Soluciones y recursos de StorageGRID

StorageGRID solutions and resources

NetApp
December 12, 2025

Tabla de contenidos

Soluciones y recursos de StorageGRID

Pasos para acceder al software de evaluación StorageGRID

Esta instrucción está destinada al personal de ventas, partners y clientes potenciales asociados con NetApp de NetApp.

Regístrese para obtener una cuenta

1. Regístrese para obtener una cuenta en "Sitio de soporte de NetApp" utilizando su correo electrónico de empresa.
   a. Asegúrese de que no ha iniciado sesión con la cuenta recién creada.
   b. Si ya tiene una cuenta, asegúrese de que no ha iniciado sesión y continúe con el siguiente paso.
2. Crear un caso de soporte no técnico para elevar los niveles de acceso a «cliente potencial». Para ello, haga clic en el ""Notifique un problema"enlace " en el pie de página de la página web.
3. Seleccione «Problema de registro» como categoría de comentarios.
4. En la sección de comentarios, escriba: "Mi dirección de correo electrónico de la cuenta es *Su-Correo-Dirección*. Me gustaría obtener acceso a un posible cliente para descargar el software de evaluación de StorageGRID».
   a. Mencione el nombre de la persona interna de NetApp que sugirió la solicitud de acceso de un posible cliente.

Descargue StorageGRID

1. Una vez revisado y aprobado su caso de soporte, el soporte de NetApp le notificará a través de correo electrónico que se le ha otorgado acceso a su cuenta.
2. Descargue el "Software de evaluación StorageGRID".

El archivo de licencia Eval está ubicado dentro del archivo zip. Se trata de StorageGRID-Webscale-<version>\vsphere\NLF000000.txt una vez descomprimido.

La descarga del software es un proceso que implica medidas de cumplimiento comercial para cumplir con los requisitos legales. Para garantizar el cumplimiento, los usuarios deben crear una cuenta y abrir un caso de soporte antes de obtener acceso. Este proceso nos ayuda a mantener el control y la documentación adecuados, al tiempo que proporciona a los clientes potenciales el software listo para la producción que necesitan.

Proporcionamos una versión de StorageGRID «lista para la producción», que no es una versión de código abierto ni alternativa. Es importante tener en cuenta que no se proporciona **soporte** a menos que el cliente potencial actualice a una licencia de producción.

Póngase en contacto con StorageGRID.Feedback@netapp.com para cualquier problema con los pasos anteriores.

Soluciones de terceros validadas

Soluciones de terceros validadas: Información general

NetApp, en colaboración con nuestros partners, ha validado estas soluciones para su uso con StorageGRID. Revise la información de esta sección para saber qué soluciones se han validado y para obtener instrucciones adicionales, si procede.

Una sus fuerzas a NetApp para acelerar la innovación en la cartera de productos, ampliar el reconocimiento de la Marca y aumentar las ventas al crear las mejores soluciones probadas de NetApp. "Conviértase en un partner de la alianza".

Soluciones de terceros validadas StorageGRID 12.0

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 12.0. + Si la solución que busca no aparece en la lista, comuníquese con su representante de cuenta de NetApp .

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Apache Kafka
- Punto de montaje de AWS
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- Collibra (Calidad de datos mínima de Collibra versión 2024,02)
- CommVault 11
- Análisis empresarial de Couchbase 2.0
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Datos de Diskover
- Dremio
- Snapshot de Elasticsearch (incluido el nivel congelado)
- Imán
- Archivo de objetos de Fujifilm

- Servidor empresarial de GitHub
- IBM Filenet
- IBM Storage Protect
- Interica
- Komprise
- Clústeres de Big Data de Microsoft SQL Server
- Modelo 9
- Modzy
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenera
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Reveille v10, versión 220706 o superior
- Rubrik CDM
- s3a
- Signiant
- Copo de nieve
- Spectra Logic en el glaciar local
- Smartstore de Splunk
- Estallido
- Almacenamiento simplificado
- Trino
- Empresa de barniz 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior
- Vertica 10.x
- Vidispine

- Tejido de almacenamiento de Virtalica
- Weka v3.10 o posterior

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- CommVault 11 Feature Release 26
- IBM Filenet
- IBM Storage Protect
- OpenText Documentum 21.4
- RUBRIK
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Gestores de claves compatibles con StorageGRID

Estas soluciones han sido probadas.

- Plataforma de seguridad criptográfica Entrust v10.4.5
- Entrust KeyControl 10,2
- Bóveda de Hashicorp 1.20.2
- Administrador de confianza de cifrado de Thales 2.20

Soluciones de terceros validadas con StorageGRID 11,9

Las siguientes soluciones de terceros se han validado para el uso con StorageGRID 11,9. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Apache Kafka
- Punto de montaje de AWS
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- Collibra (Calidad de datos mínima de Collibra versión 2024,02)
- CommVault 11
- Análisis empresarial de Couchbase 2.0
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Datos de Diskover
- Dremio
- Snapshot de Elasticsearch (incluido el nivel congelado)
- Imán
- Archivo de objetos de Fujifilm
- Servidor empresarial de GitHub
- IBM Filenet
- IBM Storage Protect
- Interica
- Komprise

- Clústeres de Big Data de Microsoft SQL Server
- Modelo 9
- Modzy
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenera
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Reveille v10, versión 220706 o superior
- Rubrik CDM
- s3a
- Signiant
- Copo de nieve
- Spectra Logic en el glaciar local
- Smartstore de Splunk
- Estallido
- Almacenamiento simplificado
- Trino
- Empresa de barniz 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior
- Vertica 10.x
- Vidispine
- Tejido de almacenamiento de Virtalica
- Weka v3.10 o posterior

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- CommVault 11 Feature Release 26
- IBM Filenet
- IBM Storage Protect
- OpenText Documentum 21.4
- RUBRIK
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Gestores de claves compatibles con StorageGRID

Estas soluciones han sido probadas.

- Plataforma de seguridad criptográfica Entrust 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
- Administrador de confianza de cifrado de Thales 2.15
- Administrador de confianza de cifrado de Thales 2.16
- Administrador de confianza de cifrado de Thales 2.20

Soluciones de terceros validadas con StorageGRID 11,8

Las siguientes soluciones de terceros se han validado para el uso con StorageGRID 11,8.
Si la solución que busca no aparece en la lista, póngase en contacto con su representante de cuentas de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Apache Kafka
- Punto de montaje de AWS
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- Collibra (Calidad de datos mínima de Collibra versión 2024,02)
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Datos de Diskover

- Dremio
- Snapshot de Elasticsearch (incluido el nivel congelado)
- Imán
- Archivo de objetos de Fujifilm
- Servidor empresarial de GitHub
- IBM Filenet
- IBM Storage Protect
- Interica
- Komprise
- Clústeres de Big Data de Microsoft SQL Server
- Modelo 9
- Modzy
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenera
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Reveille v10, versión 220706 o superior
- Rubrik CDM
- s3a
- Signiant
- Copo de nieve
- Spectra Logic en el glaciar local
- Smartstore de Splunk
- Estallido
- Almacenamiento simplificado
- Trino
- Empresa de barniz 6.0.4
- Veeam 12

- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior
- Vertica 10.x
- Vidispine
- Tejido de almacenamiento de Virtalica
- Weka v3.10 o posterior

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- CommVault 11 Feature Release 26
- IBM Filenet
- IBM Storage Protect
- OpenText Documentum 21.4
- RUBRIK
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 y posterior

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar

- Velasea

Gestores de claves compatibles con StorageGRID

Estas soluciones han sido probadas.

- 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

Soluciones de terceros validadas con StorageGRID 11,7

Las siguientes soluciones de terceros se han validado para el uso con StorageGRID 11,7. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Apache Kafka
- Punto de montaje de AWS
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- Collibra (Calidad de datos mínima de Collibra versión 2024,02)
- CommVault 11
- CTERA Portal 6
- Dalet

- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Datos de Diskover
- Dremio
- Snapshot de Elasticsearch (incluido el nivel congelado)
- Imán
- Archivo de objetos de Fujifilm
- Servidor empresarial de GitHub
- IBM Filenet
- IBM Spectrum Protect Plus
- IBM Storage Protect
- Interica
- Komprise
- Clústeres de Big Data de Microsoft SQL Server
- Modelo 9
- Modzy
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenera
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Reveille v10, versión 220706 o superior
- Rubrik CDM
- s3a
- Signiant
- Copo de nieve
- Spectra Logic en el glaciar local
- Smartstore de Splunk

- Almacenamiento simplificado
- Trino
- Empresa de barniz 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1 y posterior
- Vertica 10.x
- Vidispine
- Tejido de almacenamiento de Virtalica
- Weka v3.10 o posterior

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- CommVault 11 Feature Release 26
- IBM Filenet
- IBM Storage Protect
- OpenText Documentum 21.4
- RUBRIK
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 y posterior

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI

- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Gestores de claves compatibles con StorageGRID

Estas soluciones han sido probadas.

- 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

Soluciones de terceros validadas de StorageGRID 11.6

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 11.6. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Apache Kafka
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Datos de Diskover
- Dremio

- Imán
- Archivo de objetos de Fujifilm
- Servidor empresarial de GitHub
- IBM Filenet
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Clústeres de Big Data de Microsoft SQL Server
- Modelo 9
- Modzy
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- PixitMedia ngenera
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Reveille v10, versión 220706 o superior
- Rubrik CDM
- s3a
- Signiant
- Copo de nieve
- Spectra Logic en el glaciar local
- Smartstore de Splunk
- Almacenamiento simplificado
- Trino
- Empresa de barniz 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x

- Vidispine
- Tejido de almacenamiento de Virtalica
- Weka v3.10 o posterior

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- CommVault 11 Feature Release 26
- IBM Filenet
- OpenText Documentum 21.4
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 y posterior

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluciones de terceros validadas de StorageGRID 11.5

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 11.5. + Si la solución que busca no está en esta lista, póngase en contacto con su

representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Alluxio
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Interica
- Komprise
- Moonwalk Universal
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Rubrik CDM
- s3a
- Signiant
- Smartstore de Splunk
- Trino
- Empresa de barniz 6.0.4
- Veeam 11
- Veritas Enterprise Vault 11

- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine
- Tejido de almacenamiento de Virtalica

Soluciones de terceros validadas en StorageGRID con bloqueo de objetos

Estas soluciones se han probado en colaboración con los partners correspondientes.

- OpenText Documentum 21.4
- Veeam 11

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Gitlab
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluciones de terceros validadas de StorageGRID 11.4

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 11.4. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Interica
- Komprise
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- Archivo informativo de OpenText 16 EP7
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Rubrik CDM
- Signiant
- Smartstore de Splunk
- Empresa de barniz 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluciones de terceros validadas de StorageGRID 11.3

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 11.3. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX

- DefendX
- Interica
- Komprise
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Smartstore de Splunk
- Empresa de barniz 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH

- SilverTrak
- SoftNAS
- QStar
- Velasea

Soluciones de terceros validadas de StorageGRID 11.2

Las siguientes soluciones de terceros han sido validadas para su uso con StorageGRID 11.2. + Si la solución que busca no está en esta lista, póngase en contacto con su representante de cuenta de NetApp.

Soluciones de terceros validadas en StorageGRID

Estas soluciones se han probado en colaboración con los partners correspondientes.

- Con razón
- Bridgestor
- Cantemo
- Colaboración de contenidos Citrix
- CommVault 11
- CTERA Portal 6
- Dalet
- Datadobi
- Dinámicas de datos StorageX
- DefendX
- Interica
- Komprise
- MUY BIEN
- Nasuní
- OpenText Documentum 16.4
- OpenText Media Management 16.5 con CyanGate Cloud
- Panzura
- Puerta de enlace de archivado de punto 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext cuántico 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- Smartstore de Splunk
- Empresa de barniz 6.0.4

- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Soluciones de terceros compatibles con StorageGRID

Estas soluciones han sido probadas.

- Software de archivado
- Comunicaciones de Axis
- Congruity360
- Marcos de datos
- Plataforma EcoDigital DIVA
- Encoding.com
- Archivo de objetos de Fujifilm
- GE Centricity Enterprise Archive
- Hyland Acuo
- IBM Aspera
- Sistemas Milestone
- ONSSI
- Motor REACH
- SilverTrak
- SoftNAS
- QStar
- Velasea

Guías de características de productos

Logre un objetivo de punto de recuperación de cero con StorageGRID: Una guía completa para la replicación multisitio

Este informe técnico proporciona una guía completa para implementar estrategias de replicación de StorageGRID para lograr un Objetivo de Punto de Recuperación (RPO) de cero en caso de una falla del sitio. El documento detalla varias opciones de implementación para StorageGRID, incluyendo la replicación síncrona multisitio y la replicación asíncrona multigrid. Explica cómo se pueden configurar las políticas de gestión del ciclo de vida de la información (ILM) de StorageGRID para garantizar la durabilidad y disponibilidad de los datos en múltiples ubicaciones. Además, el informe abarca consideraciones de rendimiento, escenarios de fallos y procesos de recuperación para mantener las operaciones de los clientes sin interrupciones. El objetivo de este documento es proporcionar información para garantizar que los datos permanezcan accesibles y coherentes, incluso en caso de un fallo total del sitio, mediante el uso de técnicas de replicación tanto síncronas como asíncronas.

Información general de StorageGRID

NetApp StorageGRID es un sistema de almacenamiento basado en objetos compatible con la API estándar del sector Amazon Simple Storage Service (Amazon S3).

StorageGRID proporciona un espacio de nombres único en varias ubicaciones, con niveles variables de servicio basados en políticas de gestión del ciclo de vida de la información (ILM). Con estas políticas de ciclo de vida puede optimizar dónde residen sus datos a lo largo de su ciclo de vida.

StorageGRID permite la durabilidad y disponibilidad configurables de sus datos en soluciones locales y distribuidas geográficamente. Ya sea que sus datos estén en las instalaciones o en una nube pública, los flujos de trabajo de nube híbrida integrados permiten que su empresa aproveche servicios de nube como Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch y más.

StorageGRID Scale

Una implementación mínima de StorageGRID consta de un nodo de administración y 3 nodos de almacenamiento en un único sitio. Una sola cuadrícula puede crecer hasta 220 nodos. StorageGRID se puede implementar como un solo sitio o extenderse a 16 sitios.

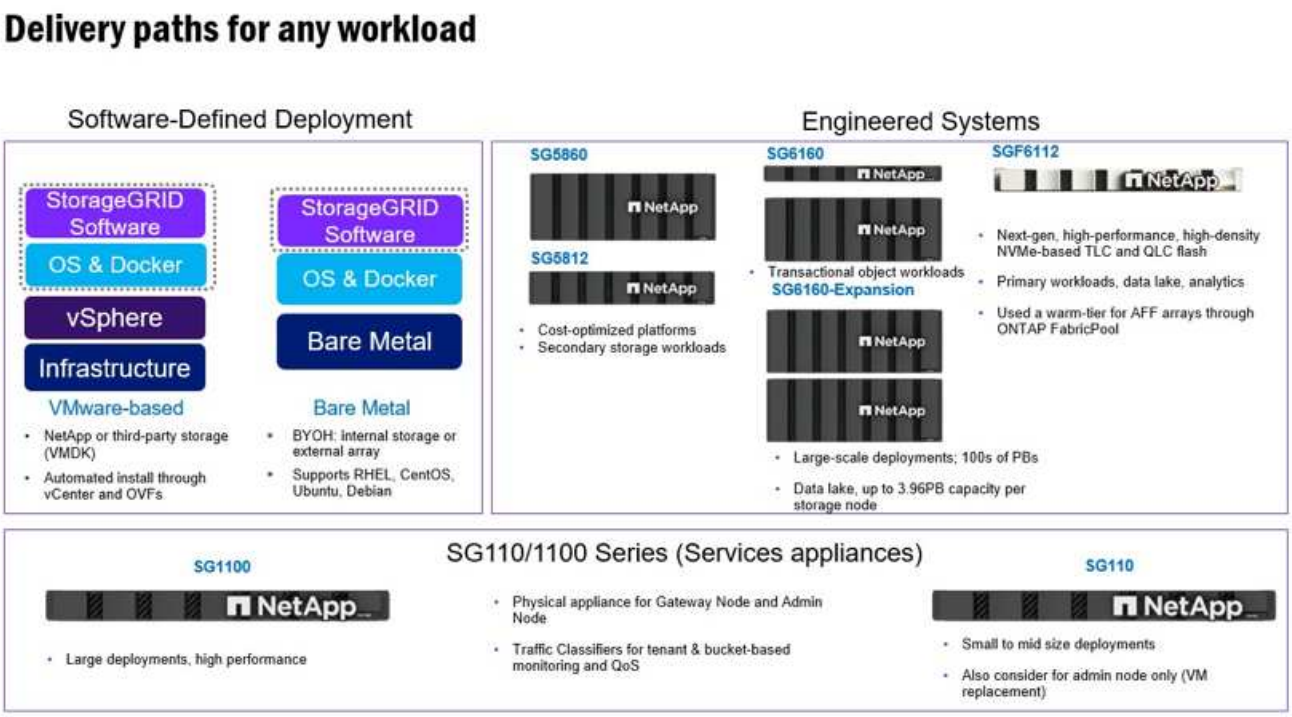
El nodo de administración contiene la interfaz de gestión, un punto central para las métricas y el registro, y mantiene la configuración de los componentes de StorageGRID . El nodo de administración también contiene un balanceador de carga integrado para el acceso a la API S3.

StorageGRID se puede implementar solo como software, como dispositivos de máquinas virtuales VMware o como dispositivos diseñados específicamente para ese fin.

Un nodo de almacenamiento se puede implementar como:

- Un nodo de solo metadatos que maximiza el recuento de objetos
- Un nodo de almacenamiento de objetos únicamente que maximiza el espacio de los objetos
- Un nodo combinado de almacenamiento de objetos y metadatos que agrega tanto el recuento de objetos como el espacio de objetos

Cada nodo de almacenamiento puede escalar a una capacidad de varios petabytes para el almacenamiento de objetos, lo que permite un único espacio de nombres en cientos de petabytes. StorageGRID también proporciona un equilibrador de carga integrado para las operaciones de API S3 llamado nodo de puerta de enlace.



StorageGRID consta de una colección de nodos ubicados en una topología de sitio. Un sitio en StorageGRID puede ser una ubicación física única o residir en una ubicación física compartida como otros sitios en la red como una construcción lógica. Un sitio StorageGRID no debe abarcar varias ubicaciones físicas. Un sitio representa una infraestructura de red de área local (LAN) compartida y un dominio de falla.

StorageGRID y dominios de fallos

StorageGRID contiene varias capas de dominios de fallo a tener en cuenta para decidir cómo diseñar su solución, cómo almacenar sus datos y dónde deben almacenarse para mitigar los riesgos de fallos.

- Nivel de cuadrícula: Una cuadrícula formada por varios sitios puede tener fallos de sitio o aislamiento y los sitios accesibles pueden seguir funcionando como la cuadrícula.
- Nivel de sitio: Los fallos dentro de un sitio pueden afectar a las operaciones de ese sitio, pero no afectarán al resto del grid.
- Nivel de nodo: Un fallo de nodo no afectará al funcionamiento del sitio.
- Nivel de disco: Un error de disco no afectará al funcionamiento del nodo.

Datos y metadatos de objeto

Con el almacenamiento de objetos, la unidad de almacenamiento es un objeto, en lugar de un archivo o un bloque. A diferencia de la jerarquía de árbol de un sistema de archivos o almacenamiento basado en bloques, el almacenamiento de objetos organiza los datos en un diseño plano y sin estructura. El almacenamiento de objetos separa la ubicación física de los datos del método utilizado para almacenar y recuperar esos datos.

Cada objeto de un sistema de almacenamiento basado en objetos tiene dos partes: Datos de objetos y metadatos de objetos.

- Los datos de objeto representan los datos subyacentes reales, por ejemplo, una fotografía, una película o un historial médico.
- Los metadatos de objetos son cualquier información que describa un objeto.

StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

Los metadatos de objetos incluyen información como la siguiente:

- Metadatos del sistema, incluido un ID único para cada objeto, el nombre del objeto, el nombre del bucket S3, el nombre o ID de la cuenta del inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- La ubicación de almacenamiento actual de la copia replicada o el fragmento codificado para borrado de cada objeto.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- En el caso de los objetos S3, todas las parejas clave-valor de etiqueta de objeto asociadas con el objeto
- Para objetos segmentados y objetos multipartes, identificadores de segmento y tamaños de datos.

Los metadatos de objetos son personalizables y ampliables, por lo que es flexible para las aplicaciones. Para obtener información detallada sobre cómo y dónde StorageGRID almacena los metadatos de objetos, vaya a "Gestione el almacenamiento de metadatos de objetos".

El sistema de gestión de la vida útil de la información (ILM) de StorageGRID se usa para orquestar la ubicación, la duración y el comportamiento de ingesta de todos los datos de objetos del sistema StorageGRID. Las reglas de ILM determinan la forma en que StorageGRID almacena objetos a lo largo del tiempo mediante réplicas de los objetos o el código de borrado del objeto en nodos y sitios. Este sistema ILM es responsable de la consistencia de los datos de objetos dentro de una cuadrícula.

Codificación de borrado

StorageGRID proporciona la capacidad de borrar datos de código a nivel de nodo y de unidad. Con los dispositivos StorageGRID , borramos con código los datos almacenados en cada nodo en todas las unidades dentro del nodo, brindando protección local contra múltiples fallas de disco que provoquen pérdida o interrupciones de datos. Las reconstrucciones a partir de fallas de unidad son locales en el nodo y no requieren que los datos se repliquen en la red.

Además, los dispositivos StorageGRID utilizan esquemas de codificación de borrado para almacenar datos de objetos en todos los nodos dentro de un sitio o distribuidos en 3 o más sitios en el sistema StorageGRID a través de las reglas ILM de StorageGRID que protegen contra fallas de nodos.

La codificación de borrado proporciona un diseño de almacenamiento resistente a fallos de nodos y sitios con una sobrecarga menor que la replicación. Todos los esquemas de codificación de borrado de StorageGRID se pueden implementar en un solo sitio siempre que se cumpla el número mínimo de nodos necesarios para

almacenar los fragmentos de datos. Esto significa que para un esquema EC de 4+2 se necesita un mínimo de 6 nodos disponibles para recibir los datos.

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%

Consistencia de metadatos

En StorageGRID, los metadatos suelen almacenarse con tres réplicas por sitio para asegurar la consistencia y la disponibilidad. Esta redundancia ayuda a mantener la integridad de los datos y la accesibilidad incluso en caso de fallo.

La consistencia predeterminada se define en un nivel de cuadrícula. Los usuarios pueden cambiar la consistencia en el nivel del depósito en cualquier momento.

Las opciones de coherencia de bloques disponibles en StorageGRID son:

- **Todo**: Proporciona el más alto nivel de consistencia. Todos los nodos del grid reciben los datos inmediatamente o la solicitud fallará.
- **Global fuerte**:
  - **Legacy Strong Global**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes en todos los sitios.
    - Este es el comportamiento predeterminado para todos los sistemas actualizados de la versión 11.9 o anterior a la versión 12.0 sin cambiar manualmente al nuevo Quorum Strong Global.
  - **Quorum Strong-global**: garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios. Ofrece consistencia para múltiples nodos o incluso en caso de falla del sitio si se puede lograr el quórum de réplica de metadatos.
    - Este es el comportamiento predeterminado para todos los sistemas recién instalados en la versión 12.0 o superior.
    - La consistencia de QUORUM se define como un quórum de réplicas de metadatos del nodo de almacenamiento, donde cada sitio tiene 3 réplicas de metadatos. Se puede calcular de la siguiente

manera: 1+((N*3)/2) donde N es el número total de sitios.

    - Por ejemplo, se debe realizar un mínimo de 5 réplicas a partir de una cuadrícula de 3 sitios con un máximo de 3 réplicas dentro de un sitio.

- **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio.
- **Read-after-new-write**(default): Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Coherencia de datos de objetos

Aunque los metadatos se replican automáticamente en y entre sitios, las decisiones sobre ubicación de almacenamiento de datos de objetos dependen de usted. Los datos de objetos se pueden almacenar en réplicas dentro de y entre sitios, códigos de borrado dentro o entre sitios o una combinación o réplicas y esquemas de almacenamiento codificados de borrado. Las reglas de ILM se pueden aplicar a todos los objetos o se pueden filtrar para que solo se apliquen a ciertos objetos, bloques o inquilinos. Las reglas de ILM definen cómo se almacenan los objetos, las réplicas o el código de borrado, el tiempo que los objetos se almacenan en esas ubicaciones, si el número de réplicas o el esquema de código de borrado debería cambiar o las ubicaciones deberían cambiar con el tiempo.

Cada regla de ILM se configurará con uno de estos tres comportamientos de procesamiento para proteger los objetos: Doble registro, equilibrada o estricta.

La opción de confirmación dual realizará inmediatamente dos copias en dos nodos de almacenamiento diferentes cualesquiera de la cuadrícula y devolverá al cliente la solicitud como exitosa. La selección del nodo se intentará dentro del sitio de la solicitud, pero en algunas circunstancias puede utilizar nodos de otro sitio. El objeto se añade a la cola ILM para ser evaluado y colocado de acuerdo con las reglas ILM.

La opción balanceada evalúa el objeto de acuerdo con la política ILM inmediatamente y coloca el objeto de forma síncrona antes de devolver la solicitud al cliente para que se haya realizado correctamente. Si la regla ILM no puede cumplirse de inmediato debido a una interrupción del servicio o a una capacidad de almacenamiento insuficiente para cumplir con los requisitos de ubicación, entonces se utilizará la confirmación dual. Una vez resuelto el problema, ILM colocará automáticamente el objeto según la regla definida.

La opción estricta evalúa el objeto de acuerdo con la política ILM inmediatamente y coloca el objeto de forma síncrona antes de devolver la solicitud al cliente para que se haya realizado correctamente. Si la regla ILM no se puede cumplir de inmediato debido a una interrupción del servicio o a un almacenamiento insuficiente para cumplir con los requisitos de ubicación, la solicitud fallará y el cliente deberá volver a intentarlo.

Balanceo de carga

StorageGRID se puede poner en marcha con acceso de cliente a través de los nodos de puerta de enlace integrada, un equilibrador de carga de 3rd partes externo, una operación por turnos de DNS o directamente en un nodo de almacenamiento. Pueden ponerse en marcha varios nodos de puerta de enlace en un sitio y configurarse en grupos de alta disponibilidad proporcionando conmutación por error automatizada y recuperación tras fallos en caso de interrupción del nodo de puerta de enlace. Puede combinar métodos de equilibrio de carga en una solución para proporcionar un único punto de acceso a todos los sitios de una solución.

Los nodos de puerta de enlace equilibrarán la carga entre los nodos de almacenamiento en el sitio donde reside el nodo de puerta de enlace de forma predeterminada. StorageGRID se puede configurar para permitir que los nodos de puerta de enlace equilibren la carga utilizando nodos de múltiples sitios. Esta configuración añadiría la latencia entre esos sitios a la latencia de respuesta a las solicitudes del cliente. Esto solo debe configurarse si la latencia total es aceptable para los clientes.

Se puede lograr un RTO de cero mediante una combinación de equilibrio de carga local y global. Para garantizar un acceso ininterrumpido a los clientes, es necesario equilibrar la carga de las solicitudes de los clientes. Una solución StorageGRID puede contener muchos nodos de puerta de enlace y grupos de alta disponibilidad en cada sitio. Para proporcionar acceso ininterrumpido a los clientes en cualquier sitio, incluso en caso de fallo del sitio, debe configurar una solución de equilibrio de carga externa en combinación con los nodos de StorageGRID Gateway. Configure grupos de alta disponibilidad de nodos de puerta de enlace que gestionen la carga dentro de cada sitio y utilice el balanceador de carga externo para equilibrar la carga entre los grupos de alta disponibilidad. El balanceador de carga externo debe configurarse para realizar una comprobación de estado que garantice que las solicitudes se envíen únicamente a los sitios operativos. Para obtener más información sobre el equilibrio de carga con StorageGRID, consulte la "Informe técnico del equilibrador de carga de StorageGRID".

Requisitos para RPO cero con StorageGRID

Para lograr un objetivo de punto de recuperación (RPO) cero en un sistema de almacenamiento de objetos, es crucial que en el momento del fallo:

- Tanto los metadatos como el contenido de los objetos se sincronizan y se consideran consistentes
- Se seguirá accediendo al contenido del objeto a pesar de producirse un error.

Para una implementación de múltiples sitios, Quorum Strong Global es el modelo de consistencia preferido para garantizar que los metadatos estén sincronizados en todos los sitios, lo que lo hace esencial para cumplir con el requisito de RPO cero.

Los objetos del sistema de almacenamiento se almacenan según las reglas de Gestión del Ciclo de Vida de la Información (ILM), que dictan cómo y dónde se almacenan los datos a lo largo de su ciclo de vida. Para la replicación síncrona, se puede considerar entre la ejecución estricta o la ejecución balanceada.

- Es necesaria una estricta ejecución de estas reglas de ILM para un objetivo de punto de recuperación cero porque garantiza que los objetos se coloquen en las ubicaciones definidas sin ningún retraso ni retroceso, de modo que se mantenga la disponibilidad y la coherencia de los datos.
- El comportamiento de procesamiento de ILM Balance de StorageGRID proporciona un equilibrio entre alta disponibilidad y resiliencia, lo que permite que los usuarios sigan procesando datos incluso en caso de un fallo del sitio.

Puestas en marcha síncronas en varios sitios

Soluciones multisitio: StorageGRID le permite replicar objetos en múltiples sitios dentro de la red de forma sincrónica. Al configurar reglas de Gestión del ciclo de vida de la información (ILM) con equilibrio o comportamiento estricto, los objetos se colocan inmediatamente en las ubicaciones especificadas. Configurar el nivel de consistencia del bucket en Quorum Strong Global también garantizará la replicación sincrónica de metadatos. StorageGRID utiliza un único espacio de nombres global que almacena las ubicaciones de los objetos como metadatos, de modo que cada nodo sabe dónde se encuentran todas las copias o piezas codificadas de borrado. Si no se puede recuperar un objeto del sitio donde se realizó la solicitud, se recuperará automáticamente de un sitio remoto sin necesidad de procedimientos de conmutación por error.

Una vez resuelto el fallo, no es necesario realizar ningún esfuerzo manual de conmutación por recuperación. El rendimiento de la replicación depende del sitio con el rendimiento de red más bajo, la máxima latencia y el

menor rendimiento. El rendimiento de un sitio se basa en el número de nodos, la velocidad y el número de núcleos de CPU, la memoria, la cantidad de unidades y los tipos de unidades.

Soluciones multigrid: StorageGRID puede replicar inquilinos, usuarios y buckets entre múltiples sistemas StorageGRID usando la replicación entre redes cruzadas (CGR). CGR puede ampliar los datos seleccionados a más de 16 sitios, aumentar la capacidad utilizable del almacén de objetos y proporcionar recuperación ante desastres. La replicación de buckets con CGR incluye objetos, versiones de objetos y metadatos, y puede ser bidireccional o unidireccional. El objetivo de punto de recuperación (RPO) depende del rendimiento de cada sistema StorageGRID y de las conexiones de red entre ellos.

Resumen:

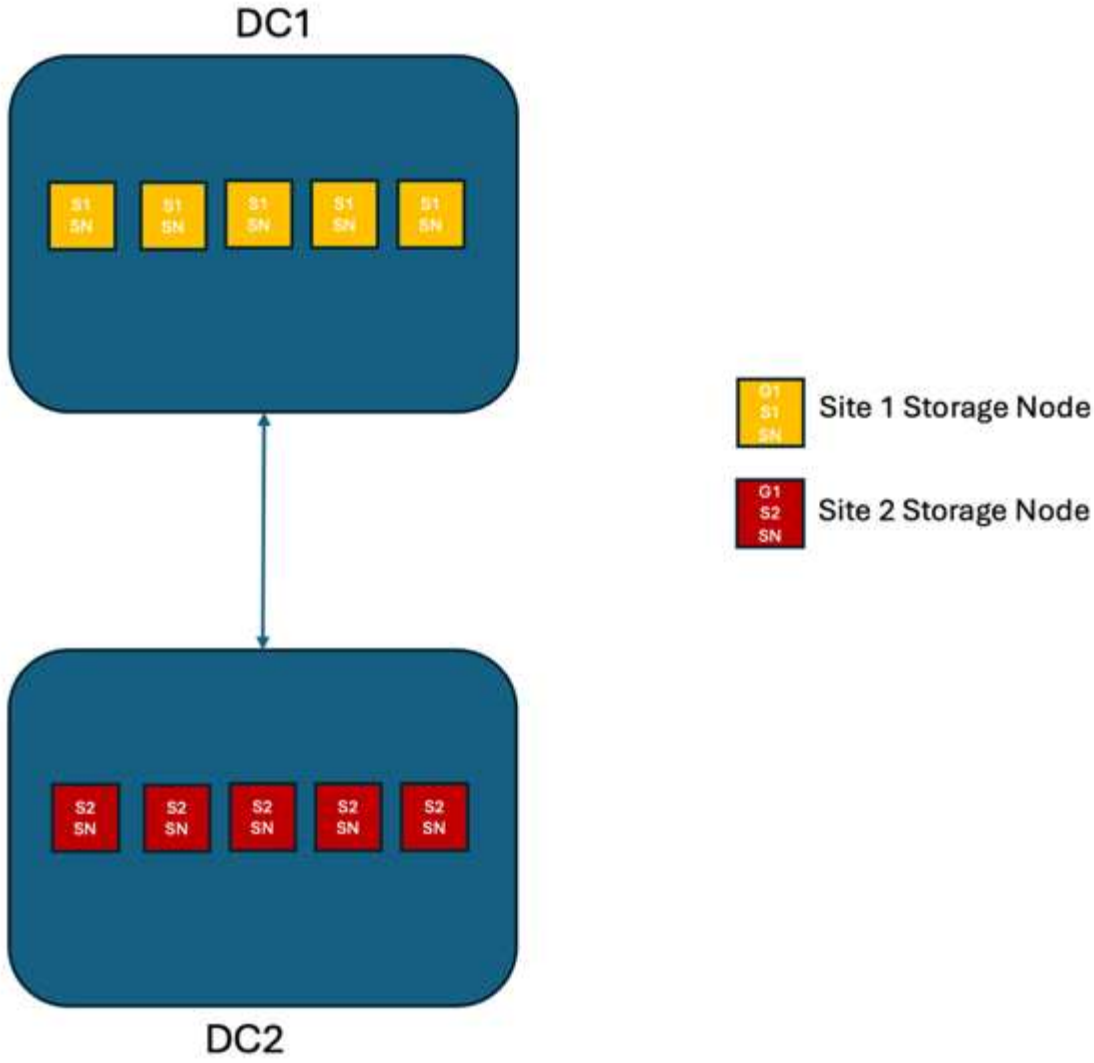
- La replicación dentro del grid incluye replicación síncrona y asíncrona, configurable mediante el comportamiento de ingesta de ILM y el control de coherencia de metadatos.
- La replicación entre grid es solo asíncrona.

Una implementación de varios sitios de Grid único

En los siguientes escenarios, las soluciones StorageGRID están configuradas con un balanceador de carga externo opcional que gestiona las solicitudes a los grupos de alta disponibilidad del balanceador de carga integrado. Esto permitirá alcanzar un RTO de cero, además de un RPO de cero. ILM está configurado con protección de ingesta balanceada para la colocación síncrona. Cada bucket está configurado con la versión Quorum del modelo de consistencia global fuerte para cuadrículas de 3 o más sitios y la versión Legacy de consistencia global fuerte para 2 sitios.

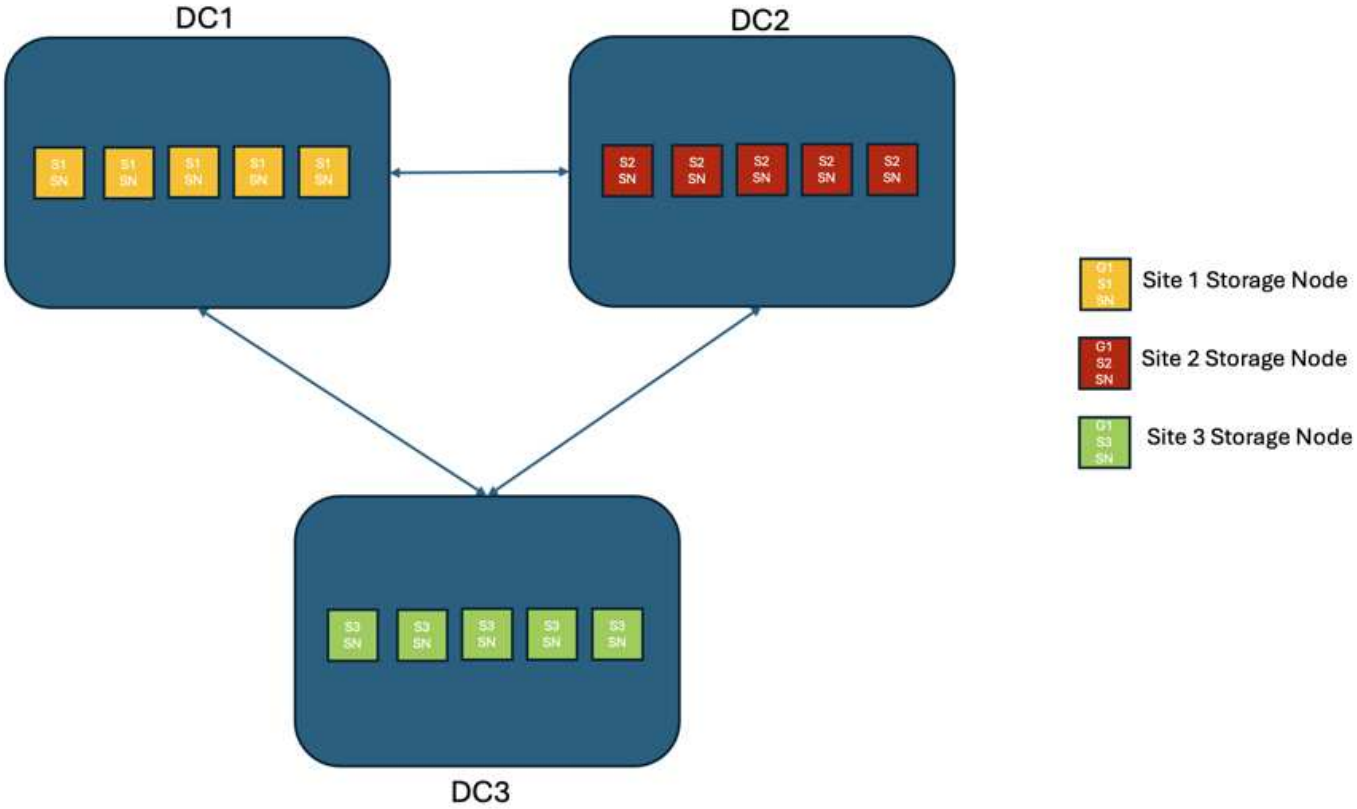
Escenario 1:

En una solución StorageGRID de dos sitios, existen al menos dos réplicas de cada objeto y 6 réplicas de todos los metadatos. Tras la recuperación tras el fallo, las actualizaciones posteriores a la interrupción se sincronizarán automáticamente con el sitio/nodos recuperados. Con solo 2 sitios, es poco probable que se logre un RPO cero en escenarios de falla más allá de la pérdida total de un sitio.



Escenario 2:

En una solución StorageGRID de tres o más sitios, hay al menos 3 réplicas o 3 fragmentos EC de cada objeto y 9 réplicas de todos los metadatos. Tras la recuperación tras el fallo, las actualizaciones posteriores a la interrupción se sincronizarán automáticamente con el sitio/nodos recuperados. Con tres o más sitios es posible lograr un RPO cero.



Escenarios de fallo en varios sitios

Fallo	Resultado en 2 sitios + Legado Fuerte Global	Resultado de 3 o más sitios + Quorum Strong Global
Fallo de unidad de nodo único	Cada dispositivo utiliza varios grupos de discos y puede mantener al menos 1 unidades por grupo sin interrupciones ni pérdida de datos.	Cada dispositivo utiliza varios grupos de discos y puede mantener al menos 1 unidades por grupo sin interrupciones ni pérdida de datos.
Fallo de un nodo en un sitio	Sin interrupción de las operaciones ni pérdida de datos.	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de varios nodos en un sitio	Interrupción de las operaciones del cliente dirigidas a este sitio, pero sin pérdida de datos. Las operaciones dirigidas al otro sitio permanecen sin interrupciones y sin pérdida de datos.	Las operaciones se dirigen a todos los demás sitios y permanecen sin interrupciones y sin pérdida de datos.

Fallo	Resultado en 2 sitios + Legado Fuerte Global	Resultado de 3 o más sitios + Quorum Strong Global
Fallo de un único nodo en múltiples sitios	Sin interrupción ni pérdida de datos si: • Existe al menos una copia replicada en la cuadrícula • Existen suficientes fragmentos de EC en la cuadrícula Las operaciones interrumpidas y el riesgo de pérdida de datos si: • No existen copias duplicadas • Existen suficientes portabrocas EC	Sin interrupción ni pérdida de datos si: • Existe al menos una copia replicada en la red. • Existen suficientes fragmentos de EC en la cuadrícula Las operaciones interrumpidas y el riesgo de pérdida de datos si: • No existen copias duplicadas • Existen suficientes portabrocas EC para recuperar el objeto
Fallo de un sitio único	Algunas operaciones del cliente se verán interrumpidas hasta que se resuelva el fallo. Las operaciones GET y HEAD continuarán sin interrupción. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo.	Sin interrupción de las operaciones ni pérdida de datos.
Fallos de un único sitio más nodo único	Algunas operaciones del cliente se verán interrumpidas hasta que se resuelva el fallo. Las operaciones de HEAD continuarán sin interrupción. Las operaciones GET continuarán sin interrupción si existe una copia replicada o suficientes fragmentos EC. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo.	Sin interrupción de las operaciones ni pérdida de datos. Posible pérdida de datos dependiendo del número de copias replicadas. La codificación de borrado local puede prevenir la pérdida de datos.

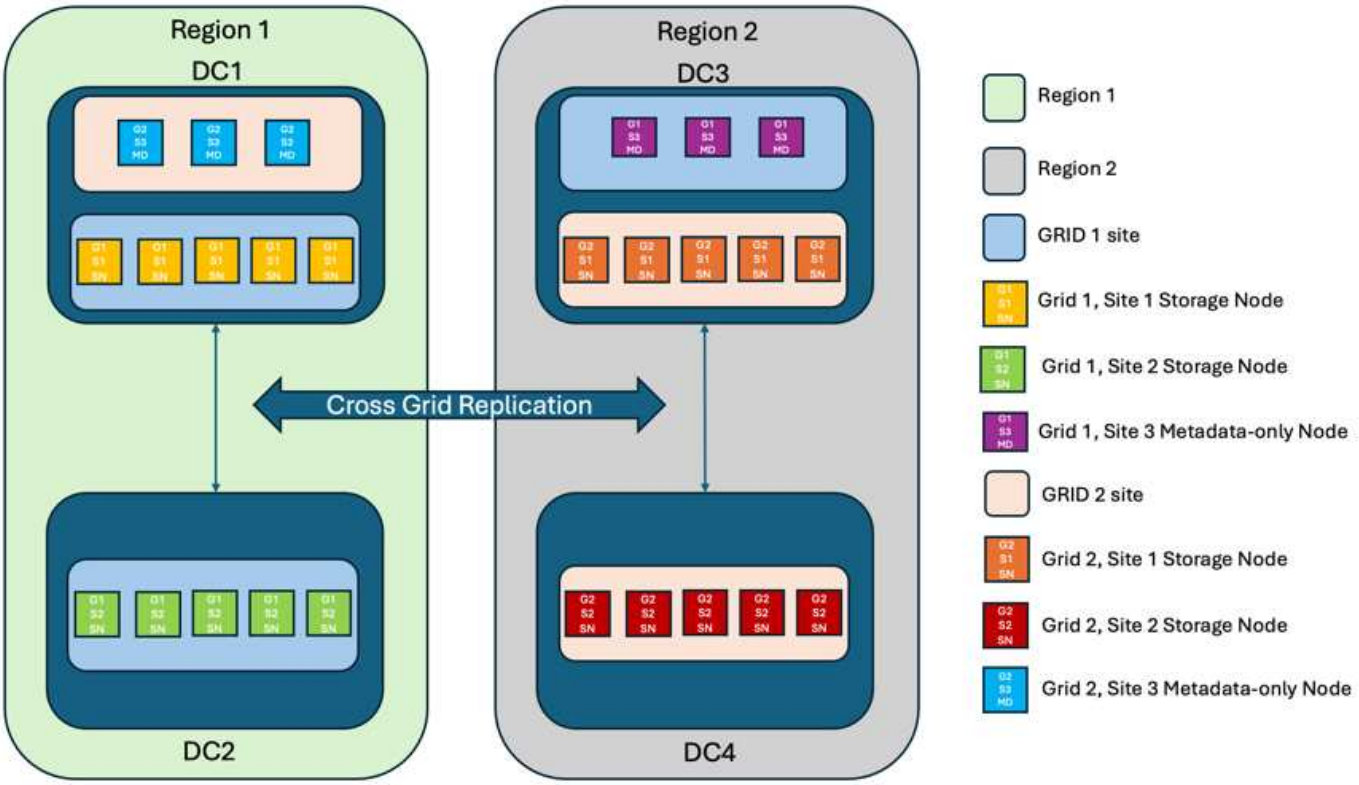
Fallo	Resultado en 2 sitios + Legado Fuerte Global	Resultado de 3 o más sitios + Quorum Strong Global
Sitio único y nodo de cada sitio restante	Solo existen dos sitios. Ver: Sitio único más un nodo único.	Las operaciones se verán interrumpidas si no se puede alcanzar el quórum de réplicas de metadatos. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo. Posible pérdida de datos por fallo permanente dependiendo del número de copias replicadas. La codificación de borrado local puede prevenir la pérdida de datos.
Fallo de varios sitios	No quedan centros operativos. Se perderán los datos si no se puede recuperar al menos un sitio en su totalidad.	Las operaciones se verán interrumpidas si no se puede alcanzar el quórum de réplicas de metadatos. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo. Posible pérdida de datos por fallo permanente si no quedan suficientes fragmentos codificados para borrado. La codificación de borrado local o las copias de seguridad pueden prevenir la pérdida de datos.
Aislamiento de red de un sitio	Las operaciones del cliente se interrumpirán hasta que se resuelva el fallo. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo. Sin pérdida de datos	Las operaciones se verán interrumpidas en el sitio aislado, pero no habrá pérdida de datos. Reduzca la consistencia del bucket a lectura después de nueva escritura o a un nivel inferior para continuar las operaciones sin interrupciones en este estado de fallo. No se han producido interrupciones en las operaciones en los sitios restantes ni pérdida de datos.

Una implementación multi-grid en varios sitios

Para agregar una capa adicional de redundancia, este escenario empleará dos clústeres StorageGRID y usará replicación entre redes para mantenerlos sincronizados. Para esta solución, cada clúster StorageGRID tendrá tres sitios. Se utilizarán dos sitios para el almacenamiento de objetos y metadatos, mientras que el tercer sitio se utilizará únicamente para metadatos. Ambos sistemas se configurarán con una regla ILM equilibrada para almacenar sincrónicamente los objetos utilizando codificación de borrado en cada uno de los

dos sitios de datos. Los buckets se configurarán con el modelo de consistencia global Quorum Strong. Cada cuadrícula se configurará con replicación entre cuadrículas bidireccional en cada segmento. Esto proporciona la replicación asincrónica entre las regiones. Opcionalmente, se puede implementar un balanceador de carga global para administrar las solicitudes a los grupos de alta disponibilidad del balanceador de carga integrado de ambos sistemas StorageGRID para lograr un RPO cero.

La solución utilizará cuatro ubicaciones igualmente divididas en dos regiones. La región 1 contendrá los 2 sitios de almacenamiento de grid 1 como cuadrícula principal de la región y el sitio de metadatos de grid 2. La región 2 contendrá los 2 sitios de almacenamiento de grid 2 como cuadrícula principal de la región y el sitio de metadatos de grid 1. En cada región, la misma ubicación puede alojar el sitio de almacenamiento de la cuadrícula principal de la región, así como el sitio de metadatos de la cuadrícula de otras regiones. El uso de nodos de metadatos como el tercer sitio proporcionará la consistencia necesaria para los metadatos y no duplicará el almacenamiento de los objetos en esa ubicación.



Esta solución con cuatro ubicaciones independientes proporciona una redundancia completa de dos sistemas StorageGRID independientes que mantienen un objetivo de punto de recuperación de 0 RPO y utilizará replicación síncrona multisitio y replicación asíncrona multi-grid. Todo sitio puede fallar sin interrumpir las operaciones de cliente en ambos sistemas StorageGRID.

En esta solución, existen cuatro copias con código de borrado de cada objeto y 18 réplicas de todos los metadatos. Esto permite el caso de múltiples escenarios de fallo sin afectar a las operaciones del cliente. En caso de que se produzcan fallos, las actualizaciones de recuperación de la interrupción se sincronizarán automáticamente con el sitio o los nodos que hayan fallado.

Escenarios de fallos de varios grid y varios sitios

Fallo	Resultado
Fallo de unidad de nodo único	Cada dispositivo utiliza varios grupos de discos y puede mantener al menos 1 unidades por grupo sin interrupciones ni pérdida de datos.
Fallo de un nodo en un sitio de un grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de un solo nodo en un sitio en cada grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de varios nodos en un sitio de un grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de varios nodos en un sitio en cada grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de un único nodo en varios sitios de un grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de un único nodo en varios sitios en cada grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de sitio único en un grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de un único sitio en cada grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallos de un sitio único más nodo en un grid	Sin interrupción de las operaciones ni pérdida de datos.
Sitio único más un nodo de cada sitio restante en un único grid	Sin interrupción de las operaciones ni pérdida de datos.
Fallo de ubicación única	Sin interrupción de las operaciones ni pérdida de datos.
Fallo en una ubicación única en cada cuadrícula DC1 y DC3	Las operaciones se interrumpirán hasta que se resuelva el fallo o se reduzca la coherencia de los bloques; cada grid pierde 2 sitios Todos los datos siguen existiendo en 2 ubicaciones
Fallo en una ubicación única en cada cuadrícula DC1 y DC4 o DC2 y DC3	Sin interrupción de las operaciones ni pérdida de datos.
Fallo en una ubicación única en cada cuadrícula DC2 y DC4	Sin interrupción de las operaciones ni pérdida de datos.
Aislamiento de red de un sitio	Las operaciones se interrumpirán en el sitio aislado, pero no se perderán datos Sin interrupciones en las operaciones de los sitios restantes ni pérdida de datos.

Conclusión

Lograr un objetivo de punto de recuperación cero (RPO) con StorageGRID es un objetivo fundamental para garantizar la durabilidad y disponibilidad de los datos en caso de fallo del sitio. Al aprovechar las sólidas estrategias de replicación de StorageGRID, incluida la replicación síncrona de varios sitios y la replicación asíncrona de varios grid, las organizaciones pueden mantener operaciones de cliente sin interrupciones y garantizar la coherencia de los datos entre varias ubicaciones. La implementación de las políticas de gestión de la vida útil de la información (ILM) y el uso de nodos solo de metadatos mejoran aún más la resiliencia y el rendimiento del sistema. Con StorageGRID, las empresas pueden gestionar sus datos con total confianza y con la tranquilidad de saber que siguen siendo accesibles y coherentes, incluso cuando se producen fallos complejos. Este enfoque integral de la replicación y la gestión de datos subraya la importancia de una planificación y ejecución meticulosas para lograr un RPO cero y proteger la información valiosa.

Cree Cloud Storage Pool para AWS o Google Cloud

Puede usar un pool de almacenamiento en cloud si desea mover objetos de StorageGRID a un bloque de S3 externo. El bloque externo puede pertenecer a Amazon S3 (AWS) o Google Cloud.

Lo que necesitará

- Se configuró StorageGRID 11.6.
- Ya ha configurado un bloque de S3 externo en AWS o Google Cloud.

Pasos

1. En Grid Manager, navegue hasta **ILM** > **agrupaciones de almacenamiento**.
2. En la sección Cloud Storage Pools de la página, seleccione **Crear**.

   Se mostrará la ventana emergente Create Cloud Storage Pool.

3. Introduzca un nombre para mostrar.
4. Seleccione **Amazon S3** en la lista desplegable Tipo de proveedor.

   Este tipo de proveedor funciona con AWS S3 o Google Cloud.

5. Introduzca el URI del bloque de S3 que se va a utilizar para el Cloud Storage Pool.

   Se permiten dos formatos:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Introduzca el nombre de bloque de S3.

   El nombre que especifique debe coincidir exactamente con el nombre del bloque de S3; de lo contrario, se producirá un error al crear el pool de almacenamiento en cloud. No se puede cambiar este valor después de guardar el pool de almacenamiento en cloud.

7. De manera opcional, introduzca el identificador de clave de acceso y la clave de acceso secreta.
8. Seleccione **no verificar certificado** en la lista desplegable.

9. Haga clic en **Guardar**.

Resultado esperado

Confirme que se ha creado un Cloud Storage Pool para Amazon S3 o Google Cloud.

Por Jonathan Wong

Cree Cloud Storage Pool para el almacenamiento BLOB de Azure

Puede usar un pool de almacenamiento en cloud si desea mover objetos de StorageGRID a un contenedor de Azure externo.

Lo que necesitará

- Se configuró StorageGRID 11.6.
- Ya ha configurado un contenedor de Azure externo.

Pasos

1. En Grid Manager, navegue hasta **ILM** > **agrupaciones de almacenamiento**.
2. En la sección Cloud Storage Pools de la página, seleccione **Crear**.

   Se mostrará la ventana emergente Create Cloud Storage Pool.

3. Introduzca un nombre para mostrar.
4. Seleccione **Azure Blob Storage** en la lista desplegable Provider Type.
5. Introduzca el URI del bloque de S3 que se va a utilizar para el Cloud Storage Pool.

   Se permiten dos formatos:

   ```
   https://host:port
   ```

   ```
   http://host:port
   ```

6. Introduzca el nombre del contenedor de Azure.

   El nombre que especifique debe coincidir exactamente con el nombre del contenedor de Azure; de lo contrario, se producirá un error al crear el pool de almacenamiento en cloud. No se puede cambiar este valor después de guardar el pool de almacenamiento en cloud.

7. De forma opcional, introduzca el nombre de cuenta y la clave de cuenta asociados del contenedor de Azure para la autenticación.
8. Seleccione **no verificar certificado** en la lista desplegable.
9. Haga clic en **Guardar**.

Resultado esperado

Confirme que se ha creado un Cloud Storage Pool para el almacenamiento BLOB de Azure.

Por Jonathan Wong

Utilice un pool de almacenamiento en el cloud para el backup

Puede crear una regla de ILM para mover objetos a un pool de almacenamiento en el cloud para backup.

Lo que necesitará

- Se configuró StorageGRID 11.6.
- Ya ha configurado un contenedor de Azure externo.

Pasos

1. En Grid Manager, navegue hasta **ILM** > **Reglas** > **Crear**.
2. Introduzca una descripción.
3. Introduzca un criterio para activar la regla.
4. Haga clic en **Siguiente**.
5. Replique el objeto en nodos de almacenamiento.
6. Agregue una regla de colocación.
7. Replique el objeto en el pool de almacenamiento en cloud
8. Haga clic en **Siguiente**.
9. Haga clic en **Guardar**.

Resultado esperado

Confirmar que el diagrama de retención muestra los objetos almacenados localmente en StorageGRID y en un pool de almacenamiento en cloud para backup.

Confirme que, cuando se activa la regla de ILM, existe una copia en el Cloud Storage Pool y puede recuperar el objeto localmente sin realizar una restauración de objetos.

Por Jonathan Wong

Configure el servicio de integración de búsqueda StorageGRID

Esta guía proporciona instrucciones detalladas para configurar el servicio de integración de búsqueda de NetApp StorageGRID con Amazon OpenSearch Service o Elasticsearch en las instalaciones.

Introducción

StorageGRID admite tres tipos de servicios de plataforma.

- **Replicación CloudMirror de StorageGRID**. Reflejar objetos específicos desde un bloque de StorageGRID en un destino externo especificado.
- **Notificaciones**. Notificaciones de eventos por bloque para enviar notificaciones sobre acciones específicas realizadas en los objetos a un Amazon simple Notification Service (Amazon SNS) externo especificado.

- **Servicio de integración de búsqueda**. Envíe metadatos de objetos de simple Storage Service (S3) a un índice de Elasticsearch especificado, donde se pueden buscar o analizar los metadatos usando el servicio externo.

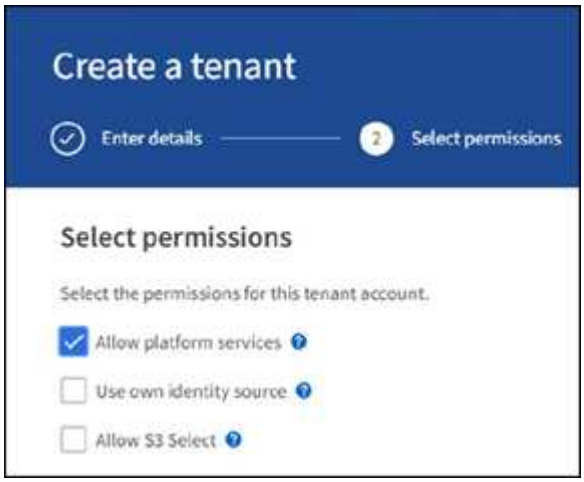
Los servicios de plataforma se configuran por el inquilino de S3 a través de la IU del administrador de inquilinos. Para obtener más información, consulte "Consideraciones sobre el uso de servicios de plataforma".

Este documento sirve como suplemento a la "Guía de inquilinos de StorageGRID 11.6" y proporciona instrucciones paso a paso y ejemplos para la configuración de endpoints y bloques para los servicios de integración de búsqueda. Las instrucciones de configuración de Amazon Web Services (AWS) o Elasticsearch en las instalaciones que se incluyen aquí son solo para fines de prueba o demostración básicos.

Las audiencias deben estar familiarizadas con Grid Manager y Tenant Manager y tener acceso al navegador S3 para realizar operaciones básicas de carga (PUT) y descarga (GET) para las pruebas de integración de búsqueda de StorageGRID.

Cree un inquilino y habilite los servicios de plataforma

1. Cree un inquilino S3 mediante Grid Manager, introduzca un nombre para mostrar y seleccione el protocolo S3.
2. En la página permisos, seleccione la opción permitir servicios de plataforma. Opcionalmente, seleccione otros permisos, si es necesario.



3. Configure la contraseña inicial del usuario raíz del inquilino o, si Identify federation está habilitada en la cuadrícula, seleccione el grupo federado con permiso de acceso raíz para configurar la cuenta de inquilino.
4. Haga clic en Iniciar sesión como raíz y seleccione cucharón: Crear y administrar cucharones.

   Esto le lleva a la página Administrador de inquilinos.

5. En Tenant Manager, seleccione My Access Keys para crear y descargar la clave de acceso S3 para realizar pruebas posteriores.

Servicios de integración de búsqueda con Amazon OpenSearch

Configuración del servicio Amazon OpenSearch (antes Elasticsearch)

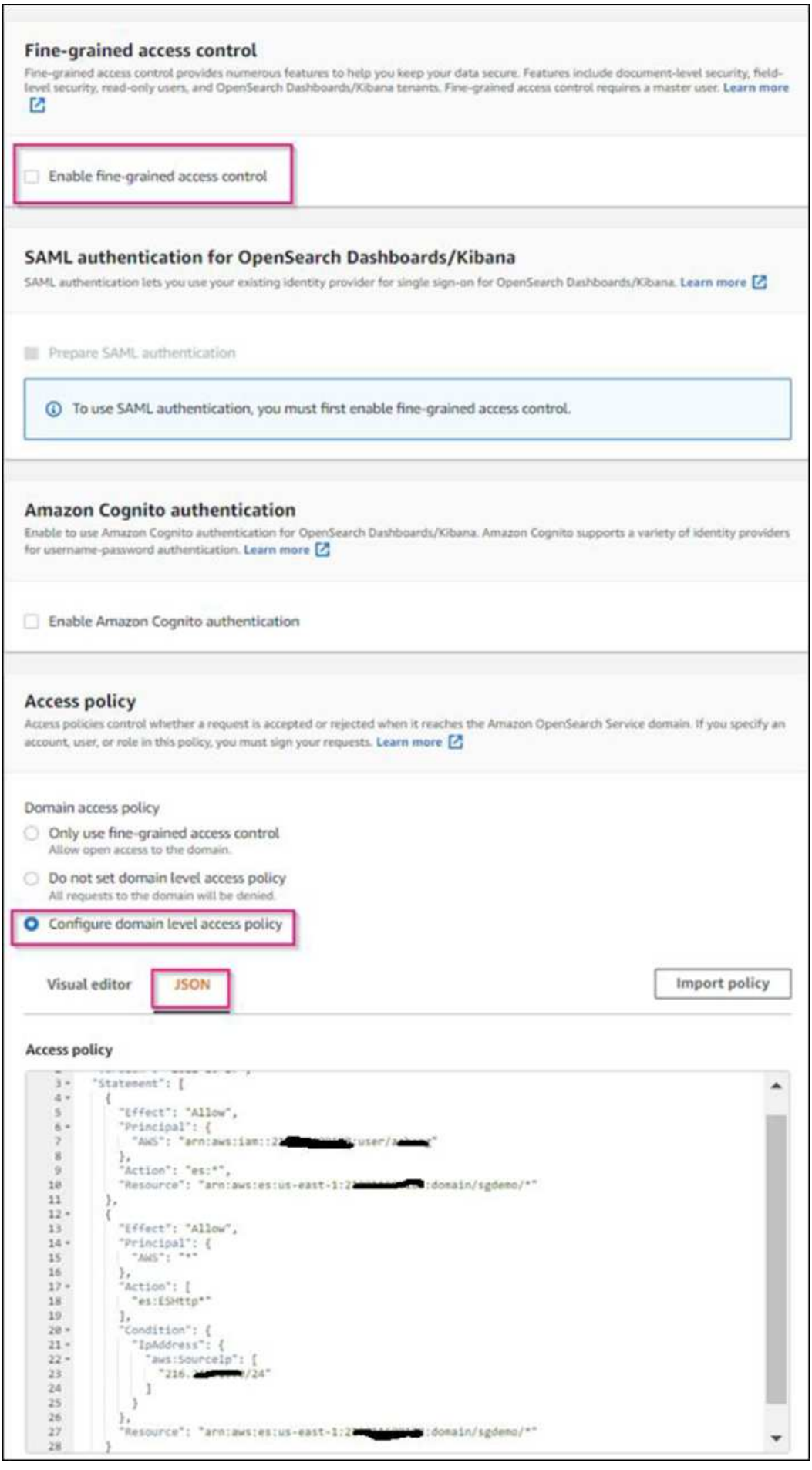
Utilice este procedimiento para una configuración rápida y sencilla del servicio OpenSearch sólo con fines de

prueba/demostración. Si utiliza Elasticsearch en las instalaciones para los servicios de integración de búsqueda, consulte la sección Servicios de integración de búsqueda con Elasticsearch en las instalaciones.

> Debe tener un inicio de sesión de la consola de AWS válido, una clave de acceso, una clave de acceso secreta y permisos para suscribirse al servicio OpenSearch.

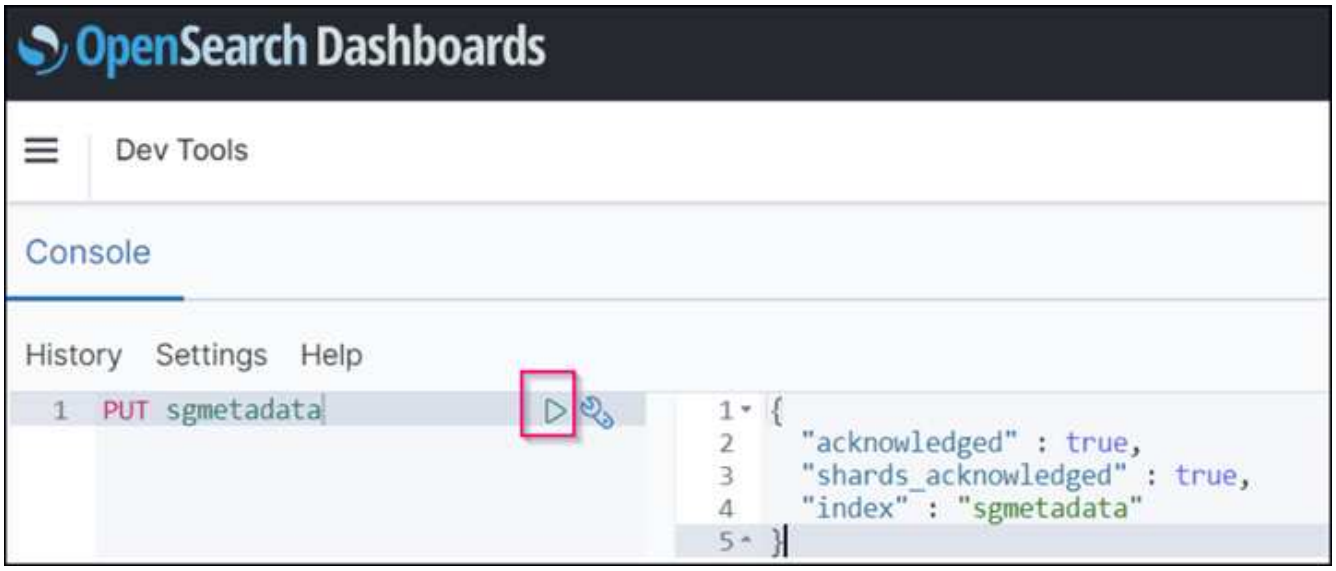
1. Cree un nuevo dominio siguiendo las instrucciones de "Introducción al servicio AWS OpenSearch", excepto lo siguiente:
   - Paso 4. Nombre de dominio: Sgdemo
   - Paso 10. Control de acceso detallado: Anule la selección de la opción Habilitar control de acceso detallado.
   - Paso 12. Política de acceso: Seleccione Configure Level Access Policy, seleccione la pestaña JSON para modificar la política de acceso mediante el ejemplo siguiente:
     - Reemplace el texto resaltado por su propio ID y nombre de usuario de gestión de acceso e identidades (IAM) de AWS.
     - Reemplace el texto resaltado (la dirección IP) por la dirección IP pública del equipo local que utilizó para acceder a la consola de AWS.
     - Abra una pestaña del navegador a. "https://checkip.amazonaws.com" Para encontrar su IP pública.

```
{

    "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/*"
        }
    ]
}
```

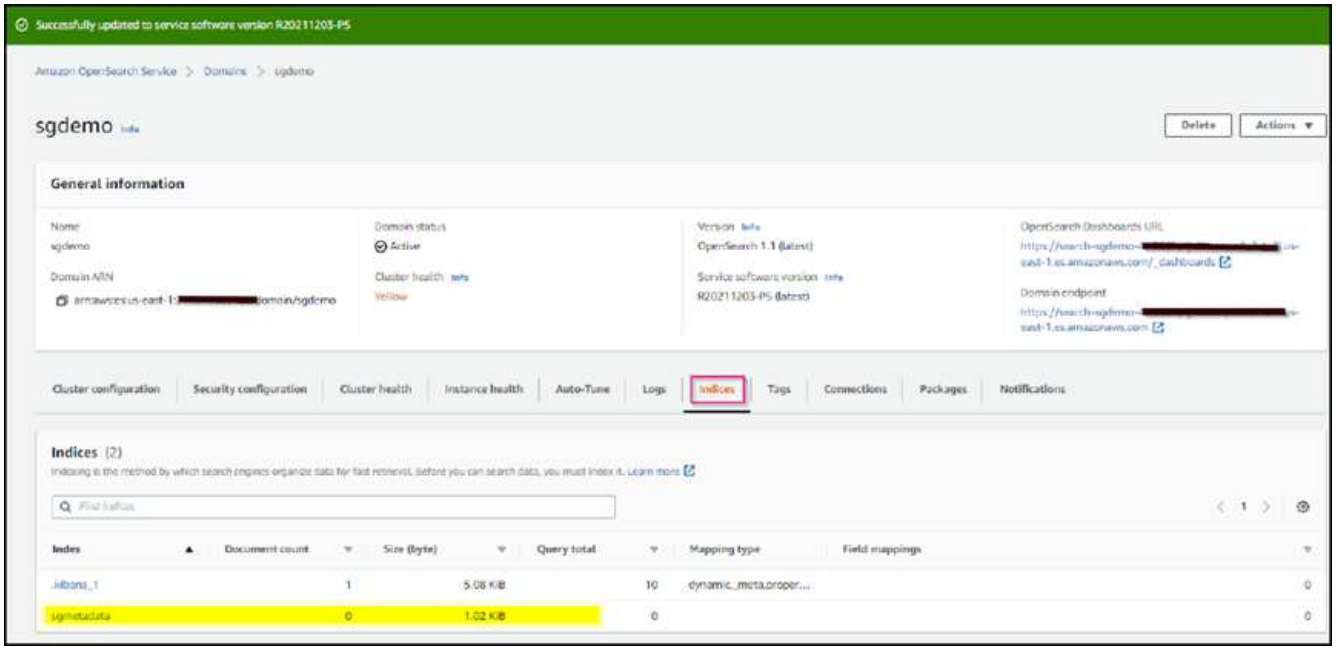

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
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. Espere de 15 a 20 minutos para que el dominio se active.

3. Haga clic en OpenSearch Dashboards URL para abrir el dominio en una nueva pestaña para tener acceso al panel. Si obtiene un error de acceso denegado, compruebe que la dirección IP de origen de la directiva de acceso esté correctamente configurada en la IP pública del equipo para permitir el acceso al panel de control de dominio.
4. En la página de bienvenida del panel, seleccione explorar por su cuenta. En el menú, vaya a Management → Dev Tools
5. En Herramientas de desarrollo → Consola , escriba `PUT <index>` Donde se usa el índice para almacenar metadatos de objetos StorageGRID. Utilizamos el nombre de índice 'gmetadata' en el siguiente ejemplo. Haga clic en el símbolo de triángulo pequeño para ejecutar el comando PUT. El resultado esperado se muestra en el panel derecho como se muestra en la siguiente captura de pantalla de ejemplo.



6. Verifique que el índice sea visible desde la IU de Amazon OpenSearch en sgdomain > Indices.

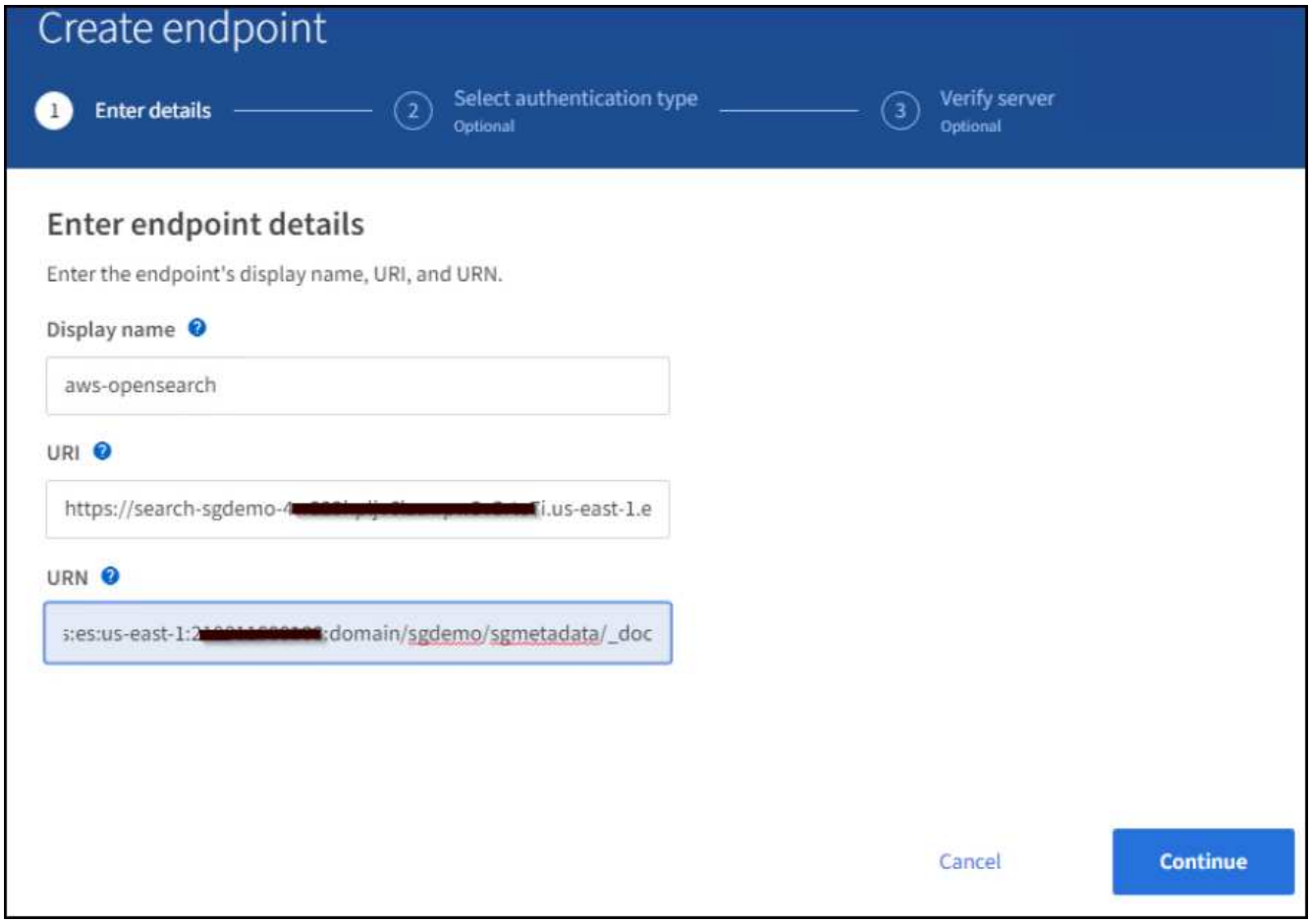


Configuración de extremos de servicios de plataforma

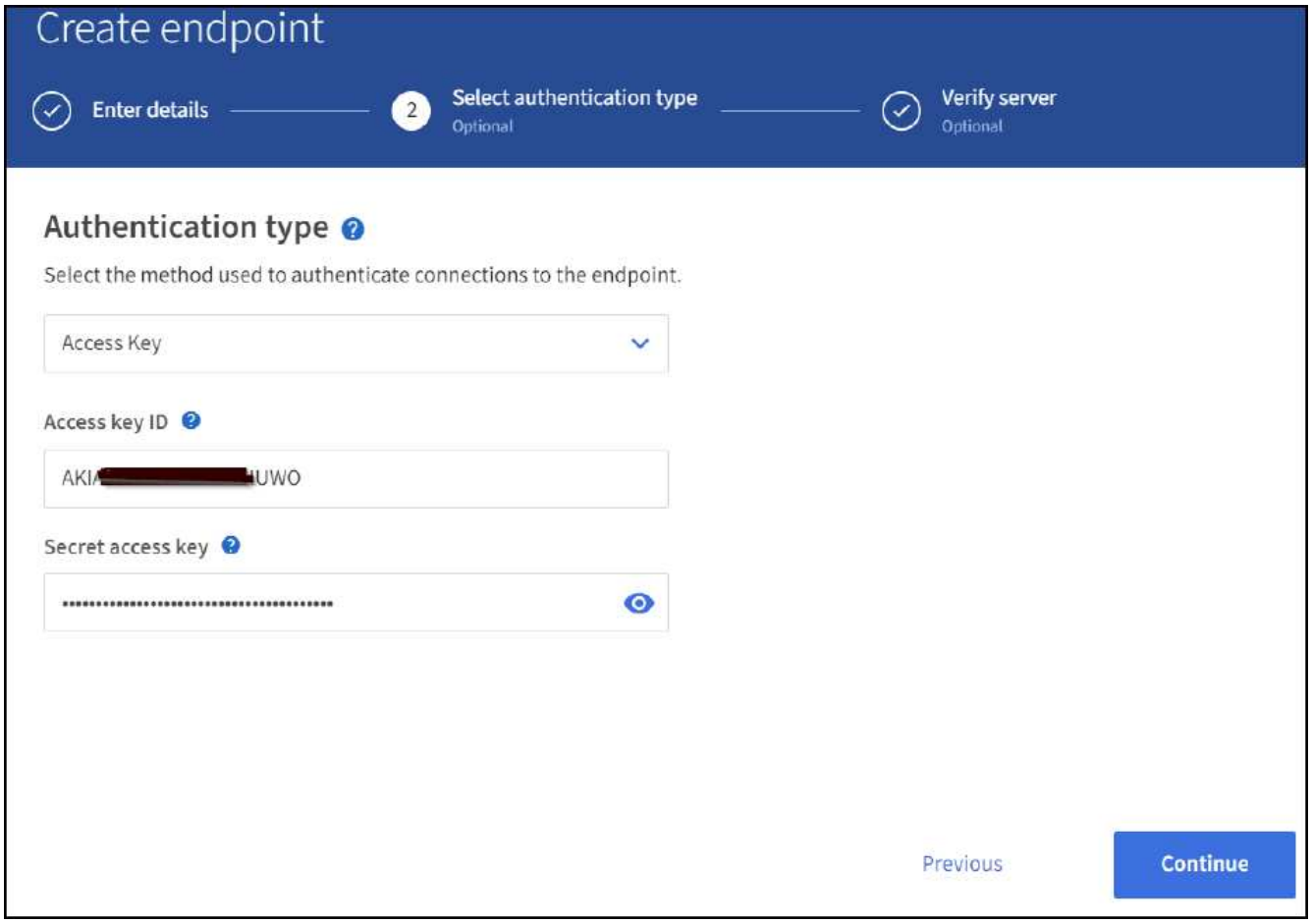
Para configurar los extremos de servicios de la plataforma, siga estos pasos:

1. En el administrador de inquilinos, vaya a ALMACENAMIENTO (S3) > extremos de servicios de la plataforma.
2. Haga clic en Create Endpoint, introduzca lo siguiente y haga clic en Continue:
   - Ejemplo de nombre para mostrar `aws-opensearch`
   - El extremo de dominio en la captura de pantalla de ejemplo bajo el paso 2 del procedimiento anterior en el campo URI.
   - El dominio ARN utilizado en el paso 2 del procedimiento anterior en el campo URN y agregue `/<index>/_doc` Al final de ARN.

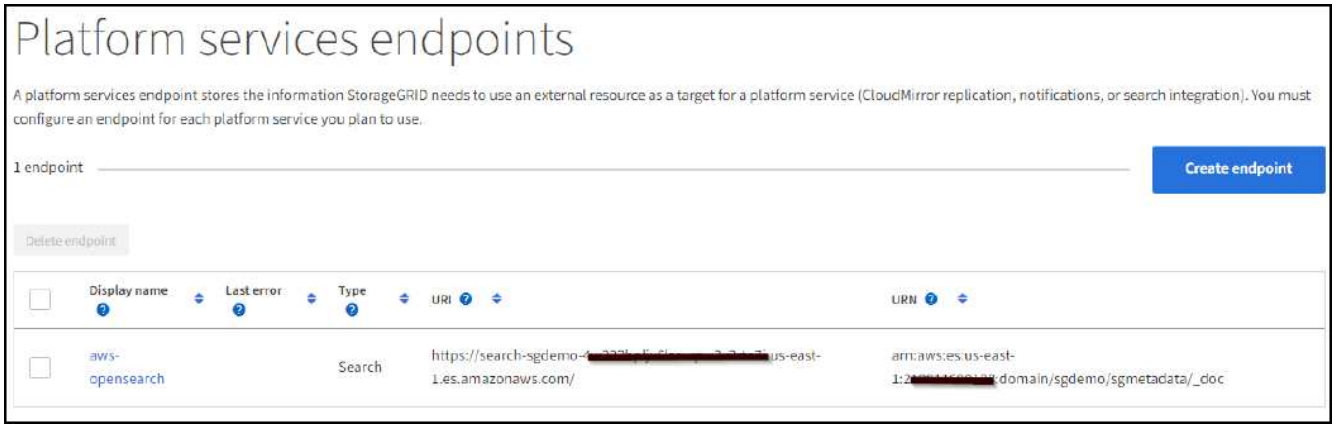
     En este ejemplo, URN se convierte en `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



3. Para acceder al dominio sgDomain de Amazon OpenSearch, elija Access Key como tipo de autenticación y, a continuación, introduzca la clave de acceso y la clave secreta de Amazon S3. Para ir a la página siguiente, haga clic en continuar.



4. Para verificar el punto final, seleccione usar certificado CA del sistema operativo y probar y crear punto final. Si la verificación se realiza correctamente, aparece una pantalla de extremo similar a la siguiente figura. Si se produce un error de verificación, compruebe que URN incluya `/<index>/_doc` Al final de la ruta, la clave de acceso y la clave secreta de AWS son correctas.



Servicios de integración de búsqueda con Elasticsearch en las instalaciones

Configuración de Elasticsearch en las instalaciones

Este procedimiento es para una configuración rápida de Elasticsearch en las instalaciones y Kibana usando docker solo para fines de pruebas. Si ya existe el servidor Elasticsearch y Kibana, vaya al paso 5.

1. Siga este "Procedimiento de instalación de Docker" para instalar el docker. Utilizamos la "Procedimiento de instalación de CentOS Docker" en esta configuración.

```
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
```

   - Para iniciar docker después del reinicio, introduzca lo siguiente:

```
sudo systemctl enable docker
```

   - Ajuste la `vm.max_map_count` valor hasta 262144:

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

   - Para mantener el ajuste después del reinicio, introduzca lo siguiente:

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

2. Siga la "Guía de inicio rápido de Elasticsearch" Sección autogestionada para instalar y ejecutar Elasticsearch y Kibana docker. En este ejemplo, instalamos la versión 8.1.

Tenga en cuenta el nombre de usuario/contraseña y el token creados por Elasticsearch, necesita esos elementos para iniciar la autenticación del extremo de la plataforma StorageGRID y la interfaz de usuario de Kibana.

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.

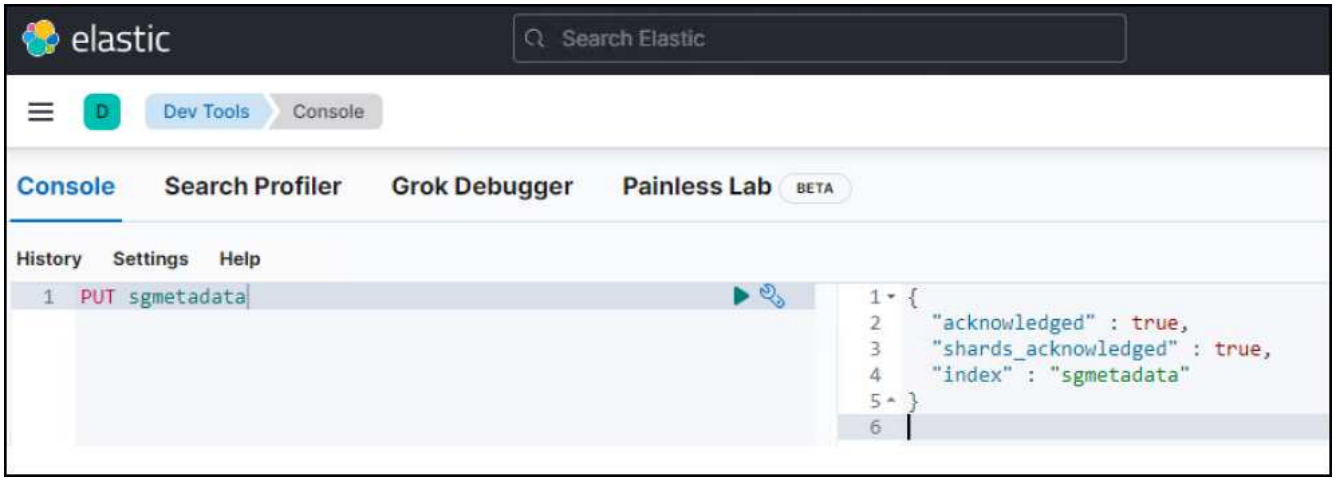
1. In a new terminal session, run:

```
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.

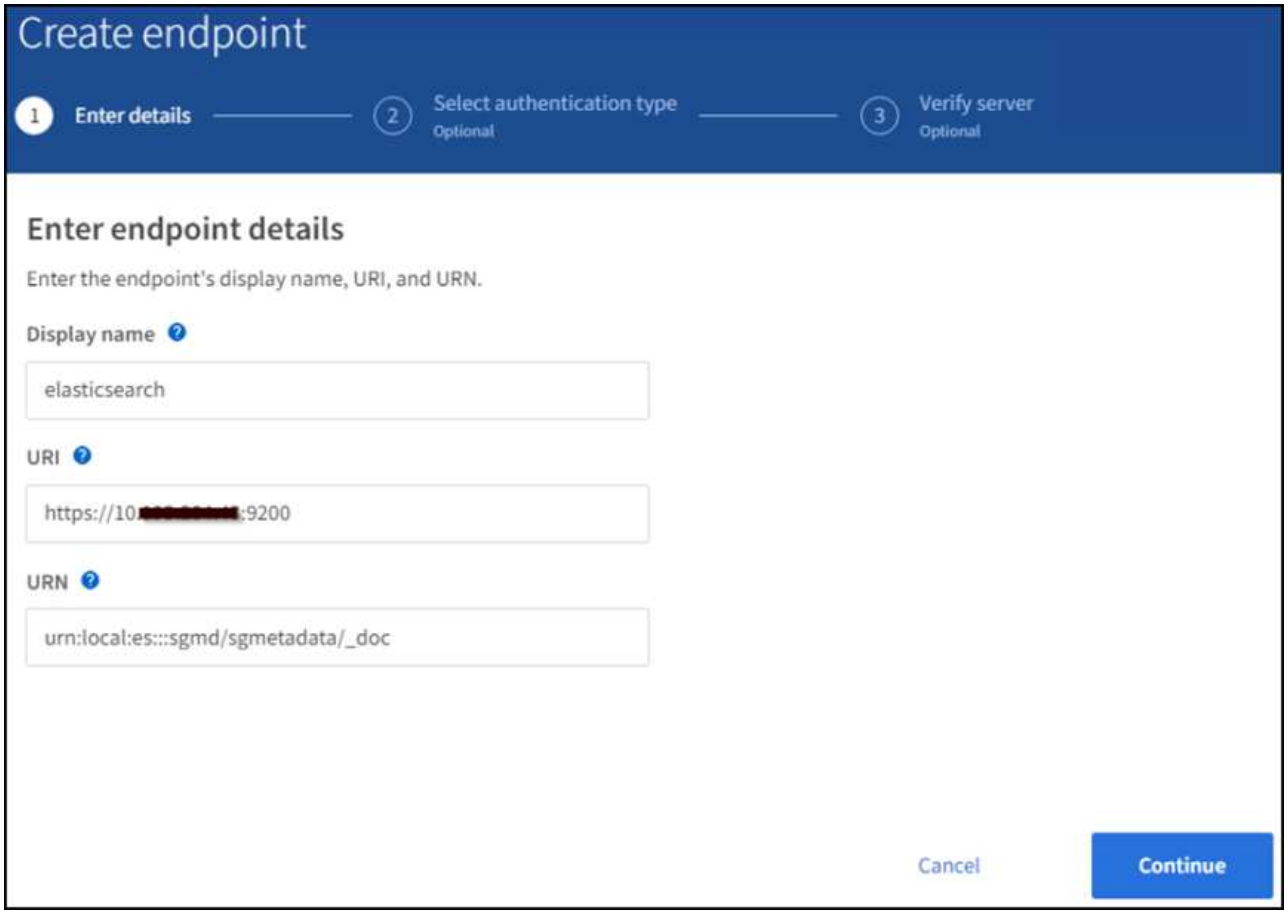
3. Después de que se haya iniciado el contenedor de Docker de Kibana, el enlace de URL `https://0.0.0.0:5601` aparecen en la consola. Reemplace 0.0.0.0 por la dirección IP del servidor en la dirección URL.
4. Inicie sesión en la interfaz de usuario de Kibana con el nombre de usuario `elastic` Y la contraseña generada por Elastic en el paso anterior.
5. Para iniciar sesión por primera vez, en la página de bienvenida del panel, seleccione explorar por su cuenta. En el menú, seleccione Management > Dev Tools.
6. En la pantalla Dev Tools Console, introduzca `PUT <index>` Dónde se usa este índice para almacenar metadatos de objetos StorageGRID. Usamos el nombre del índice `sgmetadata` en este ejemplo. Haga clic en el símbolo de triángulo pequeño para ejecutar el comando PUT. El resultado esperado se muestra en el panel derecho como se muestra en la siguiente captura de pantalla de ejemplo.



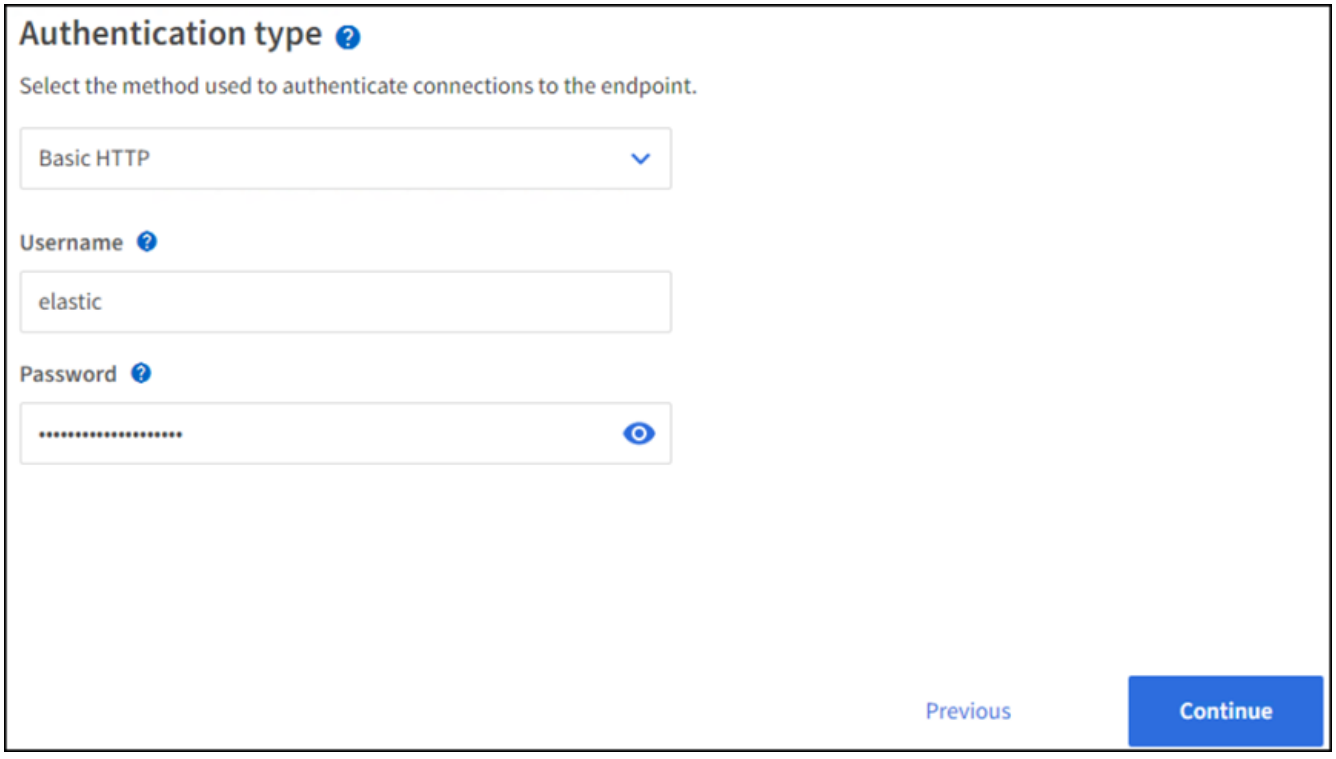
Configuración de extremos de servicios de plataforma

Para configurar extremos para servicios de plataforma, siga estos pasos:

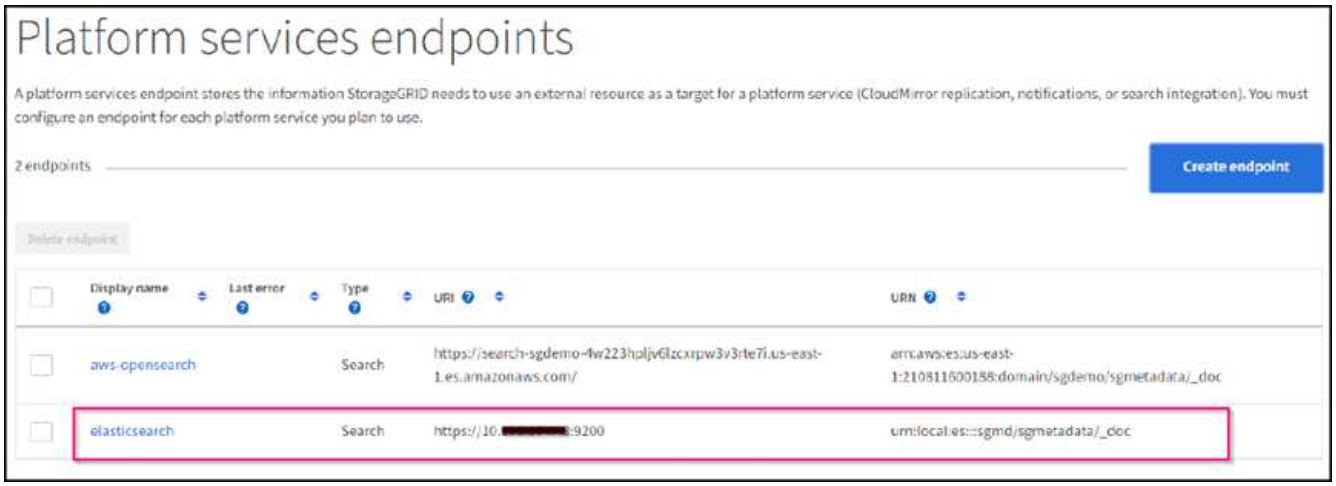
1. En el Administrador de inquilinos, vaya a ALMACENAMIENTO (S3) > extremos de servicios de la plataforma
2. Haga clic en Create Endpoint, introduzca lo siguiente y haga clic en Continue:
   - Ejemplo de nombre para mostrar: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
   - URN: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Donde el nombre de índice es el nombre que utilizó en la consola de Kibana. Ejemplo: `urn:local:es:::sgmd/sgmetadata/_doc`



3. Seleccione HTTP básico como tipo de autenticación, introduzca el nombre de usuario `elastic` Y la contraseña generada por el proceso de instalación de Elasticsearch. Para ir a la página siguiente, haga clic en continuar.



4. Seleccione no verificar certificado y probar y Crear extremo para verificar el extremo. Si la verificación se realiza correctamente, aparece una pantalla de punto final similar a la siguiente captura de pantalla. Si se produce un error en la verificación, compruebe que las entradas de URN, URI y nombre de usuario/contraseña sean correctas.



Configuración del servicio de integración de búsqueda de bloques

Una vez creado el extremo de servicio de la plataforma, el siguiente paso es configurar este servicio a nivel de bloque para enviar metadatos de objetos al extremo definido cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Puede configurar la integración de búsqueda mediante el Administrador de inquilinos para aplicar un XML de configuración de StorageGRID personalizado a un bloque de la siguiente forma:

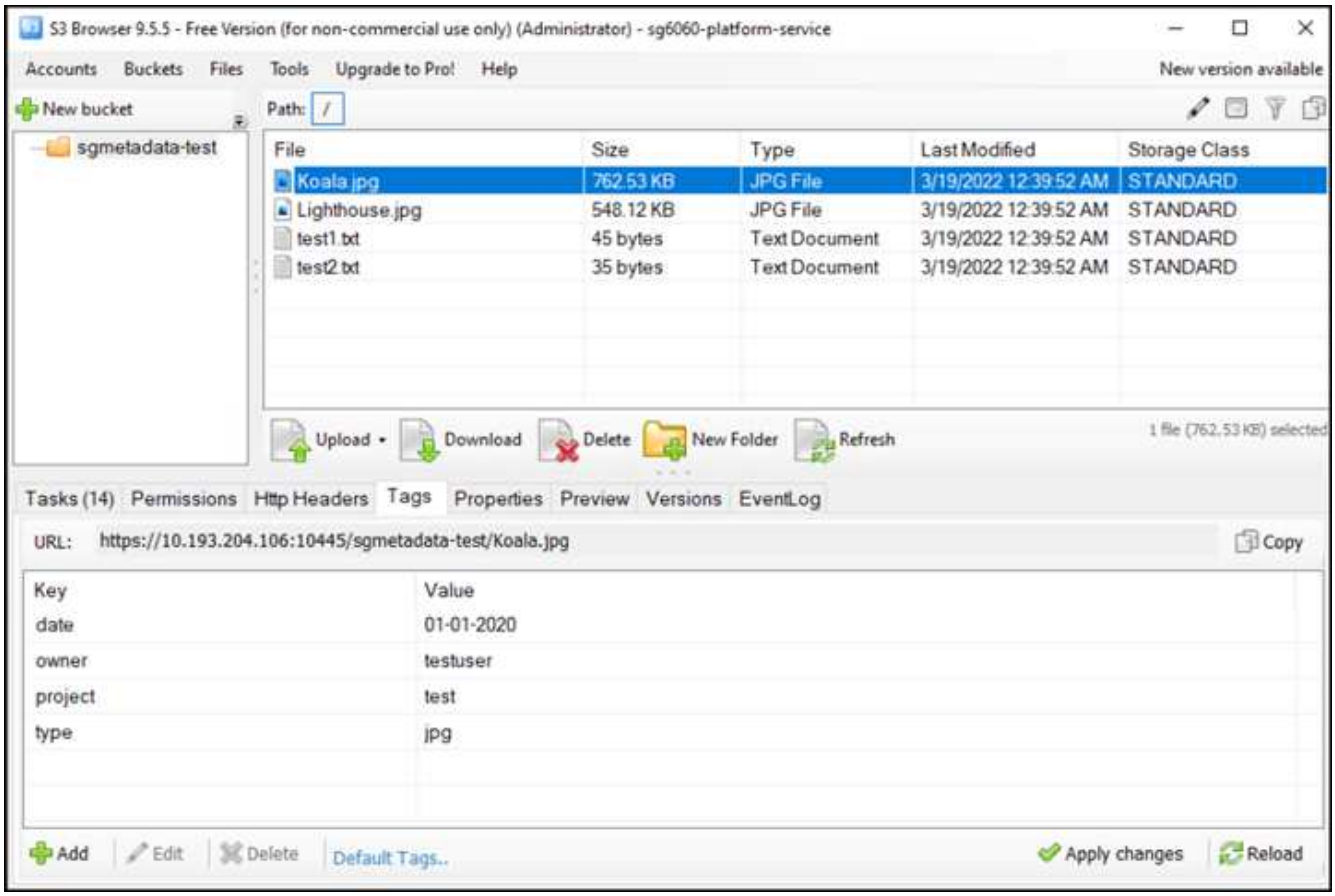
1. En el administrador de inquilinos, vaya a STORAGE(S3) > Buckets
2. Haga clic en Create Bucket, introduzca el nombre del bloque (por ejemplo, `sgmetadata-test`) y acepte el valor predeterminado `us-east-1` región.
3. Haga clic en Continue > Create Bucket.
4. Para abrir la página bucket Overview, haga clic en el nombre del bloque y, a continuación, seleccione Platform Services.
5. Seleccione el cuadro de diálogo Habilitar integración de búsqueda. En el cuadro XML proporcionado, introduzca el XML de configuración mediante esta sintaxis.

   El URN resaltado debe coincidir con el extremo de servicios de plataforma definido. Puede abrir otra pestaña del explorador para acceder al administrador de inquilinos y copiar el URN desde el extremo de servicios de plataforma definido.

   En este ejemplo, no hemos utilizado ningún prefijo, lo que significa que los metadatos de cada objeto de este bloque se envían al extremo de Elasticsearch definido previamente.

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

6. Utilice el navegador S3 para conectarse a StorageGRID con la clave secreta/acceso de inquilino y cargar objetos de prueba a. `sgmetadata-test` agrupe y añada etiquetas o metadatos personalizados a los objetos.



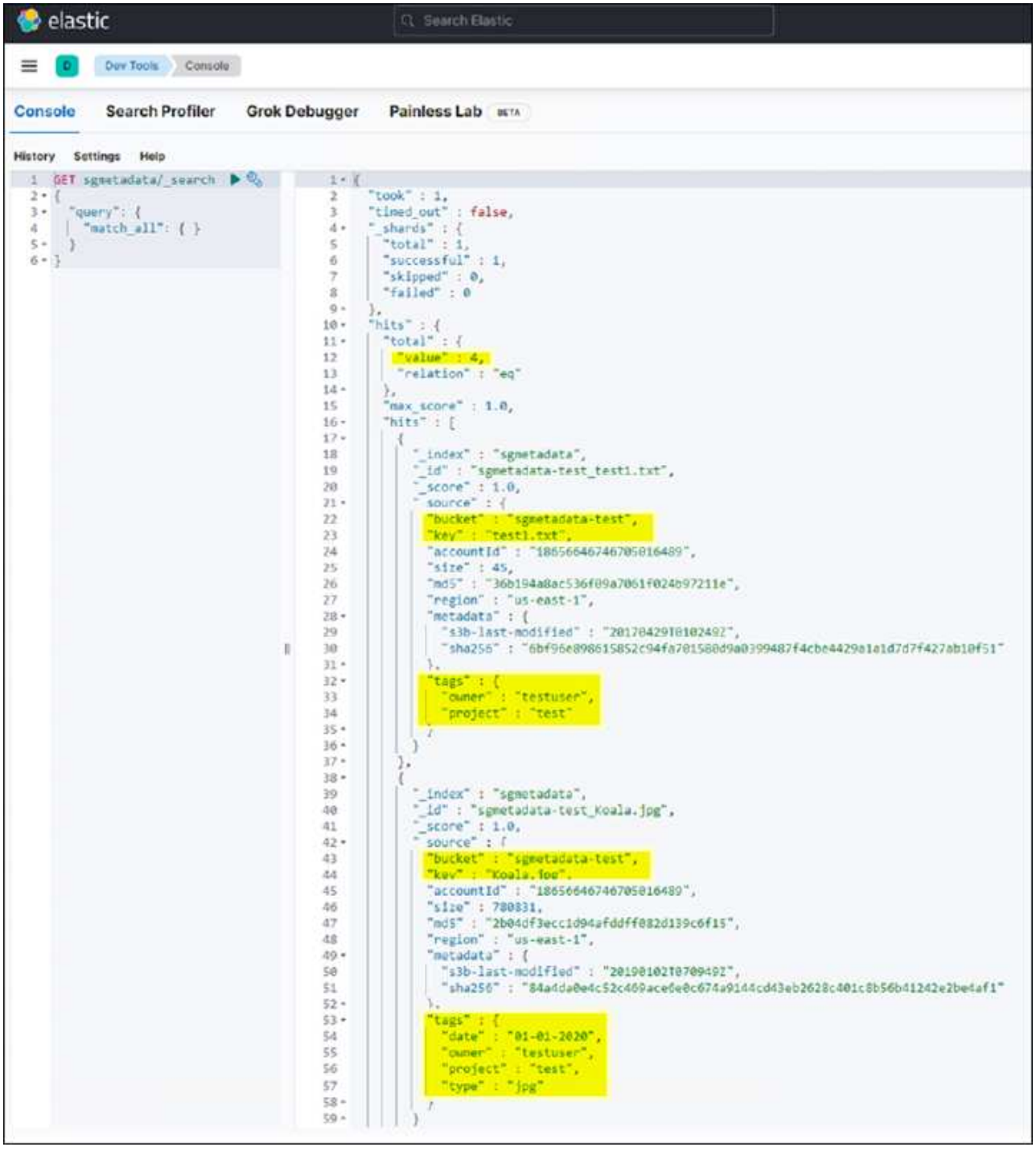
7. Utilice la interfaz de usuario de Kibana para verificar que los metadatos del objeto se cargaron en el índice de metadatos sg.

   a. En el menú, seleccione Management > Dev Tools.

   b. Pegue la consulta de ejemplo en el panel de la consola de la izquierda y haga clic en el símbolo de triángulo para ejecutarla.

      El resultado de ejemplo de consulta 1 de la siguiente captura de pantalla de ejemplo muestra cuatro registros. Esto coincide con el número de objetos del segmento.

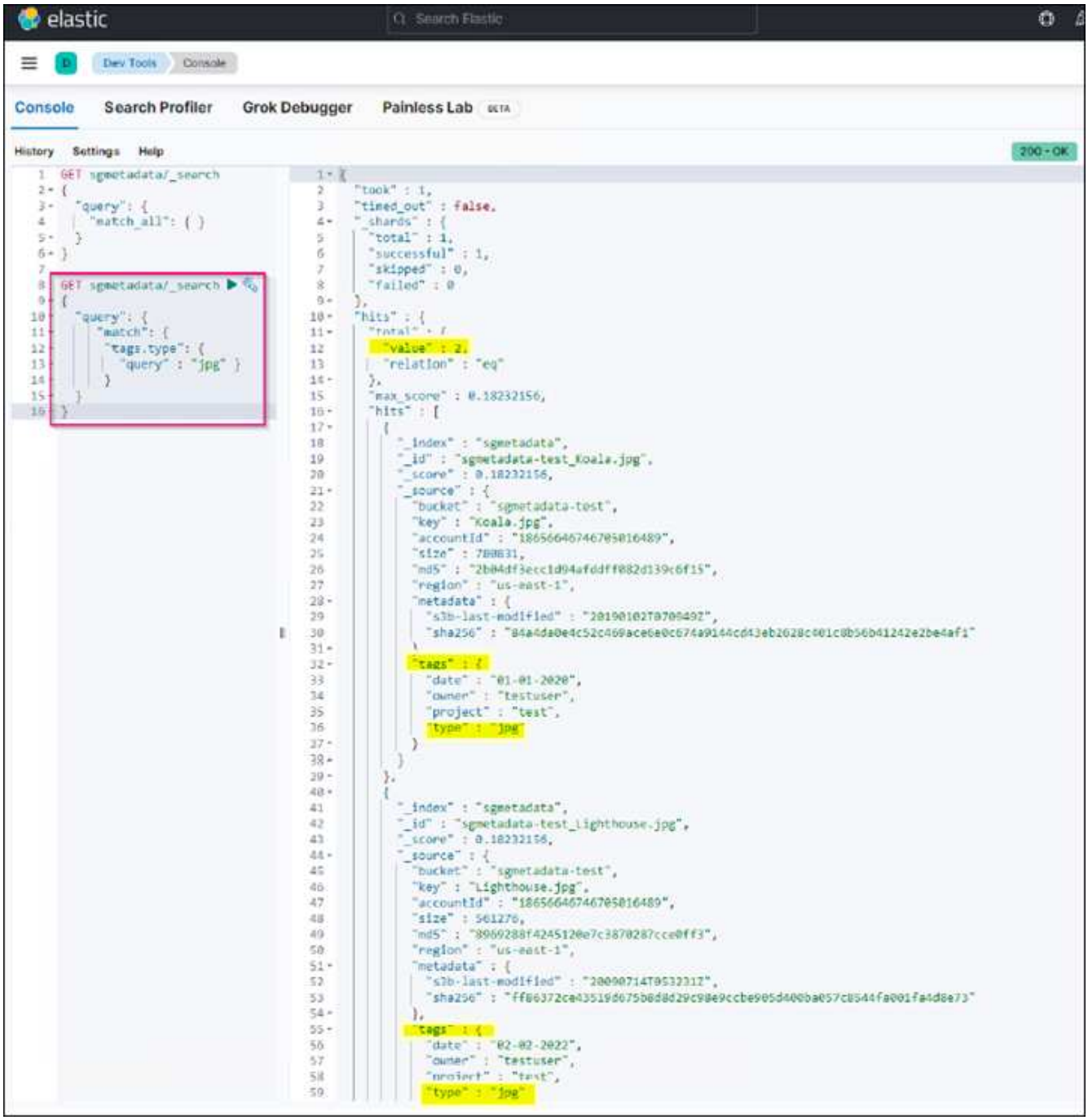
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



El resultado de ejemplo de la consulta 2 en la siguiente captura de pantalla muestra dos registros con el tipo de etiqueta jpg.

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

+



Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- "¿Qué son los servicios de plataforma"
- "Documentación de StorageGRID 11.6"

Por Angela Cheng

Clon de nodo

Consideraciones y rendimiento del clon de nodos.

Consideraciones sobre el clon de nodo

El clon de nodo puede ser un método más rápido para reemplazar nodos de dispositivos existentes para realizar una actualización tecnológica, aumentar la capacidad o aumentar el rendimiento de su sistema StorageGRID. El clon de nodos también puede ser útil para convertir a cifrado de nodos con un KMS o cambiar un nodo de almacenamiento de DDP8 a DDP16.

- La capacidad utilizada del nodo de origen no es relevante al tiempo que se requiere para que se complete el proceso de clonado. El clon de nodo es una copia completa del nodo que incluye el espacio libre en el nodo.
- Los dispositivos de origen y destino deben tener la misma versión PGE
- El nodo de destino siempre debe tener una capacidad mayor que el origen
  - Asegúrese de que el nuevo dispositivo de destino tiene un tamaño de unidad mayor que la fuente
  - Si el dispositivo de destino tiene unidades del mismo tamaño y está configurado para DDP8, puede configurar el destino para DDP16. Si el origen ya está configurado para DDP16, el clon del nodo no será posible.
  - Al pasar de dispositivos SG5660 o SG5760 a dispositivos SG6060, tenga en cuenta que el SG6060 tiene 60 unidades de capacidad, en las que el SG6060 solo tiene 58.
- El proceso de clonado del nodo requiere que el nodo de origen esté desconectado al grid durante el proceso de clonado. Si se desconecta un nodo adicional durante esta ocasión, los servicios del cliente podrían verse afectados.
- 11,8 y siguientes: Un nodo de almacenamiento solo puede estar sin conexión durante 15 días. Si el cálculo del proceso de clonación está cerca de 15 días o supera los 15 días, utilice los procedimientos de expansión y retirada.
  - 11,9: Se ha eliminado el límite de 15 días.
- Para SG6060 o SG6160 con bandejas de ampliación, debe añadir el tiempo necesario para el tamaño de unidad de bandeja correcto al momento del tiempo del dispositivo básico para obtener la duración completa del clon.
- La cantidad de volúmenes en un dispositivo de almacenamiento de destino debe ser mayor o igual que la cantidad de volúmenes en el nodo de origen. No se puede clonar un nodo de origen con volúmenes de almacenamiento de objetos 16 (rangedb) en un dispositivo de almacenamiento de destino con volúmenes de almacenamiento de objetos 12, incluso si el dispositivo de destino tiene más capacidad que el nodo de origen. La mayoría de los dispositivos de almacenamiento tienen volúmenes de almacenamiento de objetos de 16 TB, excepto el dispositivo de almacenamiento SGF6112 que solo tiene 12 volúmenes de

almacenamiento de objetos. Por ejemplo, no puede clonar de un SG5760 a un SGF6112.

Estimaciones de rendimiento de clones de nodos

Las siguientes tablas contienen estimaciones calculadas para la duración del clon del nodo. Las condiciones varían de modo que las entradas en **NEGRITA** pueden correr el riesgo de superar el límite de 15 días para un nodo inactivo.

DDP8

SG5612/SG5712/SG5812 → CUALQUIERA

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	1 día	2 días	2.5 días	3 días	4 días	4.5 días	5.5 días
25 GB	1 día	2 días	2.5 días	3 días	4 días	4.5 días	5.5 días

SG5660 → SG5760/SG5860

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	3.5 día	7 días	8.5 días	10.5 días	**13,5 días**	**15,5 días**	**18,5 días**
25 GB	3.5 día	7 días	8.5 días	10.5 días	**13,5 días**	**15,5 días**	**18,5 días**

SG5660 → SG6060/SG6160

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	2.5 día	4.5 días	5.5 días	6.5 días	9 días	10 días	**12 días**
25 GB	2 días	4 días	5 días	6 días	8 días	9 días	10 días

SG5760/SG5860 → SG5760/SG5860

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	3.5 día	7 días	8.5 días	10.5 días	**13,5 días**	**15,5 días**	**18,5 días**
25 GB	3.5 día	7 días	8.5 días	10.5 días	**13,5 días**	**15,5 días**	**18,5 días**

SG5760/SG5860 → SG6060/SG6160

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	2.5 día	4.5 días	5.5 días	6.5 días	9 días	10 días	**12 días**
25 GB	2 días	3.5 días	4.5 días	5.5 días	7 días	8 días	9.5 días

SG6060/SG6160 → SG6060/SG6160

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	2.5 día	4.5 días	5.5 días	6.5 días	8.5 días	9.5 días	11.5 días
25 GB	2 días	3 días	4 días	4.5 días	6 días	7 días	8.5 días

DDP16

SG5760/SG5860 → SG5760/SG5860

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	3.5 día	6.5 días	8 días	9.5 días	**12,5 días**	**14 días**	**17 días**
25 GB	3.5 día	6.5 días	8 días	9.5 días	**12,5 días**	**14 días**	**17 días**

SG5760/SG5860 → SG6060/SG6160

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	2.5 día	5 días	6 días	7.5 días	10 días	11 días	**13 días**
25 GB	2 días	3.5 días	4 días	5 días	6.5 días	7 días	8.5 días

SG6060/SG6160 → SG6060/SG6160

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	3 día	5 días	6 días	7 días	9.5 días	10.5 días	**13 días**
25 GB	2 días	3.5 días	4.5 días	5 días	7 días	7.5 días	9 días

Bandeja de expansión (agregar a más de SG6060 PB/SG6160 PB por cada bandeja del dispositivo de origen)

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB	Tamaño de unidad de 22 TB
10 GB	3.5 día	5 días	6 días	7 días	9.5 días	10.5 días	**12 días**
25 GB	2 días	3 días	4 días	4.5 días	6 días	7 días	8.5 días

Por Aron Klein

Reubicación del sitio de grid y procedimiento de cambio de red en todo el sitio

Esta guía describe la preparación y el procedimiento para la reubicación del sitio StorageGRID en una cuadrícula de varios sitios. Usted debe tener una comprensión completa de este procedimiento y planificar con anticipación para garantizar un proceso sin problemas y minimizar la interrupción a los clientes.

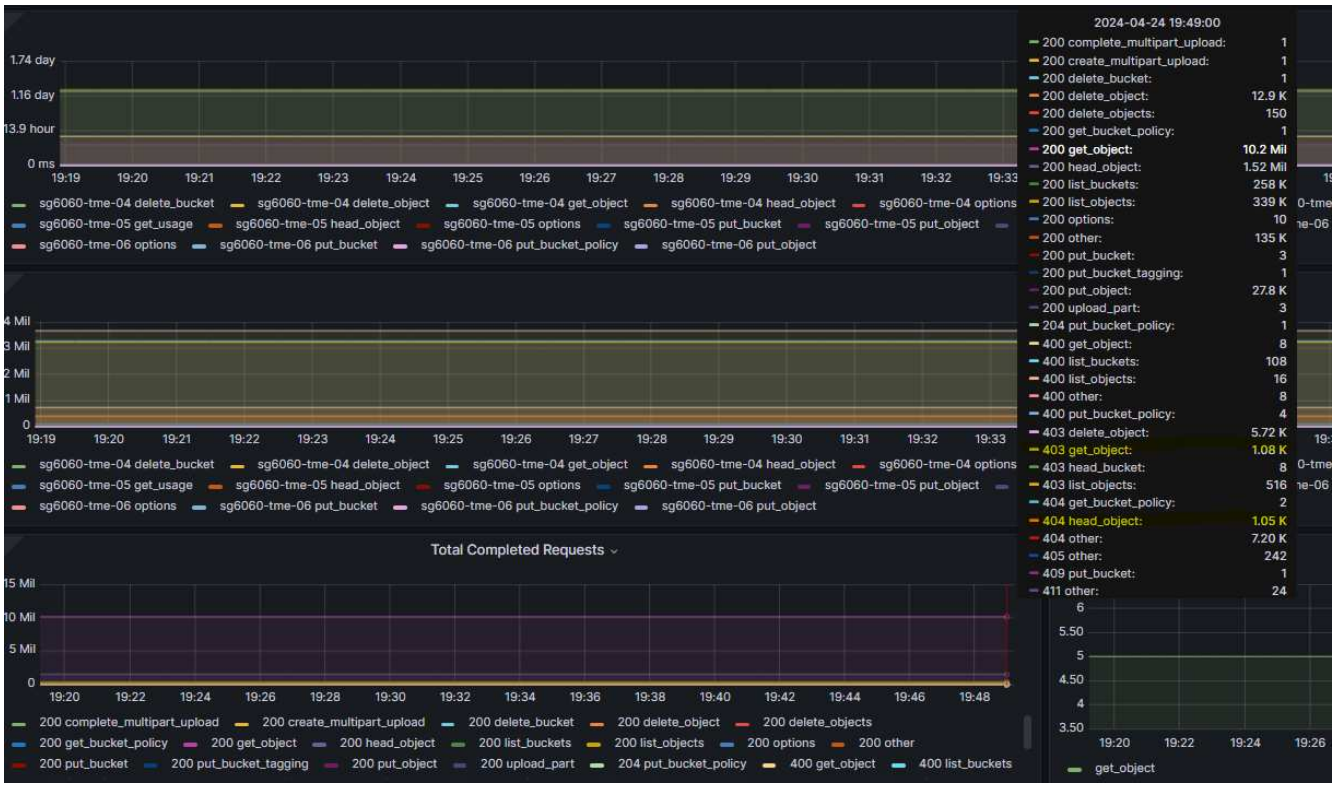
Si necesita cambiar la red de Grid de toda la Grid, consulte "Cambie las direcciones IP para todos los nodos de la cuadrícula".

Consideraciones antes de la reubicación del sitio

- El movimiento del sitio debe completarse y todos los nodos en línea en 15 días para evitar la reconstrucción de la base de datos Cassandra.

"Recupere el nodo de almacenamiento en más de 15 días"

- Si alguna regla de ILM en una política activa utiliza un comportamiento de ingesta estricto, considere cambiarla al equilibrio o a la confirmación doble si el cliente desea seguir PONIENDO objetos en el Grid durante la reubicación del sitio.
- Para los dispositivos de almacenamiento con unidades 60 o más, no mueva nunca la bandeja con unidades de disco instaladas. Etiquete cada unidad de disco y quítelas del compartimento de almacenamiento antes de empacar/mover.
- La VLAN de la red de grid del dispositivo StorageGRID se puede realizar de forma remota a través de la red de administración o la red de cliente. O bien, planifique encontrarse en las instalaciones para realizar el cambio antes o después de la reubicación.
- Compruebe si la aplicación del cliente está utilizando HEAD u OBJECT OPTIMITY antes de PUT. En caso afirmativo, cambie la consistencia del bloque a un sitio seguro para evitar el error de HTTP 500. Si no está seguro, consulte la descripción general de S3 Gráficos Grafana * Administrador de cuadrícula > Soporte > Métricas * y pase el ratón sobre el gráfico 'Total de solicitudes completadas'. Si hay un recuento muy alto de 404 objetos Get Object o 404 objetos head, es probable que una o más aplicaciones estén usando objetos head o get nonexistence. El recuento es acumulativo, pasa el ratón sobre una línea de tiempo diferente para ver la diferencia.



Procedimiento para cambiar la dirección IP de la cuadrícula antes de la reubicación del sitio

Pasos

1. Si se va a utilizar una nueva subred de red de Grid en la nueva ubicación, "Agregue la subred a la lista de subred de red de cuadrícula"
2. Inicie sesión en el nodo de administración principal, use CHANGE-ip para hacer el cambio de Grid IP, debe * almacenar en zona intermedia * el cambio antes de cerrar el nodo para su reubicación.
   a. Seleccione 2 y, a continuación, 1 para el cambio de IP de cuadrícula

