Use Swift

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

Use Swift

Use Swift: Descripción general

Las aplicaciones cliente pueden usar la API Swift de OpenStack para interactuar con el sistema StorageGRID.

StorageGRID admite las siguientes versiones específicas de Swift y HTTP.

Elemento	Versión
Especificación Swift	OpenStack Swift Object Storage API v1 a fecha de noviembre de 2015
HTTP	1.1 para obtener más información acerca de HTTP, consulte HTTP/1.1 (RFC 7230-35). **Nota**: StorageGRID no admite canalización HTTP/1.1.

Información relacionada

"OpenStack: API de almacenamiento de objetos"

Historial de soporte de la API de Swift en StorageGRID

Debe estar al tanto de los cambios en la compatibilidad del sistema StorageGRID con la API DE REST de Swift.

Liberar	Comentarios
11.6	Cambios editoriales menores.
11.5	Se ha eliminado el control de consistencia débil. En su lugar, se utilizará el nivel de consistencia disponible.
11.4	Se ha agregado compatibilidad con TLS 1.3 y se ha actualizado la lista de conjuntos de cifrado TLS compatibles. CLB está en desuso. Se añadió la descripción de la relación entre ILM y la configuración de consistencia.

Liberar	Comentarios
11.3	Las operaciones de PUT Object actualizadas para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento (las opciones equilibradas y estrictas del comportamiento de procesamiento). Se ha agregado una descripción de las conexiones de cliente que utilizan extremos de equilibrador de carga o grupos de alta disponibilidad. Lista actualizada de conjuntos de cifrado TLS admitidos. Ya no se admiten los cifrados TLS 1.1.
11.2	Cambios editoriales menores en el documento.
11.1	Se añadió compatibilidad con el uso de HTTP para conexiones de clientes Swift a los nodos de grid. Se han actualizado las definiciones de controles de coherencia.
11.0	Se ha agregado soporte para 1,000 contenedores por cada cuenta de inquilino.
10.3	Actualizaciones administrativas y correcciones en el documento. Se han eliminado secciones para configurar certificados de servidor personalizados.
10.2	Soporte inicial de la API Swift por el sistema StorageGRID. La versión compatible actualmente es la API de almacenamiento de objetos Swift de OpenStack v1.

Cómo StorageGRID implementa la API DE REST de Swift

Una aplicación cliente puede usar llamadas API DE REST de Swift para conectarse a nodos de almacenamiento y nodos de puerta de enlace para crear contenedores, así como para almacenar y recuperar objetos. De este modo, las aplicaciones orientadas a los servicios desarrolladas para OpenStack Swift pueden conectarse con el almacenamiento de objetos en las instalaciones que proporciona el sistema StorageGRID.

Gestión de objetos Swift

Una vez que se han ingerido objetos Swift en el sistema StorageGRID, se gestionan con las reglas de gestión de ciclo de vida de la información (ILM) de la política de ILM activa del sistema. Las reglas y políticas de ILM determinan la manera en que StorageGRID crea y distribuye copias de datos de objetos y la manera en que las administra. Por ejemplo, una regla de ILM puede aplicarse a los objetos en contenedores Swift específicos y puede especificar que se guarden varias copias de objetos en varios centros de datos durante un determinado número de años.

Póngase en contacto con su administrador de StorageGRID si necesita comprender cómo las políticas y las

reglas de ILM de la cuadrícula afectarán a los objetos de la cuenta de inquilino de Swift.

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de Swift inician una operación.

Garantías y controles de coherencia

De forma predeterminada, StorageGRID proporciona coherencia de lectura tras escritura para los objetos recién creados y coherencia eventual para las actualizaciones de objetos y operaciones DE CABECERA. Cualquier OBTENER después de un PUESTO completado correctamente podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

StorageGRID también le permite controlar la coherencia de cada contenedor. Puede cambiar el control de coherencia para proporcionar un equilibrio entre la disponibilidad de los objetos y la coherencia de esos objetos en diferentes nodos de almacenamiento y sitios, según lo requiera la aplicación.

Información relacionada

Gestión de objetos con ILM

OBTENGA la solicitud de consistencia del contenedor

PONGA la solicitud de consistencia del contenedor

Recomendaciones para implementar la API DE REST de Swift

Debe seguir estas recomendaciones al implementar la API DE REST de Swift para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe utilizar el control de consistencia "'disponible'". Por ejemplo, debe utilizar el control de coherencia "'disponible'" si la aplicación realiza una OPERACIÓN HEAD a una ubicación antes de realizar una operación PUT en esa ubicación.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba un número elevado de 500 errores internos de Server si uno o más nodos de almacenamiento no están disponibles.

Puede establecer el control de coherencia "'disponible'" para cada contenedor utilizando la solicitud DE consistencia DEL contenedor PUT.

