Guías de características de productos

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Tabla de contenidos

Guías de características de productos

Cree Cloud Storage Pool para AWS o Google Cloud

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

Lo que necesitará

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

Pasos

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

   Se mostrará la ventana emergente Create Cloud Storage Pool.

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

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

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

   Se permiten dos formatos:

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

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

6. Introduzca el nombre de bloque de S3.

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

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

Resultado esperado

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

Por Jonathan Wong

Cree Cloud Storage Pool para el almacenamiento BLOB de Azure

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

Lo que necesitará

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

Pasos

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

   Se mostrará la ventana emergente Create Cloud Storage Pool.

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

   Se permiten dos formatos:

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

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

6. Introduzca el nombre del contenedor de Azure.

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

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

Resultado esperado

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

Por Jonathan Wong

Utilice un pool de almacenamiento en el cloud para el backup

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

Lo que necesitará

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

Pasos

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

Resultado esperado

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

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

Por Jonathan Wong

Configure el servicio de integración de búsqueda StorageGRID

En esta guía, se ofrecen instrucciones detalladas para configurar el servicio de integración de búsquedas de NetApp StorageGRID 11.6 con Amazon OpenSearch Service o Elasticsearch en las instalaciones.

Introducción

StorageGRID admite tres tipos de servicios de plataforma.

- **Replicación CloudMirror de StorageGRID**. Reflejar objetos específicos desde un bloque de StorageGRID en un destino externo especificado.
- **Notificaciones**. Notificaciones de eventos por bloque para enviar notificaciones sobre acciones específicas realizadas en los objetos a un Amazon simple Notification Service (Amazon SNS) externo especificado.
- **Servicio de integración de búsqueda**. Envíe metadatos de objetos de simple Storage Service (S3) a un índice de Elasticsearch especificado, donde se pueden buscar o analizar los metadatos usando el servicio externo.

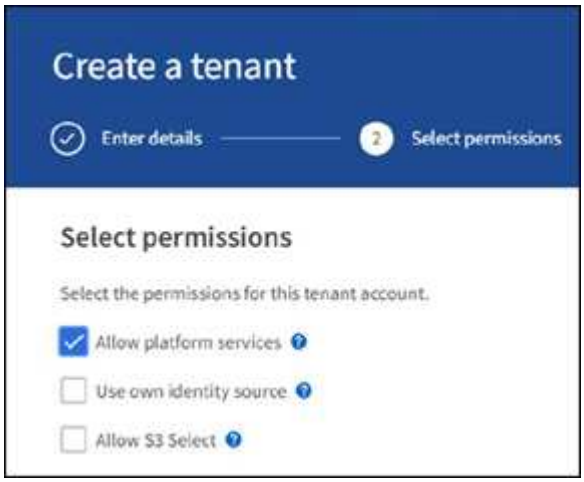
Los servicios de plataforma se configuran por el inquilino de S3 a través de la IU del administrador de inquilinos. Para obtener más información, consulte "Consideraciones sobre el uso de servicios de plataforma".

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

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

Cree un inquilino y habilite los servicios de plataforma

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



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

   Esto le lleva a la página Administrador de inquilinos.

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

Servicios de integración de búsqueda con Amazon OpenSearch

Configuración del servicio Amazon OpenSearch (antes Elasticsearch)

Utilice este procedimiento para una configuración rápida y sencilla del servicio OpenSearch sólo con fines de prueba/demostración. Si utiliza Elasticsearch en las instalaciones para los servicios de integración de búsqueda, consulte la sección Servicios de integración de búsqueda con Elasticsearch en las instalaciones.

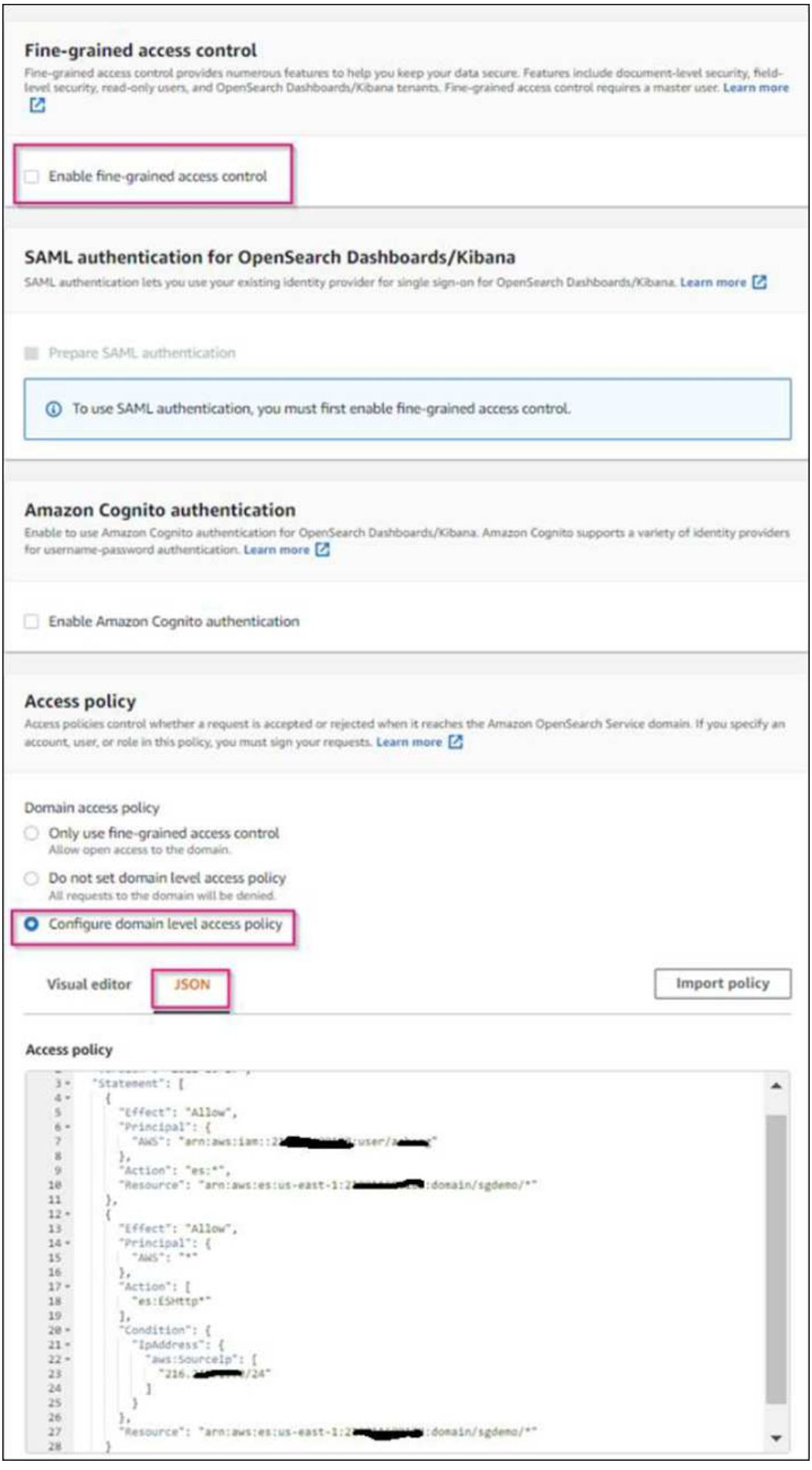
Debe tener un inicio de sesión de la consola de AWS válido, una clave de acceso, una clave de acceso secreta y permisos para suscribirse al servicio OpenSearch.

1. Cree un nuevo dominio siguiendo las instrucciones de "Introducción al servicio AWS OpenSearch",

excepto lo siguiente:

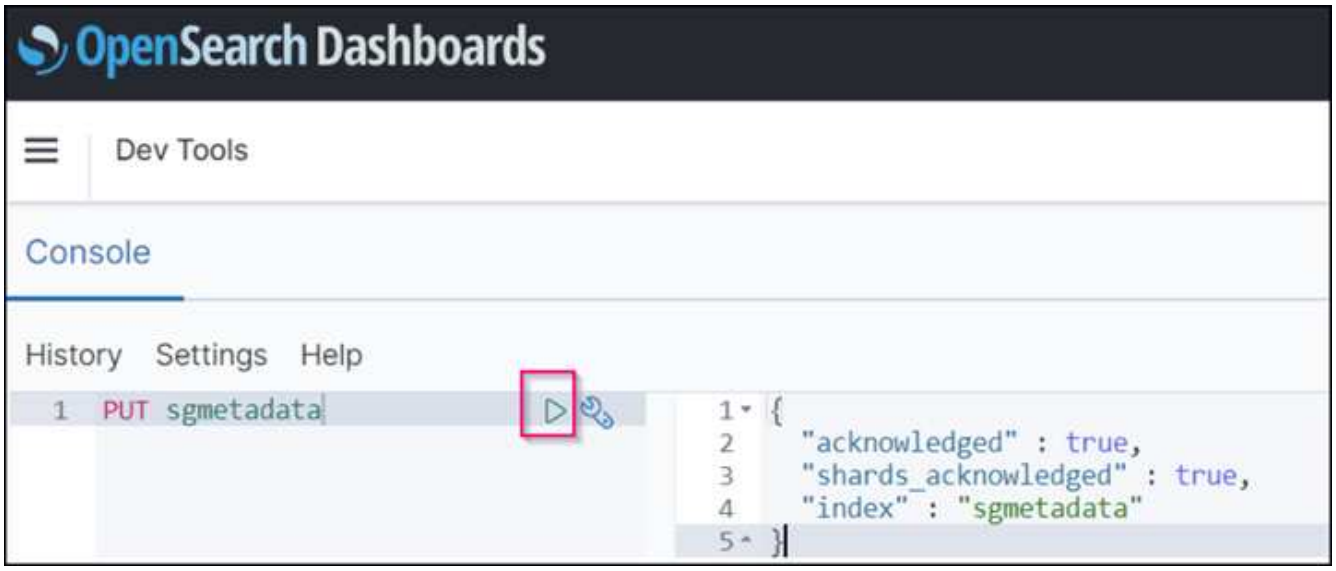
- Paso 4. Nombre de dominio: Sgdemo
- Paso 10. Control de acceso detallado: Anule la selección de la opción Habilitar control de acceso detallado.
- Paso 12. Política de acceso: Seleccione Configure Level Access Policy, seleccione la pestaña JSON para modificar la política de acceso mediante el ejemplo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

```
{

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

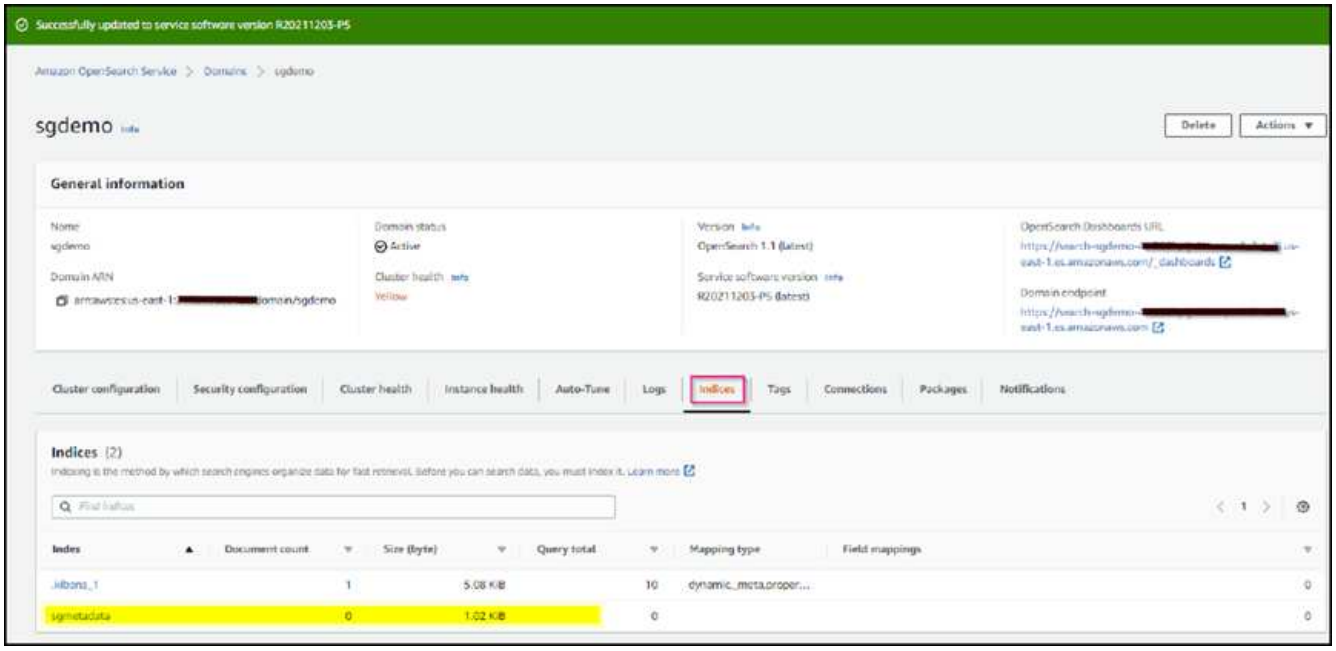

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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

2. Espere de 15 a 20 minutos para que el dominio se active.

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



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

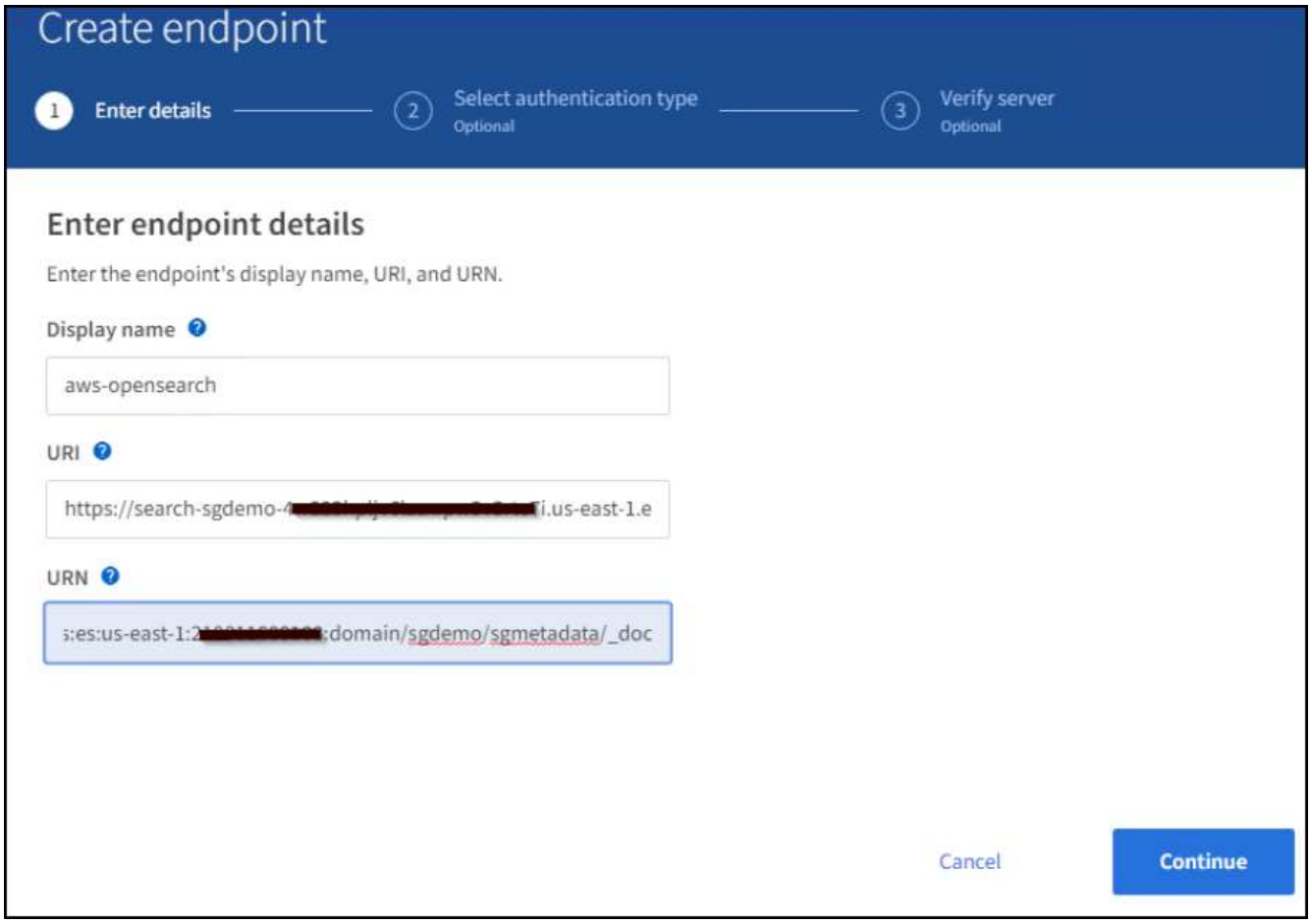


Configuración de extremos de servicios de plataforma

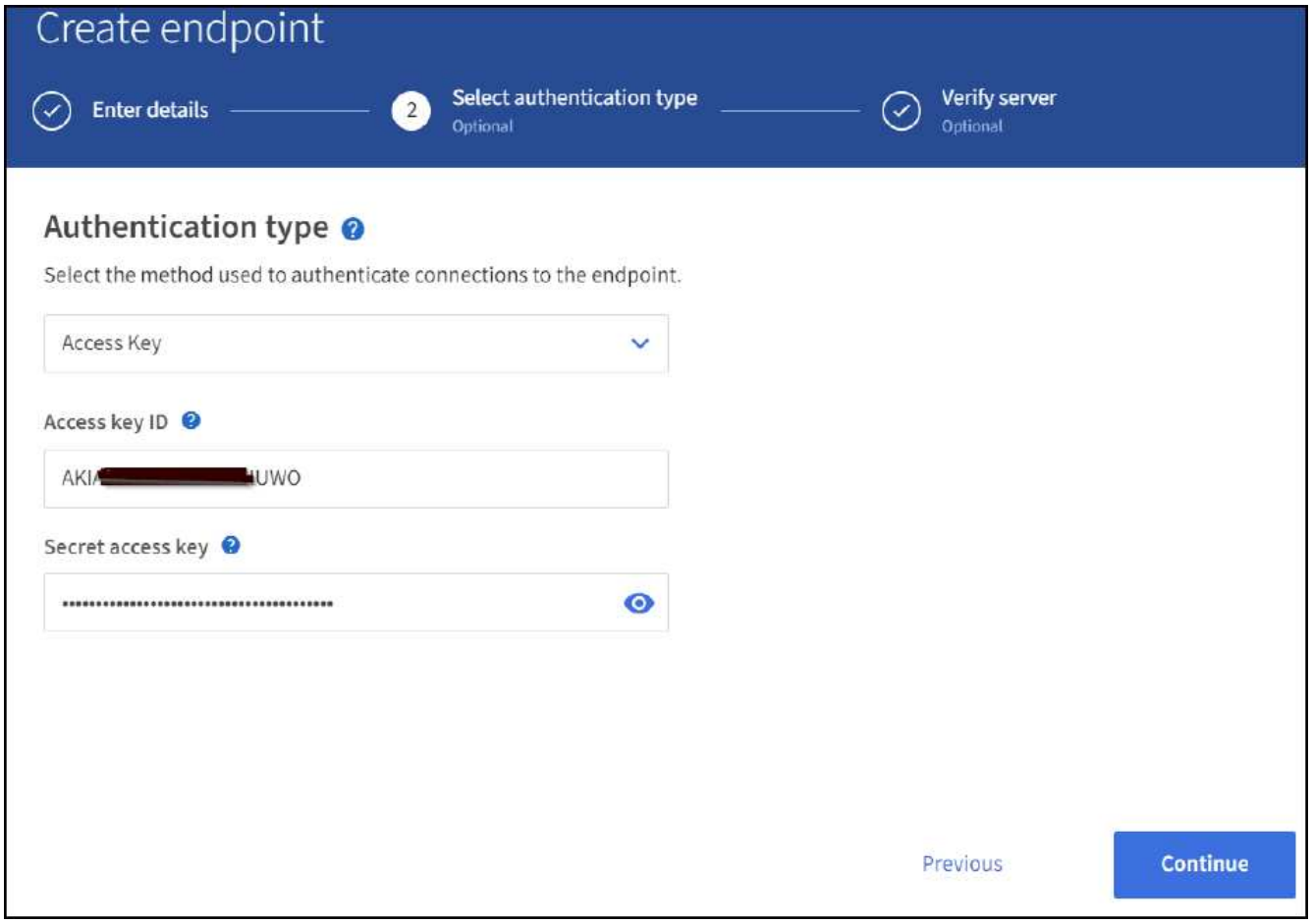
Para configurar los extremos de servicios de la plataforma, siga estos pasos:

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

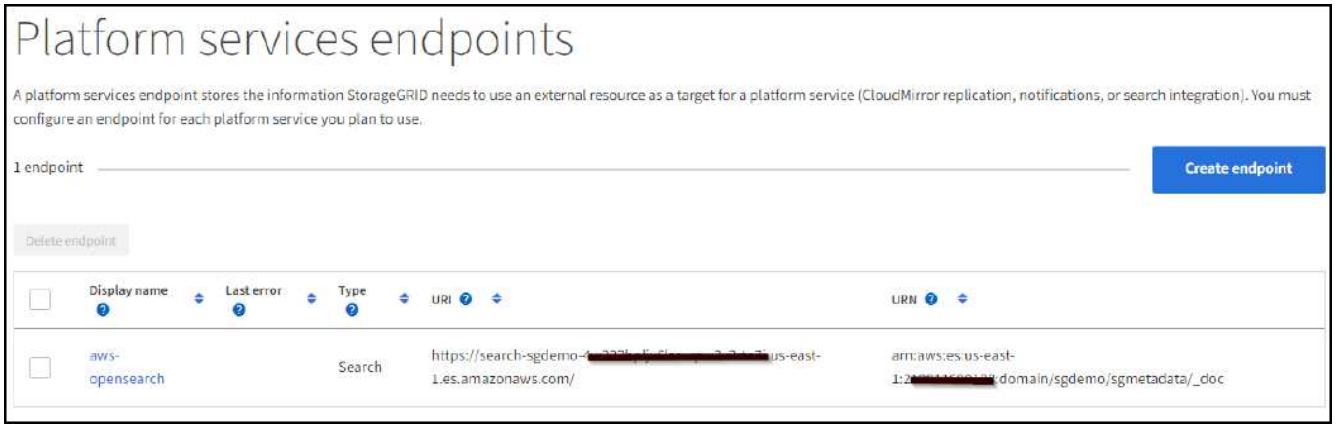
     En este ejemplo, URN se convierte en `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



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



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



Servicios de integración de búsqueda con Elasticsearch en las instalaciones

Configuración de Elasticsearch en las instalaciones

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

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

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

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