```
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. seleccione 5 para mostrar los cambios

```
================================================================================
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
```

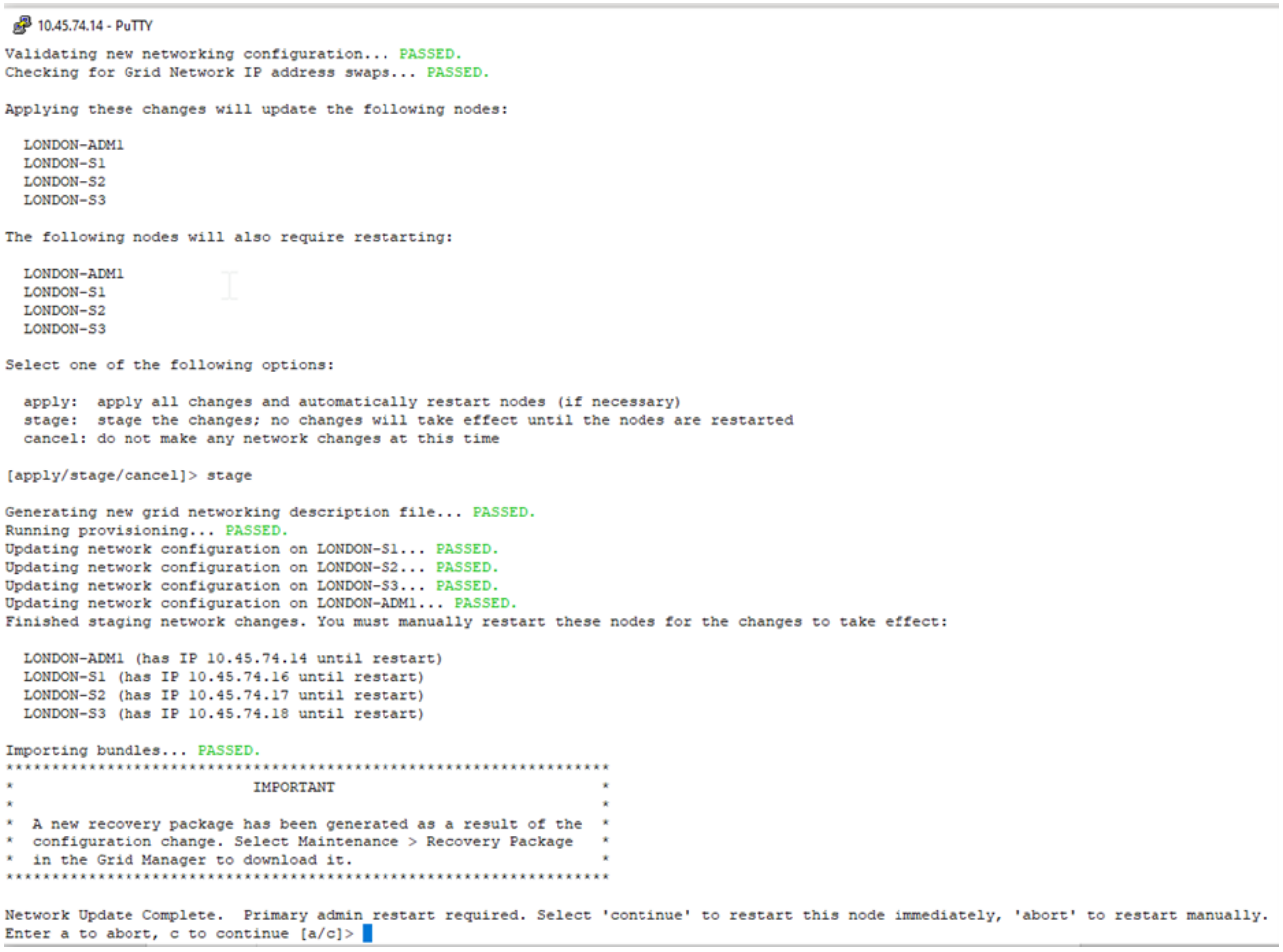
c. seleccione 10 para validar y aplicar el cambio.

```
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
```

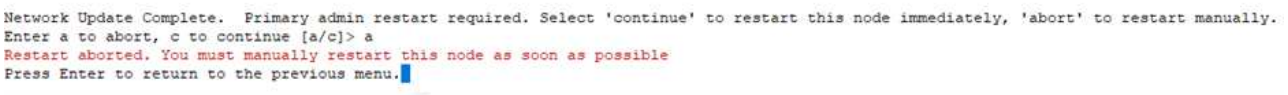
d. Debe seleccionar **stage** en este paso.

```
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. Si el nodo de administración principal está incluido en el cambio anterior, introduzca **'a' para reiniciar manualmente el nodo de administración principal**



f. Pulse ENTER para volver al menú anterior y salir de la interfaz CHANGE-ip.



3. En Grid Manager, descargue el nuevo paquete de recuperación. **Grid manager** > **Mantenimiento** > **Paquete de recuperación**
4. Si se requiere un cambio de VLAN en el dispositivo StorageGRID, consulte la sección Cambio de VLAN del dispositivo.
5. Apague todos los nodos o dispositivos en el sitio, etiquete/quite las unidades de disco si es necesario, desmonte el rack, empaquete y mueva.
6. Si tiene pensado cambiar la ip de la red de administración y/o la VLAN y la dirección ip de cliente, puede realizar el cambio después de la reubicación.

Cambio de VLAN del dispositivo

En el siguiente procedimiento se asume que tiene acceso remoto a la red de clientes o administradores del dispositivo StorageGRID para realizar el cambio de forma remota.

Pasos

1. Antes de apagar el aparato, "coloque el aparato en modo de mantenimiento".

2. Utilice un explorador para acceder a la GUI del instalador del dispositivo StorageGRID mediante https://<admin-or-client-network-ip>:8443. No se puede utilizar Grid IP debido a que la nueva IP de Grid ya está en su lugar una vez que el dispositivo se arranca en modo de mantenimiento.
3. Cambie la VLAN para la red de grid. Si accede al dispositivo a través de red de cliente, no puede cambiar la VLAN de cliente en este momento; puede cambiarlo después del movimiento.
4. ssh en el dispositivo y apague el nodo mediante 'hutdoown -h now'
5. Una vez que los dispositivos estén listos en el sitio nuevo, acceda a la interfaz gráfica de usuario del instalador del dispositivo StorageGRID mediante https://<grid-network-ip>:8443. Confirme que el almacenamiento se encuentre en estado óptimo y que la conectividad de red a otros nodos de Grid mediante las herramientas ping/nmap en la GUI.
6. Si planea cambiar la IP de red del cliente, puede cambiar la VLAN del cliente en este momento. La red cliente no está lista hasta que actualice la ip de la red cliente mediante la herramienta CHANGE-ip en el paso posterior.
7. Salga del modo de mantenimiento. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.
8. Una vez que todos los nodos estén activos y Grid no muestre ningún problema de conectividad, utilice change-ip para actualizar la red de administración del dispositivo y la red de cliente si es necesario.

Migrar el almacenamiento basado en objetos de ONTAP S3 a StorageGRID

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Demostración de migración

Esta es una demostración de la migración de usuarios y buckets de ONTAP S3 a StorageGRID.

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

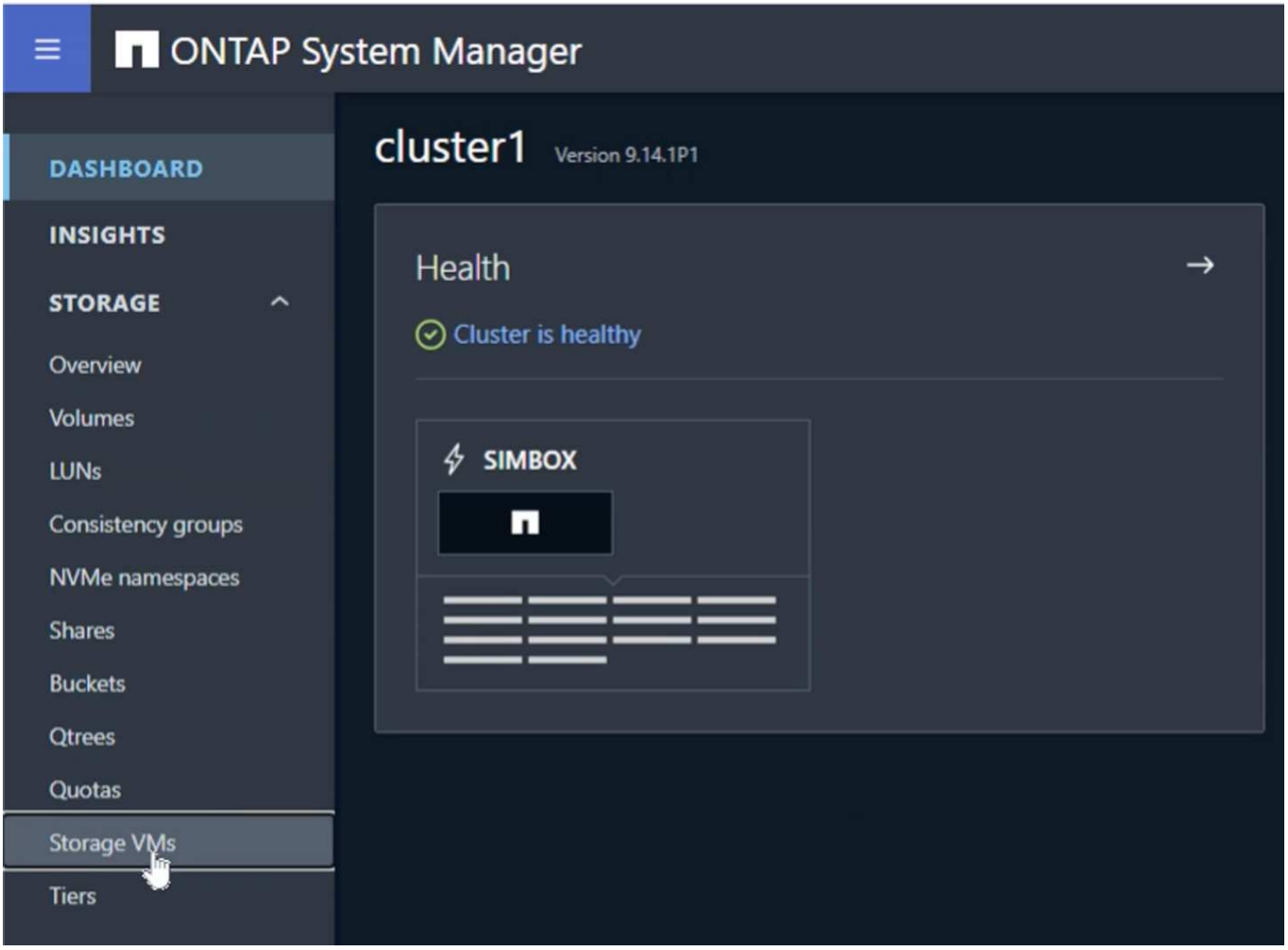
Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Preparando ONTAP

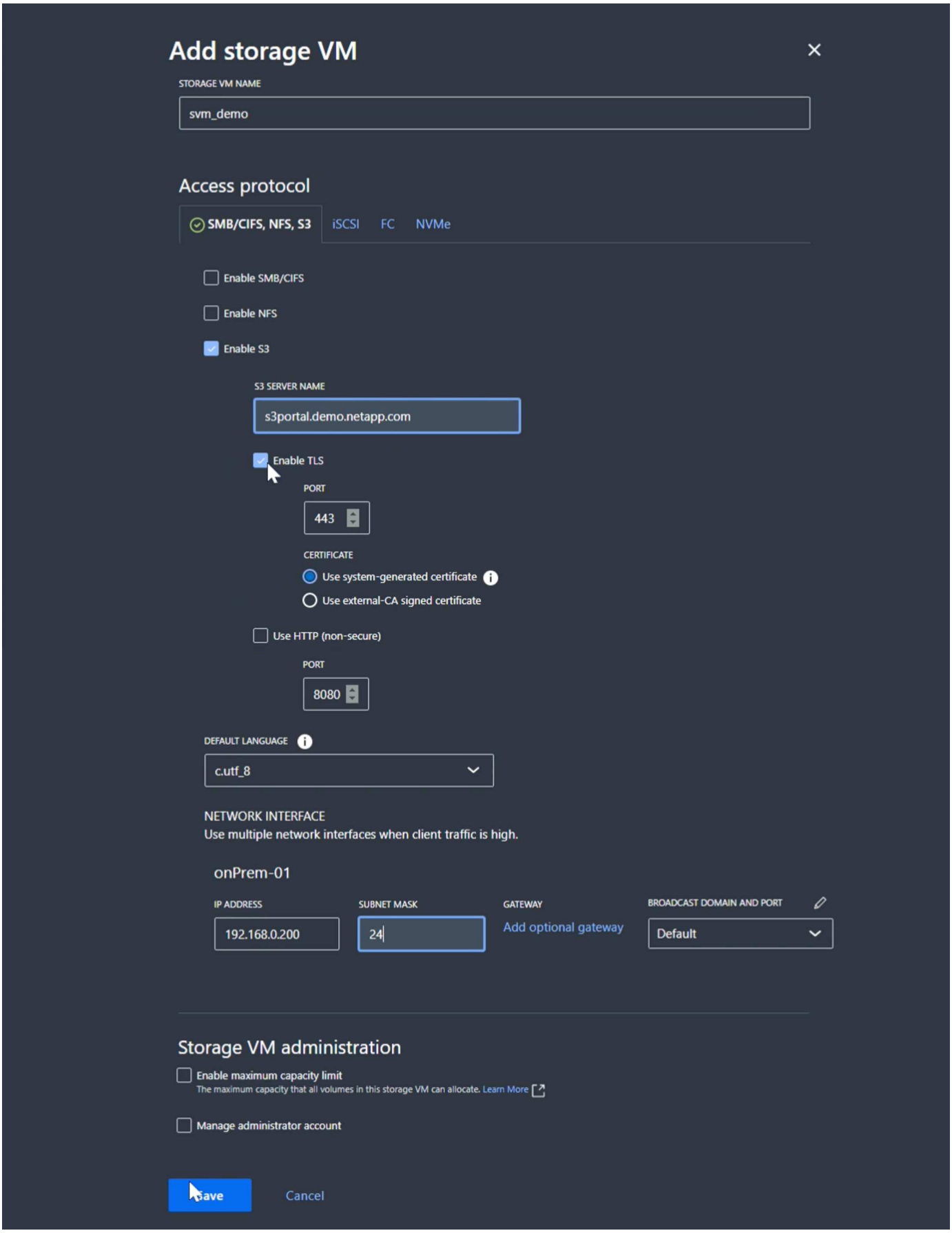
A modo de demostración, crearemos un servidor de almacén de objetos SVM, un usuario, un grupo, una política de grupo y bloques.

Cree el equipo virtual de almacenamiento

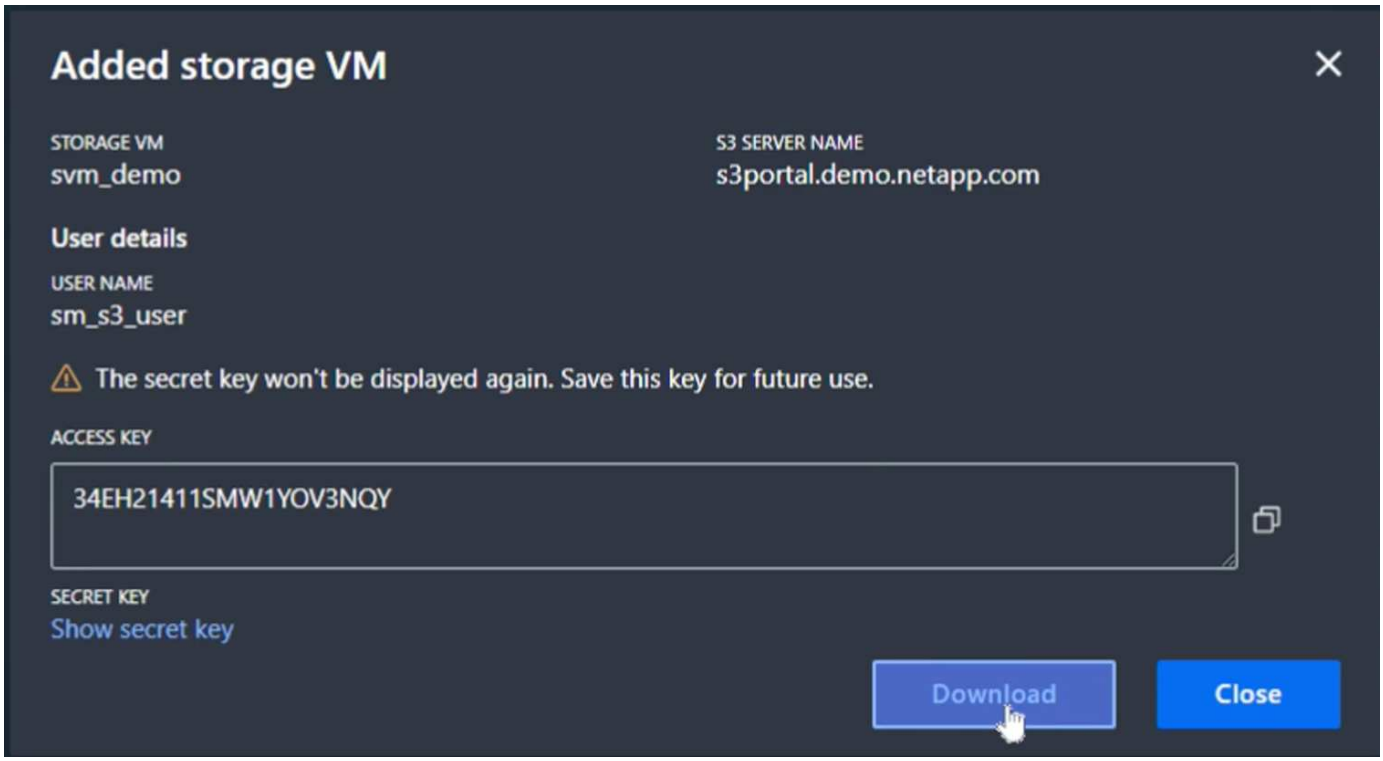
En el administrador del sistema de ONTAP, desplácese hasta Storage VM y añada una nueva máquina virtual de almacenamiento.



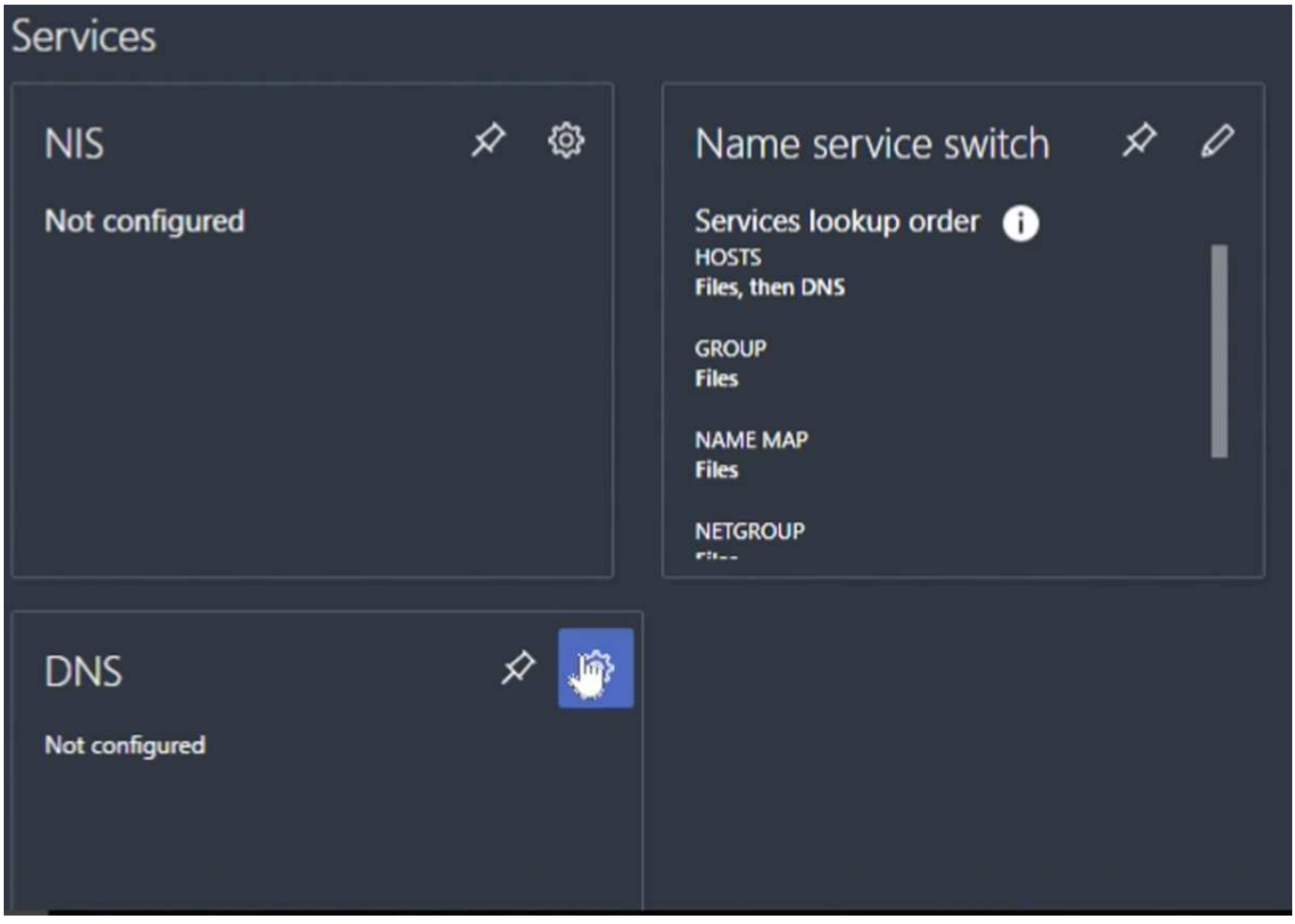
Seleccione las casillas de verificación “Enable S3” y “Enable TLS” y configure los puertos HTTP(S). Defina la IP, la máscara de subred y defina la puerta de enlace y el dominio de difusión si no utiliza el valor predeterminado o necesario en su entorno.



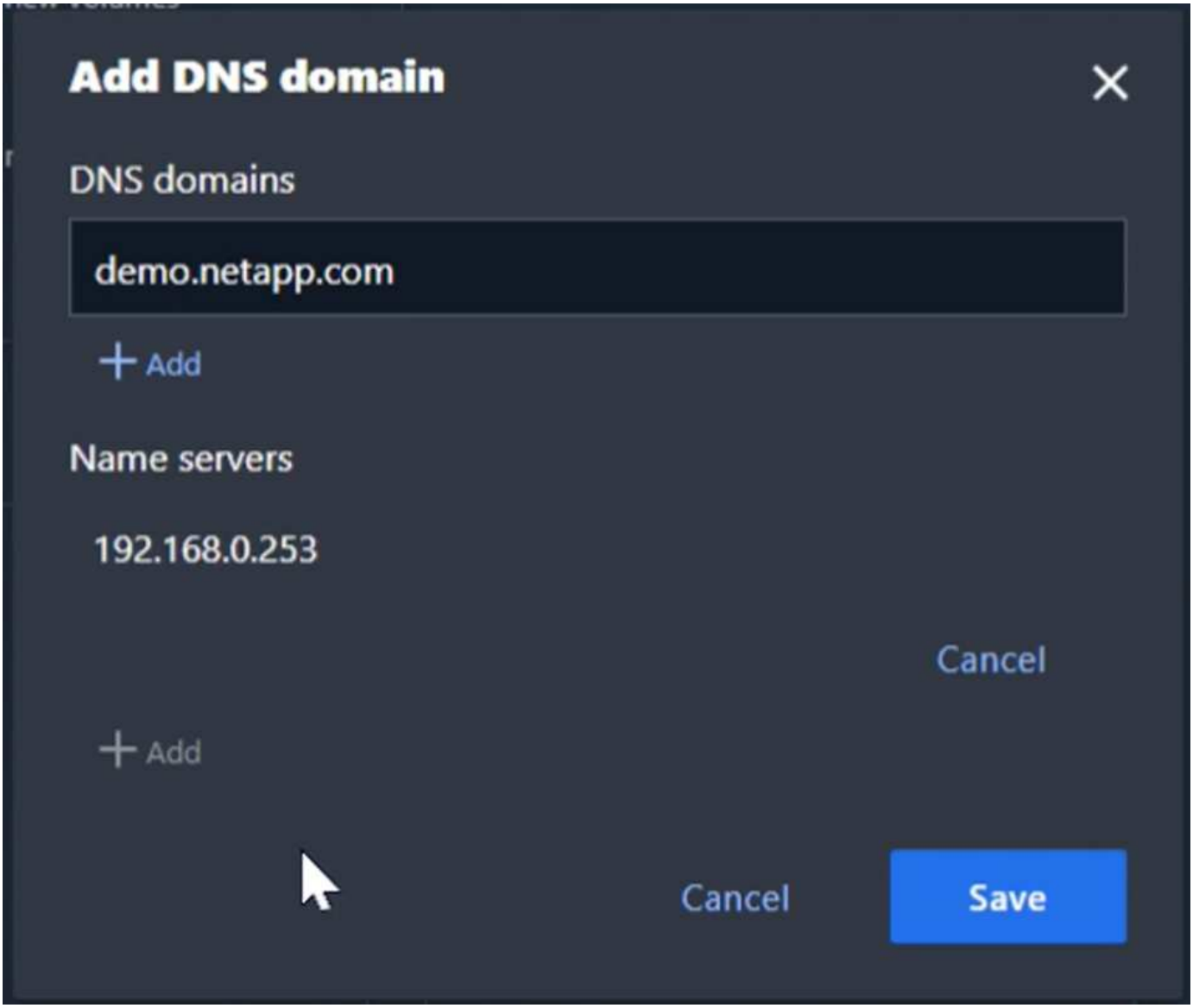
Como parte de la creación de la SVM, se creará un usuario. Descargue las S3 claves para este usuario y cierre la ventana.



Una vez creada la SVM, edite la SVM y añada la configuración de DNS.

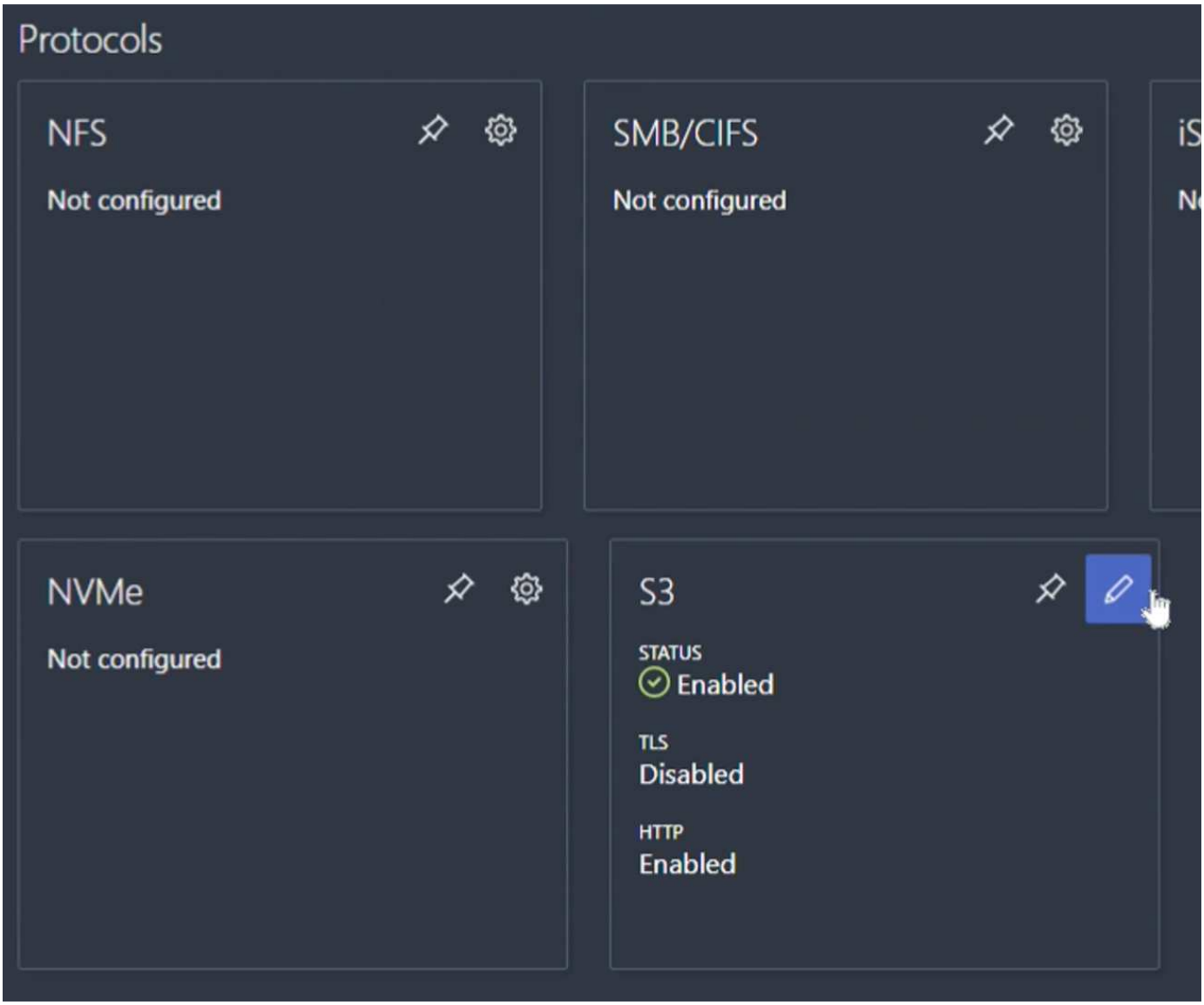


Defina el nombre de DNS y la IP.

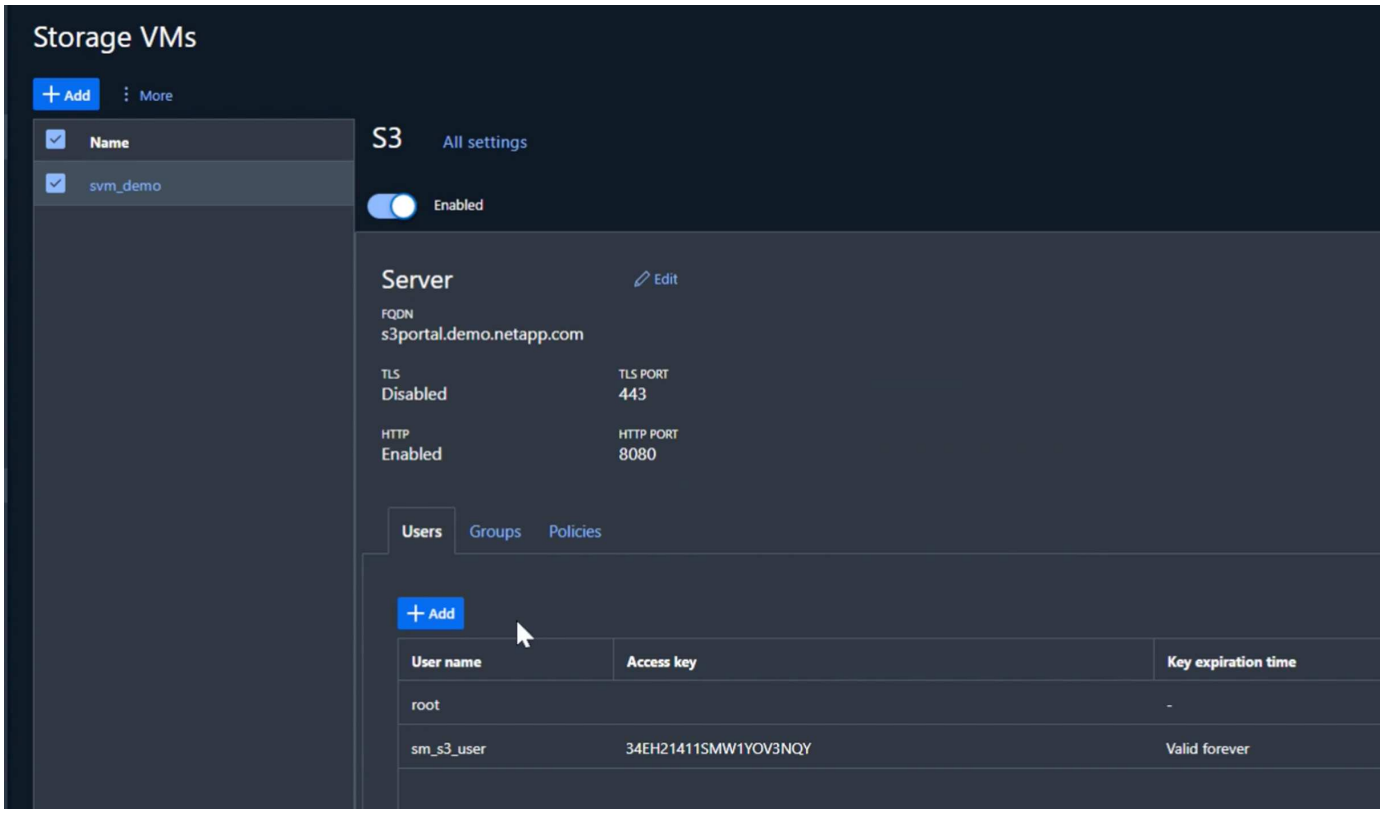


Crear usuario de SVM S3

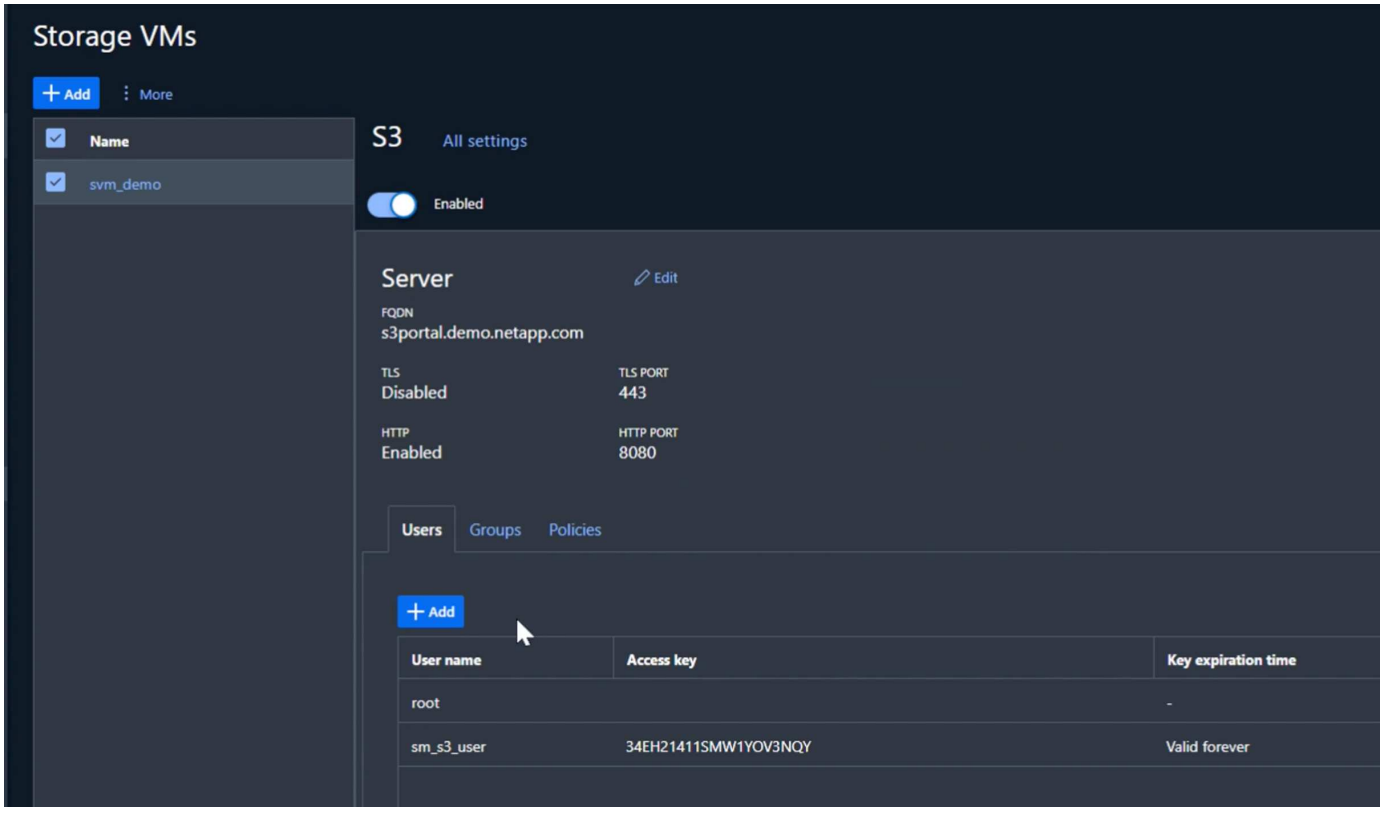
Ahora podemos configurar los S3 usuarios y el grupo. Edite la configuración de S3.



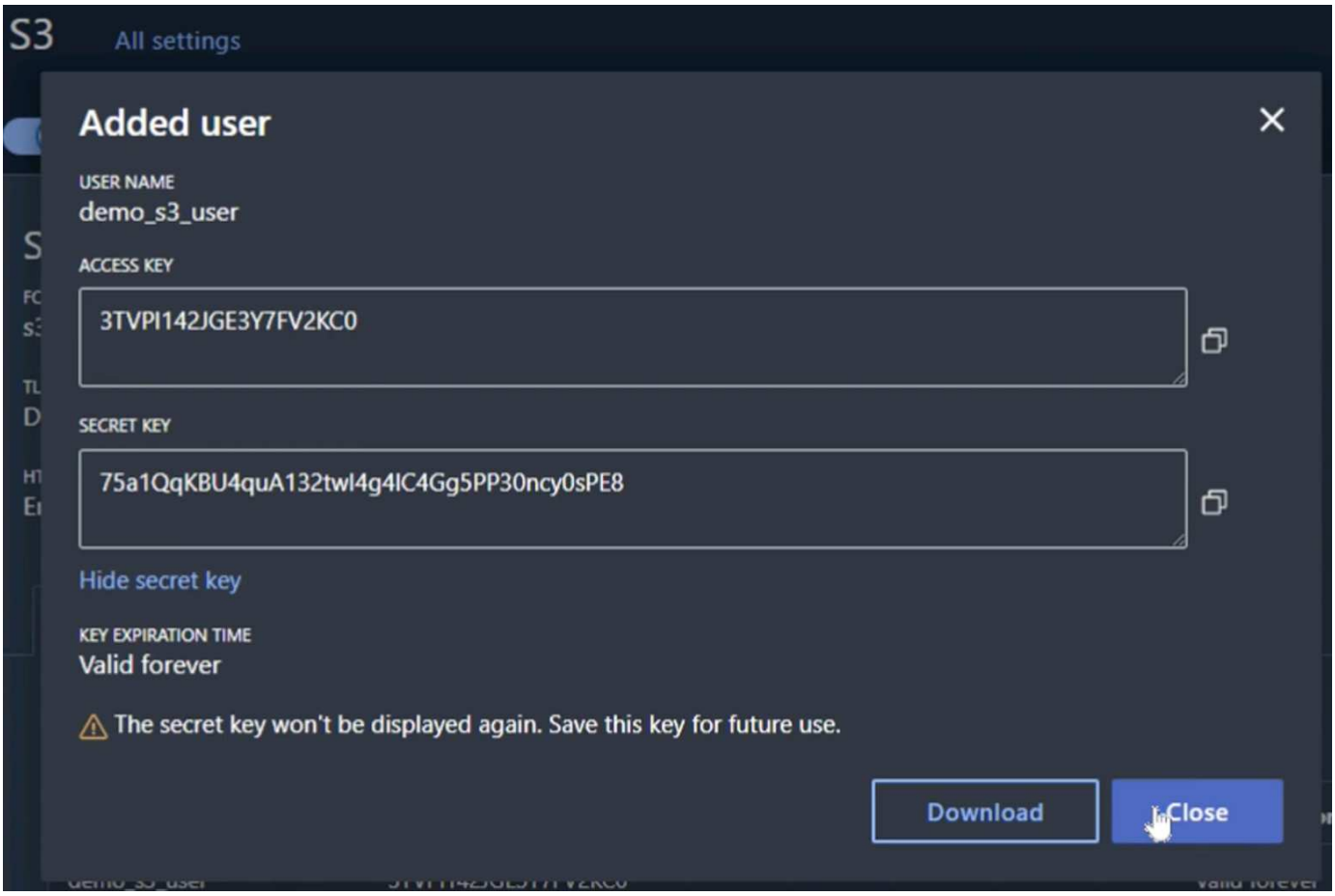
Agregar un nuevo usuario.



Introduzca el nombre de usuario y la caducidad de la clave.

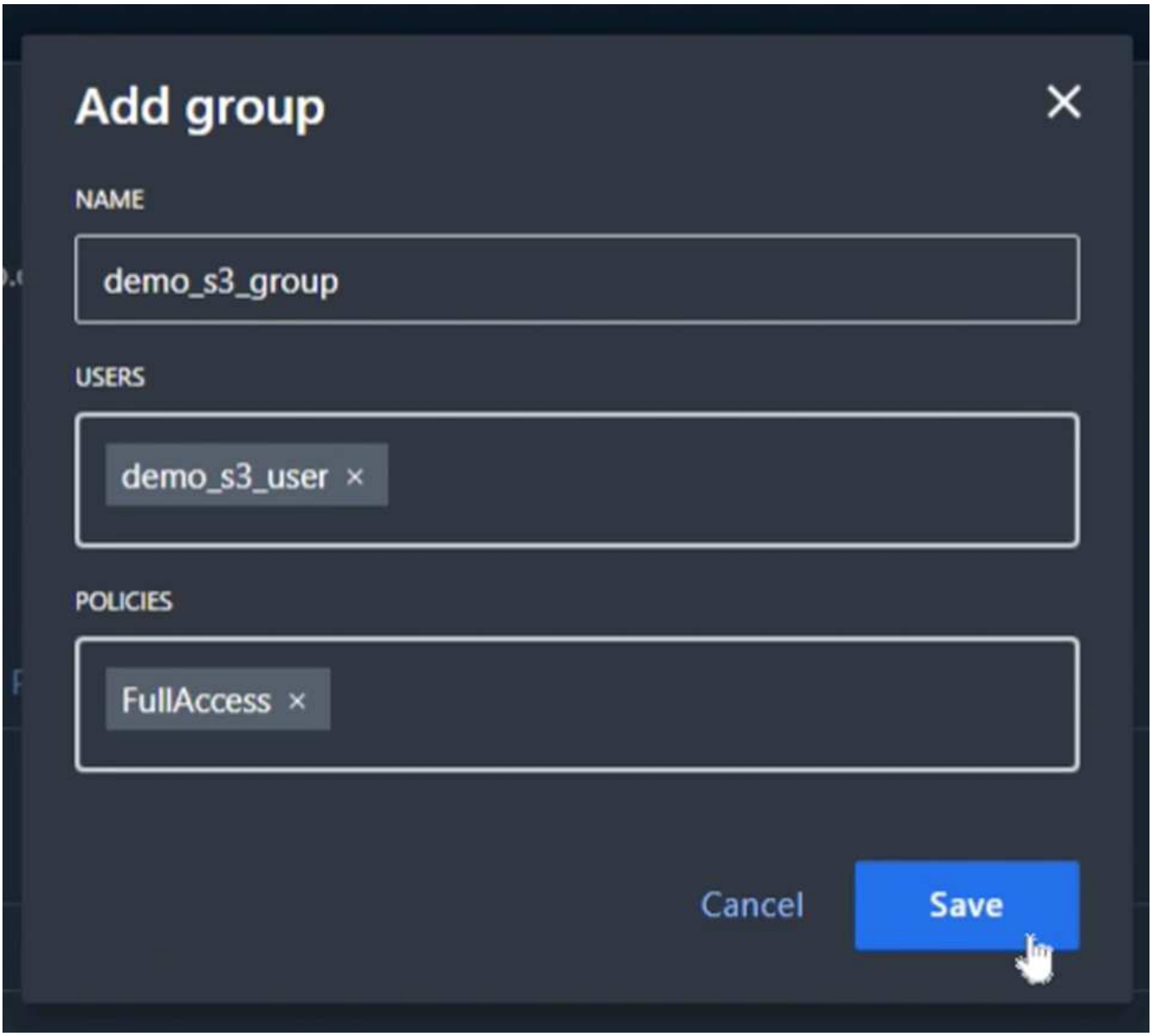


Descargue las S3 claves para el nuevo usuario.



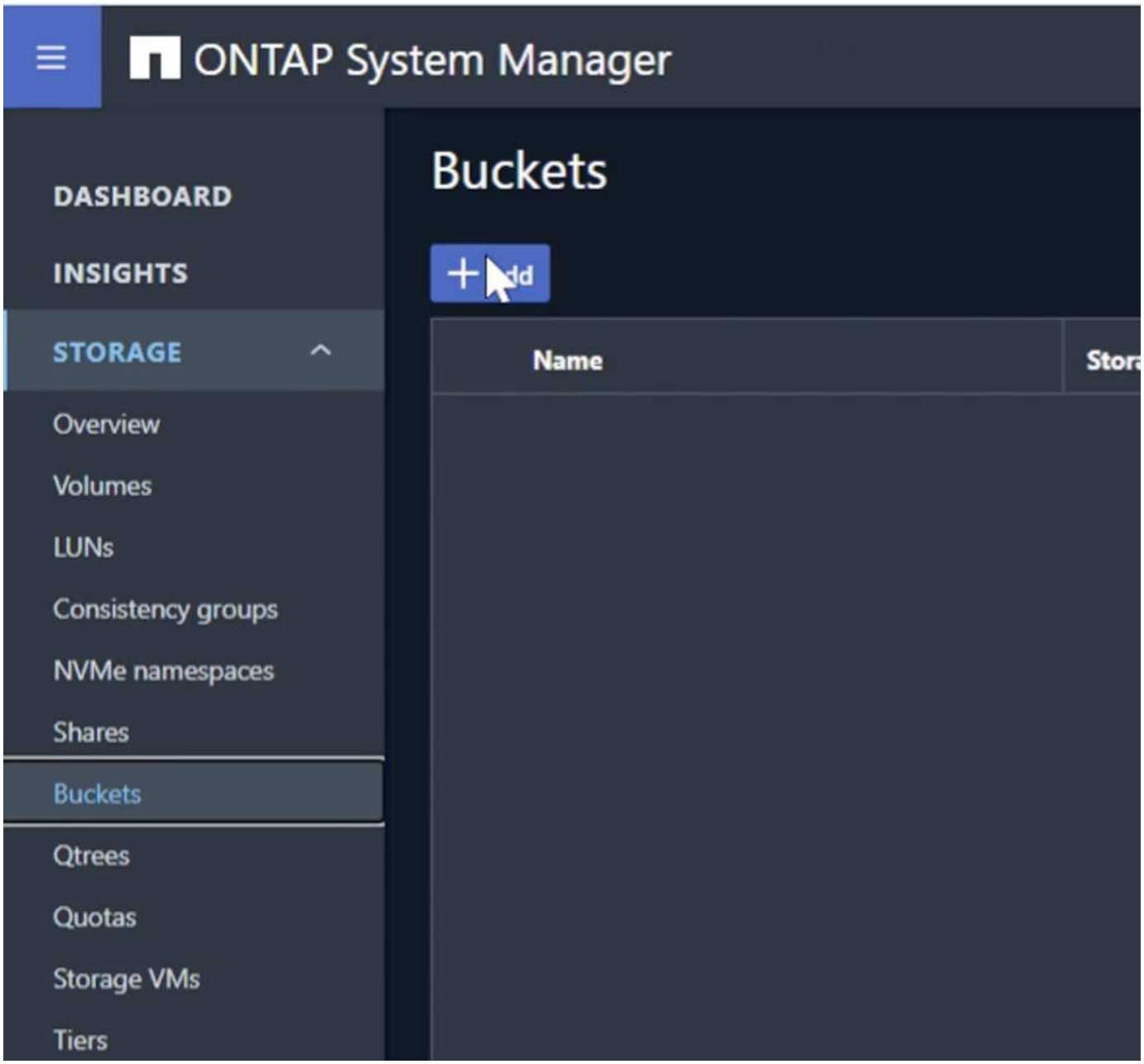
Cree un grupo de SVM S3

En la pestaña Groups de la configuración de SVM S3, añada un nuevo grupo con el usuario creado anteriormente y los permisos de acceso completo.

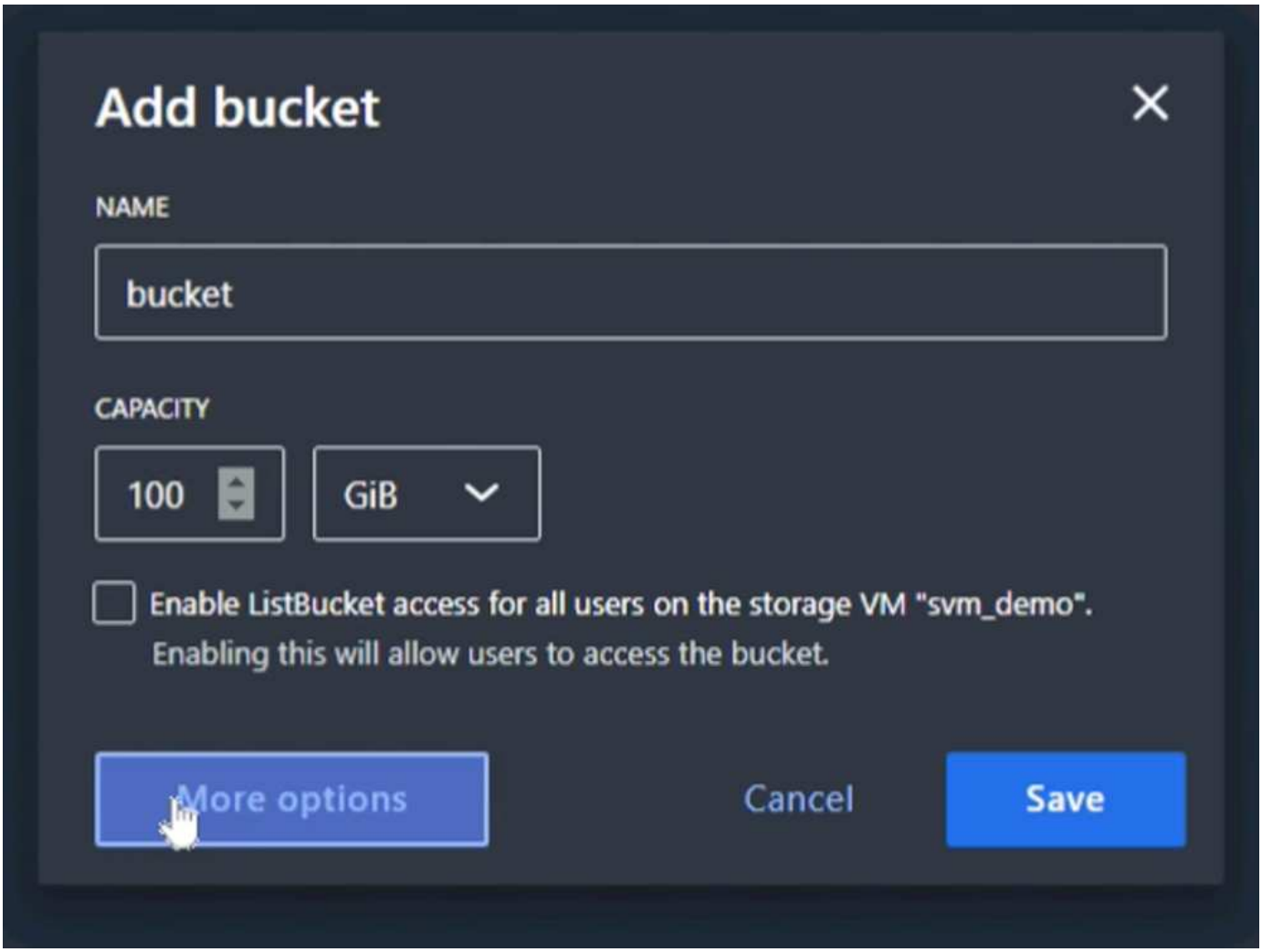


Crear bloques de SVM S3

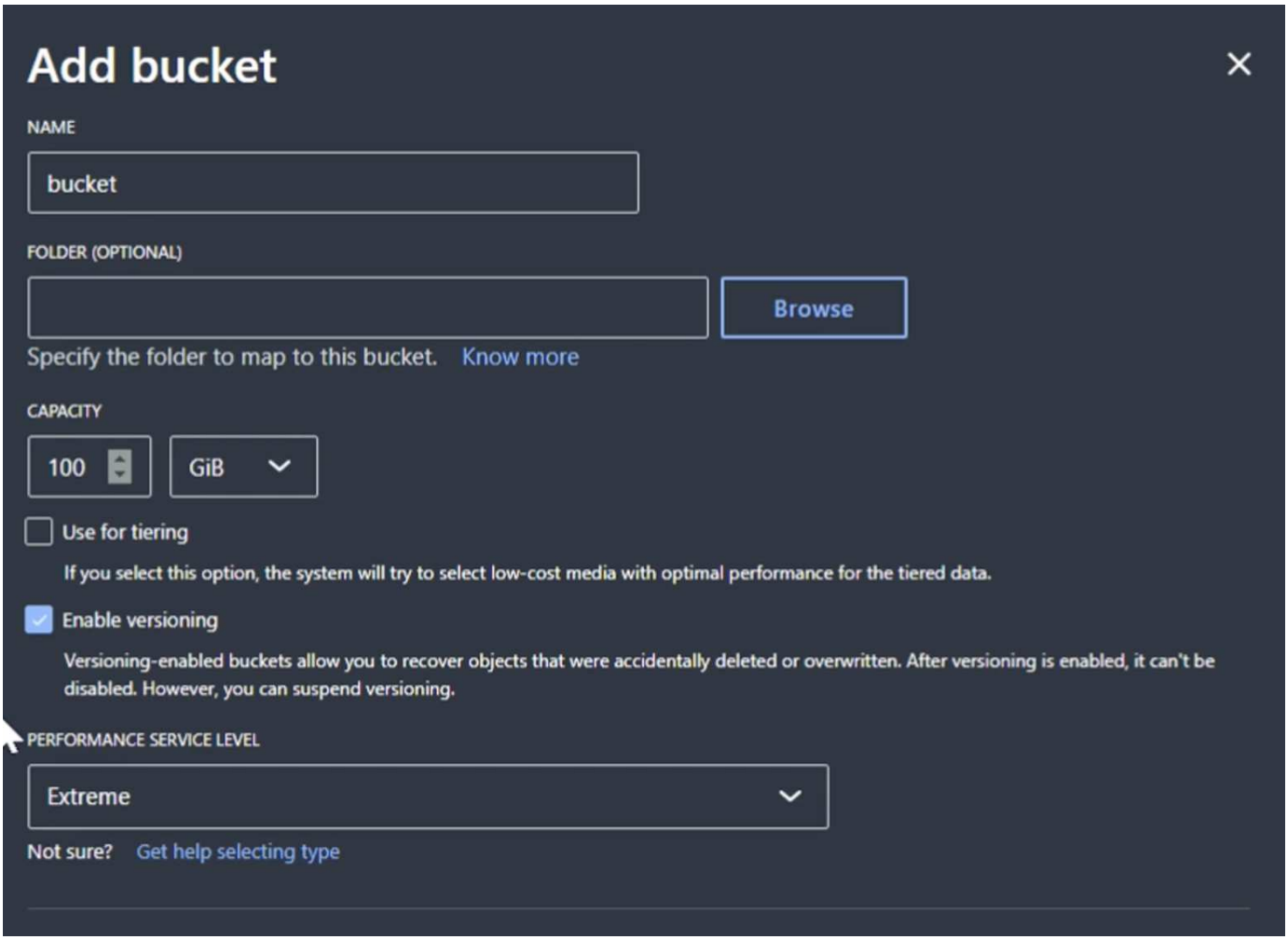
Navegue a la sección Buckets y haga clic en el botón «+Add».



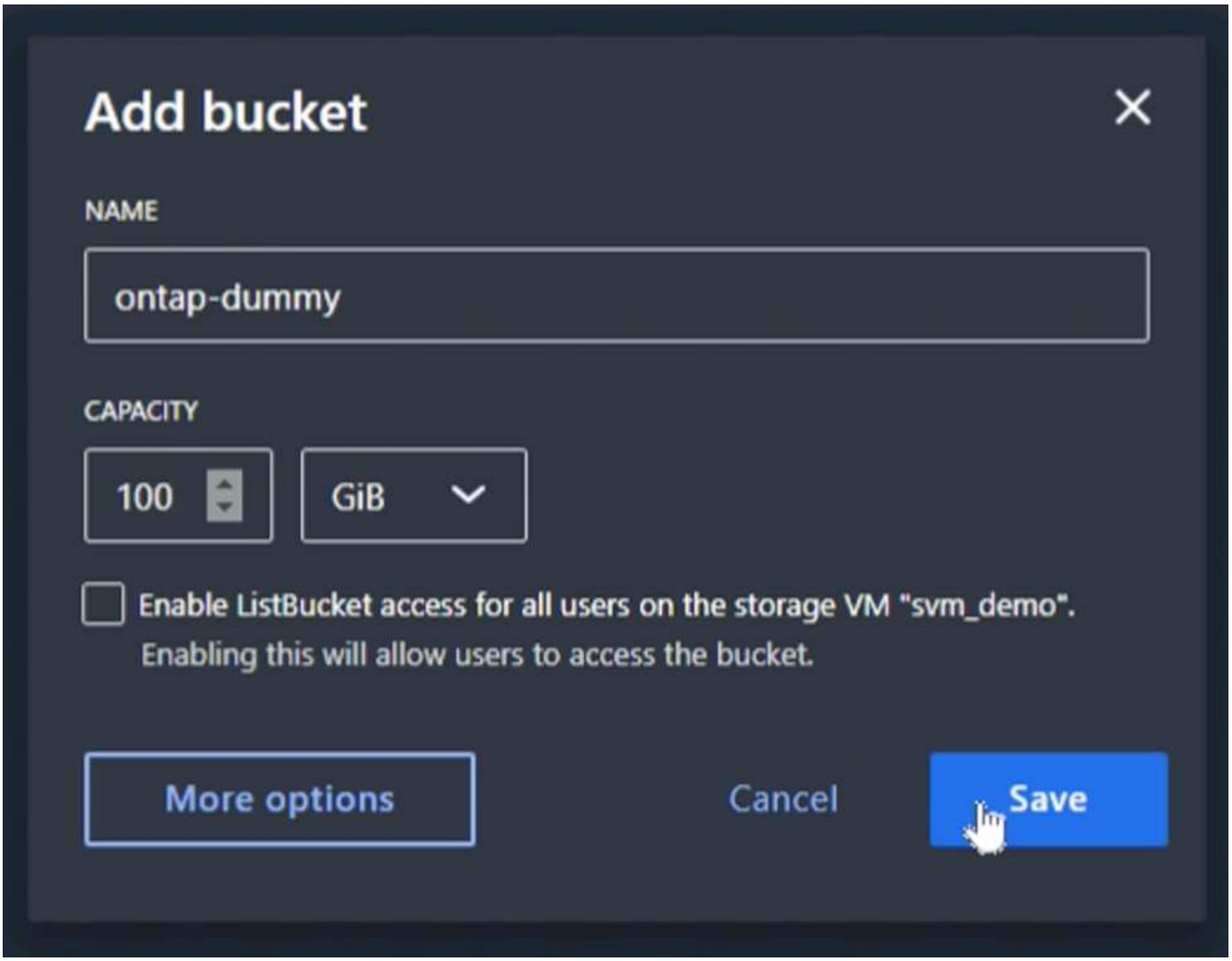
Se introduce un nombre, una capacidad y se anula la selección de la casilla de comprobación Enable ListBucket access… y se hace clic en el botón «More options».



En la sección «Más opciones», seleccione la casilla de verificación Activar control de versiones y haga clic en el botón «Guardar».



Repita el proceso y cree un segundo depósito sin el control de versiones activado. Se introduce un nombre, la misma capacidad que el bloque uno y se anula la selección de la casilla de comprobación Enable ListBucket access… y se hace clic en el botón «Save».



Por Rafael Guedes, y Aron Klein

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

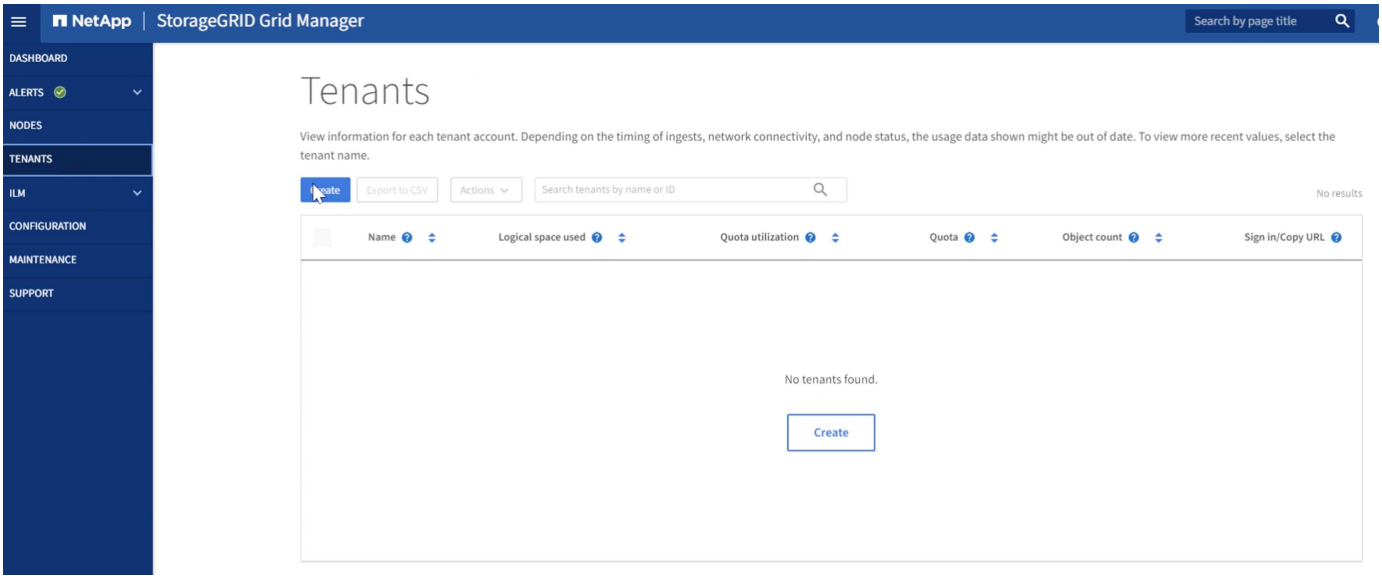
Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Preparando StorageGRID

Continuando con la configuración de esta demostración, crearemos un inquilino, un usuario, un grupo de seguridad, una política de grupo y un bucket.

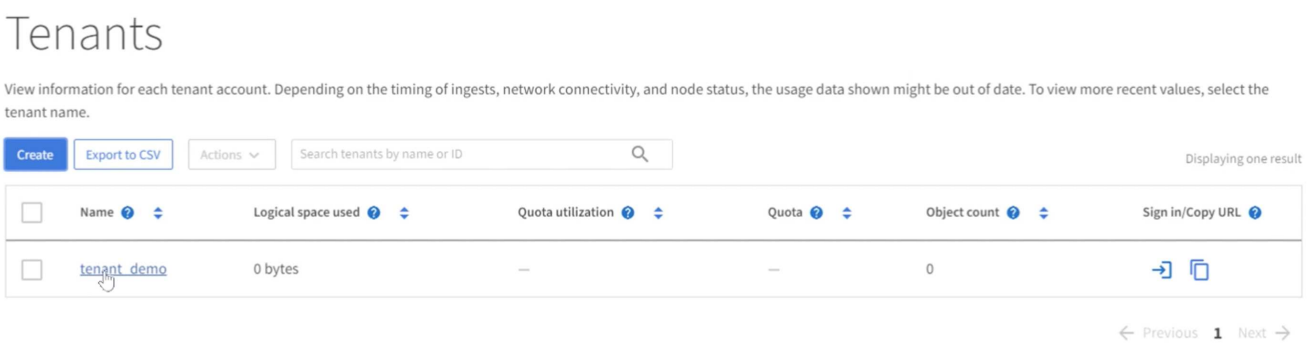
Cree el inquilino

Vaya a la pestaña «Tenentes» y haga clic en el botón «Crear»

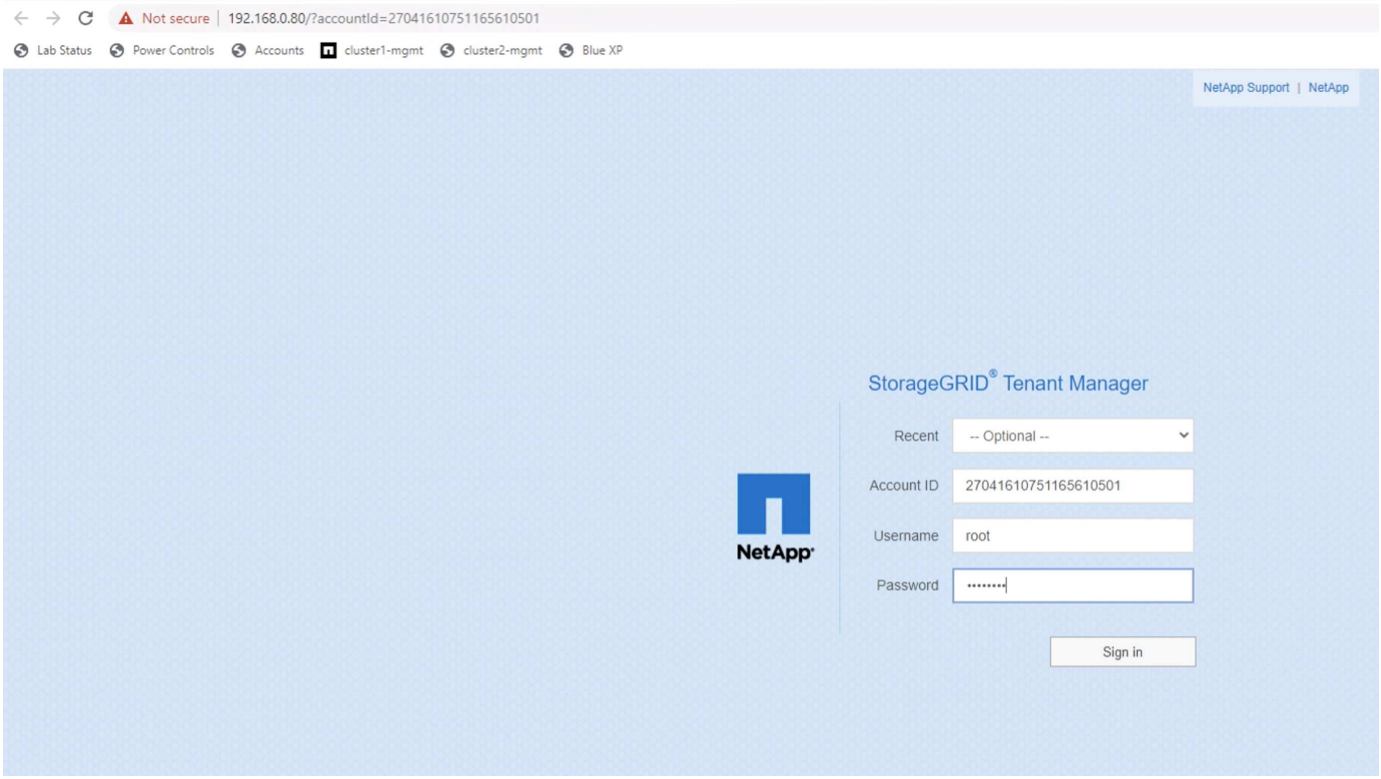


Rellene los detalles del arrendatario que proporciona un nombre de arrendatario, seleccione S3 para el tipo de cliente y no se requiere ninguna cuota. No es necesario seleccionar servicios de plataforma ni permitir S3 SELECT. Si lo desea, puede utilizar el origen de identidad propio. Establezca la contraseña root y haga clic en el botón Finalizar.

Haga clic en el nombre del inquilino para ver los detalles del inquilino. * Necesitará el ID de inquilino más tarde, así que cópielo*. Haga clic en el botón Iniciar sesión. Esto le llevará al inicio de sesión del portal de inquilinos. Guarde la URL para usarla en el futuro.

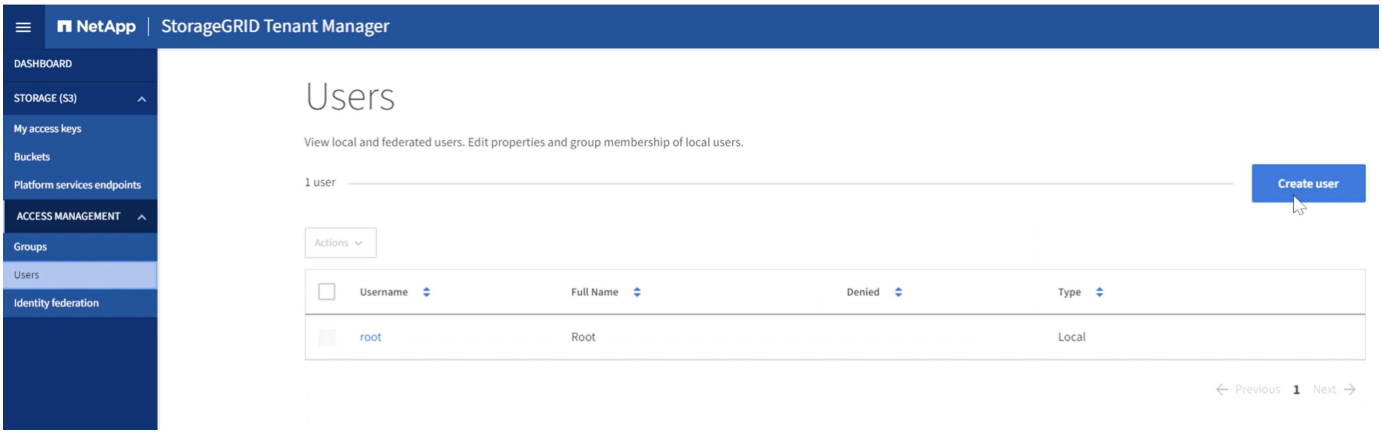


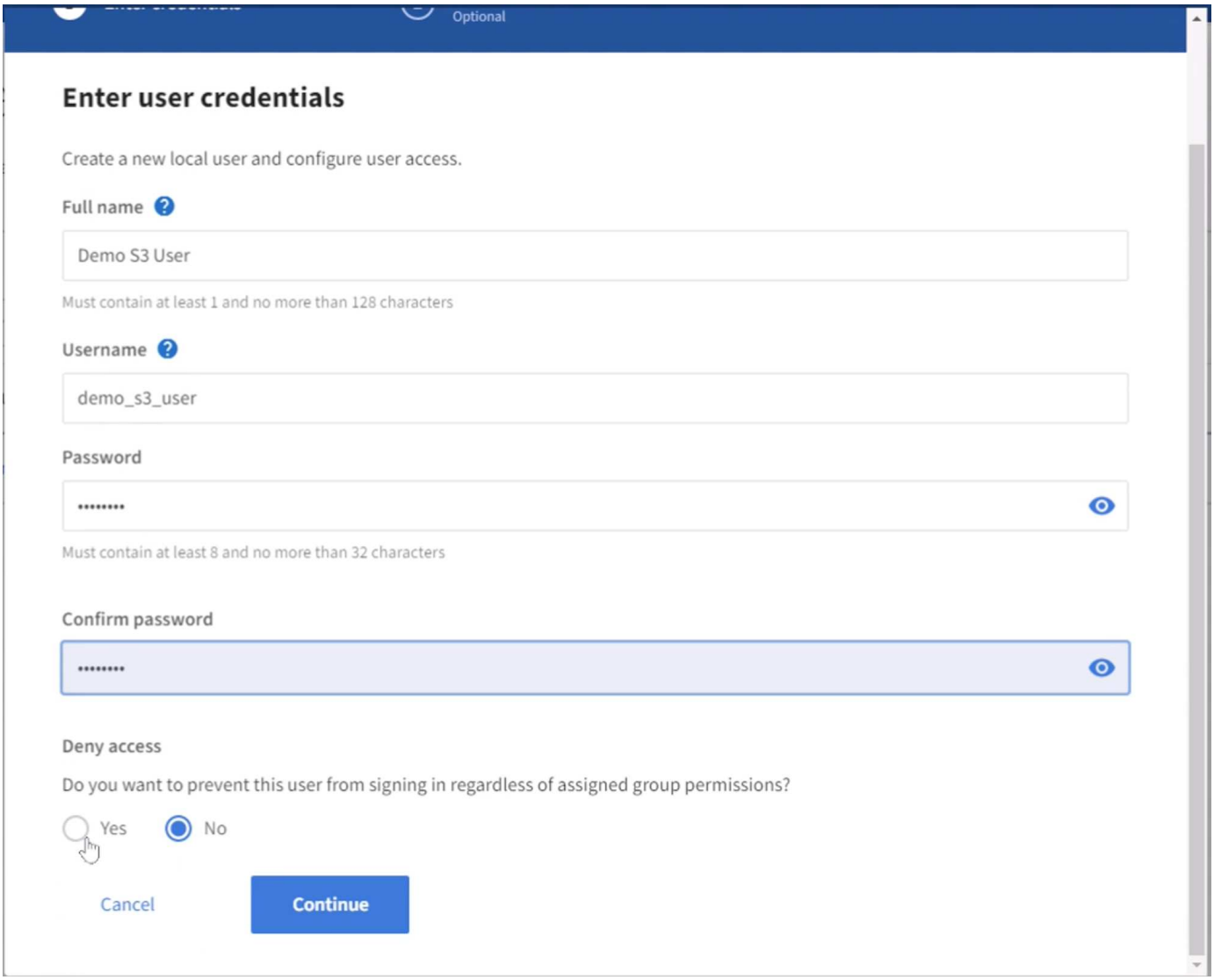
Esto le llevará al inicio de sesión del portal de inquilinos. Guarde la URL para uso futuro e introduzca las credenciales de usuario raíz.



Cree el usuario

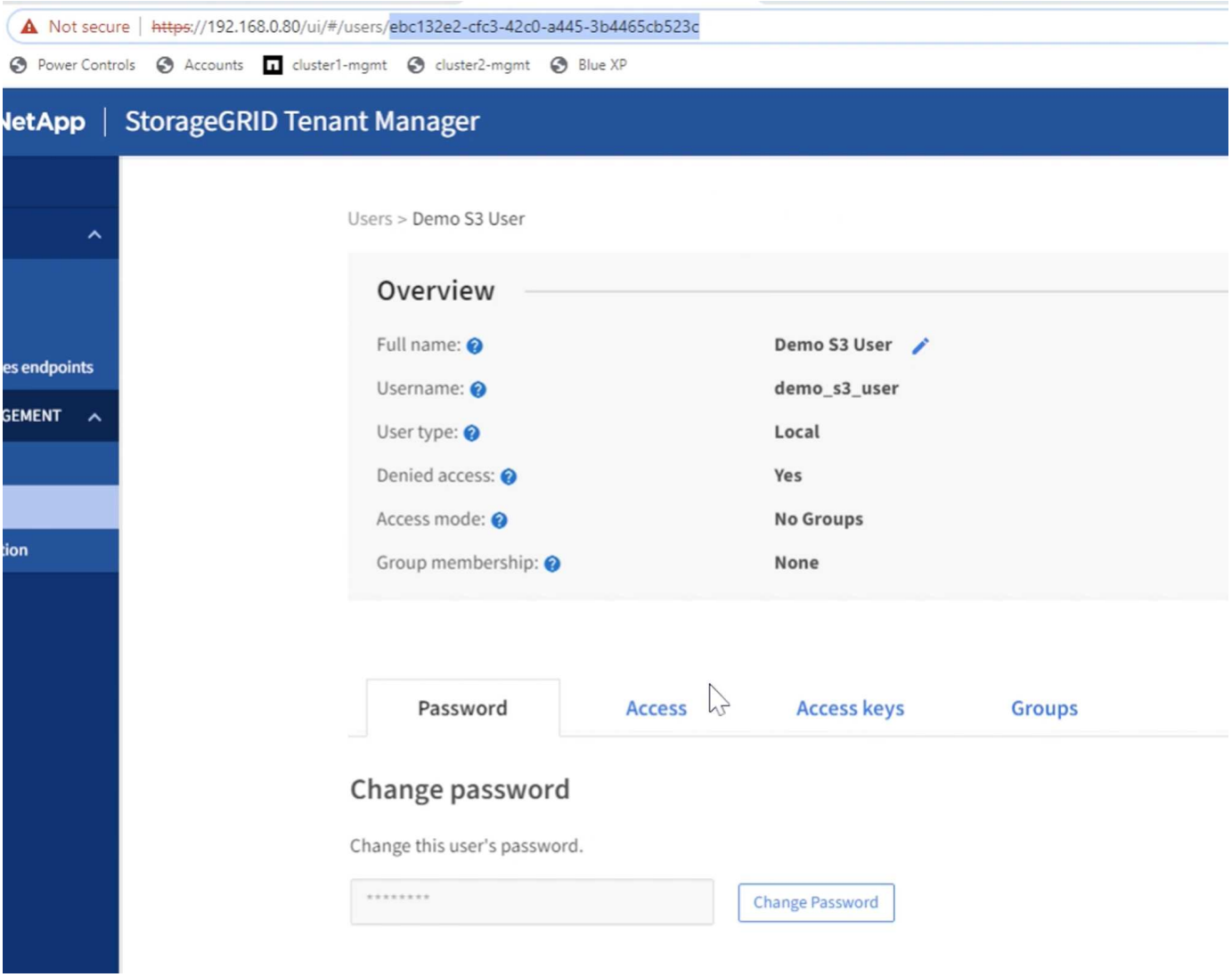
Navegue a la pestaña Usuarios y cree un nuevo usuario.



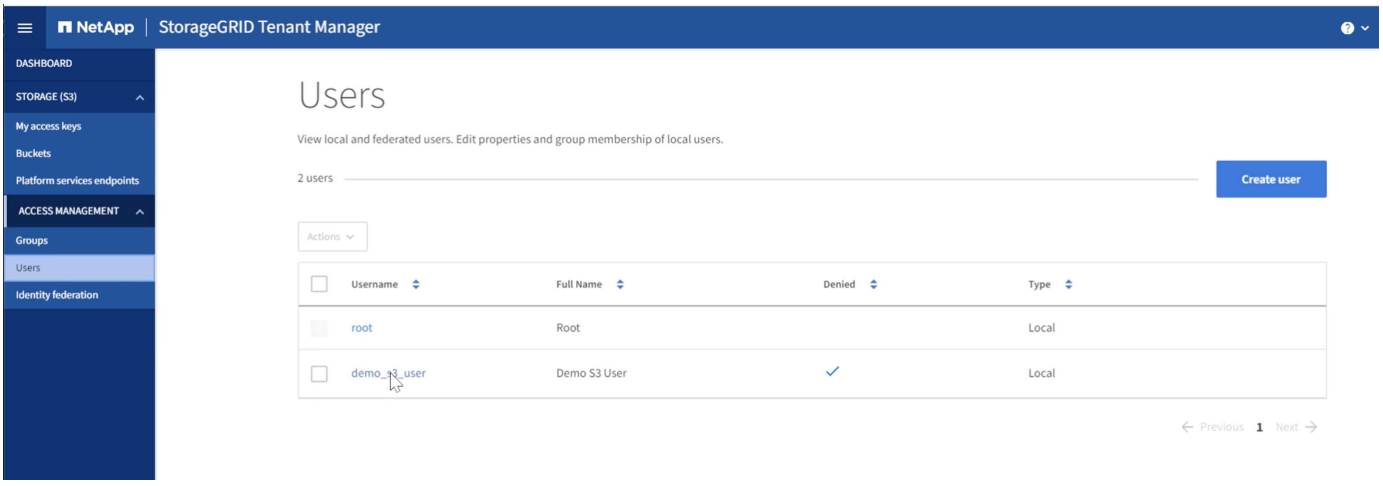


Ahora que se ha creado el nuevo usuario, haga clic en el nombre del usuario para abrir los detalles del usuario.

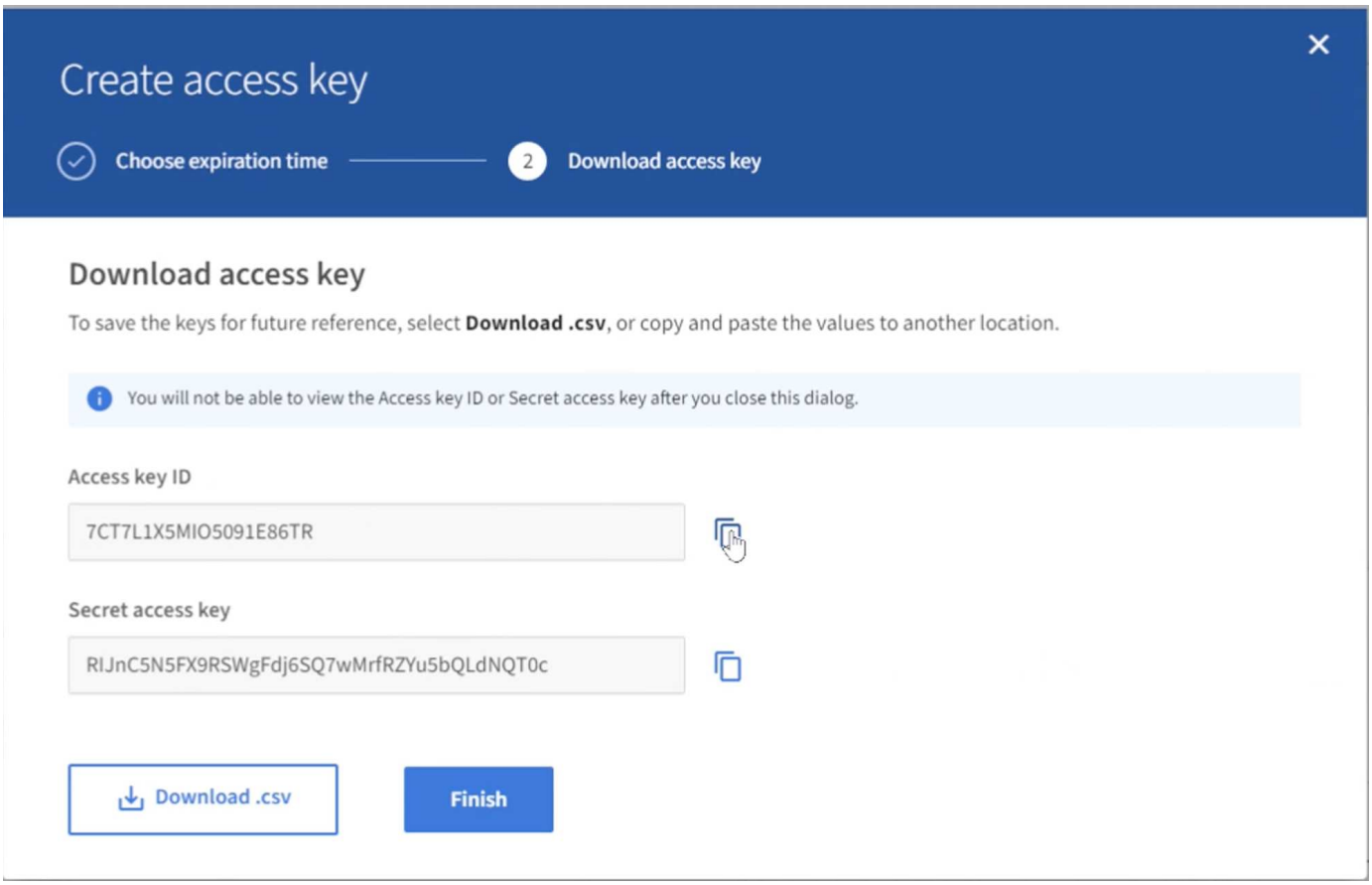
Copie el ID de usuario de la URL que se utilizará más adelante.



Para crear las S3 teclas, haga clic en el nombre de usuario.

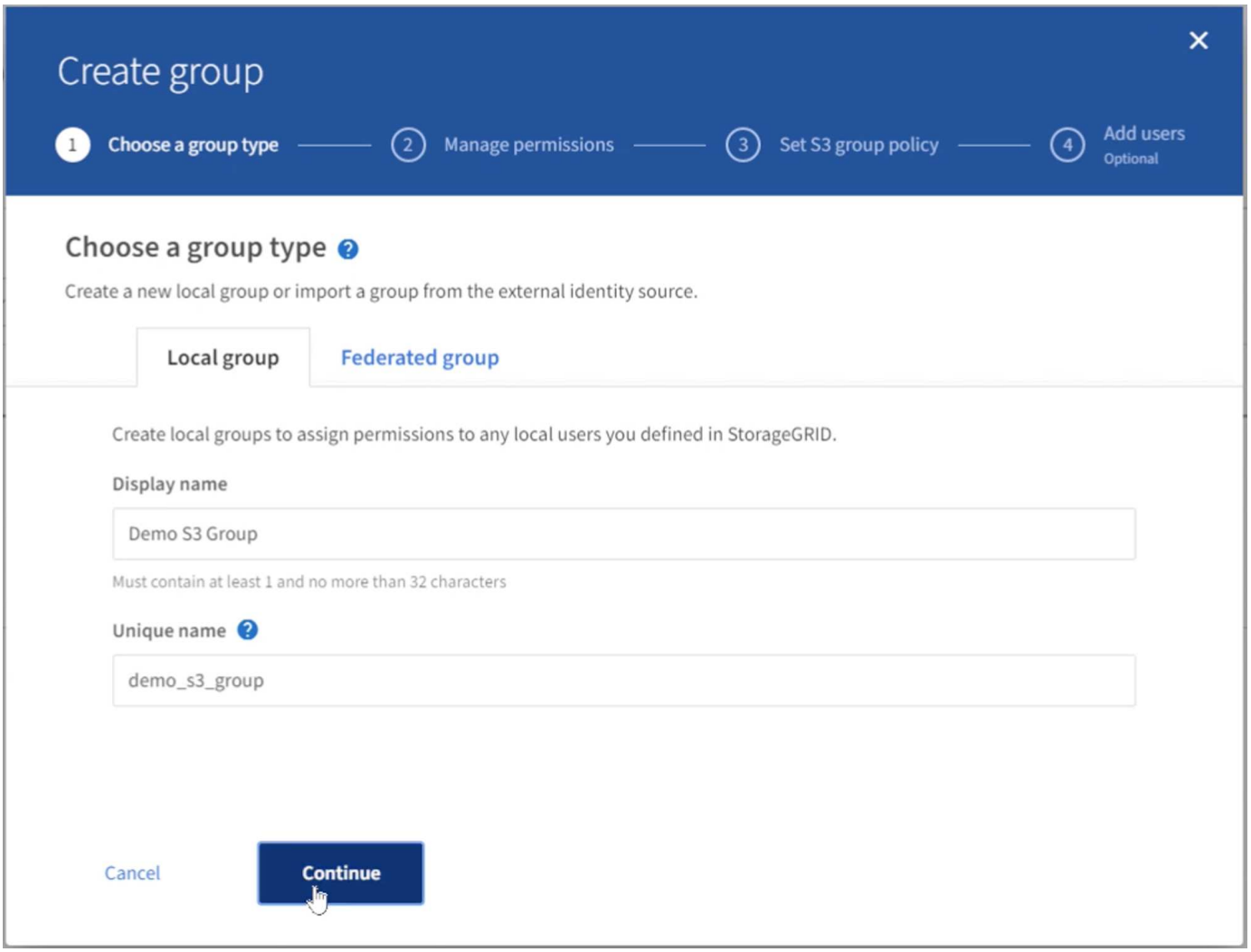


Seleccione la pestaña “Teclas de acceso” y haga clic en el botón “Crear clave”. No es necesario establecer una hora de caducidad. Descargue las S3 claves, ya que no se pueden recuperar de nuevo una vez cerrada la ventana.

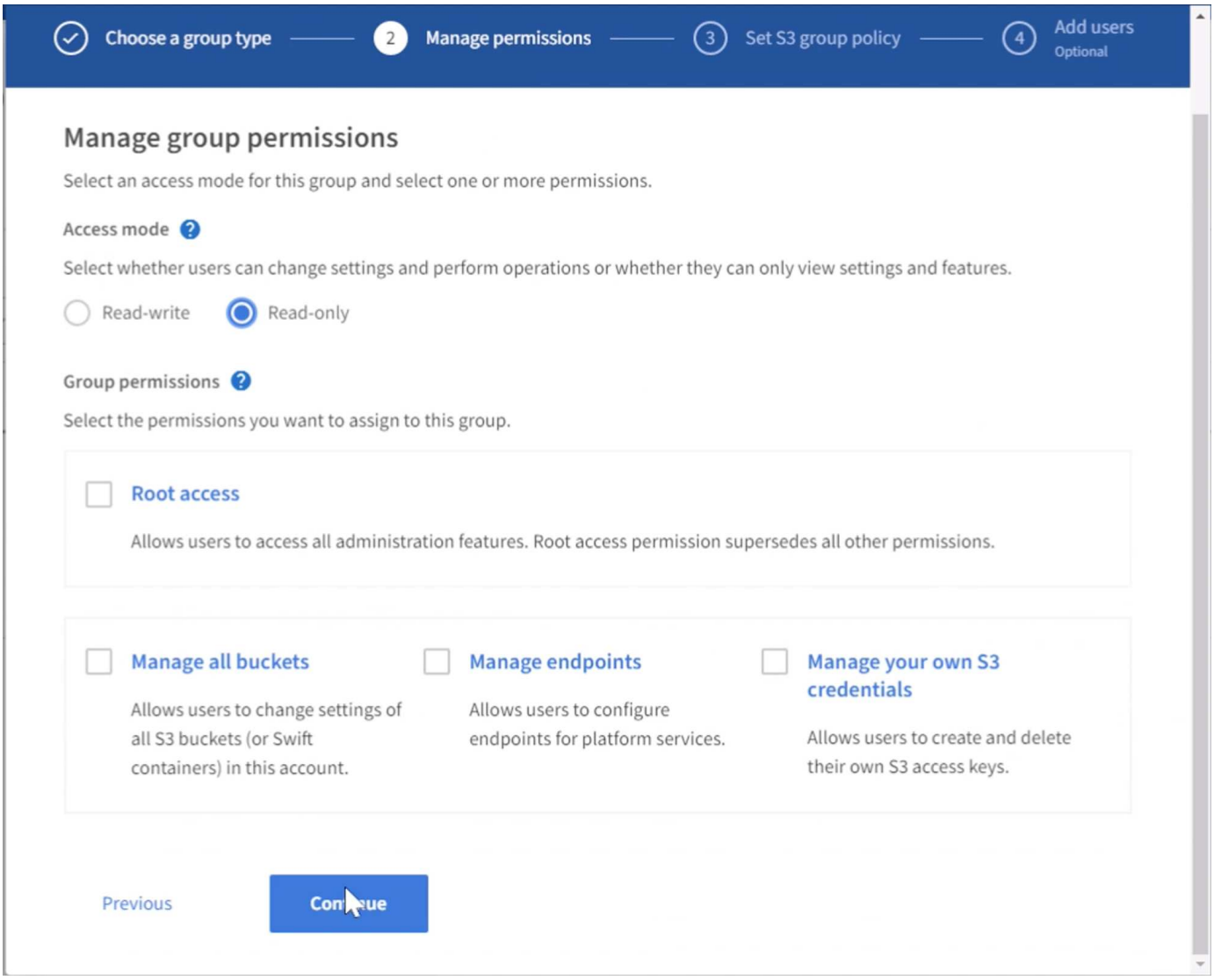


Cree el grupo de seguridad

Ahora vaya a la página Grupos y cree un nuevo grupo.

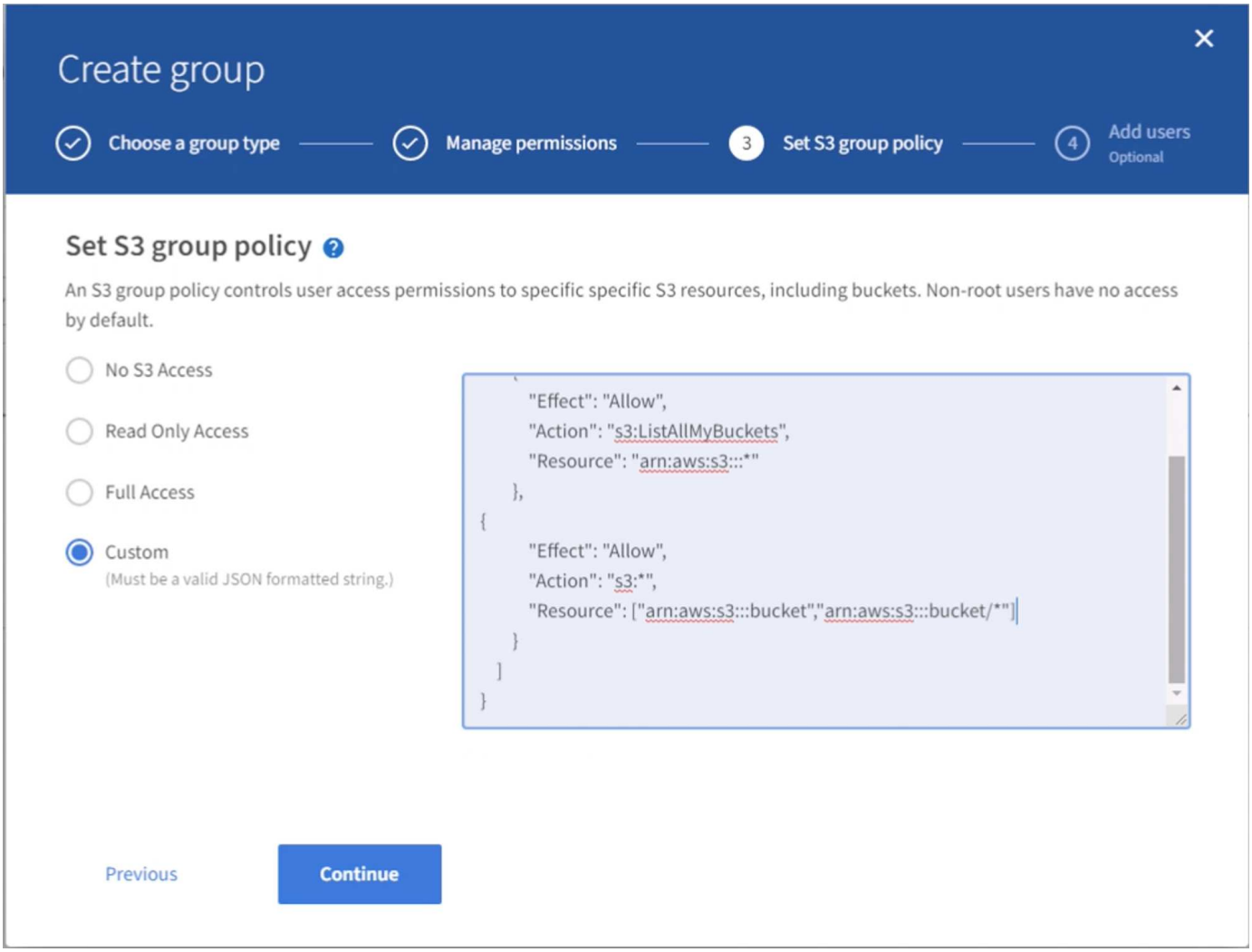


Establezca los permisos de grupo en Sólo lectura. Estos son los permisos de IU del inquilino, no los permisos S3.

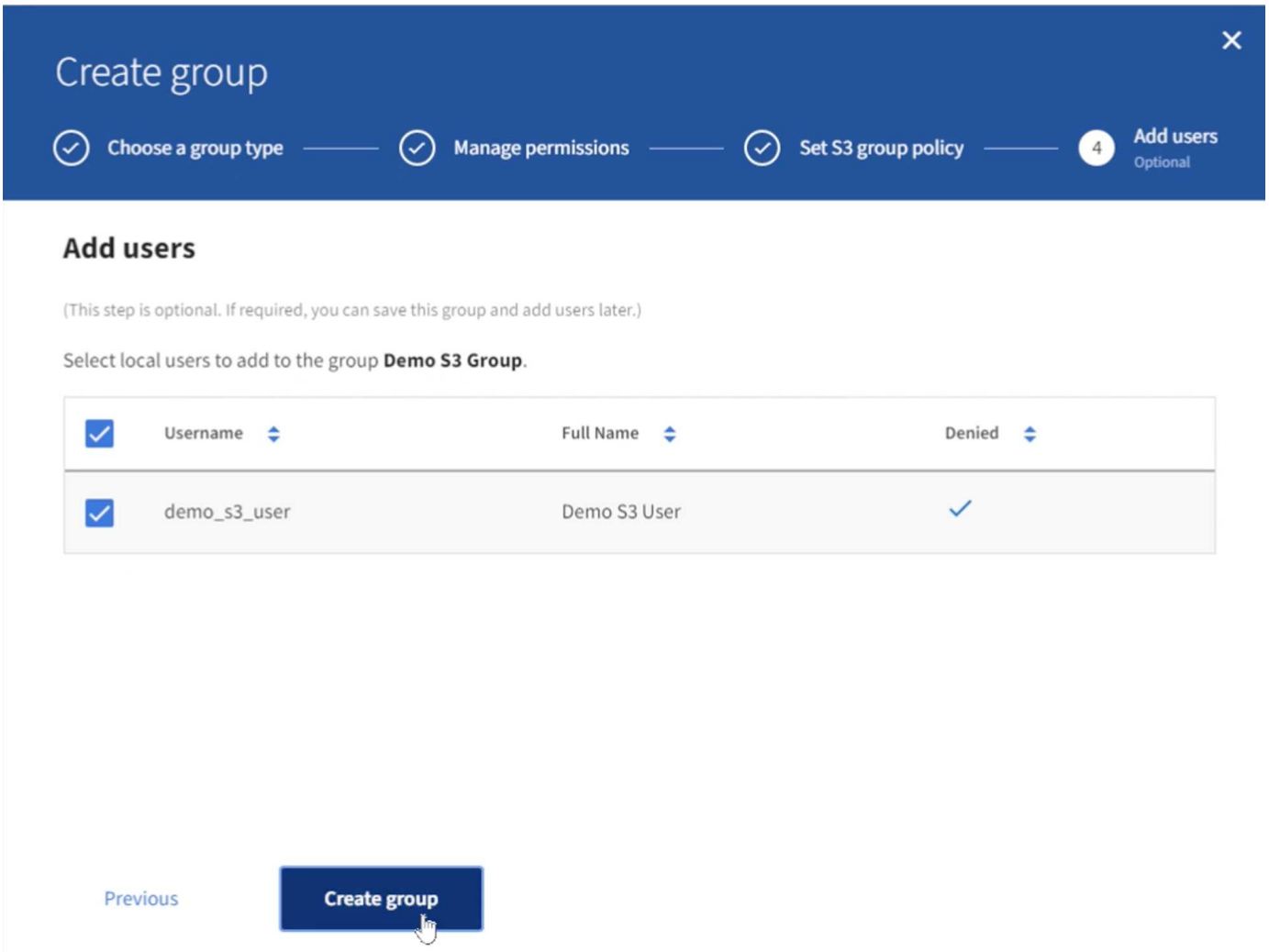


Los permisos S3 se controlan con la directiva de grupo (política de IAM). Establezca la política de grupo en Personalizar y pegue la política json en el cuadro. Esta política permitirá a los usuarios de este grupo enumerar los depósitos del arrendatario y realizar cualquier operación S3 en el depósito denominado «bucket» o subcarpetas del depósito denominado «bucket».

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

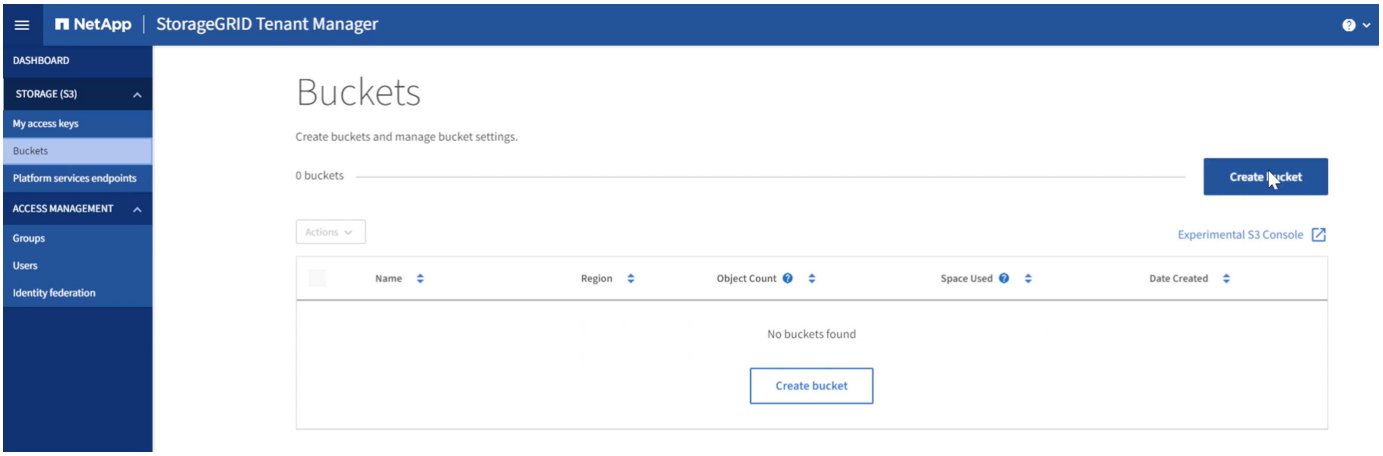


Por último, añadir el usuario al grupo y terminar.

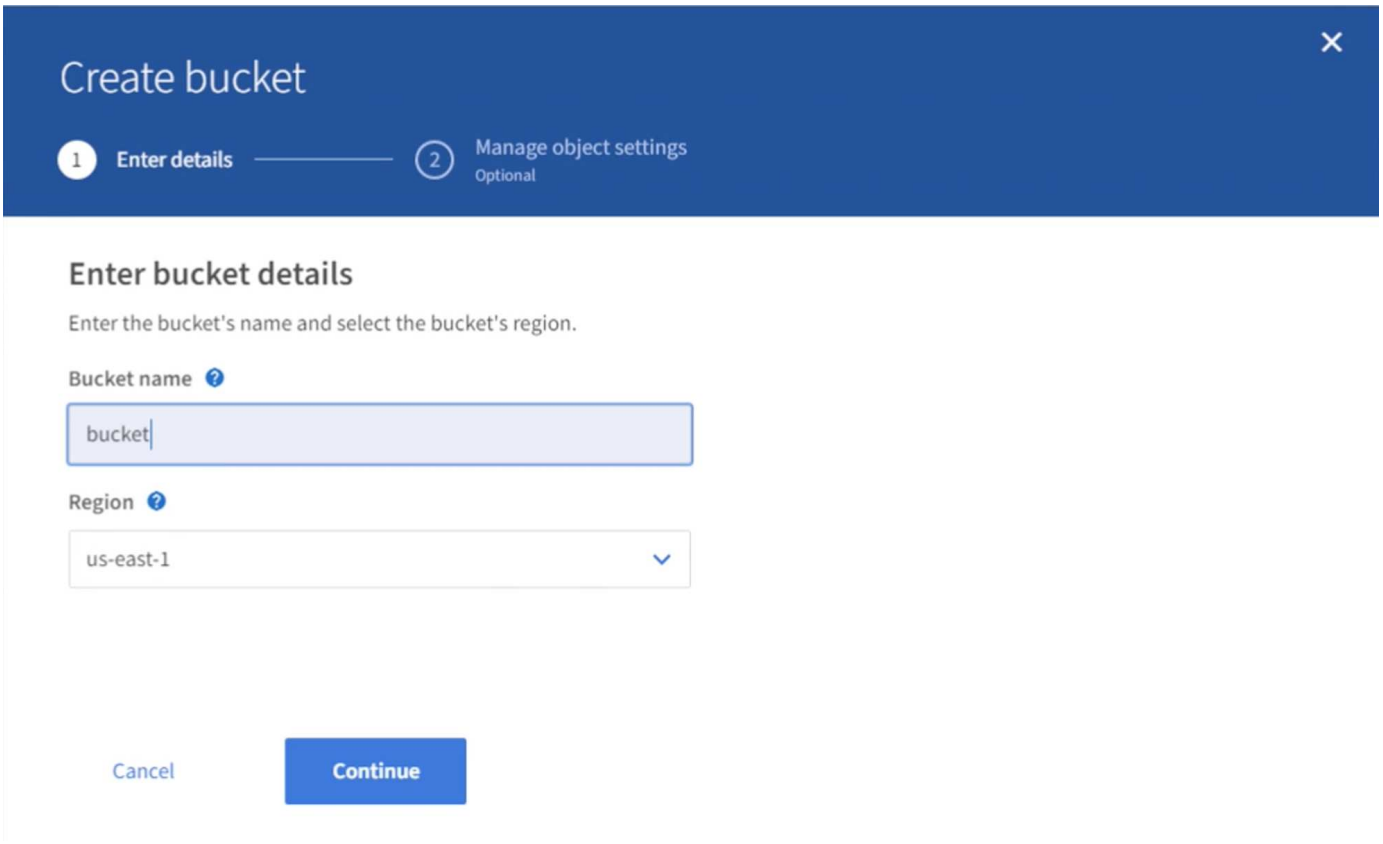


Cree dos cubos

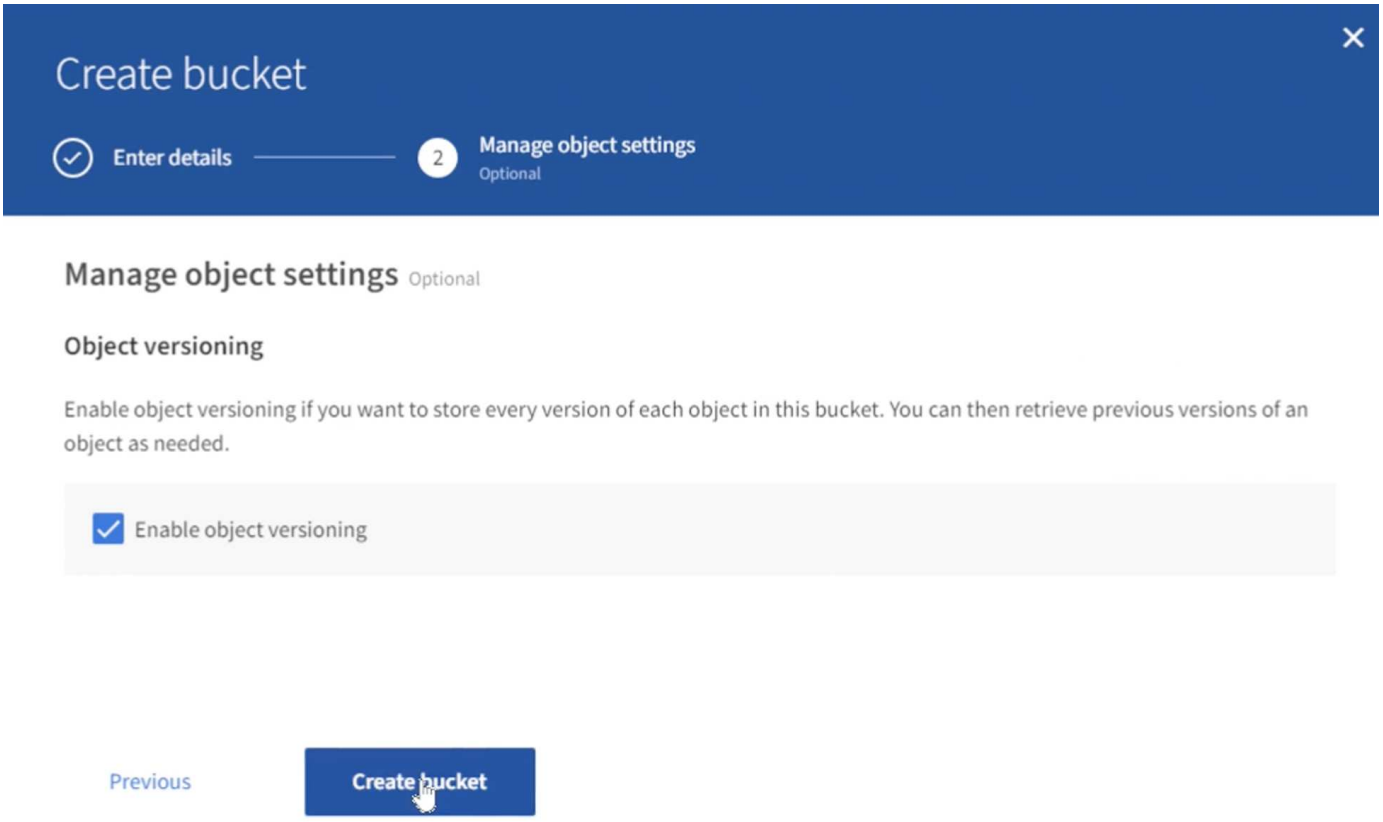
Navegue a la pestaña CUADROS y haga clic en el botón Crear CUCHO.



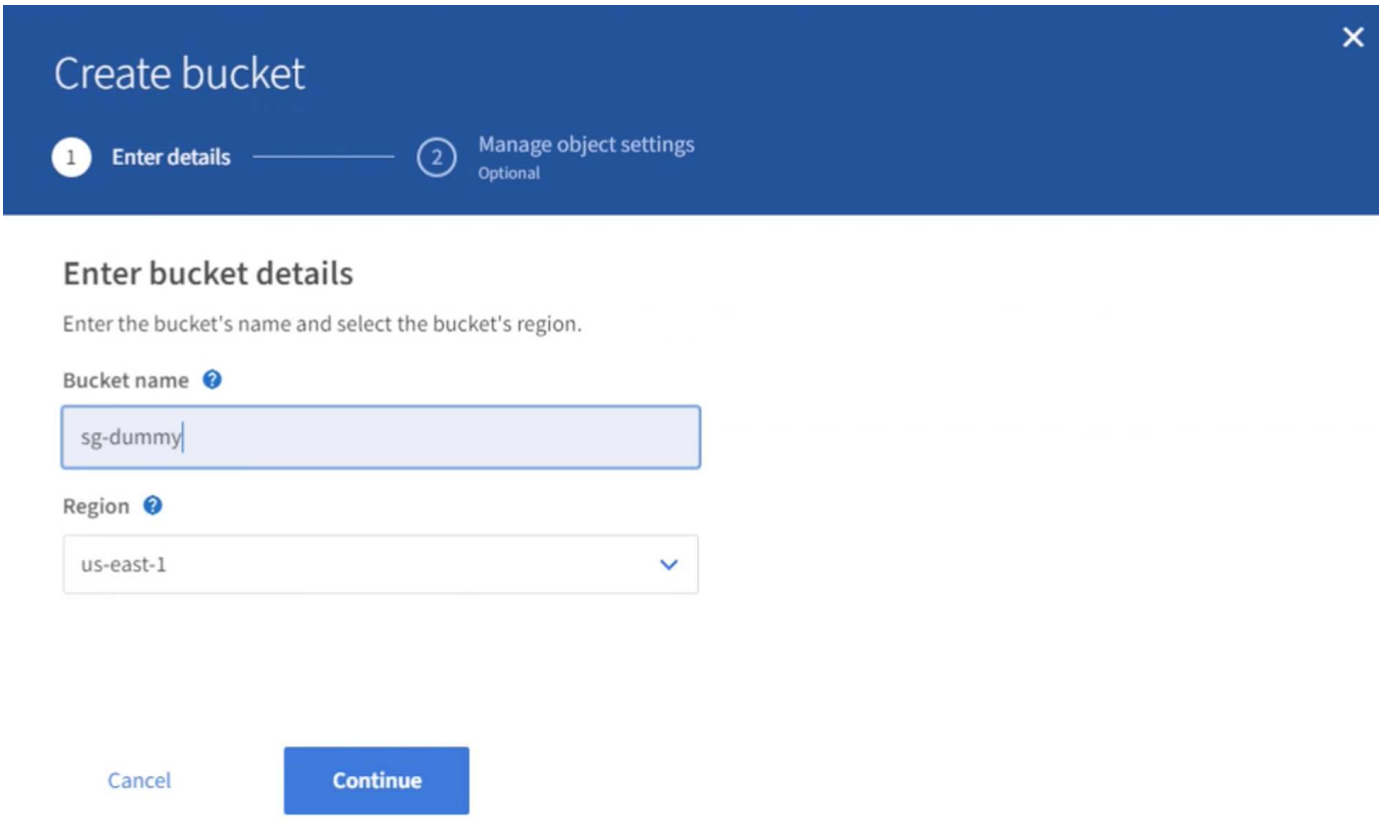
Defina el nombre y la región del período.



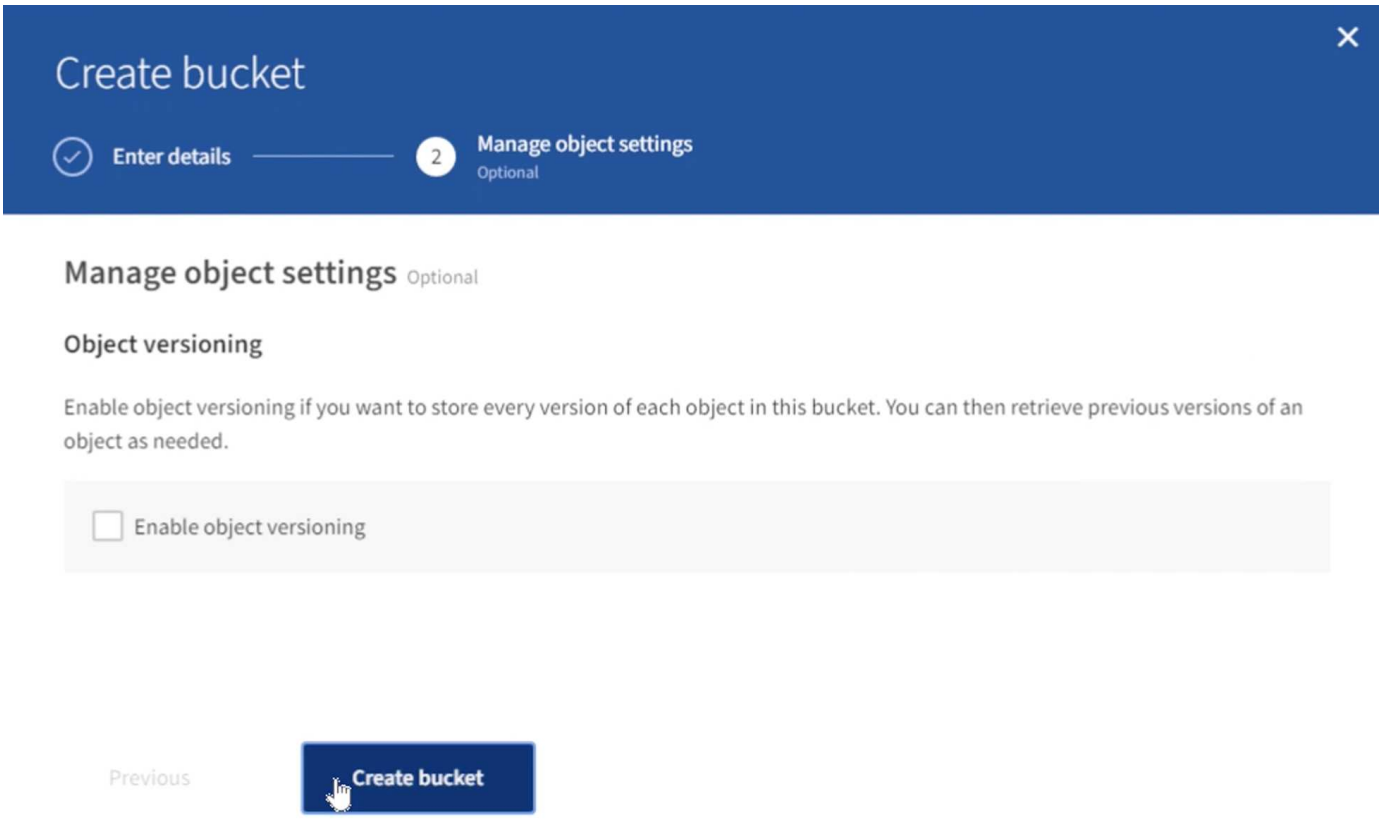
En este primer bloque, active el control de versiones.



Ahora cree un segundo bloque sin el control de versiones activado.



No active el control de versiones en este segundo bloque.



Por Rafael Guedes, y Aron Klein

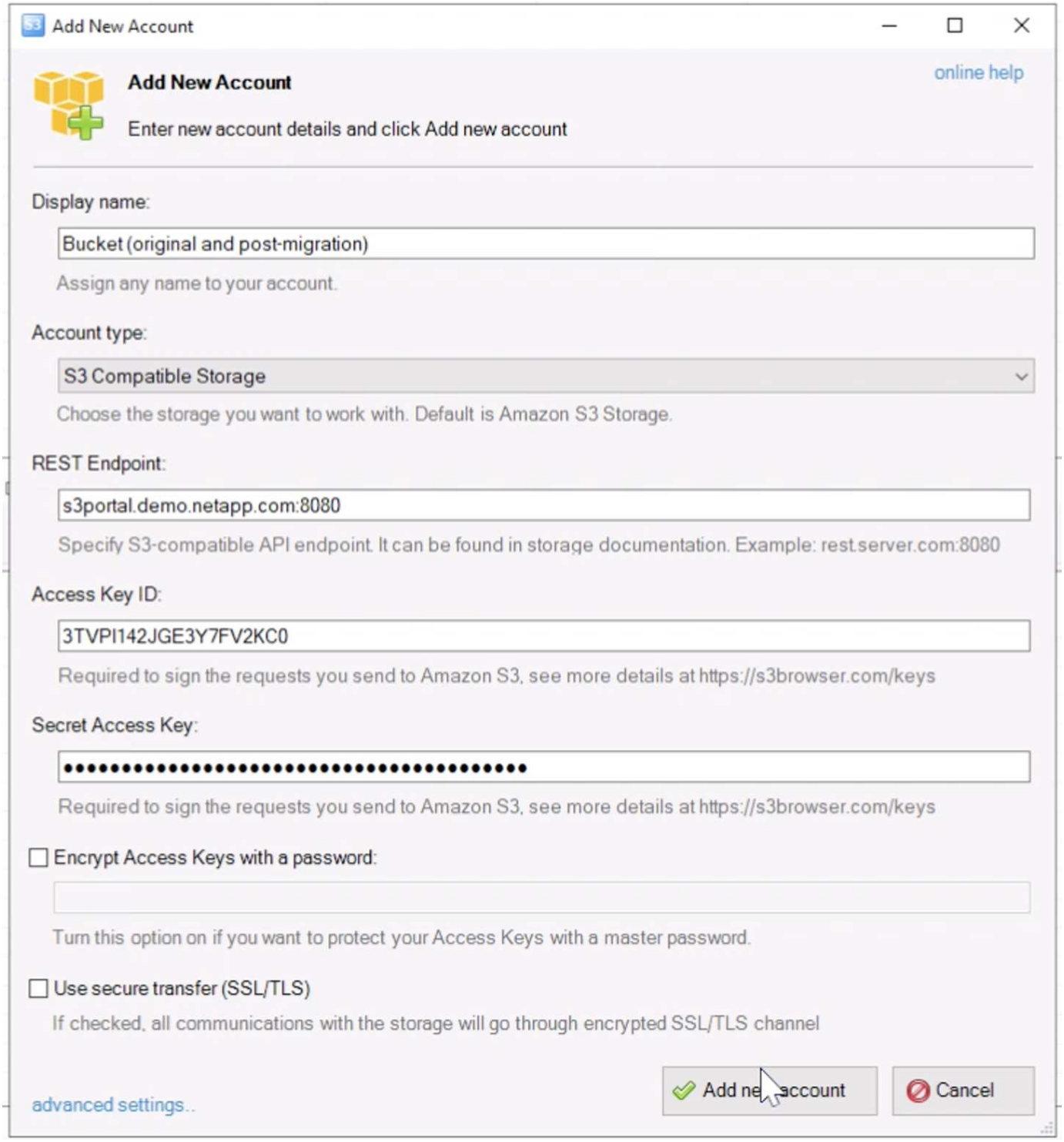
Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

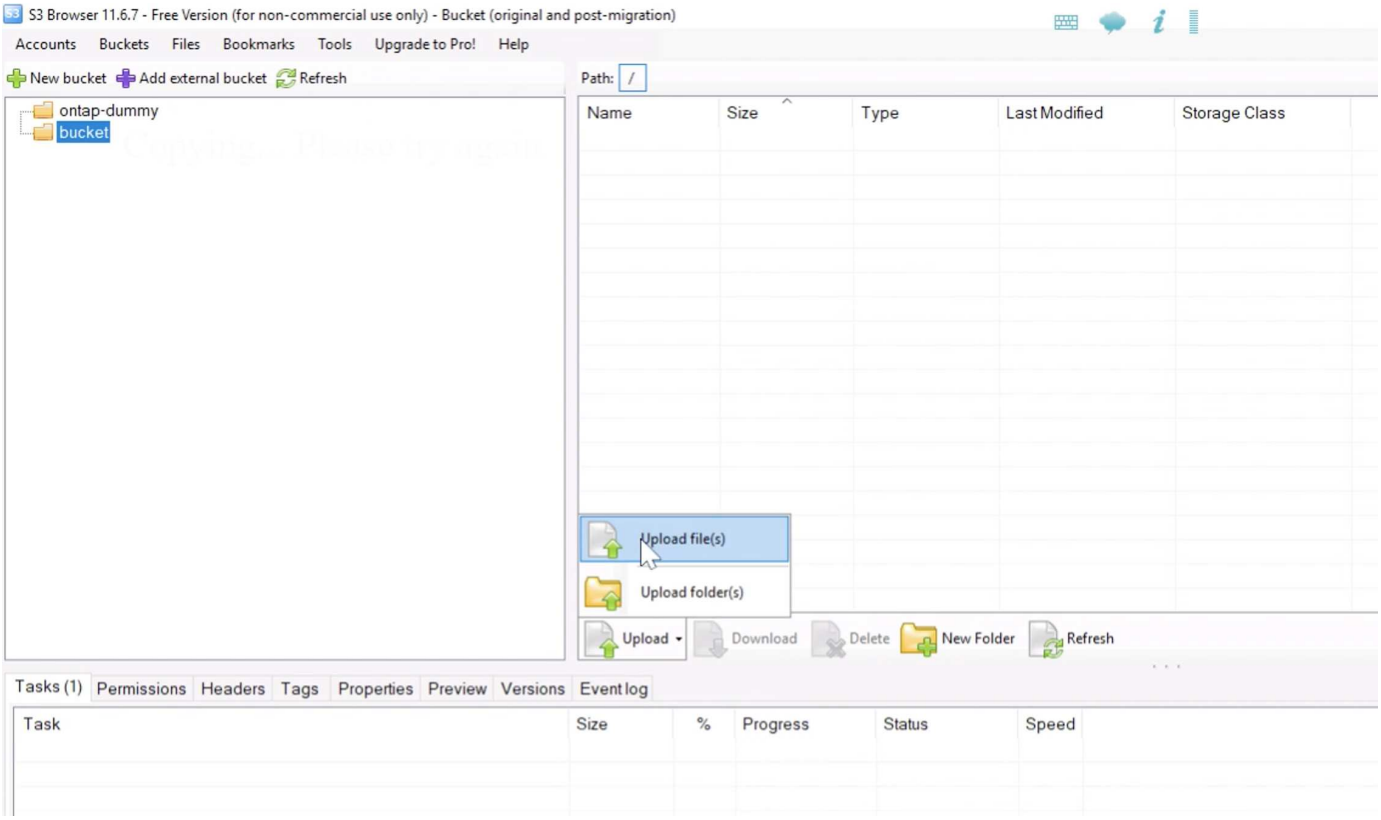
Rellene el bloque de origen

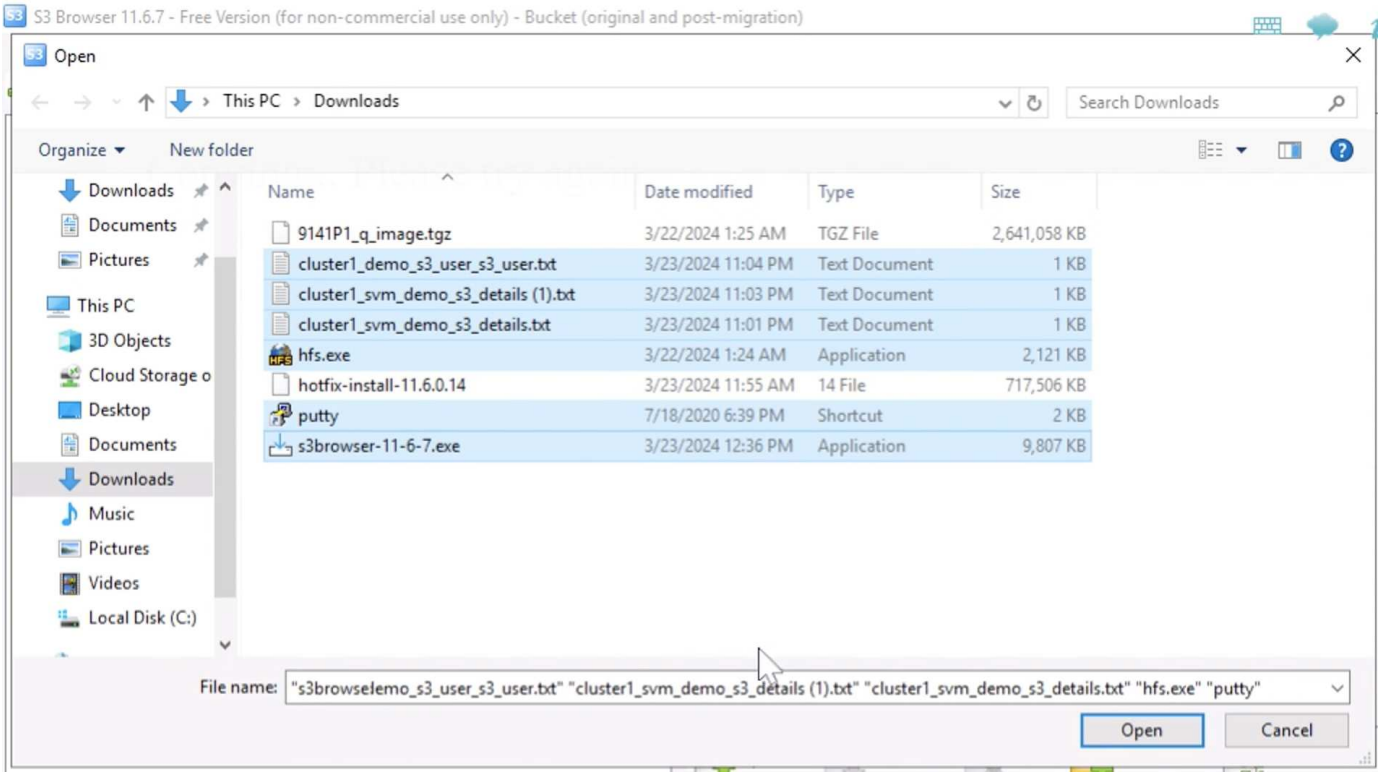
Pongamos algunos objetos en el depósito de ONTAP de origen. Usaremos S3Browser para esta demostración, pero podrías usar cualquier herramienta con la que te sientas cómodo.

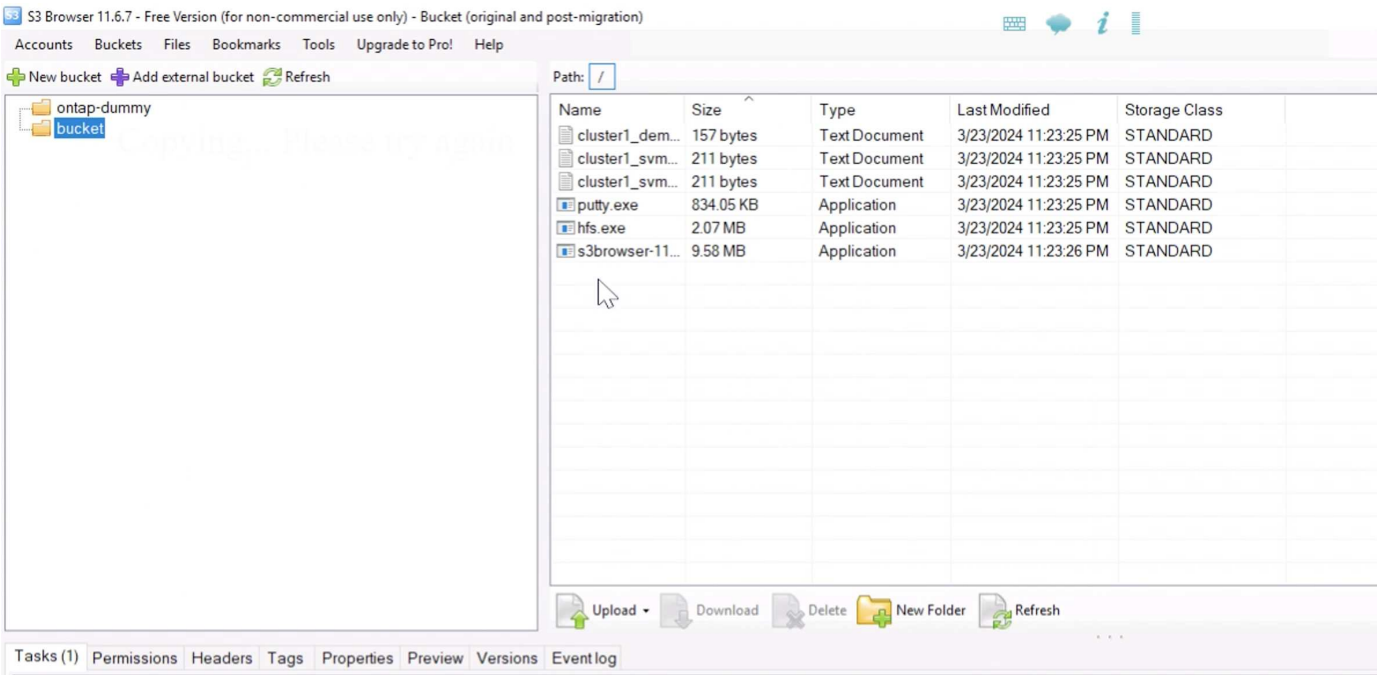
Con las claves de usuario S3 de ONTAP creadas anteriormente, configure S3Browser para conectarse al sistema ONTAP.



Ahora vamos a cargar algunos archivos en el bloque activado para el control de versiones.

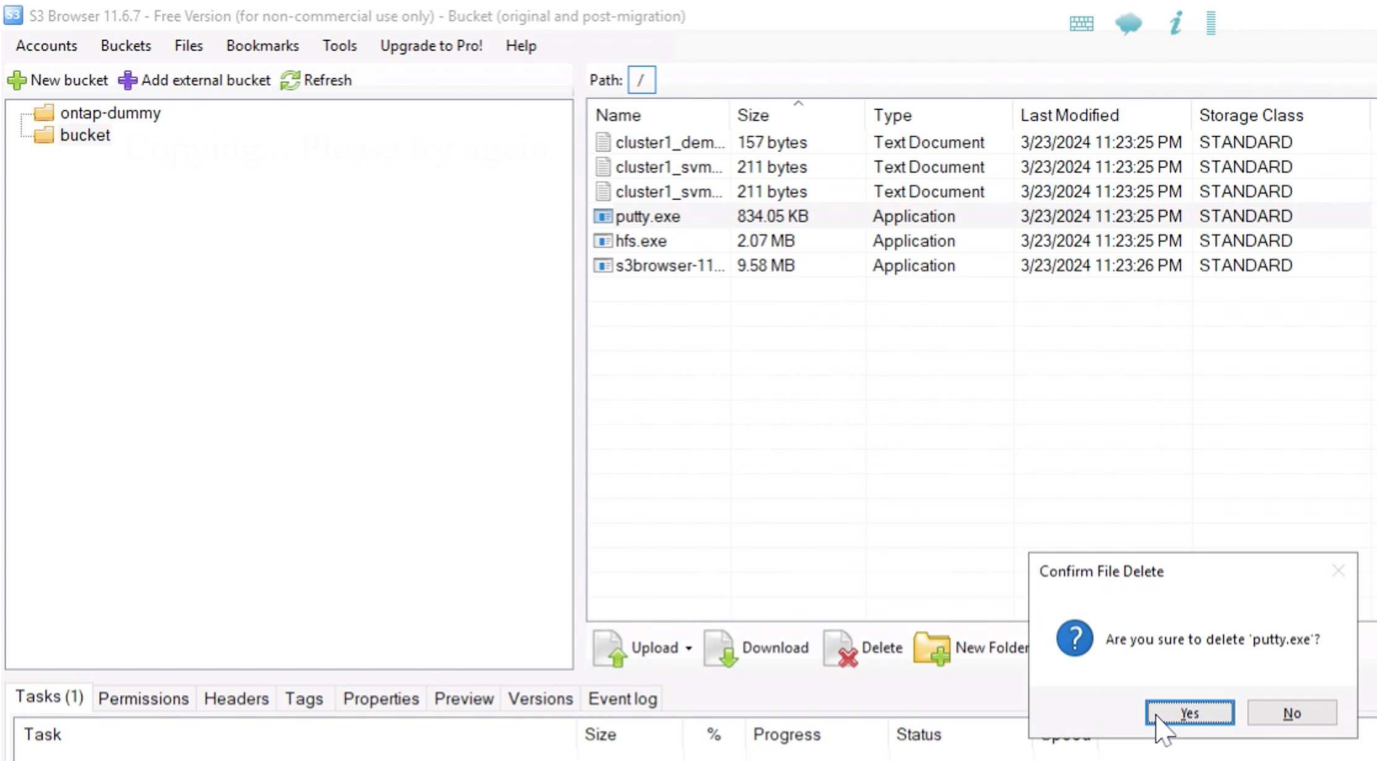

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

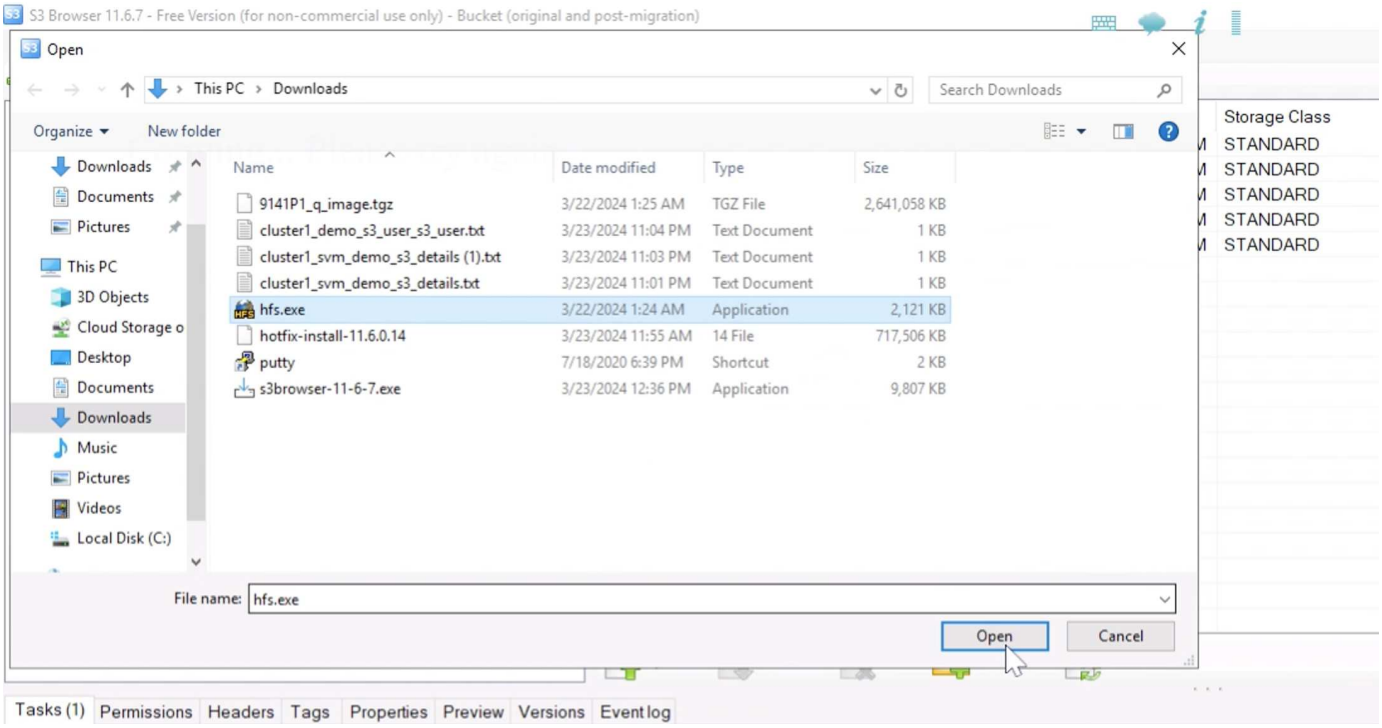


Ahora vamos a crear algunas versiones de objetos en el bloque.

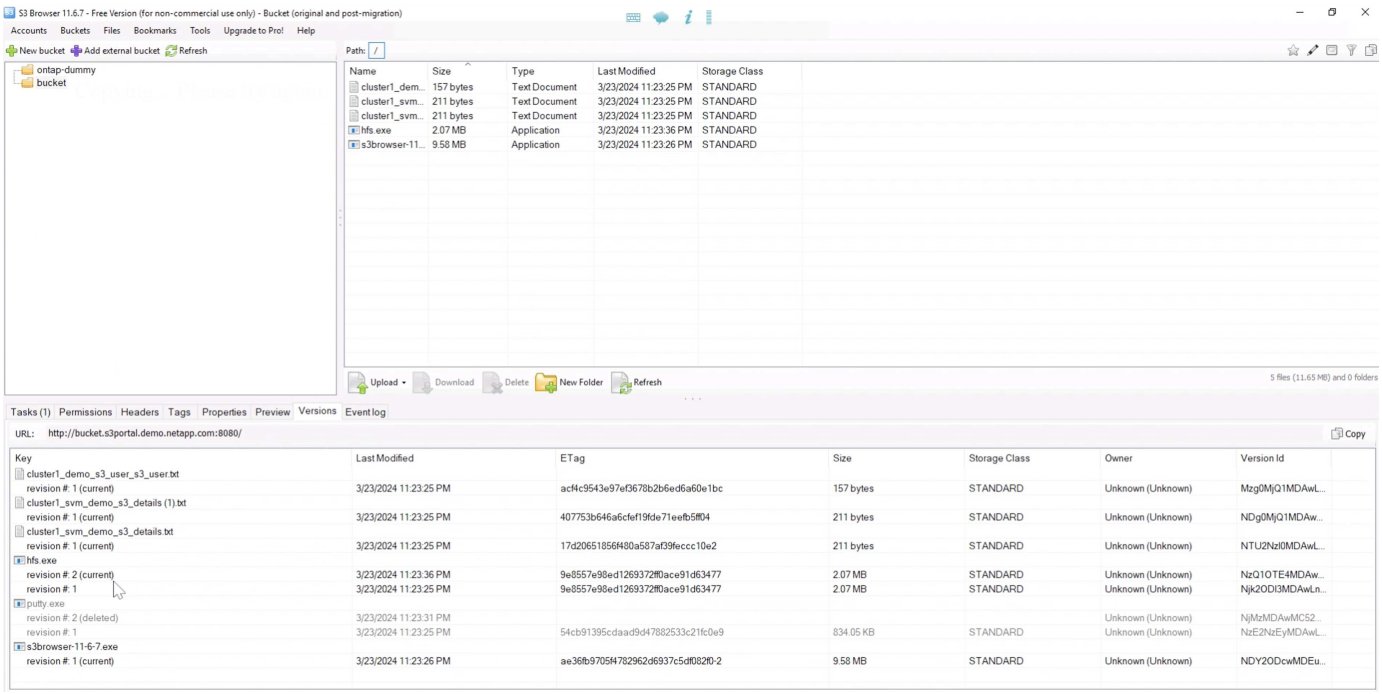
Eliminar un archivo.



Cargue un archivo que ya existe en el depósito para copiar el archivo sobre sí mismo y crear una nueva versión del mismo.



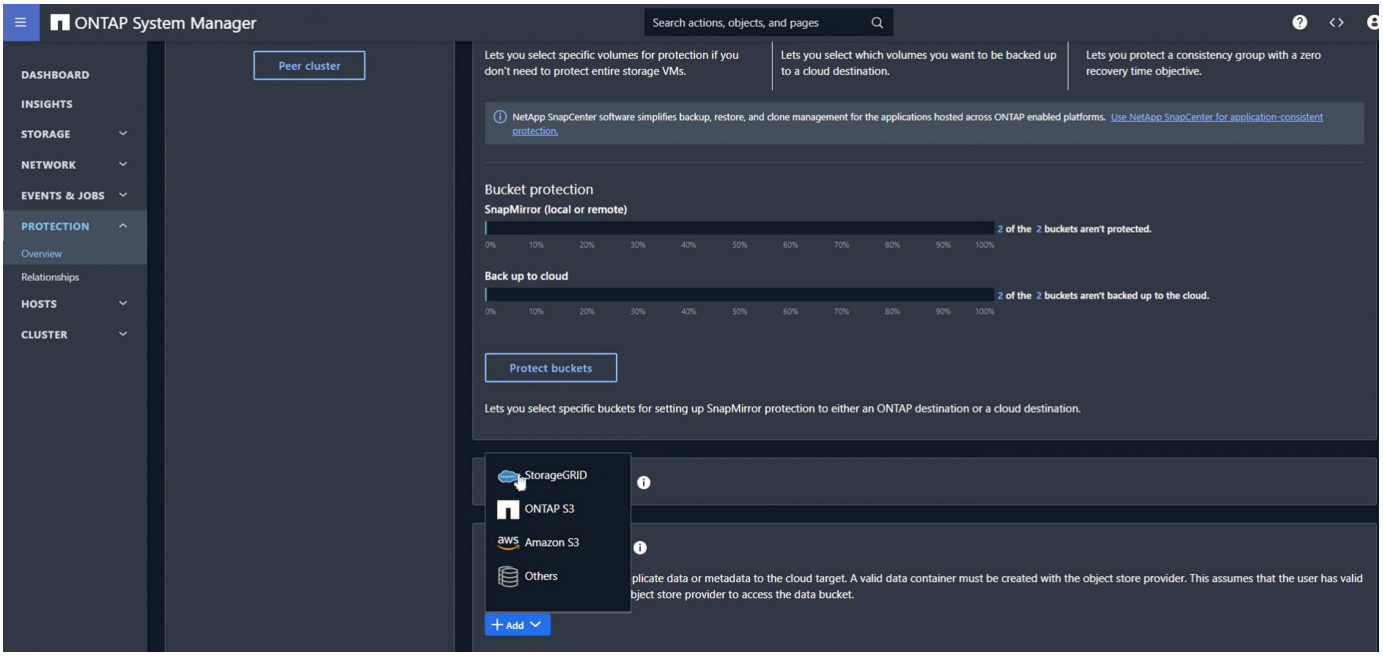
En S3Browser podemos ver las versiones de los objetos que acabamos de crear.



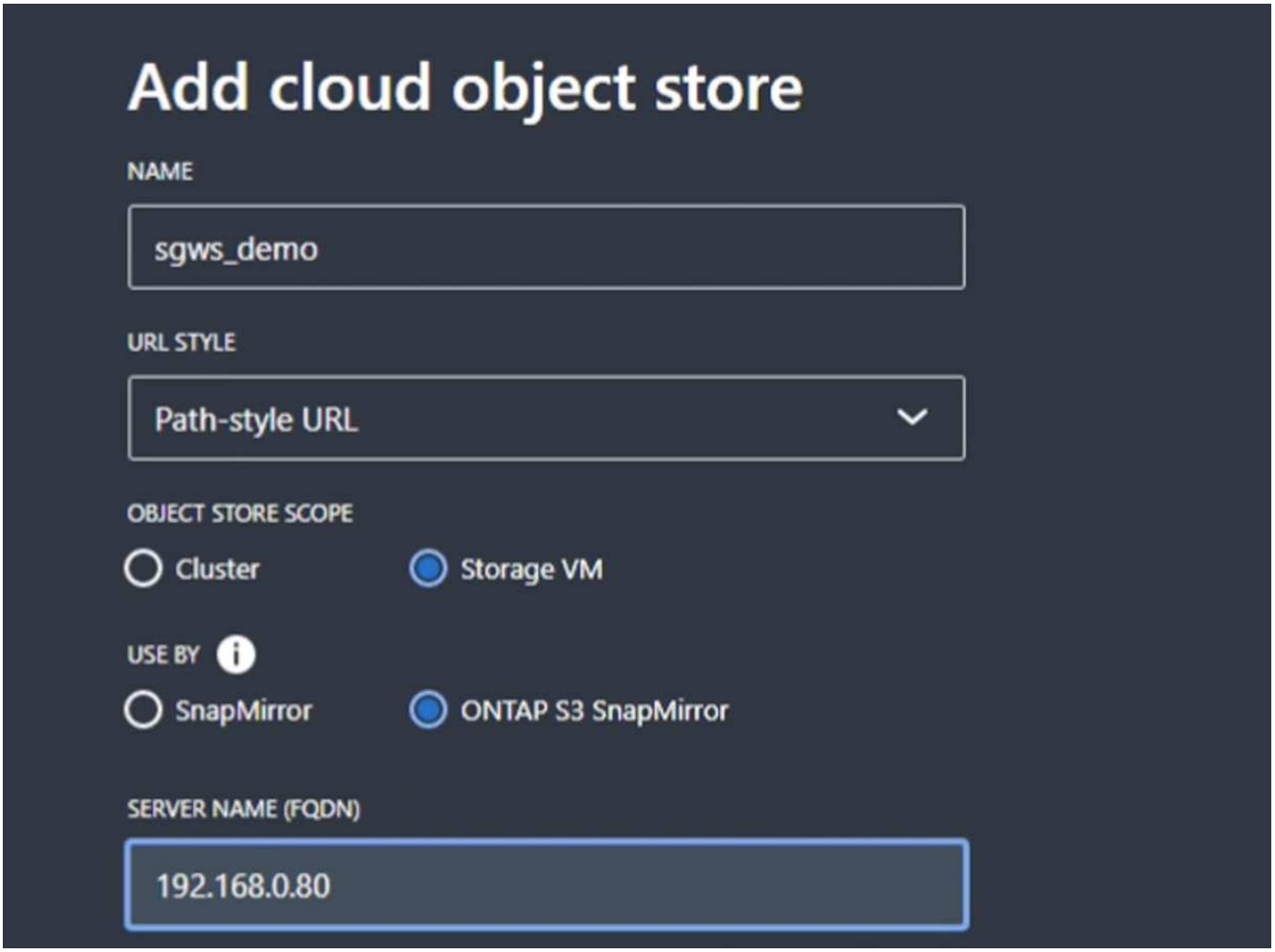
Establezca la relación de replicación

Comencemos a enviar datos de ONTAP a StorageGRID.

En ONTAP System Manager, vaya a «Protection/Overview». Desplácese hacia abajo hasta “Almacenes de objetos en la nube” y haga clic en el botón “Agregar” y seleccione “StorageGRID”.



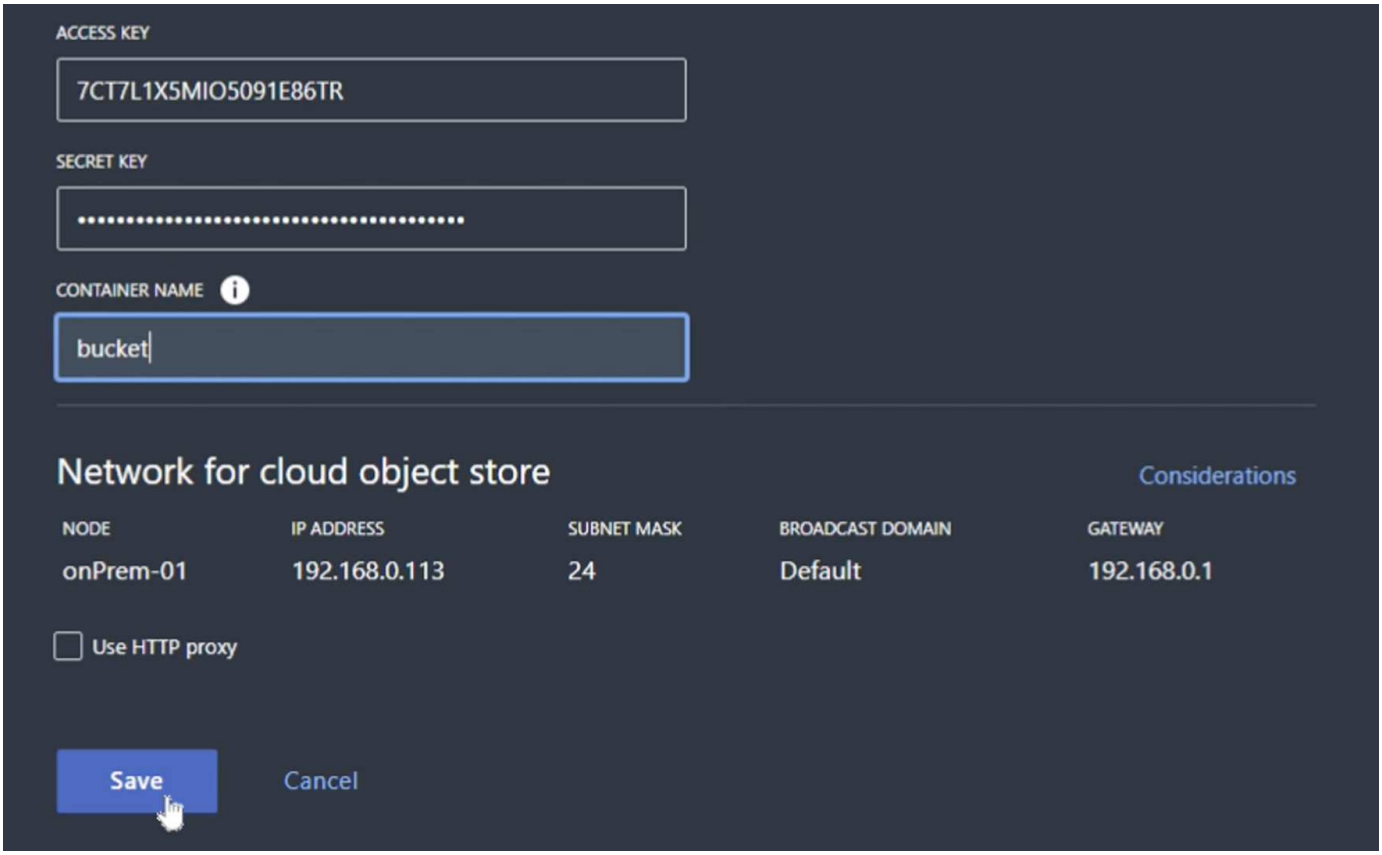
Introduzca la información de StorageGRID proporcionando un nombre, estilo de URL (para esta demostración usaremos URL de estilo de ruta). Establezca el alcance del almacén de objetos en «Storage VM».



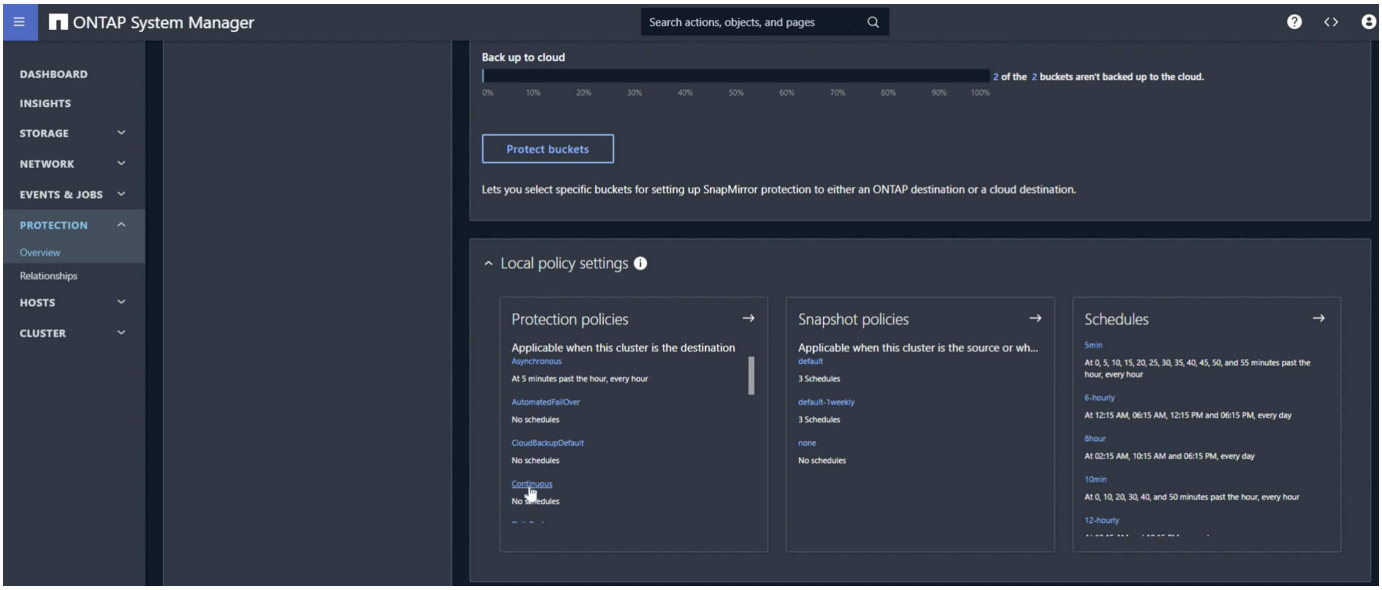
Si utiliza SSL, defina el puerto de punto final del equilibrador de carga y copie el certificado de punto final de

StorageGRID aquí. De lo contrario, desactive la casilla SSL e introduzca el puerto de punto final HTTP aquí.

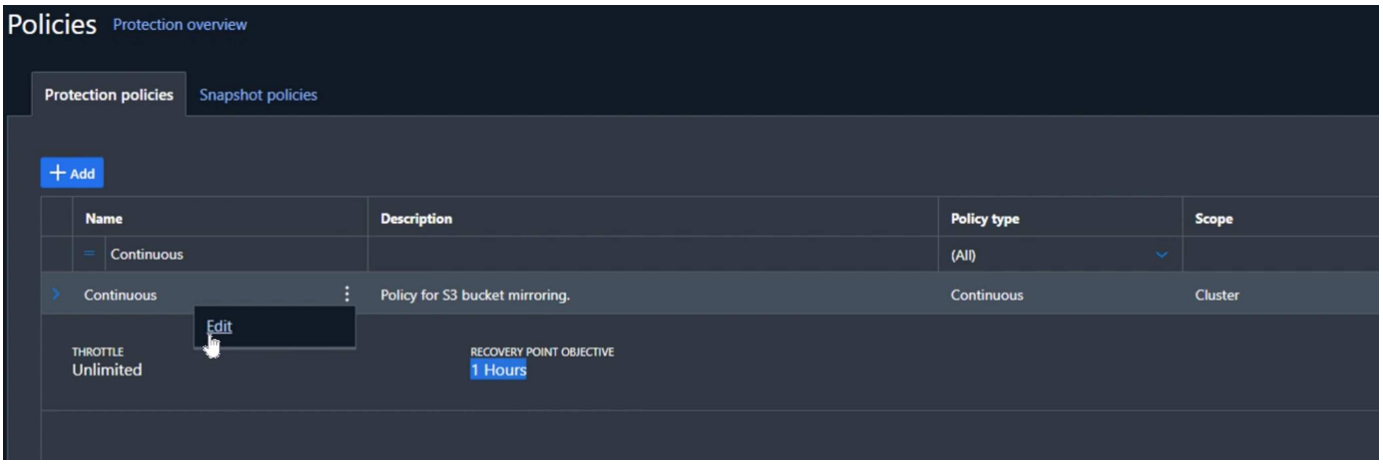
Introduzca las claves de usuario StorageGRID S3 y el nombre del bloque de la configuración de StorageGRID anterior para el destino.



Ahora que tenemos un destino configurado, podemos configurar los ajustes de política para el destino. Expanda “Configuración de directiva local” y seleccione “Continuo”.



Edite la política continua y cambie el objetivo de punto de recuperación de «1 horas» a «3 segundos».

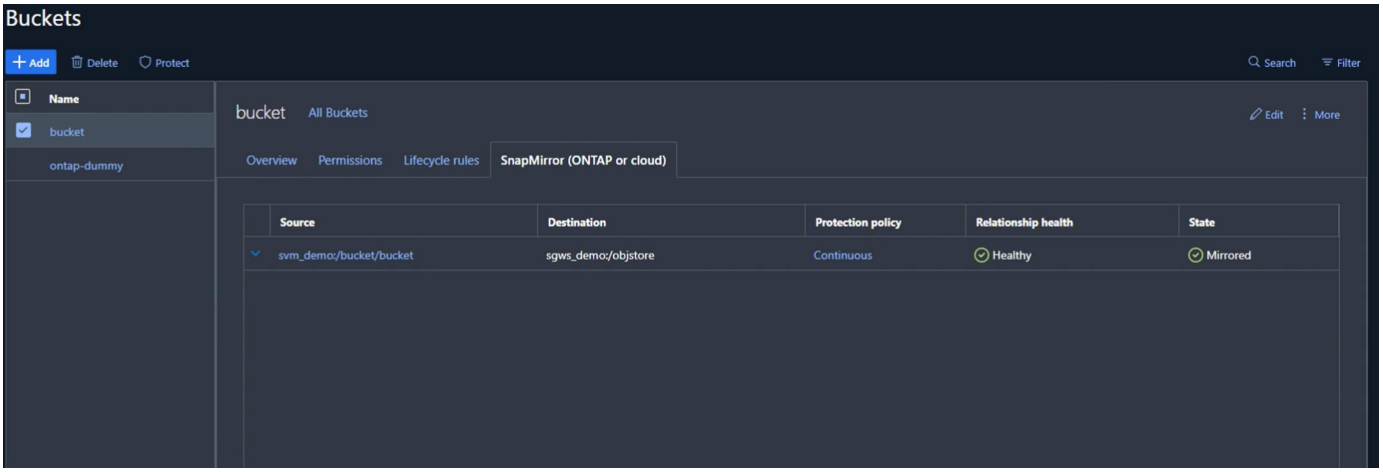


Ahora podemos configurar SnapMirror para que replique el bucket.