Recomendaciones para los nombres de objetos

En el caso de los contenedores creados en StorageGRID 11.4 o posteriores, ya no es necesario restringir los nombres de objetos para cumplir con las prácticas recomendadas de rendimiento. Por ejemplo, ahora puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de objetos.

Para los contenedores que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas

recomendaciones para los nombres de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de nombres de objetos. Esto contrasta con la anterior recomendación de AWS para prefijos de nombres. En su lugar, debe utilizar prefijos no aleatorios y no únicos, como `image`.
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en prefijos de nombre, debe aplicar un prefijo a los nombres de objeto con un nombre de directorio. Es decir, utilice este formato:

  ```
  mycontainer/mydir/f8e3-image3132.jpg
  ```

  En lugar de este formato:

  ```
  mycontainer/f8e3-image3132.jpg
  ```

Recomendaciones para «lecturas de rango»

Si se selecciona la opción **Compress Stored Objects** (**CONFIGURATION** > **System** > **Grid options**), las aplicaciones cliente Swift deberían evitar realizar operaciones GET object que especifiquen un intervalo de bytes. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es muy ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Información relacionada

OBTENGA la solicitud de consistencia del contenedor

PONGA la solicitud de consistencia del contenedor

Administre StorageGRID

Configure las conexiones y las cuentas de inquilino

Para configurar StorageGRID para aceptar conexiones desde aplicaciones cliente, es necesario crear una o más cuentas de inquilino y configurar las conexiones.

Cree y configure cuentas de inquilino de Swift

Se requiere una cuenta de inquilino de Swift para que los clientes de la API de Swift puedan almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios, y contenedores y objetos.

Las cuentas de inquilino de Swift las crea un administrador de grid de StorageGRID mediante Grid Manager o

la API de gestión de grid.

Al crear una cuenta de inquilino de Swift, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del inquilino (el ID de cuenta del inquilino se asigna automáticamente y no se puede cambiar)
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.
- Si SSO está habilitado, qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

Después de crear una cuenta de inquilino de Swift, los usuarios con permiso de acceso raíz pueden acceder al Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento

> Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Información relacionada

Administre StorageGRID

Usar cuenta de inquilino

Extremos de API de Swift compatibles

Cómo se pueden configurar las conexiones de clientes

Un administrador de grid toma opciones de configuración que afectan a la forma en que los clientes de Swift se conectan a StorageGRID para almacenar y recuperar los datos. La información específica que necesita para realizar una conexión depende de la configuración elegida.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad

> El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Al configurar StorageGRID, un administrador de grid puede utilizar Grid Manager o la API de gestión de grid para realizar los siguientes pasos, todos ellos opcionales:

1. Configure los extremos para el servicio Load Balancer.

   Debe configurar los extremos para usar el servicio Load Balancer. El servicio Load Balancer en los nodos de administrador o de puerta de enlace distribuye conexiones de red entrantes desde aplicaciones cliente hasta los nodos de almacenamiento. Al crear un extremo de equilibrio de carga, el administrador de StorageGRID especifica un número de puerto, tanto si el extremo acepta conexiones HTTP o HTTPS, como el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).

2. Configure redes de cliente no fiables.

   Si un administrador de StorageGRID configura la red cliente de un nodo para que no sea de confianza, el nodo sólo acepta conexiones entrantes en la red cliente en puertos que se configuran explícitamente como extremos equilibradores de carga.

3. Configuración de grupos de alta disponibilidad.

   Si un administrador crea un grupo de alta disponibilidad, las interfaces de red de varios nodos de administrador o nodos de puerta de enlace se colocan en una configuración de backup activo. Las conexiones de clientes se realizan mediante la dirección IP virtual del grupo de alta disponibilidad.

Para obtener más información acerca de cada opción, consulte las instrucciones para administrar StorageGRID.

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente se conectan a StorageGRID mediante la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Información necesaria para realizar conexiones de cliente

La tabla resume las distintas maneras en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Póngase en contacto con el administrador de StorageGRID para obtener más información o consulte las instrucciones para administrar StorageGRID para obtener una descripción de cómo encontrar esta información en el administrador de grid.

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo de ALTA DISPONIBILIDAD	Equilibrador de carga	La dirección IP virtual de un grupo de alta disponibilidad	• Puerto de punto final del equilibrador de carga

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo de ALTA DISPONIBILIDAD	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos Swift predeterminados: • HTTPS: 8083 • HTTP: 8085
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace **Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos Swift predeterminados: • HTTPS: 8083 • HTTP: 8085
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos Swift predeterminados: • HTTPS: 18083 • HTTP: 18085

Ejemplo

Para conectar un cliente Swift al extremo Load Balancer de un grupo de ha de nodos de Gateway, utilice una URL estructurada como se muestra a continuación:

- `https://`*`VIP-of-HA-group:LB-endpoint-port`*

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a StorageGRID. Póngase en contacto con el administrador de red local.

