StorageGRID® Webscale 11.0

Guía del Administrador del tenant

Octubre 2017 | 215-12403_A0
doccomments@netapp.com

NetApp®

Índice

Cómo administrar una cuenta tenant de StorageGRID Webscale

5

Como administrador de una cuenta tenant de StorageGRID Webscale, puede usar la Interfaz de Administración del tenant para supervisar la cantidad de almacenamiento que consume la cuenta tenant y puede administrar el control de acceso configurando grupos y usuarios.

La Guía del Administrador del tenant de StorageGRID Webscale contiene información e instrucciones para configurar, administrar y supervisar día a día una cuenta tenant de StorageGRID Webscale. Esta guía incluye instrucciones para habilitar los servicios de la plataforma, así como información sobre la configuración de las opciones del bucket para los niveles de coherencia y las últimas actualizaciones de acceso. La guía también incluye instrucciones para configurar grupos y usuarios de tipo tenant.

La Guía del Administrador del tenant no proporciona información sobre cómo utilizar el resto del sistema de StorageGRID Webscale y su área funcional. Para obtener información adicional consulte las siguientes publicaciones:

- Manual básico de la Malla, que proporciona una introducción general a StorageGRID Webscale
- Guía del Administrador, que proporciona instrucciones y explicaciones detalladas para utilizar la Interfaz de gestión para administrar todo el sistema StorageGRID Webscale
- Guía de Implementación de S3 (Servicio Simple de Almacenamiento), que proporciona instrucciones para el empleo del protocolo del cliente S3, con StorageGRID Webscale
- Guía de implementación de Swift, que proporciona instrucciones para utilizar el protocolo del cliente Swift con StorageGRID Webscale

Información relacionada

Manual básico de la Malla de StorageGRID Webscale 11.0
Guía del administrador de StorageGRID Webscale 11.0
Guía de implementación de StorageGRID Webscale 11.0 de S3 (Servicio Simple de Almacenamiento)
Guía de implementación de Swift de StorageGRID Webscale 11.0

Qué son las cuentas tenant

Una cuenta tenant permite a los clientes que usan el protocolo del Servicio Simple de Almacenamiento (S3), o el protocolo Swift, almacenar y recuperar objetos en un sistema StorageGRID Webscale.

Cada cuenta tenant admite el uso de un único protocolo, que debe especificar el administrador de la malla en el momento en que crea la cuenta. Para almacenar y recuperar objetos en un sistema StorageGRID Webscale con ambos protocolos, se requieren dos cuentas tenant: una para contenedores y objetos Swift y otra para buckets y objetos S3. Cada cuenta tenant dispone de su propia identificación, Interfaz de Administración, grupos y usuarios federados o locales, y contenedores (buckets para S3) y objetos.

Opcionalmente, puede optar por tener diferentes cuentas tenant en un sistema StorageGRID Webscale para segregar objetos almacenados por diferentes entidades. Por ejemplo, un sistema StorageGRID Webscale puede emplear varias cuentas tenant en cualquiera de estos casos de uso:

- **Casos de uso empresarial:** Si el sistema StorageGRID Webscale se utiliza en una empresa, el almacenamiento de objetos de la malla podría estar segregado en los diferentes departamentos de la organización. Por ejemplo, puede haber cuentas tenant para el departamento de Marketing, el departamento de Atención al Cliente, el departamento de Recursos Humanos, y así sucesivamente.

  Nota: Al utilizar cuentas tenant se garantiza que los tenants no podrán acceder a los datos de los demás. Sin embargo, si usa el protocolo cliente de S3, puede simplemente usar buckets de S3 y políticas de bucket para segregar objetos entre los departamentos de una empresa. No necesita usar cuentas tenant. Consulte la Guía de implementación del S3 (Servicio Simple de Almacenamiento) para obtener más información.

- **Caso de uso del proveedor de servicios:** Si un proveedor de servicios utiliza el sistema StorageGRID Webscale, el almacenamiento de objetos de la malla podría estar segregado entre las diferentes entidades que alquilan el almacenamiento. Por ejemplo, puede haber cuentas tenant para la empresa A, la empresa B, la empresa C, y así sucesivamente.

El administrador de malla de StorageGRID Webscale crea las cuentas tenant de almacenamiento utilizando la Interfaz de gestión (ya sea la interfaz de usuario o la API). Al crear una cuenta tenant, el administrador de la malla especifica la siguiente información:

- Nombre a mostrar para la cuenta tenant (la identificación de la cuenta tenant se asigna automáticamente y no se puede cambiar)
- El protocolo de cliente que utilizará la cuenta tenant (S3 o Swift)?
- Si una cuenta tenant tiene permiso para usar los servicios de la plataforma con buckets de S3
- Contraseña inicial para el usuario raíz de la cuenta tenant
- Si la cuenta tenant usará el origen de identidad que se configuró para la malla o su propio origen de identidad para la federación de identidades
- Opcionalmente, una cuota de almacenamiento para la cuenta tenant: el número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del tenant.

Tan pronto como se haya creado la cuenta tenant, puede iniciar sesión en la Interfaz de Administración del tenant para supervisar el uso del almacenamiento y configurar la federación de identidad, los grupos y los usuarios. Una vez configurados los usuarios, los usuarios del cliente S3 también utilizarán la Interfaz de Administración del tenant para crear y administrar las claves de acceso necesarias para almacenar y recuperar objetos en el sistema StorageGRID Webscale.

Esta guía proporciona instrucciones para el empleo de la interfaz de Administración del tenant. Si desea obtener más información sobre cómo crear cuentas tenant para almacenamiento, consulte la

Conceptos relacionados

Qué son los servicios de plataforma en la página 42

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)
Guía del administrador de StorageGRID Webscale 11.0

Empleo de la Interfaz de Administración del tenant

La Interfaz de Administración del tenant le permite administrar todos los aspectos de su cuenta tenant.

Puede utilizar la Interfaz de Administración del tenant para supervisar el empleo de almacenamiento y administrar cuentas de usuario con federación de identidad o crear grupos y usuarios locales. Para las cuentas tenant de S3, también puede configurar servicios de plataforma u otras opciones de los buckets de S3, y administrar claves de S3.

Requisitos de los exploradores Web

Debe utilizar un explorador web compatible.

Explorador web	Versión mínima compatible
Google Chrome	54
Microsoft Internet Explorer	11 (Modo Nativo)
Mozilla Firefox	50

Debe ajustar la ventana del explorador a un ancho recomendado.

Anchura del explorador	Píxeles
Mínimo	1024
Óptimo	1280

Inicio de sesión por primera vez

Cuando inicie sesión por primera vez en la interfaz de Administración de tenants de StorageGRID Webscale, iniciará sesión como el usuario raíz del tenant o como otro usuario del tenant creado por el administrador de la malla.

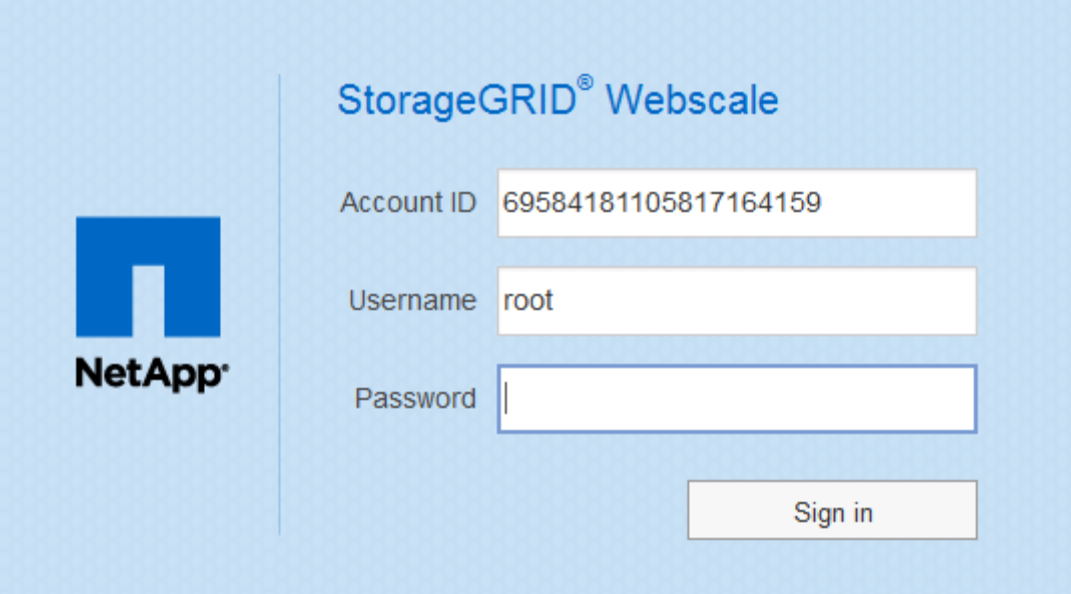
Antes de comenzar

- Debe conocer la contraseña asociada con el usuario tenant.
- Debe utilizar un explorador web compatible.

Pasos

1. Acceda a la URL de su cuenta tenant.

   Los administradores de la malla que conocen la contraseña del usuario raíz de la cuenta tenant también pueden iniciar sesión usando el enlace **Sign In** del tenant desde la Interfaz de gestión. Aparecerá la página Sign in con el campo **Account ID** (ID de la cuenta) completado.



2. Escriba el nombre de usuario en el campo **Username**.

   Por ejemplo, si está iniciando sesión como usuario raíz, escriba “root”.

3. Escriba la contraseña del usuario en el campo **Password** y haga clic en **Sign in**.

   Aparece la Interfaz de Administración del tenant. Habrá iniciado sesión.

4. Si inició sesión como usuario raíz y recibió la contraseña de alguien de otra compañía, por ejemplo de un proveedor de servicios, piense en cambiar la contraseña para garantizar su seguridad.

Tareas relacionadas

Cómo cambiar la contraseña de un usuario local en la página 30

Referencias relacionadas

Requisitos de los exploradores Web en la página 8

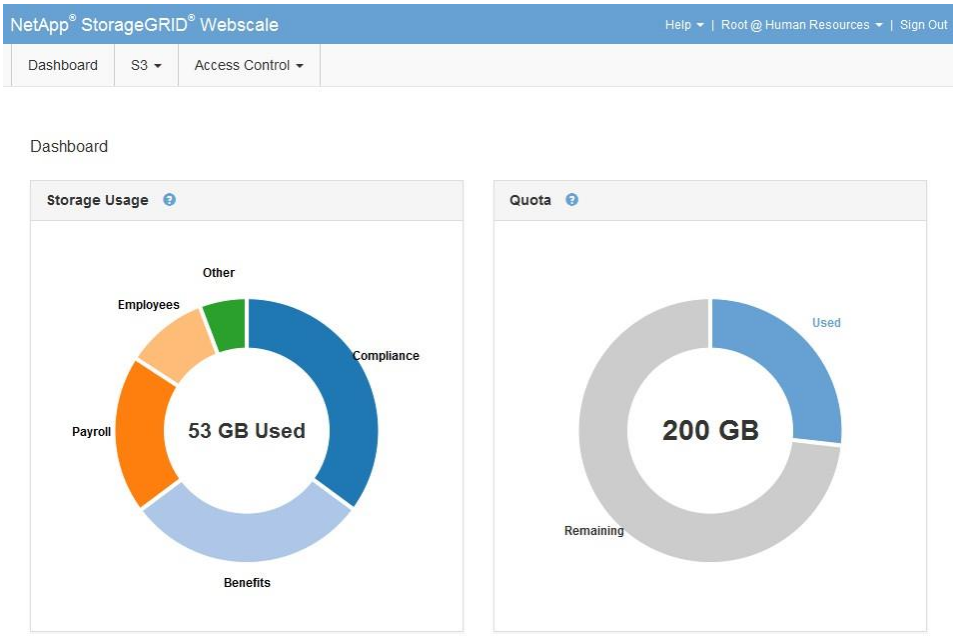
Qué es el Panel

Cuando se registra por primera vez en la Interfaz de administración de tenant, el Panel muestra cuánto espacio de almacenamiento está usando la cuenta tenant.

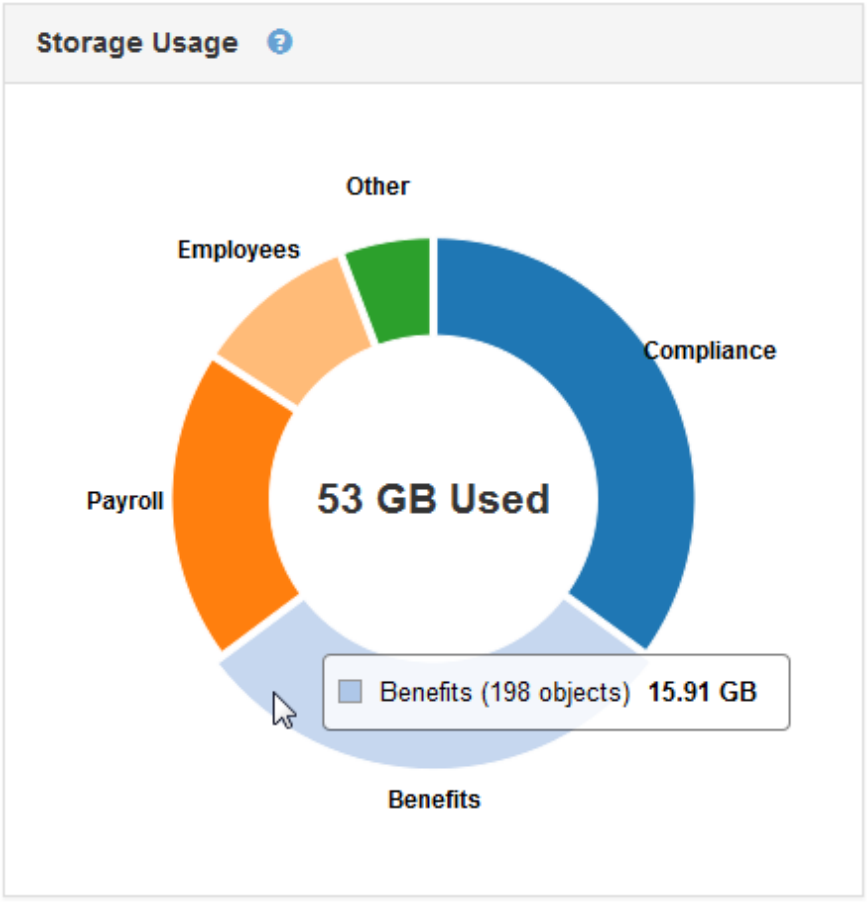
El Panel incluye dos partes:

- Storage Usage (Uso de almacenamiento): este panel muestra qué contenedores (buckets para S3) están consumiendo la mayor cantidad de almacenamiento. Se pueden mostrar hasta ocho contenedores. El segmento Other (otros) combina todos los demás contenedores, incluidos los contenedores que consumen menos del 1% del almacenamiento total.
- Cuota: si se especificó el número máximo de gigabytes, terabytes o petabytes disponibles para el tenant cuando se creó la cuenta, este panel muestra qué cantidad de esa cuota se ha utilizado y cuánta queda disponible. Si no se definió una cuota, el tenant tiene una cuota ilimitada y se muestra un mensaje informativo.

  Nota: Si la cuota se supera, la cuenta tenant no puede crear nuevos objetos.



Puede colocar el cursor sobre cualquiera de los segmentos del gráfico para obtener más información, incluida la cantidad de objetos almacenados y el total de bytes asignado a cada contenedor o bucket.



Qué se entiende por una API de Administración del tenant

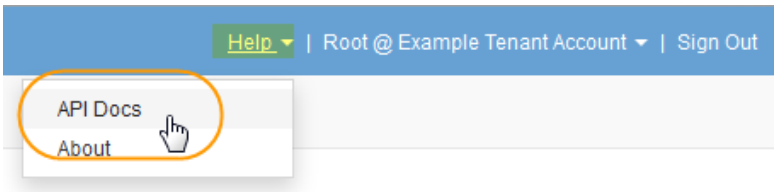
StorageGRID Webscale proporciona una API REST para administrar la cuenta tenant.

Documentación de la API de Administración del tenant

La API de Administración del tenant usa la plataforma API de código abierto, denominada Swagger, para proporcionar la documentación de la API. Swagger permite a los desarrolladores y no desarrolladores interactuar con la API mediante una interfaz de usuario que ilustra cómo la API responde a los parámetros y opciones. Esta documentación presupone que está familiarizado con las tecnologías web estándar y el formato de datos JSON (JavaScript Object Notation, Notación de Objetos de JavaScript).

> **Atención:** cualquier operación de API que realice utilizando la interfaz de usuario de Swagger es una operación dinámica. Tenga cuidado de no crear, actualizar o eliminar la configuración u otros datos por error.

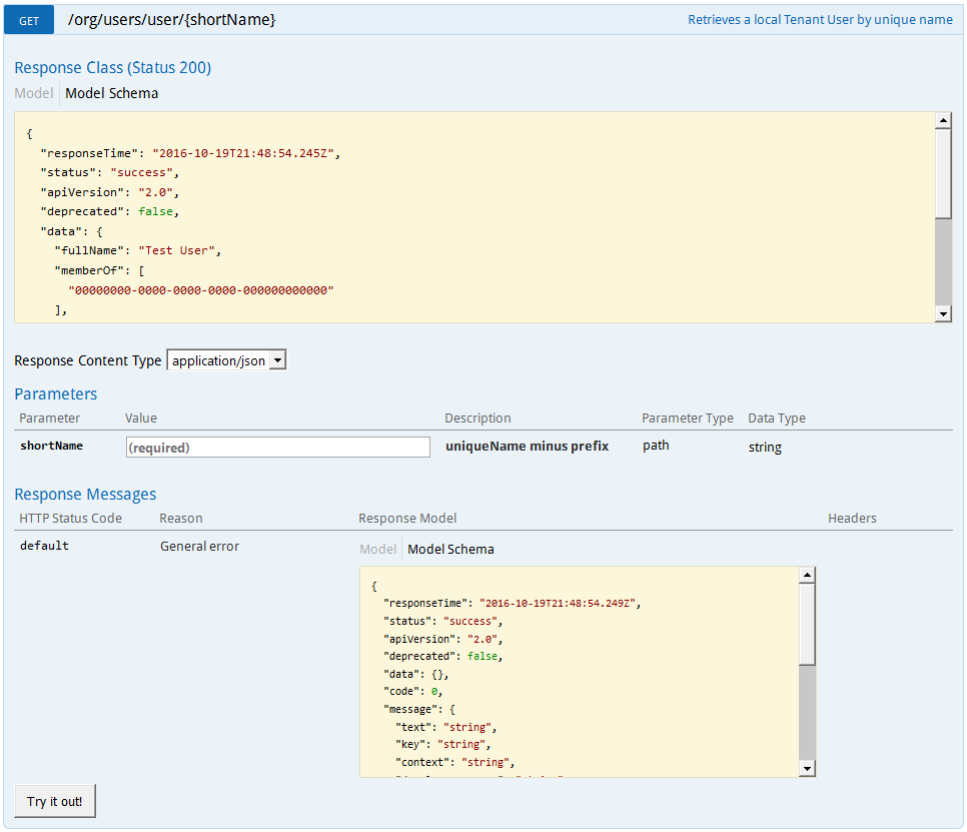
Podrá acceder a la documentación de la API de Administración del tenant iniciando sesión en la Interfaz de Administración del tenant y seleccionando **Help > API Docs** (Ayuda > Docs API) en la cabecera de la aplicación web.



API

Cada instrucción de la API de REST incluye la URL de la API, una acción HTTP, cualquier parámetro de URL requerido u opcional, y una respuesta API esperada.

La interfaz de usuario de Swagger proporciona detalles completos y documentación para cada operación de la API, como sucede en el siguiente ejemplo. Para obtener información relacionada con un usuario tenant local, deberá escribir el nombre único del usuario como el valor del parámetro `shortName` (nombre corto) y hacer clic en **Try it out** (probarlo).



La API de Administración del tenant incluye las siguientes secciones:

- **Account (Cuenta)** – Operaciones realizadas sobre la cuenta actual del tenant, incluyendo la obtención de información sobre el uso de almacenamiento.
- **auth** – Operaciones para realizar la autenticación de sesión del usuario.
  La API de Administración del tenant admite el Esquema de Autenticación Bearer Token (Bearer Token Authentication Scheme). Para que un tenant inicie sesión, deberá proporcionar el nombre de usuario, la contraseña y un Id de la cuenta en el cuerpo del JSON de la solicitud de autenticación (es decir, `POST /API/v2/authorize`). En el caso de que el usuario se autentique con éxito se le proporcionará un testigo de seguridad. Este testigo se proporcionará en la cabecera de las posteriores solicitudes de la API ("Autorización: *`testigo`* del Portador").
  Consulte "Cómo protegerse contra la falsificación de solicitudes entre sitios" para obtener información sobre cómo mejorar la seguridad de autenticación.
- **config** – Operaciones relacionadas con la edición y versiones del producto de la API de Administración del tenant. Puede enumerar la versión de la edición del producto y las versiones principales de la API admitida para dicha edición.
- **contenedores**– Operaciones sobre buckets de S3 o contenedores de Swift. Incluye opciones del nivel de consistencia para buckets S3 y contenedores de Swift. Los buckets S3 también incluyen actualizaciones de la última hora de acceso para objetos y operaciones de configuración para servicios de plataforma: Duplicación, notificaciones e integración de búsqueda de CloudMirror (notificación de metadatos).
- **deactivated-features (características desactivadas)**– operaciones para ver las características que han podido ser desactivadas.
- **endpoints**– operaciones para administrar un endpoint. Los endpoints permiten que un bucket de S3 use un servicio externo para la duplicación, notificación o integración de búsqueda de CloudMirror en StorageGRID Webscale.
- **groups (grupos)**– operaciones para gestionar grupos de tenants locales y recuperar los grupos

de tenants federados a partir de un origen de identidad externo.

- **identity-source (origen de identidad)** – Operaciones para configurar un origen de identidad externo y sincronizar manualmente el grupo federado y la información del usuario.
- **s3** – Operaciones para administrar claves de acceso S3 para los usuarios de tipo tenant.
- **usuarios**– Operaciones para ver y administrar usuarios de tipo tenant.