```
SnapMirror create -source-path sv_demo: /Bucket/bucket -destination-path sgws_demo: /Objstore -policy Continuo
```

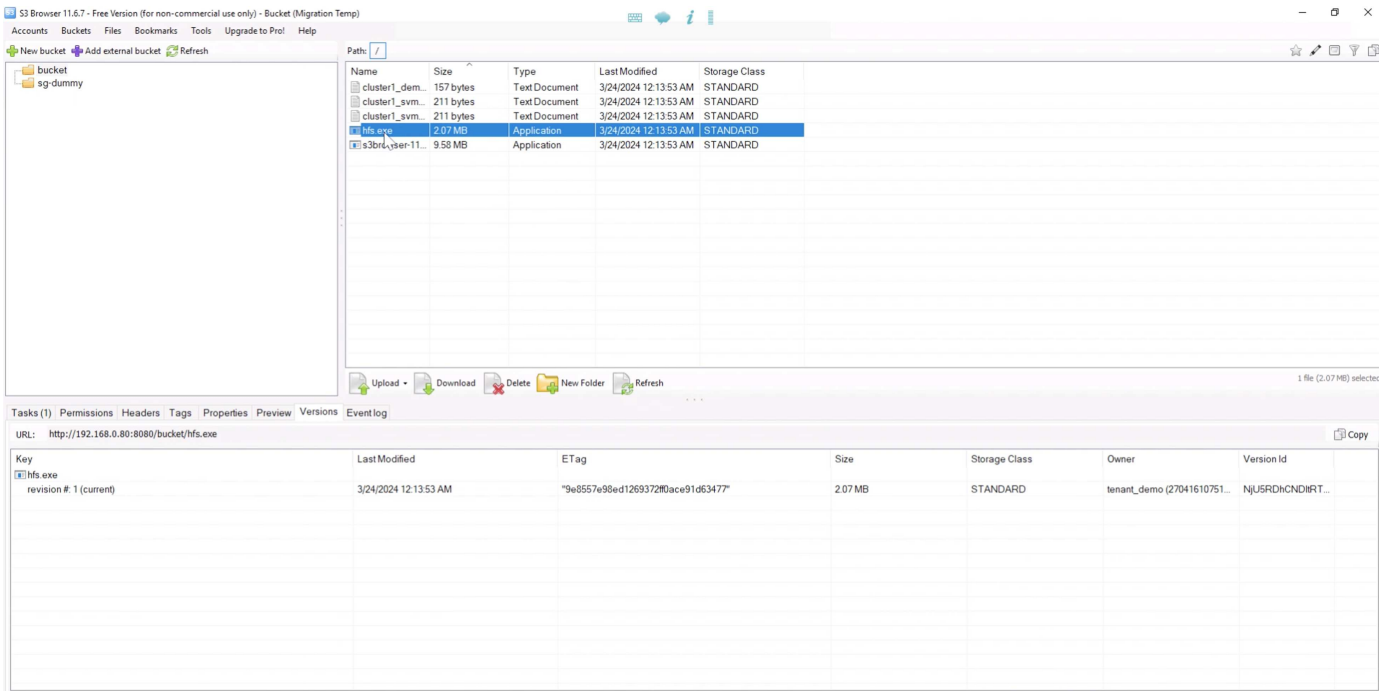
El depósito mostrará ahora un símbolo de nube en la lista de cubos bajo protección.

Si seleccionamos el bucket y vamos a la pestaña «SnapMirror (ONTAP o Cloud)», veremos el estado de reparación de SnapMirror.

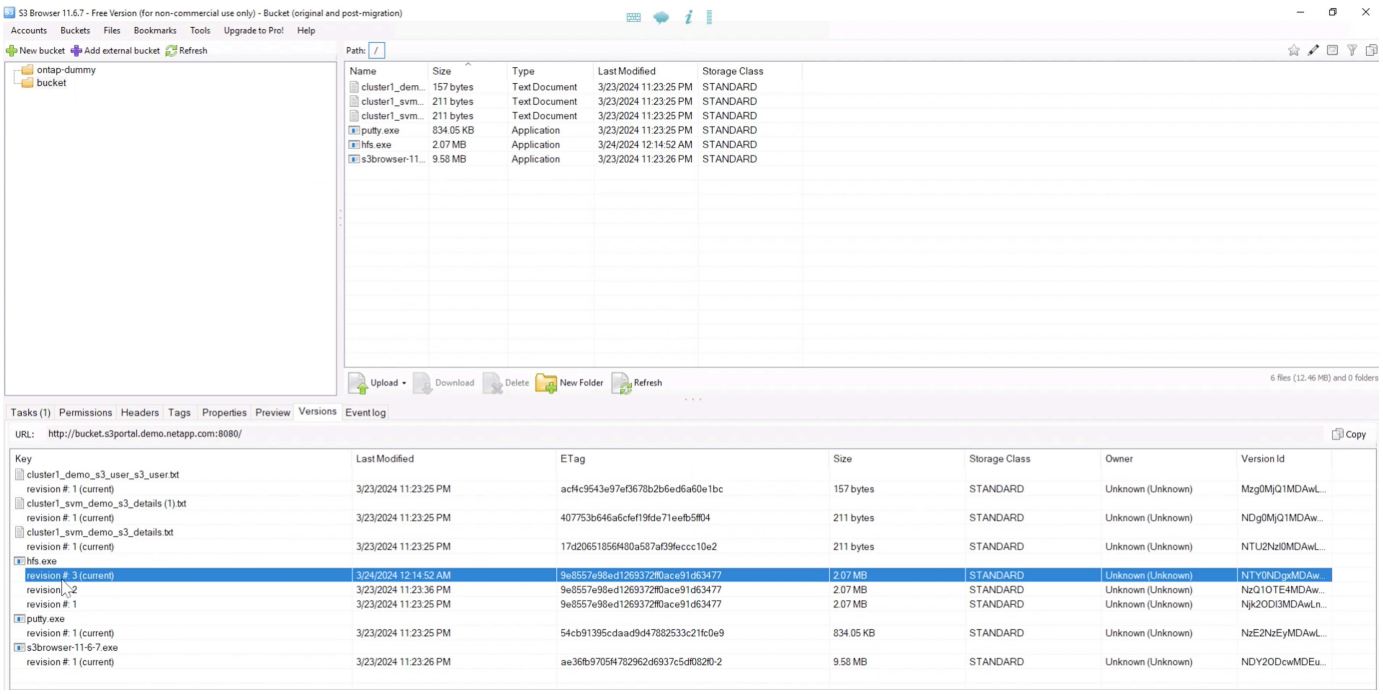


Los detalles de la replicación

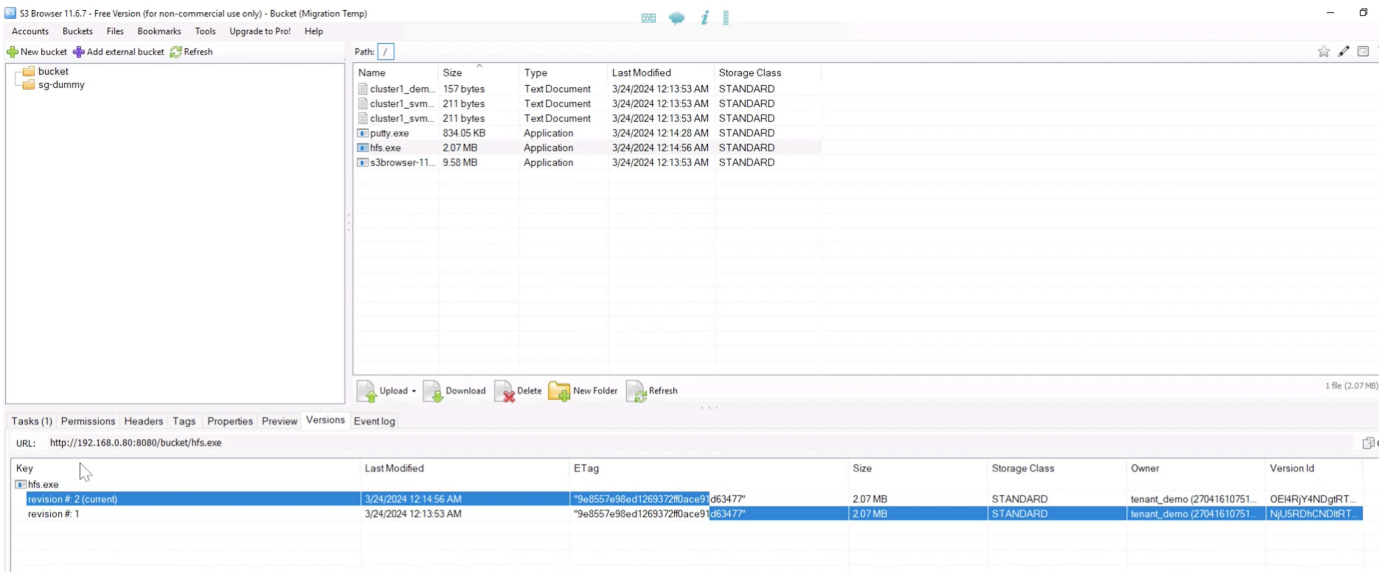
Ahora tenemos un bucket de replicación con éxito de ONTAP en StorageGRID. Pero, ¿qué es lo que realmente se está replicando? Nuestra fuente y destino son cubos versionados. ¿Las versiones anteriores también replican en el destino? Si observamos nuestro bucket de StorageGRID con S3Browser, vemos que las versiones existentes no se han replicado y que nuestro objeto eliminado no existe, ni un marcador de borrado de ese objeto. Nuestro objeto duplicado solo tiene 1 versión en el bucket de StorageGRID.



En nuestro bucket de ONTAP, vamos a añadir una nueva versión a nuestro mismo objeto que hemos usado anteriormente y ver cómo se replica.



Si miramos en la parte de StorageGRID, vemos que también se ha creado una nueva versión en este depósito, pero falta la versión inicial antes de la relación de SnapMirror.



Esto se debe a que el proceso ONTAP SnapMirror S3 sólo replica la versión actual del objeto. Es por eso que hemos creado un bucket con versiones en el lado de StorageGRID para que sea el destino. De esta forma, StorageGRID puede mantener un historial de versiones de los objetos.

Por Rafael Guedes, y Aron Klein

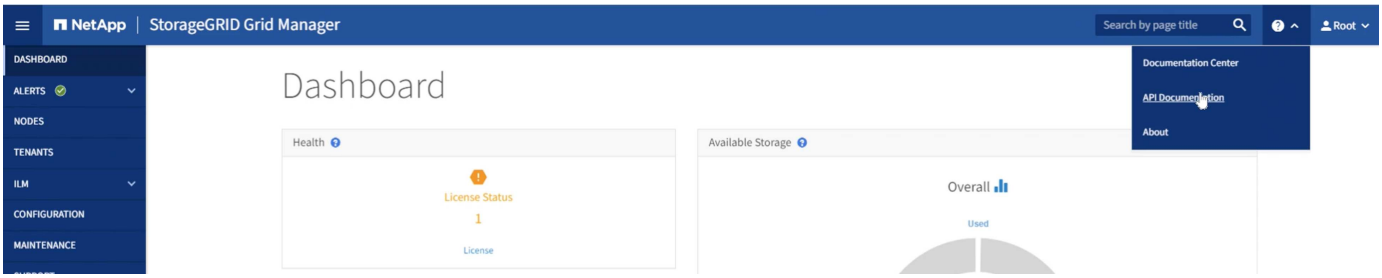
Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

Habilita S3 de nivel empresarial al migrar sin problemas el almacenamiento basado en objetos desde ONTAP S3 a StorageGRID

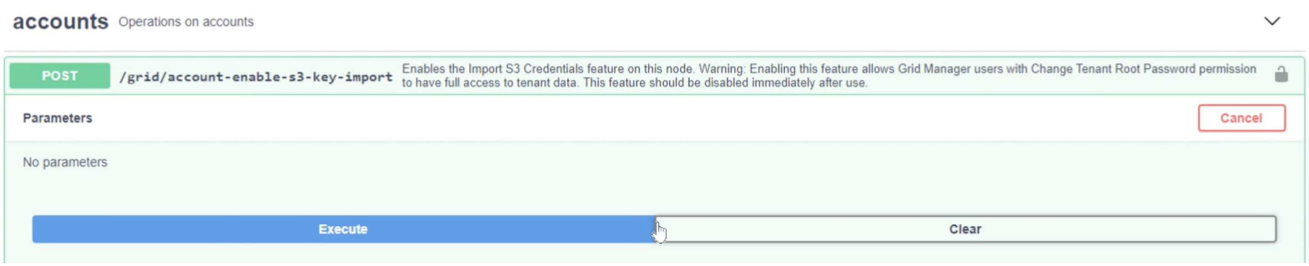
Migrar claves S3

Para una migración, la mayoría de las veces querrá migrar las credenciales de los usuarios en lugar de generar nuevas credenciales en el lado de destino. StorageGRID proporciona api para permitir la importación de claves S3 a un usuario.

Inicie sesión en la interfaz de usuario de gestión de StorageGRID (no la interfaz de usuario del administrador de inquilinos) y abra la página de Swagger de documentación de API.

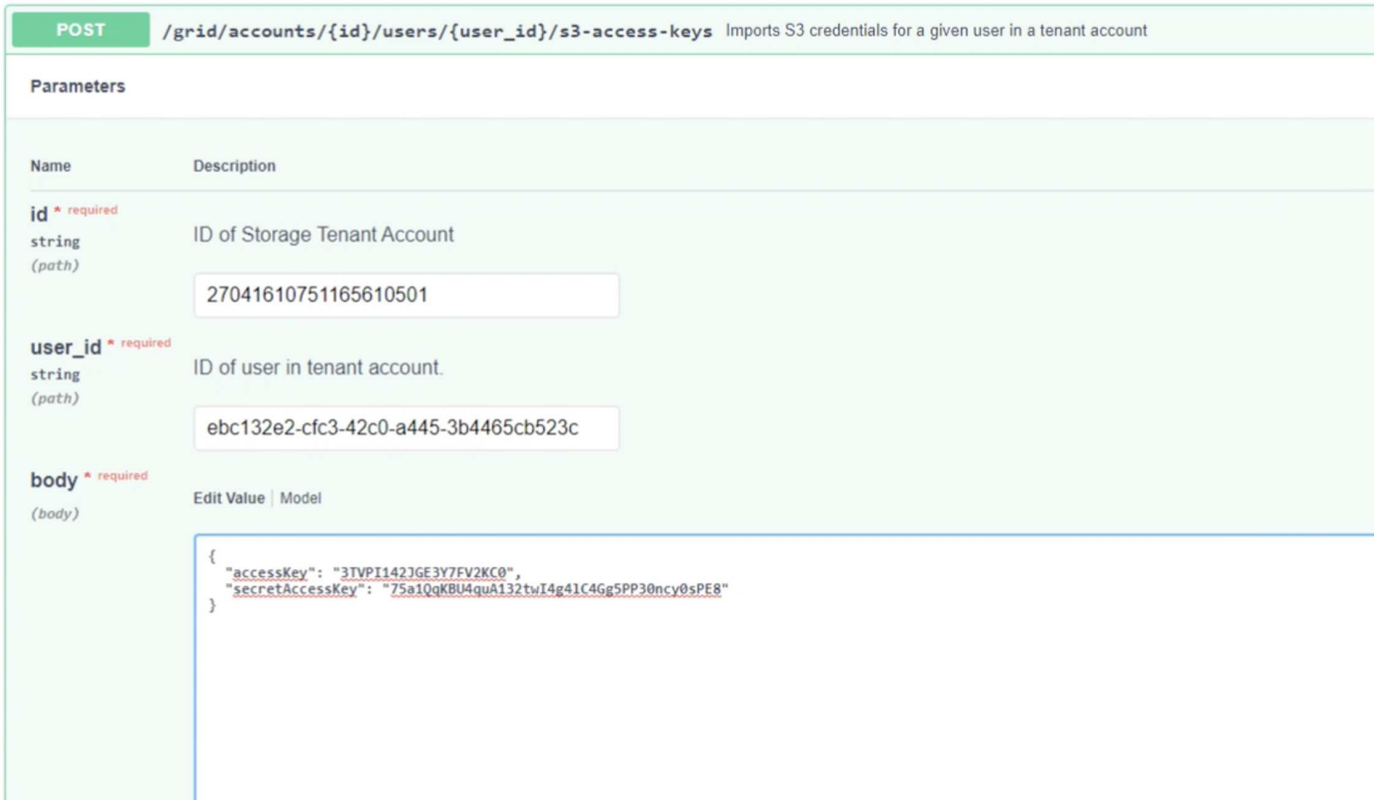


Expanda la sección «Cuentas», seleccione «POST /grid/account-enable-S3-key-import», haga clic en el botón «Pruébelo» y, a continuación, haga clic en el botón de ejecución.

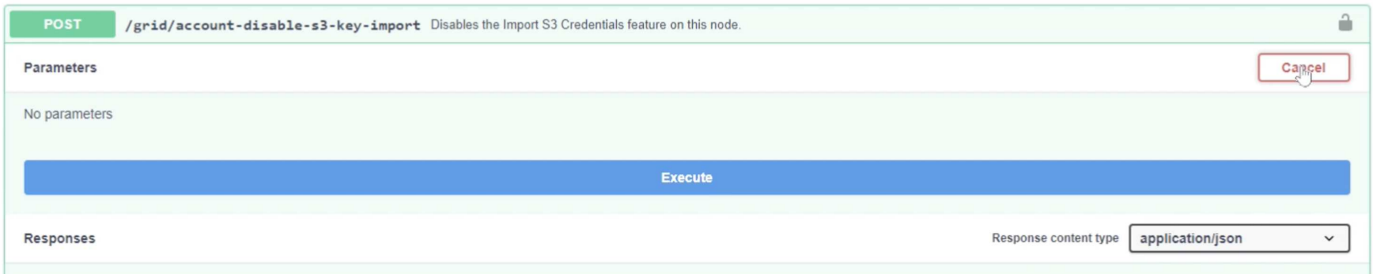


Ahora desplácese hacia abajo todavía en «accounts» para PUBLICAR /grid/accounts/{id}/users/{user_id}/S3-access-keys

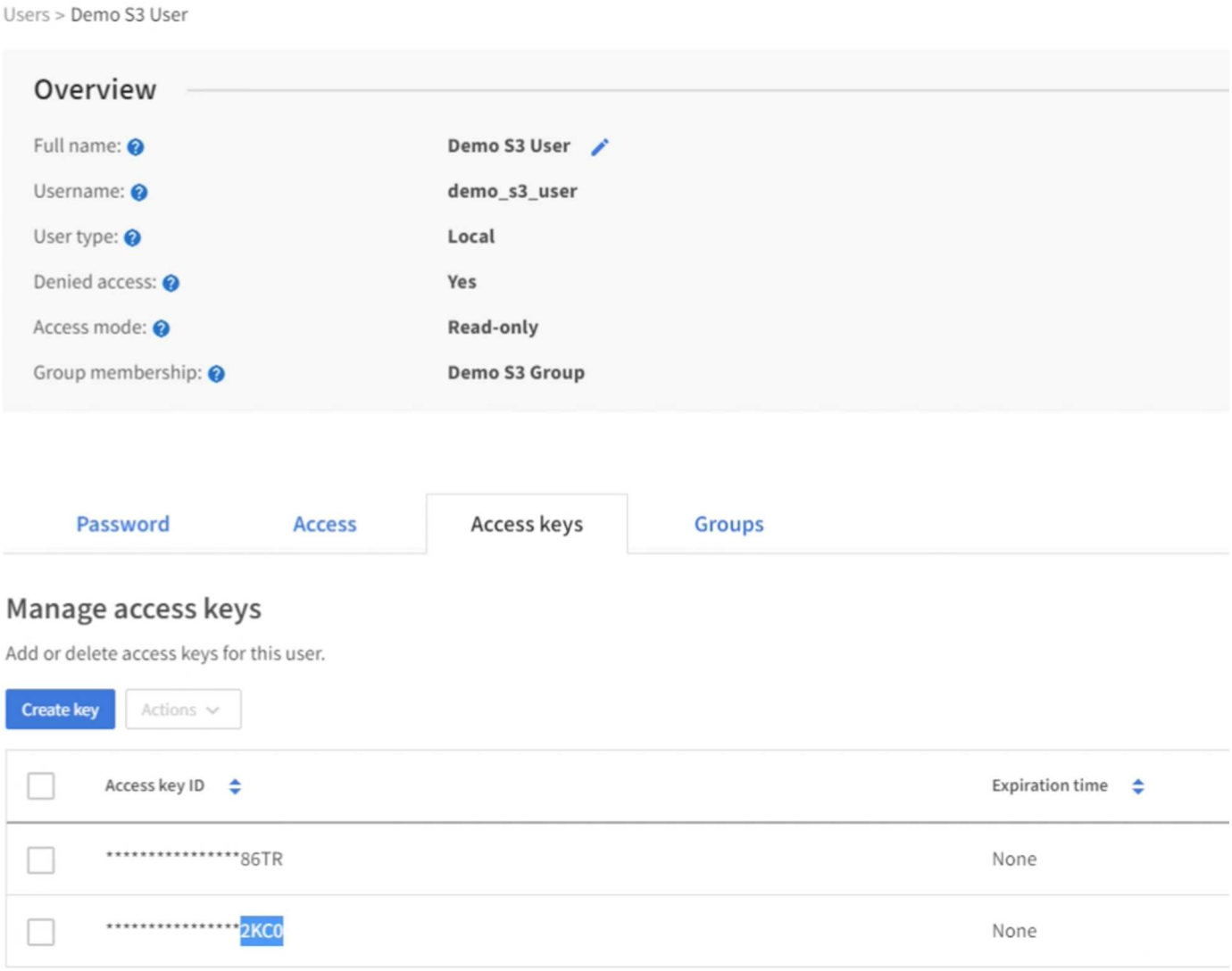
Aquí es donde vamos a introducir el ID de inquilino y el ID de cuenta de usuario que hemos recopilado anteriormente. Rellene los campos y las claves de nuestro usuario de ONTAP en el cuadro json. Puede establecer el vencimiento de las claves o eliminar el ' , ' Expires ': 123456789' y haga clic en Ejecutar.



Una vez que haya completado todas las importaciones de claves de usuario, debe deshabilitar la función de importación de claves en “cuentas” “POST /grid/account-disable-S3-key-import”



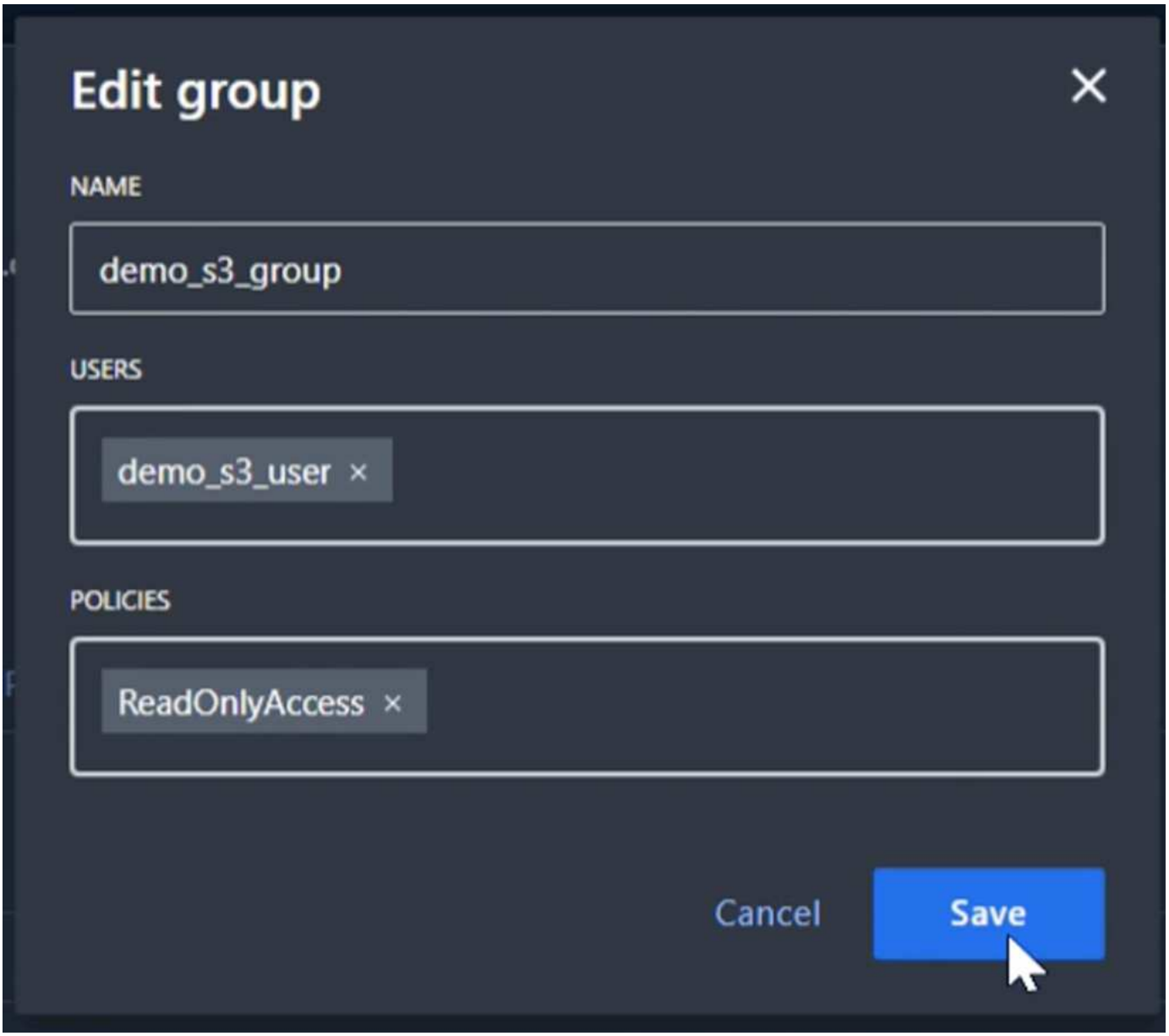
Si observamos la cuenta de usuario en la interfaz de usuario del administrador de inquilinos, podemos ver que se ha añadido la nueva clave.



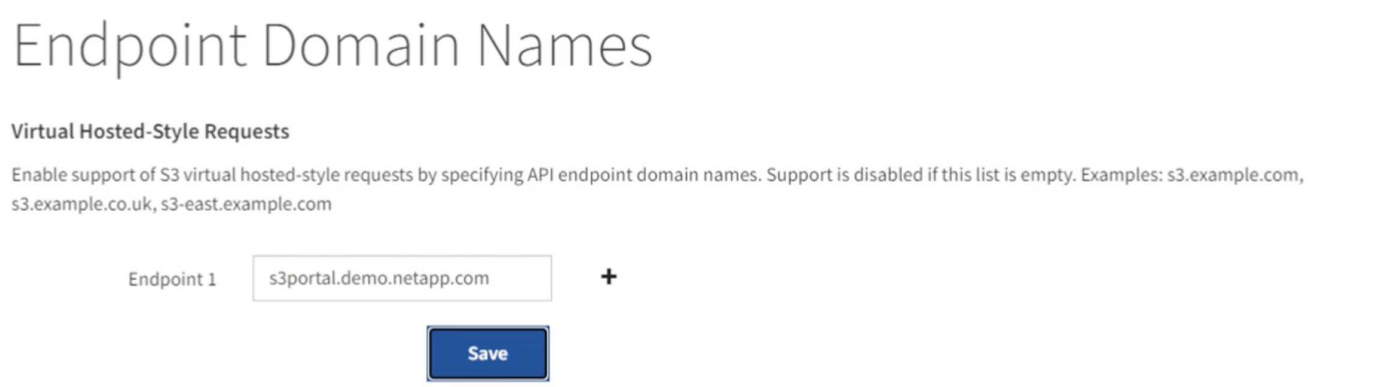
El punto de corte final

Si la intención es tener un bucket que se replica perpetuamente de ONTAP en StorageGRID, puede terminar aquí. Si se trata de una migración de ONTAP S3 a StorageGRID, entonces es el momento de ponerle fin y realizar la transición.

Dentro del administrador del sistema de ONTAP, edite el grupo S3 y establézcalo en «ReadOnlyAccess». Esto evitará que los usuarios vuelvan a escribir en el bucket de ONTAP S3.



Todo lo que queda por hacer es configurar DNS para que apunte desde el clúster de ONTAP al extremo de StorageGRID. Asegúrese de que el certificado de punto final es correcto y si necesita solicitudes de estilo alojadas virtuales, agregue los nombres de dominio de punto final en StorageGRID



Sus clientes tendrán que esperar a que el TTL caduque, o vaciar DNS para resolver el nuevo sistema para que pueda probar que todo está funcionando. Todo lo que queda es limpiar las claves temporales iniciales de S3 que utilizamos para probar el acceso a los datos StorageGRID (NO las claves importadas), eliminar las relaciones de SnapMirror y eliminar los datos de ONTAP.

Por Rafael Guedes, y Aron Klein

Guías de herramientas y aplicaciones

Utilice el conector Hadoop S3A de Cloudera con StorageGRID

Por Angela Cheng

Hadoop ha sido el favorito de los científicos de datos desde hace algún tiempo. Hadoop permite el procesamiento distribuido de grandes conjuntos de datos a través de clusters de ordenadores utilizando marcos de programación simples. Hadoop se diseñó para escalar verticalmente de un solo servidor a miles de máquinas, mientras que cada máquina poseía almacenamiento e informática local.

¿Por qué utilizar S3A para los flujos de trabajo de Hadoop?

A medida que el volumen de datos crece con el tiempo, el método de añadir nuevos equipos con sus propios recursos informáticos y de almacenamiento resulta ineficiente. Escalar de forma lineal crea retos para usar los recursos de forma eficiente y gestionar la infraestructura.

Para abordar estos retos, el cliente Hadoop S3A ofrece I/o de alto rendimiento frente al almacenamiento de objetos S3. Implementar un flujo de trabajo de Hadoop con S3A le ayuda a aprovechar el almacenamiento de objetos como repositorio de datos y le permite separar los recursos informáticos y de almacenamiento, lo que, a su vez, le permite escalar la computación y el almacenamiento de forma independiente. La disociación de la computación y el almacenamiento también le permite dedicar la cantidad adecuada de recursos a sus tareas informáticas y proporcionar capacidad en función del tamaño del conjunto de datos. Por lo tanto, es posible reducir el TCO general para los flujos de trabajo de Hadoop.

Configurar el conector S3A para usar StorageGRID

Requisitos previos

- Una URL de extremo de StorageGRID S3, una clave de acceso de inquilino s3 y una clave secreta para las pruebas de conexión Hadoop S3A.
- Un clúster Cloudera y permiso root o sudo para cada host del clúster para instalar el paquete Java.

A partir de abril de 2022, se había probado Java 11.0.14 con Cloudera 7.1.7 frente a StorageGRID 11.5 y 11.6. Sin embargo, el número de versión de Java puede ser diferente en el momento de una instalación nueva.

Instale el paquete Java

1. Compruebe la "Matriz de compatibilidad de Cloudera" Para la versión de JDK compatible.
2. Descargue el "Paquete Java 11.x." Que coincidan con el sistema operativo del clúster Cloudera. Copie este paquete en cada host del clúster. En este ejemplo, el paquete rpm se utiliza para CentOS.
3. Inicie sesión en cada host como raíz o utilice una cuenta con permiso sudo. Realice los siguientes pasos en cada host:
   a. Instale el paquete:

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

b. Compruebe dónde está instalado Java. Si se instalan varias versiones, establezca la versión recién instalada como predeterminada:

```
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. Agregue esta línea al final de `/etc/profile`. La ruta debe coincidir con la ruta de la selección anterior:

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

d. Ejecute el siguiente comando para que el perfil surta efecto:

```
source /etc/profile
```

Configuración de Cloudera HDFS S3A

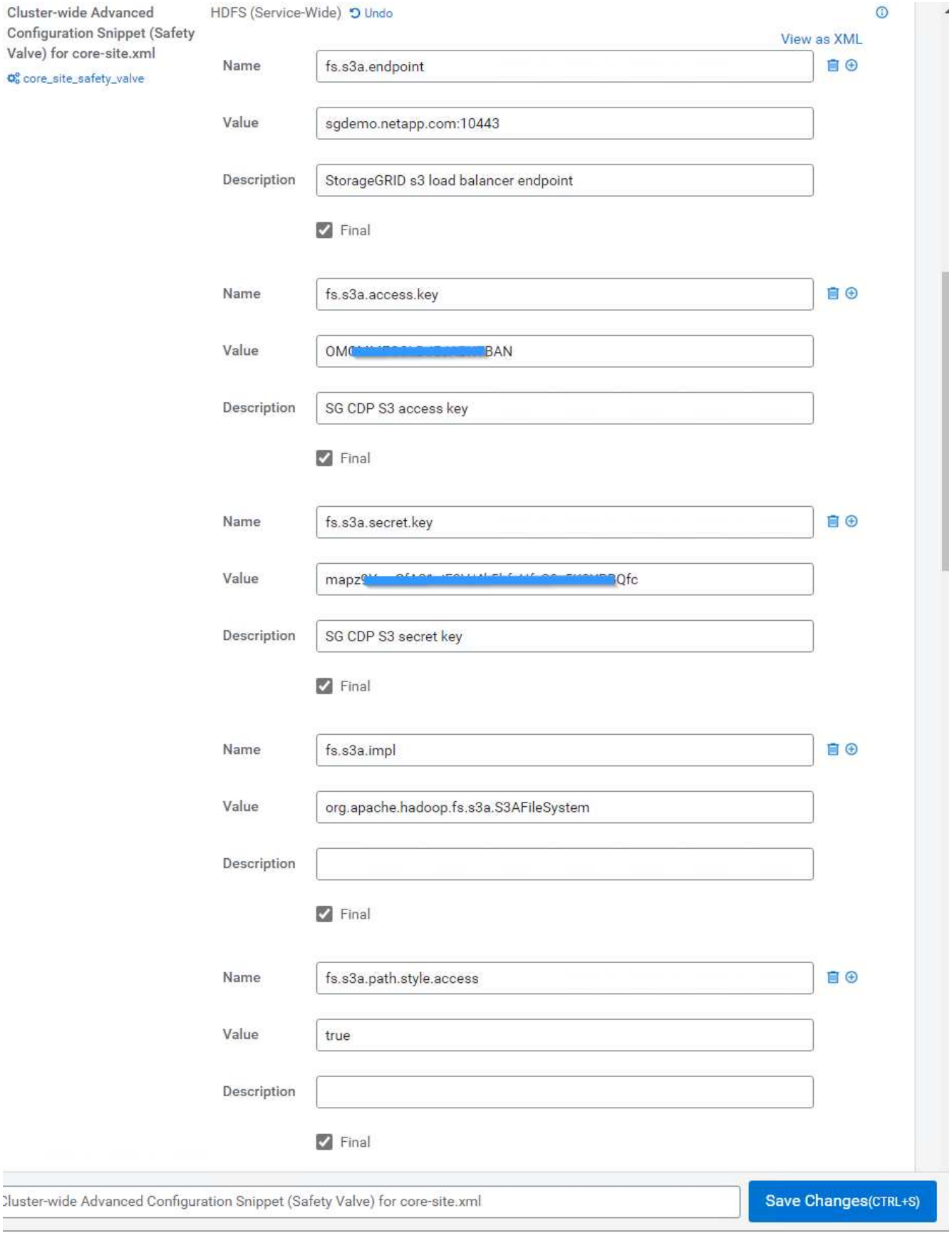
- Pasos*

1. En la interfaz gráfica de usuario de Cloudera Manager, seleccione Clusters > HDFS y seleccione Configuration.
2. En CATEGORÍA, seleccione Avanzado y desplácese hacia abajo para localizar `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Haga clic en el signo (+) y agregue los siguientes pares de valor.

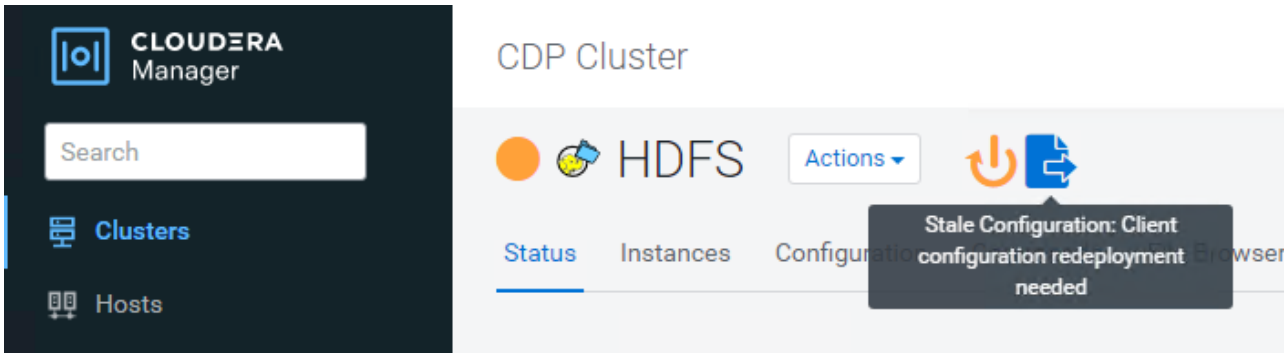
Nombre	Valor
fs.s3a.access.key	*<clave de acceso de inquilino s3 de StorageGRID>*
fs.s3a.secret.key	*<clave secreta de inquilino s3 de StorageGRID>*
fs.s3a.connection.ssl.enabled	[verdadero o falso] (el valor predeterminado es https si falta esta entrada)
fs.s3a.endpoint	*<StorageGRID S3 endpoint:Port>*

Nombre	Valor
fs.s3a.impl	Org.apache.hadoop.fs.s3a.S3AFileSystem
fs.s3a.path.style.access	[verdadero o falso] (el estilo de host virtual es el predeterminado si falta esta entrada)

Captura de pantalla de ejemplo



1. Haga clic en el botón Save Changes. Seleccione el icono Configuración obsoleta en la barra de menús de HDFS, seleccione Reiniciar servicios obsoletos en la página siguiente y seleccione Reiniciar ahora.



Probar la conexión S3A a StorageGRID

Realizar una prueba de conexión básica

Inicie sesión en uno de los hosts del clúster Cloudera y escriba `hadoop fs -ls s3a://<bucket-name>/`.

En el siguiente ejemplo se utiliza el sistema de ruta con un cubo de prueba hdfs preexistente y un objeto de prueba.

```
[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.
```

Resolución de problemas

Situación 1

Utilice una conexión HTTPS a StorageGRID y obtenga una `handshake_failure` error tras un tiempo de espera de 15 minutos.

Razón: Versión antigua de JRE/JDK utilizando un conjunto de cifrado TLS obsoleto o no compatible para la conexión con StorageGRID.

Mensaje de error de muestra

```
[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
```

Resolución: Asegúrese de que JDK 11.x o posterior esté instalado y establecido en la biblioteca Java predeterminada. Consulte la Instale el paquete Java para obtener más información.

Situación 2:

Error al conectarse a StorageGRID con mensaje de error `Unable to find valid certification path to requested target`.

Razón: el programa Java no confía en el certificado del servidor de extremo StorageGRID S3.

Mensaje de error de muestra:

```
[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
```

Resolución: NetApp recomienda el uso de un certificado de servidor emitido por una autoridad pública de firma de certificación conocida para garantizar la seguridad de la autenticación. También puede agregar un certificado de servidor o CA personalizado al almacén de confianza de Java.

Complete los siguientes pasos para agregar una CA personalizada de StorageGRID o un certificado de servidor al almacén de confianza de Java.

1. Realice una copia de seguridad del archivo Cacits de Java predeterminado existente.

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

2. Importe el certificado de extremo de StorageGRID S3 al almacén de confianza de Java.

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

Consejos para la solución de problemas

1. Aumente el nivel de registro de hadoop para DEPURAR.

   ```
   export HADOOP_ROOT_LOGGER=hadoop.root.logger=DEBUG,console
   ```

2. Ejecute el comando y dirija los mensajes del registro a error.log.

   ```
   hadoop fs -ls s3a://<bucket-name>/ &>error.log
   ```

Por Angela Cheng

Use S3cmd para probar y demostrar el acceso S3 en StorageGRID

Por Aron Klein

S3cmd es una herramienta de línea de comandos gratuita y un cliente para las operaciones S3. Puede usar s3cmd para probar y demostrar el acceso s3 en StorageGRID.

Instale y configure S3cmd

Para instalar S3cmd en una estación de trabajo o servidor, descárguelo desde "Línea de comandos del cliente S3". S3cmd está preinstalado en cada nodo StorageGRID como herramienta que ayuda a resolver problemas.

Pasos de configuración inicial

1. s3cmd --configure
2. Proporcione solo access_key y Secret_Key, para que el resto conserve los valores predeterminados.
3. ¿Probar el acceso con las credenciales proporcionadas? [Y/n]: n (omitir la prueba ya que fallará)
4. ¿Desea guardar la configuración? [S/N] y.
   a. Configuración guardada en '/root/.s3cfg'
5. En .s3cfg, haga que los campos host_base y host_bucket estén vacíos después del signo "=" :
   a. host_base =
   b. host_bucket =

> Si especifica host_base y host_bucket en el paso 4, no es necesario especificar un extremo con --host en la CLI. Ejemplo:

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

Ejemplos de comandos básicos

- * Crear un cubo:*

```
s3cmd mb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- **Lista todos los cucharones:**

```
s3cmd ls --host=<endpoint>:<port> --no-check-certificate
```

- **Lista todos los cucharones y su contenido:**

```
s3cmd la --host=<endpoint>:<port> --no-check-certificate
```

- **Lista objetos en un cubo específico:**

```
s3cmd ls s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Eliminar un cucharón:**

```
s3cmd rb s3://s3cmdbucket --host=<endpoint>:<port> --no-check-certificate
```

- * Poner un objeto:*

```
s3cmd put <file> s3://<bucket> --host=<endpoint>:<port> --no-check-certificate
```

- **Obtener un objeto:**

```
s3cmd get s3://<bucket>/<object> <file> --host=<endpoint>:<port> --no-check
-certificate
```

- **Eliminar un objeto:**

```
s3cmd del s3://<bucket>/<object> --host=<endpoint>:<port> --no-check
-certificate
```

Vertica Eon mode Database utilizando NetApp StorageGRID como almacenamiento comunitario

Por Angela Cheng

En esta guía se describe el procedimiento para crear una base de datos de Vertica Eon Mode con almacenamiento compartido en StorageGRID de NetApp.

Introducción

Vertica es un software de gestión de bases de datos analíticas. Se trata de una plataforma de almacenamiento en columnas diseñada para gestionar grandes volúmenes de datos, lo que permite un rendimiento de consultas muy rápido en una situación tradicionalmente intensiva. Una base de datos Vertica se ejecuta en uno de los dos modos: Eon o Enterprise. Puede poner en marcha ambos modos en las instalaciones o en el cloud.

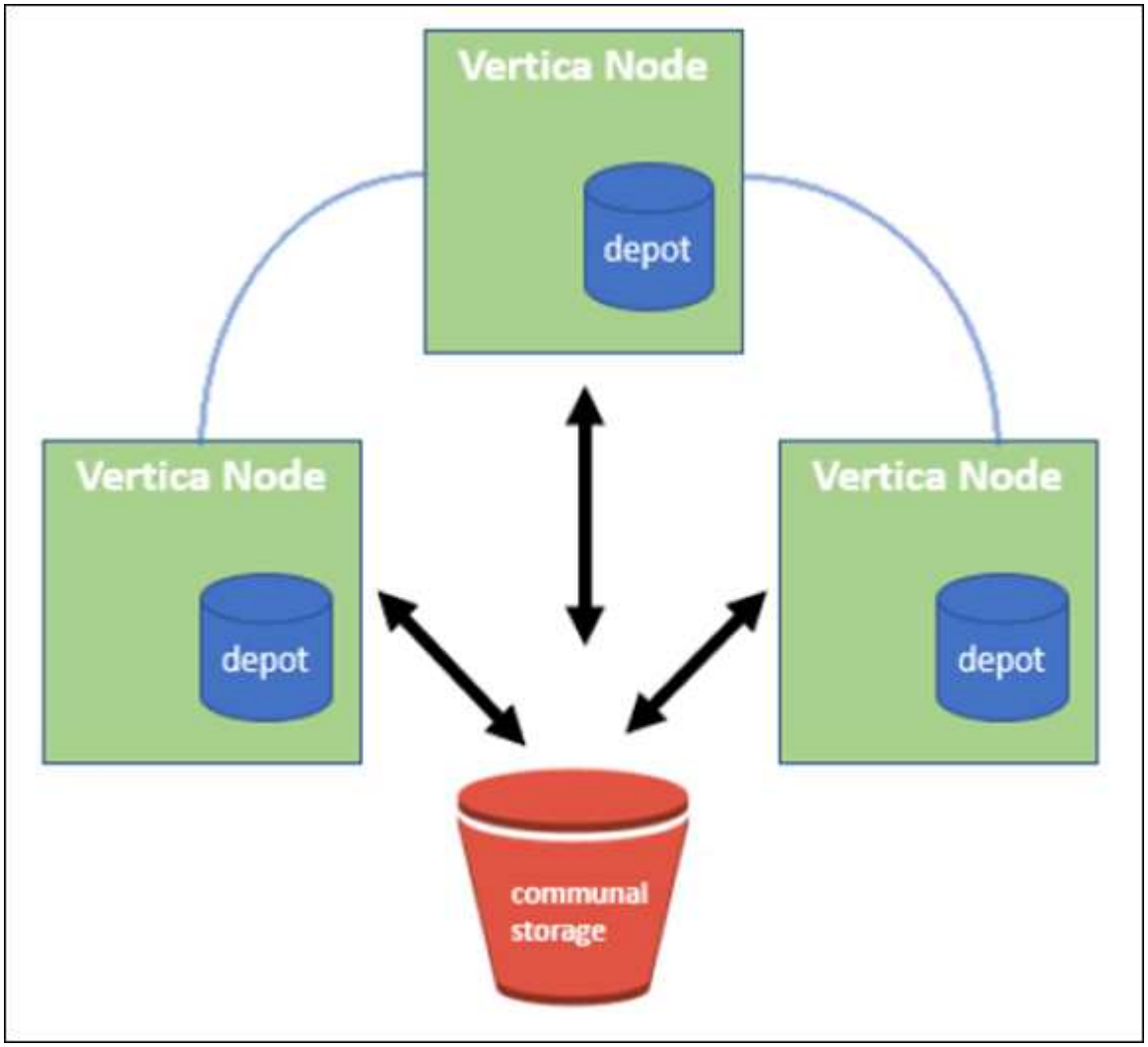
Los modos Eon y Enterprise difieren principalmente en el lugar en el que almacenan datos:

- Las bases de datos de modo Eon utilizan almacenamiento común para sus datos. Esto es recomendado por Vertica.
- Las bases de datos de Enterprise Mode almacenan los datos localmente en el sistema de archivos de nodos que componen la base de datos.

Arquitectura de modo Eon

Eon Mode separa los recursos computacionales de la capa de almacenamiento comunal de la base de datos, que permite que la computación y el almacenamiento se escalen por separado. Vertica en modo Eon está optimizada para trabajar con cargas de trabajo variables y aislarlas entre sí mediante el uso de recursos informáticos y de almacenamiento independientes.

Eon Mode almacena datos en un almacén de objetos compartidos denominado almacenamiento comunitario, un bucket de S3, que está alojado en las instalaciones o en Amazon S3.



Almacenamiento comunitario

En lugar de almacenar datos localmente, Eon Mode utiliza una única ubicación de almacenamiento comunal para todos los datos y el catálogo (metadatos). El almacenamiento comunitario es la ubicación de almacenamiento centralizada de la base de datos, compartida entre los nodos de la base de datos.

El almacenamiento comunitario tiene las siguientes propiedades:

- El almacenamiento común en el cloud o el almacenamiento de objetos en las instalaciones es más resiliente y menos susceptible a la pérdida de datos debido a fallos del almacenamiento que el almacenamiento en disco en máquinas individuales.
- Cualquier dato puede ser leído por cualquier nodo con la misma ruta.
- La capacidad no está limitada por el espacio en disco de los nodos.
- Debido a que los datos se almacenan de una manera comunitaria, puede ampliar el clúster con flexibilidad para satisfacer las demandas cambiantes. Si los datos estuvieran almacenados localmente en los nodos, añadir o quitar nodos requeriría mover cantidades considerables de datos entre nodos o bien fuera de los nodos que se van a quitar o a los nodos recién creados.

El almacén

Un inconveniente del almacenamiento común es su velocidad. Tener acceso a los datos desde una ubicación en cloud compartida es más lento que leerlos desde el disco local. Asimismo, la conexión al almacenamiento comunitario puede convertirse en un cuello de botella si muchos nodos leen datos de él a la vez. Para aumentar la velocidad del acceso a los datos, los nodos de una base de datos de Eon Mode mantienen una caché de datos de disco local denominada almacén. Al ejecutar una consulta, los nodos comprueban en primer lugar si los datos que necesitan están en el almacén. Si es así, termina la consulta utilizando la copia local de los datos. Si los datos no están en el almacén, el nodo recupera los datos del almacenamiento comunitario y guarda una copia en el almacén.

Recomendaciones de StorageGRID de NetApp

Vertica almacena datos de bases de datos en el almacenamiento de objetos como miles (o millones) de objetos comprimidos (el tamaño observado es de 200 a 500 MB por objeto. Cuando un usuario ejecuta consultas de base de datos, Vertica recupera el intervalo de datos seleccionado de estos objetos comprimidos en paralelo mediante la llamada GET del intervalo de bytes. Cada BYTE-range GET es aproximadamente de 8 KB.

Durante la prueba de 10 TB del almacén de bases de datos fuera de las consultas de los usuarios, se enviaron a la cuadrícula entre 4,000 y 10,000 solicitudes GET (byte-range GET) por segundo. Cuando se ejecuta esta prueba con dispositivos SG6060, aunque el porcentaje de uso de CPU por nodo del dispositivo es bajo (entre el 20 % y el 30 %), 2/3 veces el tiempo de la CPU espera para I/O. Se observa un porcentaje muy pequeño (0% a 0.5%) de espera de E/S en el SGF6024.

Debido a la alta demanda de IOPS pequeñas con requisitos de latencia muy bajos (la media debe ser inferior a 0.01 segundos), NetApp recomienda utilizar SFG6024 para los servicios de almacenamiento de objetos. Si el SG6060 se necesita para tamaños de base de datos muy grandes, el cliente debe trabajar con el equipo de cuentas de Vertica en el ajuste de tamaño del almacén para admitir el conjunto de datos que se consulta activamente.

Para el nodo Admin y el nodo API Gateway, el cliente puede utilizar el SG100 o SG1000. La elección depende del número de solicitudes de consulta de los usuarios en paralelo y del tamaño de la base de datos. Si el cliente prefiere utilizar un equilibrador de carga de terceros, NetApp recomienda un equilibrador de carga dedicado para la carga de trabajo con demanda de alto rendimiento. Para obtener información sobre cómo ajustar el tamaño de StorageGRID, consulte al equipo de cuentas de NetApp.

Otras recomendaciones de configuración de StorageGRID incluyen:

- **Topología de cuadrícula**. No mezcle el SGF6024 con otros modelos de dispositivos de almacenamiento en el mismo sitio de la red. Si prefiere utilizar el SG6060 para la protección de archivado a largo plazo,

mantenga el SGF6024 con un equilibrador de carga de grid dedicado en su propio sitio de grid (sitio físico o lógico) para una base de datos activa con el fin de mejorar el rendimiento. La mezcla de diferentes modelos de dispositivo en el mismo sitio reduce el rendimiento general in situ.

- **Protección de datos**. Use copias replicadas para proteger. No utilice código de borrado para una base de datos activa. El cliente puede utilizar códigos de borrado para proteger bases de datos inactivas a largo plazo.
- **No active la compresión de red**. Vertica comprime objetos antes de almacenarlos en almacenamiento de objetos. Habilitar la compresión de grid no ahorra aún más el uso del almacenamiento y reduce de forma significativa el rendimiento A nivel de byte.
- **HTTP frente a HTTPS S3 Endpoint connection**. Durante las pruebas de prueba de rendimiento, observamos una mejora del rendimiento del 5% al utilizar una conexión HTTP S3 del clúster Vertica al extremo del equilibrador de carga de StorageGRID. Esta opción debe basarse en los requisitos de seguridad del cliente.

Las recomendaciones para una configuración de Vertica incluyen:

- **La configuración predeterminada del almacén de la base de datos Vertica está activada (valor = 1) para las operaciones de lectura y escritura**. NetApp recomienda mantener la configuración de estos almacenes habilitada para mejorar el rendimiento.
- **Desactive las limitaciones de streaming**. Para obtener información detallada sobre la configuración, consulte la sección Desactivación de las limitaciones de la transmisión.

Instalación del modo Eon en las instalaciones con almacenamiento común en StorageGRID

En las siguientes secciones se describe el procedimiento para instalar el modo Eon en las instalaciones con almacenamiento común en StorageGRID. El procedimiento para configurar un almacenamiento de objetos compatible con simple Storage Service (S3) en las instalaciones es similar al procedimiento descrito en la guía de Vertica, "Instale una base de datos Eon Mode en las instalaciones".

Para la prueba funcional se utilizó la siguiente configuración:

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Tres máquinas virtuales (VM) con CentOS 7.x OS para nodos Vertica y formar un clúster. Esta configuración es sólo para la prueba funcional, no para el clúster de base de datos de producción Vertica.

Estos tres nodos se configuran con una clave Secure Shell (SSH) para permitir a SSH sin una contraseña entre los nodos del clúster.

Información necesaria de StorageGRID de NetApp

Para instalar Eon Mode en las instalaciones con almacenamiento comunitario en StorageGRID, debe tener la siguiente información de requisitos previos.

- La dirección IP o el nombre de dominio completo (FQDN) y el número de puerto del extremo de StorageGRID S3. Si utiliza HTTPS, utilice una entidad de certificación (CA) personalizada o un certificado SSL autofirmado implementado en el extremo de StorageGRID S3.
- Nombre del bloque. Debe existir previamente y estar vacío.
- El ID de clave de acceso y la clave de acceso secreta con acceso de lectura y escritura al bloque.

Creación de un archivo de autorización para acceder al extremo de S3

Los siguientes requisitos previos se aplican al crear un archivo de autorización para acceder al extremo de S3:

- Vertica está instalada.
- Un clúster está configurado, configurado y listo para la creación de bases de datos.

Para crear un archivo de autorización para acceder al extremo de S3, siga estos pasos:

1. Inicie sesión en el nodo Vertica donde se ejecutará `admintools` Para crear la base de datos Eon Mode.

   El usuario predeterminado es `dbadmin`, Creado durante la instalación del clúster Vertica.

2. Utilice un editor de texto para crear un archivo en la `/home/dbadmin` directorio. El nombre del archivo puede ser cualquier cosa que desee, por ejemplo, `sg_auth.conf`.
3. Si el extremo de S3 utiliza un puerto HTTP 80 o un puerto HTTPS 443 estándar, omita el número del puerto. Para utilizar HTTPS, configure los siguientes valores:

   ◦ `awsenablehttps = 1`, de lo contrario, establezca el valor en `0`.

   ◦ `awsauth = <s3 access key ID>:<secret access key>`

   ◦ `awsendpoint = <StorageGRID s3 endpoint>:<port>`

   Para usar una CA personalizada o un certificado SSL autofirmado para la conexión HTTPS de extremo StorageGRID S3, especifique la ruta de archivo completa y el nombre de archivo del certificado. Este archivo debe estar en la misma ubicación de cada nodo Vertica y tener permiso de lectura para todos los usuarios. Omita este paso si la CA conocida públicamente firma del certificado SSL de extremo de StorageGRID S3.

   - `awscafile = <filepath/filename>`

   Por ejemplo, consulte el siguiente archivo de ejemplo:

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

+

> En un entorno de producción, el cliente debe implementar un certificado de servidor firmado por una CA conocida públicamente en un extremo de equilibrador de carga de StorageGRID S3.

Elegir una ruta de almacén en todos los nodos de Vertica

Seleccione o cree un directorio en cada nodo para la ruta de almacenamiento del almacén. El directorio que suministre para el parámetro de ruta de almacenamiento del almacén debe tener lo siguiente:

- La misma ruta en todos los nodos del clúster (por ejemplo, `/home/dbadmin/depot`)

- El usuario dbadmin puede leer y escribir
- Almacenamiento suficiente

  De forma predeterminada, Vertica utiliza el 60% del espacio del sistema de archivos que contiene el directorio para el almacenamiento del almacén. Puede limitar el tamaño del almacén mediante el `--depot-size` en el `create_db` comando. Consulte "Ajuste de tamaño del clúster Vertica para una base de datos en modo Eon" artículo para las pautas generales de ajuste de tamaño de Vertica o consulte con su gestor de cuentas de Vertica.

  La `admintools create_db` la herramienta intenta crear la ruta del almacén para usted si no existe.

Creación de la base de datos Eon en las instalaciones

Para crear la base de datos Eon en las instalaciones, siga estos pasos:

1. Para crear la base de datos, utilice `admintools create_db` herramienta.

   La siguiente lista proporciona una breve explicación de los argumentos utilizados en este ejemplo. Consulte el documento Vertica para obtener una explicación detallada de todos los argumentos necesarios y opcionales.

   - -x <path/filename of authorization file created in “Creación de un archivo de autorización para acceder al extremo de S3” >.

     Los detalles de autorización se almacenan dentro de la base de datos después de haber creado correctamente. Puede eliminar este archivo para evitar exponer la clave secreta de S3.

   - --comunal-almacenamiento-ubicación <s3://storagegrid bucketname>
   - -S <comma-separated list of Vertica nodes to be used for this database>
   - -d <name of database to be created>
   - -p <password to be set for this new database>. Por ejemplo, consulte el siguiente comando de ejemplo:

     ```
     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>'
     ```

     La creación de una nueva base de datos tarda varios minutos en función del número de nodos de la base de datos. Al crear la base de datos por primera vez, se le solicitará que acepte el Contrato de licencia.

Por ejemplo, consulte el siguiente archivo de autorización de ejemplo y. `create db` comando:

```
[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.
```

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
61	s3://vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a07_0_0.dfs
145	s3://vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a3d_0_0.dfs
146	s3://vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a1d_0_0.dfs

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs
34	s3://vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25_0_0.dfs
41	s3://vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d_0_0.dfs
61	s3://vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a5d_0_0.dfs
131	s3://vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a19_0_0.dfs
91	s3://vertica/5f7/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a11_0_0.dfs
118	s3://vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a15_0_0.dfs
115	s3://vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a61_0_0.dfs

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs
38	s3://vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a49_0_0.dfs
38	s3://vertica/eba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a59_0_0.dfs
21521920	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000215e2.tar
6865408	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar
53947904	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219ba.tar
44932608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de.tar
256306688	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a6e.tar
8062464	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e34.tar
20024832	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021e70.tar
10444	s3://vertica/metadata/VMart/cluster_config.json
823266	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/chkpt_1.cat.gz

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/completed
822521	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/chkpt_1.cat.gz
231	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c4_4/completed
746513	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g14.cat
2596	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_3_g3.cat.gz
821065	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_4_g4.cat.gz
6440	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_5_g5.cat
8518	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_8_g8.cat

Tamaño del objeto (byte)	Ruta completa de clave de bloque/objeto
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
822930	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Desactivación de las limitaciones de la transmisión

Este procedimiento se basa en la guía de Vertica para otro almacenamiento de objetos en las instalaciones y debe ser aplicable a StorageGRID.

1. Después de crear la base de datos, desactive la `AWSStreamingConnectionPercentage` configuración del parámetro configurándolo como `0`. Esta configuración es innecesaria para una instalación local en modo Eon con almacenamiento común. Este parámetro de configuración controla el número de conexiones al almacén de objetos que Vertica utiliza para las lecturas en streaming. En un entorno cloud, esta configuración ayuda a evitar que la transmisión de datos del almacén de objetos utilice todos los identificadores de archivos disponibles. Deja algunos identificadores de archivos disponibles para otras operaciones de almacén de objetos. Debido a la baja latencia de los almacenes de objetos en las instalaciones, esta opción es innecesaria.
2. Utilice un `vsql` instrucción para actualizar el valor del parámetro. La contraseña es la contraseña de la base de datos que se establece en “creación de la base de datos Eon en las instalaciones”. Por ejemplo, consulte el siguiente resultado de muestra:

```
[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
```

Verificación de la configuración del almacén

La configuración predeterminada del almacén de la base de datos Vertica está habilitada (valor = 1) para las operaciones de lectura y escritura. NetApp recomienda mantener la configuración de estos almacenes habilitada para mejorar el rendimiento.

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

Carga de datos de muestra (opcional)

Si esta base de datos se utiliza para realizar pruebas y se eliminará, puede cargar datos de ejemplo en esta base de datos para realizar pruebas. Vertica incluye un conjunto de datos de muestra, VMart, que se encuentra en `/opt/vertica/examples/VMart_Schema/` En cada nodo Vertica. Puede encontrar más información acerca de este conjunto de datos de ejemplo "aquí".

Siga estos pasos para cargar los datos de ejemplo:

1. Inicie sesión como dbadmin en uno de los nodos Vertica: cd /opt/vertica/examples/VMart_Schema/
2. Cargue los datos de ejemplo en la base de datos e introduzca la contraseña de la base de datos cuando

se le solicite en los subpasos c y d:

a. `cd /opt/vertica/examples/VMart_Schema`

b. `./vmart_gen`

c. `vsql < vmart_define_schema.sql`

d. `vsql < vmart_load_data.sql`

3. Hay varias consultas SQL predefinidas, puede ejecutar algunas de ellas para confirmar que los datos de prueba se han cargado correctamente en la base de datos. Por ejemplo: `vsql < vmart_queries1.sql`

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- "Documentación de producto de NetApp StorageGRID 11,7"
- "Especificaciones técnicas de StorageGRID"
- "Documentación de producto de Vertica 10.1"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Septiembre de 2021	Versión inicial.

Por Angela Cheng

Análisis de registros de StorageGRID mediante pila ELK

Por Angela Cheng

Con la función StorageGRID syslog forward, es posible configurar un servidor de syslog externo para recoger y analizar mensajes de registro de StorageGRID. ELK (Elasticsearch, Logstash, Kibana) se ha convertido en una de las soluciones de análisis de registros más populares. Observe el "Análisis de registros de StorageGRID mediante vídeo ELK" para ver una configuración ELK de muestra y cómo se puede utilizar para identificar y solucionar problemas de solicitudes S3 fallidas. StorageGRID 11,9 admite la exportación del registro de acceso de extremo del equilibrador de carga a un servidor syslog externo. Vea esto "Vídeo de YouTube" para obtener más información sobre esta nueva función. Este artículo proporciona archivos de ejemplo de configuración de Logstash, consultas de Kibana, gráficos y panel para ofrecerle un inicio rápido para la gestión de registros y análisis de StorageGRID.

Requisitos

- StorageGRID 11.6.0.2 o superior
- ELK (Elasticsearch, Logstash y Kibana) 7.1x o superior instalado y en funcionamiento

Archivos de ejemplo

- "Descargue el paquete de archivos de ejemplo Logstash 7.x." + **md5 checksum** 148c23d0021d9a4bb4a6c0287464deab + **sha256 checksum** f51ec9e2e3f842d5a7861566b167a561b4373b4e7bb3c8b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b3b5
- "Descargue el paquete de archivos de ejemplo Logstash 8.x." + **md5 checksum** e11bae3a662f87c310ef363d0fe06835 + **sha256 checksum** 5c670755742cfdfd5aa7a596ba087e0153a65bcaef3934afdb682f6cd1278d
- "Descargue el paquete de archivos de ejemplo Logstash 8.x para StorageGRID 11,9" + **md5 suma de comprobación** 41272857c4a54600f95995f6ed74800d + **sha256 suma de comprobación** 67048eee8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

Suposición

Los lectores están familiarizados con la terminología y las operaciones de StorageGRID y ELK.

Instrucción

Se proporcionan dos versiones de ejemplo debido a diferencias en los nombres definidos por patrones de gruñido. + por ejemplo, el patrón de grok SYSLOGBASE en el archivo de configuración Logstash define los nombres de campo de forma diferente dependiendo de la versión de Logstash instalada.

