儲存庫從 ONTAP 複製到 StorageGRID 。但實際複寫的內容是什麼？我們的來源和目的地都是版本化的貯體。舊版是否也會複寫到目的地？如果我們使用 S3 瀏覽器查看 StorageGRID 儲存庫、就會發現現有版本並未複寫、而且刪除的物件不存在、也不會有該物件的刪除標記。我們複製的物件在 StorageGRID 儲存庫中只有 1 個版本。



在我們的 ONTAP 儲存庫中、讓我們將新版本新增至先前使用的相同物件、並瞭解其複寫方式。



如果我們看 StorageGRID 一側、我們也看到這個儲存庫中也建立了新版本、但在 SnapMirror 關係之前、卻缺少初始版本。



這是因為 ONTAP SnapMirror S3 程序只會複寫物件的目前版本。因此我們在 StorageGRID 端建立了一個版本化的貯體、以做為目的地。這樣 StorageGRID 就能維護物件的版本歷程記錄。

_ 作者： Rafael Guedes 和 Aron Klein_

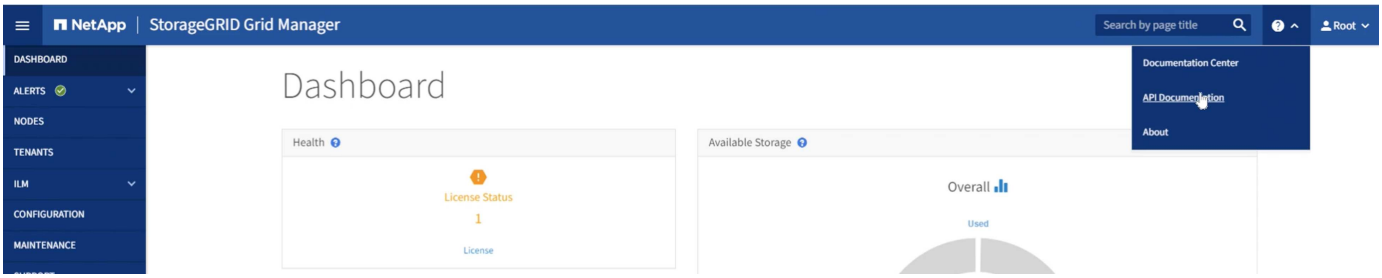
透過將物件型儲存設備從 **ONTAP S3** 順暢移轉至 **StorageGRID** 、實現企業級 **S3**

透過將物件型儲存設備從 ONTAP S3 順暢移轉至 StorageGRID 、實現企業級 S3

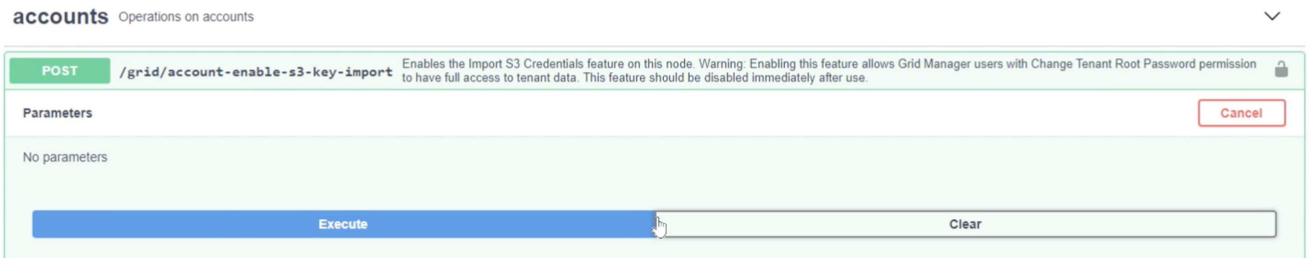
移轉 **S3** 金鑰

對於移轉、大部分時間您都想要移轉使用者的認證、而不是在目的地端產生新的認證。StorageGRID 提供 API 、可將 S3 金鑰匯入使用者。

登入 StorageGRID 管理 UI （而非租戶管理員 UI ）、開啟「 API 文件」瀏覽器頁面。

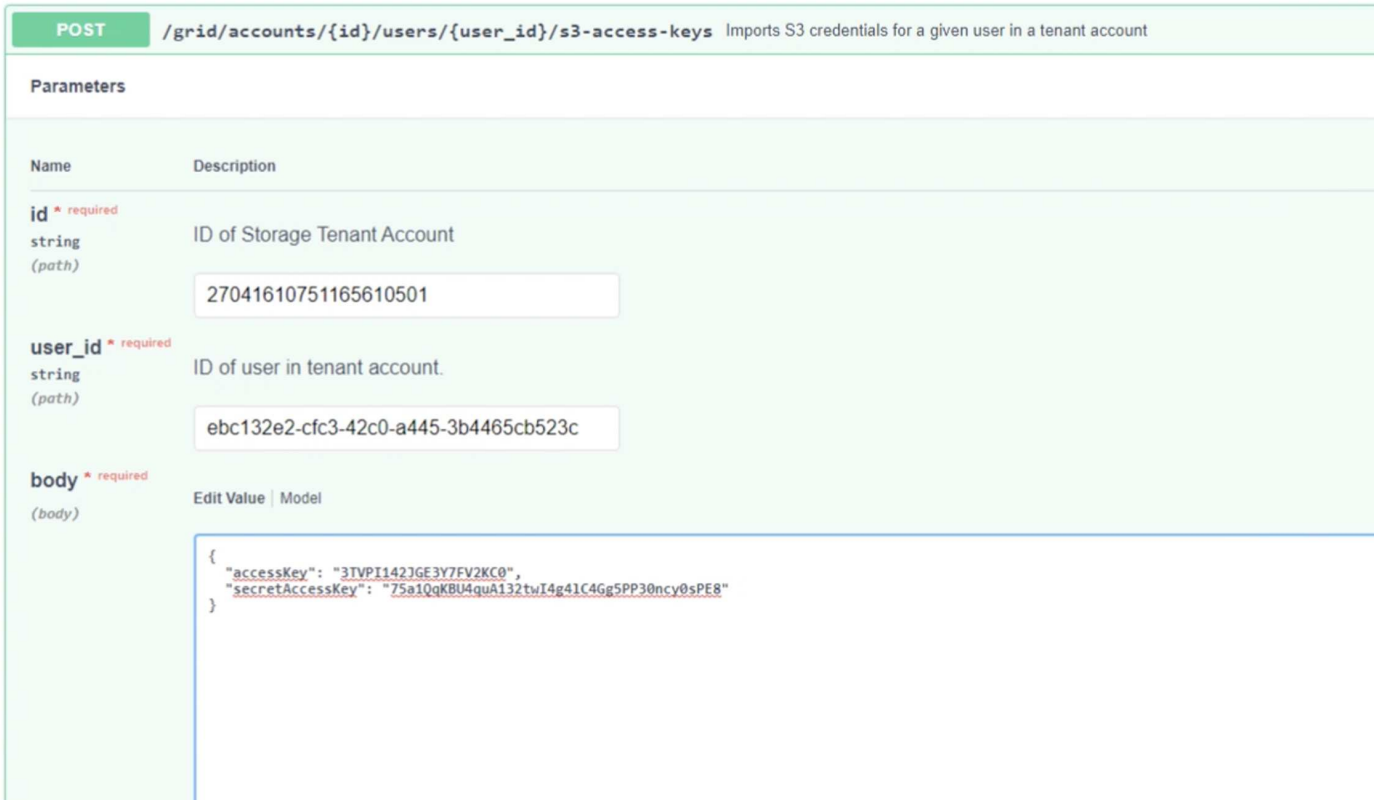


展開「帳戶」區段、選取「 POST /GRI/account-enable — s3-key-import 」、按一下「 Try it out 」（試用）按鈕、然後按一下「 execute 」（執行）按鈕。

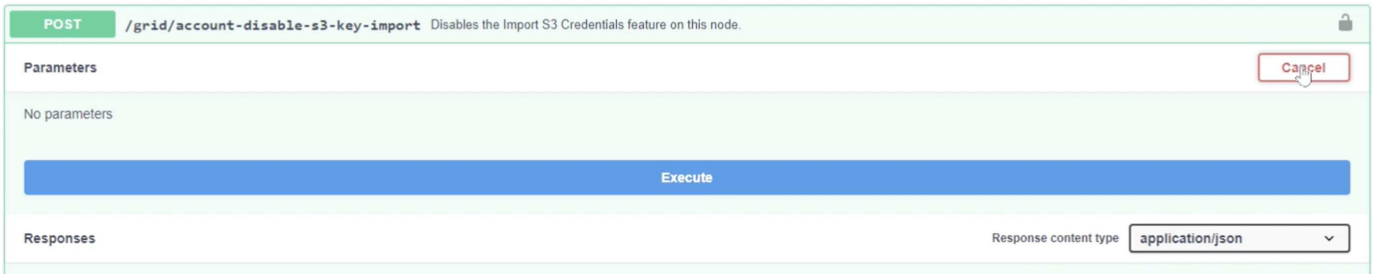


現在請在「帳戶」下方向下捲動至「 POST /GRID/accounts/{id}/user/{user_id}/s3-access-keys 」

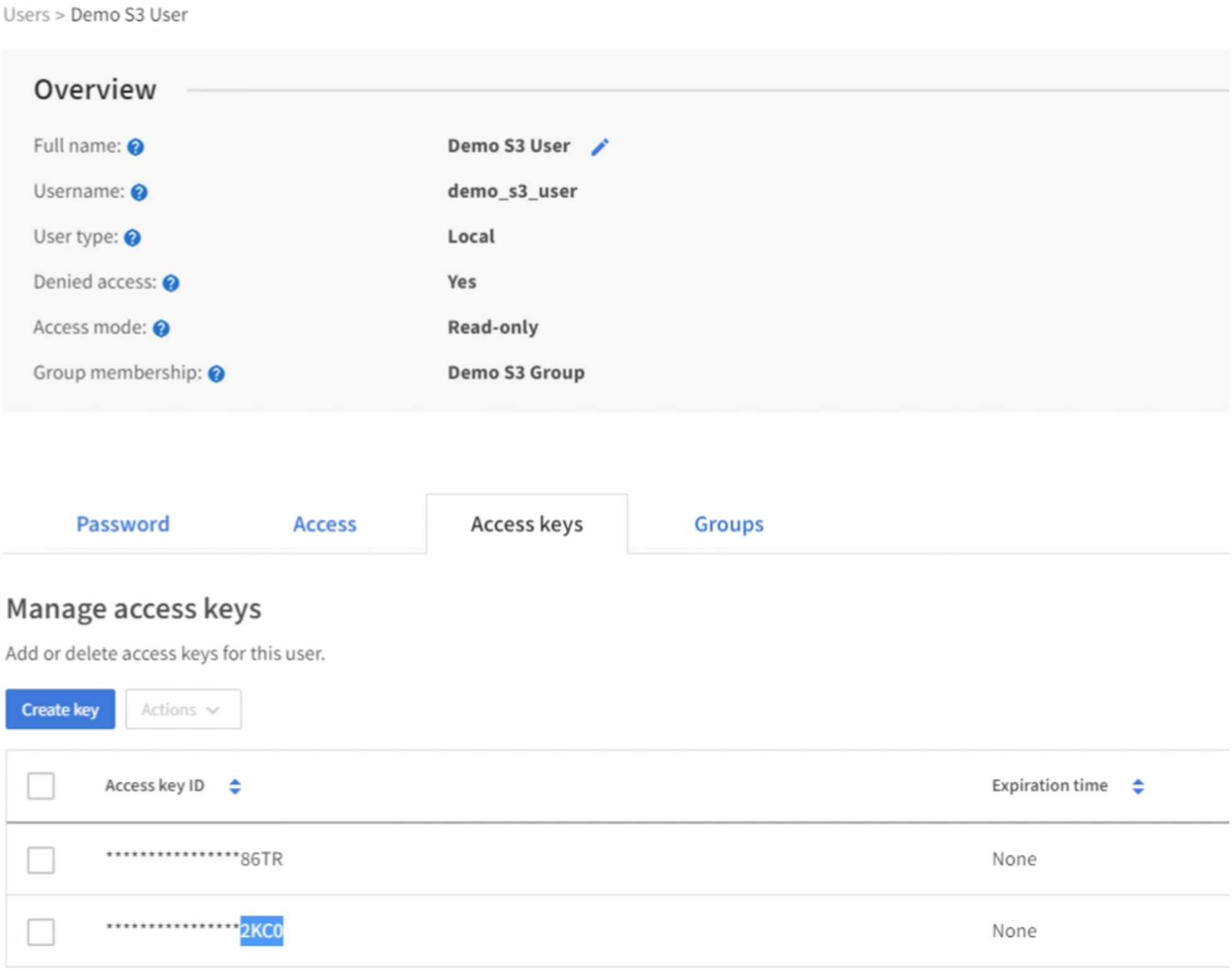
我們將在此輸入先前收集的租戶 ID 和使用者帳戶 ID 。請在 json 方塊中填入 ONTAP 使用者的欄位和金鑰。您可以設定金鑰到期日、或移除「、「 Expires 」（到期日）： 123456789 、然後按一下「 execute （執行）」。



完成所有使用者金鑰匯入後、您應該停用「帳戶」「 POST /GRI/account-disable-s3-key-import 」中的金鑰匯入功能



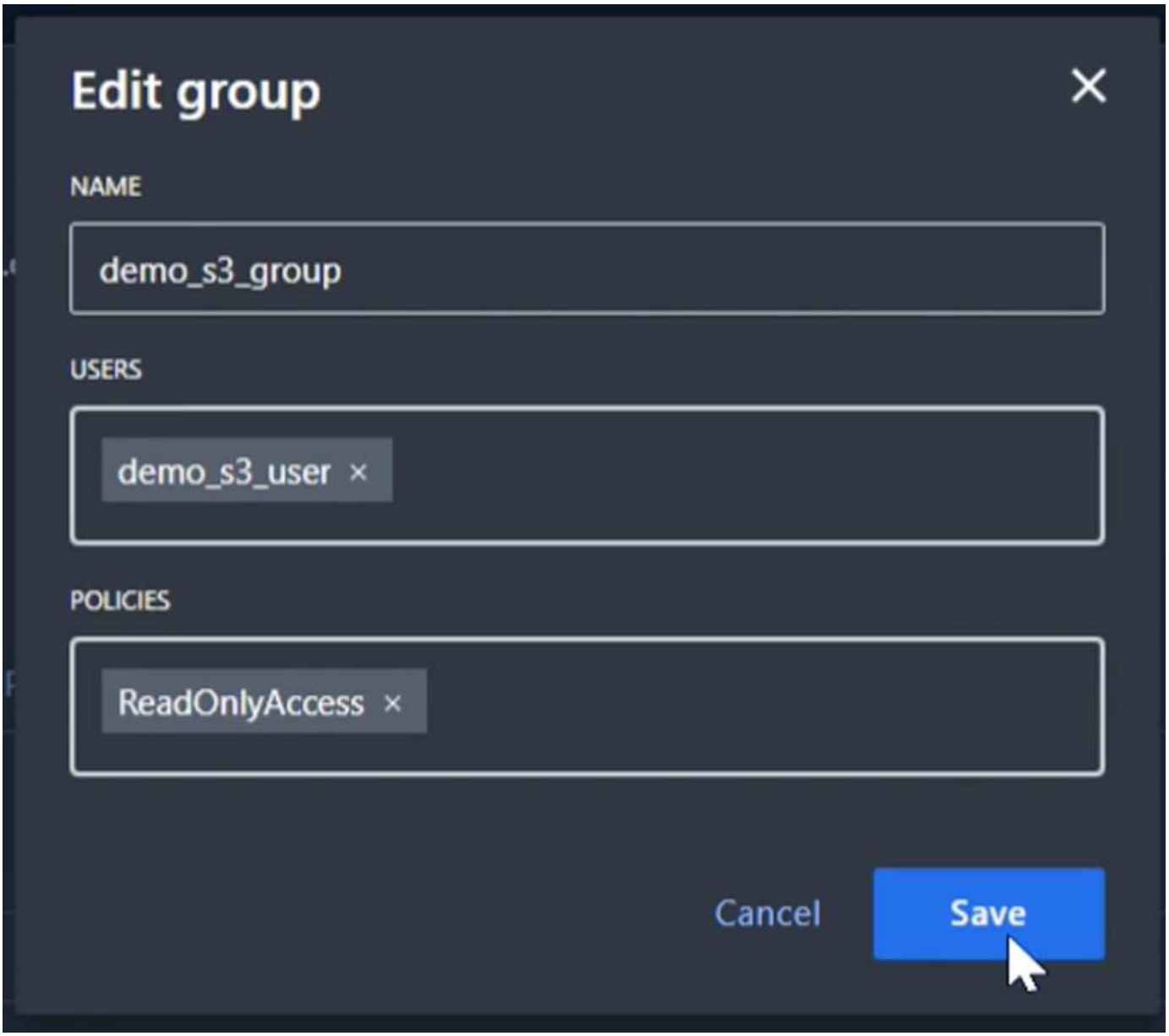
如果我們在租戶管理員 UI 中查看使用者帳戶、就會看到新金鑰已新增。



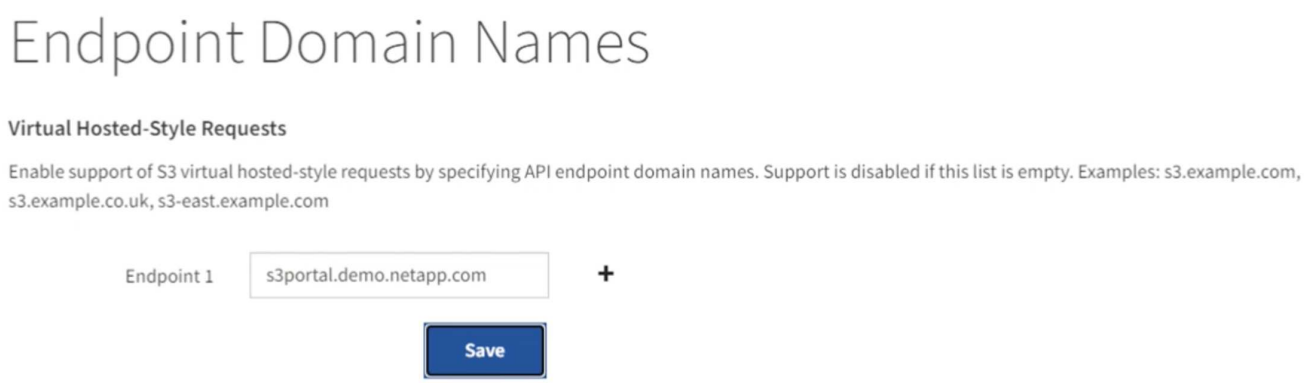
最終切換

如果打算將貯體從 ONTAP 永久複製到 StorageGRID 、您可以在此結束。如果這是從 ONTAP S3 移轉至 StorageGRID 、那麼現在正是結束移轉的好時機。

在 ONTAP 系統管理員中、編輯 S3 群組並將其設定為「 ReadOnlyAccess 」。這將防止使用者再寫入 ONTAP S3 儲存區。



剩下的只是將 DNS 設定為從 ONTAP 叢集指向 StorageGRID 端點。請確定端點憑證正確無誤、如果您需要虛擬代管樣式要求、請在 StorageGRID 中新增端點網域名稱



您的用戶端可能需要等待 TTL 過期、或是清除 DNS 以解析至新系統、以便測試一切是否正常運作。剩下的只是清理我們用來測試 StorageGRID 資料存取的初始暫存 S3 金鑰（而非匯入的金鑰）、移除 SnapMirror 關聯、以及移除 ONTAP 資料。

_ 作者： Rafael Guedes 和 Aron Klein_

工具與應用程式指南

使用Cloudera Hadoop S3連接器StorageGRID 搭配使用

_ 作者： Angela Cheng _

Hadoop 一段時間以來一直是資料科學家的最愛。Hadoop可利用簡單的程式設計架構、在多個電腦叢集之間分散處理大型資料集。Hadoop的設計可從單一伺服器擴充至數千部機器、每部機器都擁有本機運算和儲存設備。

為什麼要使用S3A來執行Hadoop工作流程？

隨著資料量隨著時間成長、使用自己的運算和儲存設備來新增機器的方法變得效率不彰。線性擴充會在有效使用資源和管理基礎架構方面帶來挑戰。

為了因應這些挑戰、Hadoop S3用戶端可針對S3物件儲存設備提供高效能I/O。運用S3A實作Hadoop工作流程、有助於將物件儲存設備當作資料儲存庫、並可將運算與儲存設備分開、進而獨立擴充運算與儲存設備。分離運算與儲存設備也能讓您將適當的資源投入運算工作、並根據資料集的大小提供容量。因此、您可以降低Hadoop工作流程的整體TCO。

設定S3A連接器以使用StorageGRID Sfor

先決條件

- 適用於Hadoop S3A連線測試的SS3端點URL、租戶S3存取金鑰及秘密金鑰。StorageGRID
- 叢集中每個主機的Cloudera叢集和root或Sudo權限、可用來安裝Java套件。

截至2022年4月為止、Java 11.0.14搭配Cloudera 7.1.7已通過StorageGRID 測試、可搭配使用不過、在新安裝時、Java版本編號可能有所不同。

安裝Java套件

1. 請檢查 "Cloudera支援對照表" 以取得支援的JDK版本。
2. 下載 "Java 11.x套件" 這與Cloudera叢集作業系統相符。將此套件複製到叢集中的每個主機。在此範例中、rpm套件用於CentOS。
3. 以root身分或使用具有Sudo權限的帳戶登入每個主機。在每個主機上執行下列步驟：
   a. 安裝套件：

      ```
      $ sudo rpm -Uvh jdk-11.0.14_linux-x64_bin.rpm
      ```

   b. 檢查Java的安裝位置。如果安裝了多個版本、請將新安裝的版本設為預設：

```
alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 +1           /usr/java/jre1.8.0_291-amd64/bin/java
  2           /usr/java/jdk-11.0.14/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

c. 將此行新增至「/etc/profile」結尾。路徑應符合上述選擇的路徑：

```
export JAVA_HOME=/usr/java/jdk-11.0.14
```

d. 執行下列命令、設定檔才會生效：

```
source /etc/profile
```

Cloudera HDFS S3組態

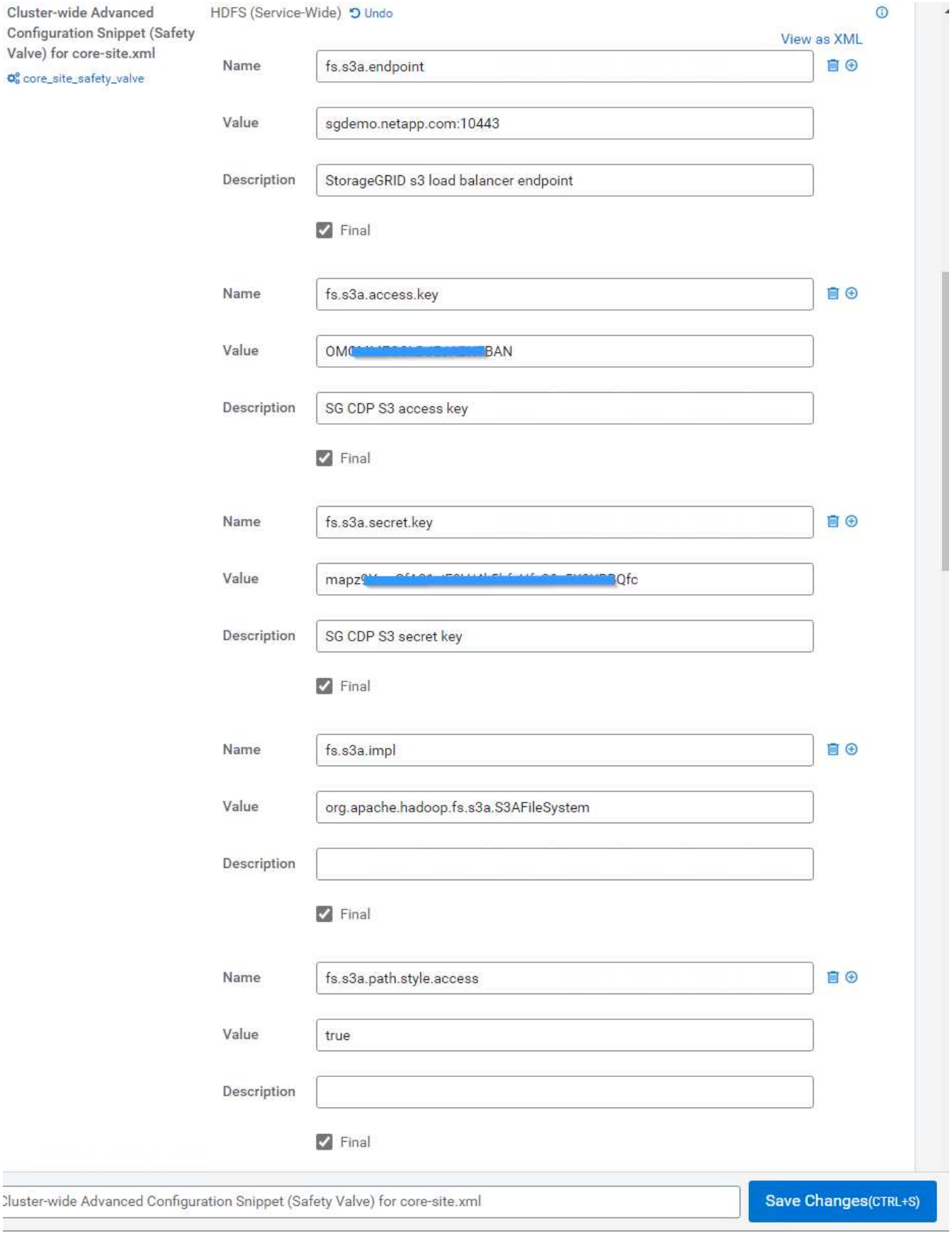
步驟

1. 從Cloudera Manager GUI中、選取叢集> HDFS、然後選取組態。
2. 在「Category（類別）」下、選取「Advanced（進階）」、然後向下捲動以找到「Cluster-wide Advanced Configuration Snsetting（安全閥）for core site.xml（叢集範圍內的進階組態片段（安全閥）
3. 按一下（+）符號、然後新增下列值配對。

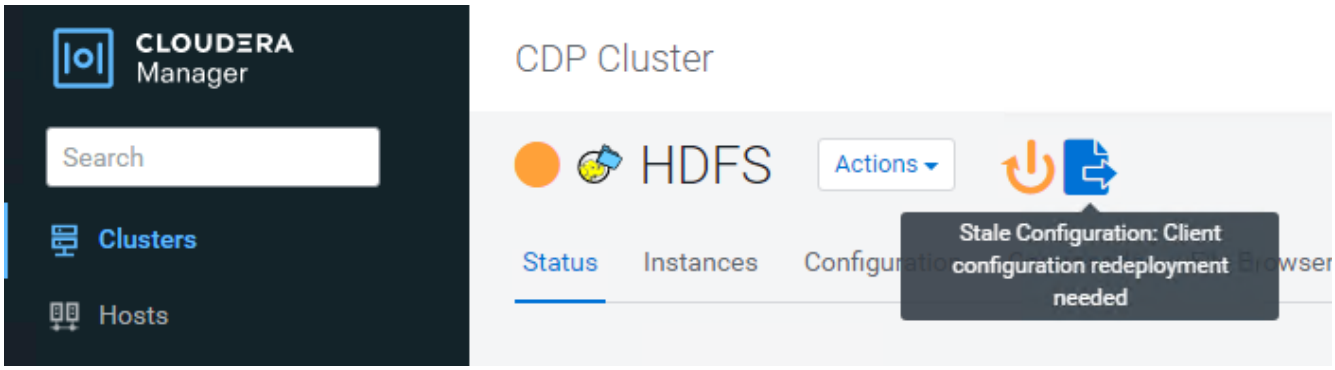
名稱	價值
fs.s3a.access.key	_<用戶S3存取金鑰、請從StorageGRID SURE>>_取得
fs.s3a.secret.key	_<租 戶S3的機密金鑰來自StorageGRID 於此
fs.s3a.connection.sse.enabled	[true或假]（如果缺少此項目、預設為https）
fs.s3a.端 點	< *StorageGRID* 支援*S3*端點：連接埠>
fs.s3a.impl	org.apache.Hadoop。fs.s3a.S3AFileSystem

名稱	價值
fs.s3a.path.樣式.access	[true或假]（如果缺少此項目、預設為虛擬主機樣式）

範例擷取畫面



4. 按一下「儲存變更」按鈕。從HDFS功能表列選取過時組態圖示、在下一頁選取重新啟動過時的服務、然後選取立即重新啟動。



測試S3A與StorageGRID Sfe的連線

執行基本連線測試

登入Cloudera叢集中的其中一部主機、然後輸入「Hadoop FS -ls s3a：//*<stucke-name>*/」。

下列範例使用路徑syle搭配預先存在的HDFS測試儲存區和測試物件。

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:24:37 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:24:37 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:24:37 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
Found 1 items
-rw-rw-rw-   1 root root       1679 2022-02-14 16:03 s3a://hdfs-test/test
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 18:24:38 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
```

疑難排解

案例**1**

使用HTTPS連線StorageGRID 進行更新、並在逾時15分鐘後收到「shipee_fuse」錯誤訊息。

*原因：*舊版JRE/JDK,使用過時或不受支援的TLS密碼套件連線StorageGRID 到S不明。

錯誤訊息範例

```
[root@ce-n1 ~]# hadoop fs -ls s3a://hdfs-test/
22/02/15 18:52:34 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/02/15 18:52:34 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/02/15 18:52:35 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/02/15 19:04:51 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/02/15 19:04:51 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
ls: doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: Received fatal alert: handshake_failure: Unable to
execute HTTP request: Received fatal alert: handshake_failure
```

*解析度：*請確定已安裝JDK 11.x或更新版本、並將Java程式庫設為預設值。請參閱 安裝Java套件 章節以取得更多資訊。

案例**2**：

無法連線StorageGRID 至包含錯誤訊息「無法找到有效的認證路徑至要求的目標」的功能。

原因： StorageGRID 不受Java程式信任*不支援SS3端點伺服器憑證。

範例錯誤訊息：

```
[root@hdp6 ~]# hadoop fs -ls s3a://hdfs-test/
22/03/11 20:58:12 WARN impl.MetricsConfig: Cannot locate configuration:
tried hadoop-metrics2-s3a-file-system.properties,hadoop-
metrics2.properties
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: Scheduled Metric snapshot
period at 10 second(s).
22/03/11 20:58:13 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system started
22/03/11 20:58:13 INFO Configuration.deprecation: No unit for
fs.s3a.connection.request.timeout(0) assuming SECONDS
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: Stopping s3a-file-system
metrics system...
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system stopped.
22/03/11 21:12:25 INFO impl.MetricsSystemImpl: s3a-file-system metrics
system shutdown complete.
22/03/11 21:12:25 WARN fs.FileSystem: Failed to initialize fileystem
s3a://hdfs-test/: org.apache.hadoop.fs.s3a.AWSClientIOException:
doesBucketExistV2 on hdfs: com.amazonaws.SdkClientException: Unable to
execute HTTP request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target: Unable to execute HTTP
request: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

解決方案： NetApp建議使用已知公共憑證簽署授權單位所核發的伺服器憑證、以確保驗證安全無虞。或者、將自訂CA或伺服器憑證新增至Java信任存放區。

完成下列步驟、將StorageGRID 一套完整的自訂CA或伺服器憑證新增至Java信任存放區。

1. 備份現有的預設Java cacerts檔案。

```
cp -ap $JAVA_HOME/lib/security/cacerts
$JAVA_HOME/lib/security/cacerts.orig
```

2. 將StorageGRID S3端點憑證匯入Java信任存放區。

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts
-storepass changeit -noprompt -alias sg-lb -file <StorageGRID CA or
server cert in pem format>
```

1. 增加Hadoop記錄層級以進行偵錯。

   '匯出Hadoop根記錄程式= Hadoop root、logger =偵錯、Console '

2. 執行命令、並將記錄訊息引導至error.log。

   「Hadoop FS -ls s3a：//<*stucke-name*>&>error.log」

_ 作者： Angela Cheng _

使用S3cmd測試StorageGRID 及示範S3在支援方面的存取

_ 作者： Aron Klein_

S3cmd是免費的命令列工具和用戶端、適用於S3作業。您可以使用s3cmd測試StorageGRID 及示範S3在支援上存取。

安裝及設定S3cmd

若要在工作站或伺服器上安裝S3cmd、請從下載 "命令列S3用戶端"。S3cmd會預先安裝在StorageGRID 每個支援的節點上、做為疑難排解的工具。

初始組態步驟

1. s3cmd --configure
2. 僅提供存取金鑰和secret金鑰、其餘部分則保留預設值。
3. 使用隨附的認證資料來測試存取？[y/n]（是/否）：n（跳過測試、因為測試會失敗）
4. 儲存設定？[y/N] y
   a. 組態已儲存至「/root/.s3cfg」
5. 在.s3cfg中、將host_base和host_bucket欄位置於"=""符號之後：
   a. host_base =
   b. host_bucket =

> 如果您在步驟4中指定host_base和host_bucket、則不需要在CLI中使用—host來指定端點。範例：

```
host_base = 192.168.1.91:8082
host_bucket = bucketX.192.168.1.91:8082
s3cmd ls s3://bucketX --no-check-certificate
```

基本命令範例

- 建立儲存庫：

  「3cmd MB S3：//s3cmd bucket -host=<終結 點>:<port>-ner-ne-check認證」

- 列出所有庫位：

  「3cmd ls --host=<端 點>:<port>---un-check認證」

- 列出所有庫存箱及其內容：

  「3cmd la -host=<終結 點>:<port>-no -check憑證」

- 列出特定儲存區中的物件：

  「3cmd ls S3：//<bucket >-host=<終結 點>:<port>-no -check憑證」

- 刪除一個桶：

  「3cmd rb s3：//s3cmd bucket -host=<終結 點>:<port>-ne-ne-check認證」

- 放置物件：

  「3cmd PUT <file> S3：//<bucket >-host=<終結 點>:<port>-no -check憑證」

- 取得物件：

  「3cmd Get S3：//<bucket >/<object>-host=<終結 點>:<port>-no -check憑證」

- 刪除物件：

  「3cmd Del S3：//<bucket >/-host=<終結 點>:<port>-no -check認證」

Vertica Eon模式資料庫使用NetApp StorageGRID 功能做為共用儲存設備

_ 作者： Angela Cheng _

本指南說明在NetApp StorageGRID 還原上建立具有公用儲存設備的Vertica Eon Mode資料庫的程序。

簡介

Vertica是分析資料庫管理軟體。它是一款柱式儲存平台、專為處理大量資料而設計、可在傳統的密集環境中、提供極快的查詢效能。Vertica資料庫以兩種模式之一執行：Eon或Enterprise。您可以在內部部署或雲端部署這兩種模式。

Eon和Enterprise模式在儲存資料的位置上主要有所不同：

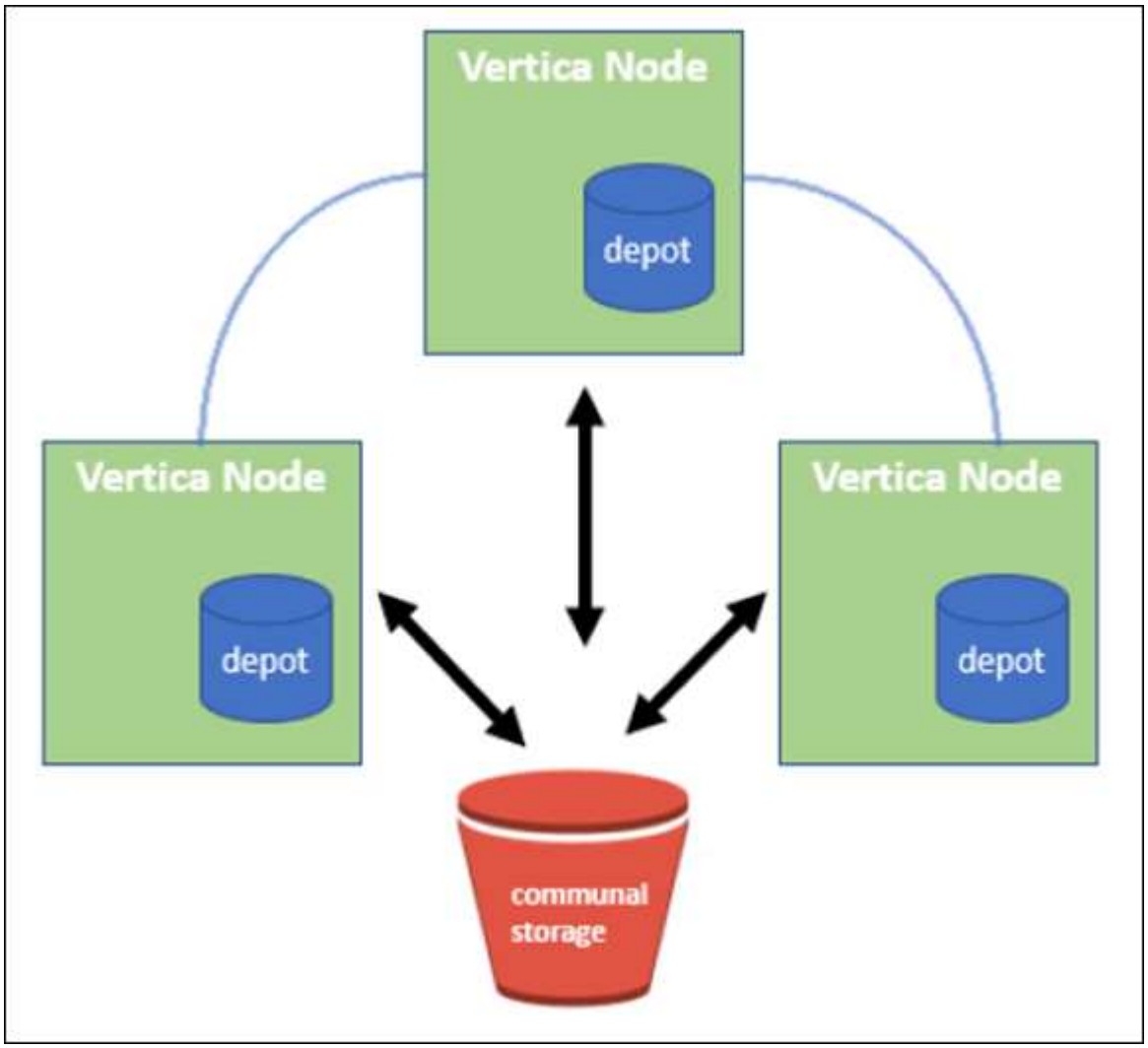
- Eon Mode資料庫使用公用儲存設備來儲存資料。這是Vertica推薦的。

- 企業模式資料庫會將資料儲存在本機的資料庫中、儲存在組成資料庫的節點檔案系統中。

Eon Mode架構

Eon Mode將運算資源與資料庫的共用儲存層區隔開來、讓運算和儲存設備能夠分開擴充。Eon Mode中的Vertica經過最佳化、可因應各種工作負載、並使用獨立的運算與儲存資源將其彼此隔離。

Eon Mode會將資料儲存在稱為公用儲存設備的共用物件儲存區中、S3儲存區是在內部部署或Amazon S3上代管。



共用儲存設備

Eon Mode不會在本機儲存資料、而是使用單一共線儲存位置來儲存所有資料和目錄（中繼資料）。公用儲存設備是資料庫的集中式儲存位置、可在資料庫節點之間共用。

公用儲存設備具有下列屬性：

- 雲端或內部部署物件儲存設備中的公用儲存設備彈性較高、而且由於儲存設備故障而導致資料遺失的可能性較個別機器上磁碟上的儲存設備來得小。
- 任何資料都可以由任何使用相同路徑的節點讀取。
- 容量不受節點上磁碟空間的限制。

- 由於資料是以社群方式儲存、因此您可以彈性擴充叢集、以因應瞬息萬變的需求。如果資料儲存在節點本機上、則新增或移除節點時、需要在節點之間移動大量資料、才能將資料從要移除的節點移出、或移到新建立的節點上。

維修中心

公用儲存設備的缺點之一、就是速度。從共享雲端位置存取資料的速度比從本機磁碟讀取慢。此外、如果許多節點同時從公用儲存設備讀取資料、則連線至公用儲存設備可能會成為瓶頸。為了改善資料存取速度、Eon Mode資料庫中的節點會維護本機磁碟快取、其中的資料稱為「倉儲」。執行查詢時、節點會先檢查所需的資料是否位於儲存庫中。如果是、則會使用資料的本機複本完成查詢。如果資料不在儲存庫中、節點會從公用儲存設備擷取資料、並將複本儲存在儲存庫中。

NetApp StorageGRID 技術建議

Vertica將資料庫資料儲存至物件儲存區、儲存為數千（或數百萬）個壓縮物件（觀察到每個物件的大小為200至500MB）。當使用者執行資料庫查詢時、Vertica會使用位元組範圍Get呼叫、從這些壓縮物件平行擷取所選的資料範圍。每個位元組範圍的Get大約為8KB。

在10TB資料庫倉儲的使用者查詢測試期間、每秒傳送4、000至10、000個Get（位元組範圍Get）要求至網格。使用SG6060應用裝置執行此測試時、雖然每個應用裝置節點的CPU使用率%很低（約20%至30%）、但2/3的CPU使用時間仍在等待I/O在SGF6024上觀察到I/O等待的百分比極低（0%至0.5%）。

由於小IOPS需求高且延遲需求極低（平均應低於0.01秒）、NetApp建議將SFG6024用於物件儲存服務。如果需要SG6060來處理非常大的資料庫大小、客戶應與Vertica客戶團隊合作調整進廠規模、以支援主動查詢的資料集。

對於管理節點和API閘道節點、客戶可以使用SG100或SG1000。選項取決於並行和資料庫大小的使用者查詢要求數量。如果客戶偏好使用協力廠商負載平衡器、NetApp建議使用專屬的負載平衡器來處理高效能需求工作負載。如需StorageGRID 調整規模、請洽詢NetApp客戶團隊。

其他StorageGRID 的功能組態建議包括：

- 網格拓撲。請勿將SGF6024與同一個網格網站上的其他儲存應用裝置機型混用。如果您偏好使用SG6060來提供長期歸檔保護、請將SGF6024與專屬的網格負載平衡器一起保留在主動式資料庫的網格站台（實體或邏輯站台）中、以提升效能。在同一個站台混合使用不同機型的應用裝置、會降低站台的整體效能。
- 資料保護。使用Replicate複本以保護資料安全。請勿對使用中的資料庫使用銷毀編碼。客戶可以使用銷毀編碼來長期保護非作用中資料庫。
- 不啟用網格壓縮。Vertica會先壓縮物件、再儲存至物件儲存。啟用網格壓縮不會進一步節省儲存使用量、也會大幅降低位元組範圍的效能。
- * HTTP與HTTPS S3端點連線*。在基準測試期間、我們觀察到使用HTTP S3連線從Vertica叢集到StorageGRID Es負載 平衡器端點時、效能提升約5%。此選項應根據客戶的安全需求而定。

Vertica組態的建議包括：

- 對於讀寫作業、會啟用* Vertica資料庫預設的進廠設定（值= 1）。NetApp強烈建議您啟用這些進廠設定、以提升效能。
- 停用串流限制。如需組態詳細資料、請參閱一節 停用串流限制。

將Eon Mode安裝在內部部署環境中、並將公用儲存設備安裝在StorageGRID 原地

以下各節說明將Eon Mode安裝在內部部署環境中、並將公用儲存設備安裝在StorageGRID 原地的程序。設定內部部署簡易儲存服務（S3）相容物件儲存設備的程序、與Vertica指南中的程序類似、 "在內部部署環境中安裝Eon Mode資料庫"。

下列設定用於功能測試：

- 零點11.4.0.4 StorageGRID
- Vertica 10.1.0
- 三部虛擬機器（VM）搭配CentOS 7.x作業系統、可讓Vertica節點組成叢集。此設定僅適用於功能測試、不適用於Vertica正式作業資料庫叢集。

這三個節點是以安全Shell（SSH）金鑰設定、以便在叢集內的節點之間不需密碼即可執行SSH。

NetApp StorageGRID 產品所需資訊

若要在StorageGRID 內部部署環境中安裝Eon Mode、並將公用儲存設備安裝在原地、您必須具備下列必要資訊。

- IP位址或StorageGRID 完整網域名稱（FQDN）和端口號。如果您使用的是HTTPS、請使用StorageGRID 在S3端點上實作的自訂憑證授權單位（CA）或自我簽署SSL憑證。
- 儲存區名稱。它必須預先存在且為空白。
- 存取金鑰ID和密碼存取金鑰、並可讀寫儲存區的存取權。

建立授權檔案以存取S3端點

建立存取S3端點的授權檔案時、必須符合下列先決條件：

- 已安裝Vertica。
- 叢集已設定、設定並準備好建立資料庫。

若要建立存取S3端點的授權檔案、請遵循下列步驟：

1. 登入Vertica節點、執行「admintool」以建立Eon Mode資料庫。

   預設使用者為「dbadmin」、是在Vertica叢集安裝期間建立的。

2. 使用文字編輯器在「/home/DBadmin'」目錄下建立檔案。檔案名稱可以是您想要的任何內容、例如「shg_auth.conf」。
3. 如果S3端點使用標準HTTP連接埠80或HTTPS連接埠443、請跳過連接埠號碼。若要使用HTTPS、請設定下列值：

   - 「awsenablehttps = 1」、否則請將值設為「0」。
   - 「awsaith =<S3存取金鑰ID>:<秘密存取金鑰>'
   - 「aws端 點=<s/s3 StorageGRID 端點>:<port>'

   若要使用自訂CA或自我簽署的SSL憑證來進行StorageGRID SESS3端點HTTPS連線、請指定憑證的完整檔案路徑和檔名。此檔案必須位於每個Vertica節點上的相同位置、並對所有使用者具有讀取權限。如

果StorageGRID 由已知的CA簽署了SESS3端點SSL憑證、請跳過此步驟。

「awscafile =<檔案路徑/檔案名稱>」

例如、請參閱下列範例檔案：

```
awsauth = MNVU4OYFAY2xyz123:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wANabcxyz
awsendpoint = s3.england.connectlab.io:10443
awsenablehttps = 1
awscafile = /etc/custom-cert/grid.pem
```

+

在正式作業環境中、客戶應在StorageGRID 一個S3負載平衡器端點上、實作由已知CA簽署的伺服器憑證。

在所有**Vertica**節點上選擇一個進廠路徑

在每個節點上為倉儲儲存路徑選擇或建立目錄。您為倉儲儲存路徑參數所提供的目錄必須具有下列項目：

- 叢集中所有節點的相同路徑（例如、「/home/DBadmin/depot」）
- DBAdmin使用者可讀取且可寫入
- 足夠的儲存容量

  根據預設、Vertica會使用60%的檔案系統空間、其中包含用於倉儲儲存設備的目錄。您可以使用「cred_db」命令中的「-kepot-sizes」引數來限制庫房的大小。請參閱 "調整Eon模式資料庫的Vertica叢集規模" 文章以瞭解一般的Vertica規模調整準則、或洽詢您的Vertica客戶經理。

  如果不存在「admintools create_db"工具、則會嘗試為您建立一個進廠路徑。

建立**Eon**內部部署資料庫

若要建立Eon內部部署資料庫、請遵循下列步驟：

1. 若要建立資料庫、請使用「admintooles create_db]工具。

   下列清單提供本範例中使用之引數的簡短說明。如需所有必要和選用引數的詳細說明、請參閱Vertica文件。

   - -x <在中建立之授權檔案的路徑/檔名 「建立授權檔案以存取S3端點」 >。

     授權詳細資料會在成功建立後儲存在資料庫內。您可以移除此檔案、以避免公開S3秘密金鑰。

   - 公用儲存位置<S3：//storagegrid Bucketname>
   - s <用於此資料庫的Vertica節點以逗號分隔的清單>
   - -d <要建立的資料庫名稱>
   - p <要為此新資料庫設定的密碼>。例如、請參閱下列命令範例：

```
admintools -t create_db -x sg_auth.conf --communal-storage
-location=s3://vertica --depot-path=/home/dbadmin/depot --shard
-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'<password>'
```

根據資料庫的節點數、建立新資料庫需要幾分鐘的時間。第一次建立資料庫時、系統會提示您接受授權合約。

例如、請參閱下列授權檔案範例和「create db]命令：

```
[dbadmin@vertica-vm1 ~]$ cat sg_auth.conf
awsauth = MNVU4OYFAY2CPKVXVxxxx:03vuO4M4KmdfwffT8nqnBmnMVTr78Gu9wAN+xxxx
awsendpoint = s3.england.connectlab.io:10445
awsenablehttps = 1

[dbadmin@vertica-vm1 ~]$ admintools -t create_db -x sg_auth.conf
--communal-storage-location=s3://vertica --depot-path=/home/dbadmin/depot
--shard-count=6 -s vertica-vm1,vertica-vm2,vertica-vm3 -d vmart -p
'xxxxxxxx'
Default depot size in use
Distributing changes to cluster.
    Creating database vmart
    Starting bootstrap node v_vmart_node0007 (10.45.74.19)
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
    Starting Vertica on all nodes. Please wait, databases with a large
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (DOWN)
    Node Status: v_vmart_node0007: (UP)
    Creating database nodes
    Creating node v_vmart_node0008 (host 10.45.74.29)
    Creating node v_vmart_node0009 (host 10.45.74.39)
    Generating new configuration information
    Stopping single node db before adding additional nodes.
    Database shutdown complete
    Starting all nodes
Start hosts = ['10.45.74.19', '10.45.74.29', '10.45.74.39']
    Starting nodes:
        v_vmart_node0007 (10.45.74.19)
        v_vmart_node0008 (10.45.74.29)
        v_vmart_node0009 (10.45.74.39)
    Starting Vertica on all nodes. Please wait, databases with a large
```

```
catalog may take a while to initialize.
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (DOWN) v_vmart_node0008: (DOWN)
v_vmart_node0009: (DOWN)
    Node Status: v_vmart_node0007: (UP) v_vmart_node0008: (UP)
v_vmart_node0009: (UP)
Creating depot locations for 3 nodes
Communal storage detected: rebalancing shards

Waiting for rebalance shards. We will wait for at most 36000 seconds.
Installing AWS package
    Success: package AWS installed
Installing ComplexTypes package
    Success: package ComplexTypes installed
Installing MachineLearning package
    Success: package MachineLearning installed
Installing ParquetExport package
    Success: package ParquetExport installed
Installing VFunctions package
    Success: package VFunctions installed
Installing approximate package
    Success: package approximate installed
Installing flextable package
    Success: package flextable installed
Installing kafka package
    Success: package kafka installed
Installing logsearch package
    Success: package logsearch installed
Installing place package
    Success: package place installed
Installing txtindex package
    Success: package txtindex installed
Installing voltagesecure package
    Success: package voltagesecure installed
Syncing catalog on vmart with 2000 attempts.
Database creation SQL tasks completed successfully. Database vmart created
successfully.
```

物件大小（位元組）	鏟斗/物件金鑰完整路徑
"61歲"	「s 3 ：//Vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a21a07_0_0_0_0.DFS'」
《145》	「s 3 ：//Vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a3d/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a3d_0_0.DFs」
《146》	「s 3 ：//Vertica/33C/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a1d/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a1d_0_0.dfs」
《40》	「s 3 ：//Vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a31 / 026d63ae9d4a33237bf0e2c2cf2a794a00a000021a31_0_0_0.DFs」
《145》	「s 3 ：//Vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a21/026d63ae9d4a33237bf0e2c2c2cf2a794a00a0000a21a21a21a21_0_0_0_0.DFS'」
"34"	「s 3 ：//Vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a25_0_0_0.DFs」
《41》	「s 3 ：//Vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a2d/026d63ae9d4a33237bf0e2c2c2cf2a794a00a000021a2a2d_0_0_0_0.DFs」
"61歲"	「s 3 ：//Vertica/52A/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a5d/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a5d_0_0.DFs」
《131》	「s 3 ：//Vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a19/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a19_0_0_0.DFS'

物件大小（位元組）	鏟斗/物件金鑰完整路徑
《91》	「s 3：//Vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a11/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a11_0_0_0.DFS'」
《118》	「s 3：//Vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a21a15_0_0_0.DFs」
《115》	「s 3：//Vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a61/026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a61_0_0_0.DFS'」
《33》	「s 3：//Vertica/ACD/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a29 / 026d63ae9d4a33237bf0e2c2cf2a794a00a000021a29_0_0_0.DFS'」
《133》	「s 3：//Vertica/b98/ 026d63ae9d4a33237bf0e2c2cf2a794a00a000021a4d /026d63ae9d4a33237bf0e2c2c2a794a00a0000a21a4d_0_0.dfs」
《38》	「s 3：//Vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a49/ 026d63ae9d4a33237bf0e2c2cf2a794a00a0000a21a49_0_0_0.DFS'」
《38》	「s 3：//Vertica/EBA / 026d63ae9d4a33237bf0e2c2cf2a794a00a0000s000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a21a59_0_0_0.DFs」
《21521920》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2c2c2a794a00a00002152/026d63ae9d4a33237bf0e2c2c2a794a00a0000a0000a0000a2152.tar」
《6865408》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a0000a2162.tar」

物件大小（位元組）	鏟斗/物件金鑰完整路徑
《204217344》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a0000a21610.tar」
《16109056》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a0000s0000217e0/026d63ae9d4a33237bf0e2c2c2a794a00a0000a0000a0000a217e0.tar」
《12853248》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a00a00002180.tar」
《8937984》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a0000187a/026d63ae9d4a33237bf0e2c2c2a794a00a0000a0000187a.tar]
《56260608》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a000018b2/026d63ae9d4a33237bf0e2c2c2a794a00a0000a0000a218b2.tar」
《53947904》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a0000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a0000a219ba.tar'」
《44932608》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a0000a0000a219de.tar」
《256306688》	「s 3：//Vertica/mata/VMart/Archites/026d63ae9d4a33237bf0e2c2c2c2a794a00a000021a6e/026d63ae9d4a33237bf0e2c2c2c2a794a00a0000a0000a00a0000a2a6a0000a6a6a6a6a6a6a6ae.tar
《8062464》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2c2cf2a794a00a000021e34/026d63ae9d4a33237bf0e2c2c2a794a00a0000a00a0000a000021e34.tar]

物件大小（位元組）	鏟斗/物件金鑰完整路徑
《20024832》	「s 3：//Vertica /中繼資料/VMart/Archites/026d63ae9d4a33237bf0e2c2cf2a794a00a000021e70-026d63ae9d4a33237bf0e2c2c2a794a00a0000a0000a70a.tar]
《104444》	「s 3：//Vertica/metadmetada/VMart/叢集_config.json」
《822666》	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/nates/c13_13/chkpt_1.cat.gz`
"254"	「s 3：//Vertica /中繼資料/VMart/nodes/v_v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/checks/c13_13/completed」
《2958》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28573/narates/c2_2/chkpt_1.cat.gz`」
《231》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/nates/c2_2/completed」
《822521》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28573/narates/c4_4/chkpt_1.cat.gz`」
《231》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/checks/c4_4/completed」
《746513》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat`」
《2596》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz`」
《821065》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz`」

物件大小（位元組）	鏟斗/物件金鑰完整路徑
《6440》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat`」
"8518"	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat`」
0	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`」
《822922》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0017/Catalog/859703b06a3456d95d0be28573a673/narates/C14_7/chkpt_1.cat.gz`」
"232"	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0017/Catalog/859703b06a3456d95d0be28575a673/nates/C14_7/completed」
《822930》	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0017/Catalog/859703b06a3456d95d0be2857a673/Txnlogs/txn_14_g7.cat.gz`
《755033》	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0017/Catalog/859703b06a3456d95d0be2857a673/Txnlogs/txn_15_g8.cat`
0	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0017/Catalog/859703b06a3456d95d0be2857a673/tiered_catalog.cat`
《822922》	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0018/Catalog/859703b06a3456d95d0be28573a673/narates/C14_7/chkpt_1.cat.gz`」
"232"	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0018/Catalog/859703b06a3456d95d0be28575a673/nates/C14_7/completed」
《822930》	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0018/Catalog/859703b06a3456d95d0be285775a673/Txnlogs/txn_14_g7.cat.gz`

物件大小（位元組）	鏟斗/物件金鑰完整路徑
《755033》	s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0018/Catalog/859703b06a3456d95d0be285775a673/Txnlogs/txn_15_g8.cat`
0	「s 3：//Vertica /中繼資料/VMart/nodes/v_vmart節點0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat`」

停用串流限制

此程序以Vertica指南為基礎、適用於其他內部部署物件儲存設備、應適用於StorageGRID 下列項目：

1. 建立資料庫之後、請將「AWSStreamingConnectionPercentage」組態參數設為「0」、以停用該參數。對於使用公用儲存設備的Eon Mode內部部署安裝、此設定是不必要的。此組態參數可控制VRTica用於串流讀取之物件存放區的連線數目。在雲端環境中、此設定有助於避免物件存放區的串流資料佔用所有可用的檔案處理代碼。它會保留一些檔案處理常用於其他物件存放區作業。由於內部部署物件存放區的延遲很低、因此不需要使用此選項。
2. 使用「vsql」陳述式來更新參數值。密碼是您在「建立Eon內部部署資料庫」中設定的資料庫密碼。例如、請參閱下列輸出範例：

```
[dbadmin@vertica-vm1 ~]$ vsql
Password:
Welcome to vsql, the Vertica Analytic Database interactive terminal.
Type:   \h or \? for help with vsql commands
        \g or terminate with semicolon to execute query
        \q to quit
dbadmin=> ALTER DATABASE DEFAULT SET PARAMETER
AWSStreamingConnectionPercentage = 0; ALTER DATABASE
dbadmin=> \q
```

正在驗證庫房設定

Vertica資料庫預設的進廠設定會啟用（值= 1）以進行讀取和寫入作業。NetApp強烈建議您啟用這些進廠設定、以提升效能。

```
vsql -c 'show current all;' | grep -i UseDepot
DATABASE | UseDepotForReads | 1
DATABASE | UseDepotForWrites | 1
```

載入範例資料（選用）

如果此資料庫即將進行測試並移除、您可以將範例資料載入此資料庫進行測試。Vertica隨附範例資料集VMart、可在每個Vertica節點的「/opt/Vertica/examples/VMart_Schema/」下找到。您可以找到此範例資料集的詳細資訊"請按這裡"。

請依照下列步驟載入範例資料：

1. 以DBAdmin身分登入任一Vertica節點：CD /opt/Vertica/examples/VMart_Schema/
2. 將範例資料載入資料庫、並在子步驟c和d中出現提示時輸入資料庫密碼：
   a. 「CD /opt/Vertica/examples/VMart_Schema」
   b. 」
   c. 「vsql < vmart定義_schema.sql'
   d. 「vsql < vmart載入資料.sql'
3. 有多個預先定義的SQL查詢、您可以執行其中一些查詢、以確認測試資料已成功載入資料庫。例如：「vsql < vmart _queries1.sql'

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- "NetApp StorageGRID 11.7 產品文件"
- "資料表StorageGRID"
- "Vertica 10.1產品文件"

版本歷程記錄

版本	日期	文件版本歷程記錄
1.0版	2021年9月	初始版本。

_ 作者： Angela Cheng _

使用elk堆疊進行記錄分析StorageGRID

_ 作者： Angela Cheng _

使用 StorageGRID 系統記錄轉送功能，您可以設定外部系統記錄伺服器來收集和分析 StorageGRID 記錄訊息。Elk（Elasticsearch、Logstash、Kibana）已成為最受歡迎的記錄分析解決方案之一。觀看 "使用elk視訊進行記錄分析StorageGRID" 以檢視範例 elk 組態、以及如何使用它來識別和疑難排解失敗的 S3 要求。StorageGRID 11.9 支援將負載平衡器端點存取記錄匯出至外部 Syslog 伺服器。請觀看此影片 "YouTube 影片"，深入瞭解這項新功能。本文提供Logstash組態、Kibana查詢、圖表和儀表板的範例檔案、協助您快速開始StorageGRID 進行資訊記錄管理和分析。

需求

- SHO11.6.0.2或更高版本StorageGRID
- Elk（Elasticsearch、Logstash和Kibana）7.1x或更新版本已安裝並開始運作

範例檔案

- "下載Logstash 7.x範例檔案套件" +* md5 checksum * 148c23d0021d9a4bb4a6c0287464deab +* sha256 checksum * f51ec9e2e3f842d5a7861566b167a561beb4373038b4e7bb3c8b3d522adf2d6
- "下載Logstash 8.x範例檔案套件" +* md5 checksum * e11bae3a662f87c310ef363d0fe06835 +* sha256 checksum * 5c670755742cfdfd5aa723a596ba087e0153a65bcaf3934afdb682f61278d
- "下載 StorageGRID 11.9 的 Logstash 8.x 範例檔案套件"+ * MD5 checksum * 41272857c4a54600f95995f6ed74800d + * sha256 checksum * 67048ee8661052719990851e1e1ad960d4902fe537a6e135e8600177188da677c9

假設

讀者熟悉StorageGRID 了功能性的技術與操作。

指示

由於Grok模式定義的名稱不同、因此提供兩個範例版本。+例如、Logstash組態檔中的SYSLOGBASE-Grok模式會根據安裝的Logstash版本、以不同的方式定義欄位名稱。

```
match => {"message" => '<%{POSINT:syslog_pri}>%{SYSLOGBASE}
%{GREEDYDATA:msg-details}'}
```

- Logstash 7.17樣本*

Field	Value
t _id	7C1MaYEBRH8UbfKnIls8
t _index	sgrid2-2022.06.15
# _score	-
t _type	_doc
@timestamp	Jun 15, 2022 @ 17:36:46.038
t host	grid2-site2-s1
t logsource	SITE2-S1
t msg-details	Reloading syslog service
t pid	628
t program	update-sysl
t syslog_pri	37
t timestamp	Jun 15 21:36:46

記錄**8.23**樣本

Table JSON

Search field names

Actions	Field	Value
▫▫▫	_id	yuhOiIEBVP6KX4EwqcyU
▫▫▫	_index	sglog-2022.06.21
▫▫▫	# _score	-
▫▫▫	@timestamp	Jun 21, 2022 @ 18:07:45.444
▫▫▫	t event.original	<28>Jun 21 22:07:45 SITE2-S3 ADE: syslog messages being dropped
▫▫▫	t host.hostname	SITE2-S3
▫▫▫	t msg-details	syslog messages being dropped
▫▫▫	t process.name	ADE
▫▫▫	t syslog_pri	28
▫▫▫	t timestamp	Jun 21 22:07:45

步驟

1. 根據您安裝的elk版本解壓縮提供的範例。範例資料夾包含兩個Logstash組態範例：* sglog-2-file.conf：此組態檔可在**StorageGRID** 不進行資料轉換的情況下、將不含資料的記錄訊息輸出至**Logstash**上的檔案。您可以使用此選項來確認**Logstash**是否接收**StorageGRID** 到任何消息、或是協助瞭解**StorageGRID** 哪些是資訊記錄模式。**+** sglog-2-es.conf：*此組態檔會StorageGRID 使用各種模式和篩選器來轉換資訊記錄訊息。其中包括範例Drop陳述式、可根據模式或篩選條件來刪除訊息。輸出會傳送至Elasticsearch以進行索引。+根據檔案內的指示自訂所選的組態檔。

2. 測試自訂的組態檔：

```
/usr/share/logstash/bin/logstash --config.test_and_exit -f <config-file-
path/file>
```

   如果傳回的最後一行與下列行類似、則組態檔沒有語法錯誤：

```
[LogStash::Runner] runner - Using config.test_and_exit mode. Config
Validation Result: OK. Exiting Logstash
```

3. 將自訂的設定檔複製到Logstash伺服器的組態：/etc/logstash/conf.d+如果您尚未在/etc/logstash/logstash.yml中啟用config.reload.automatic、請重新啟動Logstash服務。否則、請等待設定重新載入時間間隔過去。

```
 grep reload /etc/logstash/logstash.yml
# Periodically check if the configuration has changed and reload the
pipeline
config.reload.automatic: true
config.reload.interval: 5s
```

4. 檢查/var/log/logstash/logstash-plain.log、確認使用新的組態檔啟動Logstash時沒有錯誤。

5. 確認TCP連接埠已啟動並正在偵聽。+在此範例中、使用TCP連接埠5000。

```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

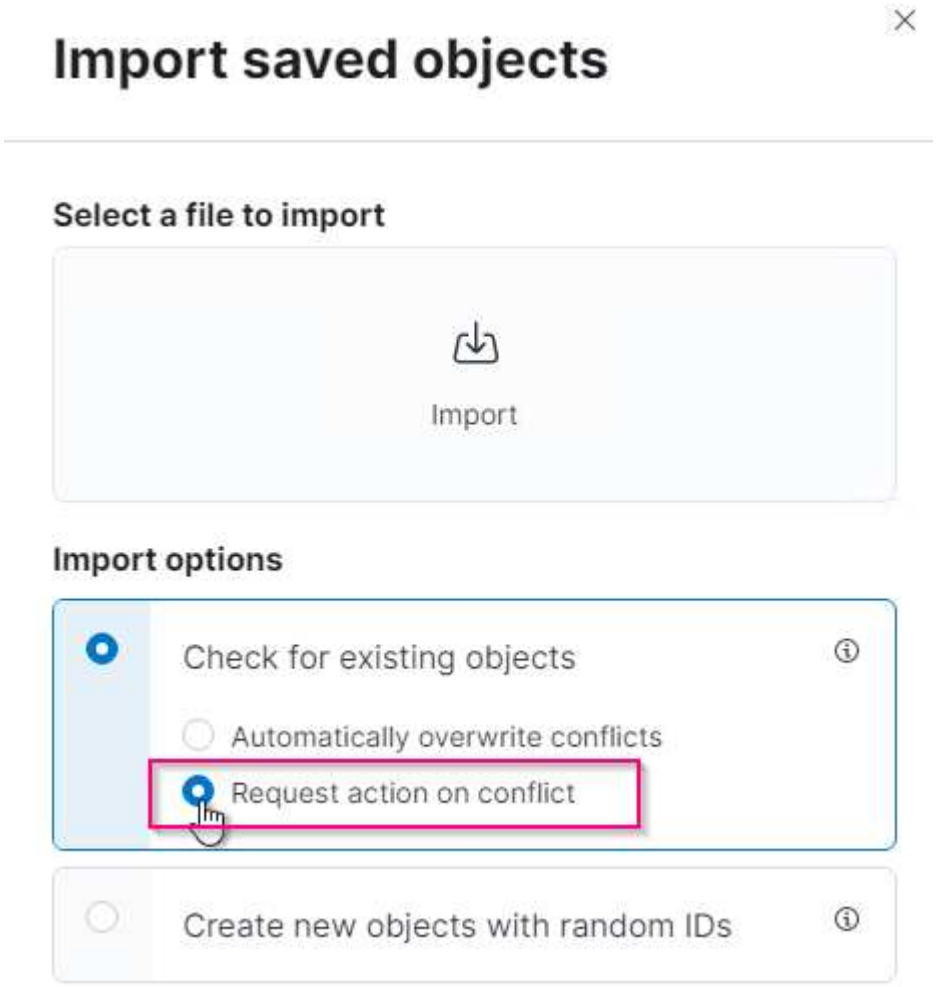
6. 從程式管理程式GUI、設定外部syslog伺服器StorageGRID 、將記錄訊息傳送至Logstash。如需詳細資訊、請參閱 "示範影片" 。

7. 您需要在Logstash伺服器上設定或停用防火牆、才能讓StorageGRID 節點連線至定義的TCP連接埠。

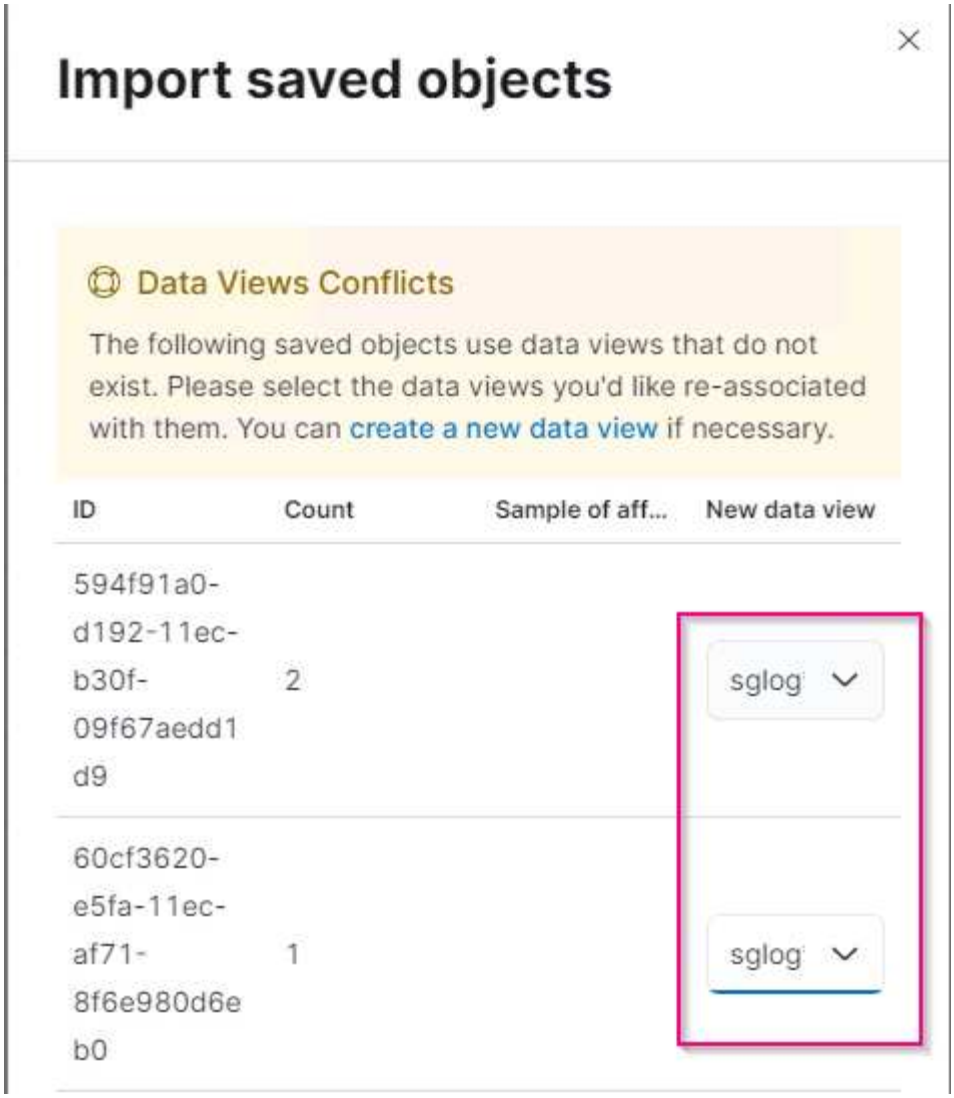
8. 從Kibana GUI中、選取「Management（管理）」→「Dev Tools（開發工具）」。在「主控台」頁面上、執行此「Get」命令、確認已在Elasticsearch上建立新索引。