Decidir usar conexiones HTTPS o HTTP

Cuando se realizan conexiones de cliente mediante un extremo de equilibrio de carga, es necesario realizar conexiones mediante el protocolo (HTTP o HTTPS) especificado para ese extremo. Para utilizar HTTP para

las conexiones de clientes a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, debe habilitar su uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando la opción de cuadrícula **Activar conexión HTTP** en el Administrador de grid. Por ejemplo, una aplicación cliente puede utilizar HTTP al probar la conexión a un nodo de almacenamiento en un entorno no de producción.

> Tenga cuidado al habilitar HTTP para una cuadrícula de producción, ya que las solicitudes se enviarán sin cifrar.

> El servicio CLB está obsoleto.

Si se selecciona la opción **Activar conexión HTTP**, los clientes deben utilizar puertos diferentes para HTTP que los que utilizan para HTTPS. Consulte las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Pruebe la conexión en la configuración de la API de Swift

Puede usar la interfaz de línea de comandos de Swift para probar la conexión con el sistema StorageGRID y verificar que puede leer y escribir objetos en el sistema.

Lo que necesitará

- Debe haber descargado e instalado python-swiftclient, el cliente de línea de comandos de Swift.

  "SwiftStack: python-swiftclient"

- Debe tener una cuenta de inquilino de Swift en el sistema StorageGRID.

Acerca de esta tarea

Si no ha configurado la seguridad, debe añadir el `--insecure` marque cada uno de estos comandos.

Pasos

1. Consulte la URL de información para la implementación de Swift de StorageGRID:

   ```
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/info
   capabilities
   ```

   Esto es suficiente para probar que la implementación de Swift es funcional. Para seguir probando la configuración de la cuenta almacenando un objeto, continúe con los pasos adicionales.

2. Coloque un objeto en el contenedor:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Obtenga el contenedor para verificar el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Elimine el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Elimine el contenedor:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Información relacionada

Cree y configure cuentas de inquilino de Swift

Configure la seguridad de la API de REST

Operaciones compatibles con la API REST de Swift

El sistema StorageGRID admite la mayoría de operaciones en la API Swift de OpenStack. Antes de integrar clientes API DE REST de Swift con StorageGRID, revise los detalles de la implementación para las operaciones de la cuenta, el contenedor y el

objeto.

Operaciones compatibles con StorageGRID

Se admiten las siguientes operaciones de API de Swift:

- Operaciones de cuentas
- Operaciones de contenedor
- Operaciones de objeto

Encabezados de respuesta comunes para todas las operaciones

El sistema StorageGRID implementa todos los encabezados comunes para las operaciones compatibles según lo definido por la API de almacenamiento de objetos Swift de OpenStack v1.

Información relacionada

"OpenStack: API de almacenamiento de objetos"

Extremos de API de Swift compatibles

StorageGRID admite los siguientes extremos de la API de Swift: La URL de la información, la URL de autenticación y la URL de almacenamiento.

URL de información

Puede determinar las capacidades y las limitaciones de la implementación de Swift de StorageGRID emitiendo una solicitud GET a la URL de la base de Swift con la ruta /info.

```
https://FQDN | Node IP:Swift Port/info/
```

En la solicitud:

- *`FQDN`* es el nombre de dominio completo.
- *`Node IP`* Es la dirección IP del nodo de almacenamiento o del nodo de puerta de enlace en la red de StorageGRID.
- *`Swift Port`* Es el número de puerto que se usa para las conexiones API de Swift en el nodo de almacenamiento o la puerta de enlace.

Por ejemplo, la siguiente URL de información solicita información desde un nodo de almacenamiento con la dirección IP 10.99.106.103 y mediante el puerto 18083.

```
https://10.99.106.103:18083/info/
```

La respuesta incluye las capacidades de la implementación Swift como diccionario JSON. Una herramienta cliente puede analizar la respuesta JSON para determinar las capacidades de la implementación y usarlas como restricciones para operaciones de almacenamiento subsiguientes.

La implementación de StorageGRID de Swift permite un acceso sin autenticar a la URL de información.

URL de autenticación

Un cliente puede utilizar la URL de autenticación de Swift para autenticarse como usuario de cuenta de inquilino.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Se deben proporcionar el ID de cuenta de inquilino, el nombre de usuario y la contraseña como parámetros en el `X-Auth-User` y.. `X-Auth-Key` solicite los encabezados de la siguiente manera:

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

En los encabezados de la solicitud:

- *`Tenant_Account_ID`* Es el ID de cuenta que asigna StorageGRID cuando se creó el inquilino de Swift. Este es el mismo ID de cuenta de arrendatario que se utiliza en la página de inicio de sesión de Gestor de inquilinos.
- *`Username`* Es el nombre de un usuario arrendatario que se ha creado en el Administrador de arrendatarios. Este usuario debe pertenecer a un grupo con permiso de administrador de Swift. No se puede configurar el usuario raíz del inquilino para usar la API DE REST de Swift.