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

Muestra de Logstash 7.17

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

Muestra de Logstash 8.23

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

- Pasos*

1. Descomprima el ejemplo proporcionado en función de la versión DE ELK instalada. + la carpeta de ejemplo incluye dos muestras de configuración de Logstash: + **sglog-2-file.conf:** este archivo de configuración envía mensajes de registro StorageGRID a un archivo en Logstash sin transformación de datos. Puede utilizar esta opción para confirmar que Logstash recibe mensajes de StorageGRID o para comprender los patrones de registro de StorageGRID. + **sglog-2-es.conf:** este archivo de configuración transforma los mensajes de registro StorageGRID utilizando varios patrones y filtros. Incluye ejemplos de sentencias DROP, que devuelven mensajes basados en patrones o filtros. La salida se envía a Elasticsearch para indizar. + Personalice el archivo de configuración seleccionado de acuerdo con la instrucción dentro del archivo.
2. Pruebe el archivo de configuración personalizado:

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

   Si la última línea devuelta es similar a la siguiente, el archivo de configuración no tiene errores de sintaxis:

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

3. Copie el archivo conf personalizado en la configuración del servidor Logstash: /Etc/logstash/conf.d + Si no ha habilitado config.reload.automatic en /etc/logstash/logstash.yml, reinicie el servicio Logstash. De lo contrario, espere a que transcurra el intervalo de recarga de la configuración.

```
 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. Compruebe /var/log/logstash/logstash-plain.log y confirme que no hay errores al iniciar Logstash con el nuevo archivo de configuración.
5. Confirme que el puerto TCP se ha iniciado y que está escuchando. + en este ejemplo, se utiliza el puerto TCP 5000.

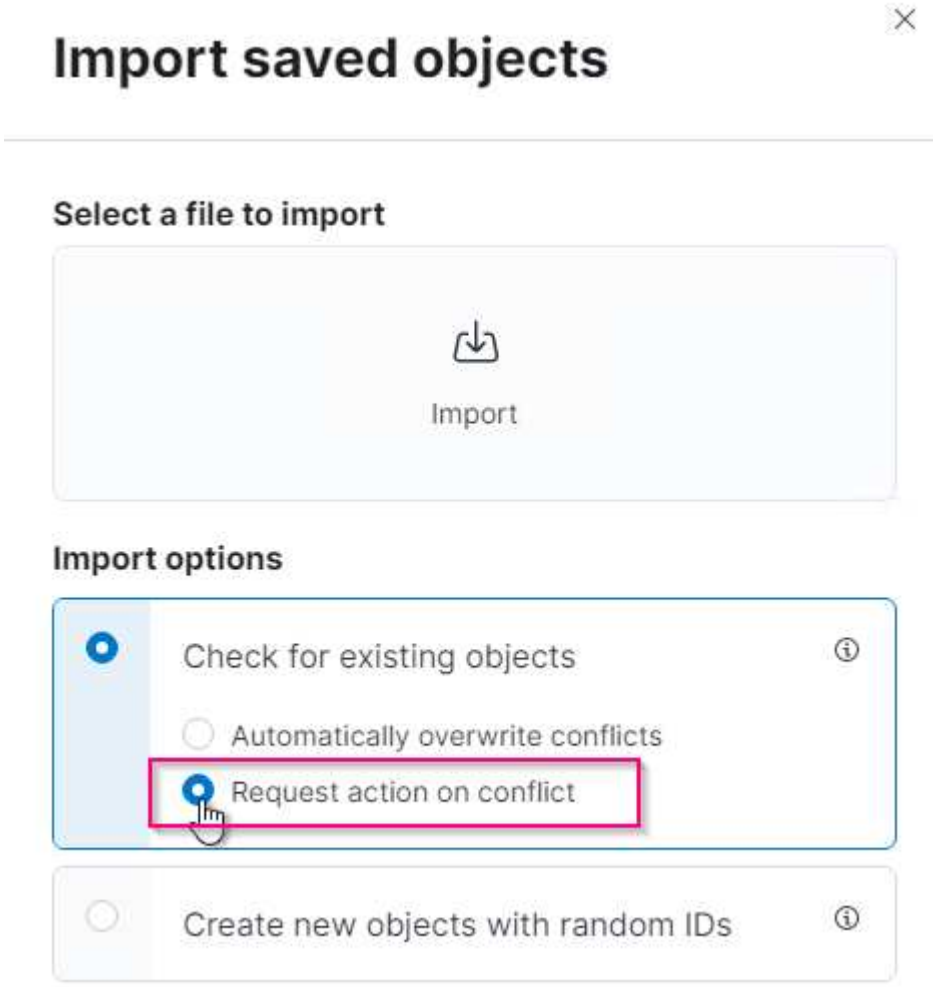
```
netstat -ntpa | grep 5000
tcp6       0      0 :::5000                 :::*
LISTEN      25744/java
```

6. Desde la interfaz gráfica de usuario del administrador StorageGRID, configure el servidor de syslog externo para que envíe mensajes de registro a Logstash. Consulte la "vídeo de demostración" para obtener más información.

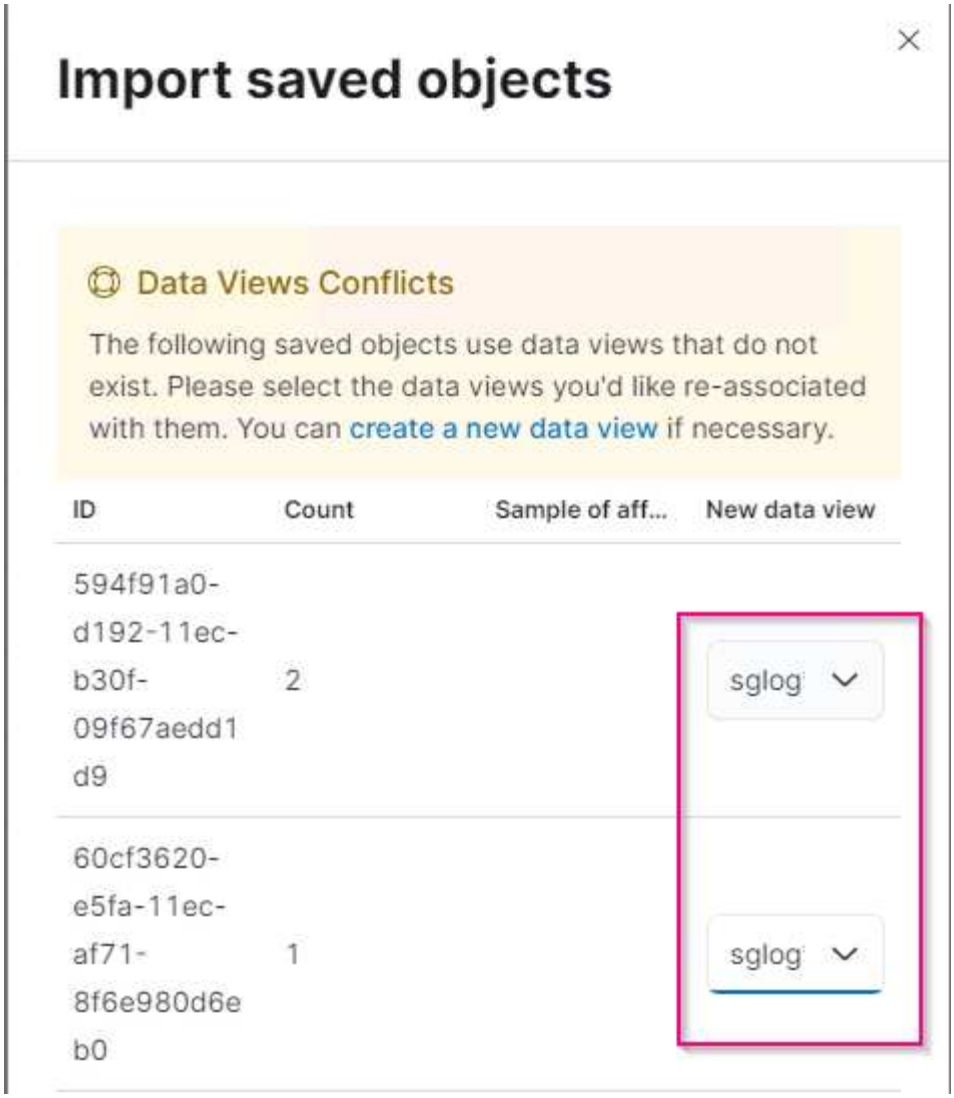
7. Debe configurar o deshabilitar el firewall en el servidor Logstash para permitir la conexión de nodos StorageGRID al puerto TCP definido.
8. En la interfaz gráfica de usuario de Kibana, seleccione Management → Dev Tools. En la página Console, ejecute este comando GET para confirmar que se han creado nuevos índices en Elasticsearch.

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

9. Desde la GUI de Kibana, cree un patrón de índice (ELK 7.x) o una vista de datos (ELK 8.x).
10. En la GUI de Kibana, escriba "objetos afeitados" en el cuadro de búsqueda que se encuentra en el centro superior. + en la página objetos guardados, seleccione Importar. En Opciones de importación, seleccione "solicitar acción en conflicto"



Importe eleLIMPORT <version>-QUERY-chart-sample.ndjson. + cuando se le solicite que resuelva el conflicto, seleccione el patrón de índice o la vista de datos que creó en el paso 8.



Se importan los siguientes objetos de Kibana: + **Query** + * audit-msg-s3rq S3-orlm + * bycast log S3 S3 mensajes relacionados + * loglevel warning o superior + * failed security event + * nginx-gw endpoint access log (disponible solo en elk8-sample-for-sg119.zip) + **Chart** + * S3 solicitudes cuentan basadas en bycast.log + * código de estado HTTP + *

Ahora está listo para realizar el análisis de registros de StorageGRID con Kibana.

Recursos adicionales

- "syslog101"
- "¿Qué es LA pila ELK"
- "Lista de patrones GROK"
- "Guía para principiantes de Logstash: GROK"
- "Una guía práctica para Logstash: Syslog profundizar"
- "Guía de Kibana: Explorar el documento"
- "Referencia de mensajes de registro de auditoría de StorageGRID"

Utilice Prometheus y Grafana para ampliar la retención de métricas

Por Aron Klein

Este informe técnico proporciona instrucciones detalladas para configurar NetApp StorageGRID con servicios externos Prometheus y Grafana.

Introducción

StorageGRID almacena métricas mediante Prometheus y proporciona visualizaciones de estas métricas a través de los paneles de Grafana integrados. Se puede acceder a las métricas de Prometheus de manera segura desde StorageGRID mediante la configuración de certificados de acceso de clientes y la habilitación del acceso a prometheus para el cliente especificado. Hoy en día, la retención de estos datos métricos está limitada por la capacidad de almacenamiento del nodo de administración. Para obtener una mayor duración y una capacidad para crear visualizaciones personalizadas de estas métricas, implementaremos un nuevo servidor Prometheus y Grafana, configuraremos nuestro nuevo servidor para reunir las métricas de la instancia de StorageGRIDs y creamos un panel con las métricas que somos importantes para nosotros. Puede obtener más información sobre las métricas de Prometheus recopiladas en el "Documentación de StorageGRID".

Federar Prometheus

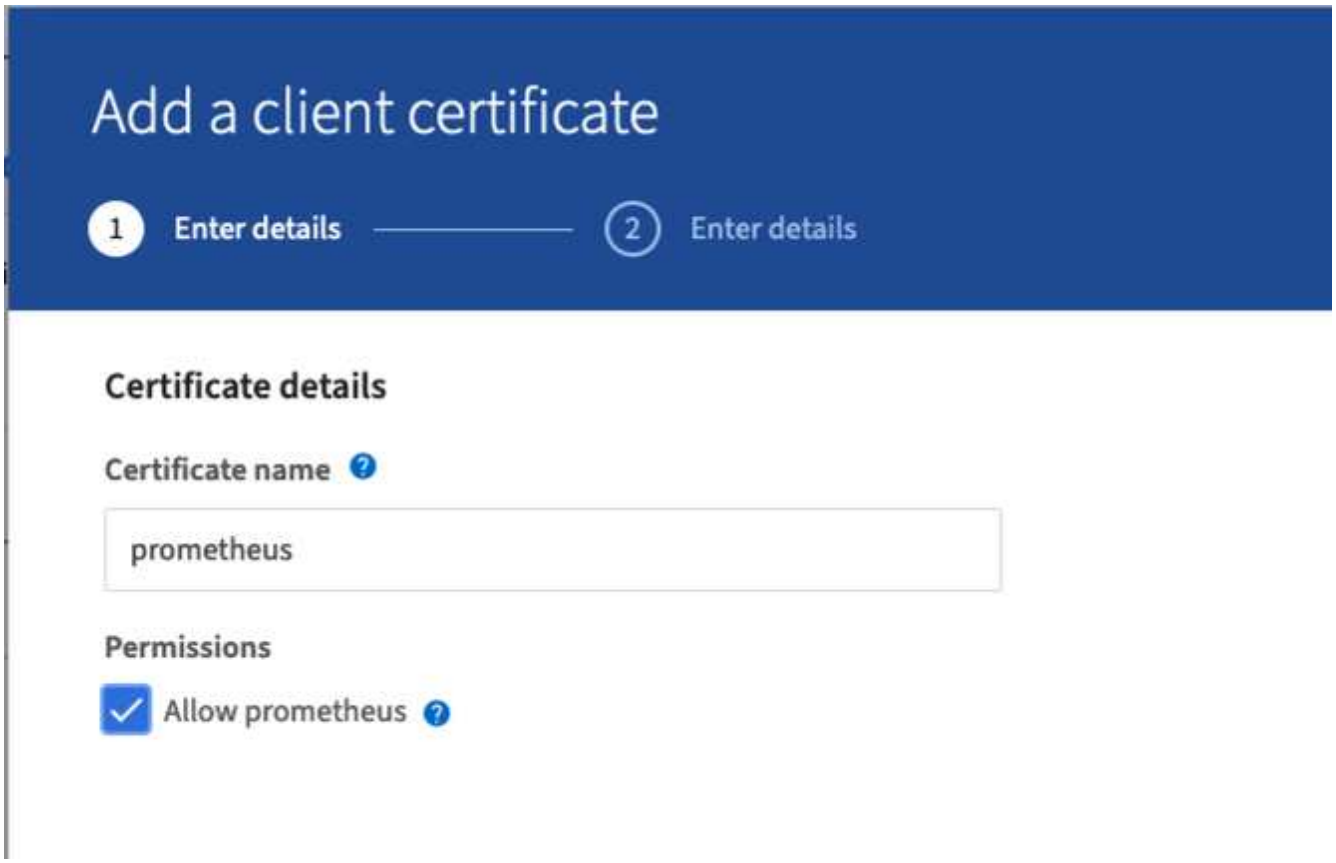
Detalles del laboratorio

A efectos de este ejemplo, usaré todas las máquinas virtuales para nodos StorageGRID 11.6 y un servidor Debian 11. La interfaz de gestión StorageGRID se configura con un certificado de CA de confianza pública. Este ejemplo no pasará por la instalación y configuración del sistema StorageGRID o la instalación de Debian linux. Puede utilizar cualquier sabor de Linux que desee, con el apoyo de Prometheus y Grafana. Tanto Prometheus como Grafana pueden instalar como contenedores Docker, crear a partir de código fuente o binarios precompilados. En este ejemplo, instalaré los binarios Prometheus y Grafana directamente en el mismo servidor Debian. Descargue y siga las instrucciones de instalación básica de https://prometheus.io y.. https://grafana.com/grafana/ respectivamente.

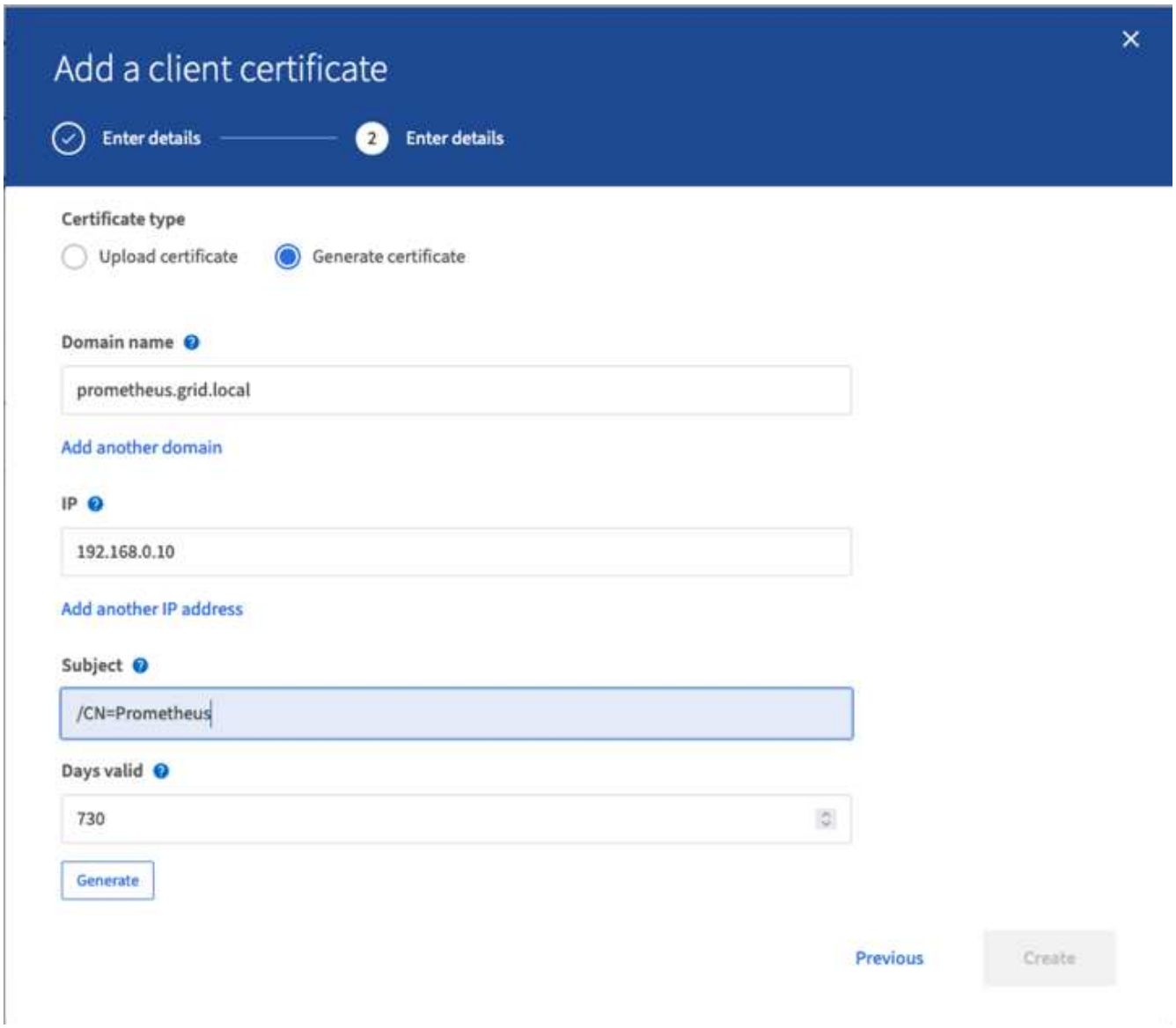
Configure StorageGRID para el acceso de Prometheus Client

Para poder acceder a las métricas de prometheus almacenadas de StorageGRID, debe generar o cargar un certificado de cliente con clave privada y habilitar el permiso para el cliente. La interfaz de gestión de StorageGRID debe tener un certificado SSL. El servidor prometheus debe confiar en este certificado mediante una CA de confianza o de forma manual si se firma automáticamente. Para leer más, visite la "Documentación de StorageGRID".

1. En la interfaz de gestión StorageGRID, seleccione "CONFIGURACIÓN" en la parte inferior izquierda y, en la segunda columna de "Seguridad", haga clic en certificados.
2. En la página certificados, seleccione la ficha "Cliente" y haga clic en el botón "Agregar".
3. Proporcione un nombre para el cliente al que se le otorgará acceso y que utilice este certificado. Haga clic en la casilla de "permisos", delante de "permitir Prometheus" y haga clic en el botón continuar.

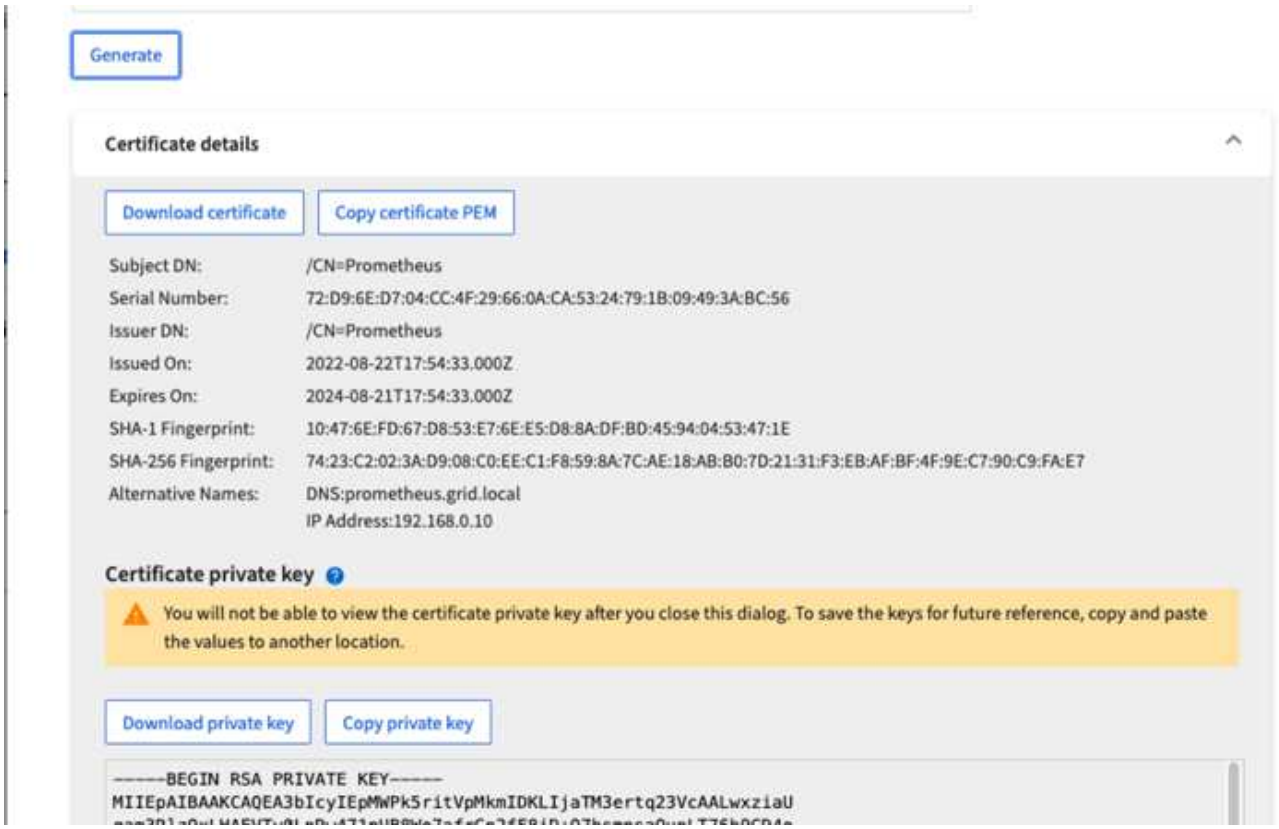


4. Si tiene un certificado firmado por CA, puede seleccionar el botón de opción "cargar certificado", pero en nuestro caso vamos a dejar que StorageGRID genere el certificado de cliente seleccionando el botón de opción "generar certificado". Los campos obligatorios se mostrarán para rellenar. Introduzca el FQDN del servidor cliente, la IP del servidor, el asunto y los días válidos. A continuación, haga clic en el botón "generar".



> 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. Descargue el archivo pem del certificado y el archivo pem de la clave privada.



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

Preparar el servidor Linux para la instalación de Prometheus

Antes de instalar Prometheus, quiero preparar mi entorno con un usuario Prometheus, la estructura de directorio y configurar la capacidad para la ubicación del almacenamiento de métricas.

1. Cree el usuario Prometheus.

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

2. Crear los directorios de Prometheus, certificado de cliente y datos de métricas.

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

3. He formateado el disco que estoy usando para la retención de métricas con un sistema de archivos ext4.

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

4. A continuación, he montado el sistema de archivos en el directorio de métricas Prometheus.

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

5. Obtenga el UUID del disco que utiliza para los datos de métricas.

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

6. Agregar una entrada en /etc/fstab/ haciendo que el montaje persista en reinicios utilizando el UUID de /dev/sdb.

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

Instalar y configurar Prometheus

Ahora que el servidor está listo, puedo iniciar la instalación de Prometheus y configurar el servicio.

1. Extraiga el paquete de instalación Prometheus

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

2. Copie los archivos binarios en /usr/local/bin y cambie la propiedad al usuario prometheus creado anteriormente

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

3. Copie las consolas y bibliotecas en /etc/prometheus

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

4. Copie el certificado de cliente y los archivos de pem de claves privadas descargados anteriormente de StorageGRID a /etc/prometheus/certs
5. Cree el archivo yaml de configuración de prometheus

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

6. Inserte la siguiente configuración. El nombre del trabajo puede ser cualquier cosa que desee. Cambie el "-Targets: ["]" al FQDN del nodo admin y, si modificó los nombres del certificado y los nombres de los archivos de claves privadas, actualice la sección tls_config para que coincida. a continuación, guarde el archivo. Si la interfaz de gestión de grid utiliza un certificado autofirmado, descargue el certificado y colóquelo con el certificado de cliente con un nombre único, y en la sección tls_config añada CA_file: /Etc/prometheus/cert/UIcert.pem

   a. En este ejemplo estoy recopilando todas las métricas que empiezan con alertManager, cassandra, nodo y StorageGRID. Puede ver más información sobre la métrica Prometheus en la "Documentación de 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']
```

> Si la interfaz de gestión de grid utiliza un certificado autofirmado, descargue el certificado y colóquelo con el certificado de cliente con un nombre único. En la sección tls_config, agregue el certificado encima del certificado de cliente y las líneas de clave privada
>
> ```
> ca_file: /etc/prometheus/cert/UIcert.pem
> ```

1. Cambie la propiedad de todos los archivos y directorios en /etc/prometheus y /var/lib/prometheus al usuario prometheus

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

2. Cree un archivo de servicio prometheus en /etc/systemd/system

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

3. Inserte las siguientes líneas, observe el --Storage.tsdb.retention.time=1 año que establece la retención de los datos de la métrica en 1 año. También puede usar --Storage.tsdb.retention.size=300GIB para basar la retención en los límites de almacenamiento. Esta es la única ubicación donde se establece la retención de las métricas.

```
[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. Vuelva a cargar el servicio systemd para registrar el nuevo servicio prometheus. a continuación, inicie y habilite el servicio prometheus.

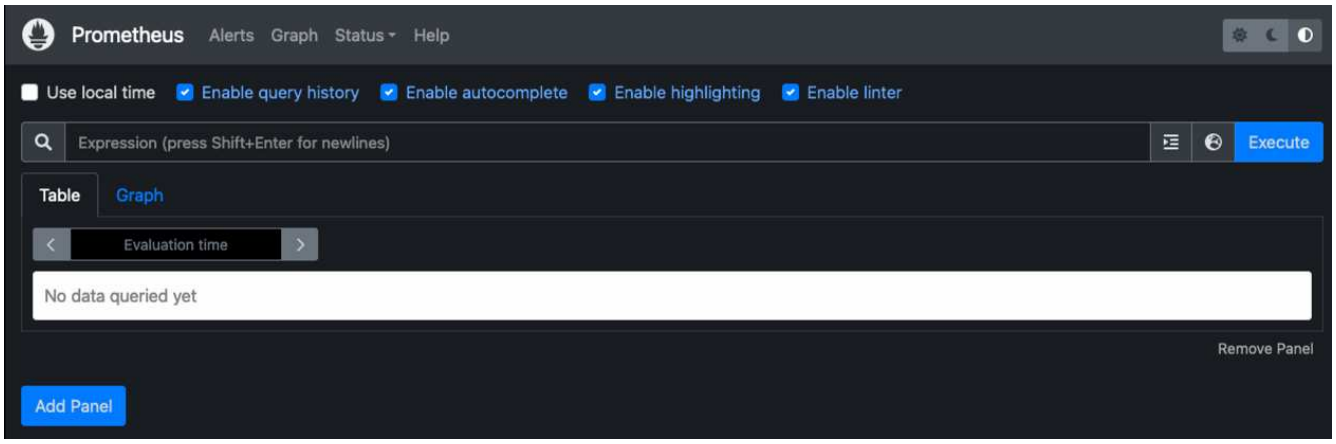
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Compruebe que el servicio está funcionando correctamente

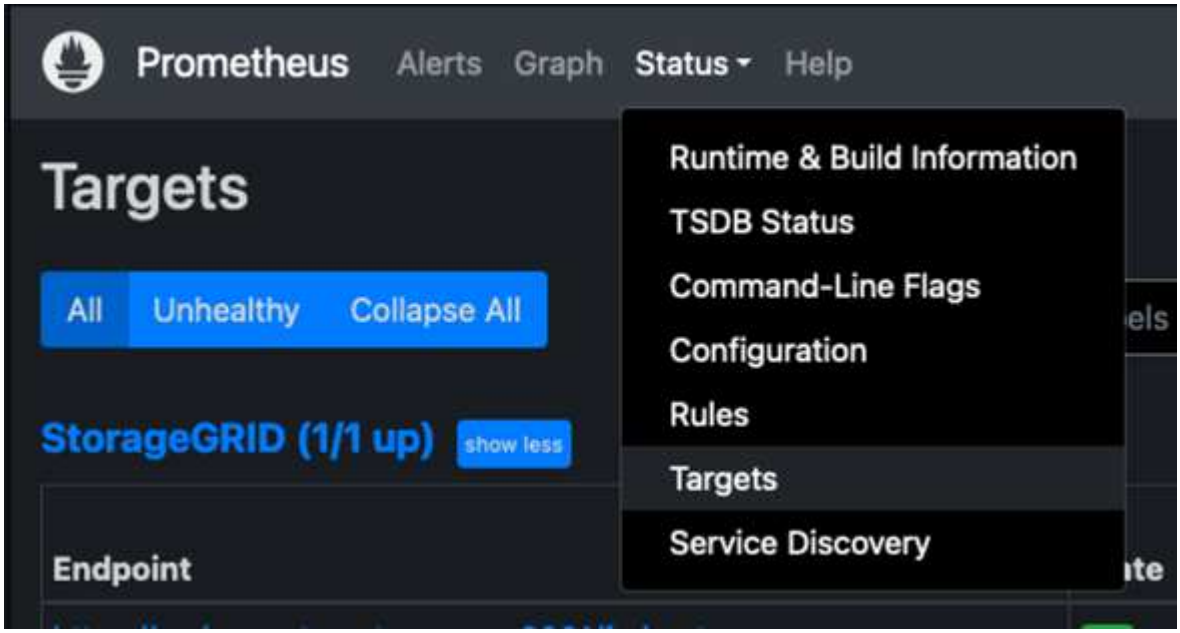
```
sudo systemctl status prometheus
```

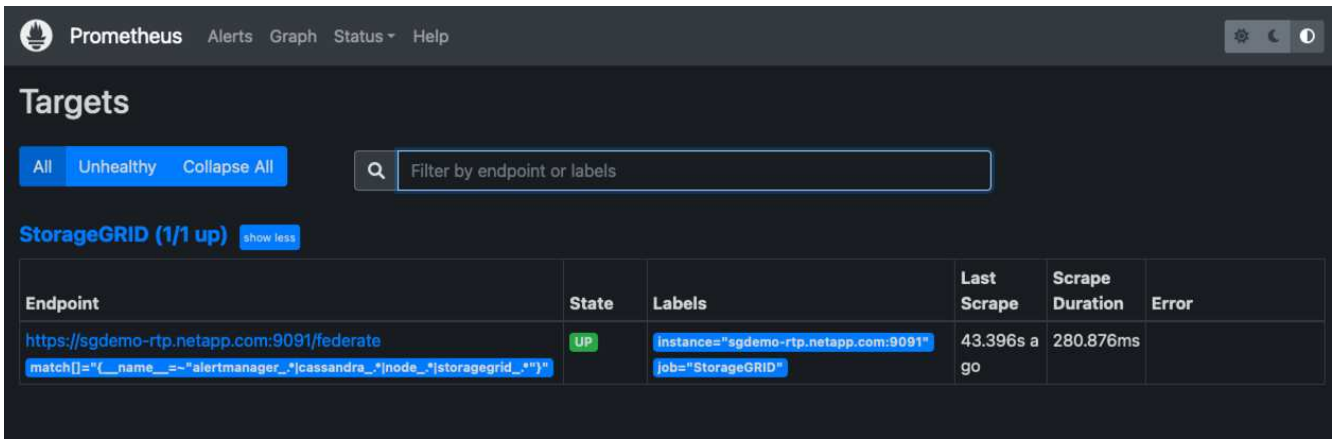
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 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. Ahora debe poder acceder a la interfaz de usuario de su servidor prometheus http://Prometheus-server:9090 Y ver la interfaz de usuario

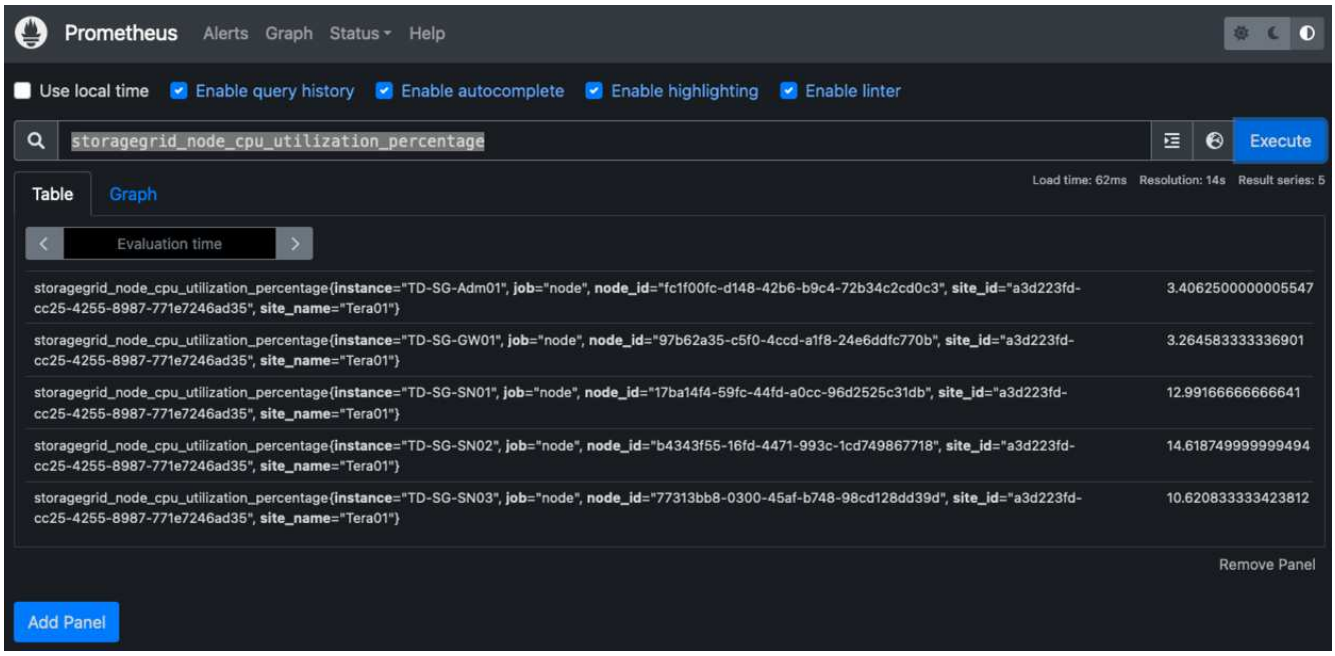


7. En "Estado", puede ver el estado del extremo StorageGRID que hemos configurado en prometheus.yml





8. En la página Graph, puede ejecutar una consulta de prueba y comprobar que los datos se están raspando correctamente. Por ejemplo, introduzca "storagegrid_node_cpu_Utilization_porcentual" en la barra de consultas y haga clic en el botón Execute.



Instalar y configurar Grafana

Ahora que prometheus está instalado y en funcionamiento, podemos pasar a la instalación de Grafana y configurar una consola

Grafana Instalation

1. Instale la última edición empresarial de Grafana

```
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. Añada este repositorio para versiones estables:

```
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. Después de agregar el repositorio.

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

4. Vuelva a cargar el servicio systemd para registrar el nuevo servicio grafana. A continuación, inicie y habilite el servicio Grafana.

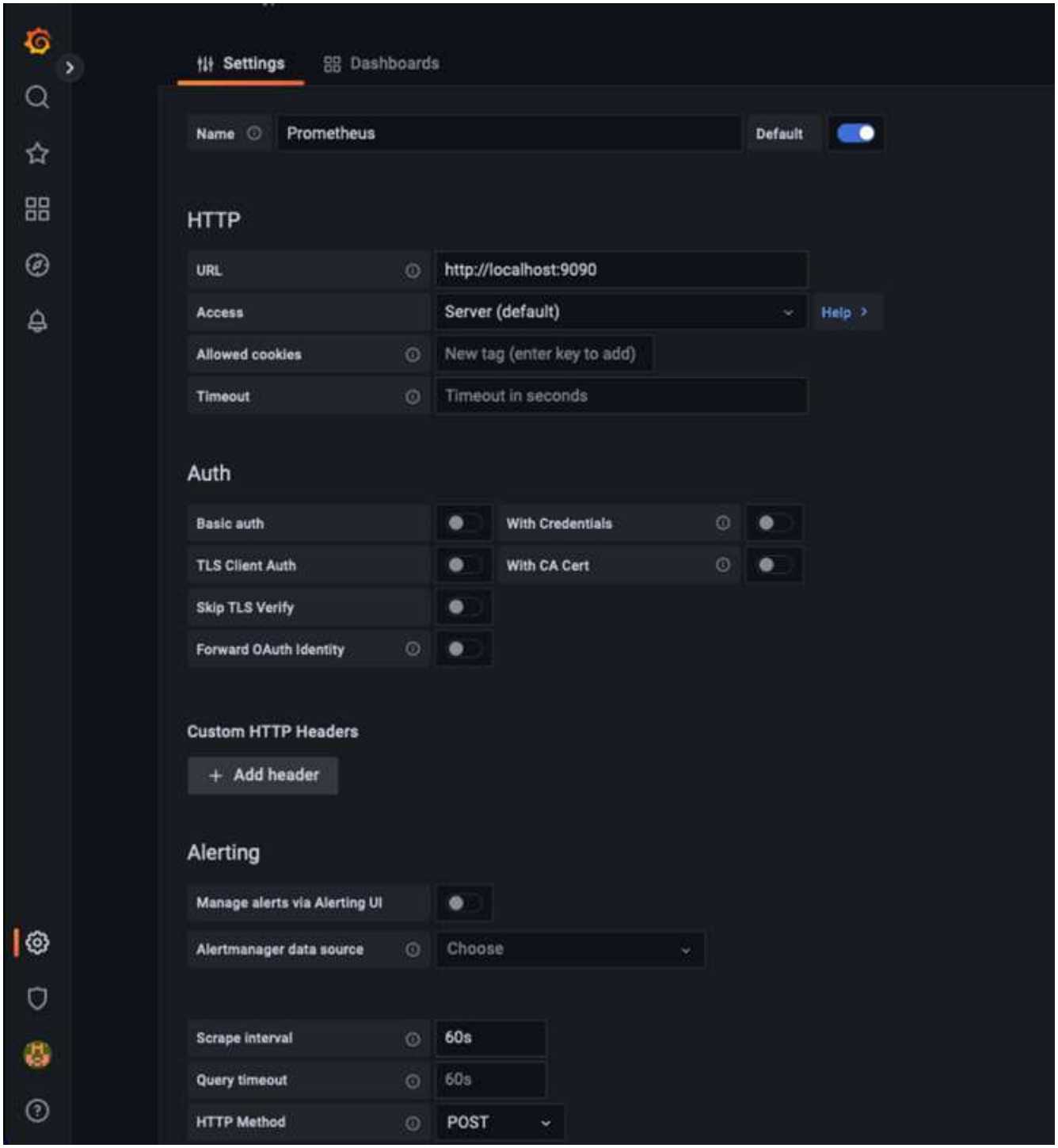
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana ya está instalado y en funcionamiento. Cuando abra un navegador a HTTP://Prometheus-Server:3000 recibirá la página de inicio de sesión de Grafana.
6. Las credenciales de inicio de sesión predeterminadas son admin/admin, y debe configurar una contraseña nueva cuando le solicite.

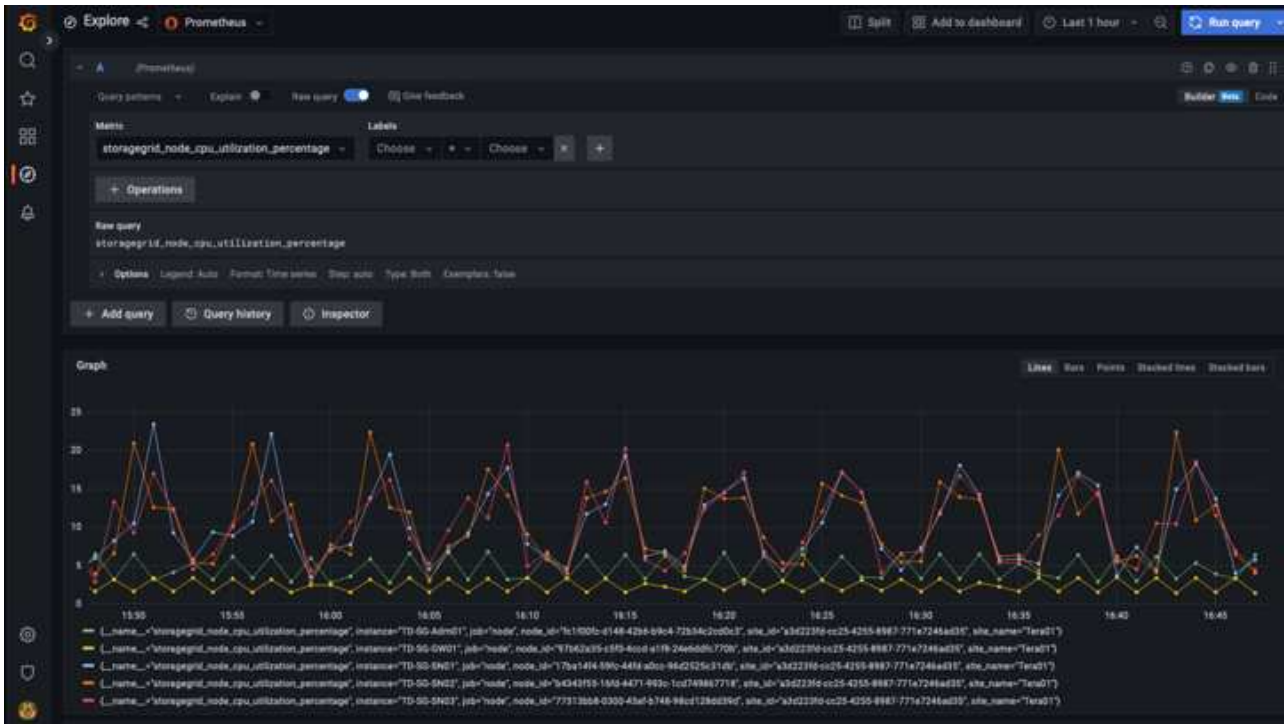
Cree un panel de Grafana para StorageGRID

Con Grafana y Prometheus instalados y en ejecución, ahora es hora de conectar los dos mediante la creación de un origen de datos y la creación de un panel

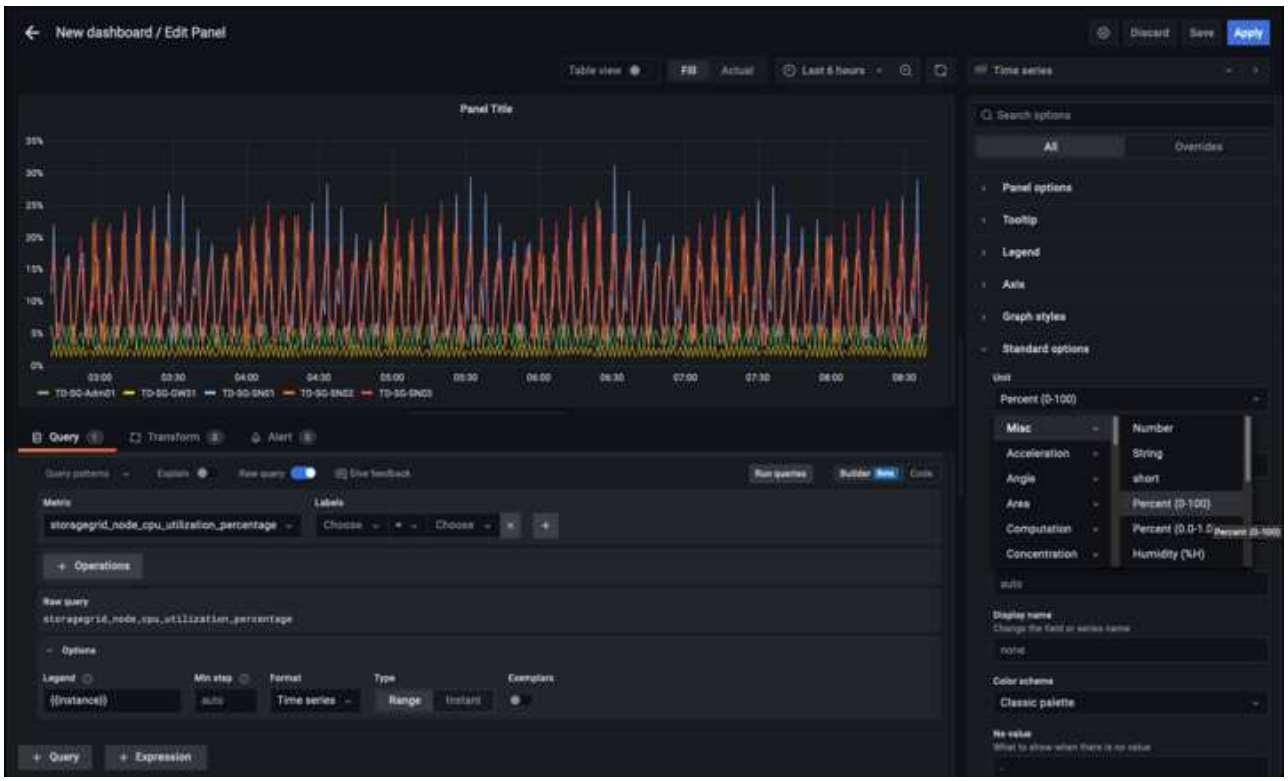
1. En el panel izquierdo, expanda "Configuración" y seleccione "orígenes de datos" y, a continuación, haga clic en el botón "Agregar origen de datos"
2. Prometheus será una de las principales fuentes de datos entre las que elegir. Si no lo es, utilice la barra de búsqueda para localizar "Prometheus"
3. Para configurar el origen Prometheus, introduzca la URL de la instancia prometheus y el intervalo de raspado para que coincidan con el intervalo Prometheus. También he deshabilitado la sección de alertas, ya que no configuré el administrador de alertas en prometheus.



4. Con la configuración deseada introducida, desplácese hacia abajo hasta la parte inferior y haga clic en "Guardar y probar"
5. Una vez que la prueba de configuración se haya realizado correctamente, haga clic en el botón explorar.
    a. En la ventana explorar, puede utilizar la misma métrica que probamos Prometheus con "storagegrid_node_cpu_Utilization_porcentual" y hacer clic en el botón "Ejecutar consulta"



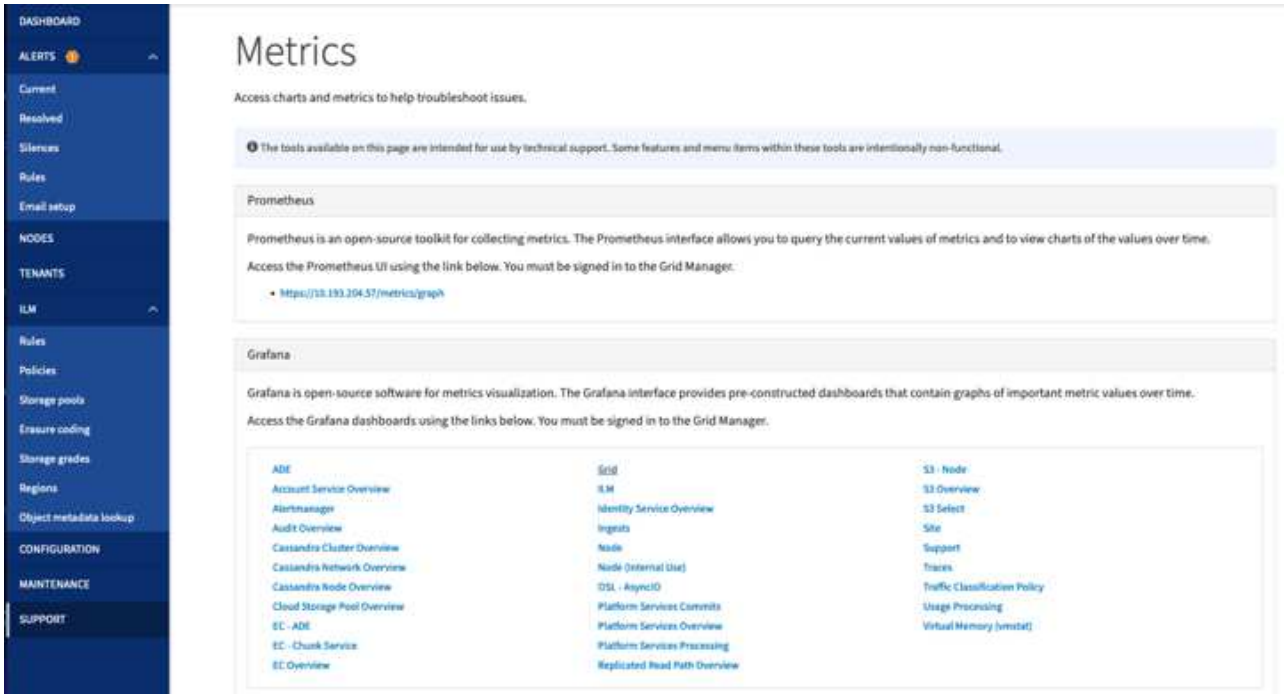
6. Ahora que tenemos configurado el origen de datos, podemos crear un panel de control.
   a. En el panel izquierdo, expanda "Paneles" y seleccione "+ New Dashboard".
   b. Seleccione "Añadir un nuevo panel"
   c. Configure el nuevo panel seleccionando una métrica, de nuevo utilizaré "storagegrid_node_cpu_Utilization_Percent", Introduzca un título para el panel, expanda "Opciones" en la parte inferior y para que la leyenda cambie a personalizado e introduzca "{{Instance}" para definir los nombres de los nodos y, en el panel derecho, en "Opciones estándar", defina "Unidad" en "Misc-100). A continuación, haga clic en "aplicar" para guardar el panel en el tablero de a bordo.



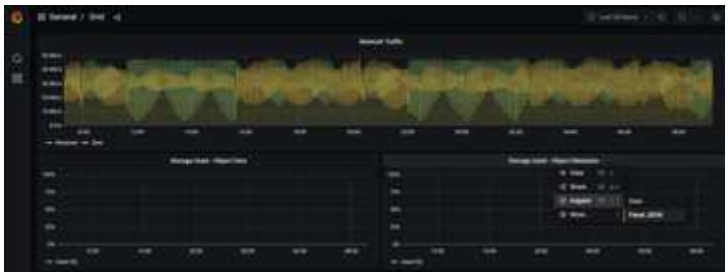
7. Podríamos seguir desarrollando nuestro panel de control como este para cada métrica que deseamos, pero por suerte StorageGRID ya dispone de paneles con paneles que podemos copiar en nuestros paneles personalizados.

   a. En el panel izquierdo de la interfaz de gestión de StorageGRID, seleccione «Soporte» y, en la parte inferior de la columna «Herramientas», haga clic en «Métricas».

   b. Dentro de las métricas, voy a seleccionar el enlace "Grid" en la parte superior de la columna central.

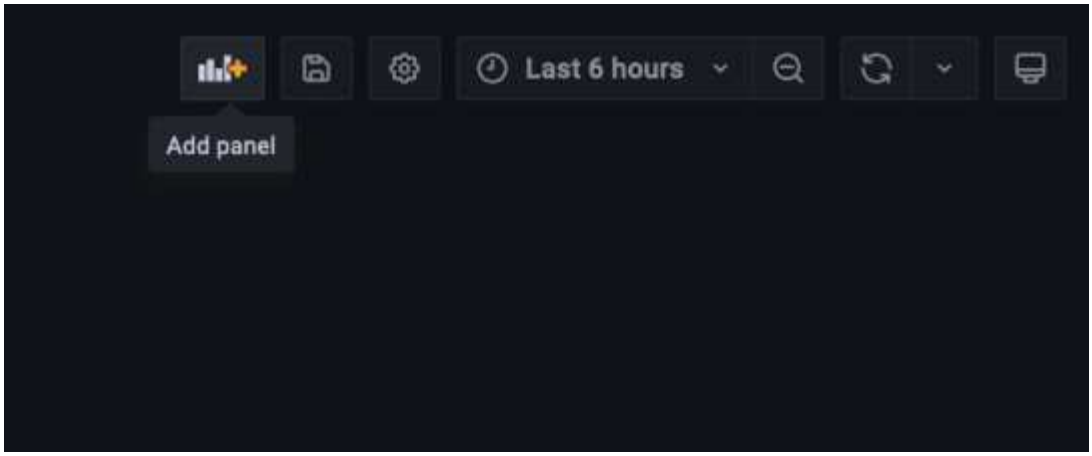


   c. En el panel de cuadrícula, permite seleccionar el panel "almacenamiento usado - metadatos de objeto". Haga clic en la flecha abajo y en el final del título del panel para ver un menú desplegable. En este menú, seleccione "inspeccionar" y "Panel JSON".



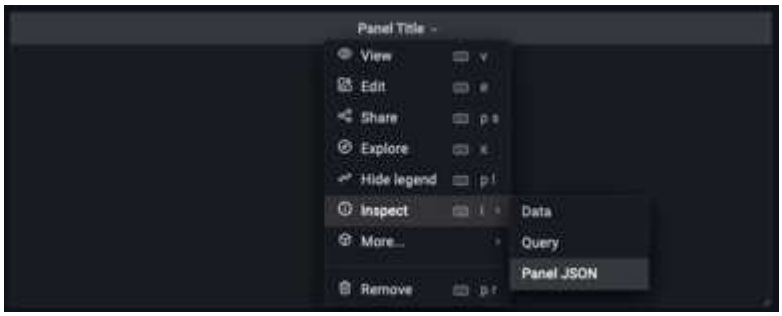
   d. Copie el código JSON y cierre la ventana.

e. En nuestro nuevo panel, haga clic en el icono para añadir un nuevo panel.

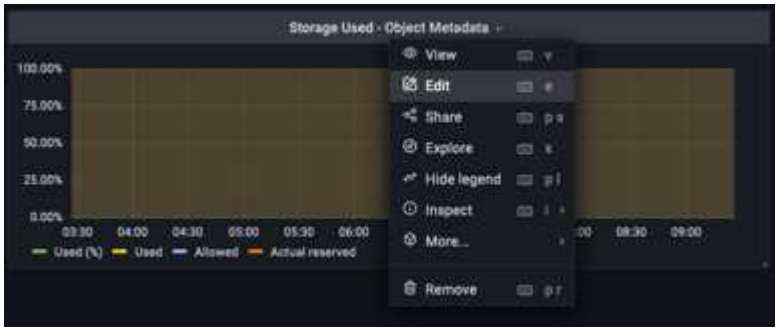


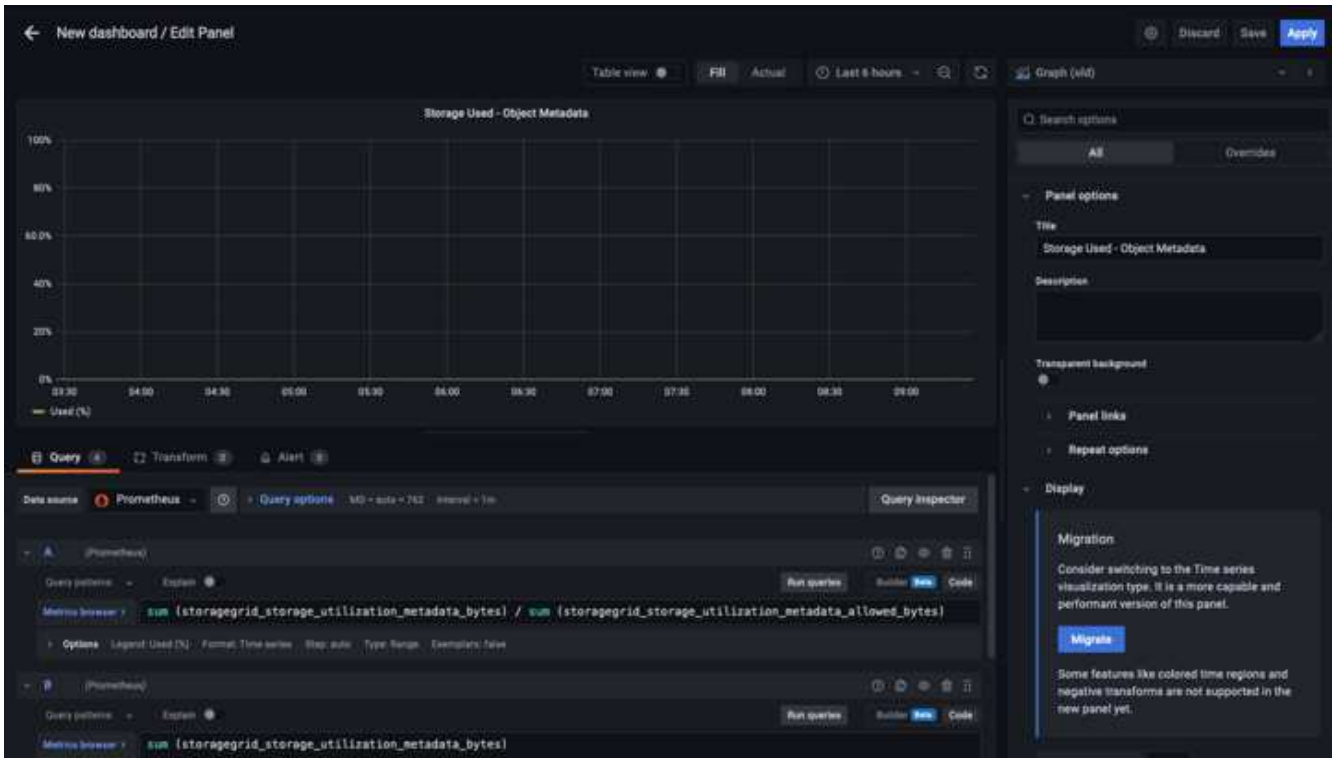
f. Aplique el nuevo panel sin realizar cambios

g. Al igual que con el panel StorageGRID, inspeccione el JSON. Quite todo el código JSON y sustitúyalo por el código copiado del panel StorageGRID.



h. Edite el nuevo panel y, a la derecha, verá un mensaje de migración con el botón "migrar". Haga clic en el botón y, a continuación, en el botón "aplicar".





8. Una vez que tenga todos los paneles en su lugar y configurados como desee. Guarde el panel haciendo clic en el icono de disco de la parte superior derecha y asigne un nombre a su panel.

Conclusión

Ahora disponemos de un servidor Prometheus con capacidad personalizable de almacenamiento y retención de datos. De este modo, podemos desarrollar nuestros propios paneles con las métricas más relevantes para nuestras operaciones. Puede obtener más información sobre las métricas de Prometheus recopiladas en el "Documentación de StorageGRID".

Utilice F5 DNS para equilibrar la carga global de StorageGRID

Por Steve Gorman (F5)

Este informe técnico proporciona instrucciones detalladas para configurar NetApp StorageGRID con servicios DNS de F5 para el equilibrio de carga global a fin de brindar una mejor disponibilidad de datos, mayor consistencia de datos y optimizar el enrutamiento de transacciones S3 cuando su red se distribuye en varios sitios y/o grupos de alta disponibilidad.

Introducción

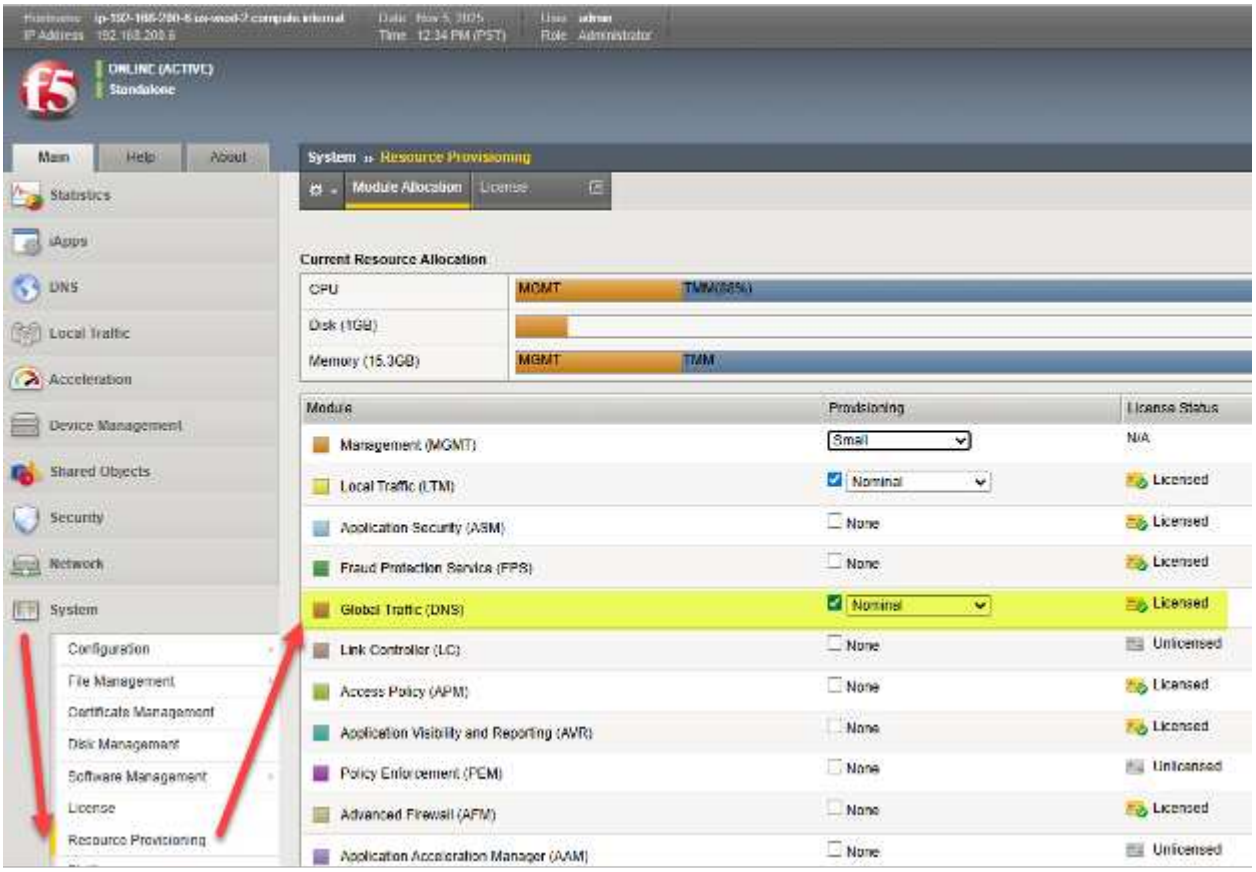
La solución F5 BIG-IP DNS, anteriormente llamada BIG-IP GTM (Global Traffic Manager) e informalmente GSLB (Global Server Load Balancing), permite lograr un acceso sin inconvenientes entre múltiples grupos de alta disponibilidad activos-activos y soluciones StorageGRID multisitio activos-activos para lograr una implementación efectiva.

Configuración de StorageGRID multisitio de F5 BIG-IP

Independientemente de la cantidad de sitios StorageGRID que se admitirán, un mínimo de dos dispositivos BIG-IP, físicos o virtuales, deben tener el módulo DNS BIG-IP habilitado y configurado. Cuantos más dispositivos DNS haya, mayor será el grado de redundancia del que se beneficiará una empresa.

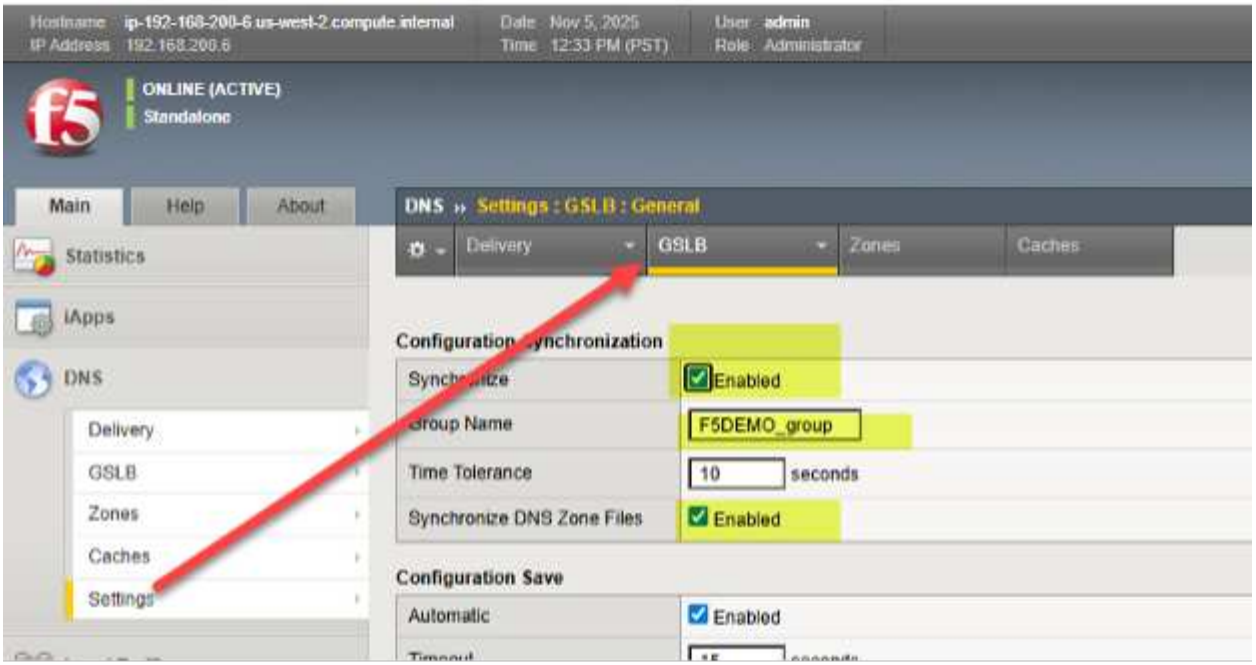
DNS BIG-IP: Primeros pasos en la configuración inicial

Una vez que el dispositivo BIG-IP haya pasado al menos por el aprovisionamiento inicial, utilice un navegador web para iniciar sesión en la interfaz TMUI (GUI de BIG-IP) y seleccione Sistema → Aprovisionamiento de recursos. Como se destaca, asegúrese de que el módulo “Tráfico global (DNS)” tenga una marca de verificación y se muestre como autorizado. Tenga en cuenta que, como en la imagen, es común que se pueda aprovisionar “Tráfico local (LTM)” en el mismo dispositivo.

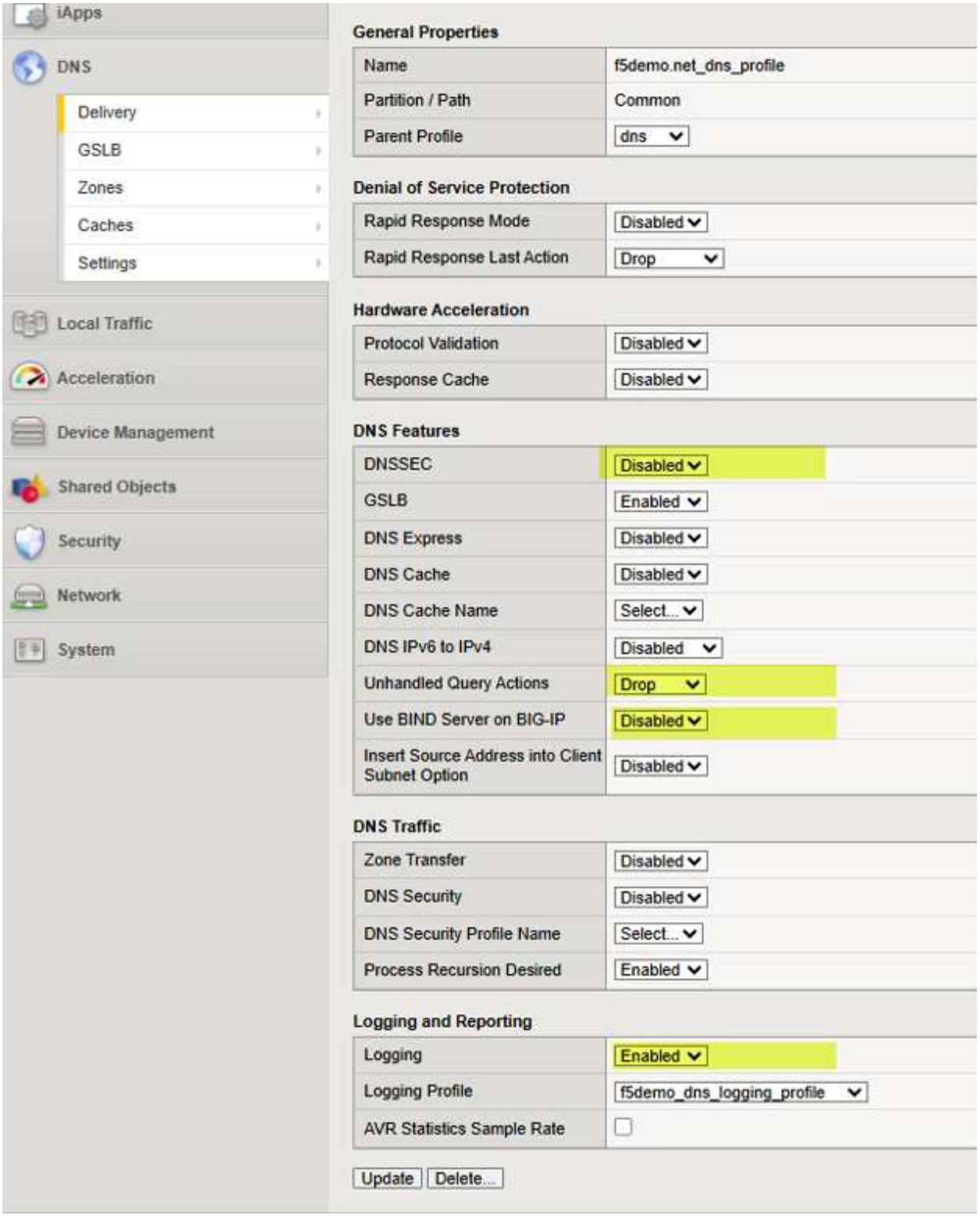


Configurar los elementos fundamentales del protocolo DNS

El primer paso hacia la gestión del tráfico global para los sitios StorageGRID es elegir la pestaña DNS, donde prácticamente se configurará toda la dirección del tráfico global, y elegir Configuración→ GLSB. Habilite las dos opciones de sincronización y elija un nombre de grupo DNS que se compartirá entre los dispositivos BIG-IP participantes.



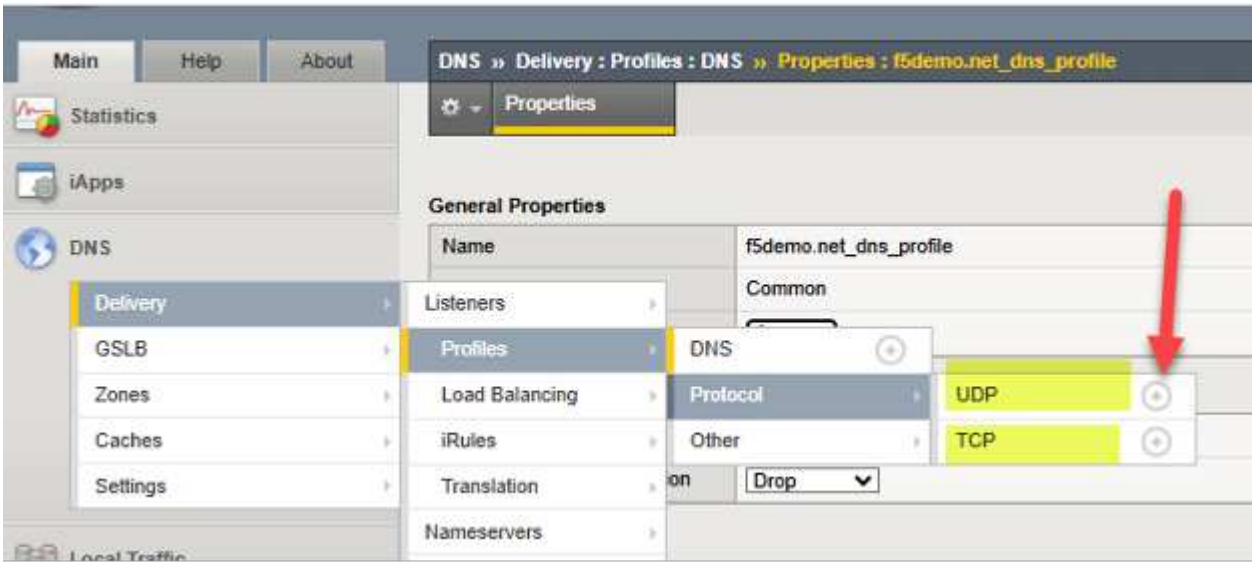
A continuación, vaya a DNS > Entrega > Perfiles > DNS: Crear y cree un perfil que regirá las capacidades de DNS que desea habilitar o deshabilitar. Si le interesa generar registros DNS específicos, consulte el enlace anterior para obtener la guía del aula de DNS. A continuación se muestra un ejemplo de un perfil DNS en funcionamiento; observe los cuatro resaltados que representan configuraciones que son valores importantes. Para mayor información, cada configuración posible se explica en el siguiente artículo de F5 KB (Knowledge Base) "aquí".



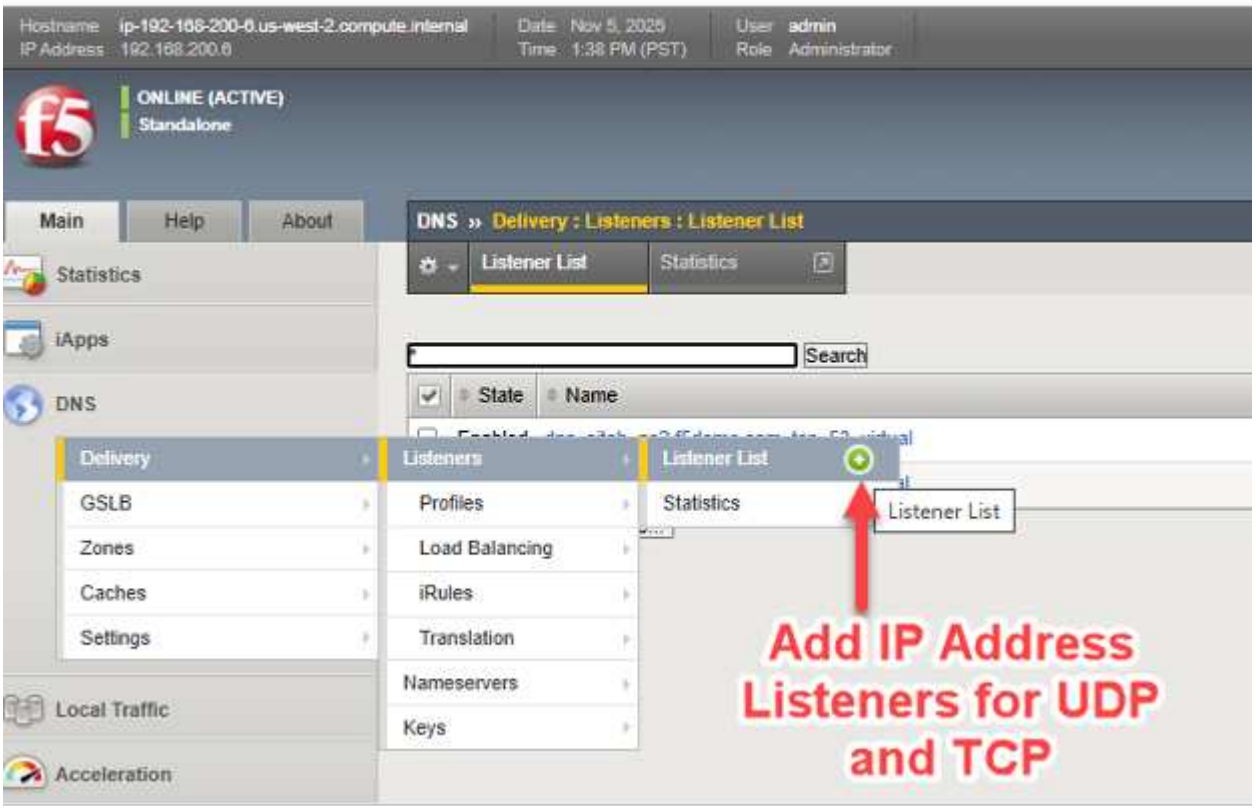
En este punto podemos ajustar las características de los protocolos UDP y TCP, a través de “perfiles” creados, que pueden transportar tráfico DNS que involucre a BIG-IP. Simplemente cree un nuevo perfil para UDP y TCP. Suponiendo que el tráfico DNS cruzará enlaces WAN, una buena práctica es simplemente heredar las características UDP y TCP que se sabe que funcionan bien en entornos WAN. Para agregar cada uno, simplemente haga clic en el ícono “+” junto a cada protocolo y configure el perfil principal de la siguiente manera:

UDP → usar el perfil “principal” “udp_gtm_dns”

TCP → usar el perfil “principal” “f5-tcp-wan”

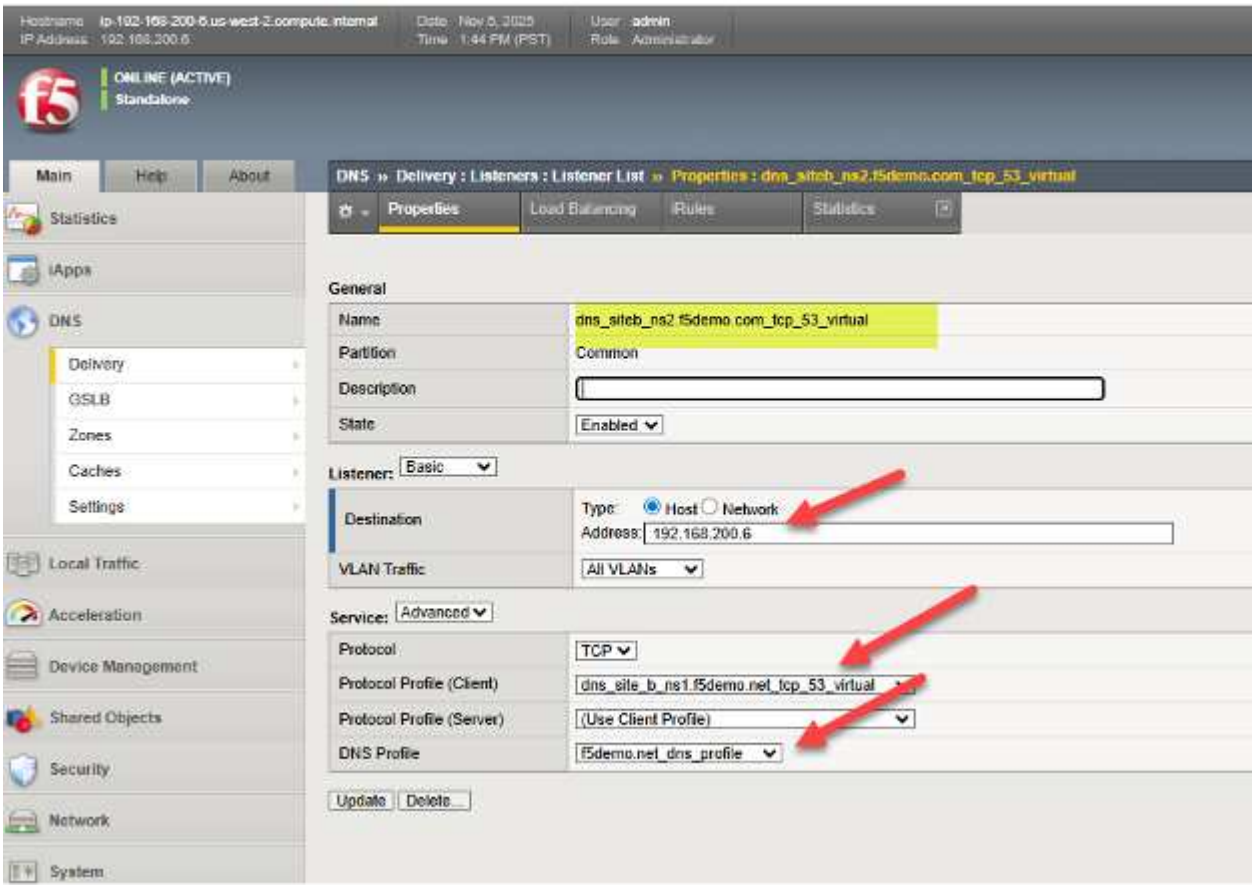


Ahora, simplemente necesitamos asignar una dirección IP para el tráfico UDP y TCP que involucra al DNS BIG-IP. Para aquellos familiarizados con BIG-IP LTM, esto es esencialmente la creación de servidores virtuales DNS, y los servidores virtuales necesitan direcciones IP de “escucha”. Como en la captura de pantalla, siga las flechas para crear servidores virtuales/de escucha para DNS/UDP y DNS/TCP.



El siguiente es un ejemplo de un DNS BIG-IP en vivo, en él vemos las configuraciones del escucha del servidor virtual TCP y podemos ver cómo se vinculan muchos de los pasos anteriores. Esto incluye hacer referencia al perfil DNS y al perfil del protocolo (TCP), así como configurar una dirección IP válida para que la utilice el DNS. Al igual que con todos los objetos que se crean con BIG-IP, es útil utilizar un nombre significativo que sirva para autoidentificar qué es el objeto, como dns/siteb/TCP53 en el nombre de ejemplo

asignado.



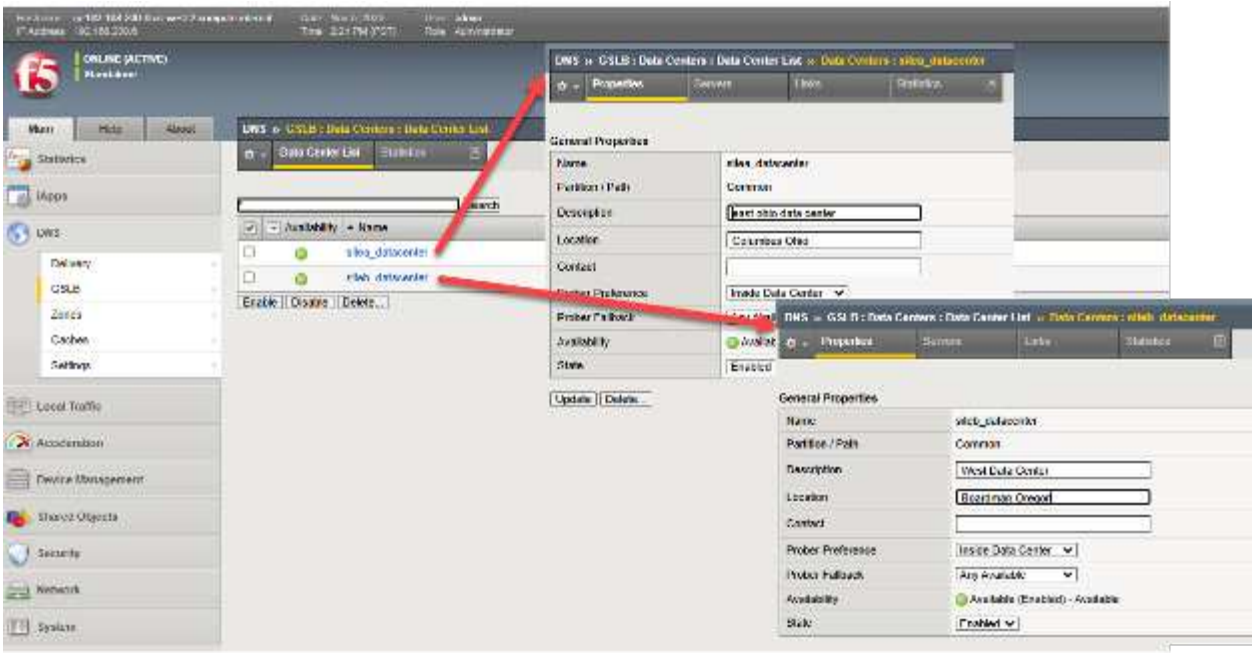
Con esto concluyen los pasos de configuración preliminares, generalmente “únicos”, de un dispositivo BIG-IP con el módulo DNS habilitado. En este punto estamos listos para pasar a los detalles específicos de la configuración de una solución de gestión de tráfico global con nuestros dispositivos, que, por supuesto, estarán vinculados a las características de los sitios StorageGRID .

Configuración de sitios de centros de datos y establecimiento de comunicaciones entre BIG-IP en cuatro pasos

Paso uno: Crear centros de datos

Cada sitio que albergará grupos de nodos que serán equilibrados de carga localmente por BIG-IP LTM, debe ingresarse en el DNS de BIG-IP. Esto debe hacerse solo en un DNS BIG-IP, ya que estamos creando un grupo DNS sincronizado para respaldar la administración del tráfico, por lo que esta configuración se compartirá entre los miembros DNS del grupo.

A través de la GUI de TMUI, seleccione DNS > GSLB > Centros de datos > Lista de centros de datos y cree una entrada para cada uno de los sitios de StorageGRID . Si utiliza una configuración de red alineada con la Figura 1, el dispositivo DNS está ubicado en otros sitios que no son StorageGRID , agregue centros de datos para estos sitios además de los sitios de almacenamiento. En este ejemplo, los sitios a y b se crean en Ohio y Oregón, las BIG-IP son dispositivos DNS y LTM duales.



Paso dos: Crear servidores (lista de todos los dispositivos BIG-IP en la solución)

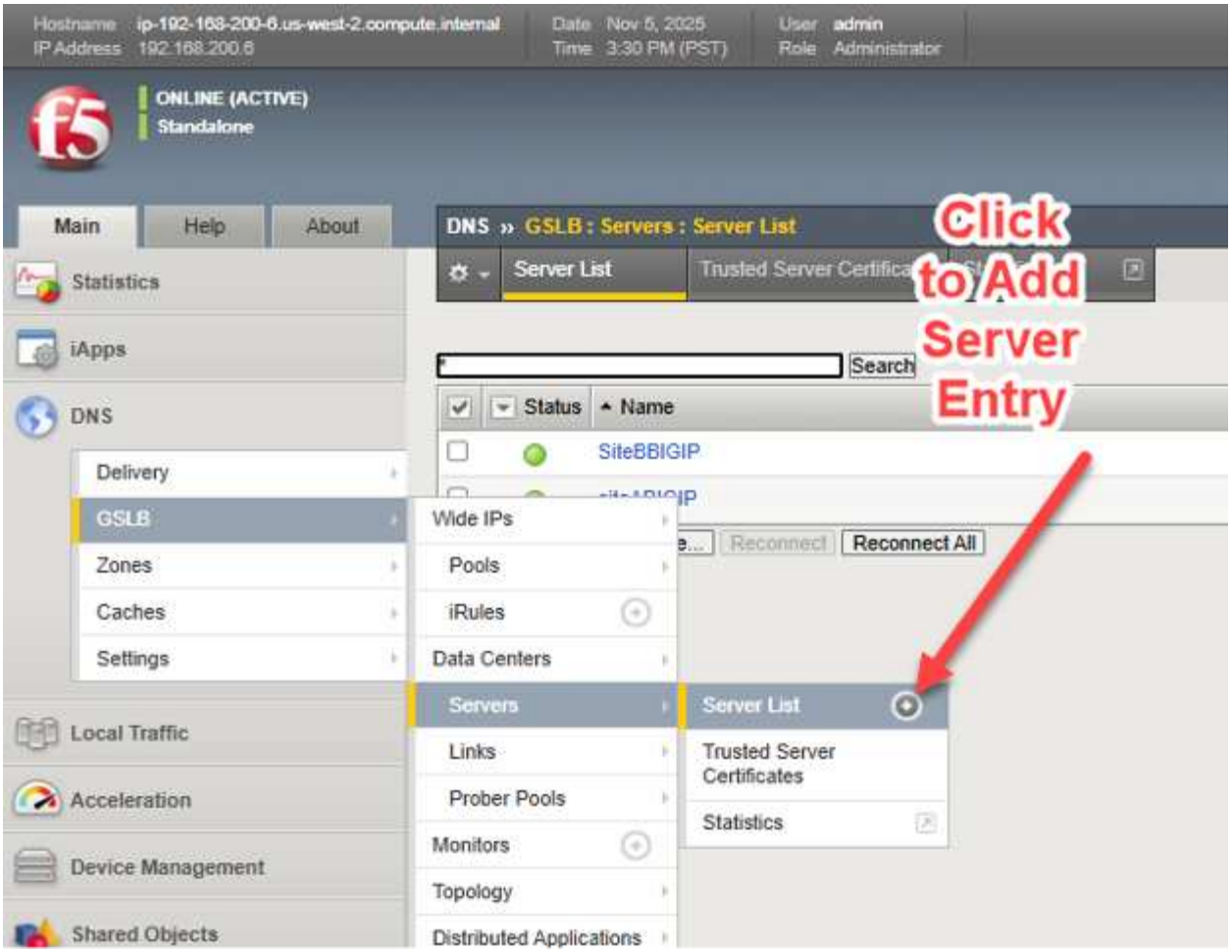
Ahora estamos listos para conectar los clústeres de sitios individuales de StorageGRID a la configuración de DNS de BIG-IP. Recordemos que el dispositivo BIG-IP en cada sitio realizará el equilibrio de carga real del tráfico S3, a través de la configuración de servidores virtuales que vinculan una dirección IP/puerto accesible "front-end" a un conjunto "pool" back-end de dispositivos de nodo de almacenamiento, utilizando direcciones IP/puertos "back-end".

Si, por ejemplo, todos los nodos de almacenamiento de un grupo se desconectaran administrativamente, tal vez para el desmantelamiento de un sitio o inesperadamente debido a verificaciones de estado fallidas en tiempo real, el tráfico se dirigirá a otros sitios mediante la alteración de las respuestas de consulta de DNS.

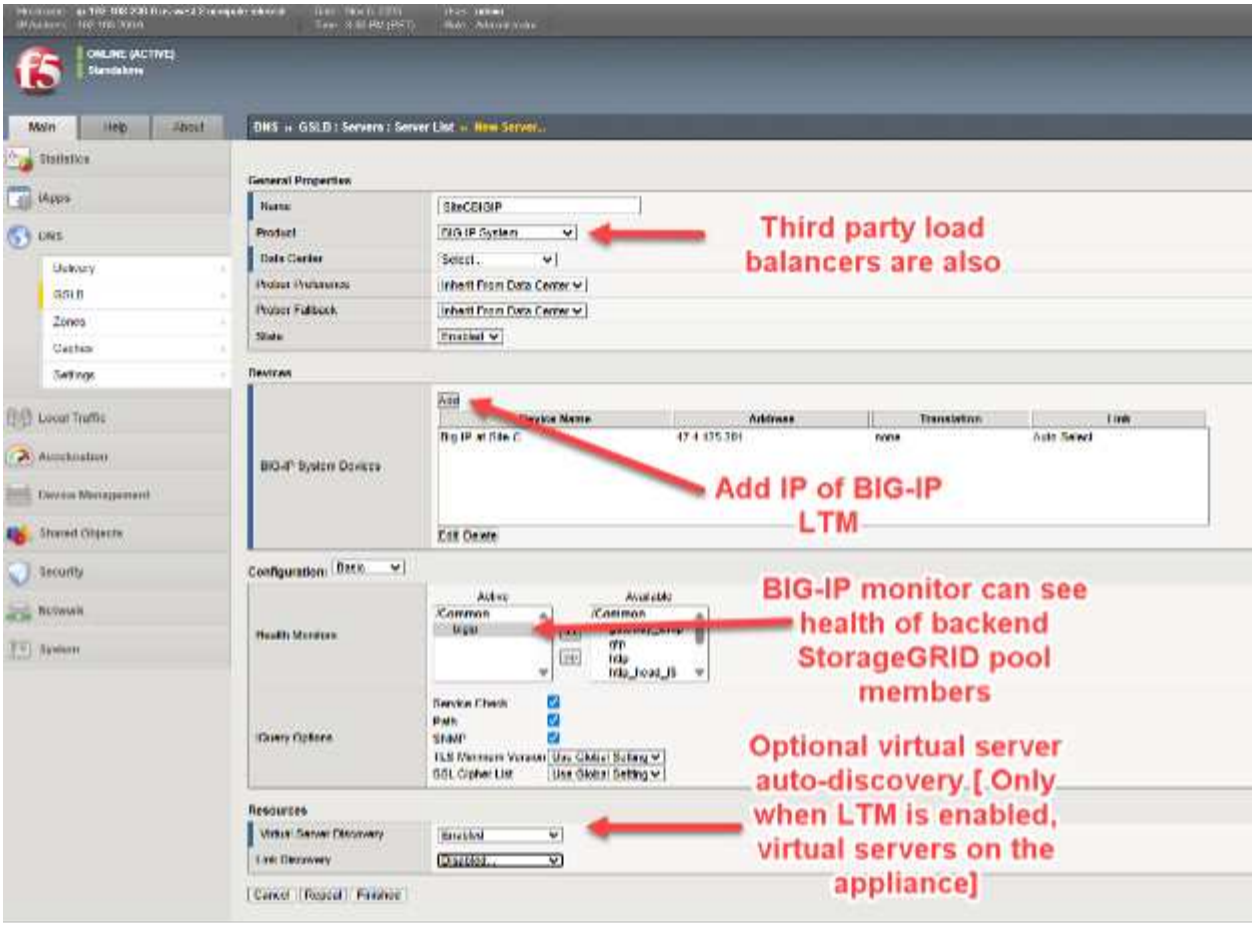
Para vincular los sitios de StorageGrid, específicamente los servidores virtuales locales, a la configuración de DNS de BIG-IP en cada dispositivo, la configuración solo debe realizarse una vez. Todo el grupo de dispositivos DNS BIG-IP tendrá sus configuraciones sincronizadas en un próximo paso.

En términos simples, crearemos una lista, denominada lista de servidores, de todos nuestros dispositivos BIG-IP, ya sea que tengan licencia para DNS, LTM o tanto DNS como LTM. Esta lista maestra se sincronizará con todos los dispositivos DNS BIG-IP una vez completada la lista.

En un dispositivo con licencia DNS BIG-IP, seleccione DNS > GSLB > Servidores > Lista de servidores y elija el botón Agregar (+).



Los cuatro elementos clave al agregar cada BIG-IP incluyen: * Seleccionar BIG-IP del menú desplegable del producto; otros balanceadores de carga son posibles pero generalmente carecen de la capacidad de respuesta de visibilidad en tiempo real cuando la salud del nodo back-end se deteriora en cada sitio. * Agregue la dirección IP del dispositivo DNS BIG-IP. Es probable que la primera vez que agregue un dispositivo DNS BIG-IP, la dirección sea la del dispositivo al que se accede mediante la GUI actual; los dispositivos futuros serán los otros dispositivos de la solución. * Elija un monitor de estado, utilice siempre “BIG-IP” cuando el balanceador de carga que se agrega es un dispositivo BIG-IP, para tener en cuenta el estado del nodo StorageGRID del back-end. * Opcionalmente, solicite el descubrimiento automático del servidor virtual si el dispositivo es un dispositivo DNS/LTM dual.

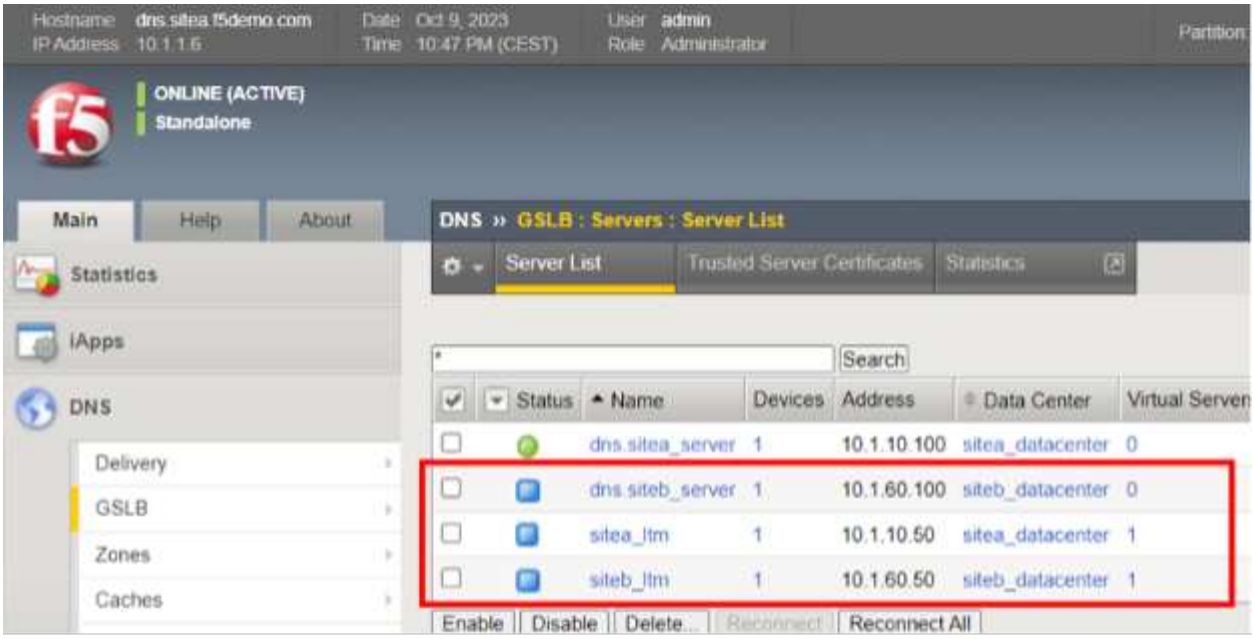


En algunas situaciones, como problemas de red transitorios o reglas de ACL de firewall entre ubicaciones de red, al agregar un dispositivo remoto en esta etapa, es posible que la detección del servidor virtual no muestre entradas para dispositivos remotos con LTM configurado. En tales casos, después de agregar el nuevo dispositivo ("servidor"), se pueden agregar manualmente los servidores virtuales como se indica a continuación. Si se agrega un dispositivo BIG-IP solo DNS, no habrá servidores virtuales para descubrir ni agregar a ese dispositivo.

Necesitamos agregar estas entradas de servidor para cada dispositivo en nuestra solución en todos los sitios, incluidos los dispositivos BIG-IP DNS, los dispositivos BIG-IP LTM y cualquier dispositivo que cumpla las funciones duales de unidades DNS y LTM.

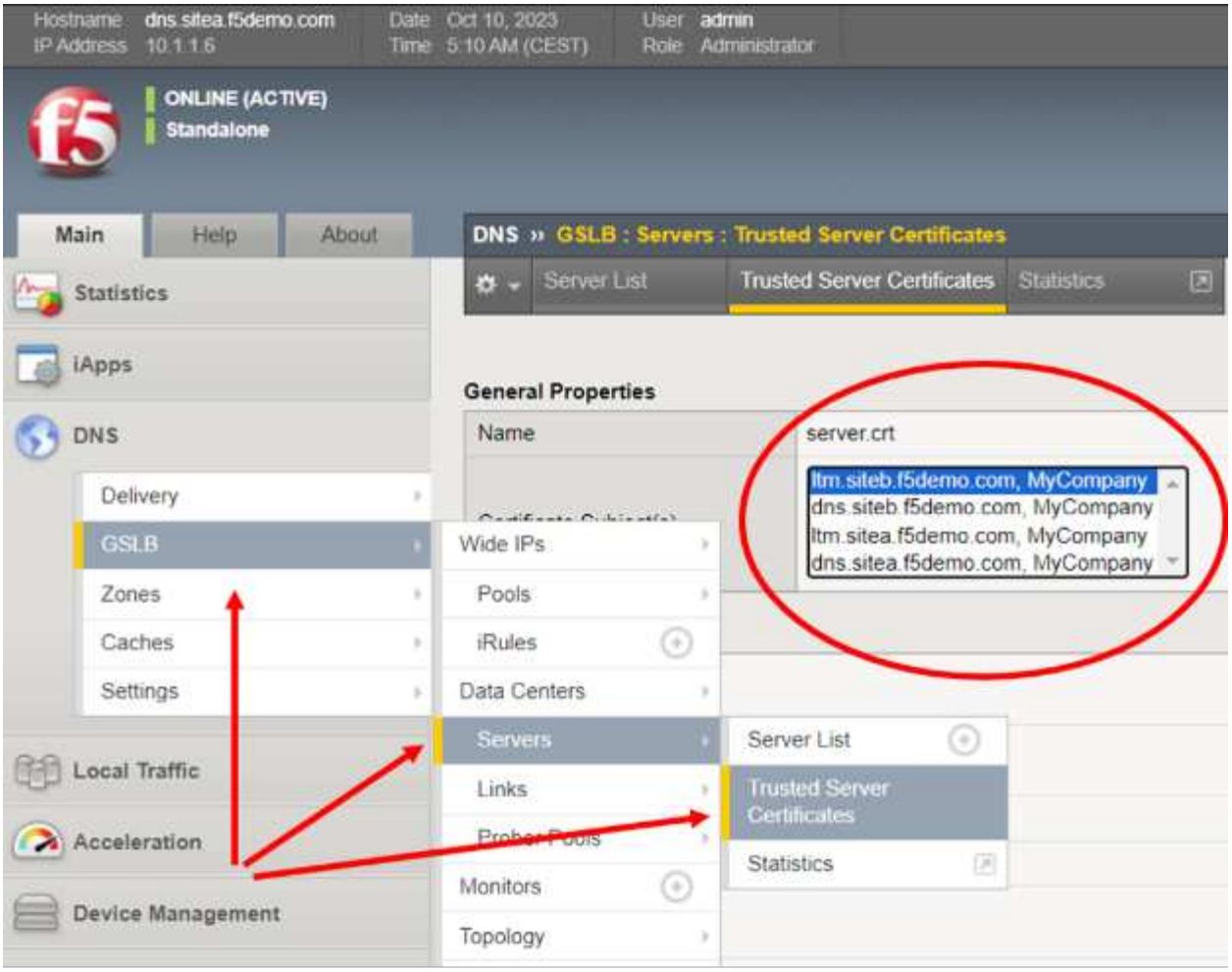
Paso tres: Establecer confianza entre todos los dispositivos BIG-IP

En el siguiente ejemplo, se han agregado cuatro dispositivos como servidores y están distribuidos en dos sitios. Tenga en cuenta que cada sitio tiene un DNS BIG-IP dedicado y un LTM BIG-IP. Sin embargo, todos los dispositivos, excepto el que está conectado actualmente, muestran íconos azules en la columna "Estado". Esto significa que aún no se ha establecido una relación de confianza con los demás dispositivos BIG-IP.



Para agregar confianza, acceda por SSH a BIG-IP donde se acaban de ingresar los detalles de configuración a través de la GUI y use la cuenta “root” para acceder a la interfaz de línea de comandos de BIG-IP. Emita el siguiente comando único en el indicador: *bigip_add*

El comando "bigip_add" extrae el certificado de administración de los dispositivos BIGIP de destino para su uso durante la configuración del canal cifrado "iQuery" entre los servidores GSLB del clúster. iQuery, de forma predeterminada, se ejecuta mediante el puerto TCP 4353 y es el latido que permite que los miembros del DNS de BOG-IP se mantengan sincronizados. Hace uso de xml y gzip en el canal cifrado. Al ejecutar "bigip_add" sin ninguna opción, el comando se ejecutará en todos los dispositivos BIGIP en la lista de servidores GSLB utilizando el nombre de usuario actual para conectarse a los puntos finales. Para comprobar rápidamente el éxito, simplemente regrese a la GUI de BIG-IP y confirme que todos los servidores ahora tienen certificados enumerados en el menú desplegable que se muestra.



Paso cuatro: Sincronizar todos los dispositivos DNS BIG-IP con el grupo DNS

El paso final permitirá que todos los dispositivos DNS BIG-IP se configuren completamente simplemente utilizando la GUI TMUI de una sola unidad. En un caso de muestra, donde hay dos sitios StorageGRID , esto significa ahora usar SSH para llegar a la línea de comando del DNS BIG-IP del **otro** sitio. Después de conectarse como root y asegurarse de que las políticas/ACL del firewall permitan que los dos dispositivos BIG-IP DNS se comuniquen en los puertos TCP 22 (SSH), 443 (HTTPS) y 4354 (protocolo F5 iQuery), emita este comando en el indicador: *gtm_add <dirección IP del primer sitio BIG-IP DNS, donde se realizaron previamente todos los pasos de la GUI>*

En este punto, todo el trabajo de configuración de DNS adicional se puede realizar en cualquier dispositivo DNS BIG-IP que se haya agregado al grupo. El comando anterior, gtm_add, no necesita aplicarse en miembros del dispositivo que sean solo LTM. Sólo los dispositivos compatibles con DNS requieren este comando para formar parte del grupo DNS sincronizado.

Configuración de sitios de centros de datos y establecimiento de comunicaciones entre BIG-IP

En este punto, se han completado todos los pasos para crear el grupo de dispositivos DNS BIG-IP subyacente y saludable. Ahora podemos continuar con la creación de nombres, FQDN, que apuntan hacia nuestros servicios web/S3 distribuidos expuestos en cada centro de datos de StorageGRID .

Estos nombres se conocen como “IP amplias” o WIP para abreviar, y son FQDN de DNS normales con registros de recursos de DNS A. Sin embargo, en lugar de apuntar a un servidor como un registro de recursos A tradicional, apuntan internamente a grupos de servidores virtuales BIG-IP. Cada pool, individualmente, puede estar formado por un conjunto de uno o más servidores virtuales. Un cliente S3 que solicita una

dirección IP para la resolución de nombres recibirá la dirección del servidor virtual S3 en el sitio StorageGRID óptimo seleccionado por la política.

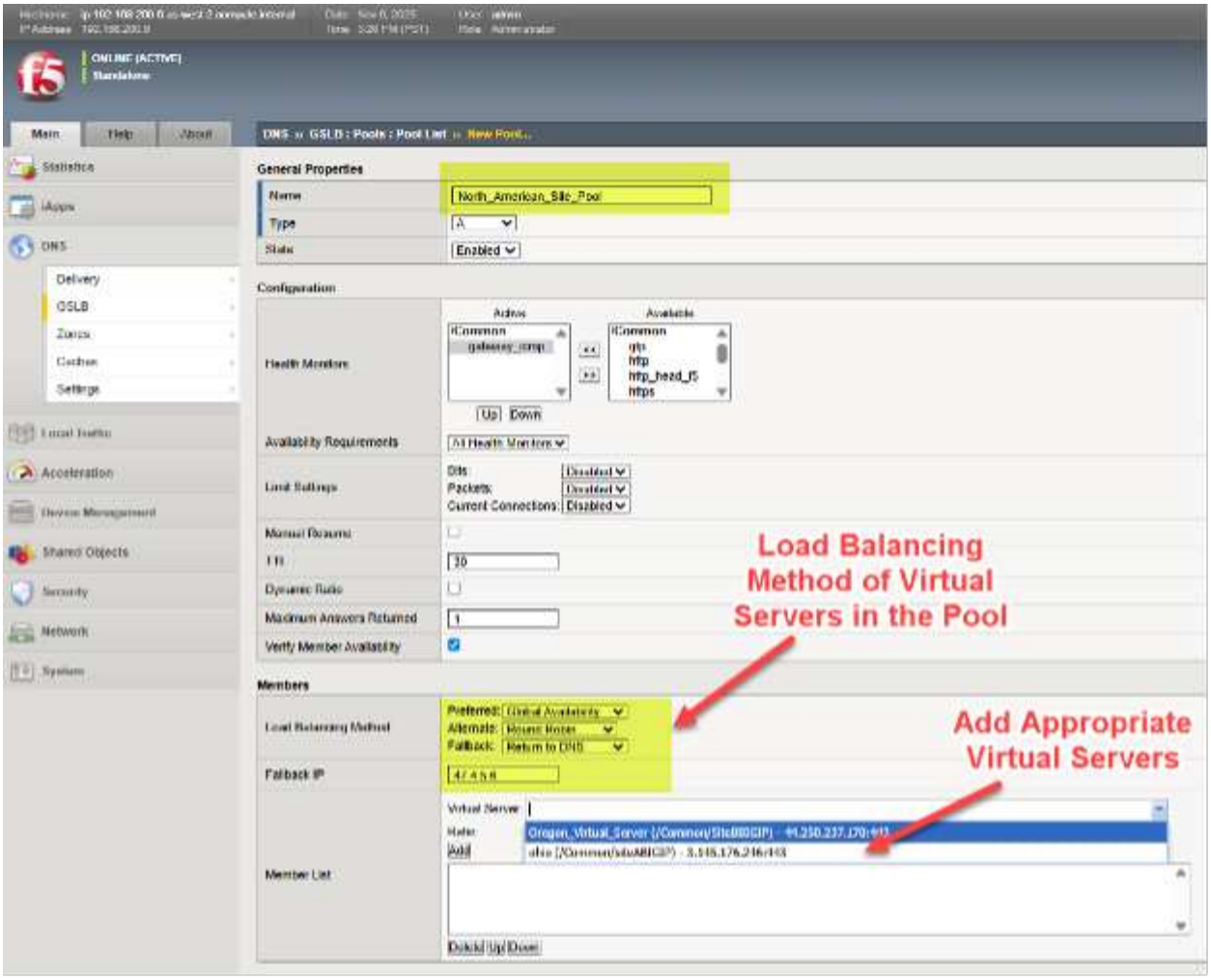
IP amplias, grupos y servidores virtuales en pocas palabras

Para dar un ejemplo simple y ficticio, un WIP para el nombre **storage.quantumvault.com** podría ver la solución DNS BIG-IP vinculada con dos grupos de servidores virtuales potenciales. El primer grupo podría estar compuesto por cuatro sitios en América del Norte, mientras que el segundo grupo podría estar compuesto por tres sitios en Europa.

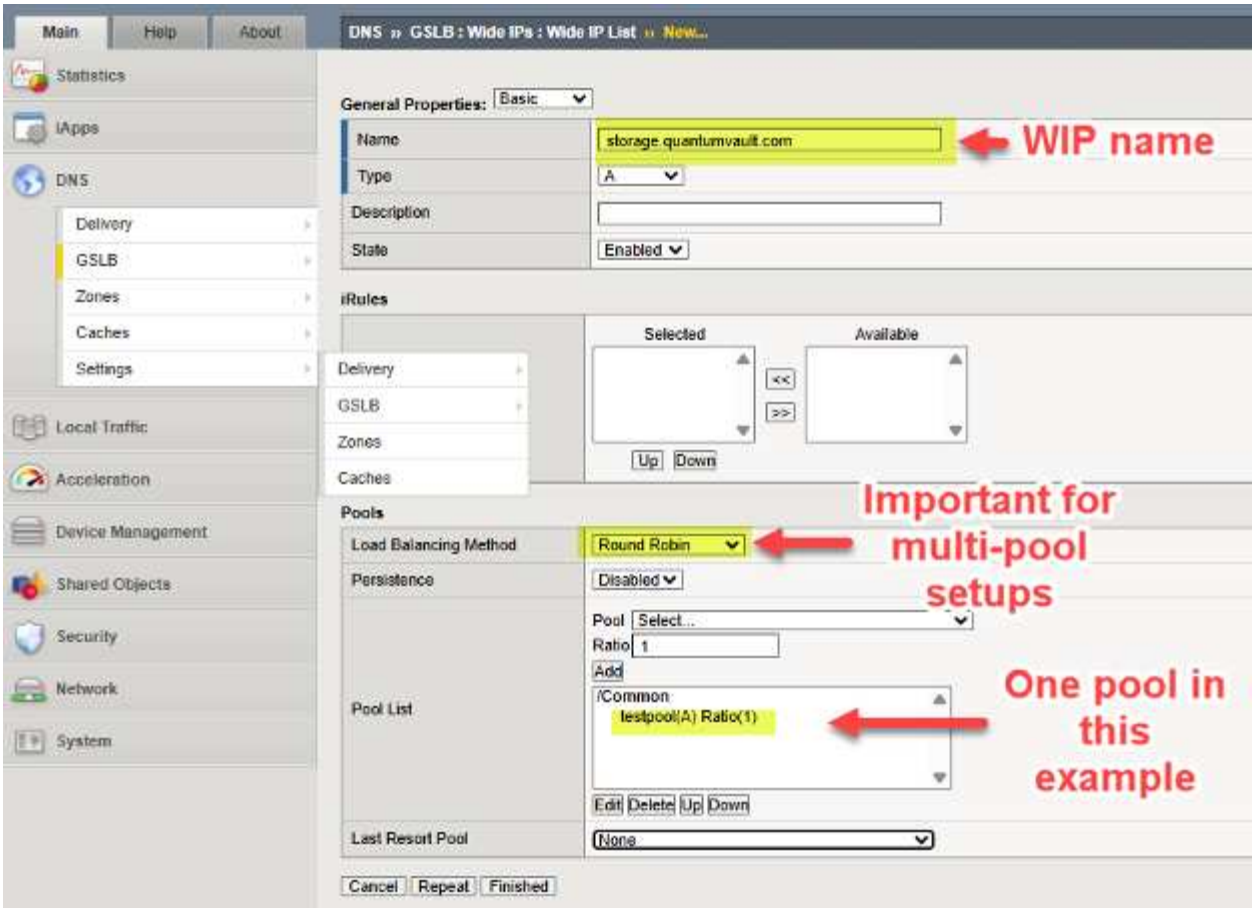
El grupo seleccionado se puede obtener a partir de una serie de decisiones políticas; tal vez se podría usar una proporción simple de 5:1 para dirigir la mayor parte del tráfico a los sitios StorageGRID de América del Norte. Quizás sea más probable una elección basada en la topología, en la que el grupo se elige de manera que, por ejemplo, todo el tráfico S3 de origen europeo se dirija a sitios europeos y el resto del tráfico S3 mundial se dirija a centros de datos de América del Norte.

Una vez que BIG-IP DNS llega a un grupo, supongamos que se seleccionó el grupo de América del Norte, el registro de recursos DNS A real devuelto para resolver storage.quantumvault.com puede ser cualquiera de los 4 servidores virtuales compatibles con BIG-IP LTM en cualquiera de los 4 sitios de América del Norte. Nuevamente, lo que se elige está determinado por políticas; existen enfoques “estáticos” simples como Round-Robin, mientras que selecciones “dinámicas” más avanzadas, como sondas de rendimiento para medir la latencia de cada sitio desde los solucionadores DNS locales, se mantienen y se utilizan como criterios para la selección del sitio.

Para configurar un grupo de servidores virtuales en un DNS BIG-IP, siga la ruta del menú **DNS > GSLB > Grupos > Lista de grupos > Agregar (+)**. En este ejemplo, podemos ver que se agregan varios servidores virtuales de América del Norte a un grupo y el enfoque preferido para equilibrar la carga, cuando se selecciona este grupo, se elige de manera escalonada.



Agregamos el WIP (Wide IP), el nombre de nuestro servicio que será resuelto por DNS, a un despliegue siguiendo DNS > GSLB > Wide IPs > Wide IP List > Create (+). En el siguiente ejemplo, proporcionamos un ejemplo de WIP para un servicio de almacenamiento habilitado para S3.



Ajuste el DNS para admitir la gestión del tráfico global

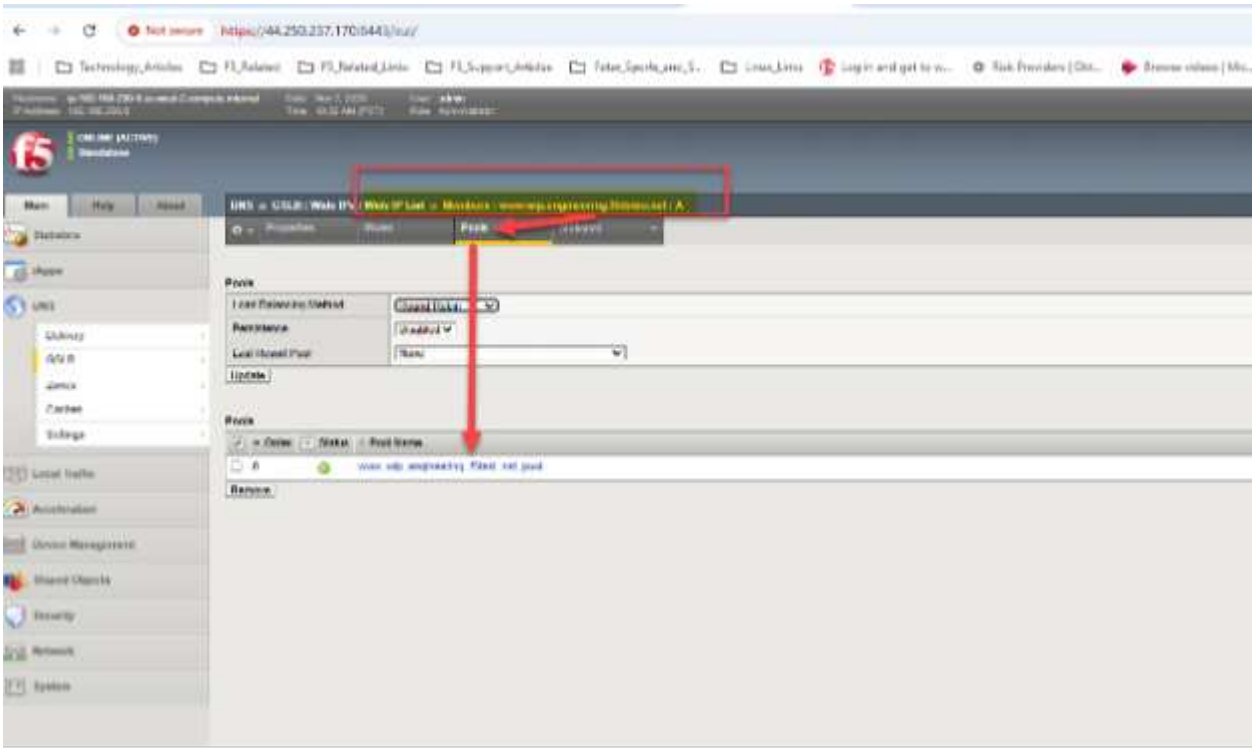
En este punto, todos nuestros dispositivos BIG-IP subyacentes están listos para realizar GSLB (equilibrio de carga global del servidor). Simplemente necesitamos ajustar y asignar los nombres utilizados para los flujos de tráfico S3 para aprovechar la solución. El enfoque general es delegar parte de un dominio DNS existente de una empresa al control de BIG-IP DNS. Esto quiere decir “dividir” una sección del espacio de nombres, un subdominio, y delegar el control de este subdominio a los dispositivos DNS BIG-IP. Técnicamente, esto se hace garantizando que los dispositivos DNS BIG-IP tengan registros de recursos DNS (RR) en el DNS empresarial y luego convirtiendo estos nombres/direcciones en registros de recursos DNS del servidor de nombres (NS) para el dominio delegado.

Hoy en día, las empresas tienen distintas formas de mantener el DNS; un método es una solución totalmente alojada. Un ejemplo de esto sería operar y administrar DNS a través de Windows Server 2025. Un enfoque alternativo puede ser que una empresa aproveche proveedores de DNS en la nube como AWS Route53 o Squarespace.

A continuación se presenta un ejemplo ficticio a modo de ilustración. Contamos con StorageGRID que admite lecturas y escrituras de objetos a través del protocolo S3 con un dominio existente administrado por AWS Route53; el dominio de ejemplo existente es f5demo.net.

Nos gustaría asignar el subdominio engineering.f5demo.net a los dispositivos DNS BIG-IP para la gestión del tráfico global. Para ello, creamos un nuevo registro de recursos NS (servidor de nombres) para engineering.f5demo.net y lo apuntamos a la lista de nombres de dispositivos DNS BIG-IP. En nuestro ejemplo, tenemos dos dispositivos DNS BIG-IP y, como tal, creamos dos registros de recursos A para ellos.

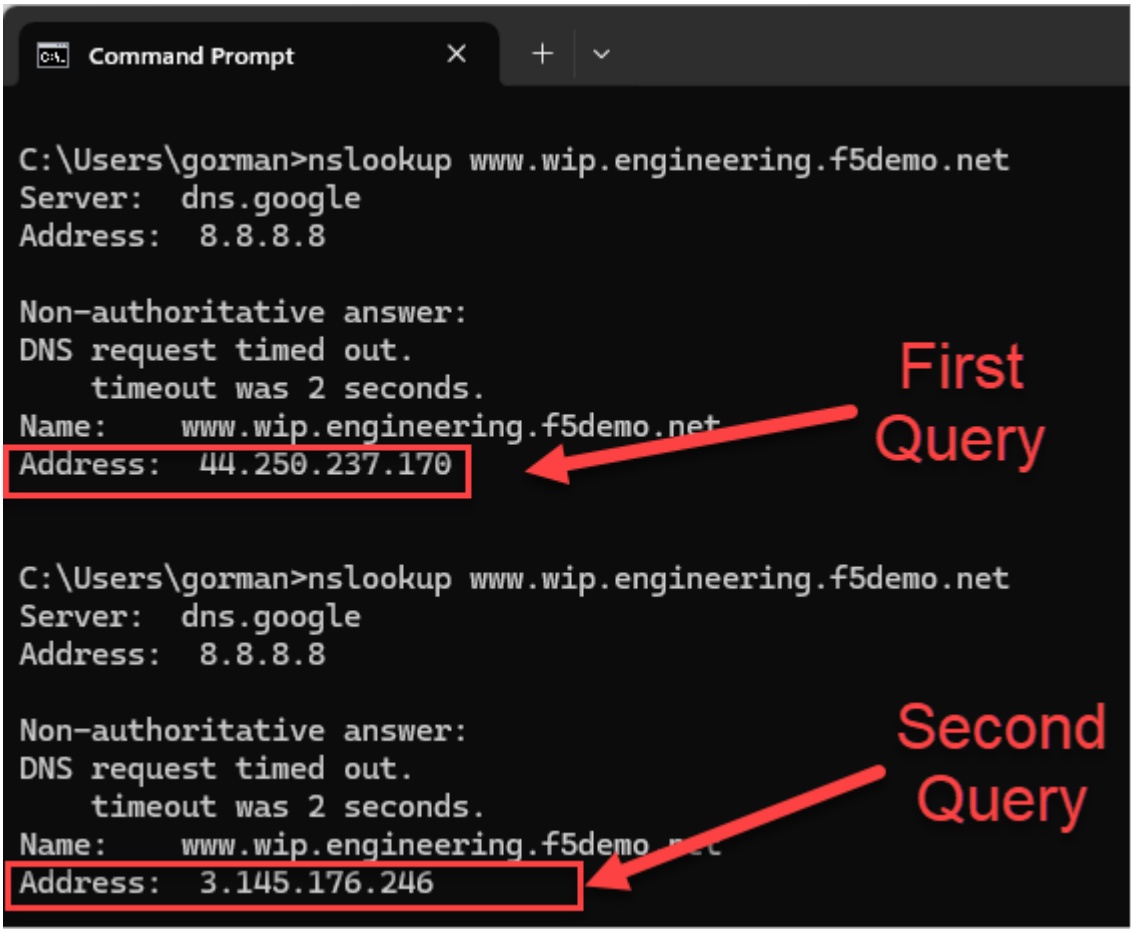
Ahora, a modo de ejemplo, configuraremos una IP ancha (WIP) en nuestro DNS BIG-IP, ya que el DNS utiliza sincronización de grupo, solo necesitamos realizar ajustes usando la GUI de un dispositivo. Dentro de la GUI de DNS de BIG-IP, vaya a **DNS > GSLB > IP anchas > Lista de IP anchas (+)**. Recuerde que en una configuración FQDN de DNS tradicional uno ingresaría una o más direcciones IPv4; en nuestro caso simplemente apuntamos a uno o más grupos de servidores virtuales StorageGRID .



En nuestro ejemplo, tenemos servidores web HTTPS genéricos ubicados en sitios de Ohio y Oregón. Con un enfoque simple de “round robin”, deberíamos poder ver el DNS global responder a las consultas para las asignaciones de registros de recursos A para *www.wip.engineering.f5demo.net* con ambas IP de servidor virtual.

Se puede realizar una prueba sencilla con navegadores web o, en el caso de S3 usando StorageGRID, quizás herramientas gráficas como S3Browser. Cada consulta DNS verá el siguiente sitio del centro de datos en el grupo utilizado como destino para el tráfico resultante, debido a nuestra elección de Round Robin dentro del grupo.

En nuestra configuración de ejemplo, podemos usar dig o nslookup para generar rápidamente una serie de dos consultas DNS y garantizar que BIG-IP DNS esté efectivamente realizando un equilibrio de carga rotatorio, lo que da como resultado que ambos sitios reciban tráfico a lo largo del tiempo.

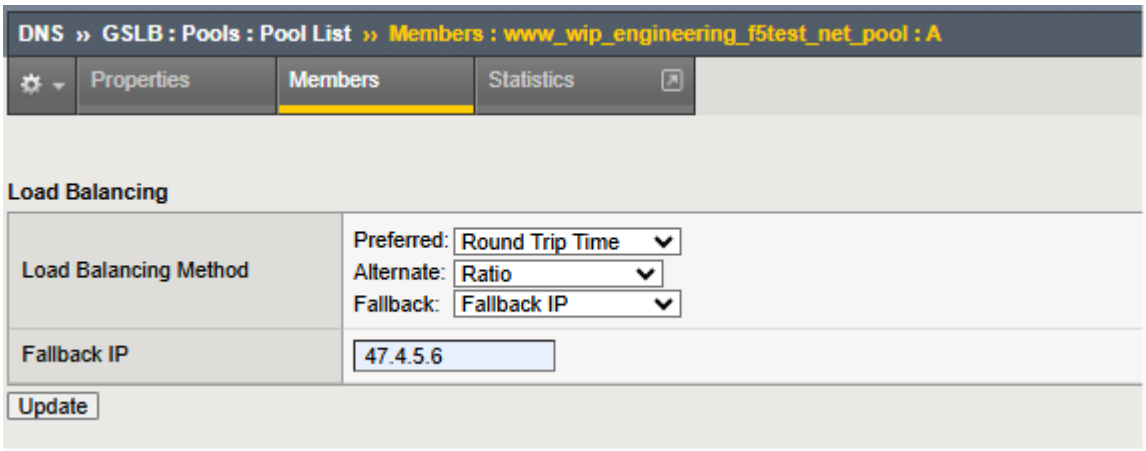


Exploración sugerida para técnicas más avanzadas

Uno de los muchos enfoques posibles sería utilizar el modo “Disponibilidad global” en lugar del simple ejemplo

“Round Robin” dado anteriormente. Con disponibilidad global, se puede dirigir tráfico al orden secuenciado de los grupos o servidores virtuales dentro de un solo grupo. De esta manera, todo el tráfico S3 podría dirigirse por defecto, por ejemplo, a un sitio de la ciudad de Nueva York.

Si los controles de estado indican un problema con la disponibilidad del nodo StorageGRID en este sitio, el tráfico podría en ese momento dirigirse a St. Louis. Si St. Louis experimenta problemas de salud, un sitio en Frankfurt podría a su vez comenzar a recibir transacciones de lectura o escritura S3. Por lo tanto, la disponibilidad global es un enfoque para la resiliencia general de la solución S3 StorageGRID . Otro enfoque es combinar y mezclar enfoques de equilibrio de carga, donde se utiliza un enfoque escalonado.



En este ejemplo, una opción “dinámica” es la primera opción de equilibrio de carga para los sitios en el grupo configurado. En el ejemplo que se muestra, se mantiene un enfoque de medición continua que utiliza un sondeo activo del rendimiento del solucionador DNS local y actúa como catalizador para la selección del sitio. Si este enfoque no está disponible, los sitios individuales se pueden seleccionar según la proporción asignada a cada uno. Con ratio, los sitios StorageGRID más grandes y con mayor ancho de banda pueden recibir más transacciones S3 que los sitios más pequeños. Finalmente, como posible escenario de recuperación ante desastres, si todos los sitios del grupo dejaran de funcionar correctamente, la IP de respaldo especificada se utiliza como el sitio de último recurso. Uno de los métodos de equilibrio de carga más interesantes de BIG-IP DNS es la “Topología”, mediante la cual se observa la fuente entrante de consultas DNS, el solucionador DNS local del usuario S3, y utilizando la información de topología de Internet se selecciona el sitio aparentemente “más cercano” del conjunto.

Por último, si los sitios abarcan todo el mundo, puede que valga la pena considerar el uso de la tecnología de “sonda” dinámica que se analiza en detalle en el manual de DNS de F5 BIG-IP. Con las sondas se pueden monitorear fuentes frecuentes de consultas DNS, tomemos como ejemplo un socio de negocio a negocio cuyo tráfico generalmente utiliza el mismo solucionador DNS local. Se pueden lanzar sondas DNS de BIG-IP desde BIG-IP LTM en cada sitio alrededor del mundo, para determinar de manera general qué sitio potencial probablemente ofrecería la latencia más baja para transacciones S3. Como tal, el tráfico proveniente de Asia podría ser mejor atendido por sitios StorageGRID asiáticos que por sitios ubicados en América del Norte o Europa.

Conclusión

La integración de F5 BIG-IP con NetApp StorageGRID aborda los desafíos técnicos relacionados con la disponibilidad y la consistencia de los datos en múltiples sitios y la optimización del enrutamiento de transacciones S3. La implementación de esta solución mejora la resiliencia, el rendimiento y la confiabilidad del almacenamiento, lo que la hace ideal para empresas que buscan una infraestructura de almacenamiento sólida, escalable y flexible.

Para obtener más información, la documentación oficial de F5 para BIG-IP DNS se puede encontrar en este enlace. "enlace". También se puede encontrar una guía de estilo de aula guiada que proporciona instrucciones

paso a paso sobre una configuración de ejemplo. "aquí".

Configuración de SNMP de Datadog

Por Aron Klein

Configurar Datadog para recopilar métricas y capturas snmp de StorageGRID.

Configurar Datadog

Datadog es una solución de supervisión que ofrece métricas, visualizaciones y alertas. La siguiente configuración se implementó con el agente de linux versión 7.43.1 en un host de Ubuntu 22.04.1 implementado localmente en el sistema StorageGRID.

Perfil de datos y archivos de captura generados a partir del archivo MIB de StorageGRID

Datadog proporciona un método para convertir archivos MIB de producto en archivos de referencia de datadog necesarios para asignar los mensajes SNMP.

Este archivo yaml de StorageGRID para la asignación de resolución de solapamiento de Datadog se generó siguiendo la instrucción encontrada "aquí". + Coloque este archivo en /etc/datadog-agent/conf.d/snmp.d/traps_dB/ +

- "Descargue el archivo yaml de captura" +
  - **md5 checksum** 42e274210719945a46172b98c379517 +
  - * sha256 checksum* d0fe5c8e6ca3c902d054f854b70a85f928cba8b7c76391d356f05d2cf73b6887 +

Este archivo yaml de perfil de StorageGRID para la asignación de métricas de Datadog generada siguiendo la instrucción encontrada "aquí". + Coloque este archivo en /etc/datatog-agent/conf.d/snmp.d/profiles/ +

- "Descargue el archivo yaml de perfil" +
  - * md5 checksum* 72bb7784f4801adda4e0c3ea77df19aa +
  - * sha256 checksum* b6b7fadd33063422a8bb8e39b3ead8ab38349ee0229926eadc85f0087b8cee +

Configuración de Datadog de SNMP para Metrics

La configuración de SNMP para métricas se puede administrar de dos maneras. Puede configurar para la detección automática proporcionando un rango de direcciones de red que contenga los sistemas StorageGRID o definiendo las IP de los dispositivos individuales. La ubicación de la configuración es diferente en función de la decisión tomada. La detección automática se define en el archivo yaml del agente datatog. Las definiciones de dispositivos explícitas se configuran en el archivo yaml de configuración de snmp. A continuación, se muestran ejemplos de cada uno para el mismo sistema StorageGRID.

Detección automática

configuración ubicada en /etc/datadir-agent/datadir.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
```