```
GET /_cat/indices/*?v=true&s=index
```

9. 從Kibana GUI建立索引模式（elk 7.x）或資料檢視（elk 8.x）。
10. 從Kibana GUI、在位於上方中心的搜尋方塊中輸入「儲存的物件」。+在「儲存的物件」頁面上、選取「匯入」。在「匯入選項」下、選取「在衝突時要求採取行動」



匯入elk<version>-query-chart-same.ndjson。+當系統提示您解決衝突時、請選取您在步驟8中建立的索引模式或資料檢視。



匯入下列 Kibana 物件： + * 查詢 bycast.log * + * 稽核 - msg-s3rq-orlm + * 廣播記錄 S3 相關訊息 + * 記錄層級警告或更高 + * 失敗安全事件 + * Ngins-GW 端點存取記錄（僅適用於 elk8-skample-for -sg119.zip ） + * 圖表 * + S3 要求根據上述儀表板的平均回應時間類型 + 回應數 * ，按儀表板數 + msg * ，以追蹤記錄 *

您現在可以StorageGRID 使用Kibana來執行資訊分析。

其他資源

- "系統記錄101."
- "什麼是elk堆疊"
- "Grok模式清單"
- "Logstash入門指南：Grok"
- "Logstash的實用指南：syslog深度探討"
- "Kibana指南–瀏覽文件"
- "零稽核記錄訊息參考StorageGRID"

使用Prometheus和Grafana來延長指標保留時間

_ 作者： Aron Klein_

本技術報告提供了配置NetApp StorageGRID與外部 Prometheus 和 Grafana 服務的詳細說明。

簡介

支援使用Prometheus儲存指標、並透過內建的Grafana儀表板提供這些指標的視覺效果。StorageGRID透過StorageGRID 設定用戶端存取憑證、並為指定的用戶端啟用Prometheus存取、可從功能表安全存取Prometheus指標。目前、保留此度量資料的能力受管理節點的儲存容量限制。為了獲得更長的持續時間、以及建立自訂的這些指標視覺效果、我們將部署新的Prometheus和Grafana伺服器、設定新伺服器、從StorageGRID執行個體中掃描指標、並建立一個儀表板、其中包含對我們來說非常重要的指標。您可以取得更多有關在中收集的Prometheus指標的資訊 "本文檔StorageGRID"。

聯盟Prometheus

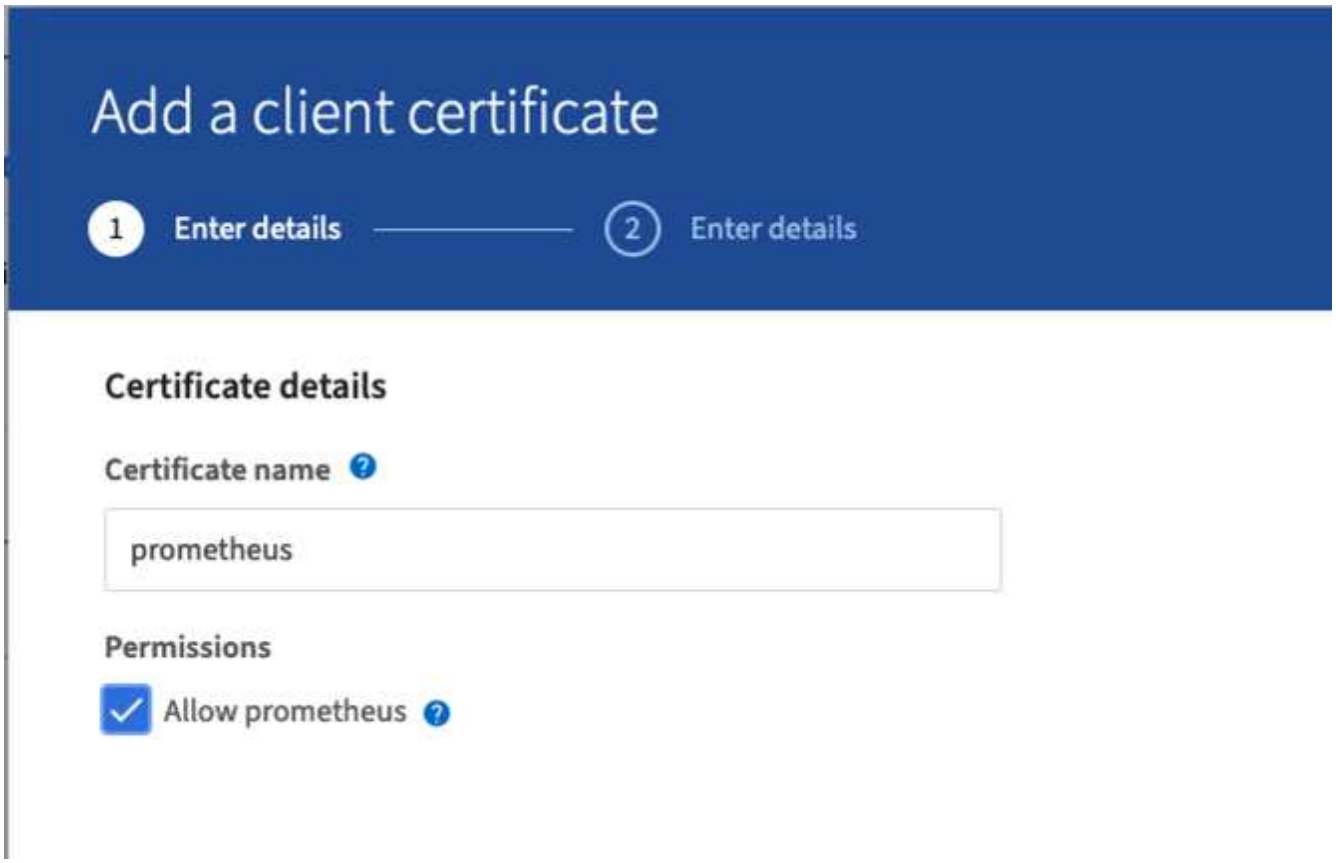
實驗室詳細資料

就本例而言、我將使用所有虛擬機器來StorageGRID 執行VMware 11.6節點、以及使用一個DEBIAN11伺服器。此解決方法介面設定了公開信任的CA憑證。StorageGRID此範例將不會安裝及設定StorageGRID 整個作業系統或是安裝的Debian Linux。您可以使用Prometheus和Grafana所支援的任何Linux風格。Prometheus和Grafana都可以安裝成Docker容器、從來源或預先編譯的二進位檔建置。在此範例中、我會將Prometheus和Grafana二進位檔案直接安裝在同一部的Debian伺服器上。請從下載並遵循基本安裝指示 https://prometheus.io 和 https://grafana.com/grafana/ 分別。

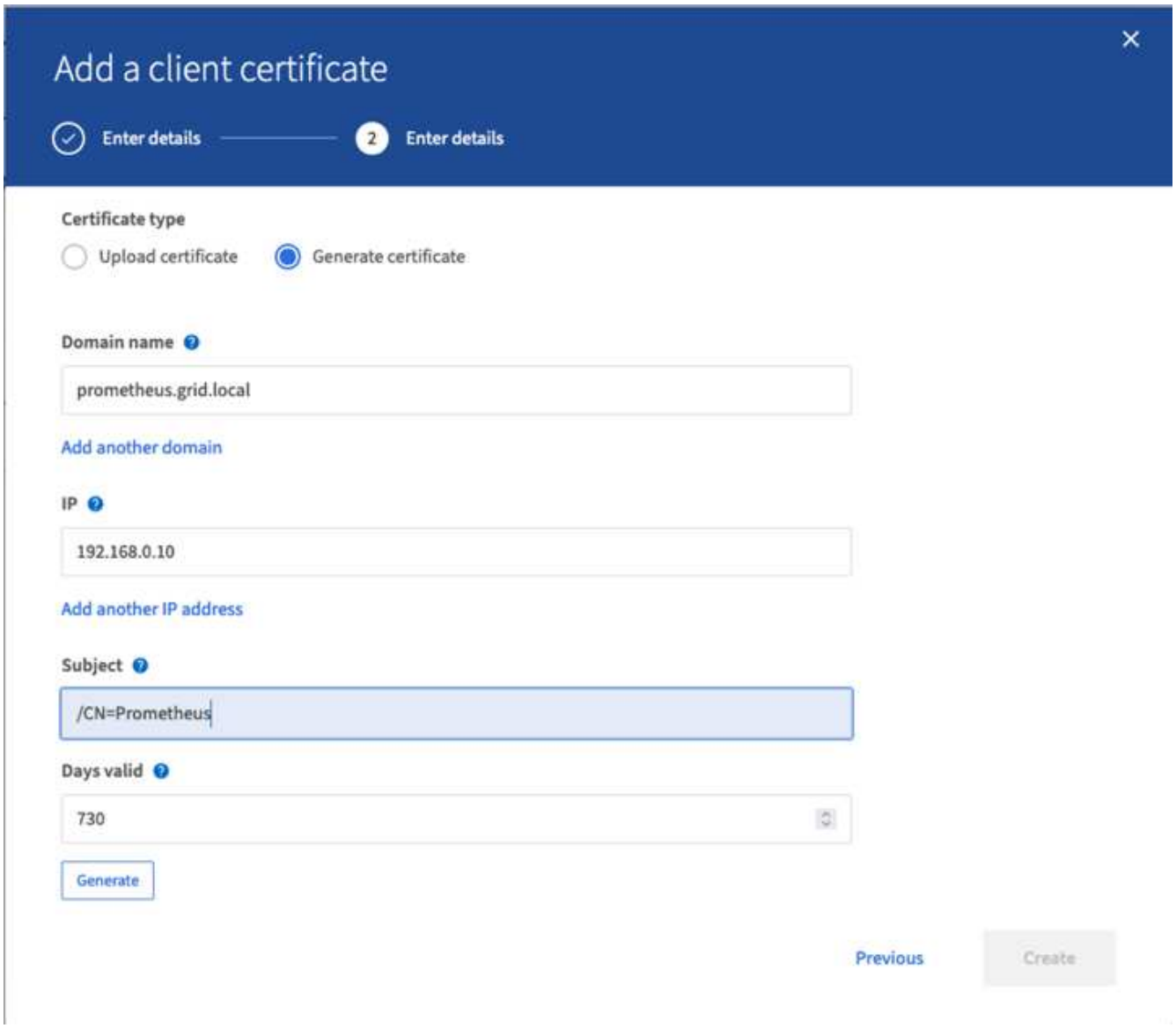
設定**StorageGRID** 驗證以供**Prometheus**用戶端存取

若要存取StorageGRID儲存的Prometheus指標、您必須使用私密金鑰產生或上傳用戶端憑證、並啟用用戶端的權限。這個介面必須具有SSL憑證。StorageGRID此憑證必須由Prometheus伺服器信任、或是由信任的CA信任、如果是自行簽署、則必須手動信任。若要瞭解更多資訊、請造訪 "本文檔StorageGRID"。

1. 在「功能區管理」介面中、選取左下角的「組態」、然後在「安全性」下的第二欄中、按一下「憑證」StorageGRID 。
2. 在「憑證」頁面上、選取「用戶端」索引標籤、然後按一下「新增」按鈕。
3. 提供將被授予存取權並使用此憑證的用戶端名稱。按一下「權限」下方的方塊、位於「允許Prometheus」前面、然後按一下「繼續」按鈕。

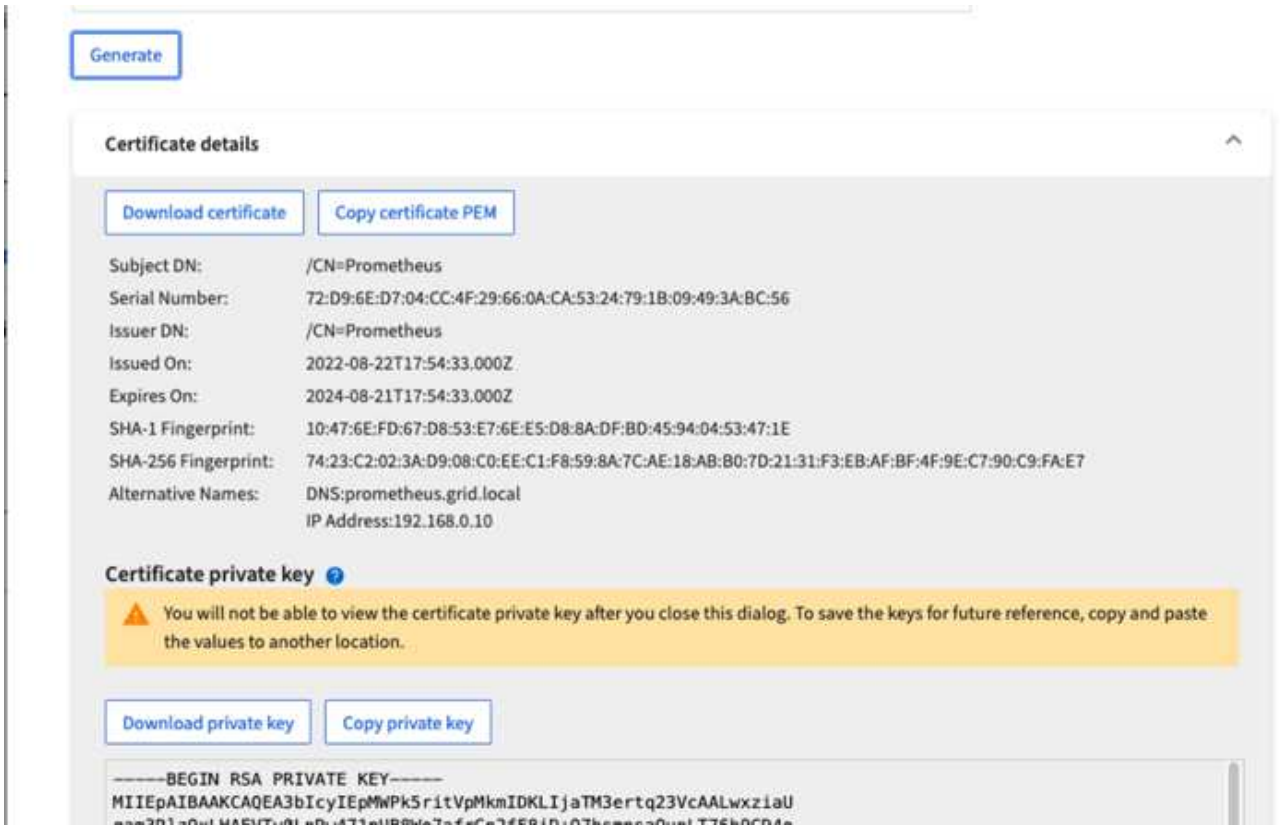


4. 如果您有CA簽署的憑證、您可以選取「上傳憑證」的選項按鈕、但在我們的案例中StorageGRID 、我們要選擇「產生憑證」的選項按鈕、讓流程無法產生用戶端憑證。必填欄位將會顯示以供填寫。輸入用戶端伺服器的FQDN、伺服器的IP、主旨及有效天數。然後按一下「產生」按鈕。



> Be mindful of the certificate days valid entry as you will need to renew this certificate in both StorageGRID and the Prometheus server before it expires to maintain uninterrupted collection.

1. 下載憑證pem檔案和私密金鑰pem檔案。



> This is the only time you can download the private key, so make sure you do not skip this step.

準備**Linux**伺服器以進行**Prometheus**安裝

在安裝Prometheus之前、我想要讓Prometheus使用者、目錄結構做好準備、並設定度量儲存位置的容量。

1. 建立Prometheus使用者。

```
sudo useradd -M -r -s /bin/false Prometheus
```

2. 建立Prometheus、用戶端憑證和指標資料的目錄。

```
sudo mkdir /etc/Prometheus /etc/Prometheus/cert /var/lib/Prometheus
```

3. 我使用ext4檔案系統來格式化我所使用的磁碟以保留指標。

```
mkfs -t ext4 /dev/sdb
```

4. 然後、我將檔案系統掛載到Prometheus度量目錄。

```
sudo mount -t auto /dev/sdb /var/lib/prometheus/
```

5. 取得您用於度量資料的磁碟uuid。

```
sudo ls -al /dev/disk/by-uuid/
   lrwxrwxrwx 1 root root   9 Aug 18 17:02 9af2c5a3-bfc2-4ec1-85d9-
ebab850bb4a1 -> ../../sdb
```

6. 在/etc/fstb/中新增項目、使掛載會在重新開機後持續使用/dev/sdb的uuid。

```
/etc/fstab
UUID=9af2c5a3-bfc2-4ec1-85d9-ebab850bb4a1 /var/lib/prometheus   ext4
defaults    0   0
```

安裝及設定**Prometheus**

現在伺服器已經準備好、我可以開始安裝Prometheus並設定服務。

1. 擷取Prometheus安裝套件

```
tar xzf prometheus-2.38.0.linux-amd64.tar.gz
```

2. 將二進位檔複製到/usr/local/bin、並將擁有權變更為先前建立的Prometheus使用者

```
sudo cp prometheus-2.38.0.linux-amd64/{prometheus,promtool}
/usr/local/bin
sudo chown prometheus:prometheus /usr/local/bin/{prometheus,promtool}
```

3. 將主控台和程式庫複製到/etc/Prometheus

```
sudo cp -r prometheus-2.38.0.linux-amd64/{consoles,console_libraries}
/etc/prometheus/
```

4. 將先前從StorageGRID 下列網址下載的用戶端憑證和私密金鑰pem檔案複製到/etc/Prometheus/certs
5. 建立Prometheus組態yaml檔案

```
sudo nano /etc/prometheus/prometheus.yml
```

6. 插入下列組態。工作名稱可以是您想要的任何內容。將「-targets：[']"（目標：[']"）變更為管理節點的FQDN、如果您變更了憑證名稱和私密金鑰檔名、請更新TLS_config區段以進行比對。然後儲存檔案。如果您的網格管理介面使用自我簽署的憑證、請下載該憑證並將其與具有唯一名稱的用戶端憑證一起放置、然後在TLS_config區段中新增ca_file:/etc/Prometheus/cert /UCERT.pem

   a. 在此範例中、我會收集所有以alertmanager、Cassandra、節點和StorageGRID VMware為開頭的指標。如需有關Prometheus指標的詳細資訊、請參閱 "本文檔StorageGRID"。

```
# my global config
global:
  scrape_interval: 60s # Set the scrape interval to every 15 seconds.
Default is every 1 minute.

scrape_configs:
  - job_name: 'StorageGRID'
    honor_labels: true
    scheme: https
    metrics_path: /federate
    scrape_interval: 60s
    scrape_timeout: 30s
    tls_config:
      cert_file: /etc/prometheus/cert/certificate.pem
      key_file: /etc/prometheus/cert/private_key.pem
    params:
      match[]:
        -
'{__name__=~"alertmanager_.*|cassandra_.*|node_.*|storagegrid_.*"}'
    static_configs:
    - targets: ['sgdemo-rtp.netapp.com:9091']
```

如果您的網格管理介面使用自我簽署的憑證、請下載該憑證、並以唯一名稱將其與用戶端憑證一起放置。在「TLs_config」區段中、將憑證新增到用戶端憑證和私密金鑰行上方

```
        ca_file: /etc/prometheus/cert/UIcert.pem
```

1. 將/etc/Prometheus中所有檔案和目錄的擁有權、以及/var/lib/Prometheus變更為Prometheus使用者

```
sudo chown -R prometheus:prometheus /etc/prometheus/
sudo chown -R prometheus:prometheus /var/lib/prometheus/
```

2. 在/etc/systemd/system中建立Prometheus服務檔案

```
sudo nano /etc/systemd/system/prometheus.service
```

3. 請插入下列行、並記下#--storage・tsdb.retitation.times=1y#、將度量資料的保留時間設為1年。或者、您也可以使用#-storage、tsdb、retrite.size=300GiB#來根據儲存限制來保留基礎資料。這是唯一可設定保留指標的位置。

```
[Unit]
Description=Prometheus Time Series Collection and Processing Server
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
        --config.file /etc/prometheus/prometheus.yml \
        --storage.tsdb.path /var/lib/prometheus/ \
        --storage.tsdb.retention.time=1y \
        --web.console.templates=/etc/prometheus/consoles \
        --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

4. 重新載入systemd服務以註冊新的Prometheus服務。然後啟動並啟用Prometheus服務。

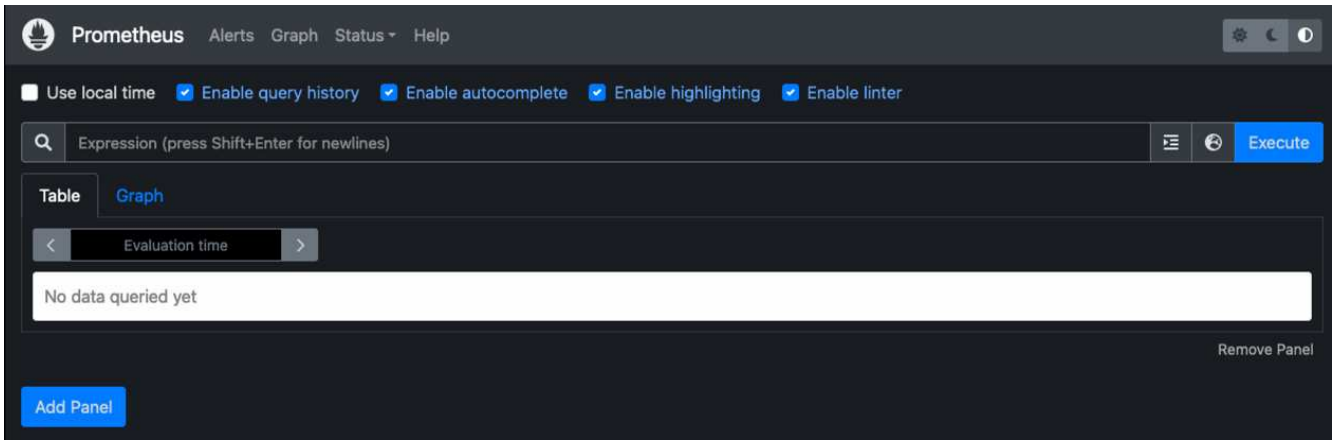
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. 檢查服務是否正常運作

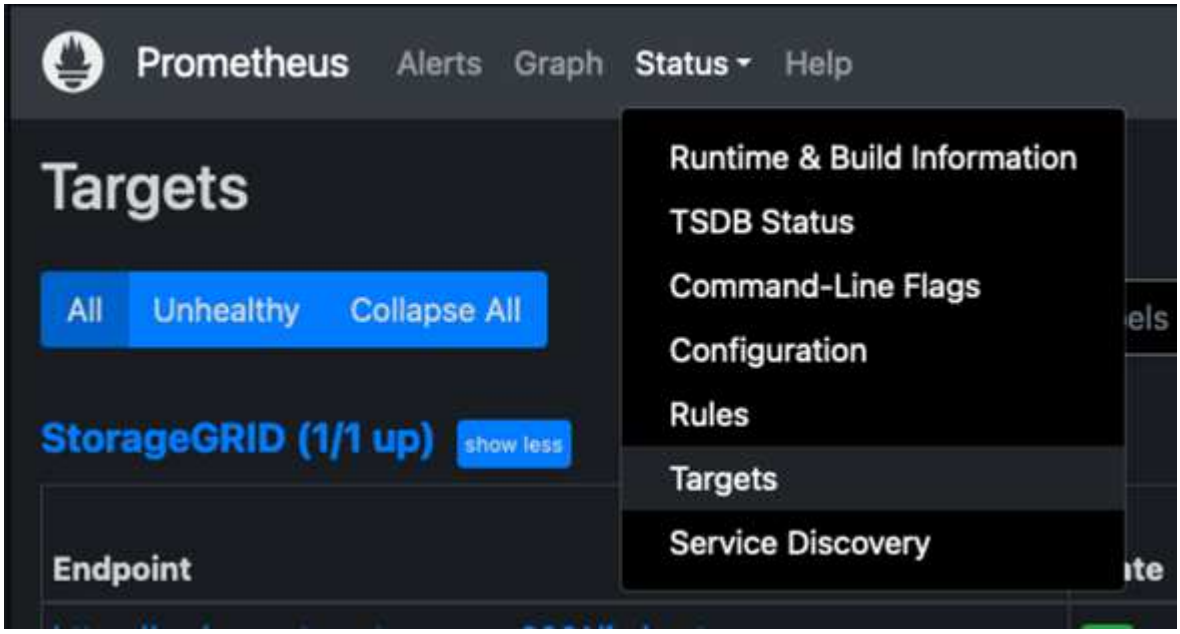
```
sudo systemctl status prometheus
```

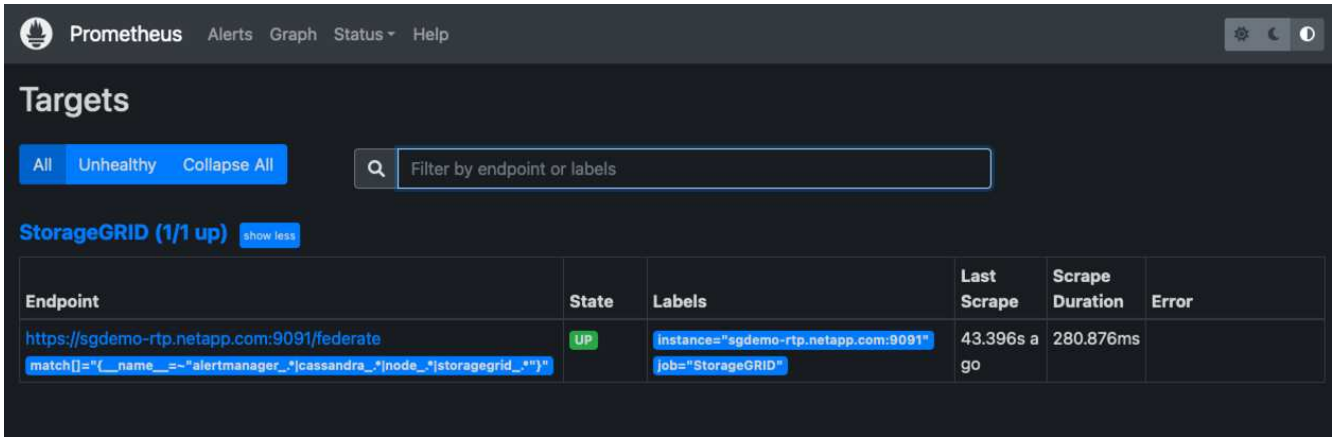
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 28818)
     Memory: 107.7M
        CPU: 1.143s
     CGroup: /system.slice/prometheus.service
             └─6498 /usr/local/bin/prometheus --config.file
/etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
--web.console.templates=/etc/prometheus/consoles --web.con>

Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.510Z caller=head.go:544 level=info component=tsdb
msg="Replaying WAL, this may take a while"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=0 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:615 level=info component=tsdb msg="WAL
segment loaded" segment=1 maxSegment=1
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.816Z caller=head.go:621 level=info component=tsdb msg="WAL
replay completed" checkpoint_replay_duration=55.57µs wal_rep>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:997 level=info fs_type=EXT4_SUPER_MAGIC
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1000 level=info msg="TSDB started"
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.831Z caller=main.go:1181 level=info msg="Loading
configuration file" filename=/etc/prometheus/prometheus.yml
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:1218 level=info msg="Completed loading
of configuration file" filename=/etc/prometheus/prometheus.y>
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=main.go:961 level=info msg="Server is ready to
receive web requests."
Aug 22 15:14:24 aj-deb-prom01 prometheus[6498]: ts=2022-08-
22T19:14:24.832Z caller=manager.go:941 level=info component="rule
manager" msg="Starting rule manager..."
```

6. 您現在應該可以瀏覽至Prometheus伺服器的UI http://Prometheus-server:9090 並查看UI

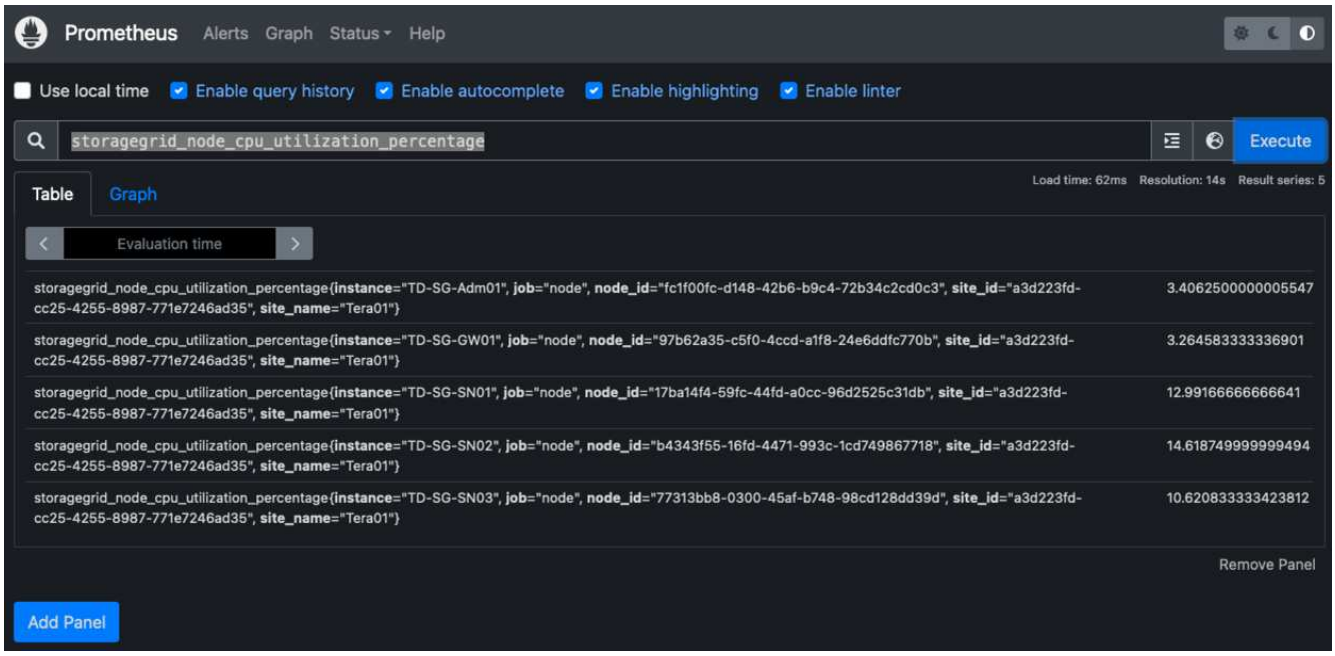


7. 在「Status（狀態）」目標下、您可以看到StorageGRID 我們在Prometheus.yml中設定的這個端點的狀態





8. 在「圖表」頁面上、您可以執行測試查詢、並驗證資料是否已成功擷取。例如、在查詢列中輸入「storagegrid節點_cpu使用率百分比」、然後按一下「執行」按鈕。



安裝及設定Grafana

現在Prometheus已經安裝完成且正常運作、我們可以繼續安裝Grafana並設定儀表板

Grafana安裝

1. 安裝最新的Grafana企業版

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key
https://packages.grafana.com/gpg.key
```

2. 為穩定版本新增此儲存庫：

```
echo "deb [signed-by=/usr/share/keyrings/grafana.key]
https://packages.grafana.com/enterprise/deb stable main" | sudo tee -a
/etc/apt/sources.list.d/grafana.list
```

3. 新增儲存庫之後。

```
sudo apt-get update
sudo apt-get install grafana-enterprise
```

4. 重新載入systemd服務以登錄新的grafana服務。然後啟動並啟用Grafana服務。

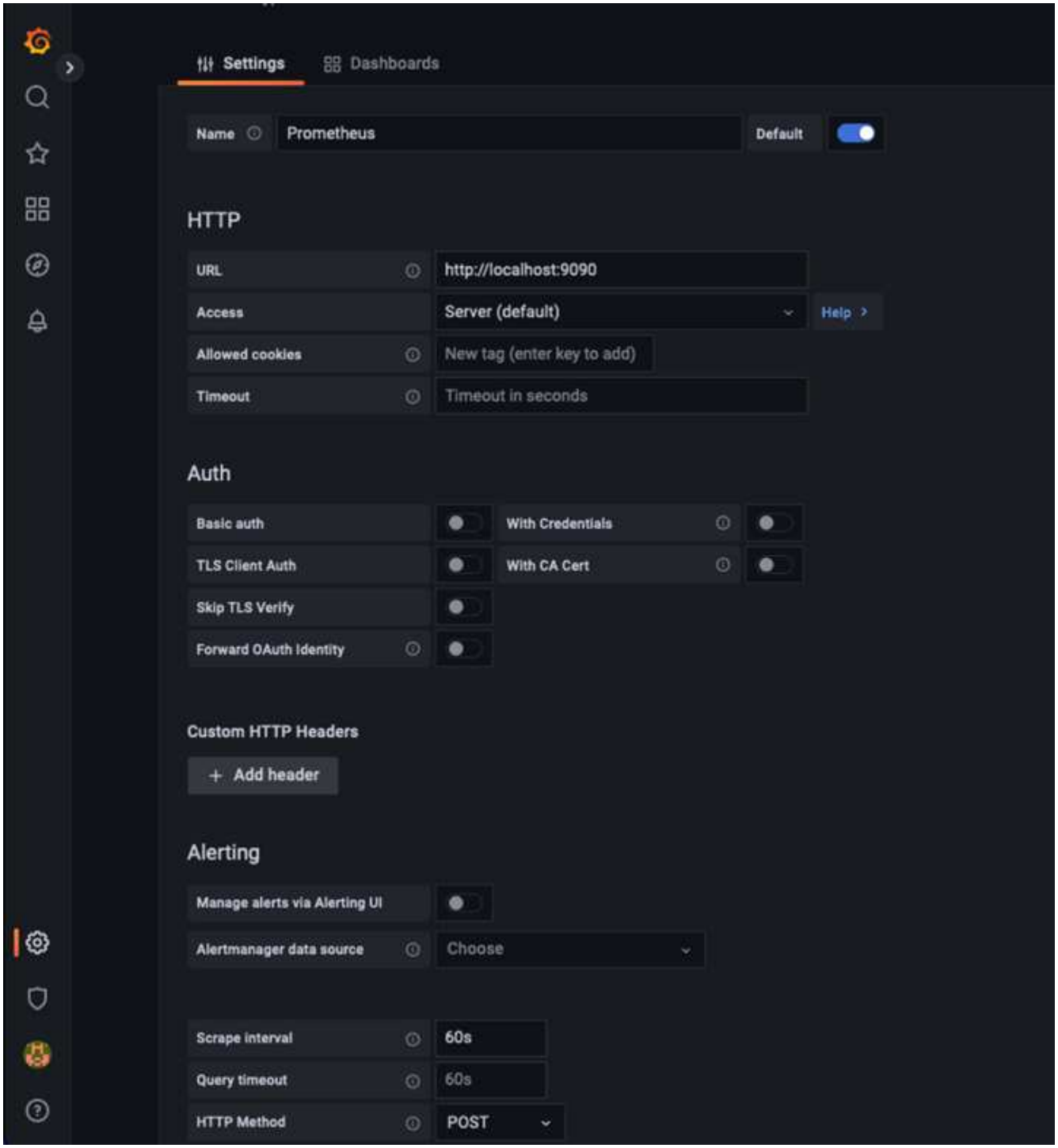
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana現已安裝並執行。當您開啟瀏覽器以存取HTTP：//Prometheus-server:3000時、您將會看到Grafana登入頁面。
6. 預設的登入認證為admin/admin、您應該在提示時設定新密碼。

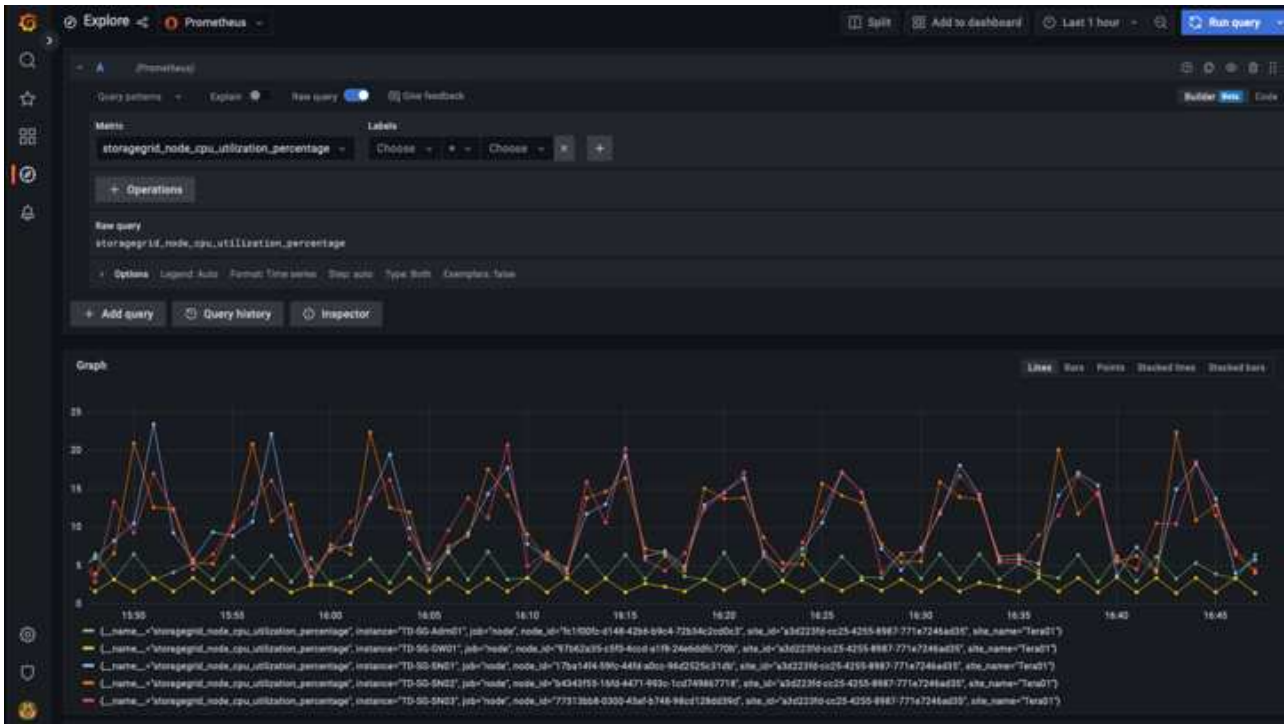
建立**Grafana**儀表板**StorageGRID** 以利執行

在安裝並執行Grafana和Prometheus之後、現在正是建立資料來源並建置儀表板來連接兩者的好時機

1. 在左窗格中展開「組態」、然後選取「資料來源」、再按一下「新增資料來源」按鈕
2. Prometheus將是最熱門的資料來源之一。如果不是、請使用搜尋列找出「Prometheus」
3. 輸入Prometheus執行個體的URL、以及符合Prometheus時間間隔的Scp強 檔時間間隔、以設定Prometheus來源。我也停用警示區段、因為我沒有在Prometheus上設定警示管理程式。



4. 輸入所需的設定後、向下捲動至底部、然後按一下「Save & test（儲存並測試）」。
5. 組態測試成功後、按一下「Explore（瀏覽）」按鈕。
   a. 在「Explore（瀏覽）」視窗中、您可以使用我們使用「storagegrid節點CPU使用率百分比」測試的相同度量、然後按一下「Run query（執行查詢）」按鈕

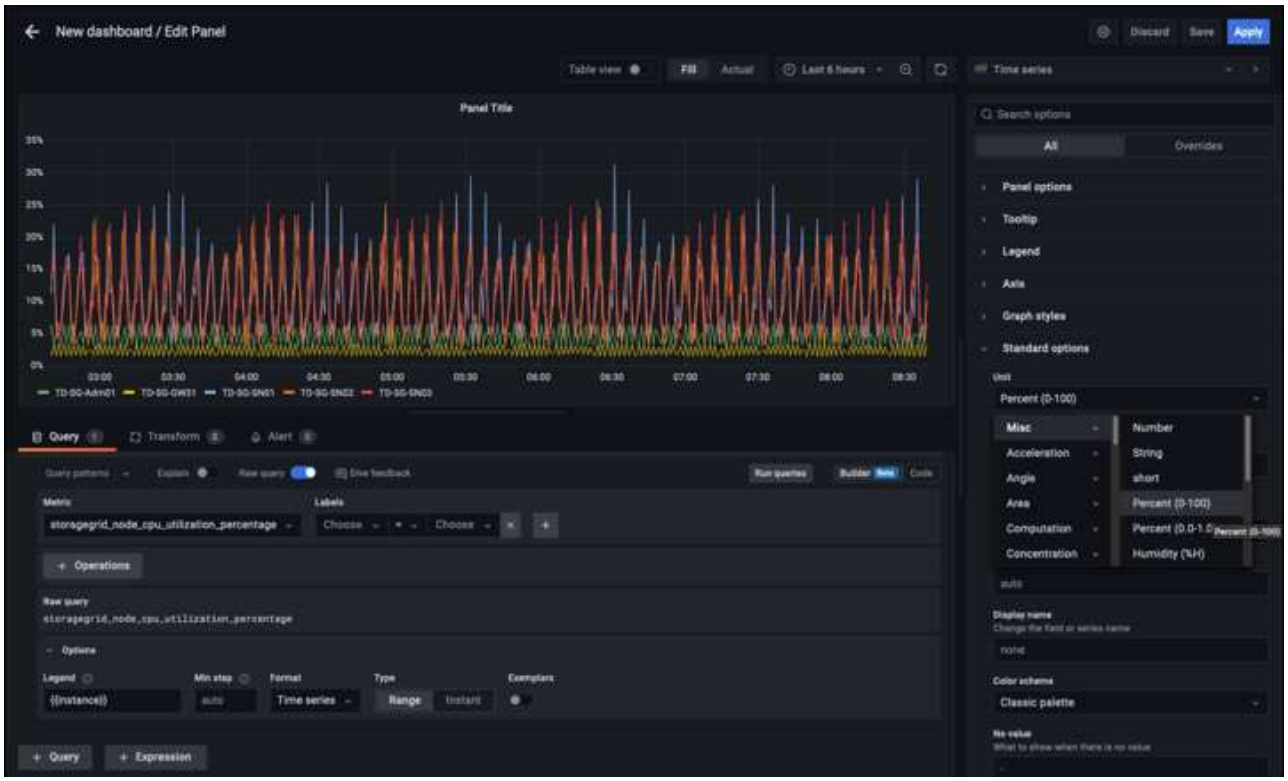


6. 現在我們已經設定好資料來源、就能建立儀表板。

   a. 在左窗格中展開「儀表板」、然後選取「+ new Dashboard」

   b. 選取「新增面板」

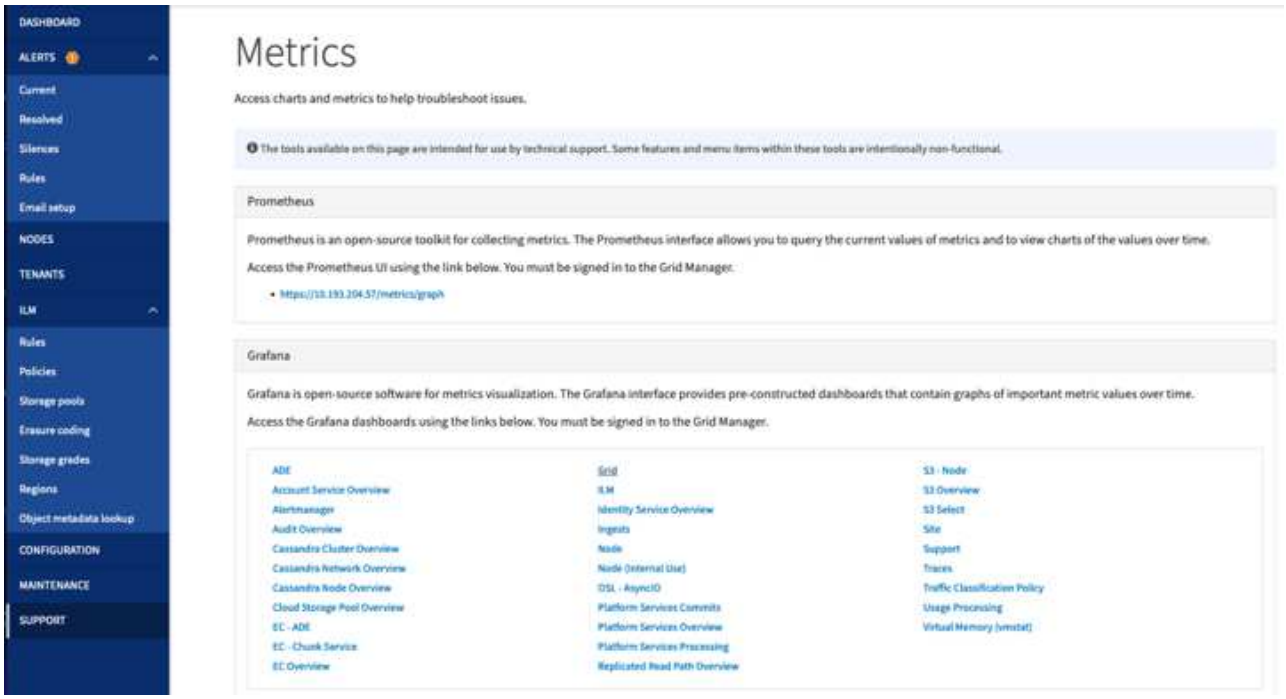
   c. 選取度量來設定新的面板、我將再次使用「storagegRid_nore_cpu使用率百分比」、輸入面板的標題、展開底部的「選項」、然後將圖例變更為自訂、並輸入「｛｛instance｝｝」以定義節點名稱、並在右窗格的「Standard options」（標準選項）下、將「Unit」設為「siscs/center百（單位）。然後按一下「套用」、將面板儲存至儀表板。



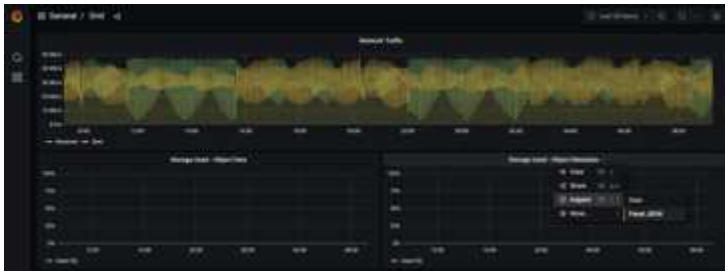
7. 我們可以針對每個所需的指標、繼續打造類似的儀表板、但幸好StorageGRID 、我們已經有儀表板可供複製到我們的自訂儀表板。

   a. 從左側窗格的「支援」選項、StorageGRID 然後在「工具」欄底部按一下「指標」。

   b. 在指標中、我要選取中間欄頂端的「Grid（網格）」連結。

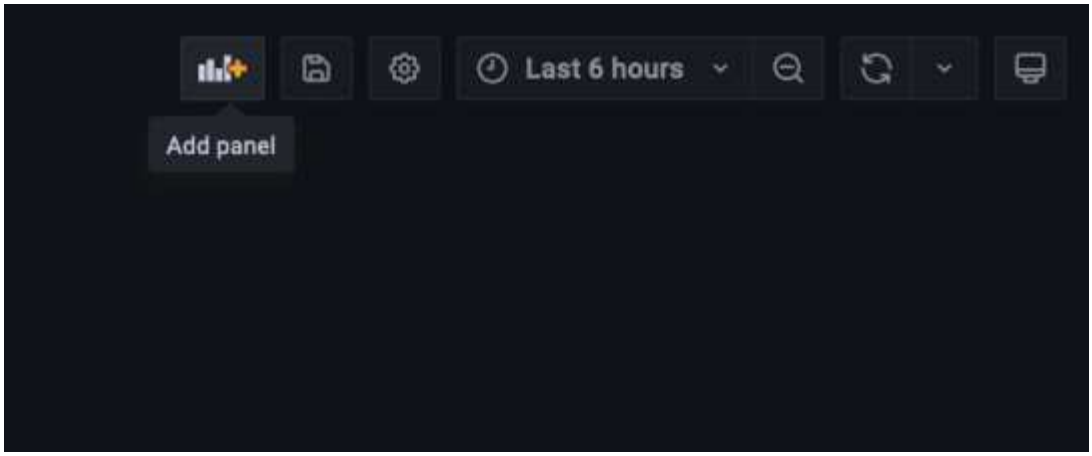


   c. 從網格儀表板中、選取「使用的儲存設備-物件中繼資料」面板。按一下小向下箭頭和面板標題的結尾、即可下拉功能表。在此功能表中、選取「檢查」和「面板Json」。



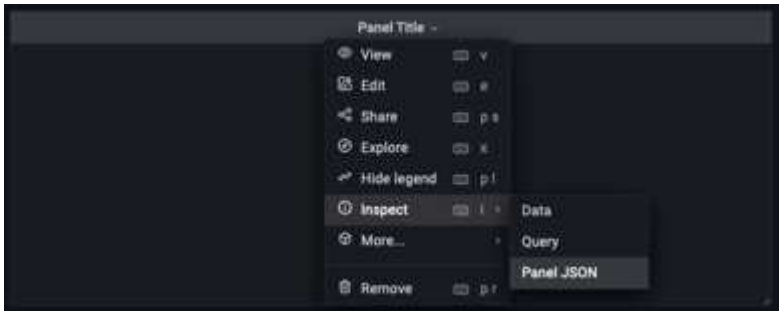
   d. 複製Json程式碼並關閉視窗。

e. 在新儀表板中、按一下圖示以新增面板。

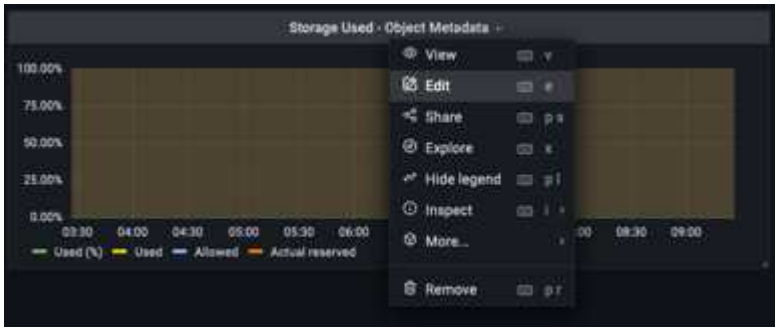


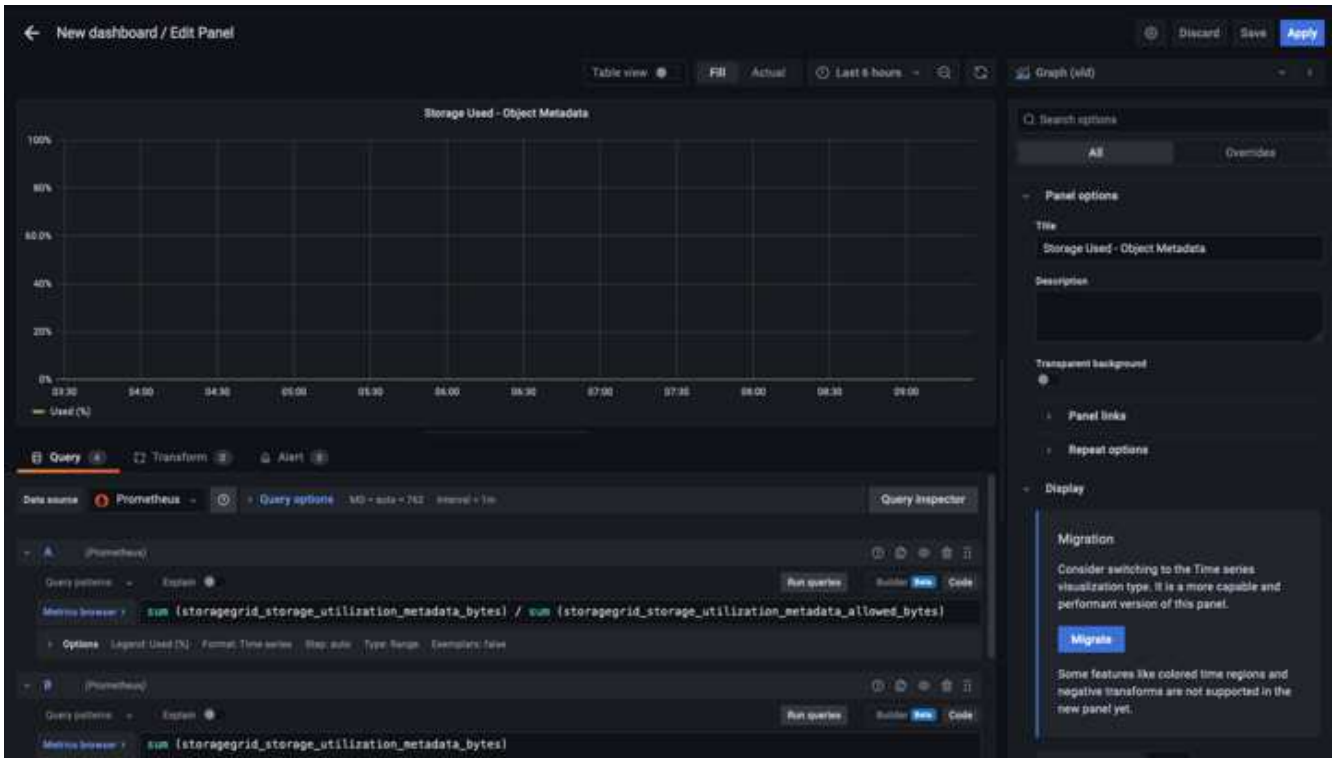
f. 套用新的面板而不做任何變更

g. 就像StorageGRID 使用「無縫面板」一樣、請檢查Json。移除所有Json程式碼、然後從StorageGRID「資訊畫面」中以複製的程式碼加以取代。



h. 編輯新的面板、右側會顯示移轉訊息、並顯示「移轉」按鈕。按一下按鈕、然後按一下「Apply（套用）」按鈕。





8. 當您將所有面板都放在適當的位置並依自己的需求進行設定之後、按一下右上角的磁碟圖示以儲存儀表板、並為儀表板命名。

結論

現在我們擁有Prometheus伺服器、可自訂資料保留和儲存容量。有了這項功能、我們就能繼續建立自己的儀表板、並提供與營運最相關的指標。您可以取得更多有關在中收集的Prometheus指標的資訊 "本文檔StorageGRID"。

使用 F5 DNS 實現StorageGRID 的全域負載平衡

作者：史蒂夫・戈爾曼 (F5)

本技術報告提供了詳細的說明，指導如何配置NetApp StorageGRID與 F5 DNS 服務，以實現全域負載平衡，從而在網格分佈於多個站點和/或 HA 群組時，提供更好的資料可用性、更高的資料一致性並優化 S3 事務路由。

簡介

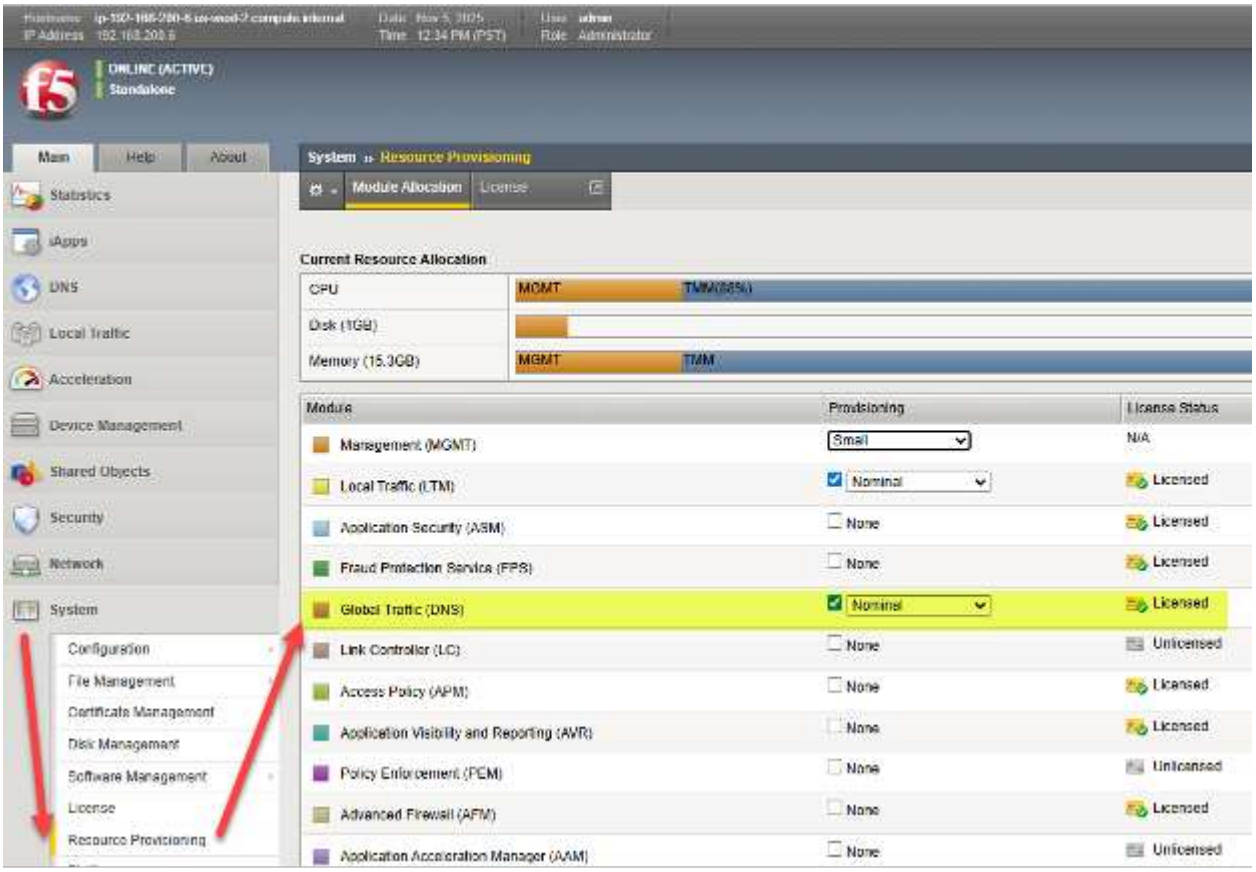
F5 BIG-IP DNS 解決方案以前稱為 BIG-IP GTM（全球流量管理器），非正式名稱為 GSLB（全球伺服器負載平衡），它允許跨多個主動-主動 HA 群組和主動多站點StorageGRID解決方案實現無縫存取。

F5 BIG-IP 多站點StorageGRID配置

無論要支援多少個StorageGRID站點，至少需要兩個 BIG-IP 設備（實體或虛擬）啟用並設定 BIG-IP DNS 模組。DNS 設備越多，企業獲得的冗餘程度就越高。

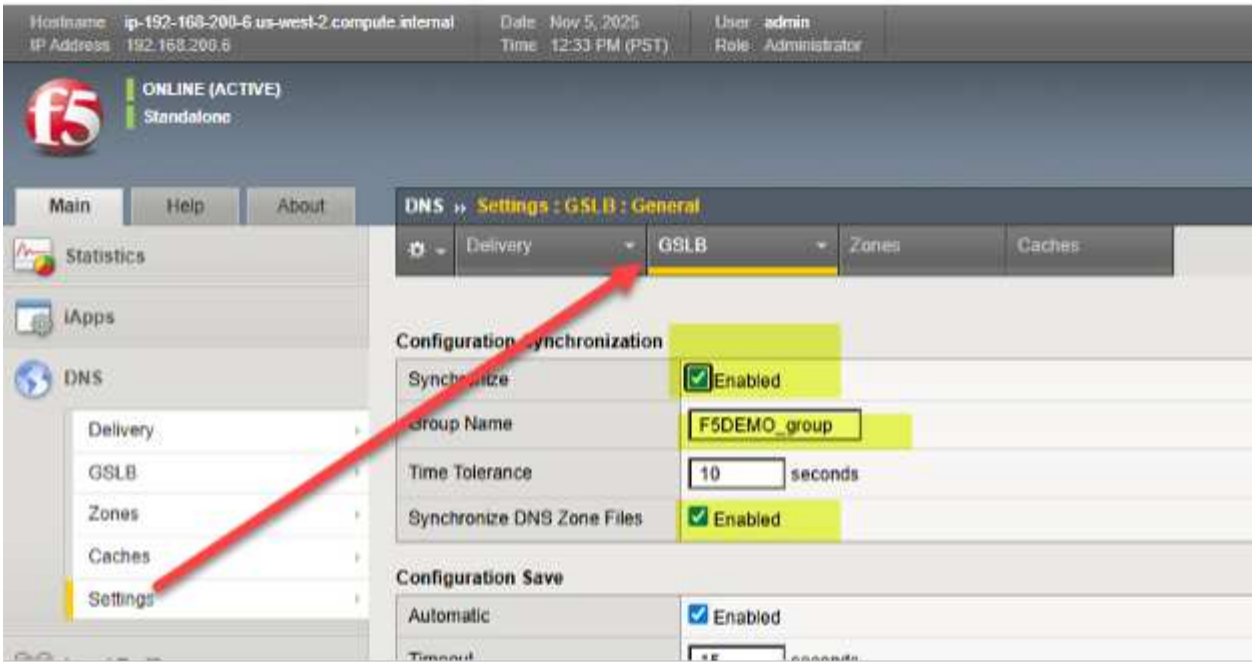
BIG-IP DNS - 初始設定入門指南

BIG-IP 設備完成至少初始設定後，使用 Web 瀏覽器登入 TMUI（BIG-IP GUI）介面，然後選擇「系統」→「資源配置」。如前所述，請確保「全球流量（DNS）」模組已勾選並顯示已取得授權。請注意，如圖所示，「本地流量 (LTM)」通常可以配置在同一裝置上。

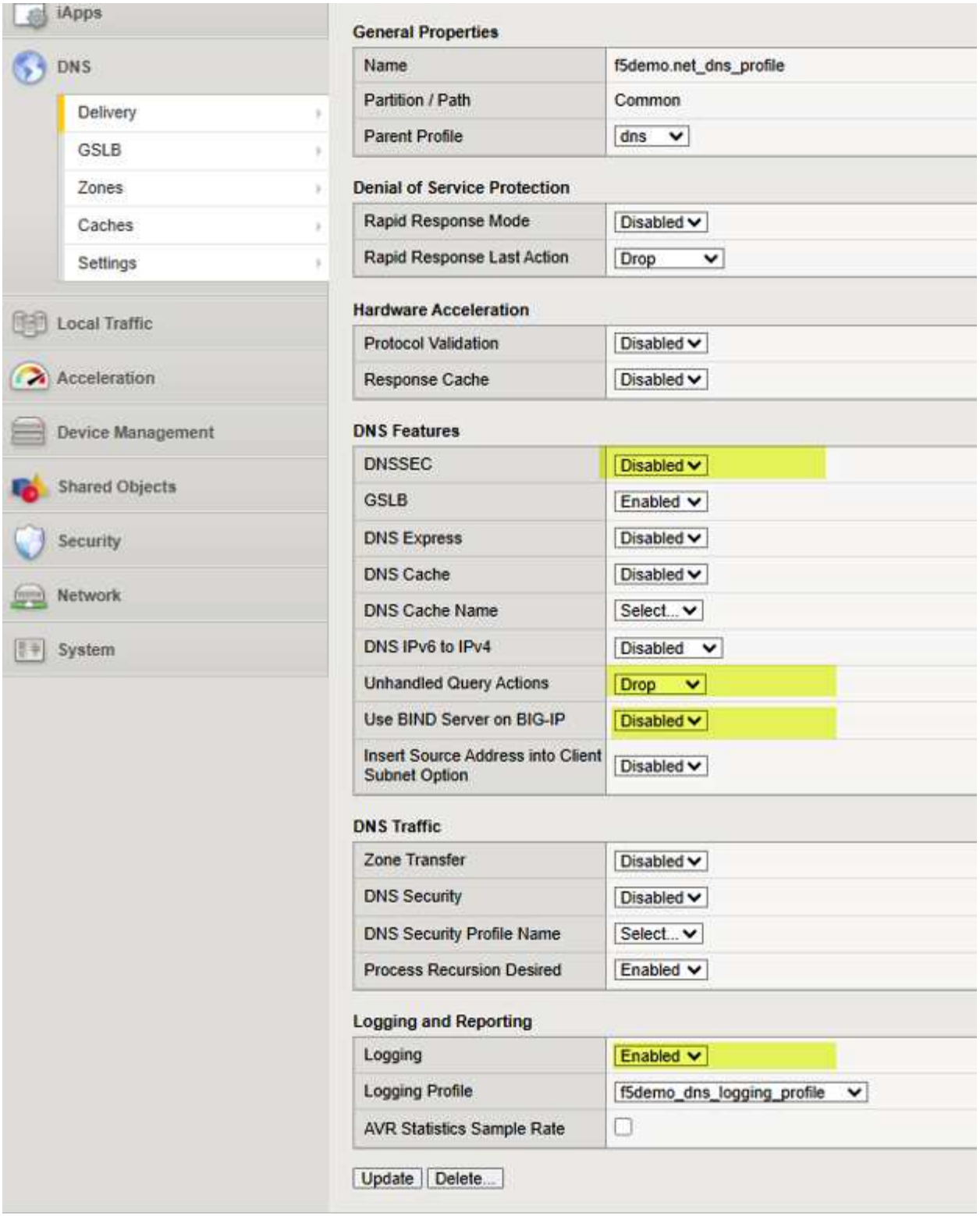


配置 **DNS** 協定基礎元素

StorageGRID站點的全域流量管理的第一步是選擇 DNS 選項卡，幾乎所有全域流量控制都會在此配置，然後選擇設定→ GLSB。啟用這兩個同步選項，並選擇一個將在參與的 BIG-IP 裝置之間共用的 DNS 群組名稱。



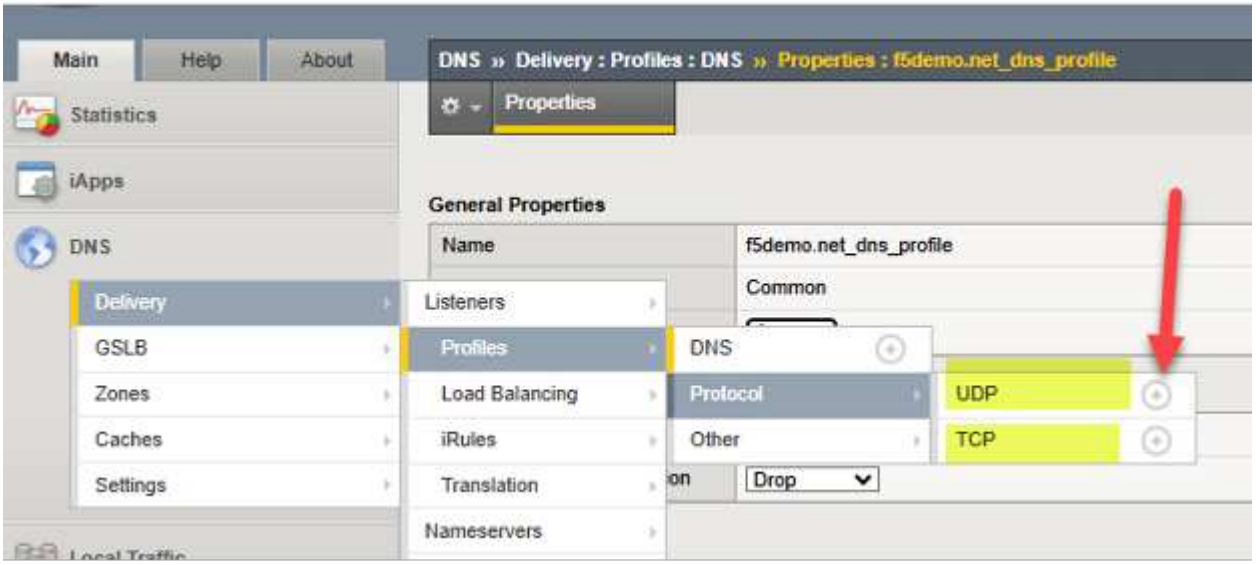
接下來，導覽至 DNS > 交付 > 設定檔 > DNS：建立並建立一個設定文件，該設定檔將控制您希望啟用或停用的 DNS 功能。如果您對產生特定 DNS 日誌感興趣，請參閱前面的 DNS 課堂指南連結。以下是一個可用的 DNS 設定檔範例，請注意四個高亮部分，它們代表重要的設定值。為了便於理解，每種可能的設定都在以下 F5 知識庫 (KB) 文章中進行了解釋。 "請按這裡"。



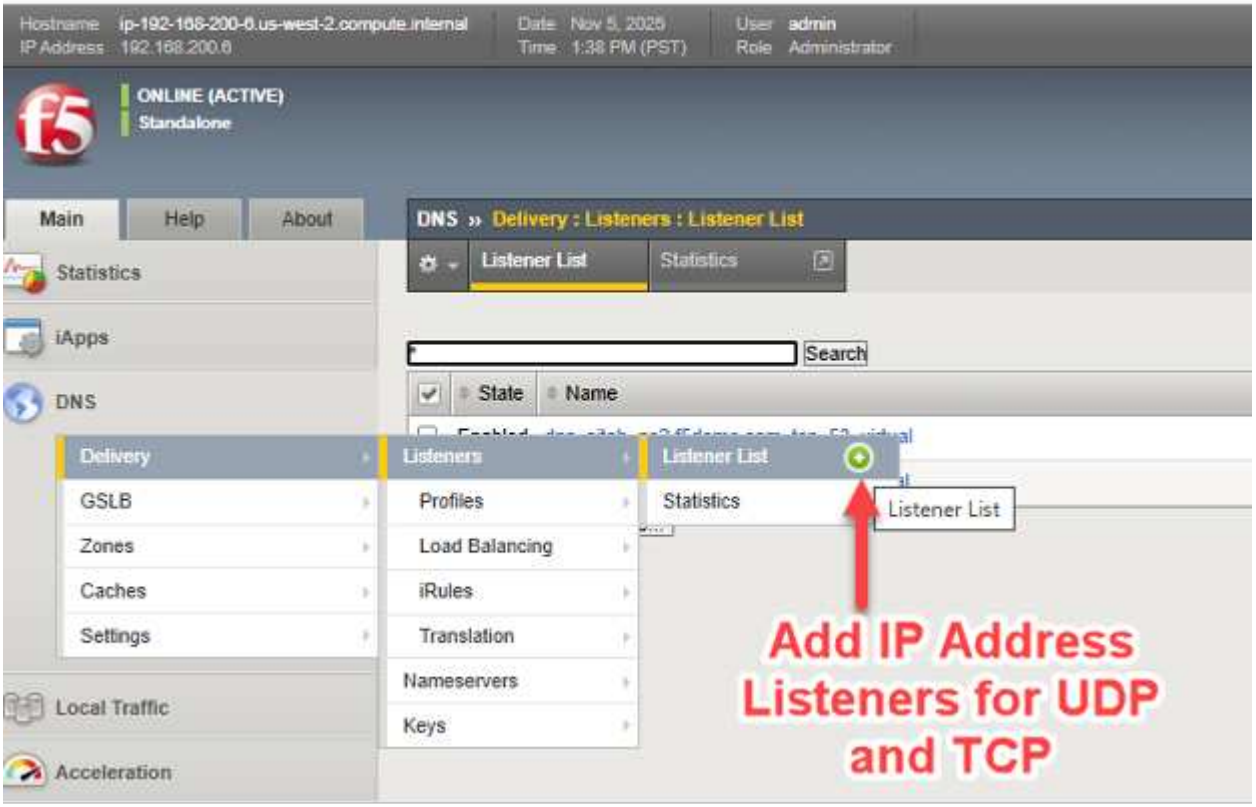
此時，我們可以透過建立的「設定檔」來調整 UDP 和 TCP 協定的特性，這兩個協定都可以承載涉及 BIG-IP 的 DNS 流量。只需為 UDP 和 TCP 建立一個新的設定檔即可。假設 DNS 流量將跨越 WAN 連結，一個好的做法是直接繼承在 WAN 環境中效能良好的 UDP 和 TCP 特性。要新增每個協議，只需點擊每個協議旁邊的“+”圖標，並將父設定檔設定為以下內容：

UDP → 使用“父”設定檔“udp_gtm_dns”

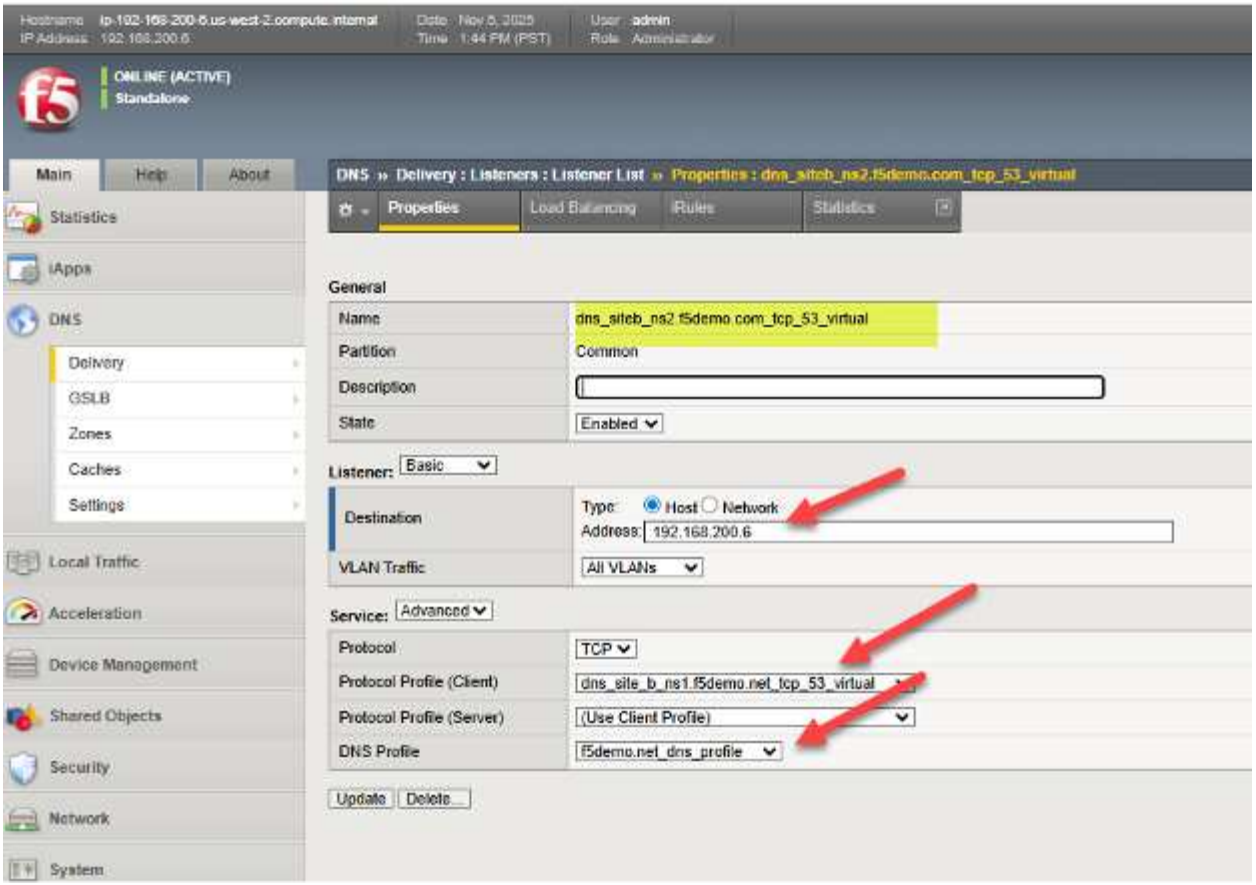
TCP → 使用“父”設定檔“f5-tcp-wan”



現在，我們只需要為涉及 BIG-IP DNS 的 UDP 和 TCP 流量分配一個 IP 位址。對於熟悉 BIG-IP LTM 的人來說，這本質上是建立 DNS 虛擬伺服器，而虛擬伺服器需要「監聽器」IP 位址。如圖所示，請依照箭頭指示建立 DNS/UDP 和 DNS/TCP 的監聽器/虛擬伺服器。



以下是來自即時 BIG-IP DNS 的範例，其中我們可以看到 TCP 虛擬伺服器監聽器設置，並可以看到它是如何將許多先前的步驟連結起來的。這包括引用 DNS 設定檔和協定 (TCP) 設定文件，以及設定 DNS 要使用的有效 IP 位址。與使用 BIG-IP 建立的所有物件一樣，使用有意義的名稱有助於識別物件是什麼，例如範例名稱中的 dns/siteb/TCP53。



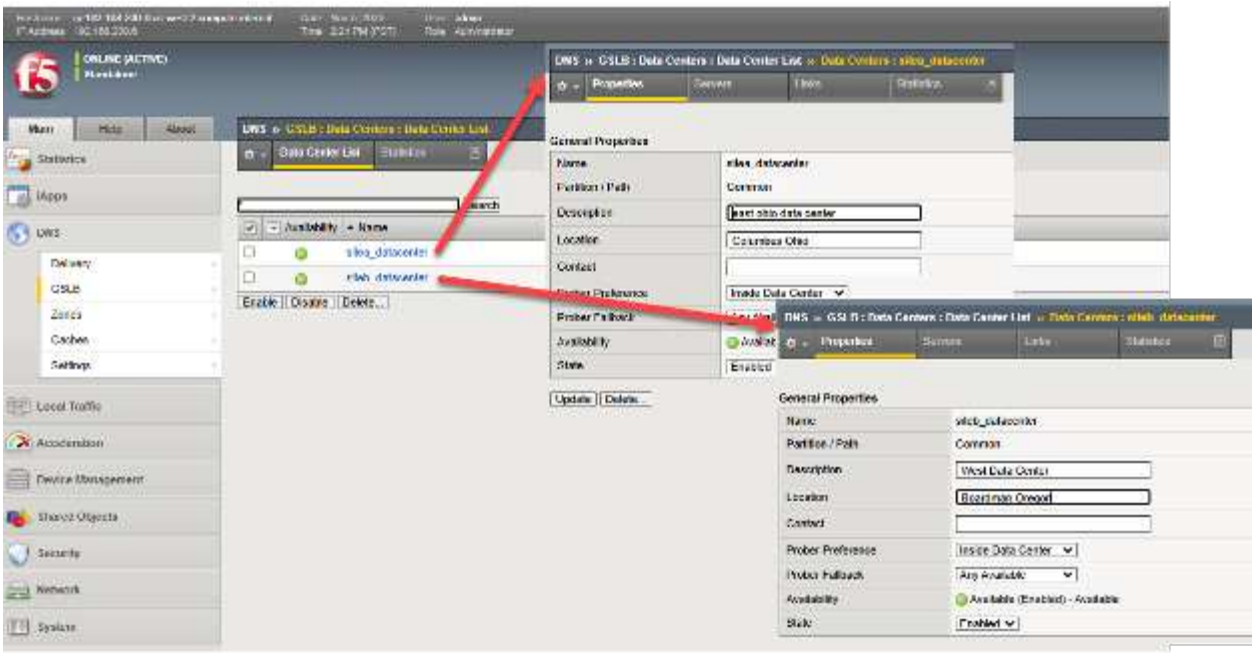
至此，啟用 DNS 模組的 BIG-IP 設備的初步設定步驟（通常是「一次性」設定步驟）就完成了。目前，我們已準備好過渡到使用我們的設備建立全球流量管理解決方案的具體細節，這當然將與StorageGRID站點的特性相關聯。

分四步驟完成資料中心站點建置與**BIG-IP**間通訊建立

第一步：建立資料中心

每個將容納由 BIG-IP LTM 進行本地負載平衡的節點叢集的站點都應該輸入到 BIG-IP DNS 中。這只需要在一個 BIG-IP DNS 上完成，因為我們正在建立一個 DNS 同步群組來支援流量管理，因此該配置將在群組的 DNS 成員之間共用。

透過 TMUI GUI，選擇 DNS > GSLB > 資料中心 > 資料中心列表，並為每個StorageGRID網站建立一個條目。如果使用與圖 1 一致的網路設置，DNS 設備位於其他非StorageGRID站點，除了儲存站點之外，還要為這些站點新增資料中心。在本例中，站點 a 和 b 分別創建在俄亥俄州和俄勒岡州，BIG-IP 是雙 DNS 和 LTM 設備。



