Informes técnicos

StorageGRID solutions and resources

NetApp
December 12, 2025

Tabla de contenidos

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.

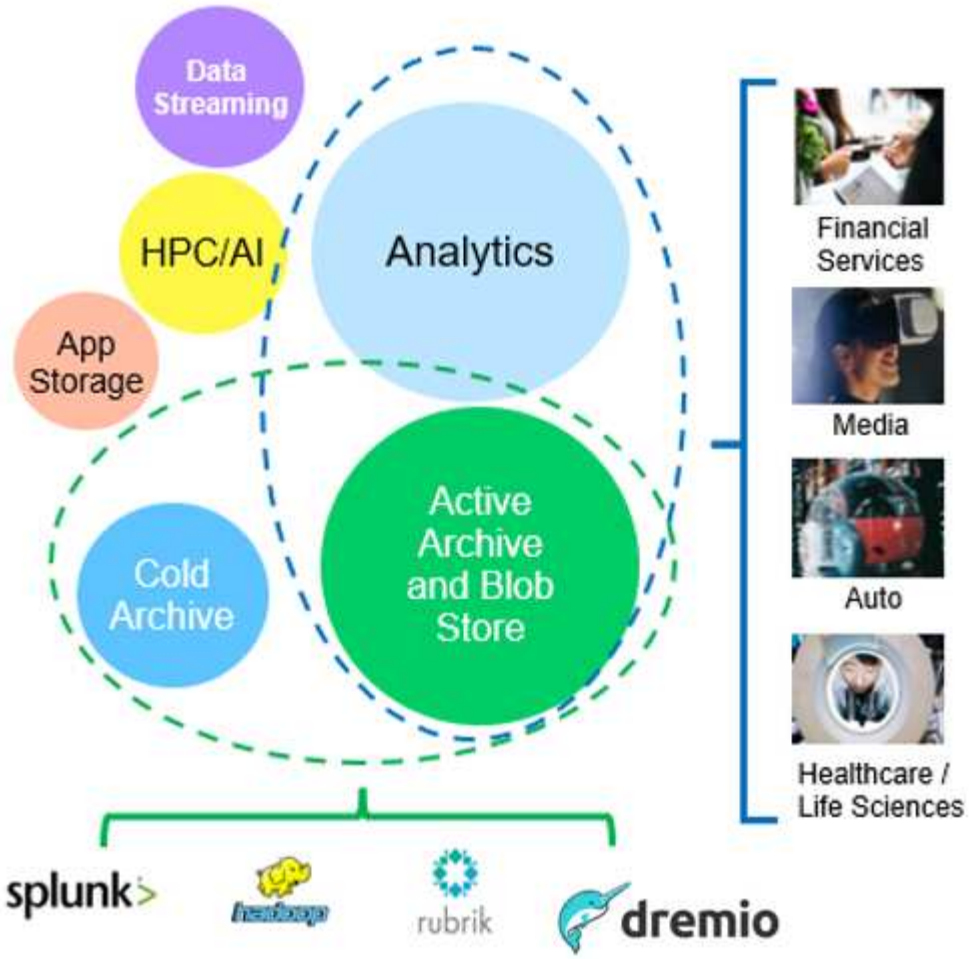
Respaldo de datos y recuperación de desastres: Las empresas pueden utilizar StorageGRID S3 como una solución confiable y rentable para hacer copias de seguridad de datos críticos y recuperarlos en caso de desastre.

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

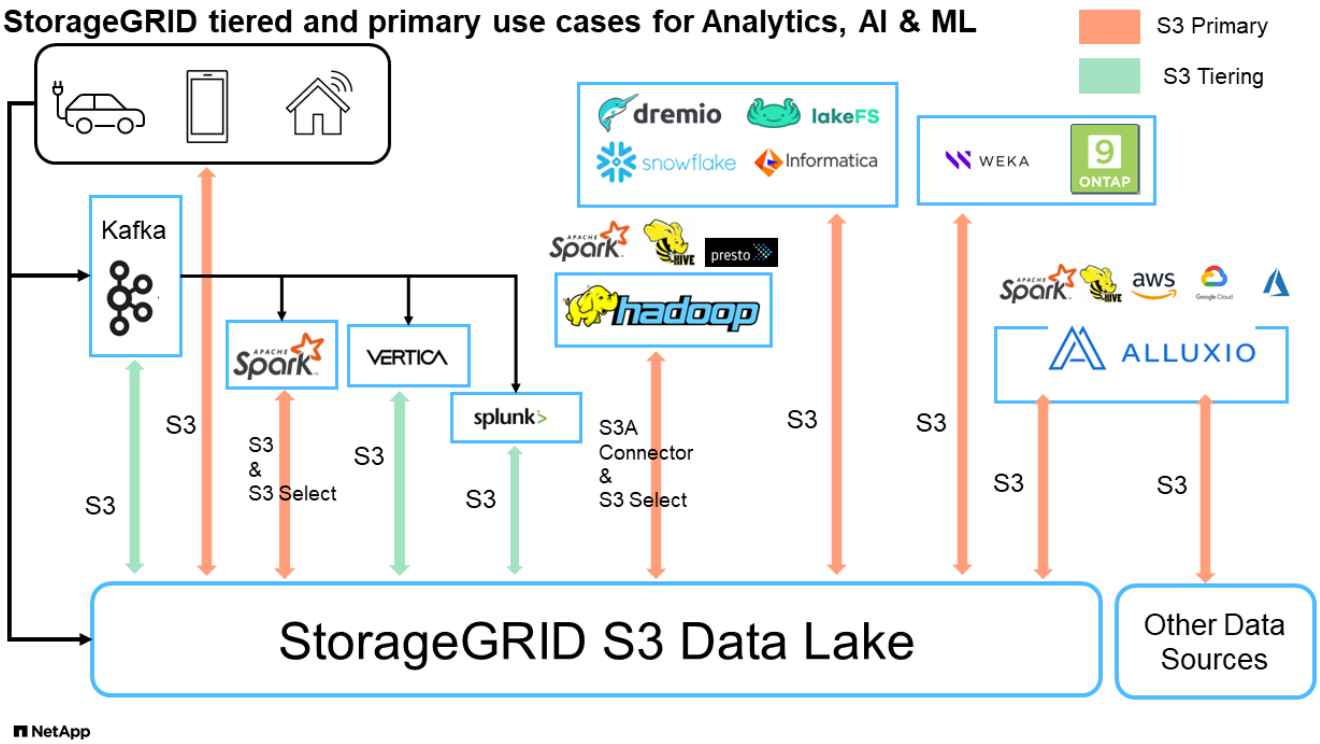


Entre los anteriores, el análisis de Big Data es uno de los casos de uso más importantes y su uso es tendencia al alza.

¿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".

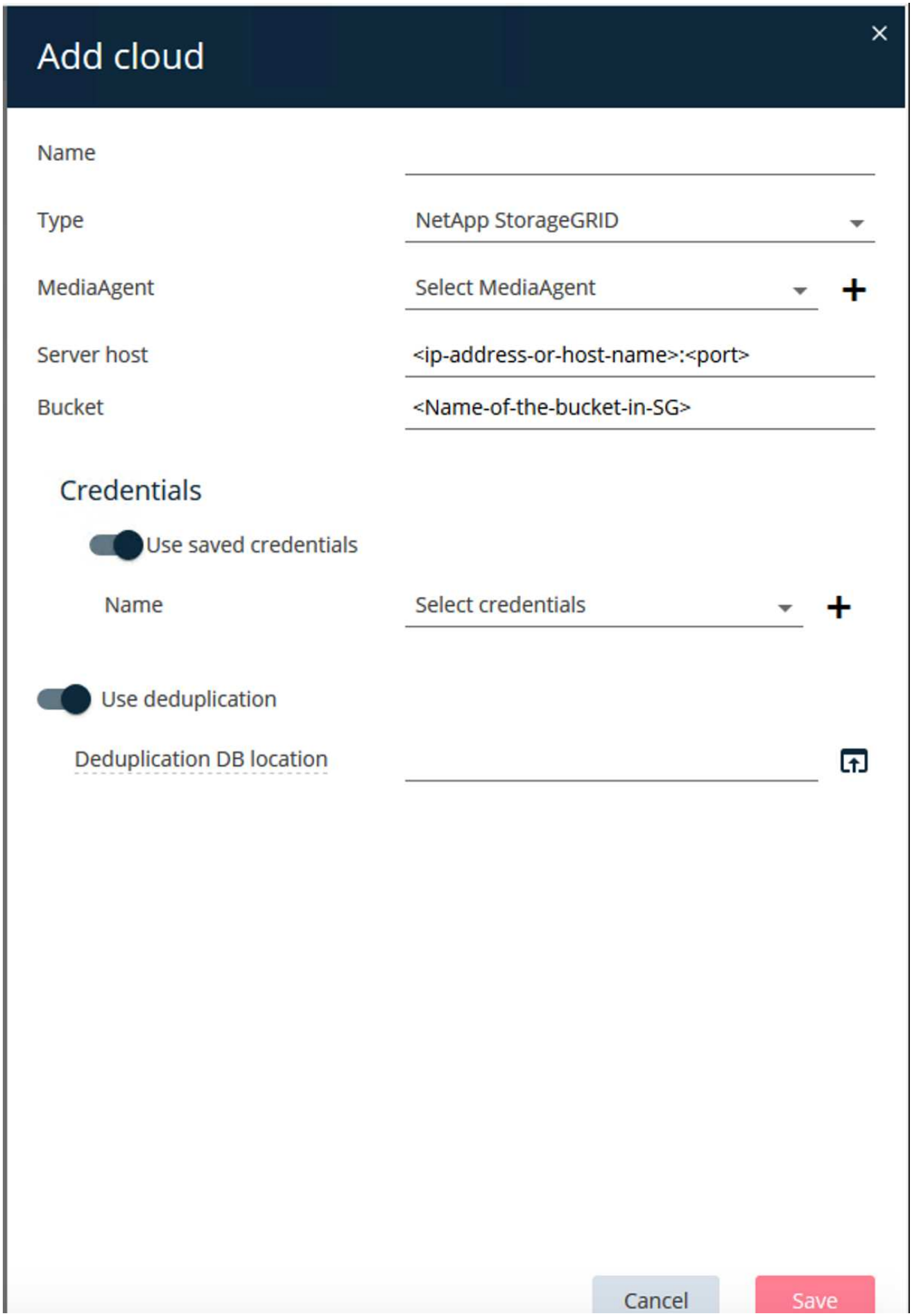
Ejecute un trabajo de protección de datos

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.

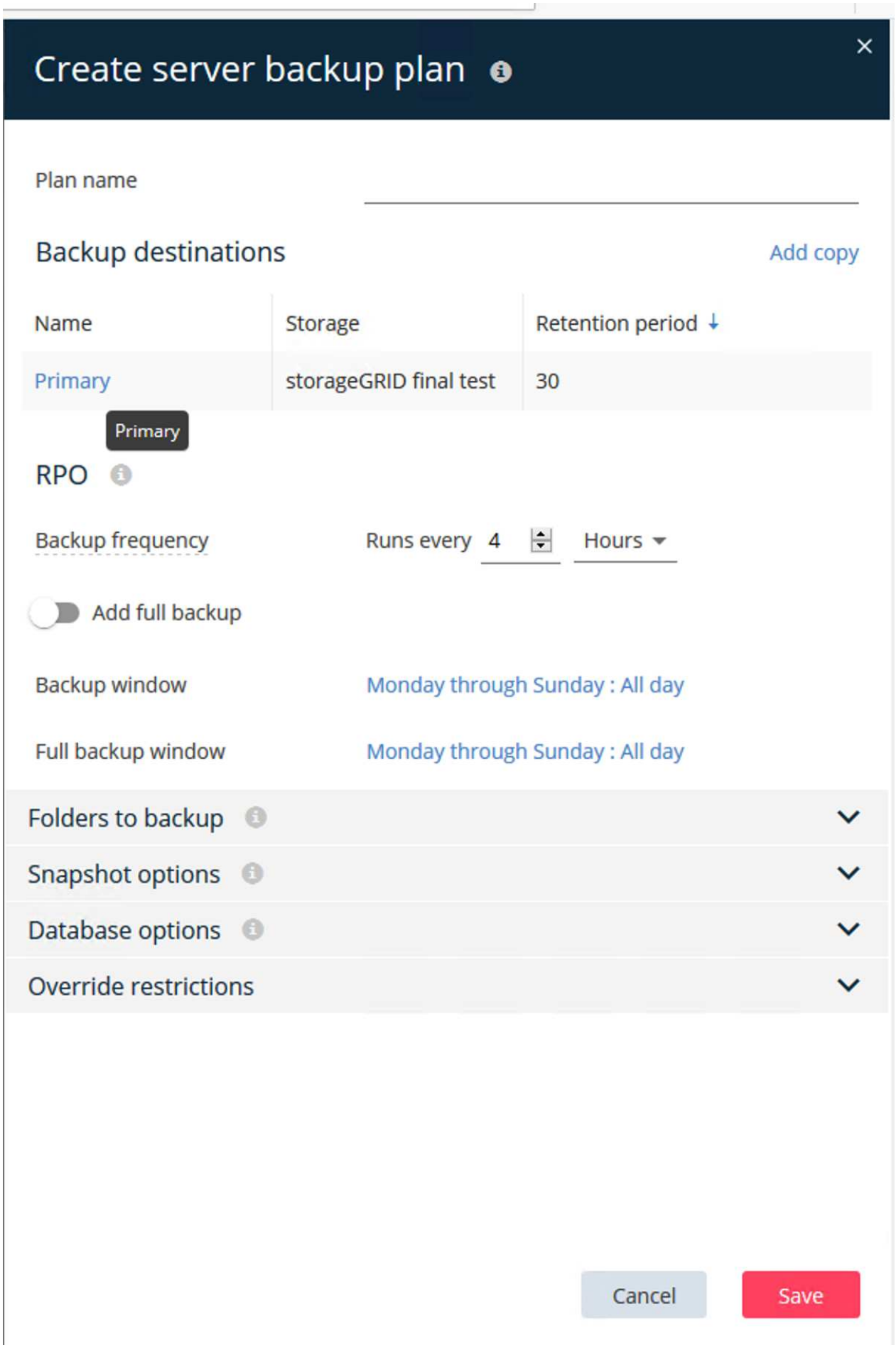
   Siga los pasos de la documentación de StorageGRID en "cómo configurar un punto final del balanceador de carga (puerto)". Asegúrese de tener un puerto HTTPS con un certificado autofirmado y la dirección IP o el nombre de dominio del extremo StorageGRID.

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.

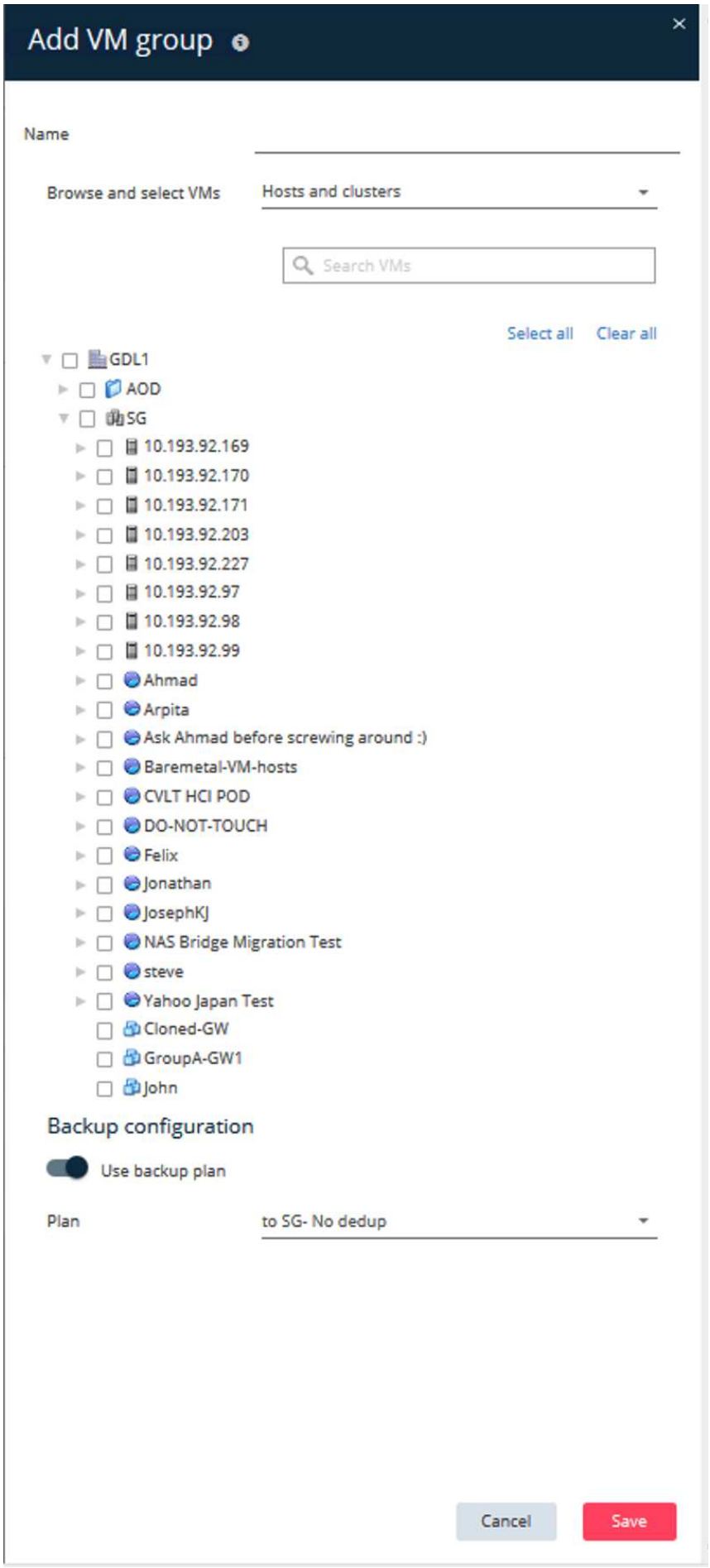

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to 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.

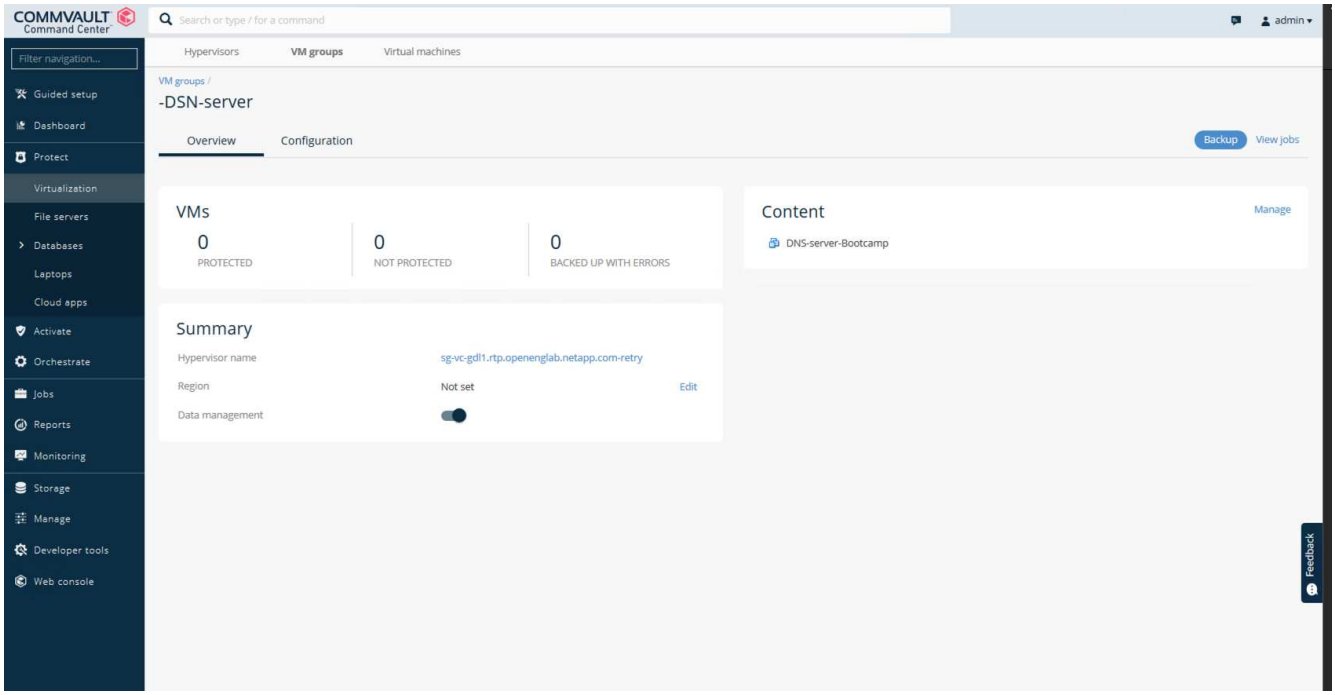
Paso 3: Inicia una tarea de backup para proteger las cargas de trabajo

Pasos

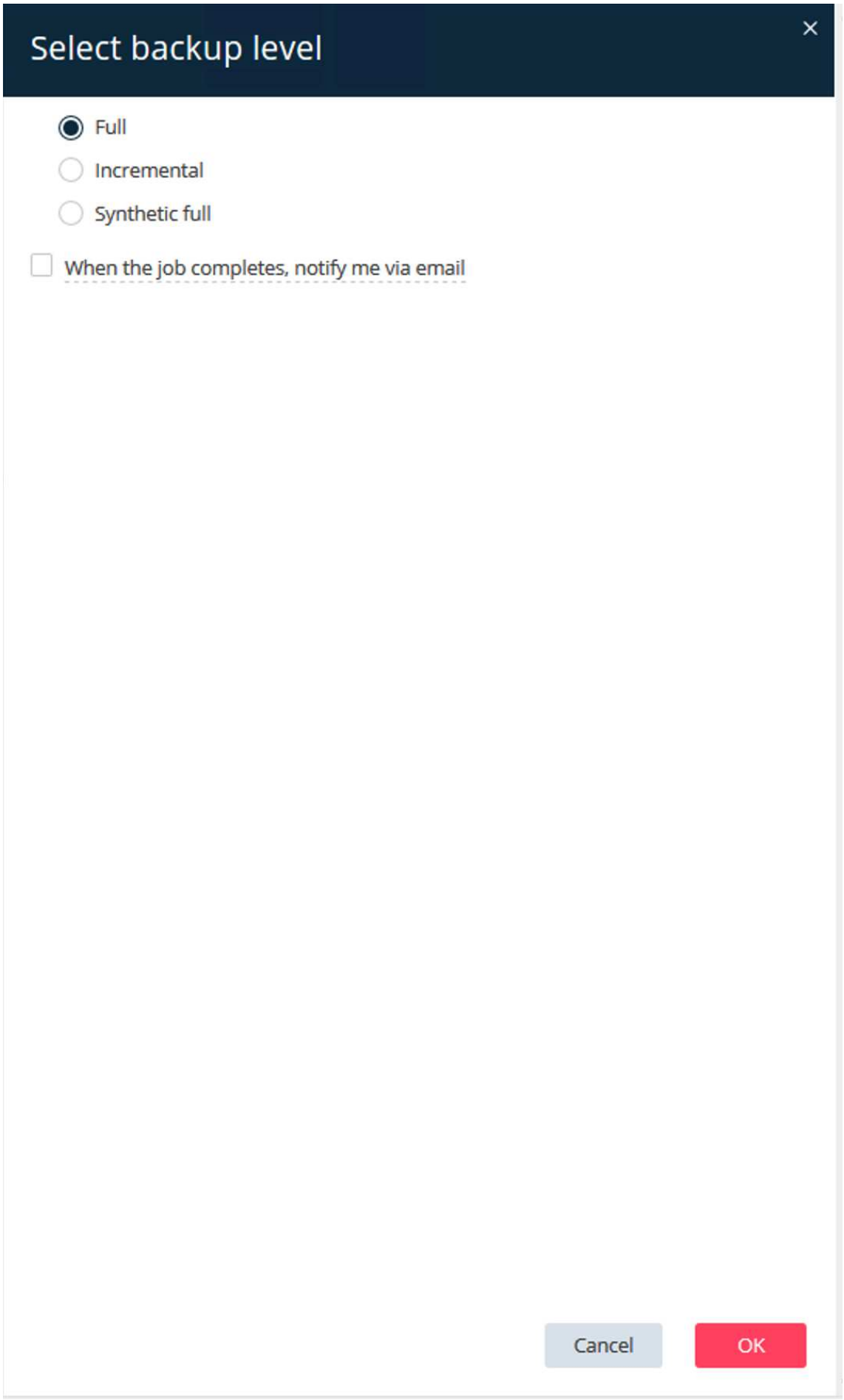
1. En Commvault Command Center, desplácese a Protect > Virtualization.
2. Añada un hipervisor de VMware vCenter Server.
3. Haga clic en el hipervisor que acaba de agregar.
4. Haga clic en Add VM group para responder al cuadro de diálogo Add VM Group para poder ver el entorno de vCenter que planea proteger.