```
sudo systemctl enable docker
```

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

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

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

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

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

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

Elasticsearch Service | Self-managed

Install and run Elasticsearch

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

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

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

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

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

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

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

Install and run Kibana

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

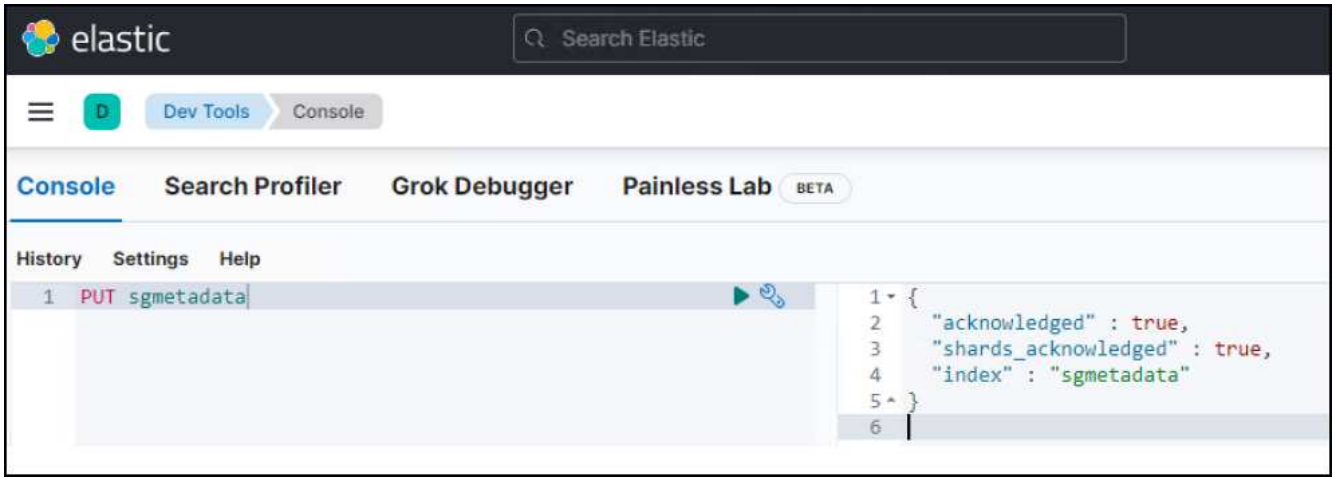
1. In a new terminal session, run:

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

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

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

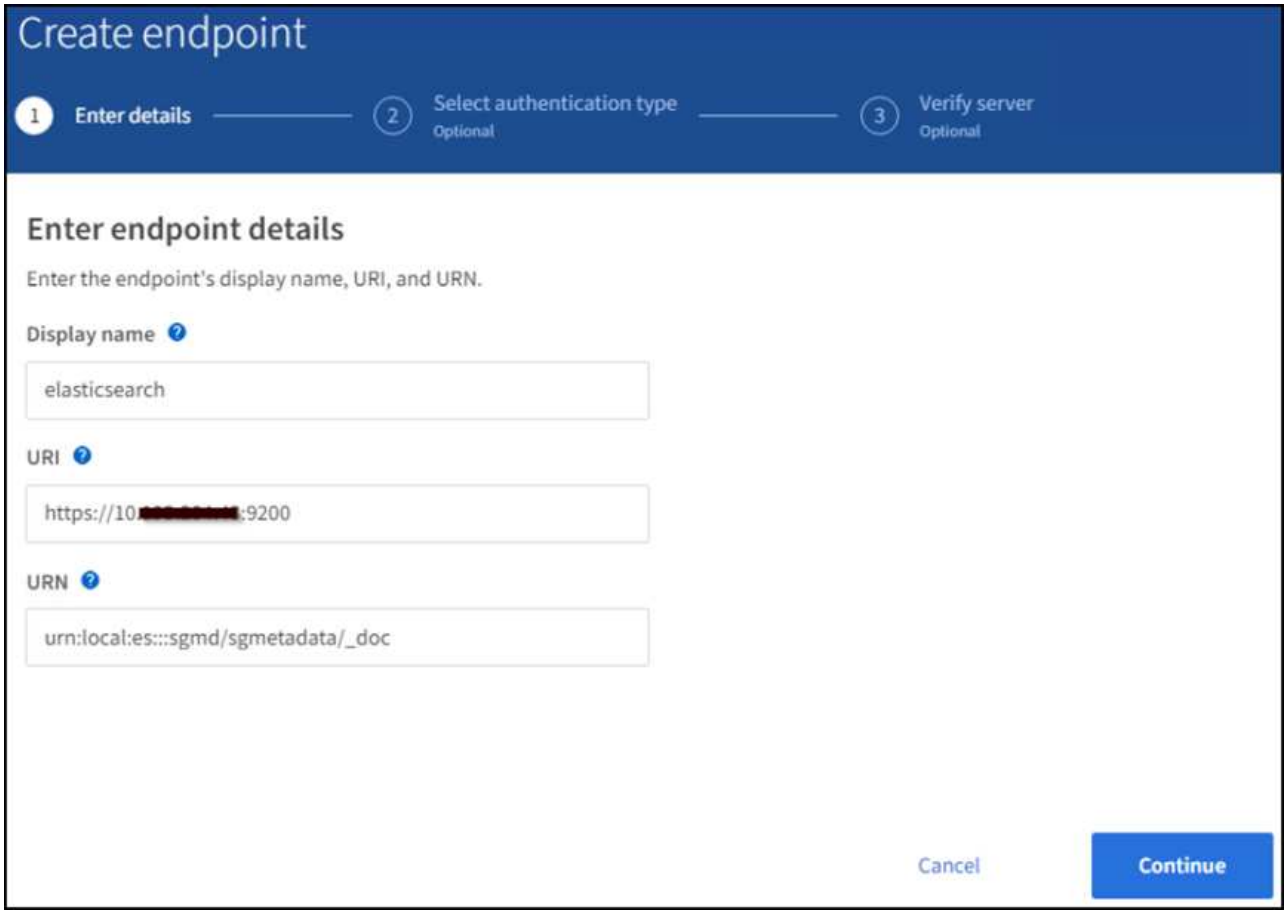
3. Después de que se haya iniciado el contenedor de Docker de Kibana, el enlace de URL `https://0.0.0.0:5601` aparecen en la consola. Reemplace 0.0.0.0 por la dirección IP del servidor en la dirección URL.
4. Inicie sesión en la interfaz de usuario de Kibana con el nombre de usuario `elastic` Y la contraseña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



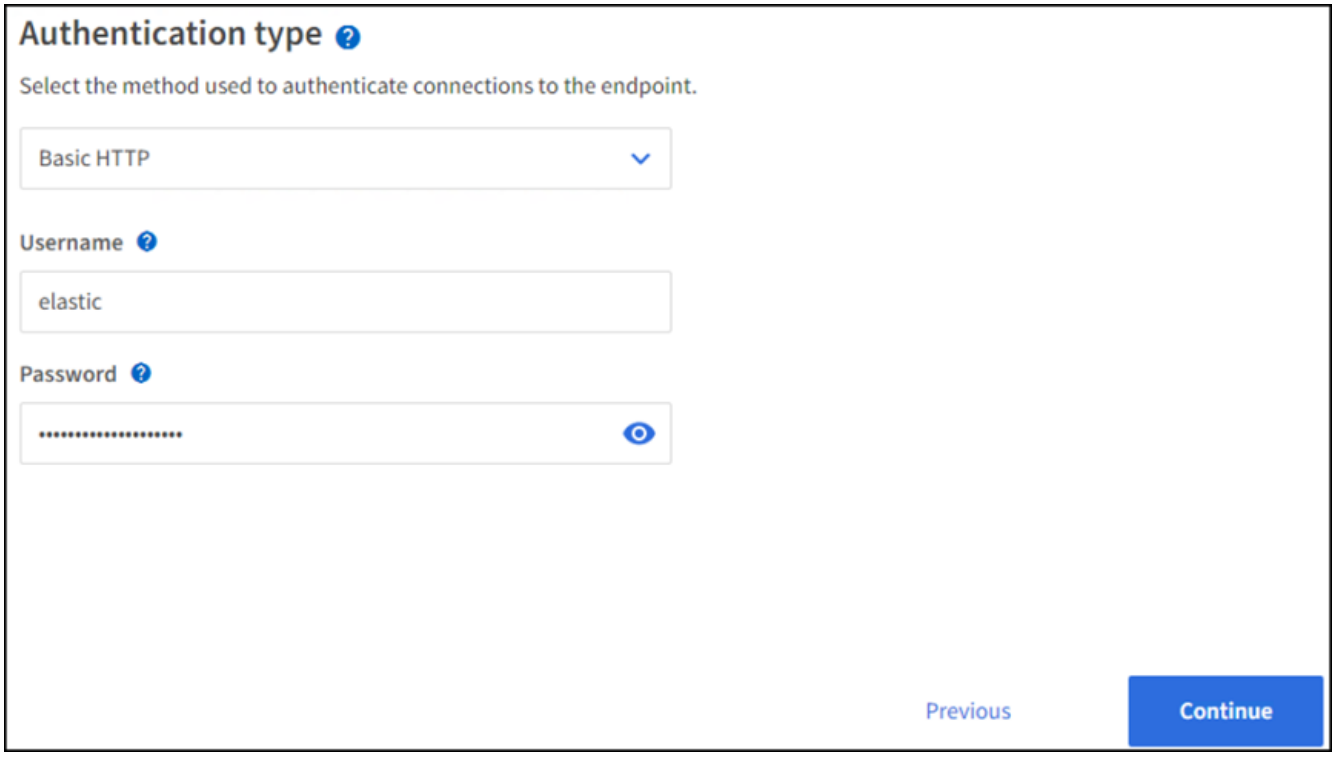
Configuración de extremos de servicios de plataforma

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

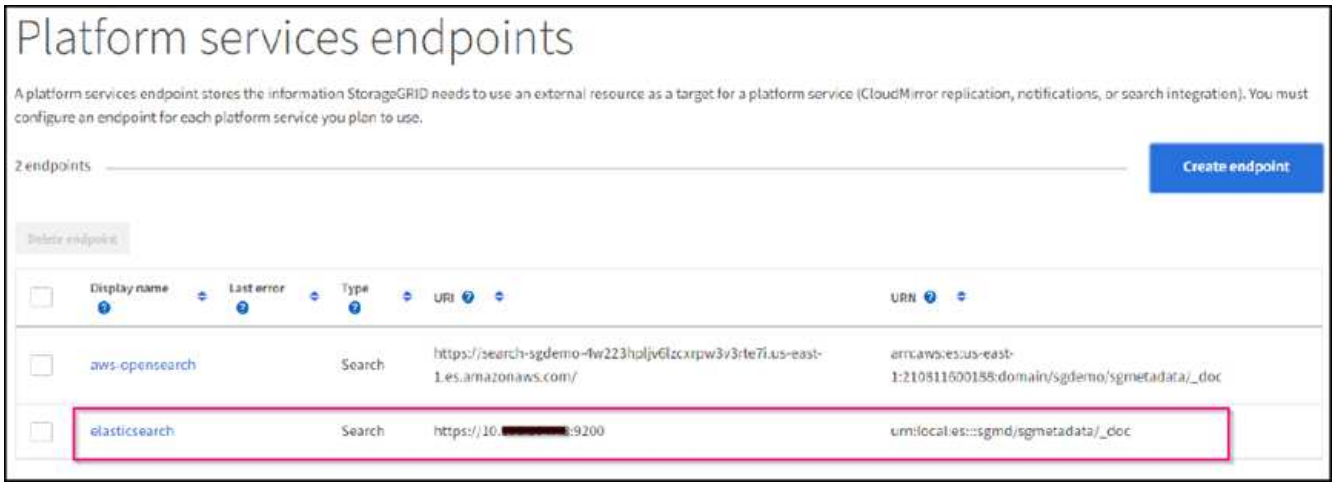
1. En el Administrador de inquilinos, vaya a ALMACENAMIENTO (S3) > extremos de servicios de la plataforma
2. Haga clic en Create Endpoint, introduzca lo siguiente y haga clic en Continue:
   - Ejemplo de nombre para mostrar: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`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



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



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



Configuración del servicio de integración de búsqueda de bloques

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

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

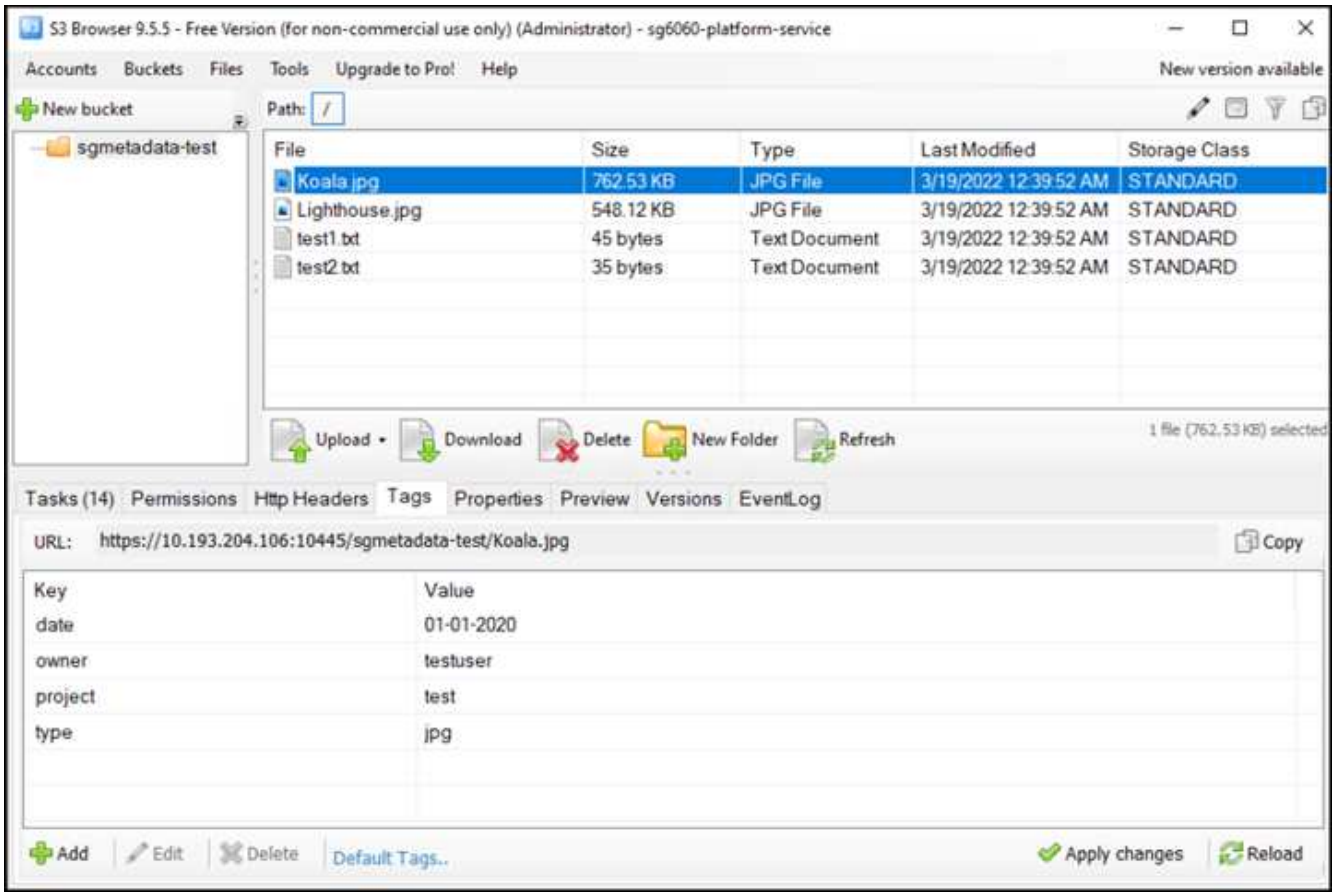
1. En el administrador de inquilinos, vaya a STORAGE(S3) > Buckets
2. Haga clic en Create Bucket, introduzca el nombre del bloque (por ejemplo, `sgmetadata-test`) y acepte el valor predeterminado `us-east-1` región.
3. Haga clic en Continue > Create Bucket.
4. Para abrir la página bucket Overview, haga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

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

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

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

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



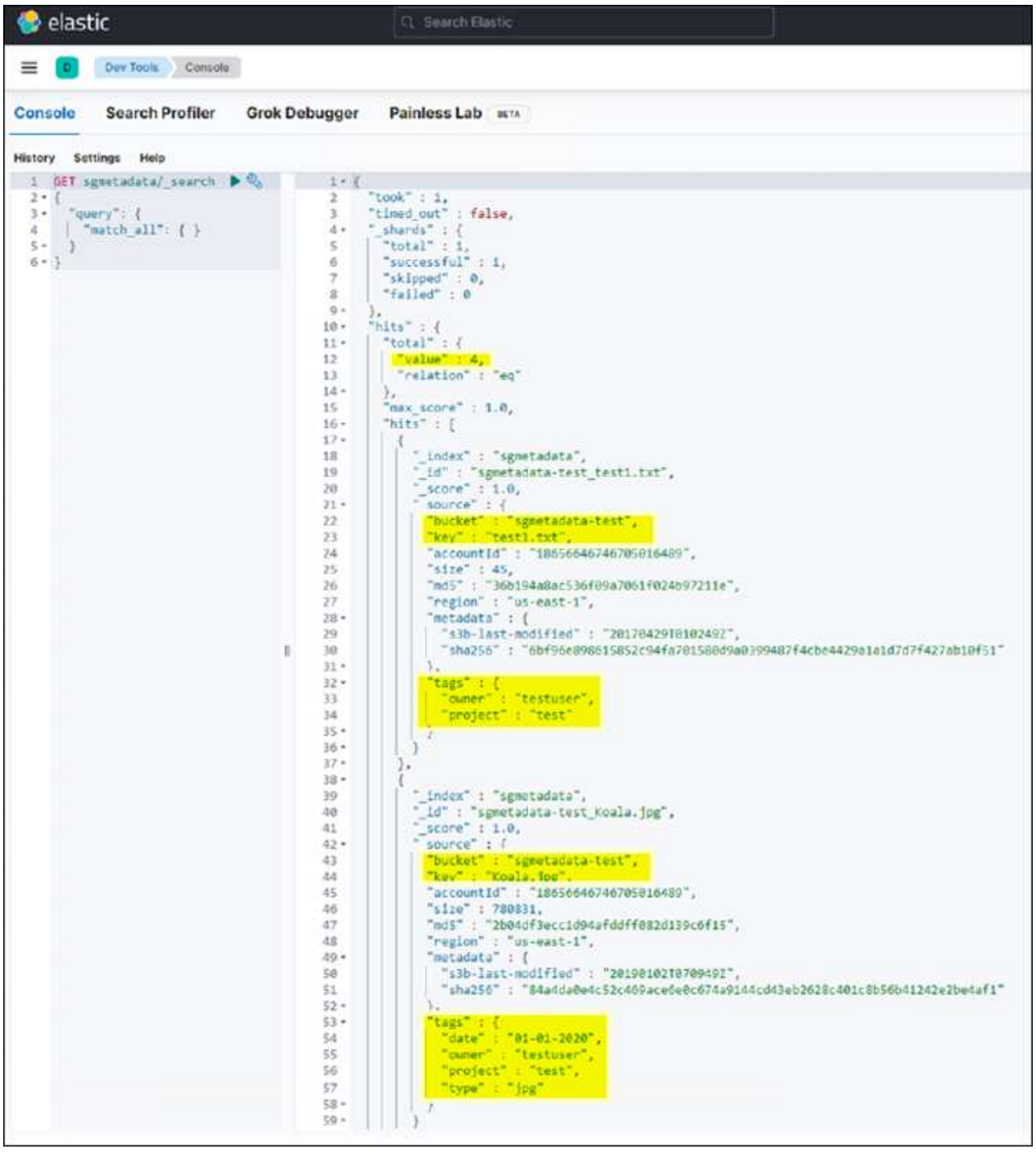
7. Utilice la interfaz de usuario de Kibana para verificar que los metadatos del objeto se cargaron en el índice de metadatos sg.

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

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

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

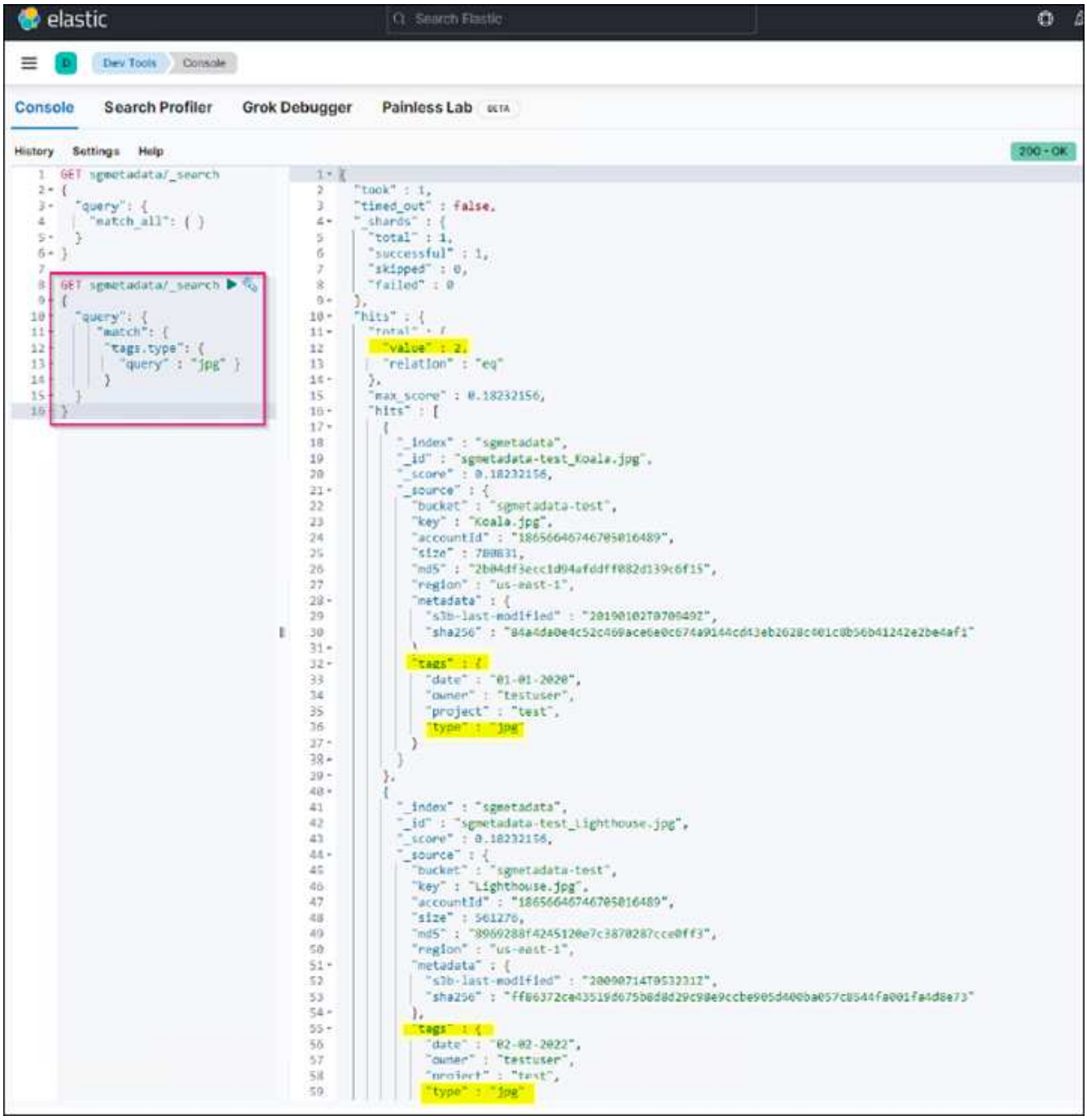
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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

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

+



Dónde encontrar información adicional

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

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

Por Angela Cheng

Clon de nodo

Consideraciones y rendimiento del clon de nodos.

Consideraciones sobre el clon de nodo

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

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

Estimaciones de rendimiento de clones de nodos

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

DDP8

SG5612 → cualquiera

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

SG5712 → any

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

SG5660 → SG5760

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	3 día	6 días	7 días	8.5 días	11.5 días	**13 días**
25 GB	3 día	6 días	7 días	8.5 días	11.5 días	**13 días**

SG5660 → SG6060

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

SG5760 → SG5760

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	3 día	6 días	7 días	8.5 días	11.5 días	**13 días**
25 GB	3 día	6 días	7 días	8.5 días	11.5 días	**13 días**

SG5760 → SG6060

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	2.5 día	4.5 días	5.5 días	6.5 días	9 días	10 días
25 GB	1.5 día	3 días	3.5 días	4.5 días	6 días	6.5 días