  Si la Federación de identidades está habilitada para la cuenta de inquilino, proporcione el nombre de usuario y la contraseña del usuario federado desde el servidor LDAP. Como alternativa, proporcione el nombre de dominio del usuario LDAP. Por ejemplo:

  `X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *`Password`* es la contraseña del usuario inquilino. Las contraseñas de usuario se crean y administran en el Administrador de inquilinos.

La respuesta a una solicitud de autenticación correcta devuelve una URL de almacenamiento y un token de autenticación, de la siguiente forma:

`X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID`

`X-Auth-Token: token`

`X-Storage-Token: token`

De forma predeterminada, el token es válido durante 24 horas desde el tiempo de generación.

Se generan tokens para una cuenta de arrendatario específica. Un token válido para una cuenta no autoriza a un usuario a acceder a otra cuenta.

URL de almacenamiento

Una aplicación cliente puede emitir llamadas a la API DE REST de Swift para realizar operaciones de cuenta, contenedor y objeto admitidas contra un nodo de puerta de enlace o un nodo de almacenamiento. Las solicitudes de almacenamiento se dirigen a la URL de almacenamiento que se devuelve en la respuesta de autenticación. La solicitud también debe incluir el encabezado X-Auth-Token y el valor devuelto por la solicitud auth.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Es posible que algunos encabezados de respuesta del almacenamiento que contienen estadísticas de uso no reflejen números precisos de los objetos modificados recientemente. Puede que en estos encabezados se deban utilizar unos minutos para que aparezcan números precisos.

Los siguientes encabezados de respuesta para las operaciones de cuentas y contenedores son ejemplos de los que contienen estadísticas de uso:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Información relacionada

Configure las conexiones y las cuentas de inquilino

Operaciones de cuentas

Operaciones de contenedor

Operaciones de objeto

Operaciones de cuentas

Las siguientes operaciones de la API de Swift se realizan en las cuentas.

OBTENGA la cuenta

Esta operación recupera la lista de contenedores asociada a las estadísticas de uso de la cuenta y la cuenta.

Se requiere el siguiente parámetro request:

- `Account`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`

- `Marker`
- `Prefix`

Una ejecución satisfactoria devuelve los siguientes encabezados con una respuesta «'HTTP/1.1 204 sin contenido» si se encuentra la cuenta y no tiene contenedores o la lista de contenedores está vacía; o una respuesta «'HTTP/1.1 200 OK'» si se encuentra la cuenta y la lista de contenedores no está vacía:

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

CUENTA principal

Esta operación recupera información de la cuenta y estadísticas de una cuenta de Swift.

Se requiere el siguiente parámetro request:

- `Account`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución satisfactoria devuelve los encabezados siguientes con una respuesta «'HTTP/1.1 204 sin contenido»:

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Información relacionada

Supervisar y auditar operaciones

Operaciones de contenedor

StorageGRID admite un máximo de 1,000 contenedores por cuenta de Swift. Las siguientes operaciones de la API de Swift se realizan en contenedores.

ELIMINAR contenedor

Esta operación elimina un contenedor vacío de una cuenta de Swift en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

OBTENGA el contenedor

Esta operación recupera la lista de objetos asociada con el contenedor junto con las estadísticas y los metadatos del contenedor en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`

- `Path`
- `Prefix`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 Success" o "HTTP/1.1 204 sin contenido":

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Contenedor DE LA CABEZA

Esta operación recupera las estadísticas y los metadatos del contenedor de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE el contenedor

Esta operación crea un contenedor para una cuenta en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado" o "HTTP/1.1 202 aceptado" (si el contenedor ya existe bajo esta cuenta):

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Un nombre de contenedor debe ser único en el espacio de nombres de StorageGRID. Si el contenedor existe en otra cuenta, se devuelve el siguiente encabezado: "Conflicto HTTP/1.1 409".

Información relacionada

Supervisar y auditar operaciones

Operaciones de objeto

Las siguientes operaciones de la API de Swift se realizan en objetos.

ELIMINAR objeto

Esta operación elimina los metadatos y el contenido de un objeto del sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los encabezados de respuesta siguientes con un `HTTP/1.1 204 No Content` respuesta:

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Al procesar una solicitud DE ELIMINACIÓN de objeto, StorageGRID intenta eliminar inmediatamente todas las

copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en un plazo de 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente.