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

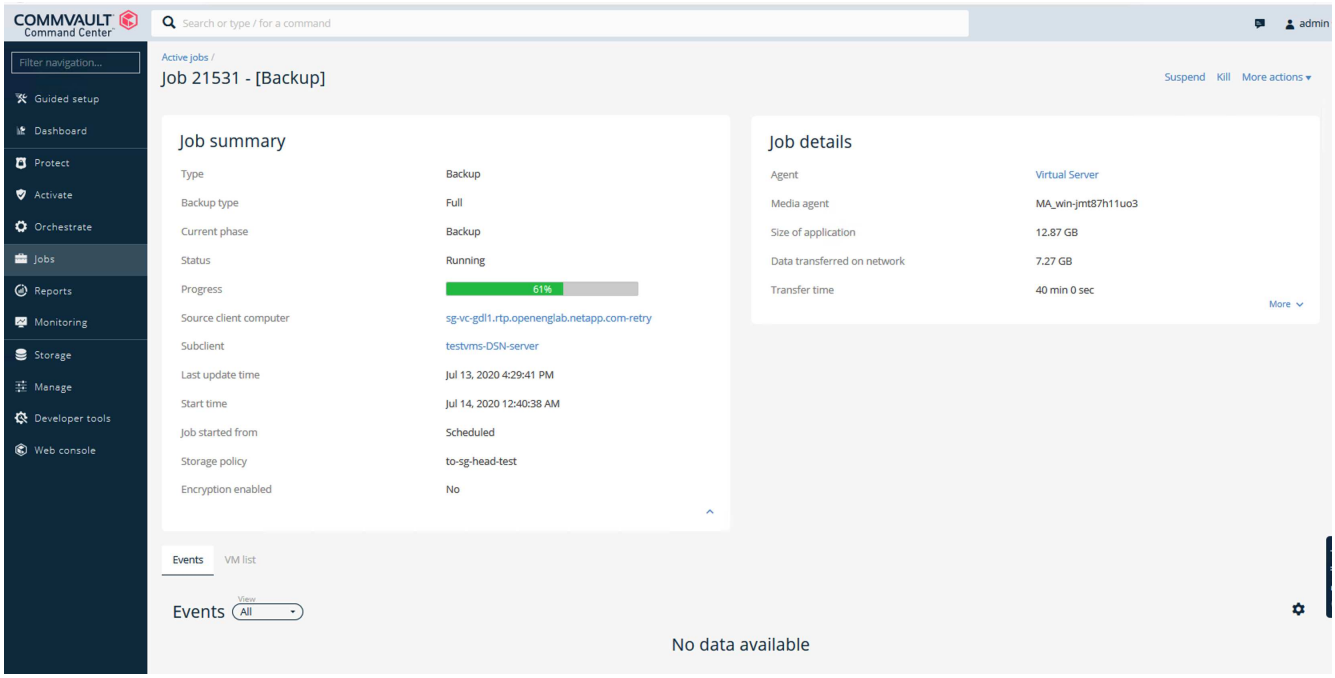
5. Seleccione un almacén de datos, una máquina virtual o una recogida de máquinas virtuales y introduzca un nombre para ella.
6. Seleccione el plan de copia de seguridad que creó en la tarea anterior.
7. Haga clic en Save para ver el grupo de máquinas virtuales que ha creado.
8. En la esquina superior 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.

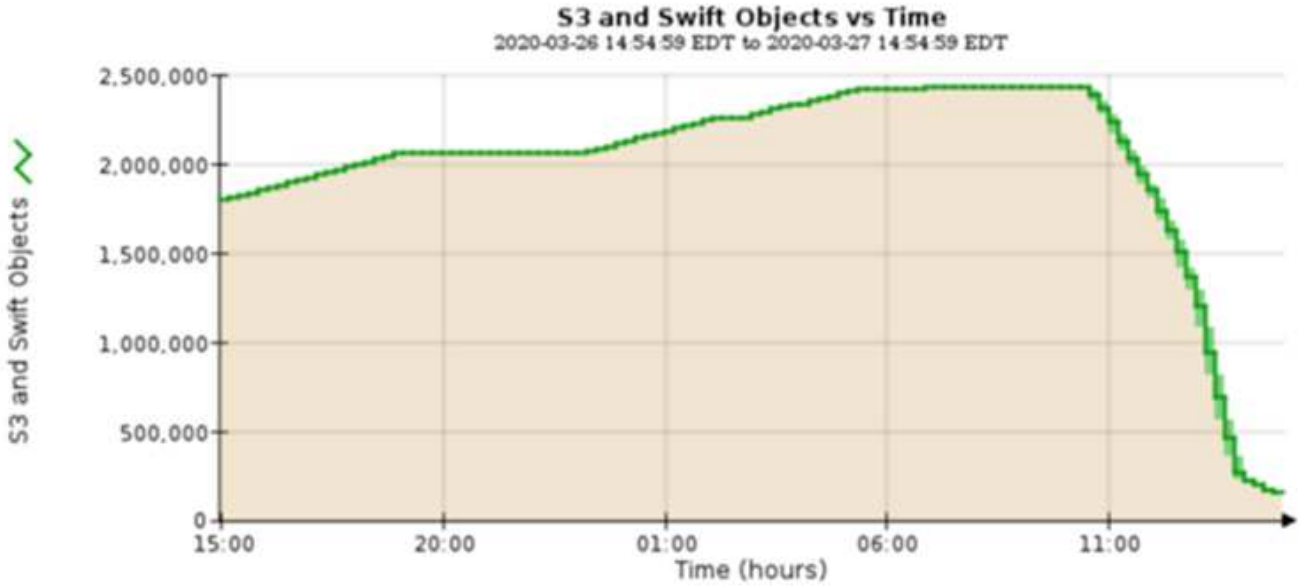
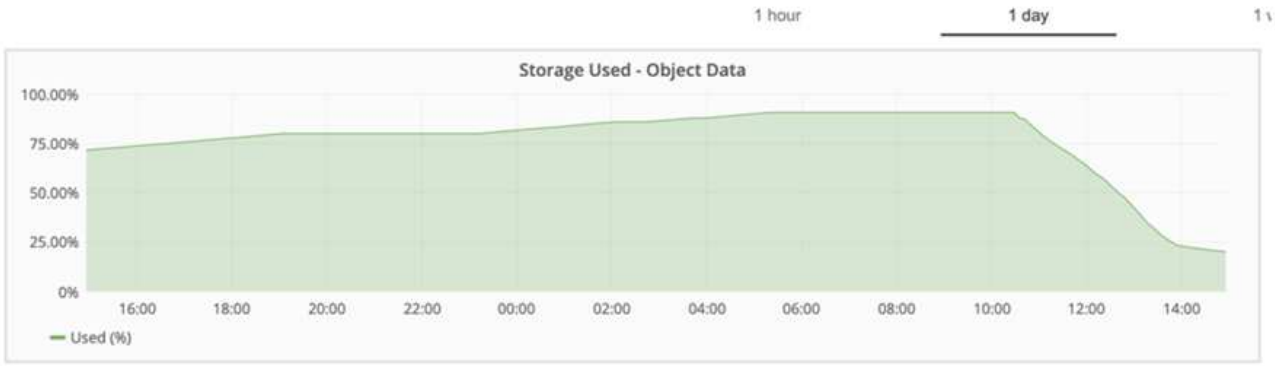


Figura 2: Liberación de 80TB TB de almacenamiento en menos de 3 horas.



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.

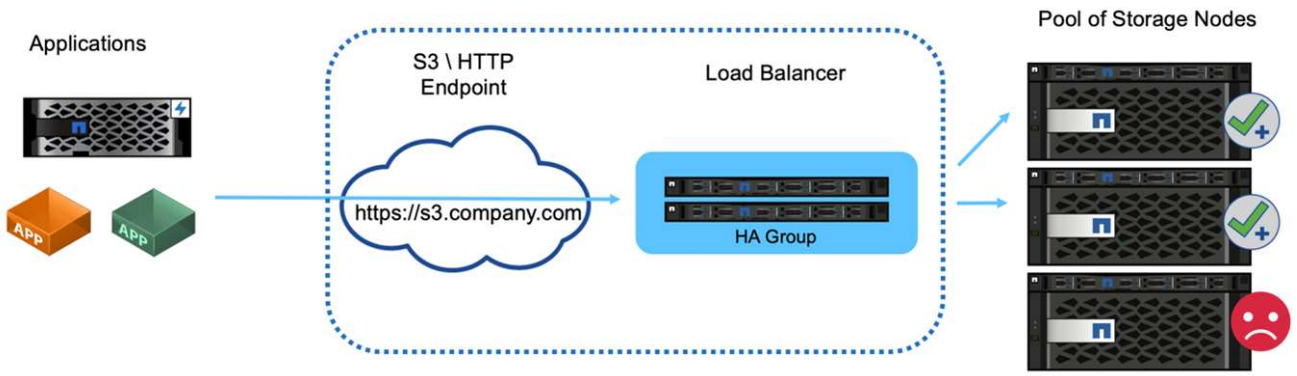
El almacenamiento de objetos es sinónimo de almacenamiento en cloud y, como cabe esperar, las aplicaciones que aprovechan el almacenamiento en cloud dirigen ese almacenamiento a través de una URL. Detrás de esa misma URL, StorageGRID puede escalar la capacidad, el rendimiento y la durabilidad en un solo 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.

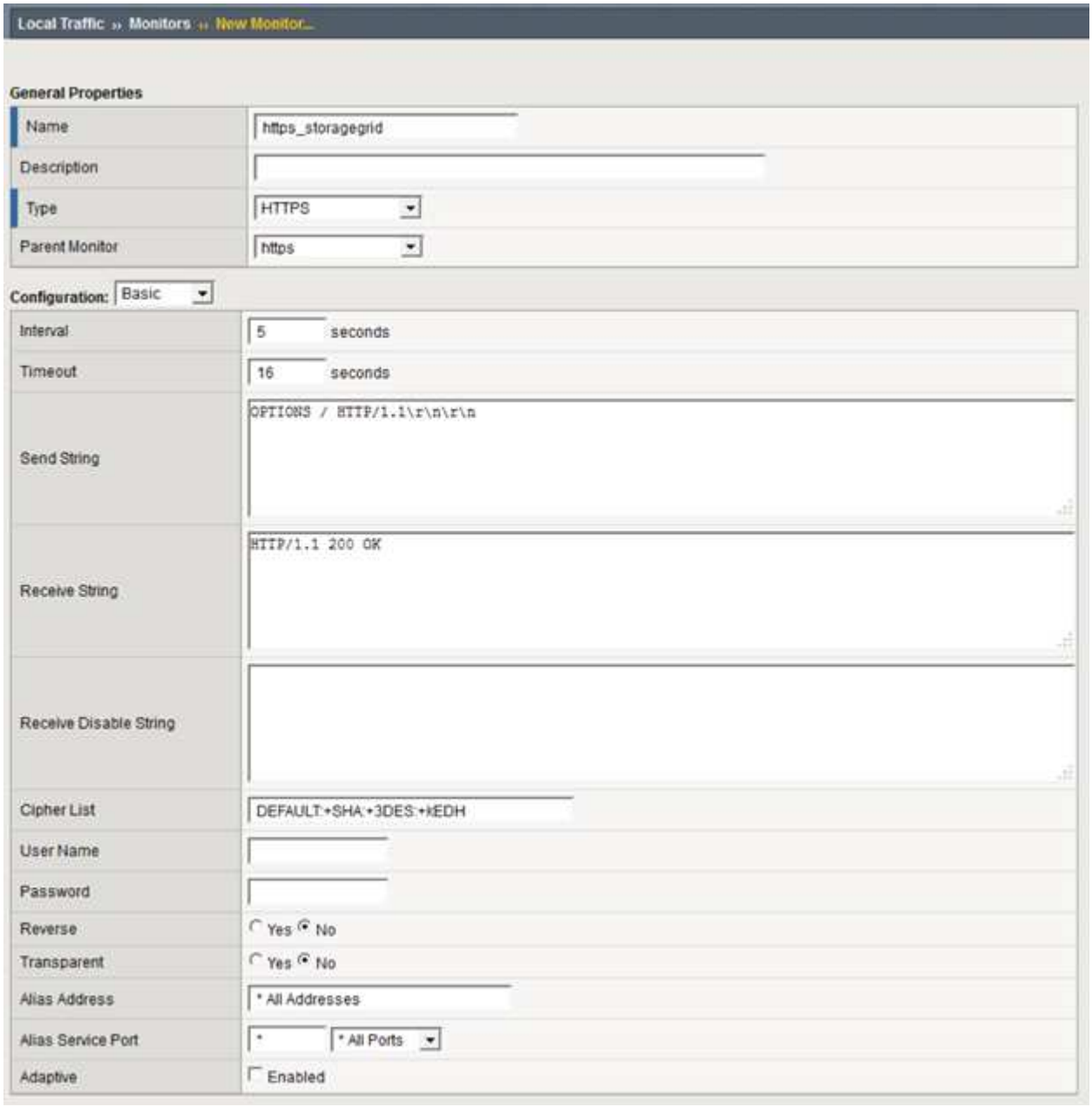
En los siguientes ejemplos se ilustran las configuraciones implantadas por los clientes de StorageGRID, incluido NetApp IT.

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`.



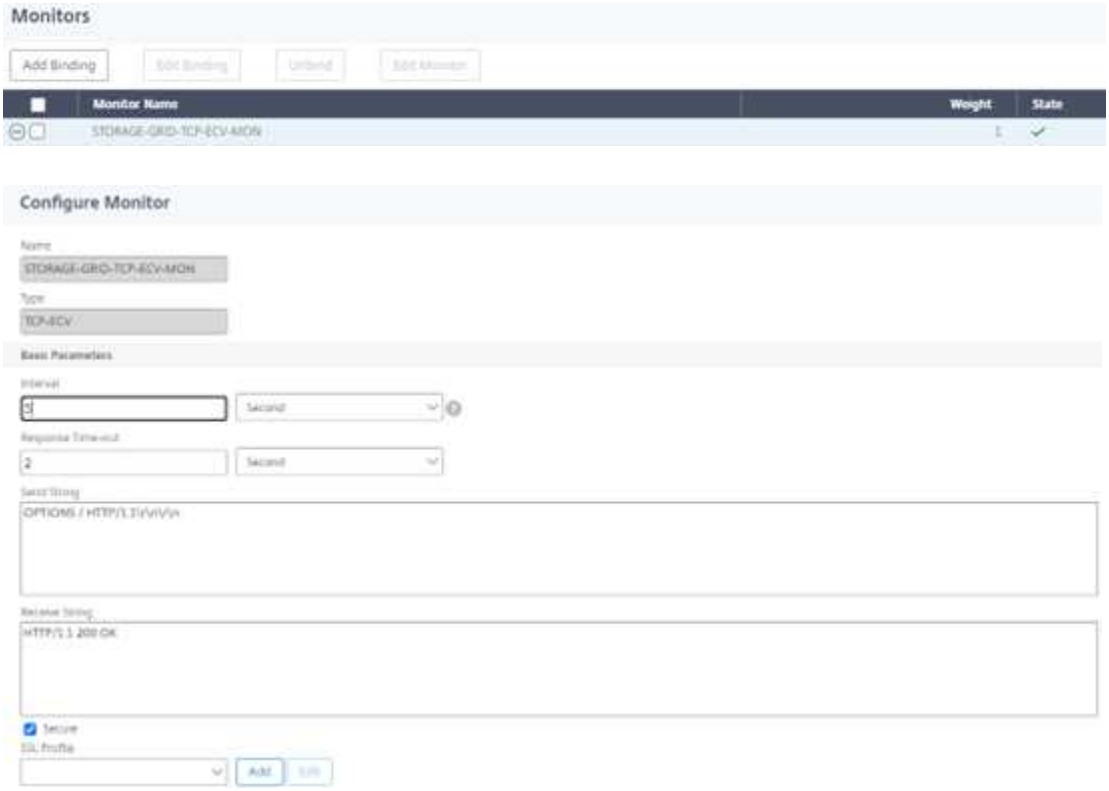
2. En Crear Pool, cree un pool para cada puerto necesario.
   a. Asigne el monitor de estado que ha creado en el paso anterior.
   b. Seleccione un método de equilibrio de carga.
   c. Seleccione el puerto de servicio: 18082 (S3).
   d. Añada nodos.

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.

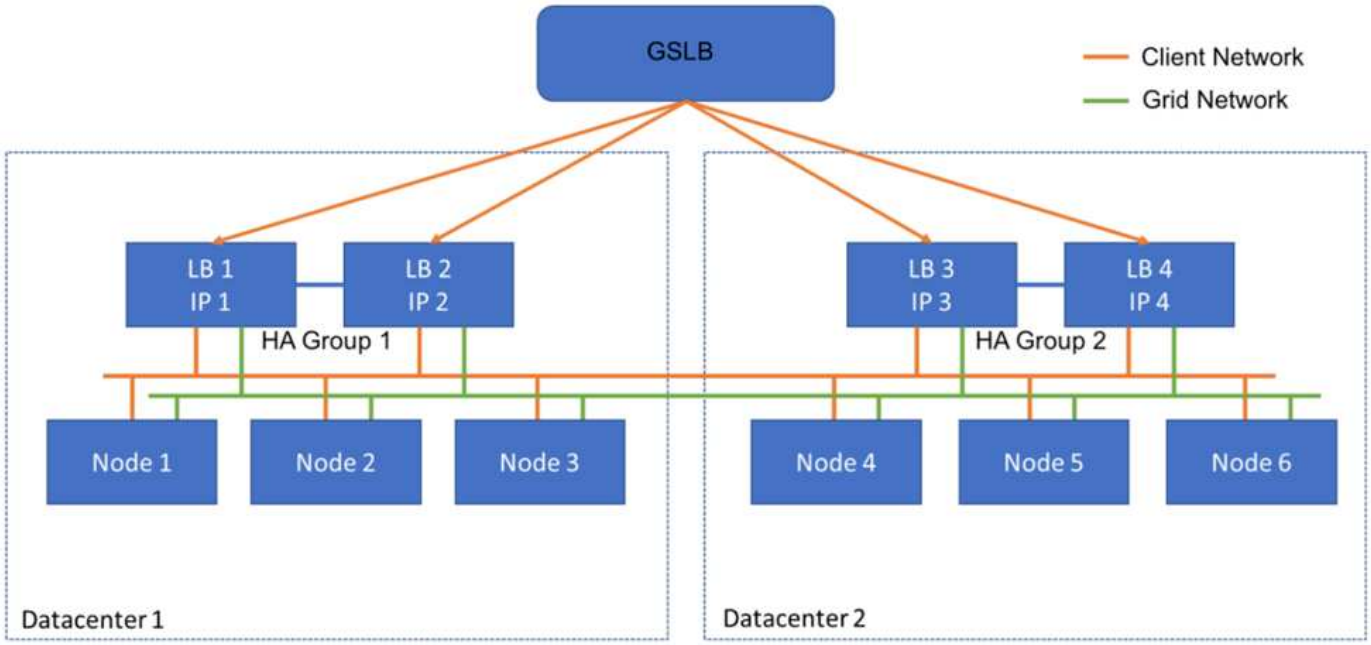
Después de configurar el equilibrador de carga, debe validar la conexión mediante herramientas como OpenSSL y la CLI de AWS. Otras aplicaciones, como S3 Browser, podrían ignorar la configuración incorrecta de SSL.