SG6060 → SG6060

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	2.5 día	4.5 días	5.5 días	6.5 días	8.5 días	9.5 días
25 GB	1.5 día	3 días	3.5 días	4 días	5.5 días	6 días

DDP16

SG5760 → SG5760

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	3.5 día	6.5 días	8 días	9.5 días	12.5 días	**14 días**
25 GB	3.5 día	6.5 días	8 días	9.5 días	12.5 días	**14 días**

SG5760 → SG6060

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
10 GB	2.5 día	5 días	6 días	7.5 días	10 días	11 días

Velocidad de la interfaz de red	Tamaño de unidad de 4 TB	Tamaño de unidad de 8 TB	Tamaño de unidad de 10 TB	Tamaño de disco de 12 TB	Tamaño de la unidad de 16 TB	Tamaño de unidad de 18 TB
25 GB	2 días	3.5 días	4 días	5 días	6.5 días	7 días

SG6060 → SG6060

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

Bandeja de expansión (a partir de SG6060 para cada bandeja en el dispositivo de origen)

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

Por Aron Klein

Cómo utilizar el remap de puertos

Es posible que tenga que reasignar un puerto entrante o saliente por varias razones. Puede que esté pasando del servicio de equilibrador de carga CLB heredado al extremo de equilibrador de carga de servicio nginx actual y mantener el mismo puerto para reducir el impacto en los clientes, que desee utilizar el puerto 443 para el cliente S3 en una red de cliente de nodo de administración o para restricciones de firewall.

Migre clientes S3 de CLB A NGINX con la asignación de puertos

En versiones anteriores a StorageGRID 11.3, el servicio de equilibrador de carga incluido en los nodos de puerta de enlace es el equilibrador de carga de conexión (CLB). En StorageGRID 11.3, NetApp presenta el servicio NGINX como una completa solución integrada para el tráfico HTTP(s) de equilibrio de carga. Puesto que el servicio CLB sigue disponible en la versión actual de StorageGRID, no puede reutilizar el puerto 8082 en la nueva configuración del extremo del equilibrador de carga. Para evitar esto, el puerto de entrada 8082 se reasigna a 10443. Esto hace que todas las solicitudes HTTPS lleguen al puerto 8082 en la redirección de la puerta de enlace al puerto 10443, pasando por alto el servicio CLB y en su lugar conectándose al servicio NGINX. Aunque las siguientes instrucciones están disponibles para VMware, la funcionalidad PORT_REMAPP existe para todos los métodos de instalación y puede utilizar un proceso similar para implementaciones sin configuración básica y dispositivos.

Puesta en marcha del nodo de puerta de enlace de máquinas virtuales de VMware

Los siguientes pasos son para una puesta en marcha de StorageGRID donde los nodos de puerta de enlace se ponen en marcha en VMware vSphere 7 como máquinas virtuales con el formato de virtualización abierta de StorageGRID (OVF). Este proceso implica la eliminación destructiva de la VM y la nueva puesta en marcha de la VM con el mismo nombre y configuración. Antes de encender la máquina virtual, cambie la propiedad VAPP para reasignar el puerto. A continuación, encienda la máquina virtual y siga el proceso de recuperación del nodo.

Requisitos previos

- Su sistema operativo es StorageGRID 11.3 o posterior
- Ha descargado y tiene acceso a los archivos de instalación de StorageGRID versión VMware instalados.
- Dispone de una cuenta de vCenter con permisos para encender y apagar equipos virtuales, cambiar la configuración de los equipos virtuales y vApps, eliminar equipos virtuales de vCenter y poner en marcha equipos virtuales por OVF.
- Ha creado un punto final de equilibrador de carga
  - El puerto está configurado para el puerto de redirección deseado
  - El certificado SSL de punto final es el mismo que el que se instala para el servicio CLB en el certificado de servidor certificados de configuración/certificados de servidor/extremos de servicio de API de almacenamiento de objetos o el cliente puede aceptar un cambio en el certificado.

> ⓘ
>
> ```
> If your existing certificate is self-signed, you cannot reuse it
> in the new endpoint. You must generate a new self-signed
> certificate when creating the endpoint and configure the clients
> to accept the new certificate.
> ```

Destruya el primer nodo de puerta de enlace

Para destruir el primer nodo de puerta de enlace, siga estos pasos:

1. Elija el nodo de puerta de enlace con el que empezar si la cuadrícula contiene más de uno.
2. Quite las IP de nodo de todas las entidades round-robin DNS o grupos de equilibradores de carga, si procede.
3. Espere a que caduque el tiempo de vida (TTL) y abra las sesiones.
4. Apague el nodo de máquina virtual.
5. Quite el nodo de máquina virtual del disco.

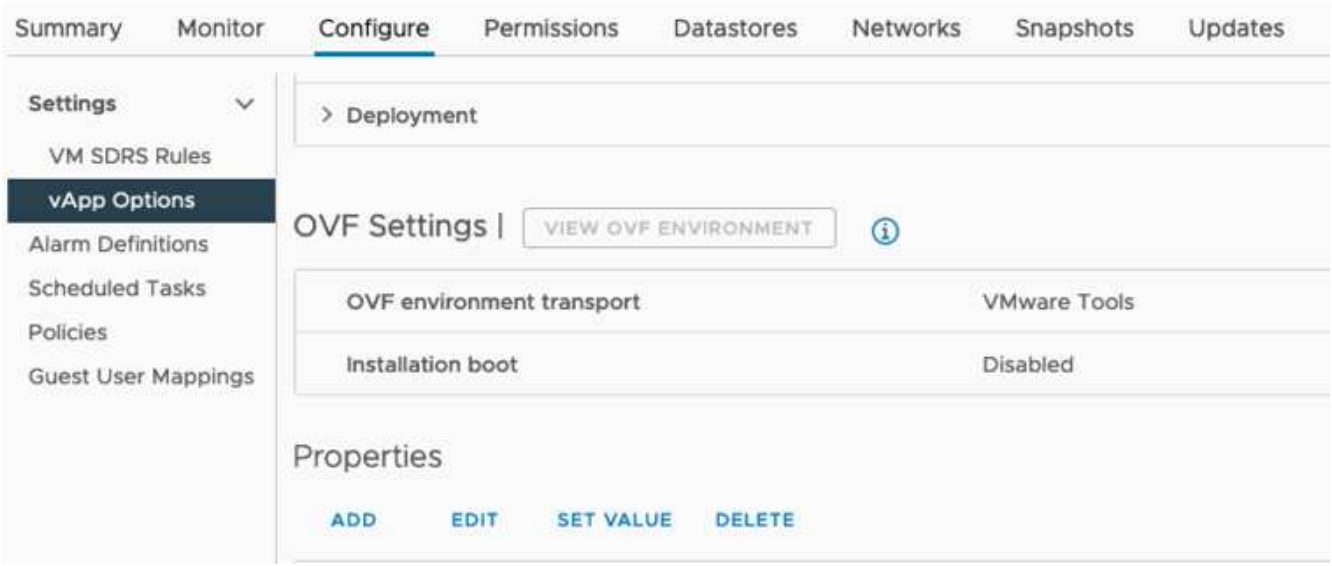
Implemente el nodo de puerta de enlace de reemplazo

Para implementar el nodo de puerta de enlace de repuesto, siga estos pasos:

1. Implemente el nuevo equipo virtual de OVF y seleccione los archivos .ovf, .mf y .vmdk en el paquete de instalación descargado del sitio de soporte:
   - vsphere-gateway.mf
   - vsphere-gateway.ovf

◦ NetApp-SG-11.4.0-20200721.1338.d3969b3.vmdk

2. Una vez implementado el equipo virtual, selecciónelo en la lista de equipos virtuales, seleccione la pestaña Configurar vApp Options.



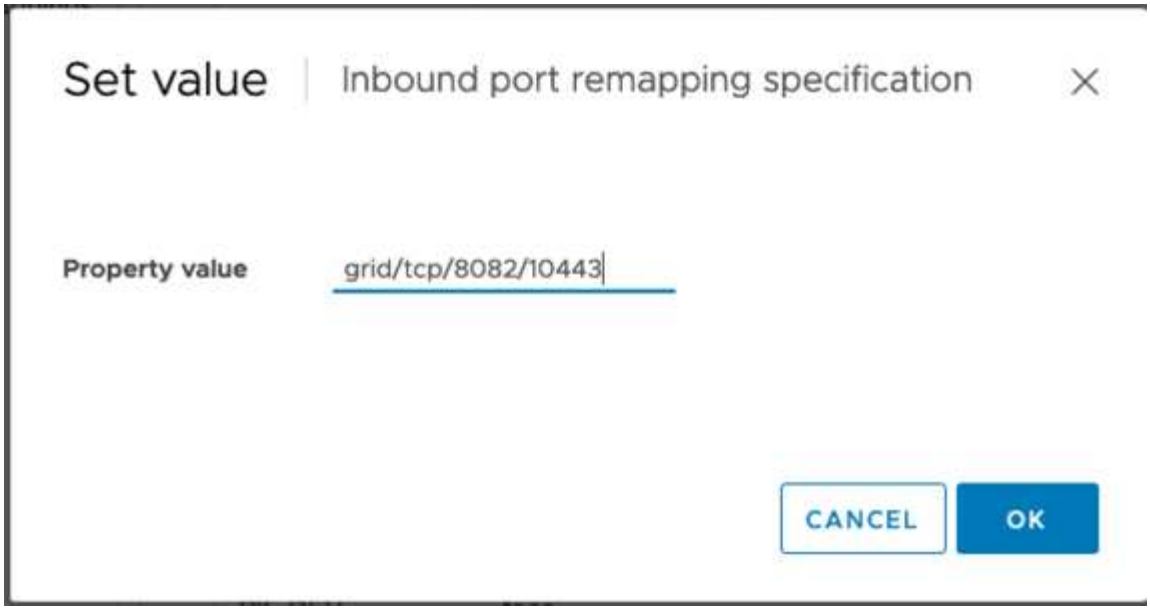
3. Desplácese hasta la sección Propiedades y seleccione LA propiedad PORT_REMAPP_INBOUND

4. Desplácese hasta la parte superior de la lista Propiedades y haga clic en Editar

5. Seleccione la ficha Tipo, confirme que la casilla de verificación configurable por el usuario está seleccionada y, a continuación, haga clic en Guardar.

6. En la parte superior de la lista Propiedades, con la propiedad “PORT_REMAPP_INBOUND” aún seleccionada, haga clic en establecer valor.

7. En el campo valor de propiedad, introduzca la red (grid, administrador o cliente), TCP, el puerto original (8082) y el puerto nuevo (10443) con “/” entre cada valor, como se describe a continuación.

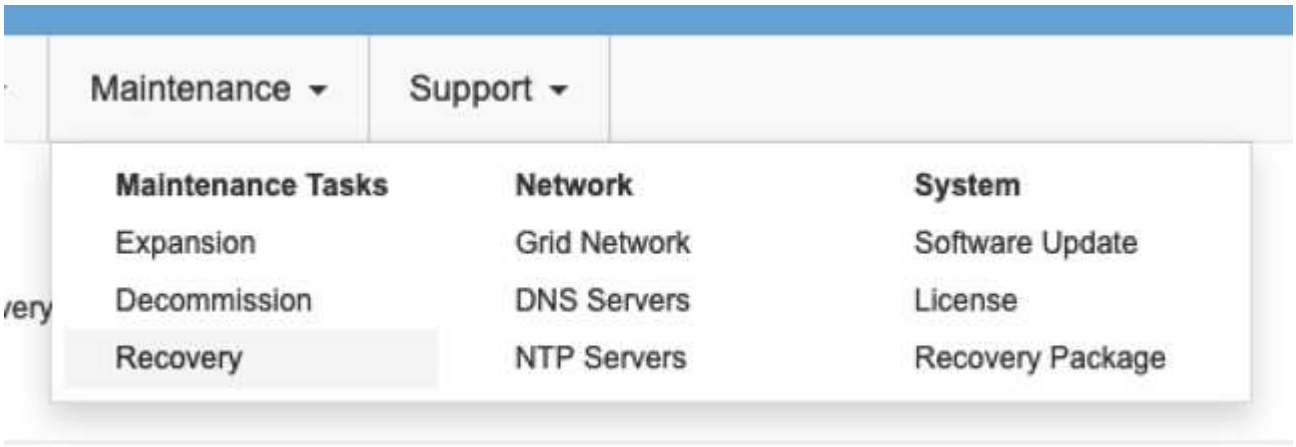


8. Si utiliza varias redes, utilice una coma (,) para separar las cadenas de red, por ejemplo, grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

Recupere el nodo de puerta de enlace

Para recuperar el nodo Gateway, siga estos pasos:

1. Desplácese hasta la sección Mantenimiento/recuperación de la IU de gestión de grid.



2. Encienda el nodo de la máquina virtual y espere a que el nodo aparezca en la sección Maintenance/Recovery Pending Nodes de la interfaz de usuario de Grid Management.

> For information and directions for node recovery, see the https://docs.netapp.com/sgws-114/topic/com.netapp.doc.sg-maint/GUID-7E22B1B9-4169-4800-8727-75F25FC0FFB1.html[Recovery and Maintenance guide]

3. Una vez recuperado el nodo, el IP se puede incluir en todas las entidades round-robin DNS o en los grupos de equilibradores de carga, si procede.

   Ahora, cualquier sesión HTTPS en el puerto 8082 va al puerto 10443

Reasignar el puerto 443 para acceder S3 de cliente en un nodo de administración

La configuración predeterminada del sistema StorageGRID para un nodo de administración o un grupo de alta disponibilidad que contiene un nodo de administración es para que los puertos 443 y 80 se reserven para la interfaz de usuario del administrador de inquilinos y de gestión, y no se puede utilizar para extremos de equilibrio de carga. La solución a esto consiste en utilizar la operación de reasignación de puertos y redirigir el puerto de entrada 443 a un nuevo puerto que se configurará como punto final de equilibrio de carga. Una vez completado este tráfico de Client S3 podrá usar el puerto 443, la IU de administración de grid solo estará accesible a través del puerto 8443 y la IU de gestión de inquilinos solo estará accesible en el puerto 9443. La característica de reasignar puerto solo se puede configurar en el momento de instalación del nodo. Para implementar un remasterp de puertos de un nodo activo en la cuadrícula, se debe restablecer al estado preinstalado. Este es un procedimiento destructivo que incluye una recuperación de nodos una vez que se ha realizado el cambio de configuración.

Registros de backup y bases de datos

Los nodos de administración contienen registros de auditoría, métricas prometheus, así como información histórica sobre atributos, alarmas y alertas. Si tiene varios nodos de administrador, tendrá varias copias de estos datos. Si no tiene varios nodos de administrador en el grid, debe asegurarse de conservar estos datos para restaurar una vez que se haya recuperado el nodo al final de este proceso. Si tiene otro nodo de administrador en la cuadrícula, puede copiar los datos de ese nodo durante el proceso de recuperación. Si no tiene otro nodo de administrador en la cuadrícula, puede seguir estas instrucciones para copiar los datos antes de destruir el nodo.

Copiar registros de auditoría

1. Inicie sesión en el nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`

f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula independiente y permita utilizar *Storage_node_01*:

a. `ssh admin@storage_node_01_IP`

b. `mkdir -p /var/local/tmp/saved-audit-logs`

3. De nuevo en el nodo de administración, detenga el servicio AMS para evitar que cree un nuevo archivo de registro: `service ams stop`

4. Cambie el nombre del archivo audit.log para que no sobrescriba el archivo existente al copiarlo al nodo de administración recuperado.

a. Cambie el nombre de audit.log por un nombre de archivo numerado único como aaaa-mm-dd.txt.1. Por ejemplo, es posible cambiar el nombre del archivo de registro de auditoría a 2015-10-25.txt.1