Control de versiones de la API de Administración del tenant

La API de Administración del tenant utiliza el control de versiones para admitir actualizaciones sin interrupciones. Por ejemplo, esta solicitud URL especifica la versión 2 de la API.

```
https://hostname_or_ip_address/api/v2/authorize
```

Las actualizaciones de la API de Administración del tenant que sean incompatibles aguas arriba se denotan mediante una nueva versión principal de la API. Por ejemplo, entre las versiones 1.1 y 2.0 se produce un salto incompatible de la API. Sin embargo, los cambios en la API de Administración del tenant que sean compatibles aguas arriba se denotan mediante cambios menores de versión de la API. Los cambios compatibles con versiones anteriores incluyen la adición de nuevos endpoints o de nuevas propiedades. Por ejemplo, entre las versiones 1.0 y 1.1 se produce un salto compatible de la API.

Cuando instale por primera vez el software StorageGRID Webscale, solo se habilita la versión más reciente de la API de Administración del tenant. Sin embargo, cuando actualice a una nueva versión principal de StorageGRID Webscale, continuará teniendo acceso a las versiones anteriores de la API, al menos a una versión principal.

Las solicitudes obsoletas se marcan como tales de las siguientes maneras:

- La cabecera de respuesta es "Deprecated: true" (Obsoleto: verdadero)
- El cuerpo de la respuesta de JSON incluye "deprecated": true

Cómo determinar qué versiones de la API son compatibles con la edición actual

Utilice la siguiente solicitud de la API para obtener una lista de las principales versiones de las API compatibles:

```
GET https://{{IP-Address}}/api/versions
{
    "responseTime": "2016-10-03T14:49:16.587Z",
    "status": "success",
    "apiVersion": "2.0",
    "data": [
        1,
        2
    ]
}
```

Cómo especificar una versión de la API para una solicitud

Puede especificar la versión de la API utilizando un parámetro de ruta (`/api/v2`) o una cabecera (`Api-Version: 2`). Si proporciona ambos valores, el valor de la cabecera anula el valor de la ruta.

```
curl https://[IP-Address]/api/v2/org/config
```

```
curl -H "Api-Version: 2" https://[IP-Address]/api/org/config
```

Cómo protegerse contra el Cross-Site Request Forgery (CSRF-Falsificación de solicitud entre sitios)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID Webscale utilizando testigos CSRF para mejorar la autenticación que utiliza cookies. La Interfaz de gestión y la Interfaz de administración del tenant activan automáticamente esta función de seguridad; otros clientes de la API pueden elegir si la habilitan en el momento de iniciar

sesión

Un atacante que pueda desencadenar una solicitud a un sitio diferente (por ejemplo, mediante un formulario POST de HTTP) puede provocar que se ejecuten ciertas solicitudes utilizando las cookies del usuario que inició sesión.

StorageGRID Webscale ayuda a protegerse contra los ataques CSRF utilizando los testigos CSRF. Cuando estén habilitadas, el contenido de una cookie específica debe coincidir con el contenido de una cabecera específica o de un parámetro de cuerpo POST específico.

Para activar esta función, asigne el valor True al parámetro `csrfToken` durante la autenticación. El valor predeterminado es false (falso).

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v2/authorize"
```

Cuando el valor es True, se asigna a la cookie `GridCsrfToken` un valor aleatorio para inicios de sesión en la Interfaz de gestión, mientras que la cookie `AccountCsrfToken` se utiliza para inicios de sesión en la Interfaz de Administración del tenant.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- La cabecera `X-Csrf-Token`, asignando al valor de la cabecera el valor de la cookie testigo CSRF.
- Para endpoints que aceptan un cuerpo codificado en formato, la solicitud puede incluir un parámetro de cuerpo de solicitud del tipo `csrfToken`.

Consulte la documentación en línea de la API para obtener ejemplos y detalles adicionales.

Nota: Las solicitudes que manejen un grupo de cookies de testigos CSRF también aplicarán la cabecera "Content-Type: application / json" para cualquier solicitud que espere un cuerpo de solicitud JSON como protección adicional contra los ataques CSRF.

Administración de acceso al sistema para los usuarios de tipo tenant

Puede garantizar a los usuarios acceso a una cuenta tenant importando usuarios y grupos desde un origen de identidad federada o creando usuarios y grupos locales. Si importa usuarios y grupos, debe otorgar a los grupos federados unos permisos adecuados para la administración de los tenants.

Configuración de la federación de identidad

Puede usar la federación de identidades para importar usuarios y grupos de tenants. El uso de la federación de identidades agiliza la configuración de los grupos y usuarios que posean una licencia y permite a los usuarios que posean una licencia iniciar sesión en la cuenta tenant utilizando credenciales conocidas.

Pasos

1. Configuración del origen de identidad federada en la página 15
2. Cómo forzar la sincronización con el origen de identidad en la página 18
3. Cómo deshabilitar la federación de identidad en la página 18

Configuración de un origen de identidad federada

Debe configurar un origen de identidad federada (tal como el Active Directory u OpenLDAP) antes de poder asignar permisos de administración a grupos y usuarios federados.

Antes de comenzar

- Debe iniciar sesión utilizando un explorador web compatible.
- Debe tener permisos de acceso específicos.
- La casilla de verificación **Uses Own Identity Source** (Utiliza una fuente de identidad propia) debe encontrarse seleccionada cuando se cree la cuenta tenant. Póngase en contacto con el administrador de la malla para obtener información o para cambiar esta configuración.

Nota: Al usar la federación de identidades, tenga en cuenta que los usuarios que solo pertenecen a un grupo primario en Active Directory no pueden iniciar sesión en la Interfaz de Administración de tenants. Para permitir que estos usuarios inicien sesión, deberá asignarles su pertenencia a un grupo creado por el usuario.

Pasos

1. Seleccione **Access Control** > **Identity Federation** (Control de acceso > Federación de identidad).
2. Seleccione **Enable Identity Federation** (Habilitar Federación de Identidad).

   Aparece información de configuración del servicio LDAP.
3. Seleccione el tipo de servicio LDAP que desee configurar desde la lista desplegable **LDAP Service Type** (Tipo de servicio LDAP).

   Puede seleccionar **Active Directory**, **OpenLDAP** u **Other** (Otros).

   Nota: Si selecciona **OpenLDAP**, debe configurar el servidor OpenLDAP. Consulte "Directrices para configurar un servidor OpenLDAP en esta guía.
4. Si selecciona **Other**, complete los campos contenidos en la sección **LDAP Attributes**

(Atributos LDAP).

- **Unique User Name** (Nombre único del usuario): El nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a `sAMAccountName` para el Active Directory y `uid` para OpenLDAP.
- **User UUID**: El nombre del atributo que contiene al identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` para el Active Directory y `entryUUID` para OpenLDAP.
- **Group Unique Name** (Nombre Único de Grupo): El nombre del atributo que contiene al identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para el Active Directory y `cn` para OpenLDAP.
- **Group UUID**: El nombre del atributo que contiene al identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para el Active Directory y `entryUUID` para OpenLDAP.

5. Especifique el servidor LDAP requerido y la información de conexión de red:

- **Hostname**: El nombre del host o la dirección IP del servidor LDAP.
- **Port**: El puerto utilizado para la conexión con el servidor LDAP. Suele ser 389.
- **Username**: El nombre de usuario utilizado para acceder al servidor LDAP, incluyendo el dominio.
  El usuario especificado debe tener permisos para listar grupos y usuarios y para acceder a los siguientes atributos:
  - `cn`
  - `sAMAccountName` o `uid`
  - `objectGUID` o `entryUUID`
  - `memberOf`
- **Password**: La contraseña asociada con el nombre de usuario.
- **Group Base DN**: El Distinguished Name (DN-Nombre distintivo) plenamente cualificado de un subárbol LDAP en el que desee buscar los grupos. En el ejemplo, todos los grupos cuyo Nombre Distintivo es relativo al DN base (DC = storagegrid, DC = example, DC = com) se pueden usar como grupos federados.

  Nota: Los valores del Unique Group Name (Nombre Único del Grupo) deben ser únicos dentro del DN base del grupo al cual pertenecen.

- **User Base DN**: El Distinguished Name (DN-Nombre distintivo) plenamente cualificado de un subárbol LDAP en el que desee buscar los usuarios.

  Nota: Los valores del Unique User Name (Nombre Único del usuario) deben ser únicos dentro del DN base del usuario al cual pertenecen.

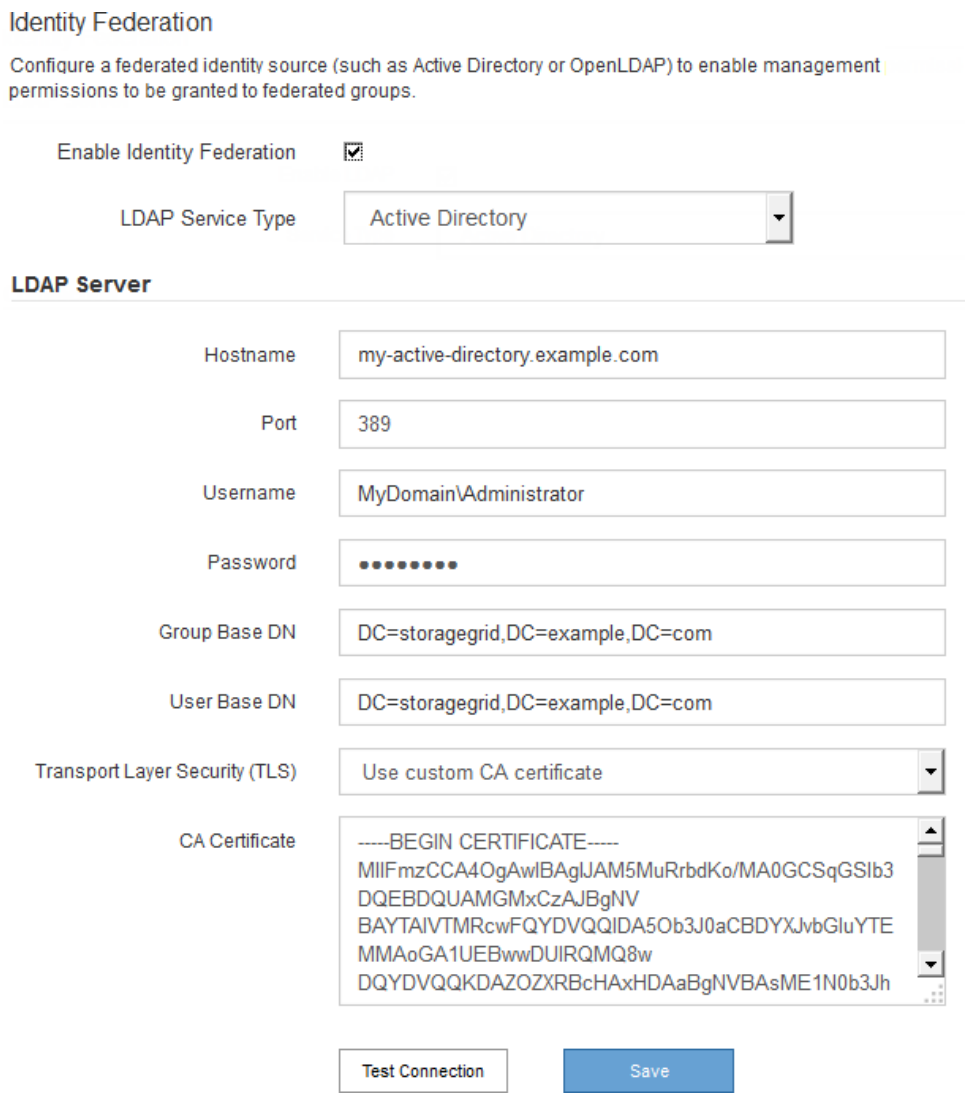
6. Seleccione una de las siguientes opciones de seguridad de la lista desplegable **Transport Layer Security (TLS)** (Seguridad de la Capa de Transporte) para especificar si se utiliza TLS para asegurar las comunicaciones con el servidor LDAP.

- **Use operating system CA certificate** (Utilizar el certificado CA del sistema operativo): Usa el certificado CA predeterminado instalado en el sistema operativo para asegurar las conexiones.
- **Use custom CA certificate** (Usar un certificado CA personalizado): Usa un certificado de seguridad personalizado.
  Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto CA Certificate (Certificado de CA).
- **Do not use TLS** (No usar TLS): El tráfico de red que circula entre el sistema StorageGRID

Webscale y el servidor LDAP no estará asegurado.

Por ejemplo:

La siguiente captura de pantalla muestra valores de configuración ejemplo para un servidor LDAP que usa el Active Directory.



7. Opcionalmente, haga clic en **Test Connection** (Probar conexión) para validar las opciones de su conexión para el servidor LDAP.
8. Haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23
Directrices para configurar un servidor OpenLDAP en la página 17

Directrices para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar determinadas opciones en el servidor OpenLDAP.

Capas memberOf y refint

Debe habilitar las capas memberOf y refint. Si desea obtener más información, consulte el apartado

"Reverse Group Membership Maintenance" en la Guía del Administrador de Software de OpenLDAP.

Indexación

Debe configurar los siguientes atributos de OpenLDAP con las palabras clave Index especificadas:

olcDbIndex: objectClass eq

olcDbIndex: uid eq,pres,sub

olcDbIndex: cn eq,pres,sub

olcDbIndex: entryUUID eq

Además, asegúrese de que los campos mencionados en la ayuda para Username (Nombre de usuario) también se encuentran indexados para obtener un rendimiento óptimo.

Para obtener más información sobre la directiva olcDBIndex utilizada con los atributos de indexación, consulte la Guía del Administrador de Software de OpenLDAP.

Información relacionada

Documentación OpenLDAP: Guía del Administrador de la Versión 2.4

Cómo forzar la sincronización con el origen de identidad

El sistema StorageGRID Webscale sincroniza periódicamente los usuarios y grupos federados desde el origen de identidad. Puede forzar la sincronización desde un principio, si así lo desea, a habilitar o restringir los permisos de usuario tan rápido como sea posible.

Antes de comenzar

- El origen de identidad debe estar habilitado.
- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Identity Federation** (Control de acceso > Federación de identidad).
2. Haga clic en **Synchronize** (Sincronizar).

   Se muestra un mensaje de confirmación que indica que la sincronización se inició correctamente.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo deshabilitar la federación de identidad

Puede desactivar de manera temporal o permanente la federación de identidades para usuarios y grupos de tenants. Cuando la federación de identidades esté deshabilitada, no hay comunicación entre el sistema StorageGRID Webscale y el origen de la identidad. Sin embargo, cualquier opción que haya configurado se conservará, lo que le permitirá volver a re-habilitar fácilmente la federación de identidades en el futuro.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que estén actualmente registrados conservarán el acceso a la cuenta tenant hasta que expire su sesión, pero no podrán iniciar sesión después de que ésta expire.
- No se producirá la sincronización entre el sistema StorageGRID Webscale y el origen de identidad.

Pasos

1. Seleccione **Access Control > Identity Federation** (Control de acceso > Federación de identidad).
2. Desactive la casilla de verificación **Enable Identity Federation** (Habilitar la Federación de Identidad).
3. Haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Administración de grupos

Los grupos de usuario le permitirán controlar qué tareas pueden desarrollar los usuarios de tipo tenant. Puede crear grupos locales o importar grupos federados desde un origen de identidad, como Active Directory u OpenLDAP.

Opciones

Creación de grupos para un tenant de S3

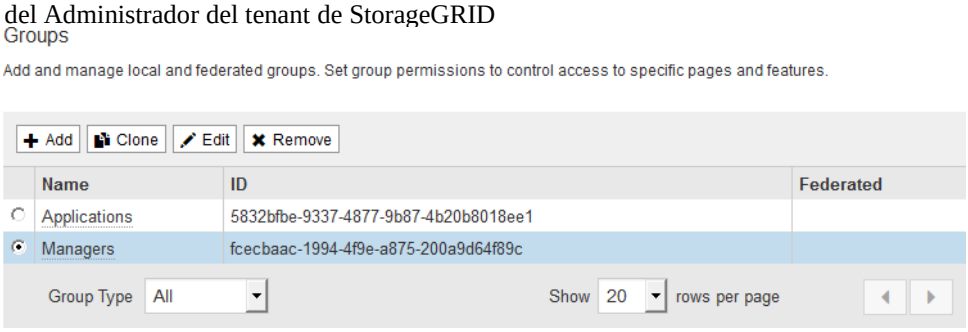
Podrá administrar los permisos de acceso para una cuenta tenant de S3 creando grupos locales o importando grupos federados. En caso necesario, también puede especificar políticas de S3 para cada grupo.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Groups** (Control de acceso > Grupos).



2. Haga clic en **Add** (Agregar).

3. Seleccione **Local** para crear un grupo local, o seleccione **Federated** para importar un grupo desde el origen de identidad previamente configurado.

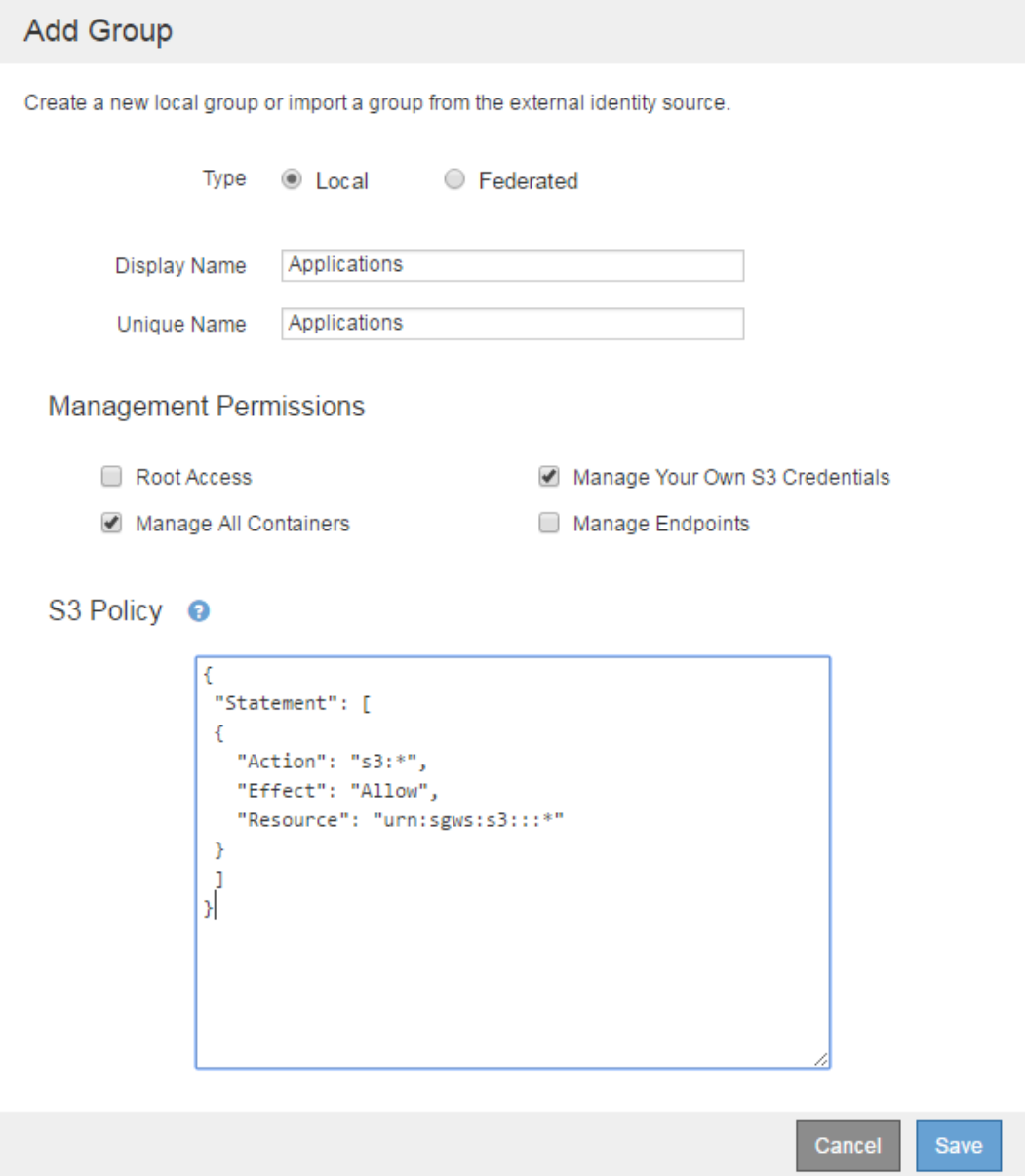
4. Introduzca el nombre del grupo.

Si selecciona...	**Escriba...**
Local	Tanto el nombre que se mostrará como un nombre único para este grupo. Puede modificar más adelante el nombre que se va a visualizar.
Federated	El nombre único del grupo federado. **Nota:** Para el Active Directory, el nombre único es el nombre asociado con el atributo `sAMAccountName`. Para OpenLDAP el nombre único es el nombre asociado con el atributo `uid`.

5. En el apartado **Permisos de Administración** seleccione los permisos de la cuenta tenant que desee asignar a este grupo.

   Consulte “Permisos de administración del tenant”.

6. Si desea unir una política de grupo a este grupo, escriba una cadena con formato JSON en el cuadro de texto **S3 Policy** (Política de S3).



Se validará la cadena JSON cuando se escriba, y solo podrá guardar cadenas de política de grupo que sean válidas.

Las políticas de grupo tienen un tamaño límite de 5.120 bytes.

Las declaraciones de política se crean utilizando esta estructura para especificar permisos:

```
<Principal> está permitida / denegada para realizar <Acción> sobre
<Recurso> cuando
se aplique <Condición>
```

Para una política de grupo no necesita especificar `<Principal>`. Principal es simplemente el grupo para el que se está especificando la política.

Por ejemplo, la siguiente política de grupo otorga permiso a los miembros del grupo para realizar todas las operaciones sobre todos los recursos que son propiedad de la cuenta tenant de S3:

```
{
 "Statement": [
  {
```

```
    "Action": "s3:*",
    "Effect": "Allow",
    "Resource": "urn:sgws:s3:::*"
  }
  ]
}
```

Nota: Consulte la Guía de Implementación de S3 (Servicio Simple de Almacenamiento) para obtener información detallada sobre las políticas de grupo, incluyendo ejemplos y sintaxis de lenguaje.

7. Haga clic en **Save** (Guardar).

   Las nuevas políticas de grupo pueden tardar hasta 15 minutos en aplicarse debido al almacenamiento en caché.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Creación de grupos para un tenant de Swift

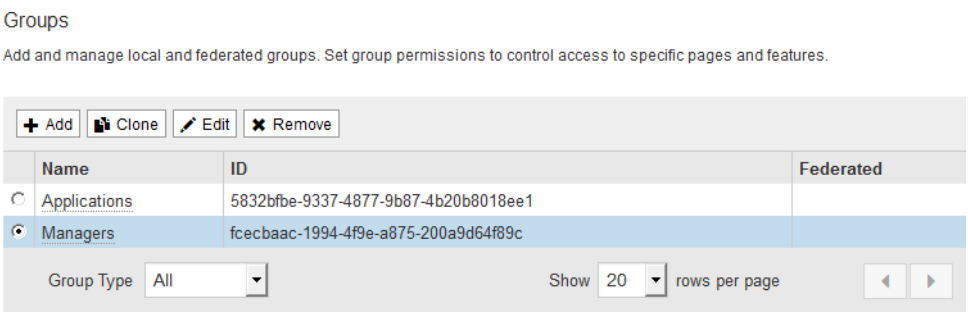
Podrá administrar los permisos de acceso para una cuenta tenant de Swift creando grupos locales o importando grupos federados.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Groups** (Control de acceso > Grupos).



2. Haga clic en **Add** (Agregar).
3. Seleccione **Local** para crear un grupo local, o seleccione **Federated** para importar un grupo desde el origen de identidad previamente configurado.
4. Introduzca el nombre del grupo.

Si selecciona...	Escriba...
Local	Tanto el nombre que se mostrará como un nombre único para este grupo. Puede modificar más adelante el nombre que se visualizará.

Si selecciona...	Escriba...
Federated	El nombre único del grupo federado. **Nota:** Para el Active Directory, el nombre único es el nombre asociado con el atributo `sAMAccountName`. Para OpenLDAP el nombre único es el nombre asociado con el atributo `uid`.

5. En el apartado **Permisos de Administración** seleccione los permisos de la cuenta tenant que desee asignar a este grupo.
6. En el apartado **Permisos de Swift**, seleccione la casilla de verificación **Administrator** si desea que los usuarios de este grupo sean Administradores de Swift.
7. Haga clic en **Save** (Guardar).

   Las nuevas políticas de grupo pueden tardar hasta 15 minutos en aplicarse debido al almacenamiento en caché.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Información relacionada

Guía de implementación de Swift de StorageGRID Webscale 11.0

Permisos de administración del tenant

Los permisos de administración de los tenants se asignan a grupos y determinan qué tareas pueden realizar los usuarios usando la Interfaz de Administración de tenants o la API de Administración de tenants. Un usuario puede pertenecer a uno o más grupos.

Para iniciar sesión en la Interfaz de administración de tenants o para usar la API de Administración de tenants, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que pueden iniciar sesión pueden realizar las siguientes tareas:

- Ver el panel
- Cambiar su propia contraseña (para usuarios locales)

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los tenants de S3 y los tenants de Swift tienen diferentes permisos de grupo.

Permiso	Descripción
Acceso raíz	Proporciona acceso a todas las funciones de administración del tenant. Permite a los usuarios la ejecución de las siguientes tareas: • Configurar un servidor de identidad • Crear, editar y eliminar grupos • Crear, editar y eliminar usuarios • Cambiar contraseñas de usuario • Tenants de S3: crea y elimina claves de acceso S3 para el usuario raíz de S3 y otros usuarios de S3
Administrador	Sólo tenants de Swift. Permite acceso completo a los datos mediante el protocolo Swift.

Permiso	Descripción
Administración de los permisos de sus propias credenciales de S3	Solo tenants de S3. Permite a los usuarios crear y eliminar sus propias claves de acceso de S3. Los usuarios que no tienen este permiso no ven la opción de menú **S3 > My Credentials** (S3> Mis credenciales).
Administrar todos los contenedores	• Tenants de S3: permite a los usuarios utilizar la Interfaz de Administración de tenants o la API de Administración de tenants para administrar la configuración de todos los buckets de S3 en la cuenta tenant, independientemente del bucket de S3 o de las directivas de grupo. Los usuarios que no disponen de este permiso no ven la opción de menú **S3 > Buckets**. • Tenants de Swift: permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift utilizando la API de Administración de tenants. El permiso Administrar todos los contenedores se puede otorgar a grupos de Swift que usan la API de Administración de tenants.
Administrar endpoints	Solo tenants de S3. Permite a los usuarios usar la Interfaz de Administración de tenants o la API de Administración de tenants para crear o editar endpoints, que se usan como destino de los servicios de la plataforma StorageGRID Webscale. Los usuarios que no tienen este permiso no ven la opción de menú **S3 > Endpoints**.

Cómo clonar un grupo

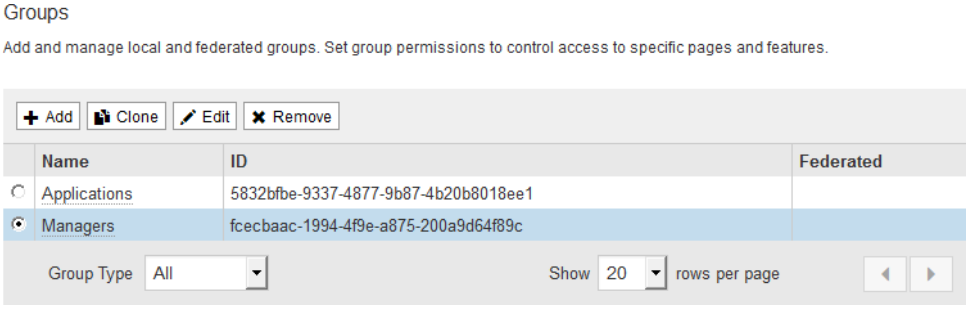
Puede crear nuevos grupos con mayor rapidez clonando un grupo existente.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Groups** (Control de acceso > Grupos).



2. Seleccione el grupo que desee clonar.

   Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren actualmente.

3. Haga clic en **Clone** (Clonar).

4. Seleccione **Local** para crear un grupo local, o seleccione **Federated** para importar un grupo desde el origen de identidad previamente configurado.

5. Introduzca el nombre del grupo.

Si selecciona...	Escriba...
Local	Tanto el nombre que se mostrará como un nombre único para este grupo. Puede modificar más adelante el nombre que se mostrará.
Federated	El nombre único del grupo federado. **Nota:** Para el Active Directory, el nombre único es el nombre asociado con el atributo `sAMAccountName`. Para OpenLDAP el nombre único es el nombre asociado con el atributo `uid`.

6. Asignación de permisos a este grupo.

7. Si clonó un grupo para un tenant de S3 puede actualizar o introducir la política S3 que desee usar para este grupo en el cuadro de texto **S3 Policy** (Política S3).

8. Haga clic en **Save** (Guardar).

Las nuevas políticas de grupo pueden tardar hasta 15 minutos en aplicarse debido al almacenamiento en caché.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo editar un grupo

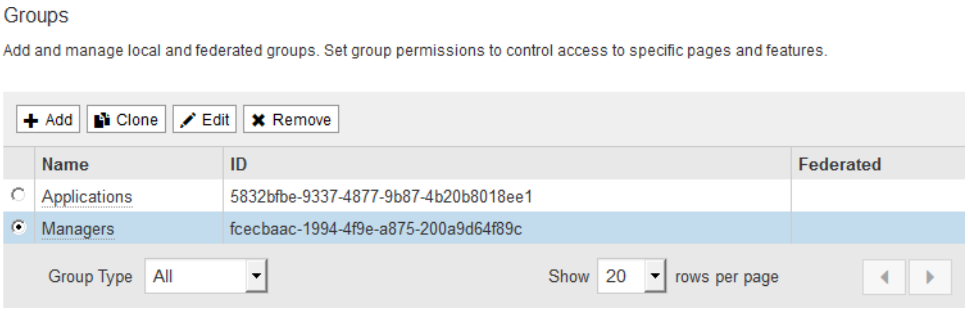
Puede editar un grupo para cambiar el nombre a visualizar de un grupo local o para actualizar los permisos.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Groups** (Control de acceso > Grupos).



2. Seleccione el grupo que desee editar.

Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren actualmente.

3. Haga clic en **Edit (Editar)**.
4. Si está editando un grupo local, actualice el nombre a visualizar según sea necesario.

   No puede cambiar el nombre único de un grupo. No puede editar el nombre de visualización de un grupo federado.
5. Actualice los permisos según sea necesario.
6. Si está editando un grupo para un tenant de S3, actualice opcionalmente la cadena JSON para la política del grupo de S3.
7. Haga clic en **Save** (Guardar).

   Los cambios realizados en las políticas de grupo pueden tardar hasta 15 minutos en aplicarse debido al almacenamiento en caché.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo eliminar un grupo

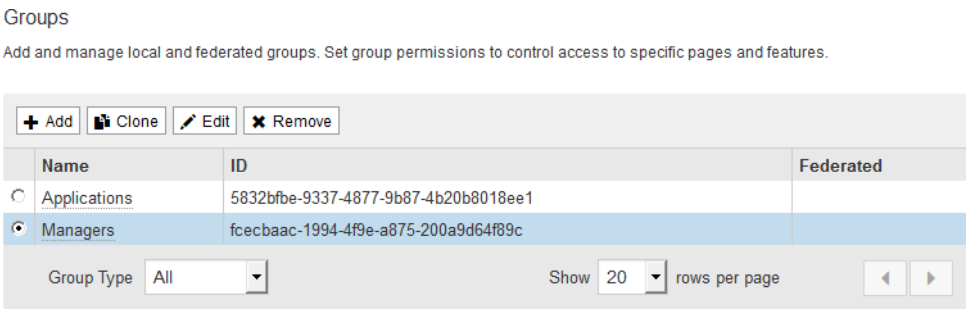
Puede eliminar un grupo. Cualquier usuario que pertenezca solo a ese grupo no podrá iniciar sesión en la Interfaz de Administración del tenant ni usar la cuenta tenant.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Groups** (Control de acceso > Grupos).



2. Seleccione el grupo que desee eliminar.

   Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren en pantalla.
3. Haga clic en **Remove** (Eliminar).
4. Haga clic en **Close** (Cerrar).

   Los cambios realizados en los permisos de acceso pueden tardar hasta 15 minutos en aplicarse

debido al almacenamiento en caché.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Administración de usuarios

Después de crear grupos locales, puede crear usuarios locales y asignarlos al grupo o grupos apropiados.

Opciones

Creación de usuarios locales

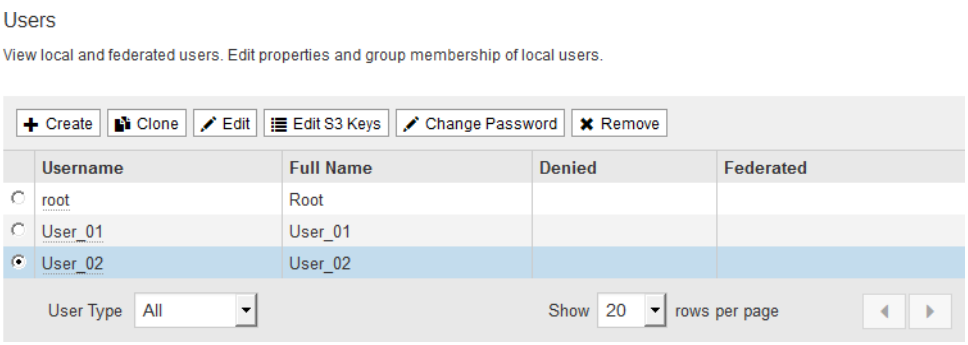
Puede crear usuarios locales y asignarlos a uno o más grupos locales para controlar sus permisos de acceso. Como los usuarios locales deben asignarse a grupos locales, debe crear los grupos antes de crear los usuarios.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

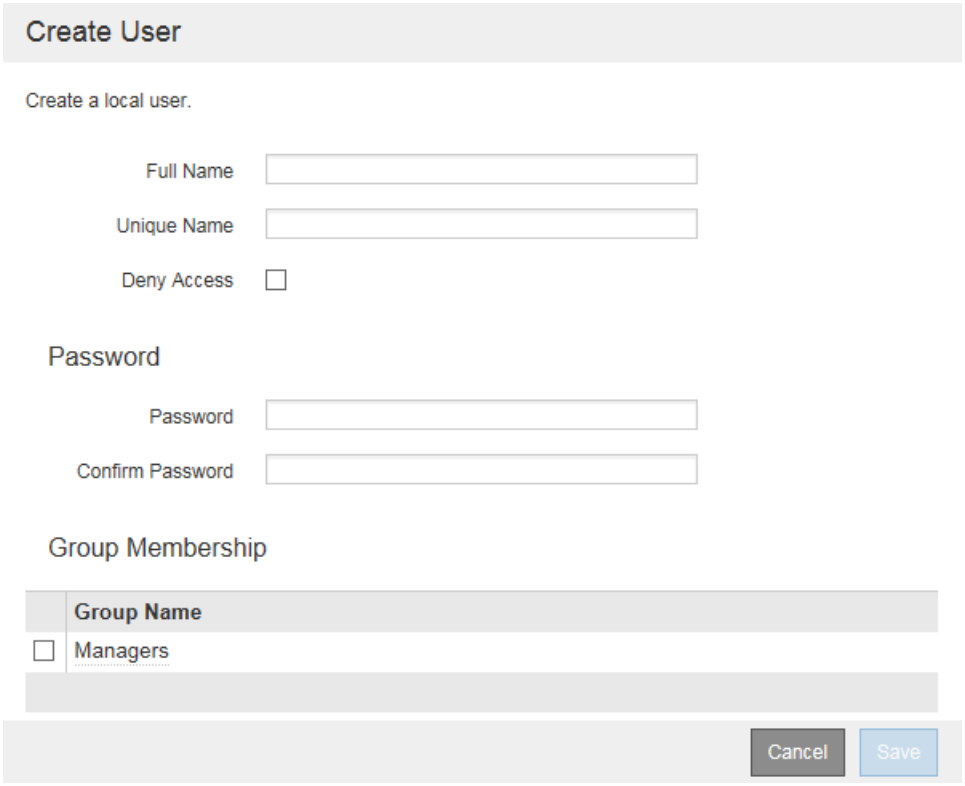
1. Seleccione **Access Control** > **Users** (Control de acceso > Usuarios).



2. Haga clic en **Create** (Crear).
3. Complete los siguientes campos.
   - **Full name** (Nombre completo): El nombre completo de este usuario, por ejemplo, el nombre de pila y el apellido de una persona o el nombre de una aplicación.
   - **Unique name** (Nombre único): El nombre único de un usuario, que se utilizará cuando éste inicia sesión.
   - **Deny access** (Denegar acceso): Si se selecciona, este usuario no podrá iniciar sesión en la cuenta tenant, incluso aunque el usuario pertenezca a uno o más grupos.

Nota: Podrá utilizar esta casilla de verificación para suspender de forma temporal la capacidad de inicio de sesión del usuario.

- **Password (Contraseña)**: La contraseña utilizada cuando el usuario inicia la sesión.



4. En la sección **Group Membership**, seleccione uno o más grupos locales.

   Los permisos son acumulativos. Los usuarios tendrán todos los permisos de todos los grupos a los que pertenezcan.

5. Haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo clonar usuarios locales

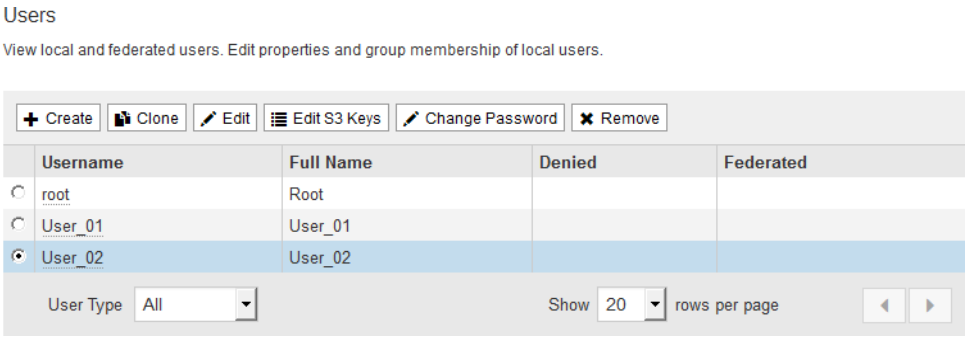
Puede clonar un usuario local para crear un nuevo usuario con mayor rapidez.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Users** (Control de acceso > Usuarios).



2. Seleccione el usuario que desee clonar.

   Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren actualmente.

3. Haga clic en **Clone** (Clonar).

4. Complete los siguientes campos.

   - **Full name** (Nombre completo): El nombre completo de este usuario, por ejemplo, el nombre de pila y el apellido de una persona o el nombre de una aplicación.
   - **Unique name** (Nombre único): El nombre único de un usuario, que se utilizará cuando éste inicie sesión.
   - **Deny access** (Denegar acceso): Si se selecciona, este usuario no podrá iniciar sesión en la cuenta tenant, incluso aunque el usuario pertenezca a uno o más grupos.

     Nota: Podrá utilizar esta casilla de verificación para suspender de forma temporal la capacidad de inicio de sesión del usuario.

   - **Password (Contraseña)**: La contraseña utilizada cuando el usuario inicia la sesión.

5. En la sección **Group Membership**, seleccione uno o más grupos locales.

   Los permisos son acumulativos. Los usuarios tendrán todos los permisos correspondientes a todos los grupos a los que pertenezcan.

6. Haga clic en **Save** (Guardar)

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo editar usuarios locales

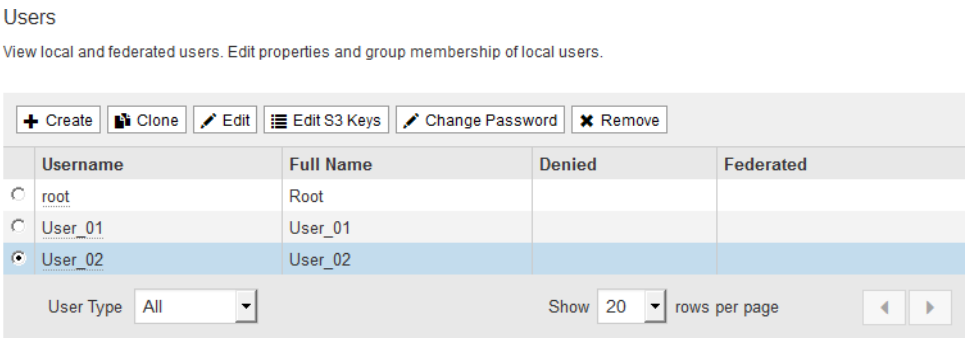
Puede editar usuarios locales para cambiar sus nombres, evitar que puedan acceder a la cuenta tenant o asignarles a diferentes grupos.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Users** (Control de acceso > Usuarios).



2. Seleccione el usuario que desee editar.

   Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren actualmente.

3. Haga clic en **Edit (Editar)**.

4. Actualice el contenido de los siguientes campos cuando sea necesario:

   - **Full name** (Nombre completo): El nombre completo de este usuario, por ejemplo, el nombre de pila y el apellido de una persona o el nombre de una aplicación.
   - **Deny access** (Denegar acceso): Si se selecciona, este usuario no podrá iniciar sesión en la cuenta tenant, incluso aunque el usuario pertenezca a uno o más grupos.

     Nota: Podrá utilizar esta casilla de verificación para suspender de forma temporal la capacidad de inicio de sesión del usuario.

5. En la sección **Group Membership** , seleccione uno o más grupos locales.

   Los permisos son acumulativos. Los usuarios tendrán todos los permisos correspondientes a todos los grupos a los que pertenezcan.

6. Haga clic en **Save** (Guardar)

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo cambiar la contraseña de un usuario local

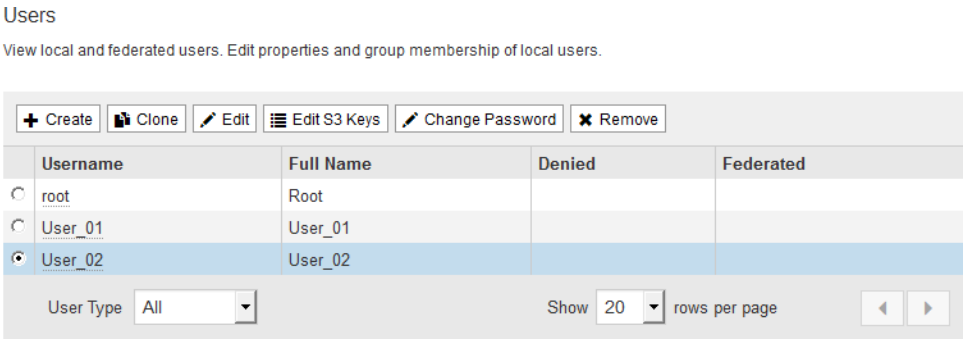
Un administrador de una licencia puede modificar las contraseñas para los usuarios locales que posean esa licencia.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Users** (Control de acceso > Usuarios).



2. Seleccione el usuario y haga clic en **Change Password** (Cambiar contraseña).

3. Escriba la nueva contraseña y haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo eliminar a los usuarios locales

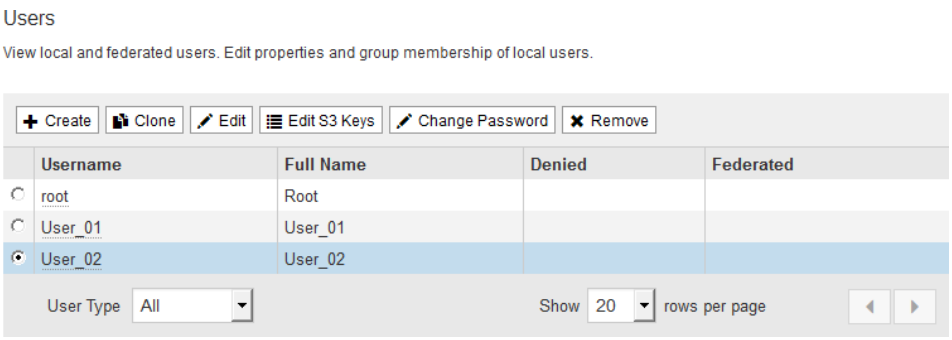
Puede eliminar permanentemente usuarios locales que ya no necesiten acceder a la cuenta tenant de StorageGRID Webscale.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Access Control > Users** (Control de acceso > Usuarios).



2. Seleccione el usuario que desee eliminar.

   Si su sistema incluye más de 20 elementos, puede especificar cuántas filas se van a mostrar simultáneamente en cada página. A continuación, puede usar la función de búsqueda de su explorador para buscar un elemento específico en las filas que se muestren actualmente.

3. Haga clic en **Remove** (Eliminar).

   Se abrirá un cuadro de diálogo de confirmación.

4. Haga clic en **OK** (Aceptar) para confirmar que desea eliminar el usuario.

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo iniciar sesión como usuario tenant

Los usuarios tenant pueden iniciar sesión como usuarios federados o como usuarios locales.

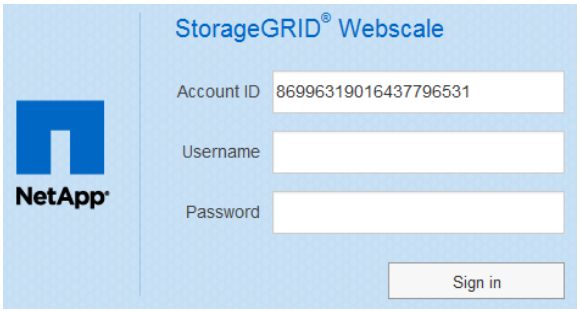
Antes de comenzar

- Debe conocer su nombre de usuario y contraseña.
- Debe tener permisos de acceso específicos.
- Debe utilizar un explorador web compatible.

Pasos

1. Acceda a la URL de su cuenta tenant.

   Aparecerá la página Sign in con el campo **Account ID** (ID de la cuenta) completado.



2. Escriba su nombre de usuario en el campo **Username.**
3. Escriba su contraseña en el campo **Password.**
4. Haga clic en **Sign in** (Iniciar sesión).

   Aparece la Interfaz de Administración del tenant. Habrá iniciado sesión.

Referencias relacionadas

Requisitos de los exploradores Web en la página 8

Administración de las cuentas tenant de S3

La Interfaz de administración de tenants le permite administrar las claves de acceso de S3, administrar la configuración por bucket para la administración de objetos o servicios de plataforma y crear endpoints para servicios de plataforma.

Administración de las claves de acceso a S3

Cada usuario de una cuenta tenant de S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID Webscale. Una clave de acceso consta de una identificación de clave de acceso y de una clave de acceso secreta.

Acerca de esta tarea

Las claves de acceso de S3 se pueden administrar en la forma indicada a continuación:

- Los usuarios que tienen el permiso **Manage Your Own S3 Credentials** (Administración de los permisos de sus propias credenciales de S3) pueden crear o eliminar sus propias claves de acceso de S3.
- Los usuarios que poseen el permiso **Root Access** (Acceso Raíz) pueden administrar las claves de acceso para la cuenta raíz de S3 y de todos los demás usuarios. Las claves de acceso raíz también proporcionan acceso completo a los buckets y objetos del tenant a menos que se inhabilite explícitamente mediante una política de bucket.

StorageGRID Webscale admite la autenticación Signature Versión 2 y Signature Versión 4. El acceso a varias cuentas no está permitido a menos que la habilite explícitamente una política de bucket.

Opciones

Creación de sus propias clave de acceso de S3

Si está utilizando un tenant de S3 y tiene el permiso correspondiente, puede crear sus propias claves de acceso S3. Debe disponer de una clave de acceso para acceder a sus buckets y objetos en la cuenta tenant de S3.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

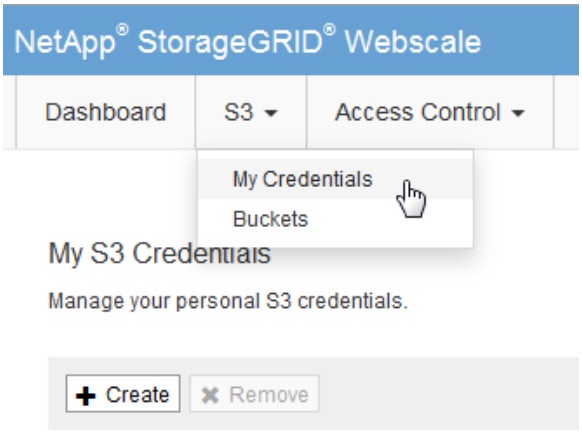
Puede crear una o más claves de acceso de S3. Las claves de acceso múltiples le permiten comenzar a usar una nueva clave sin perder temporalmente el acceso a los objetos contenidos en la cuenta. Simplemente cree la nueva clave de acceso, actualice la aplicación con su nueva identificación de clave de acceso y clave secreta, y luego elimine la clave de acceso anterior utilizando StorageGRID Webscale.