第二步：建立伺服器（解決方案中所有 **BIG-IP** 設備清單）

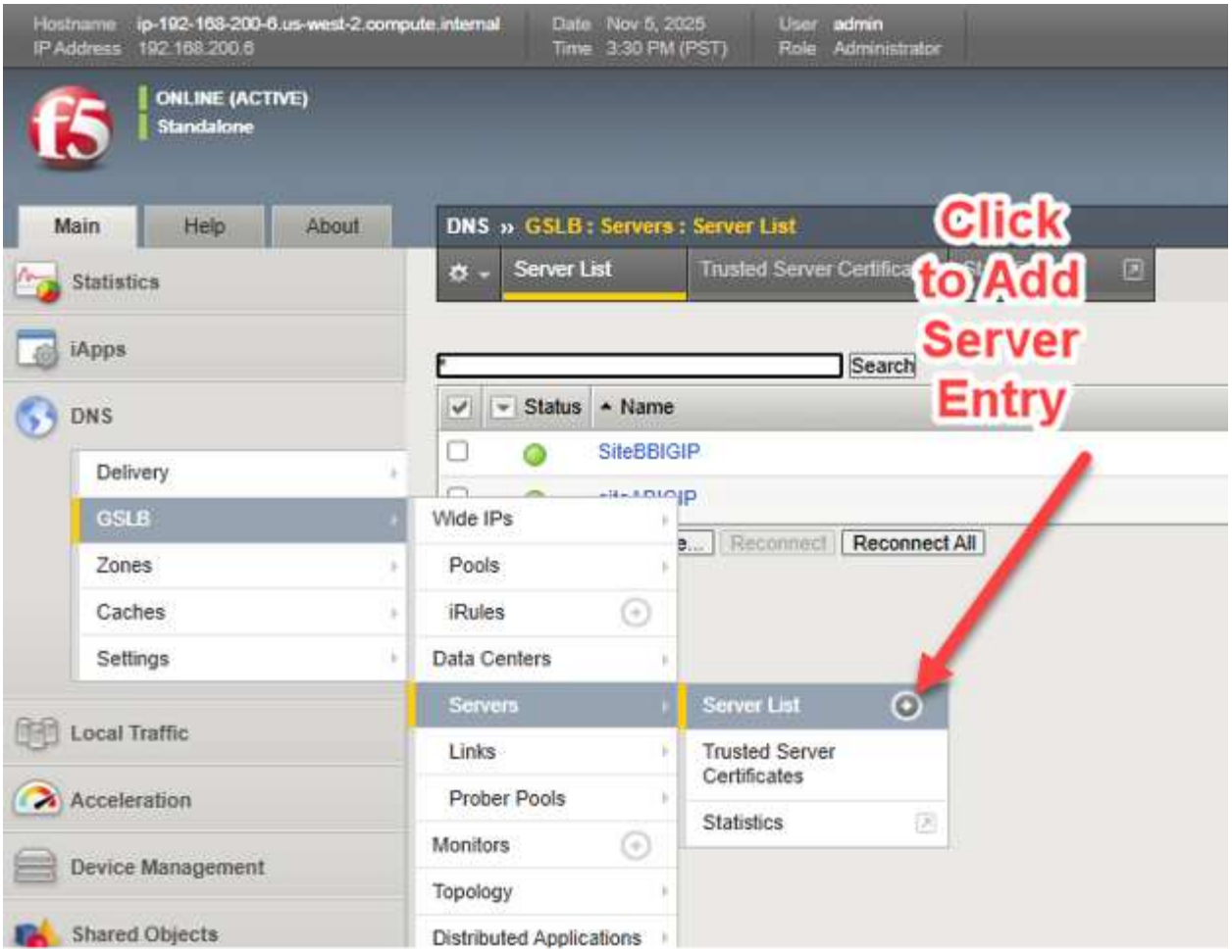
現在我們已準備好將各個StorageGRID站點叢集連接到 BIG-IP DNS 設定。回想一下，每個站點的 BIG-IP 設備將透過配置虛擬伺服器來實際進行 S3 流量的負載平衡，這些虛擬伺服器將“前端”可達 IP 位址/連接埠綁定到一組後端儲存節點設備的“池”，使用“後端”IP 位址/連接埠。

例如，如果池中的所有儲存節點因管理原因（例如網站停用）或因即時健康檢查失敗而意外離線，則流量將透過變更 DNS 查詢回應定向到其他網站。

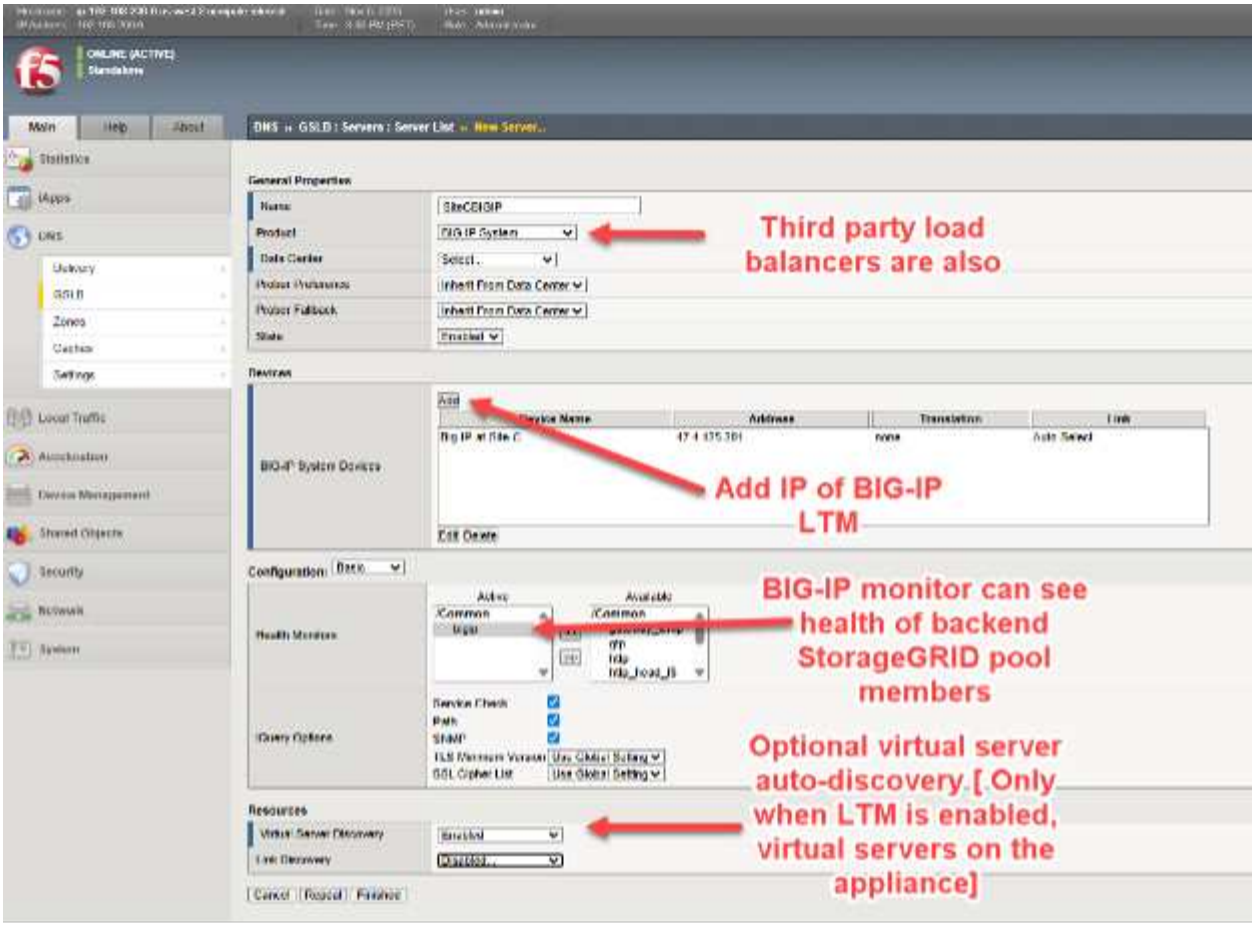
若要將 StorageGrid 網站（特別是本機虛擬伺服器）與每個裝置上的 BIG-IP DNS 配置關聯起來，只需設定一次即可。接下來，所有 BIG-IP DNS 設備都將進行同步設定。

簡單來說，我們將建立一個列表，稱為伺服器列表，其中包含我們所有的 BIG-IP 設備，無論它們是否獲得了 DNS、LTM 或 DNS 和 LTM 的許可。清單完成後，該主清單將與所有 BIG-IP DNS 設備同步。

在一台已取得 BIG-IP DNS 授權的裝置上，選擇 DNS > GSLB > 伺服器 > 伺服器列表，然後選擇新增按鈕 (+)。



在新增每個 BIG-IP 時，四個關鍵要素包括：* 從產品下拉選單中選擇 BIG-IP，雖然也可以使用其他負載平衡器，但通常缺乏在每個站點後端節點健康狀況惡化時的即時可見性和響應能力。* 新增 BIG-IP DNS 設備的 IP 位址。通常情況下，首次新增 BIG-IP DNS 設備時，位址將是目前可透過 GUI 存取的設備，以後新增的設備將是解決方案中的其他設備。* 選擇健康監視器，當新增的負載平衡器是 BIG-IP 設備時，請務必使用“BIG-IP”，以便考慮後端StorageGRID節點的健康狀況。* 如果設備是雙 DNS/LTM 設備，則可以選擇請求虛擬伺服器自動發現。

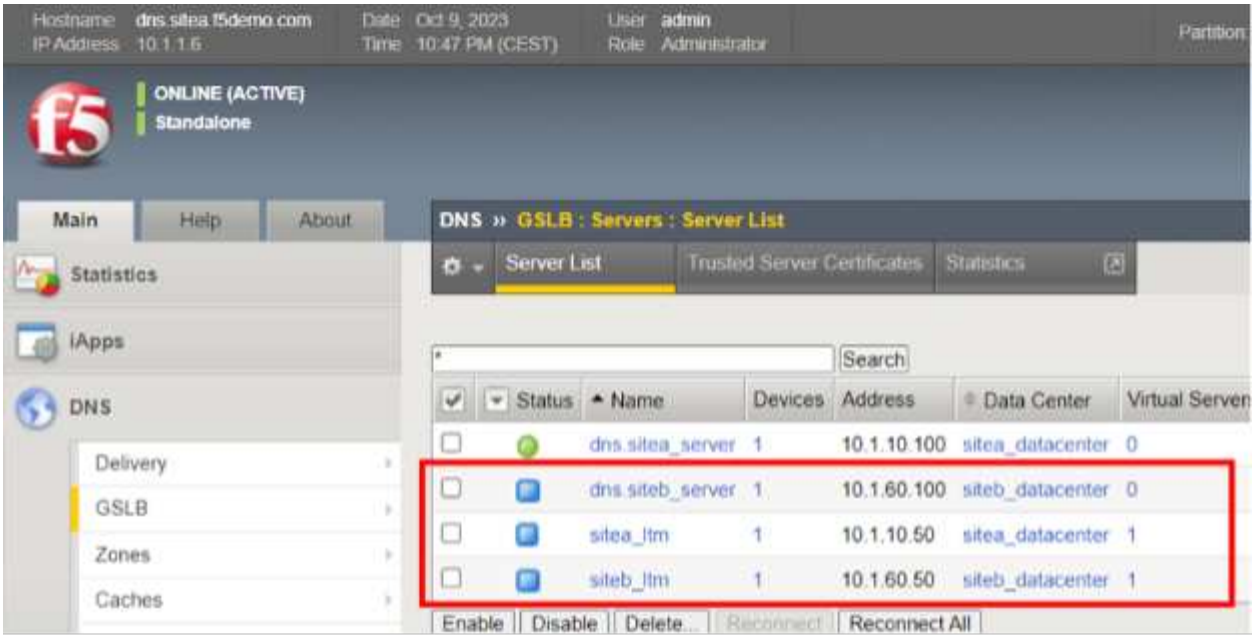


在某些情況下，例如瞬態網路問題或網路位置之間的防火牆 ACL 規則，在此階段新增遠端設備時，虛擬伺服器發現可能不會顯示已設定 LTM 的遠端設備的條目。在這種情況下，新增設備（「伺服器」）後，可以按照以下指示手動新增虛擬伺服器。如果新增的是僅用於 DNS 的 BIG-IP 設備，則不會發現或向該設備新增任何虛擬伺服器。

我們需要在所有站點上為解決方案中的每個設備新增這些伺服器項目，包括 BIG-IP DNS 設備、BIG-IP LTM 設備以及任何同時承擔 DNS 和 LTM 雙重角色的設備。

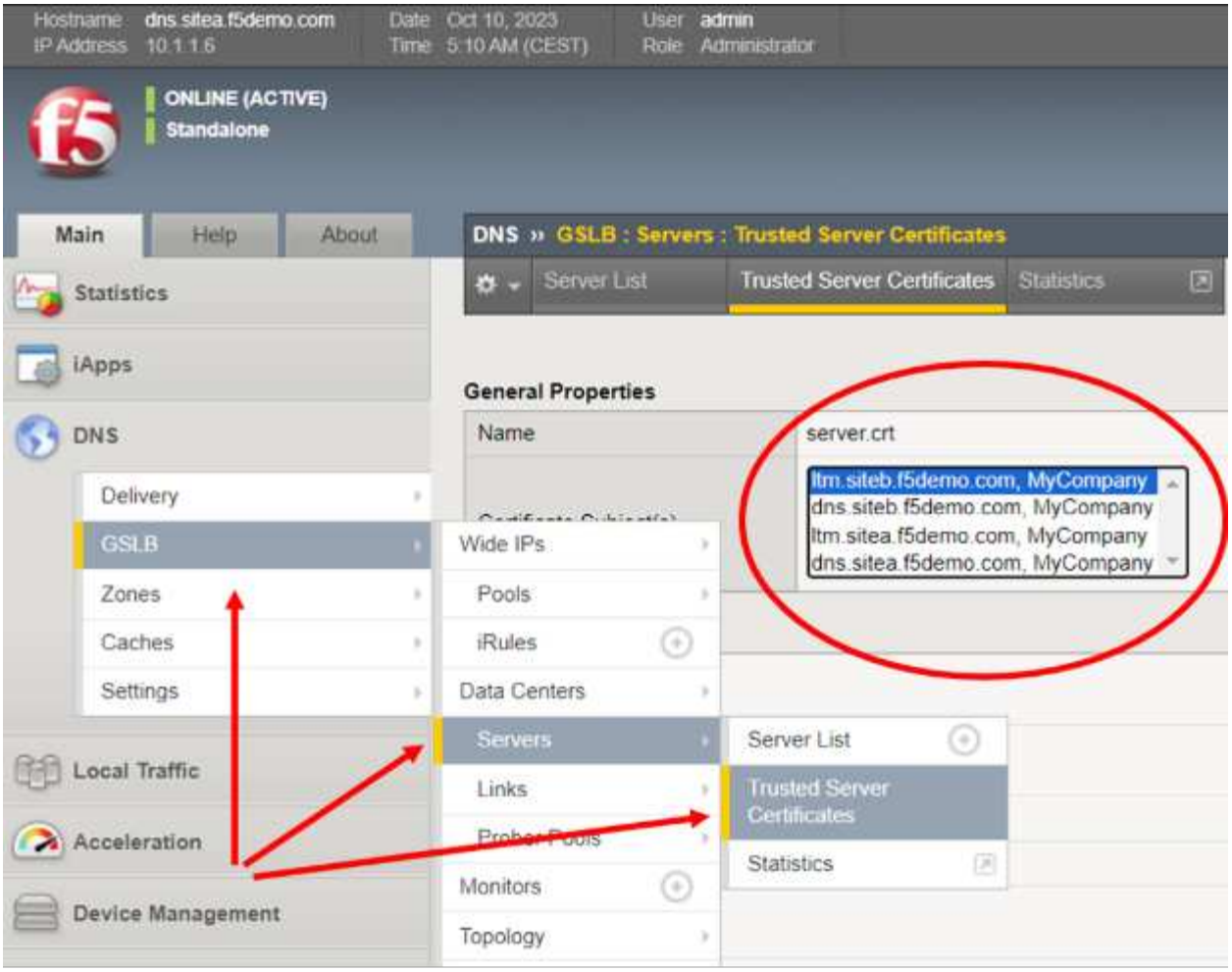
第三步：在所有**BIG-IP**設備之間建立信任

在以下範例中，新增了四台設備作為伺服器，它們分佈在兩個網站。請注意，每個站點都有專用的 BIG-IP DNS 和 BIG-IP LTM。但是，除了目前登入的裝置之外，所有其他裝置的「狀態」欄位中都顯示藍色圖示。這意味著尚未與其他 BIG-IP 設備建立信任關係。



若要新增信任，請使用 SSH 連線到剛剛透過 GUI 輸入設定詳細資訊的 BIG-IP，並使用「root」帳戶存取 BIG-IP 命令列介面。在提示符號下發出以下單一命令：*bigip_add*

“bigip_add”指令從目標BIGIP設備拉取管理證書，用於在叢集中的GSLB伺服器之間建立加密的「iQuery」通道。預設情況下，iQuery使用TCP連接埠4353運行，它是一種心跳機制，使BOG-IP DNS成員保持同步狀態。它在加密通道中使用了 xml 和 gzip。當不帶任何選項執行「bigip_add」時，該命令將使用目前使用者名稱連接到端點，對 GSLB 伺服器清單中的所有 BIGIP 設備運行。為了快速檢查是否成功，只需返回 BIG-IP GUI 並確認所有伺服器的憑證現在都列在顯示的下拉式選單中即可。



第四步：將所有 **BIG-IP DNS** 設備同步到 **DNS** 群組

最後一步將允許僅使用單一裝置的 TMUI GUI 即可完全設定所有 BIG-IP DNS 設備。例如，如果有兩個StorageGRID站點，這表示現在需要使用 SSH 存取另一個站點的 BIG-IP DNS 的命令列。以 root 使用者身分連線後，並確保防火牆策略/ACL 允許兩個 BIG-IP DNS 裝置透過 TCP 連接埠 22 (SSH)、443 (HTTPS) 和 4354 (F5 iQuery 協定) 進行通信，然後在提示字元下執行下列命令：_gtm_add <

此時，所有進一步的 DNS 配置工作都可以在已新增至該群組的任何 BIG-IP DNS 裝置上執行。對於僅支援 LTM 的裝置成員，無需應用上述命令 gtm_add。只有支援 DNS 的裝置才需要此命令加入同步 DNS 群組。

建立資料中心站點並建立**BIG-IP**間通信

至此，建立底層、健康的 BIG-IP DNS 設備群組的所有步驟均已完成。現在我們可以繼續建立指向我們在每個StorageGRID資料中心公開的分散式 Web/S3 服務的名稱、FQDN。

這些名稱稱為“廣域 IP 位址”，簡稱 WIP，它們是具有 DNS A 資源記錄的普通 DNS FQDN。然而，它們並不像傳統的 A 資源記錄那樣指向伺服器，而是在內部指向 BIG-IP 虛擬伺服器集區。每個池都可以單獨由一個或多個虛擬伺服器組成。請求 IP 位址進行名稱解析的 S3 用戶端將收到政策選擇的最佳StorageGRID網站上的 S3 虛擬伺服器的位址。

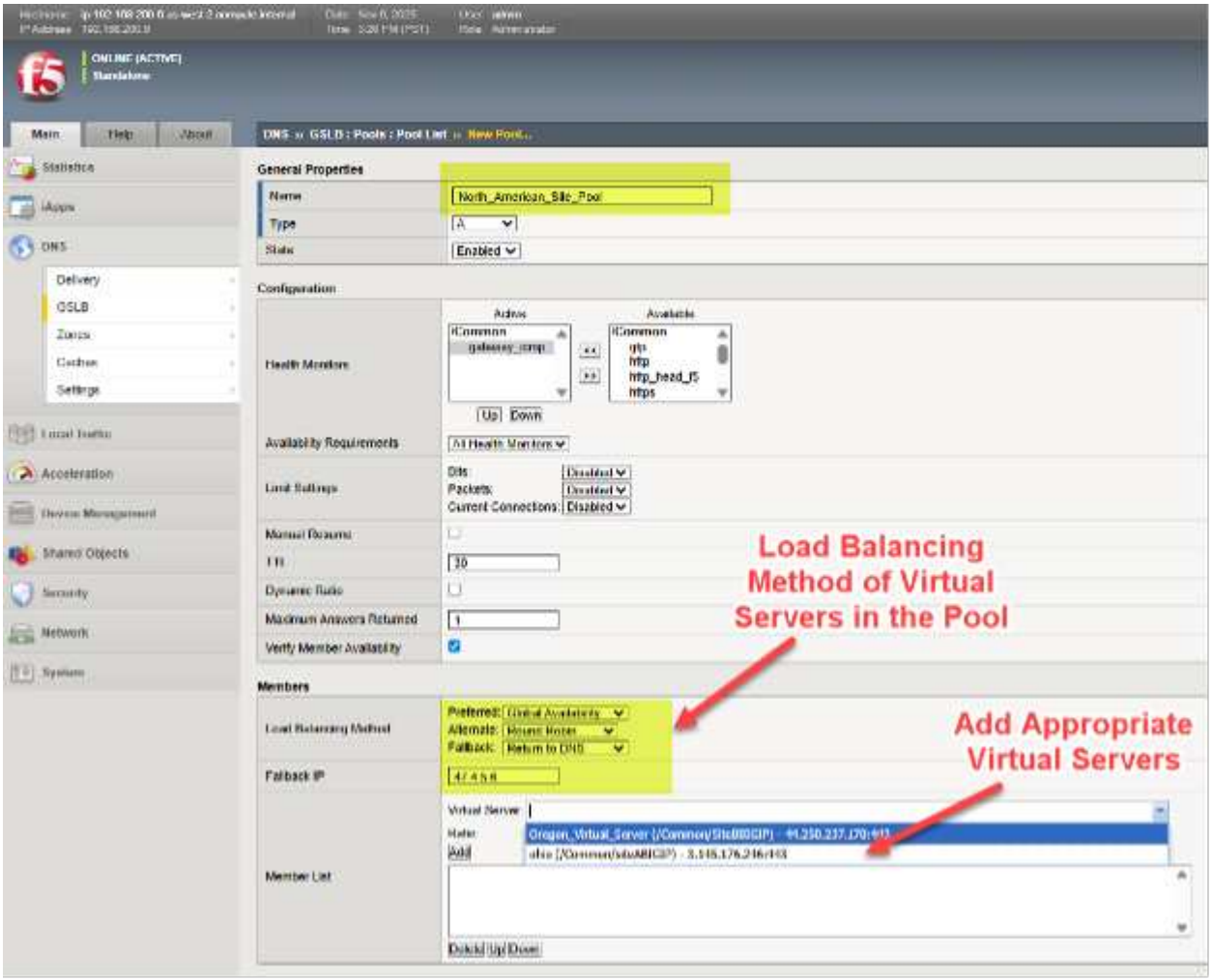
廣域**IP**、**IP**池和虛擬伺服器簡述

舉一個簡單的虛構例子，名稱 **storage.quantumvault.com** 的 WIP 可能會將 BIG-IP DNS 解決方案與兩個潛在的虛擬伺服器池連接起來。第一個池子可能由北美的 4 個地點組成；第二個池子可能由歐洲的 3 個地點組成。

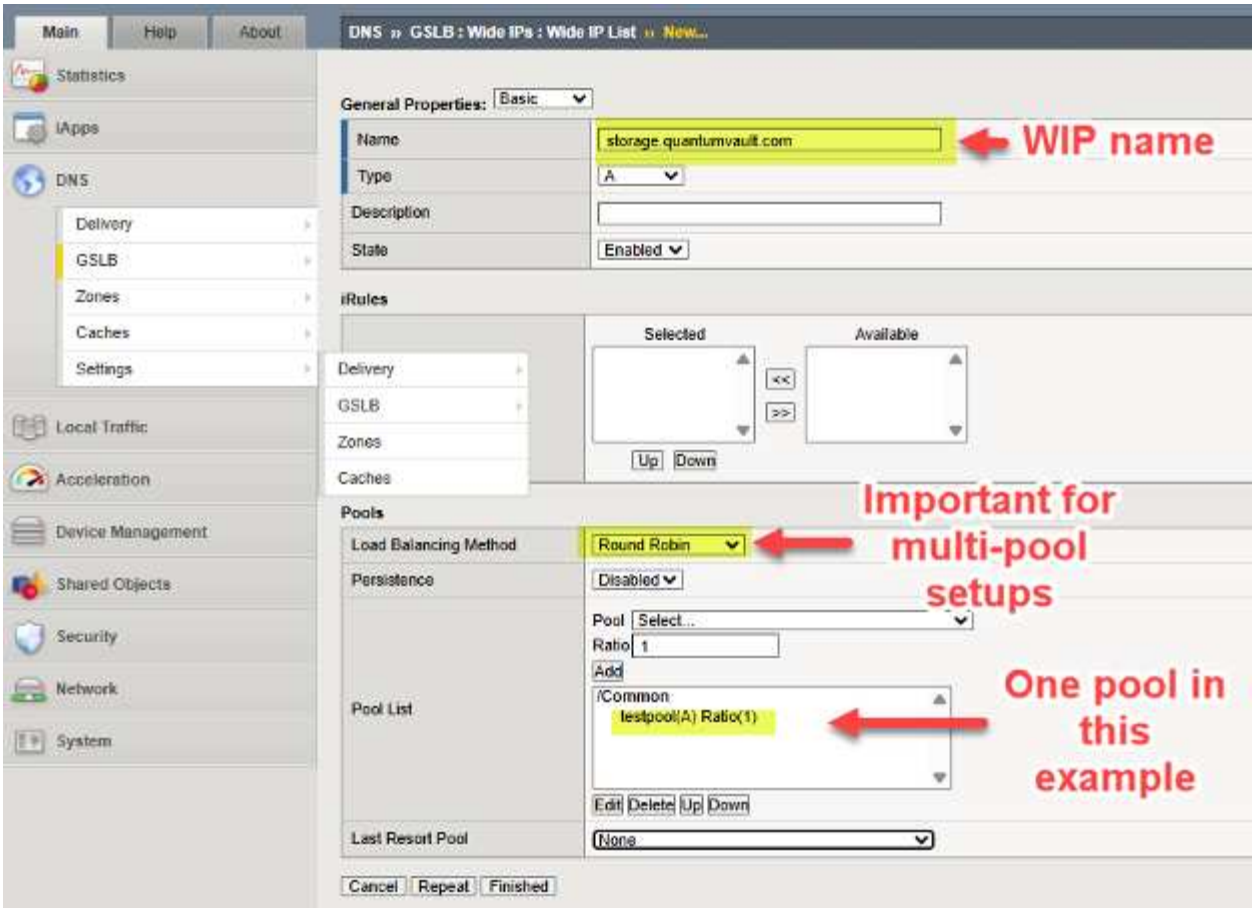
選定的池子可能是透過一系列政策決定得出的，也許可以使用 5:1 的簡單比例，將大部分流量導向北美StorageGRID站點。更有可能的是，基於拓撲結構的選擇，例如，將所有來自歐洲的 S3 流量定向到歐洲站點，而將世界其餘的 S3 流量定向到北美資料中心。

一旦 BIG-IP DNS 確定了池，假設選擇了北美池，則傳回用於解析 storage.quantumvault.com 的實際 DNS A 資源記錄可以是 BIG-IP LTM 在北美 4 個站點中支援的 4 個虛擬伺服器中的任何一個。同樣，具體選擇取決於策略，存在簡單的「靜態」方法，例如輪詢；而更高級的「動態」選擇，例如使用效能探針來測量每個網站從本地 DNS 解析器的延遲，則保留並用作網站選擇的標準。

若要在 BIG-IP DNS 上設定虛擬伺服器池，請依照功能表路徑 **DNS > GSLB > Pools > Pool List > Add (+)** 進行操作。在這個例子中，我們可以看到各種北美虛擬伺服器被加入到池中，並且選擇此池時，首選的負載平衡方法是分層選擇的。



我們將 WIP（廣域 IP），也就是我們的服務名稱（將透過 DNS 解析），依照 DNS > GSLB > 廣域 IP > 廣域 IP 清單 > 建立 (+) 的步驟新增至部署。在下面的範例中，我們提供了一個支援 S3 的儲存服務的範例 WIP。



調整 **DNS** 以支援全球流量管理

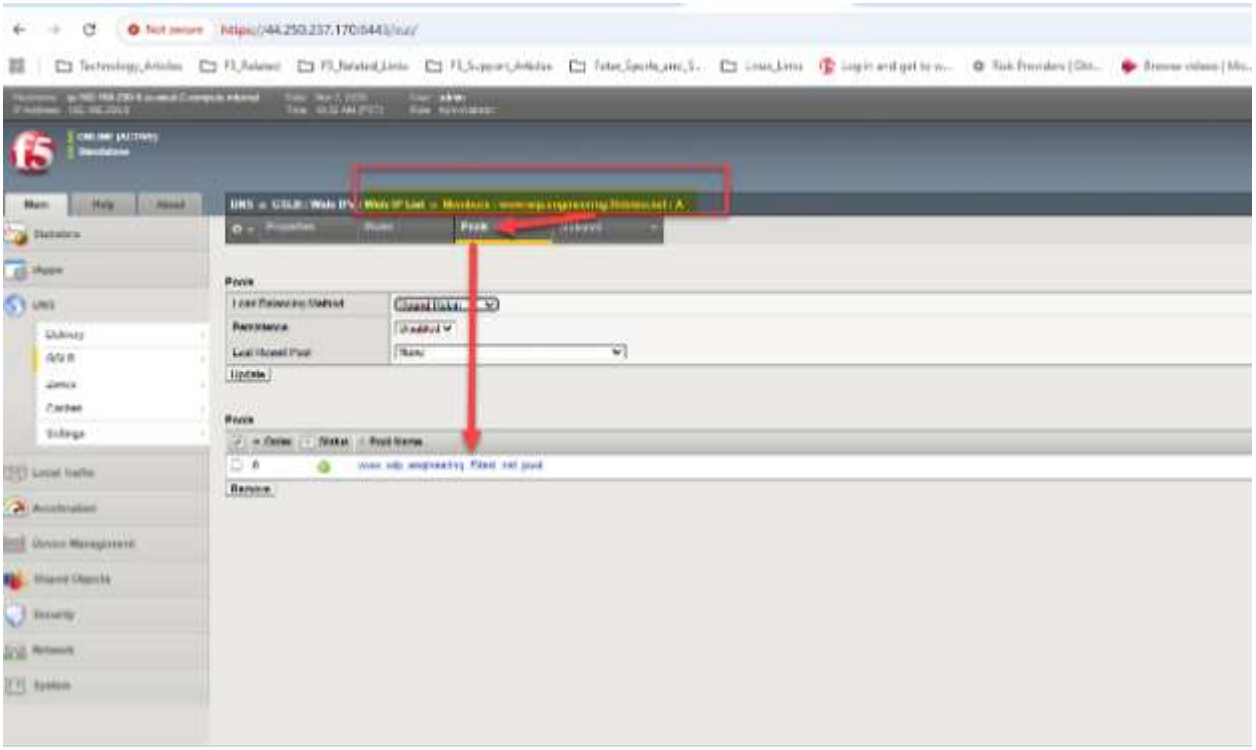
目前，我們所有的底層 BIG-IP 設備都已準備好執行 GSLB（全域伺服器負載平衡）。我們只需要調整並指派用於 S3 流量的名稱，即可利用此解決方案。一般做法是將企業現有 DNS 網域的一部分委託給 BIG-IP DNS 控制。也就是說，要「劃分」出一部分名稱空間，即一個子網域，並將該子網域的控制權委託給 BIG-IP DNS 設備。從技術上講，這是透過確保 BIG-IP DNS 設備在企業 DNS 中具有 A DNS 資源記錄 (RR)，然後將這些名稱/位址設定為委派網域的名稱伺服器 (NS) DNS 資源記錄來實現的。

如今企業維護 DNS 的方式有很多種，其中一種方法就是完全託管的解決方案。例如，透過 Windows Server 2025 執行和管理 DNS 就是這種情況。企業也可以採用另一種方法，就是利用 AWS Route53 或 Squarespace 等雲端 DNS 供應商。

以下範例純屬虛構，僅供參考。我們有StorageGRID支援透過 S3 協定對物件進行讀取和寫入，現有域由 AWS Route53 管理，現有範例域為 f5demo.net。

我們希望將子網域 engineering.f5demo.net 指派給 BIG-IP DNS 設備，以實現全球流量管理。為此，我們為 engineering.f5demo.net 建立一個新的 NS（名稱伺服器）資源記錄，並將其指向 BIG-IP DNS 裝置名稱清單。在我們的範例中，我們有兩個 BIG-IP DNS 設備，因此我們為它們建立了兩個 A 資源記錄。

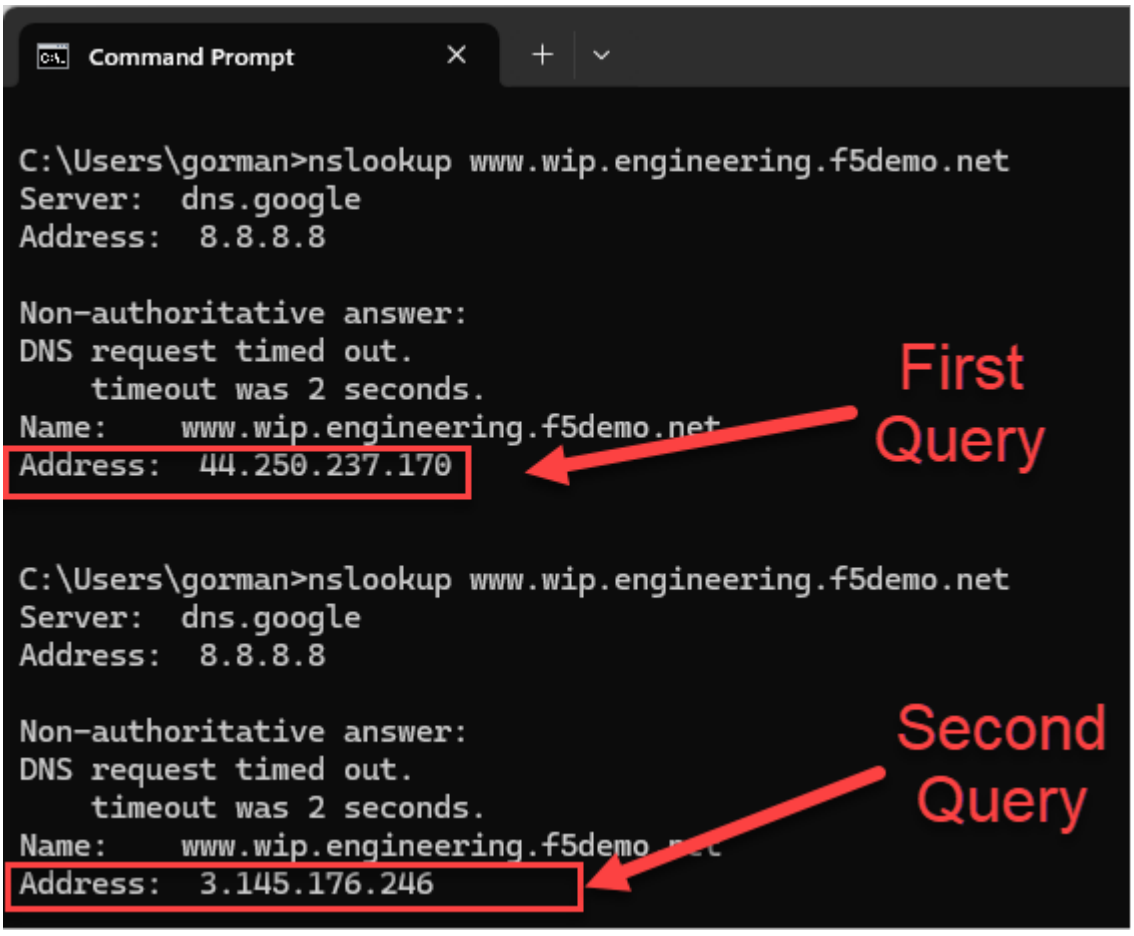
現在，我們以 BIG-IP DNS 為例，設定一個廣域 IP (WIP)。由於 DNS 使用群組同步，我們只需要使用一台裝置的 GUI 進行調整。在 BIG-IP DNS GUI 中，前往 **DNS > GSLB >** 廣域 **IP >** 廣域 **IP** 清單 **(+)**。回想一下，在傳統的 DNS FQDN 設定中，需要輸入一個或多個 IPv4 位址，而在我們的例子中，我們只需指向一個或多個StorageGRID虛擬伺服器集區。



在我們的範例中，我們在俄亥俄州和俄勒岡州網站都設有通用的 Web HTTPS 伺服器。透過簡單的「輪詢」方法，我們應該能夠看到全域 DNS 回應對 *www.wip.engineering.f5demo.net* 的 A 資源記錄映射的查詢，其中包含兩個虛擬伺服器 IP。

可以使用網頁瀏覽器進行簡單的測試，或者，對於使用StorageGRID 的S3，可以使用 S3Browser 等圖形工具進行測試。由於我們在池內選擇了輪詢調度，因此每次 DNS 查詢都會將池中的下一個資料中心網站用作後續流量的目標。

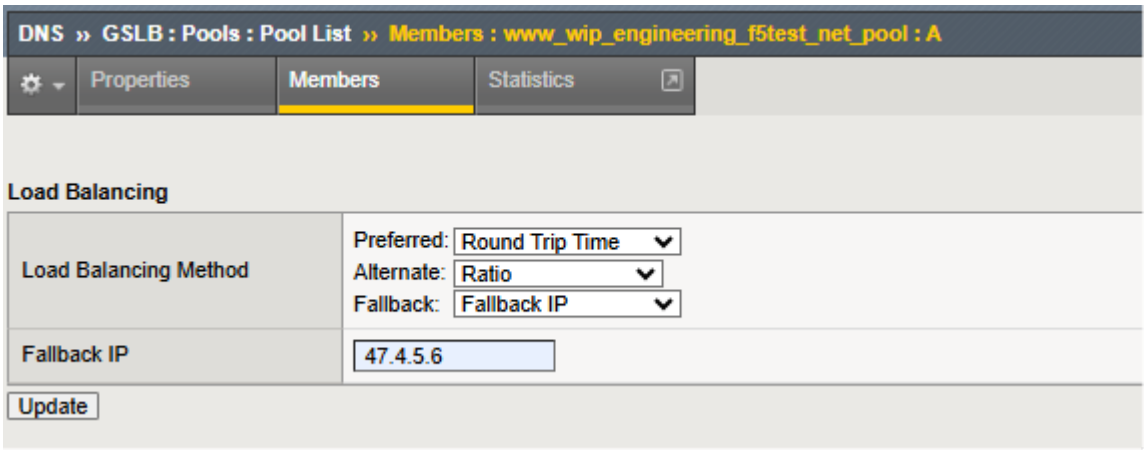
在我們的範例設定中，我們可以使用 dig 或 nslookup 快速產生一系列兩個 DNS 查詢，以確保 BIG-IP DNS 確實在進行輪詢負載平衡，讓兩個網站都能隨著時間的推移接收流量。



建議探索更高級的技術

眾多可行方法之一，是使用「全域可用性」模式，而不是上面給出的簡單「輪詢」範例。透過全域可用性，可以將流量定向到池的順序，或單一池中的虛擬伺服器。這樣一來，所有 S3 流量預設都可以導向到例如紐約市的站點。

如果健康檢查顯示此網站的StorageGRID節點可用性有問題，則流量屆時可能會被導向到聖路易斯。如果聖路易斯出現健康問題，法蘭克福的站點可以轉而開始接收 S3 讀取或寫入交易。因此，全球可用性是提高 S3 StorageGRID整體解決方案彈性的一種方法。另一種方法是混合搭配負載平衡法，採用分層法。



在這個範例中，「動態」選項是已配置池中網站的首選負載平衡方式。在所示的範例中，持續測量方法採用主動探測本機 DNS 解析器效能的方法，這是網站選擇的催化劑。如果這種方法不可行，則可以根據分配給每個站點的比例來選擇各個站點。按比例計算，規模更大、頻寬更高的StorageGRID站點可以接收比規模較小的站點更多的 S3 事務。最後，作為災難復原方案，如果池中的所有站點都發生故障，則指定的備用 IP 將用作最後的備選站點。BIG-IP DNS 中比較有趣的負載平衡方法之一是“拓撲”，它觀察 DNS 查詢的傳入來源（即 S3 用戶的本機 DNS 解析器），並利用網際網路拓撲資訊從池中選擇看似「最近」的網站。

最後，如果網站遍布全球，則值得考慮使用 F5 BIG-IP DNS 手冊中詳細討論的動態「探測」技術。透過偵測，可以監控頻繁的 DNS 查詢來源，例如，流量通常使用相同本機 DNS 解析器的企業對企業合作夥伴。可以從全球每個站點的 BIG-IP LTM 啟動 BIG-IP DNS 探測，以大致確定哪個潛在站點可能為 S3 交易提供最低延遲。因此，來自亞洲的流量可能由亞洲的StorageGRID站點提供比位於北美或歐洲的站點更好的服務。

結論

F5 BIG-IP 與NetApp StorageGRID的整合解決了與跨多個站點的資料可用性和一致性相關的技術挑戰，並優化了 S3 事務路由。部署此解決方案可增強儲存彈性、效能和可靠性，使其成為尋求強大、可擴展和靈活的儲存基礎架構的企業的理想選擇。

如需了解更多信息，請訪問此處查看 F5 官方的 BIG-IP DNS 文件。 "關聯"。還可以找到一份課堂風格的指導手冊，其中包含範例設定的逐步說明。 "請按這裡"。

Datadog SNMP組態

_ 作者： Aron Klein_

設定Datadog以收集StorageGRID 不完整的SNMP指標和陷阱。

設定Datadog

Datadog是一套監控解決方案、提供指標、視覺化和警示功能。下列組態是以Linux代理程式7.43.1版實作於Ubuntu 22.04.1主機上、部署於StorageGRID 本機的整個作業系統上。

Datadog設定檔和Traps檔案是從StorageGRID 無法還原的mib檔案產生的

Datadog提供一種方法、可將產品mib檔案轉換成對應SNMP訊息所需的datadog參考檔案。

此支援Datadog Trap解析度對應的支援程序檔會依照所找到的指示產生StorageGRID "請按這裡"。+將此檔案放在/etc/datadog-agent/conf.d/snmp.d/straps_db/+中

- "下載陷阱yaml檔案" +
  - * md5 checksum * 42e27e4210719945a46172b98c379517 +
  - * sha256 checksum * d0fe5c8e6ca3c902d054f85b70a85f928cba8b7c76391d356f05d2cf73b6887+

此支援Datadog指標對應的支援資料檔yaml檔案是依照所找到的指示產生StorageGRID "請按這裡"。+將此檔案放在/etc/datadog-agent/conf.d/snmp.d/profile/+中

- "下載設定檔yaml檔案" +
  - * md5 checksum * 72bb7784f4801adda4e0c3ea77df19a+
  - * sha256 checksum * b6b7fadd33063422a8bb8e39b3ead8ab383449ee0229926eadc85f0087b8cee +

用於度量的**SNMP Datadog**組態

可透過兩種方式來管理設定用於度量的SNMP。您可以設定自動探索、方法是提供包含StorageGRID 該系統的網路位址範圍、或定義個別裝置的IP。根據所做的決定、組態位置會有所不同。自動探索是在datadog代理yaml檔案中定義。在SNMP組態yaml檔案中設定明確的裝置定義。以下是相同StorageGRID 的支援系統的各個範例。

自動探索

組態位於/etc/datadog-agent/datadog.yaml

```
listeners:
  - name: snmp
snmp_listener:
  workers: 100  # number of workers used to discover devices concurrently
  discovery_interval: 3600  # interval between each autodiscovery in
seconds
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
  configs:
    - network_address: 10.0.0.0/24  # CIDR subnet
      snmp_version: 2
      port: 161
      community_string: 'st0r@gegrid'  # enclose with single quote
      profile: netapp-storagegrid
```

個別裝置

/etc/datadog-agent/conf.d/snmp.d/conf.yaml

```
init_config:
  loader: core  # use core check implementation of SNMP integration.
recommended
  use_device_id_as_hostname: true  # recommended
instances:
- ip_address: '10.0.0.1'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'  # enclose with single quote
- ip_address: '10.0.0.2'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
- ip_address: '10.0.0.3'
  profile: netapp-storagegrid
 community_string: 'st0r@gegrid'
- ip_address: '10.0.0.4'
  profile: netapp-storagegrid
  community_string: 'st0r@gegrid'
```

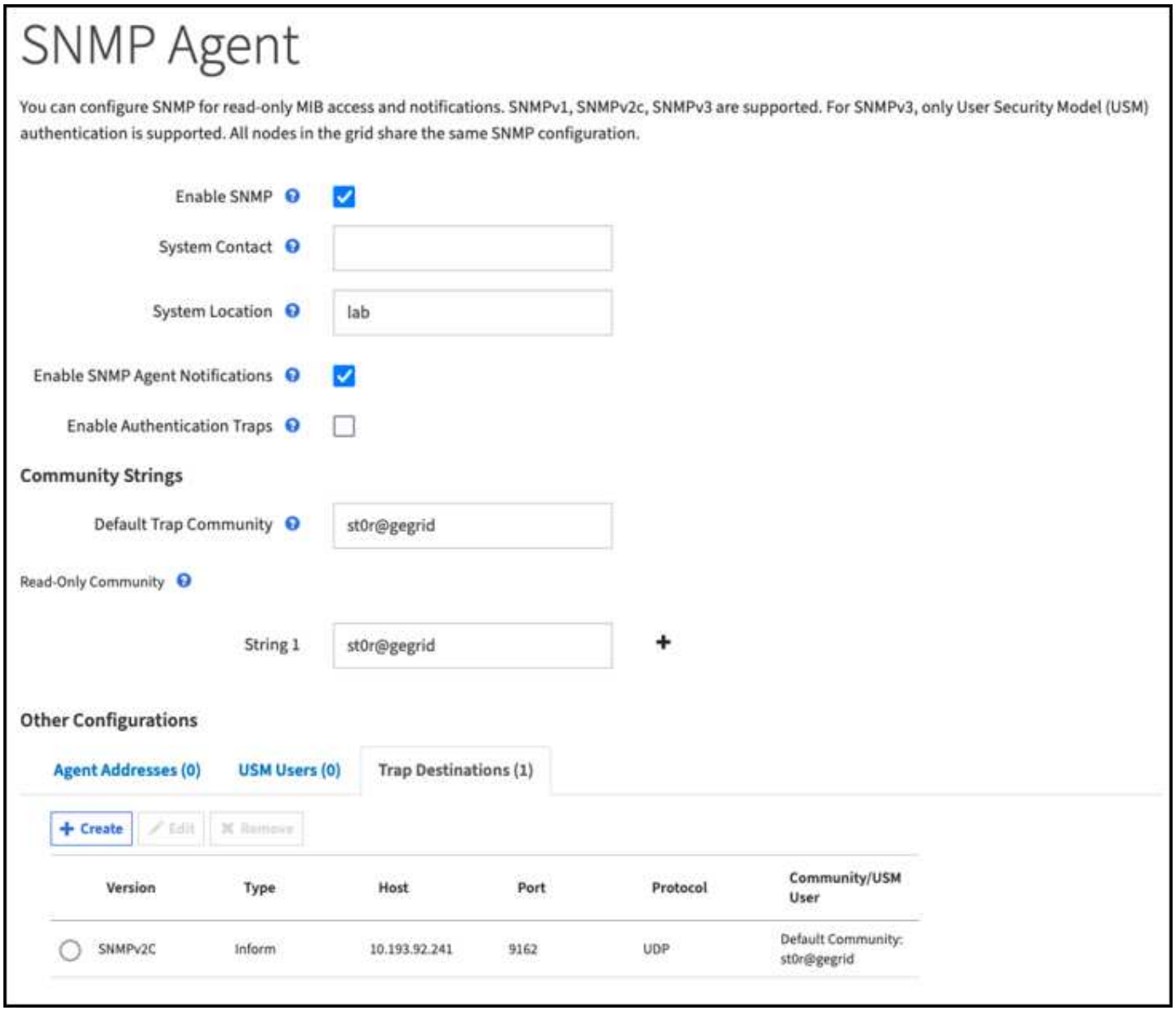
陷阱的**SNMP**組態

SNMP設陷的組態是在datadog組態yaml檔案/etc/datadog-agent/datadog.yaml中定義

```
network_devices:
  namespace:  # optional, defaults to "default".
  snmp_traps:
    enabled: true
    port: 9162 # on which ports to listen for traps
    community_strings: # which community strings to allow for v2 traps
      - st0r@gegrid
```

範例**StorageGRID** ：**SNMP**組態

您的S還原 系統中的SNMP代理程式StorageGRID 位於組態索引標籤「監控」欄下。啟用SNMP並輸入所需資訊。如果您要設定設陷、請選取「設陷目的地」、然後為包含設陷組態的Datadog代理主機建立目的地。



使用 rclone 在 StorageGRID 上移轉、放置及刪除物件

_ 作者： Siegfried HEPP 和 Aron Klein_

rclone 是免費的命令列工具和用戶端、適用於 S3 作業。您可以使用 rclone 在 StorageGRID 上移轉、複製及刪除物件資料。RClone 包含刪除貯體的功能、即使沒有清空時也能使用「清除」功能、如下例所示。

安裝並設定 rclone

若要在工作站或伺服器上安裝 rclone 、請從下載 "rclone.org"。

初始組態步驟

1. 執行組態指令碼或手動建立檔案、以建立 rclone 組態檔案。
2. 在此範例中、我會在 rclone 組態中使用 sgdemo 作為遠端 StorageGRID S3 端點的名稱。
   a. 建立組態檔 ~/.config/rclon/rclon.conf

```
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com
```

b. 執行 rclone 組態

rclone 組態

```
2023/04/13 14:22:45 NOTICE: Config file
"/root/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> sgdemo
```

```
Option Storage.
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Providers including AWS,
Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio,
SeaweedFS, and Tencent COS
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Better checksums for other remotes
   \ "hasher"
 7 / Box
   \ "box"
 8 / Cache a remote
   \ "cache"
 9 / Citrix Sharefile
   \ "sharefile"
10 / Compress a remote
   \ "compress"
11 / Dropbox
   \ "dropbox"
12 / Encrypt/Decrypt a remote
   \ "crypt"
13 / Enterprise File Fabric
   \ "filefabric"
14 / FTP Connection
```

```
   \ "ftp"
15 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
16 / Google Drive
   \ "drive"
17 / Google Photos
   \ "google photos"
18 / Hadoop distributed file system
   \ "hdfs"
19 / Hubic
   \ "hubic"
20 / In memory object storage system.
   \ "memory"
21 / Jottacloud
   \ "jottacloud"
22 / Koofr
   \ "koofr"
23 / Local Disk
   \ "local"
24 / Mail.ru Cloud
   \ "mailru"
25 / Mega
   \ "mega"
26 / Microsoft Azure Blob Storage
   \ "azureblob"
27 / Microsoft OneDrive
   \ "onedrive"
28 / OpenDrive
   \ "opendrive"
29 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore,
OVH)
   \ "swift"
30 / Pcloud
   \ "pcloud"
31 / Put.io
   \ "putio"
32 / QingCloud Object Storage
   \ "qingstor"
33 / SSH/SFTP Connection
   \ "sftp"
34 / Sia Decentralized Cloud
   \ "sia"
35 / Sugarsync
   \ "sugarsync"
36 / Tardigrade Decentralized Cloud Storage
   \ "tardigrade"
```

```
37 / Transparently chunk/split large files
   \ "chunker"
38 / Union merges the contents of several upstream fs
   \ "union"
39 / Uptobox
   \ "uptobox"
40 / Webdav
   \ "webdav"
41 / Yandex Disk
   \ "yandex"
42 / Zoho
   \ "zoho"
43 / http Connection
   \ "http"
44 / premiumize.me
   \ "premiumizeme"
45 / seafile
   \ "seafile"
```

```
Storage> 4
```

```
Option provider.
Choose your S3 provider.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 1 / Amazon Web Services (AWS) S3
   \ "AWS"
 2 / Alibaba Cloud Object Storage System (OSS) formerly Aliyun
   \ "Alibaba"
 3 / Ceph Object Storage
   \ "Ceph"
 4 / Digital Ocean Spaces
   \ "DigitalOcean"
 5 / Dreamhost DreamObjects
   \ "Dreamhost"
 6 / IBM COS S3
   \ "IBMCOS"
 7 / Minio Object Storage
   \ "Minio"
 8 / Netease Object Storage (NOS)
   \ "Netease"
 9 / Scaleway Object Storage
   \ "Scaleway"
10 / SeaweedFS S3
   \ "SeaweedFS"
11 / StackPath Object Storage
   \ "StackPath"
12 / Tencent Cloud Object Storage (COS)
   \ "TencentCOS"
13 / Wasabi Object Storage
   \ "Wasabi"
14 / Any other S3 compatible provider
   \ "Other"
provider> 14
```

```
Option env_auth.
Get AWS credentials from runtime (environment variables or
EC2/ECS meta data if no env vars).
Only applies if access_key_id and secret_access_key is blank.
Enter a boolean value (true or false). Press Enter for the
default ("false").
Choose a number from below, or type in your own value.
 1 / Enter AWS credentials in the next step.
   \ "false"
 2 / Get AWS credentials from the environment (env vars or IAM).
   \ "true"
env_auth> 1
```

```
Option access_key_id.
AWS Access Key ID.
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
access_key_id> ABCDEFGH123456789JKL
```

```
Option secret_access_key.
AWS Secret Access Key (password).
Leave blank for anonymous access or runtime credentials.
Enter a string value. Press Enter for the default ("").
secret_access_key> 123456789ABCDEFGHIJKLMN0123456789PQRST+V
```

```
Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a
region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Use this if unsure.
 1 | Will use v4 signatures and an empty region.
   \ ""
   / Use this only if v4 signatures don't work.
 2 | E.g. pre Jewel/v10 CEPH.
   \ "other-v2-signature"
region> 1
```

```
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> sgdemo.netapp.com
```

```
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
```

```
Option acl.
Canned ACL used when creating buckets and storing or copying
objects.
This ACL is used for creating objects and if bucket_acl isn't
set, for creating buckets too.
For more info visit
https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-
overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as
S3
doesn't copy the ACL from the source but rather writes a fresh
one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
   / Owner gets FULL_CONTROL.
 1 | No one else has access rights (default).
   \ "private"
   / Owner gets FULL_CONTROL.
 2 | The AllUsers group gets READ access.
   \ "public-read"
   / Owner gets FULL_CONTROL.
 3 | The AllUsers group gets READ and WRITE access.
   | Granting this on a bucket is generally not recommended.
   \ "public-read-write"
   / Owner gets FULL_CONTROL.
 4 | The AuthenticatedUsers group gets READ access.
   \ "authenticated-read"
   / Object owner gets FULL_CONTROL.
 5 | Bucket owner gets READ access.
   | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-read"
   / Both the object owner and the bucket owner get FULL_CONTROL
over the object.
 6 | If you specify this canned ACL when creating a bucket,
Amazon S3 ignores it.
   \ "bucket-owner-full-control"
acl>
```

```
Edit advanced config?
y) Yes
n) No (default)
y/n> n
```

```
--------------------
[sgdemo]
type = s3
provider = Other
access_key_id = ABCDEFGH123456789JKL
secret_access_key = 123456789ABCDEFGHIJKLMN0123456789PQRST+V
endpoint = sgdemo.netapp.com:443
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d>
```

```
Current remotes:
```

```
Name                 Type
====                 ====
sgdemo               s3
```

```
e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

基本命令範例

- 建立儲存庫：

  `rclone mkdir remote:bucket`

  ```
  rclone mkdir sgdemo:test01
  ```

  如果您需要忽略 SSL 憑證、請使用 --no 檢查憑證。

- 列出所有庫位：

```
rclone lsd remote:
```

rclone lsd sgdemo ：

- 列出特定儲存區中的物件：

```
rclone ls remote:bucket
```

rclone ls sgdemo:test01

```
    65536 TestObject.0
    65536 TestObject.1
    65536 TestObject.10
    65536 TestObject.12
    65536 TestObject.13
    65536 TestObject.14
    65536 TestObject.15
    65536 TestObject.16
    65536 TestObject.17
    65536 TestObject.18
    65536 TestObject.2
    65536 TestObject.3
    65536 TestObject.5
    65536 TestObject.6
    65536 TestObject.7
    65536 TestObject.8
    65536 TestObject.9
  33554432 bigobj
      102 key.json
       47 locked01.txt
4294967296 sequential-read.0.0
       15 test.txt
      116 version.txt
```

- 刪除一個桶：

```
rclone rmdir remote:bucket
```

rclone rmdir sgdemo:test02

- 放置物件：

```
rclone copy filename remote:bucket
```

rclone copy ~/test/testfile.txt sgdemo:test01

- 取得物件：

```
rclone copy remote:bucket/objectname filename
```

rclone copy sgdemo:test01/testfile.txt ~/test/testfileS3.txt

- 刪除物件：

```
rclone delete remote:bucket/objectname
```

rclone delete sgdemo:test01/testfile.txt

- * 移轉貯體中的物件 *

```
rclone sync source:bucket destination:bucket --progress
```

```
rclone sync source_directory destination:bucket --progress
```

rclone sync sgdemo:test01 sgdemo:clone01 --progress

```
Transferred:        4.032 GiB / 4.032 GiB, 100%, 95.484 KiB/s, ETA
0s
Transferred:           22 / 22, 100%
Elapsed time:       1m4.2s
```

使用 --Progress 或 -P 顯示工作進度。否則就沒有輸出。

- * 刪除貯體和所有物件內容 *

```
rclone purge remote:bucket --progress
```

rclone purge sgdemo:test01 --progress

```
Transferred:              0 B / 0 B, -, 0 B/s, ETA -
Checks:                46 / 46, 100%
Deleted:               23 (files), 1 (dirs)
Elapsed time:         10.2s
```

rclone ls sgdemo:test01