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:

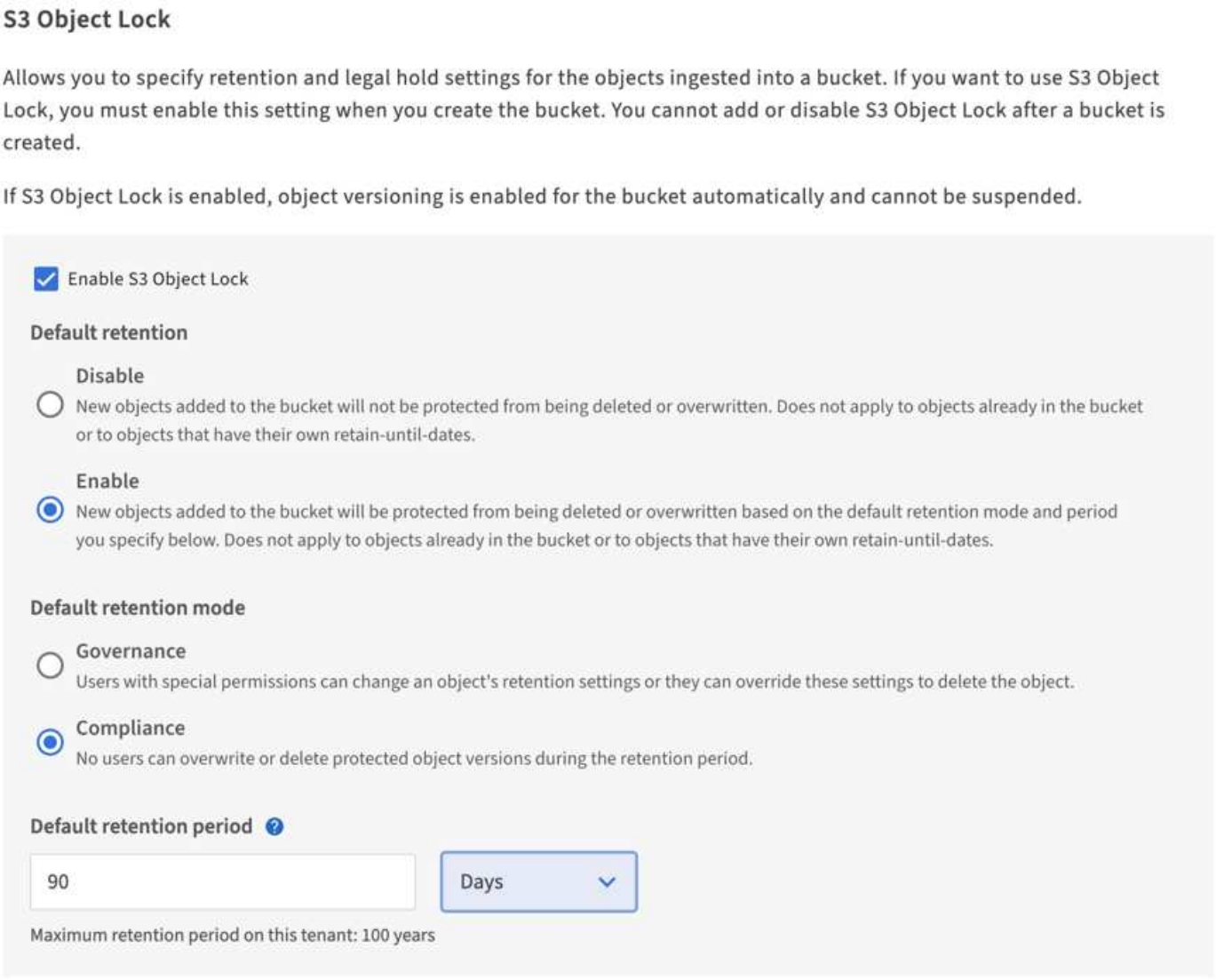
- Centro de documentación de NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Habilitación para NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentación de producto de NetApp https://www.netapp.com/support-and-training/documentation/

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.

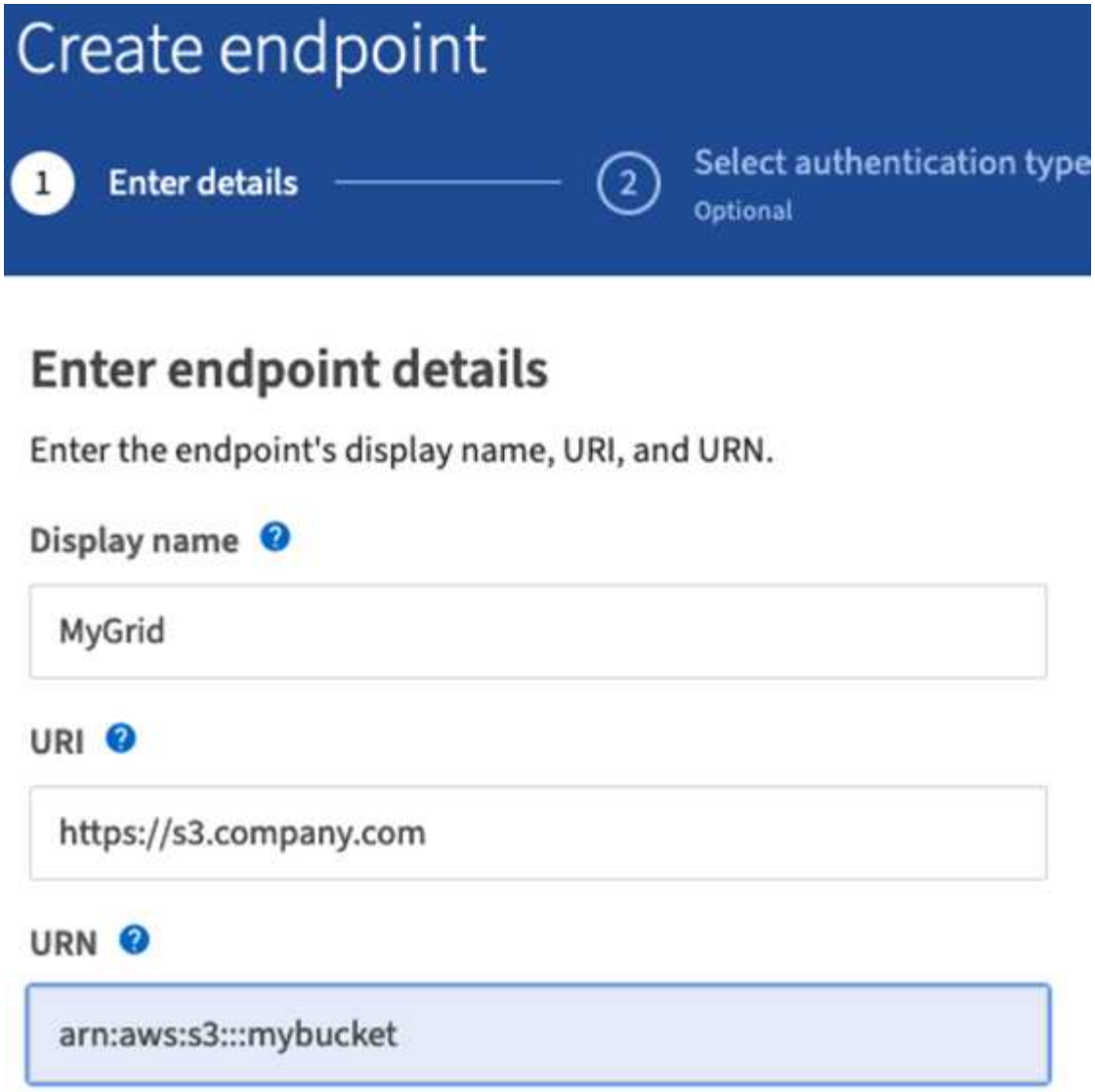
StorageGRID CloudMirror es un componente de StorageGRID que se puede configurar para replicar los objetos de un bucket en un destino definido a medida que se ingieren en el bloque de origen y no replica los eliminaciones. Puesto que CloudMirror es un componente integrado de StorageGRID, no se puede desactivar 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

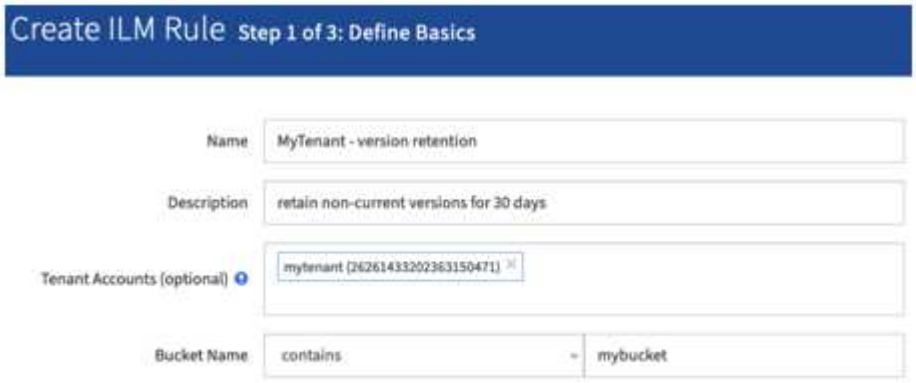
1. Para configurar CloudMirror, cree un punto final de servicios de plataforma para el destino S3.