Importante: Se puede acceder a la cuenta S3 usando la ID de la clave de acceso y la Clave secreta

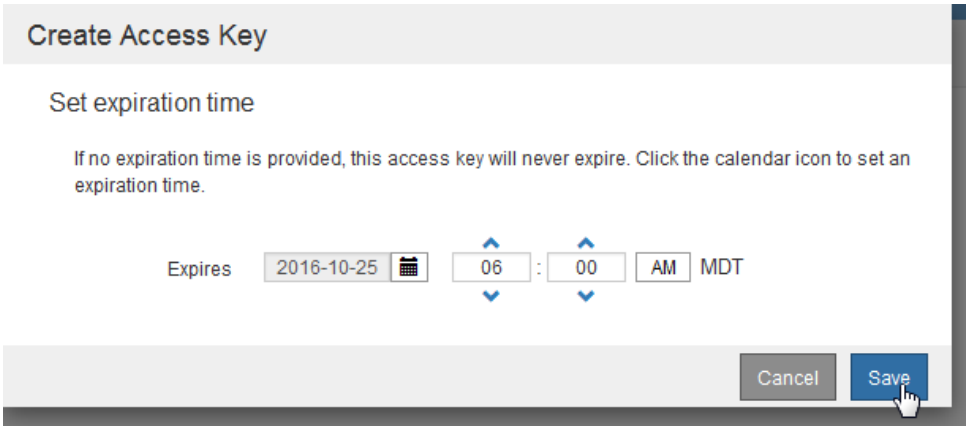
para cualquier clave mostrada actualmente. Por esta razón, proteja sus claves de acceso como lo haría con una contraseña. Modifique las claves de acceso de forma regular, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Haga clic en **S3 > My Credentials** (S3 > Mis credenciales).



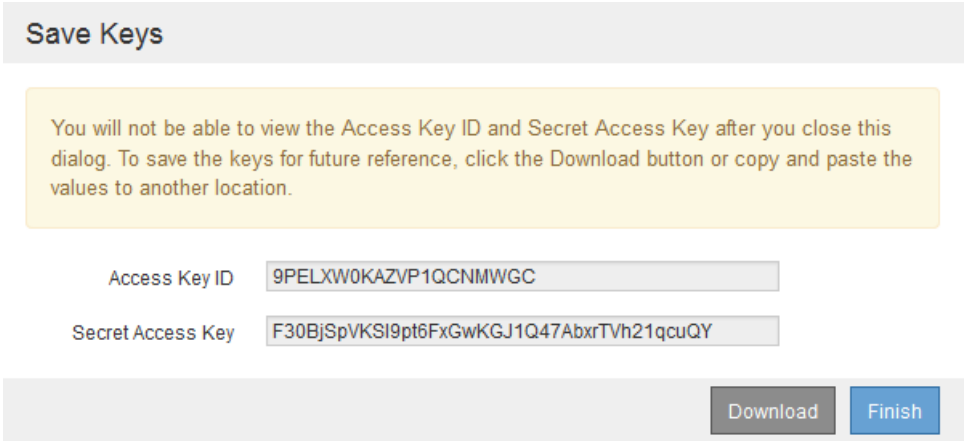
2. Haga clic en **Create** (Crear).
3. Use el control de calendario para seleccionar la fecha de caducidad y luego configure la hora o deje el valor predeterminado de Never (Nunca) y haga clic en **Save** (Guardar).



Puede definir una fecha y hora de caducidad para limitar su acceso a un cierto período de tiempo o para hacer que las claves antiguas se eliminen automáticamente. Establecer un tiempo de validez breve puede ayudar a reducir el riesgo si su identificación de clave de acceso y su clave secreta quedan expuestas accidentalmente.

Se muestra el cuadro de diálogo Save Keys (Guardar claves), que incluye su ID de clave de acceso y su clave de acceso secreta.

4. Copie el ID de la Clave de acceso y la Clave de acceso secreta en un lugar seguro, o haga clic en **Download** (Descargar) para generar un archivo de hoja de cálculo (.csv) que contenga el ID de la clave de acceso y la Clave de acceso secreta.



Importante: No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información.

5. Haga clic en **Finish** (Terminar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo eliminar sus propias clave de acceso de S3

Si está utilizando un tenant de S3 y tiene el permiso correspondiente, puede eliminar sus propias claves de acceso de S3. Después de eliminar una clave de acceso, ya no se puede usar para acceder a los objetos y los buckets en la cuenta tenant.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Debe eliminar todas las claves de acceso de su cuenta de usuario de StorageGRID Webscale que ya no esté utilizando.

Pasos

1. Haga clic en **S3 > My Credentials** (S3 > Mis credenciales).
2. Seleccione la entrada que desee eliminar.
3. Haga clic en **Remove** (Eliminar).
4. Haga clic en **OK** (Aceptar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Creación de otras claves de acceso de usuario de S3

Si está utilizando un tenant de S3 y tiene el permiso correspondiente, puede crear las claves de acceso S3 de otros usuarios.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

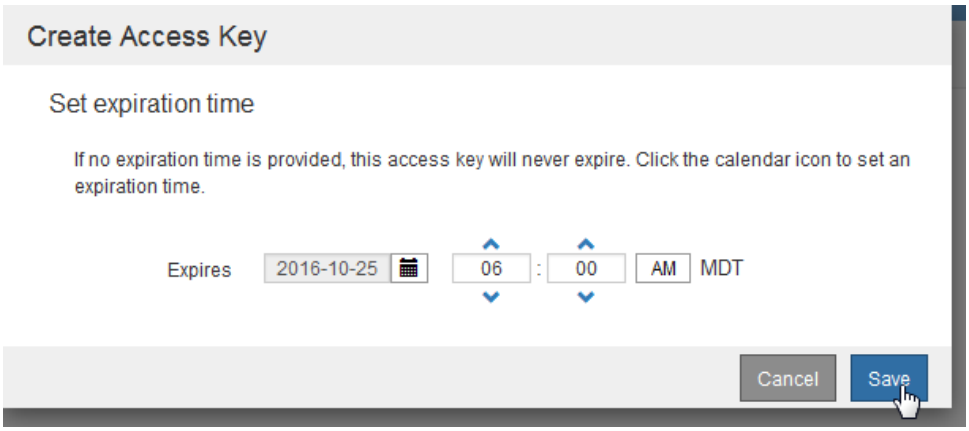
Acerca de esta tarea

Se puede acceder a la cuenta S3 usando la ID de la clave de acceso y la Clave secreta para cualquier clave mostrada actualmente. Por esta razón, proteja sus claves de acceso como protegería una contraseña. Modifique las claves de acceso de forma regular, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

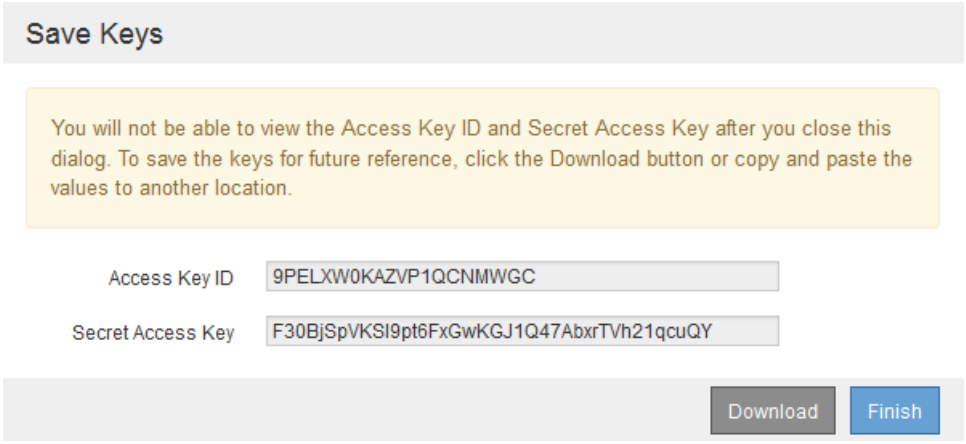
1. Haga clic en **Access Control > Users** (Control de acceso > Usuarios).
2. Seleccione el usuario cuyas teclas de acceso S3 desea administrar y haga clic en **Edit S3 Keys** (Editar claves de S3).

   Aparece el cuadro de diálogo Managing S3 Access Key (Administrar clave de acceso de S3), que muestra las claves de acceso de S3 definidas previamente para el usuario.
3. Haga clic en **Create** (Crear).
4. Use el control de calendario para seleccionar la fecha de vencimiento y luego configure la hora o deje el valor predeterminado de Never (Nunca) y haga clic en **Save** (Guardar).



   Puede definir una fecha y hora de caducidad para limitar el acceso del usuario a un cierto período de tiempo o para hacer que las claves antiguas de acceso se eliminen automáticamente. Establecer un tiempo de validez breve puede ayudar a reducir el riesgo en el caso de que el ID de la clave de acceso y la clave secreta quedan expuestas accidentalmente.

   Se muestra el cuadro de diálogo Save Keys (Guardar claves), que incluye la ID de la clave de acceso y la Clave de acceso secreta.
5. Copie el ID de la Clave de acceso y la Clave de acceso secreta en un lugar seguro, o haga clic en **Download** (Descargar) para guardar una archivo de hoja de cálculo (.csv) que contenga el ID de la clave de acceso y la Clave de acceso secreta.



Importante: No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información.

6. Haga clic en **Finish** (Terminar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo eliminar otras claves de acceso de usuarios de S3

Si está utilizando un tenant de S3 y tiene los permisos correspondientes, puede eliminar las claves de acceso de S3 de otros usuarios. Después de eliminar una clave de acceso, ya no se puede usar para acceder a los objetos y a los buckets existentes en la cuenta tenant.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Debe tener permisos de acceso específicos.

Pasos

1. Haga clic en **Access Control > Users** (Control de acceso > Usuarios).
2. Seleccione el usuario cuyas teclas de acceso S3 desea administrar y haga clic en **Edit S3 Keys** (Editar claves de S3).

   Aparece el cuadro de diálogo Managing S3 Access Key (Administrar clave de acceso de S3), que muestra las claves de acceso de S3 definidas previamente para el usuario.
3. Seleccione la entrada que desee eliminar.
4. Haga clic en **Remove** (Eliminar).
5. Haga clic en **OK** (Aceptar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo actualizar opciones de bucket de S3 para la administración de objetos

Puede actualizar el nivel de coherencia y las opciones de la hora del último acceso para los buckets de S3 para cambiar la forma en que se administran los objetos dentro de la malla. Para configurar las opciones de duplicación, notificaciones o integración de búsqueda consulte Administración de los servicios de la plataforma.

Opciones

- Cambio del nivel de coherencia en la página 38
- Cómo habilitar o deshabilitar las actualizaciones de la hora del último acceso en la página 40

Tareas relacionadas

Gestión de los servicios de plataforma en la página 42

Cambio del nivel de coherencia

Si está utilizando un tenant de S3, puede usar la Interfaz de Administración de tenants para cambiar el control de coherencia para las operaciones realizadas en los objetos en los buckets de S3. Puede utilizar la API de Administración del tenant para cambiar el control de coherencia para los tenants de S3 o los tenants de Swift.

Antes de comenzar

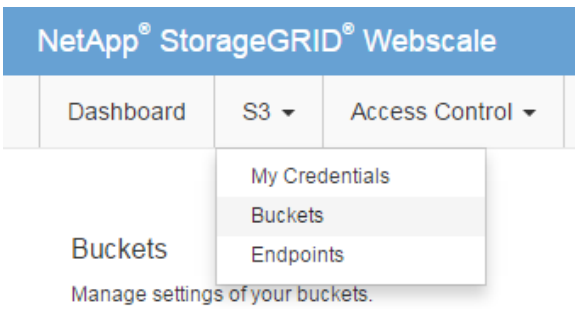
- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Los usuarios deben pertenecer a un grupo de usuarios que dispongan de los permisos **Manage All Containers** o **Root Access** (Administrar todos los Contenedores o Acceso Raíz). Estos permisos anulan la configuración de permisos en políticas de grupo o de buckets.

Acerca de esta tarea

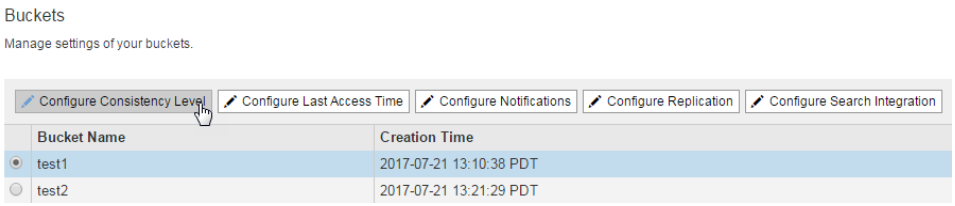
El nivel de coherencia realiza un equilibrado entre la disponibilidad de los objetos y la coherencia de esos objetos a través de diferentes Nodos de almacenamiento y sitios. En general, deberá utilizar el nivel de coherencia **Default (predeterminado)** en sus buckets. Si el nivel de coherencia predeterminado no cumple con los requisitos de coherencia o disponibilidad de la aplicación cliente, puede cambiarlo definiendo el nivel de coherencia del bucket o utilizando la cabecera `Consistency-Control` (Control de coherencia). La cabecera `Consistency- Control` sobrescribe el nivel de coherencia del bucket.

Pasos

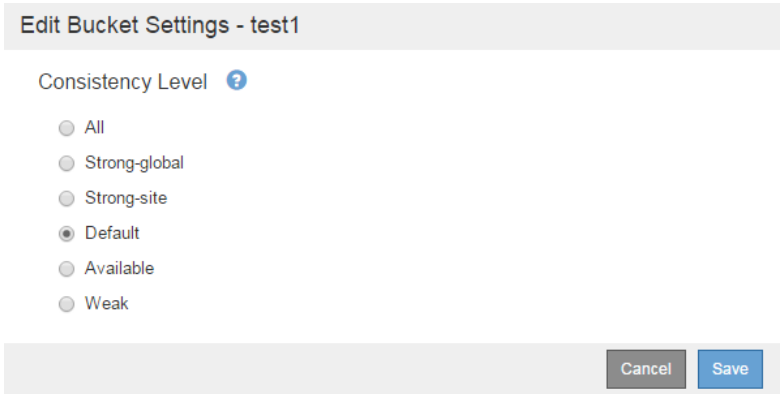
1. Haga clic en **S3 > Buckets**.



2. Seleccione un bucket de la lista.
3. Haga clic en **Configure Consistency Level** (Configurar el nivel de coherencia).



4. Seleccione un nivel de coherencia para las operaciones realizadas sobre los objetos en este bucket.



Nivel de coherencia	**Descripción**
All (todos)	Proporciona la mayor garantía de coherencia "lectura tras la escritura". Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
Strong-global (fuerte - global)	Garantiza la coherencia "lectura tras la escritura" para todas las solicitudes de los clientes en todas las sedes.
Strong-site (fuerte - sitio)	Garantiza la coherencia "lectura tras la escritura" para todas las solicitudes de los clientes dentro de una sede.
Default (predeterminado) ("lectura tras la escritura" para nuevo):	Proporciona coherencia "lectura tras la escritura" para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece alta disponibilidad y garantía de protección de datos. Coincide con las garantías de coherencia de AWS S3. **Nota:** Si su aplicación intenta operaciones HEAD sobre claves que no existen, ajuste el Nivel de coherencia a **Available (disponible) salvo que** requiera garantías de coherencia de AWS S3. De lo contrario, se puede producir un elevado número de errores del tipo "500 Internal Server error" (error interno del servidor) si uno o más nodos de almacenamiento no se encuentran disponibles.
Available (disponible) (coherencia final para operaciones HEAD):	Se comporta igual que el nivel de coherencia **default** (predeterminado), pero solo proporciona una coherencia final para las operaciones HEAD. Ofrece una disponibilidad superior para las operaciones HEAD que **Default** para el caso de que los Nodos de Almacenamiento no estén disponibles. Se distingue de las garantías de coherencia de AWS S3 solo para las operaciones HEAD.

Weak (Débil)	Proporciona coherencia final y alta disponibilidad, con garantías mínimas de protección de datos, especialmente si falla un Nodo de Almacenamiento o no está disponible. Adecuado solo para cargas de trabajo pesadas en escritura que requieran alta disponibilidad, no requieran coherencia de "lectura tras escritura" y pueden tolerar la posible pérdida de datos si falla un nodo.

5. Haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Cómo habilitar o deshabilitar las actualizaciones de la hora del último acceso

Cuando los administradores de malla crean las reglas de Administración del Ciclo de vida de la Información (ILM) para un sistema StorageGRID Webscale, pueden especificar opcionalmente que se use la hora del último acceso de un objeto para determinar si hay que mover ese objeto a una ubicación de almacenamiento diferente. Si está utilizando tenant de S3, puede aprovechar estas reglas habilitando las actualizaciones de la última hora de acceso para los objetos contenidos en un bucket S3.

Antes de comenzar

Estas instrucciones solo se aplican a los sistemas StorageGRID Webscale que incluyan al menos una regla de ILM que utilice la opción **Last Access Time** (Hora del ultimo acceso) en sus instrucciones de ubicación. Puede ignorar estas instrucciones si su sistema StorageGRID Webscale no incluye dicha regla.

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Los usuarios deben pertenecer a un grupo de usuarios que dispongan de los permisos **Manage All Containers** o **Root Access** (Administrar todos los Contenedores o Acceso Raíz). Estos permisos anulan la configuración de permisos en políticas de grupo o de buckets.

Acerca de esta tarea

Last Access Time (Última hora de acceso) es una de las opciones disponibles para la instrucción **Reference Time** (Hora de referencia) para una regla ILM. Establecer la Hora de referencia para una regla como Last Access Time (Hora del último acceso) permite a los administradores de la malla especificar que los objetos se coloquen en ciertas ubicaciones de almacenamiento en función de cuándo se recuperaron (leyeron o visualizaron) por última vez.

Por ejemplo, para garantizar que los objetos vistos recientemente permanecen en un almacenamiento más rápido, un administrador de la malla puede crear una regla ILM que especifique lo siguiente:

- Los objetos a los que se haya accedido durante el último mes deben permanecer en los Nodos de Almacenamiento locales.
- Los objetos a los que no se haya accedido durante el último mes se deben mover a una ubicación fuera del sitio.

Nota: Consulte la Guía del Administrador de StorageGRID Webscale para obtener más información.

De forma predeterminada, las actualizaciones de la hora del último acceso están deshabilitadas. Si su sistema StorageGRID Webscale incluye una regla ILM que utiliza la opción **Last Access Time** (última hora de acceso), deberá habilitar las actualizaciones de la última hora de acceso para los buckets S3 especificados en dicha regla.

La tabla siguiente resume el comportamiento aplicado a todos los objetos contenidos en el bucket cuando la hora del último acceso ha sido deshabilitada o habilitada.

Tipo de solicitud	Comportamiento si la hora del último acceso se encuentra deshabilitada (predeterminado)		Comportamiento si la hora del último acceso se encuentra habilitada	
	¿Se ha actualizado la hora del último acceso?	**¿Se ha añadido el objeto a la cola para la evaluación ILM?**	**¿Se ha actualizado la hora del último acceso?**	**¿Se ha añadido el objeto a la cola para la evaluación ILM?**
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	No	Sí	Sí
Solicitud para actualizar los metadatos de un	Sí	Sí	Sí	Sí

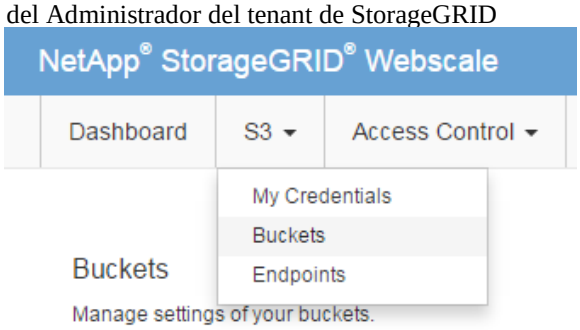
Tipo de solicitud	Comportamiento si la hora del último acceso se		Comportamiento si la hora del último acceso se encuentra	
	¿Se ha actualizado la hora del último acceso?	**¿Se ha añadido el objeto a la cola para la evaluación ILM?**	**¿Se ha actualizado la hora del último acceso?**	**¿Se ha añadido el objeto a la cola para la evaluación ILM?**
Solicitud para copiar un objeto desde un bucket a otro	• No, para la copia fuente • Sí, para la copia destino	• No, para la copia fuente • Sí, para la copia destino	• No, para la copia fuente • Sí, para la copia destino	• No, para la copia fuente • Sí, para la copia destino
Solicitud para completar una carga múltiple	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Antes de habilitar la hora del último acceso para un bucket, tenga en cuenta que la configuración habilitada puede reducir el rendimiento de StorageGRID Webscale, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento se produce porque StorageGRID Webscale debe realizar estos pasos adicionales cada vez que se recuperan objetos:

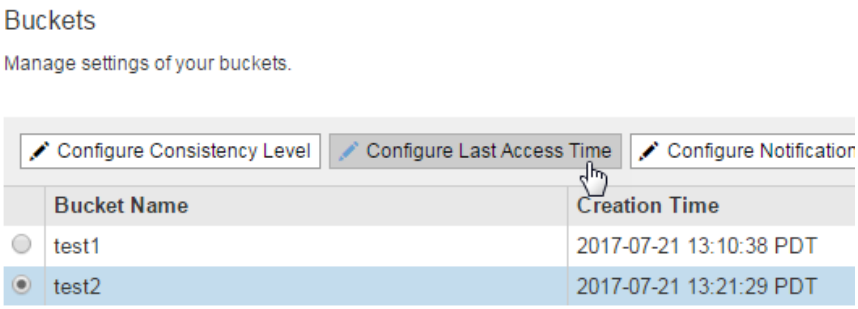
- Actualizar los objetos con nuevas marcas de tiempo
- Añadir los objetos a la cola de ILM, para que puedan ser reevaluados según las reglas y políticas actuales de ILM

Pasos

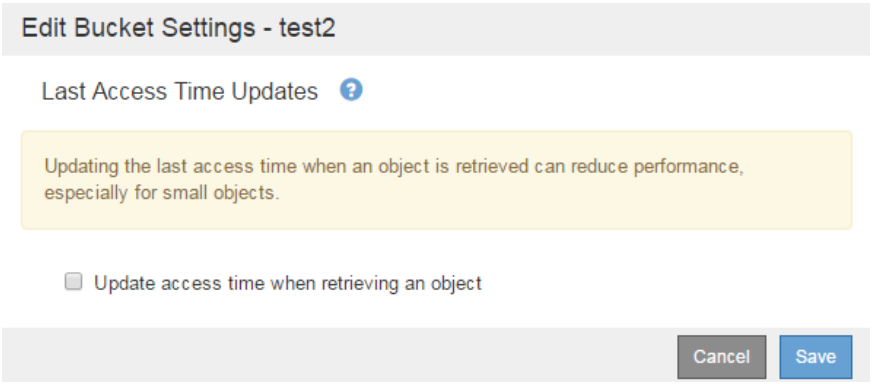
1. Haga clic en **S3 > Buckets**.



2. Seleccione un bucket de la lista.
3. Haga clic en **Configure Last Access Setting** (Configurar las opciones del último acceso).



4. Seleccione la casilla de verificación si desea actualizar la hora del último acceso al recuperar un objeto de este depósito, o desmarque la casilla si desea desactivar las actualizaciones de la hora del último acceso.



Atención: Actualizar la hora del último acceso cuando se recupera un objeto puede reducir el rendimiento, especialmente en el caso de objetos pequeños

5. Haga clic en **Save** (Guardar).

Conceptos relacionados

Permisos de administración de tenants en la página 23

Información relacionada

Guía del administrador de StorageGRID Webscale 11.0

Administración de los servicios de plataforma

Los servicios de plataforma le permiten aprovechar los servicios externos y configurar la duplicación, las notificaciones y la integración de búsqueda de CloudMirror para los buckets de S3.

Nota: StorageGRID Webscale 11.0 incluye la versión inicial de los servicios de plataforma. En la actualidad, la duplicación CloudMirror, las notificaciones y la integración de búsquedas solo resultan apropiadas para determinadas situaciones y cargas de trabajo. Tendrá que ponerse en contacto con su representante de NetApp si desea utilizar la versión inicial de estos servicios.

Qué son los servicios de plataforma

Los servicios de la plataforma StorageGRID Webscale pueden ayudarle a implementar una estrategia híbrida de nube.

Si se permite el uso de servicios de plataforma en su cuenta tenant, puede configurar los siguientes servicios para cualquier bucket de S3:

- **Duplicación de CloudMirror** El servicio de duplicación StorageGRID Webscale de CloudMirror se utiliza para duplicar objetos específicos desde un bucket de StorageGrid Webscale en un destino externo especificado.