Para obtener más información sobre cómo eliminar objetos, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

OBJETO GET

Esta operación recupera el contenido de objetos y obtiene los metadatos de objetos de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes encabezados de solicitud son opcionales:

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Una ejecución correcta devuelve los encabezados siguientes con un `HTTP/1.1 200 OK` respuesta:

- `Accept-Ranges`
- `Content-Disposition`, devuelto sólo si `Content-Disposition` se establecieron los metadatos
- `Content-Encoding`, devuelto sólo si `Content-Encoding` se establecieron los metadatos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

OBJETO HEAD

Esta operación recupera los metadatos y las propiedades de un objeto ingerido desde un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 OK":

- `Accept-Ranges`
- `Content-Disposition`, devuelto sólo si `Content-Disposition` se establecieron los metadatos
- `Content-Encoding`, devuelto sólo si `Content-Encoding` se establecieron los metadatos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

PONER objeto

Esta operación crea un objeto nuevo con datos y metadatos, o reemplaza un objeto existente con datos y metadatos en un sistema StorageGRID.

La StorageGRID admite objetos de hasta 5 TIB (5,497,558,138,880 bytes) con un tamaño.

> Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de Swift inician una operación.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes encabezados de solicitud son opcionales:

- `Content-Disposition`
- `Content-Encoding`

  No utilice chunked `Content-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Transfer-Encoding`

  No utilice comprimido ni descomprimido `Transfer-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Content-Length`

  Si una regla de ILM filtra objetos por tamaño y utiliza la ubicación síncrona durante el procesamiento, debe especificar `Content-Length`.

  > Si no sigue estas directrices para `Content-Encoding`, `Transfer-Encoding`, y. `Content-Length`, StorageGRID debe guardar el objeto para poder determinar el tamaño del objeto y aplicar la regla ILM. En otras palabras, StorageGRID debe crear de forma predeterminada copias provisionales de un objeto durante el procesamiento. Es decir, StorageGRID debe utilizar la opción Dual COMMIT para el comportamiento de procesamiento.

  Para obtener más información sobre las reglas de la ubicación síncrona y ILM, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadatos relacionados con objetos)

  Si desea utilizar la opción **tiempo de creación definido por el usuario** como tiempo de referencia para una regla de ILM, debe almacenar el valor en un encabezado definido por el usuario denominado `X-Object-Meta-Creation-Time`. Por ejemplo:

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Este campo se evalúa como segundos desde el 1 de enero de 1970.

- `X-Storage-Class: reduced_redundancy`

  Este encabezado afecta al número de copias de objeto que crea StorageGRID si la regla de ILM que coincide con un objeto ingerido especifica un comportamiento de procesamiento de Doble COMMIT o

equilibrado.

- **Commit doble**: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingesta, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
- **Balanceado**: Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto.

  La `reduced_redundancy` El encabezado se utiliza mejor cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `reduced_redundancy` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

  Con el `reduced_redundancy` la cabecera no se recomienda en otras circunstancias porque aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

  > Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

Tenga en cuenta que especificar `reduced_redundancy` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles más bajos de redundancia en el sistema StorageGRID.

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado":

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

Información relacionada

Gestión de objetos con ILM

Supervisar y auditar operaciones

SOLICITUD DE OPCIONES

La solicitud DE OPCIONES comprueba la disponibilidad de un servicio Swift individual. El nodo de almacenamiento o el nodo de puerta de enlace especificado en la URL procesan la solicitud DE OPCIONES.

MÉTODO DE OPCIONES

Por ejemplo, las aplicaciones cliente pueden emitir una solicitud DE OPCIONES al puerto Swift en un nodo de almacenamiento sin proporcionar las credenciales de autenticación Swift para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Cuando se utiliza con la URL de información o la URL de almacenamiento, el método OPTIONS devuelve una lista de verbos admitidos para la URL dada (por ejemplo, HEAD, GET, OPTIONS y PUT). El método OPTIONS no se puede utilizar con la dirección URL de autenticación.

Se requiere el siguiente parámetro request:

- `Account`

Los siguientes parámetros de solicitud son opcionales:

- `Container`
- `Object`

Una ejecución satisfactoria devuelve los encabezados siguientes con una respuesta «'HTTP/1.1 204 sin contenido». La solicitud DE OPCIONES a la URL de almacenamiento no requiere que exista el destino.

- `Allow` (Una lista de verbos admitidos para la dirección URL dada, por ejemplo, CABEZA, OBTENER, OPCIONES, Y PUESTO)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Información relacionada

Extremos de API de Swift compatibles

Respuesta de error a las operaciones de la API de Swift

Comprender las posibles respuestas de error puede ayudar a resolver las operaciones.