```
2023/04/14 09:40:51 Failed to ls: directory not found
```

使用 Veeam 備份與複寫進行部署的 StorageGRID 最佳實務做法

_ 作者： Oliver Haensel 和 Aron Klein_

本指南著重於 NetApp StorageGRID 和部分 Veeam 備份與複寫的組態。本白皮書是專為熟悉 Linux 系統、且負責與 Veeam 備份與複寫搭配維護或實作 NetApp StorageGRID 系統的儲存與網路管理員所撰寫。

總覽

儲存管理員希望透過解決方案來管理資料的成長、以滿足可用度、快速恢復目標、擴充以滿足需求、並自動化長期保留資料的原則。這些解決方案也應提供防範遺失或惡意攻擊的保護。Veeam 與 NetApp 攜手合作、共同打造結合 Veeam 備份與恢復功能與 NetApp StorageGRID 的資料保護解決方案、以供內部部署物件儲存使用。

Veeam 與 NetApp StorageGRID 提供易於使用的解決方案、可共同協助滿足全球各地快速資料成長與法規不斷增加的需求。雲端型物件儲存設備的恢復能力、擴充能力、營運效率和成本效益、是備份目標的自然選擇。本文件將針對您的 Veeam 備份解決方案和 StorageGRID 系統的組態提供指引和建議。

Veeam 的物件工作負載會建立大量的小型物件並行置放、刪除及清單作業。啟用不可變性將會增加物件存放區的要求數量、以設定保留和列出版本。備份工作的程序包括寫入每日變更的物件、然後在完成新寫入後、工作將會根據備份的保留原則刪除任何物件。備份工作的排程幾乎總是重疊的。這種重疊會導致大部分的備份時間、由物件存放區上的 50/50 Put / delete 工作負載所組成。在 Veeam 中調整工作時段設定的並行作業數、增加備份工作區塊大小、減少多物件刪除要求中的物件數目、以增加物件大小。 選擇工作完成的最長時間範圍、將可針對效能和成本最佳化解決方案。

請務必閱讀產品文檔 "Veeam 備份與複寫"和 "StorageGRID"在你開始之前。 Veeam 提供了計算器，用於了解 Veeam 基礎架構的大小和容量需求，這些計算器應在確定StorageGRID解決方案的大小之前使用。請務必在 Veeam Ready Program 網站上查看 Veeam- NetApp驗證的配置，以了解 "Veeam Ready Object 、 Object Immutable 和 Repository"。

Veeam 組態

建議的版本

建議您隨時保持最新狀態、並為 Veeam Backup & Replication 12 或 12.1 系統套用最新的 Hotfix 。目前我們建

議您至少安裝 Veeam 12 修補程式 P20230718 。

S3 儲存庫組態

橫向擴充備份儲存庫（ SOBR ）是 S3 物件儲存的容量層。容量層是主要儲存庫的延伸、提供較長的資料保留期間和較低成本的儲存解決方案。Veeam 可透過 S3 物件鎖定 API 提供不變的功能。Veeam 12 可以在橫向擴充儲存庫中使用多個儲存庫。StorageGRID 對單一貯體中的物件數量或容量沒有限制。使用多個貯體可在備份大型資料集時改善效能、而備份資料可能會在物件中達到 PB 規模。

視您的特定解決方案和需求規模而定、可能需要限制並行工作。預設設定會為每個 CPU 核心指定一個儲存庫工作插槽、並針對每個工作插槽指定 64 個並行工作插槽限制。例如、如果您的伺服器有 2 個 CPU 核心、則物件儲存區總共會使用 128 個並行執行緒。這包括「放置」、「取得」和「批次刪除」。建議您在 Veeam 備份達到新備份的穩定狀態並即將過期的備份資料後、選擇一個保守的工作時段限制、以開始調整此值。請與您的 NetApp 客戶團隊合作、適當調整 StorageGRID 系統的規模、以符合所需的時間和效能。若要提供最佳解決方案、可能需要調整工作插槽數量和每個插槽的工作限制。

備份工作組態

Veeam 備份工作可以使用不同的區塊大小選項進行設定、這些選項應該仔細考慮。預設區塊大小為 1MB 、Veeam 提供的壓縮與重複資料刪除儲存效率可為初始完整備份建立約 500KB 的物件大小、而增量工作則建立 100-200kB 物件。我們可以選擇較大的備份區塊大小、大幅提升效能、並降低物件儲存區的需求。雖然較大的區塊大小可大幅改善物件儲存區效能、但由於儲存效率效能降低、因此可能會增加主要儲存容量需求。建議將備份工作設定為 4 MB 區塊大小、以建立大約 2 MB 的物件來進行完整備份、並將 700kB-1MB 的物件大小用於遞增。客戶甚至可以考慮使用 8 MB 區塊大小來設定備份工作、這可在 Veeam 支援的協助下啟用。

執行不可變備份時、會使用物件儲存區上的 S3 物件鎖定。不可變選項會產生更多要求、要求物件存放區列出物件並更新保留資料。

當備份保留過期時、備份工作會處理物件的刪除。Veeam 會將刪除要求傳送至物件存放區、每個要求的多物件刪除要求為 1000 個物件。對於小型解決方案、可能需要調整以減少每個要求的物件數量。降低此值將有助於更平均地在 StorageGRID 系統中的節點之間分配刪除要求。建議使用下表中的值作為設定多物件刪除限制的起點。將表格中的值乘以所選應用裝置類型的節點數、即可取得 Veeam 中的設定值。如果此值等於或大於 1000 、則不需要調整預設值。如果需要調整此值、請與 Veeam 支援人員合作進行變更。

應用裝置機型	**S3** 每個節點的 **MultiObjectDeleteLimit**
SG5712	34.
SG5760	75
SG6060	200

請與您的 NetApp 客戶團隊合作、根據您的特定需求、取得建議的組態。Veeam 組態設定建議包括：

- 備份工作區塊大小 = 4MB
- SOBR 工作插槽限制 = 2-16
- 多物件刪除限制 = 34-1000

StorageGRID 組態

建議的版本

對於 Veeam 部署，建議使用具有最新修補程式的NetApp StorageGRID 11.9 或 12.0 版本。始終建議保持最新狀態並為StorageGRID系統應用最新的修補程式。

負載平衡器和 **S3** 端點組態

Veeam 要求端點僅透過 HTTPS 連線。Veeam 不支援未加密的連線。SSL 憑證可以是自我簽署的憑證、私密信任的憑證授權單位或公開信任的憑證授權單位。為了確保能持續存取 S3 儲存庫、建議在 HA 組態中至少使用兩個負載平衡器。負載平衡器可以是 StorageGRID 提供的整合式負載平衡器服務、位於每個管理節點和閘道節點、或是第三方解決方案、例如 F5 、 Kemp 、 HAProxy 、 Loadbalancer.org 等 使用 StorageGRID 負載平衡器可設定流量分類器（ QoS 規則）、以排定 Veeam 工作負載的優先順序、或將 Veeam 限制為不影響 StorageGRID 系統上的高優先順序工作負載。

S3時段

StorageGRID是一個安全的多租戶儲存系統。建議為 Veeam 工作負載建立專用租用戶。可以選擇分配儲存配額。作為最佳實踐，啟用「使用自己的身分來源」。使用適當的密碼保護租用戶根管理使用者。 Veeam Backup 12 要求 S3 儲存桶具有強一致性。 StorageGRID提供在儲存桶層級配置的多個一致性選項。對於 Veeam 從多個位置存取資料的多站點部署，請選擇「strong-global」。如果 Veeam 備份和還原僅在單一網站進行，則一致性等級應設定為「strong-site」。有關存儲桶一致性級別的更多信息，請查看 "文件"。若要使用StorageGRID進行 Veeam 不變性備份，必須在全域啟用 S3 物件鎖，並在儲存桶建立期間在儲存體桶上進行設定。

生命週期管理

StorageGRID 支援複寫和銷毀編碼、可在 StorageGRID 節點和站台之間提供物件層級保護。銷毀編碼需要至少 200kB 物件大小。Veeam 的預設區塊大小為 1MB 、產生的物件大小通常會低於 Veeam 儲存效率之後的 200 KB 建議最小大小。為了達到解決方案的效能、建議不要使用跨越多個站台的抹除編碼設定檔、除非站台之間的連線能力足以避免增加延遲或限制 StorageGRID 系統的頻寬。在多站台 StorageGRID 系統中、 ILM 規則可設定為在每個站台上儲存單一複本。為了達到極致的耐用性、可設定規則、在每個站台儲存銷毀編碼複本。使用兩個本機複本到 Veeam 備份伺服器是此工作負載最建議的實作方式。

刪除效能

Veeam 提供刪除請求率調整和備份刪除過程的調度。為了進一步調整刪除效能，您可以停用同步刪除並讓 ILM 掃描器管理物件的最終刪除。

停用同步刪除的步驟

1. 開啟StorageGRID網格管理器。
2. 在右上角，選擇問號，然後選擇 API 文件。
3. 在右上角，點擊私有 API 文件頁面連結。
4. 擴展 ilm-advanced。
5. 選擇 GET ilm-advanced。
6. 選擇“試用”，然後“執行”。
7. 查看響應結果。

    a. 如果值為空，則表示正在使用預設的 ilm-advanced 值。

    b. 如果值不為空，則表示自訂 ILM 高階值正在使用中。複製「資料」之後的所有輸出： ，從 { 開始直到倒

數第二個 }。

i. 將其保存在某些文字編輯器中。

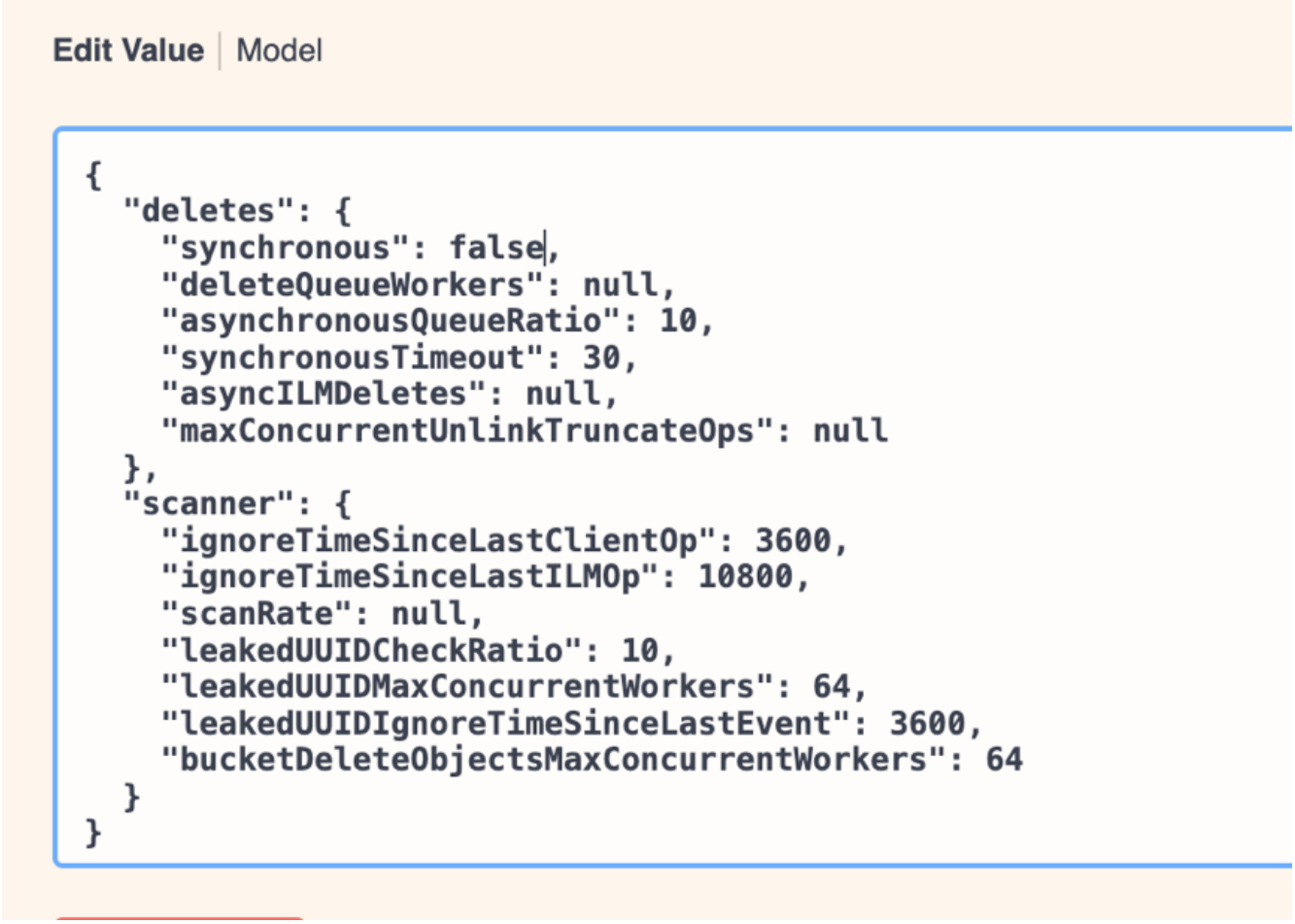
回應範例：

Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```


8. 選擇 PUT ilm-advanced。
9. 選擇「試用」開始編輯 API 主體。
   a. 預設情況下，API 主體將包含預設值，而不包含任何先前配置的自訂值。這就是為什麼執行步驟 5-7 非常重要的原因。
10. 如果在步驟 5-7 中發現非預設值，則以步驟 7 中儲存的輸出取代 API 主體。。否則，如果步驟 5-7 中的值為空，則保留 API 主體不變。
11. 在API主體框中調整以下參數：
    a. 將同步值設定為false。

    API 正文範例：

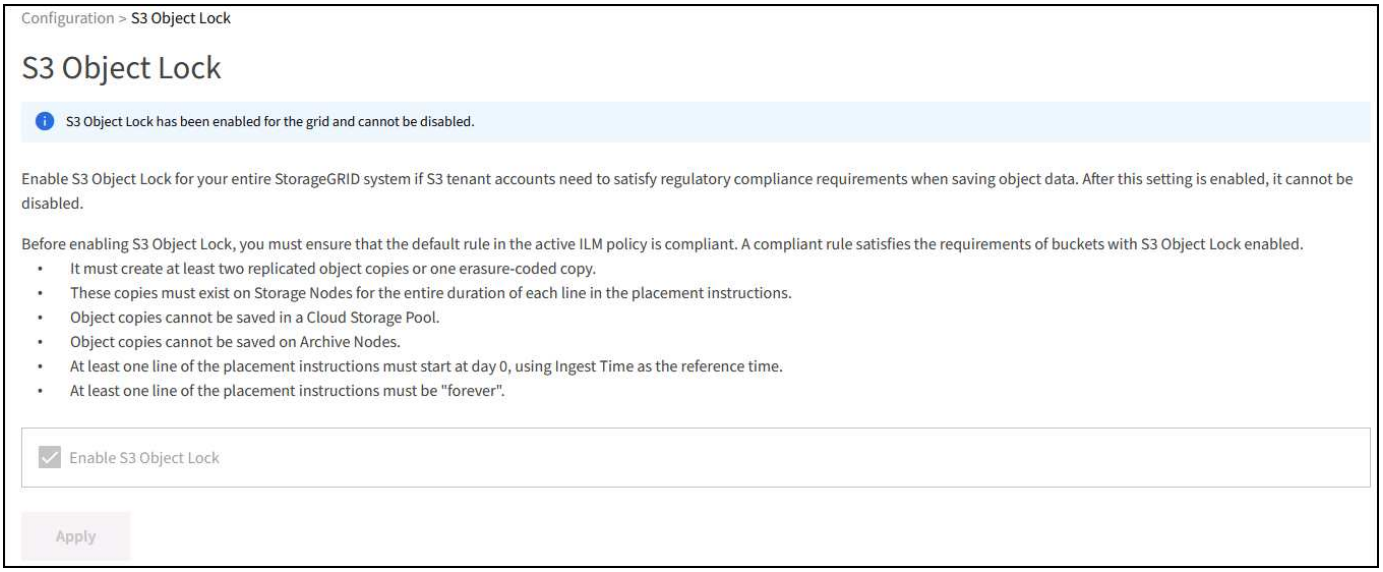


12. 完成後，選擇執行

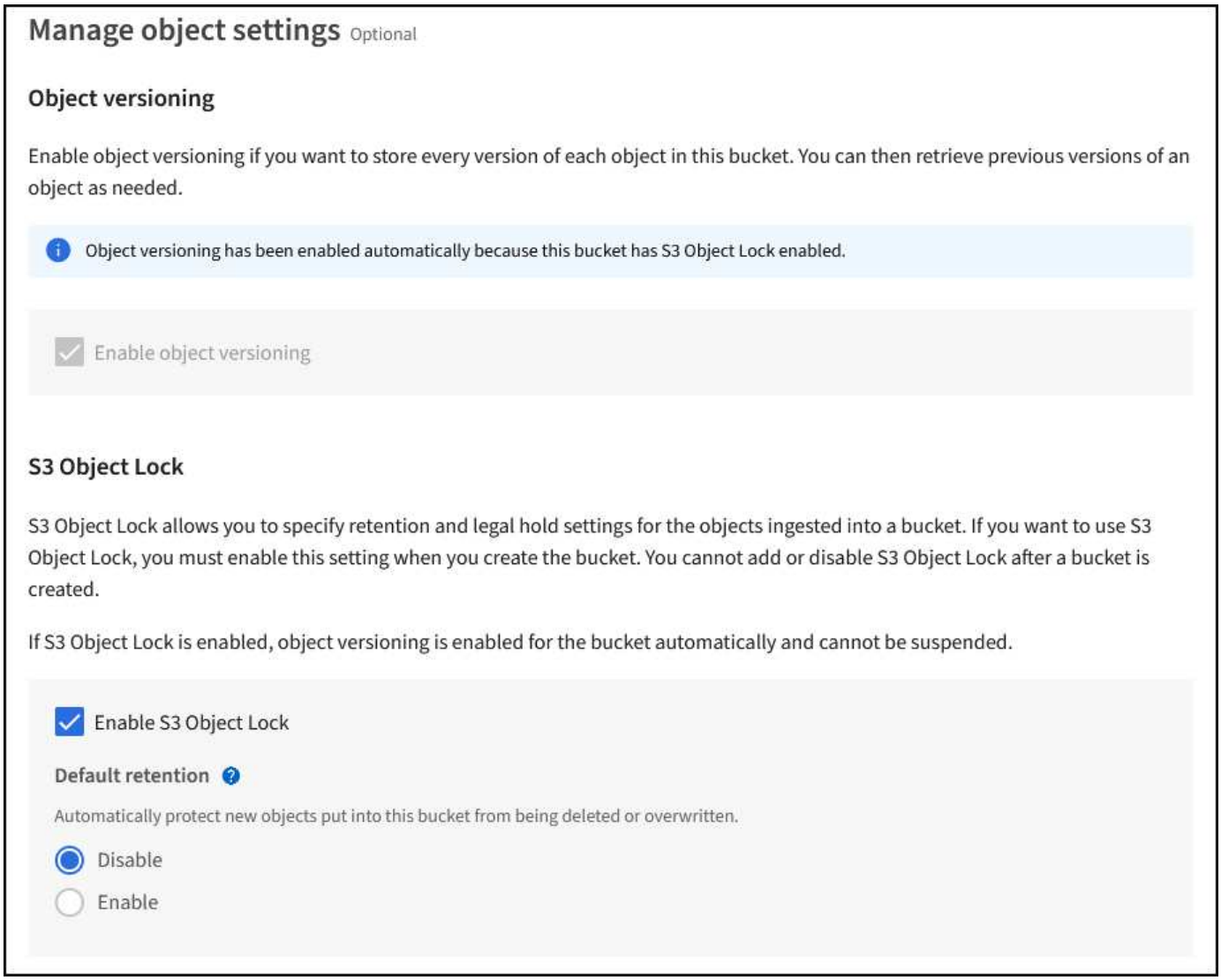
實作重點

StorageGRID

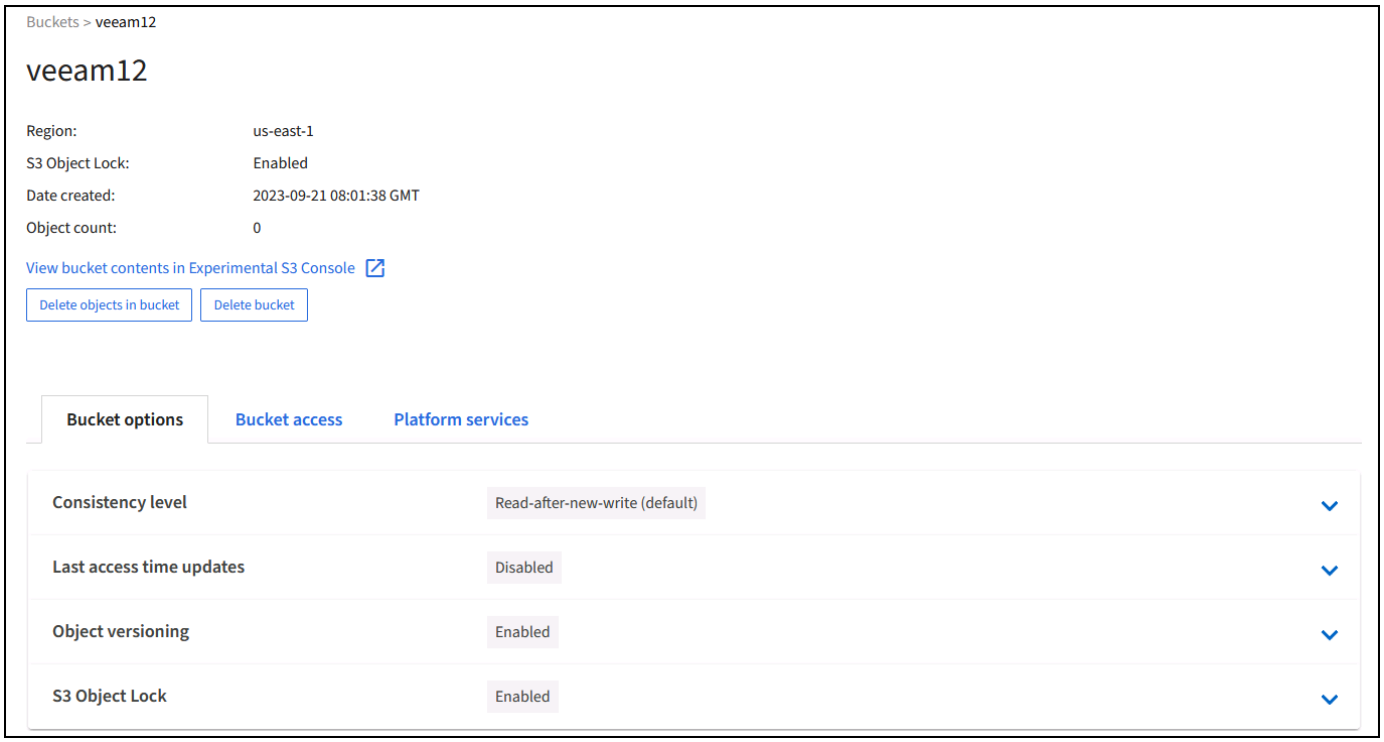
如果需要不可變性、請確保 StorageGRID 系統上已啟用物件鎖定。請在組態 /S3 物件鎖定下的管理 UI 中找到選項。



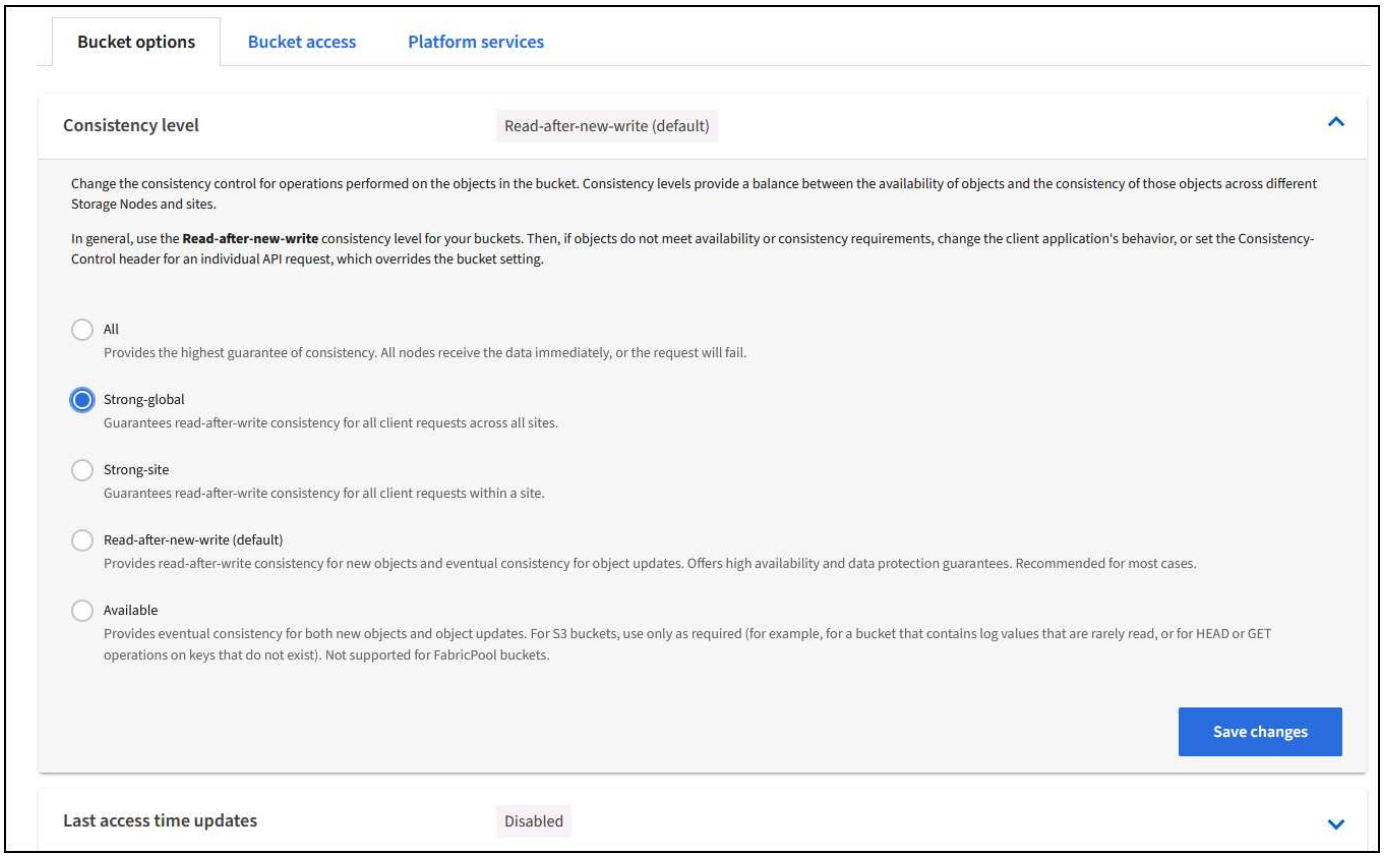
建立貯體時、如果要使用此貯體進行不可變備份、請選取「啟用 S3 物件鎖定」。這會自動啟用貯體版本管理。停用預設保留、因為 Veeam 會明確設定物件保留。如果 Veeam 未建立不可變的備份、則不應選取版本設定和 S3 物件鎖定。



建立貯體後、請前往建立之貯體的詳細資料頁面。選取一致性層級。



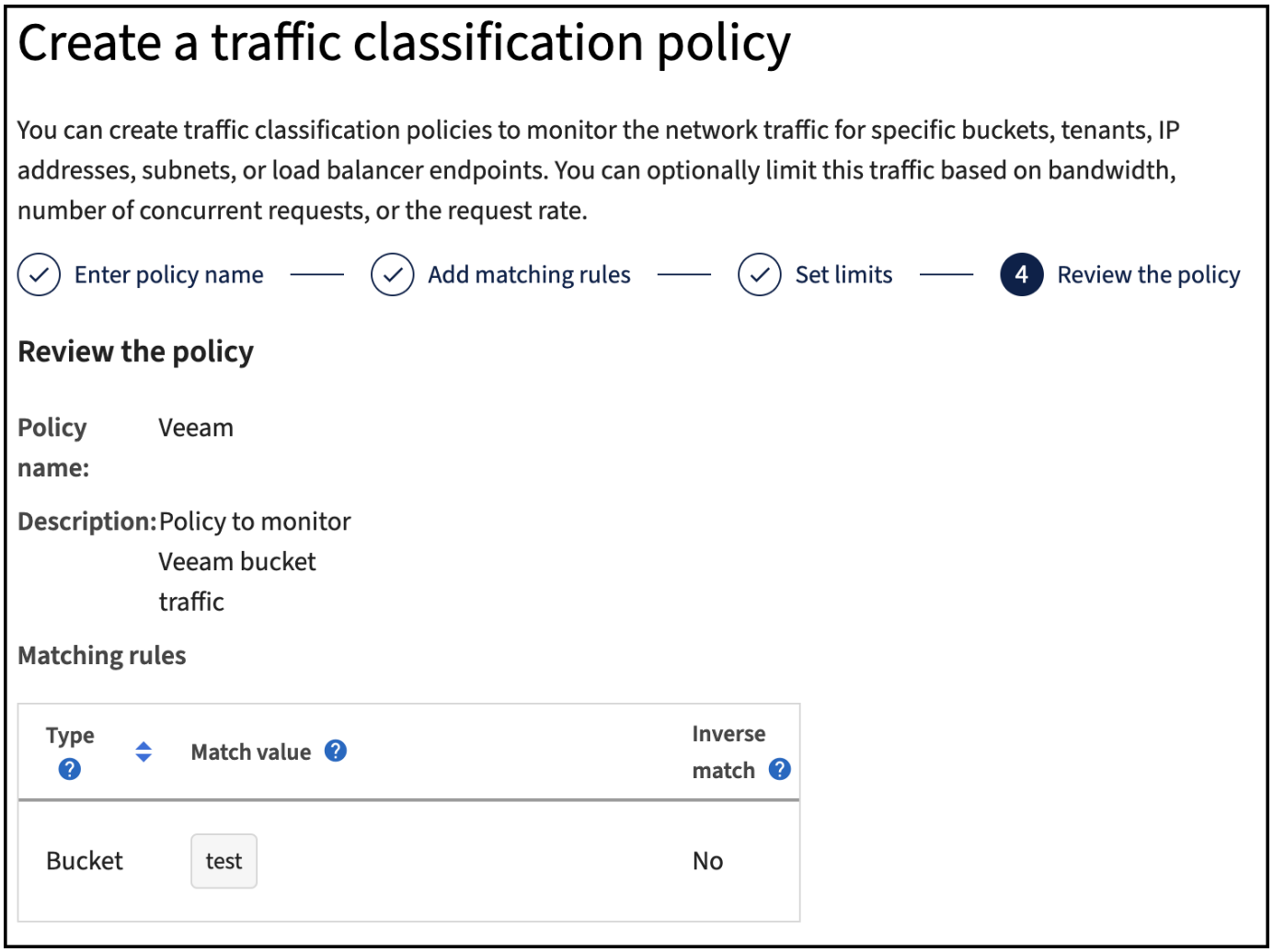
Veeam 需要 S3 儲存區的強大一致性。因此、對於 Veeam 從多個位置存取資料的多站台部署、請選取「 Strong-glob線 」。如果 Veeam 備份與還原僅發生在單一站台上、則一致性層級應設為「 Strong-site 」。儲存變更。



StorageGRID 在每個管理節點和專用閘道節點上提供整合式負載平衡器服務。使用此負載平衡器的眾多優點之一、就是能夠設定流量分類原則（ QoS ）。雖然這些指標主要用於限制應用程式對其他用戶端工作負載的影

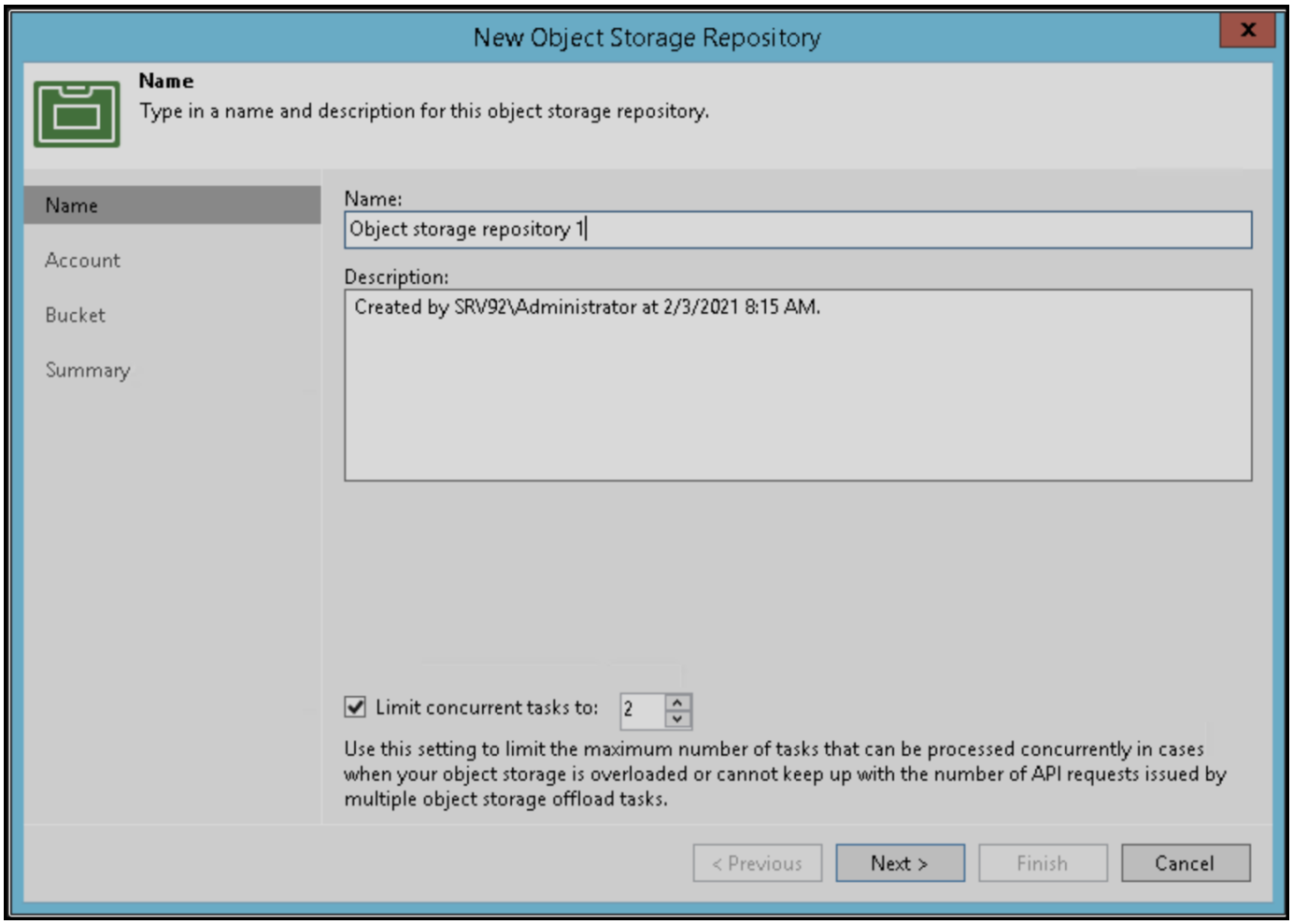
響、或是優先處理工作負載而非其他工作負載、但它們也提供額外的指標收集、以協助監控。

在組態索引標籤中、選取「流量分類」並建立新原則。命名規則、並選取貯體或租戶作為類型。輸入貯體或租戶的名稱。如果需要 QoS 、請設定限制、但對於大多數實作而言、我們只是想增加監控效益、所以請勿設定限制。

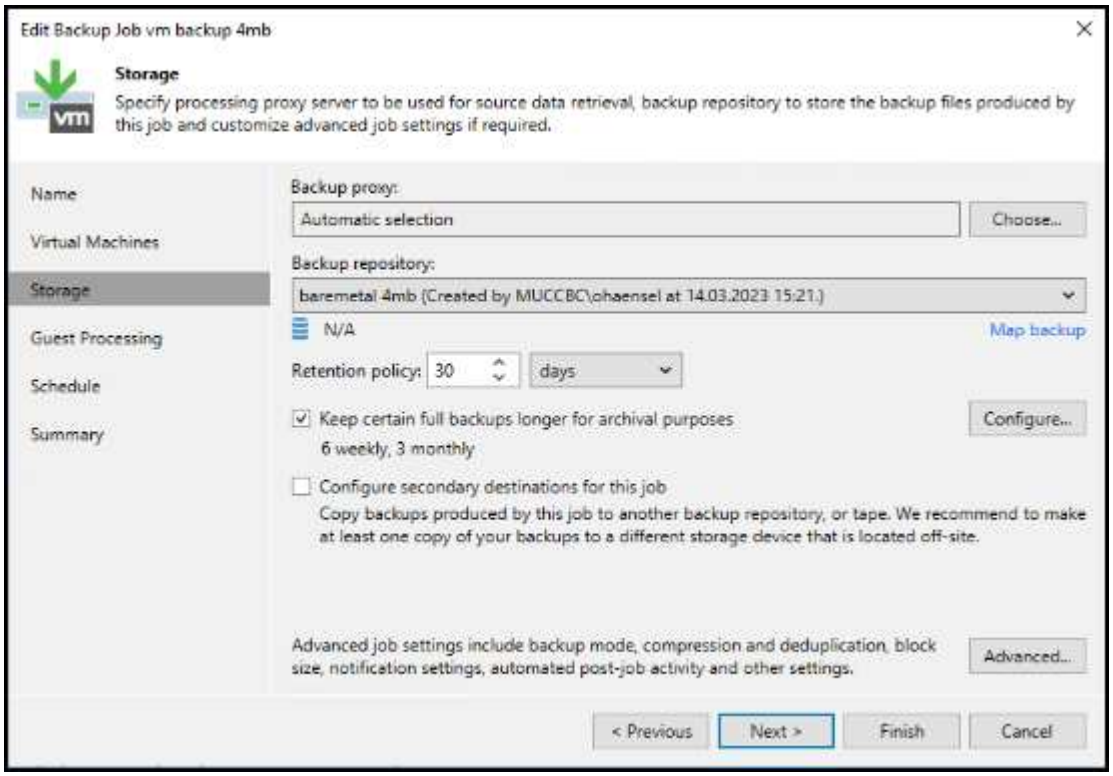


Veeam

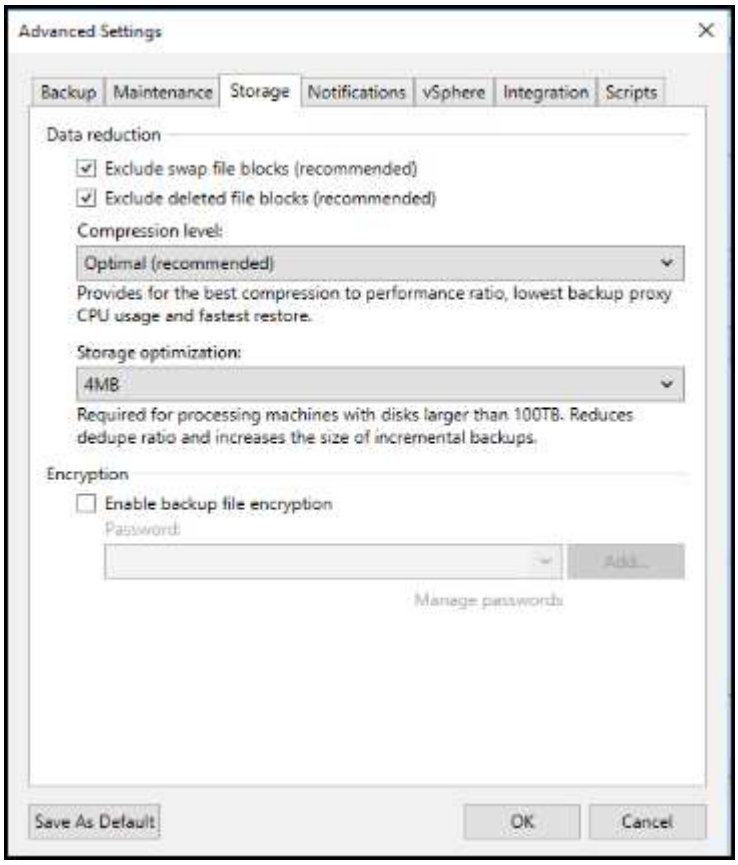
視 StorageGRID 應用裝置的型號和數量而定、可能需要選擇並設定貯體上並行作業數量的限制。



請依照 Veeam 主控台中備份工作組態的 Veeam 文件、啟動精靈。新增虛擬機器後、請選取 SOBR 儲存庫。



按一下「進階設定」、將儲存最佳化設定變更為 4 MB 或更大。應啟用壓縮與重複資料刪除。根據您的需求變更來賓設定、並設定備份工作排程。



監控 StorageGRID

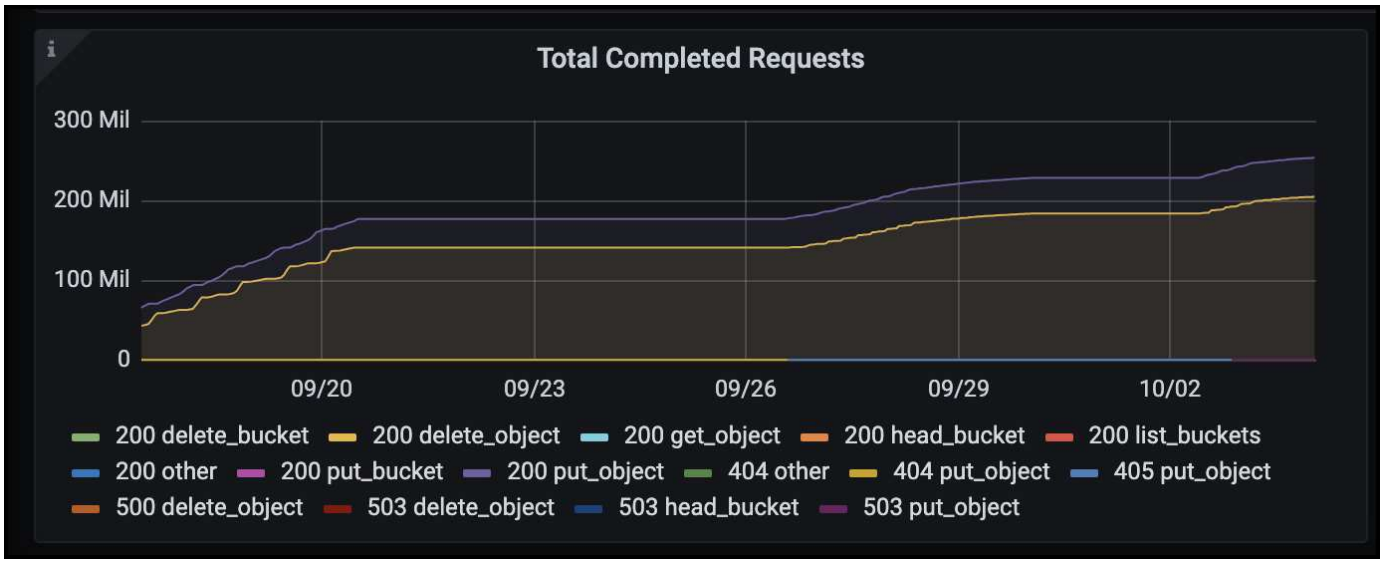
若要完整瞭解 Veeam 和 StorageGRID 如何共同執行、您必須等到第一次備份的保留時間過期。直到目前為止、 Veeam 工作負載主要由 Put 作業所組成、而且沒有發生刪除。一旦備份資料過期且正在清理、您現在可以在物件存放區中看到完全一致的使用情形、並視需要在 Veeam 中調整設定。

StorageGRID 提供便利的圖表、可監控位於「支援索引標籤度量」頁面中的系統運作。如果建立原則、則主要要查看的儀表板是 S3 概觀、 ILM 和流量分類原則。在 S3 概述儀表板中、您可以找到 S3 作業率、延遲和要求回應的相關資訊。

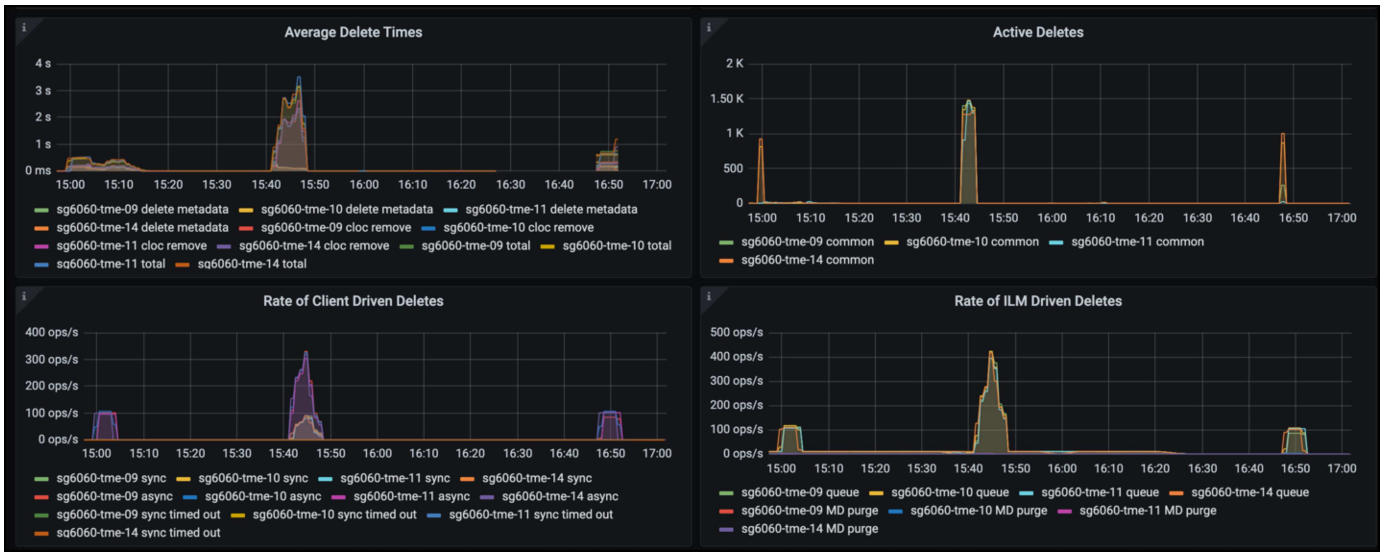
查看 S3 速率和作用中要求、您可以瞭解每個節點處理的負載量、以及依類型列出的要求總數。

「平均持續時間」圖表顯示每個節點針對每個要求類型所花費的平均時間。這是要求的平均延遲、可能是需要額外調整的好指標、或是 StorageGRID 系統有更多負載的空間。

在「完成的申請總數」圖表中、您可以依類型和回應代碼查看申請。如果您看到 200 （正常）以外的回應、這可能表示 StorageGRID 系統負載過大、傳送 503 （減慢）回應、可能需要進行一些額外調整、或是需要時間擴充系統以因應增加的負載。



在 ILM 儀表板中、您可以監控 StorageGRID 系統的刪除效能。StorageGRID 會在每個節點上同時使用同步刪除和非同步刪除、以嘗試最佳化所有要求的整體效能。



有了流量分類原則、我們可以檢視負載平衡器要求處理量、速率、持續時間、以及 Veeam 正在傳送和接收的物件大小的度量。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- "NetApp StorageGRID產品文檔"
- "Veeam 備份與複寫"

使用 StorageGRID 設定 Dremio 資料來源

_ 作者： Angela Cheng _

Dremio 支援各種資料來源、包括雲端型或內部部署物件儲存。 您可以將 Dremio 設定為使用 StorageGRID 做為物件儲存資料來源。

設定 Dremio 資料來源

先決條件

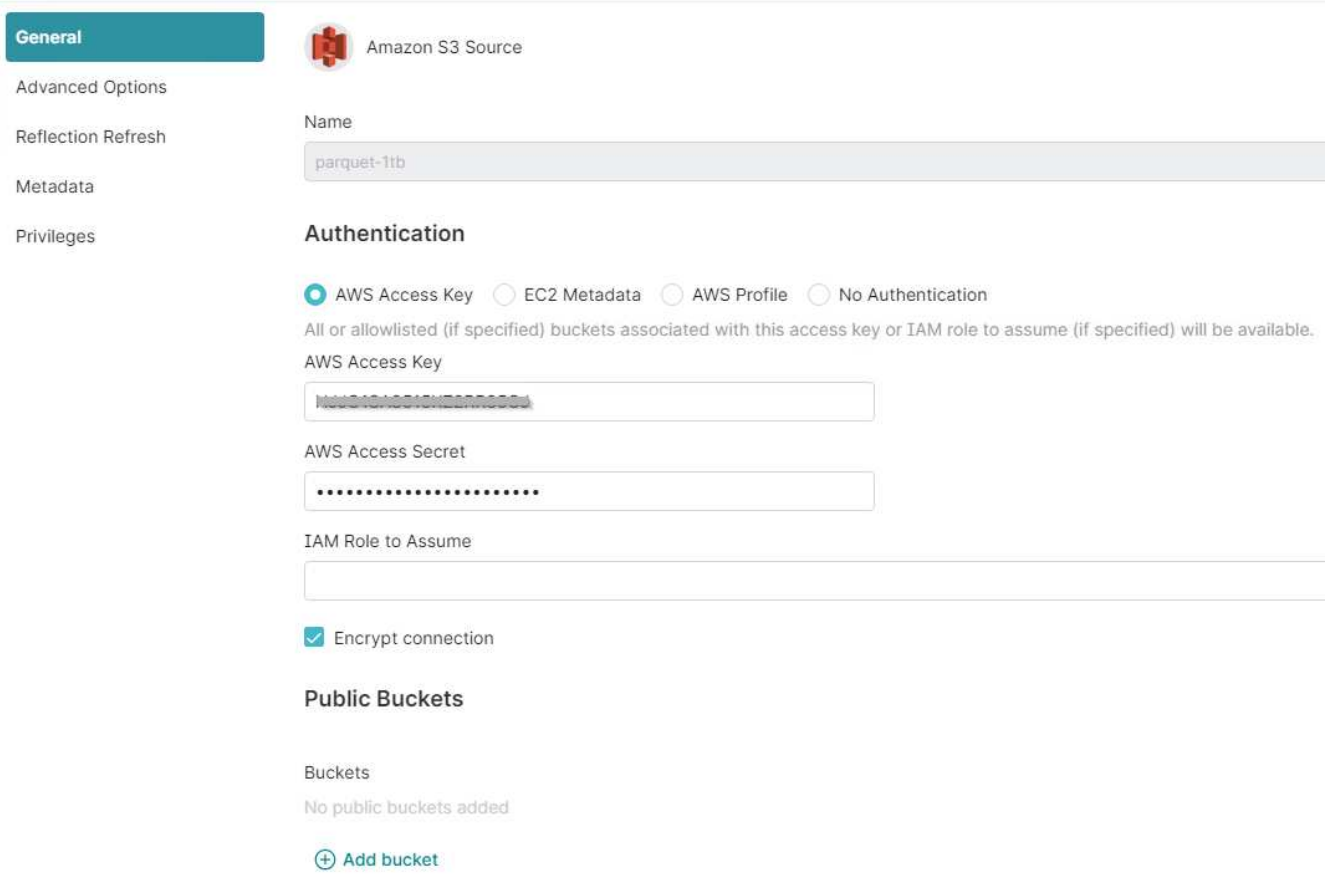
- StorageGRID S3 端點 URL 、租戶 S3 存取金鑰 ID 和秘密存取金鑰。
- StorageGRID 組態建議：停用壓縮（預設為停用）。
  Dremio 使用位元組範圍 GET 、在查詢期間同時從同一個物件中擷取不同的位元組範圍。 位元組範圍要求的一般大小為 1MB 。壓縮物件會降低位元組範圍的效能。

Dremio 指南

"連線至 Amazon S3 - 設定相容 S3 的儲存設備"。

指示

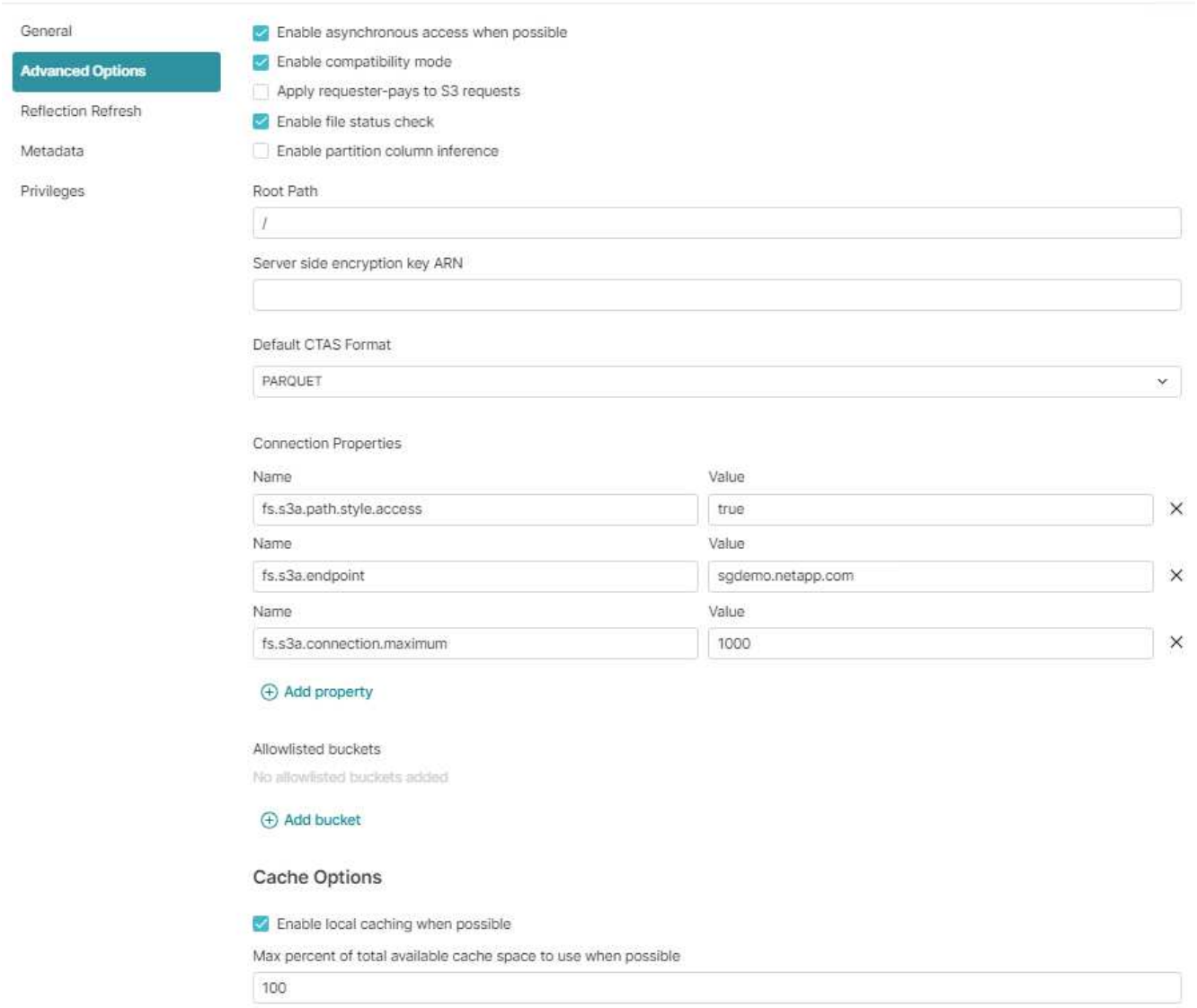
1. 在「 Dremio 資料集」頁面上、按一下 + 符號以新增來源、然後選取「 Amazon S3 」。
2. 輸入此新資料來源的名稱、 StorageGRID S3 租戶存取金鑰 ID 和秘密存取金鑰。
3. 如果使用 https 連線至 StorageGRID S3 端點、請勾選「加密連線」方塊。+
   如果為此 S3 端點使用自我簽署的 CA 認證、請遵循 Dremio 指南說明、將此 CA 認證新增至 Dremio 伺服器的 <JAVA_HOME> / JRE/lib/security
   範例擷取畫面



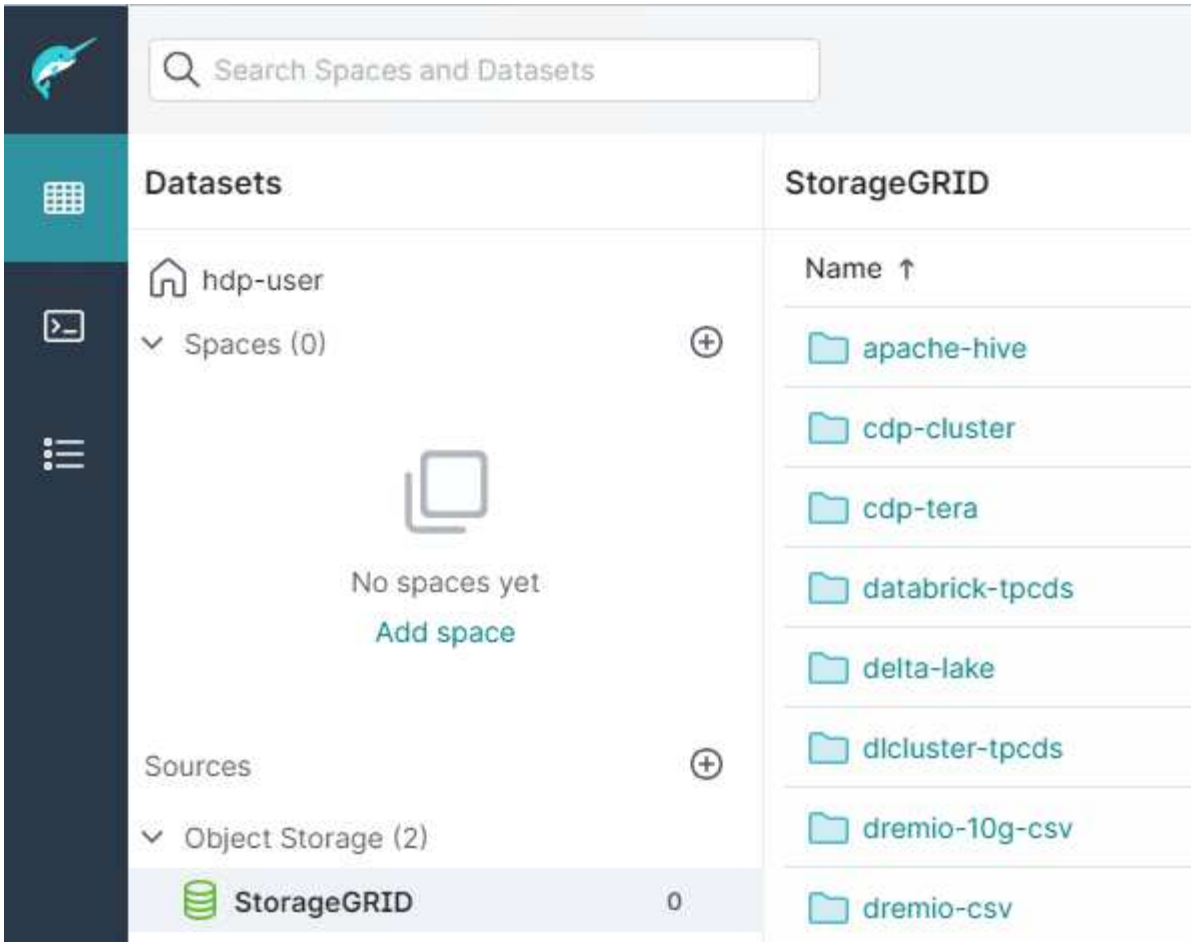
4. 按一下「進階選項」、核取「啟用相容模式」
5. 在連線內容下、按一下 + 新增內容、然後新增這些 s3a 內容。
6. fs.s3a.connection.maximum 預設為 100 。 如果您的 S3 資料集包含 100 個以上欄位的大型 Parquet 檔案、則必須輸入大於 100 的值。 請參閱 Dremio 指南以瞭解此設定。

名稱	價值
fs.s3a.端 點	< *StorageGRID* 支援*S3*端點：連接埠>
fs.s3a.path.樣式.access	是的
fs.s3a.connection.maximum	< 大於 *100*> 的值

範例擷取畫面



7. 根據您的組織或應用程式需求、設定其他 Dremio 選項。
8. 按一下「儲存」按鈕以建立此新資料來源。
9. 成功新增 StorageGRID 資料來源後、左側面板會顯示貯體清單。+
範例擷取畫面



NetApp StorageGRID 搭配 GitLab

_ 作者： Angela Cheng _

NetApp 已使用 GitLab 測試 StorageGRID 。請參閱以下 GitLab 組態範例。 請參閱 "GitLab 物件儲存組態指南" 以取得詳細資料。

物件儲存連線範例

對於 Linux 套件安裝、這是的範例 `connection` 合併表單中的設定。編輯 `/etc/gitlab/gitlab.rb` 然後新增下列行、以您要的值取代：

```
# Consolidated object storage configuration
gitlab_rails['object_store']['enabled'] = true
gitlab_rails['object_store']['proxy_download'] = true
gitlab_rails['object_store']['connection'] = {
  'provider' => 'AWS',
  'region' => 'us-east-1',
  'endpoint' => 'https://<storagegrid-s3-endpoint:port>',
  'path_stype' => 'true',
  'aws_access_key_id' => '<AWS_ACCESS_KEY_ID>',
  'aws_secret_access_key' => '<AWS_SECRET_ACCESS_KEY>'
}
# OPTIONAL: The following lines are only needed if server side encryption
is required
gitlab_rails['object_store']['storage_options'] = {
  'server_side_encryption' => 'AES256'
}
gitlab_rails['object_store']['objects']['artifacts']['bucket'] = 'gitlab-
artifacts'
gitlab_rails['object_store']['objects']['external_diffs']['bucket'] =
'gitlab-mr-diffs'
gitlab_rails['object_store']['objects']['lfs']['bucket'] = 'gitlab-lfs'
gitlab_rails['object_store']['objects']['uploads']['bucket'] = 'gitlab-
uploads'
gitlab_rails['object_store']['objects']['packages']['bucket'] = 'gitlab-
packages'
gitlab_rails['object_store']['objects']['dependency_proxy']['bucket'] =
'gitlab-dependency-proxy'
gitlab_rails['object_store']['objects']['terraform_state']['bucket'] =
'gitlab-terraform-state'
gitlab_rails['object_store']['objects']['pages']['bucket'] = 'gitlab-
pages'
```

程序和API範例

測試並示範StorageGRID 有關支援的S3加密選項

_ 作者： Aron Klein_

支援的支援功能有許多不同的方法可加密閒置的資料。StorageGRID若要深入瞭解、請參閱 "檢閱StorageGRID功能加密方法"。

本指南將示範S3 API加密方法。

伺服器端加密（SSe）

使用者可透過sse儲存物件、並使用StorageGRID 由支援的獨特金鑰來加密物件。當物件被要求時、物件會被儲存在StorageGRID 物件中的金鑰解密。

例如

- 將物件放入SS

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- 驗證加密的目標

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- 取得物件

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

使用客戶提供的金鑰進行伺服器端加密（SSE-C）

使用者可透過SSE儲存物件、並使用用戶端隨物件提供的唯一金鑰來加密物件。要求物件時、必須提供相同的金鑰才能解密及傳回物件。

SSE-C範例

- 為了測試或示範目的、您可以建立加密金鑰
  - 建立加密金鑰

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- 使用產生的金鑰放置物件

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- 物件的前端

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
            {
                "AcceptRanges": "bytes",
                "LastModified": "2022-05-02T19:20:02+00:00",
                "ContentLength": 47,
                "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
                "ContentType": "binary/octet-stream",
                "Metadata": {},
                "SSECustomerAlgorithm": "AES256",
                "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
            }
```

如果您未提供加密金鑰、您將會收到「呼叫頭物件作業時發生錯誤（404）：找不到」錯誤訊息。

- 取得物件

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

如果您未提供加密金鑰、則會在呼叫GetObject作業時收到錯誤訊息「發生錯誤（InvalidRequest）：該物件是使用伺服器端加密的形式儲存。必須提供正確的參數才能擷取物件。"

儲存區伺服器端加密（SSE-S3）

SSE-S3可讓用戶端針對儲存在儲存區中的所有物件、定義預設的加密行為。物件會使用StorageGRID 由支援的獨特金鑰進行加密。當物件被要求時、物件會被儲存在StorageGRID 檔中的金鑰解密。

Bucket SSE-S3範例

- 建立新儲存區並設定預設加密原則
  - 建立新的儲存庫

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

  - 將儲存區加密

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- 將物件放入儲存區

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 物件的前端

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- 取得物件

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

測試並示範StorageGRID S3物件鎖定功能

_ 作者： Aron Klein_

物件鎖定提供WORM模型、可防止物件遭到刪除或覆寫。物件鎖定的實作係由Cohasset進行評估、以協助符合法規要求、支援合法持有和符合法規的物件保留模式、以及預設的儲存貯體保留原則。StorageGRID

本指南將示範S3物件鎖定API。

合法持有

- 物件鎖定合法保留是套用至物件的簡單開啟/關閉狀態。

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- 使用Get作業來驗證。

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- 關閉合法保留

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- 使用Get作業來驗證。

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

法規遵循模式

- 物件保留會以保留直到時間戳記完成。

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- 確認保留狀態

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

預設保留

- 設定保留期間（以天數和年數為單位）、並使用「每個物件API」所定義的「保留截止日期」。

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- 確認保留狀態

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- 將物件放入儲存區

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 儲存區上設定的保留持續時間會轉換成物件上的保留時間戳記。

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

測試刪除具有定義保留的物件

物件鎖定是建置在版本管理之上。保留是在物件的某個版本上定義。如果嘗試刪除已定義保留的物件、但未指定版本、則會建立刪除標記作為物件的目前版本。

- 刪除已定義保留的物件

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- 列出儲存區中的物件

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - 請注意、此物件並未列出。

- 列出要查看刪除標記的版本、以及原始鎖定版本

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- 刪除物件的鎖定版本

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

StorageGRID 中的原則和權限

以下是 StorageGRID S3 的原則和權限範例。

原則的結構

在 StorageGRID 中，群組原則與 AWS 使用者（ IAM ） S3 服務原則相同。

StorageGRID 中需要群組原則。擁有 S3 存取金鑰但未指派給使用者群組的使用者，或是指派給群組的使用者，若沒有原則授予某些權限，將無法存取任何資料。

庫位和群組原則共享大部分相同的元素。原則是以 json 格式建置，可使用產生 "AWS 原則產生器"

所有原則都會定義影響，行動和資源。貯體原則也會定義主體。

「 * 效果 * 」將是「允許」或「拒絕」要求。

- 負責人 *
- 僅適用於貯體原則。
- 主體是被授與或拒絕權限的帳戶 / 使用者。
- 可定義為：
  - 萬用字元 "*"

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - 租戶中所有使用者的租戶 ID （相當於 AWS 帳戶）

```
"Principal": { "AWS": "27233906934684427525" }
```

  - 使用者（來自貯體所在租戶內部的本機或聯盟，或網格中的其他租戶）

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

  - 群組（來自貯體所在租戶內部的本機或聯盟群組，或網格中的其他租戶）。

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

「 * 行動 * 」是一組 S3 作業正在授予或拒絕給使用者。

對於群組原則，使用者必須執行 S3 ： ListBucket 動作，才能執行任何 S3 動作。

「資源 * 」是被授與或拒絕執行動作的主體所在的貯體或貯體。（可選）當策略操作有效時，可以有 * 條件 * 。

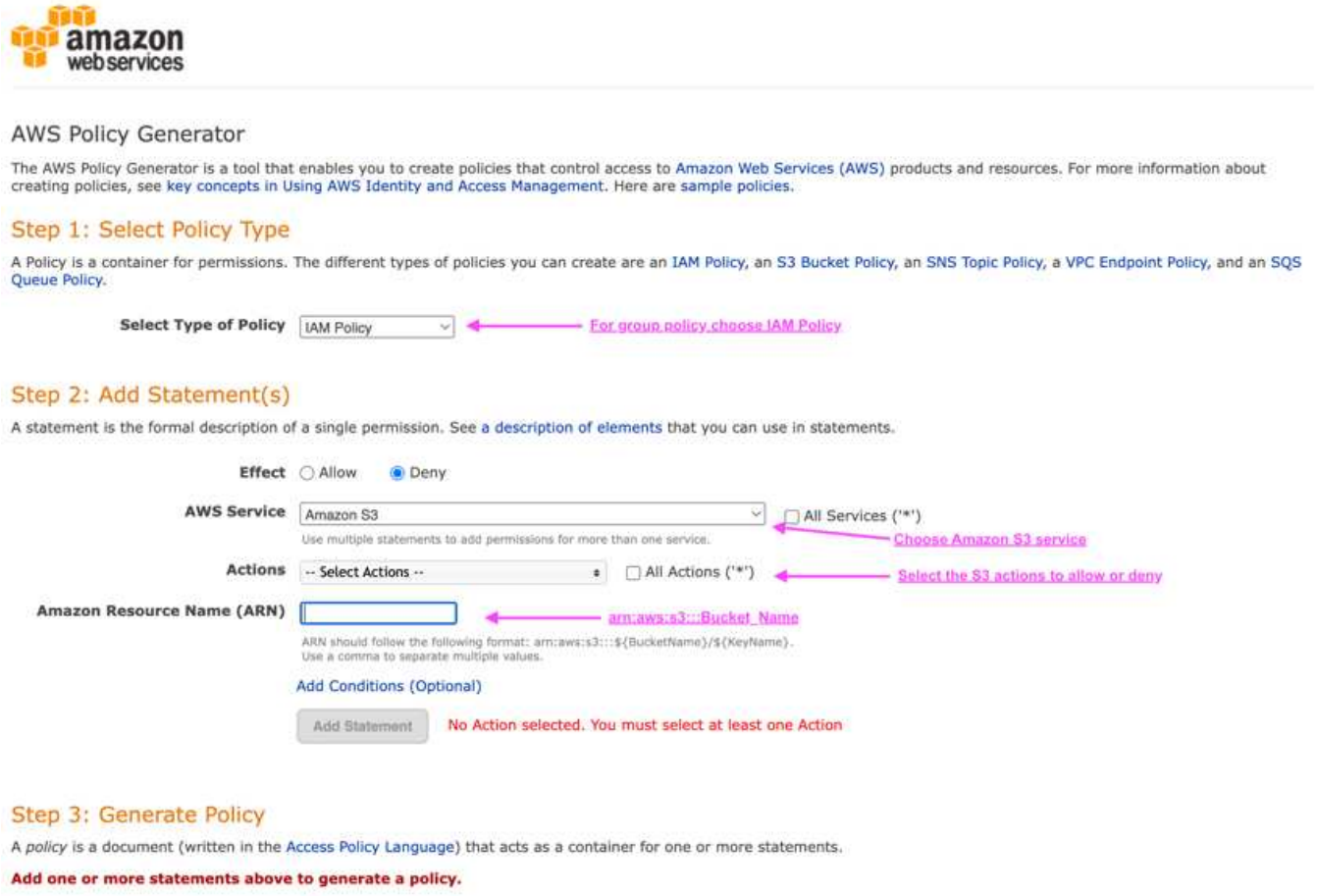
JSON 原則的格式如下：

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

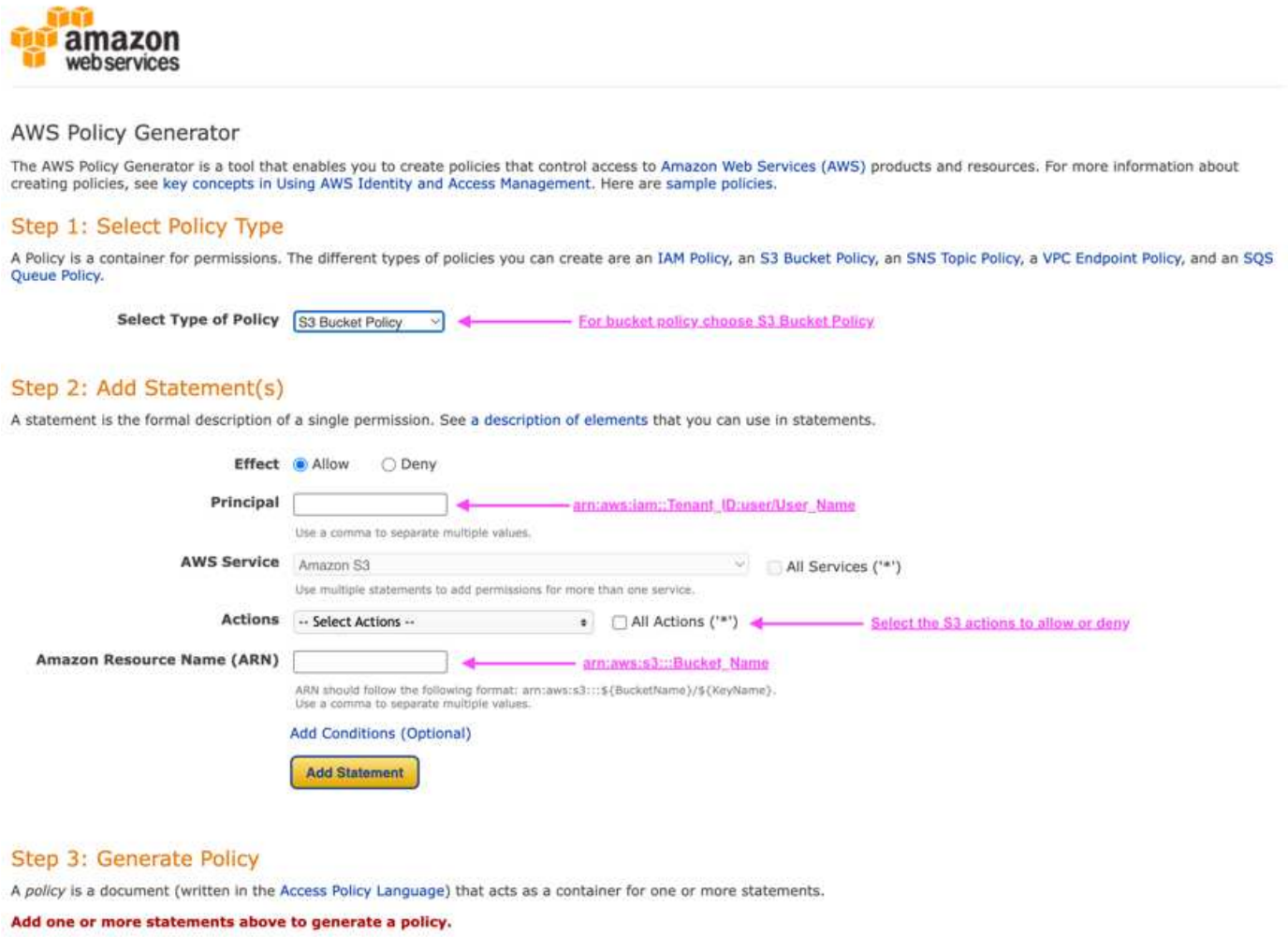
使用 **AWS** 原則產生器

AWS 原則產生器是一項絕佳工具，可協助您取得 json 程式碼，並取得您嘗試實作的正確格式和資訊。

若要產生 StorageGRID 群組原則的權限： * 選擇原則類型的 IAM 原則。* 選取所需效果的按鈕：「允許」或「拒絕」。最好先以拒絕權限啟動原則，然後在「動作」下拉式清單中新增「允許權限」 * ，然後按一下您要在此權限或「所有動作」方塊中加入的 S3 動作數量旁邊的方塊。* 在「 Amazon 資源名稱（ ARN ）」方塊中輸入貯體路徑。在貯體名稱前加上「 arn:AWS:S3 ：：：：」。例如："arn:AWS ： S3 ：：： Example_Bucket"

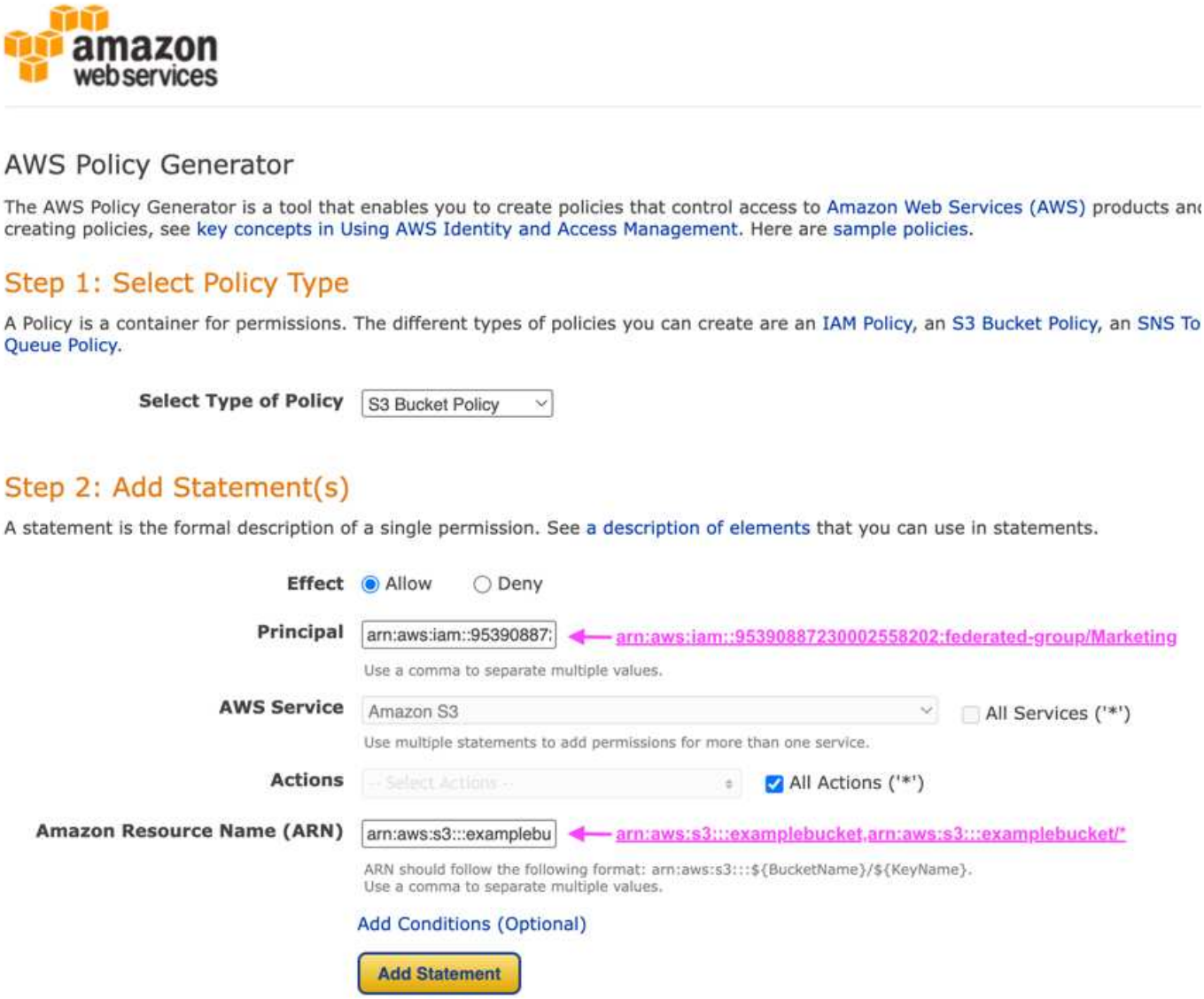


若要產生貯體原則的權限： * 針對原則類型選擇 S3 Bucket 原則。* 選取所需效果的按鈕：「允許」或「拒絕」。以拒絕權限啟動原則，然後新增允許權限 * 輸入主體的使用者或群組資訊，是個不錯的做法。* 在「動作」下拉式清單中，按一下您要在此權限或「所有動作」方塊中包含的 S3 動作數量旁邊的方塊。* 在「 Amazon 資源名稱（ ARN ）」方塊中輸入貯體路徑。在貯體名稱前加上「 arn:AWS:S3 ：：：：」。例如："arn:AWS ： S3 ：：： Example_Bucket"



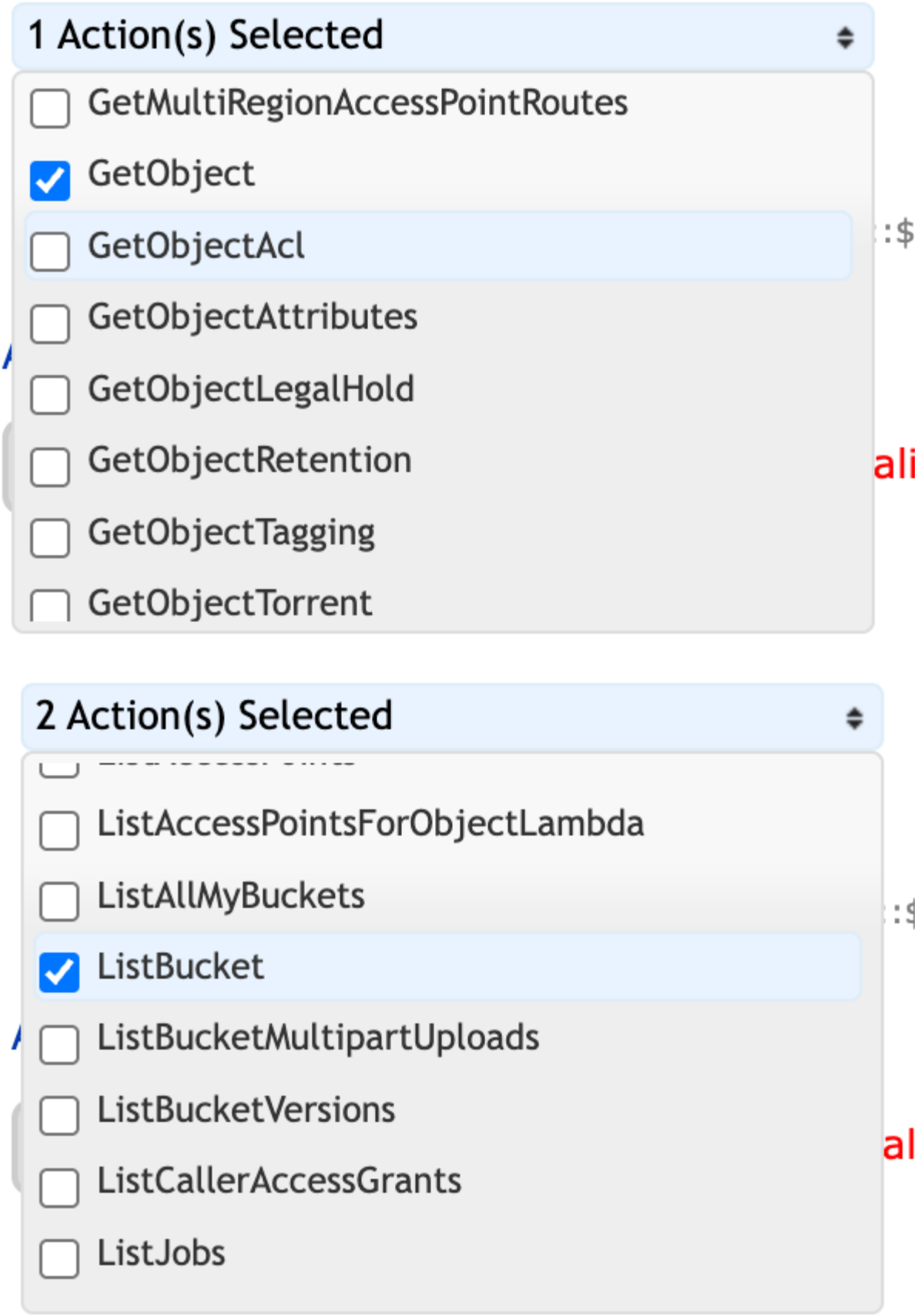
例如，如果您想要產生貯體原則，讓所有使用者都能對貯體中的所有物件執行 GetObject 作業，而只有屬於指定帳戶中「行銷」群組的使用者才可以擁有完整存取權。

- 選取 S3 Bucket Policy 做為原則類型。
- 選擇「允許」效果
- 輸入行銷群組資訊 - arn:AWs:iam::95390887230002558202:Federated -group/Marketing
- 按一下「所有動作」方塊
- 輸入貯體資訊 - arn:AWS:S3:::example_Bucket,arn:AWS:::::example_Bucket/*



- 按一下「新增說明」按鈕

- 選擇「允許」效果
- 輸入每個人的星號 *
- 按一下「 GetObject 和 ListBucket 動作」旁邊的方塊



- 輸入貯體資訊 - arn:AWS:S3:::example_Bucket,arn:AWS:::::example_Bucket/*

amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products an creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS To Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 2 Action(s) Selected All Actions ('*')

Amazon Resource Name (ARN) arn:aws:s3:::examplebu ← arn:aws:s3:::examplebucket,arn:aws:s3:::examplebucket/*

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

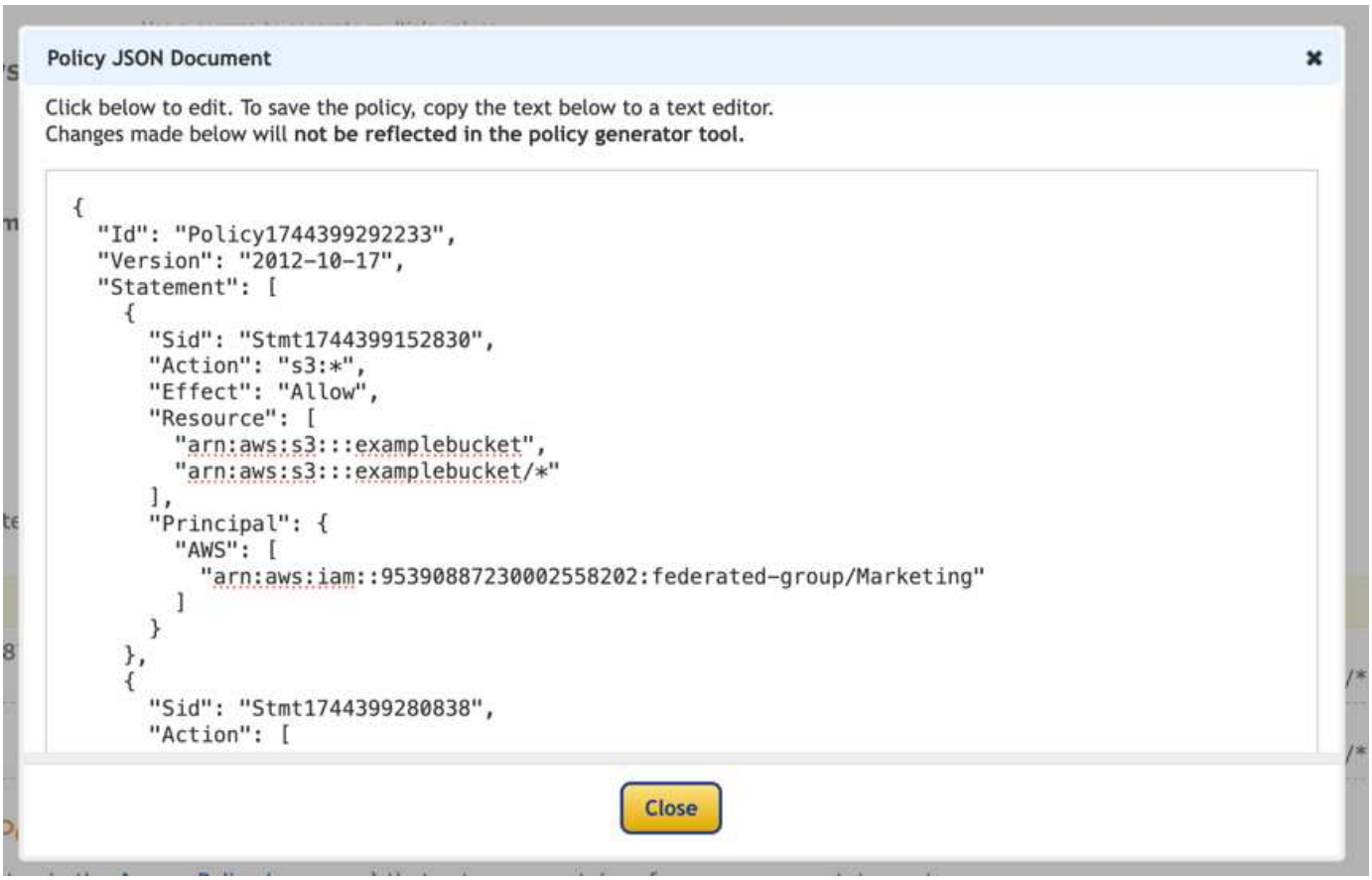
Add Statement

- 按一下「新增說明」按鈕

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• arn:aws:iam::953908872300025582O2:federated-group/Marketing	Allow	s3:*	• arn:aws:s3:::examplebucket • arn:aws:s3:::examplebucket/*	*None*
• *	Allow	• s3:GetObject • s3:ListBucket	• arn:aws:s3:::examplebucket • arn:aws:s3:::examplebucket/*	*None*

- 按一下「產生原則」按鈕，就會出現一個快顯視窗，顯示您產生的原則。



- 複製完整的 json 文字，如下所示：

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

此 json 可依原樣使用，也可移除「對帳單」行上方的 ID 和版本行，您可以針對每個權限自訂 Sid ，並針對每個權限設定更有意義的標題，也可以移除這些標題。

例如：

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

群組原則（IAM）

主目錄樣式庫存取

此群組原則僅允許使用者存取名為使用者使用者名稱之儲存區中的物件。

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

拒絕建立物件鎖定儲存區

此群組原則會限制使用者建立在貯體上啟用物件鎖定的貯體。

此原則並未在StorageGRID SUI中強制執行、只有S3 API才會強制執行。

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

物件鎖定保留限制

此 Bucket 原則將物件鎖定保留期間限制為 10 天或更短

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

限制使用者以版本 **ID** 刪除物件

此群組原則會限制使用者依照版本 ID 刪除版本管理的物件

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

將群組限制為具有唯讀存取權的單一子目錄（首碼）

此原則可讓群組成員對儲存庫中的子目錄（前置）擁有唯讀存取權。貯體名稱為「 study 」、子目錄為「 study01 」。

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:s3::: study"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

貯體原則

將儲存區限制為具有唯讀存取權的單一使用者

此原則可讓單一使用者擁有儲存區的唯讀存取權、並明確地讓Denys存取所有其他使用者。將「拒絕」陳述式分組在原則頂端、是加速評估的好做法。

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::34921514133002833665:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