  Por ejemplo, puede configurar la duplicación de CloudMirror para duplicar los registros de clientes específicos ubicados en un bucket a una organización hermana que posea su propia instancia de StorageGRID Webscale, creando esencialmente una malla híbrida entre organizaciones.

- **Notificaciones**: Las notificaciones de evento por bucket se utilizan para enviar notificaciones sobre las acciones específicas realizadas sobre objetos a un Servicio Simple de Notificación (SNS) externo y especificado.

  Por ejemplo, puede configurar alertas para que se envíen a los administradores en relación con cada uno de los objetos agregados a un bucket, donde los objetos representan los archivos de registro asociados con un evento crítico del sistema.

- **Servicio de integración de búsqueda** El servicio de integración de búsqueda se utiliza para enviar metadatos de objetos de S3 a un índice Elasticsearch especificado donde los metadatos se pueden buscar o analizar utilizando el servicio externo.

  Por ejemplo, puede configurar sus buckets para enviar metadatos de objetos de S3 a un servicio remoto de Elasticsearch. A continuación, puede usar Elasticsearch para realizar búsquedas en Buckets y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.

Debido a que la ubicación destino para los servicios de plataforma es generalmente externa a su despliegue de StorageGRID Webscale, los servicios de plataforma le brindan la potencia y flexibilidad que se deriva del uso de recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Cualquier combinación de servicios de plataforma se puede configurar para un solo bucket de S3. Por ejemplo, puede configurar el servicio CloudMirror y las notificaciones en un bucket de S3 en StorageGRID Webscale para que pueda duplicar objetos específicos del Servicio Simple de almacenamiento de AWS™, al tiempo que envía una notificación sobre cada objeto a una aplicación de supervisión externa para ayudarle a rastrear sus gastos de AWS.

Atención: El empleo de los servicios de plataforma debe haber sido habilitado para cada cuenta tenant por un administrador de StorageGRID Webscale usando la Interfaz de gestión o la API de gestión de la malla. Las cuentas tenant que se crearon en versiones de StorageGRID Webscale anteriores a la 11.0 tienen los servicios de plataforma deshabilitados de manera predeterminada. Póngase en contacto con su administrador de malla para obtener más información.

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con endpoints externos que se configuran utilizando la Interfaz de Administración de los tenants o la API de Administración de tenants. Cada endpoint representa un destino externo, como un bucket de S3 en StorageGRID Webscale, un Bucket de servicios web de Amazon, un tema del Servicio Simple de notificaciones o un clúster Elasticsearch

alojado localmente o en AWS.

Después de crear un endpoint, puede habilitar un servicio de plataforma para un bucket agregando una configuración XML al bucket. La configuración XML identifica los objetos sobre los que debe actuar el bucket, la acción que debe realizar el bucket y el endpoint que el bucket debe usar para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo, si desea que todos los objetos cuyas claves comiencen con "/ images" se dupliquen en un bucket S3 de AWS, debe agregar una configuración de duplicación en el bucket de origen. Si también desea enviar notificaciones cuando estos objetos estén almacenados en el bucket, debe agregar una configuración de notificaciones. Finalmente, si desea indexar los metadatos de sus objetos, también debe agregar la configuración de notificación de los metadatos que se utiliza para implementar la integración de búsqueda.

El formato del código XML de configuración se rige por las API REST de S3 utilizadas para implementar cada servicio de la plataforma StorageGrid Webscale:

Servicio de plataforma	**API REST de S3**
Duplicación CloudMirror	Duplicación de bucket de S3
Notificaciones	Notificación de bucket de S3
Integración de búsqueda	Notificación de metadatos del bucket de S3 (personalizar para StorageGRID Webscale)

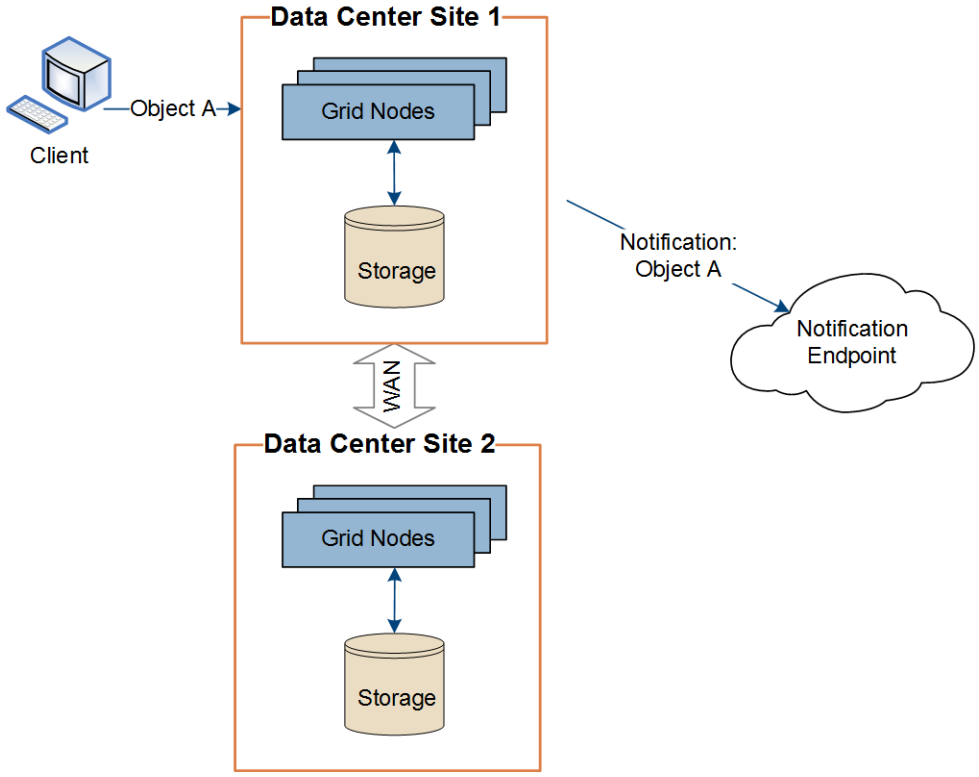
Consulte la Guía de implementación de S3 si desea obtener más información sobre como implementa StorageGRID Webscale estas APIs.

Cómo se entregan los mensajes del servicio de la plataforma

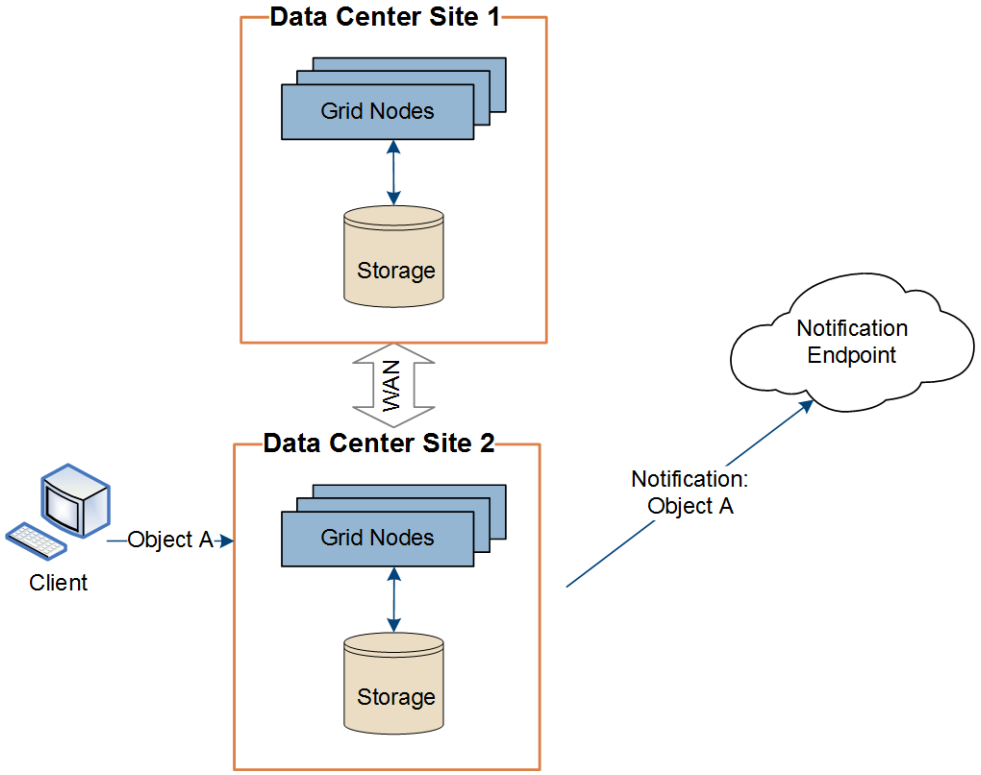
Al realizar una operación sobre un bucket que está configurado para activar un mensaje de servicios de plataforma, el mensaje se genera y se envía cuando la operación tiene éxito. Por ejemplo, si se configura un bucket para la duplicación de CloudMirror, cuando almacene con éxito un objeto en el bucket de origen se creará una copia de ese objeto y se enviará al bucket de destino. La entrega es asíncrona. Los mensajes de los servicios de la plataforma se ponen en cola para su entrega.

Si las colas crecen demasiado o si falla un servicio interno de StorageGRID Webscale, responsable de los mensajes de los servicios de la plataforma, las operaciones sobre el bucket de origen también fallarán. Este fallo impedirá que se generen más mensajes no entregados. Si el destino encuentra un problema que le impida aceptar los mensajes de los servicios de la plataforma, por ejemplo, si las credenciales se actualizan en el destino de modo que StorageGRID Webscale ya no pueda autenticarse en el servicio destino, la operación en el bucket se realiza correctamente, pero no se entregará el mensaje de los servicios de la plataforma. En esta circunstancia, el administrador de la malla verá una alarma **Total Events** (eventos totales) (SMTT) con un mensaje de error que explica la naturaleza del problema.

Todas las operaciones de los servicios de plataforma se realizan por sitio. Es decir, si realiza una operación Crear API de S3 sobre un objeto conectándose a un Nodo de Pasarela de API situado en la Sede del centro de datos 1, se activará la notificación sobre esa acción y se enviará desde la Sede del centro de datos 1.



Si posteriormente realiza una operación Eliminar de la API de S3 sobre ese mismo objeto desde la Sede del Centro de datos 2, se activará la notificación sobre la acción de eliminación y ésta se enviará desde la Sede del Centro de datos 2.



Debido a que los datos de duplicaciones, notificaciones e integración de búsqueda de CloudMirror se envían directamente desde el sitio donde se realice dicha operación, el administrador de la malla debe configurar las comunicaciones para cada sitio de manera que estos mensajes se puedan entregar desde los servicios de destino.

Conceptos relacionados

Qué son los servicios de duplicación de CloudMirror en la página 45
Qué son las notificaciones para buckets en la página 46
Qué es el servicio de integración de búsqueda en la página 47

Información relacionada

Documentación de los Servicios Web de Amazon (AWS): Duplicación entre regiones
Documentación de los Servicios Web de Amazon (AWS): Configuración de las notificaciones de los Eventos S3 de Amazon
Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Qué son los servicios de duplicación de CloudMirror

Puede habilitar la duplicación de CloudMirror para cualquier bucket de S3 en su cuenta tenant asociando el código XML de configuración de duplicación con el bucket. El software de StorageGRID Webscale repite automáticamente y de forma asíncrona los objetos especificados agregados al bucket, en el bucket de destino o en los buckets indicados en el código XML de configuración.

La duplicación de CloudMirror en StorageGRID Webscale funciona independientemente del funcionamiento de la política activa de la Administración del Ciclo de vida de la Información de la malla. El servicio CloudMirror duplica los objetos tal como están almacenados en el bucket de origen y los entrega en el bucket de destino lo antes posible. La entrega de los objetos duplicados se activa cuando se produce correctamente la ingesta de los objetos.

En StorageGRID Webscale, podrá configurar más de un bucket como el destino de la duplicación sin más que especificar diferentes destinos para cada una de las reglas en el código XML de configuración. También puede configurar la duplicación de CloudMirror en buckets versionados o no versionados, y puede especificar un bucket versionado o no versionado como destino. Puede utilizar cualquier combinación de buckets versionados o no versionados. Por ejemplo, podrá especificar un bucket versionado como el destino de un bucket origen no versionado, o viceversa. También puede realizar duplicados entre buckets no versionados.

El comportamiento del mecanismo de eliminación para el servicio de duplicación de CloudMirror es el mismo que el comportamiento del mecanismo de eliminación del servicio de Duplicación entre regiones proporcionado por el Servicio Simple de Almacenamiento de AWS; al eliminar un objeto en un bucket de origen, nunca se elimina un objeto duplicado en el destino. Si se realizan versiones de los buckets de origen y de destino, el marcador de eliminación se duplicará también. Si el bucket de destino no ha sido versionado, la eliminación de un objeto en el bucket de origen no duplicará el marcador de eliminación en el bucket de destino ni se elimina el objeto de destino.

A medida que los objetos se duplican en el bucket de destino, StorageGRID Webscale los marca como "réplicas". Un bucket de destino de StorageGRID Webscale no duplicará nuevamente los objetos marcados como réplicas, protegiéndole de bucles de duplicación accidentales. Esta marca de duplicación es interna para StorageGRID Webscale y no impide que aproveche la Duplicación entre regiones de AWS cuando se utiliza un bucket AWS de S3 como destino.

No se garantiza la exclusividad y el orden de los eventos en el bucket de destino. Se puede entregar más de una copia idéntica de un objeto fuente en el destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. En casos excepcionales, cuando el mismo objeto se actualiza simultáneamente desde dos o más sitios diferentes de StorageGRID Webscale, el orden de las operaciones en el bucket de destino puede no coincidir con el orden de los eventos en el bucket de origen.

La duplicación de CloudMirror se configura normalmente para utilizar un bucket S3 externo como destino. Sin embargo, también podría configurar la duplicación entre dos buckets en una única implementación de StorageGRID Webscale.

La duplicación de CloudMirror se realiza directamente desde el sitio donde se almacena un

objeto con la ubicación del bucket de destino. Esto significa que un administrador de la malla debe haber configurado las reglas de la interconexión de la malla y del cortafuegos en cada una de las sedes de los centros de datos para que la duplicación pueda tener éxito.

Tareas relacionadas

Configuración de la duplicación CloudMirror en la página 53

Información relacionada

Documentación de los Servicios Web de Amazon (AWS): Duplicación entre regiones

Qué son las notificaciones para buckets

Puede habilitar la notificación de eventos en los buckets de S3 para que el software StorageGRID Webscale envíe notificaciones sobre los eventos especificados a un servicio de Notificación simple (SNS) de Amazon ™ destino.

Puede configurar notificaciones de eventos asociando el código XML de configuración de notificaciones con un bucket de origen. La configuración de notificación XML sigue los convenios de S3 para configurar notificaciones de buckets, en donde se especifican los temas SNS de destino en forma del URN de un endpoint.

Las notificaciones de eventos se crean en el bucket de origen tal y como se especifica en la configuración de notificación y se entregan en el destino. Si un evento asociado con un objeto tiene éxito, se creará una notificación sobre dicho objeto y se pondrá en cola para su envío. No se garantiza la unicidad y la ordenación de las notificaciones. Se puede enviar al destino más de una notificación de un evento como resultado de las operaciones realizadas para garantizar el éxito de la entrega. Y dado que la entrega es asíncrona, no se garantiza que el orden temporal de las notificaciones en el destino coincida con el orden en que suceden los eventos en el depósito de origen, especialmente para las operaciones que se originan en diferentes sitios de StorageGRID Webscale. Podrá utilizar la clave `sequencer` en el mensaje del evento para determinar el orden de los eventos para un determinado objeto, tal y como se describe en la documentación AWS de S3.

Al igual que sucede con los otros servicios de la plataforma, las notificaciones se envían directamente desde el sitio donde ocurre un evento a la ubicación de destino. Esto significa que el administrador de la malla debe configurar las reglas de interconexión y del cortafuegos para que las notificaciones puedan entregarse a los endpoints de destino.

Notificaciones y mensajes compatibles

La notificación de eventos de StorageGRID Webscale cumple la API AWS de S3 con las siguientes limitaciones:

- No puede configurar una notificación para el evento `s3:ReducedRedundancyLostObject`. Este tipo de evento no es compatible.
- Las notificaciones de eventos enviadas desde StorageGRID Webscale utilizan el formato JSON estándar, excepto que no incluyen algunas claves y usan valores específicos para otras, como se muestra en la tabla siguiente:

Nombre de la clave	Valor de StorageGRID Webscale
eventSource	`sgws:s3`
awsRegion	no incluido
x-amz-id-2	no incluido
arn	`urn:sgws:s3:::bucket_name`

Tareas relacionadas

Configuración de las notificaciones de evento en la página 55

Información relacionada

Documentación de los Servicios Web de Amazon (AWS): Configuración de las notificaciones de los Eventos S3 de Amazon

Qué es el servicio de integración de búsqueda en la página

Puede habilitar la integración de búsqueda para buckets de S3 para que pueda usar un servicio externo de búsqueda y análisis de datos para los metadatos de sus objetos.

El servicio de integración de búsqueda es un servicio personalizado de StorageGRID Webscale que automáticamente y de forma asíncrona envía metadatos de los objetos S3 a un endpoint de destino cada vez que se actualiza un objeto o sus metadatos. A continuación puede usar herramientas sofisticadas de búsqueda, análisis de datos, visualización o de aprendizaje automático proporcionadas por el servicio de destino para buscar, analizar y obtener información de los datos de su objeto.

Puede habilitar el servicio de integración de búsqueda para cualquier bucket versionado o no versionado. La integración de búsqueda se configura asociando el XML de configuración de la notificación de los metadatos con el bucket que especifica en qué objetos actuar y el destino de los metadatos del objeto. Las notificaciones se generan en forma de un documento JSON cuyo nombre estará formado por el nombre del bucket, el nombre del objeto y el ID de la versión, si lo hubiera. Cada notificación de metadatos contiene un conjunto estándar de metadatos del sistema para el objeto, además de todas las etiquetas del objeto y los metadatos del usuario. Las notificaciones se generan y se ponen en cola para su entrega cada vez que se crea o elimina un objeto, incluso cuando se eliminan objetos como resultado de la operación de la política de Administración del Ciclo de Vida de la Información (ILM) de la malla. También se genera una notificación cuando se agregan, actualizan o eliminan metadatos o etiquetas del objeto. Tras su actualización se envía siempre el conjunto completo de metadatos y etiquetas, no solo los valores modificados.

Después de agregar el XML de configuración de la notificación de los metadatos a un bucket, las notificaciones no se envían para ningún objeto que ya estuviera en el bucket. Las notificaciones se envían para cualquier objeto de nueva creación que cree después de agregar el XML de configuración y para cualquier objeto que modifique al actualizar sus datos, metadatos de usuario o etiquetas. Para comprobar que los metadatos del objeto de S3, para todos los objetos contenidos en un bucket, se envían al destino debe configurar el servicio de integración de búsqueda inmediatamente después de crear el bucket y antes de agregar cualquier objeto, o debe realizar una acción sobre todos los objetos que ya estén en el bucket que activará el envío de un mensaje de notificación de metadatos al destino.