Pueden devolverse los siguientes códigos de estado HTTP cuando se produzcan errores durante una operación:

Nombre de error de Swift	Estado de HTTP
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 solicitud incorrecta
ACCESSDENIED	403 Prohibido

Nombre de error de Swift	Estado de HTTP
ContainerNotEmpty, ContainerAlreadyExists	409 conflicto
Internalerror	500 error de servidor interno
InvalidRange	416 rango solicitado no utilizable
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
NOTFOUND	404 no encontrado
NotImplimed	501 no implementada
Error de precondiciónError	Error de condición 412
ResourceNotFound	404 no encontrado
No autorizado	401 no autorizado
Entidad no procesable	422 entidad no procesable

Operaciones de la API de REST de StorageGRID Swift

Existen operaciones que se añaden a la API DE REST de Swift que son específicas del sistema StorageGRID.

OBTENGA la solicitud de consistencia del contenedor

El nivel de consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. La solicitud DE consistencia DEL contenedor le permite determinar el nivel de consistencia que se aplica a un contenedor en particular.

Solicitud

Solicitar encabezado HTTP	Descripción
`X-Auth-Token`	Especifica el token de autenticación Swift de la cuenta que se va a utilizar para la solicitud.
`x-ntap-sg-consistency`	Especifica el tipo de solicitud, donde `true` = OBTENER la consistencia del contenedor, y. `false` = OBTENER contenedor.

Solicitar encabezado HTTP	Descripción
`Host`	El nombre de host al que se dirige la solicitud.

Ejemplo de solicitud

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Respuesta

Encabezado HTTP de respuesta	Descripción
`Date`	La fecha y la hora de la respuesta.
`Connection`	Si la conexión con el servidor está abierta o cerrada.
`X-Trans-Id`	Identificador de transacción único para la solicitud.
`Content-Length`	La longitud del cuerpo de respuesta.

Encabezado HTTP de respuesta	Descripción
`x-ntap-sg-consistency`	El nivel de control de consistencia que se aplica al contenedor. Se admiten los siguientes valores: • **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud falla. • **Strong-global**: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios. • **Strong-site**: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio. • **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. **Nota**: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "'disponible'". • **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

Información relacionada

Usar cuenta de inquilino

PONGA la solicitud de consistencia del contenedor

La solicitud DE PUT Container permite especificar el nivel de coherencia que se aplicará a las operaciones realizadas en un contenedor. De forma predeterminada, se crean nuevos contenedores utilizando el nivel de coherencia «entre una y otra escritura».

Solicitud

Solicitar encabezado HTTP	Descripción
`X-Auth-Token`	El token de autenticación Swift de la cuenta que se va a utilizar para la solicitud.
`x-ntap-sg-consistency`	El nivel de control de coherencia que se va a aplicar a las operaciones en el contenedor. Se admiten los siguientes valores: • **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud falla. • **Strong-global**: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios. • **Strong-site**: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio. • **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. **Nota**: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "'disponible'". • **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.
`Host`	El nombre de host al que se dirige la solicitud.

Cómo interactúan los controles de consistencia y las reglas de ILM para afectar a la protección de datos

Tanto la elección del control de coherencia como la regla de ILM afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el control de consistencia usado cuando se almacena un objeto afecta a la colocación inicial de los metadatos de objetos, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta a la colocación inicial de las copias de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **Balanceado**: StorageGRID intenta hacer todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Commit doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

> Antes de seleccionar el comportamiento de procesamiento de una regla de ILM, lea la descripción completa de estos ajustes en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Ejemplo de cómo pueden interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **Nivel de coherencia**: "Strong-global" (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si en su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Ejemplo de solicitud

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Respuesta

Encabezado HTTP de respuesta	Descripción
`Date`	La fecha y la hora de la respuesta.
`Connection`	Si la conexión con el servidor está abierta o cerrada.
`X-Trans-Id`	Identificador de transacción único para la solicitud.
`Content-Length`	La longitud del cuerpo de respuesta.

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Información relacionada

Usar cuenta de inquilino

Configure la seguridad de la API de REST

Debe revisar las medidas de seguridad implementadas para la API REST y entender cómo proteger el sistema.

Cómo proporciona StorageGRID seguridad para la API de REST

Debe entender cómo el sistema StorageGRID implementa la seguridad, la autenticación y la autorización para la API DE REST.

StorageGRID usa las siguientes medidas de seguridad.

- Las comunicaciones de cliente con el servicio Load Balancer utilizan HTTPS si HTTPS está configurado para el extremo de equilibrio de carga.

Al configurar un extremo de equilibrio de carga, HTTP se puede habilitar opcionalmente. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

- De forma predeterminada, StorageGRID utiliza HTTPS para las comunicaciones del cliente con los nodos de almacenamiento y el servicio CLB en los nodos de puerta de enlace.