將貯體限制在少數具有唯讀存取權的使用者。

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

限制使用者刪除貯體中的版本化物件

此貯體原則會限制使用者（由使用者 ID 「 56622399308951294926 」識別）依版本 ID 刪除版本管理物件

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

StorageGRID 中的儲存桶生命週期

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。

什麼是生命週期配置

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）。

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。

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

令已經失效，物件仍可能保留在網格上

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

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

生命週期策略的結構

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** 僅適用於與前綴 category1/ 相符且 key2 值為 tag2 的物件。 Expiration參數指定與該篩選條件相符的物件將於 2020 年 8 月 22 日午夜到期。
2. 規則 **2** 僅適用於與前綴 category2/ 相符的物件。 Expiration參數指定與篩選器相符的物件將在提取後 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** 僅適用於與前綴 category3/ 相符的物件。 Expiration參數指定符合物件的任何非目前版本將在變為非目前版本後 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
```

標準（非版本化）儲存桶的生命週期策略範例

90 天後刪除對象

用例：此策略非常適合管理僅在有限時間內相關的數據，例如臨時文件、日誌或中間處理數據。優點：降低儲存成本並確保儲存桶整潔有序。

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

版本控制儲存桶的生命週期策略範例

10 天後刪除非目前版本

使用案例：此策略有助於管理非當前版本物件的存儲，這些物件會隨著時間的推移而累積並佔用大量空間。優勢：透過僅保留最新版本來優化儲存空間利用率。

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled"’
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

保留 **5** 個非目前版本

使用案例：當您想要保留有限數量的先前版本以用於恢復或審計目的時很有用。好處：保留足夠的非當前版本以確保足夠的歷史記錄和復原點。

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled"’
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

當不存在其他版本時移除刪除標記

使用案例：此策略有助於管理所有非目前版本刪除後留下的刪除標記，這些標記會隨著時間的推移而累積。好處：減少不必要的混亂。

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled"’
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

30 天後刪除目前版本，**60** 天後刪除非目前版本，一旦不存在其他版本，則刪除目前版本所建立的刪除標記。

使用案例：為目前版本和非目前版本提供完整的生命週期，包括刪除標記。優點：降低儲存成本，確保儲存桶整潔有序，同時保留足夠的恢復點和歷史記錄。

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

刪除沒有其他版本的刪除標記，為帶有「**accounts_** 前綴」的物件保留 **4** 個非當前版本和至少 **30** 天的歷史記錄，為所有其他物件版本保留 **2** 個版本和至少 **10** 天的歷史記錄。

使用案例：為特定物件以及其他物件提供獨特的規則，以管理目前版本和非目前版本（包括刪除標記）的完整生命週期。優點：降低儲存成本，確保儲存桶整潔有序，同時保留足夠的恢復點和歷史記錄，以滿足各種客戶需求。

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

結論

- 定期檢視和更新生命週期政策，並使其與 ILM 和資料管理目標保持一致。
- 在廣泛應用策略之前，先在非生產環境或儲存桶中測試策略，以確保其按預期工作
- 使用描述性 ID 作為規則使其更直觀，因為邏輯結構可能變得複雜
- 監控這些儲存桶生命週期策略對儲存使用情況和效能的影響，以做出必要的調整。

技術報告

StorageGRID 技術報告簡介

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。

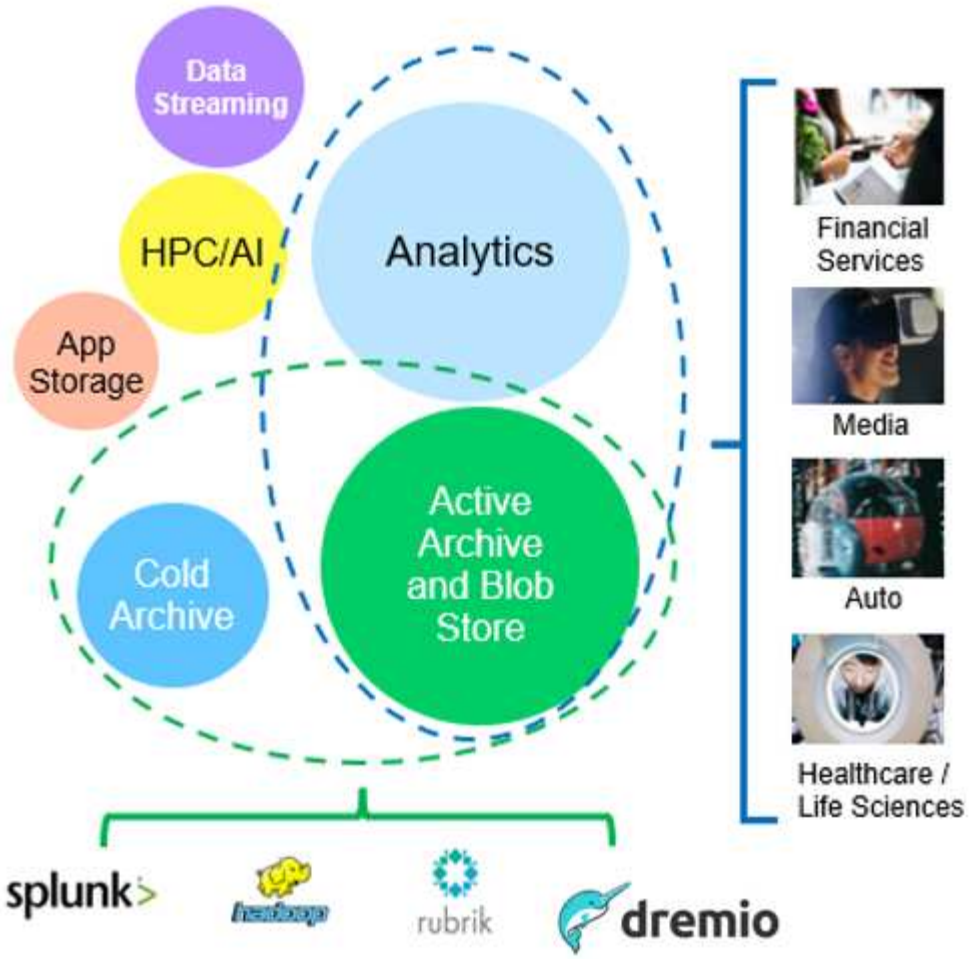
StorageGRID 提供說明文件、涵蓋數項 StorageGRID 功能與整合的最佳實務做法與建議。

NetApp StorageGRID 與巨量資料分析

NetApp StorageGRID 使用案例

NetApp StorageGRID 物件儲存解決方案提供擴充性、資料可用度、安全性及高效能。各種規模的組織、以及各行各業的組織、都會使用 StorageGRID S3 來處理各種使用案例。讓我們來探索一些典型案例：

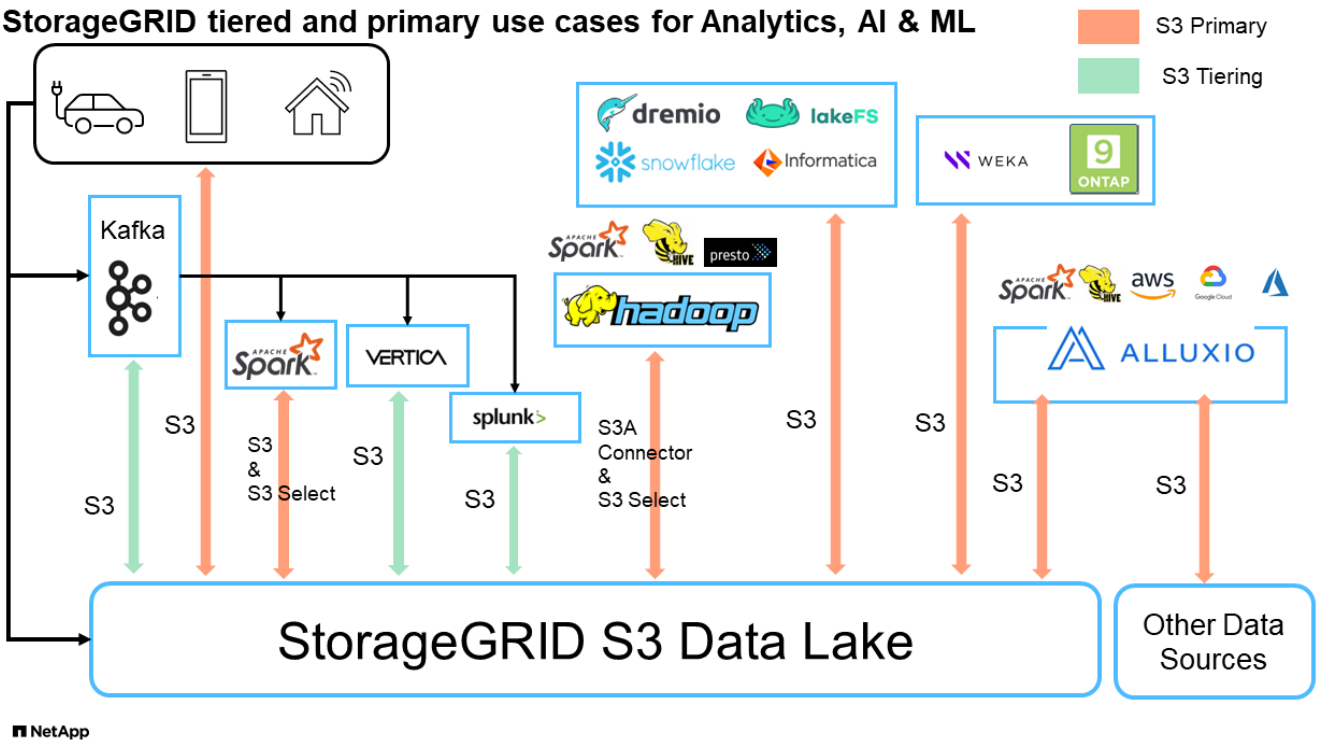
- 巨量資料分析： * StorageGRID S3 經常用作資料湖、企業可在其中儲存大量結構化和非結構化資料、以便使用 Apache Spark 、 Splunk Smartstore 和 Dremio 等工具進行分析。
- 資料分層： * NetApp 客戶使用 ONTAP 的 FabricPool 功能、在高效能本機層之間自動將資料移至 StorageGRID 。分層可釋放昂貴的 Flash 儲存空間、以儲存熱資料、同時在低成本物件儲存設備上隨時提供冷資料。如此可將效能與節約效益發揮到極致。
- 資料備份與災難恢復： * 企業可以使用 StorageGRID S3 做為可靠且具成本效益的解決方案、在發生災難時備份關鍵資料並加以恢復。
- 應用程式的資料儲存： * StorageGRID S3 可作為應用程式的儲存後端、讓開發人員輕鬆儲存及擷取檔案、影像、影片及其他類型的資料。
- 內容交付： * StorageGRID S3 可用於儲存靜態網站內容、媒體檔案及軟體下載、並提供給全球各地的使用者、運用 StorageGRID 的地理發佈和全球命名空間、提供快速可靠的內容交付。
- 資料歸檔： * StorageGRID 提供不同的儲存類型、並支援分層處理至公有長期低成本儲存選項、因此是歸檔及長期保留資料的理想解決方案、這些資料必須保留以供法規遵循或歷史用途。
- 物件儲存使用案例 *



在上述情況中、巨量資料分析是最熱門的使用案例之一、其使用率也逐漸上升。

為何選擇 **StorageGRID** 來處理資料湖？

- 更高的協同作業效率：大規模共用多站台、多租戶、並具備業界標準 API 存取功能
- 降低營運成本：單一、自我修復、自動化橫向擴充架構的操作簡易性
- 擴充性：與傳統的 Hadoop 和資料倉儲解決方案不同、 StorageGRID S3 物件儲存設備可將儲存設備與運算和資料分離、讓企業能夠隨著成長擴充儲存需求。
- 耐用性與可靠性： StorageGRID 提供 99.999% 的耐用度、這表示儲存的資料對於資料遺失具有高度抵抗能力。它也提供高可用度、確保資料隨時可供存取。
- 安全性： StorageGRID 提供各種安全功能、包括加密、存取控制原則、資料生命週期管理、物件鎖定和版本設定、以保護儲存在 S3 儲存區中的資料
- StorageGRID S3 資料湖 *



以 S3 物件儲存為基準測試資料倉儲和 Lakeouses ：比較研究

本文提供使用 NetApp StorageGRID 的各種資料倉儲和湖屋生態系統的完整基準。目標是判斷哪一種系統在 S3 物件儲存設備上的效能最佳。請參閱此資訊https://www.dremio.com/wp-content/uploads/2023/02/apache-Iceberg-TDG_ER1.pdf?aliId=eyJpIjoieDRUYjFKN2ZMbXhTRnFRWCIsInQiOiJIUUw0djJsWnlJa21iNUsyQURRalNnPT0ifQ%253D%253D["Apache 冰山：最終指南"]、深入瞭解資料流 / 湖屋架構和表格格式（ Parquet 和冰山）。

- 基準測試工具 - TPC-DS - https://www.tpc.org/tpcds/
- Big Data 生態系統
  - VM 叢集、每個都有 128G RAM 和 24 個 vCPU 、系統磁碟的 SSD 儲存設備
  - Hadoop 3.3.5 搭配 Hive 3.1.3 （ 1 個名稱節點 + 4 個資料節點）
  - Delta Lake with Spark 3.2.0 （ 1 位大師 + 4 位員工）和 Hadoop 3.3.5
  - Dremio v25.2 （ 1 名協調員 + 5 名執行者）
  - Trino v438 （ 1 名協調員 + 5 名員工）
  - Starburst v453 （ 1 名協調員 + 5 名員工）
- 物件儲存
  - NetApp ^ ® ^ StorageGRID ^ ® ^ 11.8 含 3 個 SG6060 + 1 個 SG1000 負載平衡器
  - 物件保護 - 2 份複本（結果與 EC 2+1 類似）
- 資料庫大小 1000GB
- 每項查詢測試的所有生態系統都會使用「硬碟區」格式停用快取。對於冰山格式、我們比較了 S3 取得要求的數量、以及快取停用和啟用快取的案例之間的查詢時間總計。

TPC-DS 包含 99 個複雜的 SQL 查詢、專為基準測試而設計。我們測量了執行所有 99 項查詢所需的總時間、並透過檢查 S3 要求的類型和數量來進行詳細分析。我們的測試比較了兩種常用表格格式的效率：拼花地板和冰山。

- 使用 Parquet 資料表格式的 TPC-DS 查詢結果 *

生態系統	**Hive**	德爾塔湖	夢中	**Trino**	**Starburst**
TPCDS 99 查詢總分鐘數	1084[1]	55	36	32	28
S3 要求明細	取得	1,117,184	2,074,610	3,939,690	1,504,212
1,495,039	觀察： 全方位實現	從 32 MB 物件到 2 KB 到 2 MB 的範圍達到 80% 、每秒 50 到 100 個要求	73% 的範圍從 32 MB 物件低於 100KB 、從 1000 到 1400 個要求 / 秒	從 256 MB 物件獲得 90% 的 100 萬位元組範圍、2500 年至 3000 個要求 / 秒	範圍取得大小：低於 100KB 50% 、約 16% 1 MB 、 27% 2Mb 至 9Mb 、 3500 至 4000 個要求 / 秒
範圍取得大小：低於 100KB 50% 、約 16% 1MB 、 27% 2Mb 至 9Mb 、 4000 至 5000 要求 / 秒	列出物件	312,053	24 、 158	120	509
512	標題 （不存在的物件）	156,027	12 、 103	96	0
0	標題 （存在的物件）	982,126.	922,732.	0	0
0	申請總數	2,567,390	3 、 033 、 603	3,939.906	1,504,721

[1] Hive 無法完成查詢編號 72

- TPC-DS 查詢結果、內含冰山表格格式 *

生態系統	夢中	**Trino**	**Starburst**
TPCDS 99 查詢 + 總分鐘數（停用快取）	22	28	22
TPCDS 99 查詢 + 總分鐘 [2] （啟用快取）	16.	28	21.5
S3 要求明細	Get （快取已停用）	1,985,922	938,639

生態系統	夢中	Trino	Starburst
931,582	Get （啟用快取）	611,347	30,158
3,281	觀察： 全方位實現	範圍取得大小： 67% 1MB 、 15% 100KB 、 10% 500KB 、 3500 - 4500 個要求 / 秒	範圍取得大小：低於 100KB 42% 、約 17% 1 MB 、 33% 2Mb 至 9Mb 、 3500 至 4000 個要求 / 秒
範圍取得大小：低於 100KB 43% 、約 17% 1 MB 、 33% 2Mb 至 9Mb 、 4000 至 5000 個要求 / 秒	列出物件	1465	0
0	標題 （不存在的物件）	1464	0
0	標題 （存在的物件）	3,702	509
509	要求總數（快取停用）	1,992,553	939,148

[2] Trino/Starburst 效能受到運算資源的限制；將更多 RAM 新增至叢集可縮短查詢時間。

如第一張表所示、 Hive 的速度遠低於其他現代資料湖屋生態系統。我們觀察到 Hive 傳送了大量的 S3 清單物件要求、這在所有物件儲存平台上通常都很緩慢、尤其是在處理包含許多物件的貯體時。如此可大幅增加整體查詢持續時間。此外、現代的湖屋生態系統也能同時傳送大量的 GET 要求、每秒可傳送 2 、 000 至 5 、 000 個要求、相較於 Hive 每秒 50 至 100 個要求。與 S3 物件儲存設備互動時、 Hive 和 Hadoop S3A 所提供的標準檔案系統會導致 Hive 速度緩慢。

搭配 Hive 或 Spark 使用 Hadoop （在 HDFS 或 S3 物件儲存設備上）需要對 Hadoop 和 Hive/Spark 有廣泛的瞭解、同時也需要瞭解每個服務的設定如何互動。它們一起擁有超過 1 、 000 種設定、其中許多是相互關聯的、無法分別變更。尋找設定與值的最佳組合需要大量的時間和精力。

比較 Parquet 和冰山結果時、我們發現表格格式是主要的效能因素。從 S3 要求的數量來看、冰山表格格式比 Parquet 更有效率、相較於 Parquet 格式、申請數量減少 35% 至 50% 。

Dremio 、 Trino 或 Starburst 的效能主要是由叢集的運算能力所驅動。雖然這三個系統都使用 S3A 連接器來連接 S3 物件儲存連線、但它們不需要 Hadoop 、而且這些系統也不使用 Hadoop 的 FS.s3a 設定。如此可簡化效能調校、免除學習和測試各種 Hadoop S3A 設定的需求。

從這個基準測試結果中、我們可以得出結論、針對 S3 型工作負載最佳化的大型資料分析系統是主要的效能因素。現代化的湖上環境可最佳化查詢執行、有效運用中繼資料、並提供對 S3 資料的無縫存取、因此相較於使用 S3 儲存設備時的 Hive 、效能更佳。

請參閱此 "頁面"資訊、以使用 StorageGRID 設定 Dremio S3 資料來源。

請造訪下列連結、深入瞭解 StorageGRID 和 Dremio 如何合作提供現代化且有效率的資料湖基礎架構、以及 NetApp 如何從 Hive + HDFS 移轉至 Dremio + StorageGRID 、大幅提升巨量資料分析效率。

- "利用 NetApp StorageGRID 大幅提升巨量資料的效能"
- "StorageGRID 和 Dremio 提供現代化、功能強大且有效率的資料湖基礎架構"
- "NetApp 如何透過產品分析重新定義客戶體驗"

Hadoop S3A 調校

_ 作者： Angela Cheng _

Hadoop S3A 連接器可促進 Hadoop 應用程式與 S3 物件儲存之間的順暢互動。調整 Hadoop S3A Connector 是在使用 S3 物件儲存設備時最佳化效能的關鍵。在我們開始調整詳細資料之前、讓我們先基本瞭解 Hadoop 及其元件。

什麼是 **Hadoop** ？

- Hadoop * 是功能強大的開放原始碼架構、專為處理大規模資料處理與儲存而設計。它可跨電腦叢集進行分散式儲存和平行處理。

Hadoop 的三個核心元件為：

- * Hadoop HDFS （ Hadoop 分散式檔案系統） * ：此功能可處理儲存、將資料分成區塊、並在節點之間散佈。
- * Hadoop MapReduce * ：負責處理資料、將工作分割成較小的區塊、並平行執行。
- * 哈大諾布（又是另一個資源協商者）： * "有效管理資源並排程工作"

Hadoop HDFS 和 S3A 接頭

HDFS 是 Hadoop 生態系統的重要元件、在高效率的巨量資料處理中扮演重要角色。HDFS 提供可靠的儲存與管理功能。它可確保平行處理和最佳化的資料儲存、進而加快資料存取和分析速度。

在巨量資料處理中、 HDFS 在為大型資料集提供容錯儲存方面表現優異。它透過資料複寫來達成此目標。它可以在資料倉儲環境中儲存及管理大量的結構化和非結構化資料。此外、它還能與領先業界的巨量資料處理架構（例如 Apache Spark 、 Hive 、 Pig 和 Fllink ）無縫整合、實現可擴充且有效率的資料處理。它與 Unix （ Linux ）作業系統相容、是偏好使用 Linux 環境進行巨量資料處理的組織的理想選擇。

隨著資料量隨著時間成長、將新機器新增至 Hadoop 叢集、並使用其本身的運算和儲存設備的方法變得效率不彰。線性擴充會在有效使用資源和管理基礎架構方面帶來挑戰。

為了因應這些挑戰、 Hadoop S3A 連接器提供高效能 I/O 、可與 S3 物件儲存設備相較。運用S3A實作Hadoop工作流程、有助於將物件儲存設備當作資料儲存庫、並可將運算與儲存設備分開、進而獨立擴充運算與儲存設備。分離運算和儲存設備也能讓您將適當的資源量用於運算工作、並根據資料集的大小提供容量。因此、您可以降低Hadoop工作流程的整體TCO。

Hadoop S3A 接頭調校

S3 的行為與 HDFS 不同、有些為了保留檔案系統外觀的嘗試則不佳。為了最有效地使用 S3 資源、必須仔細調整 / 測試 / 實驗。

本文中的 Hadoop 選項是以 Hadoop 3.3.5 為基礎、請參閱 "Hadoop 3.3.5 core-site.xml" 適用於所有可用選項。

附註：在每個 Hadoop 版本中、某些 Hadoop FS.s3a 設定的預設值會有所不同。請務必查看您目前 Hadoop 版本的預設值。如果這些設定未在 Hadoop 核心網站 .xml 中指定、則會使用預設值。您可以使用 Spark 或 Hive 組態選項、在執行階段覆寫值。

您一定要來這裏 "Apache Hadoop 頁面" 以瞭解每個 FS.s3a 選項。如有可能、請在非正式作業 Hadoop 叢集中

測試它們、以找出最佳值。

您應該閱讀 "使用 S3A 連接器時發揮最大效能" 以取得其他調整建議。

讓我們來探討一些重要考量：

- 1。資料壓縮 *

請勿啟用 StorageGRID 壓縮。大部分的巨量資料系統使用位元組範圍 GET 、而非擷取整個物件。使用位元組範圍取得壓縮物件會大幅降低取得效能。

2.S3A 交付人 *

一般而言、建議使用 magic s3a committer 。請參閱此 "一般 S3A 交付選項頁面" 更深入瞭解魔術棒及其相關的 s3a 設定。

Magic Committer ：

Magic Committer 特別仰賴 S3Guard 在 S3 物件存放區上提供一致的目錄清單。

有了一致的 S3 （現在就是這樣）、萬智牌委員會就能安全地與任何 S3 儲存桶搭配使用。

選擇與實驗：

視您的使用案例而定、您可以在 Staging Committer （依賴叢集 HDFS 檔案系統）和 Magic Committer 之間進行選擇。

請嘗試兩者、以判斷哪一種最適合您的工作負載和需求。

總結來說、 S3A Commiters 提供解決方案、以因應對 S3 的一致、高效能及可靠輸出承諾這項基本挑戰。其內部設計可確保資料傳輸效率、同時維持資料完整性。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable “magic committer” support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

- 3.執行緒、連線集區大小和區塊大小 *
- 每個與單一貯體互動的 **S3A** 用戶端都有其專屬的開放式 HTTP 1.1 連線集區和執行緒、可用於上傳及複製作業。
- "您可以調整這些集區大小、以在效能與記憶體 / 執行緒使用量之間取得平衡"。
- 將資料上傳至 S3 時、資料會分成區塊。預設區塊大小為 32 MB 。您可以設定 FS.s3a.block.size 屬性來自訂此值。
- 較大的區塊大小可降低上傳期間管理多個零件的成本、進而改善大型資料上傳的效能。大型資料集的建議值為 256 MB 或更高。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

*4.多部分上傳 *

s3a commiters * Always * 使用 MPU （多部分上傳）將資料上傳至 S3 儲存庫。這是為了允許：工作失敗、工作的投機性執行、以及工作在提交前中止。以下是與多部分上傳相關的一些重要規格：

- 最大物件大小： 5 TiB （ TB ）。
- 每次上傳的最大零件數： 10 、 000 。
- 零件編號：範圍從 1 到 10 、 000 （含）。

- 零件大小：介於 5 MIB 和 5 GiB 之間。值得注意的是、您的多部分上傳最後一部分沒有最小大小限制。

將較小的零件大小用於 S3 多個部分上傳、既有優點也有缺點。

- 優點 * ：
- 從網路快速恢復問題：當您上傳較小的零件時、因為網路錯誤而重新啟動失敗上傳的影響會降至最低。如果零件失敗、您只需要重新上傳該特定零件、而不需要重新上傳整個物件。
- 更佳的平行化：可以同時上傳更多零件、同時利用多執行緒或並行連線。這種平行化可提升效能、尤其是處理大型檔案時。
- 缺點 * ：
- 網路負荷：較小的零件尺寸代表需要上傳更多零件、每個零件都需要自己的 HTTP 要求。更多 HTTP 要求會增加啟動和完成個別要求的成本。管理大量的小型零件可能會影響效能。
- 複雜度：管理訂單、追蹤零件、以及確保成功上傳可能會很麻煩。如果需要中止上傳、則需要追蹤和清除所有已上傳的零件。

若為 Hadoop 、建議使用 256 MB 或以上的零件大小、以使用 FS.s3a.multite.size 。請務必將 FS.s3a.mutlipart.threshold 值設為 2 x FS.s3a.multipe.size 值。例如、 fs.s3a.multipe.size = 256M 、 fs.s3a.mutlipart.threshold 應為 512M 。

大型資料集使用較大的零件大小。請務必根據您的特定使用案例和網路條件、選擇零件尺寸來平衡這些因素。

多部分上傳是 "三步驟程序"：

1. 上傳即會啟動、 StorageGRID 會傳回上傳 ID 。
2. 物件零件會使用 upload-id.
3. 上傳所有物件零件後、會傳送完整的多個部分上傳要求與 upload-id.StorageGRID 會從上傳的零件建構物件、用戶端可以存取物件。

如果未成功傳送完整的多部分上傳要求、則零件會留在 StorageGRID 中、不會建立任何物件。當工作中斷、失敗或中止時、就會發生這種情況。零件會保留在網格中、直到多個零件上傳完成或中止、或 StorageGRID 在上傳開始後 15 天內清除這些零件。如果在某個儲存庫中有許多（數十萬到數百萬）進行中的多部分上傳、當 Hadoop 傳送「 list-multify-upload 」（此要求不依上傳 ID 篩選）時、要求可能需要很長時間才能完成或最終逾時。您可以考慮將 FS.s3a.mutlipart.purge 設為 true 、並設定適當的 FS.s3a.multipe.pure.age 值（例如 5 至 7 天、請勿使用 86400 的預設值、即 1 天）。或請 NetApp 支援人員調查情況。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

*5.緩衝區將資料寫入記憶體 *

若要提升效能、您可以在將資料上傳至 S3 之前、先緩衝寫入記憶體中的資料。這樣可以減少小寫入次數、並提高效率。

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

請記住、 S3 和 HDFS 的運作方式各不相同。為了最有效地使用 S3 資源、必須仔細調整 / 測試 / 實驗。

TR-4871 ：使用 CommVault 設定 StorageGRID 進行備份與還原

使用 StorageGRID 和 CommVault 備份和恢復資料

CommVault 與 NetApp 攜手合作、共同打造共同的資料保護解決方案、結合 CommVault Complete Backup and Recovery for NetApp 軟體與 NetApp StorageGRID 雲端儲存軟體。CommVault 完整備份與還原與 NetApp StorageGRID 提供獨特且易於使用的解決方案、可協助您滿足全球快速資料成長與法規不斷增加的需求。

許多組織想要將儲存設備移轉至雲端、擴充系統、並將長期保留資料的原則自動化。雲端型物件儲存設備的恢復能力、擴充能力、營運效率和成本效益、是備份目標的自然選擇。CommVault 與 NetApp 於 2014 年聯合驗證了他們的聯合解決方案、之後更進一步整合了兩種解決方案。全球所有類型的客戶都採用 CommVault 完整備份與還原及 StorageGRID 組合解決方案。

關於 CommVault 和 StorageGRID

CommVault 完整備份與還原軟體是一種企業級的整合式資料與資訊管理解決方案、完全以單一平台為基礎、並以統一的程式碼基礎打造而成。其所有功能都會共享後端技術、提供完全整合的資料保護、管理及存取方法所帶來的無與倫比的優勢與效益。本軟體包含可保護、歸檔、分析、複寫及搜尋資料的模組。這些模組共用一組通用的後端服務和進階功能、可彼此順暢互動。此解決方案可解決企業中資料管理的所有層面、同時提供無限的擴充性、以及前所未有的資料與資訊控制能力。

NetApp StorageGRID 即 CommVault 雲端層是企業混合雲物件儲存解決方案。您可以在多個站台上部署、無論是在特定用途的應用裝置上、或是以軟體定義的部署方式進行部署。StorageGRID 可讓您建立資料管理原則、以決定資料的儲存和保護方式。StorageGRID 會收集您開發及執行原則所需的資訊。它會檢查各種特性和需求、包括效能、耐用性、可用度、地理位置、 壽命和成本。資料在不同位置之間移動時、以及隨著時間的變化、都會受到完整的維護和保護。

StorageGRID 智慧型原則引擎可協助您選擇下列任一選項：

- 使用抹除編碼在多個站台之間備份資料、以獲得恢復能力。
- 將物件複製到遠端站台、以將 WAN 延遲和成本降到最低。

當 StorageGRID 儲存物件時、無論物件位於何處或存在多少份複本、您都能以單一物件的方式存取物件。這種行為對災難恢復至關重要、因為有了這種情況、即使資料的一個備份複本毀損、 StorageGRID 也能還原您的資料。

在主儲存設備中保留備份資料可能會很昂貴。使用 NetApp StorageGRID 時、您可以將非作用中的備份資料移轉至 StorageGRID 、藉此釋放主儲存設備上的空間、同時享有 StorageGRID 的眾多功能。備份資料的價值會隨著時間而改變、儲存資料的成本也會隨之改變。StorageGRID 可以將主儲存設備的成本降至最低、同時提高資料的耐用度。

主要功能

CommVault 軟體平台的主要功能包括：

- 完整的資料保護解決方案、可支援虛擬與實體伺服器、 NAS 系統、雲端基礎架構及行動裝置上的所有主要作業系統、應用程式及資料庫。
- 透過單一主控台簡化管理：您可以檢視、管理及存取整個企業的所有功能及所有資料與資訊。

- 多種保護方法、包括資料備份與歸檔、快照管理、資料複寫、以及電子探索的內容索引。
- 使用重複資料刪除技術來管理磁碟與雲端儲存設備、實現高效率的儲存管理。
- 整合 NetApp 儲存陣列、例如 AFF 、 FAS 、 NetApp HCI 和 E 系列陣列、以及 NetApp SolidFire ^ ® ^ 橫向擴充儲存系統。也與 NetApp Cloud Volumes ONTAP 軟體整合、可在 NetApp 儲存產品組合中、自動建立索引化的應用程式感知 NetApp Snapshot ™複本。
- 完整的虛擬基礎架構管理功能、可支援領先業界的內部部署虛擬 Hypervisor 和公有雲超大規模平台。
- 進階安全功能可限制存取關鍵資料、提供精細的管理功能、並為 Active Directory 使用者提供單一登入存取。
- 原則型資料管理、可讓您根據業務需求（而非實體位置）來管理資料。
- 頂尖的終端使用者體驗、讓使用者能夠保護、尋找及恢復自己的資料。
- API 導向的自動化功能、可讓您使用 vRealize Automation 或 Service Now 等協力廠商工具來管理資料保護與還原作業。

如需支援工作負載的詳細資訊、請造訪 "CommVault 支援的技術"。

備份選項

當您使用雲端儲存設備實作 CommVault 完整備份與還原軟體時、您有兩個備份選項：

- 備份至主要磁碟目標、並將輔助複本備份至雲端儲存設備。
- 將雲端儲存備份為主要目標。

過去、雲端或物件儲存設備的效能太低、無法用於主要備份。使用主要磁碟目標可讓客戶加快備份與還原程序、並將輔助複本作為冷備份保留在雲端上。StorageGRID 代表新一代的物件儲存設備。StorageGRID 的效能和處理量都很高、而且效能和靈活度都超越其他物件儲存廠商的要求。

下表列出 StorageGRID 每個備份選項的優點：

	主要備份至磁碟、以及輔助複本至 **StorageGRID**	主要備份至 **StorageGRID**
效能	使用即時掛載或即時恢復、以最快的恢復時間：最適合 Tier0/Tier1 工作負載。	無法用於即時掛載或即時恢復作業。適用於串流還原作業和長期保留。
部署架構	使用所有 Flash 或旋轉磁碟做為第一個備份登陸層。StorageGRID 用作次層。	使用 StorageGRID 做為全方位備份目標、簡化部署。
進階功能（即時還原）	支援	不支援

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- StorageGRID 11.9 文件中心 +https://docs.netapp.com/us-en/storagegrid-119/[]

- NetApp 產品文件
  https://docs.netapp.com
- CommVault 說明文件
  https://documentation.commvault.com/2024/essential/index.html

已測試的解決方案總覽

經測試的解決方案結合了 CommVault 與 NetApp 解決方案、打造出強大的聯合解決方案。

解決方案設定

在實驗室設定中、 StorageGRID 環境包含四個 NetApp StorageGRID SG5712 應用裝置、一個虛擬主要管理節點和一個虛擬閘道節點。SG5712 應用裝置是入門級選項、是一種基礎組態。選擇更高效能的應用裝置選項、例如 NetApp StorageGRID SG5760 或 SG6060 、可提供顯著的效能優勢。請洽詢您的 NetApp StorageGRID 解決方案架構設計師、以取得規模調整協助。

對於資料保護原則、 StorageGRID 使用整合式生命週期管理（ ILM ）原則來管理及保護資料。ILM 規則會在原則中從上到下進行評估。我們實作下表所示的 ILM 原則：

ILM 規則	限定條件	擷取行為
銷毀編碼 2+1	超過 200KB 的物件	平衡
2 複本	所有物件	雙重承諾

ILM 2 複製規則是預設規則。「刪除編碼 2+1 」規則已套用至此測試、適用於任何 200 KB 或更大的物件。預設規則已套用至小於 200KB 的物件。以這種方式應用規則是 StorageGRID 最佳實務做法。

如需此測試環境的技術詳細資料、請參閱中的解決方案設計與最佳實務一節 "NetApp 透過 CommVault 實現橫向擴充資料保護" 技術報告。

StorageGRID 硬體規格

下表說明此測試所使用的 NetApp StorageGRID 硬體。StorageGRID SG5712 應用裝置搭配 10Gbps 網路是入門級選項、代表基本組態。SG5712 也可設定為 25Gbps 網路。

硬體	數量	磁碟	可用容量	網路
StorageGRID SG5712 設備	4.	48 x 4TB （近線 SAS HDD ）	136TB	10Gbps

選擇更高效能的應用裝置選項、例如 NetApp StorageGRID SG5760 、 SG6060 或所有 Flash SGF6112 應用裝置、可提供顯著的效能優勢。請洽詢您的 NetApp StorageGRID 解決方案架構設計師、以取得規模調整協助。

CommVault 與 StorageGRID 軟體需求

下表列出安裝在 VMware 軟體上的 CommVault 和 NetApp StorageGRID 軟體的軟體需求、以供我們測試。安裝了四個 MediaAgent 資料傳輸管理員和一個 CommServe 伺服器。在測試中、我們針對 VMware 基礎架構建置了 10Gbps 網路。下表

下表列出 CommVault 軟體的整體系統需求：

元件	數量	資料存放區	尺寸	總計	所需 **IOPS** 總計
CommServe 伺服器	1.	作業系統	500GB	500GB	不適用
		SQL	500GB	500GB	不適用
MediaAgent	4.	虛擬 CPU （ vCPU ）	16.	64	不適用
		RAM	128GB	512	不適用
		作業系統	500GB	2TB	不適用
		索引快取	2TB	8TB	超過 200 個
		DDB	2TB	8TB	200 至 80 萬 K

在測試環境中、在 NetApp E 系列 E2812 儲存陣列上、 VMware 上部署了一個虛擬主要管理節點和一個虛擬閘道節點。每個節點都位於不同的伺服器上、具有下表所述的最低線上環境需求：

下表列出 StorageGRID 虛擬管理節點和閘道節點的需求：

節點類型	數量	**VCPU**	**RAM**	儲存設備
閘道節點	1.	8.	24GB	適用於作業系統的 100GB LUN
管理節點	1.	8.	24GB	適用於作業系統的 100GB LUN 200 GB LUN 用於管理節點表 200 GB LUN 用於管理節點稽核記錄

StorageGRID 規模調整指南

請洽詢您的 NetApp 資料保護專家、以瞭解您環境的特定規模。NetApp 資料保護專家可使用 CommVault Total Backup Storage Calculator 工具來估計備份基礎架構需求。此工具需要 CommVault 合作夥伴入口網站存取權。如有需要、請註冊以取得存取權。

CommVault 規模調整輸入

下列工作可用於執行探索、以調整資料保護解決方案的規模：

- 識別需要保護的系統或應用程式 / 資料庫工作負載、以及對應的前端容量（以 TB 為單位）。
- 識別需要保護的 VM/ 檔案工作負載和類似的前端容量（ TB ）。
- 找出短期和長期的保留要求。
- 識別所識別資料集 / 工作負載的每日變更率 % 。
- 找出未來 12 、 24 及 36 個月的預測資料成長。
- 根據業務需求定義資料保護 / 恢復的 RTO 和 RPO 。

如果有這項資訊可用、就可以完成備份基礎架構規模調整、進而分析所需的儲存容量。

StorageGRID 規模調整指南

在您執行 NetApp StorageGRID 規模調整之前、請先考量工作負載的下列層面：

- 可用容量
- WORM 模式
- 平均物件大小
- 效能要求
- 已套用 ILM 原則

可用容量的數量必須符合您已分層至 StorageGRID 的備份工作負載大小、以及保留排程。

WORM 模式是否會啟用？在 CommVault 中啟用 WORM 時、這會在 StorageGRID 上設定物件鎖定。這將增加所需的物件儲存容量。所需容量會因保留期間和每個備份的物件變更數量而異。

平均物件大小是一種輸入參數、可協助調整 StorageGRID 環境中的效能大小。CommVault 工作負載使用的平均物件大小取決於備份類型。

下表依備份類型列出平均物件大小、並說明還原程序從物件存放區讀取的內容：

備份類型	平均物件大小	還原行為
在 StorageGRID 中製作輔助複本	32 MB	完全讀取 32 MB 物件
將備份導向 StorageGRID （啟用重複資料刪除）	8 MB	1MB 隨機範圍讀取
將備份導向 StorageGRID （停用重複資料刪除）	32 MB	完全讀取 32 MB 物件

此外、瞭解完整備份和遞增備份的效能需求、有助於判斷 StorageGRID 儲存節點的規模。StorageGRID 資訊生命週期管理（ ILM ）原則資料保護方法可決定儲存 CommVault 備份所需的容量、並影響網格的大小調整。

StorageGRID ILM 複寫是 StorageGRID 用來儲存物件資料的兩種機制之一。當 StorageGRID 將物件指派給複寫資料的 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。

銷毀編碼是StorageGRID 由程式碼庫用來儲存物件資料的第二種方法。當 StorageGRID 將物件指派給已設定為建立銷毀編碼複本的 ILM 規則時、它會將物件資料分割成資料片段。然後、它會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。存取物件時、會使用儲存的片段重新組裝物件。如果資料片段或同位元檢查片段毀損或遺失、抹除編碼演算法可以使用剩餘資料和同位元檢查片段的子集重新建立該片段。

這兩種機制需要不同的儲存容量、如以下範例所示：

- 如果您儲存兩個複寫複本、您的儲存負荷會加倍。
- 如果您儲存的是 2+1 銷毀編碼複本、您的儲存負荷會增加 1.5 倍。

針對測試的解決方案、在單一站台上使用入門級 StorageGRID 部署：

- 管理節點： VMware 虛擬機器（ VM ）
- 負載平衡器： VMware VM
- 儲存節點： 4 個 SG5712 、含 4TB 磁碟機
- 主要管理節點和閘道節點：具有最低正式作業工作負載需求的 VMware VM

StorageGRID 也支援協力廠商負載平衡器。

StorageGRID 通常部署在兩個或多個站台中、其資料保護原則可複寫資料、以防止節點和站台層級的故障。將資料備份到 StorageGRID 後、資料就會受到多個複本或銷毀編碼的保護、這些程式碼可透過演算法來獨立分離及重新組合資料。

您可以使用調整大小工具 "Fusion" 以調整網格大小。

擴充

您可以將儲存設備新增至儲存節點、將新的網格節點新增至現有站台、或新增資料中心站台、來擴充 NetApp StorageGRID 系統。您可以在不中斷目前系統運作的情況下執行擴充作業。
StorageGRID 可為儲存節點使用較高效能的節點、或是執行負載平衡器和管理節點的實體應用裝置、或只是新增其他節點、藉此擴充效能。

如需擴充 StorageGRID 系統的詳細資訊，請參閱 "StorageGRID 11.9 擴充指南"。

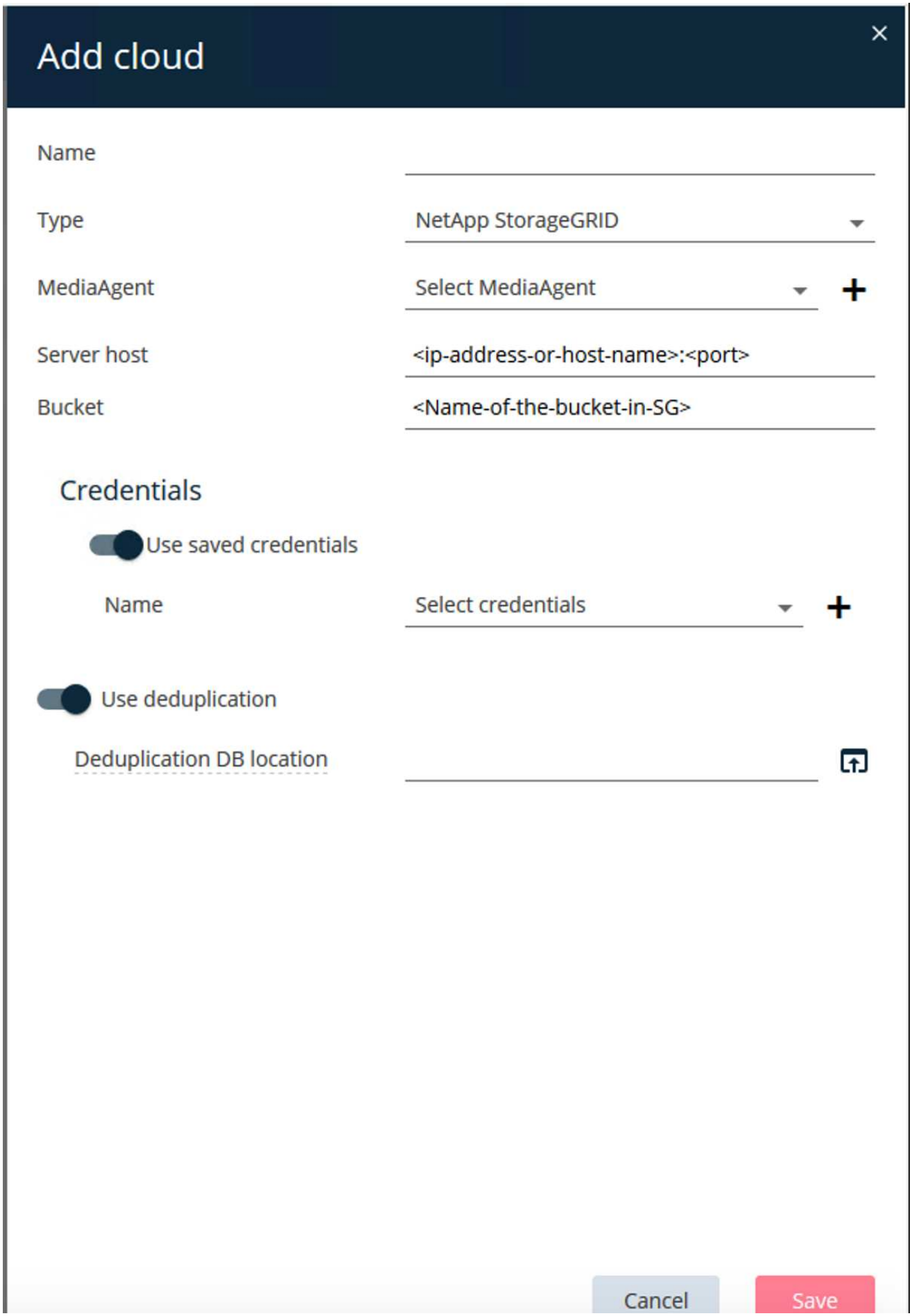
執行資料保護工作

若要使用 CommVault Complete Backup and Recovery for NetApp 來設定 StorageGRID 、請執行下列步驟、在 CommVault 軟體中將 StorageGRID 新增為雲端程式庫。

步驟 **1** ：使用 **StorageGRID** 設定 **CommVault**

步驟

1. 登入 CommVault Command Center 。在左側面板上、按一下儲存 > 雲端 > 新增以查看並回應新增雲端對話方塊：


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. 針對類型、選取 NetApp StorageGRID 。
3. 對於 MediaAgent 、請選取與雲端程式庫相關的所有項目。
4. 對於伺服器主機、請輸入 StorageGRID 端點的 IP 位址或主機名稱、以及連接埠號碼。

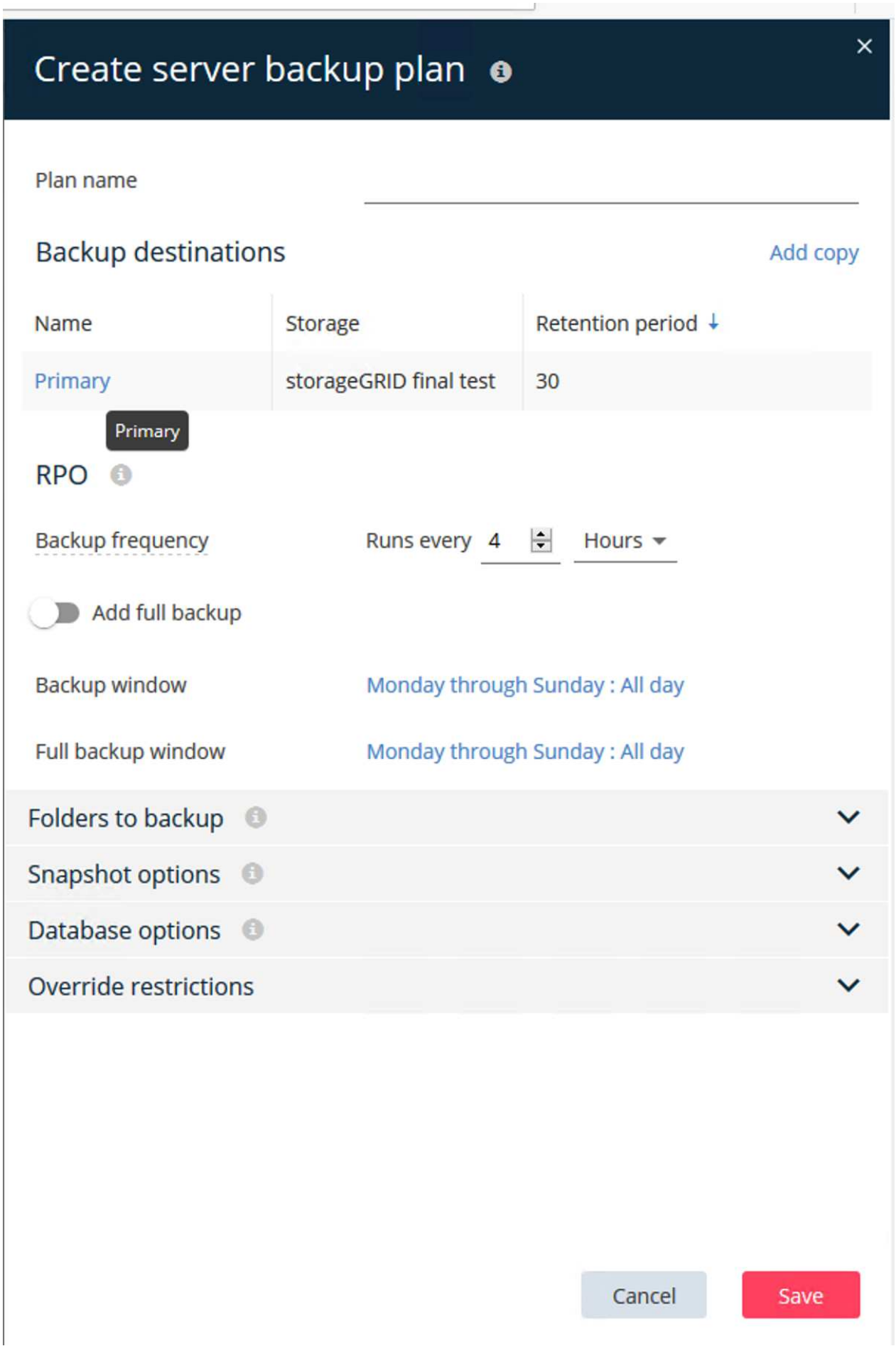
   請依照 StorageGRID 文件中的步驟進行 "如何設定負載平衡器端點（連接埠）"。請確定您有一個 HTTPS 連接埠、其中包含自我簽署的憑證、以及 StorageGRID 端點的 IP 位址或網域名稱。

5. 如果要使用重複資料刪除功能、請開啟此選項、並提供重複資料刪除資料庫位置的路徑。
6. 按一下儲存。

步驟 **2** ：以 **StorageGRID** 作為主要目標、建立備份計畫

步驟

1. 在左側面板上、選取管理 > 計畫以查看並回應「建立伺服器備份計畫」對話方塊。

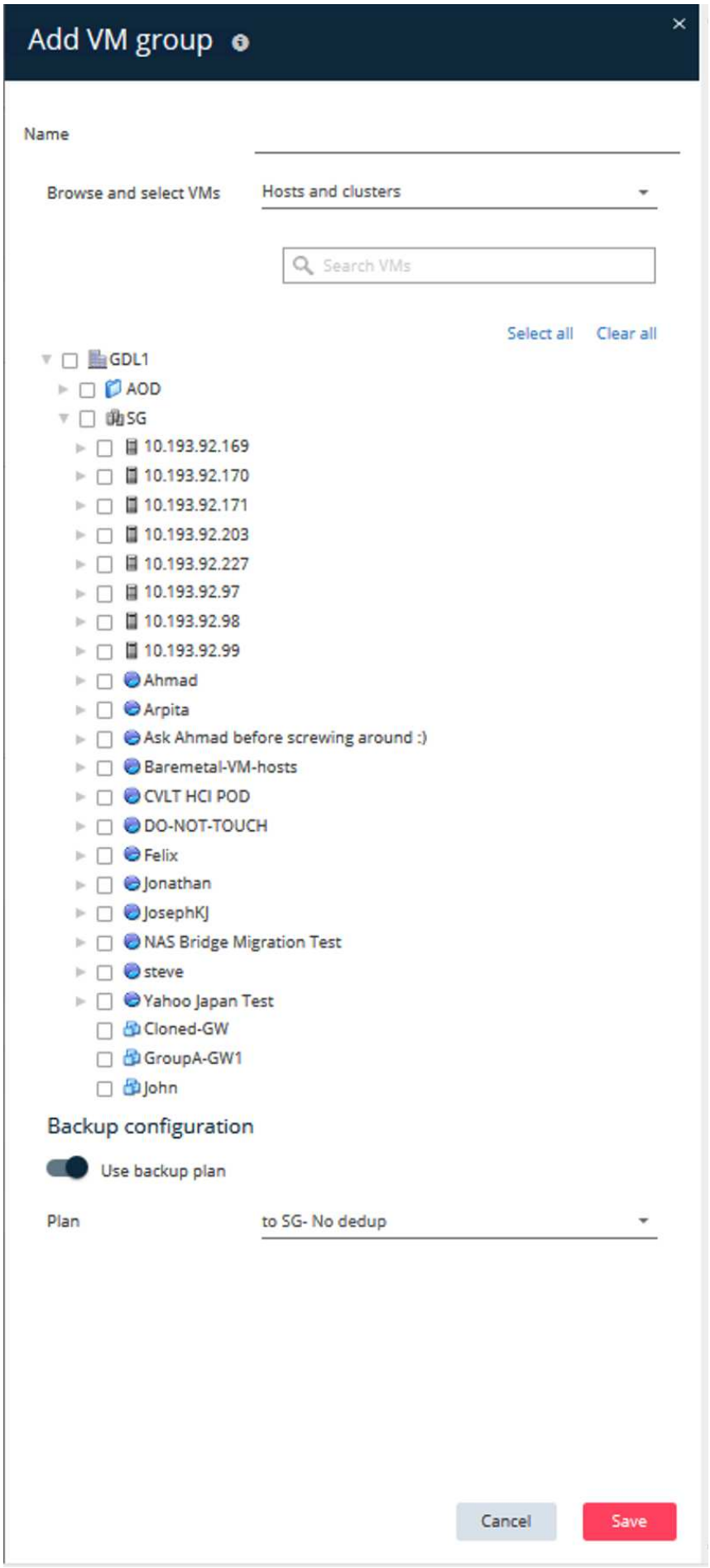

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. 輸入計畫名稱。
3. 選取您先前建立的 StorageGRID 簡易儲存服務（ S3 ）儲存備份目的地。
4. 輸入您想要的備份保留期間和恢復點目標（ RPO ）。
5. 按一下儲存。

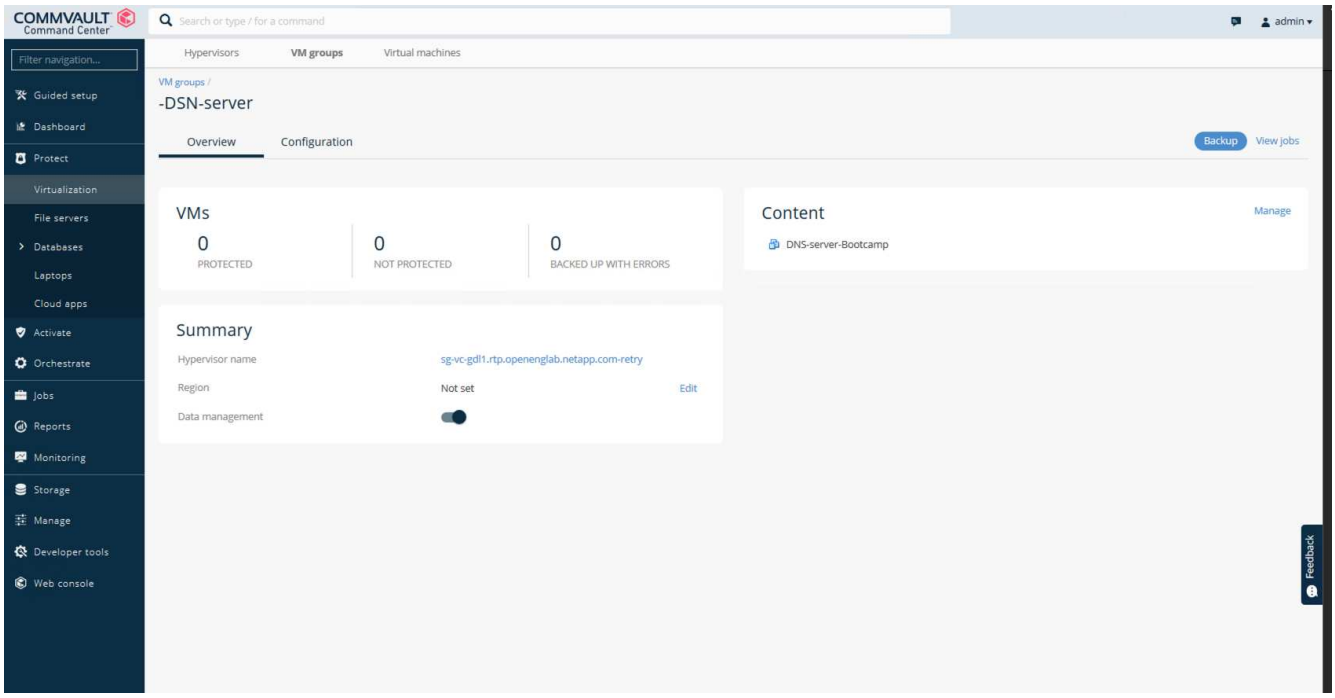
步驟 **3** ：開始備份工作以保護您的工作負載

步驟

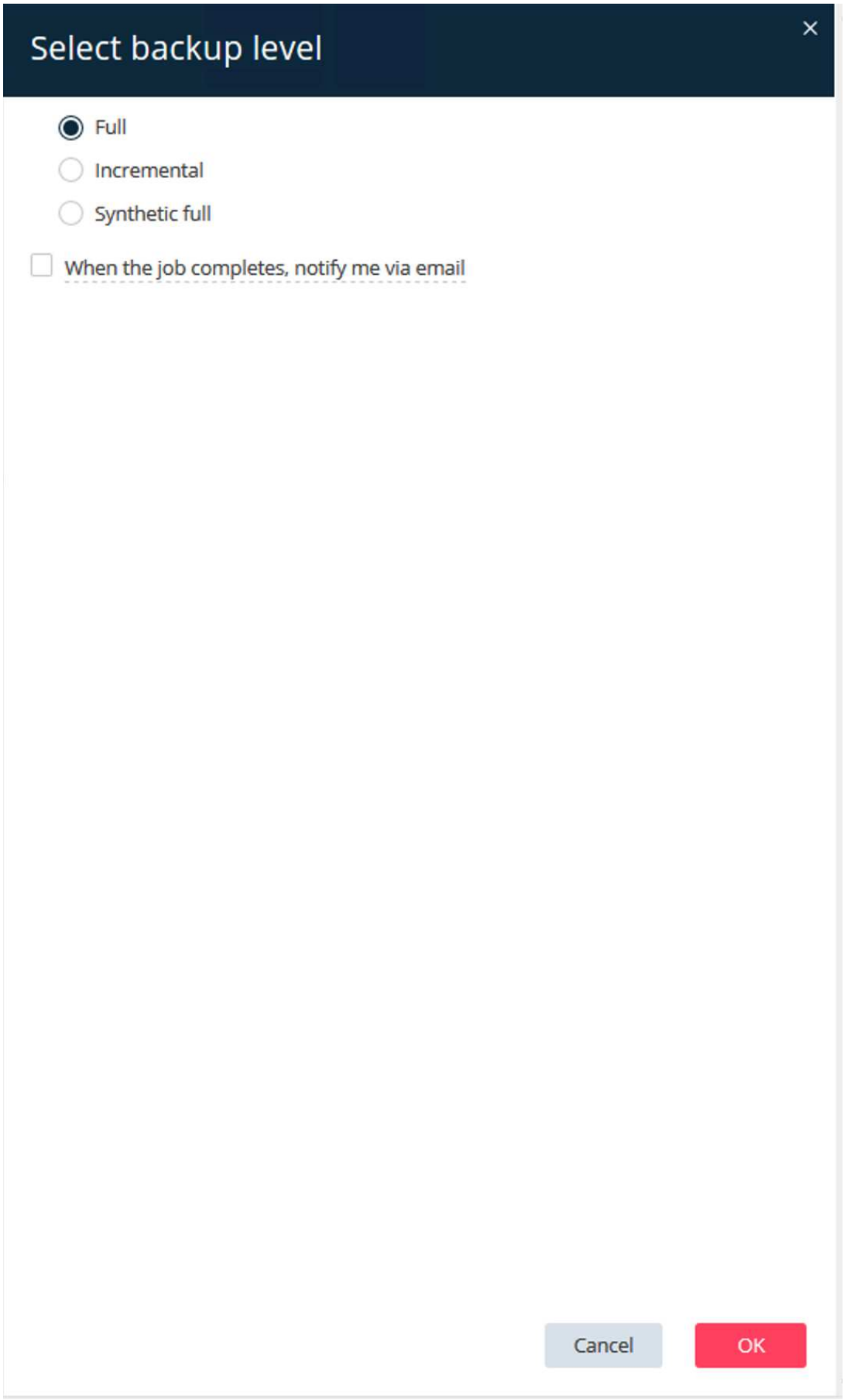
1. 在 CommVault Command Center 上、瀏覽至「 Protect 」 > 「 Virtualization 」。
2. 新增 VMware vCenter Server Hypervisor 。
3. 按一下您剛新增的 Hypervisor 。
4. 按一下「新增 VM 群組」以回應「新增 VM 群組」對話方塊、以便查看您計畫保護的 vCenter 環境。


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

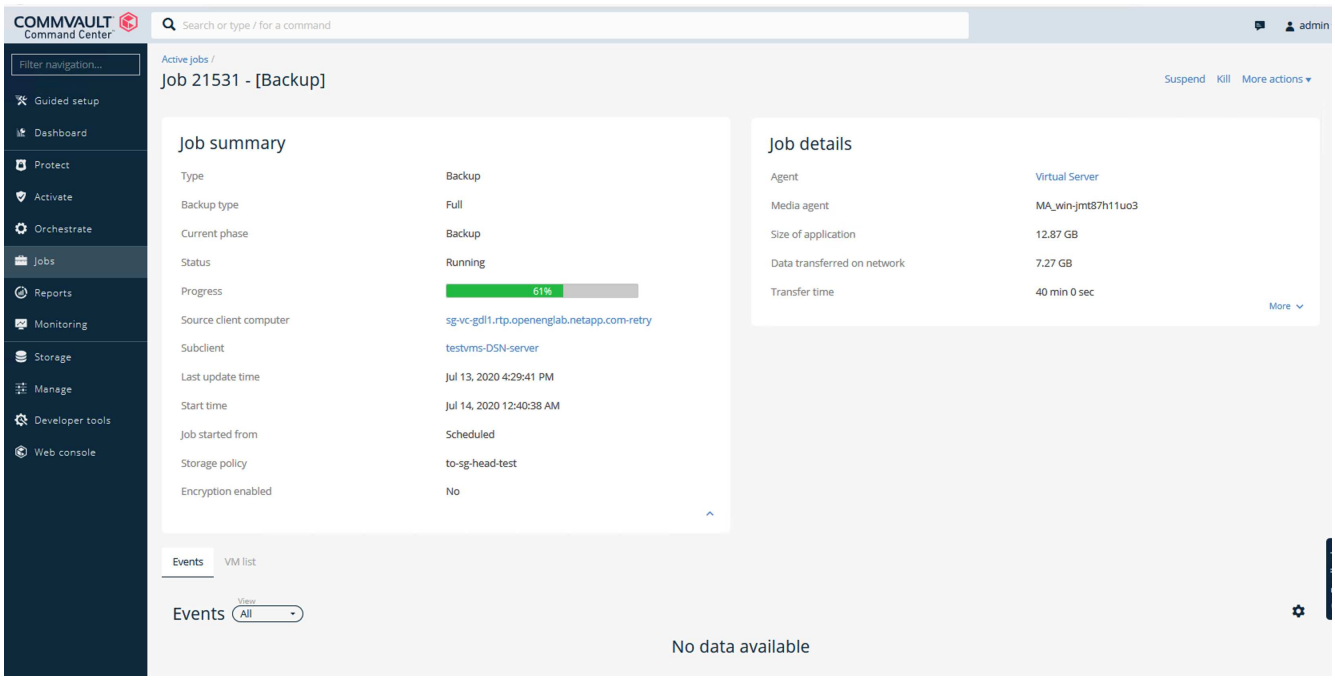
5. 選取資料存放區、 VM 或 VM 集合、然後輸入名稱。
6. 選取您在先前工作中建立的備份計畫。
7. 按一下「儲存」以查看您建立的 VM 群組。
8. 在 VM 群組視窗的右上角、選取備份：



9. 選擇 Full （完整）作為備份層級、（選擇性）在備份完成時要求電子郵件、然後按一下 OK （確定）開始備份工作：


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. 瀏覽至工作摘要頁面以檢視工作計量：



檢閱基準效能測試

在「輔助複製」作業中、四個 CommVault MediaAgent 將資料備份到 NetApp AFF A300 系統、並在 NetApp StorageGRID 上建立輔助複本。如需測試設定環境的詳細資訊、請參閱技術報告中的解決方案設計與最佳實務一節 "NetApp 透過 CommVault 實現橫向擴充資料保護" 。

這些測試是針對 100 個 VM 和 1000 個 VM 執行的、兩者都是以 50/50 混合的 Windows 和 CentOS VM 進行測試。下表顯示我們的基礎效能測試結果：

營運	備份速度	還原速度
輔助複製	2 TB/ 小時	1.27 TB/ 小時
直接往返物件（重複資料刪除開啟）	2.2 TB/ 小時	1.22 TB/ 小時

為了測試停機效能、刪除了 250 萬個物件。如圖 2 和圖 3 所示、刪除工作在 3 小時內完成、並釋放超過 80 TB 的空間。刪除工作於上午 10 ： 30 開始。

圖 **1** ：在 **3** 小時內刪除 **250** 萬（ **80 TB** ）物件。

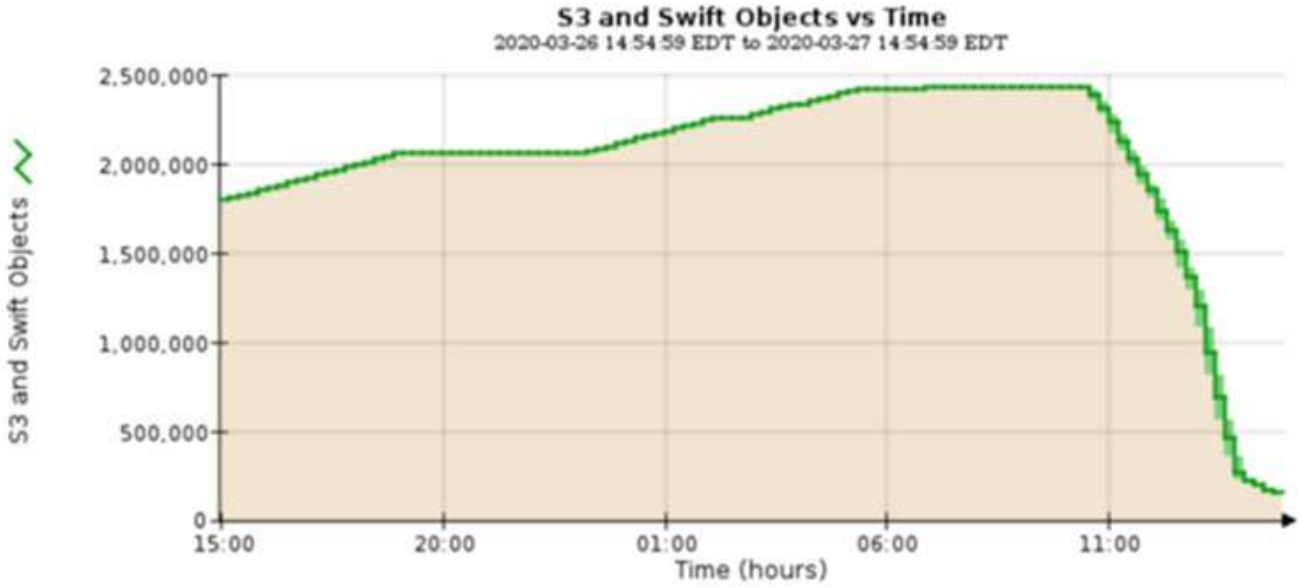
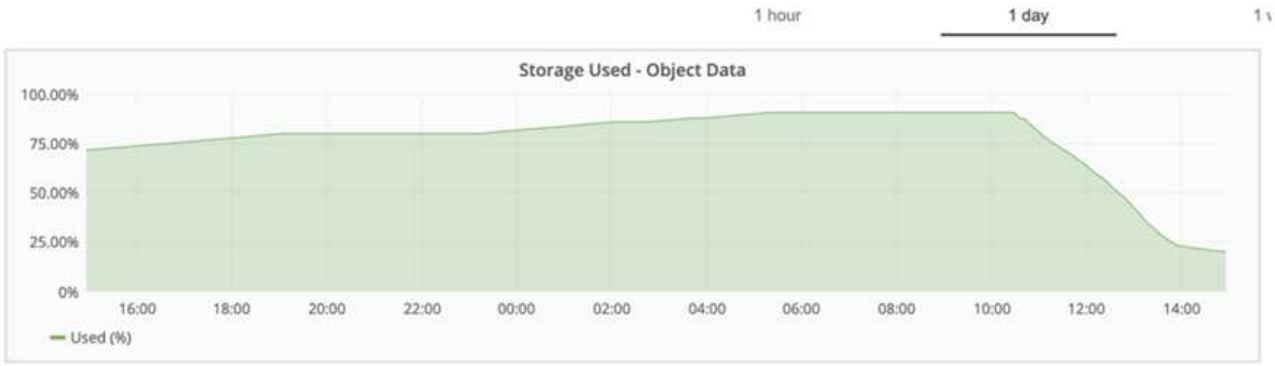


圖 **2** ：在 **3** 小時內釋放 **80TB** 的儲存空間。



貯體一致性層級建議

NetApp StorageGRID 可讓終端使用者選擇在 Simple Storage Service （ S3 ）貯體中物件上執行作業的一致性層級。

CommVault MediaAgent 是 CommVault 環境中的資料移動器。在大多數情況下、媒體代理程式都設定為在本機寫入主要 StorageGRID 站台。因此、建議在本機主要站台內建立高度一致性。當您在 StorageGRID 中建立的 CommVault 儲存區上設定一致性層級時、請遵循下列準則。

如果您的 CommVault 版本早於 11.0.0 - Service Pack 16 、請考慮將 CommVault 升級至最新版本。如果這不是選項、請務必遵循您版本的準則。

- CommVault 11.0.0 之前的版本 - Service Pack 16.* 在 11.0.0 之前的版本 - Service Pack 16 中、 CommVault 會執行 S3 head 、並在不存在的物件上執行作業、作為還原和修剪程序的一部分。將貯體一致性層級設為強式站台、以達到 CommVault 備份至 StorageGRID 的最佳一致性層級。
- CommVault 11.0.0 版 - Service Pack 16 及更新版本。 * 在 11.0.0 版 - Service Pack 16 及更新版本中、 S3 head 和 Get 作業在不存在的物件上執行的次數會降至最低。將預設的儲存區一致性層級設為「新寫入後讀取」、以確保 CommVault 和 StorageGRID 環境中的高一致性層級。

TR-4626 ：負載平衡器

將協力廠商負載平衡器搭配 **StorageGRID** 使用

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

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

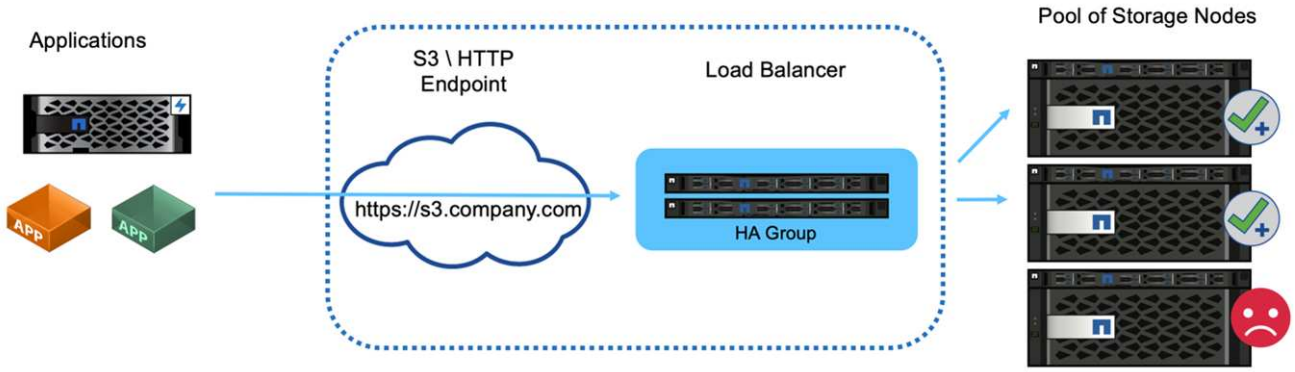
物件儲存是雲端儲存的同義詞、而且正如您所期望的、應用程式會透過 URL 利用雲端儲存位址來處理該儲存。在這個簡單的 URL 之後、 StorageGRID 可以在單一站台或跨地理分佈式站台擴充容量、效能和耐用度。使這種簡易性成爲可能的元件是負載平衡器。

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

負載平衡器基礎知識

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

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



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

本機和全域負載平衡器

負載平衡器有兩種類型：

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

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

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

使用**StorageGRID**負載平衡器

了解StorageGRID網關節點負載平衡器的作用。

實作NetApp® StorageGRID® 網關節點的一般指南。

StorageGRID 閘道節點負載平衡器與協力廠商負載平衡器的比較

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

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

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

StorageGRID 負載平衡器具有下列優點：

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

作為StorageGRID的整合節點，本地流量管理器能夠使用進階健康檢查根據儲存節點健康狀況、負載和資源可用性來分配請求。此外，當站點之間的StorageGRID連結成本設定為「0」時，它還能夠在多個站點之間分配負載。如果儲存節點不可用但網關節點在站點中可用，則負載將自動定向到網格中的另一個站點。

網關節點的負載平衡器快取功能旨在為某些工作負載（例如 AI 訓練）提供顯著的效能改進，這些工作負載在處理資料的過程中會多次重新讀取資料集。快取網關節點還可以部署在與網格其餘部分物理遠離的位置，從而在某些工作負載下實現更好的效能並降低 WAN 網路利用率。快取以讀回模式運行，其中寫入不會被緩存，也不會修改快取的狀態。每個快取網關獨立於任何其他快取網關節點運作。

有關部署StorageGRID網關節點的詳細信息，請參閱 "本文檔StorageGRID"。

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

瞭解在 StorageGRID 中實作 SSL 憑證的重要性和步驟。

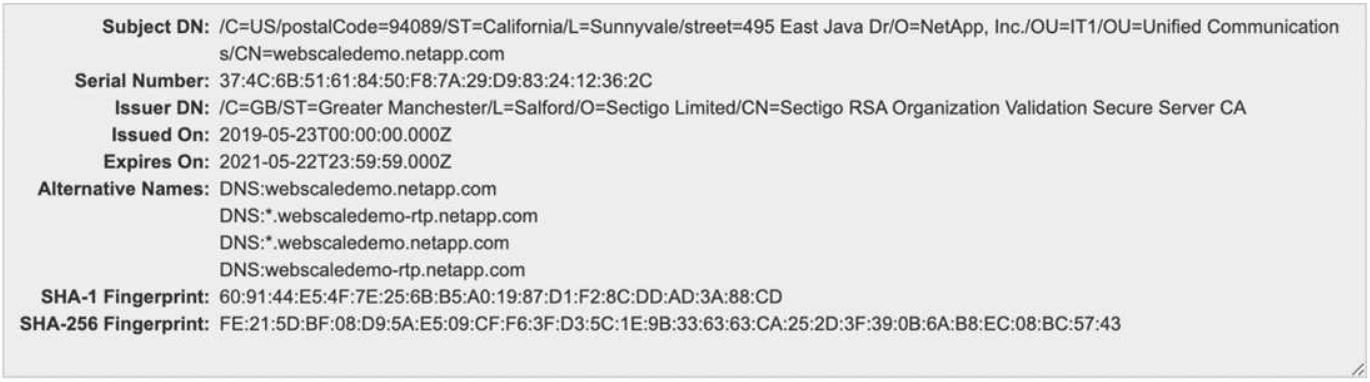
如果您使用 HTTPS 、則必須擁有安全通訊端層（ SSL ）憑證。SSL 通訊協定會識別用戶端和端點、並將它們驗證為信任的。SSL 也能加密流量。SSL 憑證必須由用戶端信任。若要達成此目的、 SSL 憑證可以來自全球信任的憑證授權單位（ CA ）、例如 DigiCert 、在基礎架構中執行的私有 CA 、或是主機產生的自我簽署憑證。

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

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

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

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



在 **StorageGRID** 中設定信任的協力廠商負載平衡器

瞭解如何在 StorageGRID 中設定信任的協力廠商負載平衡器。

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

瞭解本機流量管理負載平衡器

探索本機流量管理負載平衡器的指引、並判斷最佳組態。

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

建立儲存節點資源群組

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

- S3 HTTPS ： 18082
- S3 HTTP ： 18084

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

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

健全狀況檢查

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

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

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

建議的輪詢間隔是每秒一次、在三次失敗檢查之後、將節點標示為離線。

S3 健全狀況檢查範例

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

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

檔案或內容型健全狀況檢查

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

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

如果需要內容型健全狀況檢查、請使用專屬租戶搭配專用 S3 儲存區。

工作階段持續性

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

虛擬代管型定址

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

若要支援虛擬代管樣式、請執行下列動作：

- 支援萬用字元 DNS 查詢： * .s3.company.com

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

SSL 終止

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

支援的組態有三種：

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

傳遞組態

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

來源用戶端 **IP** 可見度

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

若要啟用 XFF 標頭來檢視用戶端應用程式的 IP 、請遵循下列步驟：

步驟

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

負載平衡策略

大多數負載平衡解決方案都提供多種負載平衡策略。以下是常見策略：

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

隨著可選擇的儲存節點數量增加、演算法的選擇變得不那麼重要。

資料路徑

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

驗證連線的發佈

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

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

瞭解 StorageGRID 組態的幾個使用案例

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

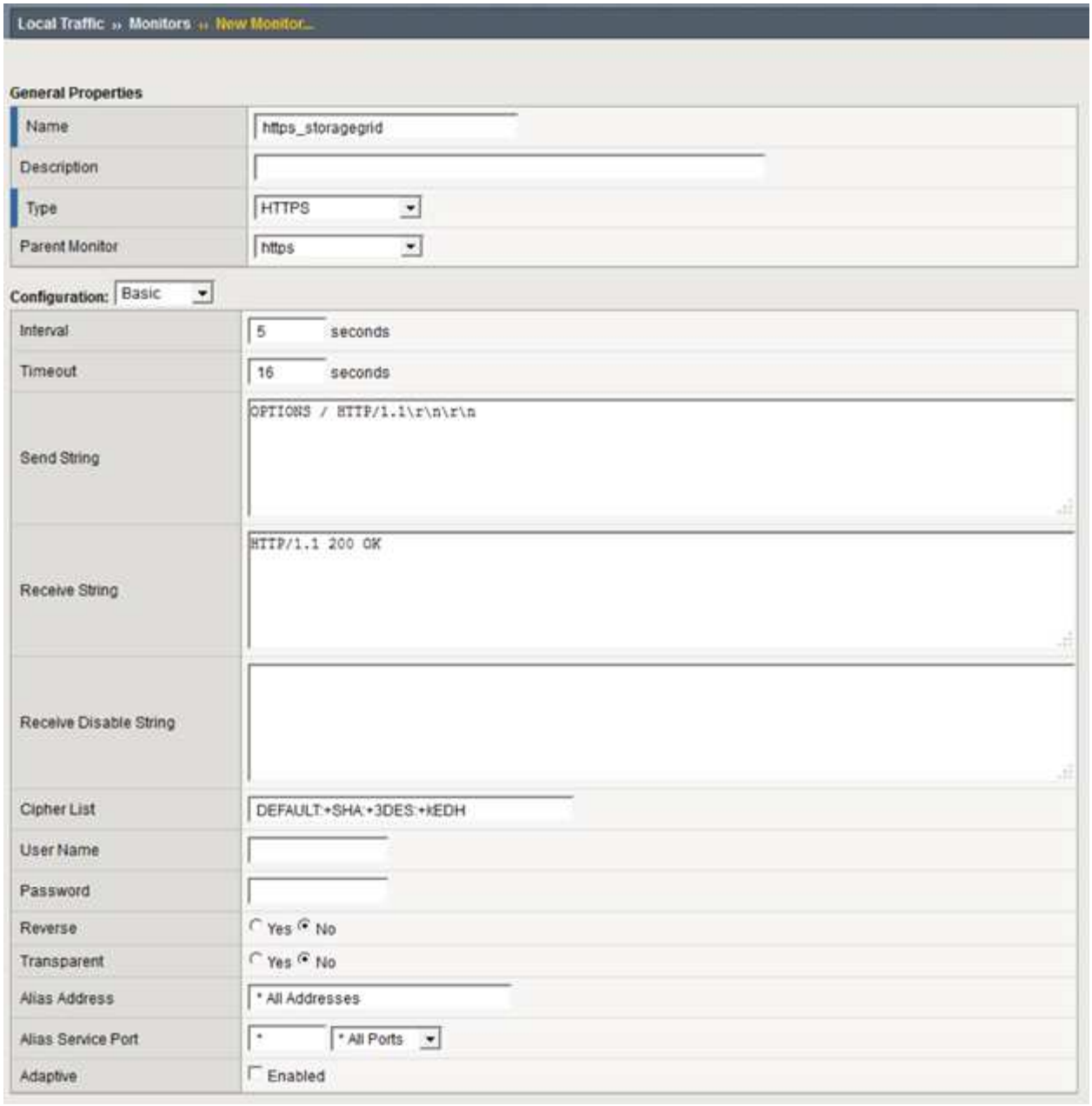
下列範例說明 StorageGRID 客戶實作的組態、包括 NetApp IT 。

F5 BIG-IP 本機流量管理程式狀態檢查監控 S3 貯體

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

步驟

1. 建立新的監視器。
   a. 在 Type （類型）字段中，輸入 `HTTPS`。
   b. 視需要設定時間間隔和逾時。
   c. 在「傳送字串」欄位中、輸入 `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n 為回車； BIG-IP 軟體的不同版本需要零、一或兩組 \r\n 順序。如需更多資訊、請參閱 https://support.f5.com/csp/article/K10655。
   d. 在接收字串欄位中、輸入： `HTTP/1.1 200 OK`。



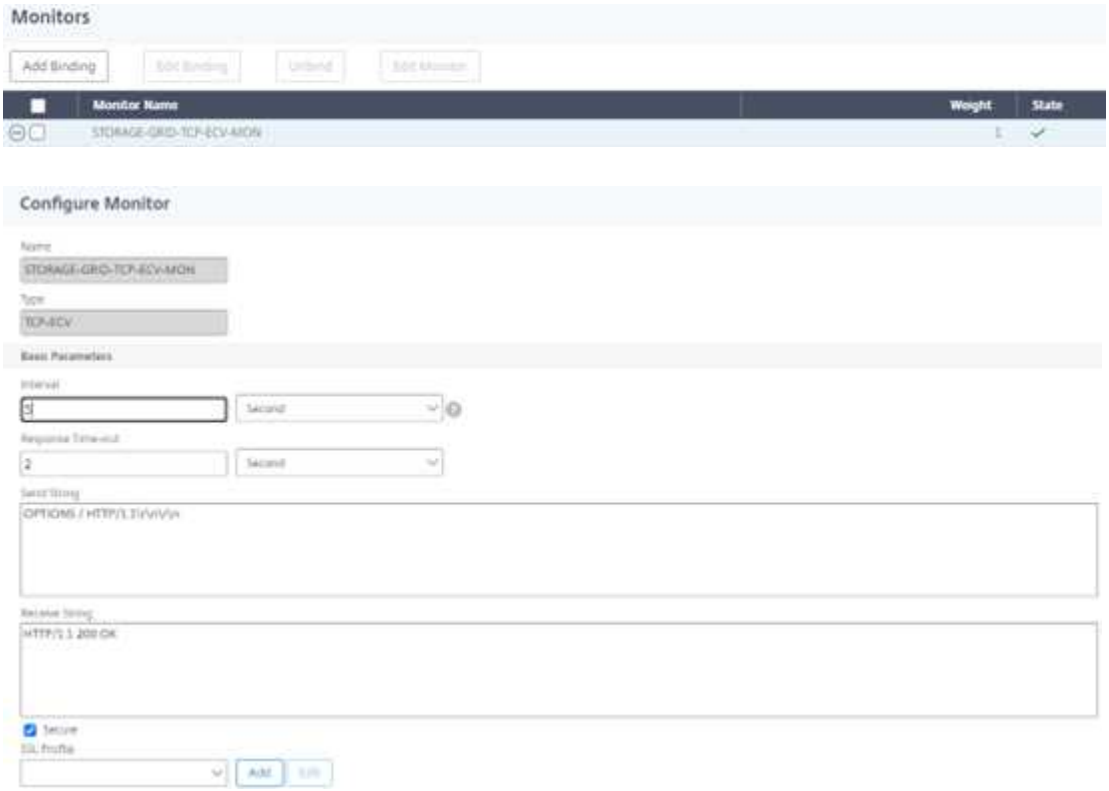
2. 在 " 建立集區 " 中，針對所需的每個連接埠建立一個集區。
   a. 指派您在上一個步驟中建立的健全狀況監視器。
   b. 選取負載平衡方法。
   c. 選取服務連接埠： 18082 （ S3 ）。
   d. 新增節點。

Citrix NetScaler

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

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

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



Loadbalancer.org

Loadbalancer.org 已經與 StorageGRID 進行了自己的整合測試，並提供了廣泛的組態指南：https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf。

Kemp

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

HAProxy

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

以下是 HAProxy 上 SSL 終止的範例：

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

以下是 SSL 傳遞的範例：

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

如需 StorageGRID 組態的完整範例、請參閱 "HAProxy 組態範例" GitHub 上的。

驗證 **StorageGRID** 中的 **SSL** 連線

瞭解如何在 StorageGRID 中驗證 SSL 連線。

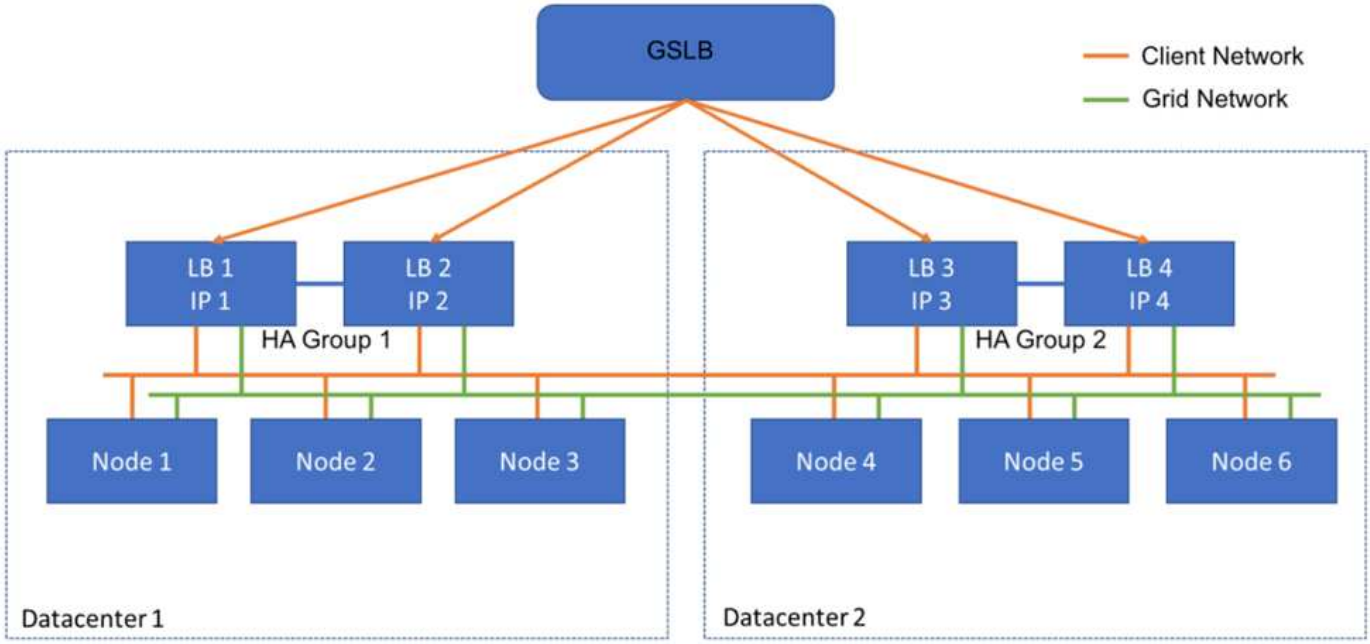
設定負載平衡器之後、您應該使用 Openssl 和 AWS CLI 等工具來驗證連線。其他應用程式（例如 S3 瀏覽器）可能會忽略 SSL 組態錯誤。

瞭解 **StorageGRID** 的整體負載平衡需求

探索 StorageGRID 中的整體負載平衡設計考量與需求。

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

時提供 GSLB 和站台本機負載平衡。



TR-4645 ：安全功能

保護物件存放區中的 **StorageGRID** 資料和中繼資料安全

探索 StorageGRID 物件儲存解決方案的整合式安全功能。

這是NetApp® StorageGRID® 中眾多安全功能的概述，涵蓋資料存取、物件和元資料、管理存取和平台安全。它已更新，包含StorageGRID 12.0 發布的最新功能。

安全性是 NetApp StorageGRID 物件儲存解決方案不可或缺的一部分。安全性特別重要、因為許多適合物件儲存的豐富內容資料類型、本質上也很敏感、而且必須遵守法規與法規。隨著 StorageGRID 功能不斷進化、軟體提供許多安全功能、對於保護組織的安全狀態和協助組織遵循業界最佳實務實務非常寶貴。

本文概述了StorageGRID 12.0 中的眾多安全功能，分為五類：

- 資料存取安全功能
- 物件和中繼資料安全功能
- 系統管理安全功能
- 平台安全功能
- 雲端整合

本文旨在成為一份安全資料表——它沒有詳細說明如何配置系統以支援其中列舉的預設未配置的安全功能。這"StorageGRID 強化指南"可在官方 "StorageGRID 文件"頁。

除了本報告中所述的功能外， StorageGRID 還遵循 "NetApp 產品安全性弱點回應與通知原則"。報告的弱點會根據產品安全性事件回應程序進行驗證及回應。