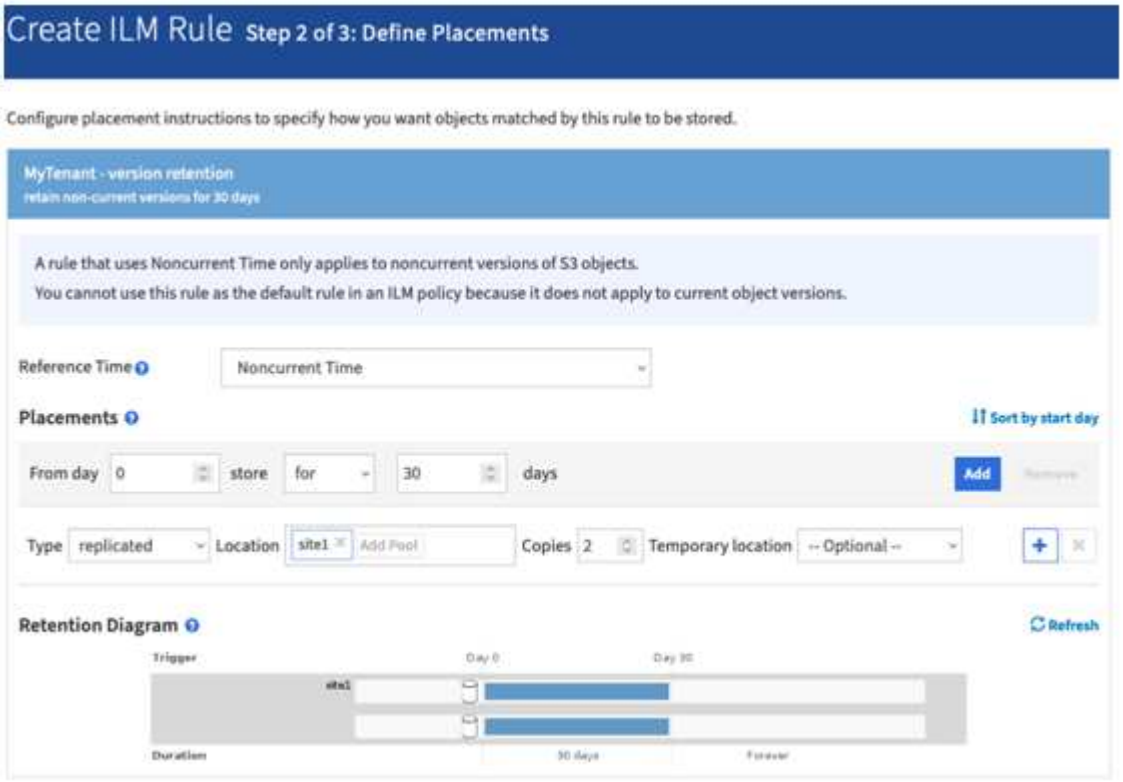


2. En el bloque de origen, configure la replicación para usar el punto final configurado.

```
<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.

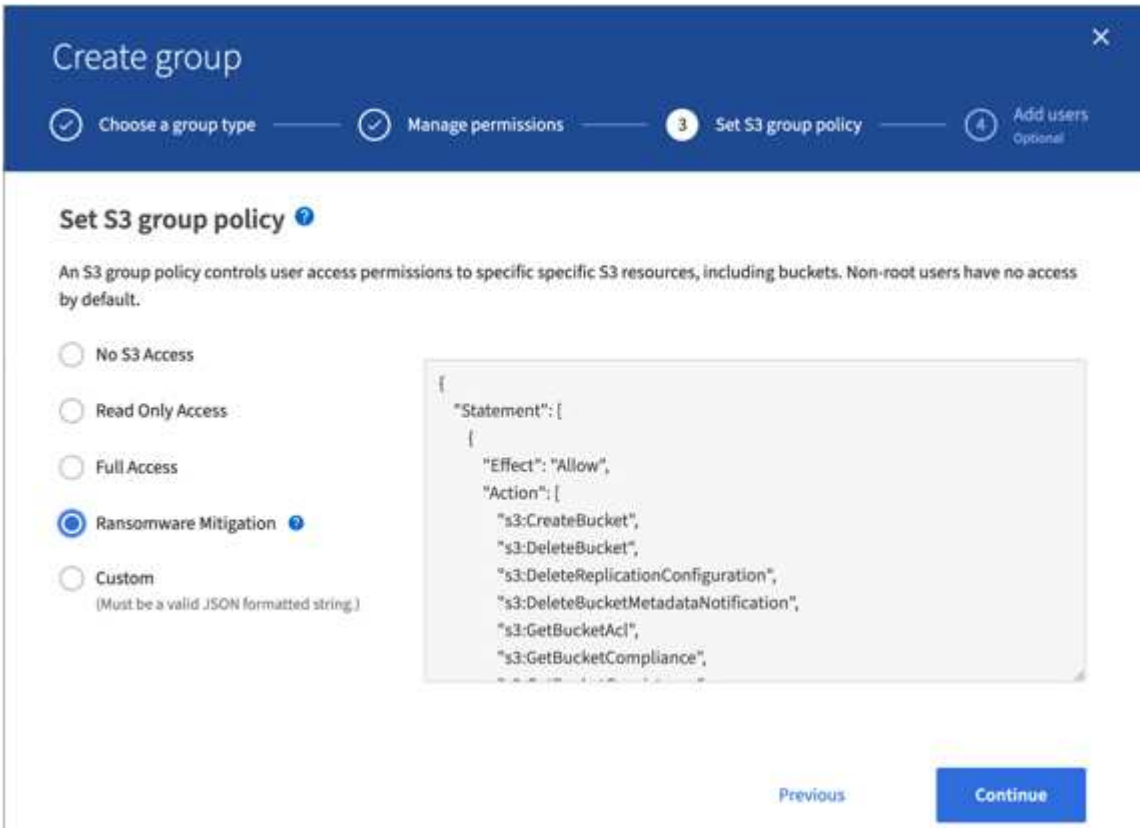
Protección frente al ransomware mediante el control de versiones con la política de protección IAM

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

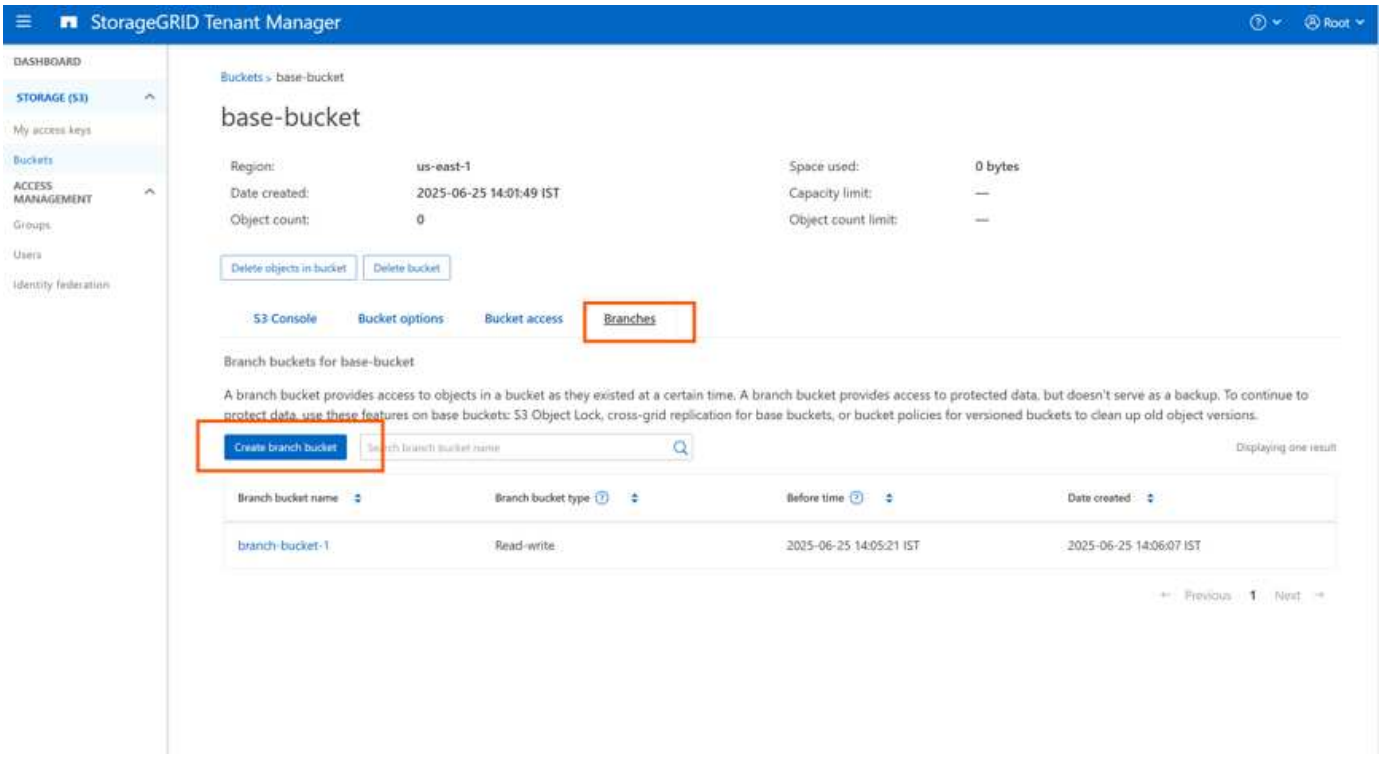
Aprenda a investigar y remediar buckets después de un posible ataque de ransomware con StorageGRID.

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.

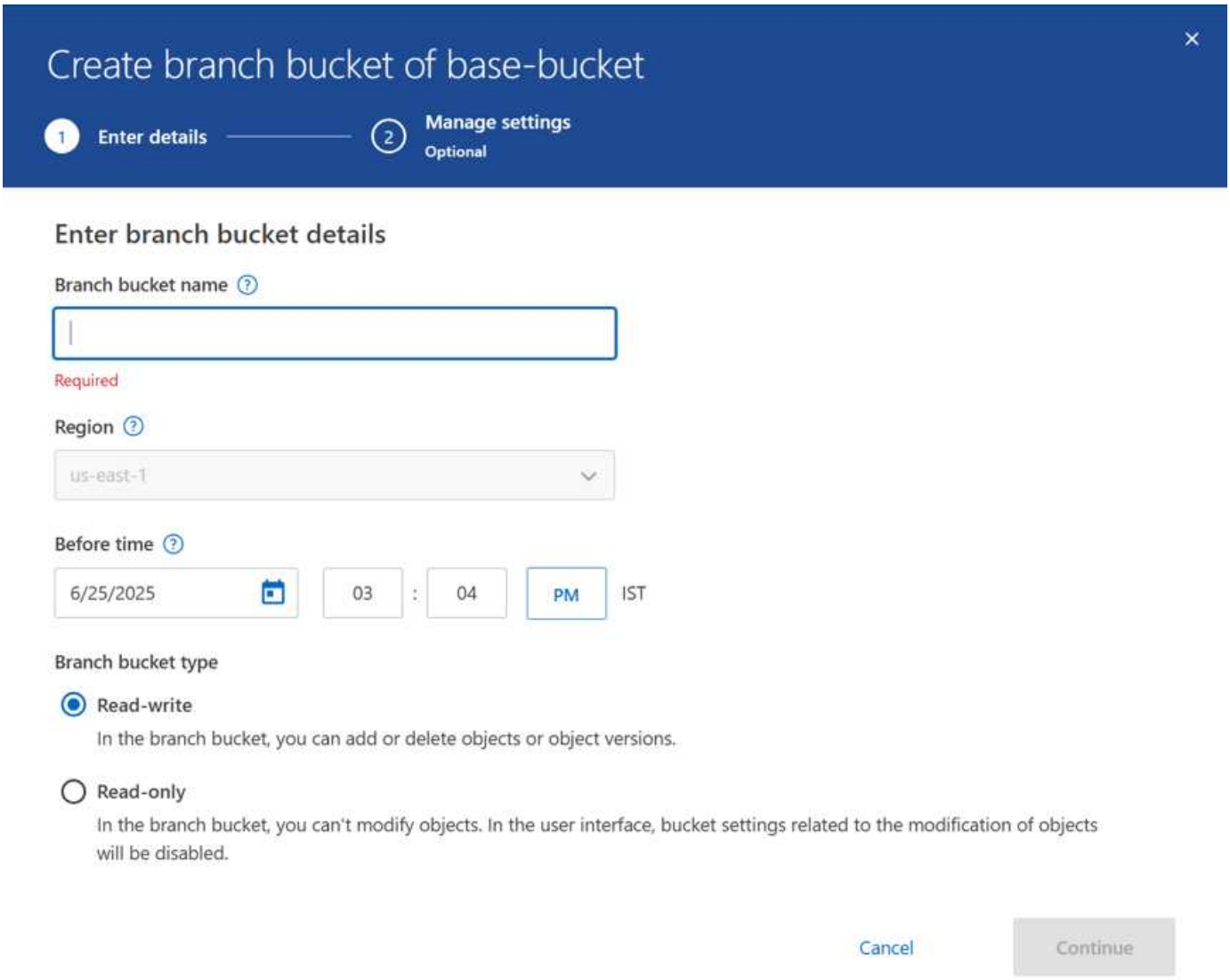
Esto significa que si sospecha que se ha producido un ataque de ransomware, puede crear un depósito de ramas de lectura y escritura, o de solo lectura, que contenga todos los objetos y versiones que existían antes del momento del ataque inicial. Puede utilizar esta rama del depósito para comparar con 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

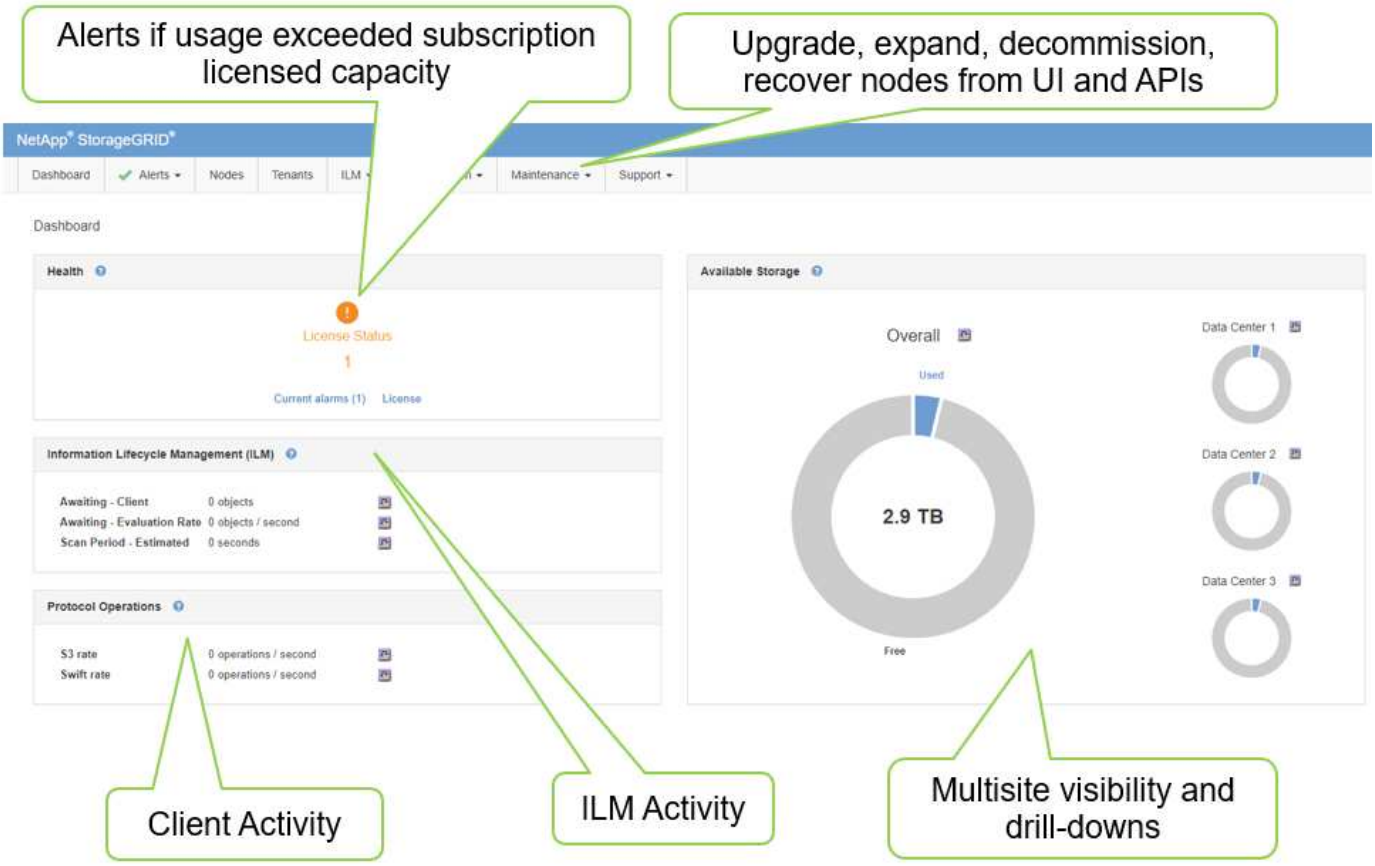
Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- 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.

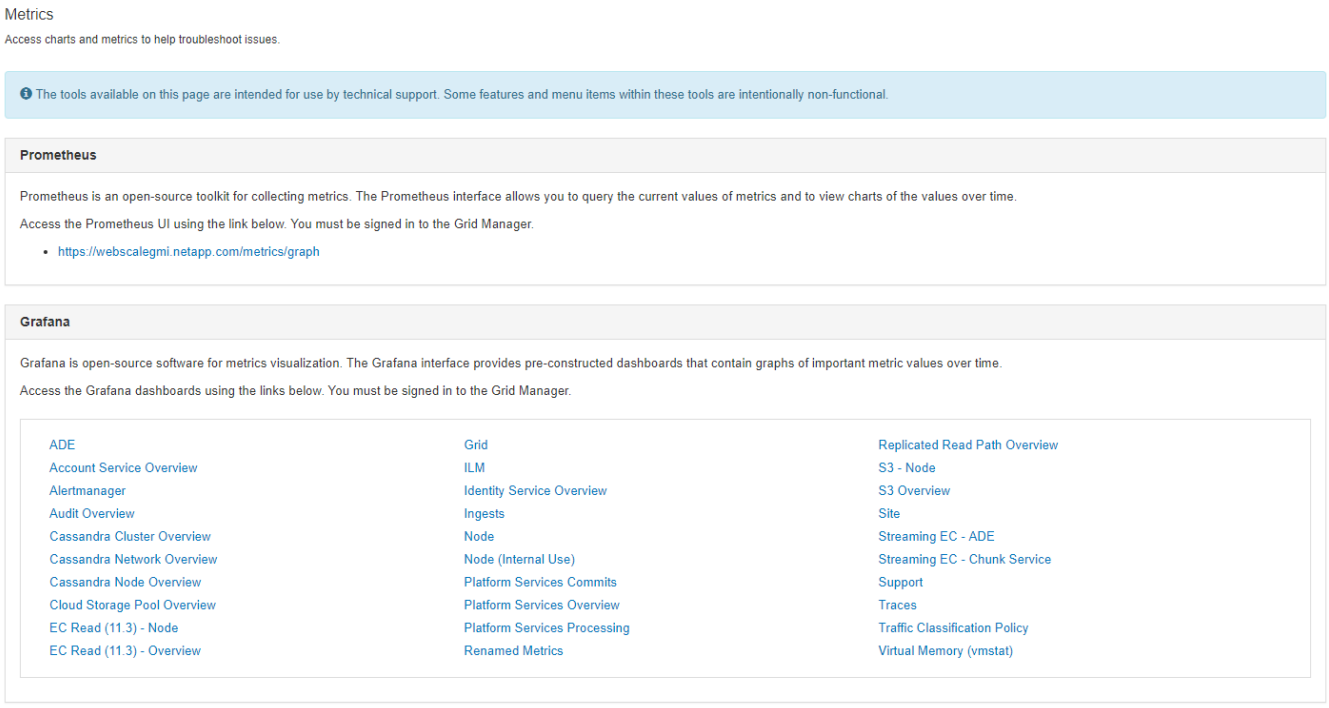
Para obtener más información sobre las alertas, consulte el documento "documentación de productos" disponible en línea y en formato PDF.

Supervisión avanzada en StorageGRID

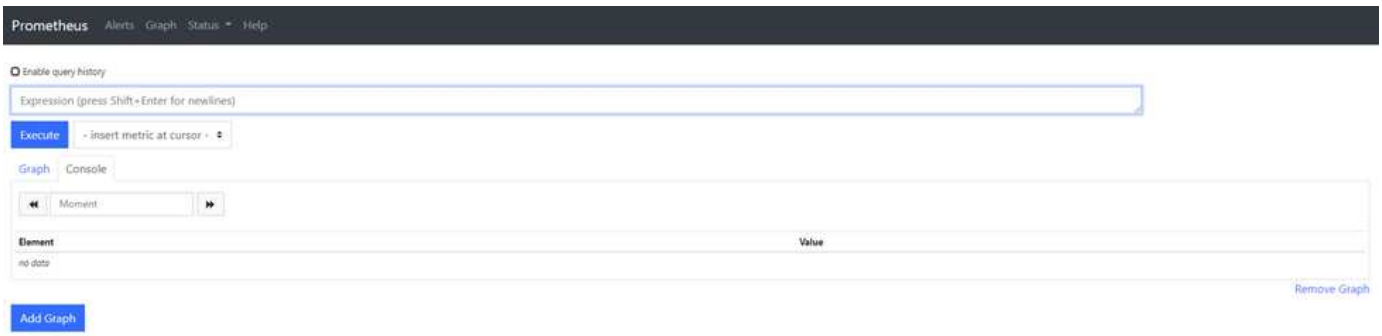
Aprenda a acceder y exportar métricas para ayudar a resolver problemas.

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.

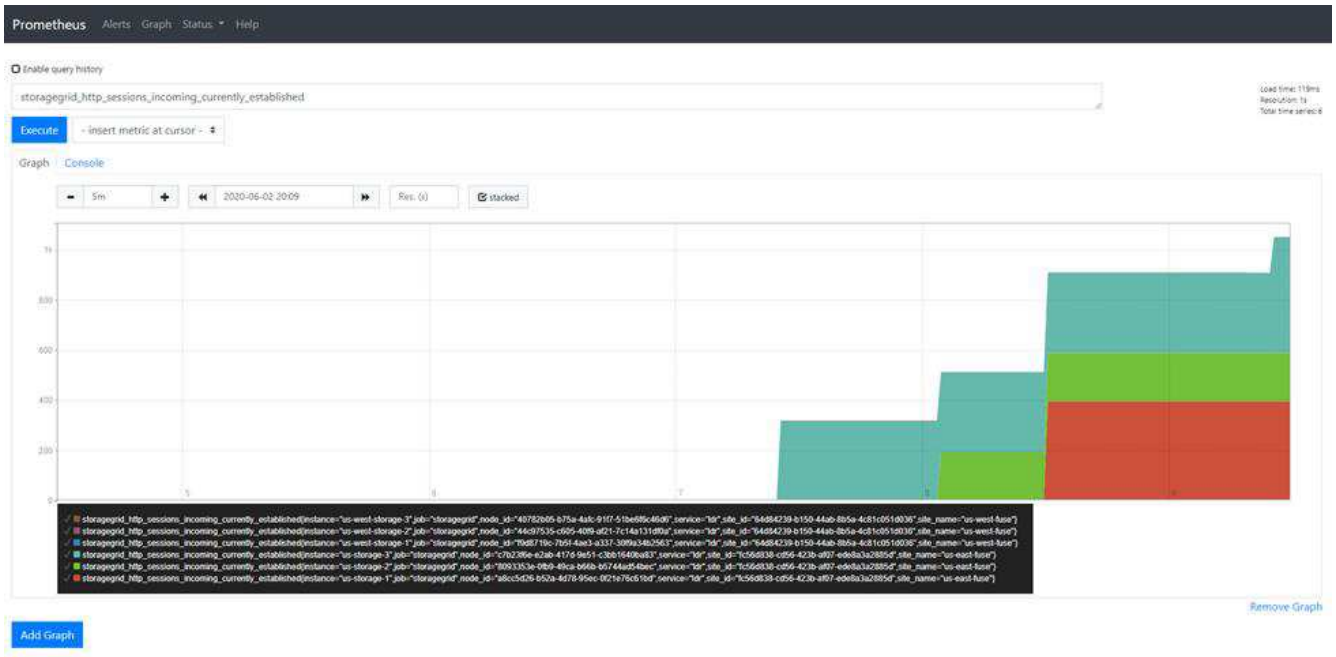


Con esta vista, puede acceder a la interfaz de Prometheus. Desde ahí, podrá buscar en las métricas disponibles e incluso experimentar con consultas.

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.

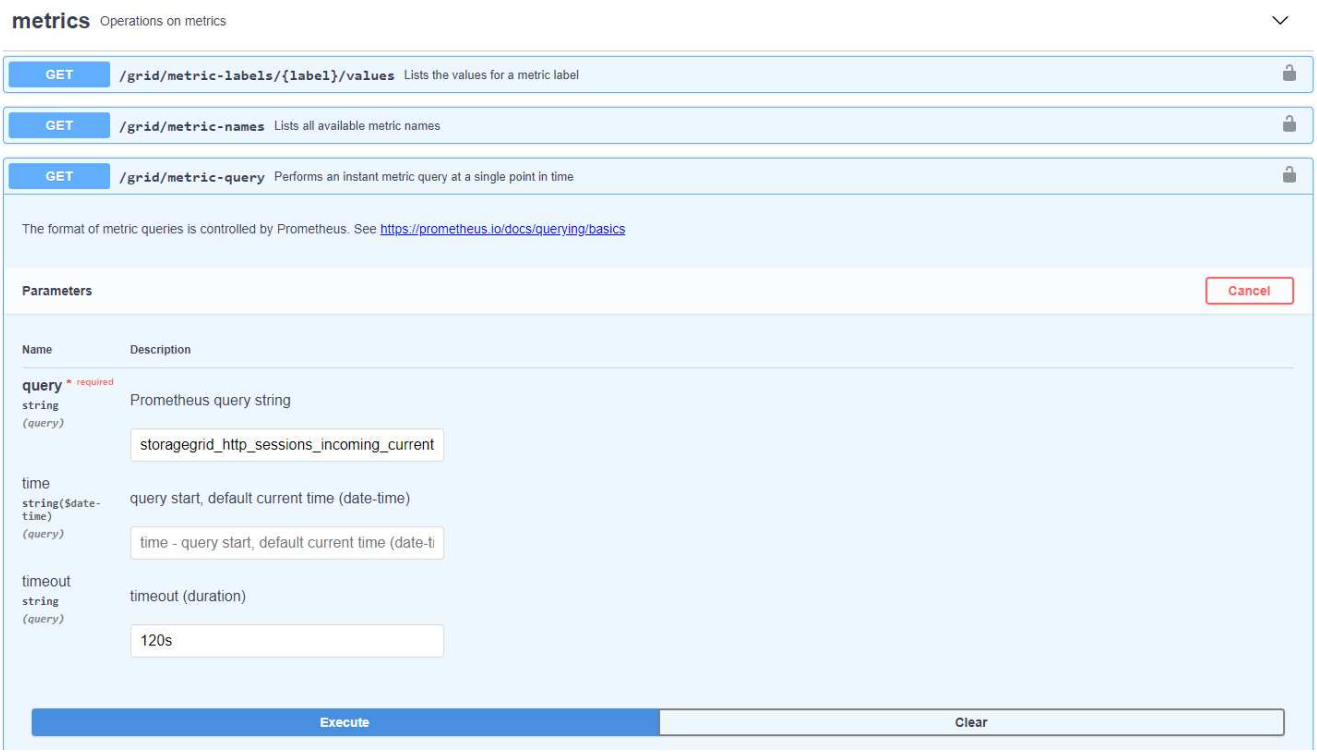
No se recomienda interactuar directamente con nuestra instancia de Prometheus porque esto requiere la apertura de puertos adicionales. El acceso a métricas a través de nuestra API es el método recomendado y seguro.

Exportar métricas a través de la API

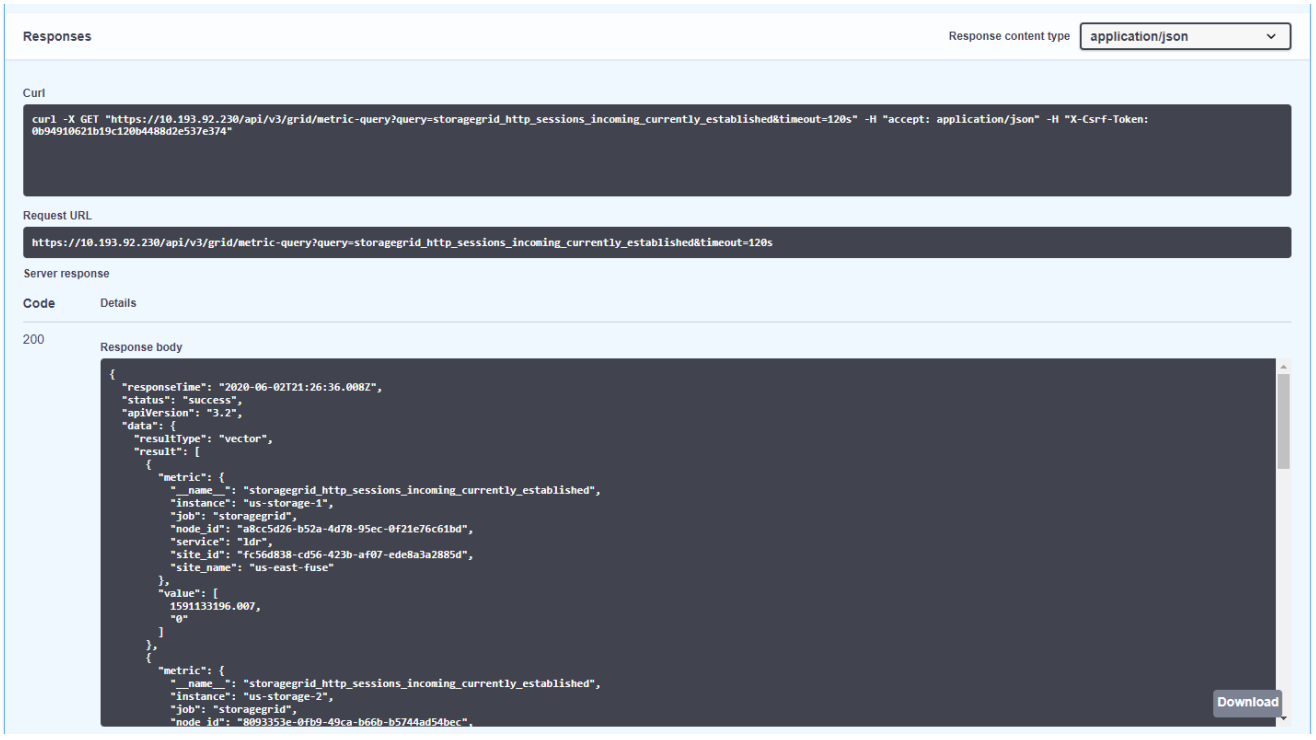
También se puede acceder a los mismos datos mediante la API de gestión de StorageGRID.

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

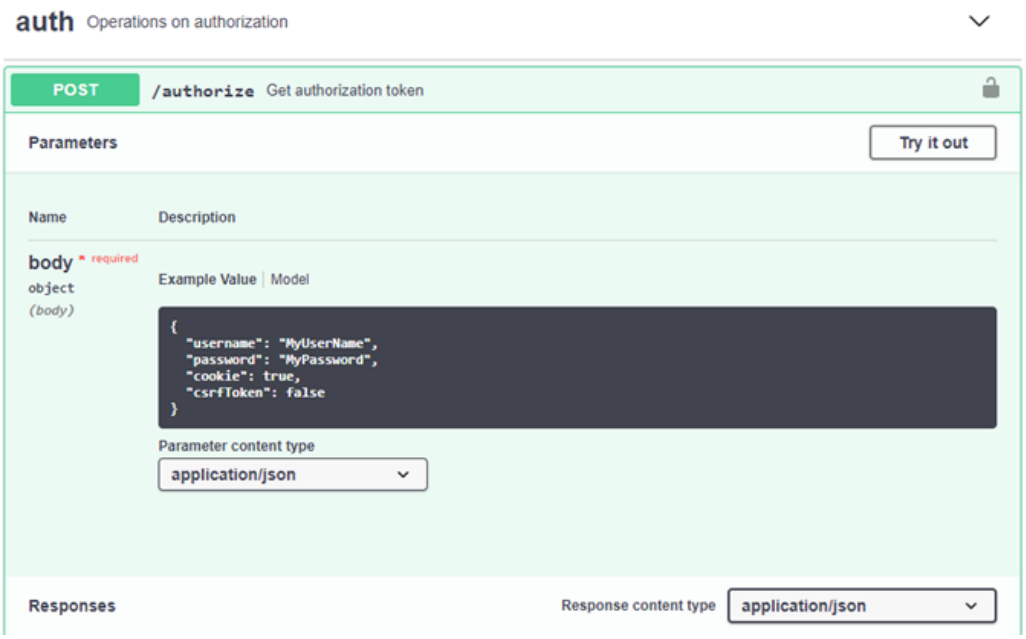
Acceda a métricas utilizando cURL en StorageGRID

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

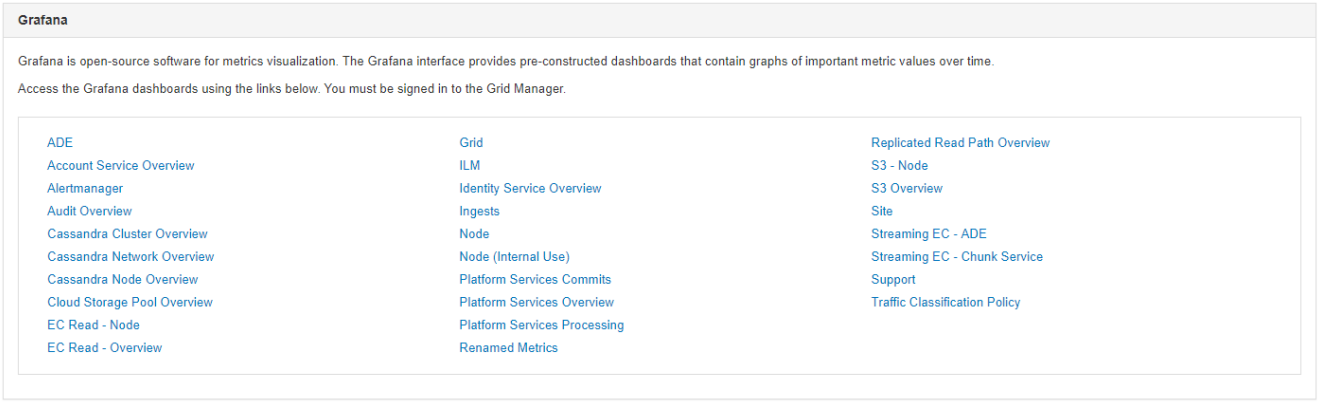
Aprende a usar la interfaz de Grafana para visualizar y supervisar tus datos de StorageGRID.

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.

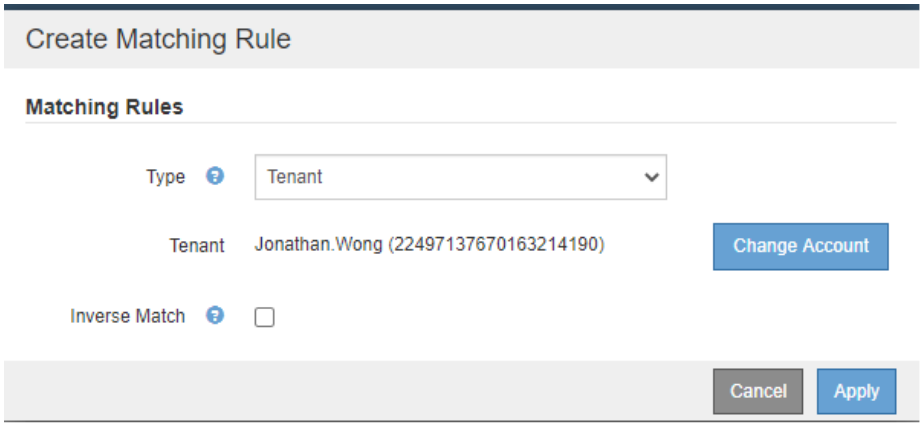
Las directivas de clasificación de tráfico proporcionan un método para supervisar y/o limitar el tráfico en función de un arrendatario específico, depósitos, subredes IP o puntos finales de equilibrio de carga. La conectividad de red y el ancho de banda son métricas especialmente importantes para StorageGRID.

Para configurar una directiva de clasificación de tráfico, siga estos pasos:

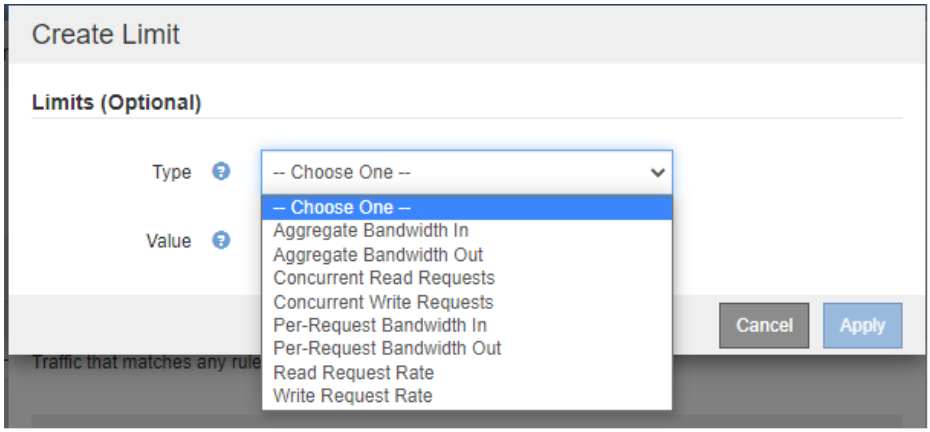
Pasos

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.

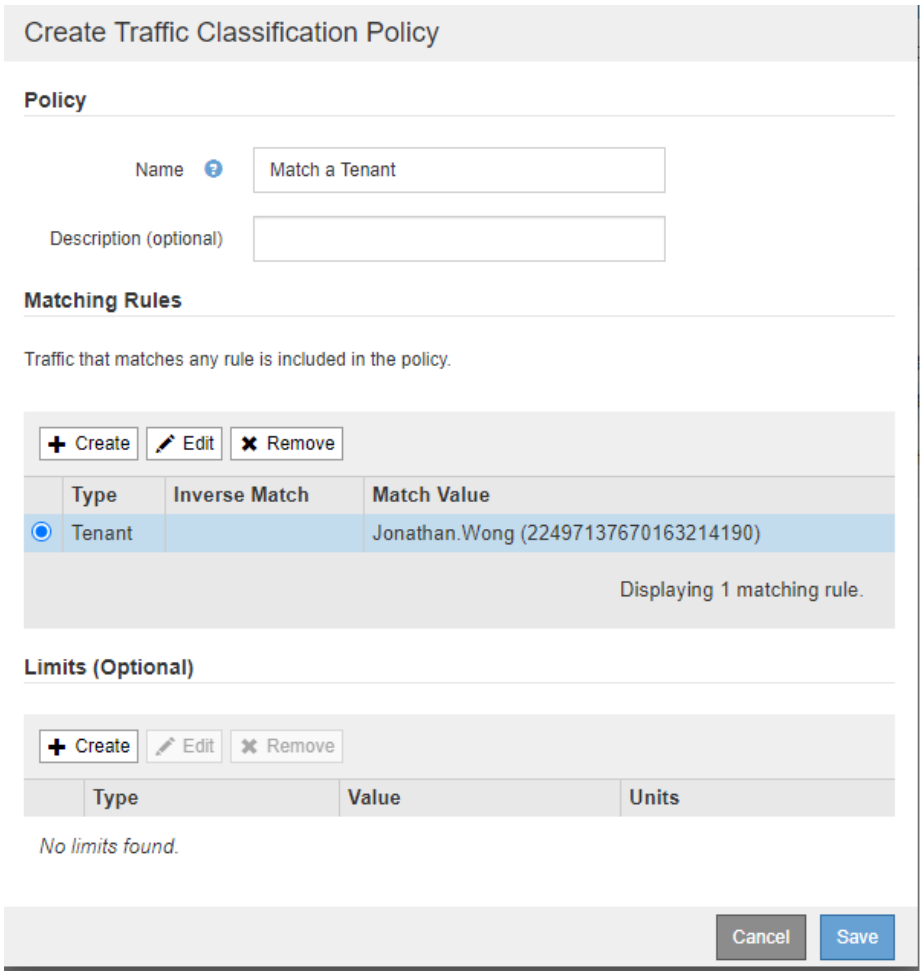
4. Cree una regla de coincidencia.



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

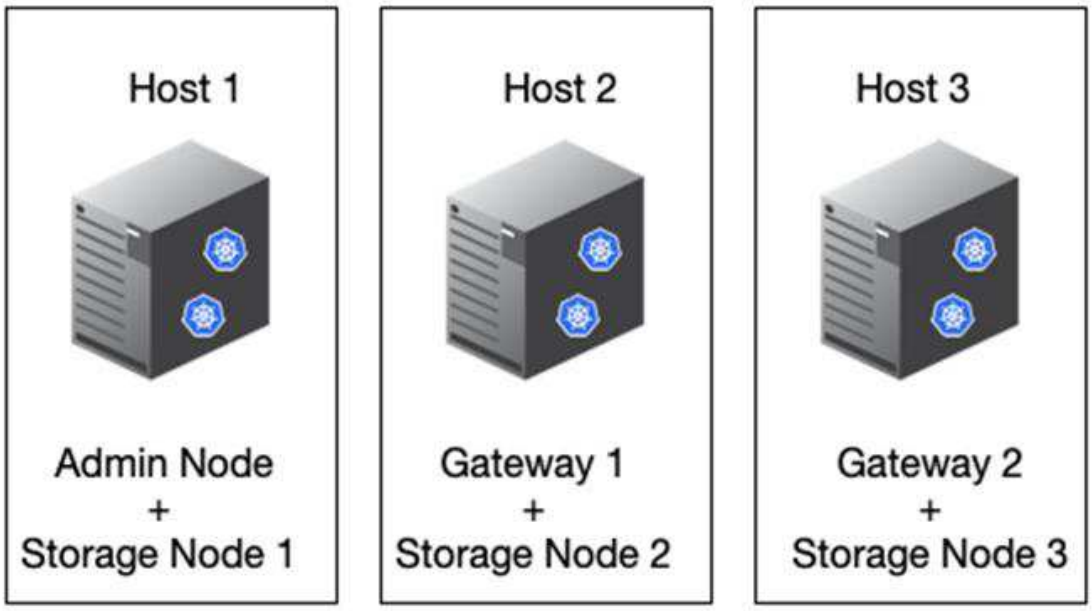
Contenedor de gateway

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

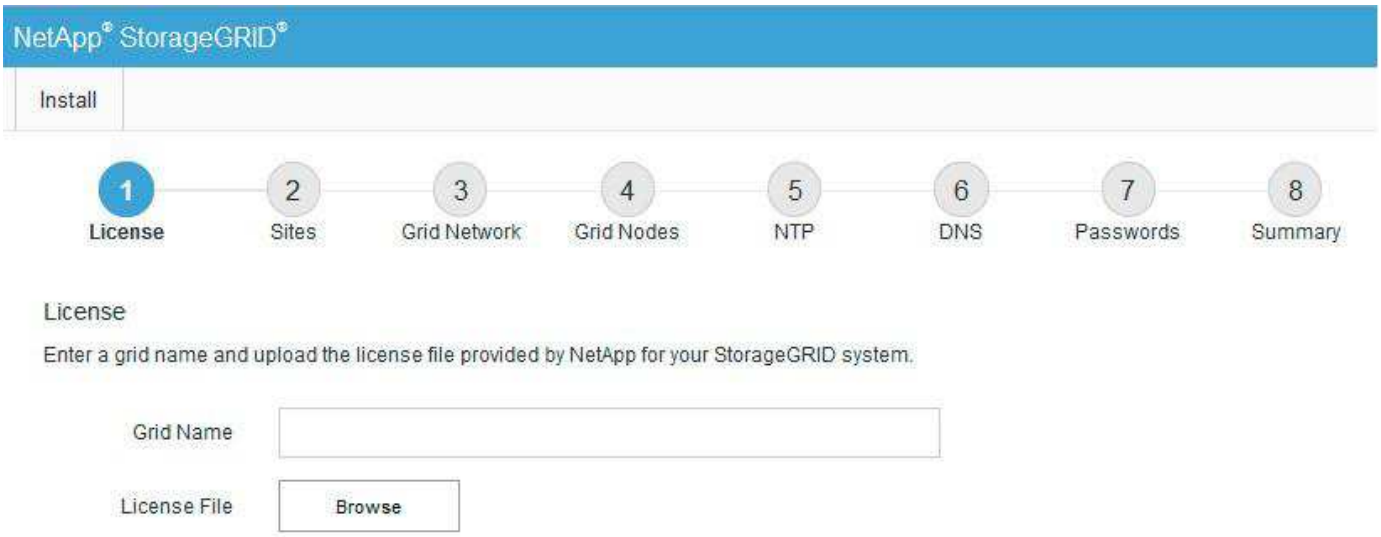
1. Acceda a Grid Manager en la siguiente dirección:

   ```
   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.