  Opcionalmente, HTTP se puede habilitar para estas conexiones. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

  El servicio CLB está obsoleto.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento de la cuadrícula están cifradas si el extremo de equilibrio de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben proporcionar encabezados de autenticación HTTP a StorageGRID para realizar operaciones de API DE REST.

Certificados de seguridad y aplicaciones cliente

Los clientes pueden conectarse al servicio Load Balancer en los nodos de Gateway o de administrador, directamente a los nodos de almacenamiento o al servicio CLB obsoleto en los nodos de Gateway.

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS mediante un certificado de servidor personalizado cargado por el administrador de grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, lo hacen utilizando el certificado que se configuró para el extremo de equilibrio de carga específico utilizado para realizar la conexión. Cada extremo tiene su propio certificado, que es un certificado de servidor personalizado cargado por el administrador de grid o un certificado que el administrador de grid generó en StorageGRID al configurar el extremo.
- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento o al servicio CLB en los nodos de puerta de enlace, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (firmados por la autoridad de certificación del sistema), o un único certificado de servidor personalizado que un administrador de grid suministra para la cuadrícula.

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Consulte las instrucciones para administrar StorageGRID para obtener información sobre la configuración de extremos de equilibrador de carga y para obtener instrucciones sobre cómo agregar un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace.

Resumen

En la siguiente tabla, se muestra cómo se implementan los problemas de seguridad en las API DE REST de S3 y Swift:

Problema de seguridad	Implementación de la API DE REST
Seguridad de la conexión	TLS
Autenticación del servidor	Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador
Autentificación de clientes	• S3: Cuenta de S3 (ID de clave de acceso y clave de acceso secreta) • Swift: Cuenta de Swift (nombre de usuario y contraseña)
Autorización de cliente	• S3: Propiedad de bloque y todas las políticas de control de acceso aplicables • Swift: Acceso a roles de administrador

Información relacionada

Administre StorageGRID

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión de seguridad de la capa de transporte (TLS).

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.

SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Paquetes de cifrado compatibles

Versión TLS	Nombre IANA de conjunto cifrado
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA 256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Suites de cifrado obsoletas

Los siguientes conjuntos de cifrado están desaprobados. La compatibilidad con estos cifrados se eliminará en una versión futura.

Nombre de IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Información relacionada

Configure las conexiones y las cuentas de inquilino

Supervisar y auditar operaciones

Puede supervisar las cargas de trabajo y las eficiencias de las operaciones del cliente al ver las tendencias de las transacciones de todo el grid o de nodos específicos. Puede utilizar mensajes de auditoría para supervisar las operaciones y transacciones del cliente.

Supervise las tasas de procesamiento y recuperación de objetos

Es posible supervisar las tasas de procesamiento y recuperación de objetos, así como las métricas para el número de objetos, consultas y verificación. Puede ver el número de intentos fallidos y correctos por las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. En la consola, busque la sección Operaciones de protocolo.

   En esta sección se resume el número de operaciones de cliente que realiza su sistema StorageGRID. La media de las tasas de protocolo se hace durante los últimos dos minutos.