Dispositivos individuales

/etc/datatog-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'
```

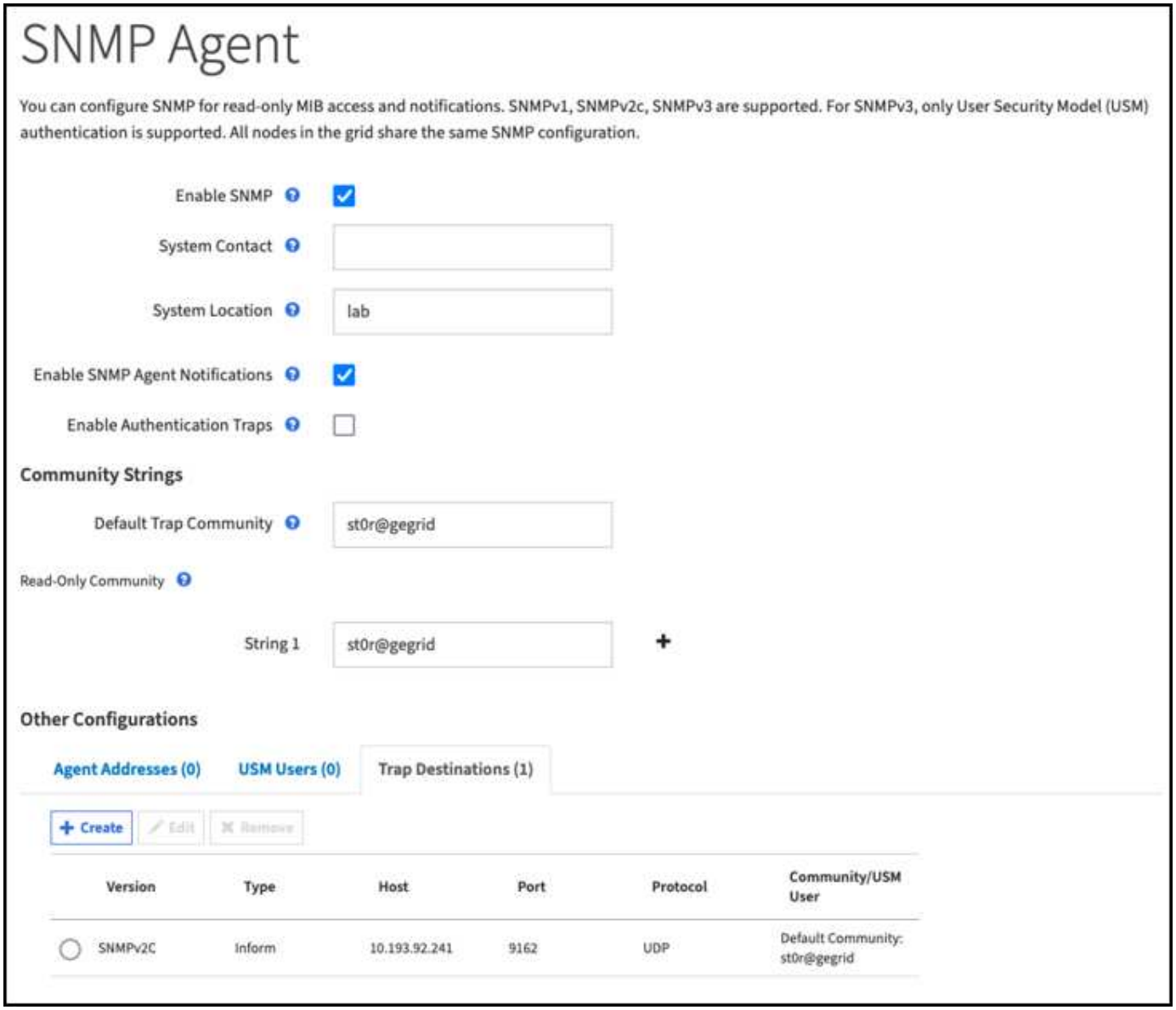
Configuración de SNMP para las capturas

La configuración de los solapamientos SNMP se define en el archivo de configuración de datadir ylma /etc/datadir-agent/datadog.ylma

```
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
```

Ejemplo de configuración de SNMP de StorageGRID

El agente SNMP del sistema StorageGRID se encuentra en la pestaña Configuración, columna Supervisión. Habilite SNMP e introduzca la información que desee. Si desea configurar capturas, seleccione "Destinos de capturas" y cree un destino para el host del agente de datos que contenga la configuración de capturas.



Utilice rclone para migrar, PONER y ELIMINAR objetos en StorageGRID

Por Siegfried Hepp y Aron Klein

Rclone es una herramienta de línea de comandos gratuita y un cliente para operaciones S3. Es posible usar rclone para migrar, copiar y eliminar datos de objetos en StorageGRID. rclone incluye la capacidad de eliminar cubos incluso cuando no están vacíos con una función de “purga” como se muestra en el siguiente ejemplo.

Instalar y configurar rclone

Para instalar rclone en una estación de trabajo o servidor, descárguelo de "rclone.org".

Pasos de configuración inicial

1. Cree el archivo de configuración rclone ejecutando el script de configuración o creando manualmente el archivo.
2. Para este ejemplo usaré sgdemo para el nombre del punto final remoto de StorageGRID S3 en la configuración rclone.
   a. Cree el archivo de configuración ~/.config/rclone/rclone.conf

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

   b. Ejecute rclone config

```
# rclone config
```

```
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
```

Ejemplos de comandos básicos

- * Crear un cubo:*

  `rclone mkdir remote:bucket`

  ```
  # rclone mkdir sgdemo:test01
  ```

  Utilice --no-check-certificate si necesita ignorar los certificados SSL.

- **Lista todos los cucharones:**

```
rclone lsd remote:
```

```
# rclone lsd sgdemo:
```

- **Lista objetos en un cubo específico:**

```
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
```

- **Eliminar un cucharón:**

```
rclone rmdir remote:bucket
```

```
# rclone rmdir sgdemo:test02
```

- * Poner un objeto:*

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

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

- **Obtener un objeto:**

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

```
# Rclone copy sgdemo:test01/Testfile.txt ~/test/testfileS3.txt
```

- **Eliminar un objeto:**

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

```
# rclone delete sgdemo:test01/testfile.txt
```

- **Migrar objetos en un cubo**

```
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
```

Utilice --Progress o -P para mostrar el progreso de la tarea. De lo contrario, no habrá ninguna salida.

- * Eliminar un cubo y todo el contenido del objeto*

```
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
```

Prácticas recomendadas de StorageGRID para la puesta en marcha con Veeam Backup and Replication

Por Oliver Haensel y Aron Klein

Esta guía se centra en la configuración de NetApp StorageGRID y, en parte, de backups y replicación de Veeam. Este documento está dirigido a administradores de almacenamiento y redes que estén familiarizados con los sistemas Linux y que tengan la tarea de mantener o implementar un sistema NetApp StorageGRID en combinación con Veeam Backup and Replication.

Descripción general

Los administradores de almacenamiento buscan gestionar el crecimiento de sus datos con soluciones que cumplen con la disponibilidad, los objetivos de recuperación rápida, los escalan para satisfacer sus necesidades y automatizan su política para la retención a largo plazo de datos. Estas soluciones también deben proporcionar protección frente a pérdidas o ataques maliciosos. Juntos, Veeam y NetApp se han asociado para crear una solución de protección de datos que combina backup y recuperación de Veeam con NetApp StorageGRID para el almacenamiento de objetos on-premises.

Veeam y NetApp StorageGRID ofrecen una solución fácil de usar que trabajan conjuntamente para ayudar a satisfacer las demandas del rápido crecimiento de los datos y las crecientes regulaciones en todo el mundo. El almacenamiento de objetos basado en cloud es conocido por su resiliencia, capacidad de escalado, eficiencia operativa y de costes que lo convierten en la opción lógica como destino para sus backups. En este documento se proporcionan instrucciones y recomendaciones para la configuración de su solución Veeam Backup y del sistema StorageGRID.

La carga de trabajo de objetos de Veeam crea una gran cantidad de OPERACIONES simultáneas DE PUT, DELETE y LIST DE objetos pequeños. Habilitar la inmutabilidad se añadirá al número de solicitudes al almacén de objetos para establecer la retención y mostrar versiones. El proceso de un trabajo de copia de seguridad incluye la escritura de objetos para el cambio diario. Después de que las nuevas escrituras se hayan completado, el trabajo eliminará cualquier objeto basado en la política de retención de la copia de seguridad. La programación de las tareas de backup casi siempre se superpondrá. Este solapamiento dará como resultado una gran parte de la ventana de backup que consiste en 50/50 carga de trabajo PUT/DELETE en el almacén de objetos. Realizar ajustes en Veeam al número de operaciones simultáneas con la configuración de la ranura de tareas, aumentar el tamaño del objeto aumentando el tamaño del bloque de trabajos de copia de seguridad, reduciendo el número de objetos en las solicitudes de eliminación de objetos

múltiples, y elegir la ventana de tiempo máximo para completar los trabajos optimizará el rendimiento y el costo de la solución.

Asegúrese de leer la documentación del producto para "Veeam Backup and Replication" y "StorageGRID" Antes de empezar. Veeam proporciona calculadoras para comprender el dimensionamiento de la infraestructura de Veeam y los requisitos de capacidad que se deben utilizar antes de dimensionar su solución StorageGRID . Consulte siempre las configuraciones validadas de Veeam- NetApp en el sitio web del Programa Veeam Ready. "Veeam Ready Object, inmutabilidad de objetos y repositorio" .

Configuración de Veeam

Versión recomendada

Siempre se recomienda mantenerse al día y aplicar las revisiones más recientes para su sistema Veeam Backup & Replication 12 o 12,1. Actualmente recomendamos instalar como mínimo el parche P20230718 de Veeam 12.

S3 Configuración del repositorio

Un repositorio de backup de escalado horizontal (SOBR) es el nivel de capacidad del almacenamiento de objetos S3. El nivel de capacidad es una extensión del repositorio primario que proporciona períodos de retención de datos más largos y una solución de almacenamiento de menor coste. Veeam ofrece la capacidad de proporcionar inmutabilidad a través de la API de bloqueo de objetos S3. Veeam 12 puede utilizar múltiples buckets en un repositorio de escalado horizontal. StorageGRID no tiene un límite en cuanto al número de objetos o de capacidad de un único bloque. El uso de varios bloques puede mejorar el rendimiento cuando se realizan backups de conjuntos de datos de gran tamaño donde los datos de backup pueden llegar a escalarse a petabytes en objetos.

En función del dimensionamiento de su solución y sus requisitos específicos, puede que sea necesario limitar las tareas simultáneas. La configuración predeterminada especifica una ranura de tareas de repositorio para cada núcleo de CPU y para cada ranura de tareas un límite de ranura de tareas simultáneas de 64. Por ejemplo, si el servidor tiene 2 núcleos de CPU, se utilizará un total de 128 subprocesos simultáneos para el almacén de objetos. Esto incluye PUT, GET y SUPR por lotes. Se recomienda seleccionar un límite conservador para las ranuras de tareas con las que empezar y ajustar este valor una vez que los backups de Veeam hayan alcanzado un estado constante de nuevos backups y datos de backup caducados. Trabaje con el equipo de su cuenta de NetApp para dimensionar el sistema de StorageGRID correctamente para satisfacer el rendimiento y los periodos de tiempo deseados. Es posible que sea necesario ajustar el número de ranuras de tareas y el límite de tareas por ranura para proporcionar la solución óptima.

Configuración de trabajos de copia de seguridad

Los trabajos de copia de seguridad de Veeam se pueden configurar con diferentes opciones de tamaño de bloque que se deben considerar cuidadosamente. El tamaño de bloque predeterminado es de 1MB KB y, con las eficiencias de almacenamiento que Veeam proporciona compresión y la deduplicación crea tamaños de objeto de aproximadamente 500KB KB para el backup completo inicial y objetos de 100-200kB MB para los trabajos incrementales. Podemos aumentar considerablemente el rendimiento y reducir los requisitos del almacén de objetos eligiendo un tamaño de bloque de backup mayor. Aunque el tamaño de bloque mayor realiza grandes mejoras en el rendimiento del almacén de objetos, se logra a costa de unos requisitos de capacidad de almacenamiento primario potencialmente mayores gracias a la reducción del rendimiento de la eficiencia del almacenamiento. Se recomienda que los trabajos de backup se configuren con un tamaño de bloque de 4MB KB que cree aproximadamente 2MB objetos para los backups completos y tamaños de objeto de 700KB a 1MB KB para los incrementales. Los clientes pueden considerar incluso configurar tareas de backup con un tamaño de bloque de 8 MB, que se puede habilitar con la ayuda del soporte de Veeam.

La implementación de backups inmutables utiliza S3 Object Lock en el almacén de objetos. La opción Inmutabilidad genera un mayor número de solicitudes al almacén de objetos para mostrar y actualizar la retención en los objetos.

A medida que las retenciones de copia de seguridad vencen, los trabajos de copia de seguridad procesarán la eliminación de objetos. Veeam envía las solicitudes de eliminación al almacén de objetos en solicitudes de eliminación de objetos múltiples de 1000 objetos por solicitud. Para soluciones pequeñas, esto puede necesitar ser ajustado para reducir el número de objetos por solicitud. Al reducir este valor, se añadirá la ventaja de distribuir de forma más uniforme las solicitudes de eliminación entre los nodos del sistema StorageGRID. Se recomienda utilizar los valores de la siguiente tabla como punto de partida en la configuración del límite de eliminación de objetos múltiples. Multiplique el valor de la tabla por el número de nodos para el tipo de dispositivo elegido para obtener el valor de la configuración en Veeam. Si este valor es igual o mayor que 1000, no es necesario ajustar el valor predeterminado. Si este valor necesita ser ajustado, por favor trabaje con el soporte de Veeam para hacer el cambio.

Modelo de dispositivo	S3MultiObjectDeleteLimit por nodo
SG5712	34
SG5760	75
SG6060	200

Trabaje en colaboración con su equipo de cuenta de NetApp para la configuración recomendada de acuerdo con sus necesidades específicas. Las recomendaciones de ajustes de configuración de Veeam incluirán:

- Tamaño del bloque de tareas de backup = 4MB
- Límite de ranura de tarea SOBR = 2-16
- Límite de eliminación de objetos múltiples = 34-1000

Configuración de StorageGRID

Versión recomendada

NetApp StorageGRID 11.9 o 12.0 con la última revisión son las versiones recomendadas para las implementaciones de Veeam. Siempre se recomienda mantenerse actualizado y aplicar las últimas revisiones para su sistema StorageGRID .

Configuración del balanceador de carga y del extremo S3

Veeam requiere que el punto final se conecte solo a través de HTTPS. Veeam no admite una conexión no cifrada. El certificado SSL puede ser un certificado autofirmado, una entidad de certificación privada de confianza o una entidad de certificación pública de confianza. Para garantizar el acceso continuo al repositorio de S3, se recomienda utilizar al menos dos equilibradores de carga en una configuración de alta disponibilidad. Los balanceadores de carga pueden ser un servicio de balanceador de carga integrado proporcionado por StorageGRID ubicado en cada nodo de administración y nodo de puerta de enlace o solución de terceros como F5, Kemp, HAProxy, Loadbalancer.org, etc. El uso de un equilibrador de carga StorageGRID proporcionará la capacidad de establecer clasificadores de tráfico (reglas de QoS) que puedan priorizar la carga de trabajo de Veeam o limitar Veeam para no afectar a las cargas de trabajo de mayor prioridad en el sistema StorageGRID.

Bloque de S3

StorageGRID es un sistema de almacenamiento seguro de múltiples inquilinos. Se recomienda crear un inquilino dedicado para la carga de trabajo de Veeam. Se puede asignar opcionalmente una cuota de almacenamiento. Como práctica recomendada, habilite “utilizar su propia fuente de identidad”. Proteja el usuario de administración raíz del inquilino con una contraseña adecuada. Veeam Backup 12 requiere una fuerte consistencia para los buckets S3. StorageGRID ofrece múltiples opciones de consistencia configuradas a nivel de depósito. Para implementaciones de múltiples sitios con Veeam accediendo a los datos desde múltiples ubicaciones, seleccione “strong-global”. Si las copias de seguridad y restauraciones de Veeam se realizan en un solo sitio, el nivel de consistencia debe establecerse en “sitio sólido”. Para obtener más información sobre los niveles de consistencia de los depósitos, revise la "documentación" . Para usar StorageGRID para las copias de seguridad de inmutabilidad de Veeam, S3 Object Lock debe estar habilitado globalmente y configurado en el depósito durante la creación del depósito.

Gestión del ciclo de vida

StorageGRID admite la replicación y el código de borrado para la protección a nivel de objeto en nodos y sitios de StorageGRID. El código de borrado requiere un tamaño de objeto de 200kB KB como mínimo. El tamaño de bloque predeterminado para Veeam de 1MB produce tamaños de objeto que a menudo pueden estar por debajo de este tamaño mínimo recomendado de 200kB después de las eficiencias de almacenamiento de Veeam. Para mejorar el rendimiento de la solución, no se recomienda utilizar un perfil de código de borrado que abarque varios sitios a menos que la conectividad entre los sitios sea suficiente para no agregar latencia ni restringir el ancho de banda del sistema StorageGRID. En un sistema StorageGRID multisitio, la regla de gestión del ciclo de vida de la información se puede configurar para almacenar una sola copia en cada sitio. Para la máxima durabilidad, se puede configurar una regla para almacenar una copia codificada de borrado en cada sitio. El uso de dos copias locales en los servidores de Veeam Backup es la implementación más recomendada para esta carga de trabajo.

Eliminar rendimiento

Veeam permite ajustar la tasa de solicitudes de eliminación y programar el proceso de eliminación de copias de seguridad. Para ajustar aún más el rendimiento de eliminación, puede deshabilitar las eliminaciones sincrónicas y dejar que el escáner ILM administre la eliminación final de objetos.

Pasos para deshabilitar las eliminaciones sincrónicas

1. Abra el Administrador de cuadrícula StorageGRID .
2. En la esquina superior derecha, seleccione el signo de interrogación y luego Documentación API.
3. En la esquina superior derecha, haga clic en el enlace de la página Documentación de API privada.
4. Expandir ilm-advanced.
5. Seleccione OBTENER ilm-advanced.
6. Seleccione Probar y luego Ejecutar.
7. Compruebe el resultado de la respuesta.

    a. Si los valores son nulos, significa que se utilizan los valores predeterminados de ilm-advanced.

    b. Si los valores no son nulos, significa que se están utilizando valores avanzados de ILM personalizados. Copia toda la salida después de "data" :, comenzando con { hasta el segundo al último }.

        i. Guárdalo en algún editor de texto.

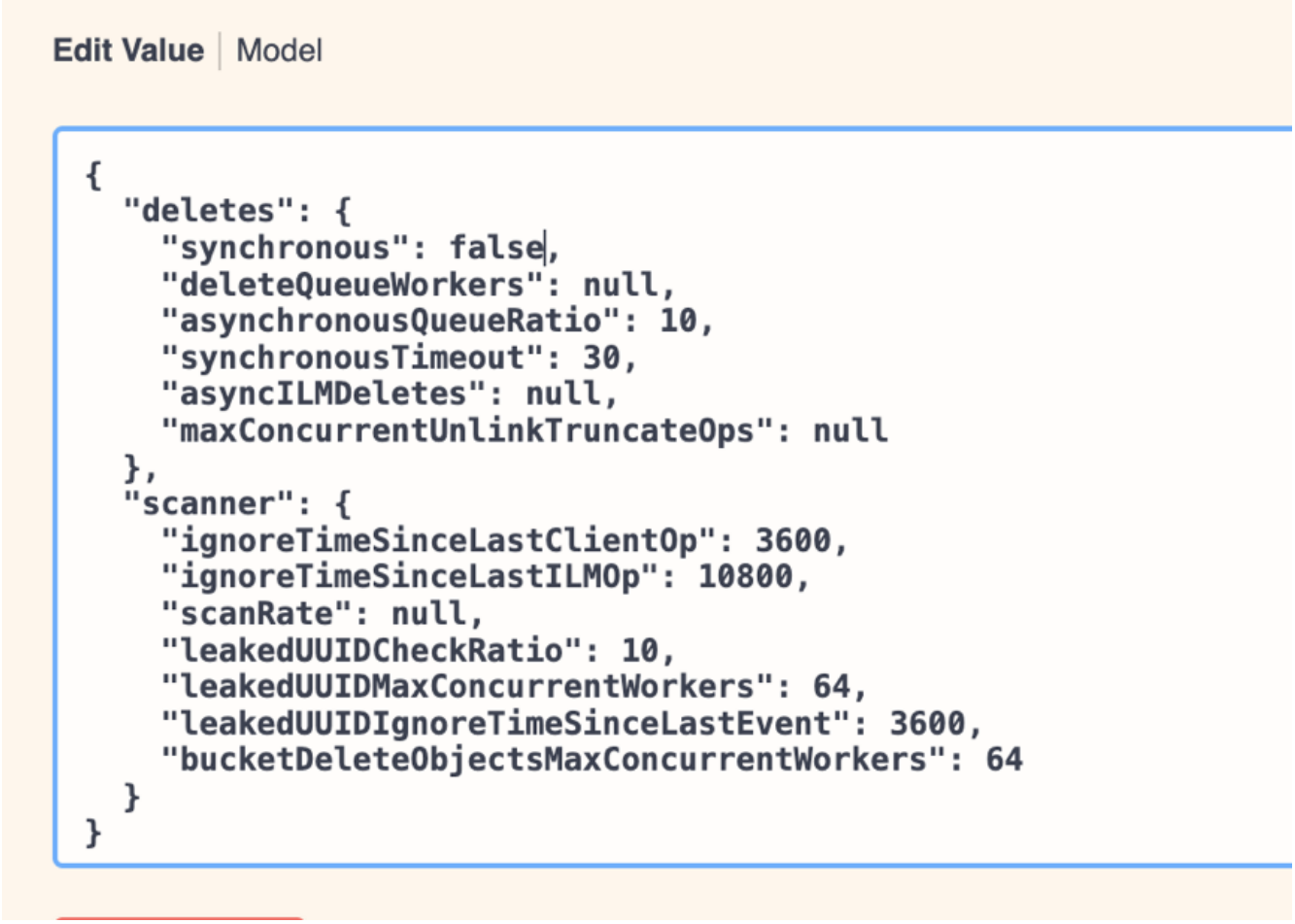
        Ejemplo de respuesta:

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. Seleccione PUT ilm-advanced.
9. Seleccione Probarlo para comenzar a editar el cuerpo de la API.
    a. De forma predeterminada, el cuerpo de la API contendrá valores predeterminados y no valores personalizados que se hayan configurado previamente. Esta es la razón por la que es MUY importante ejecutar los pasos 5 a 7.
10. Si se encuentran valores no predeterminados en el paso 5-7, reemplace el cuerpo de la API con la salida guardada en el paso 7. . De lo contrario, si los valores fueron nulos en el paso 5-7, deje el cuerpo de la API como está.
11. Ajuste los siguientes parámetros en el cuadro del cuerpo de la API:
    a. Establezca el valor sincrónico en falso.

       Ejemplo de texto del cuerpo de la API:

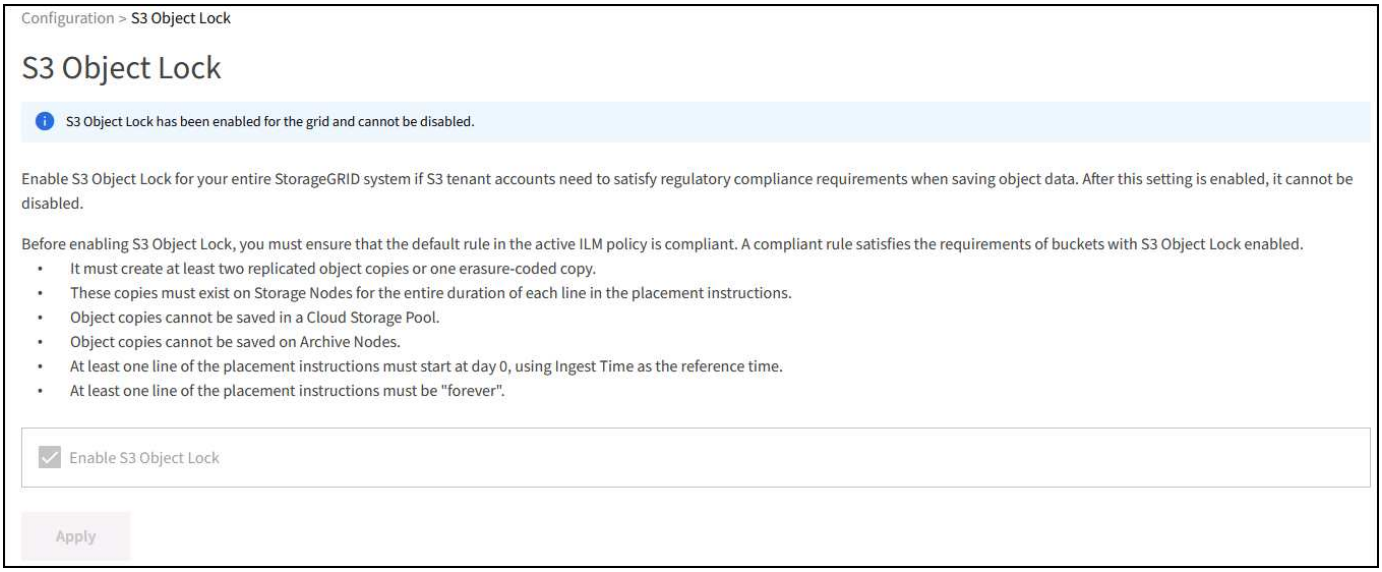


12. Una vez completado, seleccione Ejecutar

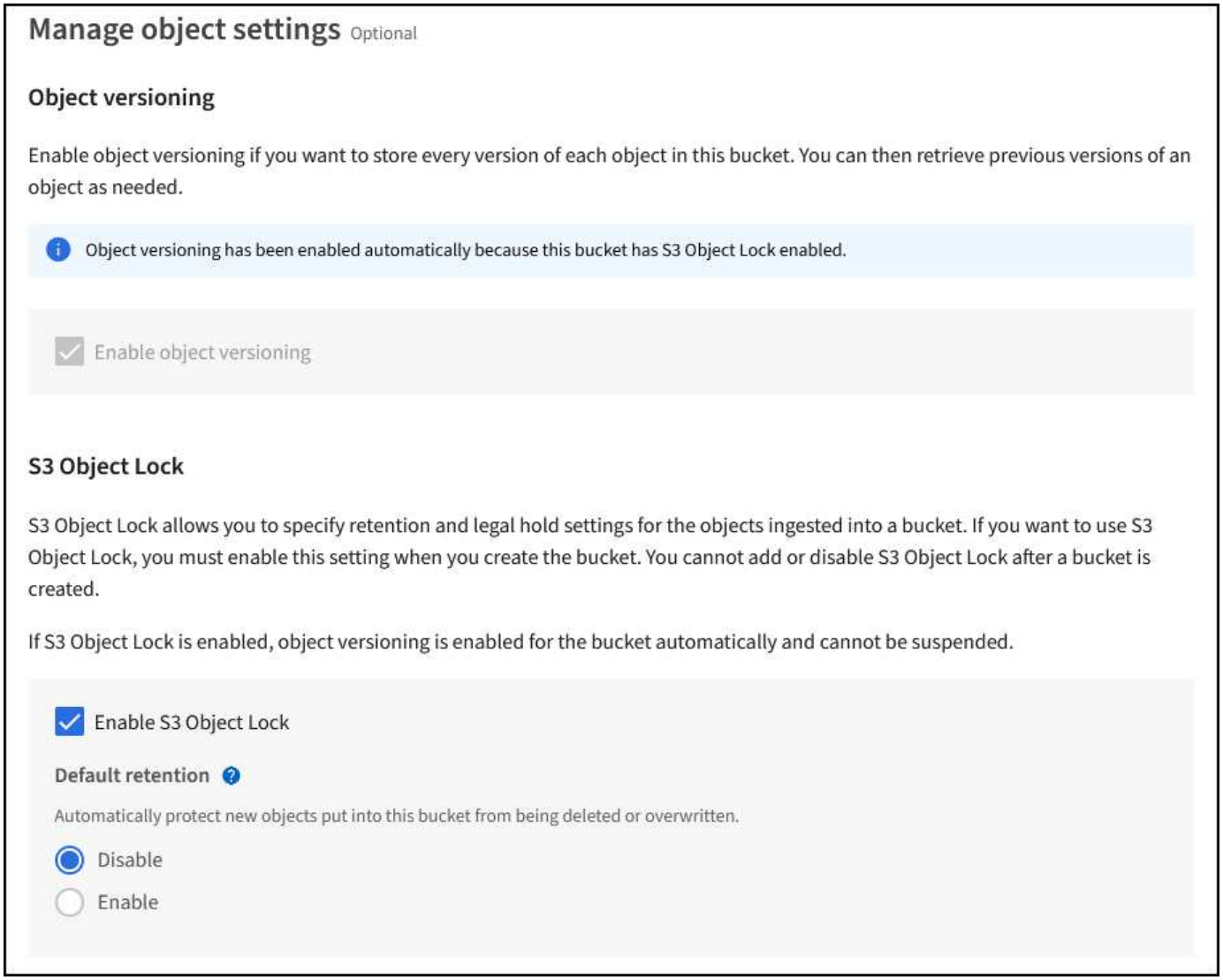
Puntos clave de implementación

StorageGRID

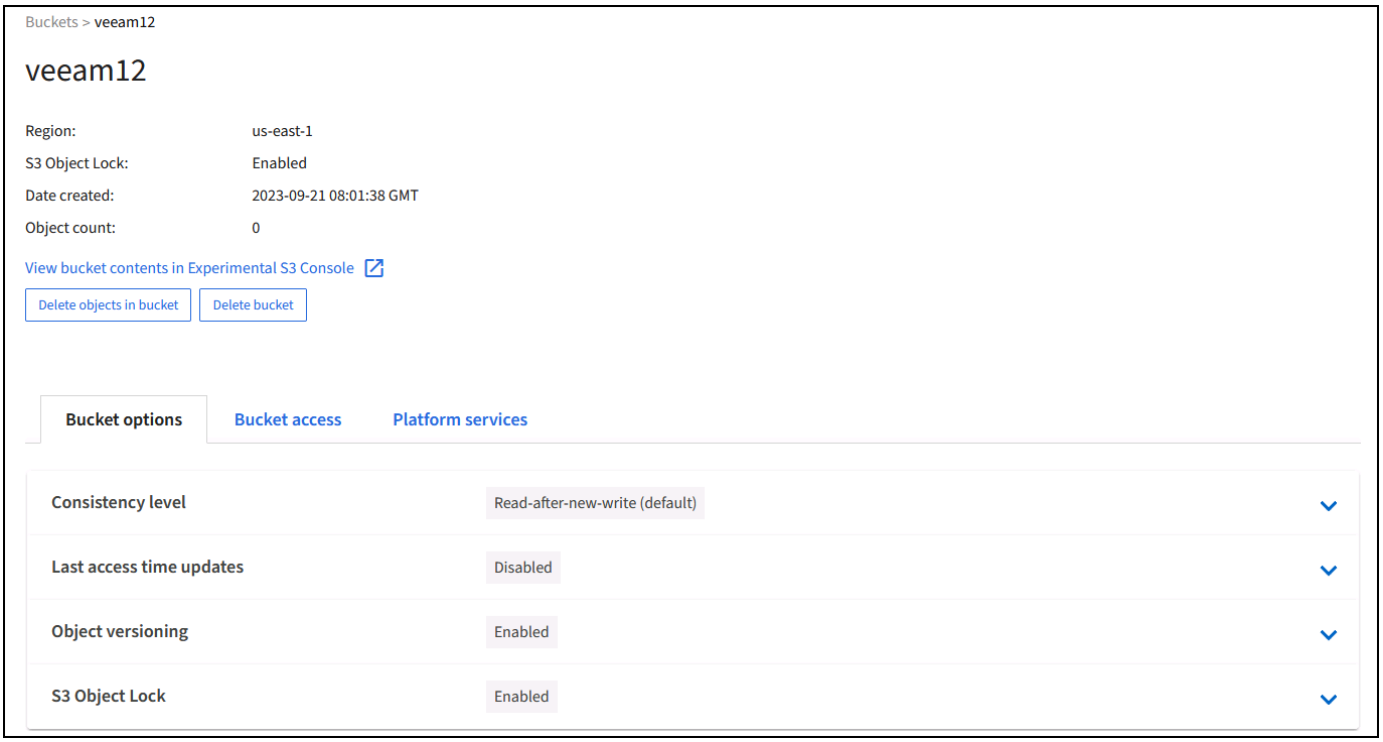
Asegúrese de que el bloqueo de objetos está activado en el sistema StorageGRID si es necesario inmutabilidad. Busque la opción en la interfaz de usuario de administración en Configuration/S3 Object Lock.



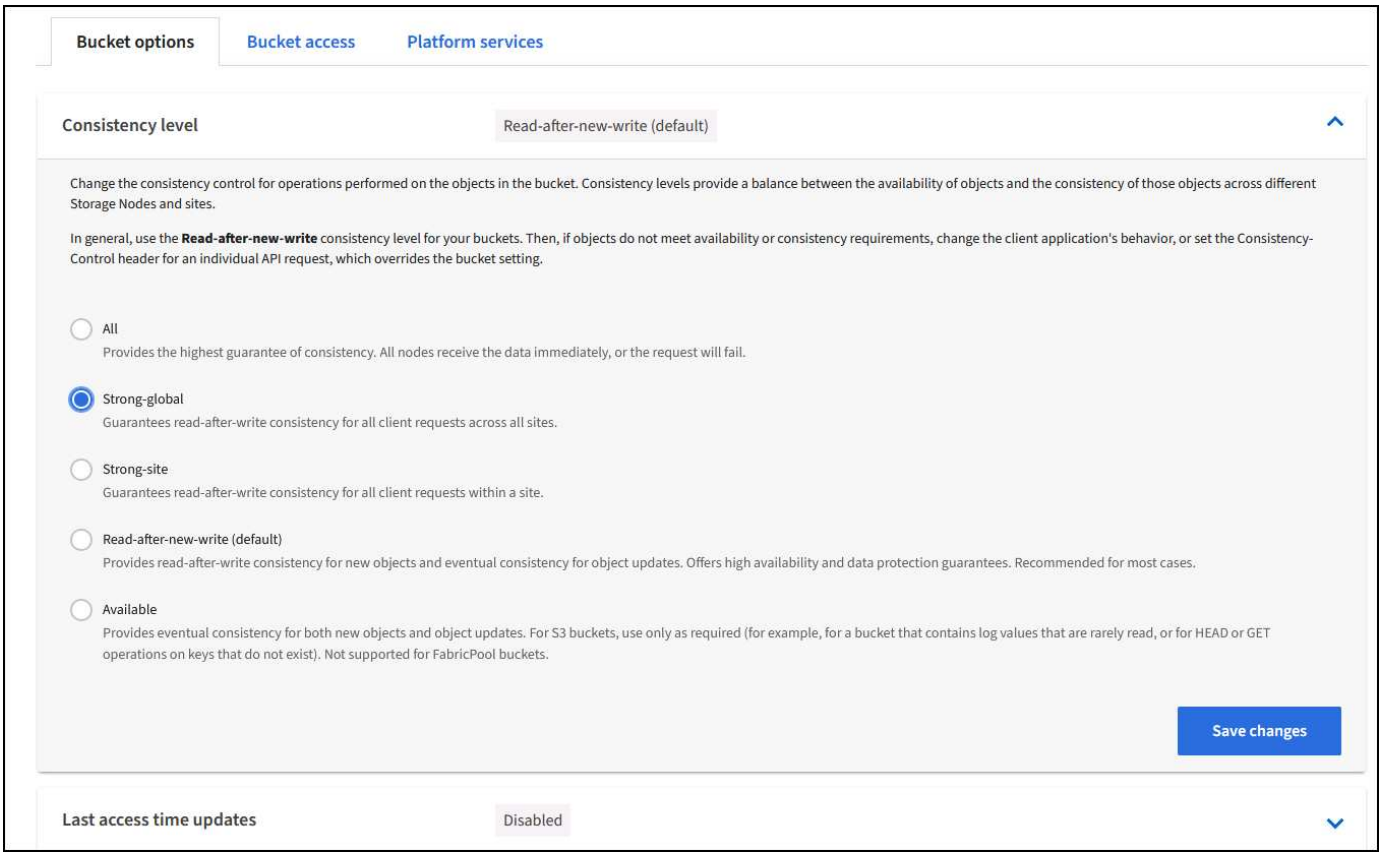
Al crear el bucket, seleccione «Enable Object Lock» (Habilitar bloqueo de objetos S3) si este bucket se va a utilizar para backups de inmutabilidad. Esto habilitará automáticamente el control de versiones de bloques. Deje desactivada la retención predeterminada, ya que Veeam establecerá la retención de objetos de forma explícita. El control de versiones y el bloqueo de objetos S3 no se deben seleccionar si Veeam no está creando copias de seguridad inmutables.



Una vez creado el bloque, vaya a la página de detalles del bloque creado. Seleccione el nivel de coherencia.



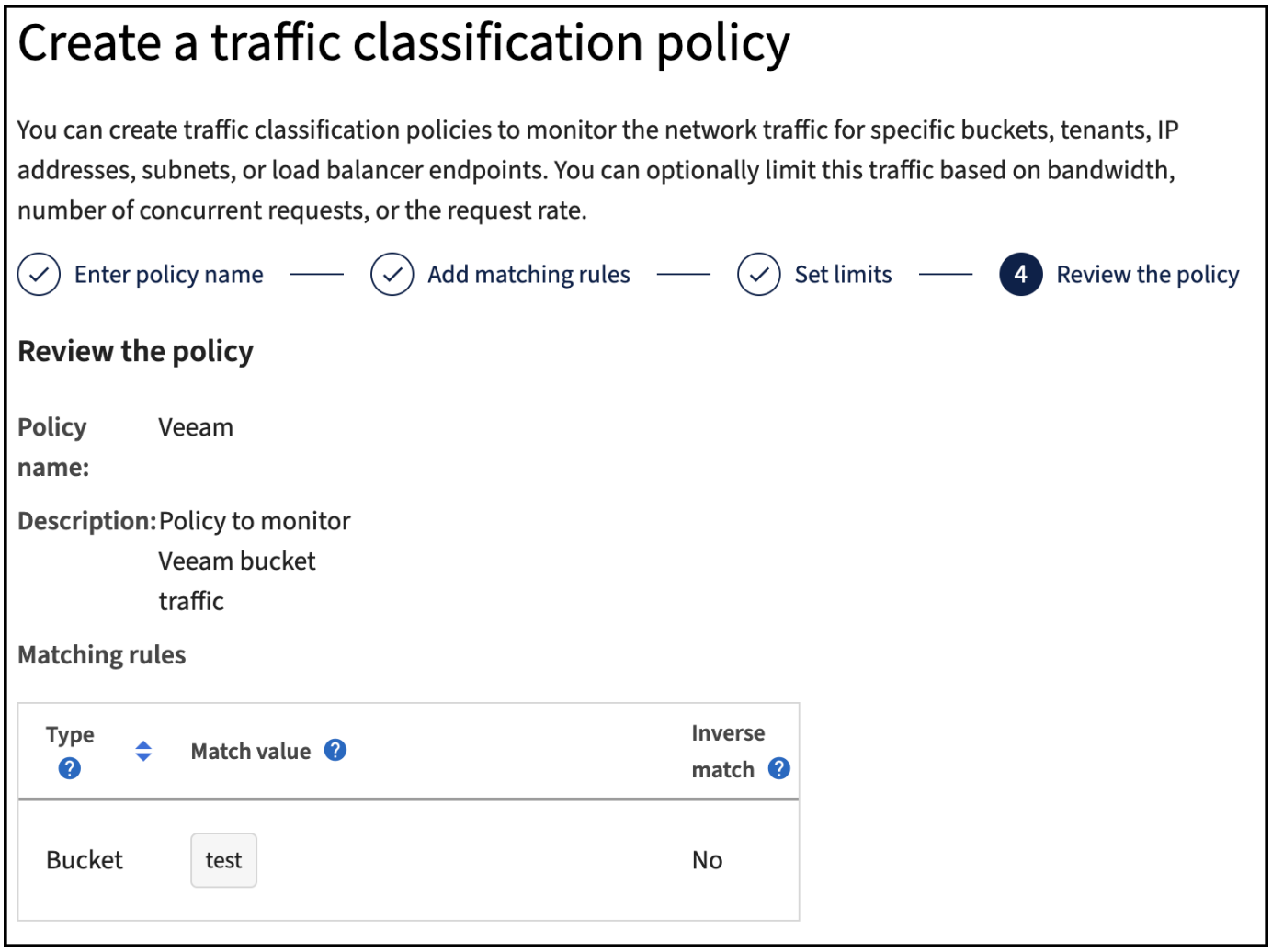
Veeam requiere una gran coherencia para bloques de S3. Por lo tanto, para implementaciones de múltiples sitios con Veeam accediendo a los datos desde múltiples ubicaciones, seleccione “strong-global”. Si los backups y restauraciones de Veeam se producen en un solo sitio, el nivel de consistencia debe establecerse en «sitio fuerte». Guarde los cambios.



StorageGRID ofrece un servicio de balanceo de carga integrado en cada nodo de administración y nodos de

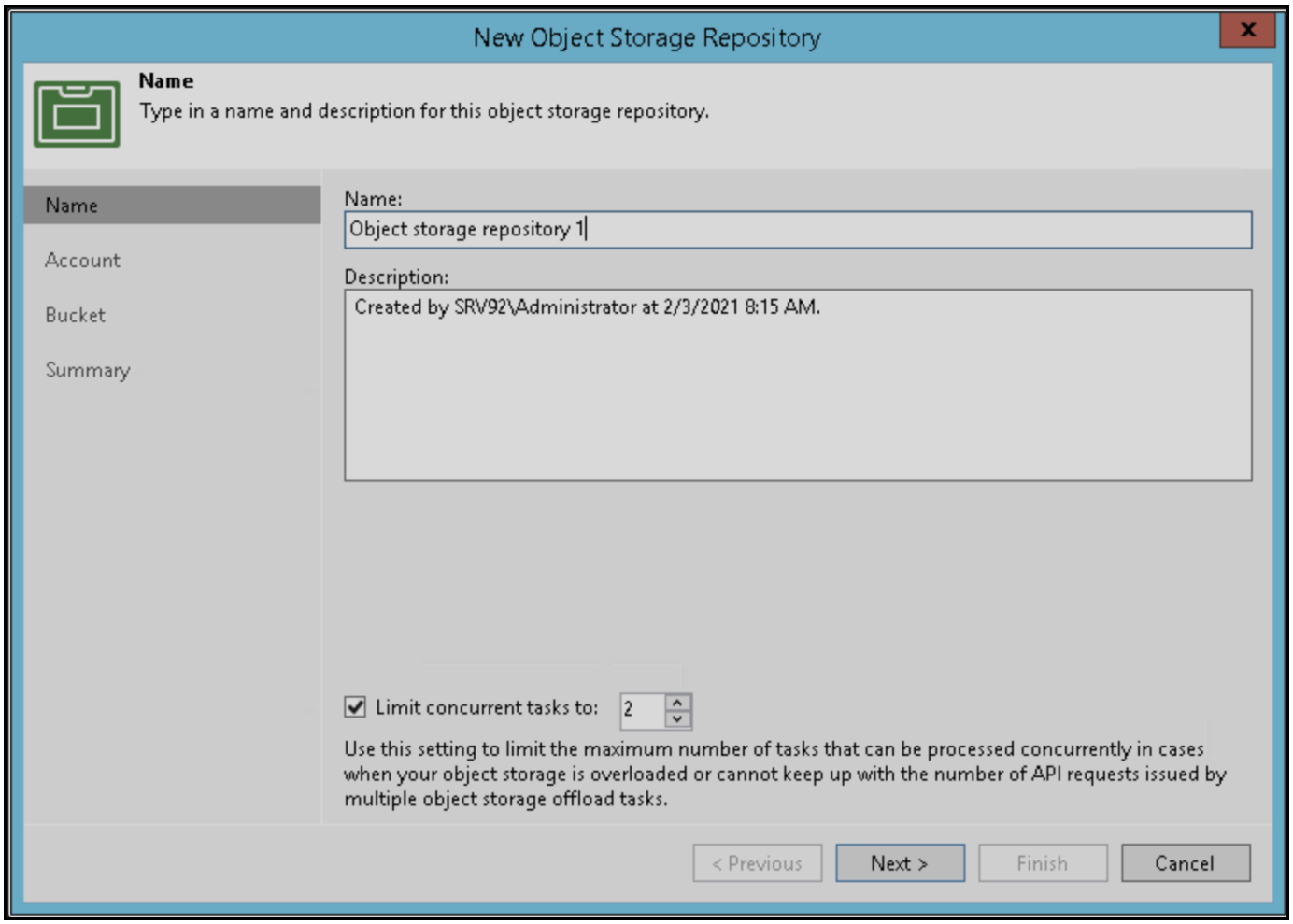
pasarela dedicados. Una de las muchas ventajas de usar este equilibrador de carga es la capacidad de configurar políticas de clasificación de tráfico (QoS). Aunque se utilizan principalmente para limitar el impacto de las aplicaciones en otras cargas de trabajo de clientes o priorizar una carga de trabajo sobre otras, también proporcionan una bonificación de la recopilación de métricas adicionales para ayudar a la supervisión.

En la pestaña de configuración, seleccione “Clasificación de tráfico” y cree una nueva política. Asigne un nombre a la regla y seleccione el tipo de cubo o arrendatario. Introduzca los nombres de los cubos o arrendatarios. Si la QoS es necesaria, establece un límite, pero para la mayoría de las implementaciones, solo queremos agregar los beneficios de monitoreo que proporciona, así que no establezcas un límite.

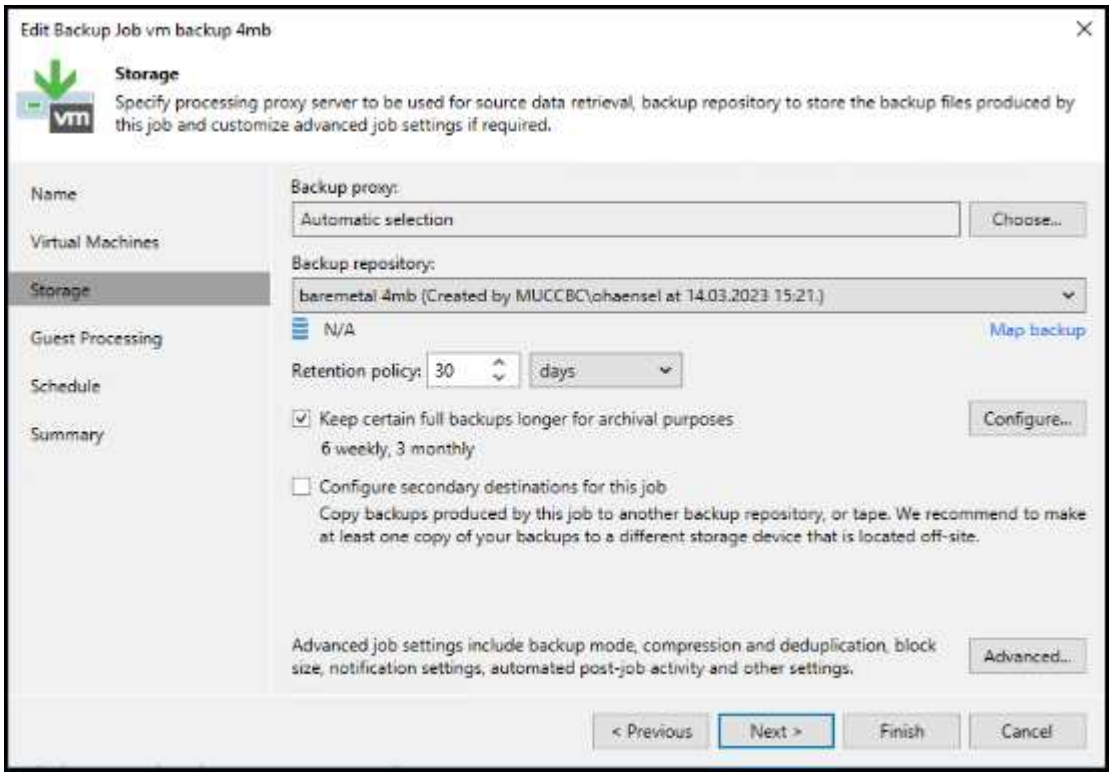


Veeam

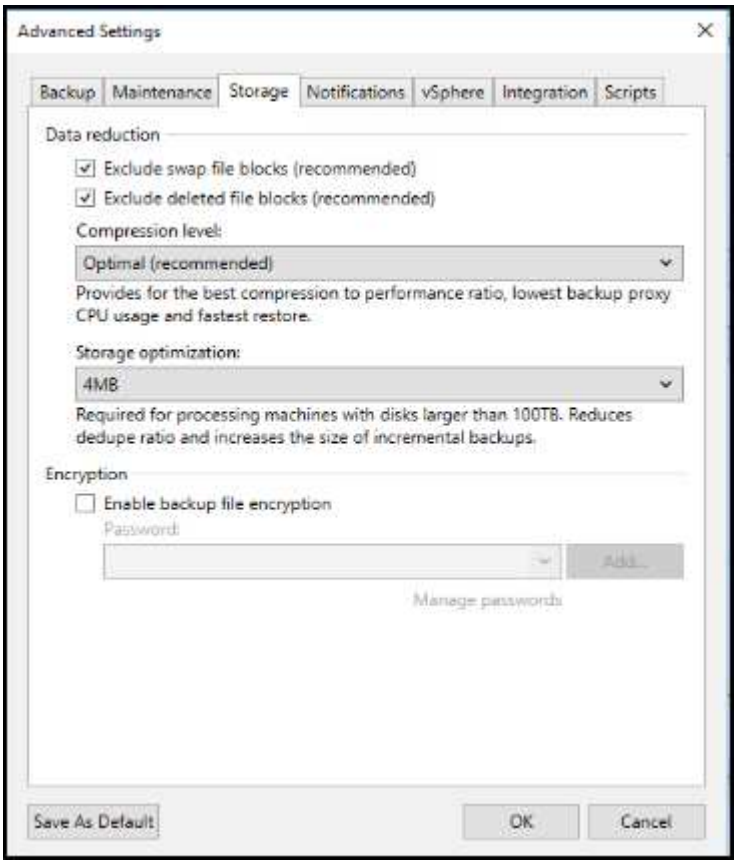
En función del modelo y la cantidad de dispositivos StorageGRID, puede que sea necesario seleccionar y configurar un límite para el número de operaciones simultáneas en el bloque.



Siga la documentación de Veeam sobre la configuración del trabajo de copia de seguridad en la consola de Veeam para iniciar el asistente. Después de agregar VM, seleccione el repositorio SOBR.



Haga clic en Configuración avanzada y cambie la configuración de optimización de almacenamiento a 4 MB o más. Se activará la compresión y la deduplicación. Cambie la configuración de invitado según sus requisitos y configure la programación de trabajos de copia de seguridad.



Supervisión de StorageGRID

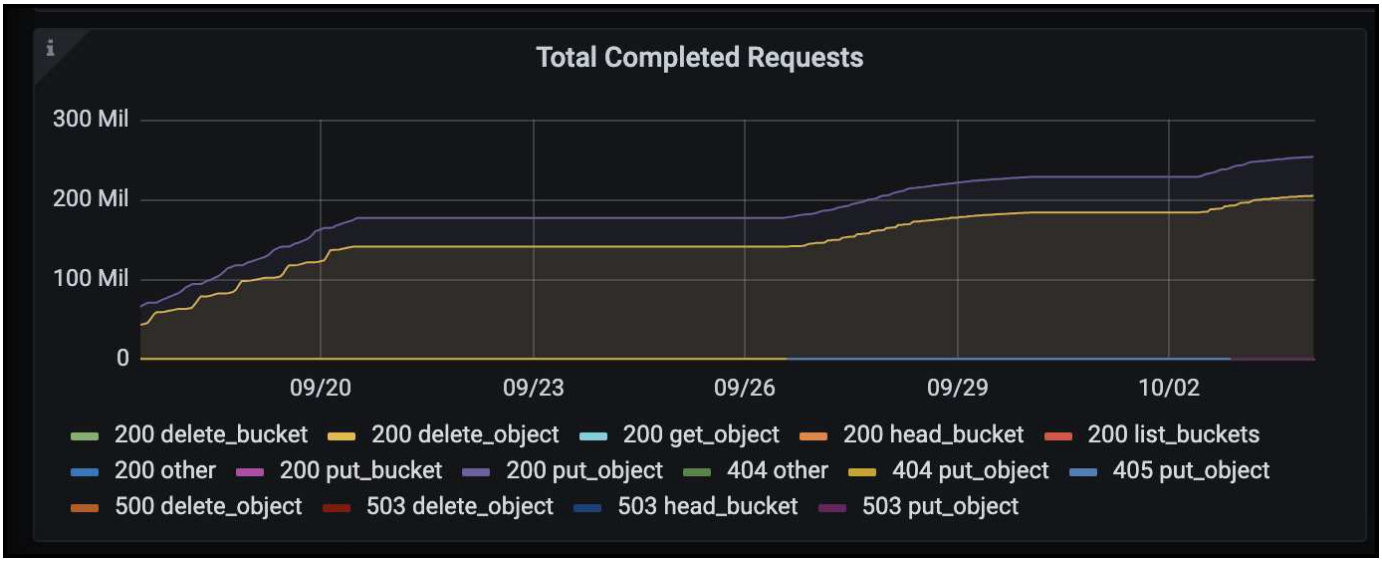
Para obtener una visión completa del rendimiento que están teniendo Veeam y StorageGRID juntos, deberá esperar hasta que haya caducado el tiempo de retención de los primeros backups. Hasta este punto, la carga de trabajo de Veeam consta principalmente de OPERACIONES PUT y no se han producido eliminaciones. Una vez que los datos de backup caducan y se producen limpiezas, ahora puede ver el uso consistente completo en el almacén de objetos y ajustar la configuración en Veeam si es necesario.

StorageGRID proporciona gráficos prácticos para supervisar el funcionamiento del sistema ubicado en la página Métricas de la pestaña Soporte. Los paneles principales a ver serán la información general de S3, ILM y la normativa de clasificación de tráfico si se crea una normativa. En el panel de Descripción general de S3 encontrará información sobre las tasas de funcionamiento de S3, las latencias y las respuestas de las solicitudes.

Si observa las tasas de S3 y las solicitudes activas, puede ver cuánta carga está manejando cada nodo y el número general de solicitudes por tipo.

El gráfico Duración Media muestra el tiempo medio que cada nodo está tomando para cada tipo de solicitud. Esta es la latencia media de la solicitud y puede ser un buen indicador de que se puede requerir un ajuste adicional, o hay espacio para que el sistema StorageGRID asuma más carga.

En el gráfico Total de Solicitudes Completadas, puede ver las solicitudes por tipo y códigos de respuesta. Si ve respuestas distintas de 200 (OK) para las respuestas, esto puede indicar un problema como que el sistema StorageGRID está recibiendo una carga elevada enviando respuestas 503 (Lento) y puede que sea necesario realizar algún ajuste adicional, o que haya llegado el momento de expandir el sistema para aumentar la carga.



En la consola de gestión de la vida útil de la información, puede supervisar el rendimiento de eliminación del sistema StorageGRID. StorageGRID usa una combinación de eliminaciones síncronas y asíncronas en cada nodo a fin de intentar optimizar el rendimiento general de todas las solicitudes.

Con una Política de clasificación de tráfico, podemos ver las métricas del rendimiento de la solicitud del equilibrador de carga, las tasas, la duración, así como los tamaños de los objetos que Veeam envía y recibe.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- "Documentación del producto NetApp StorageGRID"
- "Veeam Backup and Replication"

Configurar el origen de datos de Dremio con StorageGRID

Por Angela Cheng

Dremio admite una variedad de fuentes de datos, incluido el almacenamiento de objetos en las instalaciones o basado en cloud. Puede configurar Dremio para que utilice StorageGRID como origen de datos de almacenamiento de objetos.

Configurar el origen de datos de Dremio

Requisitos previos

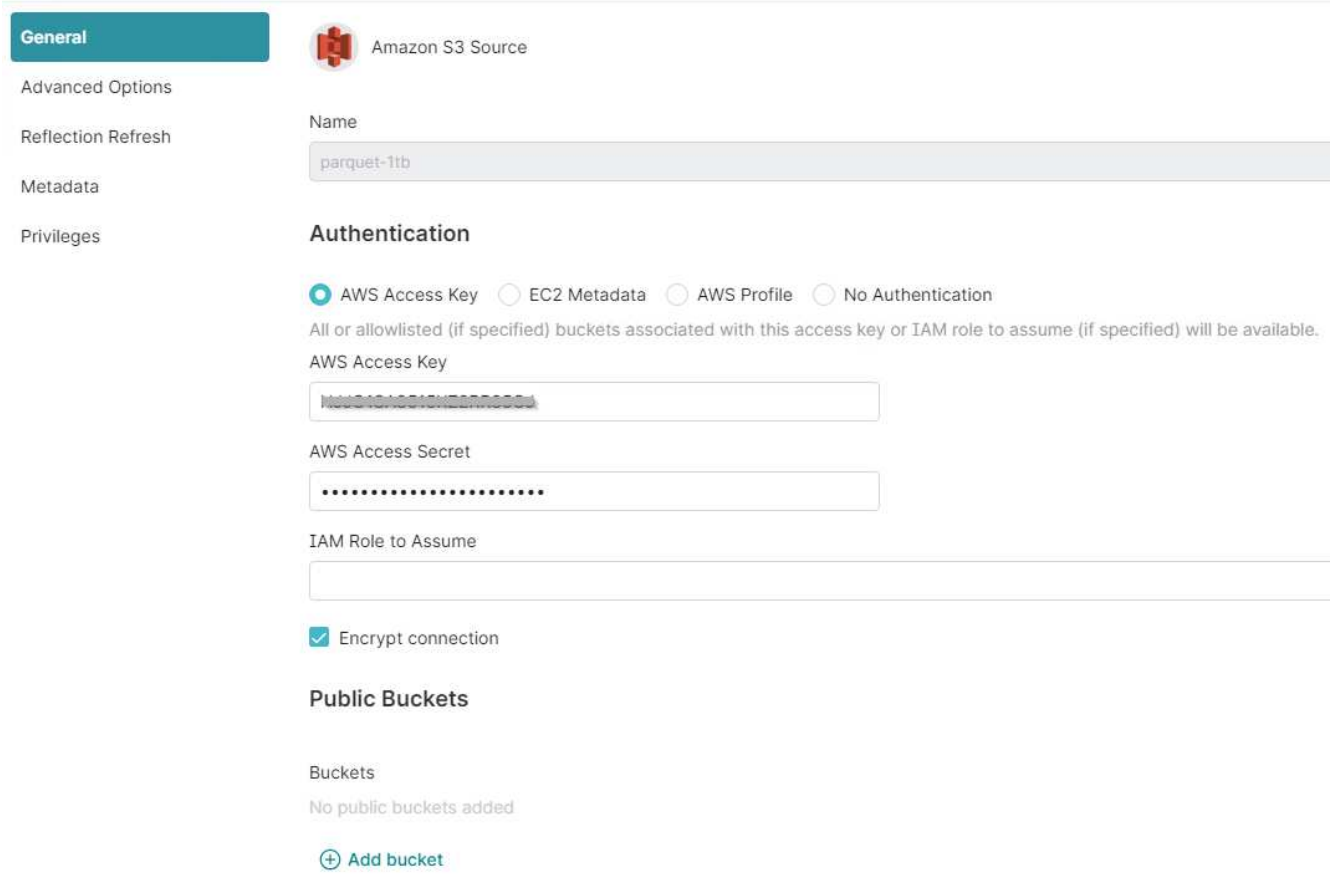
- Una URL de extremo de StorageGRID S3, un ID de clave de acceso de inquilino S3 y una clave de acceso secreta.
- Recomendación de configuración de StorageGRID: Deshabilitar la compresión (deshabilitada de forma predeterminada).
  Dremio utiliza el rango de bytes GET para recuperar diferentes rangos de bytes dentro del mismo objeto simultáneamente durante la consulta. El tamaño típico de las solicitudes de rango de bytes es 1MB. El objeto comprimido degrada el RENDIMIENTO DE LA OBTENCIÓN por rango de bytes.

Guía de Dremio

"Conexión a Amazon S3: Configuración de almacenamiento compatible con S3".

Instrucción

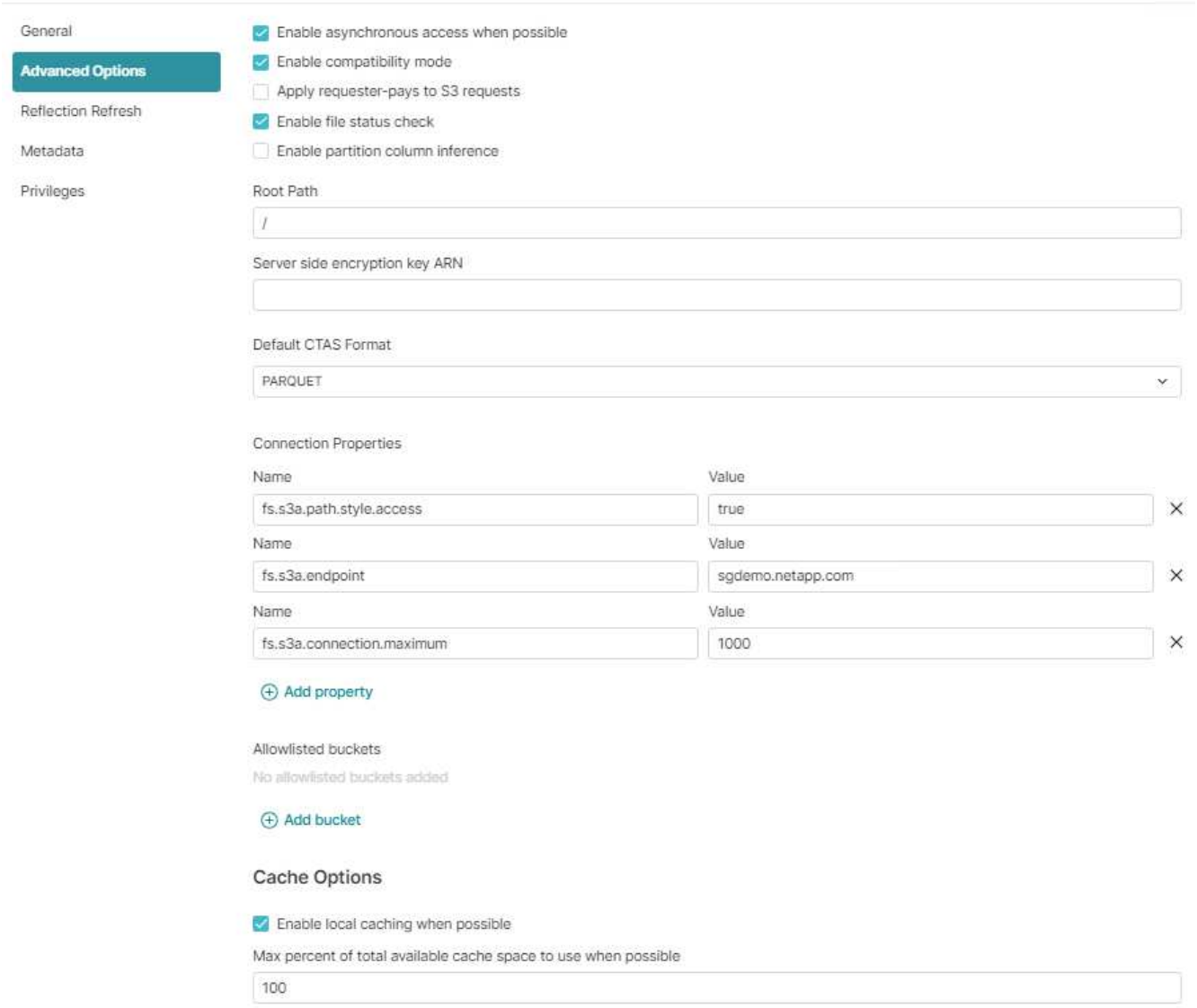
1. En la página Dremio Datasets, haga clic en el signo + para agregar una fuente, seleccione 'Amazon S3'.
2. Introduzca un nombre para este nuevo origen de datos, ID de clave de acceso de inquilino de StorageGRID S3 y clave de acceso secreta.
3. Active la casilla 'Cifrar conexión' si utiliza https para la conexión al punto final StorageGRID S3.
   Si utiliza el certificado de CA autofirmado para este punto final S3, siga las instrucciones de la guía de Dremio para agregar este certificado de CA al servidor <JAVA_HOME>/jre/lib/security + de Dremio
   Captura de pantalla de ejemplo



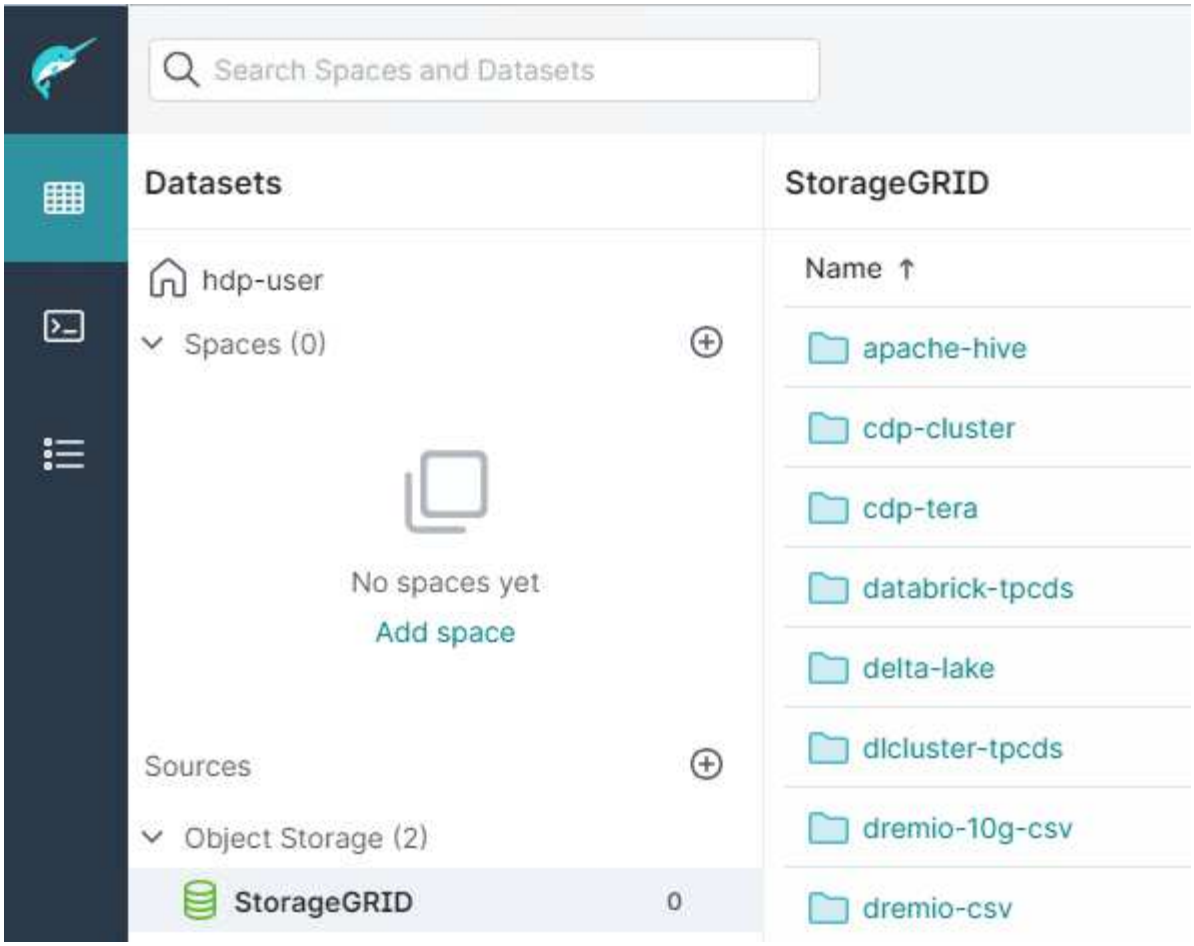
4. Haga clic en 'Opciones avanzadas', seleccione 'Activar modo de compatibilidad'
5. En Propiedades de conexión, haga clic en + Agregar propiedades y agregue estas S3A propiedades.
6. fs.s3a.connection.el valor por defecto máximo es 100. Si los conjuntos de datos S3 incluyen archivos de parquet grandes con 100 o más columnas, debe introducir un valor mayor que 100. Consulte la guía de Dremio para conocer este ajuste.

Nombre	Valor
fs.s3a.endpoint	*<StorageGRID S3 endpoint:Port>*
fs.s3a.path.style.access	verdadero
fs.s3a.conexión.máximo	*<un valor mayor que 100>*

Captura de pantalla de ejemplo



7. Configure otras opciones de Dremio según los requisitos de su organización o aplicación.
8. Haga clic en el botón Guardar para crear este nuevo origen de datos.
9. Una vez que el origen de datos StorageGRID se haya agregado correctamente, se mostrará una lista de cubos en el panel izquierdo.
   Captura de pantalla de ejemplo



NetApp StorageGRID con GitLab

Por Angela Cheng

NetApp ha probado StorageGRID con GitLab. Consulte la configuración de GitLab de ejemplo a continuación. Consulte "Guía de configuración de almacenamiento de objetos de GitLab" para obtener más detalles.

Ejemplo de conexión de almacenamiento de objetos

Para las instalaciones de Linux Package, este es un ejemplo de `connection` configuración en el formulario consolidado. Editar `/etc/gitlab/gitlab.rb` y agregue las siguientes líneas, sustituyendo los valores que desee:

```
# 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'
```

Procedimientos y ejemplos de API

Pruebe y muestre opciones de cifrado de S3 en StorageGRID

Por Aron Klein

StorageGRID y la API de S3 ofrecen varias formas diferentes de cifrar sus datos en reposo. Para obtener más información, consulte "Consulte los métodos de cifrado de StorageGRID".

En esta guía se mostrarán los métodos de cifrado de la API de S3.

Cifrado del servidor (SSE)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, la clave almacenada en StorageGRID descifra el objeto.

Ejemplo de SSE

- PONGA un objeto con SSE

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

- DIRÍJASE al objeto para verificar el cifrado

```
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": {}
}
```

- OBTENGA el objeto

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

Cifrado del servidor con claves proporcionadas por el cliente (SSE-C)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única proporcionada por el cliente con el objeto. Cuando se solicita el objeto, se debe proporcionar la misma clave para descifrar y devolver el objeto.

Ejemplo de SSE-C.

- Con fines de prueba o demostración, puede crear una clave de cifrado
  - Cree una clave de cifrado

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

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

- Coloque un objeto con la clave generada

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

- Dirigir el objeto

```
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=="
}
```

Si no proporciona la clave de cifrado, recibirá un error "se ha producido un error (404) al llamar a la operación HeadObject: Not found"

- Obtenga el objeto

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

Si no proporciona la clave de cifrado, recibirá un error que indica que se ha producido un error (InvalidRequest) al llamar a la operación GetObject: El objeto se ha almacenado utilizando un formulario de cifrado del lado del servidor. Se deben proporcionar los parámetros correctos para recuperar el objeto."

Cifrado del servidor de bloques (SSE-S3)

SSE-S3 permite al cliente definir un comportamiento de cifrado predeterminado para todos los objetos almacenados en un bloque. Los objetos se cifran con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, éste se descifra mediante una clave almacenada en StorageGRID.

Ejemplo de bloque SSE-S3

- Crear un bloque nuevo y establecer una política de cifrado predeterminada
  - Crear nuevo bloque

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

  - Put bucket Encryption

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

- Coloque un objeto en el bloque

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

- Dirigir el objeto

```
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": {}
}
```

- OBTENGA el objeto

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

Pruebe y muestre el bloqueo de objetos de S3 en StorageGRID

Por Aron Klein

El bloqueo de objetos proporciona un modelo WORM para evitar que los objetos se eliminen o se sobrescriban. La implementación de StorageGRID de un bloqueo de objetos es un activo de valor empresarial que se evalúa para ayudar a cumplir los requisitos normativos, respalda la conservación legal y el modo de cumplimiento de normativas para la retención de objetos y las políticas de retención de bloques predeterminadas.

En esta guía se demostrará la API de bloqueo de objetos S3.

Conservación legal

- La retención legal de bloqueo de objetos es un estado de activación/desactivación simple aplicado a un objeto.

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

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

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

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

- Desactivar la conservación legal

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

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

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

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

Modo de cumplimiento de normativas

- La retención de objetos se realiza con una Marca de tiempo de retención hasta.

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

- Compruebe el estado de retención

```
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"
    }
}
```

Retención predeterminada

- Establezca el período de retención en días y años en lugar de una fecha de retención hasta definida con la api por objeto.

```
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
```

- Compruebe el estado de retención

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

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

- Coloque un objeto en el bloque

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

- La duración de retención establecida en el bloque se convierte en una Marca de tiempo de retención en el objeto.

```
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"
    }
}
```

Pruebe a eliminar un objeto con una retención definida

El bloqueo de objetos se crea sobre el control de versiones. La retención se define en una versión del objeto. Si se intenta eliminar un objeto con una retención definida y no se especifica ninguna versión, se crea un marcador de borrado como la versión actual del objeto.

- Elimine el objeto con la retención definida

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

- Enumere los objetos del bloque

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

  - Observe que el objeto no aparece en la lista.
- Enumere las versiones para ver el marcador de borrado y la versión original bloqueada

```
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"
        }
    ]
}
```

- Elimine la versión bloqueada del objeto

```
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
```

Políticas y permisos en StorageGRID

Aquí hay ejemplos de políticas y permisos en StorageGRID S3.

La estructura de una política

En StorageGRID, las políticas de grupo son las mismas que las políticas de servicio S3 del usuario de AWS (IAM).

Las políticas de grupo son necesarias en StorageGRID. Un usuario con claves de acceso S3 pero no asignadas a un grupo de usuarios, o asignado a un grupo sin una política que otorgue algunos permisos, no podrá acceder a ningún dato.

Las políticas de bloque y de grupo comparten la mayoría de los mismos elementos. Las políticas se crean en formato json y se pueden generar mediante "Generador de políticas de AWS"

Todas las políticas definirán el efecto, las acciones y los recursos. Las políticas de bloque también definirán un principal.

El **efecto** será permitir o denegar la solicitud.

El **Principal**

- Solo se aplica a políticas de bloques.
- El principal es la(s) cuenta(s)/usuario(s) que se está otorgando o denegando los permisos.
- Se puede definir como:
  - Un comodín «*»

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

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

  - Un ID de inquilino para todos los usuarios de un inquilino (equivalente a la cuenta de AWS).

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

  - Un usuario (local o federado desde dentro del inquilino que reside el bloque (o bien, otro inquilino en el grid)

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

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

- Un grupo (local o federado desde dentro del inquilino que reside el bloque (o bien, otro inquilino en la cuadrícula).

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

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

La **Acción** es el conjunto de S3 operaciones que se otorgan o se deniegan al usuario(s).

> Para las políticas de grupo, la acción S3:ListBucket Permitido es necesaria para que los usuarios realicen cualquier acción S3.

El **Recurso** es el cubo o cubetas en los que los principales se otorgan o se les niega la capacidad de realizar las acciones. Opcionalmente puede haber una **condición** para cuando la acción de política es válida.

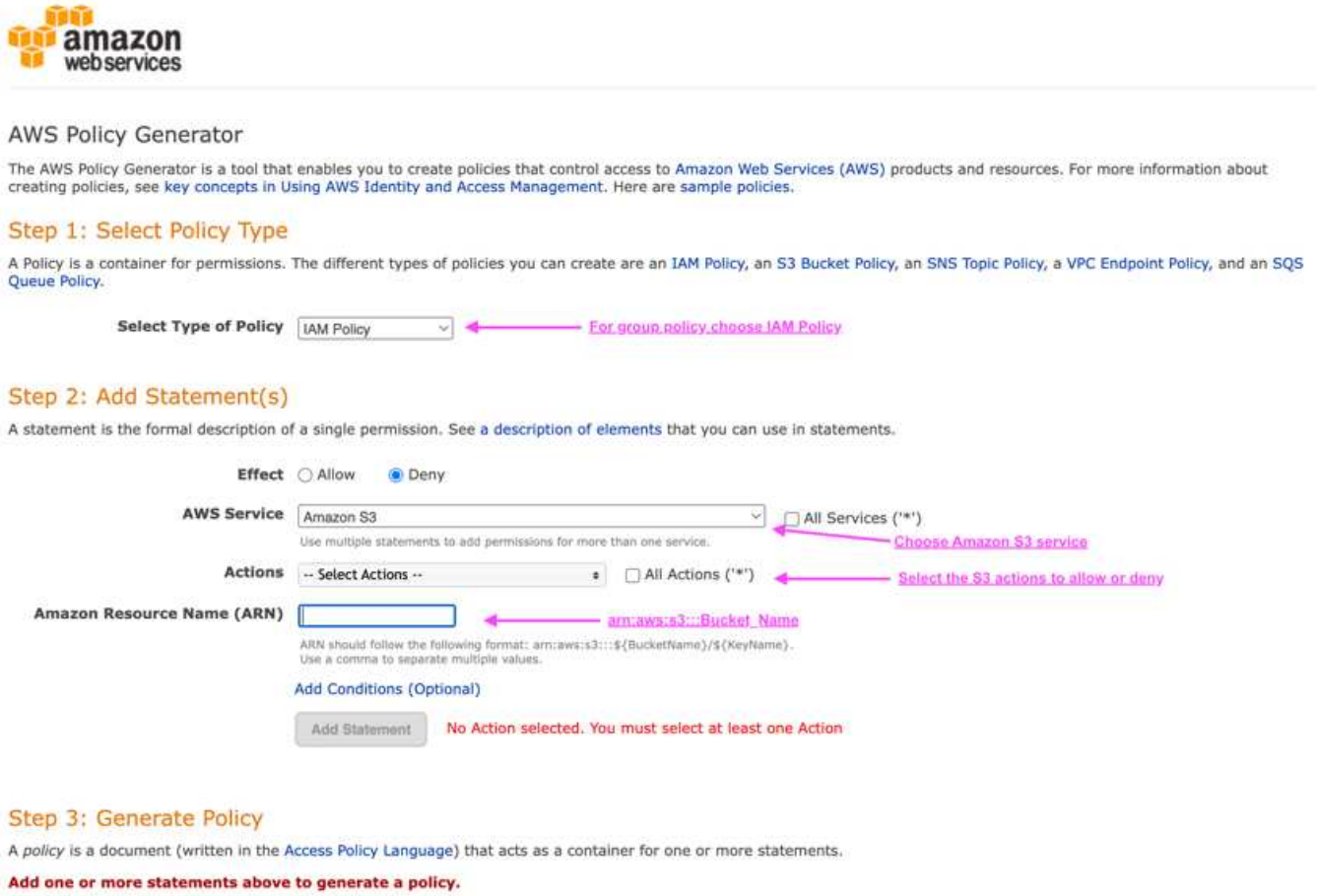
El formato de la política JSON se verá así:

```
{
  "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/*"
      ],
    }
  ]
}
```

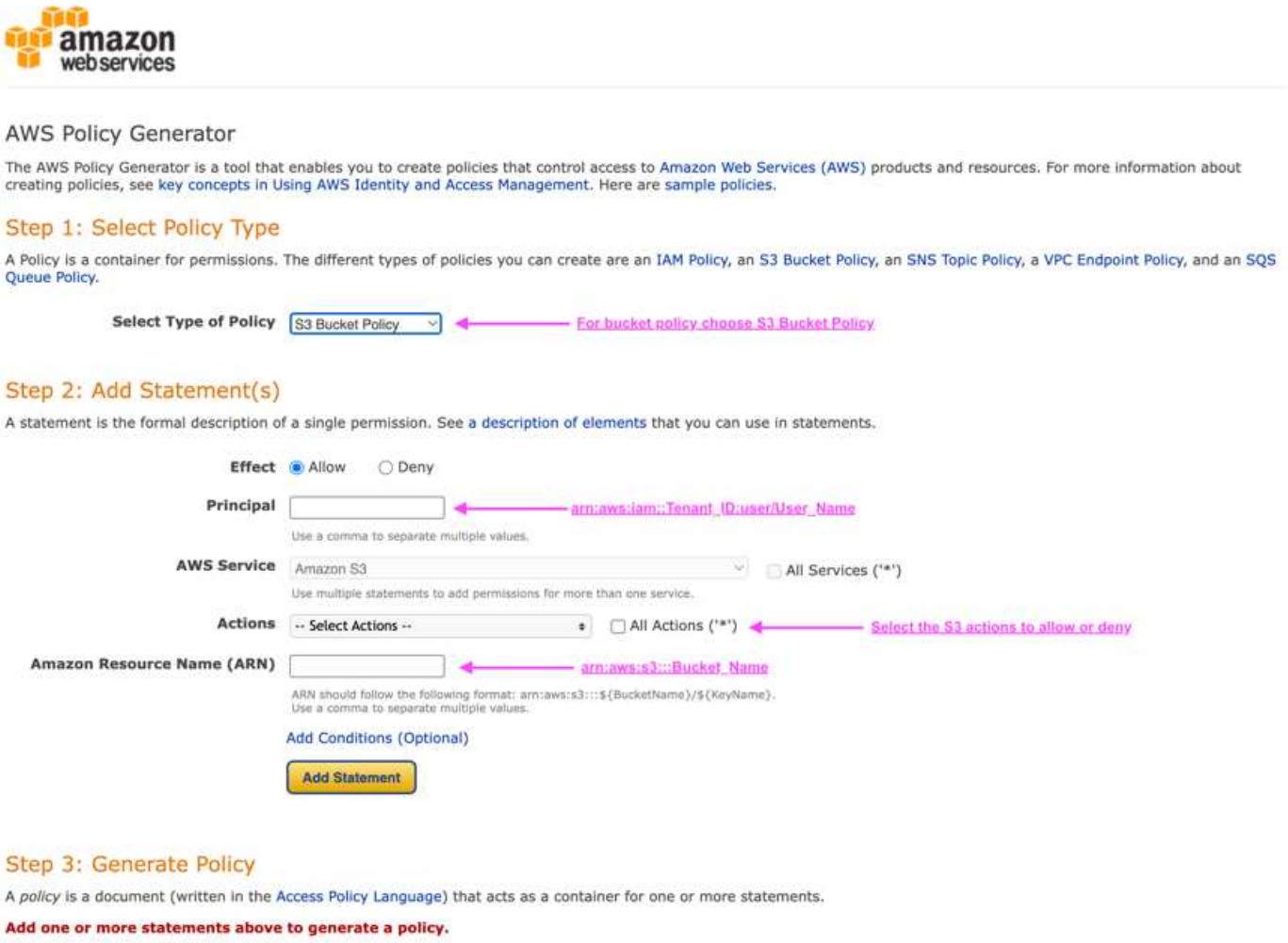
Uso del generador de políticas de AWS

El generador de políticas de AWS es una gran herramienta para ayudar a obtener el código json con el formato correcto y la información que está tratando de implementar.

Para generar los permisos para una directiva de grupo de StorageGRID: * Seleccione la política de IAM para el tipo de política. * Seleccione el botón para el efecto deseado - Permitir o Denegar. Es recomendable iniciar las directivas con los permisos de denegación y, a continuación, agregar los permisos de permiso * en el menú desplegable de acciones. Haga clic en el cuadro junto a tantas acciones de S3 que desee incluir en este permiso o en el cuadro Todas las acciones. * Escriba las rutas de acceso del depósito en el cuadro Nombre del recurso de Amazon (arn). Incluya “arn:aws:S3::” antes del nombre del depósito. «arn:aws:s3:::example_bucket»

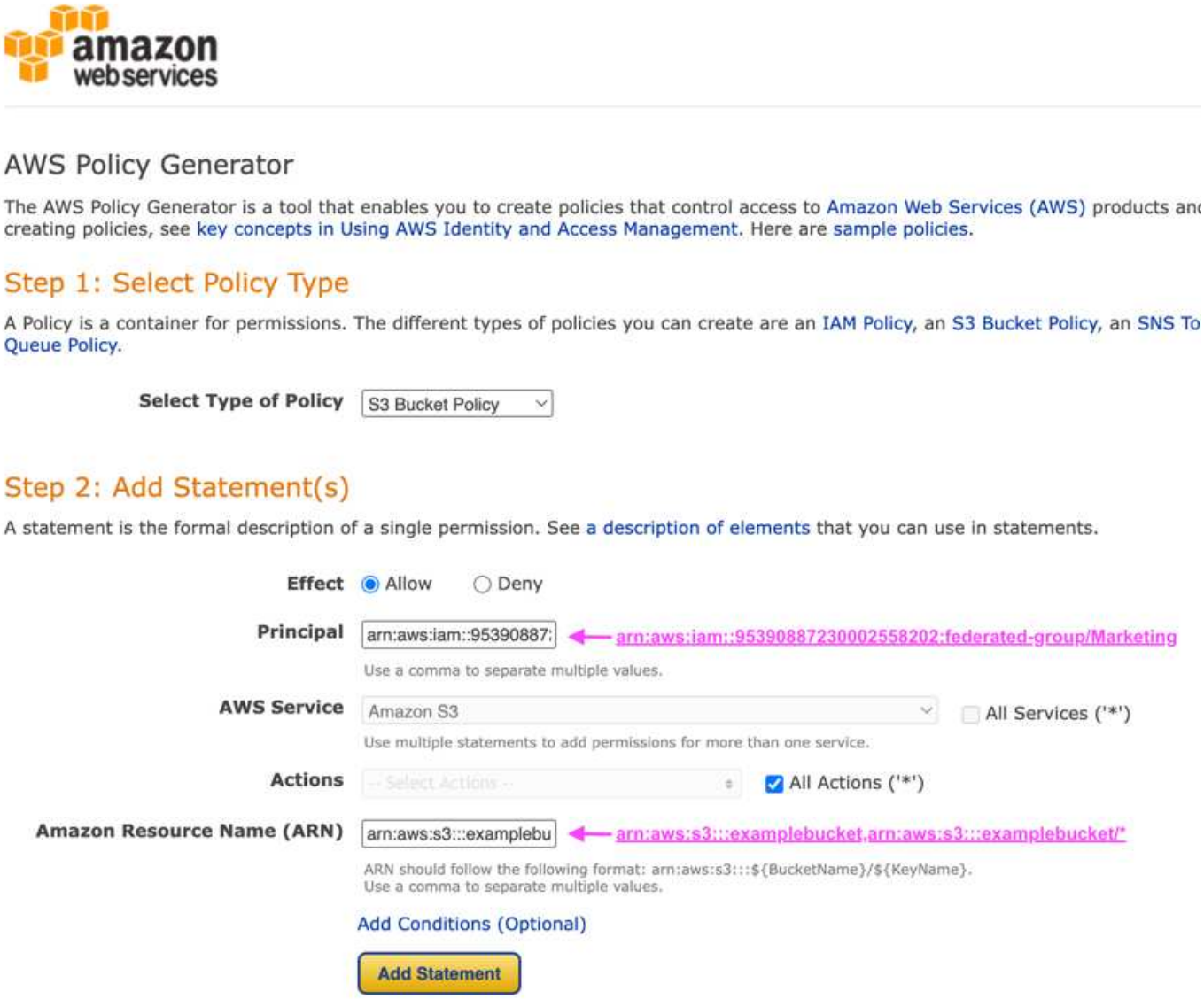


Para generar los permisos para una política de depósito: * Elija la política de bloques de S3 para el tipo de política. * Seleccione el botón para el efecto deseado - Permitir o Denegar. Es una buena práctica iniciar las políticas con los permisos de denegación y, a continuación, agregar los permisos de permiso * Tipo en la información de usuario o grupo para el Principal. * En el menú desplegable de acciones haz clic en el cuadro junto a tantas de las S3 acciones que quieras incluir en este permiso o en el cuadro “Todas las acciones”. * Escriba las rutas de acceso del depósito en el cuadro Nombre del recurso de Amazon (arn). Incluya “arn:aws:S3::” antes del nombre del depósito. «arn:aws:s3:::example_bucket»



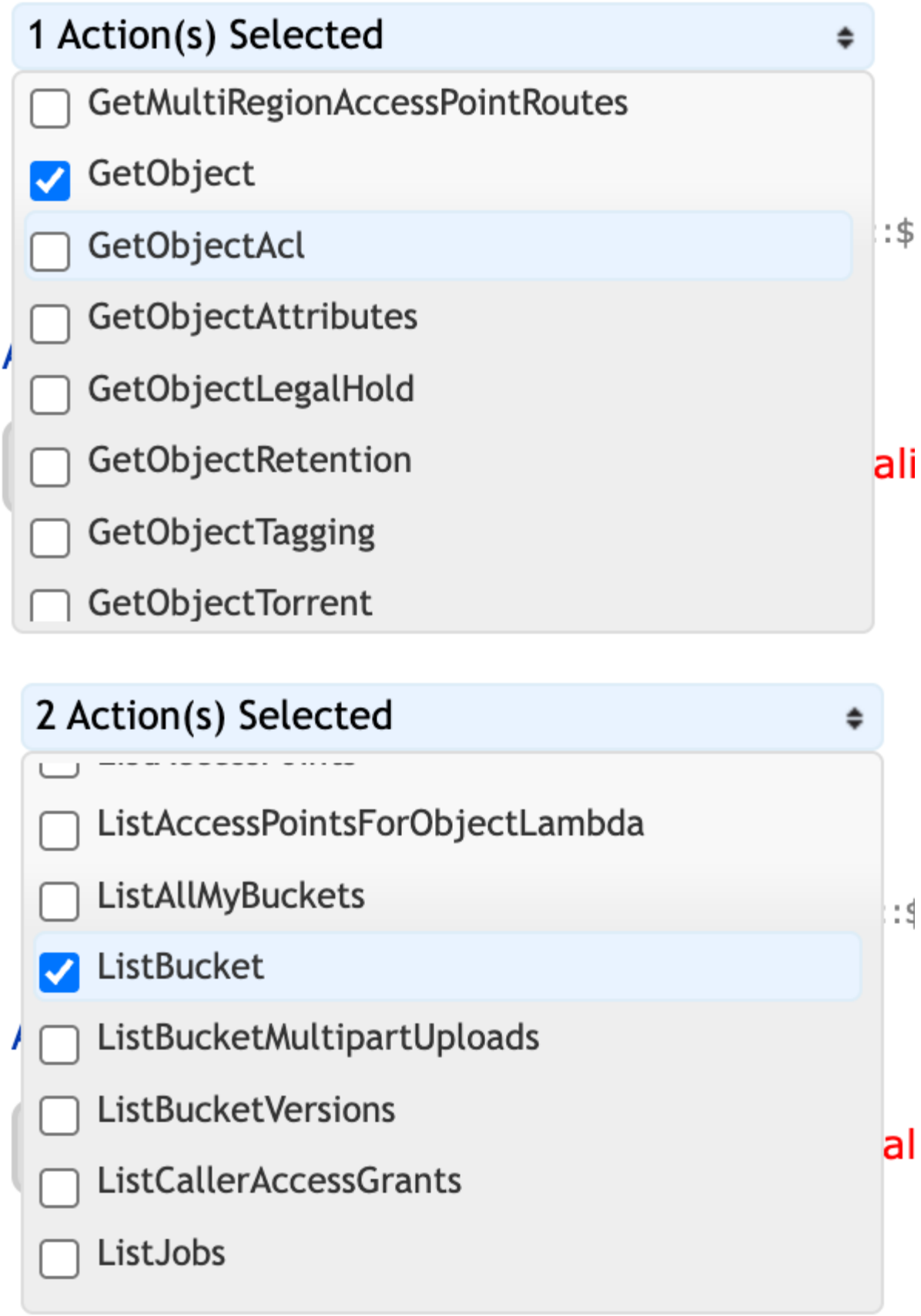
Por ejemplo, si desea generar una política de depósito para permitir que todos los usuarios realicen operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo Marketing en la cuenta especificada tienen acceso completo.

- Seleccione S3 Bucket Policy como tipo de política.
- Elija el efecto Permitir
- Introduzca la información del grupo de Marketing: arn:aws:iam::95390887230002558202:federated-group/Marketing
- Haga clic en la casilla de «Todas las acciones»
- Introduzca la información del bloque: arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*

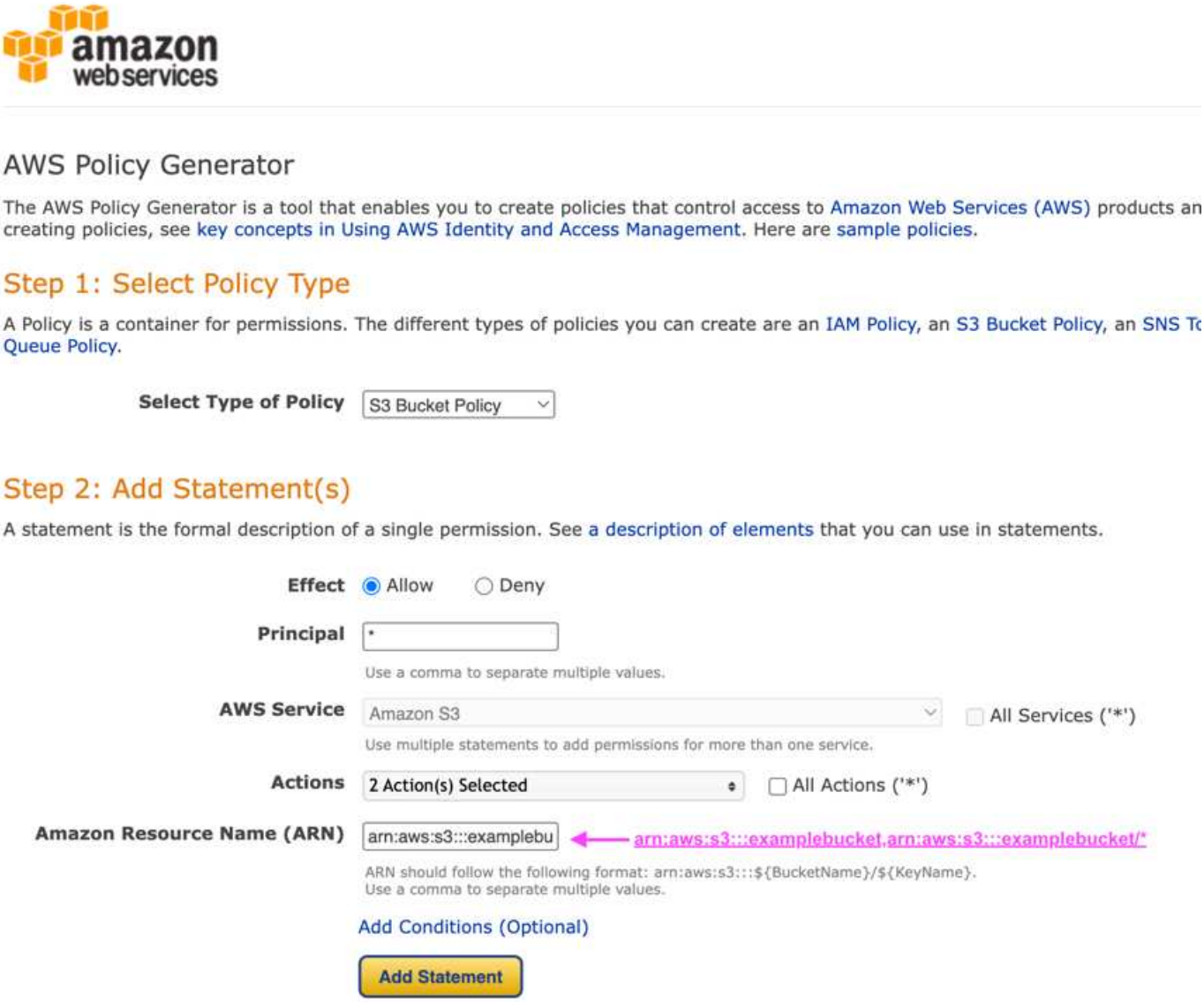


- Haga clic en el botón «Agregar declaración»

- Elija el efecto Permitir
- Introduzca el asterisco * para todos
- Haga clic en el cuadro junto a las acciones GetObject y ListBucket.

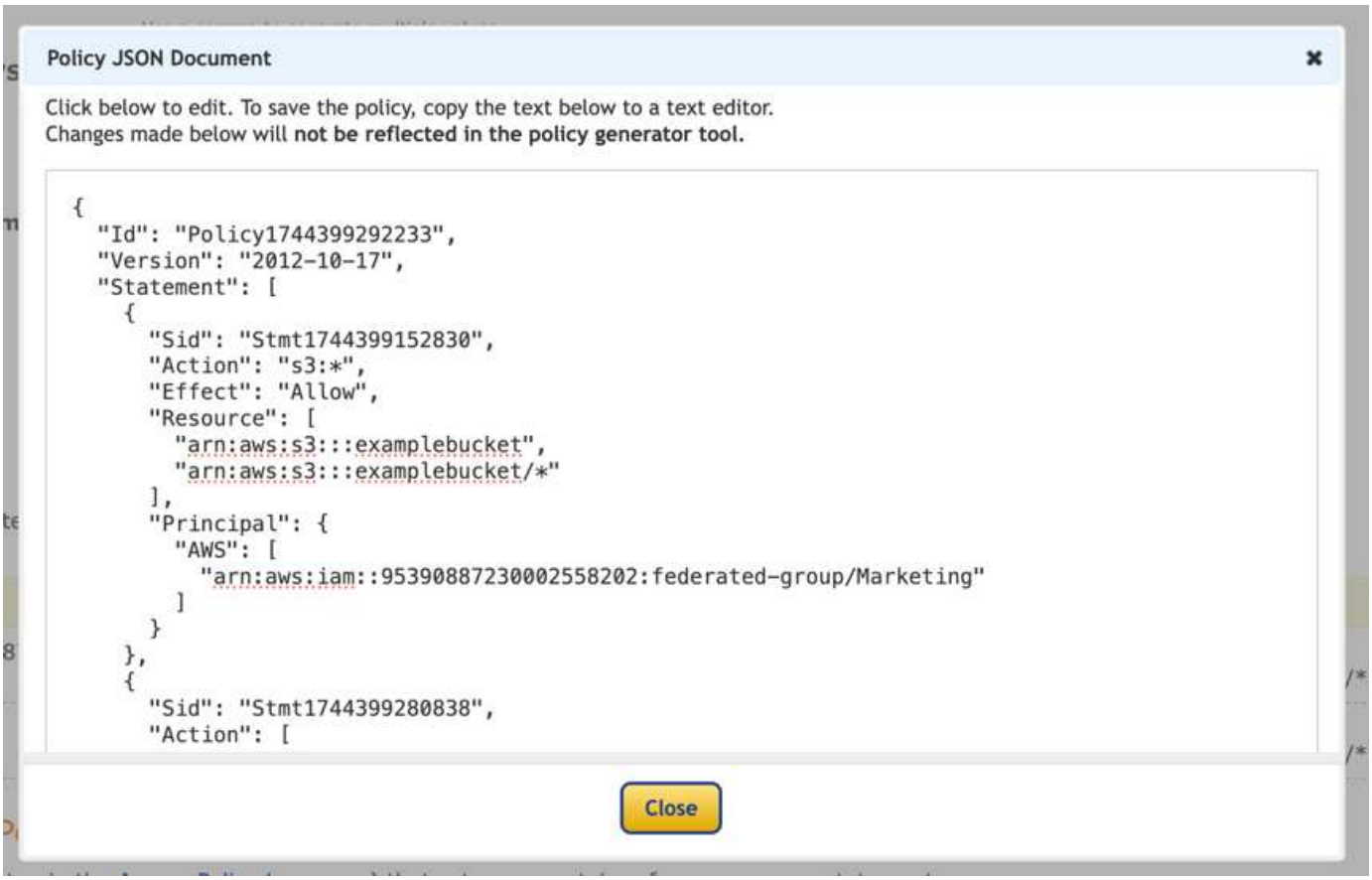


- Introduzca la información del bloque: arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*



- Haga clic en el botón «Agregar declaración»

- Haga clic en el botón “Generar Política” y aparecerá una ventana emergente con su política generada.



- Copie el texto json completo que debería tener el siguiente aspecto:

```
{
  "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": "*"
    }
  ]
}
```

Este json se puede utilizar tal cual, o puede eliminar las líneas de ID y versión encima de la línea de “Declaración” y puede personalizar el Sid para cada permiso con un título más significativo para cada permiso o también se pueden eliminar.

Por ejemplo:

```
{
  "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": "*"
    }
  ]
}
```

Políticas de grupo (IAM)

Acceso a bloque de estilo de directorio de casa

Esta política de grupo sólo permitirá a los usuarios acceder a los objetos del depósito denominado nombre de usuario de los usuarios.

```
{
"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}/*"
    }

  ]
}
```

Denegar creación de bloque de bloqueo de objetos

Esta política de grupo restringirá a los usuarios a crear un bloque con el bloqueo de objeto habilitado en el bloque.

> Esta política no se aplica en la interfaz de usuario de StorageGRID, sino que solo se aplica mediante la API de S3.

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

Límite de retención de bloqueo de objetos

Esta política de depósito restringirá la duración de la retención de bloqueo de objetos a 10 días o menos

```
{
 "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"
      }
    }
   }
  ]
}
```

Restringir a los usuarios la supresión de objetos por versionID

Esta política de grupo restringirá a los usuarios la supresión de objetos versionados por versionID

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

Restrinja un grupo a un único subdirectorio (prefijo) con acceso de solo lectura

Esta política permite a los miembros del grupo tener acceso de solo lectura a un subdirectorio (prefijo) dentro de un bloque. El nombre del depósito es «study» y el subdirectorio es «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/*"
            ]
        }
    ]
}
```

Políticas de bloques

Restringir bloque a un solo usuario con acceso de sólo lectura

Esta directiva permite a un solo usuario tener acceso de sólo lectura a un bloque y denys explícitamente acceso a todos los demás usuarios. La agrupación de las declaraciones denegadas en la parte superior de la directiva es una buena práctica para una evaluación más rápida.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::349215141330028336 65: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::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

restringe un bloque a algunos usuarios con acceso de solo lectura.

```
{
    "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/*"
        ]
      }
    ]
}
```

Restringir las eliminaciones de objetos versionados por el usuario en un depósito

Esta política de depósito restringirá a un usuario (identificado por el ID de usuario «56622399308951294926») de eliminar objetos versionados por versionID

```
{
  "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"
        ]
      }
    }
  ]
}
```

Ciclo de vida de un bucket en StorageGRID

Puede crear una configuración del ciclo de vida de S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID.

¿Qué es una configuración de ciclo de vida?

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en bloques de S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo caducarán dichos objetos (en una fecha específica o después de un número determinado de días).

Cada objeto sigue la configuración de retención de un ciclo de vida de bloques de S3 o una política de ILM. Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida del bloque. Los objetos que no coinciden con el filtro de ciclo de vida del bloque utilizan la configuración de retención de la política de ILM. Si

un objeto coincide con un filtro de ciclo de vida del bloque y no se especifica ninguna acción de caducidad explícitamente, no se utiliza la configuración de retención de la política de ILM y se implica que las versiones de los objetos se retienen permanentemente.