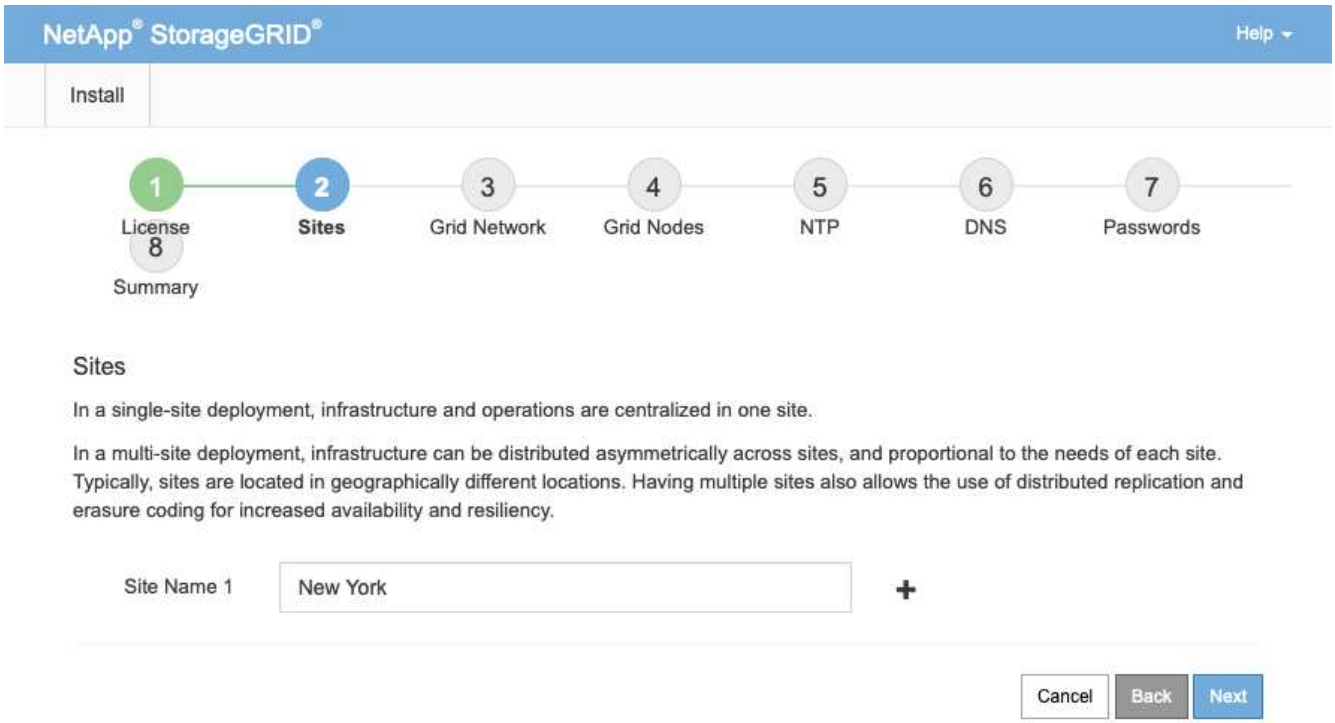
Debe especificar el nombre del sistema StorageGRID y cargar el archivo de licencia proporcionado por NetApp.

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

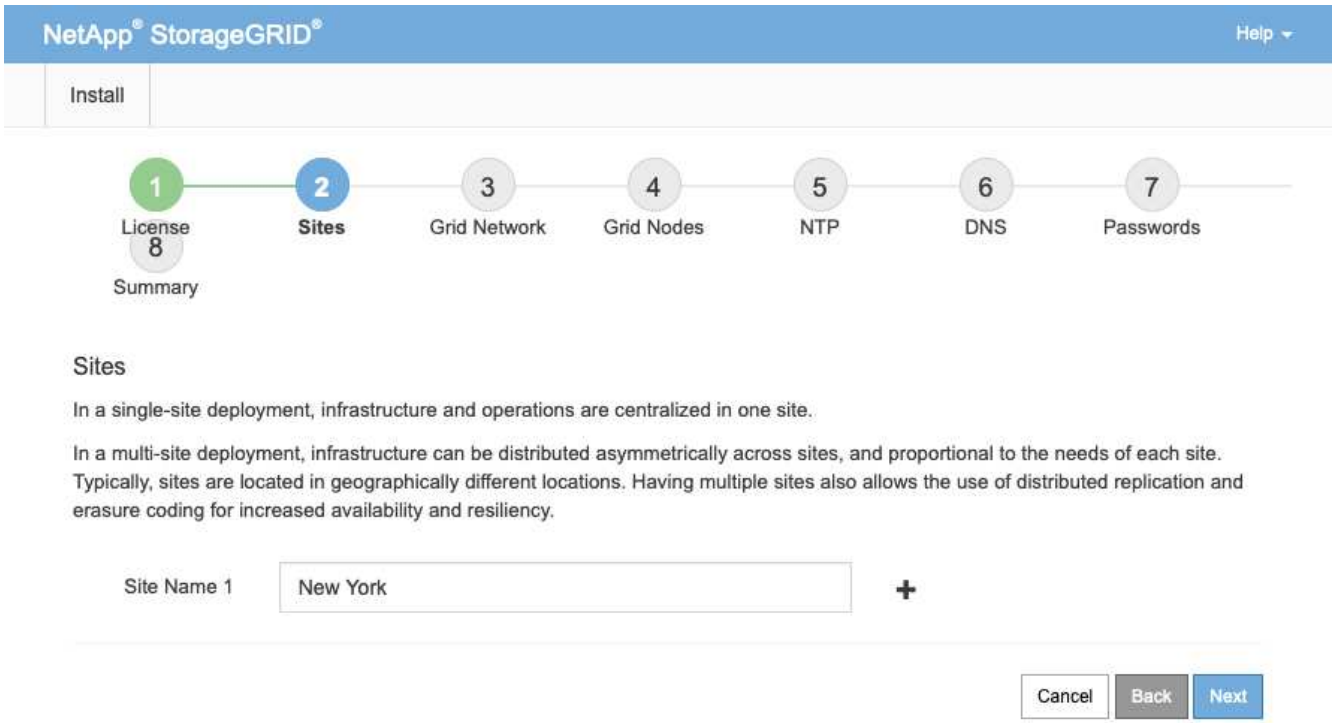
Aprenda a añadir sitios a StorageGRID para aumentar la fiabilidad y la capacidad de almacenamiento.

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.

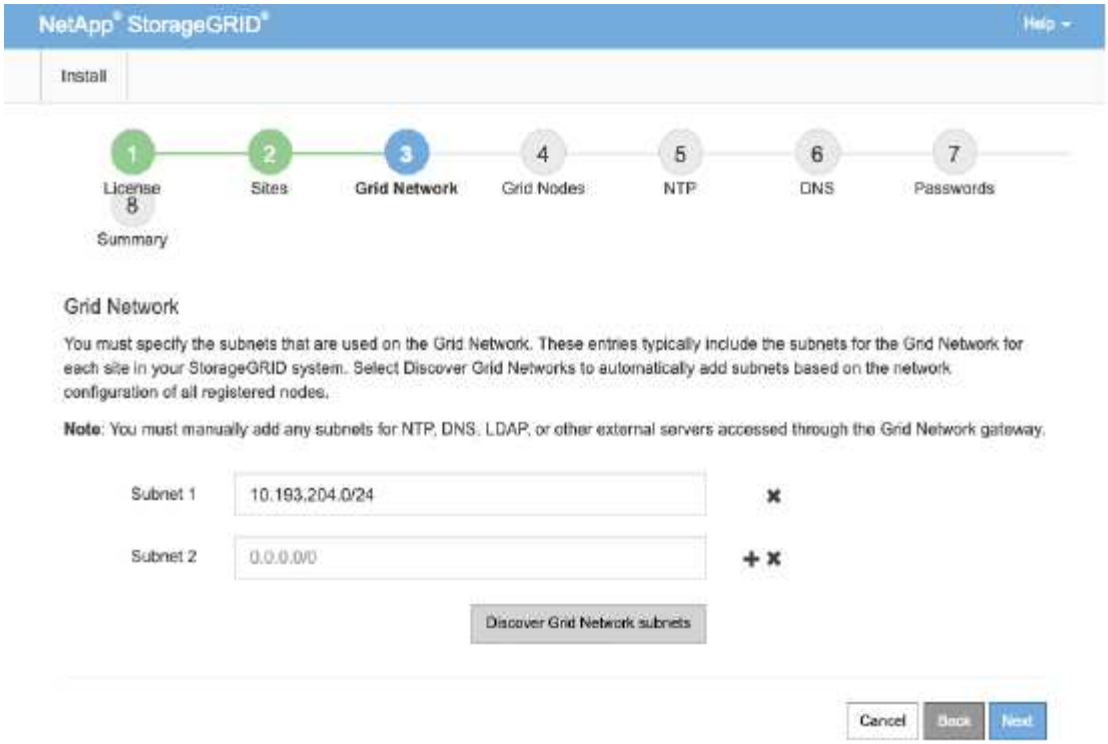
Las entradas de subred incluyen las subredes de la red de grid para cada sitio del sistema StorageGRID, además de las subredes a las que debe accederse a través de la red de grid (por ejemplo, las subredes que alojan los servidores NTP).

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.

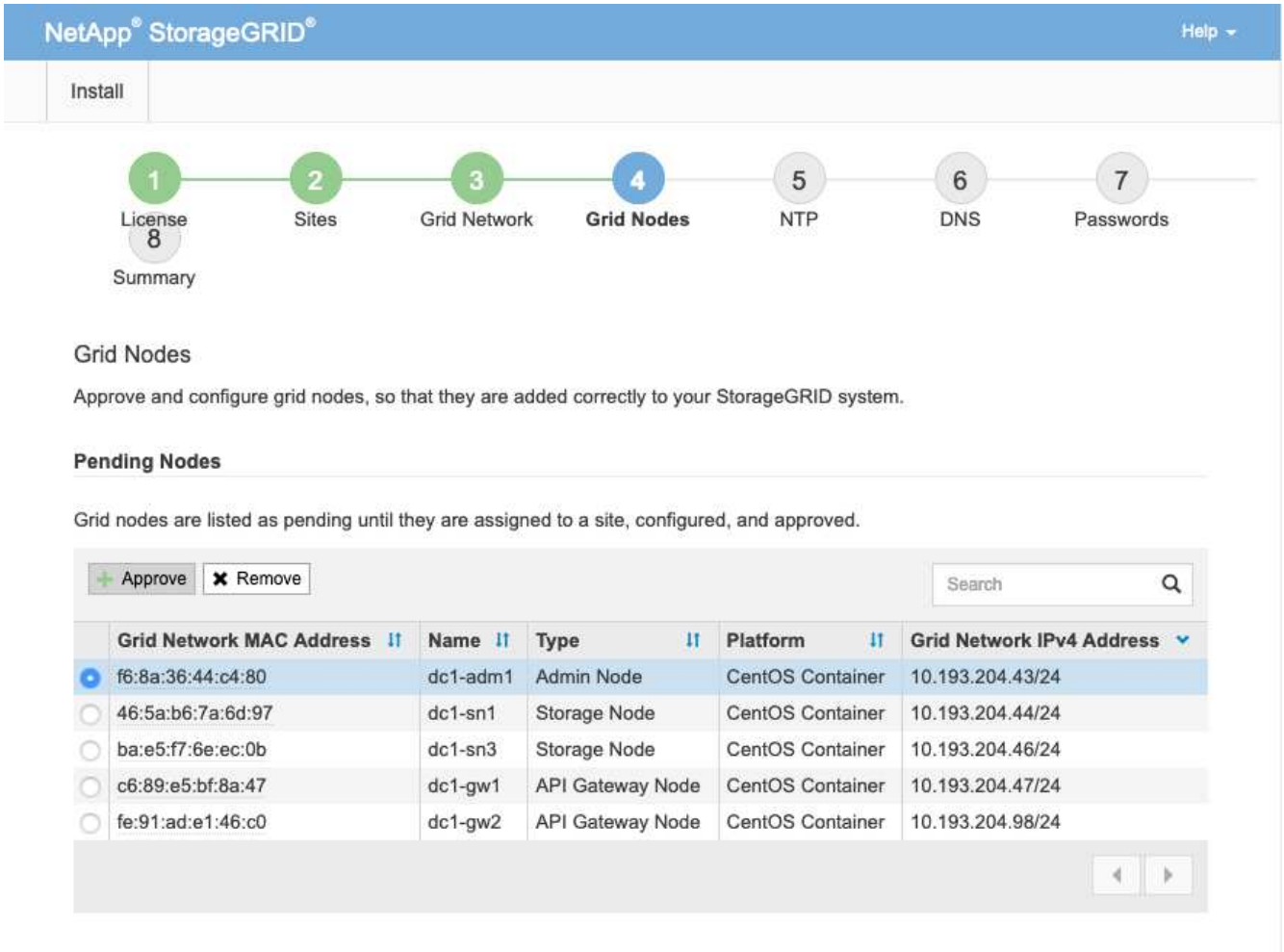
Para aprobar nodos de cuadrícula pendientes, realice los siguientes pasos:

Pasos

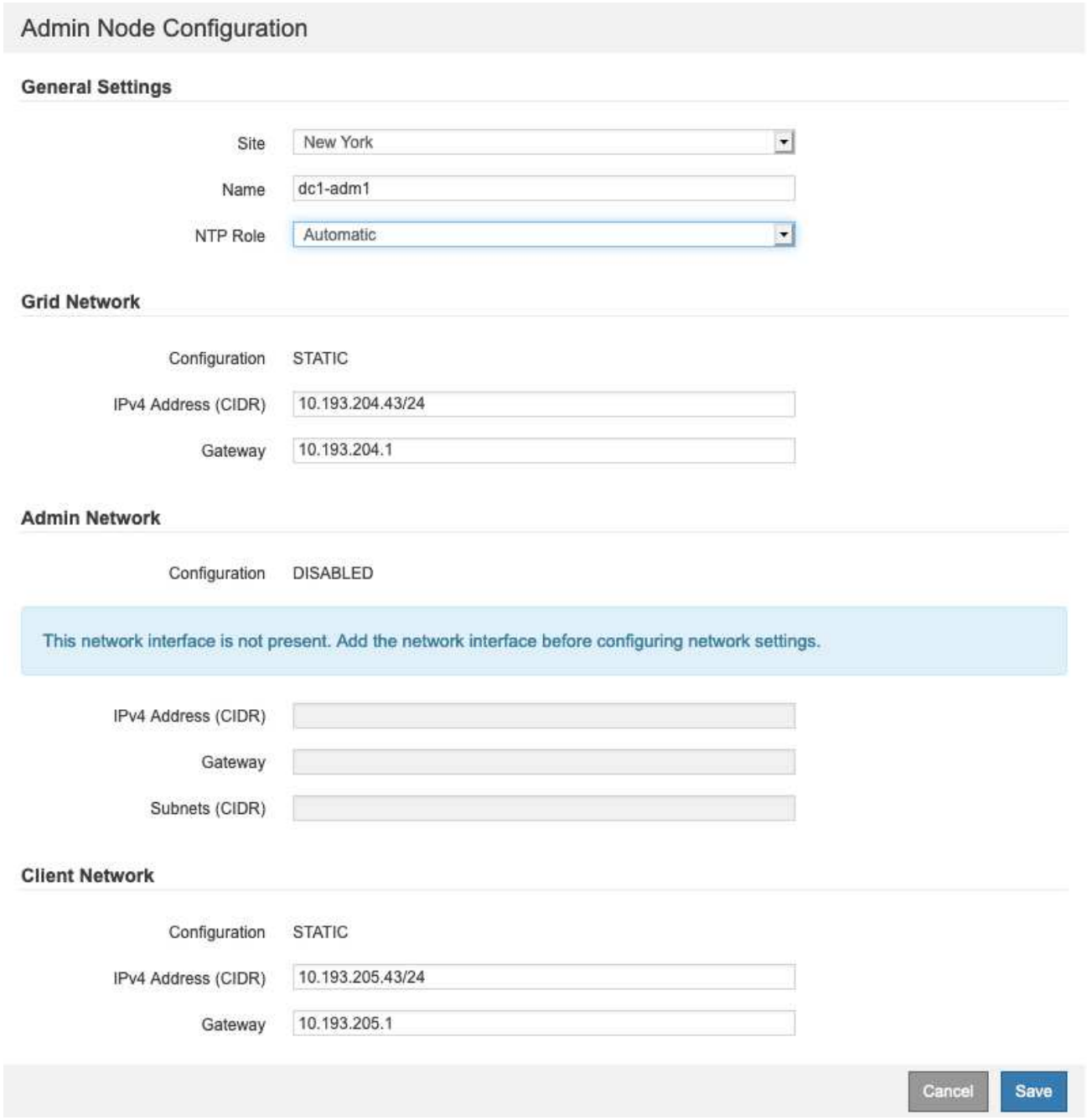
1. Revise la lista Pending Nodes y confirme que muestra todos los nodos de grid que ha implementado.