3. Seleccione **NODES**.
4. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **Load Balancer**.

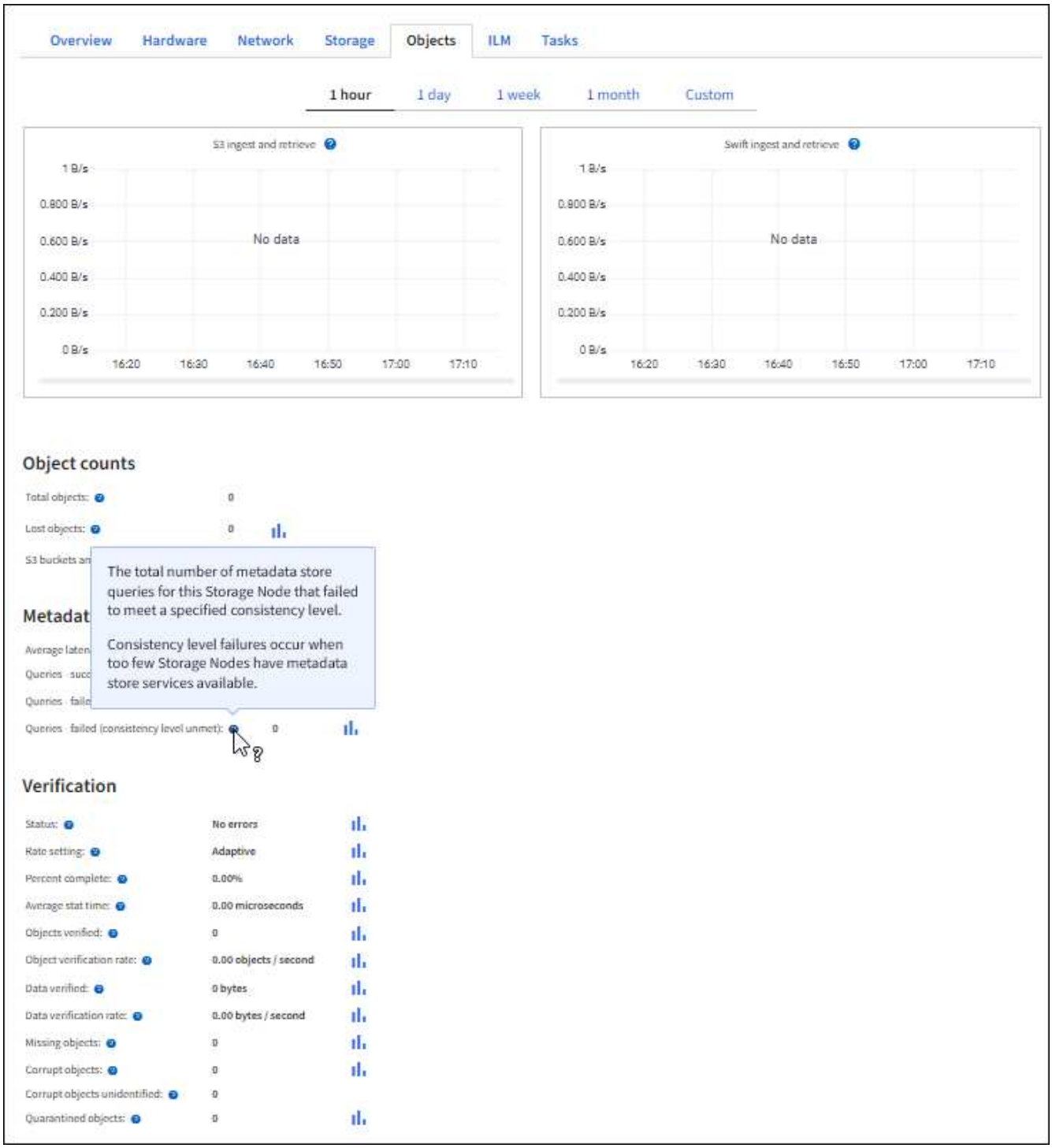
   Los gráficos muestran tendencias para todo el tráfico de cliente dirigido a los extremos de equilibrador de carga dentro de la cuadrícula. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de todo el sistema StorageGRID en bytes por segundo y bytes totales. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

6. Para ver información sobre un nodo de almacenamiento en particular, seleccione el nodo en la lista de la izquierda y haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de objetos de este nodo de almacenamiento. La pestaña también incluye métricas para el recuento de objetos, consultas y verificación. Puede hacer clic en las etiquetas para ver las definiciones de estas métricas.



7. Si desea aún más detalles:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***site*** > **Descripción general** > **Principal**.

      La sección API Operations muestra información resumida de la cuadrícula completa.

   c. Seleccione ***Storage Node*** > **LDR** > ***Client Application*** > **Overview** > **Main**

      La sección Operaciones muestra información de resumen del nodo de almacenamiento seleccionado.

Acceder y revisar registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Los mensajes de auditoría específicos de API de los registros de auditoría ofrecen datos críticos de seguridad, operación y supervisión del rendimiento que pueden ayudar a evaluar el estado del sistema.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Acerca de esta tarea

Se denomina el archivo de registro de auditoría activo `audit.log`, Y se almacena en los nodos Admin.

Una vez al día, se guarda el archivo audit.log activo y se inicia un nuevo archivo audit.log. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`.

Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original.

En este ejemplo, se muestra el archivo audit.log activo, el archivo del día anterior (2018-04-15.txt) y el archivo comprimido del día anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Vaya al directorio que contiene los archivos del registro de auditoría:`cd /var/local/audit/export`
3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Información relacionada

Revisar los registros de auditoría

Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría

Se realiza un seguimiento de todas las operaciones DE ELIMINACIÓN, GET, HEAD, POST y PUT de almacenamiento correctamente en el registro de auditoría de StorageGRID. Los fallos no se registran ni se registran solicitudes de información, autenticación u OPCIONES.

Consulte *Descripción de los mensajes de auditoría* para obtener detalles sobre la información de la que se realiza el seguimiento para las siguientes operaciones de Swift.

Operaciones de cuentas

- OBTENGA la cuenta
- CUENTA principal

Operaciones de contenedor

- ELIMINAR contenedor
- OBTENGA el contenedor
- Contenedor DE LA CABEZA
- COLOQUE el contenedor

Operaciones de objeto

- ELIMINAR objeto
- OBJETO GET
- OBJETO HEAD
- PONER objeto

Información relacionada

Revisar los registros de auditoría

Operaciones de cuentas

Operaciones de contenedor

Operaciones de objeto