```
cd /var/local/audit/export
ls -l
mv audit.log 2015-10-25.txt.1
```

5. Reinicie el servicio AMS: `service ams start`

6. Copie todos los archivos del registro de auditoría: `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

Copiar datos Prometheus

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración.

1. Cree el directorio para copiar los datos prometheus a una ubicación temporal en un nodo de cuadrícula independiente. De nuevo, utilizaremos *Storage_node_01*:

a. Inicie sesión en el nodo de almacenamiento:

i. Introduzca el siguiente comando: `ssh admin@storage_node_01_IP`

ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

iii. mkdir -p /var/local/tmp/prometheus'

2. Inicie sesión en el nodo de administrador:

a. Introduzca el siguiente comando: `ssh admin@admin_node_IP`

b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`

f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

3. En el nodo de administración, detenga el servicio Prometheus: `service prometheus stop`

   a. Copie la base de datos Prometheus del nodo de administración de origen en el nodo de ubicación del backup del nodo de almacenamiento: `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" " storage_node_01_IP:/var/local/tmp/prometheus/"`

4. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`

Información histórica de la copia de seguridad

La información histórica se almacena en una base de datos mysql. Para volcar una copia de la base de datos, necesitará el usuario y la contraseña de NetApp. Si posee otro nodo de administrador en la cuadrícula, este paso no es necesario y la base de datos se puede clonar a partir de un nodo de administrador restante durante el proceso de recuperación.

1. Inicie sesión en el nodo de administrador:

   a. Introduzca el siguiente comando: `ssh admin@admin_node_IP`

   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`

   f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Detenga los servicios de StorageGRID en el nodo de administración e inicie ntp y mysql

   a. Detenga todos los servicios: `service servermanager stop`

   b. reinicie el servicio ntp: `service ntp start`..restart mysql servicio: `service mysql start`

3. Volcar mi base de datos a /var/local/tmp

   a. introduzca el siguiente comando: `mysqldump –u username –p password mi > /var/local/tmp/mysql-mi.sql`

4. Copie el archivo de volcado mysql en un nodo alternativo, usaremos *Storage_node_01: scp /var/local/tmp/mysql-mi.sql _storage_node_01_IP:/var/local/tmp/mysql-mi.sql*

a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca: `ssh-add -D`

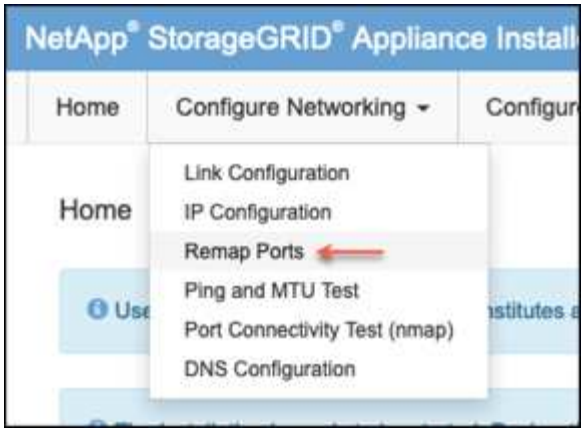
Vuelva a crear el nodo Admin

Ahora que dispone de una copia de backup de todos los datos y registros deseados en otro nodo de administrador de la cuadrícula o almacenados en una ubicación temporal, es hora de restablecer el dispositivo para poder configurar el remapa de puertos.

1. El restablecimiento de un dispositivo vuelve al estado preinstalado y solo conserva el nombre de host, las IP y las configuraciones de red. Se perderán todos los datos, por lo que nos aseguramos de contar con una copia de seguridad de cualquier información importante.
   a. introduzca el siguiente comando: `sgareinstall`

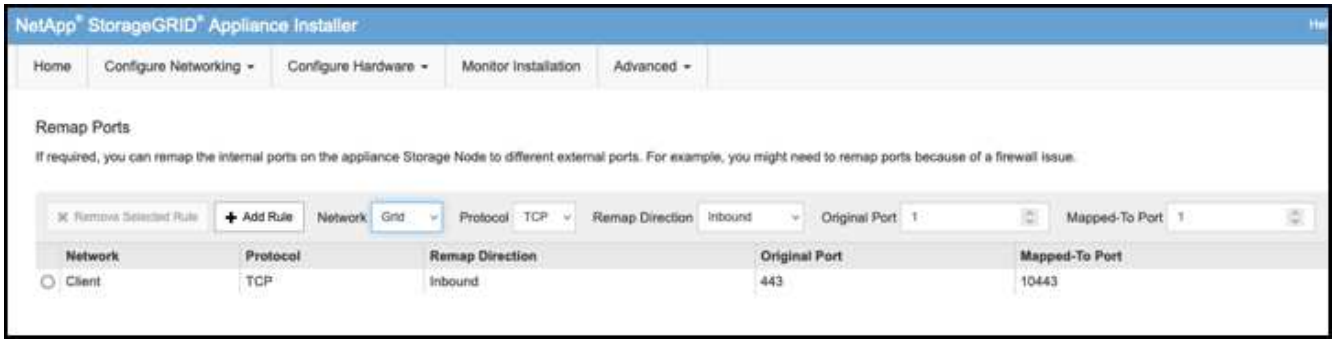
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

After running this command and waiting a few minutes for the node to
reboot,
browse to one of the following URLs to reinstall StorageGRID Webscale
on
this node:

    https://10.193.174.192:8443
    https://10.193.204.192:8443
    https://169.254.0.1:8443

Are you sure you want to continue (y/n)? y
Renaming SG installation flag file.
Initiating a reboot to trigger the StorageGRID Webscale appliance
installation wizard.
```