NetApp StorageGRID 為要求嚴苛的企業物件儲存使用案例提供進階安全功能。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID ： SEC 17a-4(f) 、 FINRA 4511 （ c ）和 CFTC 1.31 （ c ） - （ d ）法規遵循評估 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 核心加密認證 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B 熵認證 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID加拿大網路安全中心通用準則認證 https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID文件頁面https://docs.netapp.com/us-en/storagegrid/[]
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/

詞彙與縮寫

本節提供文件中所用術語的定義。

術語或縮寫	定義
S3	簡易儲存服務：
用戶端	可透過 S3 傳輸協定與 StorageGRID 進行資料存取的應用程式、或是用於管理的 HTTP 傳輸協定。
租戶管理	StorageGRID 租戶帳戶的管理員
租戶使用者	StorageGRID 租戶帳戶中的使用者
TLS	傳輸層安全性
ILM	資訊生命週期管理
LAN	區域網路
網格管理員	StorageGRID 系統管理員
網格	StorageGRID 系統
鏟斗	儲存在 S3 中的物件容器
LDAP	輕量型目錄存取傳輸協定
秒	證券交易委員會；規範交易所成員、經紀商或交易商
FINRA	金融產業監管局；遵守 SEC 法規 17a-4(f) 的格式與媒體要求
CFTC	商品期貨交易佣金；規範商品期貨交易
NIST	國家標準和技術研究所

資料存取安全功能

瞭解 StorageGRID 的資料存取安全功能。

功能	功能	影響	法規遵循
可設定的傳輸層安全性（ TLS ）	TLS 會為用戶端與 StorageGRID 閘道節點、儲存節點或負載平衡器端點之間的通訊建立信號交換傳輸協定。 StorageGRID 支援下列 TLS 加密套件： • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 支援 TLS v1.2 與 1.3 。 不支援 SSLv3、TLS v1.1 及更早版本。	讓用戶端和 StorageGRID 能夠識別和驗證彼此、並與機密性和資料完整性進行通訊。確保使用最新的 TLS 版本。密碼現在可在組態 / 安全性設定下進行設定	—

功能	功能	影響	法規遵循
可設定的伺服器憑證（負載平衡器端點）	網格管理員可以設定負載平衡器端點來產生或使用伺服器憑證。	可讓使用由其標準信任憑證授權單位（ CA ）簽署的數位憑證、針對每個負載平衡器端點、在網格和用戶端之間驗證物件 API 作業。	—
可設定的伺服器憑證（ API 端點）	網格管理員可以集中設定所有 StorageGRID API 端點、以使用組織信任 CA 簽署的伺服器憑證。	啟用使用由標準信任 CA 簽署的數位憑證、以驗證用戶端與網格之間的物件 API 作業。	—
多租戶	StorageGRID 每個網格都支援多個租戶、每個租戶都有自己的命名空間。租戶提供 S3 傳輸協定；根據預設、只有帳戶內的使用者才能存取貯體 / 容器和物件。租戶可以有一位使用者（例如、每位使用者都有自己的帳戶的企業部署）或多位使用者（例如、服務供應商部署、其中每個帳戶都是公司和服務供應商的客戶）。使用者可以是本機或同盟使用者；同盟使用者是由 Active Directory 或輕量型目錄存取通訊協定（ LDAP ）所定義。StorageGRID 提供個別租戶儀表板、讓使用者使用其本機或同盟帳戶認證登入。使用者可以根據網格管理員指派的配額、存取租戶使用量的視覺化報告、包括儲存於儲存區的資料和物件中的使用資訊。具有管理權限的使用者可以執行租戶層級的系統管理工作、例如管理使用者、群組和存取金鑰。	可讓 StorageGRID 管理員在隔離租戶存取的同時、託管來自多個租戶的資料、並透過與外部身分識別提供者（例如 Active Directory 或 LDAP ）聯合使用者來建立使用者身分識別。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
存取認證的不可否認性	每個 S3 作業都會以唯一的租戶帳戶、使用者和存取金鑰來識別和記錄。	允許 Grid 系統管理員建立哪些個人執行哪些 API 動作。	—
停用匿名存取	根據預設、 S3 帳戶的匿名存取已停用。要求者必須擁有有效的存取認證、才能存取帳戶中的貯體、容器或物件。可以使用明確的 IAM 原則來啟用對 S3 儲存區或物件的匿名存取。	允許 Grid 管理員停用或控制對貯體 / 容器和物件的匿名存取。	—

功能	功能	影響	法規遵循
法規遵循 WORM	專為符合 SEC 法規 17a-4(f) 的要求而設計、並由 Cohasset 驗證。客戶可以在貯體層級實現法規遵循。保留可延長、但絕不會減少。 資訊生命週期管理（ ILM ）規則可強制執行最低的資料保護層級。	允許具有法規資料保留要求的租戶、在儲存的物件和物件中繼資料上啟用 WORM 保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
WORM	網格管理員可啟用「停用用戶端修改」選項、以啟用全網格 WORM 、避免用戶端覆寫或刪除所有租戶帳戶中的物件或物件中繼資料。 S3 租戶管理員也可以透過指定 IAM 原則、依租戶、貯體或物件首碼來啟用 WORM 、其中包括自訂 S3 ：物件和中繼資料覆寫的 PutOverwriteObject 權限。	允許 Grid 管理員和租戶管理員控制儲存物件和物件中繼資料上的 WORM 保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
KMS 主機伺服器加密金鑰管理	網格管理員可以在網格管理程式中設定一或多個外部金鑰管理伺服器（ KMS ）、為 StorageGRID 服務和儲存設備提供加密金鑰。每個 KMS 主機伺服器或 KMS 主機伺服器叢集都使用金鑰管理互通性通訊協定（ KMIP ）、為相關 StorageGRID 站台的應用裝置節點提供加密金鑰。	資料靜止加密已完成。應用裝置磁碟區加密後、除非節點可以與 KMS 主機伺服器通訊、否則您無法存取應用裝置上的任何資料。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
自動容錯移轉	StorageGRID 提供內建的備援功能和自動容錯移轉功能。即使有多個故障、從磁碟或節點到整個站台、仍可繼續存取租戶帳戶、貯體和物件。StorageGRID 可識別資源、並自動將要求重新導向至可用的節點和資料位置。StorageGRID 站台甚至可以在著陸模式下運作；如果 WAN 中斷會中斷站台與系統其餘部分的連線、則讀取和寫入作業可以繼續使用本機資源、並在 WAN 恢復時自動恢復複寫作業。	讓 Grid 管理員能夠處理正常運作時間、 SLA 及其他合約義務、並實作業務持續性計畫。	—

功能	功能	影響	法規遵循
• S3 特有的資料存取安全功能 *	AWS 簽名第 2 版和第 4 版	簽署 API 要求可為 S3 API 作業提供驗證。Amazon 支援兩個版本的簽名版本 2 和版本 4 。簽署程序會驗證要求者的身分、保護傳輸中的資料、並防範可能的重播攻擊。	符合 AWS 對簽名版本 4 的建議、並可與舊版應用程式與簽名版本 2 向下相容。
—	S3物件鎖定	StorageGRID 中的 S3 物件鎖定功能是一種物件保護解決方案、相當於 Amazon S3 中的 S3 物件鎖定。	允許租戶建立啟用 S3 物件鎖定的貯體、以符合規定、要求特定物件保留一段固定時間或無限期。
SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)	S3 認證的安全儲存	S3 存取金鑰是以受密碼雜湊功能（ SHA-2 ）保護的格式儲存。	結合金鑰長度（ 10^{31} 隨機產生的數字）和密碼雜湊演算法、可安全儲存存取金鑰。
—	有時間限制的 S3 存取金鑰	為使用者建立 S3 存取金鑰時、客戶可以設定存取金鑰的到期日和時間。	讓 Grid 系統管理員可以選擇配置暫存 S3 存取金鑰。
—	每個使用者帳戶有多個存取金鑰	StorageGRID 可為使用者帳戶建立多個存取金鑰、並同時啟用多個存取金鑰。由於每個 API 動作都會以租戶使用者帳戶和存取金鑰記錄、因此即使多個金鑰處於作用中狀態、仍會保留不可否認性。	讓用戶端能夠不中斷地旋轉存取金鑰、並讓每個用戶端都擁有自己的金鑰、從而阻止用戶端之間的金鑰共用。
—	S3 IAM 存取原則	StorageGRID 支援 S3 IAM 原則、可讓 Grid 管理員依租戶、貯體或物件首碼指定精細的存取控制。StorageGRID 也支援 IAM 原則條件和變數、允許更多動態存取控制原則。	允許 Grid 系統管理員依整個租戶的使用者群組指定存取控制、也可讓租戶使用者指定自己的貯體和物件的存取控制。
—	S3 安全性令牌服務 API AssumeRole	StorageGRID支援 S3 STS API AssumeRole 提供具有縮小範圍的權限和有限持續時間的臨時安全憑證（存取金鑰 ID、秘密存取金鑰、會話令牌）。作為 AssumeRole API 的一部分，支援內嵌會話策略來進一步限制會話期間的權限。	允許租用戶管理員提供對對象資料的安全臨時存取。

功能	功能	影響	法規遵循
—	簡單通知服務	StorageGRID支援在物件存取時發送通知。支援以下事件類型： • s3：物件創建： • s3：物件創建：放置 • s3：物件創建：發布 • s3：物件創建：複製 • s3：物件創建：完成分段上傳 • s3：物件已移除： • s3：物件已移除：刪除 • s3：物件已移除：刪除標記已建立 • s3：對象恢復：發布	允許租用戶管理員監控對象的存取
—	使用 StorageGRID 託管金鑰（ SSE ）進行伺服器端加密	StorageGRID 支援 SSE 、可透過 StorageGRID 管理的加密金鑰、為靜止的資料提供多租戶保護。	可讓租戶加密物件。寫入和擷取這些物件需要加密金鑰。
SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)	使用客戶提供的加密金鑰（ SSE-C ）進行伺服器端加密	StorageGRID 支援 SSE-C 、可透過用戶端管理的加密金鑰、為靜止的資料提供多租戶保護。 雖然 StorageGRID 管理所有物件加密和解密作業、但使用 SSE-C 時、用戶端必須自行管理加密金鑰。	可讓用戶端使用其控制的金鑰來加密物件。寫入和擷取這些物件需要加密金鑰。

物件和中繼資料安全性

探索 StorageGRID 中的物件和中繼資料安全功能。

功能	功能	影響	法規遵循
進階加密標準（ AES ）伺服器端物件加密	StorageGRID 提供以 AES 128 和 AES 256 為基礎的伺服器端物件加密。網格管理員可以啟用加密作為全域預設設定。StorageGRID 也支援 S3 x-amz-server-Side 加密標頭、可針對每個物件啟用或停用加密。啟用時、物件會在儲存或在網格節點之間傳輸時加密。	有助於保護物件的儲存和傳輸、不受基礎儲存硬體的影響。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)

功能	功能	影響	法規遵循
內建金鑰管理	啟用加密時、每個物件都會以隨機產生的唯一對稱金鑰進行加密、此金鑰會儲存在 StorageGRID 內部、而不會有外部存取。	無需外部金鑰管理即可加密物件。	
符合聯邦資訊處理標準（ FIPS ） 140-2 標準的加密磁碟	SG5812 、 SG5860 、 SG6160 和 SGF6024 StorageGRID 應用裝置提供 FIPS 140-2 相容加密磁碟的選項。磁碟的加密金鑰可由外部 KMIP 伺服器選擇性管理。	可安全儲存系統資料、中繼資料和物件。也提供 StorageGRID 軟體型物件加密、可保護物件的儲存和傳輸。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
符合聯邦資訊處理標準 (FIPS) 140-3 的節點加密	SG5812、SG5860、SG6160、SGF6112、SG1100 和 SG110 StorageGRID設備提供符合 FIPS 140-3 的節點加密選項。節點的加密金鑰由外部 KMIP 伺服器管理。	可安全儲存系統資料、中繼資料和物件。也提供 StorageGRID 軟體型物件加密、可保護物件的儲存和傳輸。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
背景完整性掃描與自我修復	StorageGRID 在物件和子物件層級使用雜湊、校驗和循環備援檢查（ CRC ）的互鎖機制、以防止物件在儲存和傳輸時發生資料不一致、竄改或修改。StorageGRID 會自動偵測毀損和竄改的物件並加以取代、同時隔離變更的資料並向管理員發出警示。	讓 Grid 管理員能夠滿足 SLA 、法規及其他資料耐用性相關義務。協助客戶偵測試圖加密、竄改或修改資料的勒索軟體或病毒。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
原則型物件放置與保留	StorageGRID 可讓 Grid 系統管理員設定 ILM 規則、以指定物件保留、放置、保護、轉換和到期。網格管理員可以設定 StorageGRID 、依其中繼資料篩選物件、並在各種精細度層級套用規則、包括網格範圍、租戶、貯體、金鑰首碼、 以及使用者定義的中繼資料金鑰值配對。StorageGRID 有助於確保物件在整個生命週期內都依照 ILM 規則儲存、除非用戶端明確刪除。	協助強制執行資料放置、保護及保留。協助客戶達成 SLA 、以確保持久性、可用度和效能。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
背景中繼資料掃描	StorageGRID 會定期掃描背景中的物件中繼資料、以套用 ILM 指定的物件資料放置或保護變更。	協助探索毀損的物件。	

功能	功能	影響	法規遵循
可調一致性	租戶可以在貯體層級選擇一致性層級、以確保多站台連線等資源可用。	提供選項、只有在必要數量的站台或資源可用時、才會將寫入內容提交至網格。	

系統管理安全功能

探索 StorageGRID 的管理安全功能。

功能	功能	影響	法規遵循
伺服器憑證（網格管理介面）	Grid 系統管理員可以設定 Grid Management Interface 使用組織信任 CA 簽署的伺服器憑證。	使用由標準信任 CA 簽署的數位憑證、驗證管理用戶端和網格之間的管理 UI 和 API 存取。	—
管理使用者驗證	系統管理使用者會使用使用者名稱和密碼進行驗證。系統管理使用者和群組可以是本機或同盟的、從客戶的 Active Directory 或 LDAP 匯入。本機帳戶密碼以受 bcrypt 保護的格式儲存；命令列密碼以 SHA-2 保護的格式儲存。	驗證管理 UI 和 API 的管理存取權。	—
SAML 支援	StorageGRID 支援使用安全聲明標記語言 2.0 （ SAML 2.0 ）標準的單一登入（ SSO ）。啟用SSO時、所有使用者必須先經過外部身分識別供應商的驗證、才能存取Grid Manager、租戶管理程式、Grid Management API 或租戶管理API。本機使用者無法登入StorageGRID 到無法使用的功能。	為網格和租戶管理員提供更高層級的安全性、例如 SSO 和多因素驗證（ MFA ）。	NIST SP800-63
精細的權限控制	網格管理員可以將權限指派給角色、並將角色指派給管理使用者群組、以強制執行管理用戶端可以同時使用管理 UI 和 API 來執行的工作。	允許 Grid 管理員管理管理員使用者和群組的存取控制。	—

功能	功能	影響	法規遵循
分散式稽核記錄	StorageGRID 提供內建的分散式稽核記錄基礎架構、可擴充至多達 16 個站台的數百個節點。StorageGRID 軟體節點會產生稽核訊息、這些訊息會透過備援稽核轉送系統傳輸、最後會擷取到一或多個稽核記錄儲存庫中。稽核訊息會擷取物件層級精細度的事件、例如用戶端啟動的 S3 API 作業、 ILM 的物件生命週期事件、背景物件健全狀況檢查、以及從管理 UI 或 API 所做的組態變更。 審計日誌可以透過 syslog 匯出，從而允許 Splunk 和 ELK 等工具挖掘審計訊息。審計訊息有四種類型： • 系統稽核訊息 • 物件儲存稽核訊息 • HTTP 傳輸協定稽核訊息 • 管理稽核訊息 審計日誌可以儲存在 S3 儲存桶中，以便長期保留和應用程式存取。	為 Grid 管理員提供經過實證且可擴充的稽核服務、讓他們能夠為各種目標挖掘稽核資料。這類目標包括疑難排解、稽核 SLA 效能、用戶端資料存取 API 作業、以及管理組態變更。	—
系統稽核	系統稽核訊息會擷取與系統相關的事件、例如網格節點狀態、毀損的物件偵測、根據 ILM 規則在所有指定位置提交的物件、以及全系統維護工作的進度（網格工作）。	協助客戶疑難排解系統問題、並提供依據其 SLA 儲存物件的證明。SLA 是由 StorageGRID ILM 規則實作、並受到完整性保護。	—
物件儲存稽核	物件儲存稽核訊息會擷取物件 API 交易和生命週期相關事件。這些事件包括物件儲存和擷取、網格節點對網格節點傳輸和驗證。	協助客戶透過系統稽核資料進度、以及是否提供指定為 StorageGRID ILM 的 SLA 。	—

功能	功能	影響	法規遵循
HTTP 傳輸協定稽核	HTTP 傳輸協定稽核訊息會擷取與用戶端應用程式和 StorageGRID 節點相關的 HTTP 傳輸協定互動。此外、客戶可以擷取特定的 HTTP 要求標頭（例如 X 轉寄的 for 和使用者中繼資料 [x-amz-meta-*] ）進行稽核。	協助客戶稽核用戶端與 StorageGRID 之間的資料存取 API 作業、並追蹤個別使用者帳戶和存取金鑰的動作。客戶也可以將使用者中繼資料登入稽核、並使用 Splunk 或 elk 等記錄採礦工具來搜尋物件中繼資料。	—
管理稽核	管理稽核訊息會將管理使用者要求記錄到管理 UI （ Grid Management Interface ）或 API 。並非取得API或取得API要求的每個要求、都會以使用者名稱、IP和API要求類型來記錄回應。	協助 Grid 管理員建立系統組態變更記錄、記錄使用者在何時從哪個來源 IP 和目的地 IP 所做的變更。	—
TLS 1.3 支援管理 UI 和 API 存取	TLS 會為管理用戶端和 StorageGRID 管理節點之間的通訊建立信號交換傳輸協定。	可讓管理用戶端和 StorageGRID 識別及驗證彼此、並與機密性和資料完整性通訊。	—
StorageGRID 監控用的 SNMPv3	SNMPv3 同時提供強大的驗證和資料加密功能來保護隱私、進而提供安全性。在 v3 中、傳輸協定資料單元會使用 CBC-DES 進行加密、以用於加密傳輸協定。 傳送傳輸協定資料單元的使用者驗證是由 HMAC-SHA 或 HMAC-MD5 驗證傳輸協定提供。 仍支援 SNMPv2 和 v1 。	在管理節點上啟用 SNMP 代理程式、協助 Grid 管理員監控 StorageGRID 系統。	—
Prometheus計量匯出的用戶端憑證	網格管理員可以上傳或產生用戶端憑證、這些憑證可用於提供對 StorageGRID Prometheus 資料庫的安全、驗證存取。	網格管理員可以使用用戶端憑證、使用 Grafana 等應用程式從外部監控 StorageGRID 。	—

平台安全功能

瞭解 StorageGRID 的平台安全功能。

功能	功能	影響	法規遵循
內部公開金鑰基礎架構（ PKI ）、節點憑證和 TLS	StorageGRID 使用內部 PKI 和節點憑證來驗證和加密節點間通訊。節點間通訊受到 TLS 的保護。	協助保護 LAN 或 WAN 上的系統流量、特別是在多站台部署中。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
節點防火牆	StorageGRID 會自動設定 IP 表格和防火牆規則、以控制傳入和傳出網路流量、以及關閉未使用的連接埠。	協助保護 StorageGRID 系統、資料和中繼資料、防範來路不明的網路流量。	—
作業系統強化	強化 StorageGRID 實體應用裝置和虛擬節點的基礎作業系統；移除不相關的軟體套件。	有助於將潛在的攻擊面降至最低。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
定期更新平台和軟體	StorageGRID 提供包括作業系統、應用程式二進位檔和軟體更新的一般軟體版本。	協助 StorageGRID 系統以最新的軟體和應用程式二進位檔進行更新。	—
停用透過安全 Shell （ SSH ）的根登入	在所有 StorageGRID 節點上、都會停用透過 SSH 的根登入。SSH 存取使用憑證驗證。	協助客戶防範 root 登入的潛在遠端密碼破解。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
自動時間同步	StorageGRID 會自動將每個節點的系統時鐘與多個外部時間網路時間傳輸協定（ NTP ）伺服器同步。至少需要四個階層 3 或更新版本的 NTP 伺服器。	確保所有節點的時間參照相同。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
獨立的網路、用於用戶端、管理和內部網格流量	StorageGRID 軟體節點和硬體應用裝置支援多個虛擬和實體網路介面、讓客戶可以在不同的網路上分隔用戶端、管理和內部網格流量。	允許 Grid 管理員隔離內部和外部網路流量、並透過不同 SLA 的網路提供流量。	—
多個虛擬 LAN （ VLAN ）介面	StorageGRID 支援在 StorageGRID 用戶端和網格網路上設定 VLAN 介面。	允許 Grid 管理員分割和隔離應用程式流量、以確保安全性、靈活度和效能。	
不受信任的用戶端網路	不受信任的用戶端網路介面只接受已明確設定為負載平衡器端點的連接埠上的傳入連線。	確保暴露於不受信任網路的介面受到保護。	—
可設定的防火牆	管理管理、網格和用戶端網路的開放和封閉連接埠。	允許網格管理員控制連接埠的存取、並管理核准的裝置對連接埠的存取。	

功能	功能	影響	法規遵循
增強的 SSH 行為	安裝前預設禁用 SSH。在預設狀態下，僅在連結本機管理連接埠位址上啟用 SSH 存取。管理者和 root 使用者密碼設定為裝置計算控制器序號。僅允許在序列控制台和圖形控制台（BMC KVM）上登入。任何網路連接埠上的 SSH 均已停用。	增強網路存取保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
節點加密	作為 KMS 主機伺服器加密新功能的一部分、 StorageGRID 應用裝置安裝程式會新增節點加密設定。	此設定必須在裝置安裝的硬體組態階段啟用。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)

雲端整合

瞭解 StorageGRID 如何與雲端服務整合。

功能	功能	影響
以通知為基礎的病毒掃描	StorageGRID 平台服務支援事件通知。事件通知可與外部雲端運算服務搭配使用、以觸發資料上的病毒掃描工作流程。	可讓租戶管理員使用外部雲端運算服務觸發資料的病毒掃描。

TR-4921 ：勒索軟體防禦

保護 **StorageGRID S3** 物件免受勒索軟體的侵害

瞭解勒索軟體攻擊、以及如何使用 StorageGRID 安全最佳實務來保護資料。

勒索軟體攻擊不斷增加。本文件針對如何保護 StorageGRID 上的物件資料提供一些建議。

現今的勒索軟體是資料中心永遠存在的危險。勒索軟體旨在加密資料、使依賴資料的使用者和應用程式無法使用。保護從強化網路和可靠使用者安全實務的一般防禦措施開始、我們必須遵循資料存取安全實務。

勒索軟體是當今最大的安全威脅之一。NetApp StorageGRID 團隊正與我們的客戶合作、以對抗這些威脅。使用物件鎖定和版本設定功能、您可以防範不必要的變更、並從惡意攻擊中恢復。資料安全性是一項多層風險、您的物件儲存設備只是資料中心的一部分。

StorageGRID 最佳實務做法

對於 StorageGRID 、安全性最佳實務做法應包括使用 HTTPS 搭配簽署的憑證、以進行管理和物件存取。為應用程式和個人建立專屬的使用者帳戶、請勿使用租戶根帳戶來存取應用程式或存取使用者資料。換句話說、請遵循最低權限原則。使用具有定義身分識別與存取管理（ IAM ）原則的安全性群組來管理使用者權限、以及存取應用程式和使用者專屬的帳戶。有了這些措施、您仍必須確保資料受到保護。在 Simple Storage Service （ S3 ）的情況下、當物件經過修改以加密時、則是透過覆寫原始物件來完成。

防禦方法

S3 API 的主要勒索軟體保護機制是實作物件鎖定。並非所有應用程式都與物件鎖定相容、因此本報告中說明的還有兩個其他選項可保護您的物件：複寫到另一個已啟用版本設定的儲存庫、以及使用 IAM 原則進行版本設定。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

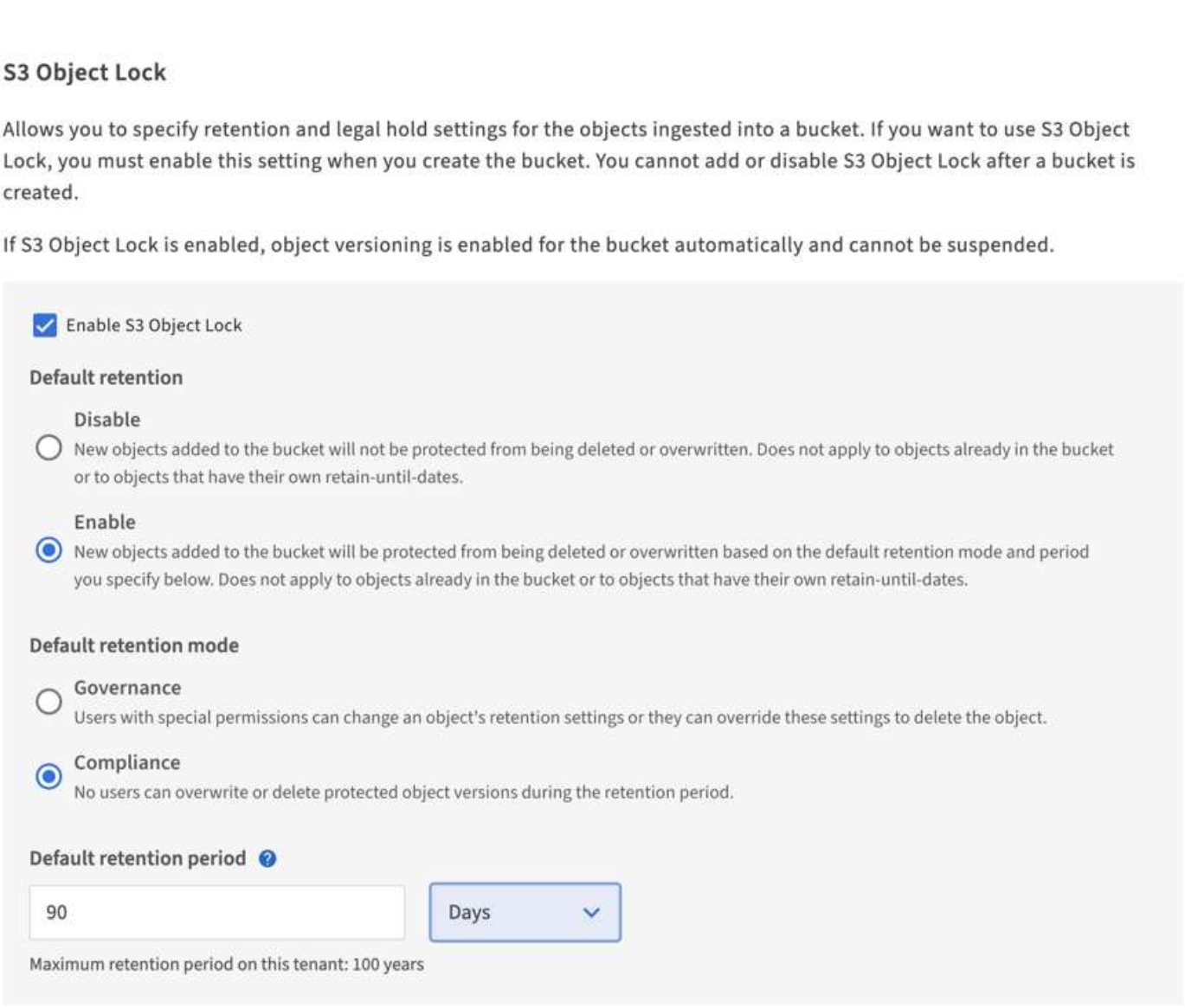
- NetApp StorageGRID文檔中心https://docs.netapp.com/us-en/storagegrid/[]
- NetApp StorageGRID 啟用 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/

使用物件鎖定的勒索軟體防禦

探索 StorageGRID 中的物件鎖定如何提供 WORM 模式來防止資料刪除或覆寫、以及它如何符合法規要求。

物件鎖定提供 WORM 模式、可防止物件遭到刪除或覆寫。StorageGRID 實作物件鎖定 "Cohasset 已評估" 有助於符合法規要求、支援合法持有、符合性模式、以及物件保留的治理模式、以及預設貯體保留原則。您必須啟用物件鎖定、以做為貯體建立和版本設定的一部分。物件的特定版本已鎖定、如果未定義版本 ID 、則保留會置於物件的目前版本上。如果目前版本已設定保留、並嘗試刪除、修改或覆寫物件、則會以刪除標記或物件的新修訂版做為目前版本來建立新版本、 鎖定的版本會保留為非目前版本。對於尚未相容的應用程式、您仍可以使用物件鎖定和儲存在貯體上的預設保留組態。定義組態之後、這會將物件保留套用至置入貯體的每個新物件。只要將應用程式設定為在保留時間過去之前不刪除或覆寫物件、就會生效。

在租用戶管理 UI 中建立儲存桶時，您可以啟用物件鎖定並配置預設保留模式和保留期限。配置後，這將為提取到該儲存桶的每個物件設定最小物件鎖定保留。



以下是使用物件鎖定 API 的幾個範例：

物件鎖定合法保留是套用至物件的簡單開 / 關狀態。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

如果成功、設定合法保留狀態不會傳回任何值、因此可以使用「取得」操作來驗證。

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

若要關閉合法保留、請套用關閉狀態。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

設定物件保留會以保留到時間戳記完成。

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

同樣地、成功後沒有傳回的值、因此您可以使用 GET 通話來驗證保留狀態。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

在啟用物件鎖定的貯體上放置預設保留、會使用以天和年為單位的保留期間。

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

如同大多數的作業一樣、成功時不會傳回任何回應、因此我們可以執行 Get 來驗證組態。

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

接下來、您可以在套用保留組態的情況下、將物件放入貯體中。

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Put 作業會傳回回應。

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

在保留物件上、上一個範例中、貯體上設定的保留期間會轉換成物件上的保留時間戳記。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

使用複製的貯體搭配版本管理功能來防範勒索軟體

瞭解如何使用 StorageGRID CloudMirror 將物件複寫到次要儲存庫。

並非所有應用程式和工作負載都能與物件鎖相容。另一個選項是將物件複寫到同一個網格中的次要儲存格（最好是存取受限的不同租戶）、或是任何其他具有 StorageGRID 平台服務 CloudMirror 的 S3 端點。

StorageGRID CloudMirror 是 StorageGRID 的一個元件、可設定為在物件擷取到來源儲存區時、將儲存區的物件複寫到定義的目的地、而不會複寫刪除內容。由於 CloudMirror 是 StorageGRID 的整合式元件、因此它無法被 S3 API 型攻擊關閉或操控。您可以在啟用版本設定的情況下、設定此複寫儲存區。在這種情況下、您需要自

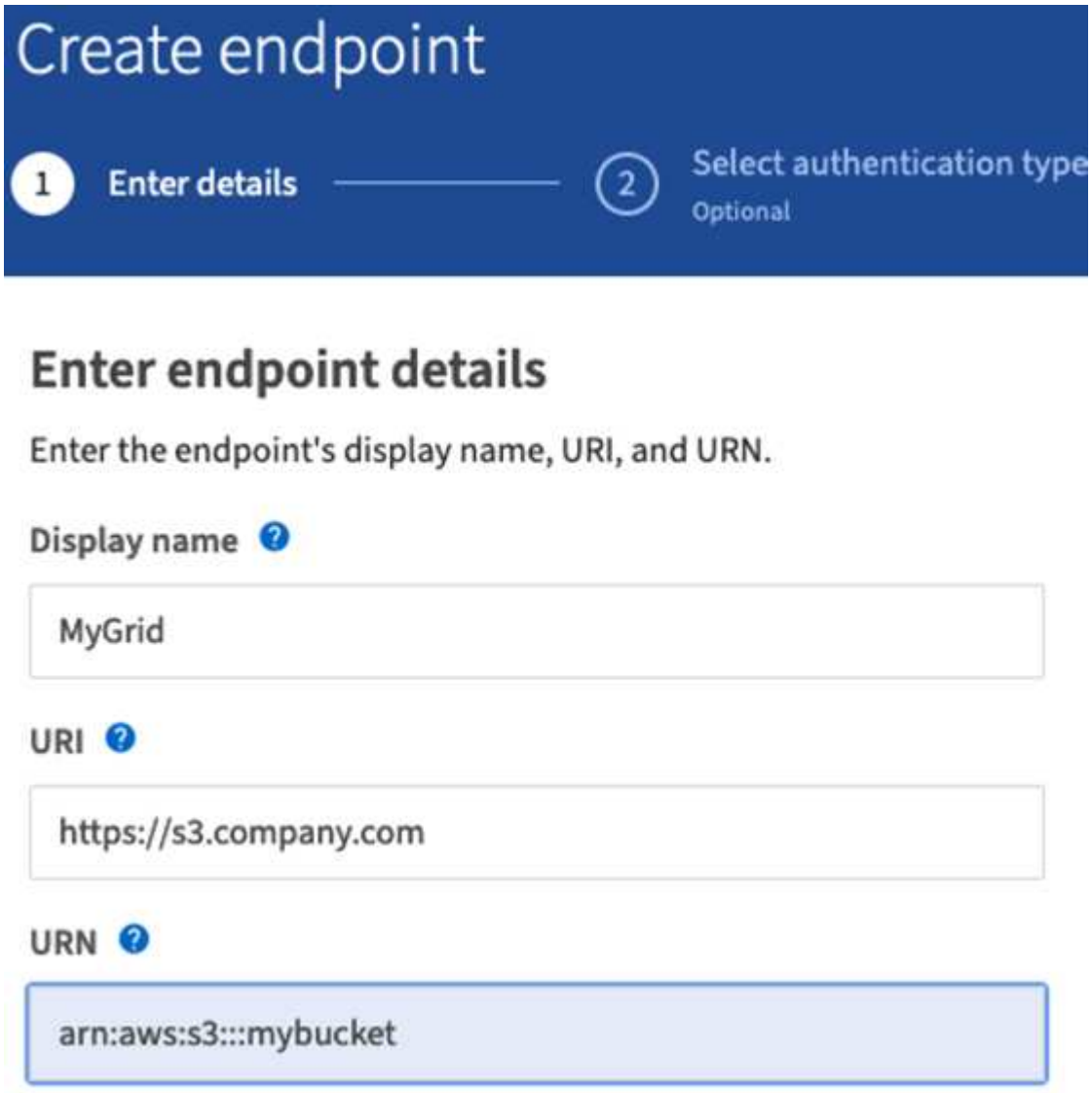
動清理複寫貯體的舊版本、以安全丟棄。因此、您可以使用 StorageGRID ILM 原則引擎。建立規則、根據非目前時間管理物件放置、時間足以識別攻擊並從攻擊中恢復。

這種方法的一個缺點是、它會使用完整的第二個儲存區複本、以及保留一段時間的多個物件版本、來消耗更多儲存空間。此外、有意從主要貯體中刪除的物件必須從複寫的貯體中手動移除。產品外部還有其他複寫選項、例如 NetApp CloudSync 、可針對類似解決方案複寫刪除內容。啟用版本設定功能而未啟用物件鎖定功能的次要貯體另一個缺點是存在許多可用來在次要位置造成損害的特殊權限帳戶。優點是、它應該是該端點或租戶貯體的唯一帳戶、而且可能會造成的影響不包括主要位置上的帳戶存取權、反之亦然。

建立來源和目的地儲存區、並使用版本設定目的地之後、您可以設定及啟用複寫、如下所示：

步驟

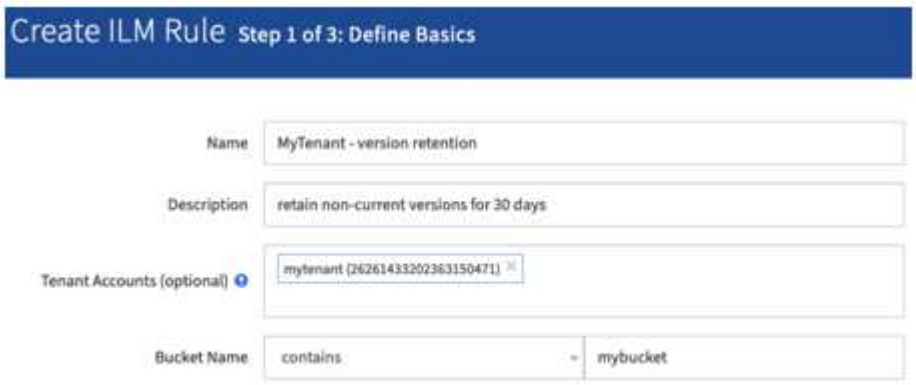
1. 若要設定 CloudMirror 、請為 S3 目的地建立平台服務端點。

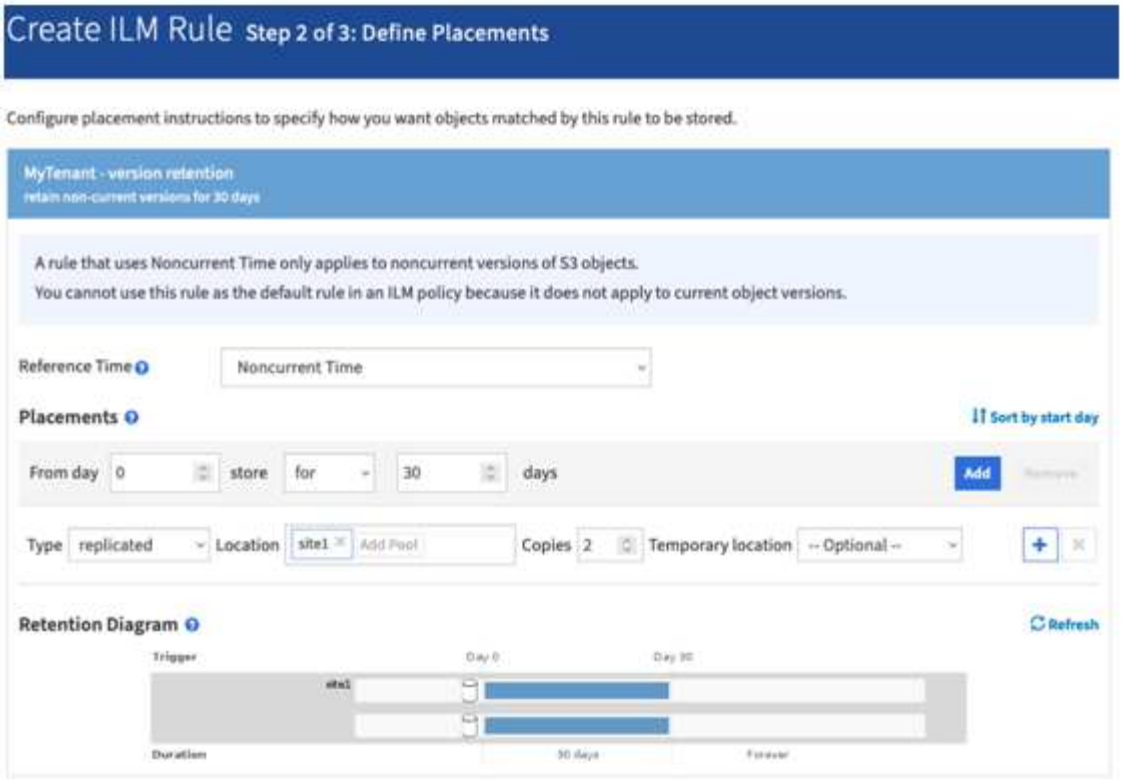


2. 在來源貯體上、將複寫設定為使用已設定的端點。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. 建立 ILM 規則以管理儲存配置和版本儲存持續時間管理。在此範例中、會設定要儲存之物件的非最新版本。





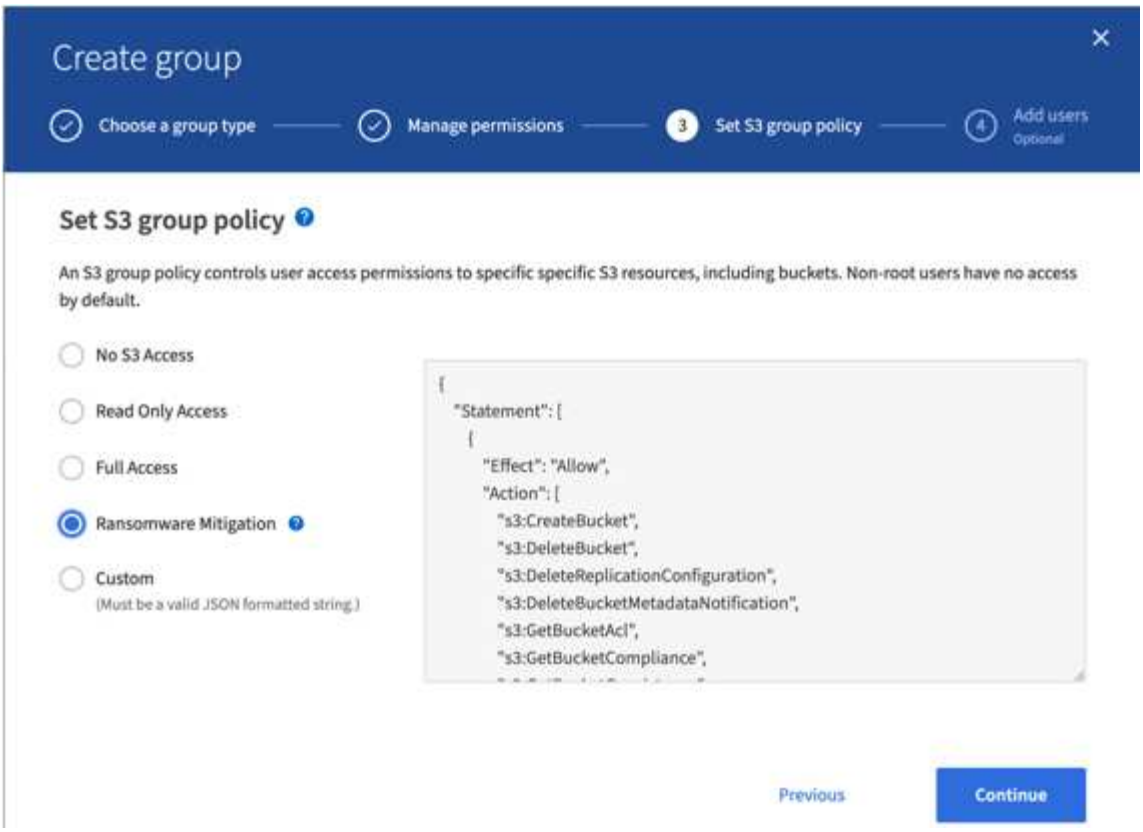
站台 1 有兩份 30 天的複本。您也可以根據在 ILM 規則中使用擷取時間做為參考時間、來設定物件目前版本的規則、以符合來源貯體儲存持續時間。物件版本的儲存位置可以進行銷毀編碼或複寫。

使用具有保護性 **IAM** 原則的版本管理功能來防範勒索軟體

瞭解如何啟用貯體的版本設定功能、並在 StorageGRID 中的使用者安全性群組上實作 IAM 原則、以保護您的資料。

在不使用物件鎖定或複寫的情況下保護資料的方法、是在貯體上啟用版本設定、並在使用者安全性群組上實作 IAM 原則、以限制使用者管理物件版本的能力。發生攻擊時、會建立新的不良資料版本作為目前版本、而最新的非最新版本則是安全無虞的資料。為了取得資料存取權而遭入侵的帳戶無法刪除或以其他方式變更保護資料的非目前版本、以供日後還原作業使用。如同先前的案例、 ILM 規則會在您選擇的期間內、管理非目前版本的保留。缺點是、仍然可能存在授權帳戶、導致不良攻擊者遭受攻擊、但所有應用程式服務帳戶和使用者都必須設定更具限制性的存取。限制性群組原則必須明確允許您希望使用者或應用程式能夠執行的每個動作、並明確拒絕您不希望使用者或應用程式能夠執行的任何動作。NetApp 不建議使用萬用字元允許、因為未來可能會引進新的動作、而且您會想要控制是否允許或拒絕。對於此解決方案、拒絕清單必須包含 DeleteObjectVersion 、 PuttBucketPolicy 、 DeleteBucketPolicy 、 PuttLifecycleConfiguration 和 PuttBucketVersioning 、以保護貯體和物件版本的版本設定、避免使用者或程式設計上的變更。

在StorageGRID中，S3 群組原則選項「勒索軟體緩解」使得實施此解決方案變得更加容易。在租用戶中建立使用者群組時，選擇群組權限後，可以看到這個可選策略。



以下是群組原則的內容、其中包含明確允許的大部分可用作業、以及最低要求的拒絕。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
```

```
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
```

```
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

勒索軟體調查和補救

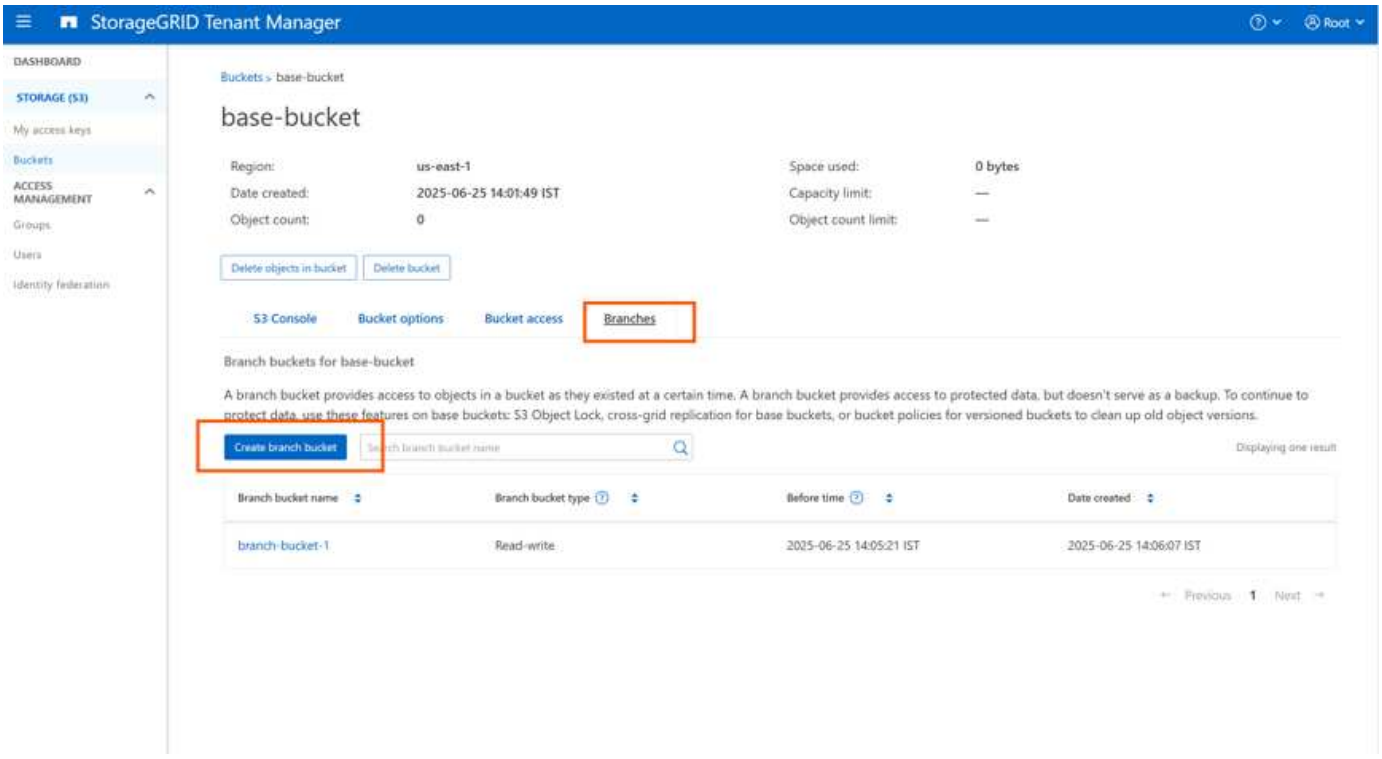
了解如何使用StorageGRID在可能發生勒索軟體攻擊後調查和修復儲存桶。

在StorageGRID 12.0 中，新增了新的分支儲存桶功能，以擴展版本控制對於勒索軟體防禦的實用性。分支儲存桶提供對儲存桶中物件的訪問，因為這些物件在某個時間存在，但前提是它們仍然存在於儲存桶中。只能為啟用版本控制的基本儲存桶建立分支儲存桶。

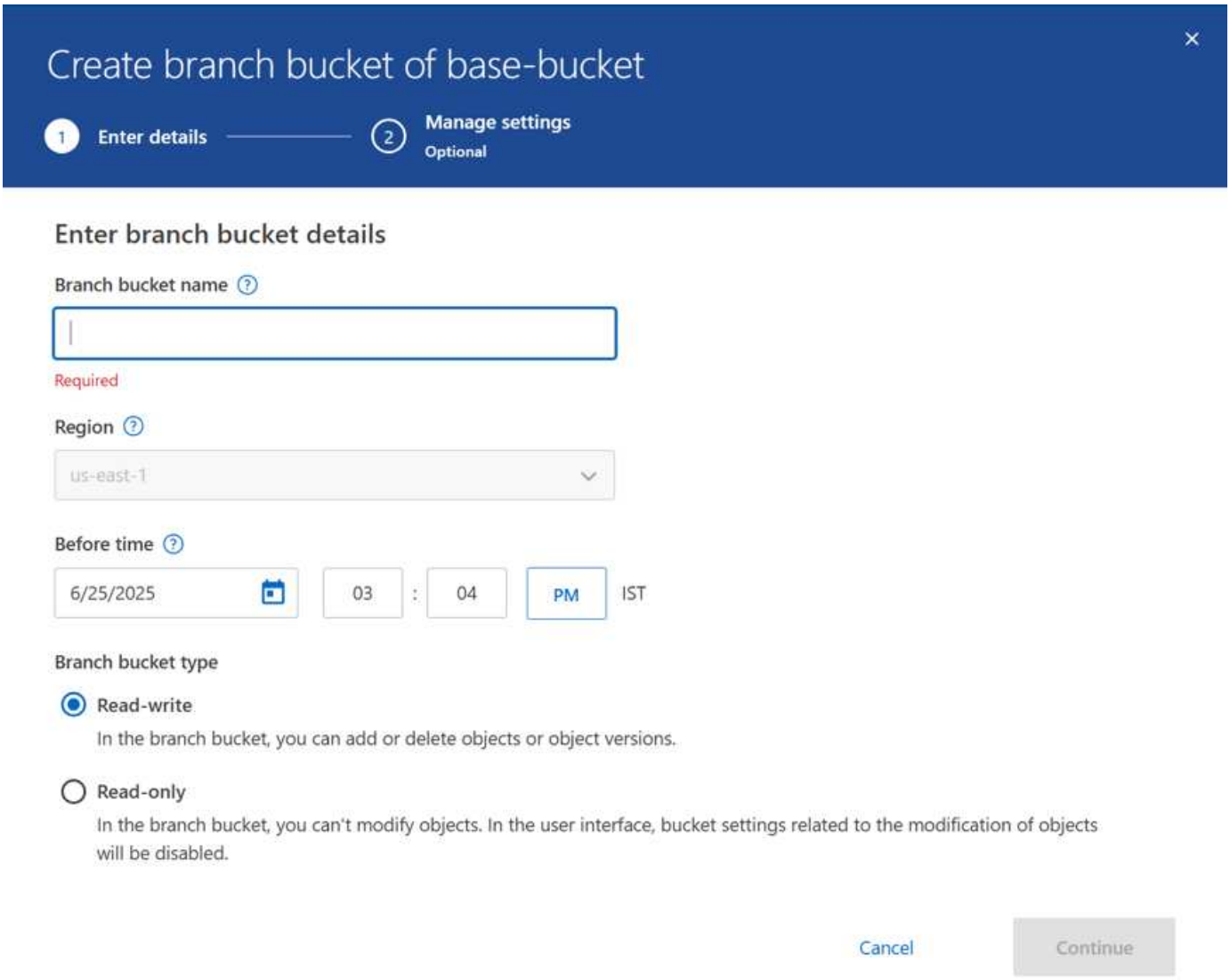
這意味著如果您懷疑發生了勒索軟體攻擊，您可以建立一個讀/寫或只讀分支儲存桶，其中包含初始攻擊之前存在的所有物件和版本。您可以使用此分支儲存桶與基本儲存桶內容進行比較，以確定哪些物件發生了變更以及該變更是否為攻擊的一部分。您也可以使用分支儲存桶，在調查攻擊的同時使用乾淨的分支繼續客戶端操作。

建立分支儲存桶

- 導航至基本儲存桶詳細資料頁面和分支標籤以建立分支儲存桶。



- 點擊「建立分支儲存桶」按鈕後，將開啟一個彈出窗口，其中預先填寫了與基本儲存桶關聯的區域的詳情。
- 在時間之前提供分支儲存桶名稱，並選擇要建立的分支儲存桶類型。



TR-4765 ：監控 StorageGRID

StorageGRID 監控簡介

瞭解如何使用 Splunk 等外部應用程式來監控 StorageGRID 系統。

有效監控 NetApp StorageGRID 物件型儲存設備、可讓管理員快速回應緊急問題、並主動新增資源來處理不斷成長的工作負載。本報告提供如何監控關鍵指標及如何運用外部監控應用程式的一般指引。本指南旨在補充現有的監控與疑難排解指南。

NetApp StorageGRID 部署通常由多個站台和許多節點組成、這些站台和節點可用來建立分散式容錯物件儲存系統。在分散式彈性儲存系統（例如 StorageGRID ）中、當網格繼續正常運作時、發生錯誤狀況是正常現象。身為系統管理員的您所面臨的挑戰、是瞭解錯誤狀況（例如節點停機）的臨界值、以及應該立即解決的問題、而非應該分析的資訊。透過分析 StorageGRID 提供的資料、您可以瞭解工作負載並做出明智的決策、例如何時新增更多資源。

StorageGRID 提供優異的文件、深入探討監控主題。本報告假設您熟悉 StorageGRID 、並已檢閱相關文件。我們不再重複這些資訊、而是參考本指南中的產品文件。StorageGRID 產品文件可在線上取得、並以 PDF 格式提

供。

本文件旨在補充產品文件、並討論如何使用外部應用程式（例如 Splunk ）來監控 StorageGRID 系統。

資料來源

若要成功監控 NetApp StorageGRID 、請務必瞭解從何處收集有關 StorageGRID 系統健全狀況和作業的資料。

- * 網路 UI 與儀表板。 *StorageGRID Grid Manager 會以最上層的檢視方式呈現您身為系統管理員、在邏輯簡報中需要看到的資訊。身為管理員、您也可以深入瞭解服務層級的資訊、以進行疑難排解和記錄收集。
- * 稽核記錄 *StorageGRID 會保留租戶動作（例如放置、取得和刪除）的精細稽核記錄。您也可以追蹤物件的生命週期、從擷取到資料管理規則的應用。
- * 指標 API *StorageGRID GMI 的基礎是開放式 API 、因為 UI 是 API 導向的。此方法可讓您使用外部監控和分析工具擷取資料。

何處可找到其他資訊

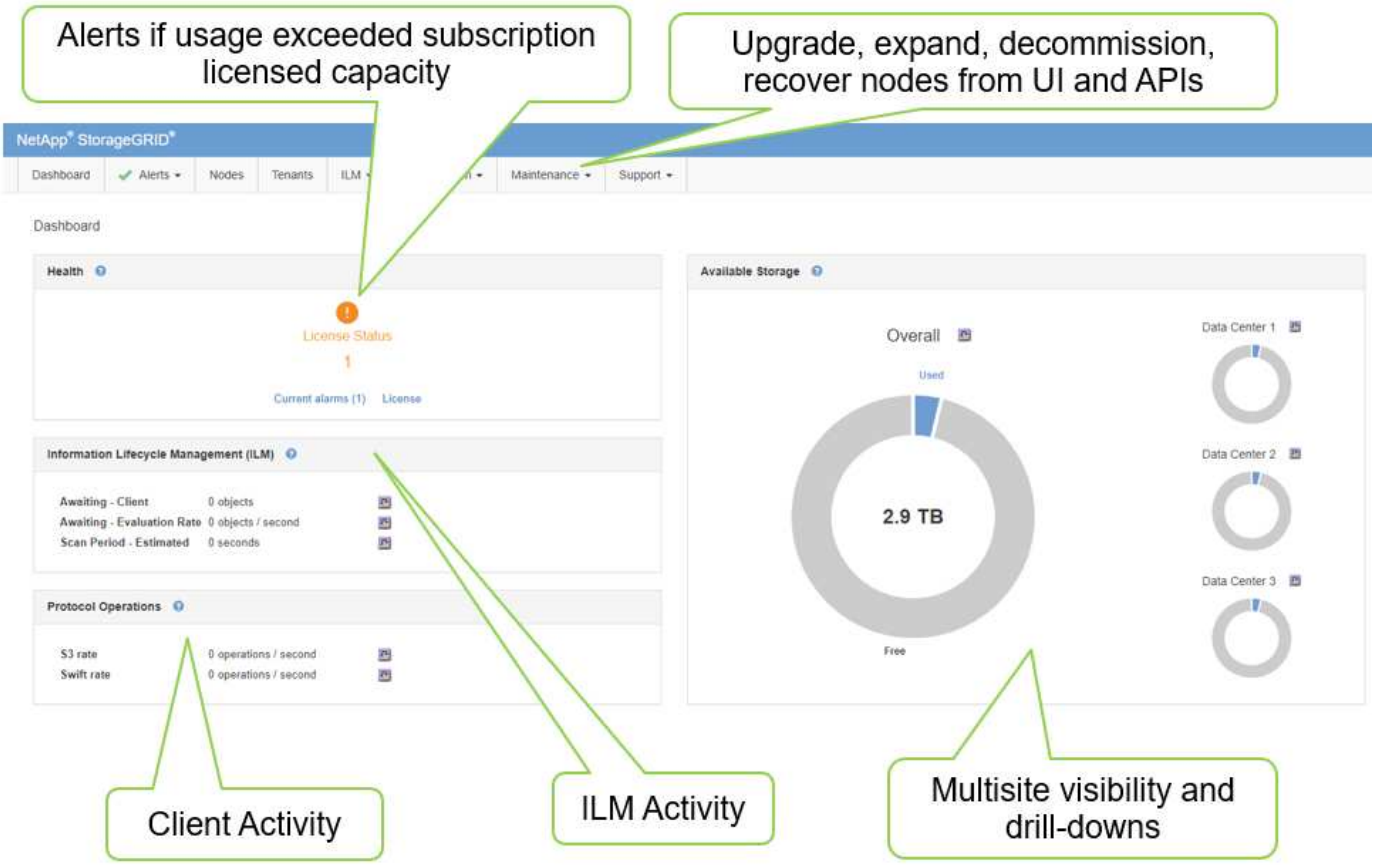
若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID 文件中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 啟用 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/
- Splunk 適用的 NetApp StorageGRID 應用程式 https://splunkbase.splunk.com/app/3898/#/details

使用 **GMI** 儀表板來監控 **StorageGRID**

StorageGRID 網格管理介面（ GMI ）儀表板提供 StorageGRID 基礎架構的集中檢視、可讓您監督整個網格的健全狀況、效能和容量。

使用 GMI 儀表板檢查網格的每個核心元件。



您應該定期監控的資訊

此技術報告的上一版本列出了定期檢查的指標與趨勢。這些資訊現在已包含在 "監控與疑難排解指南"中。

監控儲存設備

此技術報告的舊版會列出監控重要指標的位置、例如物件儲存空間、中繼資料空間、網路資源等。這些資訊現在已包含在 "監控與疑難排解指南"中。

使用警示來監控 **StorageGRID**

瞭解如何使用 StorageGRID 中的警示系統來監控問題、管理自訂警示、以及使用 SNMP 或電子郵件來延伸警示通知。

警示提供重要資訊、可讓您監控 StorageGRID 系統內的各種事件和條件。

警示系統是用來監控 StorageGRID 系統中可能發生的任何問題的主要工具。警示系統著重於系統中可據以行動的問題、並提供易於使用的介面。

我們提供各種預設警示規則、旨在協助監控及疑難排解您的系統。您可以建立自訂警示、編輯或停用預設警示、以及將警示通知靜音、以進一步管理警示。

警示也可透過 SNMP 或電子郵件通知進行擴充。

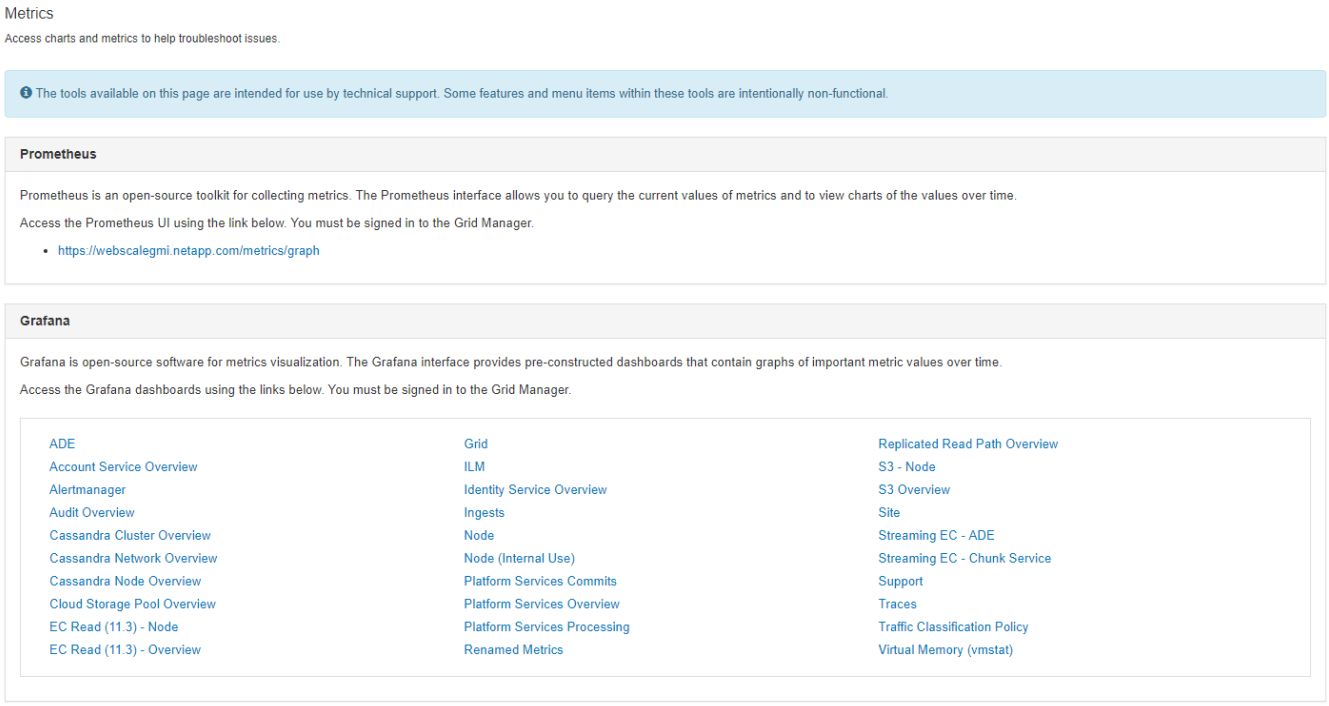
如需警示的詳細資訊、請參閱 "產品文件" 線上提供的 PDF 格式。

StorageGRID 中的進階監控功能

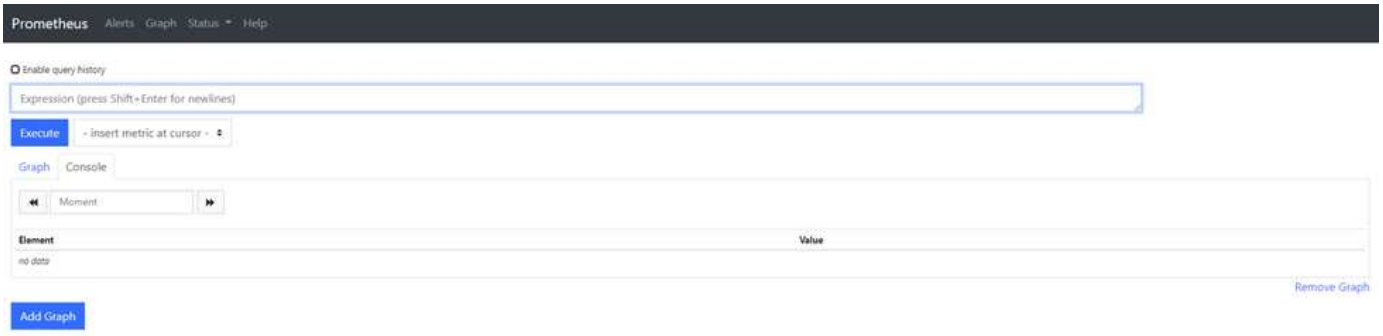
瞭解如何存取及匯出計量指標、以協助疑難排解問題。

透過 Prometheus 查詢檢視計量 API

Prometheus 是一款開放原始碼軟體、用於收集指標。若要透過 GMI 存取 StorageGRID 的內嵌 Prometheus 、請前往功能表： Support[Metrics 。



或者、您也可以直接瀏覽至連結。

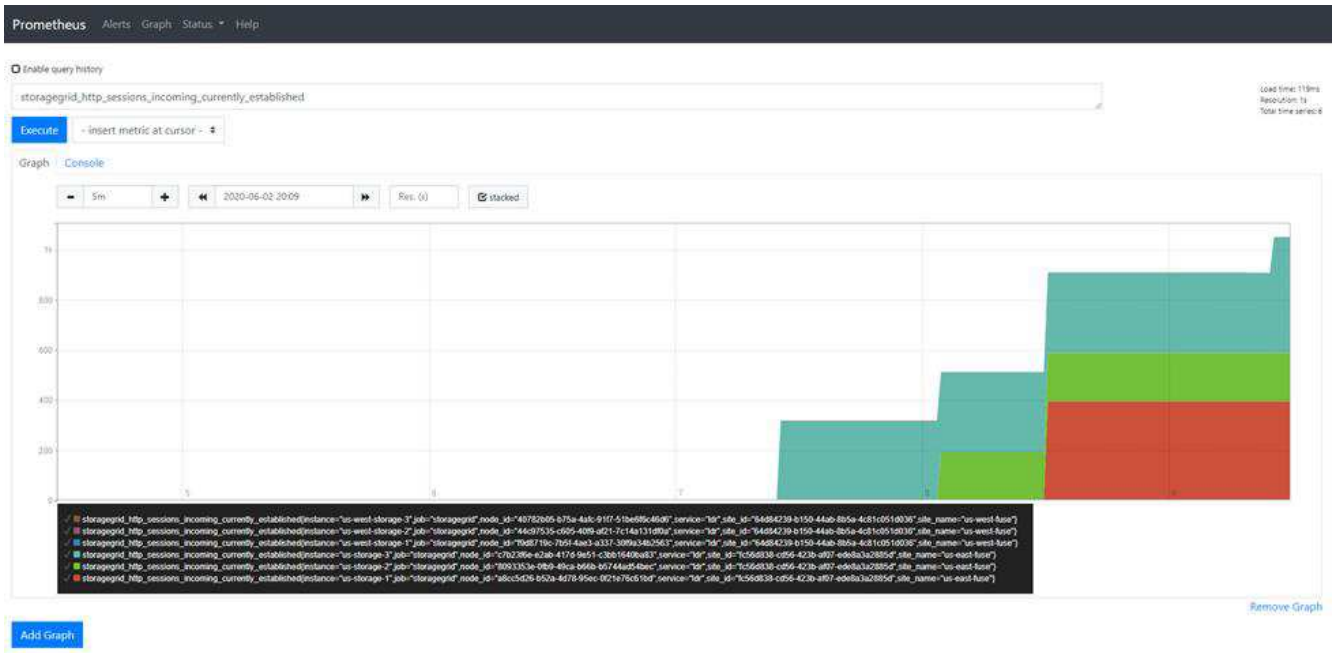


透過此檢視、您可以存取 Prometheus 介面。從這裡、您可以搜尋可用的指標、甚至是嘗試查詢。

若要進行 Prometheus URL 查詢、請遵循下列步驟：

步驟

1. 開始在查詢文字方塊中輸入。在您輸入時、會列出指標。就我們而言、只有以 StorageGRID 和 Node 為開頭的指標才是重要的。
2. 要查看每個節點的 HTTP 會話數，請鍵入 `storagegrid_http` 並選擇 `storagegrid_http_sessions_incoming_currently_established`。按一下「執行」、以圖表或主控台格式顯示資訊。



您透過此 URL 建立的查詢和圖表不會持續存在。複雜查詢會佔用管理節點上的資源。NetApp 建議您使用此檢視來探索可用的度量。

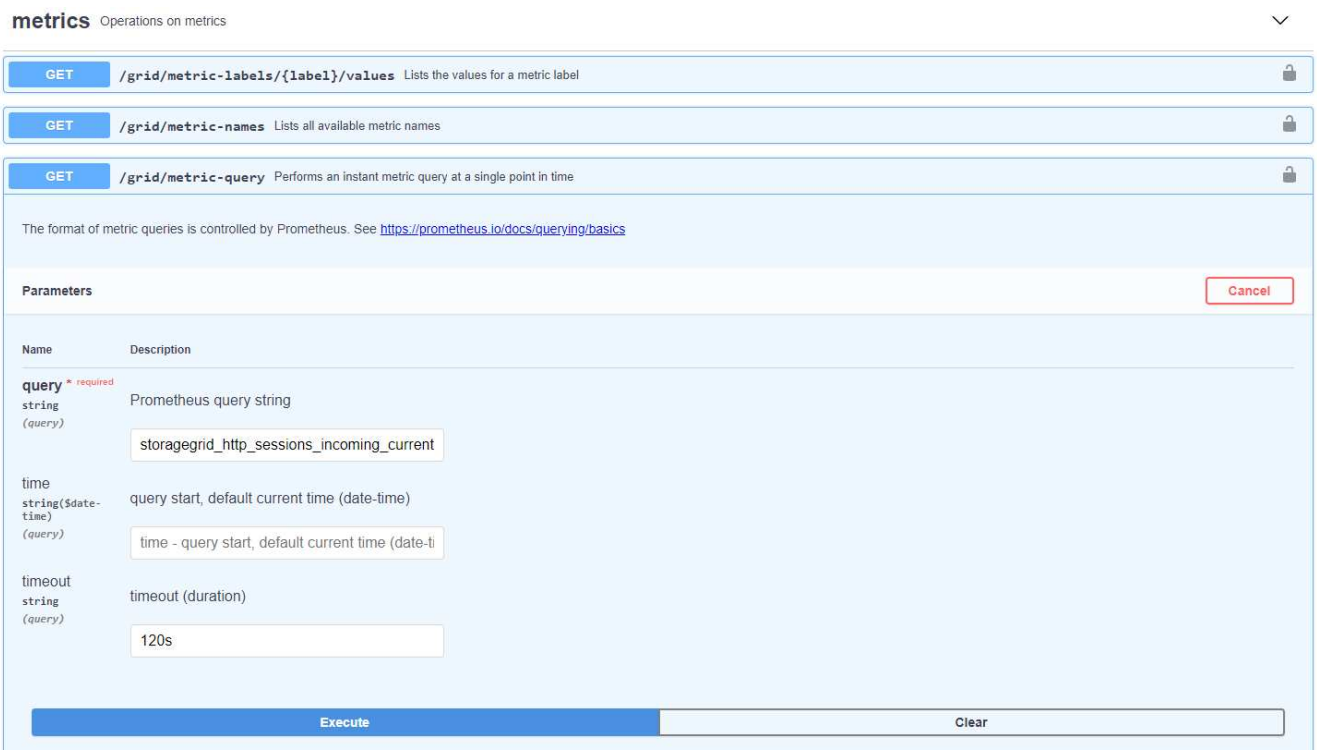
不建議直接連接至我們的 Prometheus 執行個體、因為這需要開啟額外的連接埠。建議使用我們的 API 來存取度量、這是一種安全的方法。

透過 **API** 匯出計量

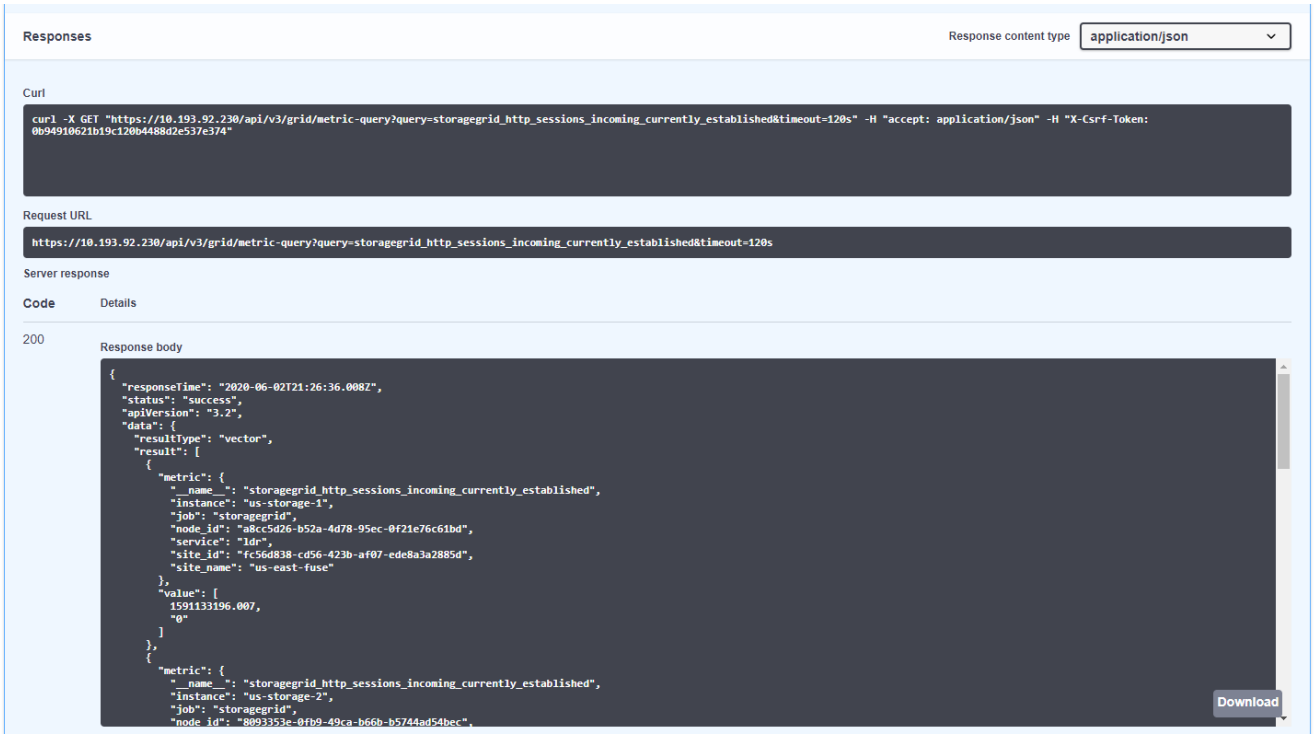
您也可以透過 StorageGRID 管理 API 存取相同的資料。

若要透過 API 匯出度量、請遵循下列步驟：

1. 從 GMI 中選取功能表：說明 [API 文件] 。
2. 向下捲動至指標、然後選取取得 /grid/metric-query 。



回應中包含的資訊與透過 Prometheus URL 查詢所取得的資訊相同。您可以再次看到目前在每個儲存節點上建立的 HTTP 工作階段數目。您也可以下載 JSON 格式的回應、以利閱讀。下圖顯示 Prometheus 查詢回應範例。



使用 API 的優點是、它可讓您執行驗證的查詢

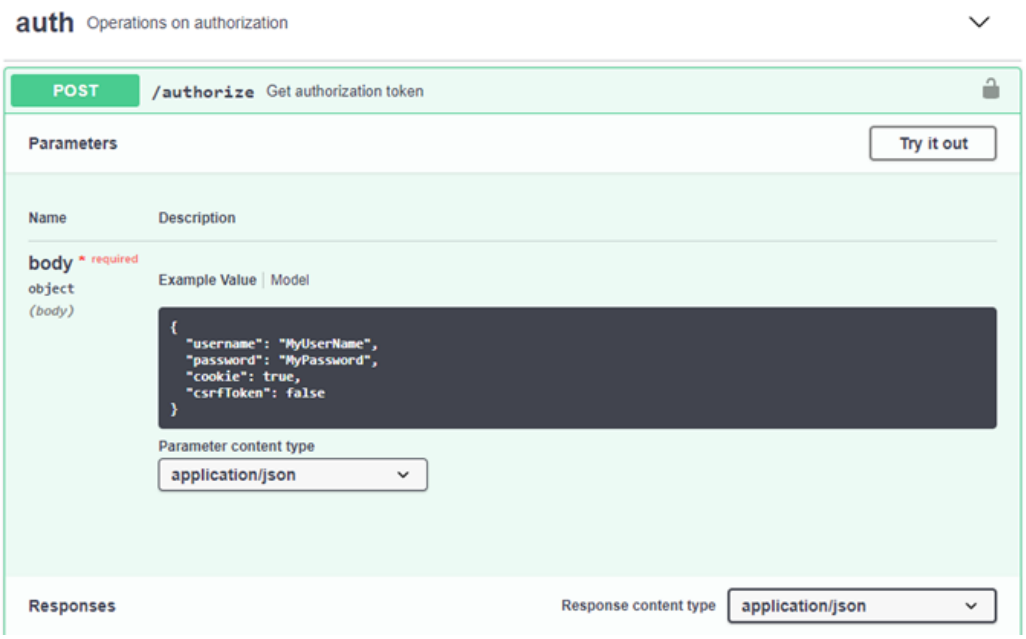
使用 StorageGRID 中的 Curl 存取指標

瞭解如何使用 Curl 透過 CLI 存取度量。

若要執行此作業、您必須先取得授權權杖。若要要求權杖、請依照下列步驟進行：

步驟

1. 從 GMI 中選取功能表：說明 [API 文件] 。
2. 向下捲動至驗證、以尋找授權作業。下列螢幕擷取畫面顯示 POST 方法的參數。



3. 按一下「試試看」、然後使用您的 GMI 使用者名稱和密碼編輯本文。
4. 按一下「執行」。
5. 複製 Curl 區段中提供的 curl 命令、然後將其貼到終端機視窗中。命令如下所示：

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

如果您的 GMI 密碼包含特殊字元、請記得使用 \ 來轉義特殊字元。例如、請更換！ 使用！

6. 執行上述 cURL 命令後、輸出會提供授權權杖、如下例所示：

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

現在您可以使用授權權杖字串、透過 Curl 存取度量。存取計量的程序類似於一節中的步驟 "StorageGRID 中的進階監控功能"。不過、為了進行示範、我們會在「度量」類別中顯示「取得 /grid/metric-labels/{label}/values 」的範例。

7. 例如、下列具有上述授權權杖的 Curl 命令會在 StorageGRID 中列出站台名稱。

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

Curl 命令將產生下列輸出：

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

使用 **StorageGRID** 中的 **Grafana** 儀表板檢視指標

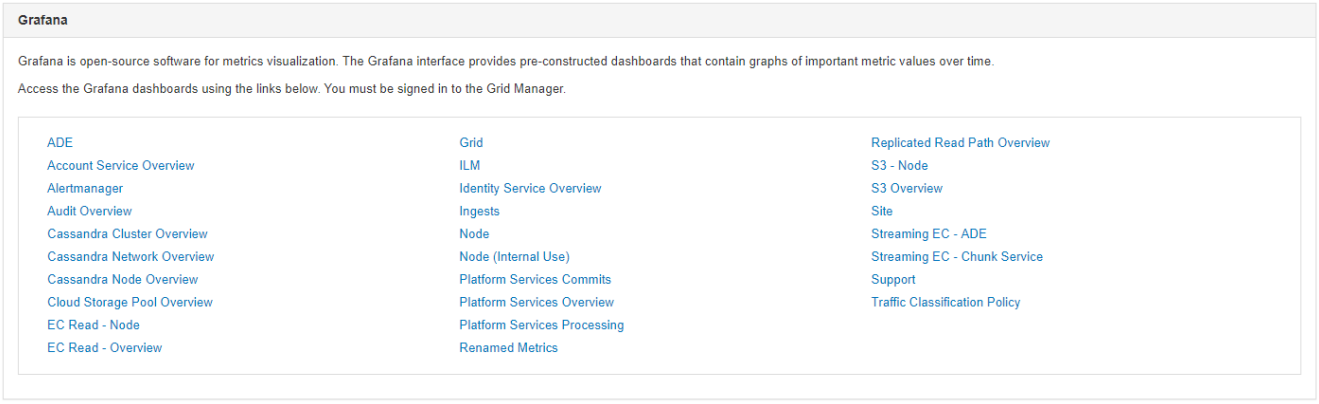
瞭解如何使用 Grafana 介面來視覺化及監控 StorageGRID 資料。

Grafana 是用於度量視覺化的開放原始碼軟體。根據預設、我們已預先建置儀表板、提供有關 StorageGRID 系統的實用且強大的資訊。

這些預先建構的儀表板不僅適用於監控、也適用於疑難排解問題。有些是供技術支援人員使用。例如、若要檢視儲存節點的度量、請遵循下列步驟。

步驟

1. 從 GMI 功能表： Support[指標] 。
2. 在「 Grafana 」區段下、選取「節點」儀表板。



3. 在 Grafana 中、將主機設定為您要檢視其度量的任何節點。在這種情況下、會選取儲存節點。提供的資訊比下列螢幕擷取畫面更多。

在 **StorageGRID** 中使用流量分類原則

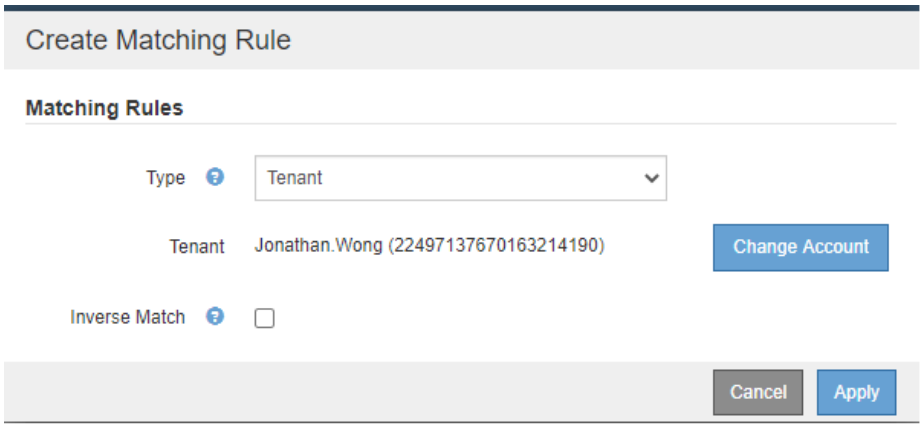
瞭解如何設定和設定流量分類原則、以管理和最佳化 StorageGRID 中的網路流量。

流量分類原則提供一種方法、可根據特定租戶、貯體、 IP 子網路或負載平衡器端點來監控及 / 或限制流量。網路連線能力和頻寬是 StorageGRID 特別重要的指標。

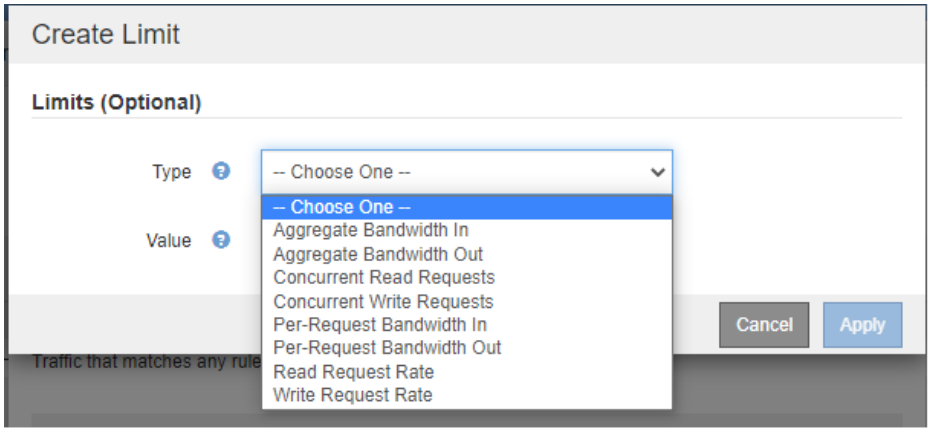
若要設定流量分類原則、請遵循下列步驟：

步驟

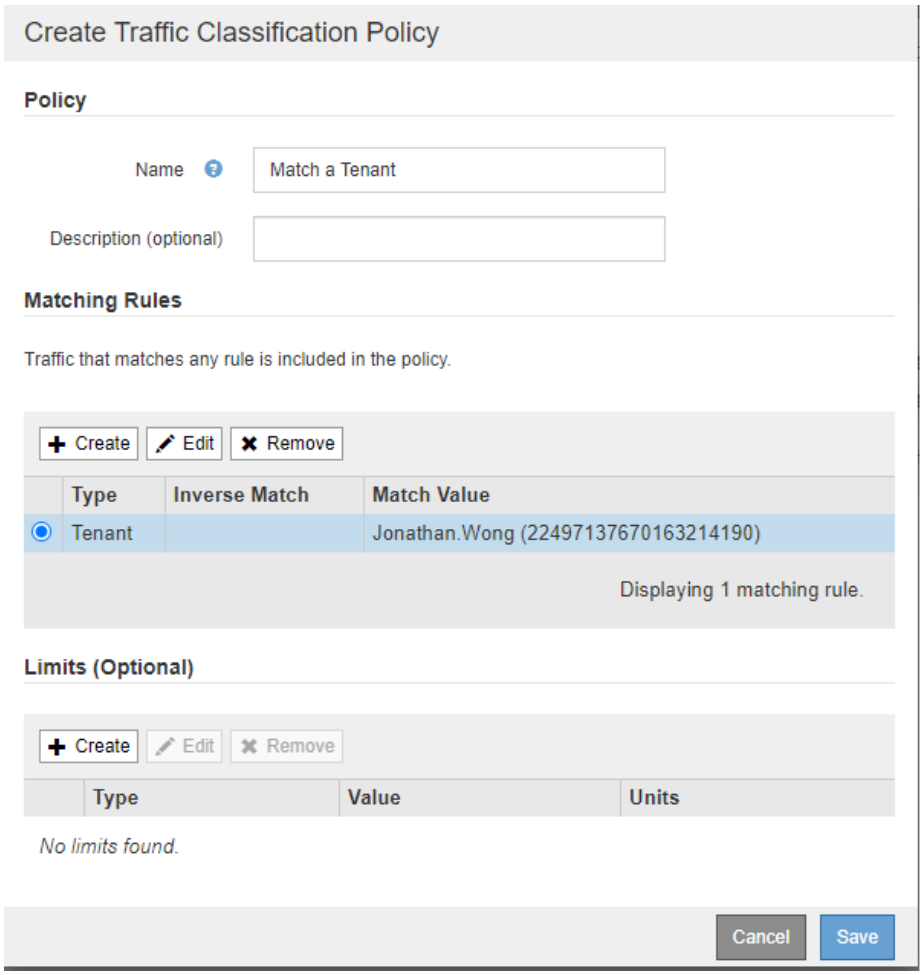
1. 在 GMI 上、瀏覽至功能表：組態 [系統設定 > 流量分類] 。
2. 按一下「建立 + 」
3. 輸入原則的名稱和說明。
4. 建立相符的規則。



5. 設定限制（選用）。



6. 儲存您的原則



若要檢視與您的流量分類原則相關的計量、請選取您的原則、然後按一下度量。系統會產生 Grafana 儀表板、顯示負載平衡器要求流量和平均要求持續時間等資訊。

使用稽核記錄來監控 **StorageGRID**

瞭解如何使用 StorageGRID 稽核記錄、深入瞭解租戶和網格活動、以及如何運用 Splunk 等工具進行記錄分析。

StorageGRID 稽核記錄可讓您收集租戶和網格活動的詳細資訊。稽核記錄可透過 NFS 公開進行分析。如需如何匯出稽核記錄的詳細指示，請參閱《系統管理員指南》。

匯出稽核之後、您可以使用 Splunk 或 Logstash + Elasticsearch 等記錄分析工具來瞭解租戶活動、或建立詳細的計費和計費報告。

StorageGRID 文件中包含稽核訊息的詳細資料。請參閱。 "稽核訊息"

使用 **StorageGRID** 應用程式來執行 **Splunk**

瞭解 Splunk 的 NetApp StorageGRID 應用程式、讓您能夠在 Splunk 平台中監控及分析 StorageGRID 環境。

Splunk 是一款軟體平台、可匯入及索引機器資料、提供強大的搜尋與分析功能。NetApp StorageGRID 應用程式是 Splunk 的附加元件、可匯入及豐富 StorageGRID 所運用的資料。

如需如何安裝、升級及設定 StorageGRID 附加元件的說明、請參閱以下網址： https://splunkbase.splunk.com/app/3895/#/details

TR-4882 ：安裝 StorageGRID 裸機網格

安裝 **StorageGRID** 簡介

瞭解如何在裸機主機上安裝 StorageGRID 。

TR-4882 提供實用的逐步指示集、可產生 NetApp StorageGRID 正常運作的安裝。安裝可能位於裸機上、或是在 Red Hat Enterprise Linux （ RHEL ）上執行的虛擬機器（ VM ）上。方法是以建議的配置和儲存組態、在三部實體（或虛擬）機器上執行六個 StorageGRID 容器化服務的「 opinioned 」（意見化）安裝。有些客戶可能會發現依照此 TR 的範例部署、較容易瞭解部署程序。

如需更深入瞭解 StorageGRID 及安裝程序、請參閱 https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html 產品文件中的 [安裝、升級及 Hotfix StorageGRID] 。

在開始部署之前，讓我們先來看看 NetApp StorageGRID 軟體的運算、儲存和網路需求。StorageGRID 在 Podman 或 Docker 內以容器化服務的形式執行。在此模型中、有些需求是指主機作業系統（裝載 Docker 的作業系統、執行 StorageGRID 軟體）。而且有些資源會直接分配給每個主機內執行的 Docker 容器。在這項部署中、為了將硬體使用量最大化、我們會為每部實體主機部署兩項服務。如需更多資訊、請繼續下一節 "安裝 StorageGRID 的必要條件"。

此 TR 中概述的步驟會導致在六個裸機主機上執行 StorageGRID 安裝。您現在有一個工作網格和用戶端網路、在大多數測試案例中都很實用。

何處可找到其他資訊

若要深入瞭解本 TR 中所述的資訊、請參閱下列文件資源：

- NetApp StorageGRID 文件中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 啟用 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/

安裝 **StorageGRID** 的必要條件

瞭解部署 StorageGRID 所需的運算、儲存、網路、泊塢視窗和節點需求。

運算需求

下表列出每種 StorageGRID 節點類型支援的最低資源需求。這些是 StorageGRID 節點所需的最低資源。

節點類型	**CPU** 核心	**RAM**
管理	8.	24GB
儲存設備	8.	24GB
閘道	8.	24GB

此外、每個實體 Docker 主機至少應分配 16 GB 的 RAM 、以便正常運作。例如、若要將表格中所述的任何兩項服務一起託管在一個實體 Docker 主機上、您可以進行下列計算：

24 + 24 + 16 = 64GB RAM 和 8 + 8 = 16 核心

由於許多現代伺服器超出這些需求、我們將六個服務（ StorageGRID 容器）合併到三個實體伺服器上。

網路需求

StorageGRID 流量的三種類型包括：

- * 網格流量（必填）。 *在網格中所有節點之間傳輸的內部StorageGRID 不完整流量。
- * 管理流量（選用）。 *用於系統管理與維護的流量。
- * 用戶端流量（選用）。 *在外部用戶端應用程式和網格之間傳輸的流量、包括S3和Swift用戶端的所有物件儲存要求。

您最多可以設定三個網路、以搭配 StorageGRID 系統使用。每種網路類型都必須位於不重疊的個別子網路上。如果所有節點都位於同一子網路、則不需要閘道位址。

在此評估中、我們會在兩個包含網格和用戶端流量的網路上部署。您可以稍後新增管理網路、以提供額外的功能。

務必將網路一致地對應到所有主機的介面。例如、如果每個節點上有兩個介面、分別是 ens192 和 ens224 、則所有主機上的所有介面都應該對應到相同的網路或 VLAN 。在此安裝中、安裝程式會將這些資料對應至 Docker 容器、將其對應為 eth0@if2 和 eth2@if3 （因為容器內的迴路是 if1 ）、因此一致的模型非常重要。

Docker 網路注意事項

StorageGRID 使用網路的方式與某些 Docker 容器實作方式不同。不使用 Docker （或 Kubernetes 或 swarm ）提供的網路。StorageGRID 實際上會將容器當成 --net=none 、這樣 Docker 就不會對容器進行任何網路連線。當容器被 StorageGRID 服務所衍生出來之後、就會從節點組態檔案中定義的介面建立新的 Macvlan 裝置。該裝

置有新的 MAC 位址、可作為獨立的網路裝置、從實體介面接收封包。然後將 Macvlan 裝置移至 Container 命名空間、並重新命名為容器內的 eth0 、 eth1 或 eth2 之一。此時、主機作業系統中不再顯示網路裝置。在我們的範例中、網格網路裝置是 Docker 容器內的 eth0 、用戶端網路是 eth2 。如果我們有管理網路、則該裝置會是容器中的 eth1 。

> 容器網路裝置的新 MAC 位址可能需要在某些網路和虛擬環境中啟用雜亂模式。此模式可讓實體裝置接收和傳送不同於已知實體 MAC 位址的 MAC 位址封包。 如果在 VMware vSphere 中執行、您必須接受雜亂模式、 MAC 位址變更、以及在執行 RHEL 時、用於處理 StorageGRID 流量的連接埠群組中的偽造傳輸。大多數情況下、 Ubuntu 或 Debian 都能正常運作、無需進行這些變更。

儲存需求

每個節點都需要 SAN 型或本機磁碟裝置、大小如下表所示。

> 表格中的數字是針對每種 StorageGRID 服務類型、而非整個網格或每個實體主機。根據部署選項、我們將在本文件稍後的中、計算每部實體主機的數量 "實體主機配置與需求"。 安裝程式會在 StorageGRID 容器本身建立標有星號的路徑或檔案系統。管理員不需要手動設定或建立檔案系統、但主機需要區塊裝置才能滿足這些需求。換句話說、區塊裝置應該使用命令來顯示 `lsblk` 、但不要在主機作業系統中格式化或掛載。

節點類型	**LUN** 用途	**LUN**數量	**LUN** 的最小大小	需要手動檔案系統	建議的節點組態項目
全部	管理節點系統空間 `/var/local` （ SSD 在此提供協助）	每個管理節點各一個	90GB	否	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
所有節點	Docker 儲存池位於 `/var/lib/docker for container pool`	每個主機（實體或 VM ）各一個	每個容器 100 GB	是– etx4	NA –格式化並以主機檔案系統掛載（未對應至容器）
管理	管理節點稽核記錄（管理容器中的系統資料） `/var/local/audit/export`	每個管理節點各一個	200GB	否	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
管理	管理節點表（管理容器中的系統資料） `/var/local/mysql_ibdata`	每個管理節點各一個	200GB	否	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`

節點類型	**LUN** 用途	**LUN**數量	**LUN** 的最小大小	需要手動檔案系統	建議的節點組態項目

儲存節點	物件儲存（區塊裝置）
	`/var/local/rangedb0` （ SSD 在此提供協助）
	`/var/local/rangedb1`
	`/var/local/rangedb2`
		每個儲存容器三個	4000GB	否	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00`
					`BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01`
					`BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

在此範例中、下表所示的磁碟大小是每種容器類型所需的。本文件稍後的、中說明每部實體主機的需求 "實體主機配置與需求"。

每種容器類型的磁碟大小

管理容器

名稱	尺寸（ **GiB** ）
Docker 儲存	100 （每個容器）
ADM-OS	90
ADM-Audit	200
ADM-MySQL	200

儲存容器

名稱	尺寸（ **GiB** ）
Docker 儲存	100 （每個容器）
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

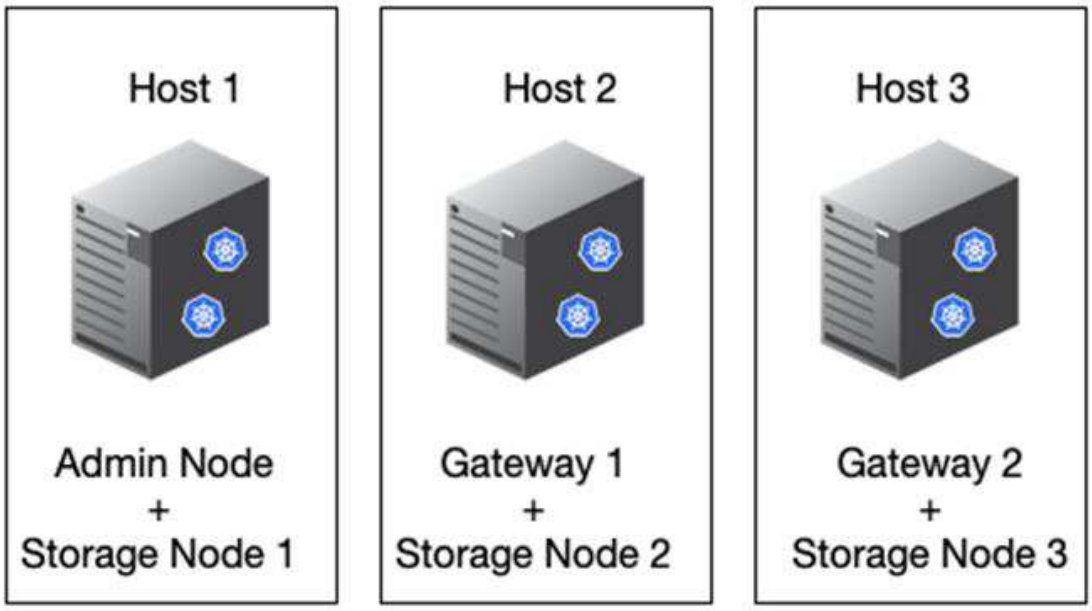
閘道容器

名稱	尺寸（ **GiB** ）
Docker 儲存	100 （每個容器）
/var/local	90

實體主機配置與需求

透過結合上表所示的運算和網路需求、您可以獲得一組基本的硬體、以安裝三部具有 16 核心、 64GB RAM 和兩個網路介面的實體（或虛擬）伺服器。如果需要較高的處理量、可以在網格或用戶端網路上連結兩個或更多介面、並在節點組態檔案中使用 VLAN 標記介面、例如 bond0.520 。如果您預期的工作負載會更密集、那麼主機和容器的記憶體就會更多。

如下圖所示、這些伺服器將裝載六個 Docker 容器、每個主機兩個。RAM 的計算方式為每個容器提供 24GB 、主機作業系統本身則提供 16GB 。



每個實體主機（或 VM ）所需的總 RAM 為 24 x 2 + 16 = 64GB 。下表列出主機 1 、 2 和 3 所需的磁碟儲存設備。

主機 **1**	尺寸（ **GiB** ）
• Docker Store*	`/var/lib/docker` （檔案系統）
200 （ 100 x 2 ）	• 管理容器 *
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
• 儲存容器 *	SN-OS `/var/local` （裝置）
90	Rangedb-0 （裝置）
4096	Rangedb-1 （裝置）

主機 **1**	尺寸（ **GiB** ）
4096	Rangedb-2 （裝置）

主機 **2.**	尺寸（ **GiB** ）
• Docker Store*	`/var/lib/docker` （共享）
200 （ 100 x 2 ）	• 閘道容器 *
GW-OS */`var/local`	100
• 儲存容器 *	*/`var/local`
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

主機 **3**	尺寸（ **GiB** ）
• Docker Store*	`/var/lib/docker` （共享）
200 （ 100 x 2 ）	• 閘道容器 *
*/`var/local`	100
• 儲存容器 *	*/`var/local`
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Docker 儲存區的計算方式是：每個 /var/local （每個容器）允許 100GB x 兩個容器 = 200GB 。

準備節點

若要準備 StorageGRID 的初始安裝、請先安裝 RHEL 9.2 版並啟用 SSH 。根據最佳實務做法設定網路介面、網路時間傳輸協定（ NTP ）、 DNS 和主機名稱。您至少需要一個已啟用網格網路的網路介面、另一個則需要用戶端網路。如果您使用的是具有 VLAN 標記的介面、請依照下列範例進行設定。否則、簡單的標準網路介面組態就足夠了。

如果您需要在網格網路介面上使用 VLAN 標記、您的組態應該有兩個檔案 `/etc/sysconfig/network-scripts/` 、格式如下：

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

本範例假設您的網格網路實體網路裝置是 enp67s0 。它也可以是綁定的設備，例如 bond0 。無論您是使用結合或標準網路介面、如果網路連接埠沒有預設 VLAN 、或是預設 VLAN 沒有與網格網路相關聯、則必須在節點組態檔案中使用 VLAN 標記介面。StorageGRID 容器本身不會取消標記乙太網路框架、因此必須由父作業系統處理。

iSCSI 的選用儲存設備設定

如果您不使用 iSCSI 儲存設備、則必須確保 host1 、 host2 和 host3 包含大小足以滿足其需求的區塊裝置。請參閱 "每種容器類型的磁碟大小" 瞭解 host1 、 host2 和 host3 儲存需求。

若要使用 iSCSI 設定儲存設備、請完成下列步驟：

步驟

1. 如果您使用外部 iSCSI 儲存設備、例如 NetApp E 系列或 NetApp ONTAP ® 資料管理軟體、請安裝下列套件：

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. 在每個主機上找到啟動器 ID 。

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. 使用步驟 2 中的啟動器名稱、將儲存裝置上的 LUN （表中所示的數量和大小）對應 "儲存需求" 至每個儲存節點。
4. 使用探索新建立的 LUN `iscsiadm` 並登入它們。

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

如需詳細資訊、請參閱 "建立 iSCSI 啟動器" Red Hat 客戶入口網站上的。

5. 若要顯示多重路徑裝置及其相關的 LUN WWID 、請執行下列命令：