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de colocación de una regla de ILM aún se apliquen al objeto. O bien, un objeto podría conservarse en la cuadrícula incluso después de que hayan transcurrido las instrucciones de ubicación de ILM para el objeto.

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: Elimine un objeto cuando se alcance una fecha especificada o cuando se alcance un número especificado de días, empezando desde el momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: Elimine un objeto cuando se alcance un número especificado de días, empezando desde el momento en que el objeto se volvió no actual.
- Filtro (prefijo, etiqueta)
- Estado *ID

StorageGRID admite el uso de las siguientes operaciones de bloques para gestionar las configuraciones del ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Estructura de una política de ciclo de vida

Como primer paso en la creación de una configuración de ciclo de vida, se crea un archivo JSON que incluye una o varias reglas. Por ejemplo, este archivo JSON incluye tres reglas, de la siguiente manera:

1. La regla 1 solo se aplica a los objetos que coinciden con el prefijo category1/ y cuyo valor de clave2 es tag2. El parámetro Expiration especifica que los objetos que coinciden con el filtro caducarán a la medianoche del 22 de agosto de 2020.
2. La regla 2 solo se aplica a los objetos que coinciden con el prefijo category2/. El parámetro Expiración especifica que los objetos que coinciden con el filtro expirarán 100 días después de su ingesta.

   > Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual supera la fecha de ingesta más el número de días, es posible que algunos objetos se eliminen del bloque en cuanto se aplique la configuración del ciclo de vida.

3. La regla 3 solo se aplica a los objetos que coinciden con el prefijo category3/. El parámetro Expiración especifica que cualquier versión no vigente de los objetos coincidentes caducará 50 días después de que dejen de estar vigentes.

```
{
    "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"
        }
    ]
}
```

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración de ciclo de vida, se aplica a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

Esta solicitud aplica la configuración del ciclo de vida en el archivo de ejemplo a los objetos de un depósito denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración del ciclo de vida se ha aplicado correctamente al bloque, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Ejemplo de políticas de ciclo de vida para depósitos estándar (sin versiones)

Eliminar objetos después de 90 días

Caso de uso: Esta política es ideal para gestionar datos relevantes por tiempo limitado, como archivos temporales, registros o datos de procesamiento intermedio. Beneficio: Reduce los costos de almacenamiento y garantiza que el bucket esté ordenado.

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

Ejemplo de políticas de ciclo de vida para depósitos versionados

Eliminar versiones no actuales después de 10 días

Caso de uso: Esta política ayuda a gestionar el almacenamiento de objetos con versiones no actuales, que pueden acumularse con el tiempo y consumir un espacio considerable. Beneficio: Optimiza el uso del

almacenamiento conservando solo la versión más reciente.

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

Mantener 5 versiones no actuales

Caso de uso: útil cuando desea conservar una cantidad limitada de versiones anteriores para fines de recuperación o auditoría. Beneficio: conserve suficientes versiones no actuales para garantizar un historial y puntos de recuperación suficientes.

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

Eliminar marcadores de eliminación cuando no existan otras versiones

Caso de uso: Esta política ayuda a gestionar los marcadores de eliminación que quedan después de eliminar todas las versiones no actuales, los cuales pueden acumularse con el tiempo. Beneficio: Reduce el desorden innecesario.

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

Eliminar versiones actuales después de 30 días, eliminar versiones no actuales después de 60 días y eliminar los marcadores de eliminación creados por la eliminación de la versión actual una vez que no existan otras versiones.

Caso de uso: Proporcionar un ciclo de vida completo para las versiones actuales y no actuales, incluyendo los marcadores de eliminación. Beneficio: Reducir los costos de almacenamiento y garantizar que el depósito esté ordenado, conservando suficientes puntos de recuperación e historial.

```
{
  "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
      }
    }
  ]
}
```

eliminar marcadores de eliminación que no tengan otras versiones, conservar 4 versiones no actuales y al menos 30 días de historial para objetos con el "prefijo account_" y mantener 2 versiones y al menos 10 días de historial para todas las demás versiones de objetos.

Caso de uso: Proporcionar reglas únicas para objetos específicos, junto con otros objetos, para gestionar el ciclo de vida completo de las versiones actuales y futuras, incluyendo los marcadores de eliminación.
Beneficio: Reducir los costos de almacenamiento y garantizar que el depósito esté ordenado, conservando suficientes puntos de recuperación e historial para satisfacer diversas necesidades del cliente.

```
{
  "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
      }
    }
  ]
}
```

Conclusión

- Revise y actualice periódicamente las políticas del ciclo de vida y alinéelas con los objetivos de ILM y gestión de datos.
- Pruebe las políticas en un entorno o contenedor que no sea de producción antes de aplicarlas ampliamente para garantizar que funcionen según lo previsto
- Utilice identificaciones descriptivas para las reglas para que sea más intuitivo, ya que la estructura lógica puede volverse compleja.
- Supervise el impacto de estas políticas de ciclo de vida del depósito en el uso y el rendimiento del almacenamiento para realizar los ajustes necesarios.

Informes técnicos

Introducción a los informes técnicos de StorageGRID

StorageGRID de NetApp es una suite de almacenamiento de objetos definido por software que admite diferentes casos de uso en entornos de multinube pública, privada e híbrida. StorageGRID ofrece compatibilidad nativa con la API de Amazon S3 y proporciona innovaciones líderes en el sector, como la gestión automatizada del ciclo de vida, para almacenar, proteger y conservar datos no estructurados de forma rentable durante largos periodos.

StorageGRID ofrece documentación para cubrir las prácticas recomendadas y las recomendaciones para varias funciones e integraciones de StorageGRID.

NetApp StorageGRID y análisis de Big Data

Casos de uso de NetApp StorageGRID

La solución de almacenamiento de objetos NetApp StorageGRID ofrece escalabilidad, disponibilidad de datos, seguridad y alto rendimiento. Organizaciones de todos los tamaños y sectores utilizan StorageGRID S3 para una amplia gama de casos de uso. Vamos a explorar algunos escenarios típicos:

- Análisis de grandes volúmenes de datos: * StorageGRID S3 se utiliza con frecuencia como un lago de datos, donde las empresas almacenan grandes cantidades de datos estructurados y no estructurados para el análisis utilizando herramientas como Apache Spark, Splunk Smartstore y Dremio.
- Organización en niveles de datos* Los clientes de NetApp utilizan la función FabricPool de ONTAP para mover datos automáticamente entre un nivel local de alto rendimiento a StorageGRID. La organización en niveles reserva el costoso almacenamiento flash para los datos calientes y mantiene los datos fríos disponibles en el almacenamiento de objetos de bajo coste. Esto maximiza el rendimiento y el ahorro.

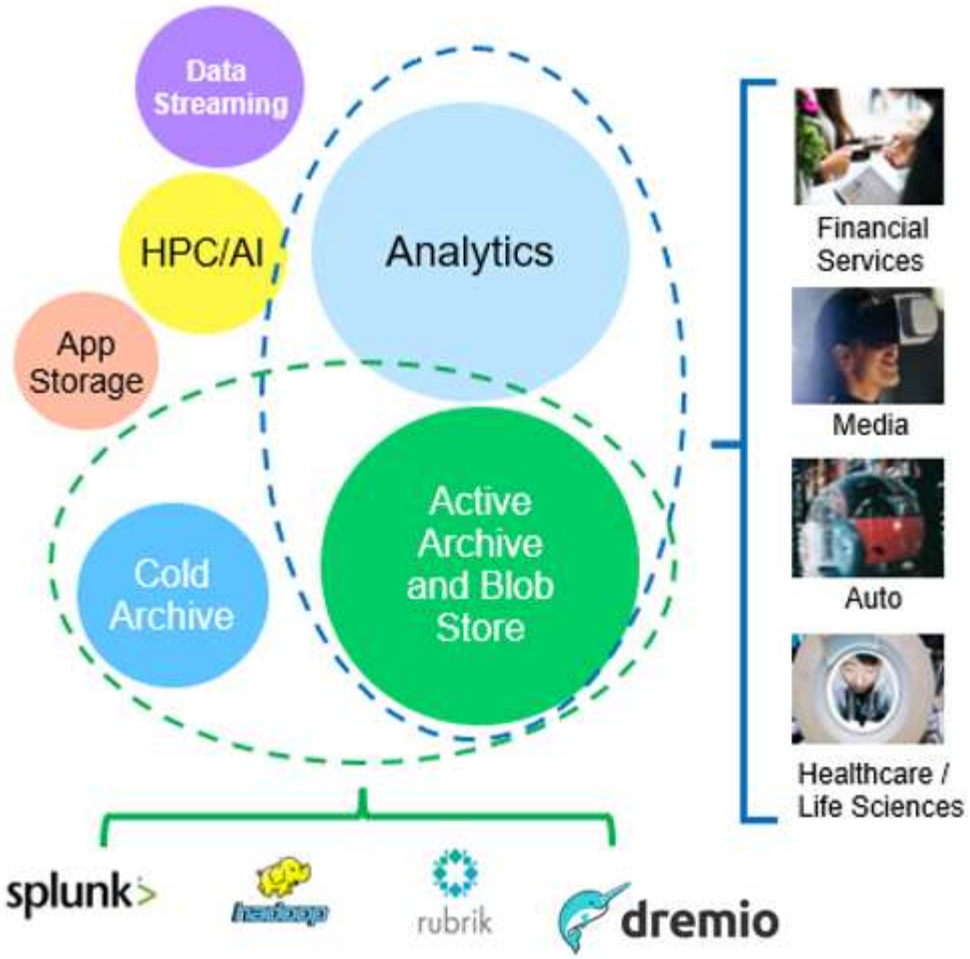
Respaldo de datos y recuperación de desastres: Las empresas pueden utilizar StorageGRID S3 como una solución confiable y rentable para hacer copias de seguridad de datos críticos y recuperarlos en caso de desastre.

Almacenamiento de datos para aplicaciones: StorageGRID S3 se puede utilizar como backend de almacenamiento para aplicaciones, lo que permite a los desarrolladores almacenar y recuperar fácilmente archivos, imágenes, videos y otros tipos de datos.

Entrega de contenido: StorageGRID S3 se puede utilizar para almacenar y entregar contenido estático del sitio web, archivos multimedia y descargas de software a usuarios de todo el mundo, aprovechando la distribución geográfica y el espacio de nombres global de StorageGRID para una entrega de contenido rápida y confiable.

- Archivo de datos:* StorageGRID ofrece diferentes tipos de almacenamiento y admite la clasificación por niveles en opciones de almacenamiento público de bajo costo a largo plazo, lo que lo convierte en una solución ideal para el archivado y la retención a largo plazo de datos que deben conservarse para fines de cumplimiento o históricos.

Casos de uso de almacenamiento de objetos

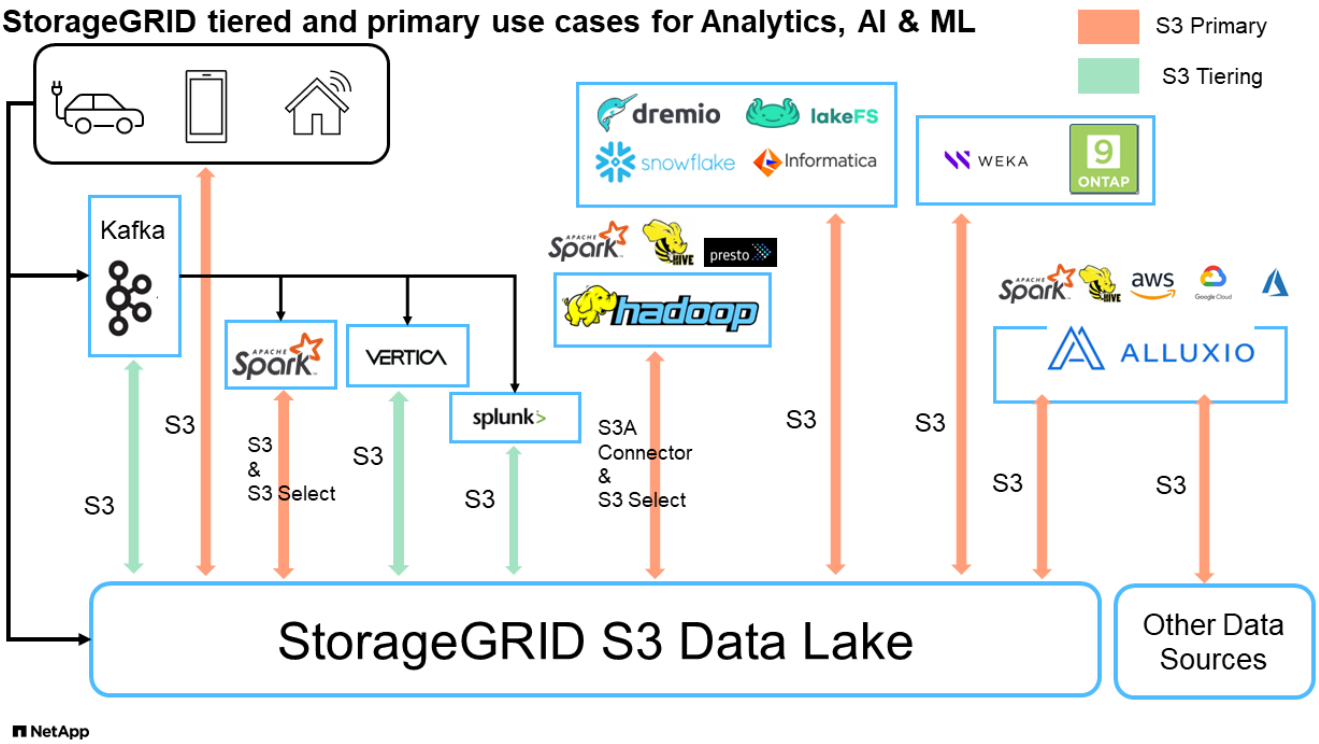


Entre los anteriores, el análisis de Big Data es uno de los casos de uso más importantes y su uso es tendencia al alza.

¿Por qué elegir StorageGRID para lagos de datos?

- Mayor colaboración: Multi-tenancy compartido masivo con acceso a API estándar del sector
- Costes operativos reducidos: Sencillez operativa de una única arquitectura de escalado horizontal automatizada y de reparación automática
- Escalabilidad: A diferencia de las soluciones tradicionales Hadoop y almacenes de datos, el almacenamiento de objetos S3 de StorageGRID separa el almacenamiento de la computación y los datos, lo que permite a la empresa escalar sus necesidades de almacenamiento a medida que crecían.
- Durabilidad y fiabilidad: StorageGRID proporciona una durabilidad del 99,999999999 %, lo que significa que los datos almacenados son muy resistentes a la pérdida de datos. También ofrece una alta disponibilidad, lo que garantiza la accesibilidad de los datos en todo momento.
- Seguridad: StorageGRID ofrece distintas funciones de seguridad, como el cifrado, la política de control de acceso, la gestión del ciclo de vida de los datos, el bloqueo de objetos y el control de versiones para proteger los datos almacenados en bloques de S3

StorageGRID S3 lagos de datos



Comparación de almacenes de datos y casas de campo con almacenamiento de objetos S3: Un estudio comparativo

Este artículo presenta una referencia exhaustiva de varios ecosistemas de almacenes de datos y almacenes de lagos utilizando NetApp StorageGRID. El objetivo es determinar qué sistema funciona mejor con el almacenamiento de objetos S3. Refiérase a esto "Apache Iceberg: La guía definitiva" para aprender más acerca de las arquitecturas de datawarehous/lakehouse y el formato de tabla (Parquet e Iceberg).

- Herramienta de referencia - TPC-DS - https://www.tpc.org/tpcds/
- Ecosistemas de Big Data
  - Clúster de equipos virtuales, cada uno con 128G GB de RAM y 24 vCPU, almacenamiento SSD para disco del sistema
  - Hadoop 3.3.5 con Hive 3.1.3 (1 nodo de nombres + 4 nodos de datos)
  - Delta Lake con Spark 3.2.0 (1 maestro + 4 trabajadores) y Hadoop 3.3.5
  - Dremio v25,2 (1 coordinador + 5 ejecutores)
  - Trino v438 (1 coordinador + 5 trabajadores)
  - Starburst v453 (1 coordinador + 5 trabajadores)
- Almacenamiento de objetos
  - NetApp® StorageGRID® 11,8 con equilibrador de carga 3 x SG6060 + 1x SG1000
  - Protección de objetos: 2 copias (el resultado es similar con EC 2+1)
- Tamaño de base de datos 1000GB
- La caché se ha desactivado en todos los ecosistemas para cada prueba de consulta utilizando el formato Parquet. Para el formato iceberg, comparamos el número de S3 solicitudes GET y el tiempo total de consulta entre los escenarios con caché desactivada y con caché habilitada.

TPC-DS incluye 99 consultas SQL complejas diseñadas para la evaluación comparativa. Medimos el tiempo total necesario para ejecutar las 99 consultas y realizamos un análisis detallado examinando el tipo y el número de solicitudes S3. Nuestras pruebas compararon la eficiencia de dos formatos de mesa populares: Parquet e iceberg.

Resultado de consulta TPC-DS con formato de tabla de parquet

Ecosistema	Subárbol	Lago Delta	Dremio	Trino	Estallido
TPCDS 99 consultas total de minutos	1084 [1]	55	36	32	28
S3 Desglose de solicitudes	OBTENGA	1.117.184	2.074.610	3.939.690	1.504.212
1.495.039	observación: Todas las gamas GET	80% rango de obtención de 2KB a 2MB de 32MB objetos, 50 - 100 solicitudes/seg	El rango del 73% se obtiene por debajo de 100KB de 32MB objetos, de 1000 a 1400 solicitudes por segundo	90% 1M bytes de rango de obtención de 256MB objetos, 2500 - 3000 solicitudes/seg	Rango OBTENER tamaño: 50% por debajo de 100KB, 16% alrededor de 1MB, 27% 2MB-9MB, 3500 - 4000 solicitudes/seg
Rango OBTENER tamaño: 50% por debajo de 100KB, 16% alrededor de 1MB, 27% 2MB-9MB, 4000 - 5000 solicitud/seg	Mostrar objetos	312.053	24.158	120	509
512	CABEZAL (objeto inexistente)	156.027	12.103	96	0
0	CABEZAL (objeto existente)	982.126	922.732	0	0

Ecosistema	Subárbol	Lago Delta	Dremio	Trino	Estallido
0	Total de solicitudes	2.567.390	3.033.603	3.939,906	1.504.721

[1] Hive no ha podido completar la consulta número 72

Resultado de consulta TPC-DS con formato de tabla iceberg

Ecosistema	Dremio	Trino	Estallido
TPCDS 99 consultas + total de minutos (caché desactivada)	22	28	22
Consultas TPCDS 99 + total de minutos [2] (caché habilitada)	16	28	21,5
S3 Desglose de solicitudes	OBTENER (caché deshabilitada)	1.985.922	938.639
931.582	OBTENER (caché habilitada)	611.347	30.158
3.281	observación: Todas las gamas GET	Tamaño DE OBTENCIÓN DE rango: 67% 1MB, 15% 100KB, 10% 500KB, 3500 - 4500 solicitudes/seg	Rango OBTENER tamaño: 42% por debajo de 100KB, 17% alrededor de 1MB, 33% 2MB-9MB, 3500 - 4000 solicitudes/seg
Rango OBTENER tamaño: 43% por debajo de 100KB, 17% alrededor de 1MB, 33% 2MB-9MB, 4000 - 5000 solicitudes/seg	Mostrar objetos	1465	0
0	CABEZAL (objeto inexistente)	1464	0
0	CABEZAL (objeto existente)	3.702	509
509	Total de Solicitudes (Caché Desactivada)	1.992.553	939.148

[2] El rendimiento de Trino/Starburst se encuentra en un cuello de botella debido a los recursos informáticos; al agregar más RAM al clúster, se reduce el tiempo total de consulta.

Como se muestra en la primera tabla, Hive es significativamente más lento que otros ecosistemas modernos de data lakehouse. Observamos que Hive envió un gran número de solicitudes de objetos de lista S3, que suelen ser lentas en todas las plataformas de almacenamiento de objetos, especialmente cuando se trata de cubos que contienen muchos objetos. Esto aumenta significativamente la duración general de la consulta. Además, los ecosistemas modernos de los lagos pueden enviar un gran número de SOLICITUDES GET en paralelo, que van desde 2.000 a 5.000 solicitudes por segundo, en comparación con las 50 a 100 solicitudes

por segundo de Hive. El mimetismo del sistema de archivos estándar de Hive y Hadoop S3A contribuye a la lentitud de Hive al interactuar con el almacenamiento de objetos S3.

El uso de Hadoop (ya sea en HDFS o en el almacenamiento de objetos S3) con Hive o Spark requiere un amplio conocimiento de Hadoop y Hive/Spark, así como un entendimiento de cómo interactúan los ajustes de cada servicio. Juntos, tienen más de 1.000 configuraciones, muchas de las cuales están interrelacionadas y no se pueden cambiar de forma independiente. Encontrar la combinación óptima de ajustes y valores requiere una gran cantidad de tiempo y esfuerzo.

Comparando los resultados de Parquet e Iceberg, notamos que el formato de tabla es un factor de rendimiento importante. El formato de tabla Iceberg es más eficiente que el Parquet en cuanto al número de solicitudes S3, con un 35% a un 50% menos de solicitudes en comparación con el formato Parquet.

El rendimiento de Dremio, Trino o Starburst está impulsado principalmente por la potencia de cálculo del clúster. Aunque los tres utilizan el conector S3A para la conexión de almacenamiento de objetos S3, no requieren Hadoop, por lo que estos sistemas no utilizan la mayoría de la configuración fs.S3A de Hadoop. Esto simplifica el ajuste del rendimiento, por lo que elimina la necesidad de aprender y probar diferentes configuraciones de Hadoop S3A.

A partir de estos resultados de las pruebas de rendimiento, podemos concluir que el sistema de análisis de Big Data optimizado para cargas de trabajo basadas en S3 es un factor de rendimiento importante. Los centros de almacenamiento modernos optimizan la ejecución de las consultas, utilizan metadatos de manera eficiente y proporcionan un acceso fluido a los datos S3, lo que resulta en un mejor rendimiento en comparación con Hive cuando se trabaja con almacenamiento S3.

Consulte esto "página" para configurar el origen de datos Dremio S3 con StorageGRID.

Visite los enlaces siguientes para obtener más información sobre cómo StorageGRID y Dremio trabajan juntos para proporcionar una infraestructura de lago de datos moderna y eficiente y cómo NetApp migró de Hive + HDFS a Dremio + StorageGRID para mejorar drásticamente la eficiencia del análisis de Big Data.

- "Impulse el rendimiento de sus Big Data con NetApp StorageGRID"
- "Infraestructura de lago de datos moderna, potente y eficiente con StorageGRID y Dremio"
- "Cómo NetApp está redefiniendo la experiencia del cliente con el análisis de productos"

Ajuste Hadoop S3A

Por Angela Cheng

El conector S3A de Hadoop facilita la interacción fluida entre aplicaciones basadas en Hadoop y almacenamiento de objetos S3. El ajuste del conector Hadoop S3A es esencial para optimizar el rendimiento cuando se trabaja con el almacenamiento de objetos S3. Antes de entrar en el ajuste de detalles, entendamos lo básico de Hadoop y sus componentes.

¿Qué es Hadoop?

- Hadoop * es un potente marco de código abierto diseñado para gestionar el procesamiento y almacenamiento de datos a gran escala. Permite el almacenamiento distribuido y el procesamiento paralelo entre clústeres de equipos.

Los tres componentes principales de Hadoop son:

- **Hadoop HDFS (Hadoop Distributed File System)**: Se encarga del almacenamiento, dividiendo los datos

en bloques y distribuyéndolos a través de los nodos.

- **Hadoop MapReduce**: Responsable del procesamiento de datos dividiendo las tareas en fragmentos más pequeños y ejecutándolas en paralelo.
- * Hadoop YARN (Otro Negociador de Recursos):* "Gestiona los recursos y programa las tareas de forma eficiente"

Hadoop HDFS y conector S3A

HDFS es un componente vital del ecosistema de Hadoop, y tiene un papel crucial en el procesamiento eficiente de Big Data. HDFS permite un almacenamiento y una gestión fiables. Garantiza el procesamiento paralelo y un almacenamiento de datos optimizado, lo que acelera el acceso y el análisis de los datos.

En el procesamiento de Big Data, HDFS ofrece almacenamiento con tolerancia a fallos para grandes conjuntos de datos. Y todo ello gracias a la replicación de datos. Puede almacenar y gestionar grandes volúmenes de datos estructurados y no estructurados en un entorno de almacén de datos. Además, se integra sin problemas con los principales marcos de procesamiento de Big Data, como Apache Spark, Hive, Pig y Flink, lo que permite un procesamiento de datos escalable y eficiente. Es compatible con sistemas operativos basados en Unix (Linux), por lo que es una opción ideal para las organizaciones que prefieren utilizar entornos basados en Linux para su procesamiento de Big Data.

A medida que ha ido creciendo el volumen de datos con el tiempo, el enfoque de añadir nuevas máquinas al clúster Hadoop con sus propios recursos informáticos y de almacenamiento se ha vuelto ineficiente. Escalar de forma lineal crea retos para usar los recursos de forma eficiente y gestionar la infraestructura.

Para abordar estos retos, el conector Hadoop S3A ofrece I/O de alto rendimiento frente al almacenamiento de objetos de S3. Implementar un flujo de trabajo de Hadoop con S3A le ayuda a aprovechar el almacenamiento de objetos como repositorio de datos y le permite separar los recursos informáticos y de almacenamiento, lo que, a su vez, le permite escalar la computación y el almacenamiento de forma independiente. La disociación de la computación y el almacenamiento también le permite dedicar la cantidad adecuada de recursos para sus tareas informáticas y proporcionar capacidad en función del tamaño del conjunto de datos. Por lo tanto, es posible reducir el TCO general para los flujos de trabajo de Hadoop.

Ajuste de conector Hadoop S3A

S3 se comporta de forma diferente a HDFS, y algunos intentos de preservar la apariencia de un sistema de archivos están excesivamente subóptimos. Es necesario realizar ajustes, pruebas y experimentos cuidadosos para hacer el uso más eficiente de los recursos de S3.

Las opciones de Hadoop incluidas en este documento se basan en Hadoop 3,3.5, consulte "Hadoop 3.3.5 core-site.xml" para todas las opciones disponibles.

Nota: El valor predeterminado de algunas configuraciones de Hadoop fs.S3A es diferente en cada versión de Hadoop. Asegúrese de consultar el valor predeterminado específico de su versión actual de Hadoop. Si no se especifica esta configuración en Hadoop core-site.xml, se utilizará el valor predeterminado. Puede anular el valor en tiempo de ejecución con las opciones de configuración de Spark o Hive.

Tienes que ir a esto "Página de Apache Hadoop" para entender cada opción fs.s3a. Si es posible, pruébalos en un clúster Hadoop que no sea de producción para encontrar los valores óptimos.

Deberías leer "Maximizar el rendimiento cuando se trabaja con el conector S3A" para otras recomendaciones de ajuste.

Veamos algunas consideraciones clave:

1. Compresión de datos

No active la compresión StorageGRID. La mayoría de los sistemas de Big Data utilizan un rango de bytes GET en lugar de recuperar todo el objeto. El uso de un rango de bytes GET con objetos comprimidos reduce considerablemente el rendimiento GET.

2. S3A comités

En general, Magic S3A committer se recomienda. Consulte este apartado "Página de opciones comunes de S3A committer" para obtener una mejor comprensión de magic committer y sus configuraciones s3a relacionadas.

Responsable de Magic:

El Magic committer confía específicamente en S3Guard para ofrecer listados de directorios consistentes en el almacén de objetos de S3.

Con S3 consistente (que ahora es el caso), el comensor Magic se puede usar de forma segura con cualquier cubo S3.

Opciones y experimentación:

En función de su caso de uso, puede elegir entre el comité de almacenamiento provisional (que se basa en un sistema de archivos HDFS del clúster) y el comité mágico.

Experimente con ambos para determinar cuál se adapta mejor a su carga de trabajo y sus requisitos.

En resumen, los Comités S3A ofrecen una solución al desafío fundamental de un compromiso de producción consistente, de alto rendimiento y fiable con S3. Su diseño interno garantiza una transferencia de datos eficiente al tiempo que mantiene la integridad de los datos.

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. Thread, tamaños de pool de conexiones y tamaño de bloque

- Cada cliente **S3A** que interactúa con un solo depósito tiene su propio conjunto dedicado de conexiones HTTP 1,1 abiertas e hilos para las operaciones de carga y copia.
- "Puede ajustar estos tamaños de pool para lograr un equilibrio entre el rendimiento y el uso de memoria/thread".
- Al cargar datos a S3, se divide en bloques. El tamaño de bloque predeterminado es de 32 MB. Puede personalizar este valor configurando la propiedad fs.S3A.block.size.
- Los bloques mayores pueden mejorar el rendimiento de las cargas de datos grandes al reducir la sobrecarga que supone gestionar piezas de varias partes durante la carga. El valor recomendado es de 256 MB o superior para un conjunto de datos grande.

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. Carga multiparte

Los responsables de S3A **SIEMPRE** usan MPU (carga multiparte) para cargar datos al cubo S3. Esto es necesario para permitir: Fallo de tarea, ejecución especulativa de tareas y abortos de trabajo antes de la confirmación. A continuación se indican algunas especificaciones clave relacionadas con las cargas de varias partes:

- Tamaño máximo de objeto: 5 TiB (terabytes).
- Número máximo de piezas por carga: 10.000.

- Números de referencia: Desde 1 hasta 10.000 (inclusive).
- Tamaño de la pieza: Entre 5 MiB y 5 GiB. Cabe destacar que no hay límite de tamaño mínimo para la última parte de la carga de varias partes.

El uso de un tamaño de pieza más pequeño para cargas de varias partes S3 tiene ventajas y desventajas.

Ventajas:

- Recuperación rápida de problemas de red: Al cargar piezas más pequeñas, se minimiza el impacto de reiniciar una carga fallida debido a un error de red. Si una pieza falla, solo necesita volver a cargar esa pieza específica en lugar de todo el objeto.
- Mejor Paralelización: Se pueden subir más partes en paralelo, aprovechando las conexiones multi-threading o concurrentes. Esta paralelización mejora el rendimiento, sobre todo cuando se trata de archivos grandes.

Desventaja:

- Sobrecarga de red: El tamaño de la pieza más pequeño significa más partes para cargar, cada parte requiere su propia solicitud HTTP. Más solicitudes HTTP aumentan la sobrecarga de iniciar y completar solicitudes individuales. La gestión de un gran número de piezas pequeñas puede afectar al rendimiento.
- Complejidad: Gestionar el pedido, realizar un seguimiento de las piezas y garantizar que las cargas sean satisfactorias puede resultar engorroso. Si es necesario anular la carga, se debe realizar un seguimiento y depurar todos los artículos que ya se han cargado.

Para Hadoop, se recomienda un tamaño de pieza de 256MB o superior para fs.S3A.multipart.size. Defina siempre el valor fs.S3A.mutlipart.threshold en 2 x fs.S3A.multipart.size. Por ejemplo, si fs.S3A.multipart.size = 256M, fs.S3A.mutlipart.threshold debe ser 512M.

Utilice un tamaño de pieza más grande para un conjunto de datos grande. Es importante elegir un tamaño de pieza que equilibre estos factores en función de su caso de uso específico y las condiciones de red.

Una carga de varias partes es un "proceso de tres pasos":

1. Se inicia la carga, StorageGRID devuelve un ID de carga.
2. Las partes del objeto se cargan mediante el identificador de carga.
3. Una vez que se han cargado todas las partes del objeto, envía una solicitud de carga completa de varias partes con upload-id. StorageGRID construye el objeto a partir de las piezas cargadas, y el cliente puede acceder al objeto.

Si la solicitud completa de carga de varias partes no se envía correctamente, las piezas permanecen en StorageGRID y no crearán ningún objeto. Esto ocurre cuando los trabajos se interrumpen, fallan o se anulan. Los artículos permanecen en la cuadrícula hasta que la carga de varias partes se completa o se anula o StorageGRID depura estos artículos si han transcurrido 15 días desde que se inició la carga. Si hay muchas (unos pocos cientos de miles o millones) cargas multiparte en curso en un depósito, cuando Hadoop envía «lista-multiparte-cargas» (esta solicitud no filtra por identificador de carga), la solicitud puede tardar mucho tiempo en completarse o eventualmente en agotarse. Puede considerar establecer fs.S3A.mutlipart.purge en true con un valor fs.S3A.multipart.purge.age apropiado (por ejemplo, 5 a 7 días, no utilice el valor predeterminado de 86400, es decir, 1 día). O póngase en contacto con el servicio de soporte de NetApp para investigar la situación.

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. Buffer escribe datos en la memoria

Para mejorar el rendimiento, puede almacenar en búfer los datos de escritura en la memoria antes de cargarlos en S3. Esto puede reducir el número de escrituras pequeñas y mejorar la eficiencia.

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

Recuerda que S3 y HDFS funcionan de distintas maneras. Es necesario realizar un ajuste/prueba/experimento

cuidadoso para hacer el uso más eficiente de los recursos de S3.

TR-4871: Configurar StorageGRID para backup y recuperación de datos con Commvault

Realice backups y recupere datos con StorageGRID y Commvault

CommVault y NetApp han colaborado para crear una solución de protección de datos conjunta que combina el software Commvault Complete Backup and Recovery para NetApp con el software NetApp StorageGRID para el almacenamiento en cloud. CommVault Complete Backup and Recovery y NetApp StorageGRID ofrecen soluciones exclusivas y fáciles de usar que funcionan conjuntamente para ayudarle a cumplir las demandas del rápido crecimiento de los datos y las crecientes normativas en todo el mundo.

Muchas organizaciones quieren migrar su almacenamiento al cloud, escalar sus sistemas y automatizar la política para la retención de datos a largo plazo. El almacenamiento de objetos basado en cloud es conocido por su resiliencia, capacidad de escalado y eficiencia operativa y de costes que lo convierten en una opción natural como destino para su backup. CommVault y NetApp certificaron conjuntamente su solución combinada en 2014 y desde entonces han diseñado una integración más profunda entre sus dos soluciones. Clientes de todo tipo en todo el mundo han adoptado la solución combinada de CommVault Complete Backup and Recovery y StorageGRID.

Acerca de Commvault y StorageGRID

El software Commvault Complete Backup and Recovery es una solución de gestión de datos e información integrada de nivel empresarial creada desde cero en una única plataforma y con una base de código unificado. Todas sus funciones comparten tecnologías back-end, lo que ofrece las ventajas y ventajas incomparables de un enfoque totalmente integrado para proteger, gestionar y acceder a los datos. El software contiene módulos que protegen, archivan, analizan, replican y buscan los datos. Los módulos comparten un conjunto común de servicios de back-end y capacidades avanzadas que interactúan entre sí a la perfección. La solución aborda todos los aspectos de la gestión de datos de su empresa, a la vez que proporciona una escalabilidad infinita y un control sin precedentes de los datos y la información.

NetApp StorageGRID, como nivel de cloud de Commvault, es una solución empresarial de almacenamiento de objetos en cloud híbrido. Puede ponerlo en funcionamiento en numerosos sitios, ya sea en un dispositivo creado para tal fin o como instalación definida por software. StorageGRID permite establecer normativas de gestión de datos que determinan cómo se almacenan y protegen los datos. StorageGRID recopila la información necesaria para desarrollar y aplicar políticas. Examina una amplia gama de características y necesidades, incluyendo rendimiento, durabilidad, disponibilidad, ubicación geográfica, longevidad y coste. Los datos se mantienen completamente y están protegidos a medida que se mueven entre ubicaciones y a medida que envejecen.

El motor de políticas inteligente de StorageGRID le ayuda a elegir una de las siguientes opciones:

- Para utilizar códigos de borrado para realizar backups de datos en varios sitios para garantizar la resiliencia.
- Para copiar objetos en sitios remotos para minimizar la latencia y el coste de WAN.

Cuando StorageGRID almacena un objeto, se accede a él como un objeto, independientemente del lugar donde esté o del número de copias que existan. Este comportamiento es crucial para la recuperación ante

desastres, ya que con él, incluso si una copia de backup de sus datos está dañada, StorageGRID puede restaurar sus datos.

Mantener los datos de backup en el almacenamiento primario puede resultar caro. Cuando usa NetApp StorageGRID, libera espacio en su almacenamiento principal migrando los datos de backup inactivos a StorageGRID y se beneficia de las numerosas funcionalidades de StorageGRID. El valor de los datos de backup cambia con el tiempo, al igual que el coste de almacenarlos. StorageGRID puede minimizar el coste de su almacenamiento primario a la vez que aumenta la durabilidad de sus datos.

Principales características

Algunas de las funciones clave de la plataforma de software Commvault son:

- Una solución de protección de datos completa compatible con los principales sistemas operativos, aplicaciones y bases de datos en servidores físicos y virtuales, sistemas NAS, infraestructuras basadas en cloud y dispositivos móviles.
- Gestión simplificada mediante una única consola: Usted puede ver, gestionar y acceder a todas las funciones y a todos los datos e información de la empresa.
- Múltiples métodos de protección, entre los que se incluyen el backup y el archivado de datos, la gestión de Snapshot, la replicación de datos y la indexación de contenido para exhibición de documentos electrónicos.
- Gestión del almacenamiento eficiente mediante la deduplicación para el almacenamiento en disco y en cloud.
- Integración con cabinas de almacenamiento de NetApp como las cabinas AFF, FAS, NetApp HCI y E-Series y sistemas de almacenamiento de escalado horizontal NetApp SolidFire® Integración también con el software NetApp Cloud Volumes ONTAP para automatizar la creación de copias Snapshot™ de NetApp indexadas y compatibles con aplicaciones en toda la cartera de almacenamiento de NetApp.
- Complete la gestión de infraestructura virtual que admite los principales hipervisores virtuales en las instalaciones y las principales plataformas de proveedores a hiperescala en el cloud público.
- Las funcionalidades de seguridad avanzadas para limitar el acceso a datos cruciales, ofrecer funcionalidades de gestión granular y proporcionar acceso de inicio de sesión único para los usuarios de Active Directory.
- Gestión de datos basada en políticas que le permite gestionar los datos en función de las necesidades empresariales, no de la ubicación física.
- Una experiencia de usuario final innovadora, que capacita a los usuarios para que protejan, encuentren y recuperen sus propios datos.
- Automatización impulsada por API, lo que le permite usar herramientas de terceros, como vRealize Automation o Service Now, para gestionar sus operaciones de protección y recuperación de datos.

Si desea información detallada sobre las cargas de trabajo compatibles, visite "Tecnologías compatibles de Commvault".

Opciones de backup

Al implementar el software Commvault Complete Backup and Recovery con almacenamiento en cloud, dispone de dos opciones de backup:

- Realice una copia de seguridad en un destino de disco primario y también realice una copia auxiliar en el almacenamiento en cloud.
- Realice un backup en el almacenamiento en cloud como destino principal.

Anteriormente, se consideraba que el almacenamiento de objetos o en el cloud tenía un rendimiento demasiado bajo para poder utilizarlo para el backup principal. El uso de un destino de disco principal permitió a los clientes acelerar los procesos de backup y restauración, así como mantener una copia auxiliar en el cloud como backup en frío. StorageGRID representa la nueva generación de almacenamiento de objetos. StorageGRID ofrece un alto rendimiento y un rendimiento masivo, así como un rendimiento y una flexibilidad más allá de lo que ofrecen otros proveedores de almacenamiento de objetos.

La siguiente tabla enumera las ventajas de cada opción de backup con StorageGRID:

	Copia de seguridad primaria en disco y copia auxiliar en StorageGRID	**Backup principal en StorageGRID**
Rendimiento	Tiempo de recuperación más rápido, con montaje activo o recuperación activa: Ideal para cargas de trabajo de Tier0/Tier1.	No se puede utilizar para operaciones de montaje activo ni de recuperación activa. Ideal para el funcionamiento de restauración de transmisión y la retención a largo plazo.
Arquitectura de puesta en marcha	Utiliza all-flash o un disco giratorio como primer nivel de aterrizaje de backup. StorageGRID se utiliza como nivel secundario.	Simplifica la puesta en marcha al usar StorageGRID como objetivo de backup todo incluido.
Funciones avanzadas (restauración en directo)	Compatible	No admitido

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Centro de documentación de StorageGRID 11,9 + https://docs.netapp.com/us-en/storagegrid-119/
- Documentación de producto de NetApp
  https://docs.netapp.com
- Documentación de CommVault
  https://documentation.commvault.com/2024/essential/index.html

Descripción general de la solución probada

La solución probada combina soluciones CommVault y NetApp para crear una potente solución conjunta.

Configuración de la solución

En la configuración de laboratorio, el entorno StorageGRID consistía en cuatro dispositivos NetApp StorageGRID SG5712, un nodo de administración principal virtual y un nodo de pasarela virtual. El dispositivo SG5712 es la opción de nivel básico, una configuración de referencia. Elegir opciones de dispositivos de mayor rendimiento como NetApp StorageGRID SG5760 o SG6060 puede proporcionar importantes ventajas de rendimiento. Consulte con su arquitecto de soluciones NetApp StorageGRID para obtener ayuda en el

dimensionamiento.

Para su política de protección de datos, StorageGRID utiliza una política integrada de gestión del ciclo de vida de la información para gestionar y proteger los datos. Las reglas de ILM se evalúan en una política de arriba a abajo. Implementamos la política de ILM que se muestra en la siguiente tabla:

Regla de ILM	Cualificadores	Comportamiento de ingesta
Código de borrado 2+1	Objetos superiores a 200KB	Equilibrado
2 Copia	Todos los objetos	Registro doble

La regla Copia de ILM 2 es la regla predeterminada. La regla de codificación de borrado 2+1 se aplicó para esta prueba a cualquier objeto 200KB o mayor. La regla predeterminada se ha aplicado a objetos menores de 200KB. La aplicación de las reglas de este modo es una mejor práctica de StorageGRID.

Para obtener detalles técnicos sobre este entorno de prueba, lea la sección Diseño de la solución y prácticas recomendadas en la "Protección de datos de escalado horizontal de NetApp con Commvault" informe técnico.

Especificaciones de hardware de StorageGRID

En la siguiente tabla se describe el hardware de NetApp StorageGRID utilizado en esta prueba. El dispositivo StorageGRID SG5712 con conexión a redes 10Gbps es la opción de gama básica y representa una configuración básica. De manera opcional, el SG5712 puede configurarse para redes 25Gbps.

Hardware subyacente	Cantidad	Disco	Capacidad utilizable	Red
Dispositivos StorageGRID SG5712	4	48 x 4TB GB (HDD SAS casi en línea)	136TB	10Gbps

Elegir opciones de dispositivos de mayor rendimiento como los dispositivos NetApp StorageGRID SG5760, SG6060 o SGF6112 all-flash puede proporcionar importantes beneficios de rendimiento. Consulte con su arquitecto de soluciones NetApp StorageGRID para obtener ayuda en el dimensionamiento.

Requisitos de software de Commvault y StorageGRID

En las tablas siguientes se enumeran los requisitos de software del software Commvault y NetApp StorageGRID instalado en el software VMware para las pruebas. Se instalaron cuatro gestores de transmisión de datos MediaAgent y un servidor CommServe. En la prueba, se implantaron conexiones de red de 10Gbps GbE para la infraestructura VMware. La siguiente tabla

En la siguiente tabla, se enumeran los requisitos totales del sistema de software Commvault:

Componente	Cantidad	Almacén de datos	Tamaño	Total	IOPS total necesario
Servidor CommServe	1	SO	500GB	500GB	n.a.

Componente	Cantidad	Almacén de datos	Tamaño	Total	IOPS total necesario
		SQL	500GB	500GB	n.a.
MediaAgent	4	Unidad central de procesamiento virtual (vCPU)	16	64	n.a.
		RAM	128GB	512	n.a.
		SO	500GB	2 TB	n.a.
		Caché de índice	2 TB	8TB	200 o posterior
		DDB	2 TB	8TB	200-80.000K

En el entorno de pruebas, se pusieron en marcha un nodo de administración primario virtual y un nodo de puerta de enlace virtual en VMware en una cabina de almacenamiento E-Series E2812 de NetApp. Cada nodo estaba en un servidor independiente con los requisitos mínimos de entorno de producción descritos en la siguiente tabla:

En la siguiente tabla se enumeran los requisitos para los nodos de administración y puerta de enlace virtuales de StorageGRID:

Tipo de nodo	Cantidad	VCPU	RAM	Reducida
Nodo de pasarela	1	8	24GB	100GB LUN para el SO
Nodo de administración	1	8	24GB	100GB LUN para el SO 200GB LUN para tablas del nodo Admin 200GB LUN para el registro de auditoría del nodo de administración

Guía de tamaños de StorageGRID

Consulte a sus especialistas en protección de datos de NetApp para conocer el tamaño específico de su entorno. Los especialistas en protección de datos de NetApp pueden usar la herramienta Calculadora de almacenamiento de backup total de Commvault para estimar los requisitos de la infraestructura de backup. La herramienta requiere acceso al

portal de partners de Commvault. Regístrese para acceder, si es necesario.

Entradas para configuración de Commvault

Se pueden usar las siguientes tareas para detectar el dimensionamiento de la solución de protección de datos:

- Identifique las cargas de trabajo del sistema o de aplicaciones o bases de datos y la capacidad de interfaz correspondiente (en terabytes [TB]) que necesitarán protegerse.
- Identifique la carga de trabajo de equipos virtuales/archivos y la capacidad de interfaz (TB) similar que deberá protegerse.
- Identificar los requisitos de retención a corto y largo plazo.
- Identificar la tasa de porcentaje de cambio diario para los conjuntos de datos/cargas de trabajo identificados.
- Identifique el crecimiento de datos previsto para los próximos 12, 24 y 36 meses.
- Defina el RTO y el RPO para la protección y la recuperación de datos de acuerdo con las necesidades del negocio.

Cuando está disponible esta información, el ajuste del tamaño de la infraestructura de backup puede efectuarse desglosando las capacidades de almacenamiento requeridas.

Guía de tamaños de StorageGRID

Antes de realizar el ajuste de tamaño de NetApp StorageGRID, tenga en cuenta estos aspectos de su carga de trabajo:

- Capacidad utilizable
- Modo WORM
- Tamaño medio del objeto
- Requisitos de rendimiento
- Política de ILM aplicada

La cantidad de capacidad utilizable debe acomodar el tamaño de la carga de trabajo de backup que se ha organizado en niveles en StorageGRID y la programación de retención.

¿Se activará o no el modo WORM? Si WORM está habilitado en Commvault, se configurará el bloqueo de objetos en StorageGRID. Esto aumentará la capacidad de almacenamiento de objetos requerida. La cantidad de capacidad necesaria variará según la duración de la retención y la cantidad de cambios de objetos con cada backup.

El tamaño medio de objeto es un parámetro de entrada que ayuda a ajustar el tamaño para el rendimiento en un entorno StorageGRID. Los tamaños de objeto medios que se utilizan para una carga de trabajo de Commvault dependen del tipo de backup.

En la siguiente tabla, se enumeran los tamaños de objeto medios por tipo de backup y se describe lo que el proceso de restauración lee en el almacén de objetos:

Tipo de backup	Tamaño medio del objeto	Comportamiento de restauración
Haga una copia auxiliar en StorageGRID	32MB	Lectura completa del objeto 32MB
Dirigir el backup a StorageGRID (deduplicación activada)	8MB	Lectura de rango aleatorio de 1MB KB
Dirigir el backup a StorageGRID (deduplicación deshabilitada)	32MB	Lectura completa del objeto 32MB

Además, conocer sus requisitos de rendimiento para realizar backups completos y backups incrementales le ayuda a determinar el tamaño de los nodos de almacenamiento de StorageGRID. Los métodos de protección de datos de políticas de gestión del ciclo de vida de la información de StorageGRID determinan la capacidad necesaria para almacenar backups de Commvault y afectan al tamaño del grid.

La replicación de gestión de la vida útil de la información de StorageGRID es uno de los dos mecanismos que usa StorageGRID para almacenar datos de objetos. Cuando StorageGRID asigna objetos a una regla de ILM que replica los datos, el sistema crea copias exactas de los datos de los objetos y almacena las copias en los nodos de almacenamiento.

El código de borrado es el segundo método que utiliza StorageGRID para almacenar datos de objetos. Cuando StorageGRID asigna objetos a una regla de ILM que está configurada para crear copias con código de borrado, divide los datos de los objetos en fragmentos de datos. A continuación, calcula fragmentos de paridad adicionales y almacena cada fragmento en un nodo de almacenamiento diferente. Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o un fragmento de paridad se daña o se pierde, el algoritmo de código de borrado puede volver a crearlo usando un subconjunto de los datos restantes y fragmentos de paridad.

Los dos mecanismos requieren cantidades diferentes de almacenamiento, como muestran los siguientes ejemplos:

- Si almacena dos copias replicadas, la sobrecarga del almacenamiento se dobla.
- Si almacena una copia con código de borrado de 2+1, la sobrecarga de almacenamiento aumenta 1,5 veces.

Para la solución probada, se utilizó una puesta en marcha de StorageGRID de gama básica en un único sitio:

- Nodo de administración: Máquina virtual de VMware (VM)
- Balanceador de carga: VM de VMware
- Nodos de almacenamiento: 4x SG5712 TB con unidades de 4TB TB
- Nodo de administración principal y nodo de pasarela: Máquinas virtuales de VMware con los requisitos mínimos de carga de trabajo de producción

StorageGRID también es compatible con balanceadores de carga de terceros.

StorageGRID suele ponerse en marcha en dos o más sitios con políticas de protección de datos que replican datos para protegerlos contra los fallos de nodo y sitio. Al realizar un backup de los datos en StorageGRID, estos están protegidos por varias copias o por un código de borrado que separa y reensambla los datos de forma fiable mediante un algoritmo.

Puede usar la herramienta de ajuste de tamaño "Fusion" para ajustar el tamaño de la cuadrícula.

Escalado

Puede ampliar un sistema NetApp StorageGRID añadiendo almacenamiento a los nodos de almacenamiento, añadiendo nuevos nodos de grid a un sitio existente o añadiendo un nuevo sitio de centro de datos. Puede realizar ampliaciones sin interrumpir el funcionamiento del sistema actual.
StorageGRID escala el rendimiento usando nodos de mayor rendimiento para los nodos de almacenamiento o el dispositivo físico que ejecuta el balanceador de carga y los nodos de administración, o simplemente añadiendo nodos adicionales.

> Para obtener más información sobre la ampliación del sistema StorageGRID, consulte "Guía de ampliación de StorageGRID 11,9".

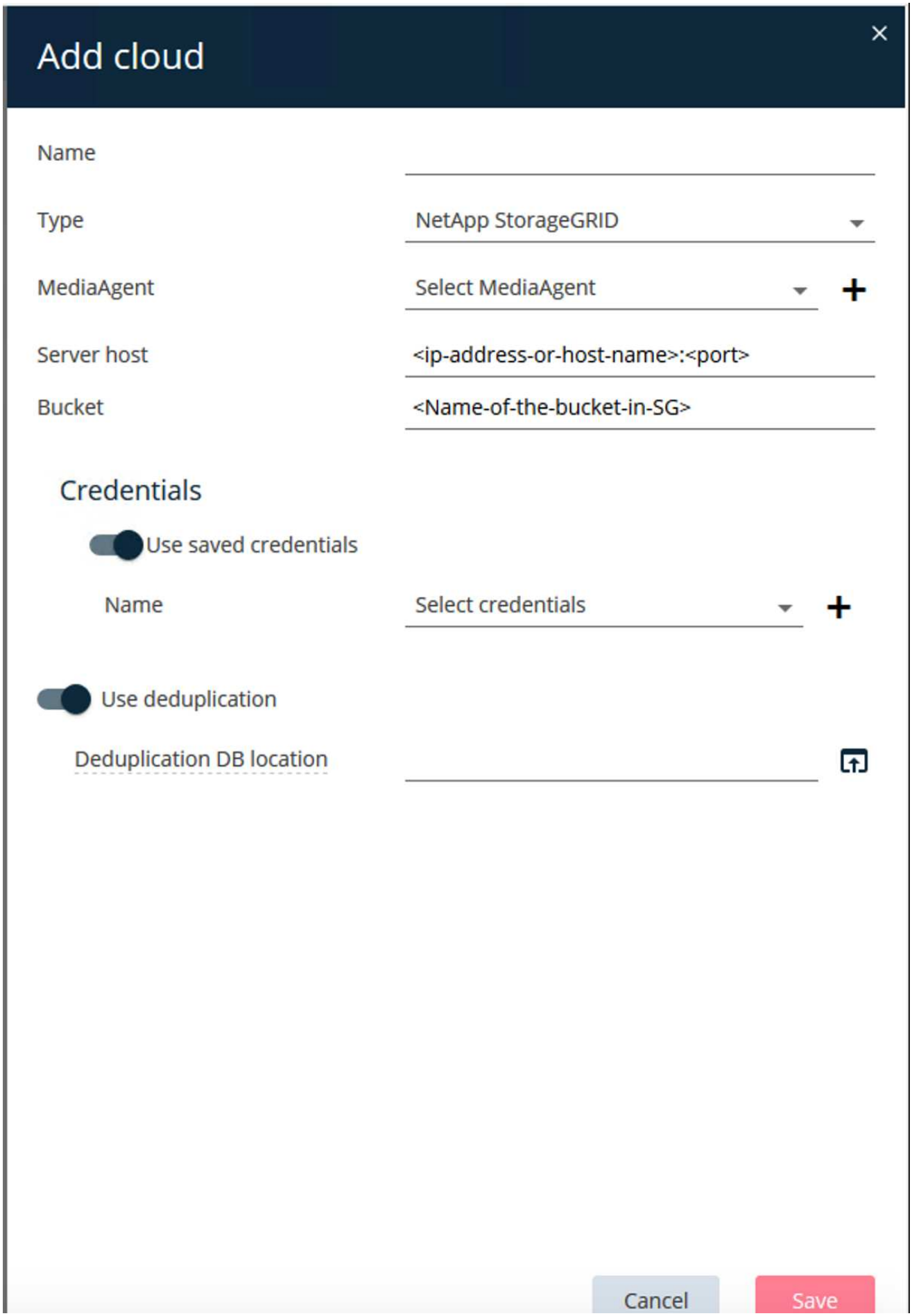
Ejecute un trabajo de protección de datos

Para configurar StorageGRID con Commvault Complete Backup and Recovery for NetApp, se llevaron a cabo los siguientes pasos para añadir StorageGRID como biblioteca de cloud dentro del software Commvault.

Paso 1: Configure Commvault con StorageGRID

Pasos

1. Inicie sesión en el Centro de comandos de Commvault. En el panel izquierdo, haga clic en Almacenamiento > Cloud > Add para ver y responder al cuadro de diálogo Add Cloud:


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. En Tipo, seleccione NetApp StorageGRID.
3. Para MediaAgent, seleccione todas las que estén asociadas a la biblioteca en la nube.
4. Para el host del servidor, introduzca la dirección IP o el nombre de host del punto final de StorageGRID y el número de puerto.

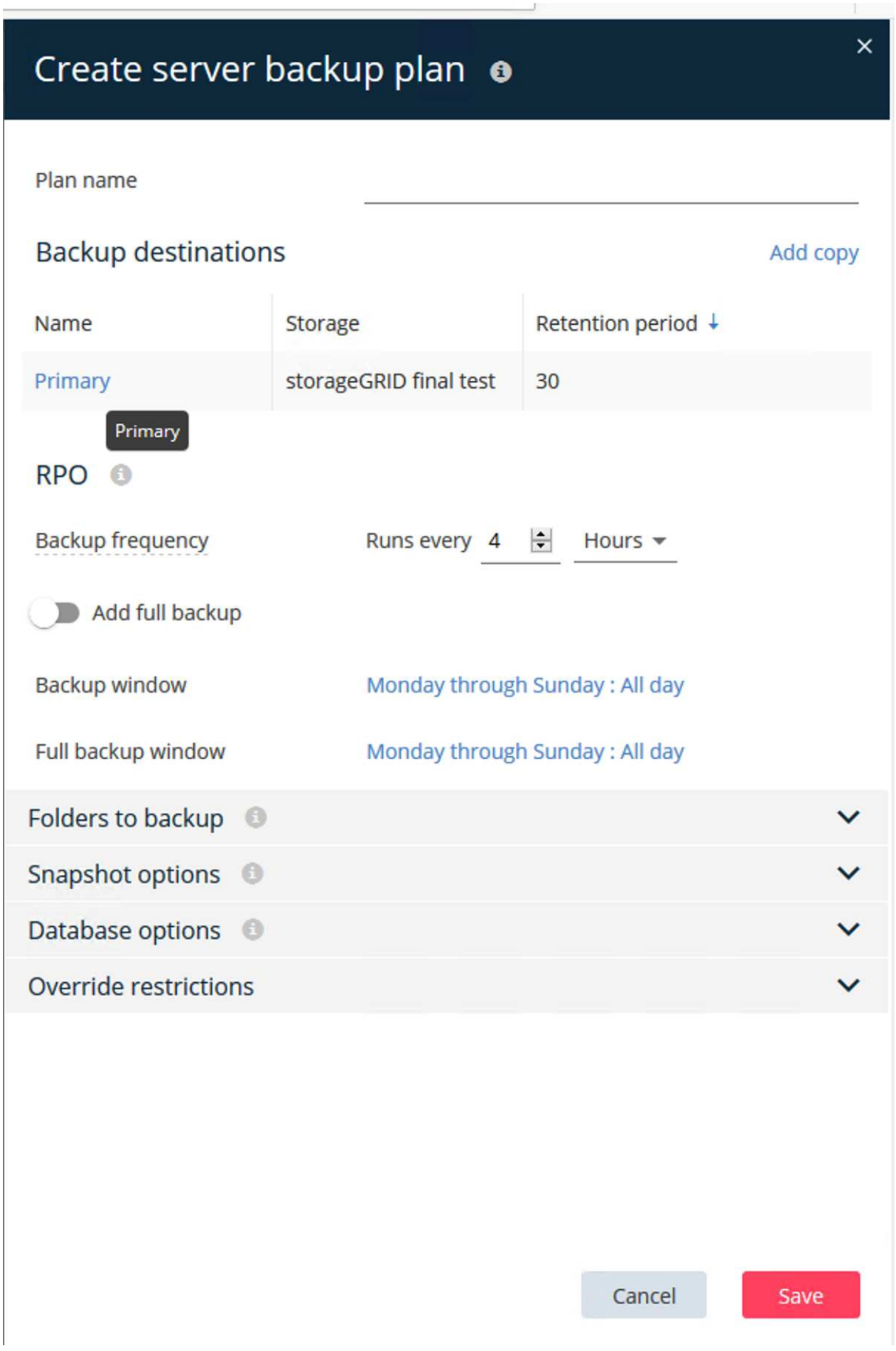
   Siga los pasos de la documentación de StorageGRID en "cómo configurar un punto final del balanceador de carga (puerto)". Asegúrese de tener un puerto HTTPS con un certificado autofirmado y la dirección IP o el nombre de dominio del extremo StorageGRID.

5. Si desea utilizar la deduplicación, active esta opción y proporcione la ruta a la ubicación de la base de datos de deduplicación.
6. Haga clic en Guardar.

Paso 2: Cree un plan de respaldo con StorageGRID como destino primario

Pasos

1. En el panel izquierdo, seleccione Administrar > Planes para ver y responder al cuadro de diálogo Crear plan de copia de seguridad del servidor.

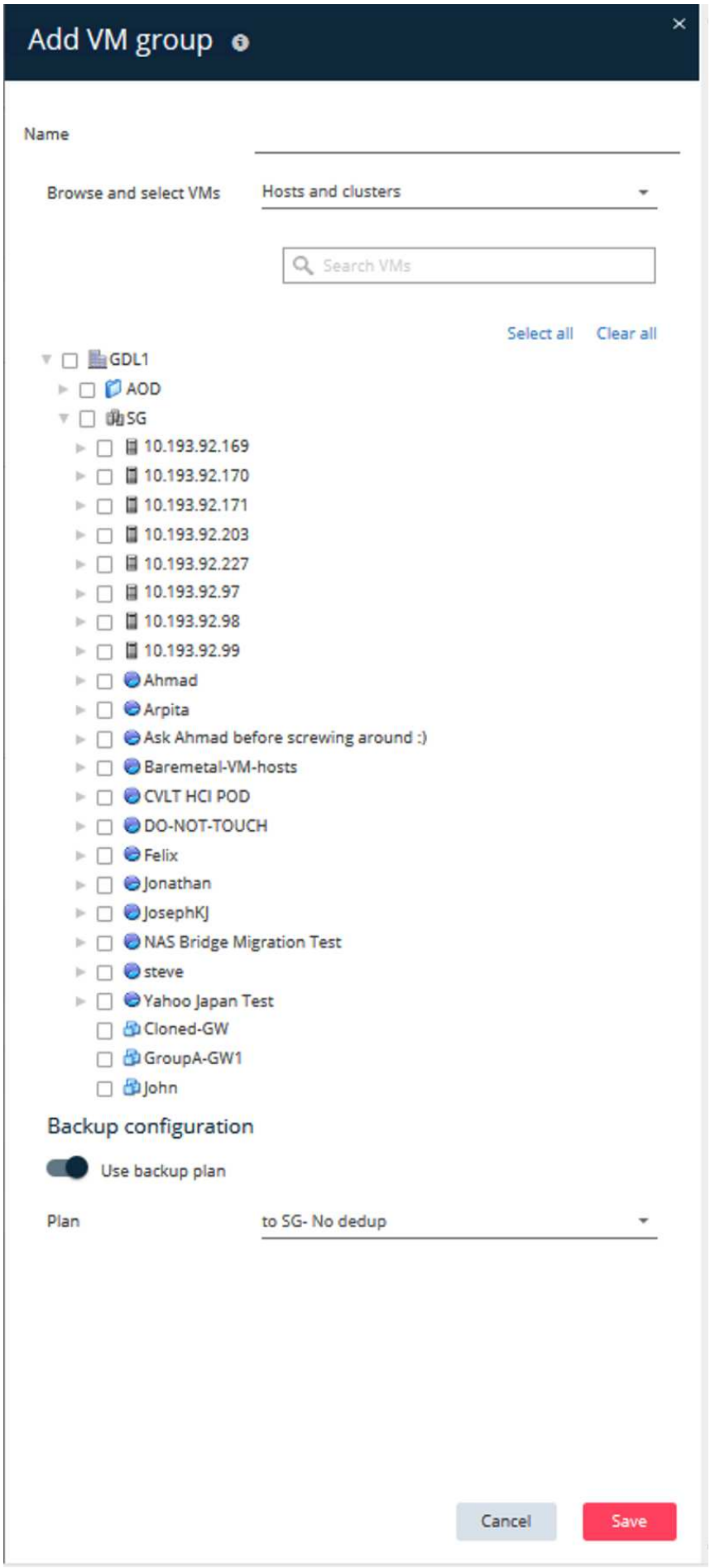

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Introduzca un nombre de plan.
3. Seleccione el destino de backup de almacenamiento de StorageGRID Simple Storage Service (S3) que creó anteriormente.
4. Introduzca el período de retención de backup y el objetivo de punto de recuperación (RPO) que desee.
5. Haga clic en Guardar.

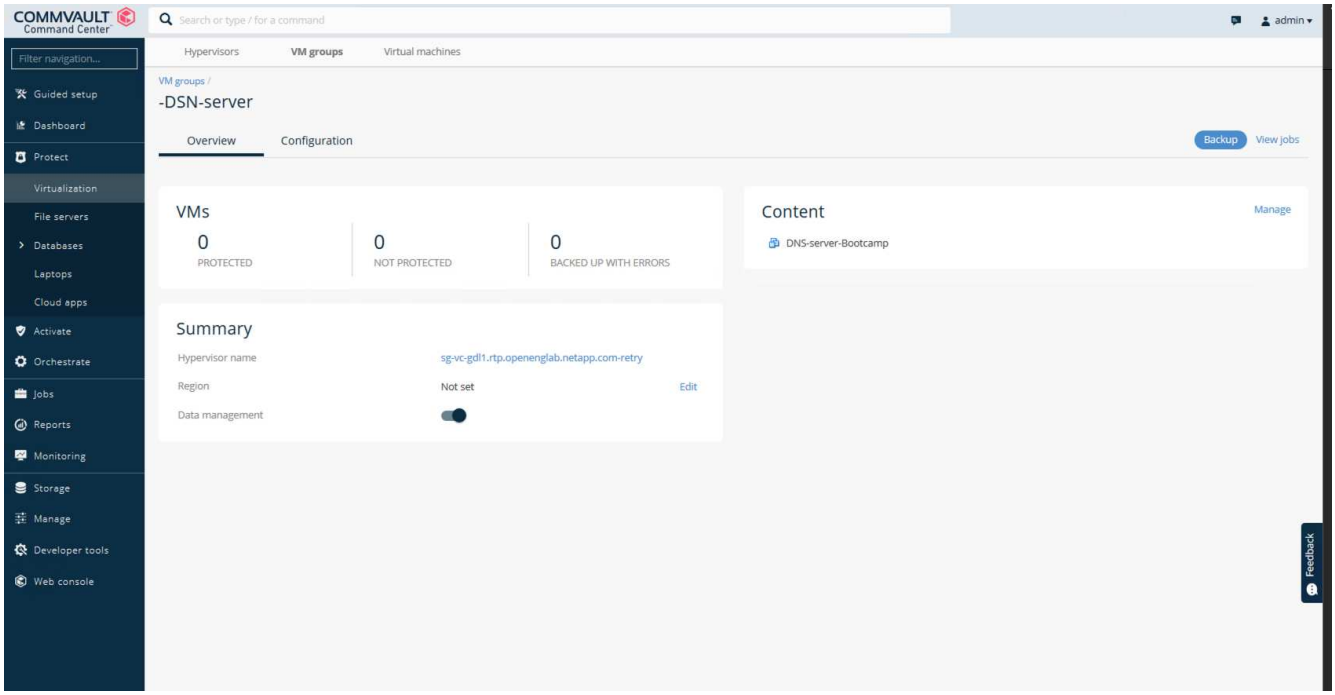
Paso 3: Inicia una tarea de backup para proteger las cargas de trabajo

Pasos

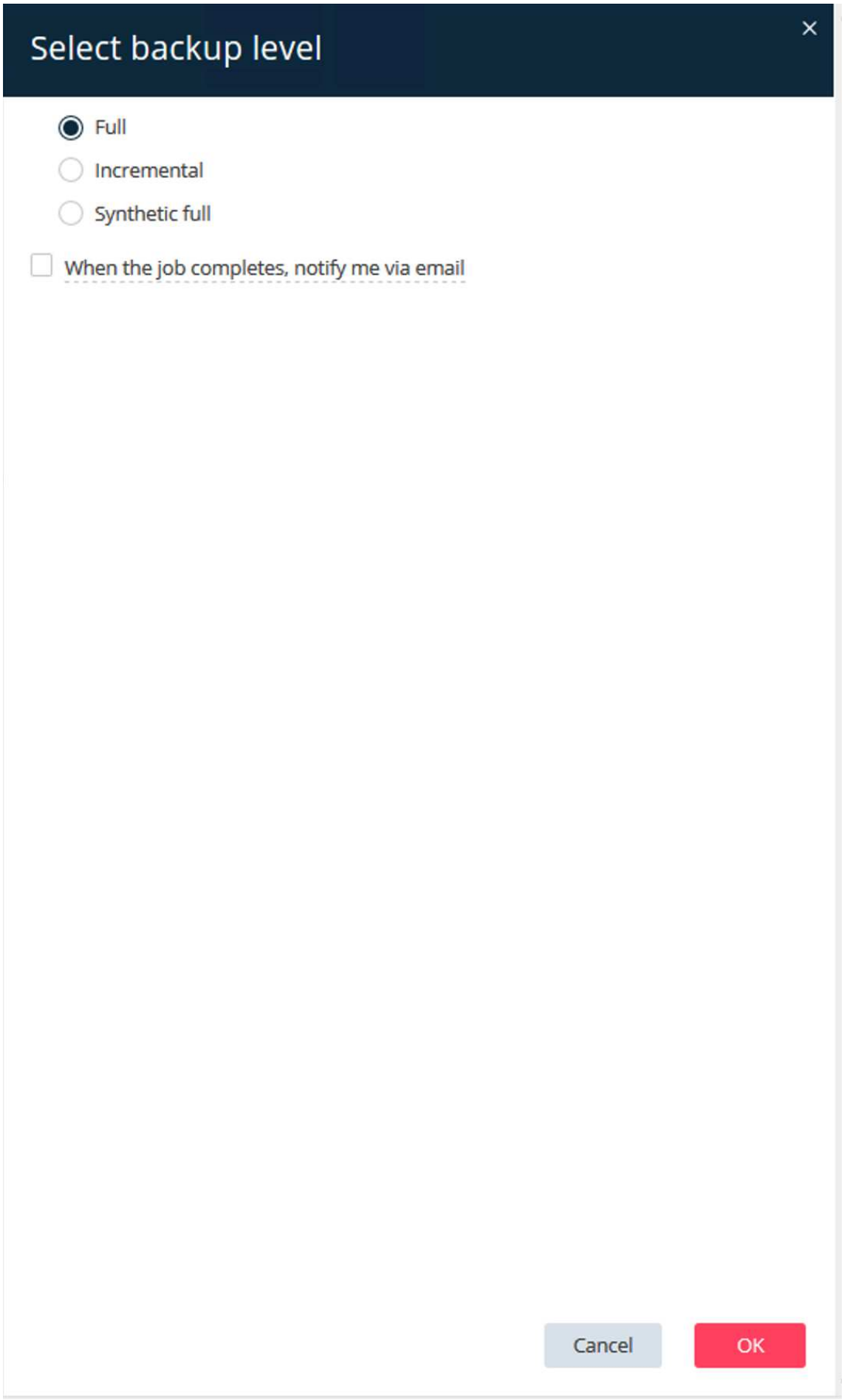
1. En Commvault Command Center, desplácese a Protect > Virtualization.
2. Añada un hipervisor de VMware vCenter Server.
3. Haga clic en el hipervisor que acaba de agregar.
4. Haga clic en Add VM group para responder al cuadro de diálogo Add VM Group para poder ver el entorno de vCenter que planea proteger.


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

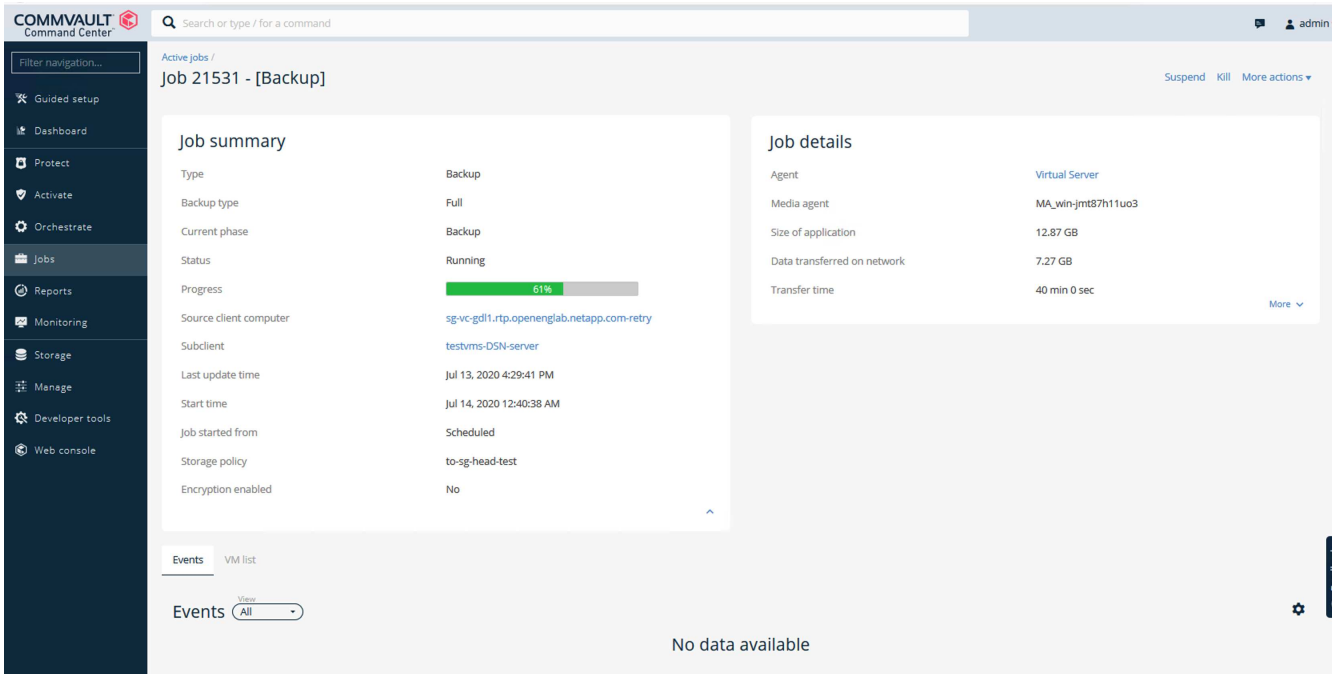
5. Seleccione un almacén de datos, una máquina virtual o una recogida de máquinas virtuales y introduzca un nombre para ella.
6. Seleccione el plan de copia de seguridad que creó en la tarea anterior.
7. Haga clic en Save para ver el grupo de máquinas virtuales que ha creado.
8. En la esquina superior derecha de la ventana VM group, seleccione Backup:



9. Seleccione Completo como nivel de copia de seguridad, (opcionalmente) solicite un correo electrónico cuando la copia de seguridad haya terminado, luego haga clic en Aceptar para que se inicie su trabajo de copia de seguridad:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Acceda a la página de resumen de trabajos para ver las métricas de trabajo:



Revise las pruebas de rendimiento básicas

En la operación Copia auxiliar, cuatro CommVault MediaAgent realizaron backups de los datos en un sistema NetApp AFF A300 y se creó una copia auxiliar en NetApp StorageGRID. Si desea obtener información detallada sobre el entorno de configuración de pruebas, lea la sección Diseño de la solución y mejores prácticas del "Protección de datos de escalado horizontal de NetApp con Commvault" informe técnico.

Las pruebas se llevaron a cabo con 100 equipos virtuales y 1000 equipos virtuales, ambas pruebas con una combinación de 50/50 equipos virtuales Windows y CentOS. La siguiente tabla muestra los resultados de nuestras pruebas de rendimiento de referencia:

Funcionamiento	Velocidad de backup	Velocidad de restauración
Copia AUX	2 TB/hora	1,27 TB/hora
Directo hacia y desde objetos (deduplicación activada)	2,2 TB/hora	1,22 TB/hora

Para probar el rendimiento anticuado, se eliminaron 2,5 millones de objetos. Como se muestra en las figuras 2 y 3, la ejecución de eliminación se realizó en menos de 3 horas y se liberaron más de 80TB TB de espacio. La ejecución de eliminación comenzó a las 10:30 AM.

Figura 1: Eliminación de 2,5 millones (80TB) de objetos en menos de 3 horas.

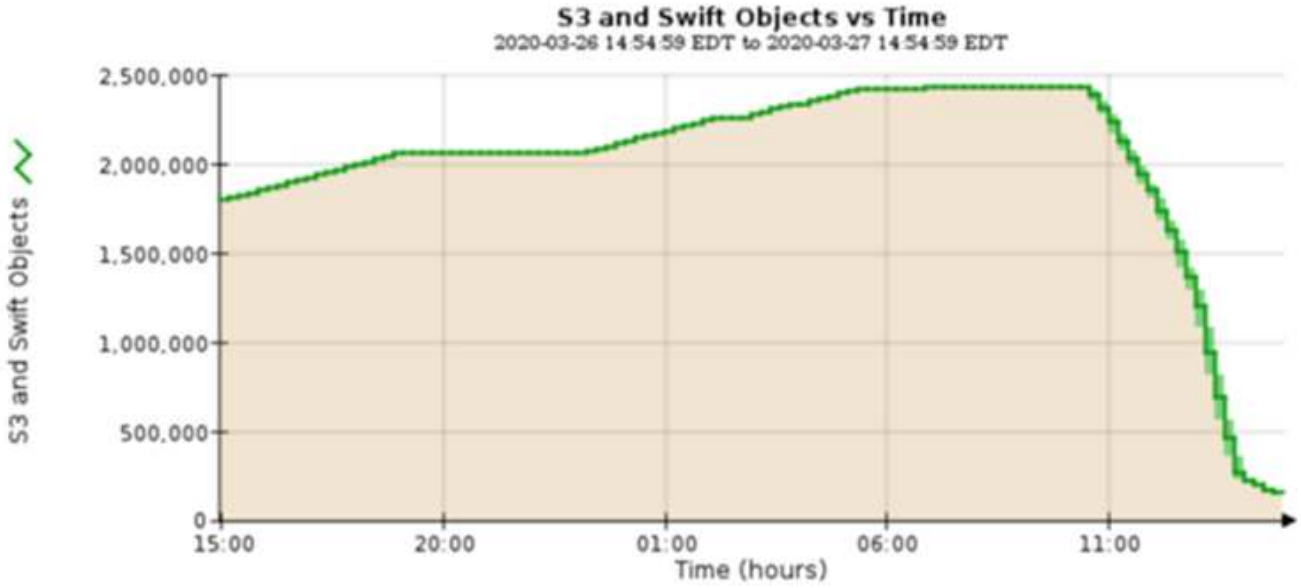
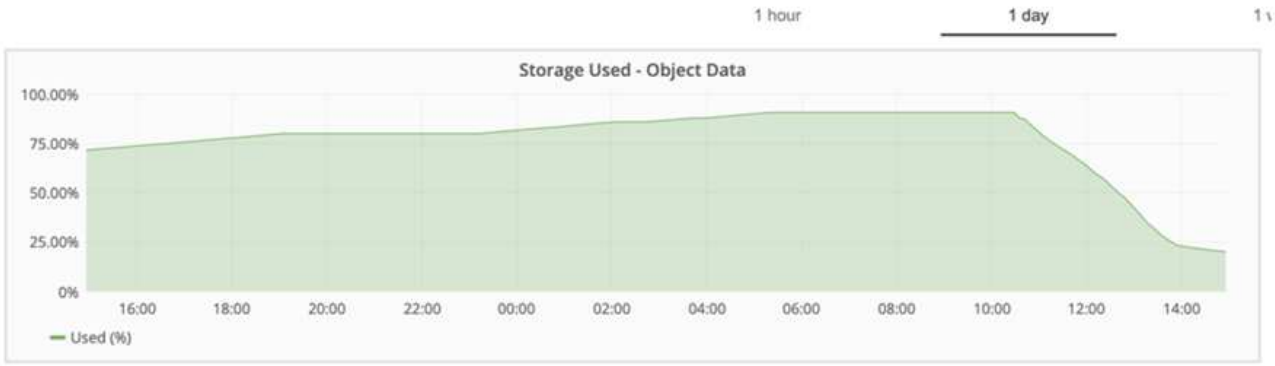


Figura 2: Liberación de 80TB TB de almacenamiento en menos de 3 horas.



Recomendación de nivel de coherencia del bloque

NetApp StorageGRID permite al usuario final seleccionar el nivel de coherencia de las operaciones realizadas en los objetos en bloques de Simple Storage Service (S3).

CommVault MediaAgent son transportadores de datos en un entorno Commvault. En la mayoría de los casos, los MediaAgent están configurados para escribir localmente en un sitio StorageGRID principal. Por esta razón, se recomienda un alto nivel de consistencia dentro de un sitio primario local. Use las siguientes directrices cuando defina el nivel de coherencia en los buckets Commvault creados en StorageGRID.

Si tiene una versión de CommVault anterior a la 11.0.0 - Service Pack 16, considere la posibilidad de actualizar CommVault a la versión más reciente. Si eso no es una opción, asegúrese de seguir las pautas para su versión.

- Versiones de CommVault anteriores a 11.0.0 - Service Pack 16.* En versiones anteriores a 11.0.0 - Service Pack 16, CommVault realiza operaciones S3 HEAD y GET en objetos no existentes como parte del proceso de restauración y poda. Establece el nivel de coherencia de buckets en sitio fuerte para alcanzar el nivel óptimo de coherencia para los backups de Commvault en StorageGRID.
- CommVault versiones 11.0.0 - Service Pack 16 y posteriores.* En las versiones 11.0.0 - Service Pack 16 y posteriores, se minimiza el número de operaciones S3 HEAD y GET realizadas en objetos no existentes.

Establezca el nivel de coherencia de bloques predeterminado en Read-after-new-write para garantizar un nivel de coherencia alto en el entorno Commvault y StorageGRID.

TR-4626: Balanceadores de carga

Use balanceadores de carga de terceros con StorageGRID

Obtenga información sobre el papel de un equilibrador de carga global y de terceros en sistemas de almacenamiento de objetos como StorageGRID.

Guía general para implementar NetApp® StorageGRID® con equilibradores de carga de terceros.

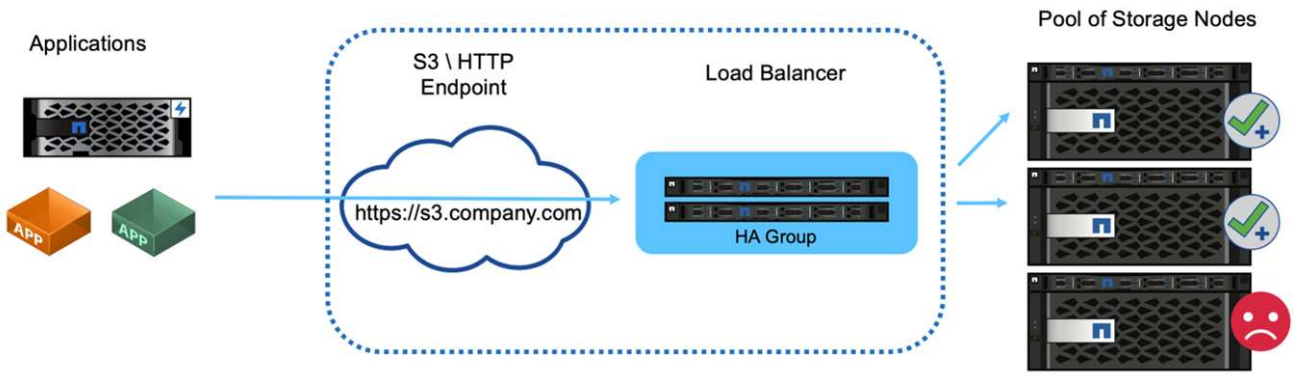
El almacenamiento de objetos es sinónimo de almacenamiento en cloud y, como cabe esperar, las aplicaciones que aprovechan el almacenamiento en cloud dirigen ese almacenamiento a través de una URL. Detrás de esa misma URL, StorageGRID puede escalar la capacidad, el rendimiento y la durabilidad en un solo sitio o en sitios con distribución geográfica. El componente que hace posible esta sencillez es un equilibrador de carga.

El objetivo de este documento es informar a los clientes de StorageGRID sobre las opciones de equilibrio de carga y proporcionar una guía general para la configuración de equilibradores de carga de terceros.

Conceptos básicos del equilibrador de carga

Los balanceadores de carga son un componente esencial de un sistema de almacenamiento de objetos de clase empresarial como StorageGRID. StorageGRID consta de varios nodos de almacenamiento, cada uno de los cuales puede presentar el espacio de nombres Simple Storage Service (S3) completo para una instancia de StorageGRID determinada. Los balanceadores de carga crean un extremo de alta disponibilidad detrás del que podemos colocar nodos StorageGRID. StorageGRID es única entre los sistemas de almacenamiento de objetos compatibles con S3, ya que proporciona su propio balanceador de carga, pero también admite balanceadores de carga de uso general o de terceros, como F5, Citrix Netscaler, HA Proxy, NGINX, etc.

En la siguiente figura se utiliza la URL de ejemplo/ nombre de dominio completamente cualificado (FQDN) “s3.company.com”. El equilibrador de carga crea una IP virtual (VIP) que se resuelve en el FQDN mediante DNS y, a continuación, dirige las solicitudes de las aplicaciones a un pool de nodos de StorageGRID. El balanceador de carga realiza una comprobación del estado de cada nodo y solo establece conexiones con nodos en buen estado.



La figura muestra el equilibrador de carga proporcionado por StorageGRID, pero el concepto es el mismo para los equilibradores de carga de terceros. Las aplicaciones establecen una sesión HTTP mediante la VIP del balanceador de carga y el tráfico pasa a través del balanceador de carga a los nodos de almacenamiento. De forma predeterminada, todo el tráfico, desde la aplicación al balanceador de carga y desde el balanceador de

carga al nodo de almacenamiento se cifra a través de HTTPS. HTTP es una opción compatible.

Equilibradores de carga locales y globales

Existen dos tipos de equilibradores de carga:

- **Administradores de tráfico local (LTM)**. Distribuye las conexiones en un pool de nodos en un único sitio.
- **Global Service Load Balancer (GSLB)**. Distribuye las conexiones en múltiples sitios, equilibradores de carga LTM con equilibrio de carga eficaz. Piense en un GSLB como un servidor DNS inteligente. Cuando un cliente solicita una URL de extremo de StorageGRID, el GSLB lo resuelve al VIP de un LTM según la disponibilidad u otros factores (por ejemplo, qué sitio puede proporcionar una latencia menor para la aplicación). Aunque siempre se requiere un LTM, un GSLB es opcional en función del número de sitios de StorageGRID y los requisitos de su aplicación.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Centro de documentación de NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Consideraciones de diseño del equilibrador de carga StorageGRID F5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load Equilibrio de NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp: NetApp StorageGRID de equilibrio de carga https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Utilice balanceadores de carga de StorageGRID

Obtenga información sobre la función de un equilibrador de carga de nodo de puerta de enlace de StorageGRID .

Orientación general para la implementación de nodos de puerta de enlace NetApp® StorageGRID®.

Equilibrador de carga de nodo de puerta de enlace StorageGRID frente al equilibrador de carga de terceros

StorageGRID es único entre los proveedores de almacenamiento de objetos compatibles con S3, ya que proporciona un balanceador de carga nativo disponible como dispositivo, máquina virtual o contenedor específicamente creados. El balanceador de carga proporcionado por StorageGRID también se conoce como nodo de puerta de enlace.

Para los clientes que no poseen aún un balanceador de carga, como F5, Citrix, etc., la implementación de un balanceador de carga de terceros puede ser muy compleja. El balanceador de carga de StorageGRID simplifica enormemente las operaciones del balanceador de carga.

El nodo de puerta de enlace es un equilibrador de carga de alto rendimiento, altamente disponible y de nivel empresarial. Los clientes pueden optar por implementar el nodo de pasarela, el equilibrador de carga de terceros, o incluso ambos, en el mismo grid. El nodo de puerta de enlace es un gestor de tráfico local frente a un GSLB.

El equilibrador de carga de StorageGRID ofrece las siguientes ventajas:

- **Simplicidad**. Configuración automática de pools de recursos, comprobaciones de estado, parches y mantenimiento, todo gestionado por StorageGRID.
- **Actuación**. El balanceador de carga StorageGRID está dedicado a StorageGRID, puede proporcionar almacenamiento en caché de alto rendimiento y no compite con otras aplicaciones por el ancho de banda.
- **Coste**. La máquina virtual (VM) y las versiones de contenedor se proporcionan sin coste adicional.
- **Clasificaciones de tráfico**. La función de clasificación de tráfico avanzada permite reglas de calidad de servicio específicas de StorageGRID junto con análisis de cargas de trabajo.
- **Futuras características específicas de StorageGRID**. StorageGRID continuará optimizando y añadiendo características innovadoras al equilibrador de carga en los próximos lanzamientos.

Como nodo integrado de StorageGRID, el administrador de tráfico local tiene la capacidad de usar una verificación de estado avanzada para distribuir solicitudes en función del estado del nodo de almacenamiento, la carga y la disponibilidad de recursos. Además, tiene la capacidad de distribuir la carga entre múltiples sitios cuando los costos del enlace StorageGRID se establecen en "0" entre los sitios. En el caso de que los nodos de almacenamiento no estén disponibles pero el nodo de enlace esté disponible en un sitio, la carga se dirigirá automáticamente a otro sitio en la red.

La función de almacenamiento en caché del equilibrador de carga del nodo de puerta de enlace está diseñada para proporcionar una mejora sustancial del rendimiento para ciertas cargas de trabajo (como el entrenamiento de IA) que vuelven a leer un conjunto de datos varias veces como parte del procesamiento de esos datos. Los nodos de puerta de enlace de almacenamiento en caché también se pueden implementar físicamente distantes del resto de la red, lo que permite un mejor rendimiento y una menor utilización de la red WAN en algunas cargas de trabajo. La caché funciona en un modo de lectura diferida, donde las escrituras no se almacenan en caché y no modifican el estado de la caché. Cada nodo de puerta de enlace de almacenamiento en caché funciona independientemente de cualquier otro nodo de puerta de enlace de almacenamiento en caché.

Para obtener detalles sobre la implementación del nodo de puerta de enlace de StorageGRID , consulte la "Documentación de StorageGRID" .

Aprenda a implementar certificados SSL para HTTPS en StorageGRID

Comprender la importancia y los pasos para implementar certificados SSL en StorageGRID.

Si utiliza HTTPS, debe tener un certificado de capa de sockets seguros (SSL). El protocolo SSL identifica los clientes y los puntos finales, validándolos como de confianza. SSL también proporciona cifrado del tráfico. Los clientes deben confiar en el certificado SSL. Para lograr esto, el certificado SSL puede provenir de una autoridad de certificación (CA) de confianza mundial, como DigiCert, una CA privada que se ejecuta en su infraestructura, o un certificado autofirmado generado por el host.

El método preferido es utilizar un certificado de CA de confianza global, ya que no se requieren acciones adicionales en el cliente. El certificado se carga en el equilibrador de carga o StorageGRID, y los clientes confían y se conectan al extremo.

El uso de una CA privada requiere la raíz y todos los certificados subordinados se agregan al cliente. El proceso para confiar en un certificado de CA privado puede variar según el sistema operativo y las aplicaciones del cliente. Por ejemplo, en ONTAP para FabricPool, debe cargar cada certificado en la cadena de forma individual (certificado raíz, certificado subordinado, certificado de extremo) en el clúster de ONTAP.

El uso de un certificado autofirmado requiere que el cliente confíe en el certificado proporcionado sin ninguna

CA para verificar la autenticidad. Es posible que algunas aplicaciones no acepten certificados autofirmados y no tengan capacidad de ignorar la verificación.

La ubicación del certificado SSL en la ruta de StorageGRID del equilibrador de carga del cliente depende de dónde se necesite la terminación SSL. Puede configurar un equilibrador de carga para que sea el punto final de terminación del cliente y, a continuación, volver a cifrar o cifrar en caliente con un nuevo certificado SSL para la conexión del equilibrador de carga a StorageGRID. O puede pasar por el tráfico y dejar que StorageGRID sea el punto final de terminación SSL. Si el equilibrador de carga es el punto final de terminación SSL, el certificado se instala en el equilibrador de carga y contiene el nombre del asunto para el nombre/URL de DNS y cualquier nombre de URL/DNS alternativo para el que un cliente está configurado para conectarse al destino StorageGRID a través del equilibrador de carga. incluyendo cualquier nombre de comodín. Si el equilibrador de carga está configurado para la transferencia directa, el certificado SSL se debe instalar en StorageGRID. De nuevo, el certificado debe contener el nombre del asunto para el nombre/URL de DNS y cualquier nombre de URL/DNS alternativo para el que un cliente esté configurado para conectarse al destino de StorageGRID a través del equilibrador de carga, incluidos los nombres de comodines. No es necesario incluir los nombres de nodos de almacenamiento individuales en el certificado, solo las URL de extremo.

Configurar equilibrador de carga de terceros de confianza en StorageGRID

Aprenda a configurar el equilibrador de carga de terceros de confianza en StorageGRID.

Si utiliza uno o más equilibradores de carga externos de capa 7 y un bucket o políticas de grupo de S3 basadas en IP, StorageGRID debe determinar la dirección IP del remitente real. Para ello, consulte el cabezal X-Forward-For (XFF), que el equilibrador de carga inserta en la solicitud. Dado que el encabezado XFF se puede suplantar fácilmente en las solicitudes enviadas directamente a los nodos de almacenamiento, StorageGRID debe confirmar que un equilibrador de carga de capa 7 de confianza dirige cada solicitud. Si StorageGRID no puede confiar en el origen de la solicitud, ignorará la cabecera XFF. Hay una API de gestión de grid que permite configurar una lista de equilibradores de carga de capa 7 externos de confianza. Esta nueva API es privada y está sujeta a cambios en futuros lanzamientos de StorageGRID. Para obtener la información más actualizada, consulte el artículo de la base de conocimientos, "Cómo configurar StorageGRID para que funcione con equilibradores de carga de capa 7 de terceros".

Obtenga más información sobre los equilibradores de carga del gestor de tráfico local

Explore las directrices para los balanceadores de carga de gestor de tráfico local y determine la configuración óptima.

A continuación se presenta como guía general para la configuración de equilibradores de carga de terceros. Trabaje con el administrador de balanceo de carga para determinar la configuración óptima para su entorno.

Cree un grupo de recursos de nodos de almacenamiento

Agrupe los nodos de almacenamiento de StorageGRID en un pool de recursos o un grupo de servicios (la terminología puede diferir con equilibradores de carga específicos). Los nodos de almacenamiento de StorageGRID presentan la API S3 en los puertos siguientes:

- S3 HTTPS: 18082
- S3 HTTP: 18084

La mayoría de los clientes eligen presentar las API en el servidor virtual a través de los puertos HTTPS y HTTP estándar (443 y 80).

> Cada sitio de StorageGRID requiere tres nodos de almacenamiento predeterminados, dos de los cuales deben estar en buen estado.

Comprobación del estado

Los balanceadores de carga de terceros requieren un método para determinar el estado de cada nodo y su elegibilidad para recibir tráfico. NetApp recomienda el método HTTP `OPTIONS` para realizar la comprobación del estado. El equilibrador de carga emite solicitudes HTTP `OPTIONS` a cada nodo de almacenamiento individual y espera una `200` respuesta del estado.

Si algún nodo de almacenamiento no proporciona `200` una respuesta, ese nodo no puede atender solicitudes de almacenamiento. Los requisitos de la aplicación y del negocio deben determinar el tiempo de espera para estas comprobaciones y la acción que realiza el equilibrador de carga.

Por ejemplo, si tres de los cuatro nodos de almacenamiento del centro de datos 1 están inactivos, podría dirigir todo el tráfico al centro de datos 2.

El intervalo de sondeo recomendado es de una vez por segundo y marca al nodo como desconectado después de tres comprobaciones que han fallado.

S3 ejemplo de comprobación de estado

En el siguiente ejemplo, enviamos `OPTIONS` y comprobamos `200 OK`. Utilizamos `OPTIONS` porque Amazon S3) no admite solicitudes no autorizadas.

```
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
```

Comprobaciones de estado basadas en archivos o contenidos

En general, NetApp no recomienda comprobaciones de estado basadas en archivos. Normalmente, un archivo pequeño —`healthcheck.htm`, por ejemplo, se crea en un depósito con una política de sólo lectura. El equilibrador de carga recupera y evalúa este archivo. Este enfoque tiene varias desventajas:

- **Depende de una sola cuenta.** Si la cuenta propietaria del archivo está deshabilitada, la comprobación del estado genera errores y no se procesa ninguna solicitud de almacenamiento.
- **Normas de protección de datos.** El esquema de protección de datos predeterminado es un enfoque de dos copias. En este escenario, si los dos nodos de almacenamiento que alojan el archivo de comprobación de estado no están disponibles, la comprobación del estado genera un error y las solicitudes de almacenamiento no se envían a nodos de almacenamiento en buen estado, lo que se vuelve sin conexión.
- **Bloat de registro de auditoría.** El equilibrador de carga recupera el archivo de cada nodo de almacenamiento cada X minutos, lo que crea muchas entradas del registro de auditoría.
- **Recursos intensivos.** Recuperar el archivo de comprobación de estado de cada nodo cada pocos segundos consume recursos de grid y de red.

Si se requiere una comprobación del estado basada en contenido, utilice un inquilino dedicado con un depósito dedicado de S3.

Persistencia de la sesión

La persistencia de la sesión, o la persistencia, hace referencia al tiempo en que una sesión HTTP determinada puede persistir. De forma predeterminada, los nodos de almacenamiento descartan las sesiones tras 10 minutos. Una mayor persistencia puede dar lugar a un mejor rendimiento, ya que las aplicaciones no tienen que restablecer sus sesiones para cada acción; sin embargo, mantener estas sesiones abiertas consume recursos. Si determina que su carga de trabajo se beneficiará, puede reducir la persistencia de la sesión en un

equilibrador de carga de terceros.

Direccionamiento virtual tipo alojado

El estilo hospedado virtual es ahora el método predeterminado para AWS S3, y aunque StorageGRID y muchas aplicaciones aún admiten el estilo de ruta, es mejor implementar el soporte virtual de estilo hospedado. Las solicitudes virtuales de estilo alojado tienen el bucket como parte del nombre del host.

Para admitir el estilo hospedado virtual, haga lo siguiente:

- Soporte de búsquedas de DNS comodín: *.s3.company.com
- Utilice un certificado SSL con nombres alternativos de asunto para admitir comodines: *.s3.company.com Algunos clientes han expresado preocupaciones de seguridad sobre el uso de certificados comodín. StorageGRID sigue admitiendo el acceso al estilo de ruta, al igual que las aplicaciones clave como FabricPool. Dicho esto, ciertas llamadas a la API S3 fallan o se comportan incorrectamente sin soporte virtual alojado.

Terminación SSL

Existen ventajas de seguridad para la terminación SSL en equilibradores de carga de terceros. Si el equilibrador de carga está comprometido, la rejilla se divide.

Hay tres configuraciones compatibles:

- **SSL pass-through.** El certificado SSL se instala en StorageGRID como certificado de servidor personalizado.
- **Terminación SSL y re-encriptación (recomendado).** Esto puede ser beneficioso si ya está realizando la gestión de certificados SSL en el equilibrador de carga en lugar de instalar el certificado SSL en StorageGRID. Esta configuración proporciona la ventaja de seguridad adicional de limitar la superficie de ataque al equilibrador de carga.
- **Terminación SSL con HTTP.** En esta configuración, SSL se termina en el equilibrador de carga de terceros y la comunicación del equilibrador de carga a StorageGRID no está cifrada para aprovechar la descarga de SSL (con bibliotecas SSL integradas en procesadores modernos esto es de beneficio limitado).

Pasar por la configuración

Si prefiere configurar el equilibrador de carga para la transferencia, debe instalar el certificado en StorageGRID. Vaya al menú:Configuración[Certificados de servidor > Object Storage API Service Endpoints Certificado de servidor].

Visibilidad de la IP del cliente de origen

StorageGRID 11,4 introdujo el concepto de un equilibrador de carga de terceros de confianza. Para reenviar la IP de la aplicación cliente a StorageGRID, debe configurar esta función. Para obtener más información, consulte "Cómo configurar StorageGRID para que funcione con equilibradores de carga de capa 7 de terceros."

Para activar el encabezado XFF que se utilizará para ver la IP de la aplicación cliente, siga estos pasos:

Pasos

1. Registre la IP del cliente en el registro de auditoría.

2. Use `aws:SourceIp` la política de grupo o bloque S3.

Estrategias de equilibrio de carga

La mayoría de las soluciones de equilibrio de carga ofrecen múltiples estrategias para el equilibrio de carga. Las siguientes son estrategias comunes:

- **Round robin.** Un ajuste universal pero sufre con pocos nodos y grandes transferencias obstruyendo nodos individuales.
- **Menos conexión.** Una buena opción para cargas de trabajo de objetos pequeños o mixtos, lo que produce una distribución igual de las conexiones a todos los nodos.

La elección del algoritmo se vuelve menos importante, con un mayor número de nodos de almacenamiento entre los que elegir.

Ruta de datos

Todos los datos fluyen a través de los balanceadores de carga del gestor de tráfico local. StorageGRID no admite el enrutamiento directo del servidor (DSR).

Verificando la distribución de las conexiones

Para verificar que su método distribuye la carga uniformemente entre los nodos de almacenamiento, compruebe las sesiones establecidas en cada nodo en un sitio determinado:

- **Método UI.** Vaya al menú:Soporte[Métricas > Visión General de S3 > Sesiones HTTP de LDR]
- **API de métricas.** Uso `storagegrid_http_sessions_incoming_currently_established`

Obtenga información sobre pocos casos de uso de las configuraciones de StorageGRID

Explora pocos casos prácticos de las configuraciones de StorageGRID implementadas por los clientes y EL DEPARTAMENTO DE TI de NetApp.

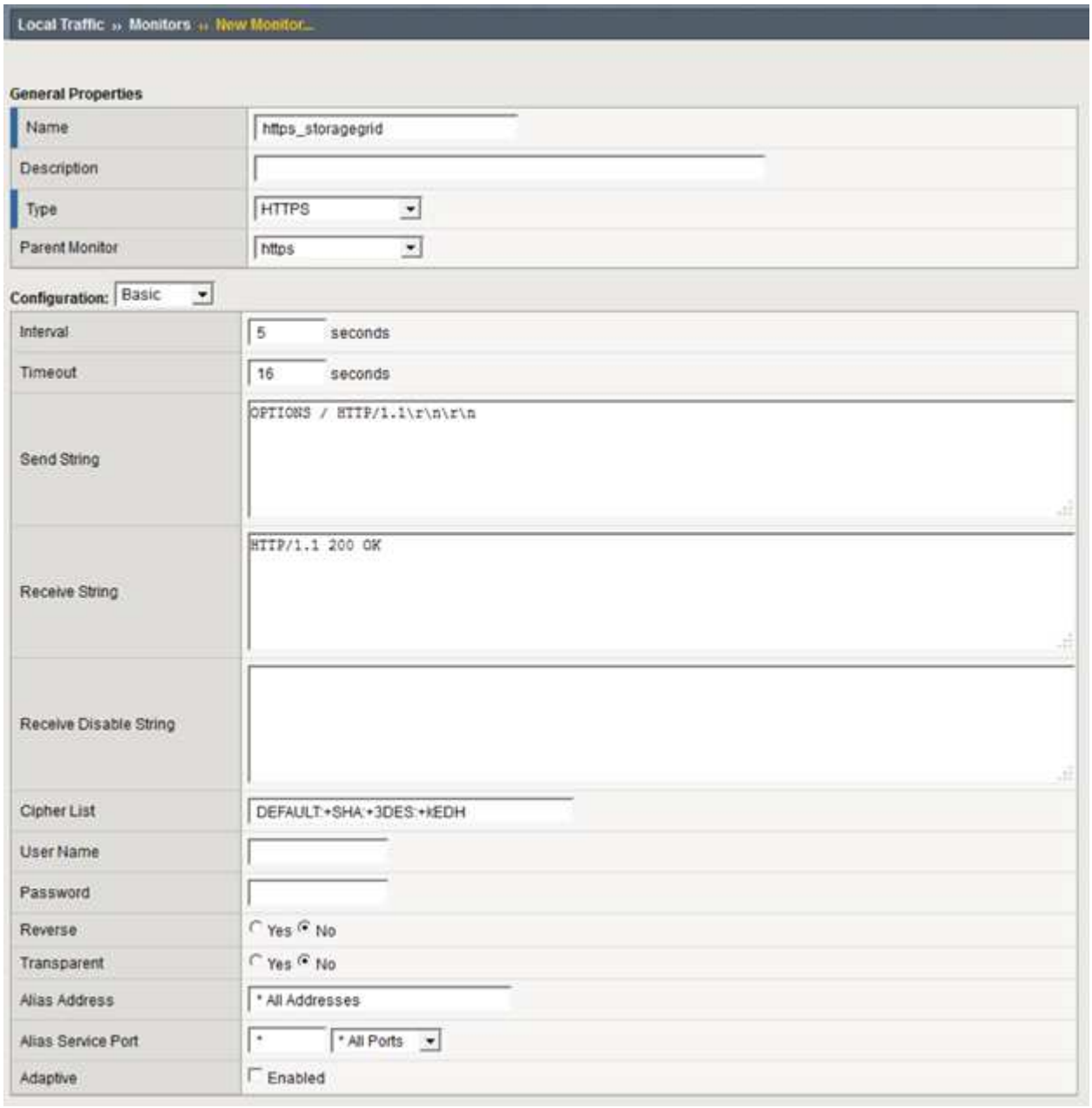
En los siguientes ejemplos se ilustran las configuraciones implantadas por los clientes de StorageGRID, incluido NetApp IT.

Monitor de comprobación de estado del administrador de tráfico local BIG-IP F5 para el cubo S3

Para configurar el monitor de comprobación del estado del administrador de tráfico local BIG-IP F5, siga estos pasos:

Pasos

1. Cree un nuevo monitor.
   a. En el campo Tipo, introduzca `HTTPS`.
   b. Configure el intervalo y el tiempo de espera como desee.
   c. En el campo Cadena de envío, introduzca `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n son devoluciones de carro; las diferentes versiones del software BIG-IP requieren cero, uno o dos conjuntos de secuencias \r\n. Para obtener más información, consulte https://support.f5.com/csp/article/K10655.
   d. En el campo Cadena de recepción, introduzca: `HTTP/1.1 200 OK`.



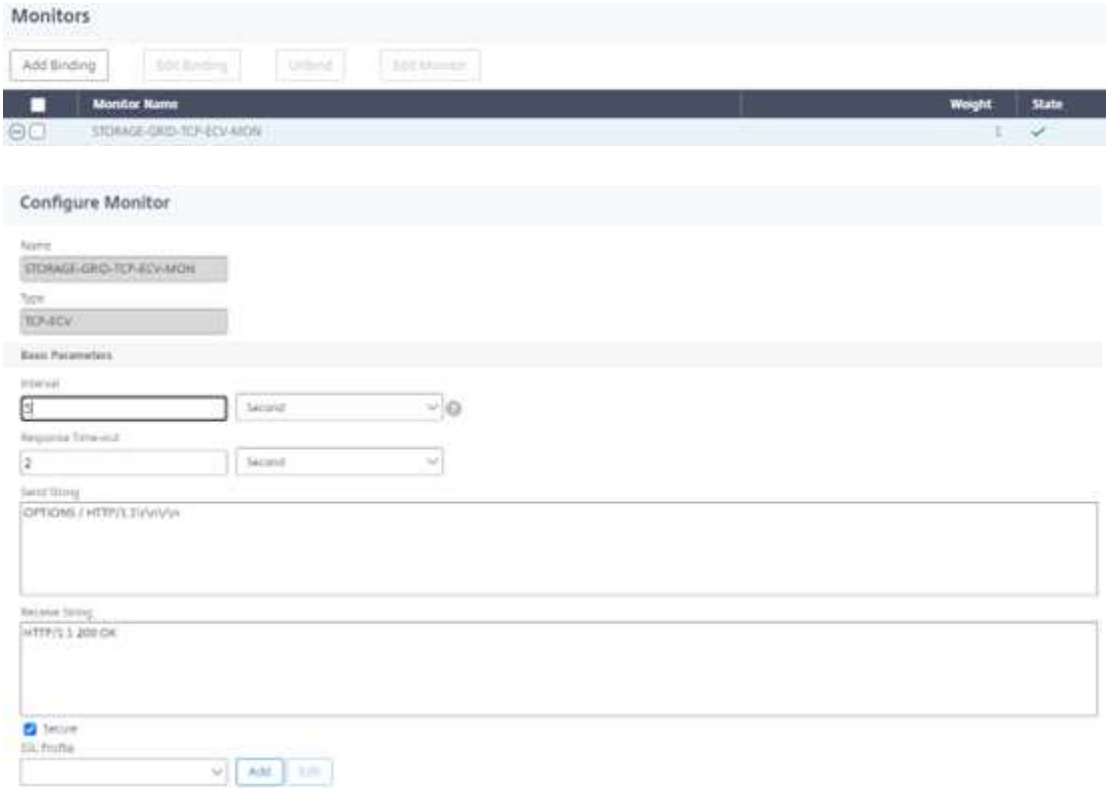
2. En Crear Pool, cree un pool para cada puerto necesario.
   a. Asigne el monitor de estado que ha creado en el paso anterior.
   b. Seleccione un método de equilibrio de carga.
   c. Seleccione el puerto de servicio: 18082 (S3).
   d. Añada nodos.

Citrix NetScaler

Citrix NetScaler crea un servidor virtual para el punto final de almacenamiento y hace referencia a los nodos de almacenamiento de StorageGRID como servidores de aplicaciones, que a continuación se agrupan en servicios.

Utilice el monitor de comprobación de estado HTTPS-ECV para crear un monitor personalizado para realizar la comprobación de estado recomendada mediante la solicitud de OPCIONES y la recepción `200`. HTTP-ECV se configura con una cadena de envío y valida una cadena de recepción.

Para obtener más información, consulte la documentación de Citrix, "Configuración de ejemplo para el monitor de comprobación del estado de HTTP-ECV".



Loadbalancer.org

Loadbalancer.org ha realizado sus propias pruebas de integración con StorageGRID y cuenta con una amplia guía de configuración: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp ha llevado a cabo sus propias pruebas de integración con StorageGRID y tiene una extensa guía de configuración: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Configure HAProxy para que utilice la solicitud de OPCIONES y compruebe si hay una respuesta de estado 200 para la comprobación de estado en haproxy.cfg. Puede cambiar el puerto de enlace del front-end a un puerto diferente, por ejemplo, 443.

El siguiente es un ejemplo de terminación SSL en HAProxy:

```
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
```

A continuación se muestra un ejemplo para la transferencia SSL:

```
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
```

Para obtener ejemplos completos de configuraciones para StorageGRID, consulte "Ejemplos de configuración de HAProxy" en GitHub.

Valide la conexión SSL en StorageGRID

Aprenda a validar la conexión SSL en StorageGRID.

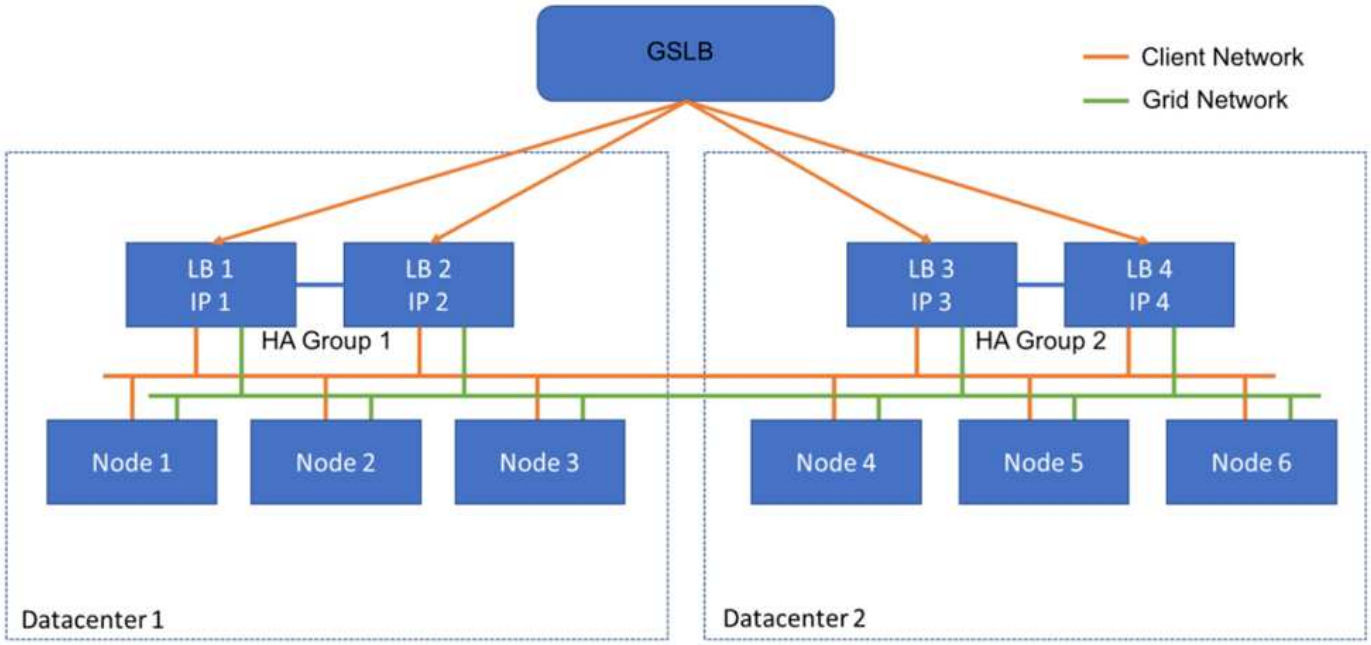
Después de configurar el equilibrador de carga, debe validar la conexión mediante herramientas como OpenSSL y la CLI de AWS. Otras aplicaciones, como S3 Browser, podrían ignorar la configuración incorrecta de SSL.

Comprender los requisitos globales de equilibrio de carga para StorageGRID

Explore las consideraciones y requisitos de diseño para el equilibrio de carga global en StorageGRID.

El equilibrio de carga global requiere la integración con DNS para proporcionar enrutamiento inteligente entre varios sitios de StorageGRID. Esta función está fuera del dominio StorageGRID y debe ser proporcionada por una solución de terceros, como los productos de equilibrio de carga descritos anteriormente y/o una solución de control de tráfico DNS como Infoblox. Este equilibrio de carga de nivel superior proporciona enrutamiento

inteligente al sitio de destino más cercano en el espacio de nombres, así como detección de interrupciones y redireccionamiento al siguiente sitio en el espacio de nombres. Una implementación típica de GSLB consiste en el GSLB de nivel superior con pools de sitios que contienen equilibradores de carga de sitio-local. Los balanceadores de carga del sitio contienen pools de los nodos de almacenamiento del sitio local. Esto puede incluir una combinación de equilibradores de carga de terceros para funciones GSLB y StorageGRID que proporciona el equilibrio de carga local de sitio, o una combinación de terceros, o muchos de los terceros mencionados anteriormente pueden proporcionar tanto GSLB como equilibrio de carga local de sitio.



TR-4645: Funciones de seguridad

Protege los datos y metadatos de StorageGRID en un almacén de objetos

Descubra las funciones de seguridad integrales de la solución de almacenamiento de objetos de StorageGRID.

Esta es una descripción general de las numerosas características de seguridad de NetApp® StorageGRID®, que abarcan el acceso a datos, objetos y metadatos, acceso administrativo y seguridad de la plataforma. Se ha actualizado para incluir las funciones más nuevas lanzadas con StorageGRID 12.0.

La seguridad es una parte integral de la solución de almacenamiento de objetos de NetApp StorageGRID. La seguridad es especialmente importante porque muchos tipos de datos de contenido enriquecido que se adaptan perfectamente al almacenamiento de objetos también son confidenciales por naturaleza y sujetos a regulaciones y cumplimiento de normativas. A medida que las funcionalidades de StorageGRID continúan evolucionando, el software pone a su disposición muchas funciones de seguridad imprescindibles para proteger la política de seguridad de la organización y ayudar a la organización a cumplir las prácticas recomendadas del sector.

Este documento es una descripción general de las numerosas características de seguridad en StorageGRID 12.0, divididas en cinco categorías:

- Funciones de seguridad de acceso a los datos
- Funciones de seguridad de objetos y metadatos

- Funciones de seguridad de administración
- Funciones de seguridad de la plataforma
- Integración del cloud

Este documento pretende ser una hoja de datos de seguridad; no detalla cómo configurar el sistema para admitir las funciones de seguridad enumeradas en él que no están configuradas de manera predeterminada. El "Guía para el fortalecimiento de StorageGRID" está disponible en la página oficial "Documentación de StorageGRID" página.

Además de las capacidades descritas en este informe, StorageGRID sigue el "Política de notificación y respuesta de vulnerabilidad de seguridad de los productos de NetApp". Las vulnerabilidades informadas se verifican y responden a ellas según el proceso de respuesta a incidentes de seguridad del producto.