2. Cuando haya transcurrido un periodo de tiempo, el dispositivo se reiniciará y podrá acceder a la IU del nodo PGE.
3. Vaya a Configurar redes



4. Seleccione la red, el protocolo, la dirección y los puertos deseados y, a continuación, haga clic en el botón Agregar regla.

> La reasignación del puerto de entrada 443 en LA red DE CUADRÍCULA interrumpirá la instalación y los procedimientos de expansión. No se recomienda reasignar el puerto 443 en la red DE RED.



5. Una de las reasignaciones de puerto deseadas se ha agregado, puede volver a la ficha de inicio y hacer clic en el botón Iniciar instalación.

Ahora puede seguir los procedimientos de recuperación del nodo de administrador en el "documentación de productos"

Restaurar bases de datos y registros

Ahora que el nodo de administrador se ha recuperado, podrá restaurar las métricas, los registros y la información histórica. Si tiene otro nodo de administrador en la cuadrícula, siga la "documentación de productos" utilizando los scripts *prometheus-clone-db.sh* y *mi-clone-db.sh*. Si este es el único nodo de administrador y decide realizar una copia de seguridad de estos datos, puede seguir los pasos que se indican a continuación para restaurar la información.

Vuelva a copiar los registros de auditoría

1. Inicie sesión en el nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`

f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. Copie los archivos de registro de auditoría conservados en el nodo admin recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. Por motivos de seguridad, elimine los registros de auditoría del nodo de grid con errores después de verificar que se han copiado correctamente al nodo de administrador recuperado.
4. Actualice la configuración de usuario y grupo de los archivos de registro de auditoría en el nodo de administración recuperado: `chown ams-user:bycast *`

También debe restaurar cualquier acceso de cliente preexistente al recurso compartido de auditoría. Para obtener más información, consulte las instrucciones para administrar StorageGRID.