```
# multipath -ll
```

如果您不使用 iSCSI 搭配多重路徑裝置、只要以唯一的路徑名稱掛載裝置、即可持續進行裝置變更和重新開機。

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

如果移除或新增裝置、只要使用 `/dev/sdx` 裝置名稱可能會在稍後發生問題。 如果您使用多重路徑裝置、請修改 `/etc/multipath.conf` 檔案以使用別名、如下所示。

視配置而定、這些裝置可能出現在所有節點上、也可能不存在。

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

在主機作業系統中安裝 Docker 之前、請先格式化並掛載 LUN 或磁碟備份 `/var/lib/docker`。其他 LUN 是在節點組態檔中定義、直接由 StorageGRID 容器使用。也就是說、它們不會出現在主機作業系統中、它們會出現在容器本身、而這些檔案系統則由安裝程式處理。

如果您使用的是 iSCSI 備份 LUN 、請在您的 fstab 檔案中放入類似以下的內容。如前所述、其他 LUN 不需要掛載於主機作業系統中、但必須顯示為可用的區塊裝置。

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

準備安裝 **Docker**

若要準備 Docker 安裝、請完成下列步驟：

步驟

1. 在所有三台主機上的 Docker 儲存磁碟區上建立檔案系統。

```
# sudo mkfs.ext4 /dev/sd?
```

如果您使用的 iSCSI 設備具有多路徑功能，請使用 `/dev/mapper/Docker-Store`。

2. 建立 Docker 儲存磁碟區裝載點：

```
# sudo mkdir -p /var/lib/docker
```

3. 將泊塢視窗儲存容量裝置的類似項目新增至 `/etc/fstab`。

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

只有在使用 iSCSI 裝置時、才建議使用下列 `_netdev` 選項。如果您不需要使用本機區塊裝置 `_netdev defaults` 、建議您使用。

```
/dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
```

4. 掛載新的檔案系統並檢視磁碟使用率。

```
# sudo mount /var/lib/docker
[root@host1]# df -h | grep docker
/dev/sdb 200G 33M 200G 1% /var/lib/docker
```

5. 基於效能考量、請關閉交換並停用。

```
$ sudo swapoff --all
```

6. 若要保留設定、請從 /etc/fstab 移除所有交換項目、例如：

```
/dev/mapper/rhel-swap swap defaults 0 0
```

如果無法完全停用交換、可能會嚴重降低效能。

7. 對節點執行測試重新開機、以確保該 `/var/lib/docker` 磁碟區持續存在、且所有磁碟裝置都會恢復正常。

安裝 **Docker for StorageGRID**

瞭解如何安裝 Docker for StorageGRID 。

若要安裝 Docker 、請完成下列步驟：

步驟

1. 為 Docker 設定 yum repo 。

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. 安裝所需的套件。

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. 啟動 Docker 。

```
sudo systemctl start docker
```

4. 測試 Docker 。

```
sudo docker run hello-world
```

5. 請確定 Docker 在系統啟動時執行。

```
sudo systemctl enable docker
```

為 **StorageGRID** 準備節點組態檔案

瞭解如何為 StorageGRID 準備節點組態檔案。

在高層級、節點組態程序包括下列步驟：

步驟

1. 在所有主機上建立 `/etc/storagegrid/nodes` 目錄。

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. 為每部實體主機建立所需的檔案、以符合容器 / 節點類型配置。在此範例中、我們在每部主機上的每部實體主機上建立兩個檔案。

> 檔案名稱會定義實際的安裝節點名稱。例如 `dc1-adm1.conf` ，成爲名爲的節點 `dc1-adm1`。

— 主機 1 ：
`dc1-adm1.conf`
`dc1-sn1.conf`

— 主機 2 ：
`dc1-gw1.conf`
`dc1-sn2.conf`

— 主機 3 ：
`dc1-gw2.conf`
`dc1-sn3.conf`

正在準備節點組態檔案

下列範例使用 `/dev/disk/by-path` 格式。您可以執行下列命令來驗證正確的路徑：

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

以及以下命令：

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

主要管理節點範例

檔案名稱範例：

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

範例檔案內容：

磁碟路徑可以遵循下列範例、或使用 `/dev/mapper/alias` 樣式命名。請勿使用區塊裝置名稱、例如 `/dev/sdb` 在重新開機時可能會變更、並對您的網格造成重大損害。

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

儲存節點範例

檔案名稱範例：

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

範例檔案內容：

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

閘道節點範例

檔案名稱範例：

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

範例檔案內容：

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

安裝 **StorageGRID** 相依性和套件

瞭解如何安裝 StorageGRID 相依性和套件。

若要安裝 StorageGRID 相依性和套件、請執行下列命令：

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

驗證 **StorageGRID** 組態檔案

瞭解如何驗證 StorageGRID 組態檔案的內容。

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。

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、則每個組態檔案的輸出都會顯示通過：

```
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
```

如果組態檔案不正確、問題會顯示為警告和錯誤。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
```

啟動StorageGRID 「支援服務」

瞭解如何啟動 StorageGRID 主機服務。

若要啟動 StorageGRID 節點、並確保它們在主機重新開機後重新啟動、您必須啟用並啟動 StorageGRID 主機服務。

若要啟動 StorageGRID 主機服務、請完成下列步驟。

步驟

1. 在每個主機上執行下列命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

> 開始程序在初始執行時可能需要一些時間。

2. 執行下列命令以確保部署繼續進行：

```
sudo storagegrid node status node-name
```

3. 對於任何返回或狀態的節點 `Not-Running` `Stopped`，請運行以下命令：

```
sudo storagegrid node start node-name
```

例如、假設有下列輸出、您就可以啟動 `dc1-adm1` 節點：

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. 如果您先前已啟用並啟動 StorageGRID 主機服務（或不確定是否已啟用並啟動服務）、請執行下列命令：

```
sudo systemctl reload-or-restart storagegrid
```

在 StorageGRID 中設定 Grid Manager

瞭解如何在主要管理節點上的 StorageGRID 中設定 Grid Manager 。

從主要管理節點上的 Grid Manager 使用者介面設定 StorageGRID 系統、以完成安裝。

高階步驟

設定網格並完成安裝涉及下列工作：

步驟

1. 瀏覽至 Grid Manager
2. "指定StorageGRID 不含授權的資訊"
3. "新增站台至 StorageGRID"
4. "指定網格網路子網路"
5. "核准擱置的網格節點"
6. "指定 NTP 伺服器資訊"
7. "指定網域名稱系統伺服器資訊"
8. "指定StorageGRID 「系統密碼」"
9. "檢閱組態並完成安裝"

瀏覽至 **Grid Manager**

使用 Grid Manager 定義設定 StorageGRID 系統所需的所有資訊。

開始之前、必須先部署主要管理節點、並完成初始啟動順序。

若要使用 Grid Manager 來定義資訊、請完成下列步驟。

步驟

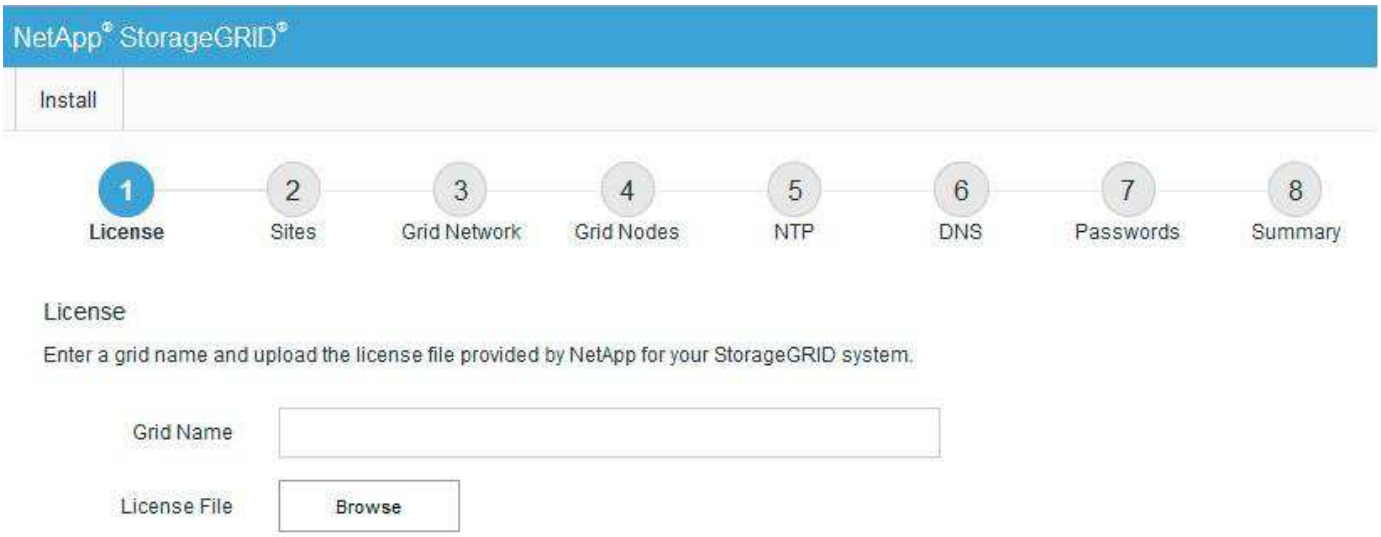
1. 存取 Grid Manager 、網址如下：

   ```
   https://primary_admin_node_grid_ip
   ```

   或者、您也可以在連接埠 8443 上存取 Grid Manager 。

   ```
   https://primary_admin_node_ip:8443
   ```

2. 按一下「安裝 StorageGRID 系統」。隨即顯示用於設定 StorageGRID 網格的頁面。



新增 **StorageGRID** 授權詳細資料

瞭解如何上傳 StorageGRID 授權檔案。

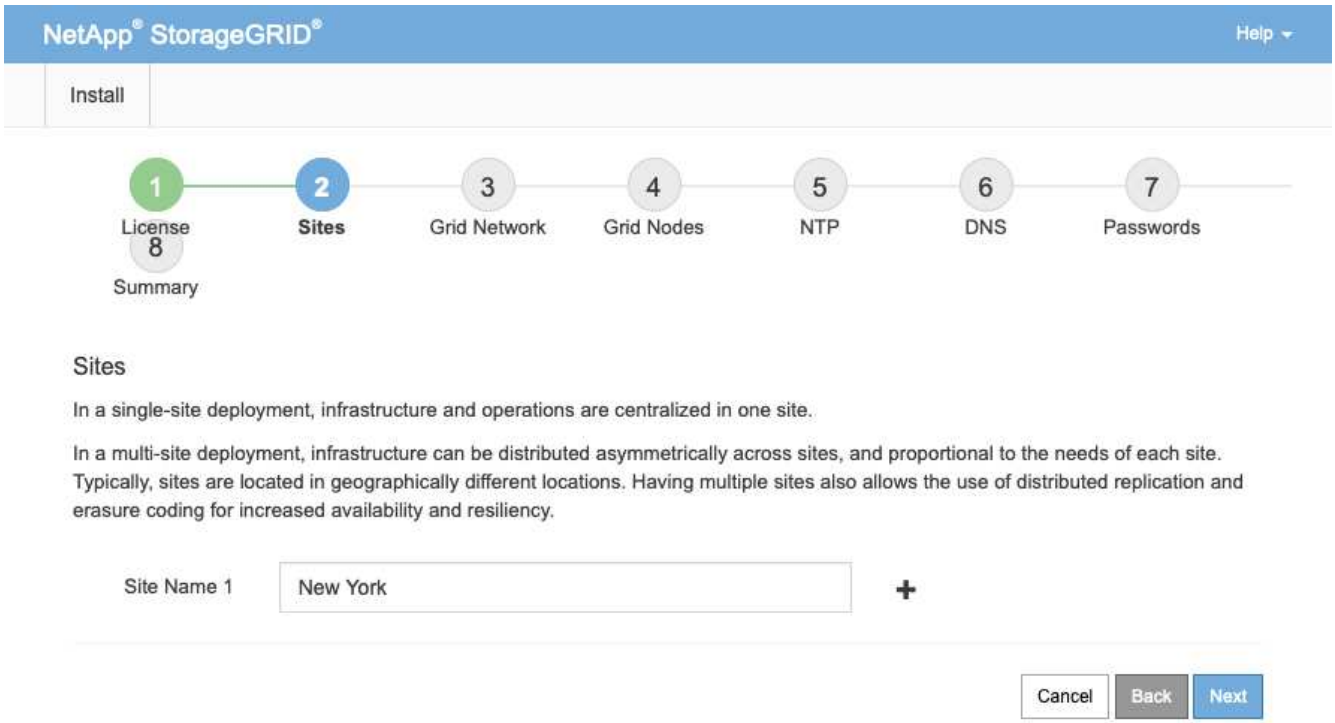
您必須指定StorageGRID 您的系統名稱、並上傳NetApp提供的授權檔案。

若要指定 StorageGRID 授權資訊、請完成下列步驟：

步驟

1. 在「授權」頁面的「網格名稱」欄位中、輸入 StorageGRID 系統的名稱。安裝後、名稱會顯示為網格拓撲樹狀結構的最上層。
2. 單擊瀏覽，找到 NetApp 許可證文件 (`NLF-unique-id.txt`) ，然後單擊打開。授權檔案已驗證、並顯示序號和授權儲存容量。

> 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. 按一下「下一步」

新增站台至 **StorageGRID**

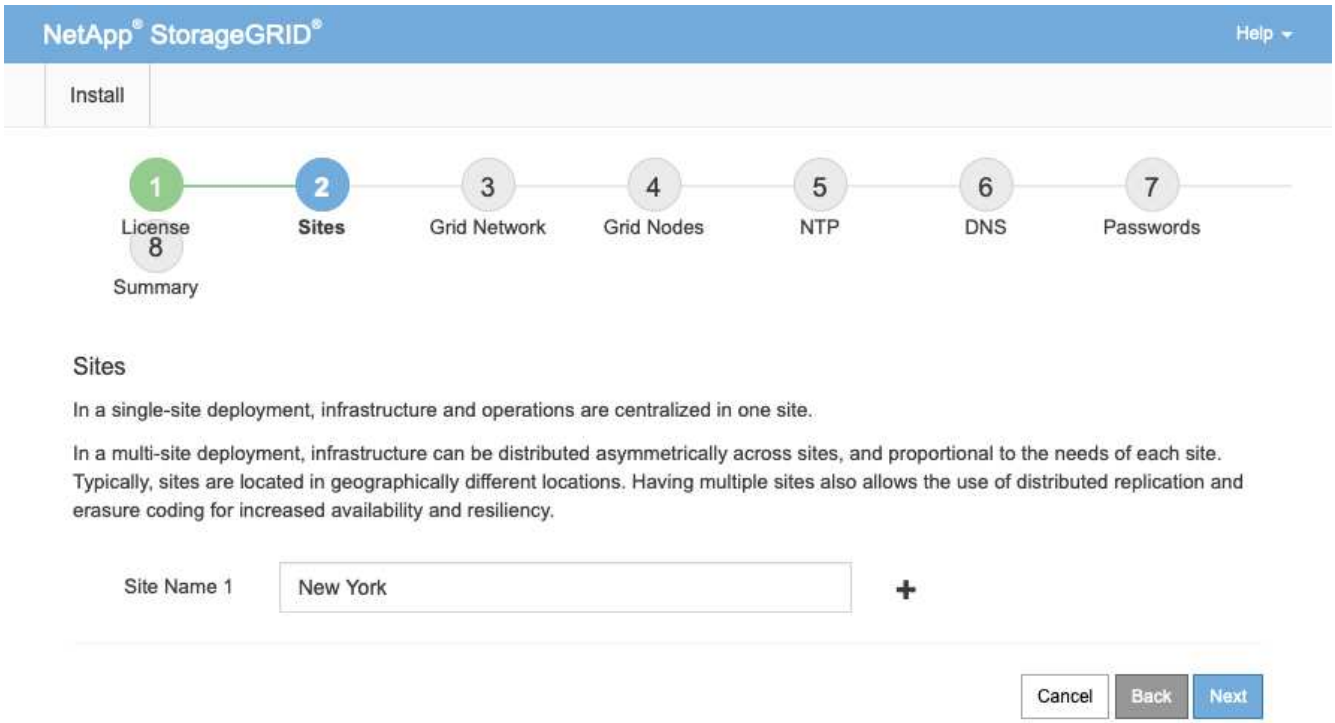
瞭解如何將站台新增至 StorageGRID 、以提高可靠性和儲存容量。

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。

若要新增站台、請完成下列步驟：

步驟

1. 在「站台」頁面上、輸入站台名稱。
2. 若要新增其他網站、請按一下最後一個網站項目旁的加號、然後在新的「網站名稱」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. 按一下「下一步」

為 **StorageGRID** 指定網格網路子網路

瞭解如何為 StorageGRID 設定網格網路子網路。

您必須指定網格網路上使用的子網路。

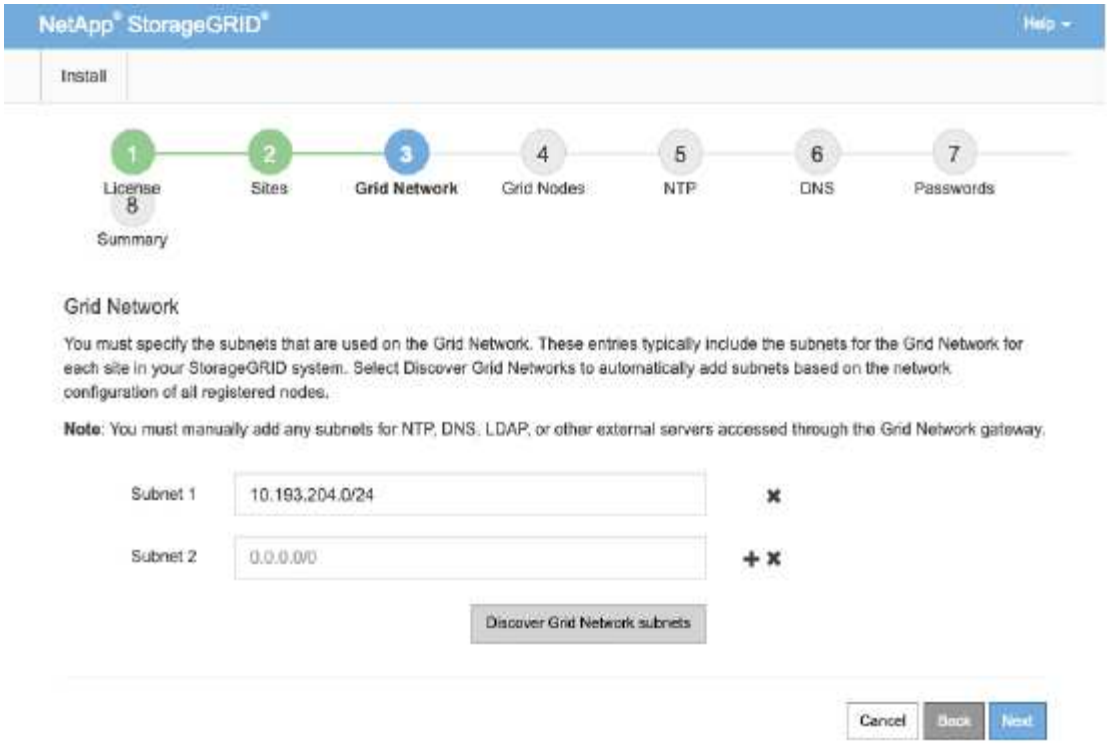
子網路項目包括 StorageGRID 系統中每個站台的網格網路子網路、以及必須透過網格網路存取的任何子網路（例如、裝載 NTP 伺服器的子網路）。

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。

若要指定網格網路子網路、請完成下列步驟：

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. 按一下最後一個項目旁的加號、以新增額外的網路項目。如果您已部署至少一個節點、請按一下「探索網格網路子網路」、以自動填入網格網路子網路清單、其中包含已向 Grid Manager 註冊的網格節點所報告的子網路。



3. 按一下「下一步」

核准 **StorageGRID** 的網格節點

瞭解如何檢閱和核准任何加入 StorageGRID 系統的擱置網格節點。

您必須先核准每個網格節點、才能加入 StorageGRID 系統。

開始之前、必須部署所有虛擬和 StorageGRID 應用裝置網格節點。

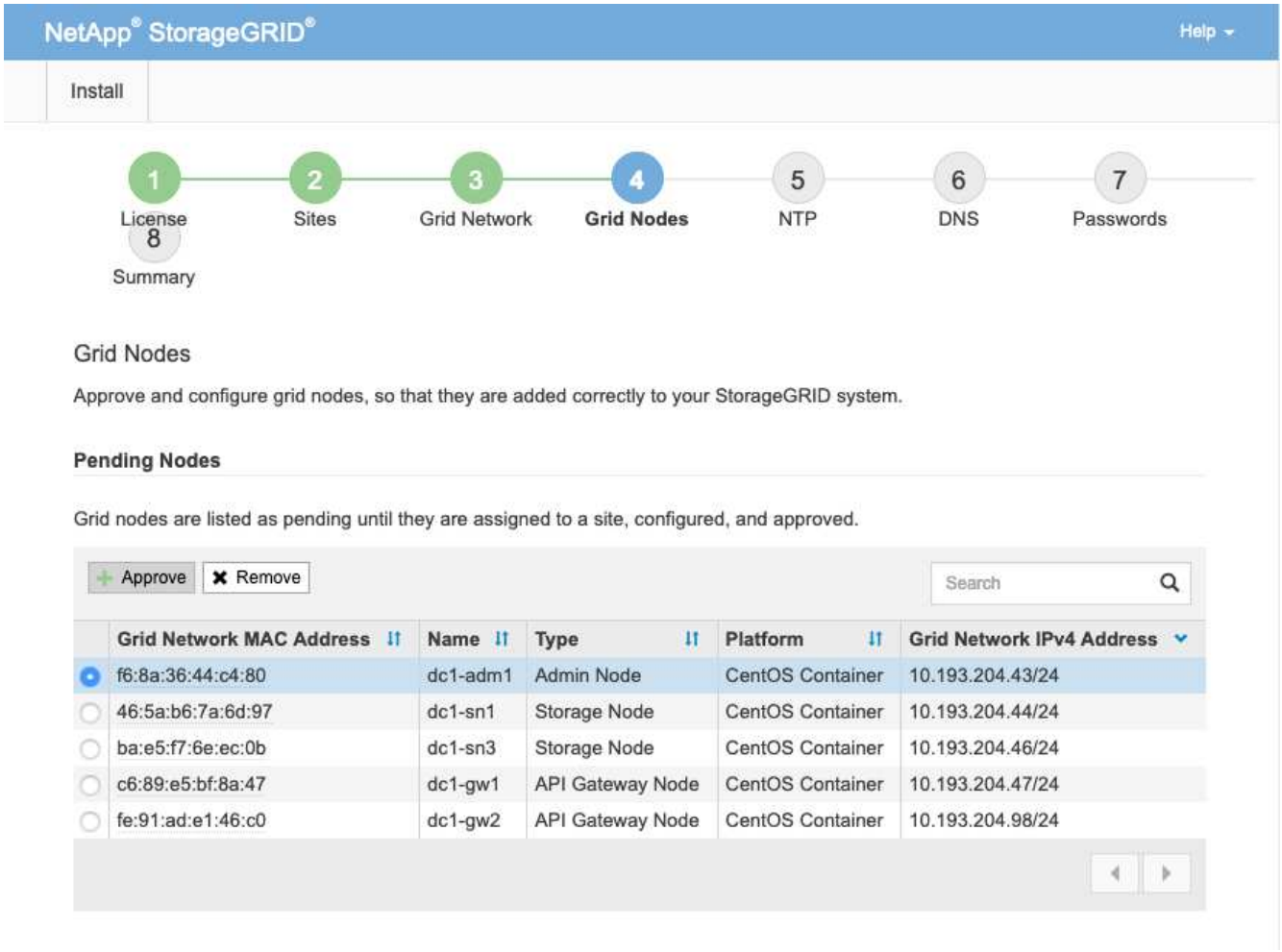
若要核准擱置的網格節點、請完成下列步驟：

步驟

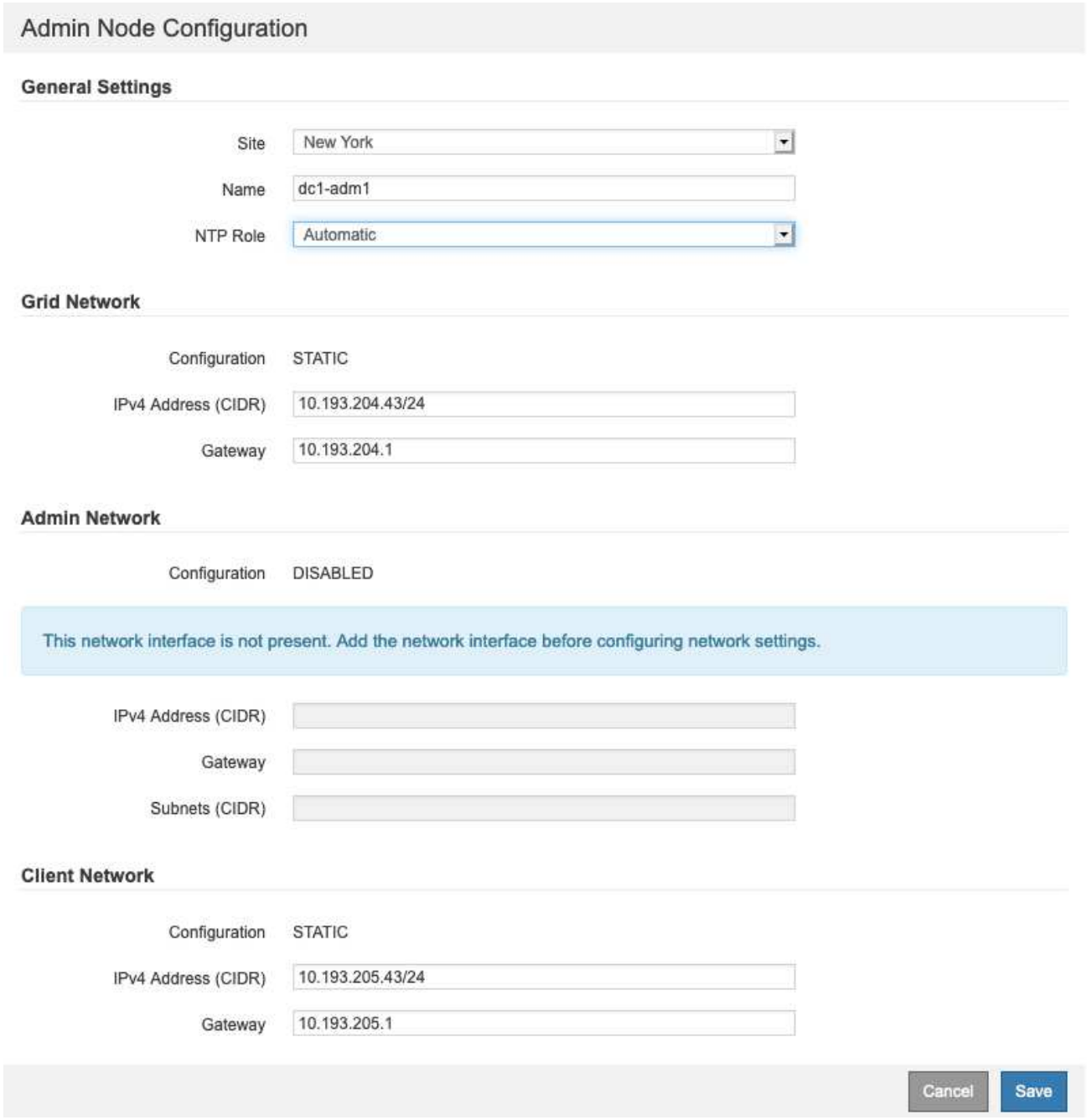
1. 檢閱「擱置節點」清單、並確認它顯示您部署的所有網格節點。

   如果缺少網格節點、請確認已成功部署。

2. 按一下您要核准之擱置節點旁的選項按鈕。



3. 按一下「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。

--**Name** ：將指派給節點的主機名稱、以及將在 Grid Manager 中顯示的名稱。名稱預設為您在節點部署期間指定的名稱、但您可以視需要變更名稱。

--* NTP 角色 * ：網格節點的 NTP 角色。選項包括「自動」、「主要」和「用戶端」。選取「自動」選項會將主要角色指派給管理節點、具有管理網域控制器（ 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。

--*ADC 服務（僅限儲存節點） * ：選取「自動」、讓系統判斷節點是否需要 ADC 服務。ADC服務會追蹤網

格服務的位置和可用度。每個站台至少有三個儲存節點必須包含 ADC 服務。部署之後、您無法將該ADC服務新增至節點。

5. 在 Grid Network 中、視需要修改下列內容的設定：

   --*IPv4 位址（ CIDR ） * ：網格網路介面的 CIDR 網路位址（容器內的 eth0 ）。例如 `192.168.1.234/24`：。

   --Gateway ：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。

   > 如果您為網格網路組態選取 DHCP 、並在此處變更值、則新值會在節點上設定為靜態位址。請確定產生的 IP 位址不在 DHCP 位址集區中。

6. 若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。

   > 如果您為管理網路組態選取 DHCP 、並在此處變更值、則新值會在節點上設定為靜態位址。請確定產生的 IP 位址不在 DHCP 位址集區中。

   - 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、選取功能表：進階 [重新開機] 。重新開機可能需要數分鐘的時間。
     b. 選取功能表：設定網路 [連結組態] 並啟用適當的網路。
     c. 選取功能表：設定網路 [IP 組態] 並設定啟用的網路。
     d. 返回首頁、然後按一下「開始安裝」。
     e. 在 Grid Manager 中：如果節點列在 Approved Nodes 表中、請重設節點。
     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。您應該已經在「IP組態」頁面上填入您提供的資訊。如需更多資訊、請參閱應用裝置機型的安裝與維護說明。

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。

   - 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、選取功能表：進階 [重新開機] 。重新開機可能需要數分鐘的時間。
     b. 選取功能表：設定網路 [連結組態] 並啟用適當的網路。
     c. 選取功能表：設定網路 [IP 組態] 並設定啟用的網路。
     d. 返回首頁、然後按一下「開始安裝」。

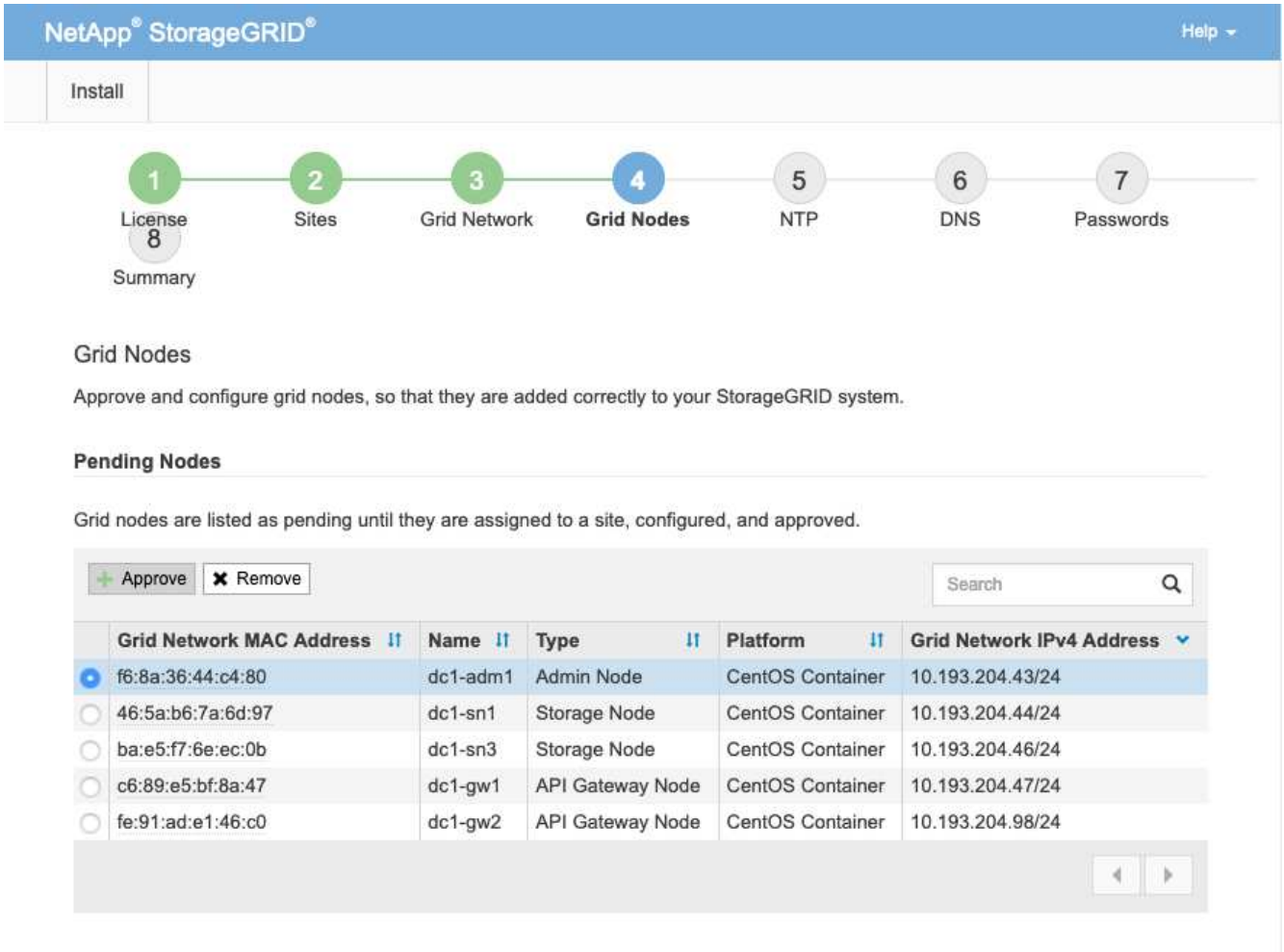
e. 在 Grid Manager 中：如果節點列在 Approved Nodes 表中、請重設節點。

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。您應該已經在「IP組態」頁面上填入您提供的資訊。如需更多資訊、請參閱設備的安裝與維護說明。

8. 按一下儲存。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待定網格節點、重複步驟 1-8 。

您必須核准網格中所需的所有節點。不過、您可以在按一下「摘要」頁面上的「安裝」之前、隨時返回此頁面。若要修改已核准網格節點的內容、請按一下其選項按鈕、然後按一下編輯。

10. 完成網格節點的核准後、請按一下「下一步」。

指定 **StorageGRID** 的 **NTP** 伺服器詳細資料

瞭解如何指定 StorageGRID 系統的 NTP 組態資訊、以便讓在不同伺服器上執行的作業保持同步。

若要避免時間漂移問題、您必須指定第 3 層或更高層的四個外部 NTP 伺服器參考資料。

指定外部NTP來源進行正式作業層級StorageGRID 的安裝時、請勿在Windows Server 2016之前的Windows版本上使用Windows Time（W32Time）服務。舊版 Windows 上的時間服務不夠準確、 Microsoft 不支援在 StorageGRID 等要求嚴苛的環境中使用。