El servicio de integración de búsqueda de StorageGRID Webscale admite un clúster Elasticsearch como destino. Al igual que sucede con otros servicios de la plataforma, el destino se especifica en el endpoint cuyo URN se utiliza en el XML de configuración para el servicio.

Las notificaciones de integración de búsqueda se envían directamente desde el sitio en el que se activa la actualización de los metadatos al endpoint de destino. Esto significa que un administrador de malla debe configurar las reglas de interconexión y del cortafuegos en cada sede de los centros de datos para que los documentos se puedan enviar al índice Elasticsearch de destino.

Consulte la Interoperability Matrix Tool (Herramienta de la matriz de interoperabilidad) para obtener más información sobre las versiones compatibles de Elasticsearch.

Tareas relacionadas

Empleo de la Interfaz de Administración del tenant para configurar el servicio de integración de búsqueda en la página 62

Referencias relacionadas

Configuración XML para la integración de búsqueda en la página 58
Metadatos de objetos incluidos en las notificaciones de metadatos en la página 61
JSON generados por el servicio de integración de búsqueda en la página 62

Información relacionada

Interoperability Matrix Tool de NetApp

Qué es un endpoint

Un endpoint almacena la información sobre un servicio remoto que se necesita para permitir que StorageGRID Webscale utilice el recurso externo como objetivo para un servicio de plataforma.

Por ejemplo, para duplicar objetos desde un bucket de StorageGRID Webscale a un bucket del Servicio Simple de Almacenamiento de AWS, el sistema necesita proporcionar credenciales y un URI del bucket a AWS. Esta información se almacena en el endpoint.

Cada tipo de servicio de plataforma requiere su propio endpoint, por lo que, al menos, necesita configurar un endpoint para cada servicio de plataforma que piense utilizar. Después de definir un endpoint, utilizará el URN del endpoint como el destino en el código XML de configuración que utilice para habilitar el servicio.

Podrá utilizar el mismo endpoint como el destino para más de un bucket origen. Por ejemplo, puede configurar varios buckets orígenes para enviar metadatos de objetos al mismo endpoint de integración de búsqueda para poder realizar búsquedas entre varios buckets. También puede configurar un bucket origen para usar más de un endpoint como destino, lo que le permite hacer cosas tales como enviar notificaciones sobre la creación de objetos a un tema SNS y notificaciones sobre eliminación de objetos a un segundo tema SNS.

Debe definir el endpoint utilizado como destino para un servicio de plataforma antes de configurar un servicio de plataforma para un bucket, o fallará la configuración del servicio.

El acceso a los servicios de plataforma se habilita por cada tenant y esta operación la realiza un administrador de StorageGRID Webscale. Los endpoints solo pueden ser creados y utilizados por usuarios tenant que cuenten con los permisos apropiados, en una malla cuya interconexión haya sido configurada para permitir que los nodos de almacenamiento accedan a recursos externos de endpoint. Póngase en contacto con su administrador de malla para obtener más información.

Endpoints para la duplicación de CloudMirror

StorageGRID Webscale es compatible con los endpoints de duplicación que representan los buckets de S3. Estos buckets deben ser alojados en Servicios Web de Amazon, el mismo o un despliegue remoto de StorageGRID Webscale, u otro servicio.

Para utilizar como endpoint un bucket de S3 alojado en un sistema StorageGRID Webscale deberá especificar un Nodo de Pasarela API en la definición del endpoint.

Endpoints para notificaciones

StorageGRID Webscale es compatible con los endpoints del Servicio Simple de Notificación (SNS). No es compatible con los endpoints de AWS Lambda o Simple Queue Service (SQS).

Endpoints para el servicio de integración de búsqueda

StorageGRID Webscale es compatible con los endpoints de integración de búsqueda que representan a los clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden ser alojados en una nube de AWS o en un centro de datos local.

El endpoint de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debe crear el índice en Elasticsearch antes de crear el endpoint en StorageGRID Webscale o fallará la creación del endpoint. No necesita crear el tipo antes de crear el endpoint. StorageGRID Webscale creará el tipo, si fuera necesario, cuando envíe los metadatos del objeto al endpoint.

Cómo se especifican los endpoints

Un endpoint se especifica utilizando un grupo de campos que identifican al recurso externo al que representa el endpoint y que establecerá la forma en que se accede al recurso. Puede crear un endpoint utilizando la API de Administración del tenant o la Interfaz de Administración del tenant.

StorageGRID Webscale valida los endpoints a medida que los vaya creando, por lo que tendrá que garantizar que el recurso especificado en el endpoint existe y que se puede alcanzar antes de crear dicho endpoint.

Cuando cree un endpoint utilizando la API de Administración del tenant deberá incluir la siguiente información en el JSON del endpoint. Cuando cree un endpoint utilizando la Interfaz de Administración del tenant deberá especificar la siguiente información en un cuadro de diálogo.

Campo	Descripción
Display Name (Nombre de visualización)	Un nombre que describe brevemente el endpoint y su propósito. El tipo de servicio de plataforma que permite el endpoint se muestra junto al nombre del endpoint cuando se enumera en la página de endpoints, por lo que no es necesario que esta información se incluya en el nombre.
URI	El Identificador Único de Recurso (URI) del endpoint. Deberá especificar el URI del endpoint en uno de los siguientes formatos: • `https://host:port` • `http://host:port` Si no especifica un puerto, se utiliza de forma predeterminada el puerto 443 para los URI de HTTPS y el puerto 80 para los URI de HTTP. Por ejemplo, un endpoint para un bucket alojado en StorageGRID Webscale puede tener un URI con el formato `https://api-gateway-node.storagegrid.example.com: 8082` mientras que el URI de un bucket hospedado en AWS puede ser `https://s3-aws- region.amazonaws.com`

<table>
<tr><th>Campo</th><th>Descripción</th></tr>
<tr><td>Urn</td><td>
El Nombre Único de Recurso (URN) del endpoint. Utilizará el URN para hacer referencia a este endpoint cuando cree el XML de configuración para un servicio de plataforma. El URN para cada endpoint debe ser único.

Elementos requeridos

El tercer elemento del URN especifica el tipo de servicio de plataforma, y el último elemento del URN identifica el recurso destino específico en el URI destino.

<table>
<tr><th>Servicio</th><th>Tipo</th><th>Recurso específico</th></tr>
<tr><td>Duplicación CloudMirror</td><td>s3</td><td>bucket-name (nombre de bucket)</td></tr>
<tr><td>Notificaciones</td><td>sns</td><td>sns-topic-name (nombre de tema sns)</td></tr>
<tr><td>Integración de</td><td>es</td><td>domain-name/index-name/type-name</td></tr>
</table>
Nota: Para los endpoints de integración de búsqueda, antes de crear el endpoint debe crear el índice Elasticsearch, pero no el tipo. La validación del endpoint solo se realiza utilizando el índice de Elasticsearch. El tipo se crea dinámicamente cuando se envían los metadatos del objeto al destino.

URN para servicios alojados en AWS

Para las entidades de AWS, el URN completo es un ARN válido de AWS:

• arn:aws:s3:::bucket-name

• arn:aws:sns:region:account-id:topic-name

• arn:aws:es:region:account-ID:domain/domain-name/index-name/type-name

Nota: Para un endpoint de integración de búsqueda de AWS, el nombre-dominio debe incluir la cadena literal domain/, tal y como se muestra aquí.

URN para servicios alojados de forma local

Para los servicios alojados localmente, puede especificar el URN de tal forma que cree un URN válido y único, siempre que el URN incluya los elementos necesarios en las posiciones tercera y última. Puede dejar en blanco los elementos indicados como opcional o puede especificarlos de tal forma que ayude a identificar el recurso y que haga que el URN sea único:

• urn:mysite:s3:optional:optional:bucket-name

• urn:mysite:sns:optional:optional:sns-topic-name

• urn:mysite:es:optional:optional:domain-name/index-name/type- name

Nota: Para los endpoints de integración de búsqueda alojados de forma local, el elemento domain-name (nombre-dominio) puede ser cualquier cadena siempre que el URN del endpoint sea único.

Para un endpoint de CloudMirror alojado en StorageGRID Webscale, podrá especificar un URN válido que comience por urn:sgws.

• urn:sgws:s3:optional:optional:bucket-name
</td></tr>
</table>

Campo	Descripción
ID de la clave de acceso	Es el identificador de la clave de acceso para el servicio de destino, formateado como una clave de acceso de AWS. Para acceso anónimo al destino, omita tanto el Identificador de la Clave de Acceso como la Clave de Acceso Secreta.
Clave de acceso secreta	Es la Clave de Acceso Secreta para el servicio de destino, formateado como una clave de acceso secreta de AWS. Para acceso anónimo al destino, omita tanto el Identificador de la Clave de Acceso como la Clave de Acceso Secreta.
Validación de certificado	Es el método de validación del certificado utilizado para las conexiones TLS al recurso del endpoint: • Emplear el certificado CA del sistema operativo. Si selecciona esta opción, StorageGRID Webscale utiliza su certificado predeterminado del sistema operativo para verificar la conexión con el recurso del endpoint. Esta opción es equivalente a enviar un certificado 'null' utilizando la API de endpoint. • Utilizar un certificado CA personalizado. Si prefiere utilizar un certificado personalizado para verificar la conexión TLS con el recurso de endpoint, seleccione esta opción. Aparecerá un cuadro de texto para que pueda añadir el certificado CA personalizado en formato PEM. • No verificar el certificado Al seleccionar esta opción impide la verificación del certificado utilizado para la conexión TLS. Se corresponde con la opción 'insecureTLS' en la API de endpoint.
CA Certificado	Un campo de texto que puede utilizar para añadir un certificado CA personalizado en formato PEM para su empleo en la verificación del endpoint cuando utilice TLS.

Creación de un endpoint utilizando la Interfaz de Administración del tenant

Debe crear al menos un endpoint del tipo correcto antes de poder habilitar un servicio de plataforma.

Antes de comenzar

- Debe iniciar sesión en la Interfaz de Administración del tenant utilizando un explorador compatible.
- Un administrador de malla de StorageGRID Webscale debe haber habilitado los servicios de plataforma para su cuenta tenant.
- Deberá pertenecer a un grupo de usuarios que disponga del permiso **Manage EndPoints** (Administrar endpoints).
- Debe comprobar que el recurso al que hace referencia el endpoint ha sido creado:
  - **Duplicación CloudMirror**: bucket de S3
  - **Notificación de evento**: tema SNS
  - **Integración de búsqueda**: Índice Elasticsearch

    Nota: Debe crear el índice Elasticsearch, pero no el tipo, antes de crear el endpoint. La validación del endpoint se realiza utilizando el índice de Elasticsearch. El tipo se creará dinámicamente cuando se envíen los metadatos del objeto al destino.
- Debe disponer de toda la información necesaria para crear el endpoint, tal y como se indica en “Cómo se especifican los endpoints.”

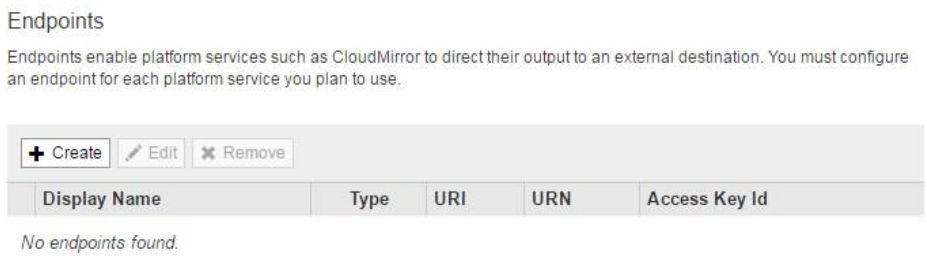
Acerca de esta tarea

Después de crear un endpoint, podrá editarlo volviendo a **S3 > Endpoints** y seleccionar **Edit** (Editar). Sin embargo, el URN de un endpoint no se puede cambiar una vez que el endpoint se haya creado.

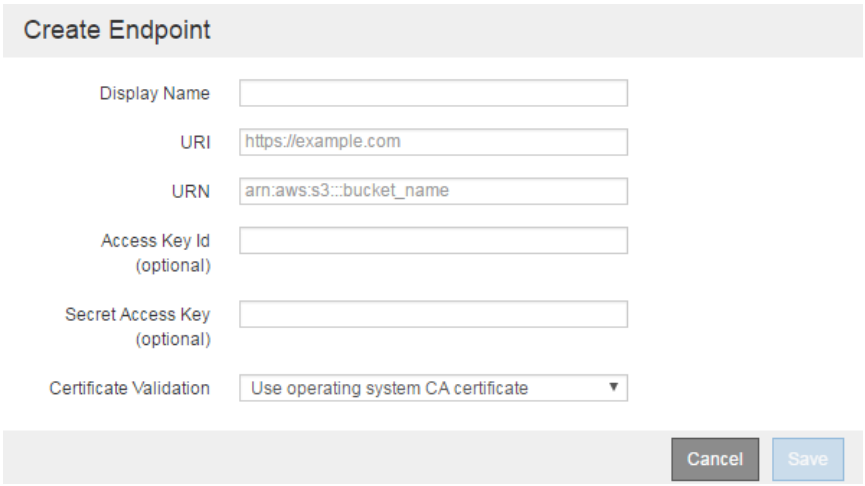
Pasos

1. Haga clic en **S3 > Endpoints**.

   Se abre la página EndPoints y muestra la lista de endpoints que ya han sido configurados.



2. Haga clic en **Create** (Crear) para crear un nuevo endpoint.



3. Complete cada uno de los campos mostrados en el cuadro de diálogo **Create Endpoint** (Crear endpoint).

   Consulte “Cómo se especifican los endpoints” para obtener más información.

4. Haga clic en **Save** (Guardar).

   Cuando almacene un endpoint, StorageGRID Webscale valida la existencia del endpoint que ha configurado y que se puede acceder al mismo utilizando las credenciales que ha especificado.

   Si fallase la validación del endpoint, recibirá un mensaje de error que explica el motivo de dicho fallo. Resuelva el problema e intente crear de nuevo el endpoint.

   Nota: La creación del endpoint fallará si los servicios de plataforma no están habilitados para su cuenta tenant. Póngase en contacto con su administrador de malla de StorageGRID Webscale.

Después de terminar

Una vez que haya configurado un endpoint, podrá utilizar su URN para configurar un servicio de plataforma.

Conceptos relacionados

Cómo se especifican los endpoints en la página 49

Configuración de la duplicación CloudMirror

El servicio de Duplicación CloudMirror de StorageGRID Webscale permite a un tenant la duplicación automática de objetos en un bucket de S3 externo. Podrá habilitar la duplicación utilizando la Interfaz de Administración del tenant.

Atención: StorageGRID Webscale 11.0 incluye la versión inicial de los servicios de plataforma. La duplicación CloudMirror, las notificaciones y la integración de búsquedas solo resultan apropiadas para determinadas situaciones y cargas de trabajo. Tendrá que ponerse en contacto con su representante de NetApp si desea utilizar la versión inicial de estos servicios.

Antes de comenzar

- Debe haber creado ya un bucket que actuará como origen de la duplicación. Los buckets se crean utilizando la API de S3 en StorageGRID Webscale.
- Un administrador de malla de StorageGRID Webscale debe haber habilitado los servicios de plataforma para su cuenta tenant.
- El endpoint que intente utilizar como destino para la duplicación de CloudMirror debe existir y debe conocer su URN.
- Debe pertenecer al grupo de usuarios que tiene los permisos **Administrar todos los contenedores** o **Acceso Raíz**, que le permitirán administrar las opciones para todos los buckets de S3 en su cuenta tenant. Estos permisos sobrescriben las opciones de permisos contenidos en las políticas de grupo o de bucket cuando configure el bucket utilizando la Interfaz de Administración del tenant.

Acerca de esta tarea

La duplicación CloudMirror copia los objetos contenidos en un bucket origen en el bucket destino que se especificó en un endpoint. Para habilitar la duplicación de CloudMirror para un bucket, debe crear y aplicar un código XML de configuración de duplicación de bucket que sea válido. El XML de configuración de duplicación debe utilizar un URN de endpoint de bucket de S3 como destino.

Si desea obtener información general sobre la duplicación de buckets y la forma de configurar esta operación, consulte la documentación de Amazon sobre duplicación entre regiones. Si desea obtener información sobre cómo implementa StorageGRID Webscale la API de configuración para la duplicación de buckets de S3, consulte la Guía de implementación de S3 en StorageGRID Webscale.

Si habilita la duplicación de CloudMirror sobre un bucket que contiene objetos, se duplicarán los nuevos objetos que añada al bucket pero no sucederá lo mismo con los objetos que ya existan en el bucket. Debe actualizar los objetos existentes para activar la duplicación.

Pasos

1. Habilitar la duplicación para su bucket origen:

   a. Utilice un editor de texto para crear el código XML de configuración necesario para habilitar la duplicación, tal y como se especifica en la API de duplicación del Servicio Simple de Almacenamiento (S3).

      Cuando elabore el código XML utilice el URN de un endpoint del bucket de S3 como destino.

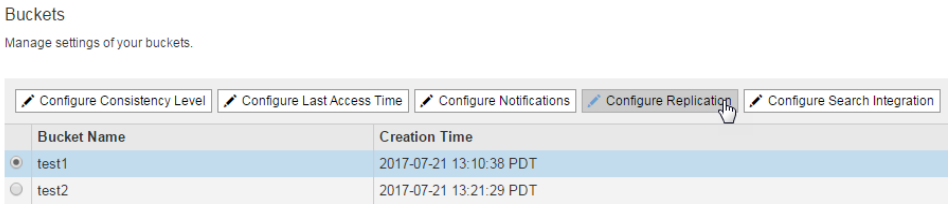
      #### Ejemplo

      ```
      <ReplicationConfiguration>
          <Role></Role>
          <Rule>
              <Status>Enabled</Status>
      ```

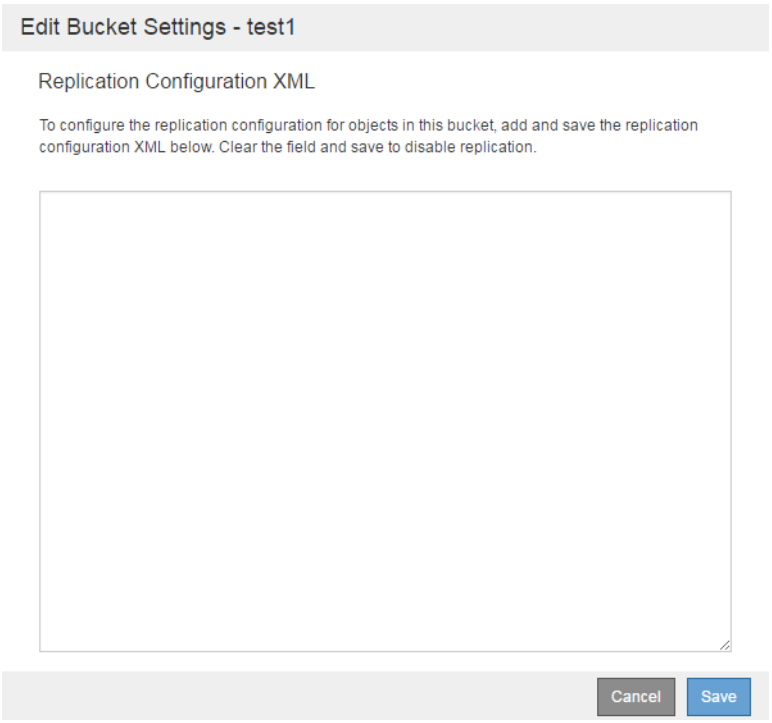
```
        <Prefix>2017</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

