Use a API Swift REST

StorageGRID

NetApp
March 10, 2025

Índice

Use Swift

Saiba como os aplicativos clientes podem usar a API OpenStack Swift para fazer interface com o sistema StorageGRID.

- "Suporte à API OpenStack Swift no StorageGRID"
- "Configurando contas de locatário e conexões"
- "Operações suportadas pela API REST Swift"
- "Operações da API REST do StorageGRID Swift"
- "Configurando a segurança para a API REST"
- "Operações de monitoramento e auditoria"

Suporte à API OpenStack Swift no StorageGRID

O StorageGRID suporta as seguintes versões específicas do Swift e HTTP.

Item	Versão
Especificação Swift	API de storage de objetos OpenStack Swift v1 em novembro de 2015
HTTP	1,1 para obter mais informações sobre HTTP, consulte HTTP/1,1 (RFCs 7230-35). **Nota**: O StorageGRID não suporta a canalização HTTP/1,1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Histórico do suporte à API Swift no StorageGRID

Você deve estar ciente das alterações no suporte do sistema StorageGRID para a API REST Swift.

Solte	Comentários
11,5	Removido o controle de consistência fraca. O nível de consistência disponível será usado em vez disso.
11,4	Adicionado suporte para TLS 1,3 e lista atualizada de pacotes de criptografia TLS suportados. O CLB está obsoleto. Adicionada descrição da inter-relação entre ILM e a configuração de consistência.

Solte	Comentários
11,3	Operações PUT Object atualizadas para descrever o impactos das regras de ILM que usam o posicionamento síncrono na ingestão (as opções equilibradas e rigorosas para o comportamento de ingestão). Adicionada descrição das conexões de cliente que usam pontos de extremidade do balanceador de carga ou grupos de alta disponibilidade. Lista atualizada dos conjuntos de encriptação TLS suportados. As cifras TLS 1,1 não são mais suportadas.
11,2	Pequenas alterações editoriais ao documento.
11,1	Adicionado suporte para o uso de HTTP para conexões de cliente Swift para nós de grade. Atualizadas as definições dos controles de consistência.
11,0	Adicionado suporte para 1.000 contentores para cada conta de locatário.
10,3	Atualizações administrativas e correções do documento. Seções removidas para configurar certificados de servidor personalizados.
10,2	Suporte inicial da API Swift pelo sistema StorageGRID. A versão atualmente suportada é a API de armazenamento de objetos OpenStack Swift v1.

Como o StorageGRID implementa a API Swift REST

Um aplicativo cliente pode usar chamadas de API REST do Swift para se conetar a nós de storage e nós de Gateway para criar contentores e armazenar e recuperar objetos. Isso permite que aplicativos orientados a serviços desenvolvidos para o OpenStack Swift se conetem com storage de objetos no local fornecido pelo sistema StorageGRID.

Gerenciamento de objetos Swift

Depois que os objetos Swift foram ingeridos no sistema StorageGRID, eles são gerenciados pelas regras de gerenciamento do ciclo de vida da informação (ILM) na política ativa de ILM do sistema. As regras e a política do ILM determinam como o StorageGRID cria e distribui cópias de dados de objetos e como gerencia essas cópias ao longo do tempo. Por exemplo, uma regra ILM pode se aplicar a objetos em contentores Swift específicos e pode especificar que várias cópias de objetos sejam salvas em vários data centers por um certo número de anos.

Entre em Contato com o administrador do StorageGRID se você precisar entender como as regras e políticas do ILM da grade afetarão os objetos em sua conta de locatário do Swift.

Solicitações de cliente conflitantes

As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O momento para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes Swift iniciam uma operação.

Garantias de consistência e controles

Por padrão, o StorageGRID fornece consistência de leitura após gravação para objetos recém-criados e consistência para atualizações de objetos e operações HEAD. Qualquer GET seguindo um PUT concluído com sucesso será capaz de ler os dados recém-escritos. As substituições de objetos existentes, atualizações de metadados e exclusões são, eventualmente, consistentes. As substituições geralmente levam segundos ou minutos para se propagar, mas podem levar até 15 dias.

O StorageGRID também permite que você controle a consistência por contentor. Você pode alterar o controle de consistência para fazer uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de storage e sites, conforme necessário pela aplicação.

Informações relacionadas

"Gerenciar objetos com ILM"

"OBTER solicitação de consistência de contêiner"

"COLOQUE o pedido de consistência do recipiente"

Recomendações para a implementação da API Swift REST

Você deve seguir estas recomendações ao implementar a API REST do Swift para uso com o StorageGRID.

Recomendações para heads to non-existent objects

Se seu aplicativo verifica rotineiramente para ver se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o controle de consistência ""disponível"". Por exemplo, você deve usar o controle de consistência "disponível" se seu aplicativo executar uma operação DE CABEÇA para um local antes de executar uma OPERAÇÃO DE COLOCAÇÃO nesse local.

Caso contrário, se a operação PRINCIPAL não encontrar o objeto, você poderá receber um número alto de 500 erros de servidor interno se um ou mais nós de storage não estiverem disponíveis.

Você pode definir o controle de consistência "disponível" para cada recipiente usando o pedido de consistência de contentor PUT.

Recomendações para nomes de objetos

Você não deve usar valores aleatórios como os primeiros quatro carateres de nomes de objetos. Em vez disso, você deve usar prefixos não aleatórios, não exclusivos, como imagem.