   > 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.

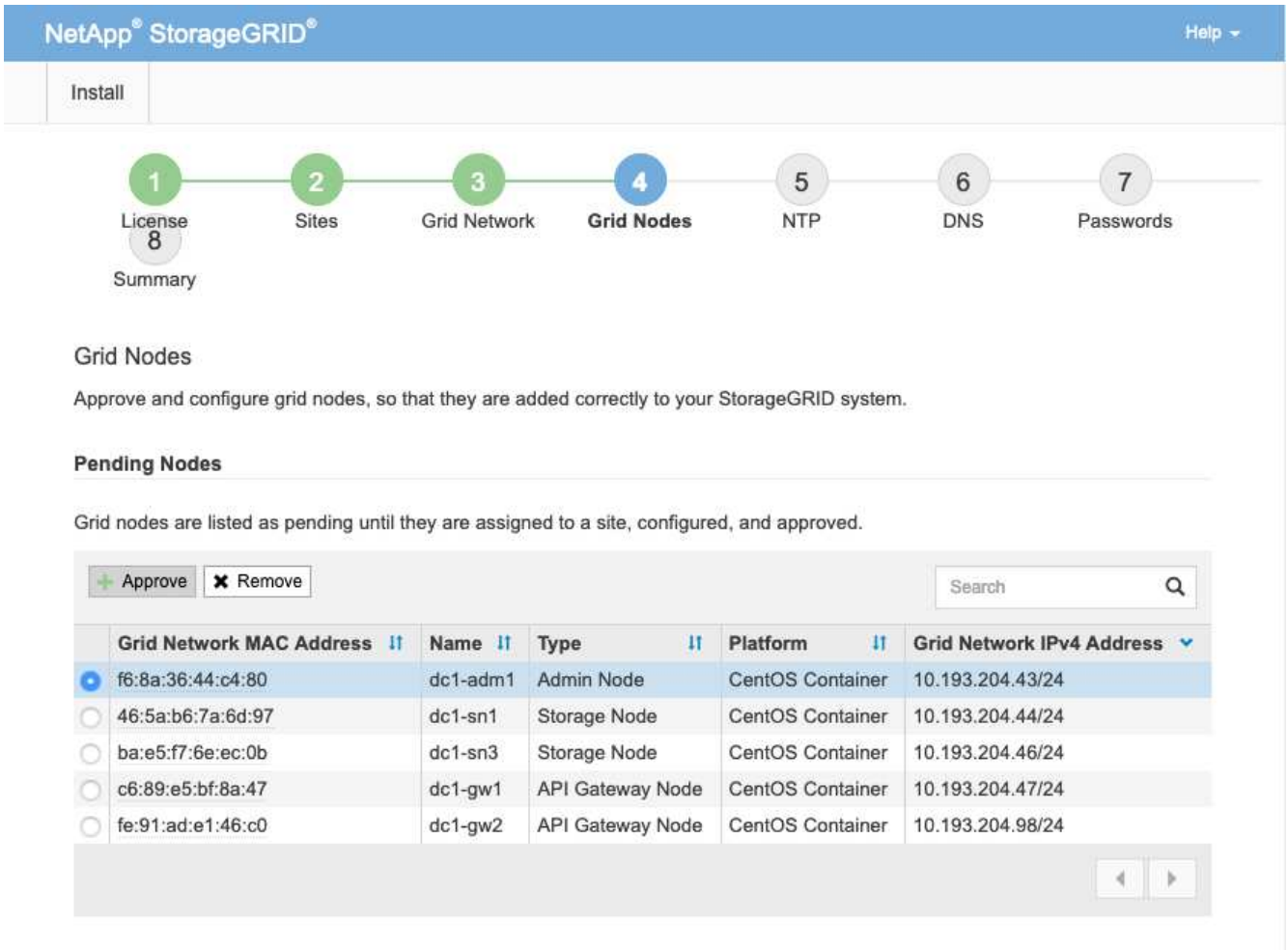
Si seleccionó DHCP para la configuración de red de administración y cambia aquí el valor, el nuevo valor se configura como una dirección estática en el nodo. Asegúrese de que la dirección IP resultante no esté en un pool de direcciones DHCP.

- 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.

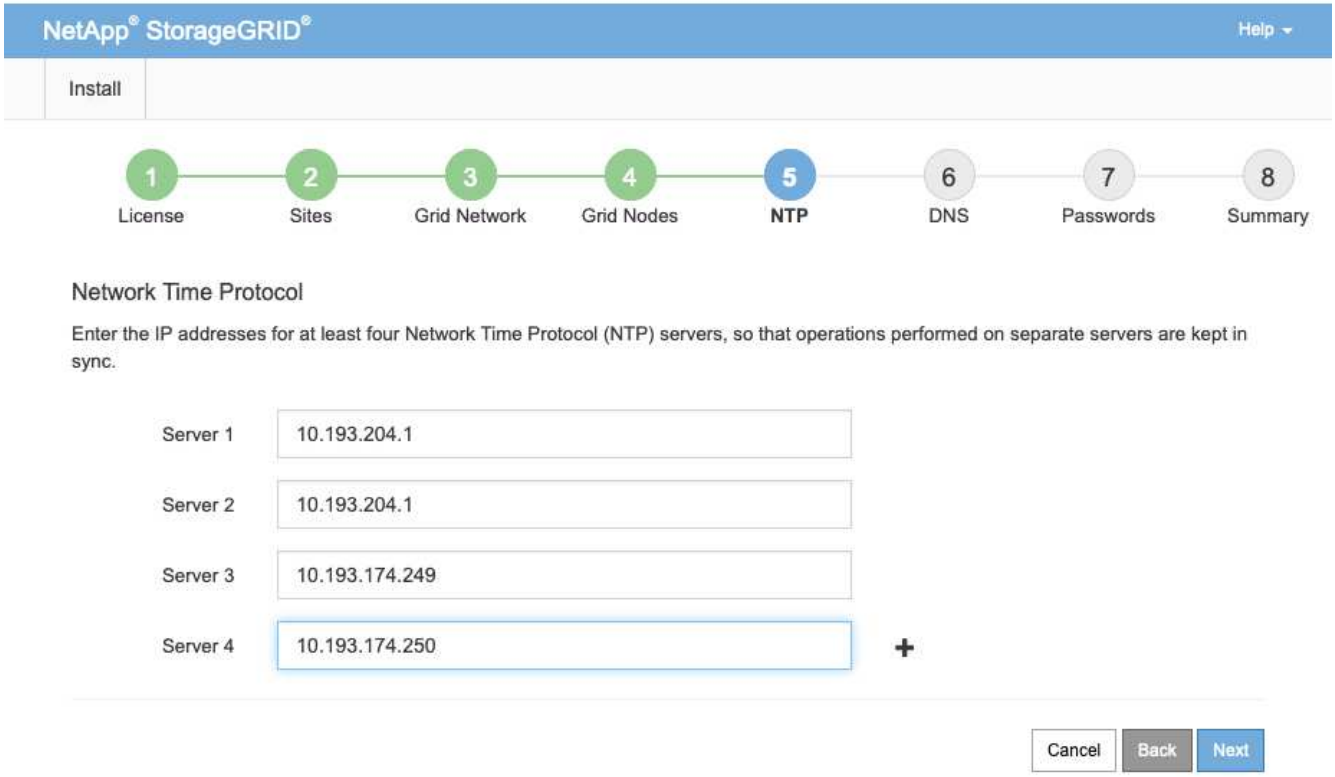
Los nodos a los que se asignaron anteriormente los roles NTP primarios utilizan los servidores NTP externos.

> 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.

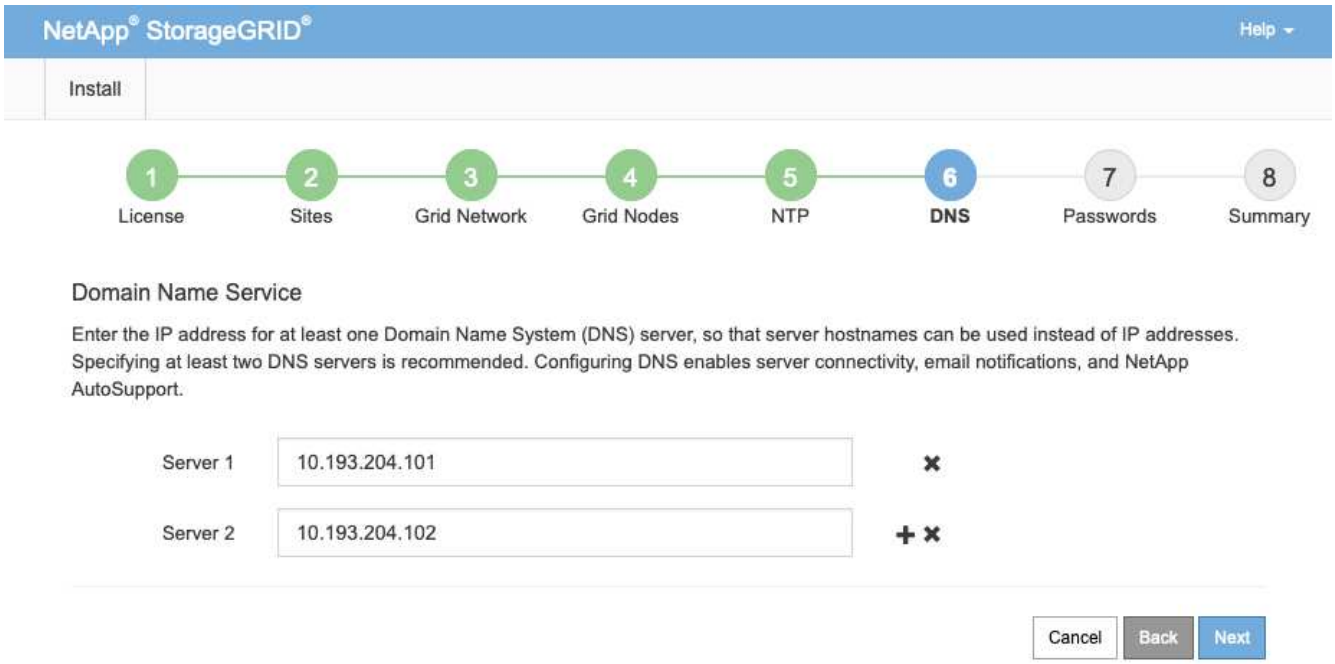
La especificación de la información del servidor DNS le permite utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones de correo electrónico y mensajes de NetApp AutoSupport®. NetApp recomienda especificar al menos dos servidores DNS.

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.

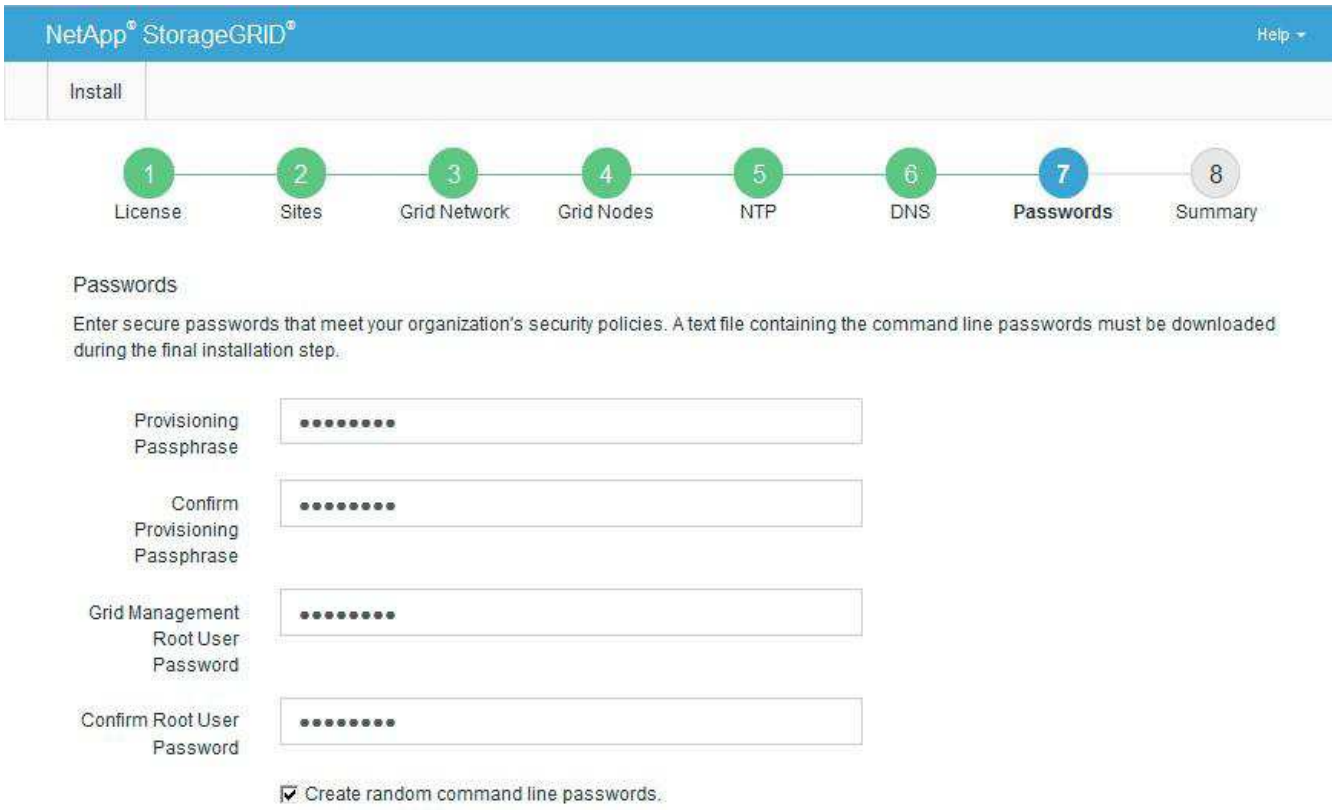
Especifique las contraseñas del sistema para StorageGRID

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.

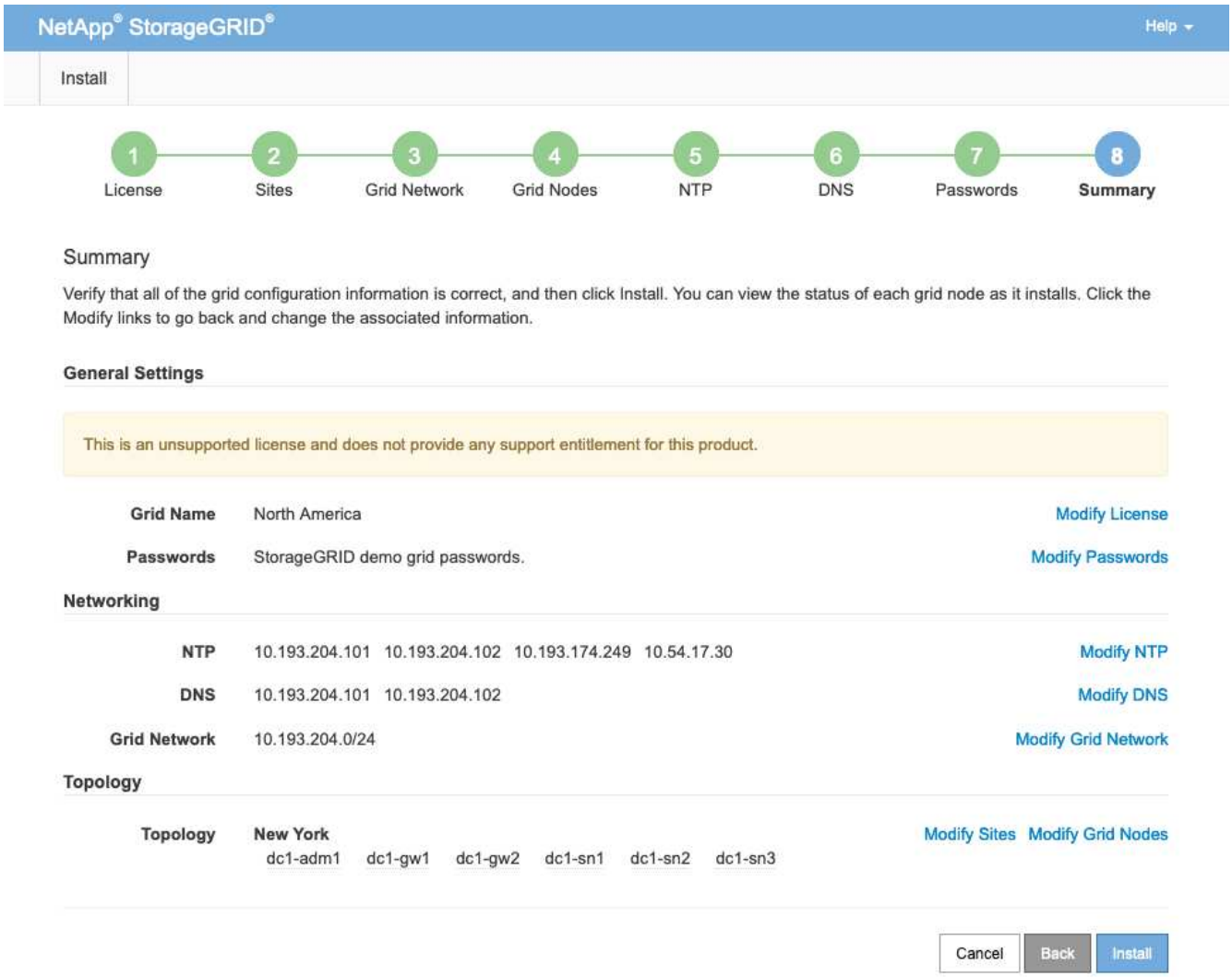
Revisar la configuración y completar la instalación de StorageGRID

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.

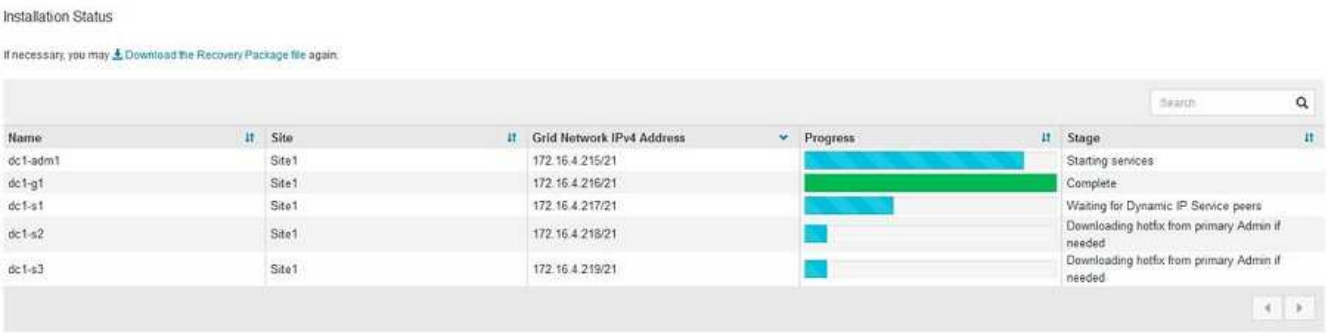
   Cuando la instalación avanza hasta el punto en el que se define la topología de cuadrícula, se le solicita que descargue el archivo Recovery Package (`.zip`) y confirme que puede acceder al contenido de este archivo. Debe descargar el archivo del paquete de recuperación para poder recuperar el sistema 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

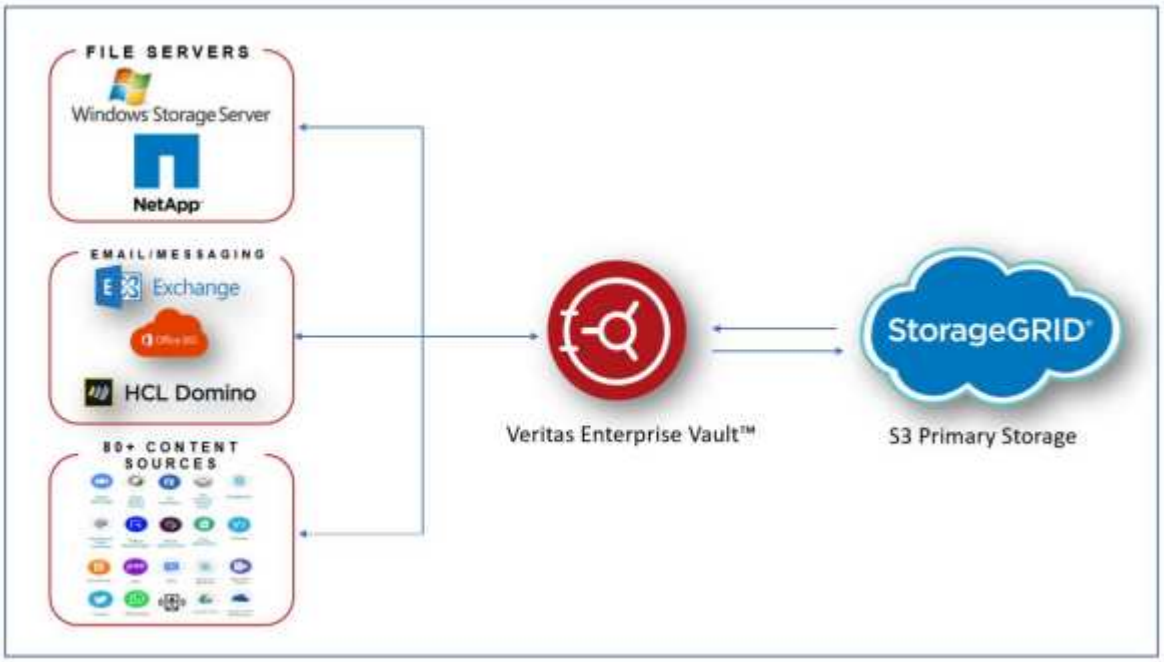
Introducción a la configuración de StorageGRID para conmutación por error del sitio

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.