b. En la Interfaz de Administración de tenants vaya a **s3 > Buckets**.

c. Seleccione el bucket origen y haga clic en **Configure Replication (Configurar duplicación)**.



d. Pegue la configuración de duplicación en el cuadro de texto y haga clic en **Save** (Guardar).



Nota: El empleo de los servicios de plataforma debe haber sido habilitado para cada cuenta tenant por un administrador de StorageGRID Webscale usando la Interfaz de gestión o la API de gestión de la Malla. Póngase en contacto con su administrador de malla si se produce un error cuando guarde el XML de configuración.

2. Verifique que la duplicación se ha configurado correctamente:

a. Añada un objeto al bucket origen que cumpla los requisitos para la duplicación tal y como se especifica en la configuración de duplicación.

En el ejemplo mostrado anteriormente se duplicarán los objetos que tengan el prefijo “2017”.

b. Confirme que el objeto ha sido duplicado en el bucket destino.

Para los objetos de pequeño tamaño, la duplicación se realiza con rapidez.

Ha configurado su bucket origen para la duplicación de buckets en StorageGRID Webscale.

Conceptos relacionados

Qué son los servicios de duplicación de CloudMirror en la página 45

Tareas relacionadas

Creación de un endpoint utilizando la Interfaz de Administración del tenant en la página 51

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)
Documentación de los Servicios Web de Amazon (AWS): Duplicación entre regiones

Configuración de las notificaciones de evento

Al habilitar las notificaciones de evento de S3 para un bucket habilita a un tenant para que envíe notificaciones sobre los eventos especificados a un servicio de destino que sea compatible con el Servicio Simple de Notificación ™(SNS) de AWS. Puede configurar notificaciones para un bucket utilizando la Interfaz de Administración del tenant.

Atención: StorageGRID Webscale 11.0 incluye la versión inicial de los servicios de plataforma. La duplicación CloudMirror, las notificaciones y la integración de búsquedas solo resultan apropiadas para determinadas situaciones y cargas de trabajo. Tendrá que ponerse en contacto con su representante de NetApp si desea utilizar la versión inicial de estos servicios.

Antes de comenzar

- Debe haber creado ya un bucket que actuará como origen de las notificaciones. Los buckets se crean utilizando la API de S3 en StorageGRID Webscale.
- Un administrador de malla de StorageGRID Webscale debe haber habilitado los servicios de plataforma en su cuenta tenant.
- El endpoint que intente utilizar como destino para las notificaciones de evento debe existir, y usted debe disponer de su URN.
- Debe pertenecer al grupo de usuarios que tiene los permisos **Administrar todos los contenedores** o **Acceso Raíz**, que le permitirán administrar las opciones para todos los buckets de S3 en su cuenta tenant. Estos permisos sobrescriben las opciones de permisos contenidos en las políticas de grupo o de bucket cuando configure el bucket utilizando la Interfaz de Administración del tenant.

Acerca de esta tarea

Después de configurar las notificaciones de evento, siempre que se produzca un evento especificado para un objeto en el bucket origen, se generará una notificación y se enviará al Servicio Simple de Notificación (SNS) utilizado como endpoint de destino. Para habilitar las notificaciones para un bucket, debe crear y aplicar un código XML de configuración de notificación que sea válido. El Código XML de configuración de notificación debe utilizar como destino un URN de endpoint de notificaciones .

Si desea obtener información general sobre notificaciones de evento y sobre cómo configurarlas, consulte la documentación de Amazon. Si desea obtener información sobre cómo implementa StorageGRID Webscale la API de configuración para la notificación de buckets de S3, consulte la Guía de implementación de S3 en StorageGRID Webscale.

Si habilita la notificación de eventos para un bucket que contiene objetos, las notificaciones se enviarán solo para las acciones que se ejecuten cuando se haya almacenado la configuración de la notificación.

Pasos

1. Habilite las notificaciones para su bucket origen:

   a. Utilice un editor de texto para crear el código XML de configuración de notificación necesario para habilitar las notificaciones de eventos, tal y como se especifica en la API de notificación del Servicio Simple de Almacenamiento (S3).

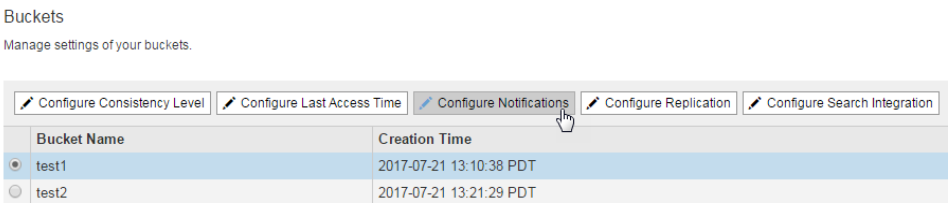
      Cuando configure el código XML, utilice el URN de un endpoint de notificaciones de evento como tema de destino.

      #### Ejemplo

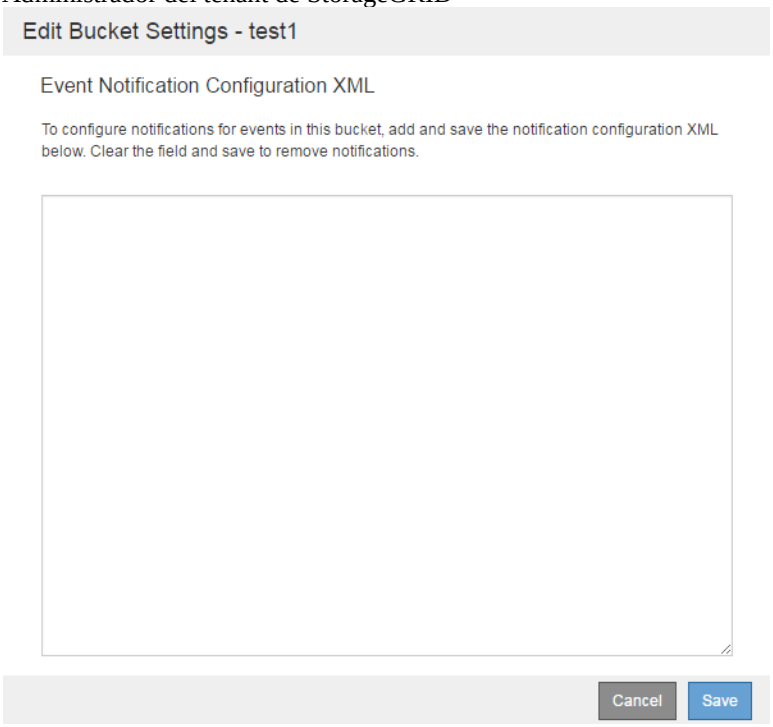
      ```
      <NotificationConfiguration>
        <TopicConfiguration>
           <Id>Image-created</Id>
           <Filter>
              <S3Key>
                <FilterRule>
                  <Name>prefix</Name>
                  <Value>images/</Value>
                </FilterRule>
              </S3Key>
          <Filter>
          <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
          <Event>s3:ObjectCreated:*</Event>
         </TopicConfiguration>
       </NotificationConfiguration>
      ```

   b. En la Interfaz de Administración de tenants vaya a **s3 > Buckets**.

   c. Seleccione el bucket origen y haga clic en **Configure Notifications (Configurar notificaciones)**.

   d. Pegue el código XML de configuración de las notificaciones en el cuadro de texto y haga clic en **Save** (Guardar).



Nota: El empleo de los servicios de plataforma debe haber sido habilitado para cada cuenta tenant por un administrador de StorageGRID Webscale usando la Interfaz de gestión o la API de gestión de la malla. Póngase en contacto con su administrador de malla si se produce un error cuando guarde el Código XML de configuración.

2. Verifique que las notificaciones de evento se han configurado correctamente.

   a. Realice una acción sobre un objeto en el bucket origen que cumpla con los requisitos para activar una configuración tal y como se indica en el Código XML de configuración.

   En el ejemplo mostrado anteriormente, se envía una notificación de evento cuando se crea un objeto con el prefijo "images/",

   b. Confirme que se ha entregado una notificación al tema SNS destino.

Ejemplo


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"111111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"111111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
```

```
    ]
}
```

Por ejemplo, si su tema destino se encuentra alojado en el Servicio Simple de Notificación de AWS, podrá configurar el servicio para enviarle un correo electrónico cuando se entregue la notificación.

Si el tema destino recibe la notificación, habrá configurado adecuadamente su bucket origen para las notificaciones de StorageGRID Webscale.

Conceptos relacionados

Qué son las notificaciones para buckets en la página 46

Tareas relacionadas

Creación de un endpoint utilizando la Interfaz de Administración del tenant en la página 51

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Documentación de los Servicios Web de Amazon (AWS): Configuración de las notificaciones de los Eventos S3 de Amazon

Configuración del servicio de integración de búsqueda para un bucket de S3

Integración de búsqueda es un servicio personalizado de StorageGRID Webscale que envía metadatos de objetos a un índice de búsqueda destino siempre que se cree, elimine o se actualicen los metadatos de un objeto.

> **Atención:** StorageGRID Webscale 11.0 incluye la versión inicial de los servicios de plataforma. La duplicación CloudMirror, las notificaciones y la integración de búsquedas solo resultan apropiadas para determinadas situaciones y cargas de trabajo. Tendrá que ponerse en contacto con su representante de NetApp si desea utilizar la versión inicial de estos servicios.

La integración de búsqueda se configura aplicando el código XML de configuración de StorageGRID Webscale a un bucket. Esta guía documenta el código XML de configuración de notificación de metadatos utilizado para habilitar la integración de búsqueda, los metadatos del objeto que se envían al endpoint de destino y el formato del documento JSON que contiene los metadatos que se crean y envían. También describe el procedimiento para aplicar el código XML de configuración utilizando la Interfaz de Administración del tenant.

Como el servicio de integración de búsqueda envía los metadatos de objeto a un destino, su código XML de configuración se denominada código XML de configuración de la notificación de metadatos. Este código XML de configuración es diferente, e independiente, del código XML de configuración de notificación utilizado para habilitar las notificaciones de eventos.

Consulte la Guía de implementación de S3 en StorageGRID Webscale para obtener más información sobre las API personalizadas de configuración de notificación de metadatos de un bucket en StorageGRID Webscale.

Tareas relacionadas

Empleo de la Interfaz de Administración del tenant para configurar el servicio de integración de búsqueda en la página 62

Referencias relacionadas

Configuración XML para la integración de búsqueda en la página 58
Metadatos de objetos incluidos en las notificaciones de metadatos en la página 61
JSON generados por el servicio de integración de búsqueda en la página 62

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Código XML de configuración para la integración de búsqueda

El servicio de integración de búsqueda se configura utilizando un conjunto de reglas contenidas entre `las etiquetas: <MetadataNotificationConfiguration></MetadataNotificationConfiguration>`. Cada regla especifica los objetos a los que se aplica y el destino donde el sistema StorageGRID Webscale debe enviar los metadatos del objeto.

Los objetos se pueden filtrar utilizando el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos para objetos con el prefijo "\images" a un destino y los metadatos de objetos con el prefijo "/videos" a otro. Aquellas configuraciones que cuenten con prefijos que se superpongan no resultarán válidas y serán rechazadas cuando se envíen. Por ejemplo, no se permitiría una configuración que incluyera una regla para objetos con el prefijo "prueba" y una segunda regla para objetos con el prefijo "prueba2".

Los destinos se deben especificar utilizando el URN de un endpoint de StorageGRID Webscale que haya sido creado para el servicio de integración de búsqueda. Estos endpoints hacen referencia a un índice y al tipo definido sobre un clúster Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-ID:domain/mydomain/myindex/
mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

La tabla mostrada a continuación describe los elementos contenidos en el código XML de configuración de la notificación de metadatos.

Nombre	**Descripción**	**¿Necesario?**
MetadataNotificationConfiguration	Etiqueta contenedor para las reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de Regla.	Sí
Rule (regla)	Etiqueta contenedor para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazarán las reglas que tengan prefijos superpuestos. Incluida en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único para la regla. Incluida en el elemento Rule (regla)	No
Status (estado)	El estado puede ser 'Enabled' o 'Disabled' (Habilitado o Deshabilitado). No se realiza ninguna acción para las reglas que estén deshabilitadas.	Sí
Prefix (Prefijo)	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para coincidir con todos los objetos, especifique un prefijo vacío. Incluida en el elemento Rule (regla)	Sí
Destination (Destino)	Etiqueta contenedor para el destino de una regla. Incluida en el elemento Rule (regla)	Sí

Nombre	Descripción	¿Necesario
Urn	URN de destino donde se envían los metadatos del objeto. Debe ser el URN de un endpoint de StorageGRID Webscale con las siguientes propiedades: • "es" debe ser el tercer elemento. • El URN debe finalizar con el índice y el tipo donde se almacenan los metadatos, en la forma "nombre de dominio / miíndice/ mitipo". Los endpoints se configuran utilizando la Interfaz de Administración de tenants o la API de Administración de tenants. Tienen el siguiente formato: • `arn:aws:es:`*`region`*`:`*`account-ID`*`:domain/`*`mydomain/myindex/mytype`* `urn:mysite:es::: `*`mydomain/myindex/mytype`* El endpoint debe configurarse antes de enviar el código XML de configuración o la configuración fallará produciendo un error 404. La Urn está incluida en el elemento Destination (Destino)	Sí

El código XML de configuración de notificación de metadatos que se muestra puede ayudarle a entender mejor cómo construir su propio código XML.

Configuración de notificación de metadatos que es de aplicación a todos los objetos.

En este ejemplo, se envían al mismo destino los metadatos de objeto para todos los objetos

```
 <MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuración de notificación de metadatos con dos reglas

En este ejemplo, los metadatos de los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos correspondientes a los objetos que coinciden con el prefijo `/videos` se envían a otro destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
```

```
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-domain/
graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-domain/
graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Deshabilitación del servicio de integración de búsqueda de un bucket

Hay dos formas de deshabilitar la integración de búsqueda para un bucket. Si está utilizando directamente el API de S3, podrá utilizar una solicitud de notificación de metadatos de bucket de tipo DELETE tal y como se describe en la Guía de implementación de S3. Si está utilizando la Interfaz de Administración del tenant, podrá acceder a **S3 > Buckets** y simplemente eliminar el Código XML de configuración de la integración de búsqueda.

Tareas relacionadas

Empleo de la Interfaz de Administración del tenant para configurar el servicio de integración de búsqueda en la página 62

Referencias relacionadas

Metadatos de objetos incluidos en las notificaciones de metadatos en la página 61
JSON generados por el servicio de integración de búsqueda en la página 62

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Metadatos de objetos incluidos en notificaciones de metadatos

La tabla siguiente enumera todos los campos que se incluyen en el documento JSON que se envía al endpoint de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bucket, el nombre del objeto y la ID de la versión, si está presente.

Tipo	Nombre del elemento	Descripción
Información del bucket y del objeto	bucket	Nombre del bucket
	key (clave)	Nombre de la clave del objeto
	versionID	Versión del objeto, para los objetos contenidos en buckets con versión
Metadatos del sistema	md5	hash del objeto
	size (tamaño)	Tamaño del objeto (en bytes) tal y como se presenta ante un cliente HTTP
Metadatos de usuario	metadata *key:value (Clave:valor)*	Todos los metadatos de usuario para el objeto, como pares clave-valor

Etiquetas	tags `key:value (Clave:valor)`	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bucket, se genera un documento JSON que se envía al endpoint de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas de un objeto.

El siguiente ejemplo muestra un JSON que podría generarse cuando se crea un objeto con la clave SGWS / Tagging.txt en un bucket llamado "test". El bucket "test" no está versionado, por lo que la etiqueta versionID está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Empleo de la Interfaz de administración del tenant para configurar el servicio de integración de búsqueda

Configurar el servicio de integración de búsqueda para un bucket de S3 permite a la malla enviar metadatos de objetos a un índice Elasticsearch destino. Puede configurar el servicio de integración de búsqueda utilizando la Interfaz de Administración del tenant.

Antes de comenzar

- Previamente ha debido crear un bucket de S3 cuyo contenido desee indexar. Los buckets se crean utilizando la API de S3 en StorageGRID Webscale.
- Un administrador de malla de StorageGRID Webscale debe haber habilitado los servicios de plataforma para su cuenta tenant.
- El endpoint que intente utilizar como destino para el servicio de integración de búsqueda debe existir y debe disponer de su URN.
- Debe pertenecer al grupo de usuarios que tiene los permisos **Administrar todos los contenedores** o **Acceso Raíz**, que le permitirán administrar las opciones para todos los buckets de S3 existentes en su cuenta tenant. Estos permisos sobrescriben las opciones de permisos contenidos en las políticas de grupo o de bucket cuando configure el bucket utilizando la Interfaz de Administración del tenant.

Acerca de esta tarea

Una vez que haya configurado el servicio de integración de búsqueda para un bucket origen, al crear un objeto o actualizar los metadatos o etiquetas del objeto desencadenará el envío de los metadatos del objeto al endpoint de destino. Si habilita el servicio de integración de búsqueda para un bucket que ya contenga objetos, las notificaciones de metadatos no se enviarán automáticamente para los objetos que ya existan. Deberá actualizar dichos objetos ya existentes para garantizar que sus metadatos se añaden al índice de búsqueda de destino.

Pasos

1. Habilitar la integración de búsqueda para su bucket origen:

   a. Utilice un editor de texto para crear el código XML de notificación de metadatos requerido para habilitar la integración de búsqueda.

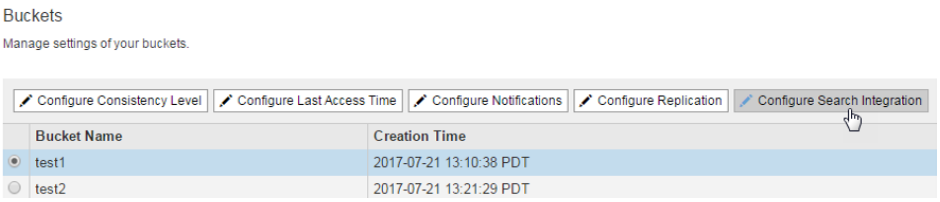
      Consulte “XML de configuración para la integración de búsqueda” si desea obtener más información. Cuando configure el XML, utilice el URN de un endpoint de integración de búsqueda como destino.