NetApp StorageGRID ofrece funciones de seguridad avanzadas para casos de uso de almacenamiento de objetos empresariales muy exigentes.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- NetApp StorageGRID: Evaluación del cumplimiento de las normas SEC 17a-4(f), FINRA 4511(c) y CFTC 1,31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Certificación de cifrado de kernel NetApp StorageGRID NIST FIPS 140-3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- Certificación de entropía NetApp StorageGRID NIST SP 800-90B https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- Certificación de criterios comunes del Centro Canadiense de Ciberseguridad de NetApp StorageGRID https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- Página de documentación de StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

Términos y acrónimos

En esta sección se proporcionan definiciones de la terminología utilizada en el documento.

Término o acrónimo	Definición
S3	Servicio de almacenamiento simple.
Cliente	Una aplicación que puede interactuar con StorageGRID mediante el protocolo S3 para el acceso a los datos o el protocolo HTTP para la gestión.
Administrador de inquilinos	El administrador de la cuenta de inquilino de StorageGRID
Usuario inquilino	Un usuario dentro de una cuenta de inquilino de StorageGRID
TLS	Seguridad de la capa de transporte
ILM	Gestión del ciclo de vida de la información
LAN	Red de área local

Término o acrónimo	Definición
Administrador de grid	El administrador del sistema StorageGRID
Cuadrícula	El sistema StorageGRID
Cucharón	Un contenedor para objetos almacenados en S3
LDAP	Protocolo ligero de acceso a directorios
SEG	Securities and Exchange Commission; regula los miembros, agentes y distribuidores de las operaciones
FINRA	Autoridad reguladora de la industria financiera; aplaza los requisitos de formato y medios de la norma SEC 17a-4(f)
CFTC	Commodity Futures Trading Comissions; regula el comercio de futuros de materias primas
NIST	Instituto Nacional de Estándares y Tecnología

Funciones de seguridad de acceso a los datos

Obtenga más información sobre las funciones de seguridad del acceso a los datos en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Seguridad de la capa de transporte configurable (TLS)	TLS establece un protocolo de apretón de manos para la comunicación entre un cliente y un nodo de pasarela StorageGRID, un nodo de almacenamiento o un extremo del balanceador de carga. StorageGRID admite los siguientes conjuntos de cifrado para TLS: • 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 Compatibilidad con TLS v1,2 y 1,3. No se admiten SSLv3, TLS v1.1 y anteriores.	Permite que un cliente y StorageGRID se identifiquen y autentiquen entre sí y se comuniquen con confidencialidad e integridad de los datos. Garantiza el uso de una versión de TLS reciente. Los cifrados ahora se pueden configurar en la configuración de configuración/seguridad	—

Función	Función	Impacto	Cumplimiento de normativas
Certificado de servidor configurable (punto final del equilibrador de carga)	Los administradores de grid pueden configurar puntos finales del equilibrador de carga para generar o utilizar un certificado de servidor.	Permite el uso de certificados digitales firmados por su entidad de certificación (CA) de confianza estándar para autenticar las operaciones de API de objetos entre grid y cliente por punto final de equilibrador de carga.	—
Certificado de servidor configurable (extremo de API)	Los administradores de grid pueden configurar de forma centralizada todos los puntos finales de la API de StorageGRID para que utilicen un certificado de servidor firmado por la CA de confianza de su organización.	Permite el uso de certificados digitales firmados por su CA de confianza estándar para autenticar operaciones de API de objetos entre un cliente y el grid.	—

Función	Función	Impacto	Cumplimiento de normativas
Multi-tenancy	StorageGRID admite varios inquilinos por grid, cada cliente cuenta con su propio espacio de nombres. Un inquilino proporciona un protocolo S3; de forma predeterminada, el acceso a bloques/contenedores y objetos está restringido a los usuarios de la cuenta. Los inquilinos pueden tener un usuario (por ejemplo, un despliegue empresarial, en el que cada usuario tiene su propia cuenta) o varios usuarios (por ejemplo, un despliegue de proveedor de servicios, en el que cada cuenta es una empresa y un cliente del proveedor de servicios). Los usuarios pueden ser locales o federados; los usuarios federados los define Active Directory o el protocolo ligero de acceso a directorios (LDAP). StorageGRID ofrece una consola por inquilino, en la que los usuarios inician sesión con las credenciales de cuentas locales o federadas. Los usuarios pueden acceder a informes visualizados sobre el uso de los inquilinos respecto de la cuota asignada por el administrador de grid, incluida la información de uso en datos y objetos almacenados por bloques. Los usuarios con permiso administrativo pueden llevar a cabo tareas de administración del sistema a nivel de inquilino, como gestionar usuarios y grupos y claves de acceso.	Permite que los administradores de StorageGRID alojen datos de varios inquilinos aislando el acceso de los inquilinos y establecer la identidad de usuario mediante la federación de usuarios con un proveedor de identidades externo, como Active Directory o LDAP.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
No rechazo de credenciales de acceso	Cada operación de S3 se identifica y se registra con una cuenta de inquilino, un usuario y una clave de acceso únicos.	Permite a los administradores de Grid establecer qué acciones de API realizan cada persona.	—

Función	Función	Impacto	Cumplimiento de normativas
Acceso anónimo deshabilitado	De forma predeterminada, el acceso anónimo está desactivado para las cuentas S3. Un solicitante debe tener una credencial de acceso válida para un usuario válido en la cuenta de inquilino para acceder a depósitos, contenedores u objetos dentro de la cuenta. El acceso anónimo a bloques u objetos de S3 se puede habilitar con una política de IAM explícita.	Permite a los administradores de Grid desactivar o controlar el acceso anónimo a bloques/contenedores y objetos.	—
WORM de cumplimiento de normativas	Diseñado para cumplir con los requisitos de la normativa SEC 17a-4(f) y validado por Cohasset. Los clientes pueden habilitar el cumplimiento de normativas a nivel del bucket. La retención se puede ampliar pero nunca se puede reducir. Las reglas de gestión de la vida útil de la información (ILM) aplican niveles de protección de datos mínimos.	Permite a los inquilinos con requisitos de retención de datos normativos para habilitar la protección WORM en los objetos almacenados y los metadatos de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
GUSANO	Los administradores de grid pueden habilitar WORM en toda la cuadrícula habilitando la opción Disable Client Modify, que impide que los clientes sobrescriban o eliminen objetos o metadatos de objetos en todas las cuentas de inquilino. S3 Los administradores de inquilinos también pueden habilitar WORM por inquilino, bloque o prefijo de objeto especificando la política de IAM, que incluye el permiso personalizado S3: PutOverwriteObject para la sobrescritura de objetos y metadatos.	Permite que los administradores de Grid y los administradores de inquilinos controlen la protección WORM en los objetos almacenados y los metadatos de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Gestión de claves de cifrado del servidor host KM	Los administradores de grid pueden configurar uno o varios servidores de gestión de claves externos (KMS) en Grid Manager para proporcionar claves de cifrado para servicios de StorageGRID y aplicaciones de almacenamiento. Cada servidor de host KMS o clúster de servidores de host KMS utiliza el protocolo de interoperabilidad de gestión de claves (KMIP) para proporcionar una clave de cifrado a los nodos del dispositivo en el sitio de StorageGRID asociado.	Se logra el cifrado de los datos en reposo. Una vez cifrados los volúmenes del dispositivo, no puede acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el servidor host KMS.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Recuperación automatizada tras fallos	StorageGRID proporciona redundancia incorporada y conmutación por error automatizada. El acceso a las cuentas, los bloques y los objetos de inquilino puede continuar incluso si hay varios fallos, desde discos o nodos a sitios enteros. StorageGRID tiene en cuenta recursos y redirige automáticamente las solicitudes a los nodos y las ubicaciones de datos disponibles. Los sitios StorageGRID incluso pueden funcionar en modo interno; si una interrupción en WAN desconecta un sitio del resto del sistema, las operaciones de lectura y escritura pueden continuar con los recursos locales y la replicación se reanuda automáticamente cuando se restaura la WAN.	Permite a los administradores de Grid abordar el tiempo de actividad, los acuerdos de nivel de servicios y otras obligaciones contractuales, así como implementar planes de continuidad empresarial.	—

Función	Función	Impacto	Cumplimiento de normativas
Características de seguridad de acceso a datos específicas de S3	AWS Signature versión 2 y versión 4	Las solicitudes de API de firma proporcionan autenticación para las operaciones de API de S3. Amazon admite dos versiones de Signature Version 2 y 4. El proceso de firma verifica la identidad del solicitante, protege los datos en tránsito y protege contra posibles ataques de repetición.	Se alinea con la recomendación de AWS para la versión de firma 4 y permite la compatibilidad con versiones anteriores con aplicaciones anteriores con la versión de firma 2.
—	Bloqueo de objetos de S3	La función Bloqueo de objetos S3 de StorageGRID es una solución de protección de objetos equivalente a Bloqueo de objetos S3 en Amazon S3.	Permite a los inquilinos crear buckets con S3 Object Lock habilitado para cumplir con las regulaciones que requieren que ciertos objetos se conserven durante un período de tiempo fijo o indefinidamente.
Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)	Almacenamiento seguro de credenciales S3	Las claves de acceso S3 se almacenan en un formato protegido por una función de hash de contraseña (SHA-2).	Permite el almacenamiento seguro de claves de acceso mediante una combinación de longitud de clave (un número generado aleatoriamente 10^{31}) y un algoritmo de hash de contraseña.
—	Teclas de acceso S3 con límite de tiempo	Al crear una clave de acceso S3 para un usuario, los clientes pueden establecer una fecha y hora de caducidad en la clave de acceso.	Ofrece a los administradores de Grid la opción de aprovisionar claves de acceso S3 temporales.

Función	Función	Impacto	Cumplimiento de normativas
—	Múltiples claves de acceso por cuenta de usuario	StorageGRID permite crear varias claves de acceso y estar activas simultáneamente para una cuenta de usuario. Dado que cada acción de API se registra con una cuenta de usuario de inquilino y una clave de acceso, el no repudio se conserva a pesar de que hay varias claves activas.	Permite a los clientes rotar las claves de acceso sin interrupciones y permite que cada cliente tenga su propia clave, lo que desalienta el uso compartido de claves entre los clientes.
—	S3 Política de acceso de IAM	StorageGRID admite políticas de IAM S3, lo que permite a los administradores de Grid especificar control de acceso granular por inquilino, bloque o prefijo de objeto. StorageGRID también admite condiciones y variables de política de IAM, lo que permite políticas de control de acceso más dinámicas.	Permite a los administradores de Grid especificar el control de acceso por grupos de usuarios para todo el inquilino; también permite a los usuarios inquilinos especificar el control de acceso para sus propios bloques y objetos.
—	API del servicio de token de seguridad S3 AssumeRole	StorageGRID admite la API AssumeRole de S3 STS para proporcionar credenciales de seguridad temporales (ID de clave de acceso, clave de acceso secreta, token de sesión) con permisos de alcance reducido y duración limitada. Las políticas de sesión en línea para restringir aún más los permisos durante la sesión son compatibles como parte de la API AssumeRole.	Permite a los administradores de inquilinos proporcionar acceso temporal seguro a los datos de los objetos.

Función	Función	Impacto	Cumplimiento de normativas
—	Servicio de notificación simple	StorageGRID admite el envío de notificaciones sobre el acceso a objetos. Se admiten los siguientes tipos de eventos: • s3:ObjetoCreado: • s3:ObjetoCreado:Poner • s3:ObjetoCreado:Publicación • s3:ObjetoCreado:Copiar • s3:Objeto creado:Carga multiparte completa • s3:Objeto eliminado: • s3:ObjetoEliminado:Eliminar • s3:Objeto eliminado:Eliminar marcador creado • s3:Restaurar objeto:Publicar	Permite a los administradores de inquilinos supervisar el acceso a los objetos
—	Cifrado del lado del servidor con claves gestionadas por StorageGRID (SSE)	StorageGRID admite SSE, lo que permite la protección multitenant de datos en reposo con claves de cifrado gestionadas por StorageGRID.	Permite a los inquilinos cifrar objetos. Se necesita una clave de cifrado para escribir y recuperar estos objetos.
Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)	Cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)	StorageGRID admite SSE-C, lo que permite la protección multitenant de los datos en reposo con claves de cifrado gestionadas por el cliente. Aunque StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, con SSE-C, el cliente debe gestionar las claves de cifrado por sí mismo.	Permite a los clientes cifrar los objetos con claves que controlan. Se necesita una clave de cifrado para escribir y recuperar estos objetos.

Seguridad de objetos y metadatos

Explora las funciones de seguridad de objetos y metadatos en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Cifrado de objetos del lado del servidor del estándar de cifrado avanzado (AES)	StorageGRID proporciona cifrado de objetos en el servidor basado en AES 128 y AES 256. Los administradores de grid pueden activar el cifrado como valor predeterminado global. StorageGRID también admite el encabezado de cifrado de lado del servidor x-amz S3 para permitir habilitar o deshabilitar el cifrado por objeto. Cuando está activado, los objetos se cifran cuando se almacenan o están en tránsito entre los nodos de la cuadrícula.	Ayuda a proteger el almacenamiento y la transmisión de objetos, independientemente del hardware de almacenamiento subyacente.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Gestión de claves incorporada	Cuando se habilita el cifrado, cada objeto se cifra con una clave simétrica única generada aleatoriamente, que se almacena en StorageGRID sin acceso externo.	Permite el cifrado de objetos sin necesidad de gestión de claves externa.	
Discos de cifrado compatibles con el estándar de procesamiento de información federal (FIPS) 140-2	Los dispositivos StorageGRID SG5812, SG5860, SG6160 y SGF6024 ofrecen la opción de discos de cifrado conformes a la normativa FIPS 140-2-2. Las claves de cifrado para los discos pueden gestionarse opcionalmente un servidor KMIP externo.	Permite un almacenamiento seguro de datos, metadatos y objetos del sistema. También ofrece cifrado de objetos basado en software StorageGRID, que protege el almacenamiento y la transmisión de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Cifrado compatible con el Estándar Federal de Procesamiento de Información (FIPS) 140-3 para nodos	Los dispositivos StorageGRID SG5812, SG5860, SG6160, SGF6112, SG1100 y SG110 ofrecen la opción de cifrado de nodo compatible con FIPS 140-3. Las claves de cifrado de los nodos son administradas por un servidor KMIP externo.	Permite un almacenamiento seguro de datos, metadatos y objetos del sistema. También ofrece cifrado de objetos basado en software StorageGRID, que protege el almacenamiento y la transmisión de objetos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Exploración de integridad de fondo y reparación automática	StorageGRID usa un mecanismo interconectado compuesto por hashes, sumas de comprobación y comprobaciones de redundancia cíclicas (CRC) en el nivel de objeto y subobjeto para ofrecer protección frente a la incoherencia, manipulación o modificación de datos, tanto cuando los objetos se encuentran en almacenamiento como en tránsito. StorageGRID detecta automáticamente los objetos dañados o alterados, y los reemplaza mientras pone en cuarentena los datos modificados y alerta al administrador.	Permite a los administradores de Grid cumplir los acuerdos de nivel de servicios, las normativas y otras obligaciones relativas a la durabilidad de los datos. Ayuda a los clientes a detectar virus o ransomware que intentan cifrar, manipular o modificar datos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Retención y ubicación de objetos basadas en políticas	StorageGRID permite que los administradores de Grid configuren las reglas de ILM, las cuales especifican la retención de objetos, la ubicación, la protección, la transición y la caducidad. Los administradores de grid pueden configurar StorageGRID para que filtre objetos por sus metadatos y para aplicar reglas a distintos niveles de granularidad, incluidos todo el grid, inquilino, bloque, prefijo de clave o. y pares clave-valor de metadatos definidos por el usuario. StorageGRID ayuda a garantizar que los objetos se almacenan según las reglas de ILM durante sus ciclos de vida, a menos que el cliente los elimine de manera explícita.	Ayuda a aplicar la ubicación, la protección y la retención de los datos. Ayuda a los clientes a lograr el acuerdo de nivel de servicio en cuanto a durabilidad, disponibilidad y rendimiento.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Análisis de metadatos en segundo plano	StorageGRID analiza periódicamente los metadatos de objetos en segundo plano para aplicar cambios en la ubicación o la protección de los datos de objetos según lo especificado por ILM.	Ayuda a detectar objetos corruptos.	

Función	Función	Impacto	Cumplimiento de normativas
Coherencia ajustable	Los inquilinos pueden seleccionar niveles de coherencia en el nivel del bucket para garantizar que estén disponibles recursos, como la conectividad multisitio.	Proporciona la opción de confirmar las escrituras en el grid solo cuando hay un número necesario de sitios o recursos disponibles.	

Funciones de seguridad de administración

Descubra las funciones de seguridad de administración en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Certificado de servidor (interfaz de gestión de grid)	Los administradores de grid pueden configurar la interfaz de gestión de grid para que utilice un certificado de servidor firmado por la CA de confianza de su organización.	Permite el uso de certificados digitales firmados por su CA estándar y de confianza para autenticar el acceso de API y de interfaz de usuario de gestión entre un cliente de gestión y el grid.	—
Autenticación de usuario administrativa	Los usuarios administrativos se autentican con el nombre de usuario y la contraseña. Los usuarios y grupos administrativos pueden ser locales o federados, importados desde Active Directory o LDAP del cliente. Las contraseñas de la cuenta local se almacenan en un formato protegido por bcrypt; las contraseñas de la línea de comandos se almacenan en un formato protegido por SHA-2.	Autentica el acceso administrativo a la interfaz de usuario de gestión y las API.	—

Función	Función	Impacto	Cumplimiento de normativas
Soporte de SAML	StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2,0 (SAML 2,0). Cuando se habilita SSO, todos los usuarios deben estar autenticados por un proveedor de identidades externo antes de poder acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid o a la API de gestión de inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.	Permite niveles adicionales de seguridad para administradores de grid e inquilinos, como SSO y la autenticación multifactor (MFA).	NIST SP800-63
Control granular de permisos	Los administradores de grid pueden asignar permisos a roles y asignar roles a grupos de usuarios administrativos, lo que aplica qué tareas se permite que lleven a cabo los clientes administrativos desde la interfaz de usuario de gestión como las API.	Permite a los administradores de Grid gestionar el control de acceso de usuarios y grupos administradores.	—

Función	Función	Impacto	Cumplimiento de normativas
Registro de auditorías distribuido	StorageGRID ofrece una infraestructura de registro de auditorías incorporada y distribuida que se puede ampliar a cientos de nodos en hasta 16 sitios. Los nodos de software de StorageGRID generan mensajes de auditoría, que se transmiten a través de un sistema de retransmisión de auditoría redundante y, en última instancia, se capturan en uno o más repositorios de registros de auditoría. Eventos de captura de mensajes de auditoría con una granularidad a nivel de objeto, como operaciones de API S3 iniciadas por el cliente, eventos de ciclo de vida de los objetos por ILM, comprobaciones del estado de los objetos en segundo plano y cambios de configuración realizados desde las API o la interfaz de usuario de gestión. Los registros de auditoría se pueden exportar mediante syslog, lo que permite que los mensajes de auditoría se puedan extraer mediante herramientas como Splunk y ELK. Hay cuatro tipos de mensajes de auditoría: • Mensajes de auditoría del sistema • Mensajes de auditoría del almacenamiento de objetos • Mensajes de auditoría de protocolo HTTP • Mensajes de auditoría de gestión Los registros de auditoría se pueden almacenar en un depósito S3 para su retención a largo plazo y acceso a las aplicaciones.	Proporciona a los administradores de Grid un servicio de auditoría probado y escalable y les permite extraer datos de auditoría para diversos objetivos. Entre estos objetivos se incluyen la solución de problemas, la auditoría del rendimiento del SLA, las operaciones de API de acceso a los datos del cliente y los cambios en la configuración de gestión.	—

Función	Función	Impacto	Cumplimiento de normativas
Auditoría del sistema	Los mensajes de auditoría del sistema capturan eventos relacionados con el sistema, como los estados de nodo de grid, la detección de objetos dañados, los objetos comprometidos en todas las ubicaciones especificadas por regla de ILM y el progreso de las tareas de mantenimiento en todo el sistema (tareas de grid).	Ayuda a los clientes a solucionar problemas del sistema y ofrece pruebas de que los objetos se almacenan según su acuerdo de nivel de servicio. Los acuerdos de nivel de servicio se implementan mediante reglas de ILM de StorageGRID y están protegidos para la integridad.	—
Auditoría de almacenamiento de objetos	Los mensajes de auditoría del almacenamiento de objetos capturan los eventos relacionados con el ciclo de vida y las transacciones de la API del objeto. Entre estos eventos se incluyen almacenamiento y recuperación de objetos, transferencias de grid-nodo a grid-nodo y verificaciones.	Ayuda a los clientes a auditar el progreso de los datos a través del sistema y si se están entregando el SLA, especificado como gestión del ciclo de vida de la información de StorageGRID.	—
Auditoría de protocolo HTTP	Los mensajes de auditoría del protocolo HTTP capturan las interacciones del protocolo HTTP relacionadas con las aplicaciones cliente y los nodos StorageGRID. Además, los clientes pueden capturar encabezados de solicitud HTTP específicos (como X-forward-for y metadatos de usuario [x-amz-meta-*]) en la auditoría.	Ayuda a los clientes a auditar las operaciones de API de acceso a los datos entre clientes y StorageGRID, y rastrea una acción en una cuenta de usuario individual y una clave de acceso. Los clientes también pueden registrar metadatos de usuario en auditorías y utilizar herramientas de extracción de registros como Splunk o ELK para buscar metadatos de objetos.	—
Auditoría de gestión	Los mensajes de auditoría de gestión registran las solicitudes del usuario administrador a las API o la interfaz de usuario de gestión (Grid Management Interface). Cada solicitud que no sea UNA solicitud GET o HEAD a la API registra una respuesta con el nombre de usuario, la IP y el tipo de solicitud a la API.	Ayuda a los administradores de Grid a establecer un registro de los cambios de configuración del sistema realizados por cada usuario desde qué IP de origen y qué IP de destino en qué momento.	—

Función	Función	Impacto	Cumplimiento de normativas
Soporte de TLS 1,3 para el acceso a la API e IU de gestión	TLS establece un protocolo de apretón de manos para la comunicación entre un cliente de administrador y un nodo de administrador de StorageGRID.	Permite a un cliente administrativo y a StorageGRID identificarse y autenticarse entre sí, y comunicarse con confidencialidad e integridad de los datos.	—
SNMPv3 para la supervisión de StorageGRID	SNMPv3 ofrece seguridad al ofrecer autenticación sólida y cifrado de datos para mayor privacidad. Con v3, las unidades de datos de protocolo se cifran, utilizando CBC-DES para su protocolo de cifrado. La autenticación de usuario de quién envió la unidad de datos de protocolo se proporciona mediante el protocolo de autenticación HMAC-SHA o HMAC-MD5. SNMPv2 y v1 siguen siendo compatibles.	Ayuda a los administradores de grid a supervisar el sistema StorageGRID mediante la activación de un agente SNMP en el nodo de administración.	—
Certificados de cliente para la exportación de métricas Prometheus	Los administradores de grid pueden cargar o generar certificados de cliente que se pueden utilizar para proporcionar acceso seguro y autenticado a la base de datos de StorageGRID Prometheus.	Los administradores de grid pueden utilizar certificados de cliente para supervisar StorageGRID externamente con aplicaciones como Grafana.	—

Funciones de seguridad de la plataforma

Obtenga más información sobre las características de seguridad de la plataforma en StorageGRID.

Función	Función	Impacto	Cumplimiento de normativas
Infraestructura de clave pública interna (PKI), certificados de nodo y TLS	StorageGRID utiliza una PKI interna y certificados de nodo para autenticar y cifrar la comunicación entre nodos. La comunicación entre nodos está protegida por TLS.	Ayuda a proteger el tráfico del sistema a través de LAN o WAN, especialmente en una implementación multisitio.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Función	Función	Impacto	Cumplimiento de normativas
Firewall de nodo	StorageGRID configura automáticamente tablas IP y reglas de firewall para controlar el tráfico de red entrante y saliente, así como para cerrar los puertos no utilizados.	Ayuda a proteger el sistema de StorageGRID, los datos y los metadatos frente al tráfico de red no solicitado.	—
Endurecimiento del SO	El sistema operativo básico de dispositivos físicos StorageGRID y nodos virtuales está reforzado; se eliminan los paquetes de software no relacionados.	Ayuda a minimizar posibles superficies de ataque.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Actualizaciones periódicas de la plataforma y del software	StorageGRID proporciona versiones regulares de software que incluyen sistemas operativos, binarios de aplicaciones y actualizaciones de software.	Ayuda a mantener el sistema StorageGRID actualizado con los binarios de software y aplicaciones actuales.	—
Inicio de sesión raíz desactivado a través de shell seguro (SSH)	El inicio de sesión raíz a través de SSH está deshabilitado en todos los nodos StorageGRID. El acceso SSH utiliza autenticación de certificados.	Ayuda a los clientes a protegerse contra posibles fallos remotos de contraseña del inicio de sesión root.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Sincronización de tiempo automatizada	StorageGRID sincroniza automáticamente los relojes del sistema de cada nodo en varios servidores de protocolo de tiempo de redes de tiempo (NTP) externos. Se requieren al menos cuatro servidores NTP de estrato 3 o posterior.	Asegura la misma referencia de tiempo en todos los nodos.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Redes independientes para el tráfico de grid interno, de administración y de clientes	Los nodos de software y los dispositivos de hardware de StorageGRID admiten múltiples interfaces de red físicas y virtuales, para que los clientes puedan separar el tráfico de grid interno, de administración y de clientes en diferentes redes.	Permita a los administradores de Grid segregar el tráfico de red interno y externo y distribuir tráfico a través de redes con diferentes SLA.	—

Función	Función	Impacto	Cumplimiento de normativas
Varias interfaces de LAN virtual (VLAN)	StorageGRID admite la configuración de interfaces VLAN en sus redes de grid y cliente de StorageGRID.	Permita que los administradores de Grid dividan y aíslen el tráfico de aplicaciones para mejorar la seguridad, la flexibilidad y el rendimiento.	
Red cliente no confiable	La interfaz de red de cliente no confiable acepta conexiones entrantes solo en puertos que se han configurado explícitamente como puntos finales de equilibrio de carga.	Garantiza que las interfaces expuestas a redes que no son de confianza estén protegidas.	—
Firewall configurable	Gestionar puertos abiertos y cerrados para redes de administración, grid y cliente.	Permitir a los administradores de grid controlar el acceso a los puertos y administrar el acceso de dispositivos aprobados a los puertos.	
Comportamiento SSH mejorado	Deshabilitar SSH de forma predeterminada antes de la instalación. En el estado predeterminado, el acceso SSH solo está habilitado en la dirección de los puertos de administración local del enlace. Las contraseñas de usuario administrador y raíz se establecen en el número de serie del controlador de cómputo del dispositivo. El inicio de sesión solo está permitido en la consola serie y en la consola gráfica (BMC KVM). SSH en cualquier puerto de red está deshabilitado.	Mejora la protección del acceso a la red.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)
Cifrado de nodos	Como parte de la nueva función de cifrado del servidor host KMS, se agrega una nueva configuración de cifrado de nodos al instalador de dispositivos StorageGRID.	Este ajuste se debe activar durante la etapa de configuración de hardware de la instalación del dispositivo.	Normativa SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regla 4511(c)

Integración del cloud

Comprende cómo StorageGRID se integra con los servicios en nube.

Función	Función	Impacto
Detección de virus basada en notificaciones	Los servicios de la plataforma StorageGRID admiten notificaciones de eventos. Las notificaciones de eventos se pueden usar con servicios de cloud computing externos para activar flujos de trabajo de análisis de virus en los datos.	Permite a los administradores inquilinos activar el análisis de virus de los datos mediante servicios de cloud computing externos.

TR-4921: Defensa contra ransomware

Protege objetos de StorageGRID S3 contra el ransomware

Obtén más información sobre los ataques de ransomware y cómo proteger los datos con las prácticas recomendadas de seguridad de StorageGRID.

Los ataques de ransomware están en auge. Este documento proporciona algunas recomendaciones sobre cómo proteger los datos de objetos en StorageGRID.

Hoy en día, el ransomware es el peligro siempre presente en los centros de datos. El ransomware está diseñado para cifrar datos y dejarlos inutilizables por los usuarios y las aplicaciones que dependen de ellos. La protección comienza con las defensas habituales de las redes reforzadas y las prácticas de seguridad de usuario sólidas, y tenemos que seguir con las prácticas de seguridad de acceso a los datos.

El ransomware es una de las mayores amenazas de seguridad de hoy en día. El equipo de NetApp StorageGRID está trabajando con nuestros clientes para mantenerse a la cabeza de estas amenazas. Con el uso de bloqueo de objetos y control de versiones, puede protegerse frente a alteraciones no deseadas y recuperarse de ataques maliciosos. La seguridad de datos es una aventura de múltiples capas, donde tu almacenamiento de objetos es solo una parte del centro de datos.

Mejores prácticas de StorageGRID

Para StorageGRID, las prácticas recomendadas de seguridad deben incluir el uso de HTTPS con certificados firmados tanto para la gestión como para el acceso a los objetos. Cree cuentas de usuario dedicadas para aplicaciones e individuos, y no utilice las cuentas raíz de inquilino para el acceso a aplicaciones o el acceso a los datos de usuario. En otras palabras, siga el principio de privilegio mínimo. Utilice grupos de seguridad con directivas de gestión de acceso e identidad definidas (IAM) para controlar los derechos de usuario y acceder a cuentas específicas de las aplicaciones y los usuarios. Con estas medidas, aún debe asegurarse de que los datos estén protegidos. En el caso de Simple Storage Service (S3), cuando se modifican objetos para cifrarlos, se realiza mediante una sobrescritura del objeto original.

Métodos de defensa

El principal mecanismo de protección contra ransomware en la API S3 es implementar el bloqueo de objetos. No todas las aplicaciones son compatibles con el bloqueo de objetos, por lo que hay otras dos opciones para proteger los objetos que se describen en este informe: Replicación a otro depósito con control de versiones activado y control de versiones con políticas de IAM.

Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

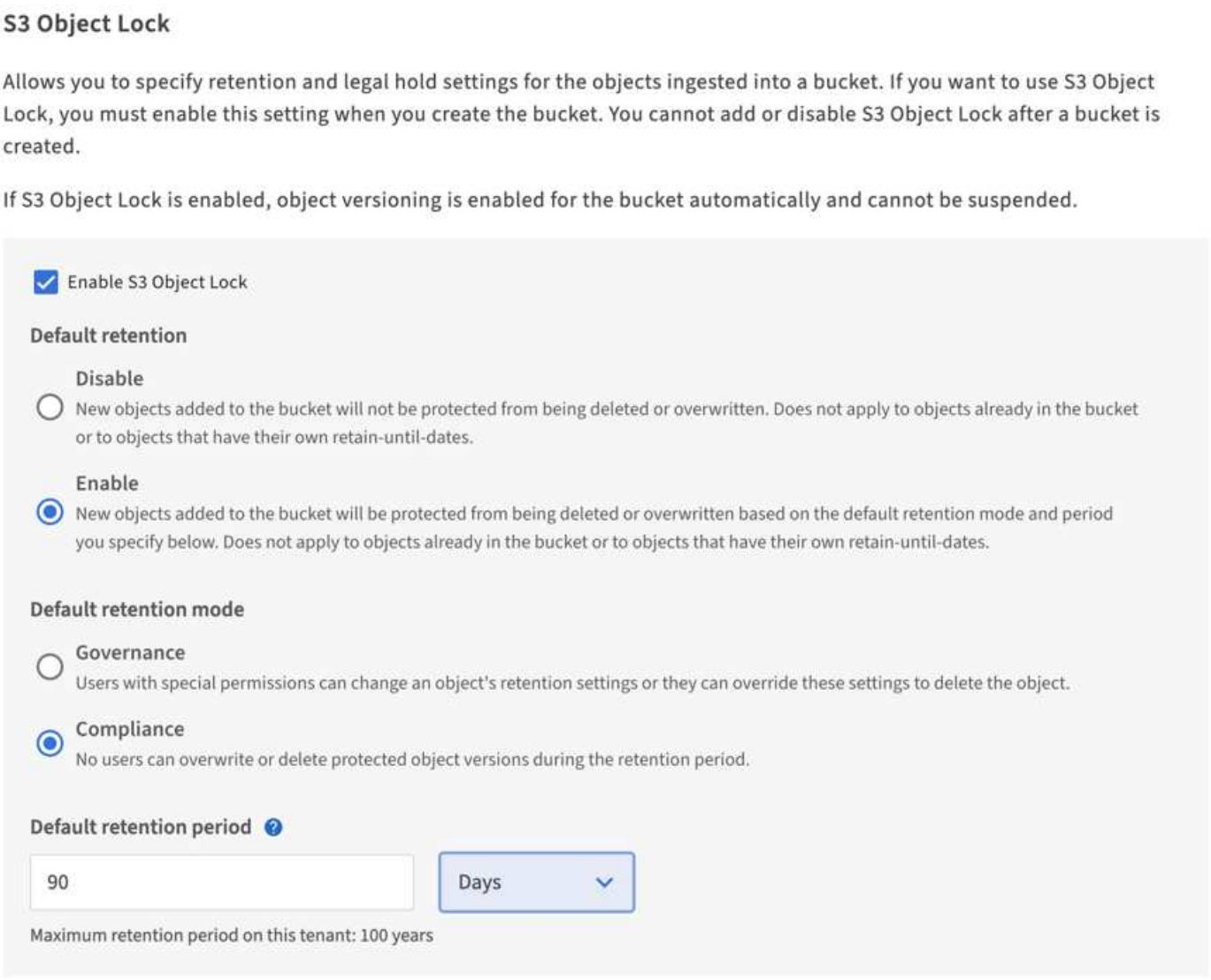
- Centro de documentación de NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

Defensa contra ransomware mediante bloqueo de objetos

Explore cómo el bloqueo de objetos en StorageGRID ofrece un MODELO WORM para evitar la eliminación o sobrescritura de datos y cómo cumple con los requisitos normativos.

El bloqueo de objetos proporciona un MODELO WORM para evitar que se eliminen o se sobrescriban objetos. La implementación de StorageGRID del bloqueo de objetos es "Cohasset evaluado" para ayudar a cumplir los requisitos normativos, dar soporte a la conservación legal, el modo de cumplimiento de normativas y el modo de gobierno para la retención de objetos y las políticas de retención de bloques predeterminadas. Debe habilitar el bloqueo del objeto como parte de la creación y el control de versiones del bloque. Se bloquea una versión específica de un objeto y, si no se define ningún ID de versión, la retención se coloca en la versión actual del objeto. Si la versión actual tiene la retención configurada y se intenta suprimir, modificar o sobrescribir el objeto, se crea una nueva versión con un marcador de supresión o la nueva revisión del objeto como la versión actual, y la versión bloqueada se conserva como una versión no actual. Para las aplicaciones que aún no son compatibles, es posible que pueda seguir usando el bloqueo de objetos y una configuración de retención predeterminada ubicada en el bloque. Una vez definida la configuración, esto aplica una retención de objetos a cada nuevo objeto puesto en el bloque. Esto funciona siempre que la aplicación esté configurada para no eliminar ni sobrescribir los objetos antes de que haya pasado el tiempo de retención.

Al crear un depósito en la interfaz de usuario de administración de inquilinos, puede habilitar el bloqueo de objetos y configurar un modo de retención y un período de retención predeterminados. Cuando se configura esto, se establecerá una retención de bloqueo de objeto mínima en cada objeto que se ingiera en ese depósito.



A continuación, se muestran algunos ejemplos que utilizan la API de bloqueo de objetos:

La retención legal de bloqueo de objeto es un estado simple de activación/desactivación aplicado a un objeto.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

Si se establece el estado de retención legal, no se devuelve ningún valor si se realiza correctamente, por lo que se puede verificar con una OPERACIÓN GET.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Para desactivar la retención legal, aplique el estado OFF.

```
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"
    }
}
```

La configuración de la retención de objetos se realiza con una marca de tiempo Retain until.

```
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
```

Una vez más, no hay valor devuelto en el éxito, por lo que puede verificar el estado de retención de manera similar con una llamada GET.

```
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"
    }
```

Al colocar una retención predeterminada en un bloque habilitado para el bloqueo de objetos, se utiliza un período de retención en días y años.

```
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
```

Al igual que con la mayoría de estas operaciones, no se devuelve ninguna respuesta al éxito, por lo que podemos realizar un GET para que la configuración se verifique.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

A continuación, puede colocar un objeto en el depósito con la configuración de retención aplicada.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

La operación PUT devuelve una respuesta.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

En el objeto de retención, la duración de retención definida en el bloque en el ejemplo anterior se convierte en una marca de tiempo de retención en el objeto.

```
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"
    }
}
```

Protección contra ransomware mediante bloque replicado con control de versiones

Descubre cómo replicar objetos en un bloque secundario mediante CloudMirror de StorageGRID.

No todas las aplicaciones y cargas de trabajo serán compatibles con el bloqueo de objetos. Otra opción es replicar los objetos en un depósito secundario, ya sea en la misma cuadrícula (preferiblemente un inquilino diferente con acceso restringido), o cualquier otro extremo S3 con el servicio de plataforma StorageGRID,

CloudMirror.

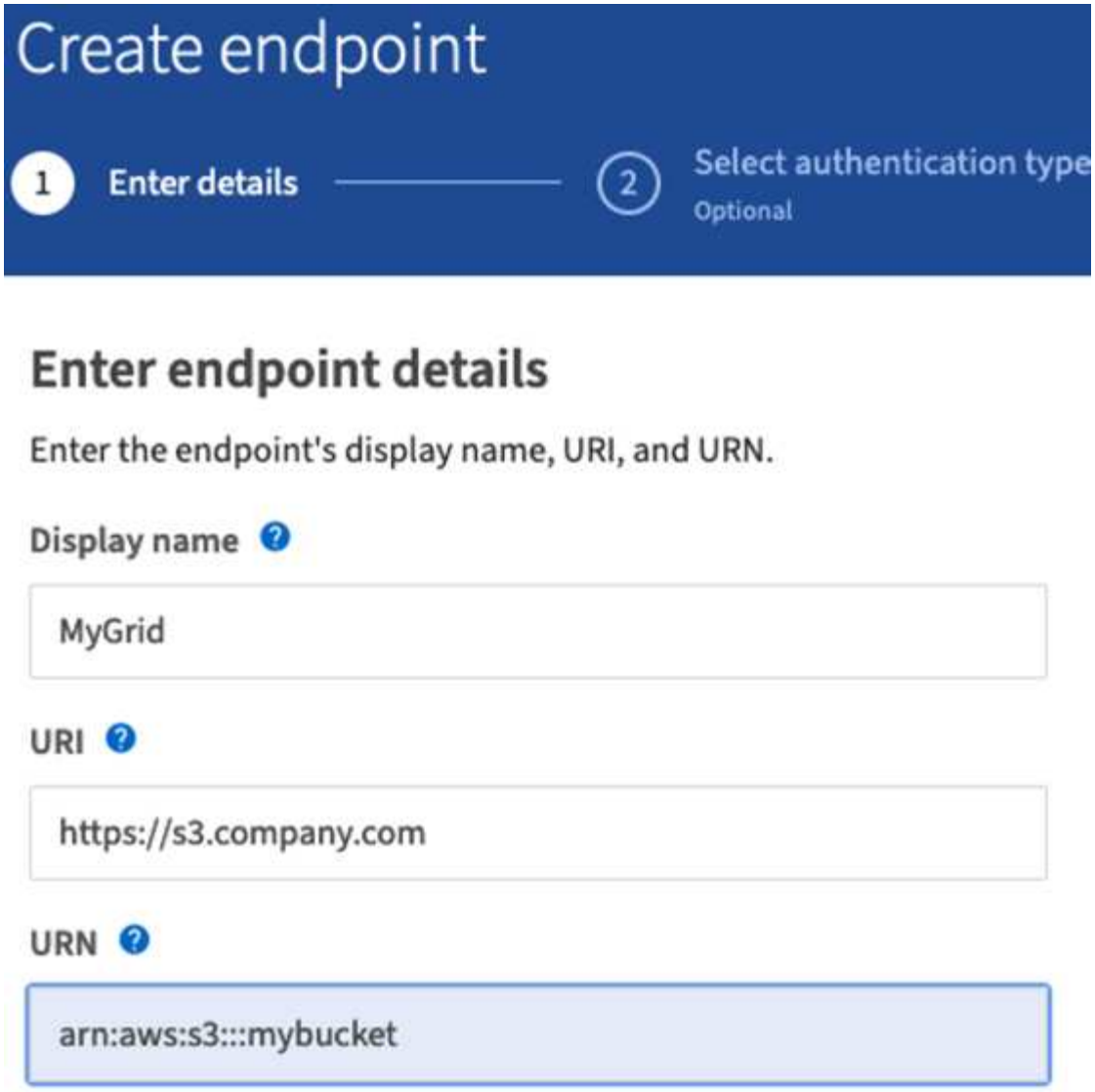
StorageGRID CloudMirror es un componente de StorageGRID que se puede configurar para replicar los objetos de un bucket en un destino definido a medida que se ingieren en el bloque de origen y no replica los eliminaciones. Puesto que CloudMirror es un componente integrado de StorageGRID, no se puede desactivar ni manipular mediante un ataque basado en API S3. Puede configurar este bucket replicado con el control de versiones activado. En este escenario, necesita una limpieza automática de las versiones antiguas del depósito replicado que son seguras de descartar. Para ello, puede utilizar el motor de políticas de gestión de la vida útil de la información de StorageGRID. Cree reglas para administrar la ubicación del objeto en función del tiempo no corriente durante varios días suficientes para identificarse y recuperarse de un ataque.

Un inconveniente de este enfoque es que consume más almacenamiento al disponer de una segunda copia completa del bloque y varias versiones de los objetos que se conservan durante cierto tiempo. Además, los objetos que se eliminaron intencionalmente del bloque primario deben eliminarse manualmente del bloque replicado. Hay otras opciones de replicación fuera del producto, como NetApp CloudSync, que pueden replicar eliminaciones para una solución similar. Otra desventaja para el bucket secundario que está activado el control de versiones y no el bloqueo de objetos activado es que existe una serie de cuentas con privilegios que se pueden utilizar para causar daños en la ubicación secundaria. La ventaja es que debe ser una cuenta única para ese extremo o bloque de inquilinos y es probable que el compromiso no incluya el acceso a las cuentas en la ubicación principal o viceversa.

Después de crear los buckets de origen y de destino y de configurar el destino con el control de versiones, puede configurar y habilitar la replicación del siguiente modo:

Pasos

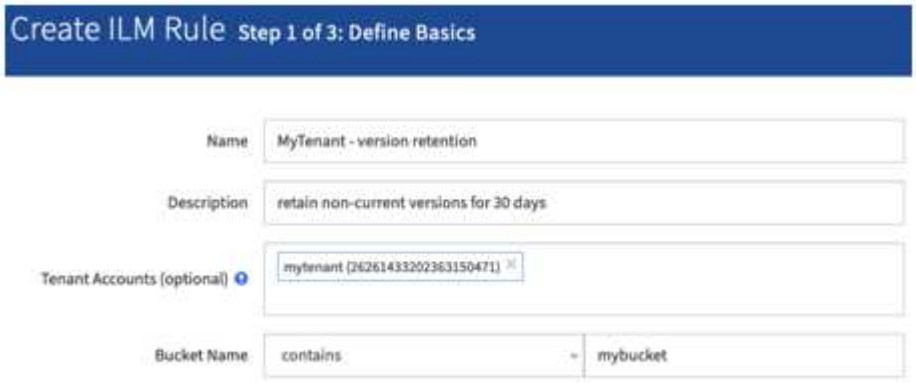
1. Para configurar CloudMirror, cree un punto final de servicios de plataforma para el destino S3.

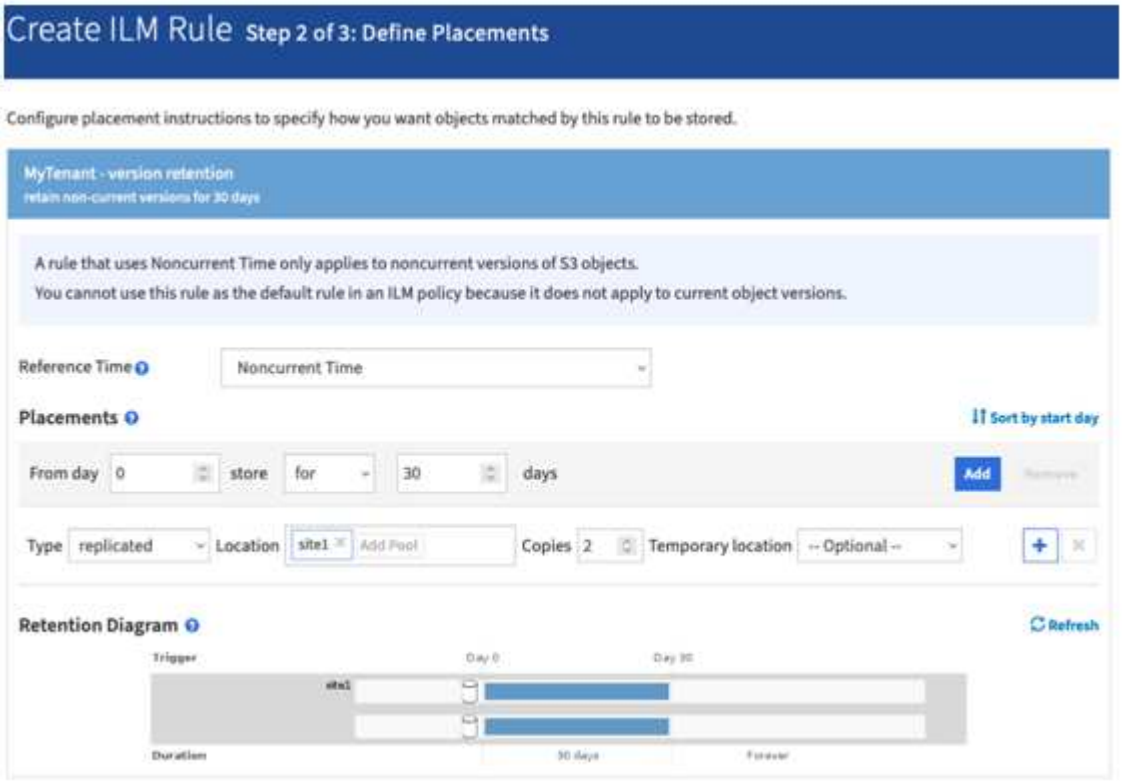


2. En el bloque de origen, configure la replicación para usar el punto final configurado.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Cree reglas de ILM para gestionar la ubicación del almacenamiento y la gestión de la duración del almacenamiento de versiones. En este ejemplo, se configuran las versiones no actuales de los objetos que se van a almacenar.





Hay dos copias en el sitio 1 durante 30 días. También configura las reglas para la versión actual de los objetos en función de usar el tiempo de ingesta como tiempo de referencia en la regla de ILM para que coincida con la duración del almacenamiento del bloque de origen. La ubicación del almacenamiento para las versiones de objetos puede codificarse para el borrado o replicarse.

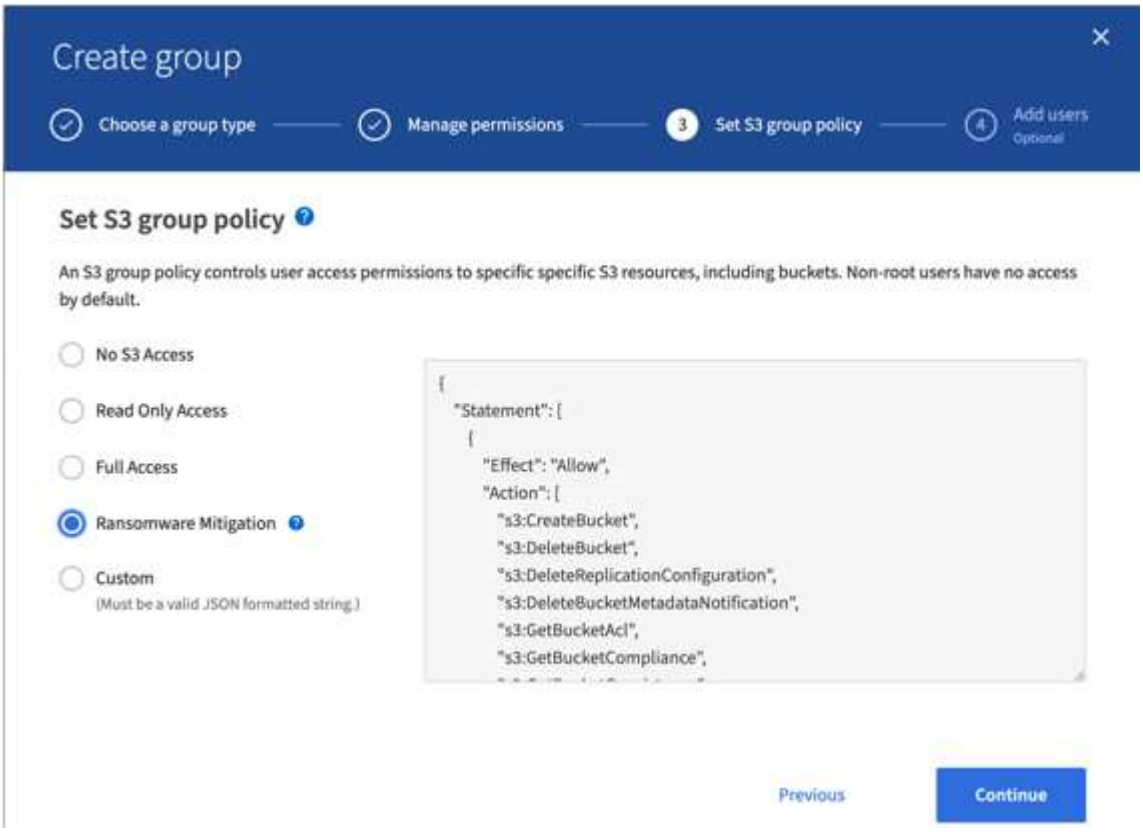
Protección frente al ransomware mediante el control de versiones con la política de protección IAM

Aprenda a proteger sus datos habilitando el control de versiones en el bloque e implementando políticas de IAM en grupos de seguridad de usuarios en StorageGRID.

Un método para proteger los datos sin utilizar el bloqueo de objetos o la replicación consiste en habilitar el control de versiones en el bloque e implementar políticas de IAM en los grupos de seguridad de usuarios para limitar la capacidad de los usuarios de administrar versiones de los objetos. En caso de un ataque, se crean nuevas versiones erróneas de los datos como la versión actual, y la versión no actual más reciente son los

datos limpios seguros. Las cuentas comprometidas para obtener acceso a los datos no tienen acceso para eliminar o alterar de otro modo la versión no actual que los protege para operaciones de restauración posteriores. Al igual que en la situación anterior, las reglas de ILM gestionan la retención de las versiones no actualizadas con el tiempo que elija. El inconveniente es que todavía existe la posibilidad de que existan cuentas privilegiadas para un ataque de agente malicioso, pero todas las cuentas de servicio de aplicaciones y los usuarios deben configurarse con un acceso más restrictivo. La política de grupo restrictivo debe permitir explícitamente que cada acción que desee que los usuarios o la aplicación sean capaces de rechazar y de forma explícita cualquier acción que no desee que sean capaces de realizar. NetApp no recomienda utilizar un comodín Permitir porque se puede introducir una nueva acción en el futuro y se quiere controlar si se permite o se rechaza. Para esta solución, la lista de denegación debe incluir DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration y PutBucketVersioning para proteger la configuración de versiones del bucket y las versiones del objeto de los cambios programáticos o del usuario.

En StorageGRID , la opción de política de grupo S3 “Mitigación de ransomware” facilita la implementación de esta solución. Al crear un grupo de usuarios en el inquilino, después de seleccionar los permisos del grupo, puede ver esta política opcional.



A continuación se muestra el contenido de la política de grupo que incluye la mayoría de las operaciones disponibles explícitamente permitidas y el mínimo requerido denegado.

```
{
    "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:::*"
        }
    ]
}
```

Investigación y remediación de ransomware

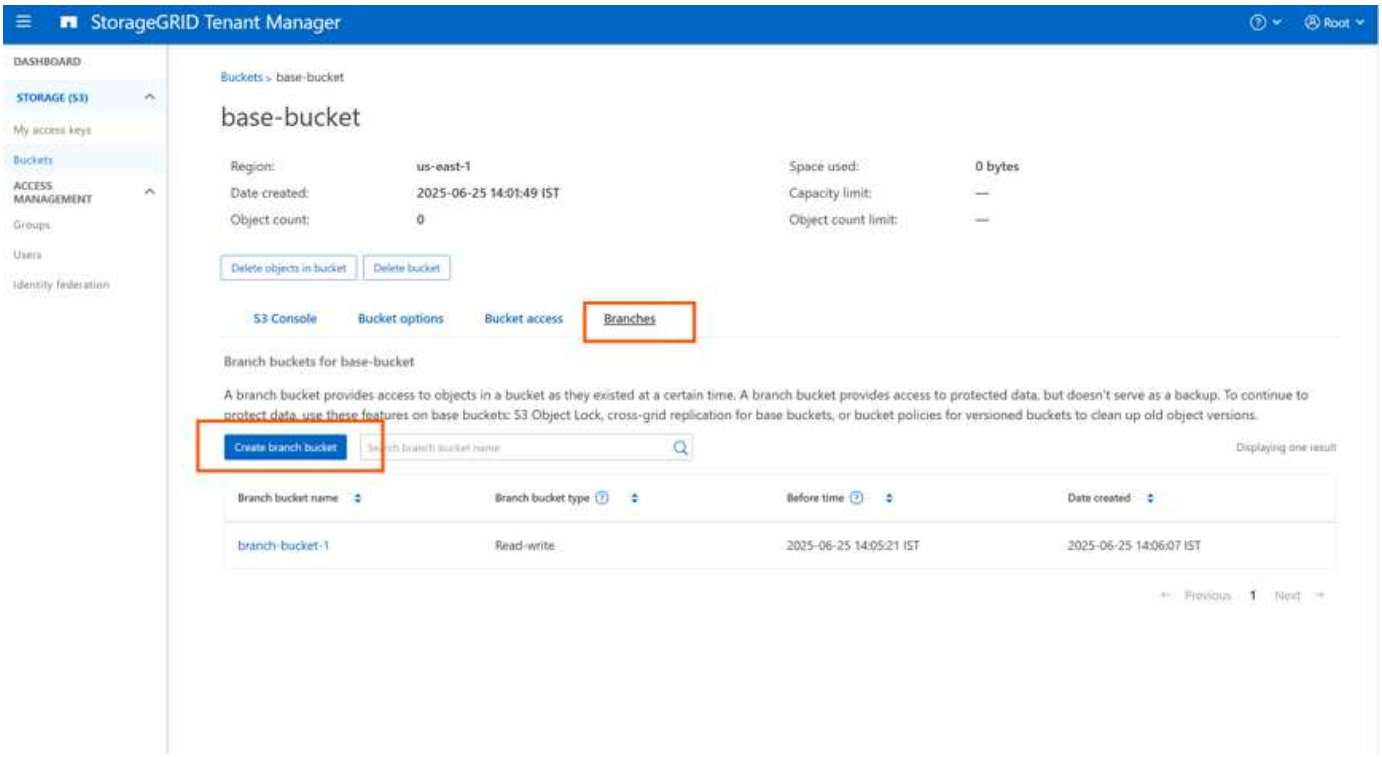
Aprenda a investigar y remediar buckets después de un posible ataque de ransomware con StorageGRID.

En StorageGRID 12.0, se agregó la nueva función de depósito de ramas para ampliar la utilidad del control de versiones para la defensa contra ransomware. Un bucket de rama proporciona acceso a los objetos de un bucket tal como existían en un momento determinado, siempre que todavía existan en el bucket. Los depósitos de ramas solo se pueden crear para depósitos base con control de versiones habilitado.

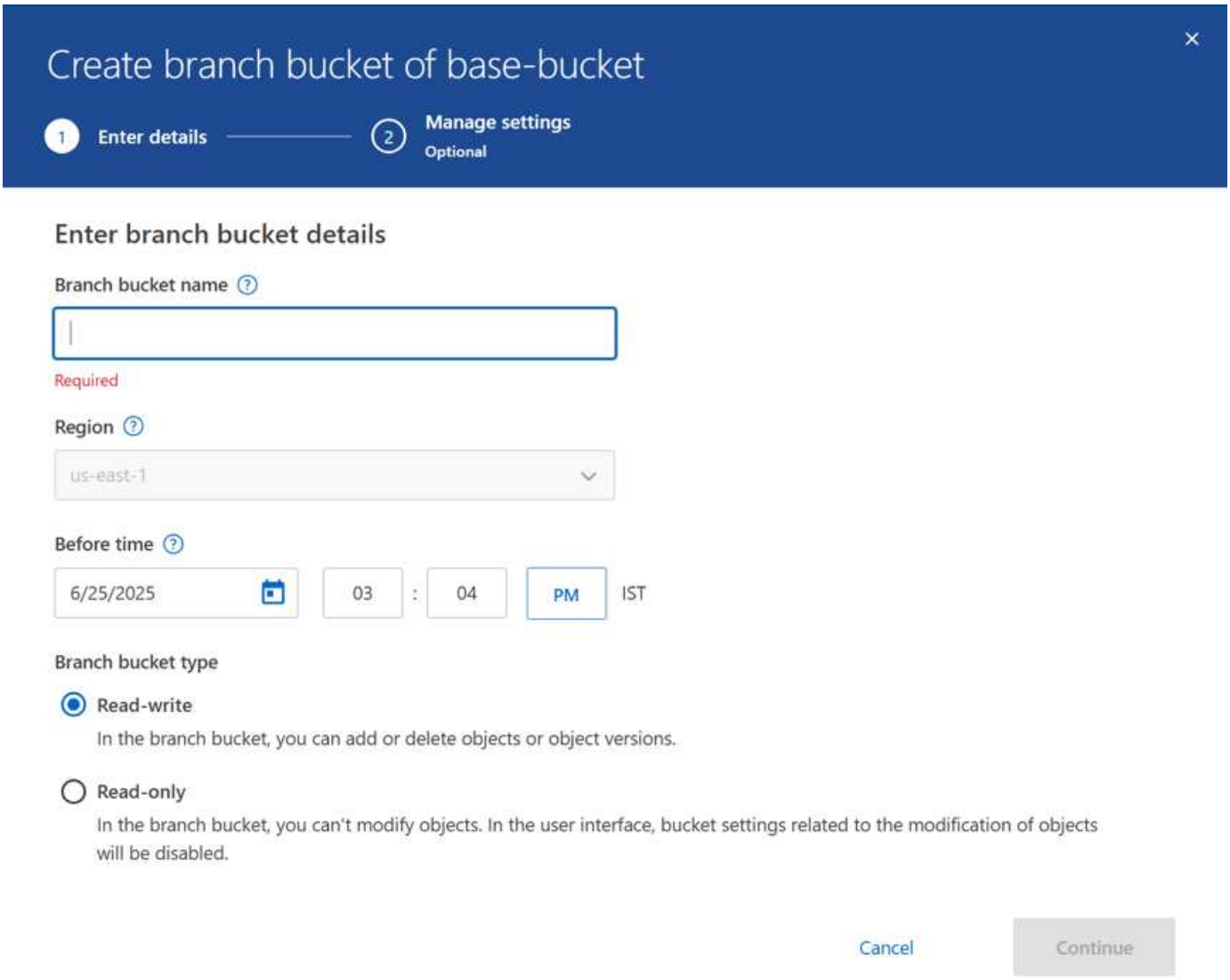
Esto significa que si sospecha que se ha producido un ataque de ransomware, puede crear un depósito de ramas de lectura y escritura, o de solo lectura, que contenga todos los objetos y versiones que existían antes del momento del ataque inicial. Puede utilizar esta rama del depósito para comparar con el contenido del depósito base para determinar qué objetos han cambiado y si el cambio fue parte del ataque o no. También puede utilizar una rama bucket para continuar las operaciones del cliente utilizando la rama limpia mientras investiga el ataque.

Creación de un depósito de rama

- Vaya a la página de detalles del depósito base y a la pestaña Ramas para crear un depósito de ramas.



- Una vez que se hace clic en el botón Crear rama, se abrirá una ventana emergente con detalles predefinidos de la región asociada con el ramal base.
- Proporcione el nombre de la rama, con anticipación, y seleccione qué tipo de rama desea crear.



TR-4765: Monitor StorageGRID

Introducción a la supervisión StorageGRID

Descubra cómo supervisar su sistema StorageGRID mediante aplicaciones externas, como Splunk.

La supervisión eficaz del almacenamiento basado en objetos de NetApp StorageGRID permite a los administradores responder rápidamente a problemas urgentes y añadir recursos de forma proactiva para gestionar las cargas de trabajo crecientes. Este informe proporciona orientación general sobre cómo supervisar las métricas clave y cómo aprovechar las aplicaciones de supervisión externas. Está diseñado para complementar la guía de monitorización y solución de problemas existente.

Una puesta en marcha de NetApp StorageGRID suele constar de varios sitios y muchos nodos que funcionan para crear un sistema de almacenamiento de objetos distribuido y tolerante a fallos. En un sistema de almacenamiento distribuido y resiliente como StorageGRID, es normal que existan condiciones de error mientras el grid sigue funcionando correctamente. El reto para usted como administrador es comprender el umbral en el que las condiciones de error (como nodos de inactividad) presentan un problema que debe abordarse inmediatamente frente a la información que debe analizarse. Al analizar los datos que presenta

StorageGRID, puede comprender su carga de trabajo y tomar decisiones fundamentadas, como cuándo se deben agregar más recursos.

StorageGRID ofrece una excelente documentación que se centra en el tema de la supervisión. En este informe se asume que está familiarizado con StorageGRID y que ha revisado la documentación sobre él. En lugar de repetir esta información, consulte la documentación del producto que figura en esta guía. La documentación de los productos de StorageGRID está disponible en línea y en formato PDF.

El objetivo de este documento es complementar la documentación del producto y tratar la forma de supervisar el sistema de StorageGRID mediante aplicaciones externas como Splunk.

Orígenes de datos

Para supervisar correctamente NetApp StorageGRID, es importante saber dónde recopilar datos sobre el estado y las operaciones de su sistema StorageGRID.

- **Web UI y Dashboard.** StorageGRID Grid Manager presenta una vista de nivel superior de la información que usted, como administrador, necesita ver en una presentación lógica. Como administrador, también puede profundizar en la información de los niveles de servicio para la solución de problemas y la recopilación de registros.
- **Registros de auditoría.** StorageGRID mantiene registros de auditoría granulares de acciones de inquilinos, como PONER, OBTENER y ELIMINAR. También puede realizar el seguimiento del ciclo de vida de un objeto desde la ingesta hasta la aplicación de las reglas de gestión de datos.
- **API de métricas.** Subyacentes al GMI de StorageGRID son API abiertas, ya que la IU está condicionada por API. Este enfoque le permite extraer datos mediante herramientas externas de supervisión y análisis.

Dónde encontrar información adicional

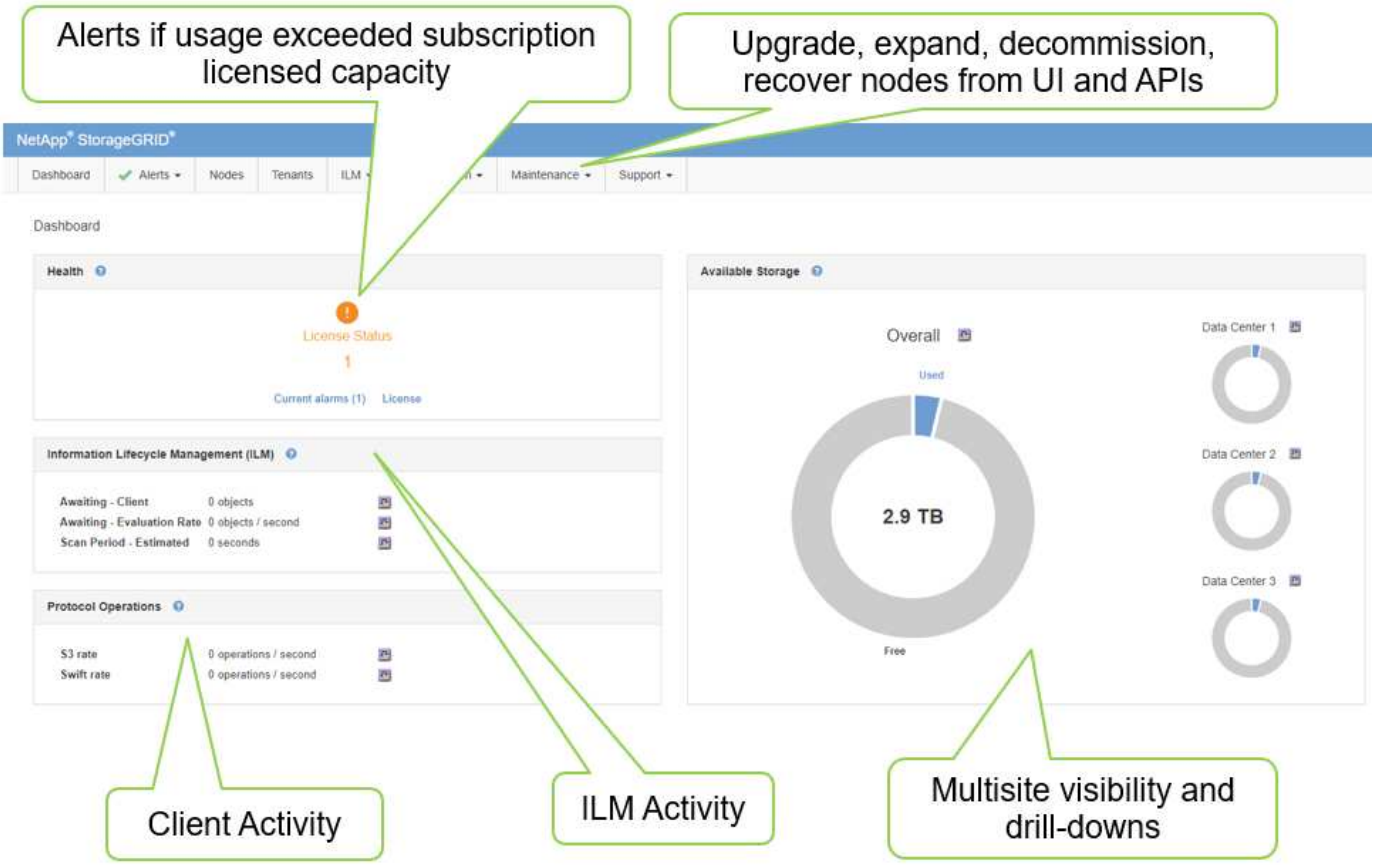
Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Centro de documentación de NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/
- Aplicación de NetApp StorageGRID para Splunk https://splunkbase.splunk.com/app/3898/#/details

Utilice el panel de control de GMI para supervisar StorageGRID

El panel de la interfaz de gestión de grid (GMI) de StorageGRID proporciona una vista centralizada de la infraestructura de StorageGRID, lo que permite supervisar el estado, el rendimiento y la capacidad de todo el grid.

Utilice el panel de control de GMI para examinar cada componente principal de la cuadrícula.



Información que debe controlar regularmente

En una versión anterior de este informe técnico se indicaban las métricas que se debían comprobar periódicamente frente a las tendencias. Esa información ahora está incluida en el "Guía de supervisión y solución de problemas".

Supervisión del almacenamiento

Una versión anterior de este informe técnico muestra dónde supervisar métricas importantes, como espacio de almacenamiento de objetos, espacio de metadatos, recursos de red, etc. Esa información ahora está incluida en el "Guía de supervisión y solución de problemas".

Utilice alertas para supervisar StorageGRID

Aprenda a usar el sistema de alertas en StorageGRID para supervisar problemas, gestionar alertas personalizadas y ampliar las notificaciones de alertas con SNMP o correo electrónico.

Las alertas proporcionan información crítica que le permite supervisar los diversos eventos y condiciones del sistema StorageGRID.

El sistema de alertas está diseñado para ser la herramienta principal para supervisar cualquier problema que se pueda producir en el sistema StorageGRID. El sistema de alertas se centra en problemas prácticos en el sistema y ofrece una interfaz fácil de usar.

Proporcionamos una variedad de reglas de alerta predeterminadas que tienen como objetivo ayudar a supervisar y solucionar problemas de su sistema. Para gestionar aún más las alertas, puede editar o

deshabilitar alertas predeterminadas y silenciar las notificaciones de alertas.

Las alertas también se pueden ampliar mediante SNMP o notificaciones por correo electrónico.

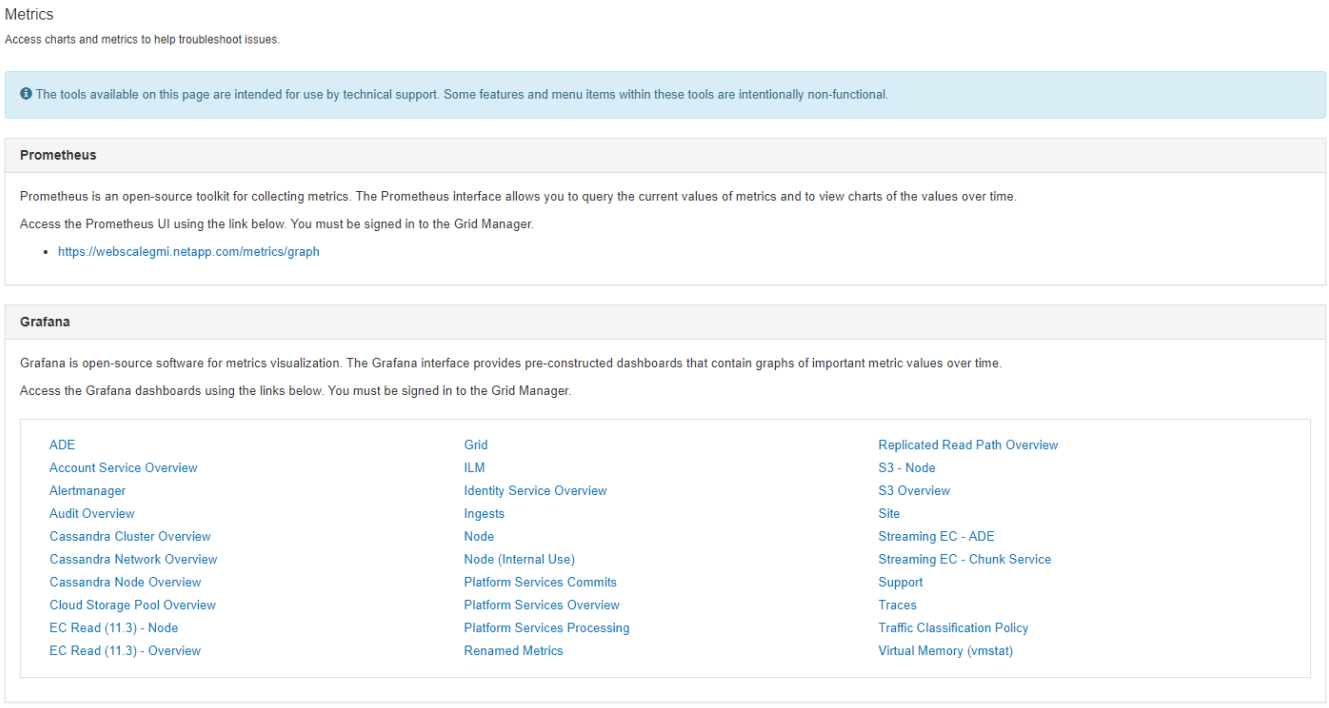
Para obtener más información sobre las alertas, consulte el documento "documentación de productos" disponible en línea y en formato PDF.

Supervisión avanzada en StorageGRID

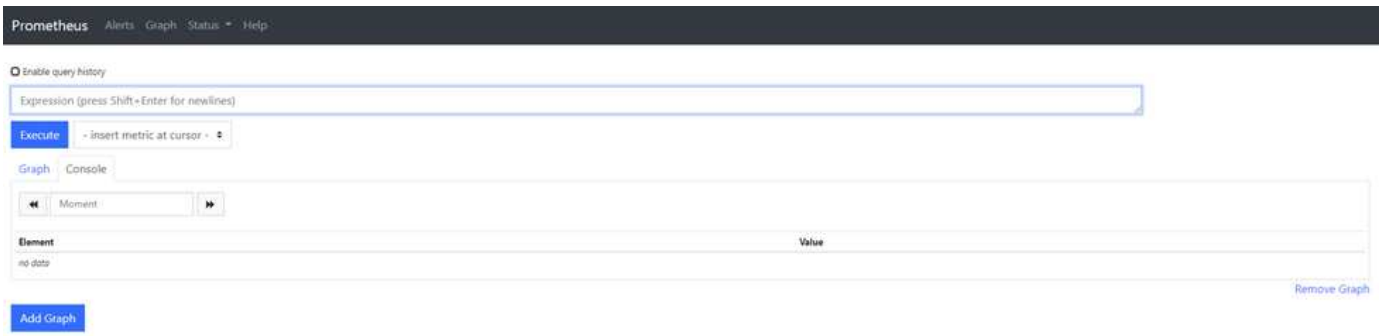
Aprenda a acceder y exportar métricas para ayudar a resolver problemas.

Permite ver la API de métricas a través de una consulta de Prometheus

Prometheus es un software de código abierto para recopilar métricas. Para acceder a Prometheus integrado de StorageGRID mediante la GMI, vaya a MENU:Soporte[Métricas].



Como alternativa, puede navegar directamente al enlace.

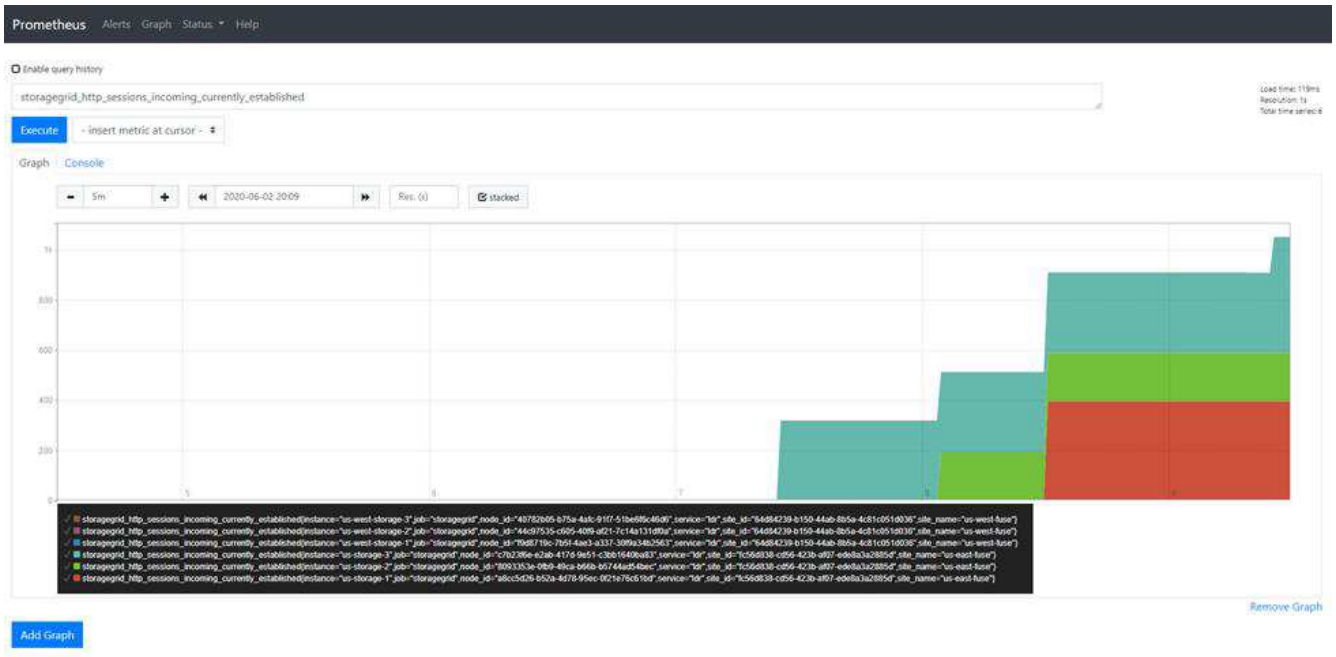


Con esta vista, puede acceder a la interfaz de Prometheus. Desde ahí, podrá buscar en las métricas disponibles e incluso experimentar con consultas.

Para realizar una consulta de URL de Prometheus, siga estos pasos:

Pasos

1. Comience a escribir en el cuadro de texto de la consulta. A medida que escribe, se muestran las métricas. Para nuestros propósitos, solo las métricas que comienzan con StorageGRID y Node son importantes.
2. Para ver el número de sesiones HTTP de cada nodo, escriba `storagegrid_http` y seleccione `storagegrid_http_sessions_incoming_currently_established`. Haga clic en Ejecutar y muestre la información en formato de gráfico o consola.



Las consultas y los gráficos que se crean a través de esta URL no persisten. Las consultas complejas consumen recursos en el nodo de administración. NetApp recomienda utilizar esta vista para explorar las métricas disponibles.

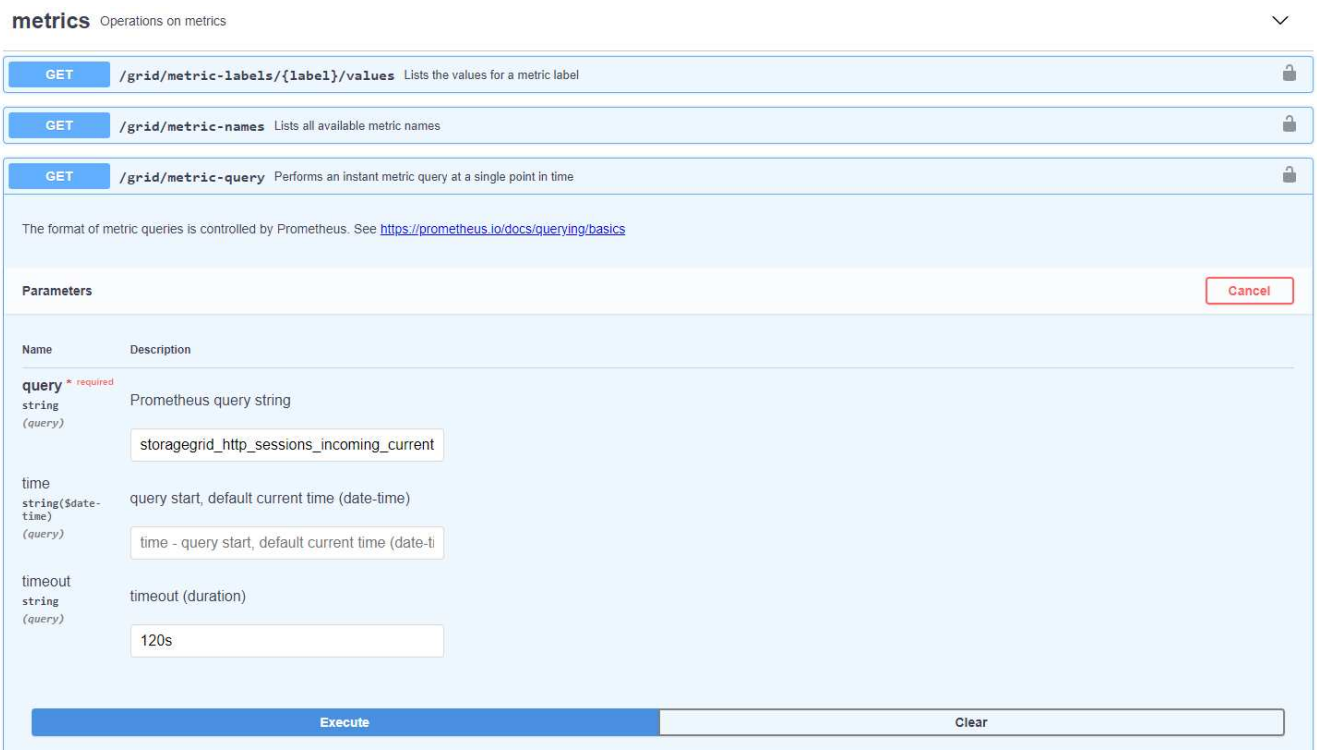
No se recomienda interactuar directamente con nuestra instancia de Prometheus porque esto requiere la apertura de puertos adicionales. El acceso a métricas a través de nuestra API es el método recomendado y seguro.

Exportar métricas a través de la API

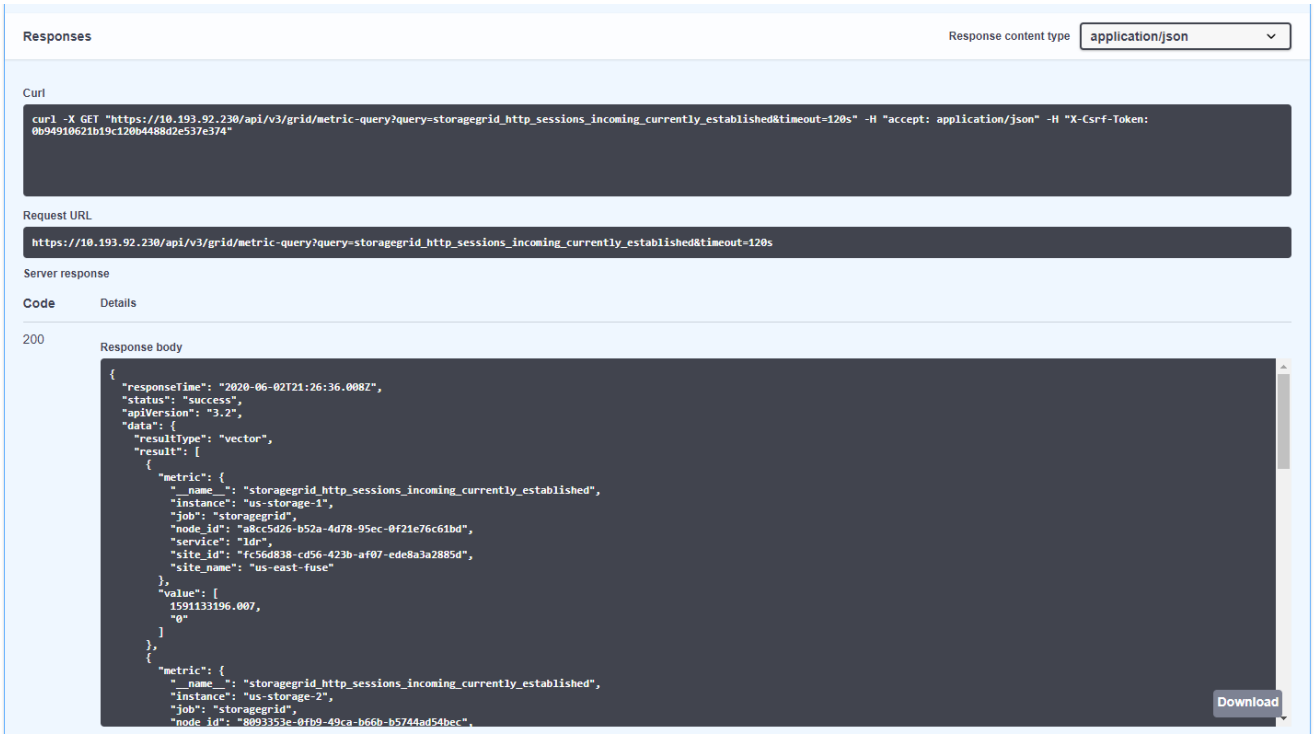
También se puede acceder a los mismos datos mediante la API de gestión de StorageGRID.

Para exportar métricas a través de la API, siga estos pasos:

1. En el GMI, seleccione MENU:Ayuda[Documentación de API].
2. Desplácese hasta Metrics y seleccione GET /grid/metric-query.



La respuesta incluye la misma información que puede obtener a través de una consulta URL de Prometheus. Puede volver a ver el número de sesiones HTTP que se han establecido actualmente en cada nodo de almacenamiento. También puede descargar la respuesta en formato JSON para su lectura. En la siguiente figura se muestran respuestas de consulta de Prometheus de ejemplo.



La ventaja de usar la API es que le permite realizar consultas autenticadas

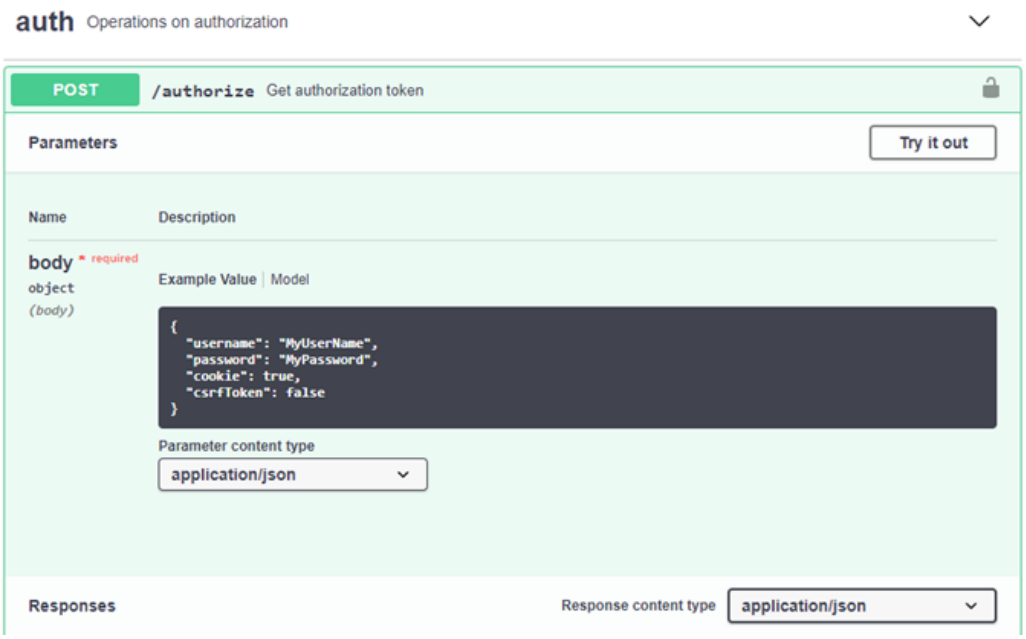
Acceda a métricas utilizando cURL en StorageGRID

Aprenda a acceder a las métricas a través de la CLI usando cURL.

Para realizar esta operación, primero debe obtener un token de autorización. Para solicitar un token, siga estos pasos:

Pasos

1. En el GMI, seleccione MENU:Ayuda[Documentación de API].
2. Desplácese hacia abajo hasta Aut. Para buscar operaciones en autorización. La siguiente captura de pantalla muestra los parámetros del método POST.



3. Haga clic en Pruébalo y edite el cuerpo con su nombre de usuario y contraseña de GMI.
4. Haga clic en Ejecutar.
5. Copie el comando cURL que se proporciona en la sección cURL y péguelo en una ventana de terminal. El comando tiene el siguiente aspecto:

```
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
```

> Si la contraseña de GMI contiene caracteres especiales, recuerde utilizar \ para escapar de caracteres especiales. Por ejemplo, sustituir! con \!

6. Después de ejecutar el comando curl anterior, la salida le da un token de autorización como el siguiente ejemplo:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Ahora puede utilizar la cadena de token de autorización para acceder a las métricas a través de cURL. El proceso para acceder a las métricas es similar a los pasos de la sección "Supervisión avanzada en StorageGRID". Sin embargo, a efectos de demostración, se muestra un ejemplo con GET /grid/metric-labels/{label}/values seleccionado en la categoría Metrics.

7. A modo de ejemplo, el siguiente comando cURL con el token de autorización anterior enumerará los nombres del sitio en StorageGRID.

```
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"
```

El comando curl generará la siguiente salida:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Ver métricas mediante el panel de Grafana en StorageGRID

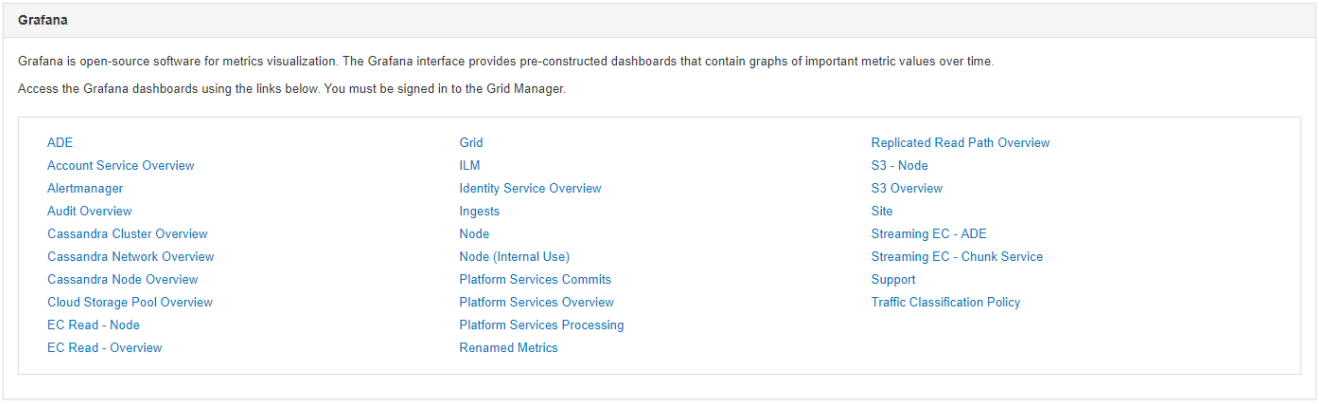
Aprende a usar la interfaz de Grafana para visualizar y supervisar tus datos de StorageGRID.

Grafana es un software de código abierto para la visualización de métricas. Por defecto, tenemos consolas prediseñadas que proporcionan información útil y potente sobre su sistema StorageGRID.

Estos paneles de control prediseñados no solo son útiles para la supervisión, sino también para solucionar un problema. Algunas están destinadas al soporte técnico. Por ejemplo, para ver las métricas de un nodo de almacenamiento, siga estos pasos.

Pasos

1. En el GMI, menú:Soporte[Métricas].
2. En la sección Grafana, seleccione el panel de control Nodo.



3. En Grafana, defina los hosts en el nodo en el que desee ver las métricas. En este caso, se selecciona un nodo de almacenamiento. Se proporciona más información que las siguientes capturas de pantalla.

Use las directivas de clasificación del tráfico en StorageGRID

Aprenda a configurar y configurar las directivas de clasificación del tráfico para gestionar y optimizar el tráfico de red en StorageGRID.

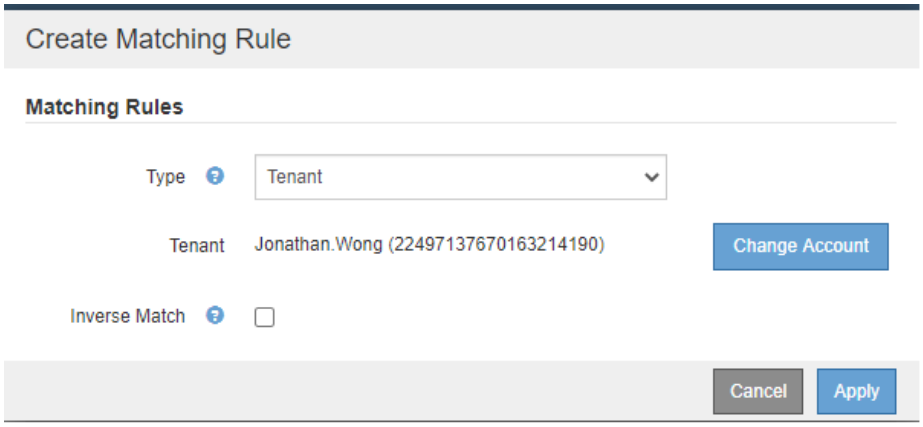
Las directivas de clasificación de tráfico proporcionan un método para supervisar y/o limitar el tráfico en función de un arrendatario específico, depósitos, subredes IP o puntos finales de equilibrio de carga. La conectividad de red y el ancho de banda son métricas especialmente importantes para StorageGRID.

Para configurar una directiva de clasificación de tráfico, siga estos pasos:

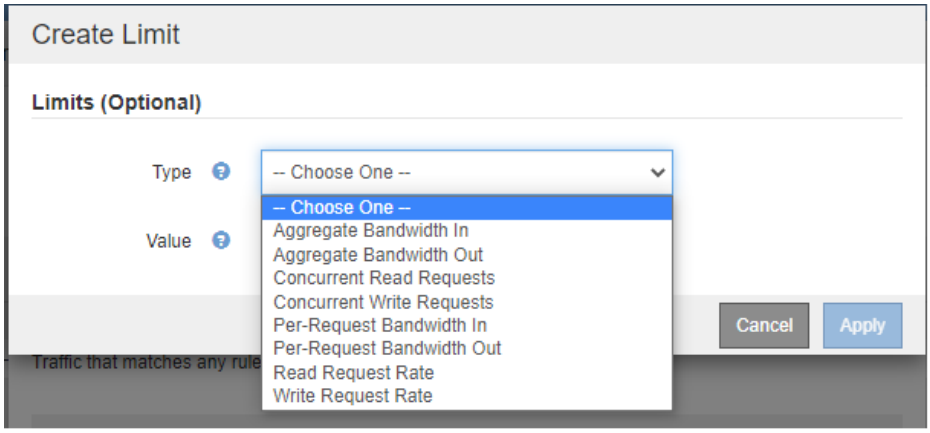
Pasos

1. En el GMI, navegue al menú:Configuración[Ajustes del sistema > Clasificación del tráfico].
2. Haga clic en Crear +
3. Introduzca un nombre y una descripción para la política.

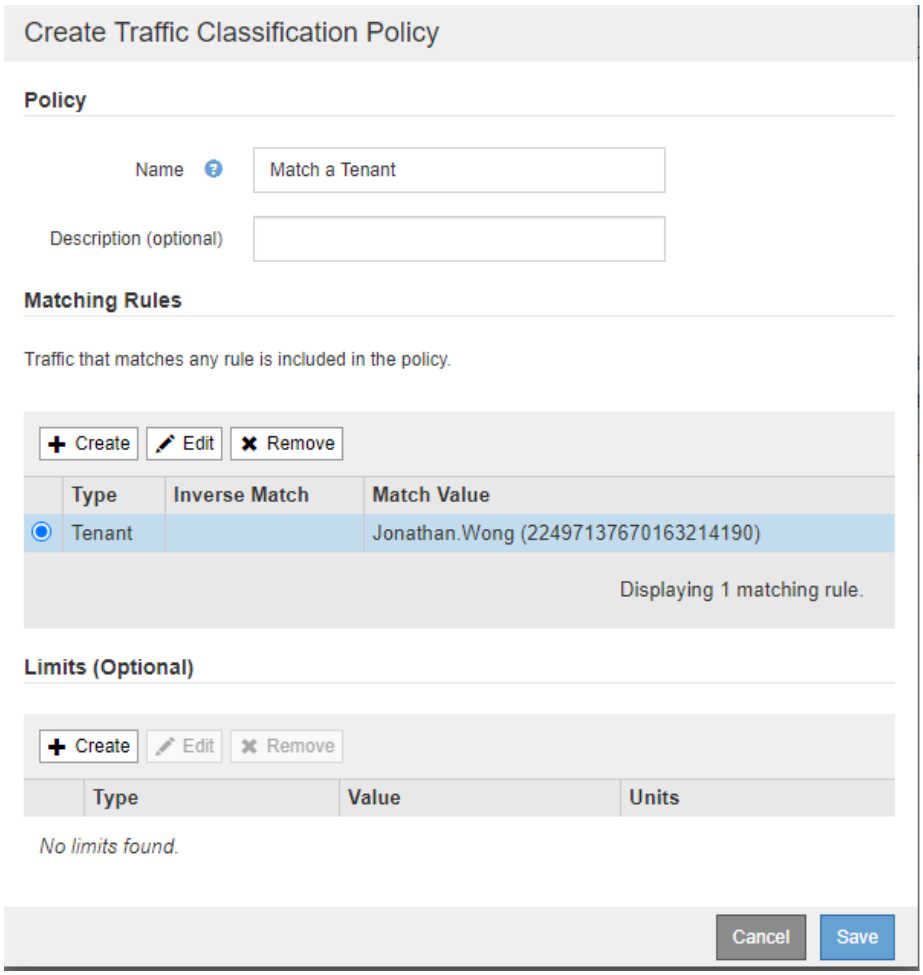
4. Cree una regla de coincidencia.



5. Establezca un límite (opcional).



6. Guarde su política



Para ver las métricas asociadas a su directiva de clasificación de tráfico, seleccione su política y haga clic en Métricas. Se genera un panel de Grafana que muestra información como el tráfico de solicitudes de equilibrador de carga y la duración media de solicitudes.

Utilice los registros de auditoría para supervisar StorageGRID

Aprenda a usar el registro de auditoría de StorageGRID para obtener información detallada sobre la actividad de inquilino y grid, y cómo aprovechar herramientas como Splunk para análisis de registros.

El registro de auditoría de StorageGRID permite recopilar información detallada sobre la actividad del inquilino y el grid. El registro de auditoría puede exponerse para análisis mediante NFS. Para obtener instrucciones detalladas sobre cómo exportar el registro de auditoría, consulte la Guía del administrador de.

Una vez exportada la auditoría, puede usar herramientas de análisis de registro como Splunk o Logstash + Elasticsearch para comprender la actividad de los inquilinos o para crear informes detallados de facturación y pago por uso.

Los detalles sobre los mensajes de auditoría se incluyen en la documentación de StorageGRID. Consulte "Auditar mensajes".

Utilice la aplicación StorageGRID para Splunk

Obtenga más información sobre la aplicación NetApp StorageGRID para Splunk que le permite supervisar y analizar su entorno StorageGRID en la plataforma Splunk.

Splunk es una plataforma de software que importa e indexa datos de máquina para ofrecer potentes funciones de búsqueda y análisis. La aplicación de NetApp StorageGRID es un complemento para Splunk que importa y enriquece los datos que se aprovechan de StorageGRID.

Las instrucciones sobre cómo instalar, actualizar y configurar el complemento StorageGRID se pueden encontrar aquí: https://splunkbase.splunk.com/app/3895/#/details

TR-4882: Instale una cuadrícula StorageGRID con configuración básica

Introducción a la instalación de StorageGRID

Aprenda a instalar StorageGRID en hosts bare metal.

TR-4882 proporciona un conjunto práctico de instrucciones paso a paso que produce una instalación de funcionamiento de NetApp StorageGRID. La instalación puede estar en configuración básica o en máquinas virtuales que se ejecuten en Red Hat Enterprise Linux (RHEL). El enfoque consiste en realizar una instalación «revisada» de seis servicios contenerizados de StorageGRID en tres máquinas físicas (o virtuales) en una configuración de diseño y almacenamiento sugerida. A algunos clientes es posible que les resulte más fácil comprender el proceso de puesta en marcha siguiendo el ejemplo de puesta en marcha en este TR.

Para obtener información más detallada sobre StorageGRID y el proceso de instalación, consulte https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html [Install, upgrade, and hotfix StorageGRID] en la documentación del producto.

Antes de iniciar la puesta en marcha, examinemos los requisitos de computación, almacenamiento y redes del software de NetApp StorageGRID. StorageGRID se ejecuta como un servicio en contenedores dentro de Podman o Docker. En este modelo, algunos requisitos hacen referencia al sistema operativo del host (el sistema operativo que aloja Docker, que ejecuta el software StorageGRID). Además, algunos de los recursos se asignan directamente a los contenedores de Docker que se ejecutan dentro de cada host. En esta

implementación, con el fin de maximizar el uso del hardware, estamos implementando dos servicios por host físico. Para obtener más información, continúe en la siguiente sección, "Requisitos previos para instalar StorageGRID".

Los pasos descritos en este TR dan como resultado una instalación de StorageGRID en seis hosts sin configuración básica. Ahora tiene una red de red y cliente que funcionan, lo cual es útil en la mayoría de los escenarios de prueba.

Dónde encontrar información adicional

Si desea obtener más información sobre la información descrita en este TR, consulte los siguientes recursos de documentación:

- Centro de documentación de NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

Requisitos previos para instalar StorageGRID

Obtenga más información sobre la computación, el almacenamiento, la red, el Docker y los requisitos de nodos para poner en marcha StorageGRID.

Requisitos de computación

La siguiente tabla enumera los requisitos mínimos de recursos admitidos para cada tipo de nodo StorageGRID. Estos son los recursos mínimos necesarios para los nodos StorageGRID.

Tipo de nodo	Núcleos de CPU	RAM
Admin	8	24GB
Reducida	8	24GB
Puerta de enlace	8	24GB

Además, cada host Docker físico debe tener un mínimo de 16GB GB de RAM asignado para que funcione correctamente. Así, por ejemplo, para alojar dos de los servicios descritos en la tabla juntos en un host físico de Docker, debe realizar el siguiente cálculo:

24 + 24 +16 = 64GB GB de RAM y 8 + 8 = 16 núcleos

Debido a que muchos servidores modernos superan estos requisitos, combinamos seis servicios (contenedores StorageGRID) en tres servidores físicos.

Requisitos de red

Los tres tipos de tráfico StorageGRID incluyen:

- **Tráfico de red (requerido).** El tráfico interno de StorageGRID que viaja entre todos los nodos de la cuadrícula.
- **Tráfico de administración (opcional).** El tráfico utilizado para la administración y el mantenimiento del sistema.
- **Tráfico de clientes (opcional).** El tráfico que se desplaza entre aplicaciones cliente externas y la

cuadrícula, incluidas todas las solicitudes de almacenamiento de objetos de los clientes S3 y Swift.

Puede configurar hasta tres redes para usarlas con el sistema StorageGRID. Cada tipo de red debe estar en una subred independiente sin superposición. Si todos los nodos están en la misma subred, no es necesaria una dirección de puerta de enlace.

Para esta evaluación, implementaremos en dos redes, que contienen el tráfico de grid y cliente. Es posible agregar una red de administración más tarde para servir esa función adicional.

Es muy importante asignar las redes de forma coherente a las interfaces en todos los hosts. Por ejemplo, si hay dos interfaces en cada nodo, ens192 y ens224, deberían asignarse todas a la misma red o VLAN en todos los hosts. En esta instalación, el instalador los asigna a los contenedores Docker como eth0@IF2 y eth2@IF3 (porque el bucle invertido es IF1 dentro del contenedor), y por lo tanto un modelo consistente es muy importante.

Nota sobre las redes de Docker

StorageGRID usa las redes de una forma distinta a algunas implementaciones de contenedores Docker. No utiliza las redes proporcionadas por Docker (ni Kubernetes o Swarm). En su lugar, StorageGRID realmente genera el contenedor como --net=none para que Docker no haga nada para conectar el contenedor a la red. Una vez que el servicio StorageGRID ha generado el contenedor, se crea un nuevo dispositivo macvlan a partir de la interfaz definida en el archivo de configuración del nodo. Ese dispositivo tiene una nueva dirección MAC y actúa como un dispositivo de red independiente que puede recibir paquetes de la interfaz física. El dispositivo macvlan se mueve entonces al espacio de nombres del contenedor y se renombra para ser uno de eth0, eth1 o eth2 dentro del contenedor. En ese momento, el dispositivo de red ya no está visible en el sistema operativo del host. En nuestro ejemplo, el dispositivo de red grid es eth0 dentro de los contenedores Docker y la red cliente es eth2. Si tuviéramos una red de administración, el dispositivo estaría eth1 en el contenedor.

> La nueva dirección MAC del dispositivo de red del contenedor puede requerir que se active el modo promiscuo en algunos entornos de red y virtuales. Este modo permite que el dispositivo físico reciba y envíe paquetes para direcciones MAC que difieren de la dirección MAC física conocida. Si se ejecuta en VMware vSphere, debe aceptar el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas en los grupos de puertos que servirán al tráfico StorageGRID cuando ejecute RHEL. Ubuntu o Debian funciona sin estos cambios en la mayoría de las circunstancias.

Requisitos de almacenamiento

Cada nodo requiere dispositivos de disco locales o basados en SAN con los tamaños mostrados en la siguiente tabla.

> Los números de la tabla son para cada tipo de servicio StorageGRID, no para toda la cuadrícula ni para cada host físico. Según las opciones de implementación, calcularemos los números de cada host físico en , más adelante en "La distribución y los requisitos del host físico"este documento. Las rutas o sistemas de archivos marcados con un asterisco serán creados en el propio contenedor StorageGRID por el instalador. El administrador no requiere ninguna configuración manual ni la creación del sistema de archivos, pero los hosts necesitan dispositivos de bloques para satisfacer estos requisitos. En otras palabras, el dispositivo de bloque debe aparecer mediante el comando `lsblk` , pero no debe formatearse ni montarse en el sistema operativo host.

Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño mínimo de LUN	Se requiere un sistema de archivos manual	Entrada de configuración de nodo sugerida
Todo	Espacio del sistema del nodo de administración `/var/local` (SSD útil aquí)	Uno para cada nodo de administración	90GB	No	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
Todos los nodos	Pool de almacenamiento de Docker en `/var/lib/docker for container pool`	Uno para cada host (físico o VM)	100GB por contenedor	Sí – etx4	NA: Formatear y montar como sistema de archivos host (no asignado en el contenedor)
Admin	Registros de auditoría del nodo de administración (datos del sistema en el contenedor de administración) `/var/local/audit/export`	Uno para cada nodo de administración	200GB	No	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Admin	Tablas de nodos de administración (datos del sistema en el contenedor de administración) `/var/local/mysql_ibdata`	Uno para cada nodo de administración	200GB	No	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Nodos de almacenamiento	Almacenamiento de objetos (dispositivos de bloques) `/var/local/rangedb0` (SSD de utilidad aquí) `/var/local/rangedb1` `/var/local/rangedb2`	Tres para cada contenedor de almacenamiento	4000GB	No	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

En este ejemplo, los tamaños de disco mostrados en la siguiente tabla son necesarios por tipo de contenedor. Los requisitos por host físico se describen en "La distribución y los requisitos del host físico", más adelante en este documento.

Tamaños de disco por tipo de contenedor

Contenedor de administración

Nombre	Tamaño (GiB)
Almacén de Docker	100 (por contenedor)
ADM-OS	90
ADM-Auditoría	200
ADM-MySQL	200

Contenedor de almacenamiento

Nombre	Tamaño (GiB)
Almacén de Docker	100 (por contenedor)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

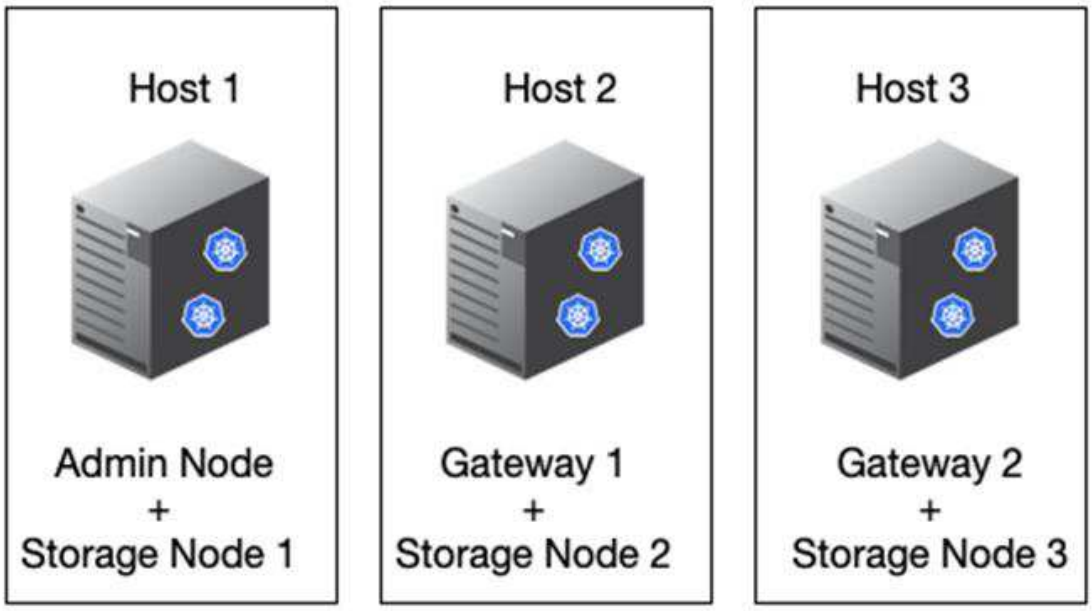
Contenedor de gateway

Nombre	Tamaño (GiB)
Almacén de Docker	100 (por contenedor)
/var/local	90

La distribución y los requisitos del host físico

Combinando los requisitos de computación y de red mostrados en la tabla anterior, puede obtener un conjunto básico de hardware necesario para esta instalación de tres servidores físicos (o virtuales) con 16 núcleos, 64GB GB de RAM y dos interfaces de red. Si se desea un rendimiento superior, es posible vincular dos o más interfaces en la red de grid o la red de cliente y utilizar una interfaz etiquetada con VLAN como bond0,520 en el archivo de configuración de nodos. Si espera cargas de trabajo más intensas, será mejor tener más memoria tanto para el host como para los contenedores.

Como se muestra en la siguiente figura, estos servidores alojarán seis contenedores Docker, dos por host. La RAM se calcula proporcionando 24GB GB por contenedor y 16GB GB para el propio SO host.



La RAM total necesaria por host físico (o VM) es de 24 x 2 + 16 GB = 64GB GB. En las siguientes tablas, se enumeran el almacenamiento en disco requerido para los hosts 1, 2 y 3.

Host 1	**Tamaño (GiB)**
Docker Store	`/var/lib/docker` (Sistema de archivos)
200 (2 de 100 tb)	**Admin Container**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Contenedor de almacenamiento	SN-OS `/var/local` (dispositivo)
90	Rangedb-0 (Dispositivo)
4096	Rangedb-1 (Dispositivo)
4096	Rangedb-2 (Dispositivo)

Host 2	**Tamaño (GiB)**
Docker Store	`/var/lib/docker` (Compartido)
200 (2 de 100 tb)	**Gateway Container**
GW-OS *`/var/local`	100

Host 2	Tamaño (GiB)
Contenedor de almacenamiento	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Host 3	Tamaño (GiB)
Docker Store	/var/lib/docker (Compartido)
200 (2 de 100 tb)	**Gateway Container**
*/var/local	100
Contenedor de almacenamiento	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

El almacén de Docker se calculó permitiendo dos contenedores por /var/local (por contenedor) x 100GB TB = 200GB TB.

Preparar los nodos

Para prepararse para la instalación inicial de StorageGRID, primero instale RHEL versión 9,2 y habilite SSH. Configure las interfaces de red, el protocolo de tiempo de redes (NTP), DNS y el nombre de host según las prácticas recomendadas. Necesita al menos una interfaz de red activada en la red de grid y otra para la red de cliente. Si utiliza una interfaz con etiqueta VLAN, configúrela según los ejemplos que aparecen a continuación. De lo contrario, bastará con una configuración de interfaz de red estándar simple.

Si necesita usar una etiqueta VLAN en la interfaz de red de grid, la configuración debe tener dos archivos en /etc/sysconfig/network-scripts/ el siguiente formato:

```
# 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
```

En este ejemplo se asume que el dispositivo de red físico para la red de grid es enp67s0. También podría ser un dispositivo unido como bond0. Ya sea que utilice una conexión o una interfaz de red estándar, debe usar la interfaz etiquetada por VLAN en el archivo de configuración de nodos si el puerto de red no tiene una VLAN predeterminada o si la VLAN predeterminada no está asociada a la red de grid. El contenedor de StorageGRID en sí no utiliza tramas Ethernet, por lo que debe ser manejado por el SO principal.

Configuración de almacenamiento opcional con iSCSI

Si no utiliza almacenamiento iSCSI, debe asegurarse de que host1, host2 y host3 contengan dispositivos de bloque de tamaño suficiente para satisfacer sus requisitos. Consulte "Tamaños de disco por tipo de contenedor" para conocer los requisitos de almacenamiento de host1, host2 y host3.

Para configurar el almacenamiento con iSCSI, complete los siguientes pasos:

Pasos

1. Si utiliza almacenamiento iSCSI externo, como el software de gestión de datos NetApp E-Series o NetApp ONTAP®, instale los siguientes paquetes:

   ```
   sudo yum install iscsi-initiator-utils
   sudo yum install device-mapper-multipath
   ```

2. Busque el ID del iniciador en cada host.

   ```
   # cat /etc/iscsi/initiatorname.iscsi
   InitiatorName=iqn.2006-04.com.example.node1
   ```

3. Con el nombre del iniciador del paso 2, asigne las LUN del dispositivo de almacenamiento (del número y tamaño que se muestran en "Requisitos de almacenamiento" la tabla) a cada nodo de almacenamiento.
4. Detecte las LUN recién creadas con `iscsiadm` e inicie sesión en ellas.

```
# 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.
```

Para obtener más información, consulte "Crear un iniciador de iSCSI" en el Portal de clientes de Red Hat.

5. Para mostrar los dispositivos multivía y sus WWID de LUN asociados, ejecute el siguiente comando:

```
# multipath -ll
```

Si no está utilizando iSCSI con dispositivos multivía, simplemente monte el dispositivo con un nombre de ruta único que persistirá los cambios del dispositivo y se reiniciará por igual.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

El simple uso `/dev/sdx` de nombres de dispositivos podría causar problemas más adelante si los dispositivos se quitan o agregan. Si está utilizando dispositivos multivía, modifique el `/etc/multipath.conf` archivo para usar alias de la siguiente manera.

Es posible que estos dispositivos estén o no presentes en todos los nodos, en función de la distribución.

```
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
}
}
```

Antes de instalar Docker en el sistema operativo host, formatee y monte el respaldo de LUN o disco `/var/lib/docker`. Las demás LUN se definen en el archivo de configuración del nodo y los contenedores de StorageGRID los utilizan directamente. Es decir, no aparecen en el sistema operativo host; aparecen en los propios contenedores y el instalador gestiona esos sistemas de archivos.

Si utiliza una LUN respaldada por iSCSI, coloque algo similar a la siguiente línea en el archivo fstab. Como se indica, las otras LUN no necesitan estar montadas en el sistema operativo del host, pero deben aparecer

como dispositivos de bloque disponibles.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Preparar la instalación de Docker

Para preparar la instalación de Docker, lleve a cabo los siguientes pasos:

Pasos

1. Crear un sistema de archivos en el volumen de almacenamiento de Docker en los tres hosts.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Si utiliza dispositivos iSCSI con multivía, utilice `/dev/mapper/Docker-Store`.

2. Cree el punto de montaje de volumen de almacenamiento de Docker:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Agregue una entrada similar para el docker-storage-volume-device a `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   La siguiente `_netdev` opción solo se recomienda si utiliza un dispositivo iSCSI. Si está utilizando un dispositivo de bloque local `_netdev` no es necesario y `defaults` se recomienda.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Monte el nuevo sistema de archivos y vea el uso del disco.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Desactive el intercambio y desactívelo por motivos de rendimiento.

   ```
   $ sudo swapoff --all
   ```

6. Para mantener la configuración, elimine todas las entradas de intercambio de /etc/fstab como:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

> Si no se deshabilita por completo el intercambio, el rendimiento se puede reducir considerablemente.

7. Ejecute un reinicio de prueba del nodo para asegurarse de que el `/var/lib/docker` volumen es persistente y que todos los dispositivos de disco devuelven.

Instale Docker para StorageGRID

Aprenda a instalar Docker para StorageGRID.

Para instalar Docker, lleve a cabo los siguientes pasos:

Pasos

1. Configure el repositorio yum para Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Instale los paquetes necesarios.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Inicie Docker.

```
sudo systemctl start docker
```

4. Pruebe Docker.

```
sudo docker run hello-world
```

5. Asegúrese de que Docker se ejecuta al iniciar el sistema.

```
sudo systemctl enable docker
```

Prepare los archivos de configuración de nodos para StorageGRID

Aprenda a preparar los archivos de configuración de nodos para StorageGRID.