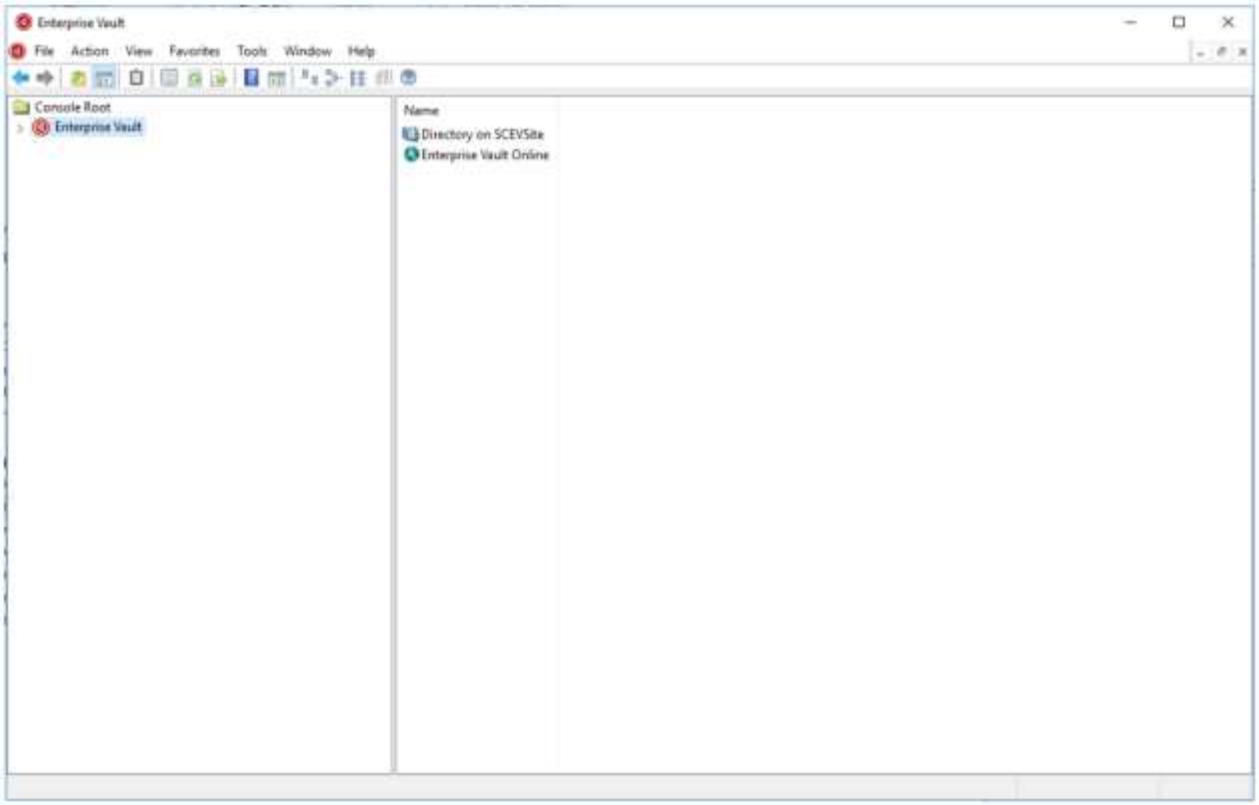
- Se han creado grupos de almacenes de almacén y un almacén de almacén. Si quiere más información, consulte la Guía de administración de veritas Enterprise Vault.
- Se creó un inquilino de StorageGRID, una clave de acceso, una clave secreta y un bloque.
- Se creó un extremo de equilibrador de carga de 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

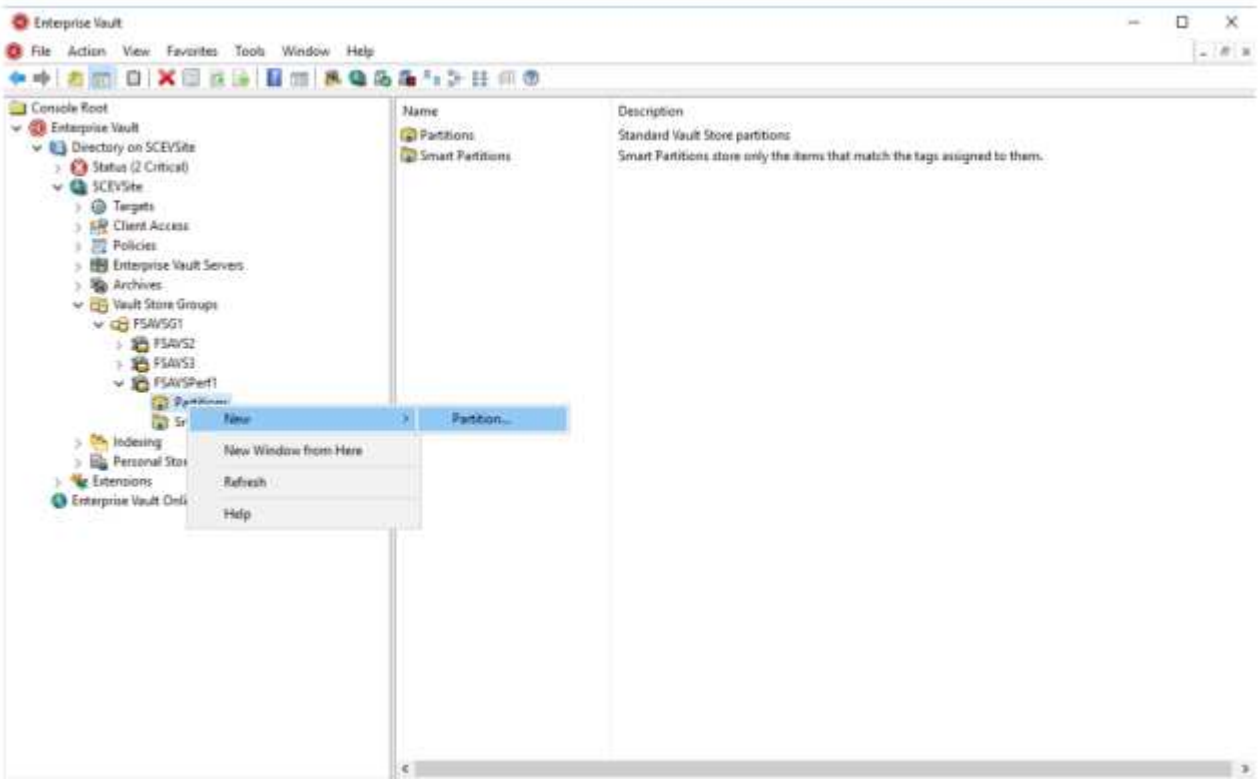
Para configurar StorageGRID con veritas Enterprise Vault, siga estos pasos:

Pasos

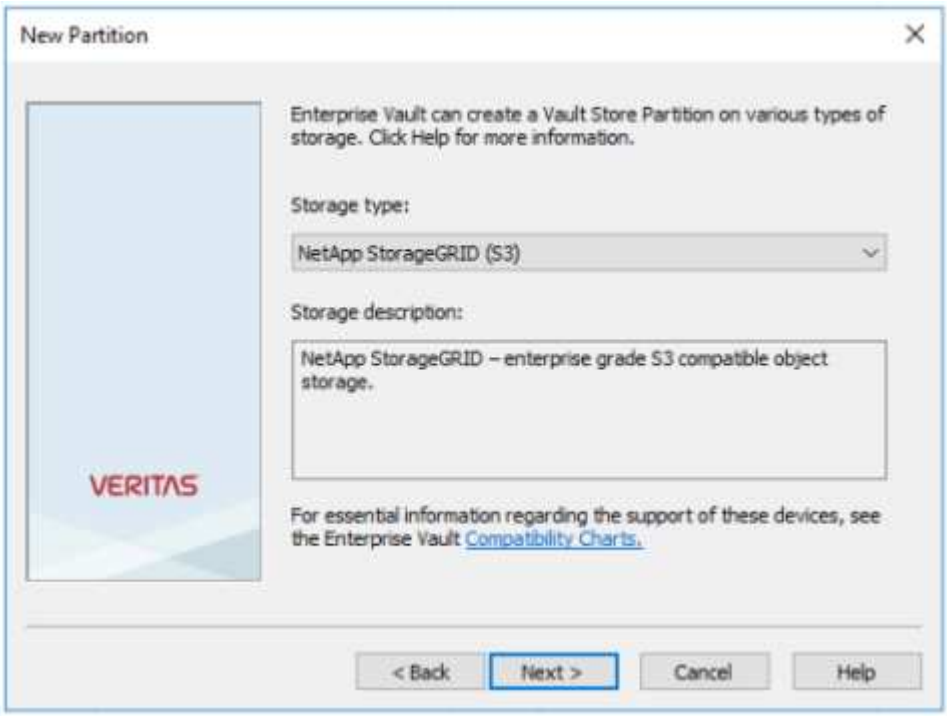
1. Inicie la consola de administración de Enterprise Vault.



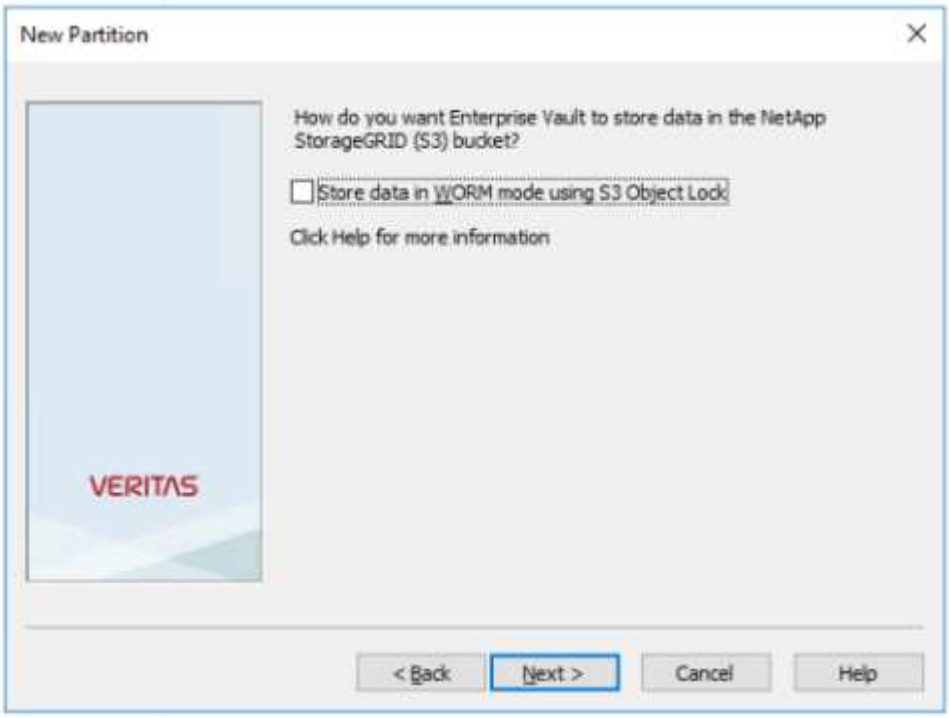
2. Cree una nueva partición de almacén de almacén en el almacén de almacén apropiado. Expanda la carpeta Grupos de Almacén de Almacén y, a continuación, el almacén de almacén apropiado. Haga clic con el botón derecho del ratón en Partición y seleccione el menú Nuevo[Partición].



3. Siga el asistente de creación de nueva partición. En el menú desplegable Storage Type, seleccione NetApp StorageGRID (S3). Haga clic en Siguiente.

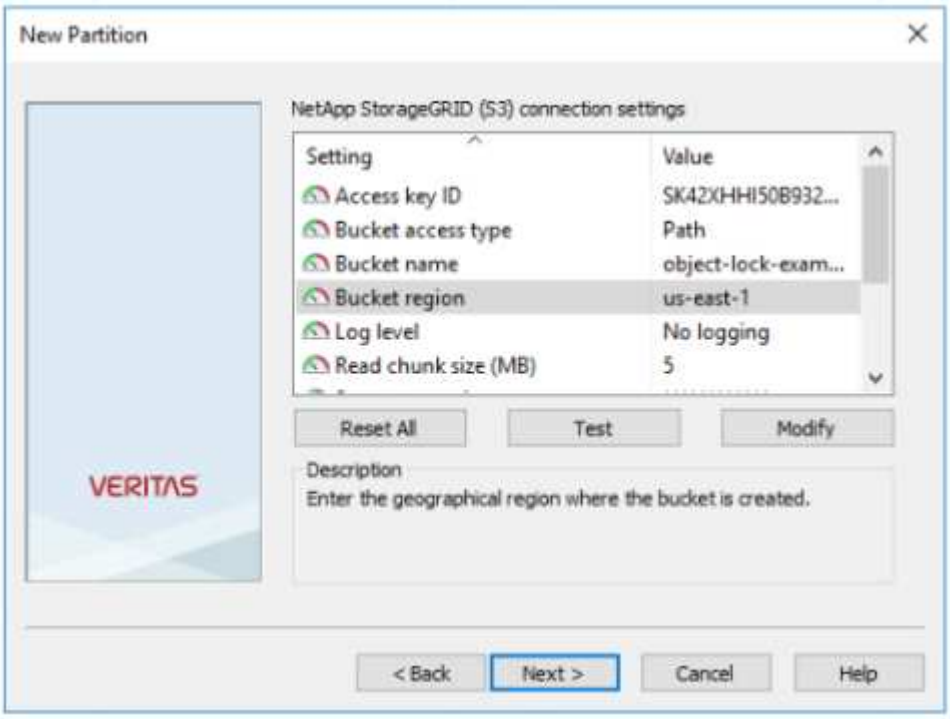


4. Deje la opción Almacenar datos en modo WORM con bloqueo de objetos S3 sin marcar. Haga clic en Siguiente.

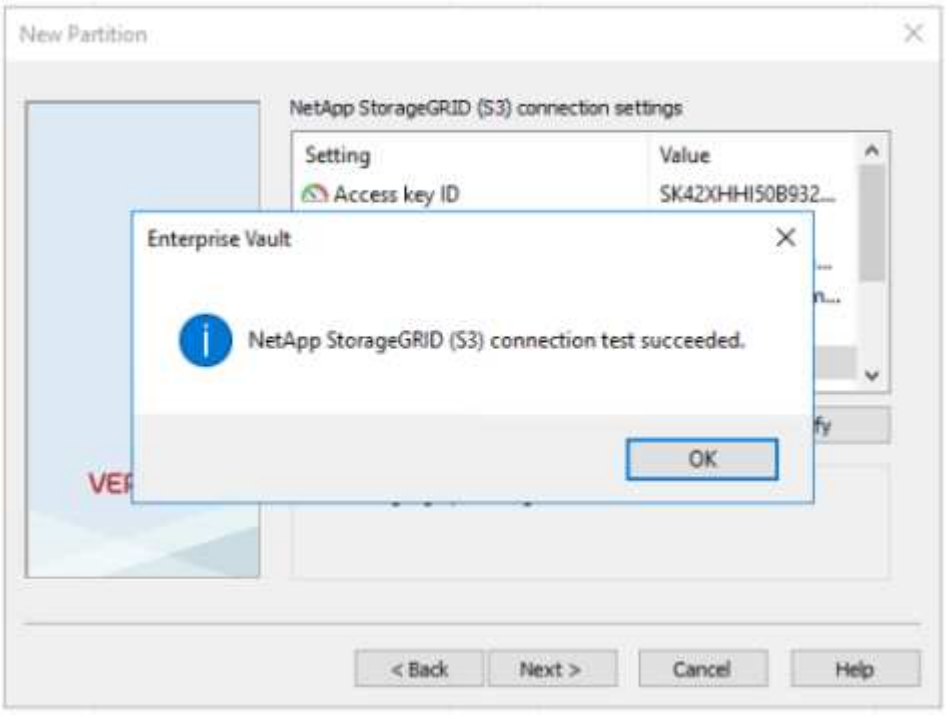


5. En la página de configuración de conexión, proporcione la siguiente información:
   - ID de clave de acceso
   - Clave de acceso secreta
   - Nombre de host del servicio: Asegúrese de incluir el puerto de punto final del equilibrador de carga (LBE) configurado en StorageGRID (como https://<hostname>:<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.

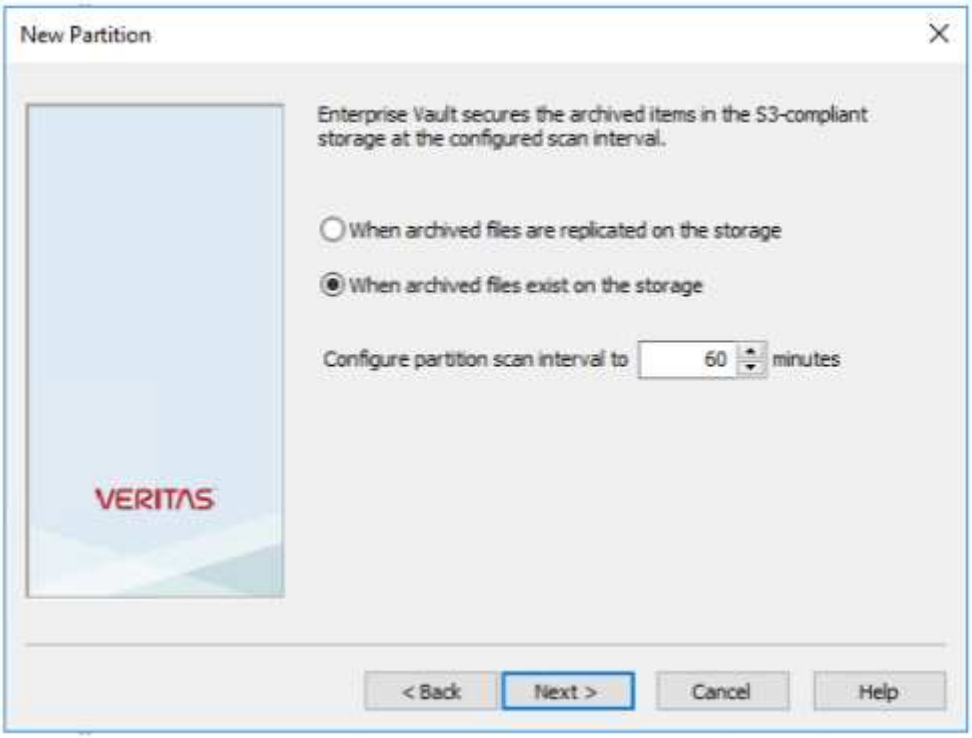


6. Para verificar la conexión con el depósito de StorageGRID, haga clic en Probar. Compruebe que la prueba de conexión se ha realizado correctamente. Haga clic en Aceptar y, a continuación, en Siguiente.

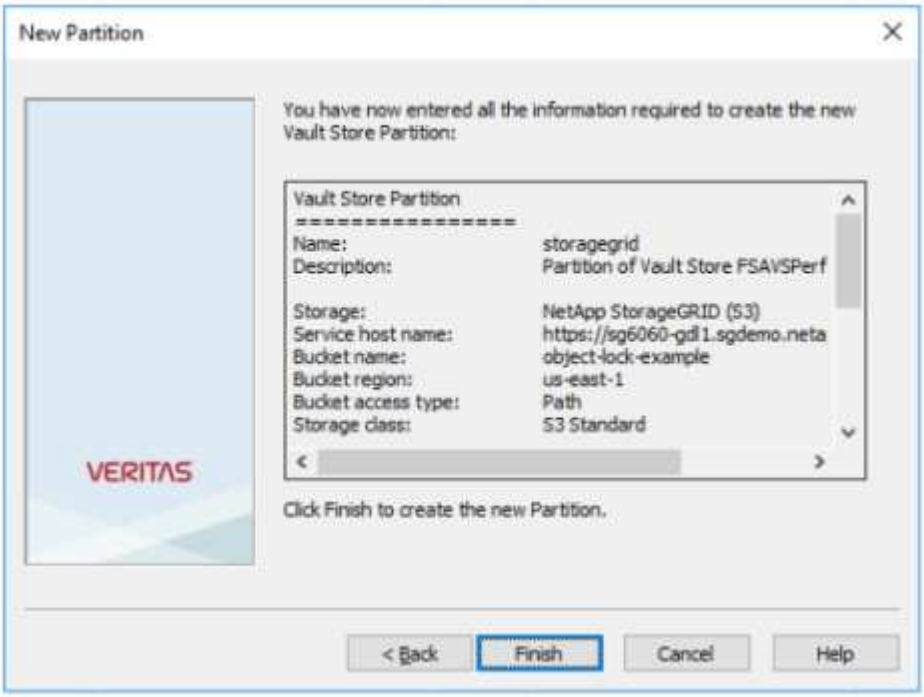


7. StorageGRID no admite el parámetro de replicación S3. Para proteger los objetos, StorageGRID utiliza las reglas de gestión del ciclo de vida de la información (ILM) para especificar esquemas de protección de datos: Varias copias o código de borrado. Seleccione la opción Cuando existen archivos archivados en el

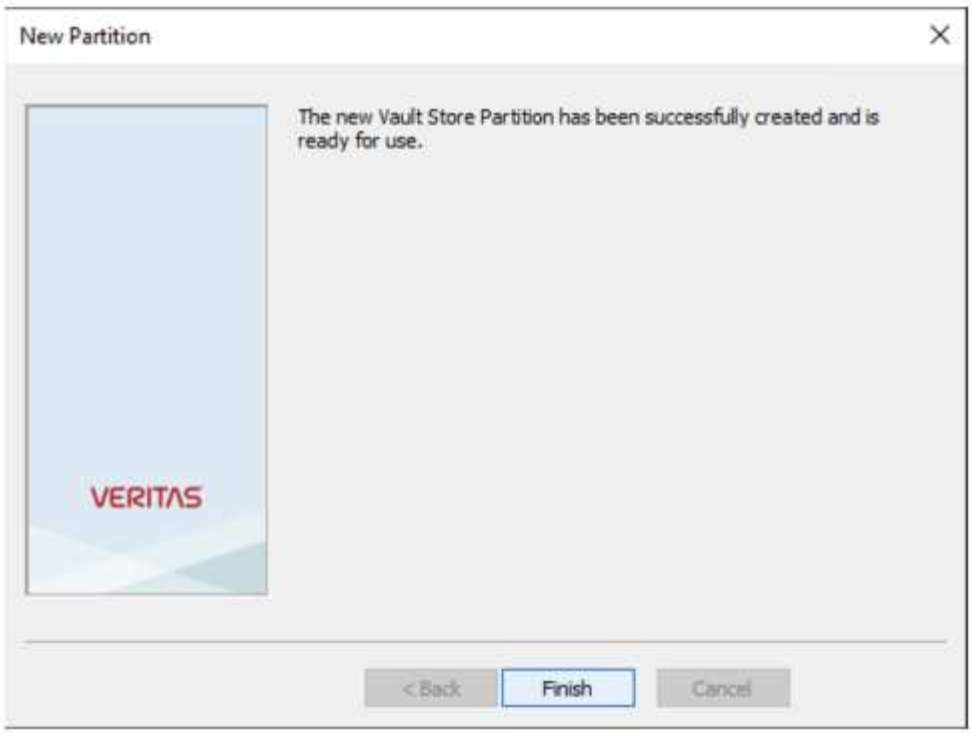
almacenamiento y haga clic en Siguiente.