Ejemplo

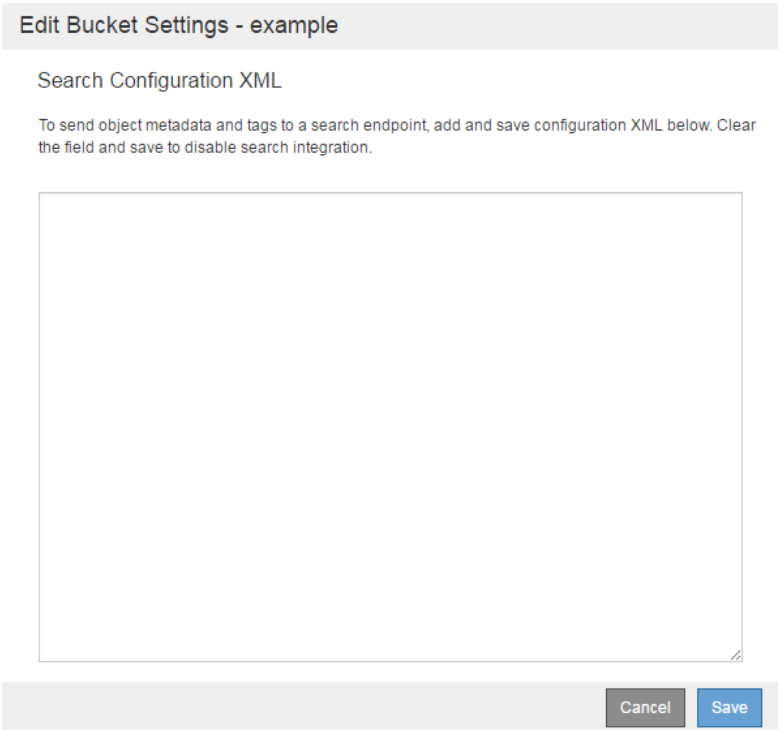
```
<MetadataNotificationConfiguration>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:11111111111111:domain/
mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

b. En la Interfaz de Administración de tenants vaya a **s3 > Buckets**.

c. Seleccione el bucket origen y haga clic en **Configure Search Integration (Configurar Integración de búsqueda)**.



d. Pegue el código XML de configuración de la notificación de metadatos en el cuadro de texto y haga clic en **Save** (Guardar).



Nota: El empleo de los servicios de plataforma debe haber sido habilitado para cada cuenta tenant por un administrador de StorageGRID Webscale usando la Interfaz de gestión o la API de gestión de la malla. Póngase en contacto con su administrador de malla si se produce un error cuando guarde el Código XML de configuración.

2. Verifique que el servicio de integración de búsqueda ha sido configurado correctamente:

a. Añada un objeto al bucket origen que cumpla los requisitos para desencadenar una notificación de metadatos tal y como se especifica en el Código XML de configuración.

   En el ejemplo mostrado anteriormente, todos los objetos añadidos al bucket desencadenan una notificación de metadatos.

b. Confirme que se añade un documento JSON que contiene los metadatos y etiquetas de los objetos al índice de búsqueda especificado en el endpoint.

Habrá configurado su bucket origen para dar soporte al servicio de integración de búsqueda.

Conceptos relacionados

Qué es el servicio de integración de búsqueda en la página 47

Tareas relacionadas

Creación de un endpoint utilizando la Interfaz de Administración del tenant en la página 51

Referencias relacionadas

Configuración de XML para la integración de búsqueda en la página 58.

Información relacionada

Guía de implementación de StorageGRID Webscale 11.0 S3 (Servicio Simple de Almacenamiento)

Glosario

ACL

Lista de control de acceso. Especifica qué usuarios o grupos de usuarios tienen permiso para acceder a un objeto y qué operaciones tienen permitidas, por ejemplo, lectura, escritura y ejecución.

activo, modo de copia de seguridad

Método para enlazar dos puertos físicos por motivos de redundancia. En el modo copia de seguridad-activo solo un puerto se encuentra activo cada vez. Si fallara el puerto que está activo, su puerto de respaldo proporciona automáticamente una conexión a prueba de fallos. Véase también: LACP.

ADC, servicio

Controlador del Dominio Administrativo. El servicio ADC mantiene información sobre la topología, proporciona servicios de autenticación y responde a consultas planteadas desde los servicios LDR, CMN y CLB. El servicio ADC está presente en cada uno de los primeros tres nodos de almacenamiento instalados en un sitio.

ADE

Entorno Distribuido Asíncrono. Entorno de desarrollo propietario utilizado como marco de trabajo para los servicios dentro del sistema StorageGRID Webscale.

Admin, red de

Uno de los tres tipos de redes existentes en un sistema StorageGRID Webscale. La red Admin es una red cerrada utilizada para el mantenimiento y la administración del sistema. La red Admin suele ser una red privada y no necesita ser enrutable entre sitios. La red Admin es opcional. Véase también Cliente, red; Malla, red de.

Admin, nodo de

Uno de los cuatro tipos de nodos de maya existentes en un sistema StorageGRID Webscale. Los nodos Admin proporcionan servicios para la interfaz de usuario, configuración del sistema y registros de auditoría. Véase también; primario, nodo de Admin, API, nodo de pasarela; Archivo, nodo de; Almacenamiento, nodo de.

Amazon s3

Servicio web propietario de Amazon para el almacenamiento y recuperación de datos.

AMS, Servicio

Sistema de administración de auditoría. El servicio AMS supervisa y registra en un archivo de texto de registro todos los eventos auditados del sistema así como las transacciones. El servicio AMS está presente en el nodo Admin.

API, nodos de pasarela

Uno de los cuatro tipos de nodos de maya existentes en un sistema StorageGRID Webscale. El Nodo de pasarela de API proporciona funciones de equilibrado de carga en el sistema StorageGRID Webscale y se utiliza para distribuir la carga de trabajo cuando varias aplicaciones cliente ejecutan operaciones de ingesta y recuperación. Los Nodos de pasarela API incluyen un servicio Connection Load Balancer (CLB). Véase también: Admin, Nodo de, Archivo, Nodo de y Almacenamiento, nodo de.

ARC, servicio

El servicio ARC proporciona la interfaz de administración con la que puede configurar las conexiones para el almacenamiento externo en archivos, como la nube a través de una interfaz de S3 o mediante middleware de TSM. El servicio ARC está presente en el Nodo de archivo.

Archivo, Nodo de

Uno de los cuatro tipos de nodos de maya existentes en un sistema StorageGRID

Webscale. Los Nodos de archivo gestionan el archivado de datos de los objetos en un sistema externo de almacenamiento y archivo. Véase también: Admin, Nodo de, API, Nodo de pasarela y Almacenamiento, nodo de.

auditoría, mensaje de

Información sobre un evento que ha ocurrido en el sistema StorageGRID Webscale y que ha sido capturado y registrado en un archivo.

Base64

Un algoritmo de codificación de datos normalizado que permite convertir los datos de 8 bits en un formato que utiliza un juego de caracteres más pequeño, lo que le permite pasar de forma segura a través de sistemas heredados que pueden procesar solo texto ASCII básico (orden inferior) excluyendo los caracteres de control. Consulte RFC 2045 para ver más detalles.

Bundle

Una colección estructurada de información de configuración utilizada internamente por diversos componentes del sistema StorageGRID Webscale. Los bundles se estructuran en formato contenedor.

Cassandra

Una base de datos de código abierto que es escalable y distribuida, proporciona alta disponibilidad y maneja grandes cantidades de datos entre varios servidores. El sistema StorageGRID Webscale utiliza una base de datos Cassandra para administrar los metadatos de los objetos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proporcionar redundancia y proteger los metadatos de los objetos contra posibles pérdidas. Las copias se cargan equilibradas entre todos los Nodos de almacenamiento en cada sitio.

CBID

Identificador del Bloque de Contenido. Un identificador interno único de una pieza de contenido dentro del sistema StorageGRID Webscale.

CIDR

Enrutamiento entre dominios sin clases. Una notación utilizada para describir de manera compacta una máscara de subred utilizada para definir un rango de direcciones IP. En notación CIDR, la máscara de subred se expresa como una dirección IP en notificación decimal con punto, seguida de una barra invertida y el número de bits existentes en la subred. Por ejemplo: 192.0.2.0/24.

CLB, servicio

Connection Load Balancer (Equilibrador de carga de la conexión). El servicio CLB proporciona una pasarela en el sistema StorageGRID Webscale para las aplicaciones cliente que se conectan mediante HTTP. El servicio CLB forma parte del Nodo de Pasarela de la API

Cliente, red

Uno de los tres tipos de redes existentes en un sistema StorageGRID Webscale. La red cliente es una red abierta utilizada para proporcionar acceso a las aplicaciones cliente, incluyendo S3 y Swift. La red cliente proporciona protocolo cliente para acceder a la malla, por lo que la red Grid (Malla) puede aislarse y protegerse. La red Cliente es opcional. Véase también Admin, red; Malla, red de.

CMN, servicio

Nodo de Administración de Configuración. El servicio CMN gestiona las configuraciones a nivel sistema y las tareas de la malla. Hay un servicio CMN por sistema StorageGRID Webscale. El servicio CMN está presente en el nodo Admin primario.

CMS, servicio

Sistema de Administración de Contenidos. El servicio CMS administra los datos de objetos puestos en cola por el sistema ILM heredado. El servicio CMS está presente en los nodos de Almacenamiento.

instrucción

En HTTP una instrucción en la cabecera de la solicitud tal como GET, HEAD, DELETE, OPTIONS, POST o PUT. También conocido como " método HTTP".

contenedor

Uno de los siguientes:

- Tipo de objeto creado cuando un objeto se divide en segmentos. Un objeto contenedor enumera la información de la cabecera para todos los segmentos del objeto dividido y es utilizado por el servicio LDR para ensamblar el objeto segmentado cuando lo recupera una aplicación cliente. Véase también: segmento contenedor.
- Un mecanismo en la capa de aplicación que empaqueta juntos el código y las dependencias. Varios contenedores pueden ejecutarse como procesos aislados en la misma máquina. El software en contenedores opera de forma coherente en todos los entornos.

contenido, ID del bloque de

Véase CBID.

contenido, asa del

Véase UUID.

CSTR

Cadena de longitud variable terminada en Null.

DC

Sede del Centro de datos

DDS, Servicio

Almacén distribuido de datos alojado en un Nodo de Almacenamiento, el servicio de Almacén Distribuido de Datos (DDS) presenta una interfaz con la base de datos Cassandra para administrar los metadatos de los objetos.

distribuida, almacén de valor de clave

Es la base de datos Cassandra utilizada para almacenar metadatos de objetos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proporcionar redundancia y proteger los metadatos de los objetos de posibles pérdidas. Las copias se cargan equilibradas entre todos los Nodos de almacenamiento en cada sitio. Véase también: Cassandra.

DNS

Sistema de Nombres de Dominio.

borrado, código de

Método utilizado por StorageGRID Webscale para almacenar datos de objeto. Cuando StorageGRID Webscale hace coincidir los objetos con una regla de ILM que está configurada para crear copias codificadas con borrado, divide los datos del objeto en fragmentos de datos, calcula otros fragmentos de paridad y almacena cada fragmento en un Nodo de almacenamiento diferente. Cuando se accede a un objeto, la aplicación reensambla el objeto utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompe o se pierde, el algoritmo de codificación de borrado puede recrear dicho fragmento utilizando los datos restantes y los fragmentos de paridad. Véase también: duplicación.

borrado, esquema de codificación de

Método utilizado para controlar cuántos fragmentos de datos y cuántos fragmentos de paridad se crean para un objeto codificado para borrado. Los esquemas de codificación de borrado disponibles dependerán de cuántos Nodos de almacenamiento y sitios forman el grupo de almacenamiento que desea utilizar.

Fibra, canal de

Una tecnología de interconexión utilizada principalmente para almacenamiento.

Malla, Interfaz de gestión de la

La interfaz basada en explorador utilizada para supervisar, configurar y administrar un sistema StorageGRID Webscale.

Malla, red de

Uno de los tres tipos de redes existentes en un sistema StorageGRID Webscale. La red de malla se utiliza para todo el tráfico interno de StorageGRID Webscale. Proporciona conectividad entre todos los nodos existentes en la malla, entre todos los sitios y subredes. Se requiere la red de Malla. Véase también Admin, redy Cliente, red.

malla, nodo de la

El bloque de construcción básico del software para el sistema StorageGRID Webscale, por ejemplo, Nodo Admin o Nodo de Almacenamiento. Cada tipo de nodo de malla consta de un conjunto de servicios que realizan un grupo especializado de tareas.

malla, tarea de la

Scripts de todo el sistema utilizados para desencadenar diversas acciones que implementan cambios específicos en el sistema StorageGRID Webscale.

ILM

Administración del Ciclo de vida de la Información. Un proceso de gestión de la ubicación y duración del almacenamiento del contenido en función del valor del contenido, del coste de almacenamiento, del acceso al rendimiento, del cumplimiento normativo y de otros factores. Véase también: borrado, codificación de; duplicación, y almacenamiento, grupo de.

LACP

Protocolo de Control de Agregación de Enlace. También conocido como IEEE 802.3ad. Método para enlazar dos puertos físicos por motivos de redundancia para formar un único canal lógico, que permite un rendimiento superior. Si un puerto falla, el otro puerto proporciona una conexión a prueba de fallos. Se reduce el rendimiento pero la conectividad no se pierde. Véase también: activo, modo de copia de seguridad.

LAN

Red de Área Local. Una red de ordenadores interconectados que se encuentra limitado a un área pequeña, tal como un edificio o un campus. Una LAN se puede considerar como un nodo en Internet o de una red de área amplia.

latencia

Tiempo de duración del proceso de una transacción o para transmitir una unidad de datos de extremo a extremo. Cuando se evalúa el rendimiento del sistema, se deberán analizar el rendimiento y la latencia. Véase también: rendimiento.

LDR, servicio

Enrutador Local de Distribución. El servicio LDR administra el almacenamiento y transfiere el contenido dentro del sistema StorageGRID Webscale. El servicio LDR está presente en los nodos de Almacenamiento.

Linux

Cualquiera de las plataformas Linux compatibles para los despliegues de StorageGRID Webscale, incluyendo Red Hat Enterprise Linux, Ubuntu, CentOS y Debian.

LUN

Véase: Objetos, almacenamiento de.

mDNS

Sistema de Nombres de Dominio Multidifusión. Sistema que resuelve direcciones IP en una pequeña red cuando todavía no se ha instalado un servidor DNS.

metadatos

Información relacionada o que describe un objeto almacenado en el sistema StorageGRID Webscale. Por ejemplo, hora de la ingesta.

MLAG

Grupo de Agregación de Enlace Multi-Chasis. Un tipo de grupo de agregación de enlaces que utiliza dos (y en ocasiones más) conmutadores para proporcionar redundancia en caso de que uno de los conmutadores falle.

MTU

Unidad de Transmisión Máxima. El paquete o marco de mayor tamaño que se puede enviar en cualquier transmisión.

nombres, espacio de

Un conjunto cuyos elementos son nombres únicos. No existe garantía de que un nombre perteneciente a un espacio de nombres no se repita en otro espacio de nombres.

nearline (casi en línea)

Un término que describe el almacenamiento de datos que no es "online" (lo que implica que está instantáneamente disponible, cómo un disco giratorio) ni "offline" (en donde se incluyen los medios de almacenamiento fuera del sitio). Un ejemplo de ubicación de almacenamiento de datos nearline es una cinta que está cargada en una biblioteca de cintas, pero que no está montada.

NFS

Sistema de archivos de red. Un protocolo que permite el acceso a los archivos de red como si estuvieran almacenados en discos locales.

NMS, servicio

Sistema de Administración de Red. El servicio NMS activa las opciones de supervisión, informes y configuración que se muestran a través de la Interfaz de gestión de la malla del sistema StorageGRID Webscale. El servicio AMS está presente en los nodos Admin. Véase también: Admin, nodo de.

nodo, ID del

Un número de identificación asignado a un servicio en el sistema StorageGRID Webscale. Cada servicio (tal como un servicio NMS o un servicio ADC) debe tener un ID único de nodo. El número se ajusta durante la configuración del sistema y se une a certificados de autenticación.

NTP

Protocolo de Tiempo de Red. Protocolo utilizado para sincronizar relojes distribuidos sobre una red de latencia variable, tal como Internet.

Objeto

Una construcción artificial que divide el contenido entre datos y metadatos. Los datos son la sustancia del objeto, por ejemplo los datos de imagen, registros médicos o archivos de audio que desea almacenar. Los metadatos describen al objeto y se utilizan para clasificar e identificar a los datos del objeto.

Objeto, segmentación del

Un proceso de StorageGRID Webscale que divide a los objetos de gran tamaño en un conjunto de objetos más pequeños (segmentos) y crea un contenedor de segmentos para rastrear la colección. El contenedor del segmento contiene el UUID para la recopilación de los objetos pequeños así como información de la cabecera para cada uno de los objetos pequeños contenidos en la colección. Todos los objetos pequeños de la colección tienen el mismo tamaño. Véase también: segmento contenedor.

objetos, almacenamiento de

Un enfoque de almacenamiento de datos donde se accede a los datos mediante identificadores únicos y no por una jerarquía de directorios y archivos definida por el usuario. Cada objeto cuenta con datos (por ejemplo, una imagen) y metadatos (por ejemplo, la fecha en que se capturó la imagen). Las operaciones de almacenamiento de objetos actúan sobre objetos completos a diferencia de lo que sucede con la lectura y escritura de bytes como suele suceder con los archivos y se proporcionan mediante API o HTTP en lugar de NAS (CIFS/NFS) o protocolos de bloque (iSCSI/ FC/FCOE).

objetos, almacén de

Un sistema de archivos configurados en un volumen de disco. La configuración incluye una estructura y recursos específicos de directorios que se inician durante la instalación del sistema.

OID

Identificador del objeto. El identificador único de un objeto.

plataforma, servicios de

Servicios de StorageGRID Webscale que permiten a una cuenta tenant configurar sus buckets de S3 para potenciar los servicios externos, ampliando la funcionalidad de StorageGRID Webscale. Por ejemplo, un tenant puede configurar el servicio de duplicación de CloudMirror para habilitar la duplicación automática de los objetos a un bucket remoto de S3.

primario, nodo de Admin

El nodo de Admin que aloja el servicio CMN. Cada sistema StorageGRID Webscale dispone solo de un Nodo de Admin primario. Véase también: Admin, nodo de.

aprovisionamiento

El proceso de generar un Paquete de recuperación nuevo o actualizado.

quorum

Una mayoría simple: 50% + 1. Cierta funcionalidad del sistema requiere un quorum del número total de un tipo particular de servicio.

Recuperación, paquete de

Archivo `.zip` que contiene archivos y software específicos del despliegue necesario para instalar, expandir, actualizar y mantener un sistema StorageGRID Webscale. El paquete también contiene información de integración y configuración específica del sistema, incluyendo nombres del host del servidor y direcciones IP, y contraseñas altamente confidenciales que se necesitan durante el mantenimiento, actualización y expansión del sistema.

duplicación

Métodos utilizados por StorageGRID Webscale para almacenar datos de un objeto. Cuando StorageGRID Webscale ajusta objetos a una regla ILM que se ha configurado para crear copias duplicadas, el sistema crea copias exactas de los datos de un objeto y almacena las copias en diferentes Nodos de Almacenamiento o Nodos de Archivo. Véase también: borrado, código de.

SATA

Conexión Avanzada de Tecnología Serie. Una tecnología de conexión utilizada para conectar un servidor y dispositivos de almacenamiento.

SCSI

Interfaz de Sistemas Informáticos Pequeños. Una tecnología de conexión utilizada para conectar servidores y dispositivos periféricos, tales como sistemas de almacenamiento.

segmento contenedor

Un objeto creado por el sistema StorageGRID Webscale durante el proceso de segmentación. La segmentación de objetos divide a los objetos de gran tamaño en un conjunto de objetos más pequeños (segmentos) y crea un contenedor de segmentos para rastrear la colección. Un contenedor del segmento contiene el UUID para la recopilación de los objetos segmentados así como información de cabecera para cada uno de los objetos pequeños contenidos en la colección. Cuando se ensamblan, el conjunto de segmentos vuelve a crear el objeto original. Véase también: objetos, segmentación de.

servidor

Término utilizado específicamente para referirse al hardware. También se puede referir a una máquina virtual.

servicio

Una unidad del sistema StorageGRID Webscale, tal como el servicio ADC, servicio NMS o el servicio SSM. Cada servicio realiza tareas críticas únicas para el funcionamiento normal de un sistema StorageGRID Webscale.

Sitio SSh **Ssh**

Un centro de datos donde se almacenan objetos. Los sitios se definen cuando se despliegan los nodos de la malla de StorageGRID Webscale durante la instalación o en

una ampliación. Cada sitio es un grupo lógico de los nodos Storage

ageGRID Webscale que se co-ubican geográficamente o se agrupan de alguna forma para proporcionar tolerancia a fallos.

Segura, shell. Una shell de UNIX y los protocolos de soporte utilizados para registrar en un ordenador remoto y ejecutar instrucciones sobre un canal autenticado y cifrado.

SSL

Capa de Conexión Segura. El protocolo criptográfico original utilizado para habilitar comunicaciones seguras a través de Internet. Véase también: TLS.

SSM, servicio

Monitor del estado del servidor. Un componente del software StorageGRID Webscale que supervisa el estado del hardware e informa al servicio NMS. Cada nodo de la malla ejecuta una instancia del servicio SSM.

Almacenamiento, nodo de

Uno de los cuatro tipos de nodos de maya existentes en un sistema StorageGRID Webscale. Los nodos de almacenamiento proporcionan capacidad y servicios de almacenamiento para almacenar, mover, verificar y recuperar objetos que se encuentran almacenados en discos. Los nodos de almacenamiento se pueden alojar en máquinas virtuales o asociadas con la aplicación StorageGRID Webscale. Véase también: Admin, Nodo de, API, Nodo de pasarela y Archivo, nodo de.

almacenamiento, grupo de

El elemento de una regla ILM que determina el lugar de almacenamiento de las copias duplicadas de un objeto. Véase también: duplicación.

almacenamiento, volumen de

Véase Objetos, almacenamiento de

StorageGRID

Marca registrada de NetApp, Inc., utilizada para un sistema de software y su arquitectura de malla de almacenamiento de objetos.

TCP/IP

Protocolo de Control de Transmisión / Protocolo de Internet. Proceso de encapsulado y transmisión de paquetes de datos a través de la red. Incluye un reconocimiento positivo de las transmisiones.

rendimiento

La cantidad de datos que se pueden transmitir o el número de transacciones que puede procesar un sistema o subsistema en un periodo de tiempo dado. Véase también: latencia.

Tivoli, Administrador de almacenamiento

Producto de almacenamiento de IBM que gestiona el almacenamiento y la recuperación de datos desde recursos de almacenamiento extraíbles.

TLS

Seguridad de la Capa de Transporte. Un protocolo criptográfico utilizado para habilitar comunicaciones seguras a través de Internet. Consulte RFC 2246 para ver más detalles.

URI

Identificador Universal de Recursos. Un conjunto genérico de todos los nombres o direcciones utilizados para hacer referencia a recursos a los que se les puede dar servicio desde un sistema informático. Estas direcciones se representan como cadenas de texto cortas.

URN

Nombre Universal de Recurso. Un URI que utiliza un formato específico descrito por RFC 8141. Los URN se definen para ser globalmente únicos dentro de un espacio de nombres definido y no especifica el protocolo de acceso o la ubicación del recurso.

UTC

Abreviatura internacional independiente del idioma que hace referencia a la hora estándar común de cualquier lugar del mundo.

UUID

Identificador Único Universal. Identificador único para cada pieza de contenido en el sistema StorageGRID Webscale. UUID proporciona a las aplicaciones cliente un gestor de contenidos que les permite acceder a los contenidos en una forma que no interfiere con la administración del sistema StorageGRID Webscale del mismo contenido. Número de 128 bits que tiene la garantía de ser único. Consulte RFC 4122 para ver más detalles.

virtual, máquina (VM)

Una plataforma de software que permite la instalación de un sistema operativo y de software, sustituye a un servidor físico y permite compartir los recursos de un servidor físico entre varios servidores virtuales.

VLAN

Red de Área Local virtual (o LAN virtual). Grupo de dispositivos que se encuentran ubicados en diferentes segmentos de LAN pero que están configurados para comunicarse como si estuvieran unidos al mismo conmutador de red.

WAN

Red de Área Amplia. Una red de ordenadores interconectados que abarca una gran área geográfica, tal como un país.

XFS

Sistema de archivos escalable y de alto rendimiento.

XML

Lenguaje de Marcado Extensible. Un formato de texto para la representación extensible de información estructurada; clasificada según su tipo y gestionada como si fuera una base de datos. XML cuenta con la ventaja de que se puede verificar, es legible por el ser humano y fácilmente intercambiable entre distintos sistemas.

Información del copyright

Información de marca comercial

Cómo enviar comentarios sobre la documentación y recibir notificaciones de actualización

Puede ayudarnos a mejorar la calidad de nuestra documentación enviándonos sus comentarios. Puede recibir notificaciones automáticas cuando se libere inicialmente la documentación del nivel de producción (GA / FCS) o cuando se realicen cambios importantes en los documentos de nivel de producción existentes.

Si tiene sugerencias para mejorar este documento, envíenos sus comentarios por correo electrónico.

doccomments@netapp.com

Para ayudarnos a dirigir sus comentarios al departamento correcto, incluya en el asunto el nombre del producto, la versión y el sistema operativo.

Si desea que se le notifique automáticamente cuando se edite la documentación del nivel de producción o cuando se realicen cambios importantes en los documentos de nivel de producción existentes, siga la cuenta de Twitter @NetAppDoc.

También puede ponerse en contacto con nosotros de las siguientes maneras:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Teléfono: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Teléfono de soporte: +1 (888) 463-8277

Índice

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

W