En líneas generales, el proceso de configuración de nodos incluye los siguientes pasos:

Pasos

1. Cree el `/etc/storagegrid/nodes` directorio en todos los hosts.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Cree los archivos necesarios por host físico para que coincidan con la distribución de tipo de contenedor/nodo. En este ejemplo, creamos dos archivos por host físico en cada máquina host.

> El nombre del archivo define el nombre de nodo real para la instalación. Por ejemplo, `dc1-adm1.conf` se convierte en un nodo llamado `dc1-adm1`.

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

Preparando los archivos de configuración del nodo

Los siguientes ejemplos utilizan el `/dev/disk/by-path` formato. Puede verificar las rutas correctas ejecutando los siguientes comandos:

```
[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
```

Y estos comandos:

```
[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
```

Ejemplo de nodo de administración principal

Nombre de archivo de ejemplo:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Contenido del archivo de ejemplo:

> Las rutas de acceso a los discos pueden seguir los siguientes ejemplos o `/dev/mapper/alias` utilizar la nomenclatura de estilos. No utilice nombres de dispositivos de bloqueo, `/dev/sdb` como porque pueden cambiar al reiniciar y causar grandes daños a la red.

```
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
```

Ejemplo de un nodo de almacenamiento

Nombre de archivo de ejemplo:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Contenido del archivo de ejemplo:

```
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
```

Ejemplo de nodo de pasarela

Nombre de archivo de ejemplo:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Contenido del archivo de ejemplo:

```
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
```

Instale las dependencias y los paquetes de StorageGRID

Descubra cómo instalar las dependencias y paquetes de StorageGRID.

Para instalar las dependencias y paquetes de StorageGRID, ejecute los siguientes comandos:

```
[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
```

Valide los archivos de configuración de StorageGRID

Aprenda a validar el contenido de los archivos de configuración para StorageGRID.

Después de crear los archivos de configuración en `/etc/storagegrid/nodes` para cada uno de sus nodos StorageGRID, debe validar el contenido de esos archivos.

Para validar el contenido de los archivos de configuración, ejecute el siguiente comando en cada host:

```
sudo storagegrid node validate all
```

Si los archivos son correctos, la salida muestra PASADO para cada archivo de configuración:

```
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
```

Si los archivos de configuración no son correctos, los problemas se muestran como ADVERTENCIA y ERROR. Si se encuentra algún error de configuración, debe corregirlo antes de continuar con la instalación.

```
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
```

Inicie el servicio de host StorageGRID

Aprenda a iniciar el servicio de host StorageGRID.

Para iniciar los nodos StorageGRID y asegurarse de que se reinicien después de reiniciar el host, debe habilitar e iniciar el servicio del host StorageGRID.

Para iniciar el servicio de host StorageGRID, complete los siguientes pasos.

Pasos

1. Ejecute los siguientes comandos en cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

> El proceso de inicio puede tardar algún tiempo en la ejecución inicial.

2. Ejecute el siguiente comando para asegurarse de que se sigue la implementación:

```
sudo storagegrid node status node-name
```

3. Para cualquier nodo que devuelva un estado de `Not-Running` o `Stopped`, ejecute el siguiente comando:

```
sudo storagegrid node start node-name
```

   Por ejemplo, si se da la siguiente salida, se iniciaría el `dc1-adm1` nodo:

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Si habilitó e inició previamente el servicio de host de StorageGRID (o si no está seguro de si el servicio se habilitó y se inició), también ejecute el siguiente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configure Grid Manager en StorageGRID

Aprenda a configurar Grid Manager en StorageGRID en el nodo de administración principal.

Complete la instalación configurando el sistema StorageGRID desde la interfaz de usuario de Grid Manager

en el nodo de administración principal.

Escalones de alto nivel

La configuración de la cuadrícula y la finalización de la instalación implican las siguientes tareas:

Pasos

1. Navegue a Grid Manager
2. "Especifique la información de licencia de StorageGRID"
3. "Agregar sitios a StorageGRID"
4. "Especifique las subredes de red de cuadrícula"
5. "Aprobar los nodos de cuadrícula pendientes"
6. "Especifique la información del servidor NTP"
7. "Especifique la información del servidor del sistema de nombres de dominio"
8. "Especifique las contraseñas del sistema StorageGRID"
9. "Revise la configuración y complete la instalación"

Navegue a Grid Manager

Utilice Grid Manager para definir toda la información necesaria para configurar el sistema StorageGRID.

Antes de comenzar, el nodo de administración principal debe desplegarse y haber completado la secuencia de inicio inicial.

Para utilizar Grid Manager para definir información, realice los siguientes pasos.

Pasos

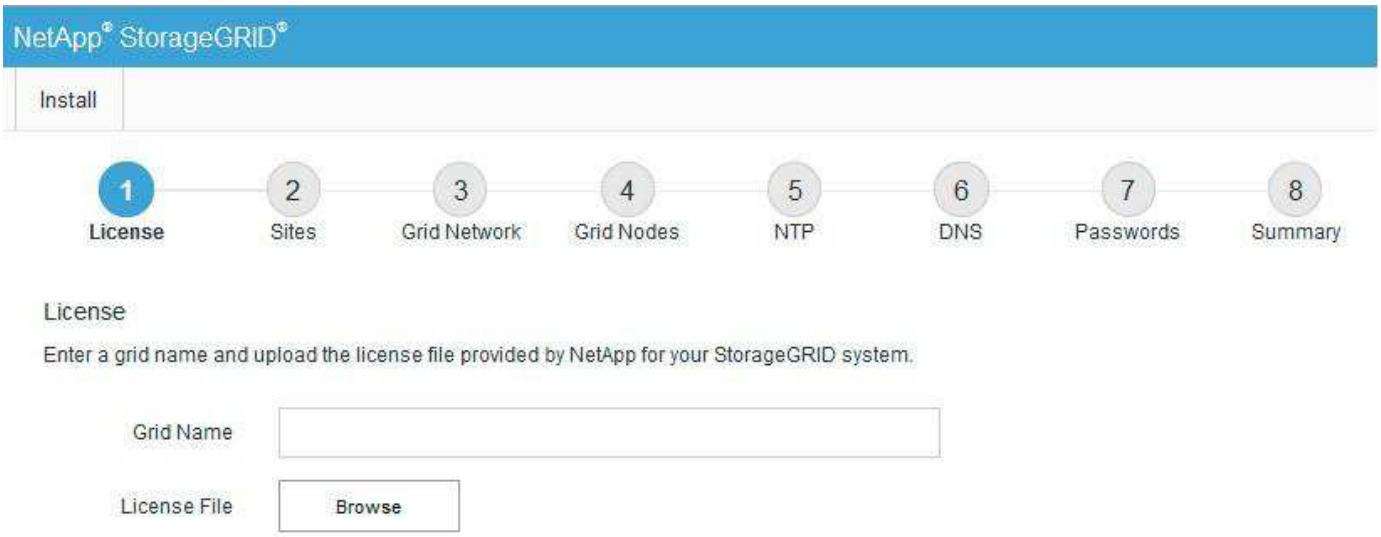
1. Acceda a Grid Manager en la siguiente dirección:

   ```
   https://primary_admin_node_grid_ip
   ```

   También puede acceder a Grid Manager en el puerto 8443.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Haga clic en Instalar un sistema StorageGRID. Se muestra la página utilizada para configurar una cuadrícula StorageGRID.



Añada detalles de la licencia de StorageGRID

Aprenda a cargar el archivo de licencia de StorageGRID.

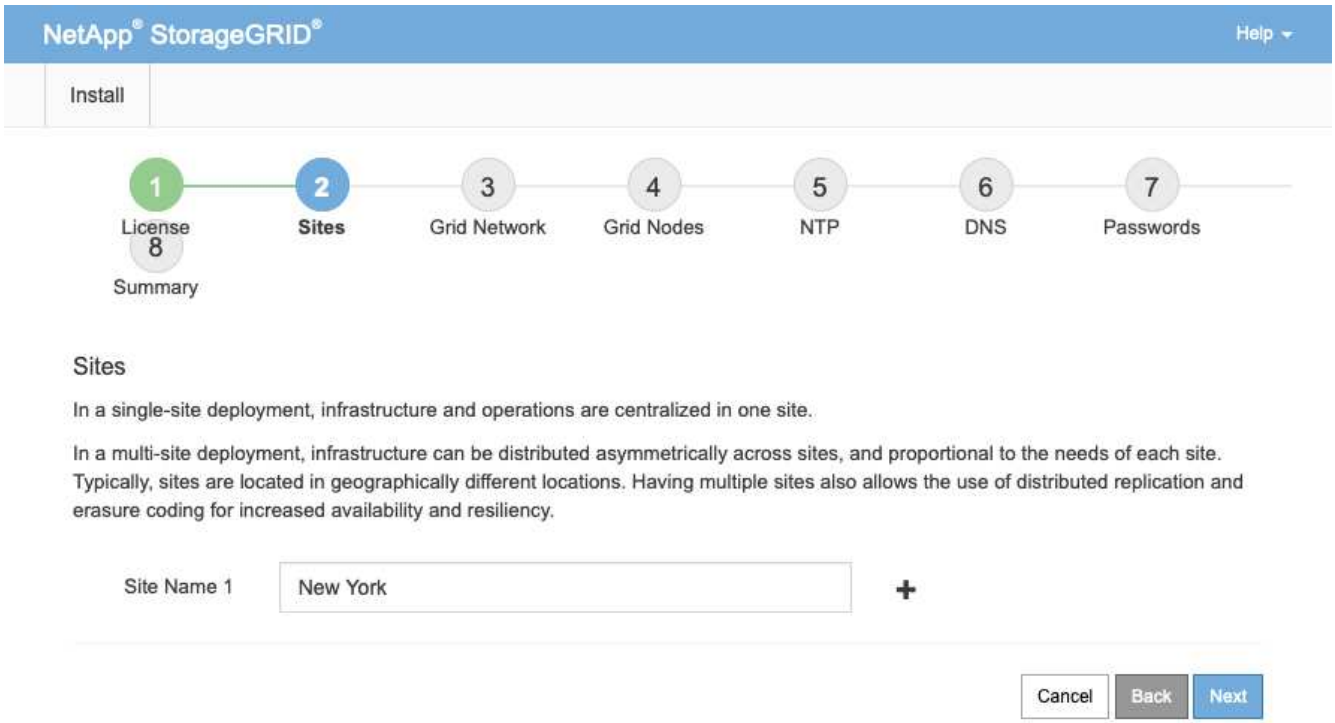
Debe especificar el nombre del sistema StorageGRID y cargar el archivo de licencia proporcionado por NetApp.

Para especificar la información de licencia de StorageGRID, realice los siguientes pasos:

Pasos

1. En la página License, en el campo Grid Name, introduzca un nombre para el sistema StorageGRID. Después de la instalación, el nombre se muestra como el nivel superior en el árbol de topología de cuadrícula.
2. Haga clic en Examinar, busque el archivo de licencia de NetApp (`NLF-unique-id.txt`) y haga clic en Abrir. El archivo de licencia se valida y se muestran el número de serie y la capacidad de almacenamiento con licencia.

> El archivo de instalación de StorageGRID incluye una licencia gratuita que no proporciona ningún derecho de soporte para el producto. Puede actualizar a una licencia que ofrezca soporte tras la instalación.



3. Haga clic en Siguiente.

Agregar sitios a StorageGRID

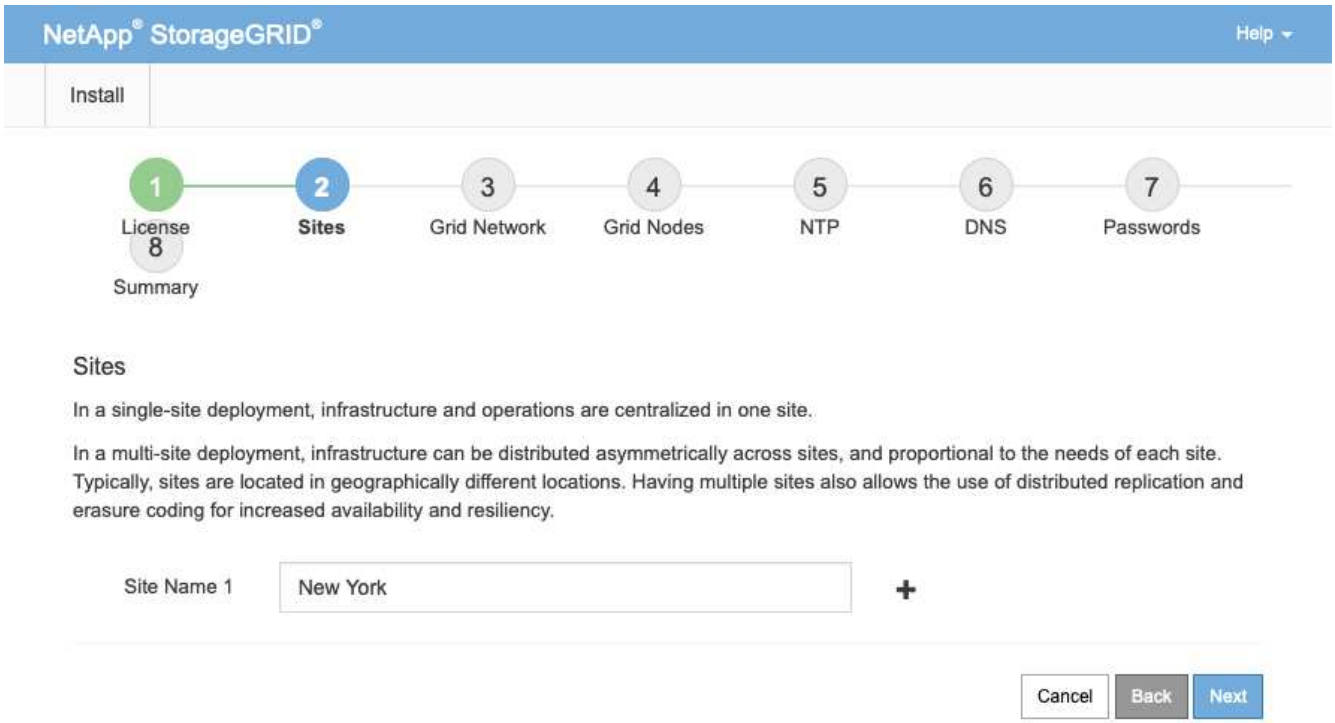
Aprenda a añadir sitios a StorageGRID para aumentar la fiabilidad y la capacidad de almacenamiento.

Al instalar StorageGRID, debe crear al menos un sitio. Puede crear sitios adicionales para aumentar la fiabilidad y la capacidad de almacenamiento de su sistema StorageGRID.

Para agregar sitios, realice los siguientes pasos:

Pasos

1. En la página Sitios, introduzca el nombre del sitio.
2. Para agregar sitios adicionales, haga clic en el signo más junto a la última entrada del sitio e introduzca el nombre en el nuevo cuadro de texto Nombre del sitio. Agregue tantos sitios adicionales como sea necesario para la topología de la cuadrícula. Puede agregar hasta 16 sitios.



3. Haga clic en Siguiente.

Especifique las subredes de red de grid para StorageGRID

Aprenda a configurar las subredes de red de grid para StorageGRID.

Debe especificar las subredes que se utilizan en la red de cuadrícula.

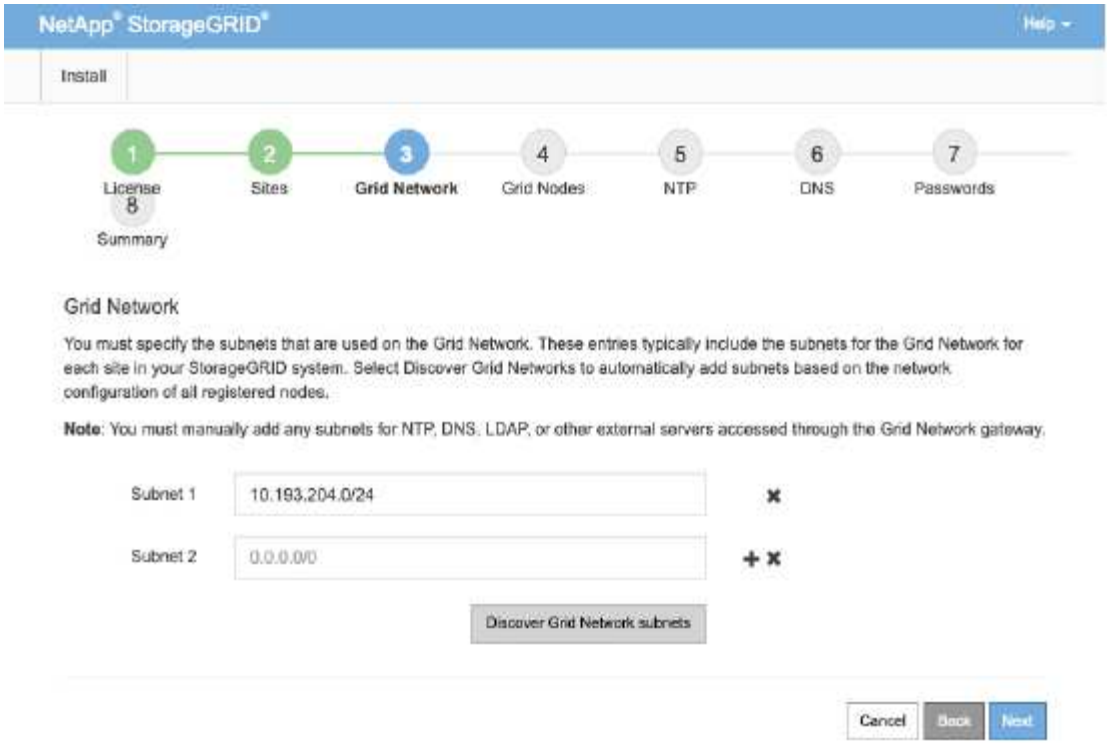
Las entradas de subred incluyen las subredes de la red de grid para cada sitio del sistema StorageGRID, además de las subredes a las que debe accederse a través de la red de grid (por ejemplo, las subredes que alojan los servidores NTP).

Si tiene varias subredes de grid, se requiere la puerta de enlace de red de grid. Todas las subredes de la cuadrícula especificadas deben ser accesibles a través de esta puerta de enlace.

Para especificar subredes de red de grid, realice los siguientes pasos:

Pasos

1. En el cuadro de texto Subred 1, especifique la dirección de red CIDR para al menos una red de cuadrícula.
2. Haga clic en el signo más situado junto a la última entrada para añadir una entrada de red adicional. Si ya ha desplegado al menos un nodo, haga clic en Detectar subredes de redes de grid para rellenar automáticamente la lista de subredes de red de grid con las subredes notificadas por los nodos de grid que se han registrado con Grid Manager.



3. Haga clic en Siguiente.

Aprobar nodos de cuadrícula para StorageGRID

Aprenda a revisar y aprobar cualquier nodo de grid pendiente que se una al sistema StorageGRID.

Debe aprobar cada nodo de cuadrícula antes de unirse al sistema StorageGRID.

> Antes de comenzar, se deben poner en marcha todos los nodos de grid de dispositivos virtuales y StorageGRID.

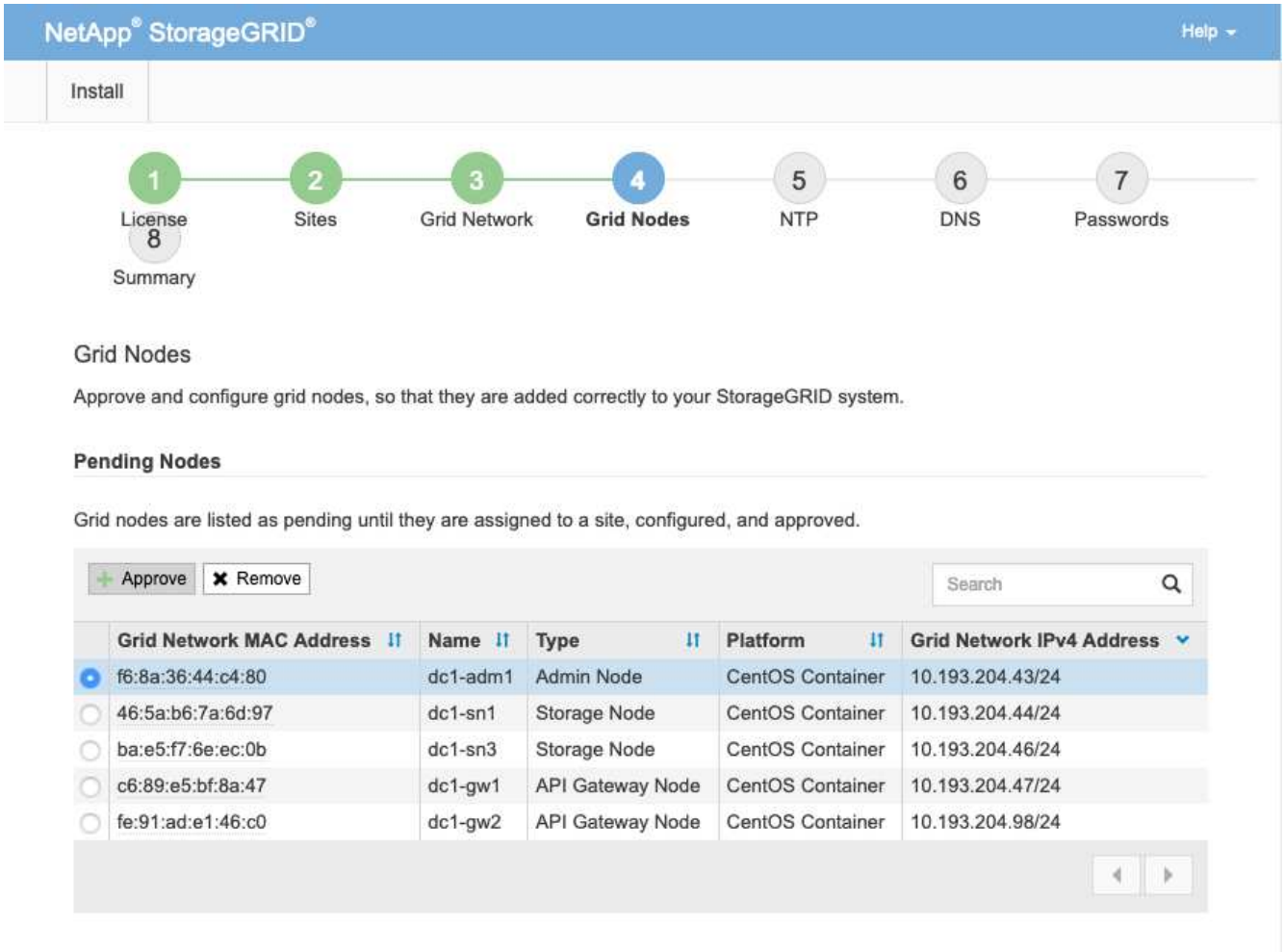
Para aprobar nodos de cuadrícula pendientes, realice los siguientes pasos:

Pasos

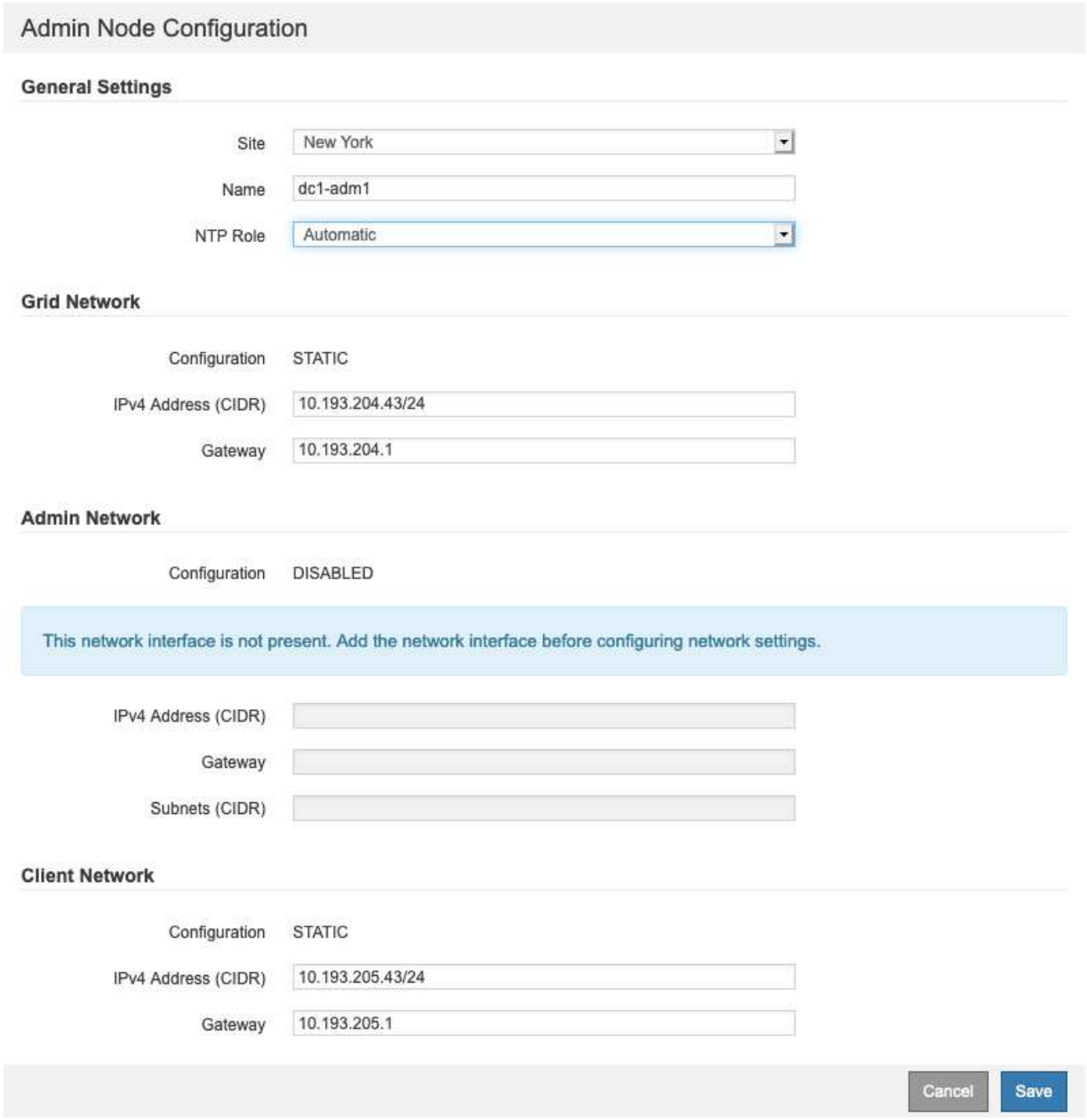
1. Revise la lista Pending Nodes y confirme que muestra todos los nodos de grid que ha implementado.

   > Si falta un nodo de cuadrícula, confirme que se ha implementado correctamente.

2. Haga clic en el botón de radio situado junto a un nodo pendiente que desee aprobar.



3. Haga clic en Aprobar.
4. En Configuración general, modifique la configuración de las siguientes propiedades, según sea necesario.



— **Sitio**: El nombre del sistema del sitio para este nodo de red.

— **Nombre**: El nombre de host que se asignará al nodo, y el nombre que se mostrará en Grid Manager. El nombre predeterminado es el nombre especificado durante la implementación del nodo, pero puede cambiar el nombre según sea necesario.

— **Rol NTP**: El rol NTP del nodo de la red. Las opciones son Automático, Primario y Cliente. Al seleccionar la opción Automático, se asigna el rol primario a los nodos de administración, los nodos de almacenamiento con servicios de controlador de dominio administrativo (ADC), los nodos de puerta de enlace y cualquier nodo de cuadrícula que tenga direcciones IP no estáticas. A todos los demás nodos de grid se les asigna el rol de cliente.

Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

— **Servicio ADC (solo nodos de almacenamiento)**: Seleccione Automático para que el sistema determine si el nodo requiere el servicio ADC. El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puede agregar el servicio ADC a un nodo después de haberlo implementado.

5. En Grid Network, modifique la configuración de las siguientes propiedades según sea necesario:

— **Dirección IPv4 (CIDR)**: La dirección de red CIDR para la interfaz de red de red (eth0 dentro del contenedor). Por ejemplo, `192.168.1.234/24`.

— **Gateway**: La puerta de enlace de red de red. Por ejemplo, `192.168.0.1`.

Si hay varias subredes de grid, se requiere la puerta de enlace.

Si seleccionó DHCP para la configuración de red de cuadrícula y cambia el valor aquí, el nuevo valor se configura como una dirección estática en el nodo. Asegúrese de que la dirección IP resultante no esté en un pool de direcciones DHCP.

6. Para configurar la red de administración del nodo de cuadrícula, agregue o actualice los ajustes en la sección Admin Network según sea necesario.

Introduzca las subredes de destino de las rutas que salen de esta interfaz en el cuadro de texto Subredes (CIDR). Si hay varias subredes de administrador, se requiere la puerta de enlace de administrador.

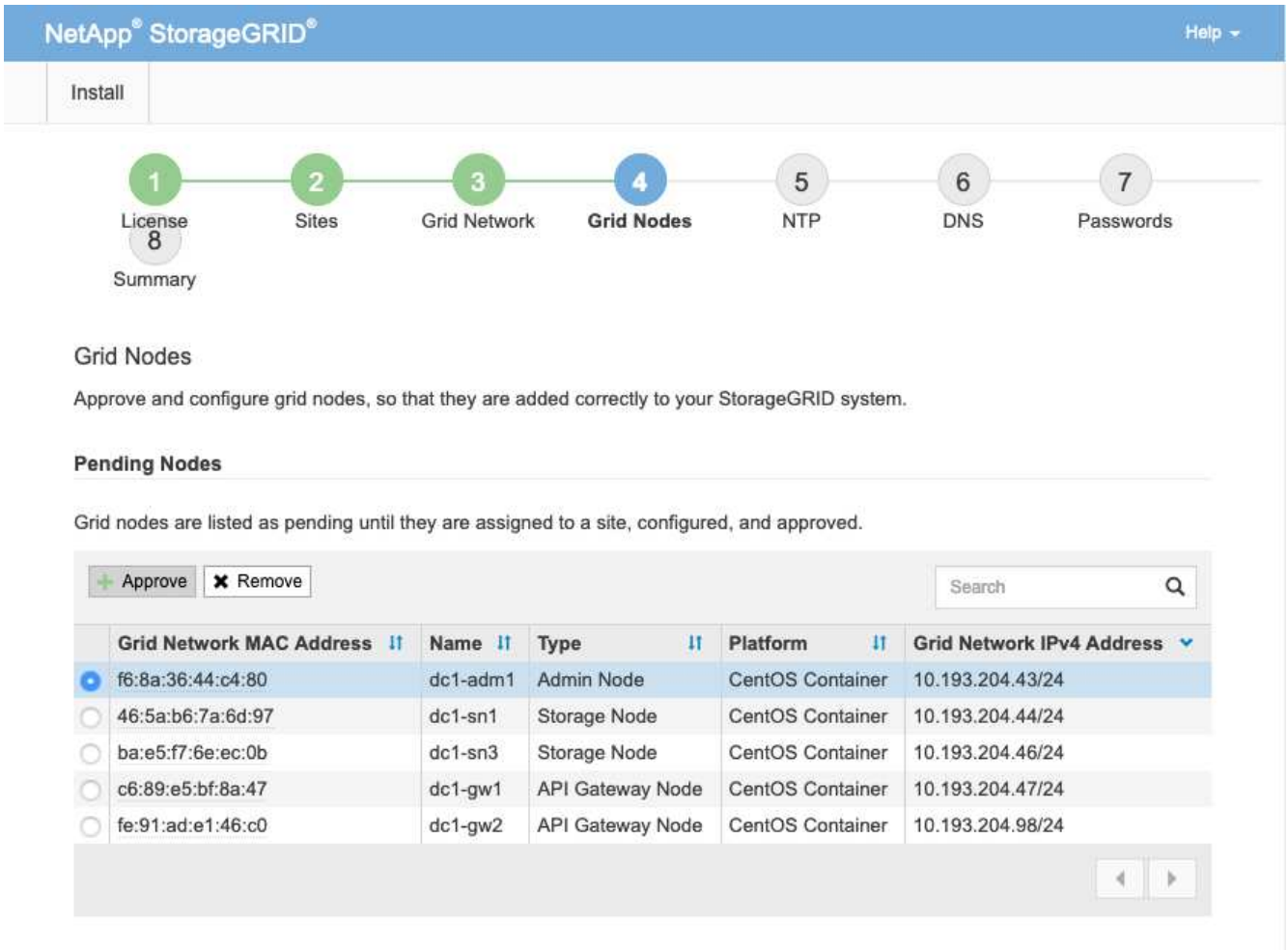
Si seleccionó DHCP para la configuración de red de administración y cambia aquí el valor, el nuevo valor se configura como una dirección estática en el nodo. Asegúrese de que la dirección IP resultante no esté en un pool de direcciones DHCP.

- Dispositivos*: Para un dispositivo StorageGRID, si la red de administración no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:
  a. Reinicie el dispositivo: En el instalador del dispositivo, seleccione **Avanzado › Reiniciar**. El reinicio puede tardar varios minutos.
  b. Seleccione MENU:Configure Networking[Link Configuration] y habilite las redes adecuadas.
  c. Seleccione MENU:Configure Networking[IP Configuration] y configure las redes habilitadas.
  d. Vuelva a la página de inicio y haga clic en Iniciar instalación.
  e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, restablezca el nodo.
  f. Quite el nodo de la tabla Pending Nodes.
  g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
  h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página IP Configuration. Para obtener información adicional, consulte las instrucciones de instalación y mantenimiento del modelo de dispositivo.

7. Si desea configurar la Red cliente para el nodo de cuadrícula, agregue o actualice los ajustes en la sección Red cliente según sea necesario. Si se configura la red de cliente, se requiere la puerta de enlace y se convierte en la puerta de enlace predeterminada del nodo después de la instalación.

   Electrodomésticos: Para un dispositivo StorageGRID, si la red cliente no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del dispositivo, seleccione **Avanzado › Reiniciar**. El reinicio puede tardar varios minutos.
   b. Seleccione MENU:Configure Networking[Link Configuration] y habilite las redes adecuadas.
   c. Seleccione MENU:Configure Networking[IP Configuration] y configure las redes habilitadas.
   d. Vuelva a la página de inicio y haga clic en Iniciar instalación.
   e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, restablezca el nodo.
   f. Quite el nodo de la tabla Pending Nodes.
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página IP Configuration. Para obtener más información, consulte las instrucciones de instalación y mantenimiento del dispositivo.
8. Haga clic en Guardar. La entrada del nodo de grid se mueve a la lista de nodos aprobados.



9. Repita los pasos 1-8 para cada nodo de cuadrícula pendiente que desee aprobar.

   Debe aprobar todos los nodos que desee de la cuadrícula. Sin embargo, puede volver a esta página en cualquier momento antes de hacer clic en Instalar en la página Resumen. Para modificar las propiedades de un nodo de cuadrícula aprobado, haga clic en su botón de opción y, a continuación, haga clic en Editar.

10. Cuando haya terminado de aprobar los nodos de cuadrícula, haga clic en Siguiente.

Especifique los detalles del servidor NTP para StorageGRID

Aprenda a especificar la información de configuración NTP para su sistema StorageGRID para que las operaciones realizadas en servidores independientes puedan mantenerse sincronizadas.

Para evitar problemas con la desviación de tiempo, debe especificar cuatro referencias de servidor NTP externo del estrato 3 o superior.

> Al especificar el origen NTP externo para una instalación StorageGRID de nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de hora en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible con Microsoft para su uso en entornos exigentes como StorageGRID.

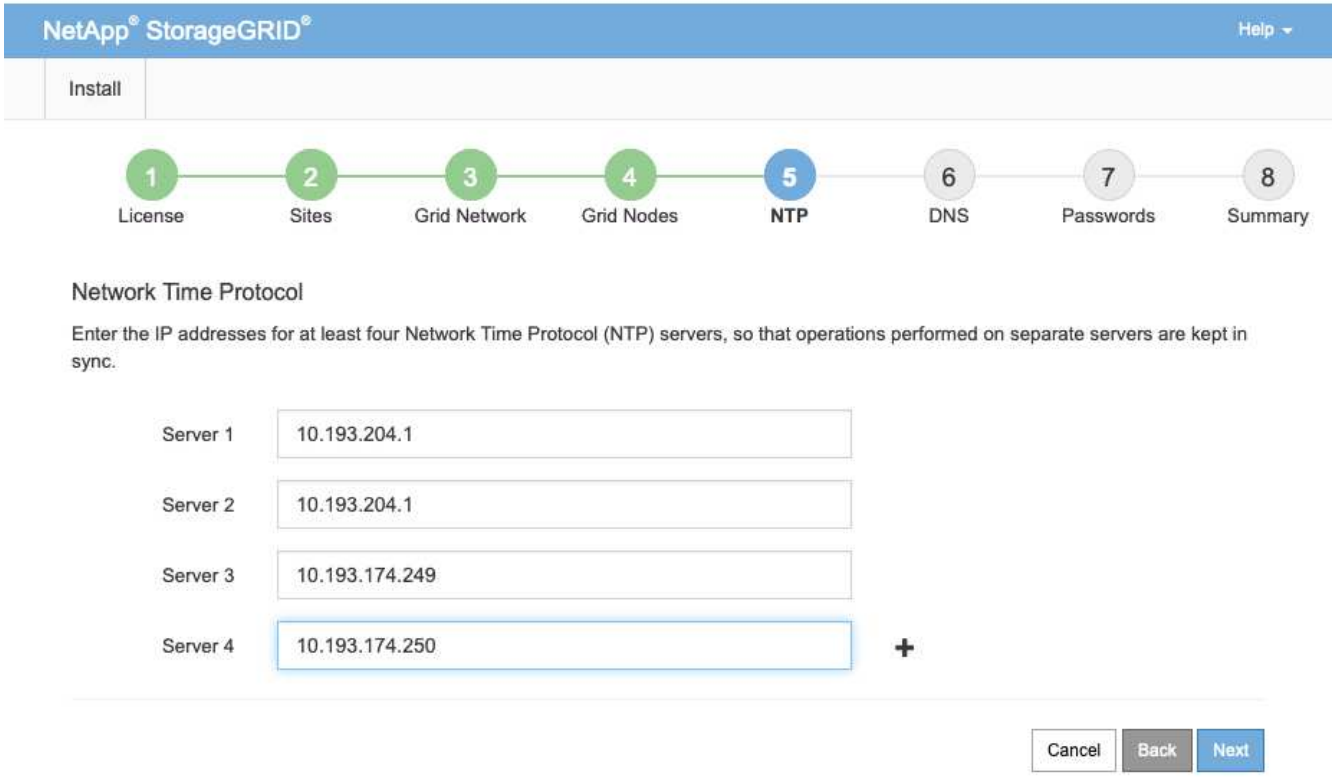
Los nodos a los que se asignaron anteriormente los roles NTP primarios utilizan los servidores NTP externos.

> La red cliente no se activa lo suficientemente temprano en el proceso de instalación para ser la única fuente de servidores NTP. Asegúrese de que se pueda acceder al menos a un servidor NTP a través de la red de grid o la red de administración.

Para especificar la información del servidor NTP, realice los siguientes pasos:

Pasos

1. En los cuadros de texto Server 1 to Server 4, especifique las direcciones IP para al menos cuatro servidores NTP.
2. Si es necesario, haga clic en el signo más junto a la última entrada para agregar más entradas de servidor.



3. Haga clic en Siguiente.

Especifique los detalles del servidor DNS para StorageGRID

Aprenda a configurar el servidor DNS para StorageGRID.

Debe especificar la información DNS del sistema StorageGRID de modo que pueda acceder a los servidores externos mediante nombres de host en lugar de direcciones IP.

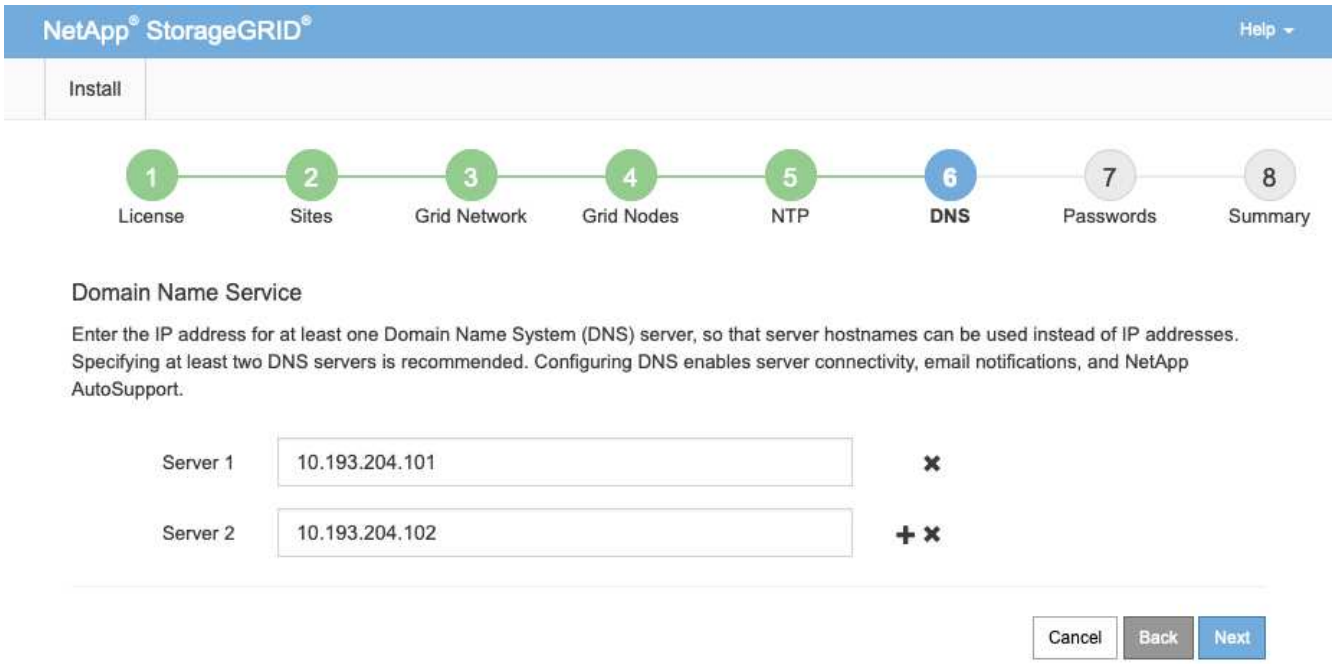
La especificación de la información del servidor DNS le permite utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones de correo electrónico y mensajes de NetApp AutoSupport®. NetApp recomienda especificar al menos dos servidores DNS.

Debe seleccionar los servidores DNS a los que puede acceder cada sitio localmente en el caso de que la red sea de destino.

Para especificar la información del servidor DNS, complete los siguientes pasos:

Pasos

1. En el cuadro de texto Server 1, especifique la dirección IP de un servidor DNS.
2. Si es necesario, haga clic en el signo más situado junto a la última entrada para agregar más servidores.



3. Haga clic en Siguiente.

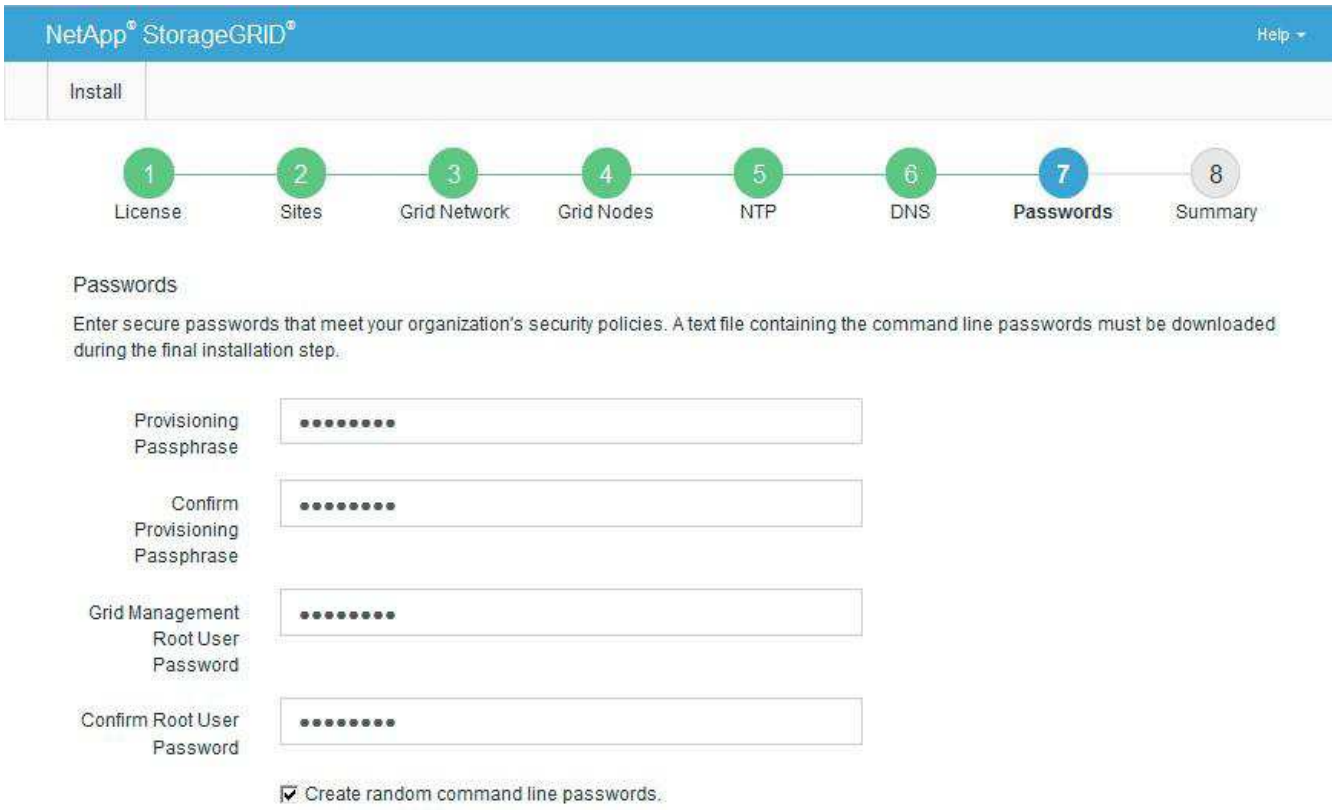
Especifique las contraseñas del sistema para StorageGRID

Aprenda a proteger su sistema StorageGRID configurando la clave de acceso de aprovisionamiento y la contraseña de usuario raíz de administración de grid.

Para introducir las contraseñas que se utilizarán para proteger el sistema StorageGRID, siga estos pasos:

Pasos

1. En Passphrase de aprovisionamiento, introduzca la clave de acceso de aprovisionamiento que se necesitará para realizar cambios en la topología de grid del sistema StorageGRID. Debe registrar esta contraseña en un lugar seguro.
2. En Confirm Provisioning Passphrase, vuelva a introducir la clave de acceso de provisionamiento.
3. En Contraseña de usuario raíz de gestión de grid, introduzca la contraseña que desea utilizar para acceder a Grid Manager como usuario raíz.
4. En Confirmar contraseña de usuario raíz, vuelva a introducir la contraseña de Grid Manager.



5. Si va a instalar una cuadrícula con fines de prueba de concepto o demostración, desactive la opción Crear contraseñas de línea de comandos aleatoria.

   En las implementaciones de producción, las contraseñas aleatorias deben utilizarse siempre por motivos de seguridad. Anule la selección de la opción Crear contraseñas de línea de comandos aleatoria solo para cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a los nodos de cuadrícula desde la línea de comandos mediante la cuenta raíz o de administrador.

   > Al hacer clic en Instalar en la página Resumen, se le pedirá que descargue el archivo Paquete de recuperación (`sgws-recovery-packageid-revision.zip`). Debe descargar este archivo para completar la instalación. Las contraseñas para acceder al sistema se almacenan en el `Passwords.txt` archivo, contenido en el archivo del paquete de recuperación.

6. Haga clic en Siguiente.

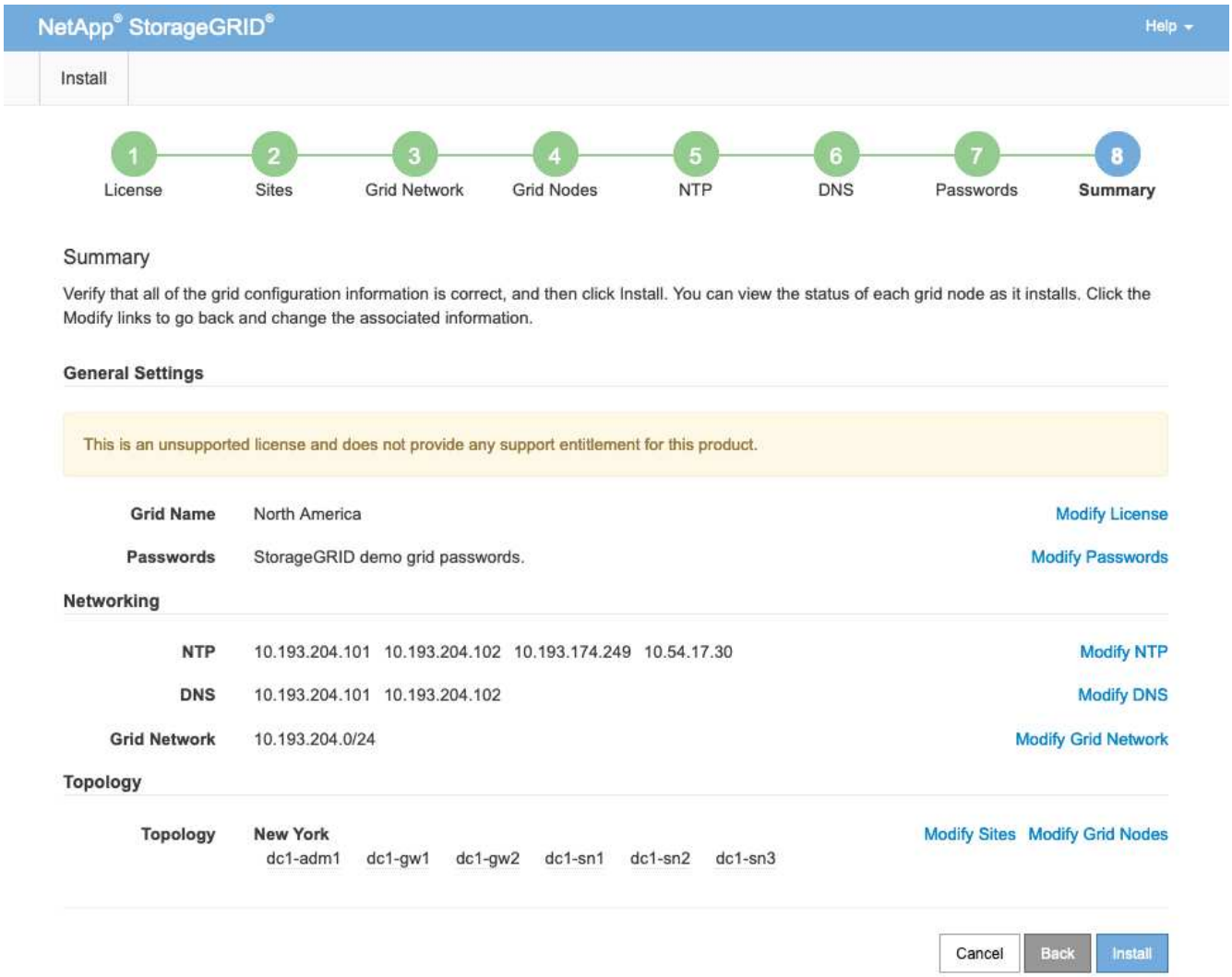
Revisar la configuración y completar la instalación de StorageGRID

Aprenda a validar la información de configuración de grid y a completar el proceso de instalación de StorageGRID.

Para asegurarse de que la instalación se complete correctamente, revise cuidadosamente la información de configuración que ha introducido. Siga estos pasos.

Pasos

1. Abra la página Resumen.



2. Verifique que toda la información de configuración de la cuadrícula sea correcta. Utilice los enlaces Modify de la página Summary para volver atrás y corregir los errores.
3. Haga clic en instalar.

> Si un nodo está configurado para usar la red cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red cliente al hacer clic en Instalar. Si pierde conectividad, asegúrese de acceder al nodo de administración principal a través de una subred accesible. Para obtener más información, consulte «Instalación y aprovisionamiento de red».

4. Haga clic en Download Recovery Package.

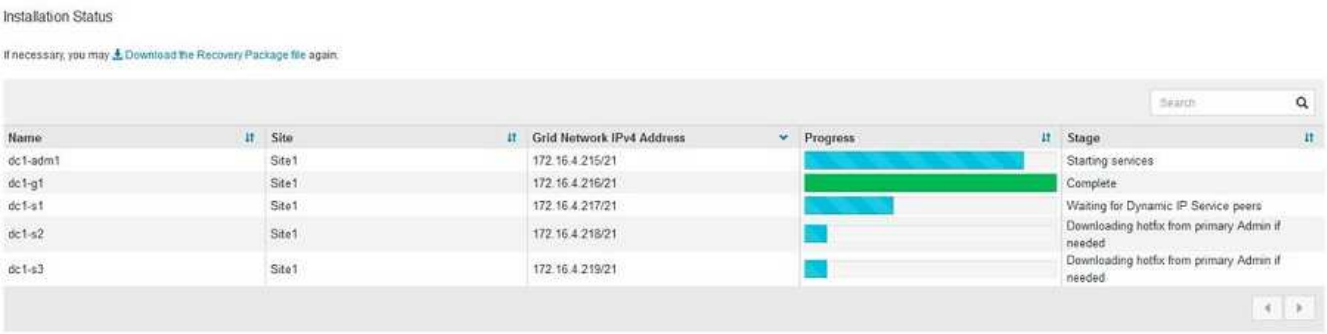
   Cuando la instalación avanza hasta el punto en el que se define la topología de cuadrícula, se le solicita que descargue el archivo Recovery Package (`.zip`) y confirme que puede acceder al contenido de este archivo. Debe descargar el archivo del paquete de recuperación para poder recuperar el sistema StorageGRID en caso de que falle uno o más nodos de grid.

   Compruebe que puede extraer el contenido del `.zip` archivo y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

5. Seleccione la opción He descargado y verificado correctamente el archivo del paquete de recuperación y, a continuación, haga clic en Siguiente.

Si la instalación aún está en curso, se abre la página Estado de la instalación. Esta página indica el progreso de la instalación para cada nodo de cuadrícula.



Cuando se alcanza la etapa completa para todos los nodos de cuadrícula, se abre la página de inicio de sesión para Grid Manager.

6. Inicie sesión en Grid Manager como usuario raíz con la contraseña que especificó durante la instalación.

Actualice los nodos de configuración básica en StorageGRID

Conozca el proceso de actualización de nodos con configuración básica en StorageGRID.

El proceso de actualización de los nodos con configuración básica es distinto al de los dispositivos o los nodos de VMware. Antes de realizar una actualización de un nodo de configuración básica, primero debe actualizar los archivos RPM en todos los hosts antes de ejecutar la actualización a través de la GUI.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

Ahora puede continuar con la actualización de software a través de la GUI.

TR-4907: Configuración de StorageGRID con veritas Enterprise Vault

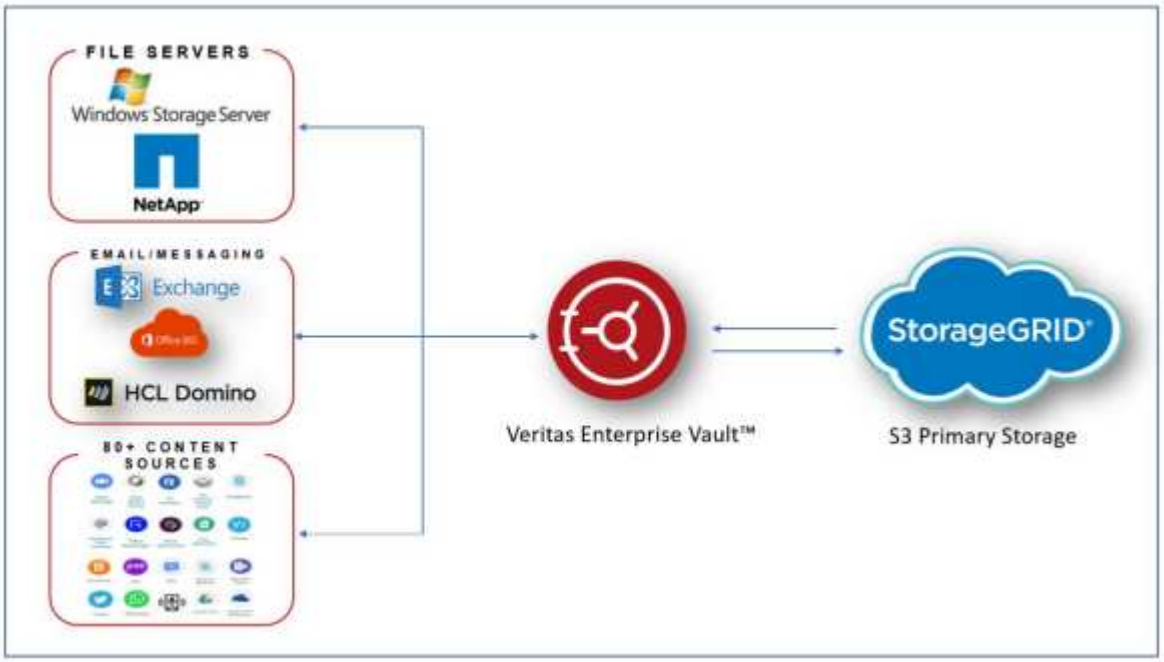
Introducción a la configuración de StorageGRID para conmutación por error del sitio

Descubre cómo veritas Enterprise Vault utiliza StorageGRID como destino de almacenamiento principal para la recuperación ante desastres.

Esta guía de configuración proporciona los pasos para configurar NetApp® StorageGRID® como destino de almacenamiento principal con veritas Enterprise Vault. También describe cómo configurar StorageGRID para conmutación por error de sitios en un escenario de recuperación ante desastres (DR).

Flexible y escalable

StorageGRID proporciona un objetivo de backup de cloud compatible con S3 en las instalaciones para veritas Enterprise Vault. La figura siguiente muestra la arquitectura veritas Enterprise Vault y StorageGRID.



Dónde encontrar información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Centro de documentación de NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/

- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

Configuración de StorageGRID y veritas Enterprise Vault

Descubra cómo implementar configuraciones básicas para StorageGRID 11,5 o posterior y veritas Enterprise Vault 14,1 o posterior.

Esta guía de configuración se basa en StorageGRID 11,5 y Enterprise Vault 14,1. Para el almacenamiento en modo de escritura única y lectura múltiple (WORM) utilizando bloqueo de objetos de S3 KB, se utilizó StorageGRID 11,6 y Enterprise Vault 14.2.2. Para obtener información más detallada sobre estas directrices, consulte "Documentación de StorageGRID" la página o póngase en contacto con un experto de StorageGRID.

Requisitos previos para configurar StorageGRID y veritas Enterprise Vault

- Antes de configurar StorageGRID con veritas Enterprise Vault, compruebe los siguientes requisitos previos:

> Para el ALMACENAMIENTO WORM (Object Lock), se requiere StorageGRID 11,6 o superior.

- Hay instalado veritas Enterprise Vault 14,1 o superior.

> Para el ALMACENAMIENTO WORM (Object Lock), se requiere Enterprise Vault versión 14.2.2 o superior.

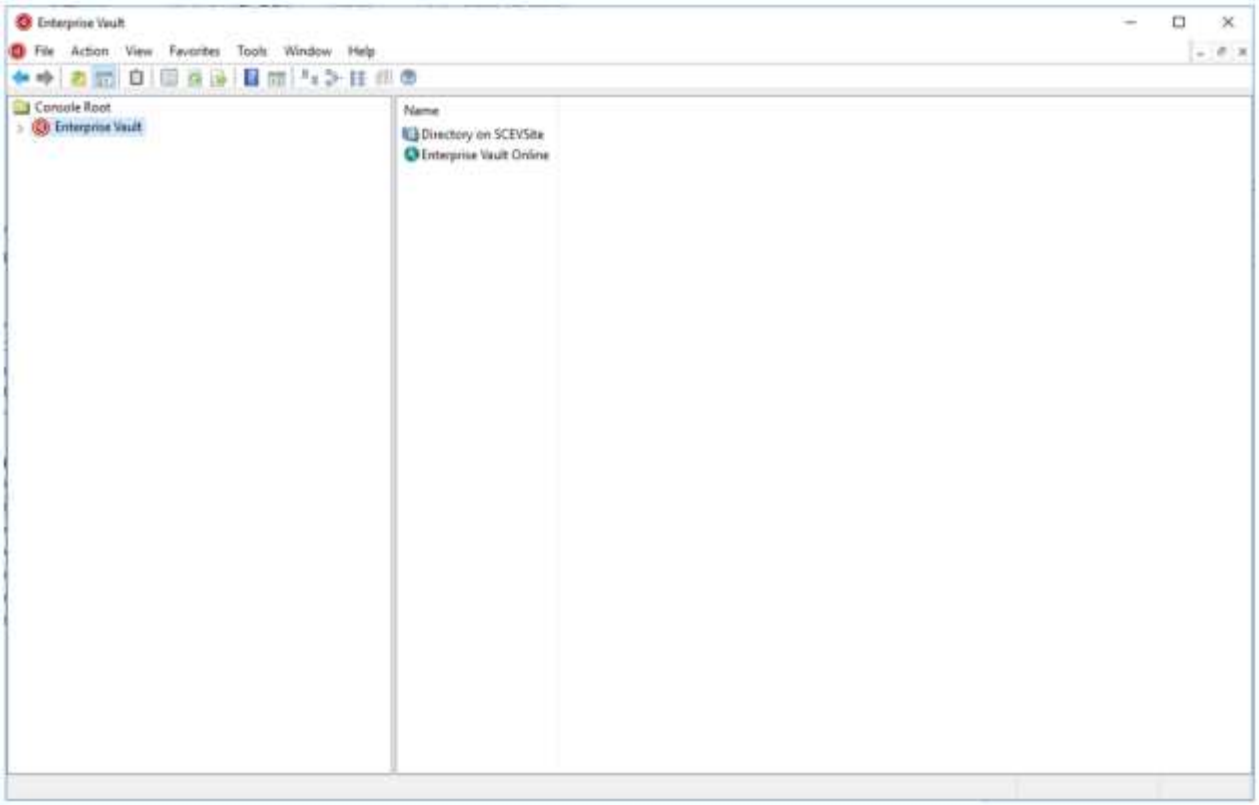
- Se han creado grupos de almacenes de almacén y un almacén de almacén. Si quiere más información, consulte la Guía de administración de veritas Enterprise Vault.
- Se creó un inquilino de StorageGRID, una clave de acceso, una clave secreta y un bloque.
- Se creó un extremo de equilibrador de carga de StorageGRID (HTTP o HTTPS).
- Si utiliza un certificado autofirmado, agregue el certificado de CA autofirmado de StorageGRID a los servidores de Enterprise Vault. Para obtener más información, consulte este "Artículo de la base de conocimientos de veritas".
- Actualice y aplique el archivo de configuración más reciente de Enterprise Vault para habilitar soluciones de almacenamiento compatibles como NetApp StorageGRID. Para obtener más información, consulte este "Artículo de la base de conocimientos de veritas".

Configuración de StorageGRID con veritas Enterprise Vault

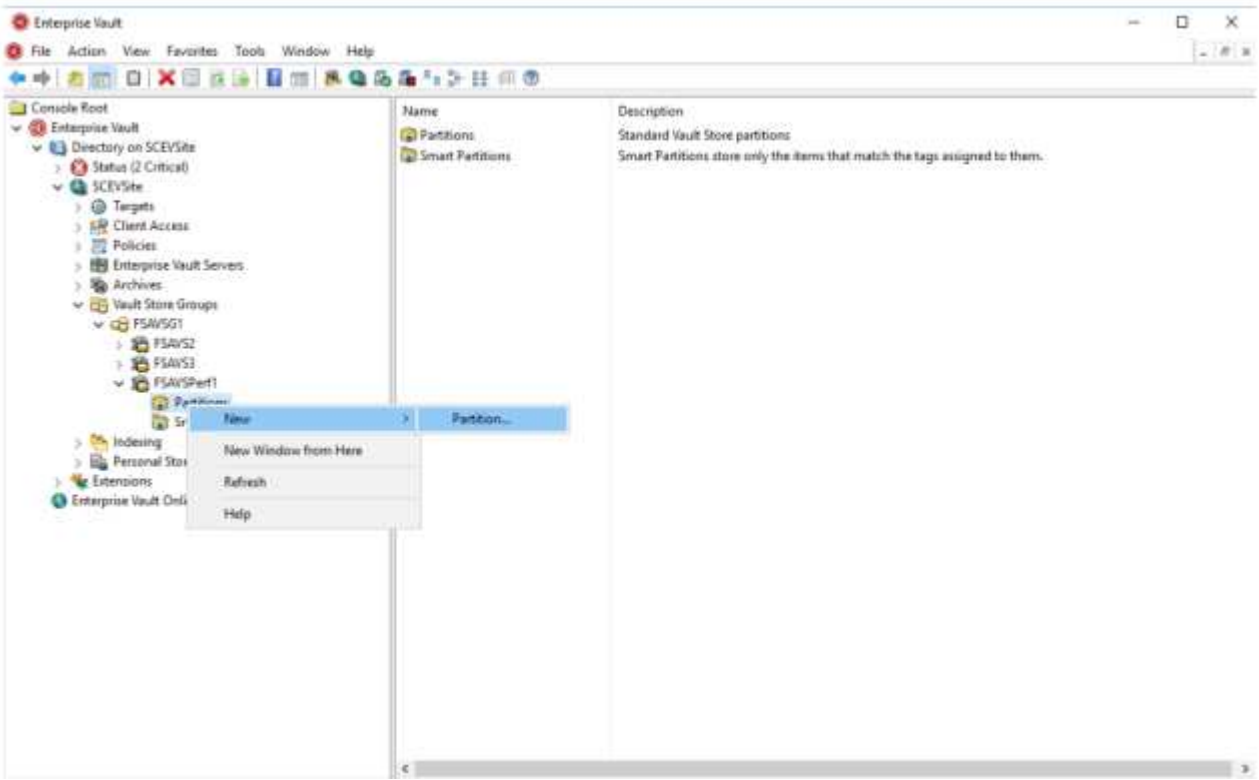
Para configurar StorageGRID con veritas Enterprise Vault, siga estos pasos:

Pasos

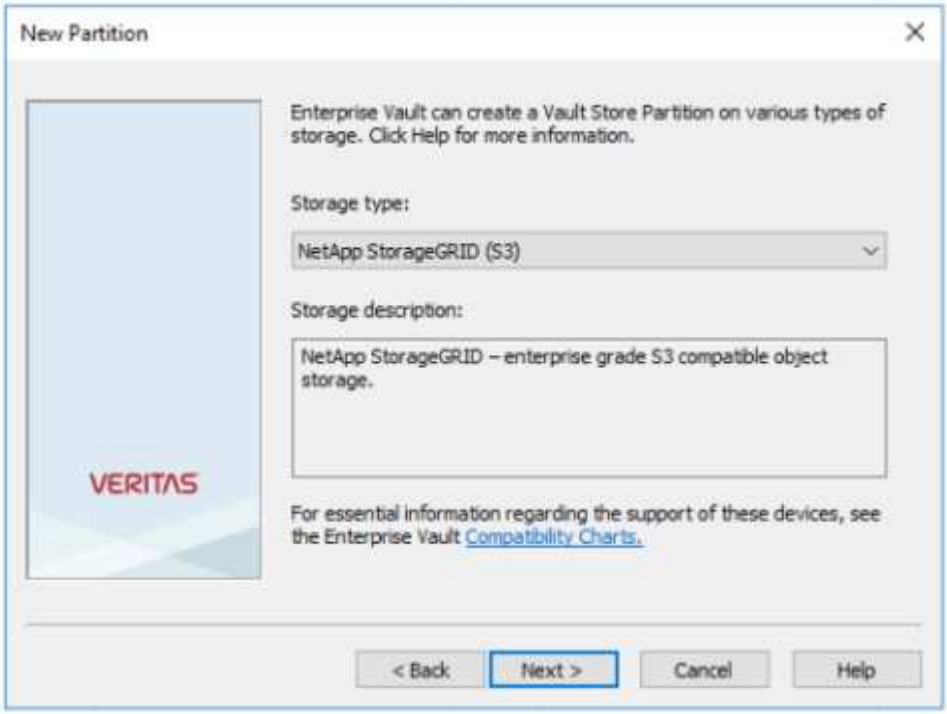
1. Inicie la consola de administración de Enterprise Vault.



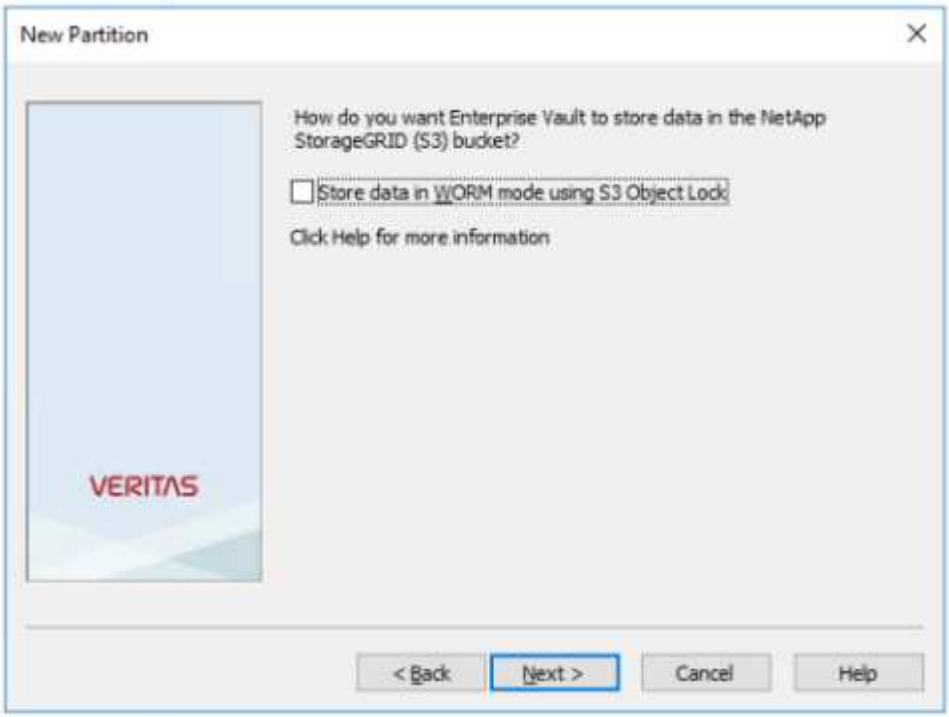
2. Cree una nueva partición de almacén de almacén en el almacén de almacén apropiado. Expanda la carpeta Grupos de Almacén de Almacén y, a continuación, el almacén de almacén apropiado. Haga clic con el botón derecho del ratón en Partición y seleccione el menú Nuevo[Partición].



3. Siga el asistente de creación de nueva partición. En el menú desplegable Storage Type, seleccione NetApp StorageGRID (S3). Haga clic en Siguiente.

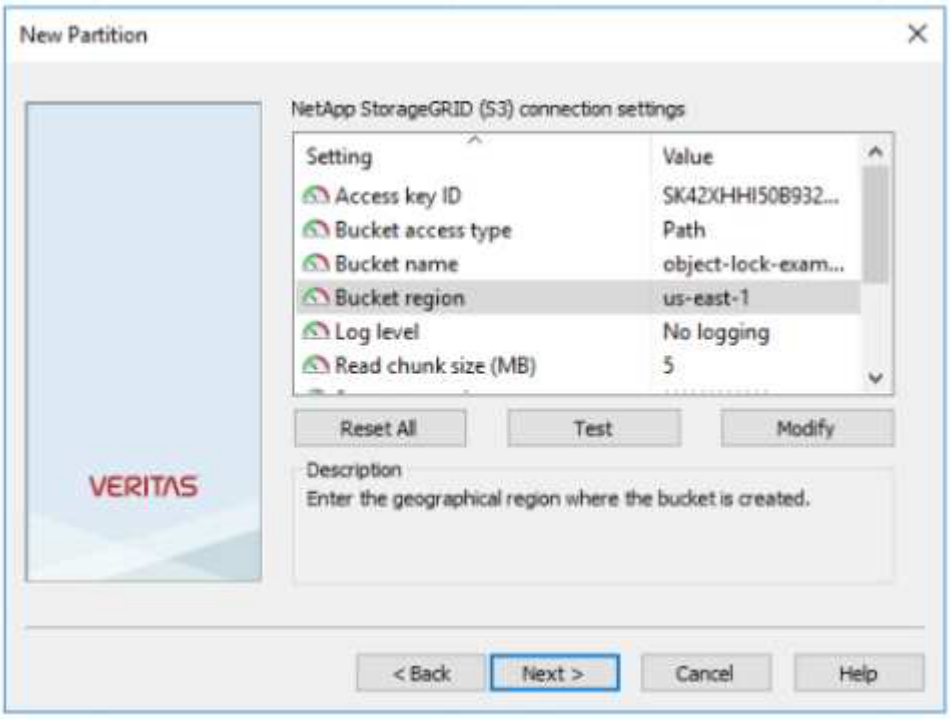


4. Deje la opción Almacenar datos en modo WORM con bloqueo de objetos S3 sin marcar. Haga clic en Siguiente.

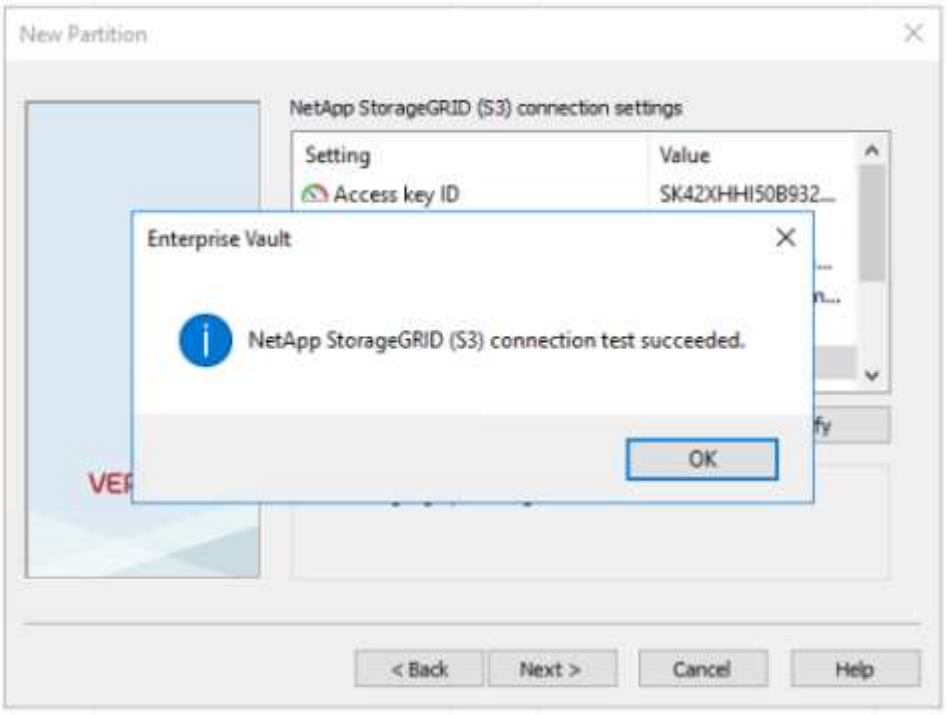


5. En la página de configuración de conexión, proporcione la siguiente información:
   - ID de clave de acceso
   - Clave de acceso secreta
   - Nombre de host del servicio: Asegúrese de incluir el puerto de punto final del equilibrador de carga (LBE) configurado en StorageGRID (como https://<hostname>:<LBE_port>)

- Nombre del bloque: Nombre del bloque de destino creado previamente. veritas Enterprise Vault no crea el bloque.
- Región de bloque: `us-east-1` Es el valor predeterminado.

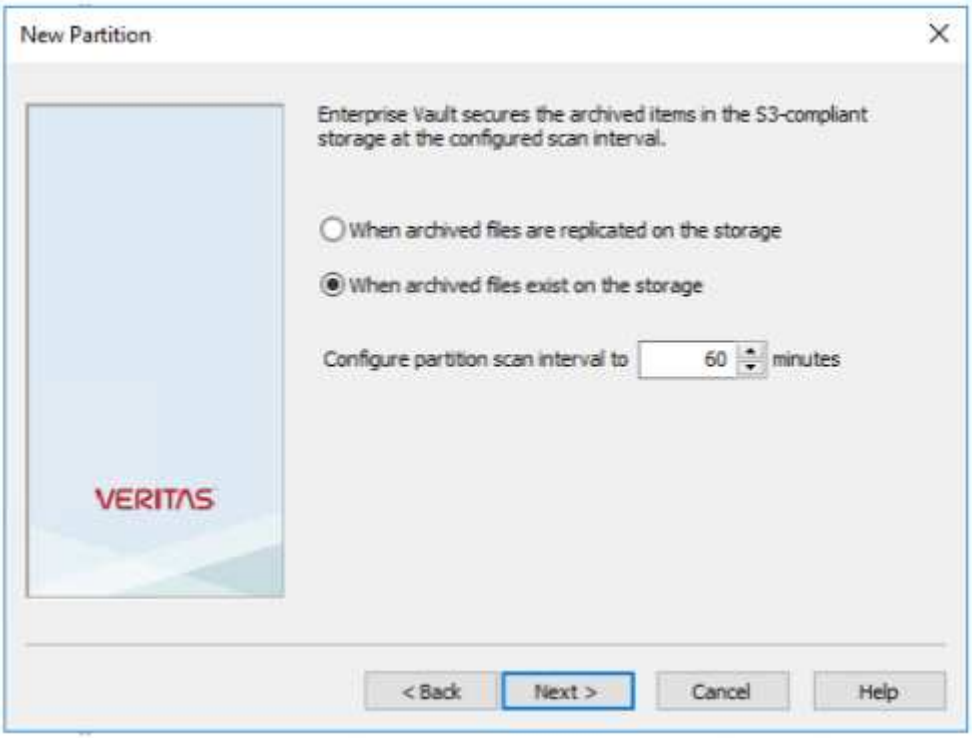


6. Para verificar la conexión con el depósito de StorageGRID, haga clic en Probar. Compruebe que la prueba de conexión se ha realizado correctamente. Haga clic en Aceptar y, a continuación, en Siguiente.

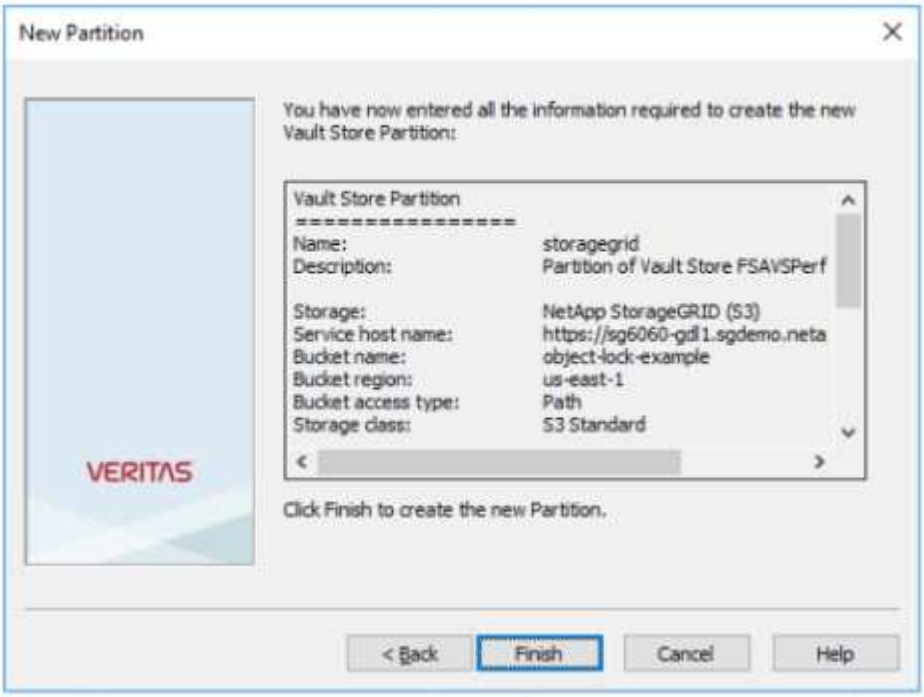


7. StorageGRID no admite el parámetro de replicación S3. Para proteger los objetos, StorageGRID utiliza las reglas de gestión del ciclo de vida de la información (ILM) para especificar esquemas de protección de datos: Varias copias o código de borrado. Seleccione la opción Cuando existen archivos archivados en el

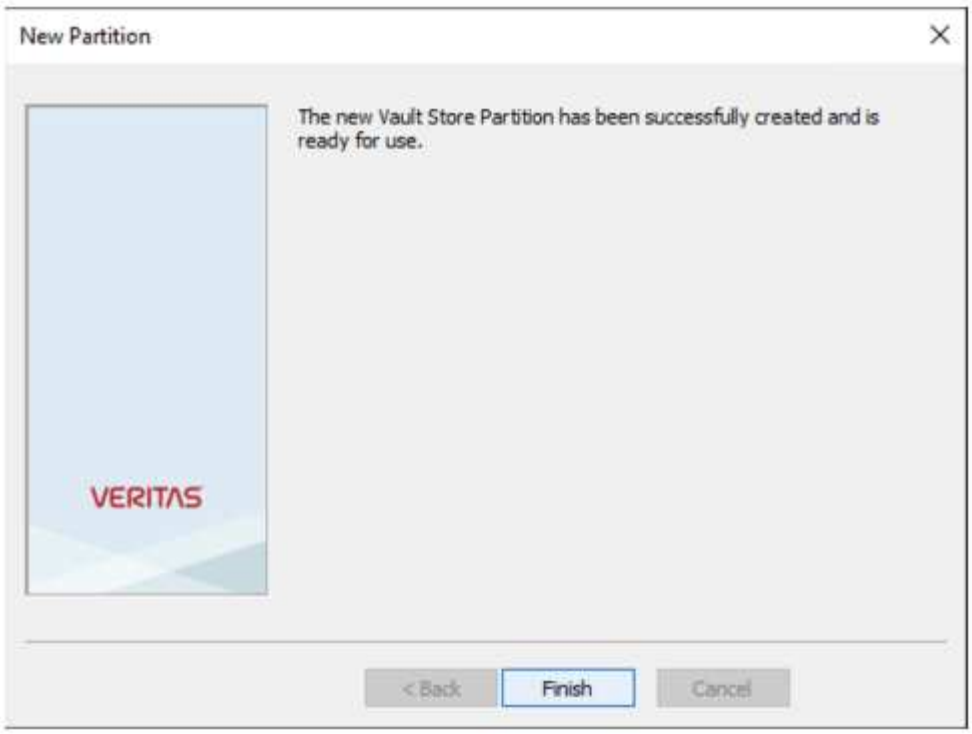
almacenamiento y haga clic en Siguiente.



8. Compruebe la información en la página de resumen y haga clic en Finish.



9. Una vez creada correctamente la nueva partición del almacén de almacén, puede archivar, restaurar y buscar datos en Enterprise Vault con StorageGRID como almacenamiento primario.



Configurar el bloqueo de objetos de StorageGRID S3 para el ALMACENAMIENTO WORM

Aprenda a configurar StorageGRID para el almacenamiento WORM con el bloqueo de objetos de S3.

Requisitos previos para configurar StorageGRID para ALMACENAMIENTO WORM

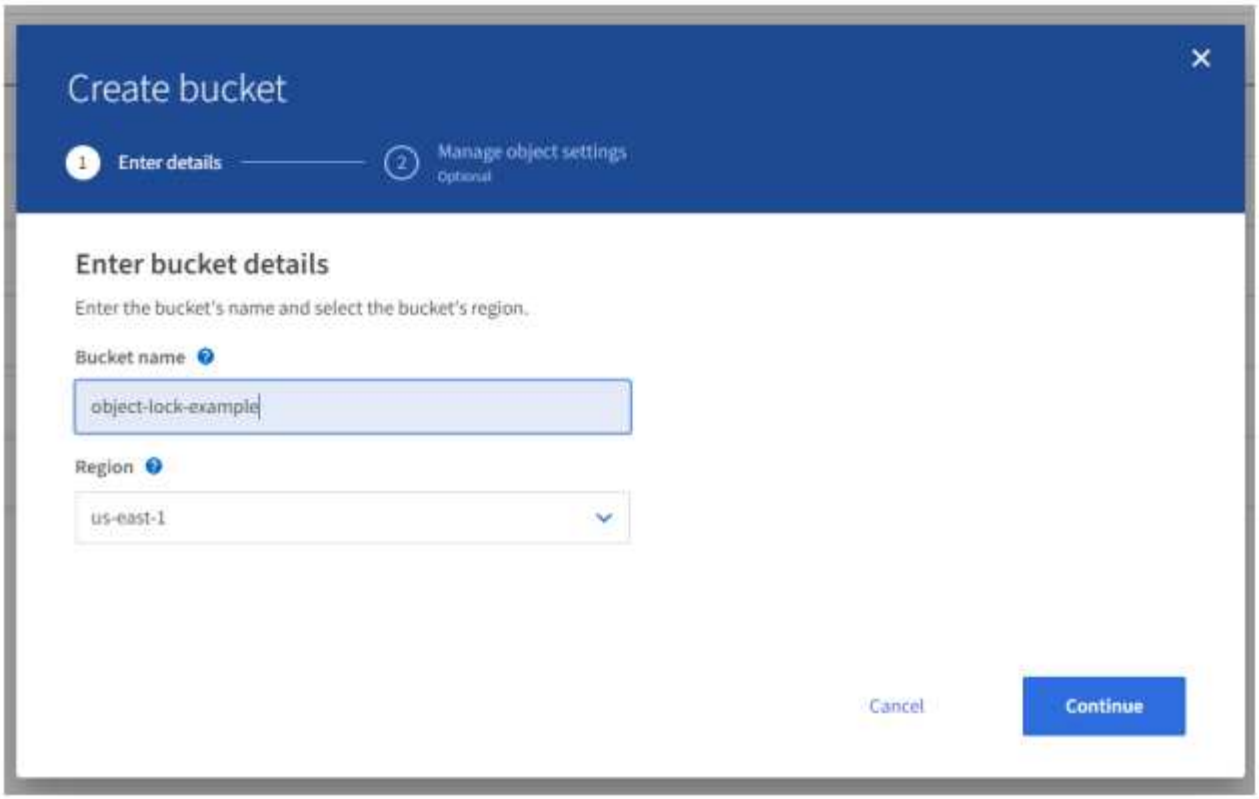
Para el ALMACENAMIENTO WORM, StorageGRID utiliza Object Lock de S3 para conservar objetos para garantizar el cumplimiento de normativas. Para ello se requiere StorageGRID 11,6 o posterior, donde se introdujo la retención de bloques predeterminados de S3 bloqueos de objetos. Enterprise Vault también requiere la versión 14.2.2 o superior.

Configure la retención de bloques predeterminados de bloqueo de objetos de StorageGRID S3

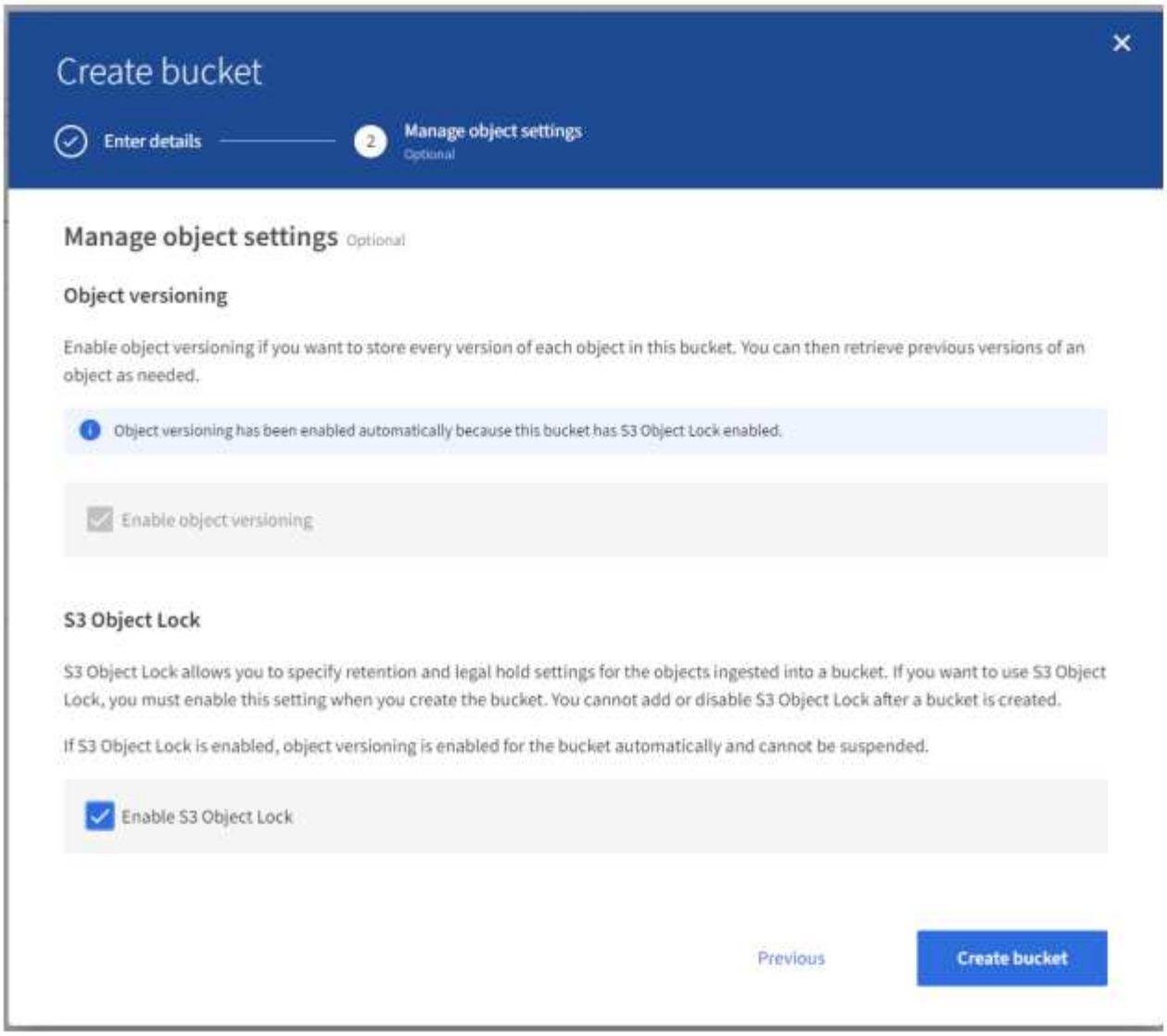
Para configurar la retención predeterminada del depósito de bloqueo de objetos de StorageGRID S3, lleve a cabo los siguientes pasos:

Pasos

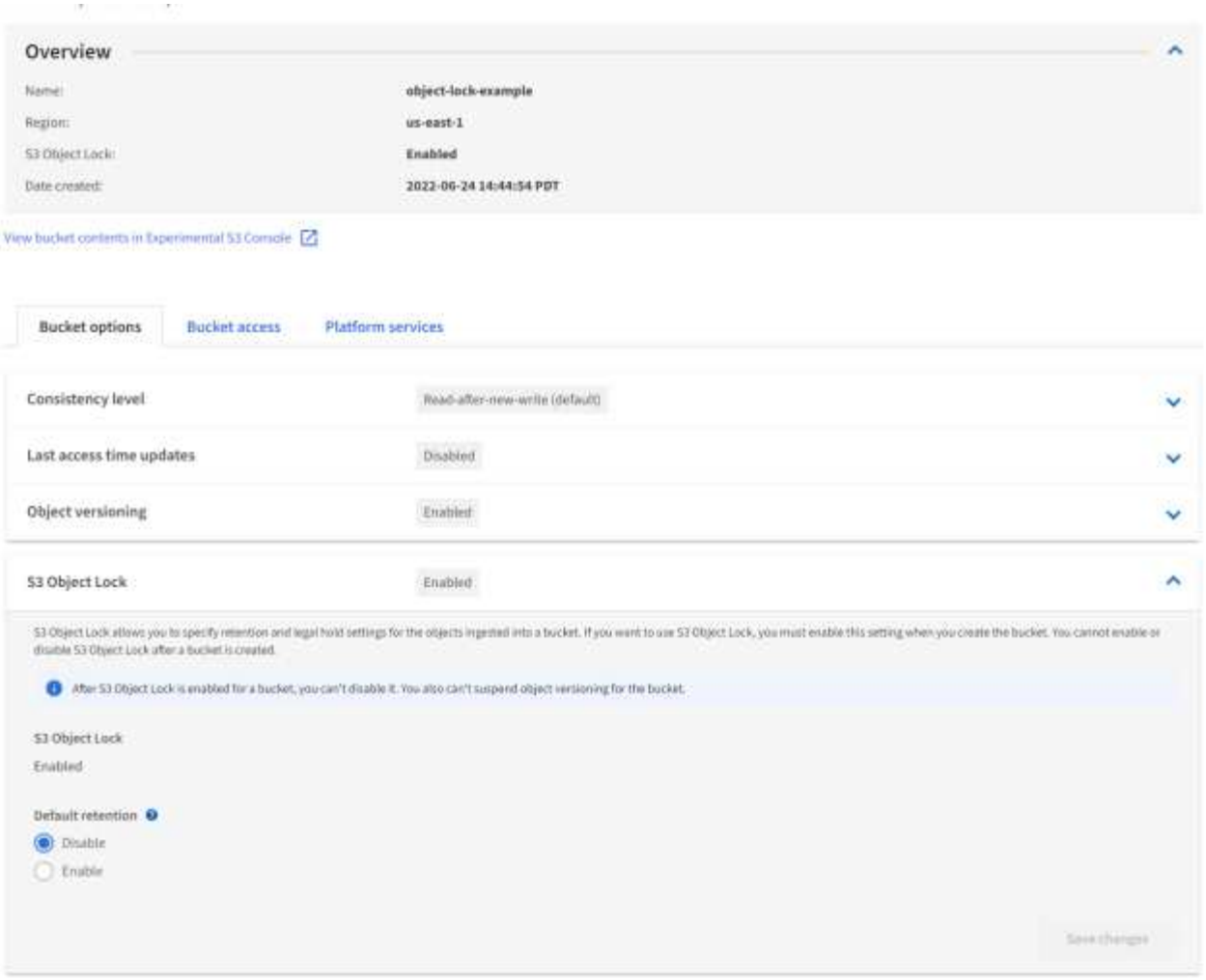
1. En el Administrador de inquilinos de StorageGRID, cree un bloque y haga clic en Continue



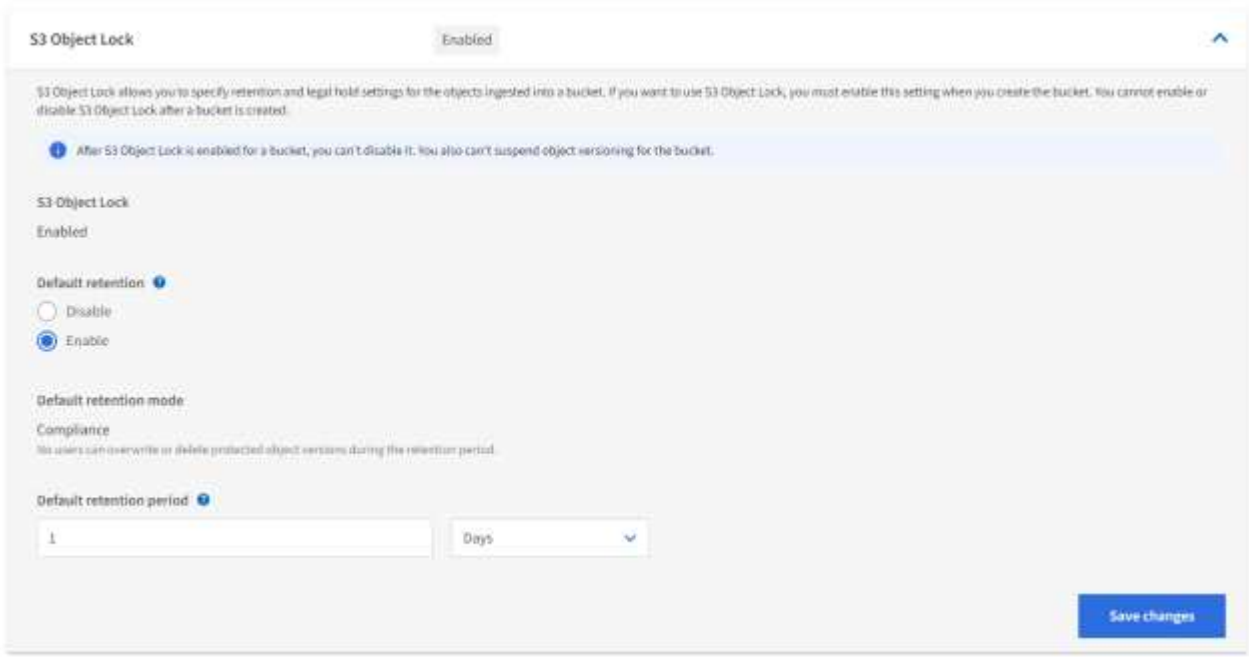
2. Seleccione la opción Enable S3 Object Lock y haga clic en Create Bucket.



3. Una vez creado el cucharón, seleccione el cucharón para ver las opciones del cucharón. Expanda la opción desplegable Bloqueo de objetos S3.



4. En Retención predeterminada, seleccione Habilitar y establezca un período de retención predeterminado de 1 día. Haga clic en Save Changes.



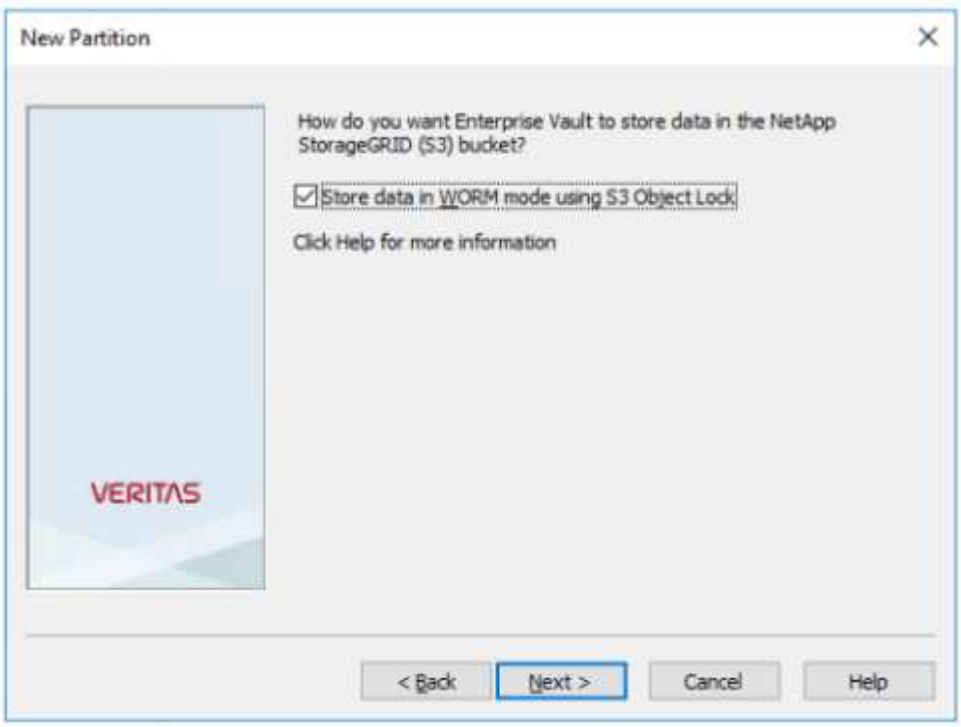
Enterprise Vault ya puede utilizar el bloque para almacenar DATOS WORM.

Configure Enterprise Vault

Para configurar Enterprise Vault, realice los siguientes pasos:

Pasos

1. Repita los pasos 1-3 en la "Configuración básica" sección, pero esta vez seleccione la opción Almacenar datos en el modo WORM utilizando S3 Object Lock. Haga clic en Siguiente.



2. Al introducir la configuración de conexión de S3 Bucket, asegúrese de introducir el nombre de un bucket de S3 que tenga habilitada la retención predeterminada de S3 Object Lock.
3. Pruebe la conexión para verificar la configuración.

Configurar la recuperación tras fallos del sitio StorageGRID para la recuperación ante desastres

Aprende a configurar la conmutación al nodo de respaldo del sitio StorageGRID en un escenario de recuperación de desastres.

Es un común que la puesta en marcha de una arquitectura de StorageGRID sea multisitio. Los sitios pueden ser activo-activo o activo-pasivo para recuperación de desastres. En un escenario de recuperación ante desastres, asegúrese de que veritas Enterprise Vault puede mantener la conexión con su almacenamiento principal (StorageGRID) y continuar procesando y recuperando los datos durante un fallo del centro. En esta sección se proporciona orientación de configuración de alto nivel para una puesta en marcha activo-pasivo en dos sitios. Para obtener información detallada sobre estas directrices, consulte "Documentación de StorageGRID" la página o póngase en contacto con un experto de StorageGRID.

Requisitos previos para configurar StorageGRID con veritas Enterprise Vault

Antes de configurar la conmutación por error del sitio StorageGRID, verifique los siguientes requisitos previos:

- Existe una puesta en marcha de StorageGRID en dos sitios, por ejemplo, site1 y Site2.
- Se ha creado un nodo de administración que ejecuta el servicio del equilibrador de carga o un nodo de pasarela, en cada sitio, para el equilibrio de carga.
- Se ha creado un extremo de equilibrador de carga de StorageGRID.

Configurar la recuperación tras fallos del sitio StorageGRID

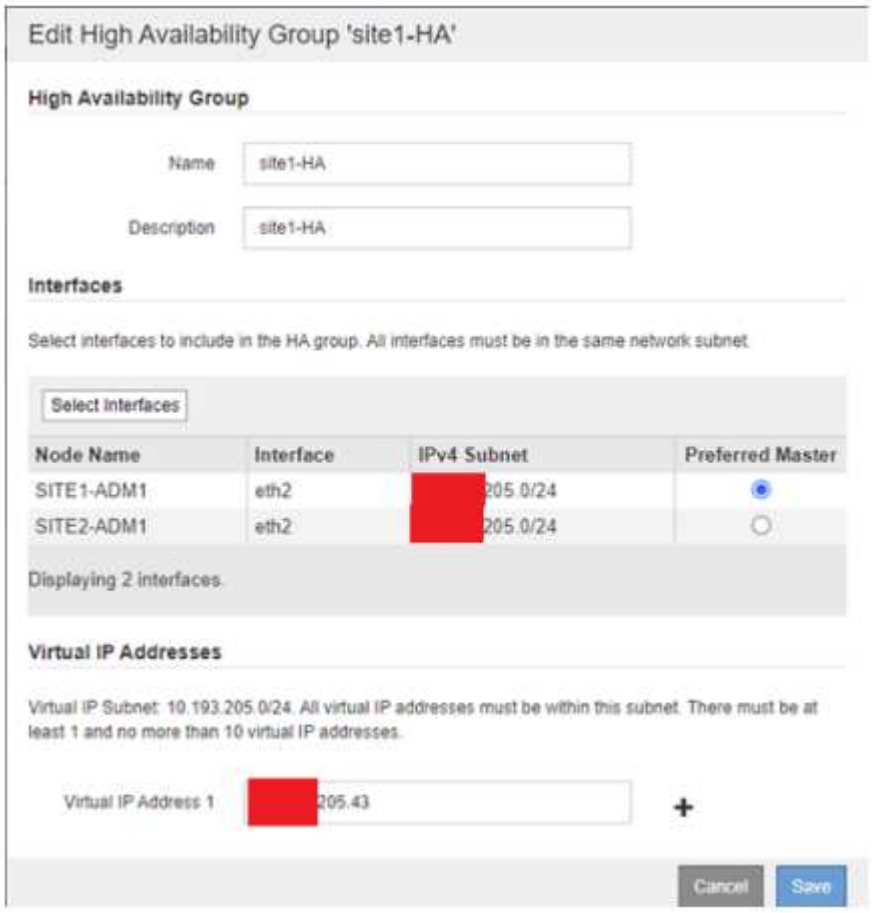
Para configurar la conmutación por error del sitio StorageGRID, lleve a cabo los siguientes pasos:

Pasos

1. Para garantizar la conectividad con StorageGRID durante los fallos del sitio, configure un grupo de alta disponibilidad. En la interfaz del administrador de grid de StorageGRID (GMI), haga clic en Configuración, Grupos de alta disponibilidad y + Crear.

   [grupo de alta disponibilidad de creación vertical/versas]

2. Especifique la información obligatoria. Haga clic en Seleccionar interfaces e incluya las interfaces de red de site1 y Site2 donde site1 (el sitio principal) es el maestro preferido. Asigne una dirección IP virtual dentro de la misma subred. Haga clic en Guardar.



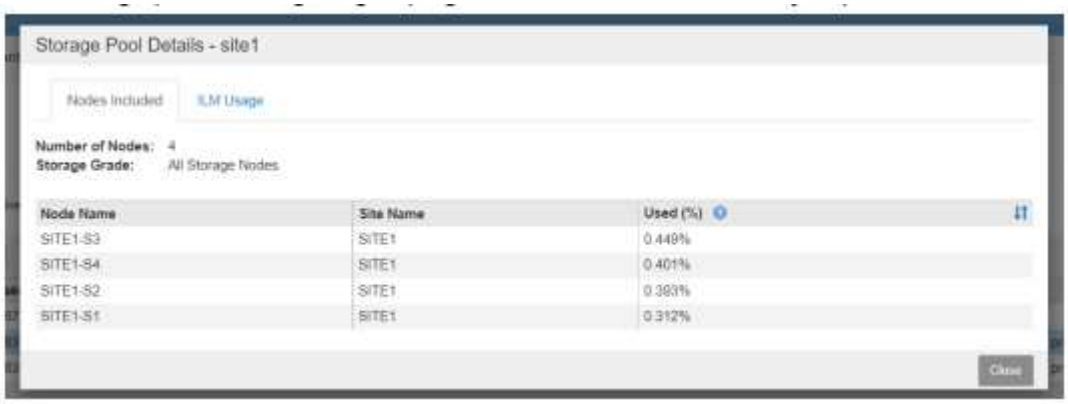
3. Esta dirección IP virtual (VIP) debe asociarse al nombre de host S3 utilizado durante la configuración de

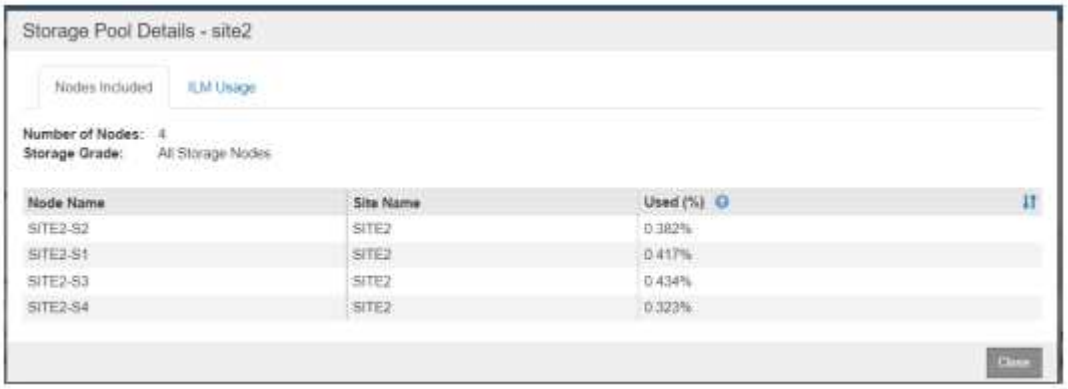
particiones de veritas Enterprise Vault. La dirección VIP resuelve el tráfico a site1 y, durante el fallo de site1, la dirección VIP redirige el tráfico de forma transparente A Site2.

4. Asegúrese de que los datos se replican tanto en site1 como en Site2. De esta forma, si site1 falla, los datos de objetos siguen disponibles en Site2. Para ello, primero se configuran los pools de almacenamiento.

   En StorageGRID GMI, haga clic en ILM, Pools de almacenamiento y, a continuación, en + Create. Siga al asistente para crear dos pools de almacenamiento: Uno para site1 y otro para Site2.

   Los pools de almacenamiento son agrupaciones lógicas de nodos que se utilizan para definir la ubicación del objeto





5. En StorageGRID GMI, haga clic en ILM, Reglas y, a continuación, en + Crear. Siga el asistente para crear una regla de ILM que especifique una copia para almacenar por sitio con un comportamiento de ingesta de equilibrada.

6. Agregue la regla de ILM a una política de ILM y active la política.

Esta configuración da como resultado el siguiente resultado:

- Una IP de extremo virtual S3 donde site1 es el primario y Site2 es el extremo secundario. Si site1 falla, el VIP se conmuta a Site2.
- Cuando se envían datos archivados desde veritas Enterprise Vault, StorageGRID garantiza que se almacene una copia en site1 y que se almacene otra en Site2. Si site1 falla, Enterprise Vault sigue ingiriendo y recuperando de Site2.

> Ambas configuraciones son transparentes para veritas Enterprise Vault. El punto final S3, el nombre del depósito, las claves de acceso, etc. son los mismos. No es necesario volver a configurar los ajustes de conexión S3 en la partición de veritas Enterprise Vault.

Pasos para acceder al software de evaluación StorageGRID

Esta instrucción está destinada al personal de ventas, partners y clientes potenciales asociados con NetApp de NetApp.

Regístrese para obtener una cuenta

1. Regístrese para obtener una cuenta en "Sitio de soporte de NetApp" utilizando su correo electrónico de empresa.
   a. Asegúrese de que no ha iniciado sesión con la cuenta recién creada.
   b. Si ya tiene una cuenta, asegúrese de que no ha iniciado sesión y continúe con el siguiente paso.
2. Crear un caso de soporte no técnico para elevar los niveles de acceso a «cliente potencial». Para ello, haga clic en el ""Notifique un problema"enlace " en el pie de página de la página web.
3. Seleccione «Problema de registro» como categoría de comentarios.
4. En la sección de comentarios, escriba: "Mi dirección de correo electrónico de la cuenta es *Su-Correo-Dirección*. Me gustaría obtener acceso a un posible cliente para descargar el software de evaluación de StorageGRID».
   a. Mencione el nombre de la persona interna de NetApp que sugirió la solicitud de acceso de un posible cliente.

Descargue StorageGRID

1. Una vez revisado y aprobado su caso de soporte, el soporte de NetApp le notificará a través de correo electrónico que se le ha otorgado acceso a su cuenta.
2. Descargue el "Software de evaluación StorageGRID".

El archivo de licencia Eval está ubicado dentro del archivo zip. Se trata de StorageGRID-Webscale-<version>\vsphere\NLF000000.txt una vez descomprimido.

La descarga del software es un proceso que implica medidas de cumplimiento comercial para cumplir con los requisitos legales. Para garantizar el cumplimiento, los usuarios deben crear una cuenta y abrir un caso de soporte antes de obtener acceso. Este proceso nos ayuda a mantener el control y la documentación adecuados, al tiempo que proporciona a los clientes potenciales el software listo para la producción que necesitan.

Proporcionamos una versión de StorageGRID «lista para la producción», que no es una versión de código abierto ni alternativa. Es importante tener en cuenta que no se proporciona **soporte** a menos que el cliente potencial actualice a una licencia de producción.

Póngase en contacto con StorageGRID.Feedback@netapp.com para cualquier problema con los pasos anteriores.

Blogs de StorageGRID de NetApp

Puede encontrar algunos de los grandes blogs de StorageGRID de NetApp aquí:

- 16 2024 de febrero: "Presentación de StorageGRID 11,8: Mayor seguridad, simplicidad y experiencia de usuario"
- 16 2024 de febrero: "Presentamos 11,8 de StorageGRID"
- 2 2024 de febrero: "Presentación del resumen de la solución StorageGRID + lakeFS"
- Dic 12 2023: "Análisis de Big Data en StorageGRID: Dremio se ejecuta 23 veces más rápido que Apache Hive"
- Noviembre de 7 2023: "Spectra Logic Glaciar en las instalaciones con StorageGRID"
- Octubre de 17 2023: "Pasando de Hadoop: Modernización del análisis de datos con Dremio y StorageGRID"
- Septiembre de 1 2023: "Aprovechamiento de Cloud Insights para supervisar y recopilar registros mediante bits fluentes"
- Agosto de 30 2023: "Mountpoint para Amazon S3 File System ahora es GA"
- Mayo de 16 2023: "Presentamos StorageGRID 11,7 y el nuevo dispositivo de almacenamiento de objetos all-flash SGF6112"
- Mayo de 16 2023: "Novedades de la familia de almacenamiento de objetos de StorageGRID"
- Marzo de 30 2023: "Punto de montaje para la versión alfa de Amazon S3 con StorageGRID"
- Marzo de 30 2023: "Utilice BlueXP para proteger Epic EHR con una política de backup conforme a las normativas 3:2:1"
- Marzo de 14 2023: "Cómo realizar backups de las bases de datos de EHR de Epic Systems con un comando en una arquitectura compatible con 3:2:1"
- 14 2023 de febrero: "¿Qué tienen en común el chocolate, el esquí, los relojes y los mainframes?"
- Ene 18 2023: "StorageGRID S3 Object Lock validado para veritas NetBackup"
- Ene 16 2023: "StorageGRID renueva la certificación de cumplimiento NF203 e ISO/IEC 25051"
- Dic 6 2022: "StorageGRID obtiene la certificación de cumplimiento de KPMG"
- Noviembre de 23 2022: "IA explicable con MLOps impulsado por NetApp y Modzy"
- Noviembre de 7 2022: "Compatibilidad con StorageGRID y ONTAP S3: Diferencias, similitudes e integración"
- Octubre de 5 2022: "Cloud Insights de NetApp añade consolas a la galería de StorageGRID"
- Octubre de 5 2022: "Descongele sus datos en StorageGRID para copo de nieve"
- Septiembre de 26 2022: "StorageGRID de NetApp para proveedores de servicios"
- Septiembre de 19 2022: "Soporte de bloqueo de datos y protección frente a ransomware para StorageGRID"
- Septiembre de 1 2022: "Tome estas métricas y grafíquelas"
- Agosto de 23 2022: "Cree su lago de datos en StorageGRID"
- Agosto de 17 2022: "Todo comienza con Object Locking… Creación de un ecosistema de almacenamiento S3 para aplicaciones de backup esenciales"
- Agosto de 16 2022: "Integración de StorageGRID con la pila ELK de código abierto para mejorar la

experiencia del cliente"

- Agosto de 5 2022: "StorageGRID de NetApp obtiene una certificación de seguridad de criterios comunes"
- 26 2022 de julio: "Consulte la creciente lista de soluciones de partners validadas para StorageGRID"
- 9 2022 de junio: "Utilice el conector Hadoop S3A de Cloudera con StorageGRID"
- Mayo de 26 2022: "StorageGRID: Almacenar y gestionar los datos de backup y replicación on-premises"
- Mayo de 24 2022: "Modernice sus cargas de trabajo de análisis con NetApp y Alluxio"
- Mayo de 10 2022: "Lab on Demand es su mejor herramienta de venta para StorageGRID"

Documentación de StorageGRID de NetApp

Puede encontrar la documentación completa de cada versión de StorageGRID de NetApp aquí:

- "Dispositivos StorageGRID"
- "Software StorageGRID 11.5 - 12.0"

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

https://library.netapp.com/ecm/ecm_download_file/2879263

https://library.netapp.com/ecm/ecm_download_file/2881511