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

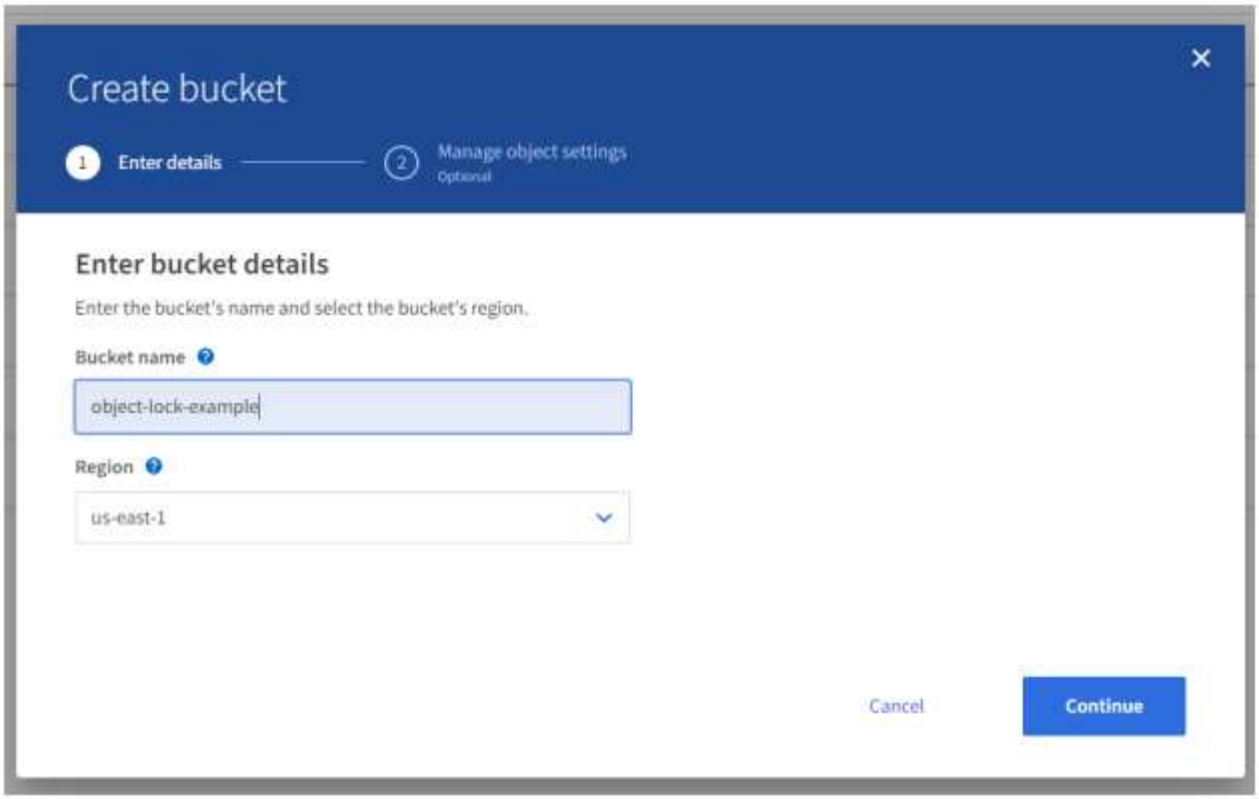
Para el ALMACENAMIENTO WORM, StorageGRID utiliza Object Lock de S3 para conservar objetos para garantizar el cumplimiento de normativas. Para ello se requiere StorageGRID 11,6 o posterior, donde se introdujo la retención de bloques predeterminados de S3 bloqueos de objetos. Enterprise Vault también requiere la versión 14.2.2 o superior.

Configure la retención de bloques predeterminados de bloqueo de objetos de StorageGRID S3

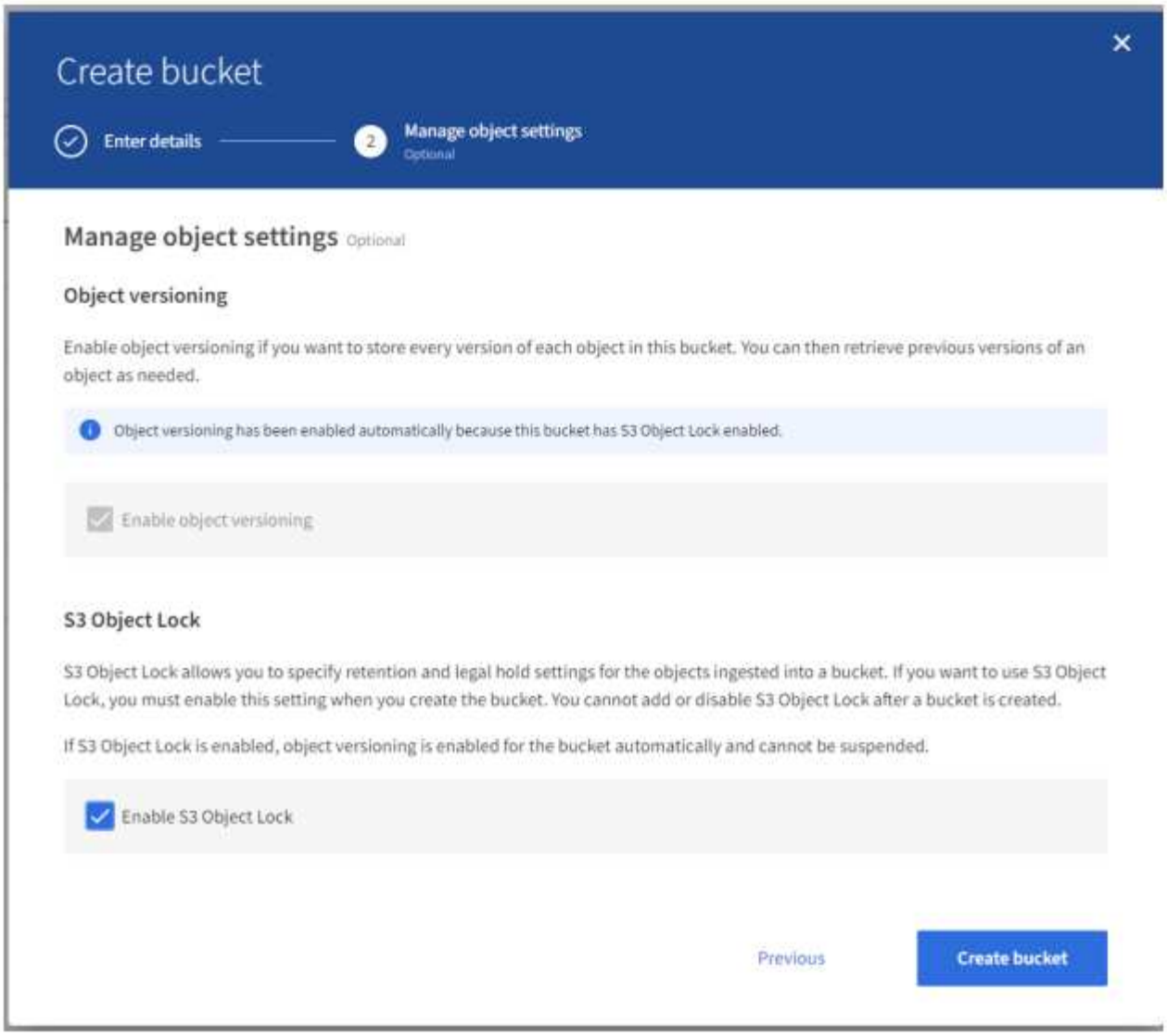
Para configurar la retención predeterminada del depósito de bloqueo de objetos de StorageGRID S3, lleve a cabo los siguientes pasos:

Pasos

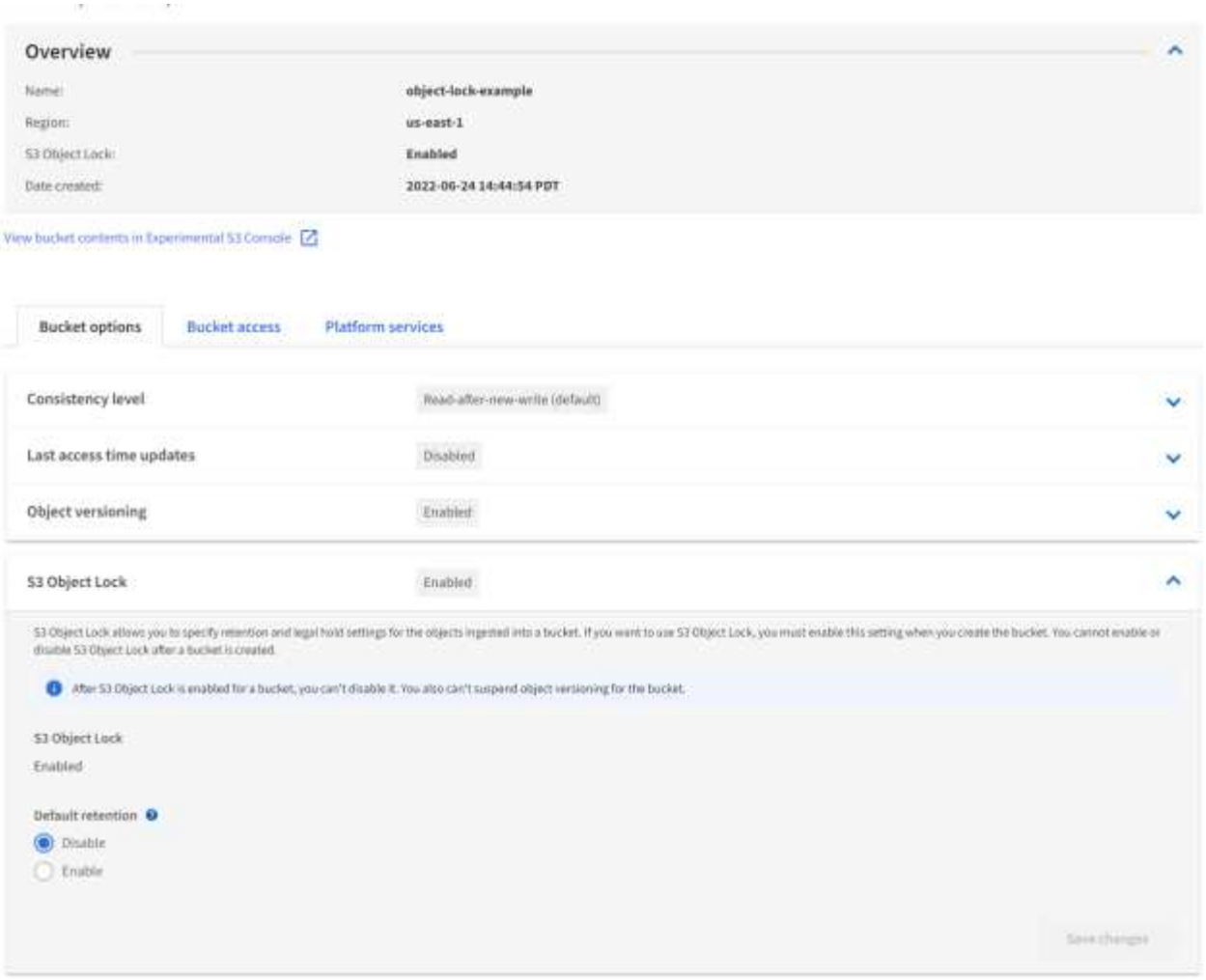
1. En el Administrador de inquilinos de StorageGRID, cree un bloque y haga clic en Continue



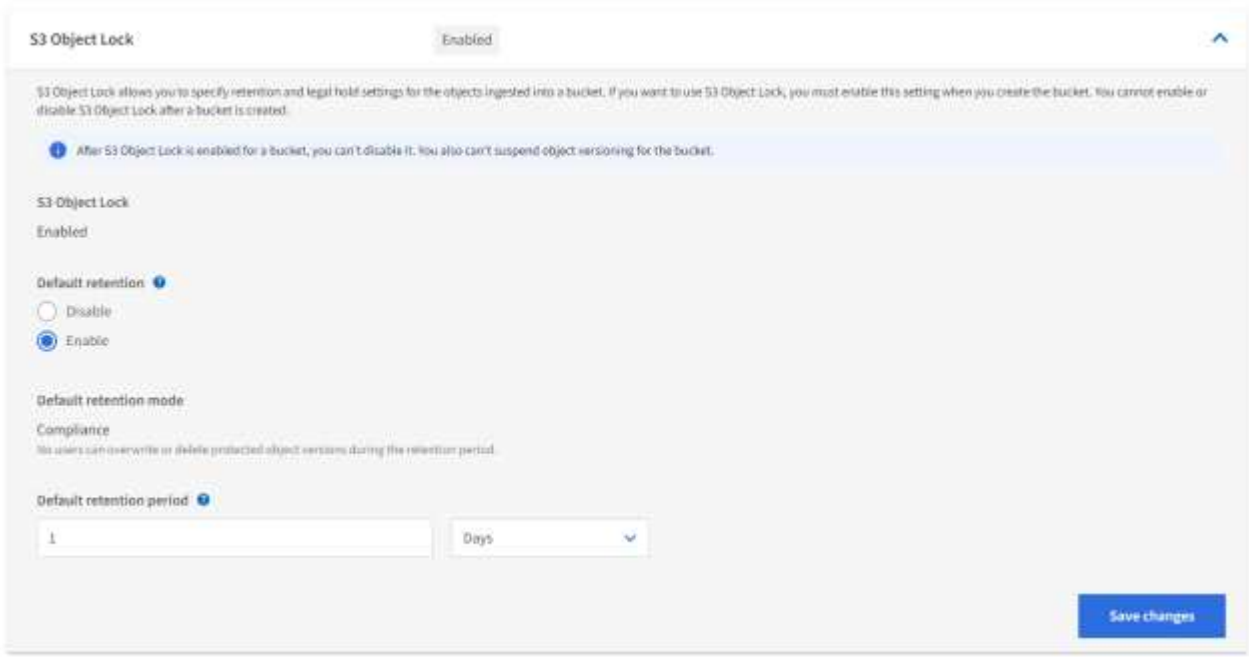
2. Seleccione la opción Enable S3 Object Lock y haga clic en Create Bucket.



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.



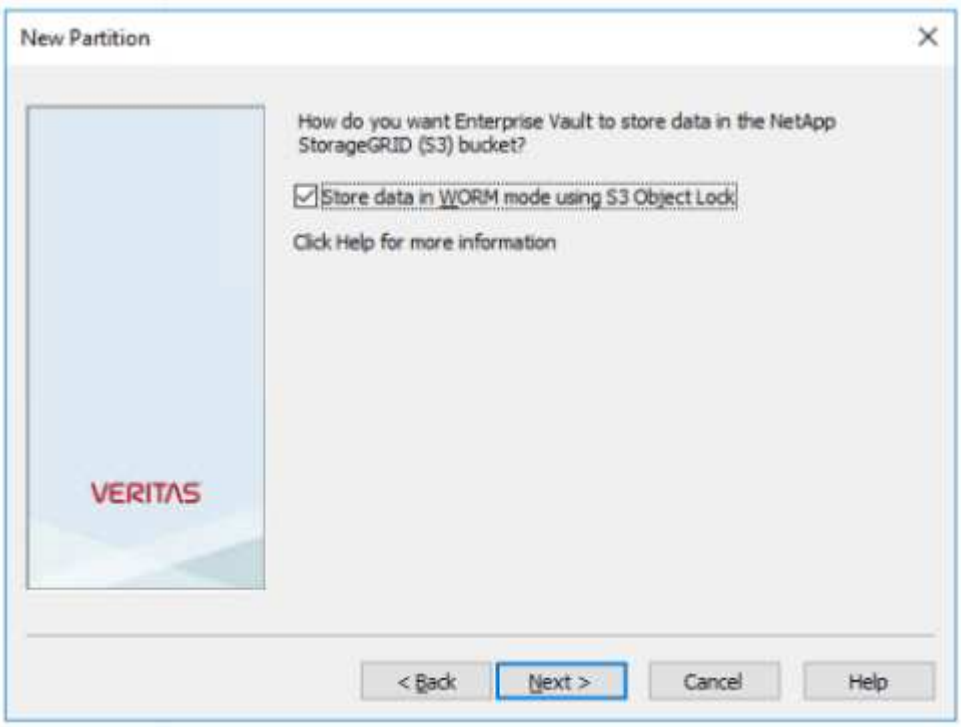
Enterprise Vault ya puede utilizar el bloque para almacenar DATOS WORM.

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

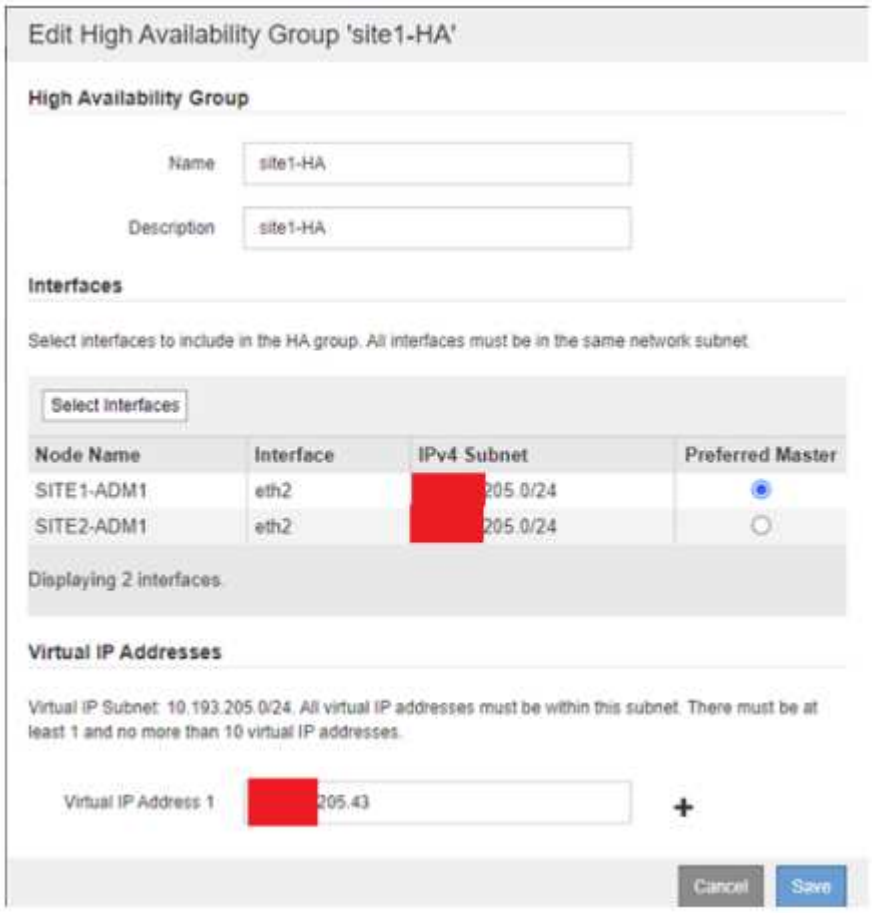
Para configurar la conmutación por error del sitio StorageGRID, lleve a cabo los siguientes pasos:

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.



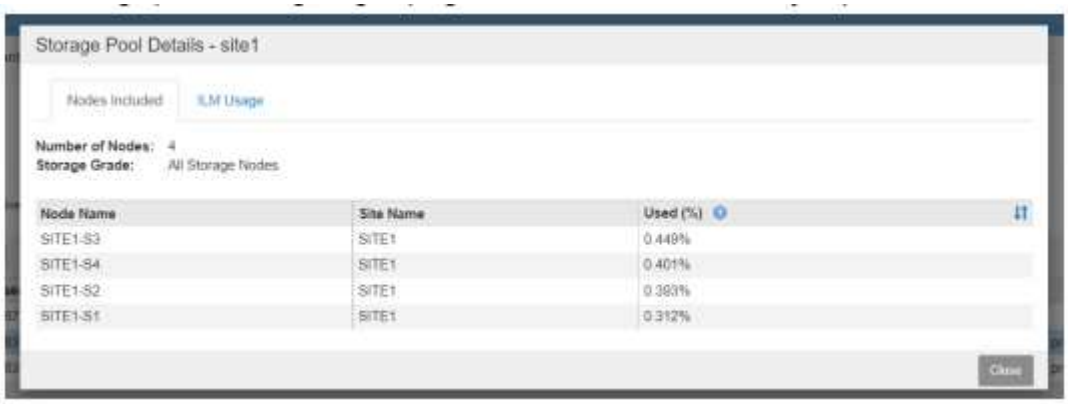
3. Esta dirección IP virtual (VIP) debe asociarse al nombre de host S3 utilizado durante la configuración de

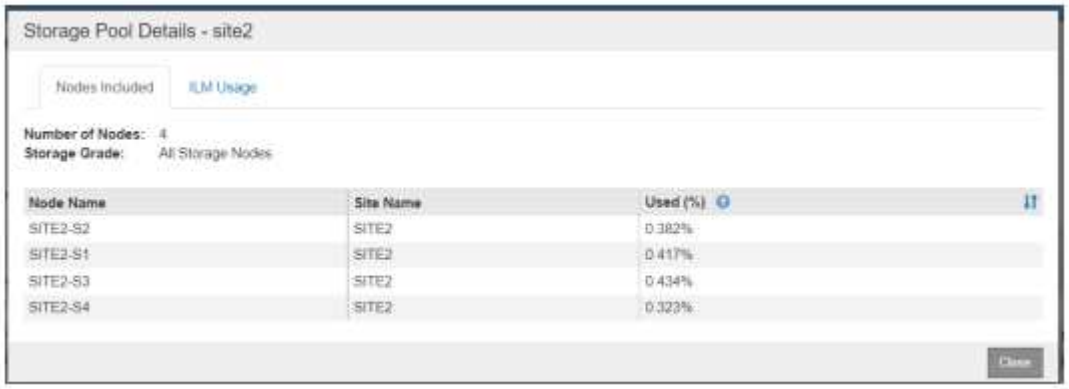
particiones de veritas Enterprise Vault. La dirección VIP resuelve el tráfico a site1 y, durante el fallo de site1, la dirección VIP redirige el tráfico de forma transparente A Site2.

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.