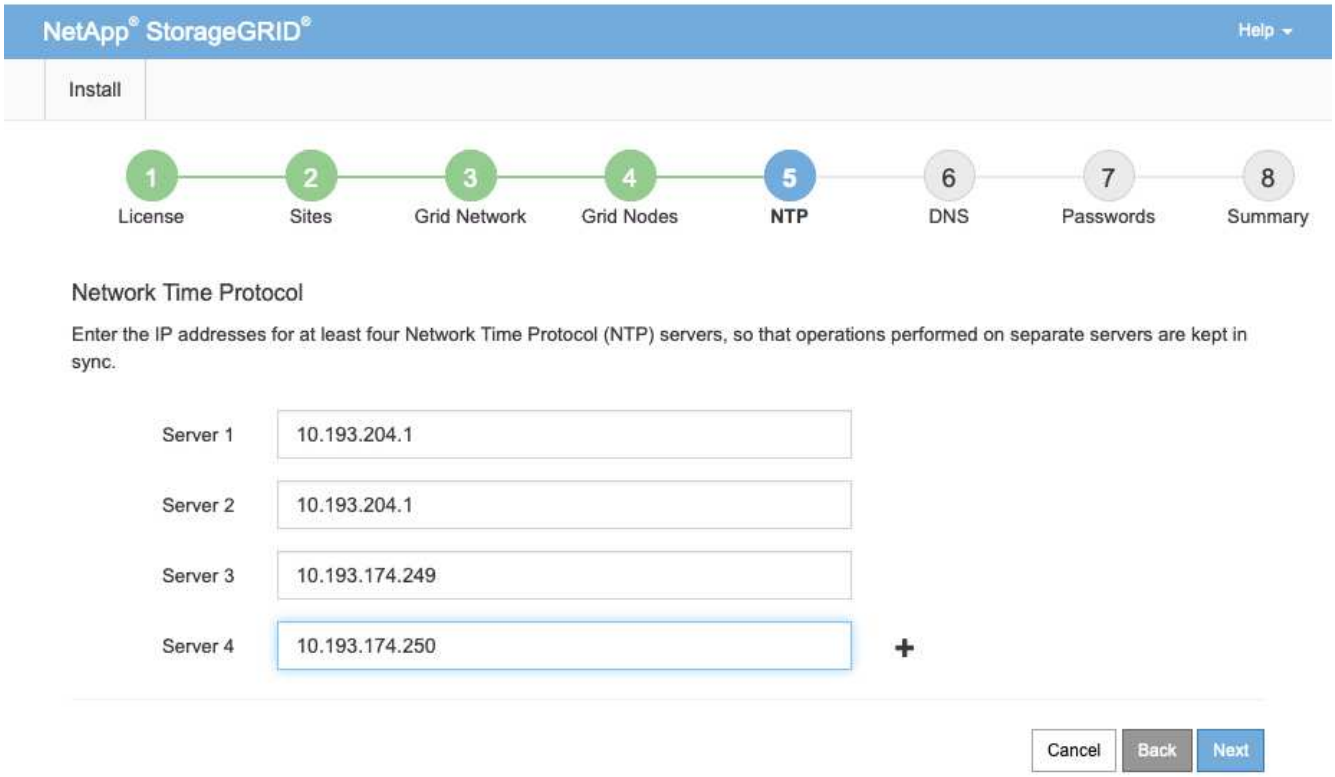
外部 NTP 伺服器會由先前指派主要 NTP 角色的節點使用。

在安裝程序中、用戶端網路未提早啟用、無法成為唯一的 NTP 伺服器來源。請確定至少可以透過網格網路或管理網路連線到一個 NTP 伺服器。

若要指定 NTP 伺服器資訊、請完成下列步驟：

步驟

1. 在伺服器 1 至伺服器 4 文字方塊中、指定至少四個 NTP 伺服器的 IP 位址。
2. 如有必要、請按一下最後一個項目旁的加號、以新增更多伺服器項目。



3. 按一下「下一步」

指定 **StorageGRID** 的 **DNS** 伺服器詳細資料

瞭解如何設定 StorageGRID 的 DNS 伺服器。

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。

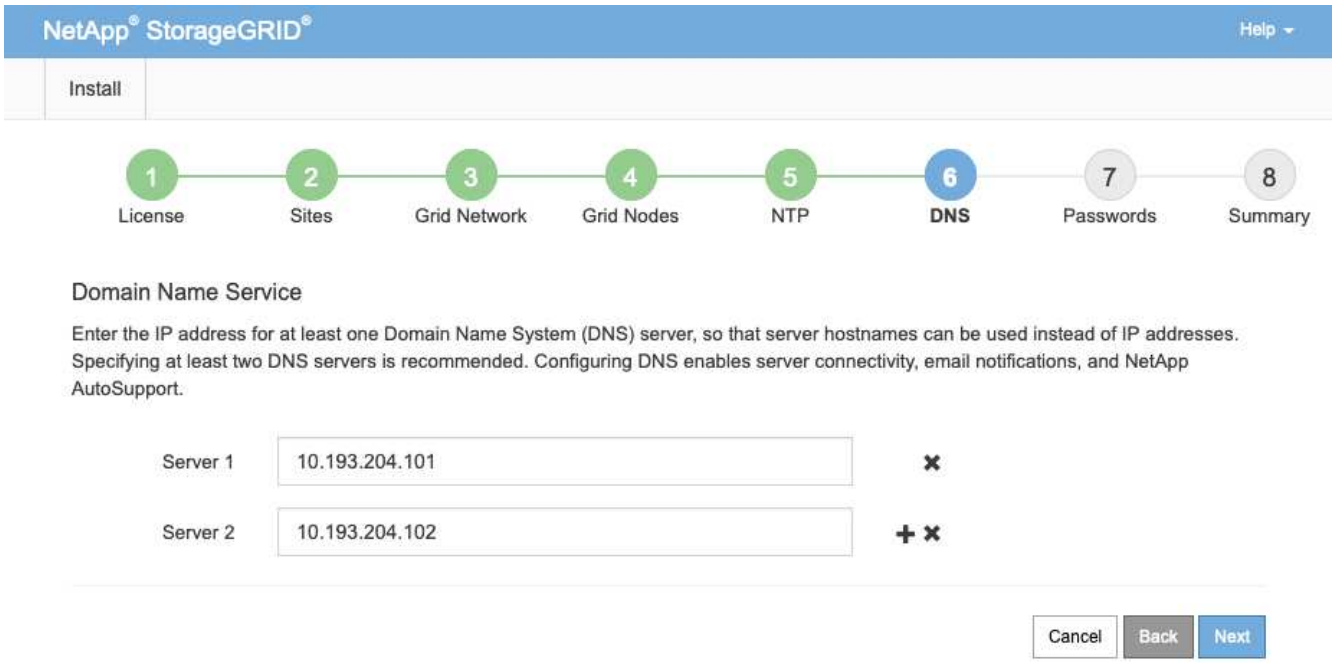
指定 DNS 伺服器資訊可讓您使用完整網域名稱（ FQDN ）主機名稱、而非 IP 位址來接收電子郵件通知和 NetApp AutoSupport ® 訊息。NetApp 建議指定至少兩部 DNS 伺服器。

您應該選取DNS伺服器、以便每個站台在網路中斷時、都能在本機存取。

若要指定 DNS 伺服器資訊、請完成下列步驟：

步驟

1. 在伺服器 1 文字方塊中、指定 DNS 伺服器的 IP 位址。
2. 如有必要、請按一下最後一個項目旁的加號、以新增更多伺服器。



3. 按一下「下一步」

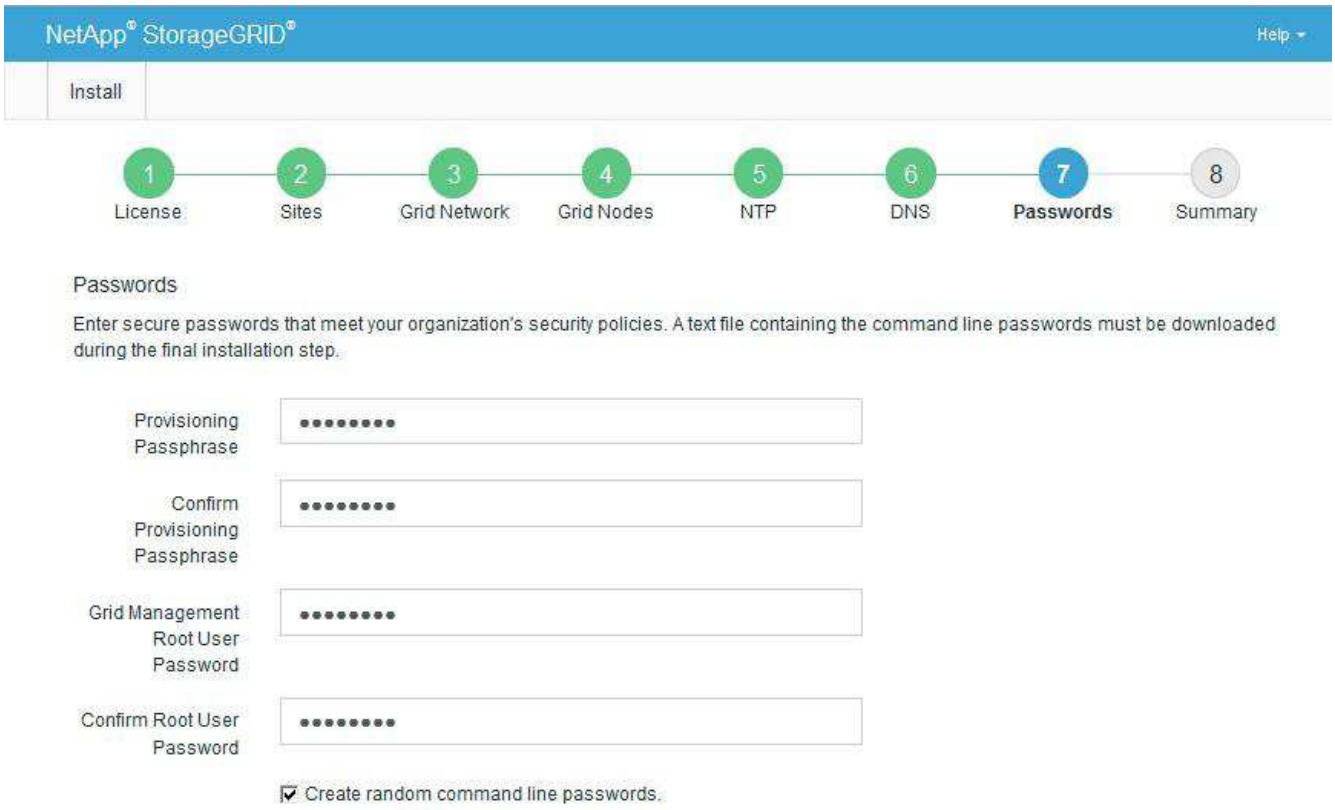
指定 **StorageGRID** 的系統密碼

瞭解如何透過設定資源配置密碼和 Grid Management root 使用者密碼來保護 StorageGRID 系統的安全。

若要輸入用來保護 StorageGRID 系統安全的密碼、請依照下列步驟進行：

步驟

1. 在「資源配置密碼」中、輸入變更 StorageGRID 系統網格拓撲所需的資源配置密碼。您應該在安全的地方記錄此密碼。
2. 在確認資源配置密碼中、重新輸入資源配置密碼。
3. 在 Grid Management Root User Password （網格管理根使用者密碼）中、輸入密碼以作為 root 使用者存取 Grid Manager 。
4. 在確認根使用者密碼中、重新輸入 Grid Manager 密碼。



5. 如果您為了概念驗證或示範目的而安裝網格、請取消選取「建立隨機命令列密碼」選項。

   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、請取消選取「僅為展示網格建立隨機命令列密碼」選項。

   > 在 Summary （摘要）頁面上單擊 Install （安裝）時，系統將提示您下載 Recovery Package 文件 (`sgws-recovery-packageid-revision.zip`）。您必須下載此檔案才能完成安裝。存取系統的密碼會儲存在 `Passwords.txt` 包含在恢復套件檔案中的檔案中。

6. 按一下「下一步」

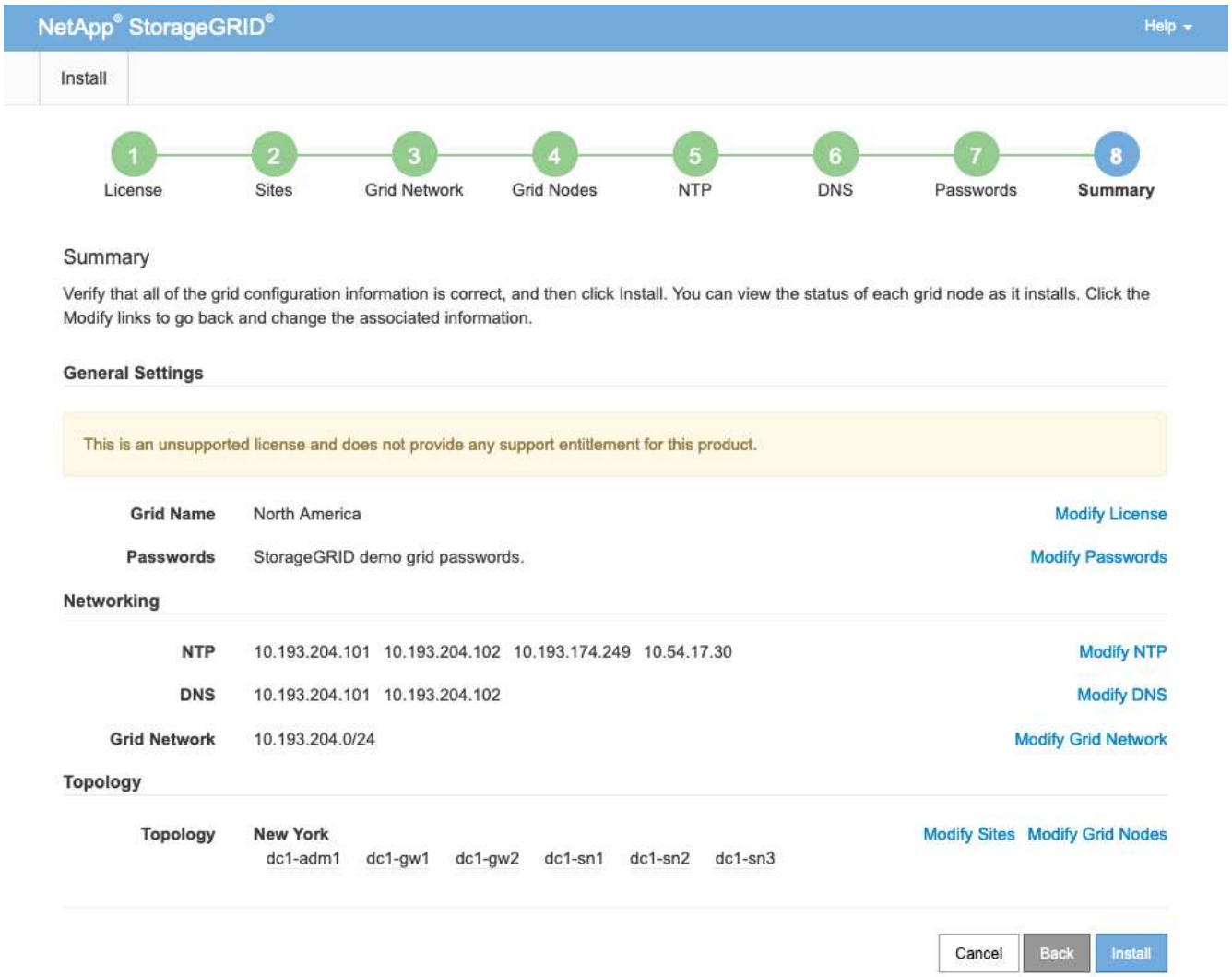
檢閱組態並完成 **StorageGRID** 安裝

瞭解如何驗證網格組態資訊、並完成 StorageGRID 安裝程序。

為了確保安裝順利完成、請仔細檢閱您輸入的組態資訊。請遵循下列步驟。

步驟

1. 檢視摘要頁面。



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. 按一下「安裝」。

> 如果節點設定為使用用戶端網路、則當您按一下「安裝」時、該節點的預設閘道會從網格網路切換至用戶端網路。如果連線中斷、請確定您是透過可存取的子網路存取主管理節點。如需詳細資訊、請參閱「網路安裝與配置」。

4. 按一下下載恢復套件。

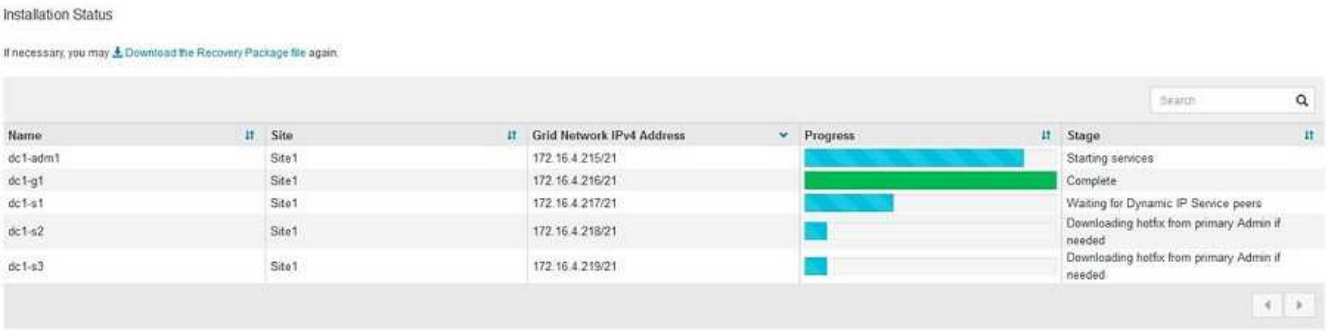
   當安裝過程進入網格拓撲定義點時，系統會提示您下載恢復軟件包文件）並確認您可以訪問此文件的 (`.zip` 內容。您必須下載「恢復套件」檔案、以便在一或多個網格節點故障時恢復 StorageGRID 系統。

   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。

5. 選取「我已成功下載並驗證修復套件檔案」選項、然後按一下「下一步」。

如果安裝仍在進行中、則會開啟「安裝狀態」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、會開啟 Grid Manager 的登入頁面。

6. 以 root 使用者身分登入 Grid Manager 、並使用您在安裝期間指定的密碼。

升級 **StorageGRID** 中的裸機節點

瞭解 StorageGRID 中裸機節點的升級程序。

裸機節點的升級程序與應用裝置或 VMware 節點的升級程序不同。在執行裸機節點升級之前、您必須先升級所有主機上的 RPM 檔案、然後才能透過 GUI 執行升級。

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

現在您可以透過 GUI 繼續進行軟體升級。

TR-4907 ：使用 Veritas Enterprise Vault 設定 StorageGRID

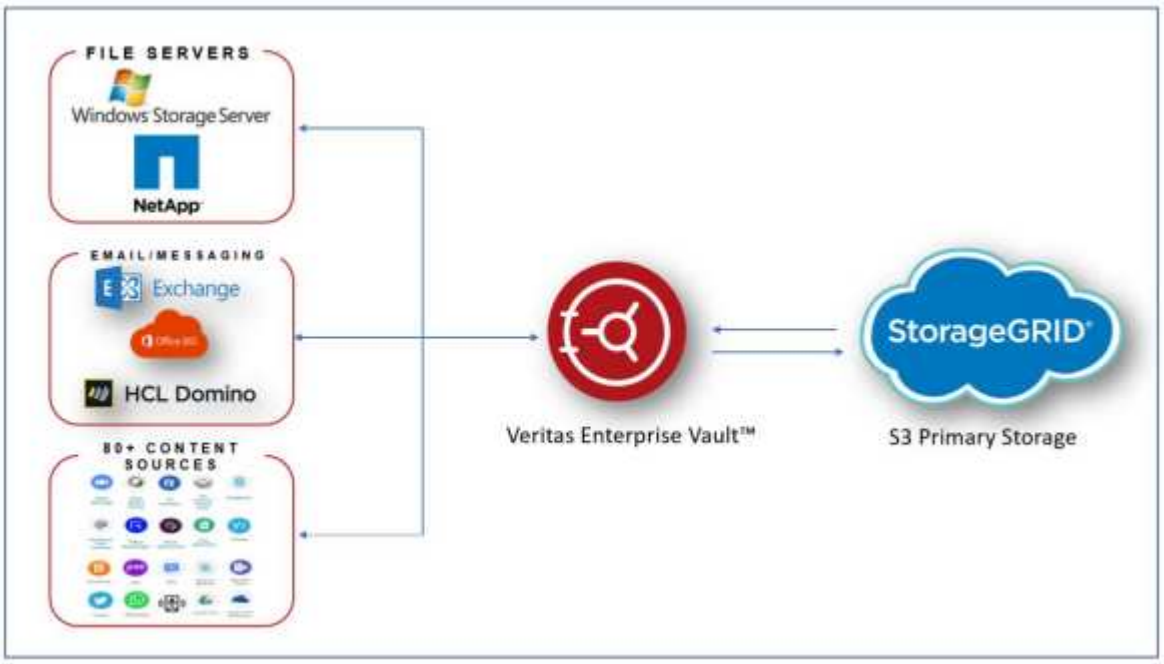
設定 StorageGRID 進行站台容錯移轉簡介

瞭解 Veritas Enterprise Vault 如何使用 StorageGRID 做為災難恢復的主要儲存目標。

本組態指南提供將 NetApp ® StorageGRID ® 設定為 Veritas Enterprise Vault 主要儲存目標的步驟。同時也說明如何在災難恢復（ DR ）案例中設定 StorageGRID 以進行站台容錯移轉。

參考架構

StorageGRID 為 Veritas Enterprise Vault 提供內部部署且與 S3 相容的雲端備份目標。下圖說明 Veritas Enterprise Vault 和 StorageGRID 架構。



何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID 文件中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 啟用 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/

設定 StorageGRID 和 Veritas Enterprise Vault

瞭解如何實作 StorageGRID 11.5 以上版本和 Veritas Enterprise Vault 14.1 以上版本的基本組態。

本組態指南以 StorageGRID 11.5 和 Enterprise Vault 14.1 為基礎。使用 S3 物件鎖定、 StorageGRID 11.6 和 Enterprise Vault 14.2.2 讀取多項（ WORM ）模式儲存設備一次寫入。如需這些準則的詳細資訊、請參閱 "StorageGRID 文件" 頁面或聯絡 StorageGRID 專家。

設定 **StorageGRID** 和 **Veritas Enterprise Vault** 的先決條件

- 在使用 Veritas Enterprise Vault 設定 StorageGRID 之前、請先確認下列先決條件：

> ⓘ 對於 WORM 儲存（物件鎖定）、需要 StorageGRID 11.6 或更高版本。

- 已安裝 Veritas Enterprise Vault 14.1 或更新版本。

> ⓘ 對於 WORM 儲存（物件鎖定）、需要 Enterprise Vault 14.2.2 版或更新版本。

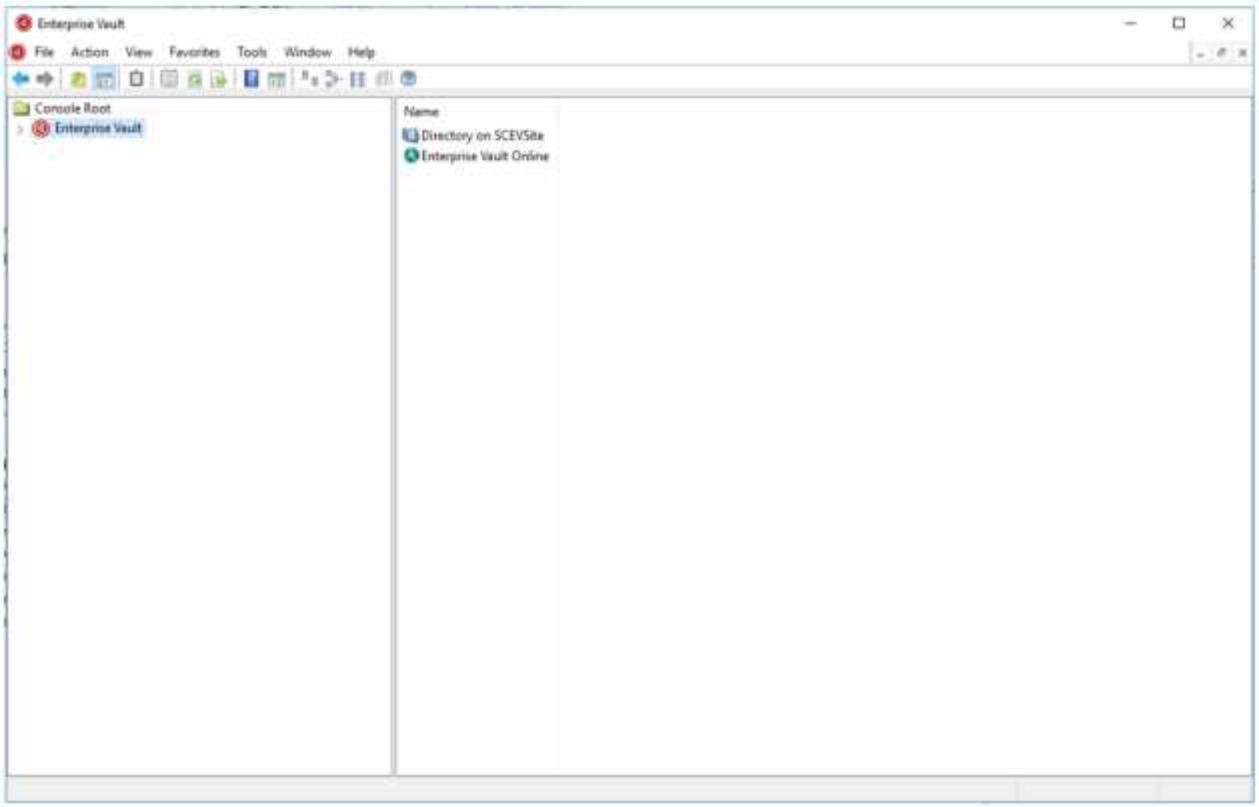
- 已建立資料保險箱儲存區群組和資料保險箱儲存區。如需詳細資訊、請參閱《 Veritas Enterprise Vault 管理指南》。
- 已建立 StorageGRID 租戶、存取金鑰、秘密金鑰和貯體。
- 已建立 StorageGRID 負載平衡器端點（ HTTP 或 HTTPS ）。
- 如果使用自我簽署的憑證、請將 StorageGRID 自我簽署的 CA 憑證新增至 Enterprise Vault 伺服器。如需詳細資訊，請參閱本 "Veritas 知識庫文章"。
- 更新並套用最新的 Enterprise Vault 組態檔案、以啟用支援的儲存解決方案、例如 NetApp StorageGRID 。如需詳細資訊，請參閱本 "Veritas 知識庫文章"。

使用 **Veritas Enterprise Vault** 設定 **StorageGRID**

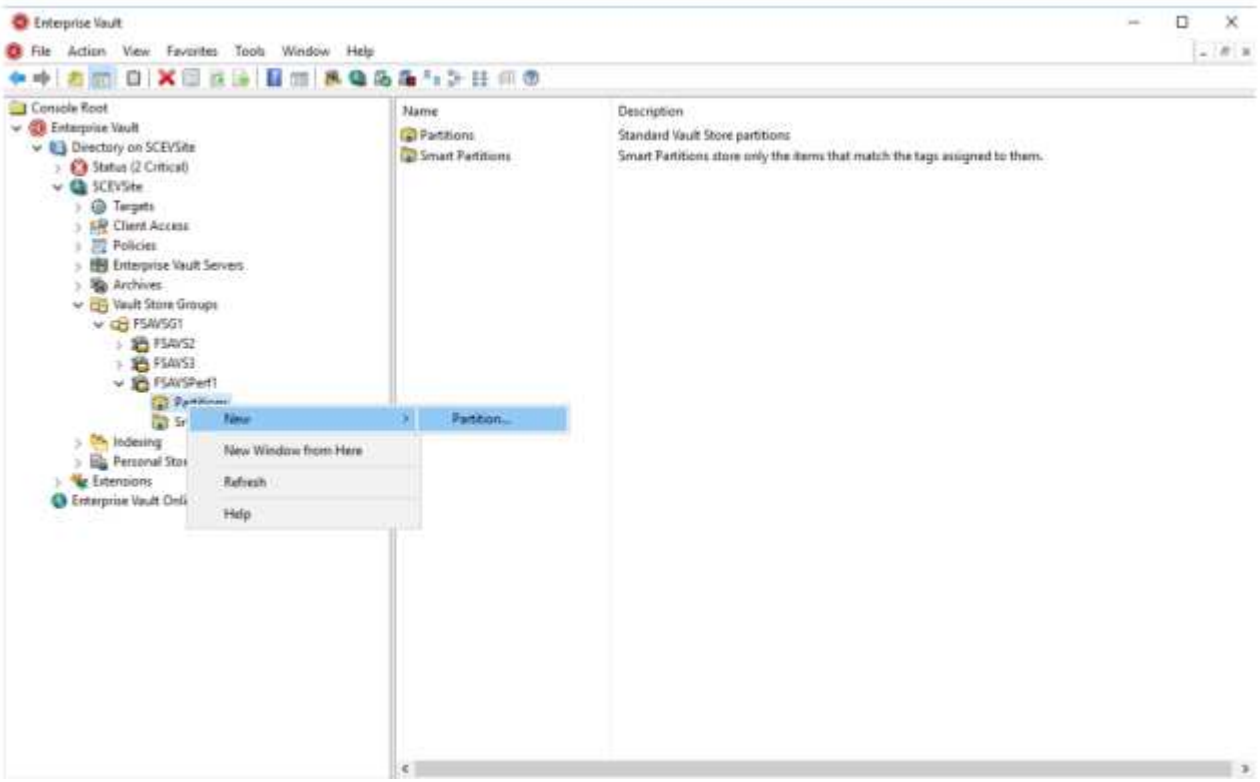
若要使用 Veritas Enterprise Vault 設定 StorageGRID 、請競爭下列步驟：

步驟

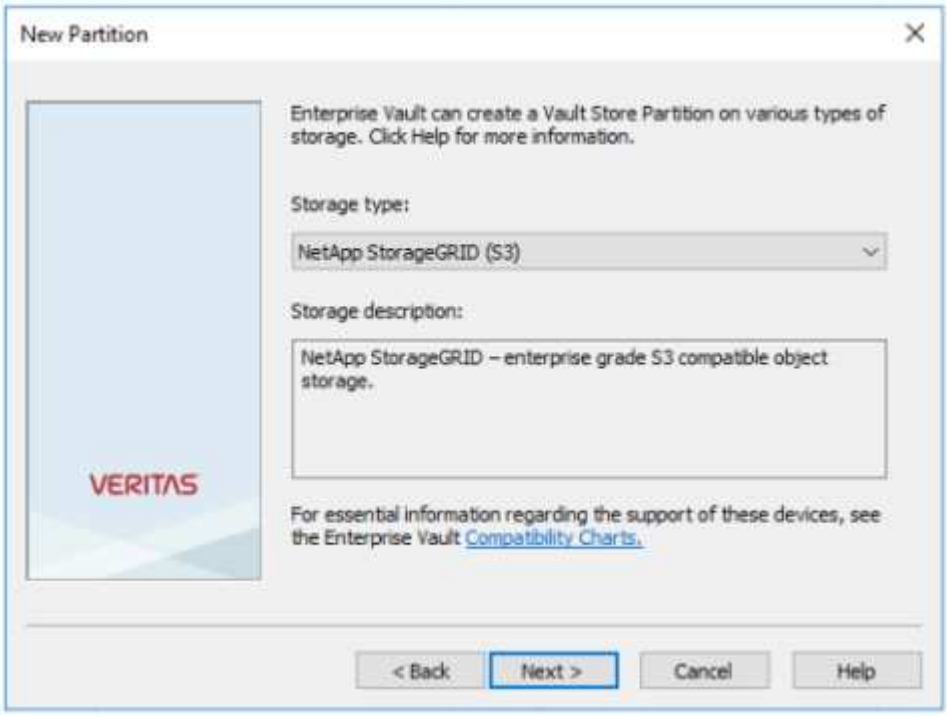
1. 啟動 Enterprise Vault Administration 主控台。



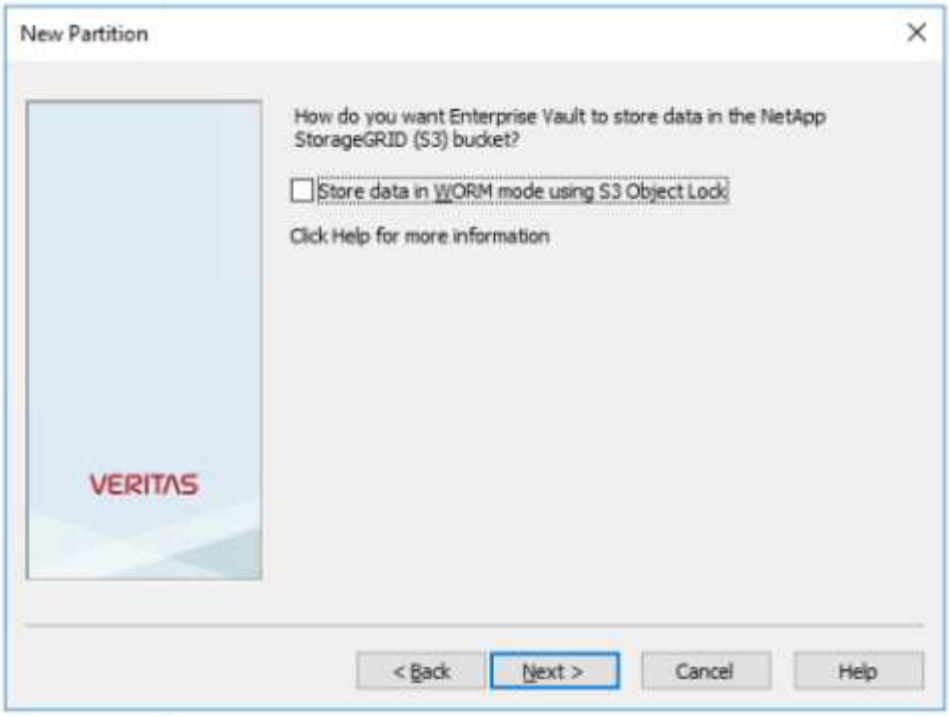
2. 在適當的資料保險箱儲存區中建立新的資料保險箱儲存區分割區。展開資料保險箱儲存群組資料夾、然後展開適當的資料保險箱儲存區。在分割區上按一下滑鼠右鍵、然後選取功能表：新增 [分割區] 。



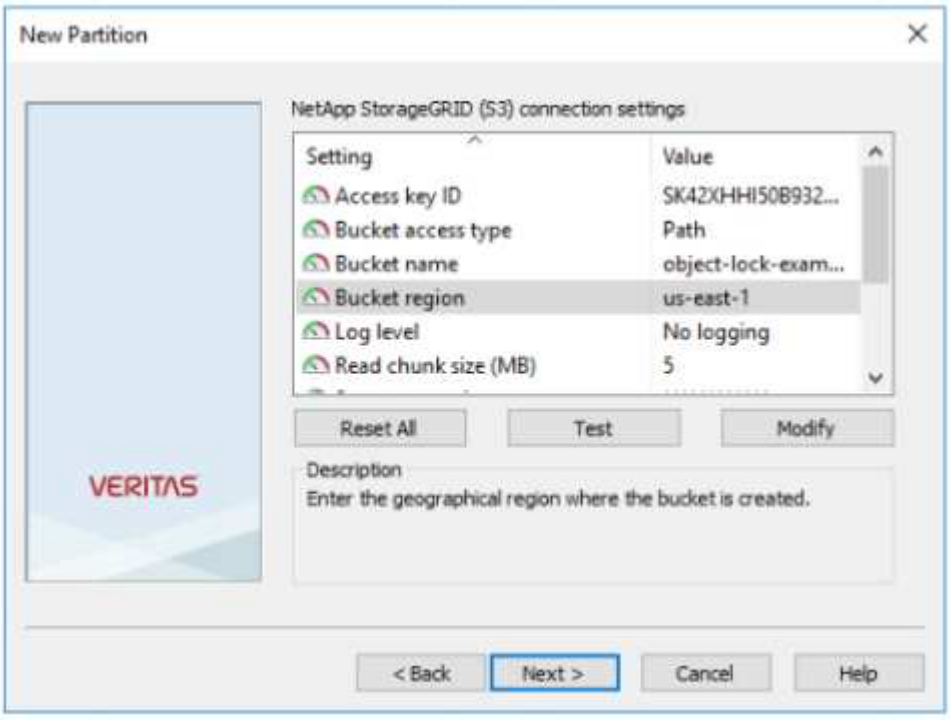
3. 按照新建分區創建嚮導進行操作。從儲存類型下拉式功能表中、選取 NetApp StorageGRID （ S3 ）。按一下「下一步」



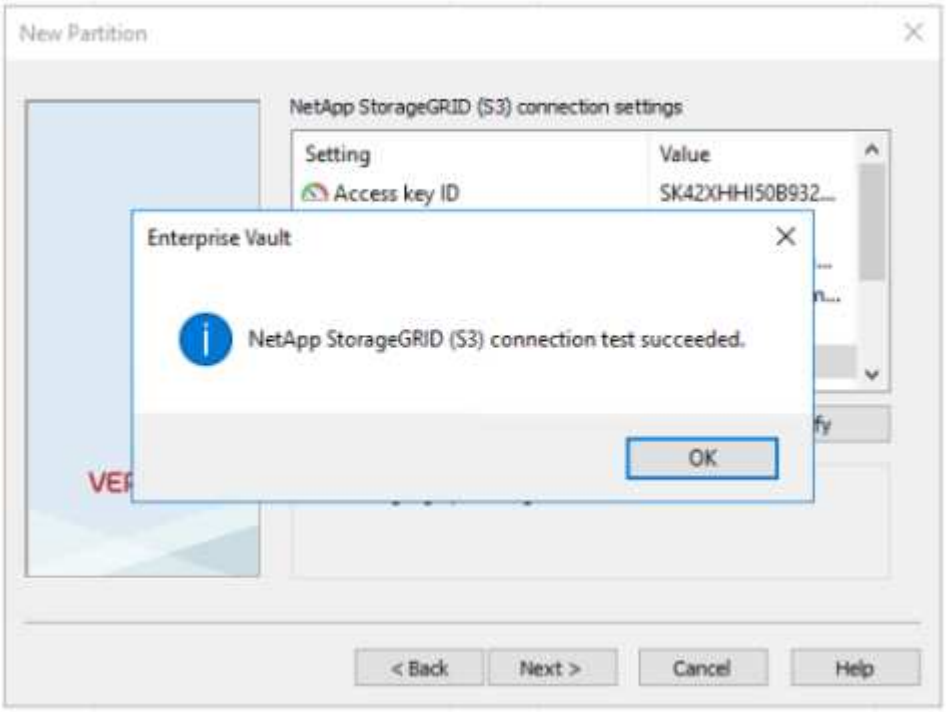
4. 取消核取「使用 S3 物件鎖定將資料儲存在 WORM 模式」選項。按一下「下一步」



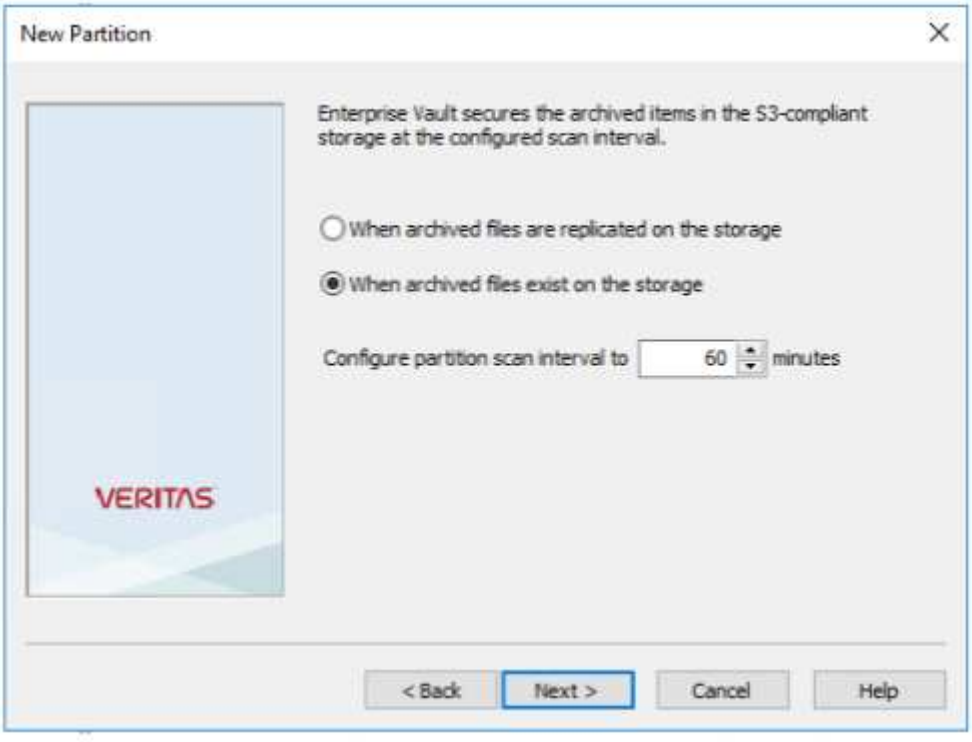
5. 在連線設定頁面上、提供下列資訊：
   - 存取金鑰ID
   - 機密存取金鑰
   - 服務主機名稱：確保包含在 StorageGRID 中設定的負載平衡器端點（ LBE ）連接埠（例如： https ： <hostname> ： <LBE_port> ）
   - 貯體名稱：預先建立的目標貯體名稱。 Veritas Enterprise Vault 不會建立貯體。
   - 貯體區域： `us-east-1` 為預設值。



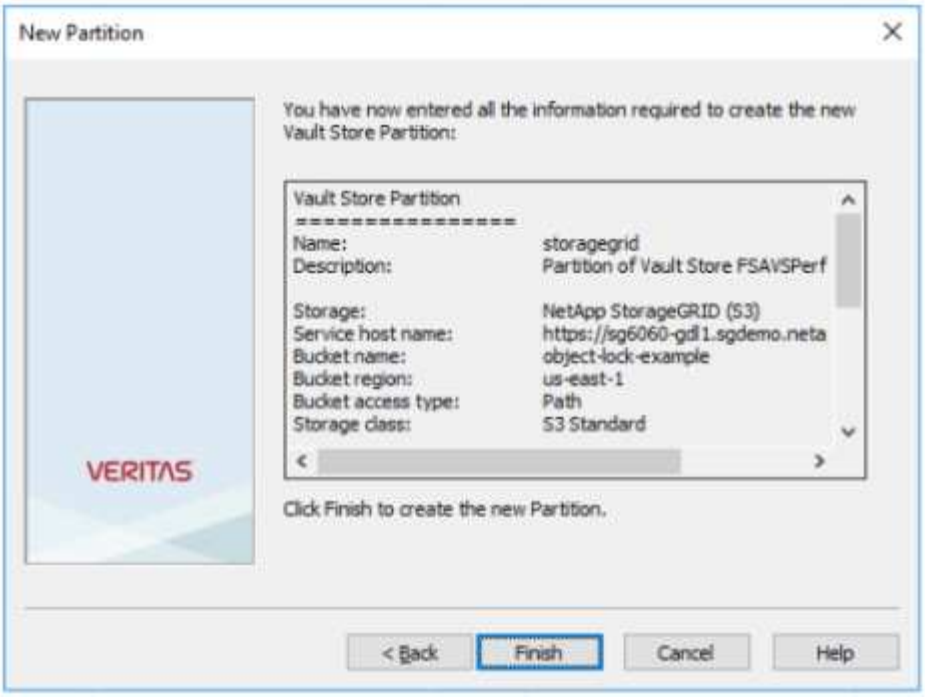
6. 若要驗證與 StorageGRID 貯體的連線、請按一下測試。確認連線測試成功。按一下確定、然後按下一步。



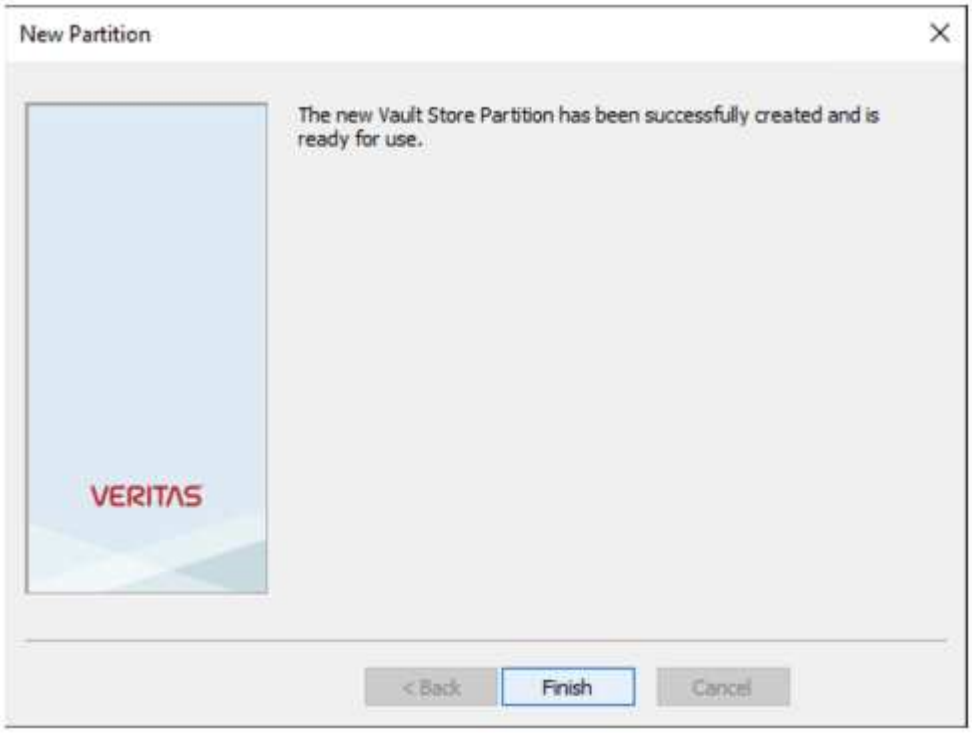
7. StorageGRID 不支援 S3 複寫參數。為了保護您的物件、 StorageGRID 使用資訊生命週期管理（ ILM ）規則來指定資料保護方案 - 多個複本或銷毀編碼。選取「儲存選項」上的「當歸檔檔案存在時」、然後按「下一步」。



8. 確認摘要頁面上的資訊、然後按一下「完成」。



9. 成功建立新的資料保險箱存放區分割區之後、您可以將 StorageGRID 做為主要儲存設備、在 Enterprise Vault 中歸檔、還原及搜尋資料。



針對 **WORM** 儲存設定 **StorageGRID S3** 物件鎖定

瞭解如何使用 S3 物件鎖定來設定 StorageGRID for WORM 儲存設備。

設定 **StorageGRID for WORM** 儲存設備的必要條件

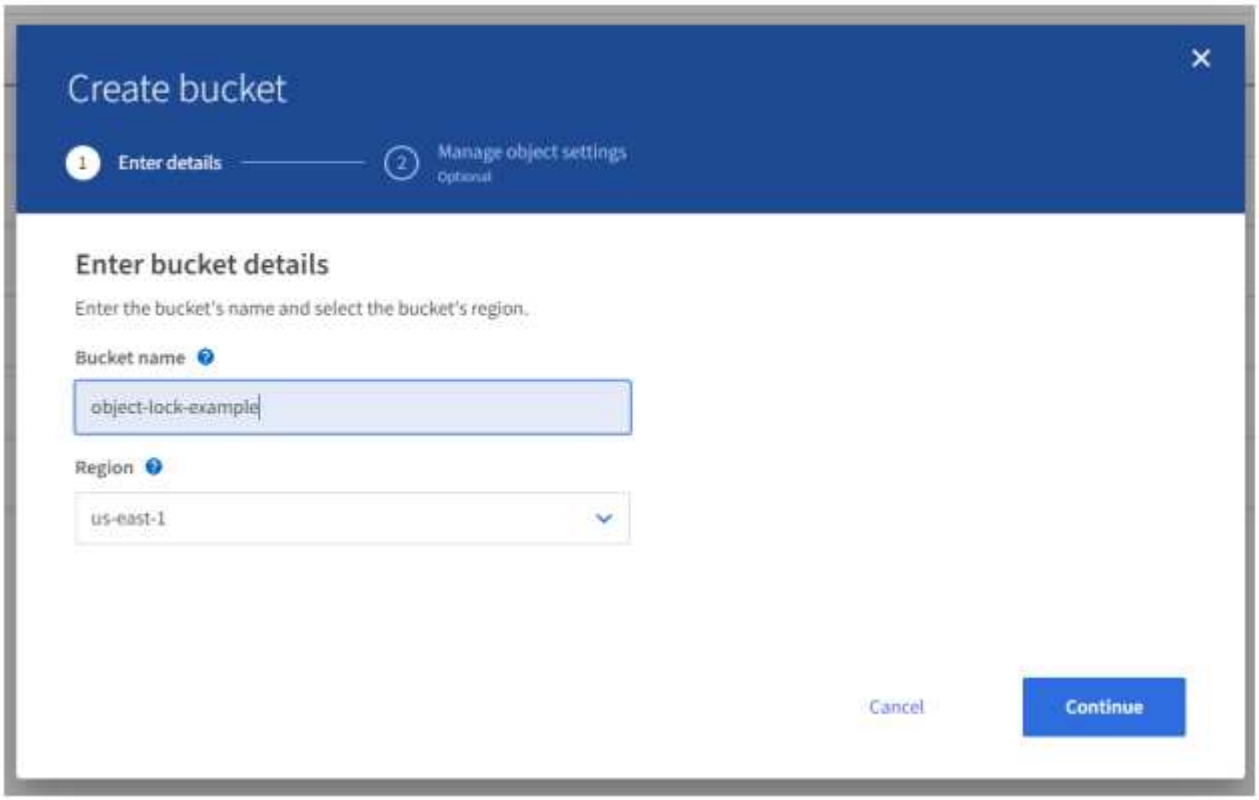
對於 WORM 儲存設備、 StorageGRID 使用 S3 物件鎖定來保留物件以符合法規要求。這需要 StorageGRID 11.6 或更高版本、其中引進了 S3 物件鎖定預設貯體保留。Enterprise Vault 也需要 14.2.2 版或更新版本。

設定 **StorageGRID S3** 物件鎖定預設貯體保留

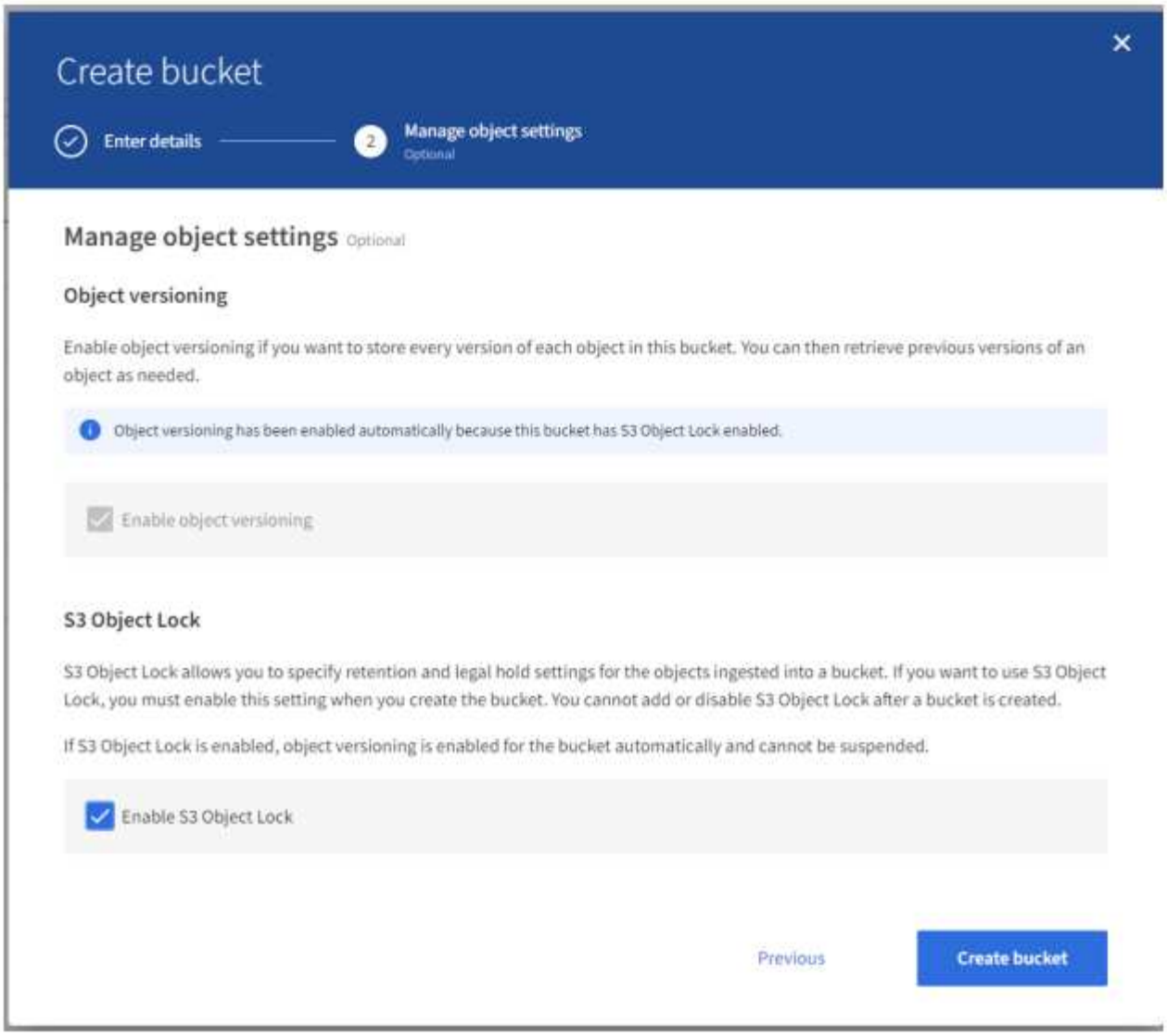
若要設定 StorageGRID S3 物件鎖定預設貯體保留、請完成下列步驟：

步驟

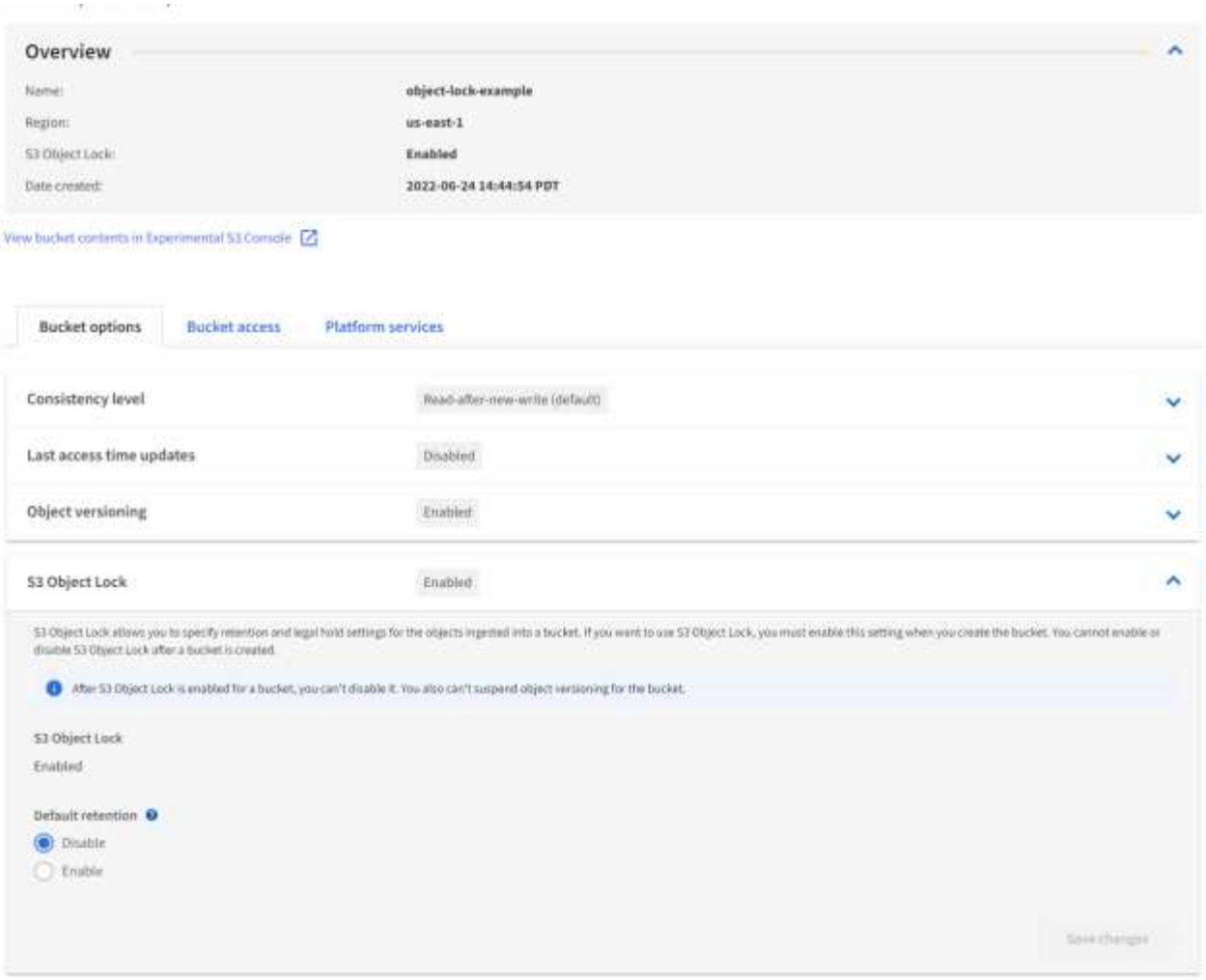
1. 在 StorageGRID 租戶管理器中、建立一個貯體、然後按一下「繼續」



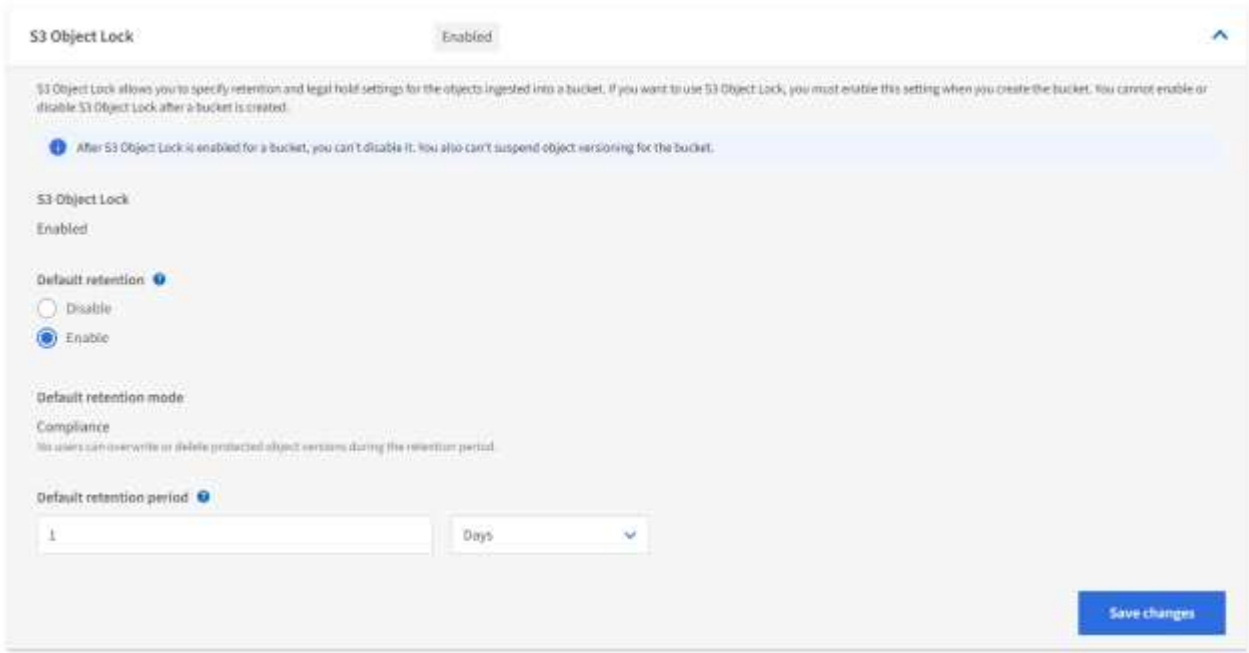
2. 選取「啟用 S3 物件鎖定」選項、然後按一下「建立儲存庫」。



3. 建立貯體後、請選擇貯體以檢視貯體選項。展開「 S3 物件鎖定」下拉式選項。



4. 在「預設保留」下、選取「啟用」、並將預設保留期間設為 1 天。按一下儲存變更。



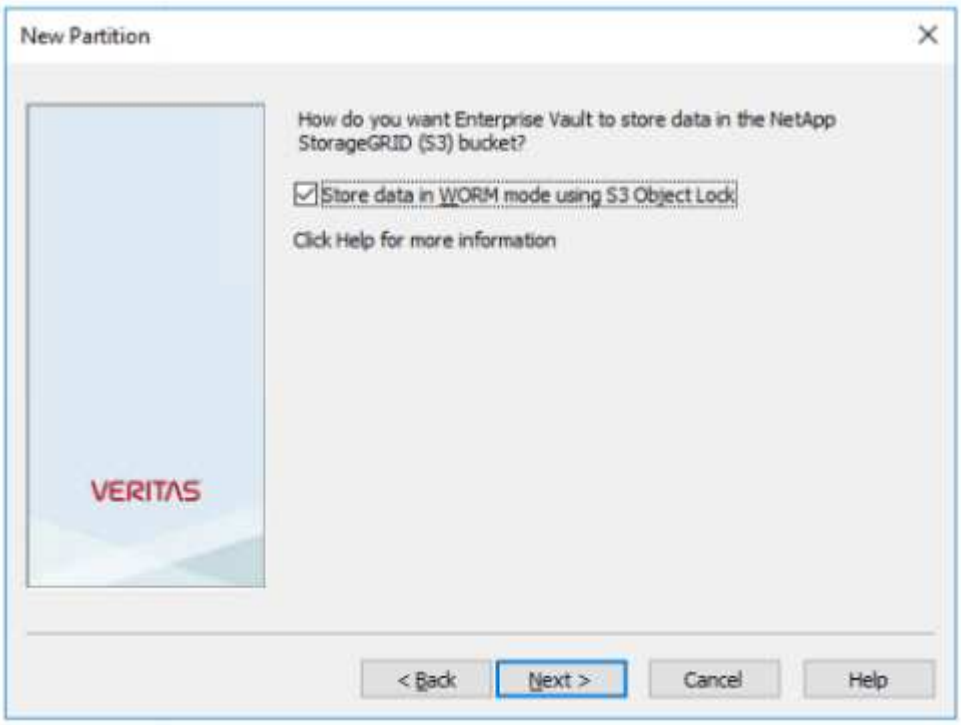
現在 Enterprise Vault 已準備好使用儲存 WORM 資料的儲存庫。

設定 **Enterprise Vault**

若要設定 Enterprise Vault 、請完成下列步驟：

步驟

1. 重複本節中的步驟 1-3 、 "基本組態" 但這次請選擇「使用 S3 物件鎖定將資料儲存在 WORM 模式」選項。按一下「下一步」



2. 輸入 S3 Bucket 連線設定時、請務必輸入已啟用 S3 物件鎖定預設保留功能的 S3 儲存區名稱。
3. 測試連線以驗證設定。

設定 **StorageGRID** 站台容錯移轉以進行災難恢復

瞭解如何在災難恢復案例中設定 StorageGRID 站台容錯移轉。

StorageGRID 架構部署通常是多站台部署。站台可以是主動式主動式或主動式被動式、以供 DR 使用。在 DR 案例中、請確定 Veritas Enterprise Vault 可以維持與其主要儲存設備（ StorageGRID ）的連線、並在站台故障期間繼續擷取及擷取資料。本節提供雙站台主動被動式部署的高階組態指南。 如需這些準則的詳細資訊、請參閱 "StorageGRID 文件" 頁面或聯絡 StorageGRID 專家。

使用 **Veritas Enterprise Vault** 設定 **StorageGRID** 的先決條件

設定 StorageGRID 站台容錯移轉之前、請先確認下列先決條件：

- 有兩個站台的 StorageGRID 部署、例如站台 1 和站台 2 。
- 已在每個站台上建立執行負載平衡器服務的管理節點或閘道節點、以進行負載平衡。

- 已建立 StorageGRID 負載平衡器端點。

設定 **StorageGRID** 站台容錯移轉

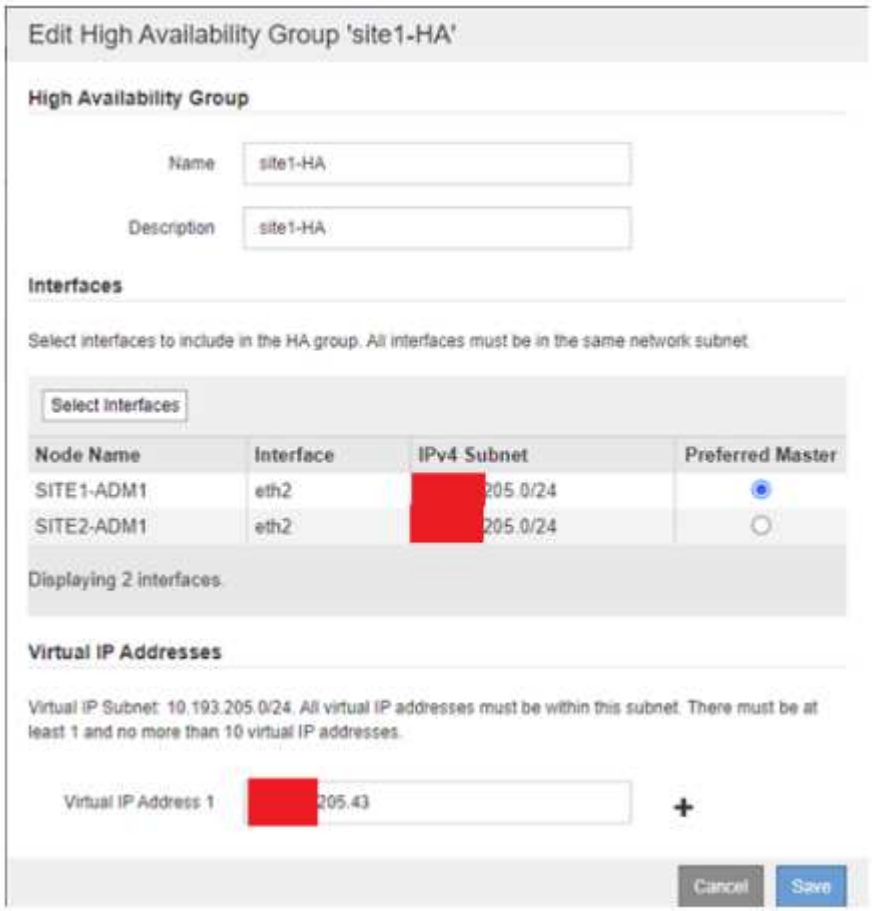
若要設定 StorageGRID 站台容錯移轉、請完成下列步驟：

步驟

1. 若要確保在站台故障期間連線至 StorageGRID 、請設定高可用度（ HA ）群組。從 StorageGRID Grid Manager 介面（ GMI ）、按一下組態、高可用度群組和 + 建立。

   [Vertas/Veritas-cree-high Availability 群組]

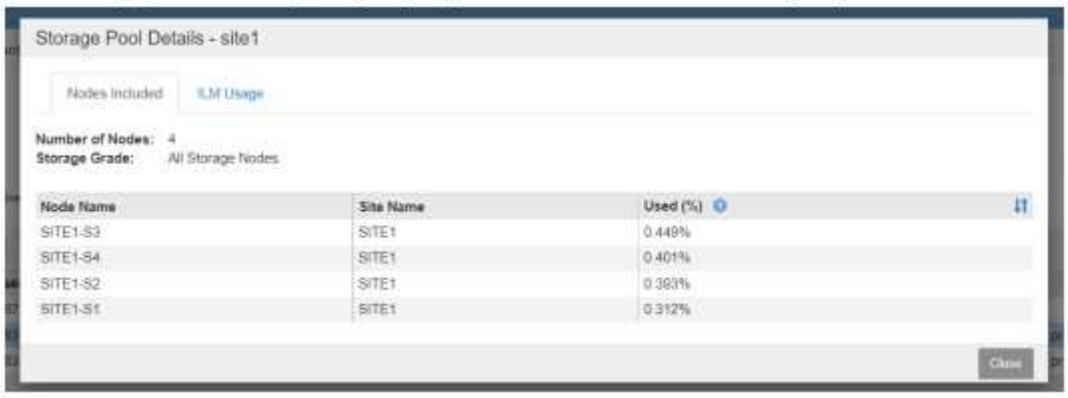
2. 輸入所需資訊。按一下「 Select Interfaces 」（選取介面）、同時納入站台 1 和站台 2 的網路介面、其中站台 1 （主要站台）是慣用的主要站台。在同一個子網路中指派虛擬 IP 位址。按一下儲存。

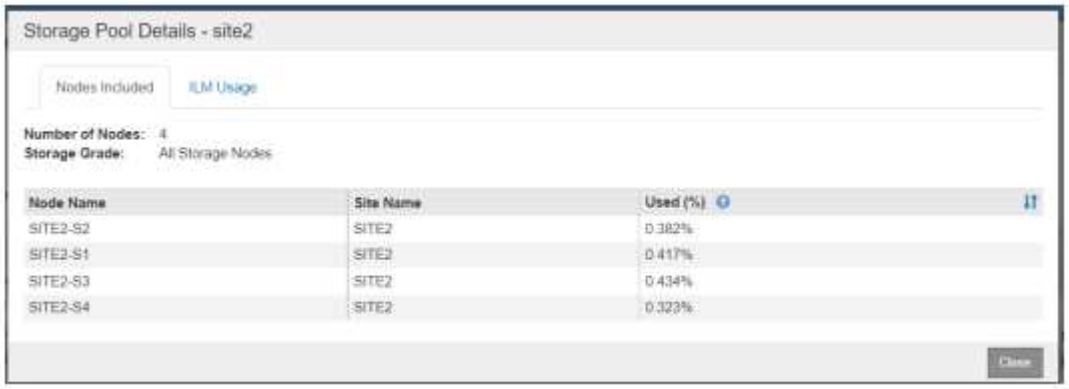


3. 此虛擬 IP （ VIP ）位址應與在 Veritas Enterprise Vault 分割區組態期間使用的 S3 主機名稱相關聯。VIP 位址可解析到站台 1 的流量、而在站台 1 故障期間、 VIP 位址會透明地將流量重新路由到站台 2 。
4. 請確定資料同時複寫到站台 1 和站台 2 。如此一來、如果 Site1 失敗、則物件資料仍可從 Site2 取得。這是透過先設定儲存資源池來完成的。

   在 StorageGRID GMI 中、按一下 ILM 、儲存資源池、然後按一下 + Create 。按照精靈的指示、建立兩個儲存資源池：一個用於站台 1 、另一個用於站台 2 。

   儲存資源池是用於定義物件放置的節點邏輯群組





5. 從 StorageGRID GMI 按一下 ILM 、規則、然後按一下 + 建立。依照精靈的指示、建立 ILM 規則、指定每個站台儲存一個複本的擷取行為為「平衡」。

6. 將 ILM 規則新增至 ILM 原則並啟動原則。

此組態會產生下列結果：

- 虛擬 S3 端點 IP 、其中站台 1 是主要端點、站台 2 則是次要端點。如果 Site1 發生故障、 VIP 會故障移轉至 Site2 。
- 當從 Veritas Enterprise Vault 傳送歸檔資料時、 StorageGRID 會確保一個複本儲存在站台 1 、另一個 DR 複本則儲存在站台 2 。如果 Site1 失敗、 Enterprise Vault 會繼續從 Site2 擷取和擷取。

> 這兩種組態對 Veritas Enterprise Vault 都是透明的。S3 端點、貯體名稱、存取金鑰等項目都相同。無需重新設定 Veritas Enterprise Vault 分割區上的 S3 連線設定。

存取 StorageGRID 評估軟體的步驟

本指示適用於與 NetApp 合作的 NetApp 銷售人員、合作夥伴和潛在客戶。

註冊帳戶

1. 使用您的企業電子郵件在上註冊帳戶 "NetApp 支援網站" 。
   a. 請確定您未使用新建立的帳戶登入。
   b. 如果您已經有帳戶，請確定您尚未登入，然後繼續下一步。
2. 建立非技術支援案例、將存取層級提升至「潛在客戶」。若要這麼做、請按一下 ""回報問題"網站頁尾中的「」連結。
3. 選擇「註冊問題」作為意見回饋類別。
4. 在「意見」區段中，寫下：「我的帳戶電子郵件地址是 _ 您的電子郵件地址 _ 。我想讓潛在客戶存取下載 StorageGRID 評估軟體。」
   a. 提及 NetApp 內部人員的姓名、該人員建議您存取潛在客戶。

下載 StorageGRID

1. 在您的支援案例經過審查與核准之後、 NetApp 支援人員將透過電子郵件通知您您帳戶已獲授予潛在客戶存取權。
2. 下載 "StorageGRID 評估軟體"。

試用版授權檔案位於 zip 檔案中。檔案解壓縮後即為 StorageGRID-Webscale 、 <version> 、 vSphere\NLF000000.txt 。

下載軟體是一種程序、需要採取貿易法規遵循措施、以符合法律要求。為了確保法規遵循、使用者必須先建立帳戶並開啟支援案例、才能取得存取權。這項程序有助於我們維持適當的控制與文件記錄、同時為潛在客戶提供他們所需的正式作業軟體。

我們提供「正式作業就緒」版本的 StorageGRID 、這不是開放原始碼或替代版本。請務必注意、 * 除非潛在客戶升級至正式作業授權、否則不提供 * 支援 * 。

如有上述步驟的任何問題、請聯絡 StorageGRID.Feedback@netapp.com 。

NetApp StorageGRID 部落格

您可以在這裡找到一些很棒的 NetApp StorageGRID 部落格：

- 2024 年 2 月 16 日： "StorageGRID 11.8 簡介：增強的安全性、簡易性和使用者體驗"
- 2024 年 2 月 16 日： "隆重介紹 StorageGRID 11.8"
- 2024 年 2 月 2 日： "發表 StorageGRID + LakeFS 解決方案簡介"
- 2023 年 12 月 12 日： "StorageGRID 上的巨量資料分析： Dremio 的執行速度比 Apache Hive 快 23 倍"
- 2023 年 11 月 7 日： "SPECtra Logic on -Prem Glacier 搭配 StorageGRID"
- 2023 年 10 月 17 日： "繼續從 Hadoop ：利用 Dremio 和 StorageGRID 將資料分析現代化"
- 2023 年 9 月 1 日： "利用 Cloud Insights 使用 Fluent 位元來監控及收集記錄"
- 2023 年 8 月 30 日： "Amazon S3 檔案系統的安裝點現在已成為 GA"
- 2023 年 5 月 16 日： "介紹 StorageGRID 11.7 和全新的 All Flash 物件儲存設備 SGF6112"
- 2023 年 5 月 16 日： "StorageGRID 物件儲存系列的新功能"
- 2023 年 3 月 30 日： "適用於 Amazon S3 Alpha 版本與 StorageGRID 的安裝點"
- 2023 年 3 月 30 日： "使用 BlueXP 以符合 3 ： 2 ： 1 的備份原則來保護 Epic EHR"
- 2023 年 3 月 14 日： "如何在符合 3 ： 2 ： 1 的架構中、使用單一命令來備份 Epic Systems EHR 資料庫"
- 2023 年 2 月 14 日： "巧克力、滑雪、手錶和大型主機有哪些共同點？"
- 2023 年 1 月 18 日： "StorageGRID S3 物件鎖定已通過驗證、適用於 Veritas NetBackup"
- 2023 年 1 月 16 日： "StorageGRID 更新 NF203 與 ISO/IEC 25051 法規遵循認證"
- 2022 年 12 月 6 日： "StorageGRID 獲得 KPMG 法規遵循認證"
- 2022 年 11 月 23 日： "運用 NetApp 和 Modzy 技術提供的 MLOps 來說明 AI"
- 2022 年 11 月 7 日： "StorageGRID 和 ONTAP S3 支援：差異、相似點和整合"
- 2022 年 10 月 5 日： "NetApp Cloud Insights 新增 StorageGRID 圖庫儀表板"
- 2022 年 10 月 5 日： "將 StorageGRID for Snowflake 上的資料除霜"
- 2022 年 9 月 26 日： "適用於服務供應商的 NetApp StorageGRID"
- 2022 年 9 月 19 日： "StorageGRID 的 DataLock 和勒索軟體保護支援"
- 2022 年 9 月 1 日： "請採用這些指標並加以圖表化"
- 2022 年 8 月 23 日： "在 StorageGRID 上建構您的資料湖"
- 2022 年 8 月 17 日： "一切都從物件鎖定開始… 為關鍵備份應用程式打造 S3 儲存生態系統"
- 2022 年 8 月 16 日： "將 StorageGRID 與開放原始碼 elk 堆疊整合、以提升客戶體驗"
- 2022 年 8 月 5 日： "NetApp StorageGRID 獲得通用標準安全認證"
- 2022 年 7 月 26 日： "查看 StorageGRID 驗證合作夥伴解決方案的不斷成長清單"
- 2022 年 6 月 9 日： "使用Cloudera Hadoop S3連接器StorageGRID 搭配使用"
- 2022 年 5 月 26 日： "StorageGRID ：儲存及管理內部部署備份與複寫資料"

- 2022 年 5 月 24 日： "利用 NetApp 和 Alluxio 將分析工作負載現代化"
- 2022 年 5 月 10 日： "隨選實驗室是 StorageGRID 的最佳銷售工具"

NetApp StorageGRID 產品文件

您可以在StorageGRID 這裡找到每個NetApp版本的完整文件：

- "StorageGRID 應用裝置"
- "StorageGRID軟體 11.5 - 12.0"

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/"

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/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511