Restaurar métricas de Prometheus

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración.

1. Inicie sesión en el nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`
   f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

```
When you are logged in as root, the prompt changes from `$` to `#`.
```

2. En el nodo de administración, detenga el servicio Prometheus: `service prometheus stop`
   a. Copie la base de datos Prometheus de la ubicación temporal del backup al nodo de administración: `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. compruebe que los datos están en la ruta correcta y que han finalizado `ls /var/local/mysql_ibdata/prometheus/data/`
3. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`

Restaurar información histórica

1. Inicie sesión en el nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`
   f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

   ```
   When you are logged in as root, the prompt changes from `$` to `#`.
   ```

2. Copie el archivo de volcado mysql del nodo alternativo: `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. Detenga los servicios de StorageGRID en el nodo de administración e inicie ntp y mysql
   a. Detenga todos los servicios: `service servermanager stop`
   b. reinicie el servicio ntp: `service ntp start`..restart mysql servicio: `service mysql start`
4. Borre la base de datos mi y cree una nueva base de datos vacía: `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. restaure la base de datos mysql desde el volcado de la base de datos: `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. Reinicie todos los demás servicios `service servermanager start`

Por Aron Klein

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

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

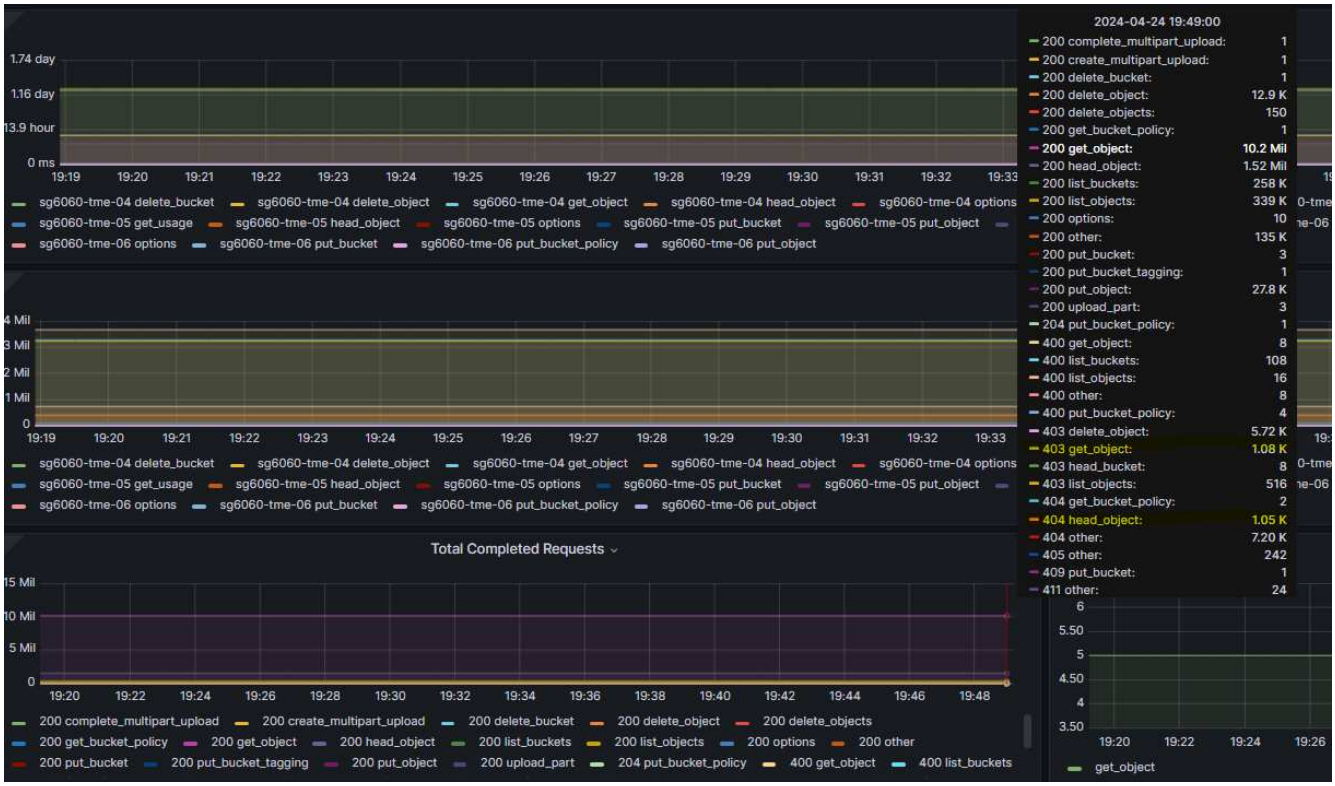
Si necesita cambiar la red de Grid de toda la Grid, consulte "Cambie las direcciones IP para todos los nodos de la cuadrícula".

Consideraciones antes de la reubicación del sitio

- El movimiento del sitio debe completarse y todos los nodos en línea en 15 días para evitar la reconstrucción de la base de datos Cassandra.
  "Recupere el nodo de almacenamiento en más de 15 días"
- Si alguna regla de ILM en una política activa utiliza un comportamiento de ingesta estricto, considere cambiarla al equilibrio o a la confirmación doble si el cliente desea seguir PONIENDO objetos en el Grid

durante la reubicación del sitio.

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



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

Pasos

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

```
Editing: Node IP/subnet and gateway

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

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

b. seleccione 5 para mostrar los cambios

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

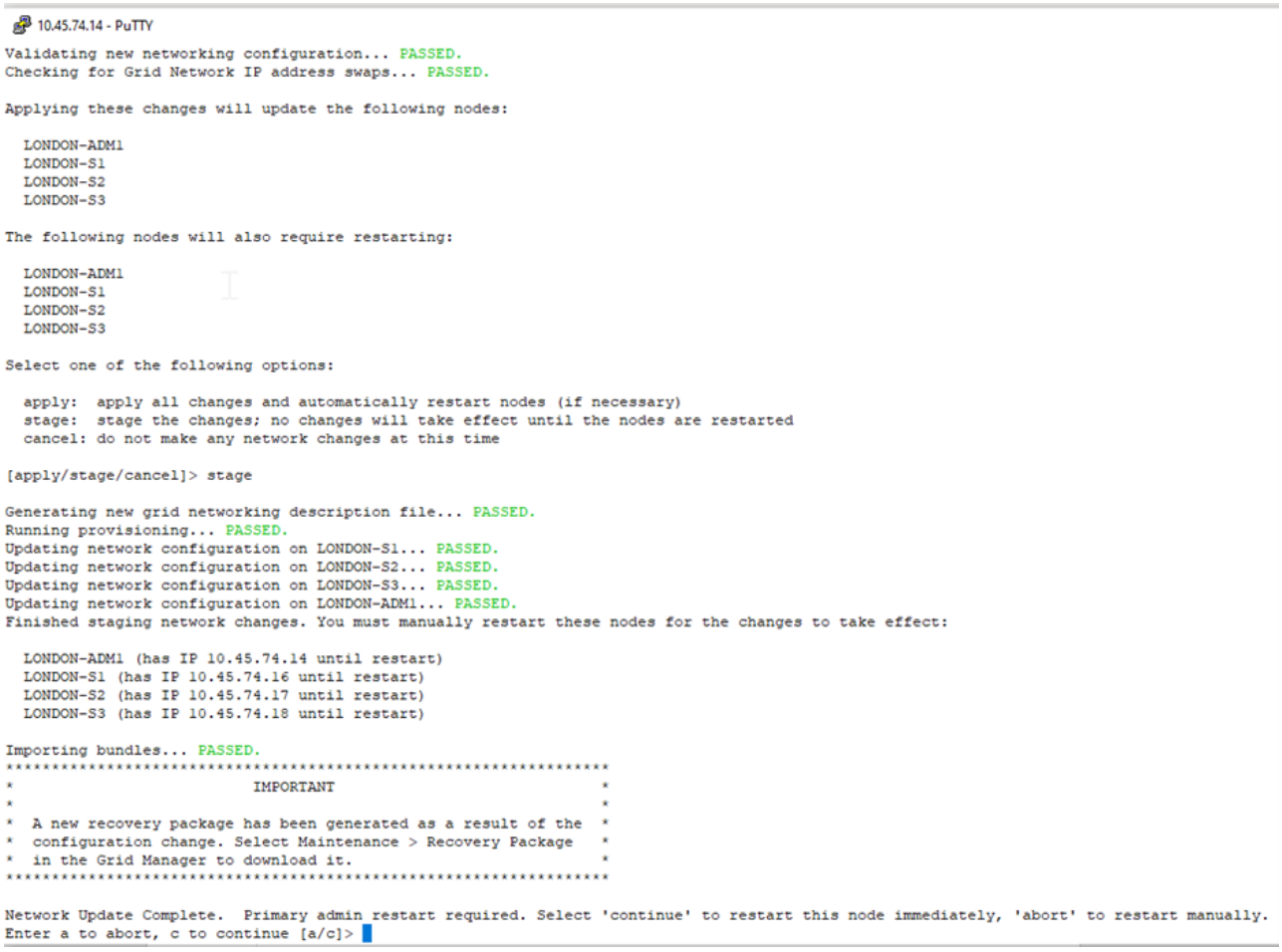
c. seleccione 10 para validar y aplicar el cambio.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask and gateway
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection: 10
```

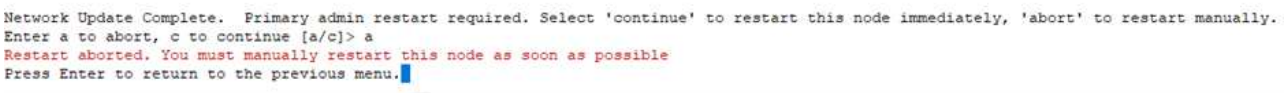
d. Debe seleccionar **stage** en este paso.

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

Applying these changes will update the following nodes:

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

The following nodes will also require restarting:

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

Select one of the following options:

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

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

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



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



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

Cambio de VLAN del dispositivo

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

Pasos

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

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