Se você precisar usar carateres aleatórios e exclusivos em prefixos de nome de objeto, você deve prefixar os nomes de objeto com um nome de diretório. Ou seja, use este formato:

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

Em vez deste formato:

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

Recomendações para "leituras de intervalo"

Se a opção **Compress Stored Objects** estiver selecionada (**Configuration System Settings Grid Options**), os aplicativos cliente Swift devem evitar executar operações de objeto GET que especificam um intervalo de bytes que serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é muito ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

> Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

Informações relacionadas

"OBTER solicitação de consistência de contêiner"

"COLOQUE o pedido de consistência do recipiente"

"Administrar o StorageGRID"

Configurando contas de locatário e conexões

Configurar o StorageGRID para aceitar conexões de aplicativos cliente requer a criação de uma ou mais contas de locatário e a configuração das conexões.

Criando e configurando contas de locatário Swift

Uma conta de locatário Swift é necessária antes que os clientes da API Swift possam armazenar e recuperar objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários, além de contentores e objetos.

As contas de locatário Swift são criadas por um administrador de grade do StorageGRID usando o Gerenciador de grade ou a API de gerenciamento de grade.

Ao criar uma conta de locatário Swift, o administrador da grade especifica as seguintes informações:

- Nome de exibição para o locatário (o ID da conta do locatário é atribuído automaticamente e não pode ser alterado)
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).

- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.
- Se o SSO estiver ativado, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

Depois que uma conta de locatário Swift for criada, os usuários com a permissão de acesso root podem acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do uso do storage

> Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

Informações relacionadas

"Administrar o StorageGRID"

"Use uma conta de locatário"

"Endpoints de API Swift compatíveis"

Como as conexões do cliente podem ser configuradas

Um administrador de grade faz escolhas de configuração que afetam a forma como os clientes Swift se conetam ao StorageGRID para armazenar e recuperar dados. As informações específicas que você precisa para fazer uma conexão dependem da configuração escolhida.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

> O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Ao configurar o StorageGRID, um administrador de grade pode usar o Gerenciador de grade ou a API de gerenciamento de grade para executar as seguintes etapas, todas opcionais:

1. Configure endpoints para o serviço Load Balancer.

   Você deve configurar endpoints para usar o serviço Load Balancer. O serviço Load Balancer em nós de administração ou nós de gateway distribui conexões de rede recebidas de aplicativos clientes para nós de

storage. Ao criar um endpoint de balanceador de carga, o administrador do StorageGRID especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).

2. Configurar redes de clientes não confiáveis.

   Se um administrador do StorageGRID configurar a rede cliente de um nó para não ser confiável, o nó só aceita conexões de entrada na rede cliente em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

3. Configurar grupos de alta disponibilidade.

   Se um administrador criar um grupo de HA, as interfaces de rede de vários nós de Admin ou nós de Gateway serão colocadas em uma configuração de backup ativo. As conexões de cliente são feitas usando o endereço IP virtual do grupo HA.

Para obter mais informações sobre cada opção, consulte as instruções para administrar o StorageGRID.

Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos cliente se conetam ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

Informações necessárias para fazer conexões com o cliente

A tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Contate o administrador do StorageGRID para obter mais informações ou consulte as instruções de administração do StorageGRID para obter uma descrição de como localizar essas informações no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	• Porta de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas Swift padrão: • HTTPS: 8083 • HTTP: 8085
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas Swift padrão: • HTTPS: 18083 • HTTP: 18085

Exemplo

Para conetar um cliente Swift ao endpoint do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

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

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.6 e o número da porta de um endpoint do Swift Load Balancer for 10444, um cliente Swift poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.6:10444`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

Decidir usar conexões HTTPS ou HTTP

Quando as conexões de cliente são feitas usando um endpoint de Load Balancer, as conexões devem ser feitas usando o protocolo (HTTP ou HTTPS) especificado para esse endpoint. Para usar HTTP para conexões de cliente a nós de armazenamento ou ao serviço CLB em nós de gateway, você deve habilitar seu uso.

Por padrão, quando os aplicativos cliente se conetam a nós de armazenamento ou ao serviço CLB nos nós de Gateway, eles devem usar HTTPS criptografado para todas as conexões. Opcionalmente, você pode habilitar conexões HTTP menos seguras selecionando a opção de grade **Ativar conexão HTTP** no Gerenciador de Grade. Por exemplo, um aplicativo cliente pode usar HTTP ao testar a conexão com um nó de armazenamento em um ambiente que não seja de produção.

> Tenha cuidado ao ativar o HTTP para uma grade de produção, já que as solicitações serão enviadas sem criptografia.

> O serviço CLB está obsoleto.

Se a opção **Enable HTTP Connection** estiver selecionada, os clientes devem usar portas diferentes para HTTP do que para HTTPS. Consulte as instruções para administrar o StorageGRID.

Informações relacionadas

"Administrar o StorageGRID"

Testando sua conexão na configuração da API Swift

Você pode usar o Swift CLI para testar sua conexão com o sistema StorageGRID e verificar se você pode ler e gravar objetos no sistema.

O que você vai precisar

- Você deve ter baixado e instalado Python-swiftclient, o cliente de linha de comando Swift.
- Você deve ter uma conta de locatário Swift no sistema StorageGRID.

Sobre esta tarefa

Se você não tiver configurado a segurança, você deve adicionar o `--insecure` sinalizador a cada um desses comandos.

Passos

1. Consulte o URL de informações para sua implantação do StorageGRID Swift:

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

   Isso é suficiente para testar se sua implantação do Swift está funcional. Para testar ainda mais a configuração da conta armazenando um objeto, continue com as etapas adicionais.

2. Coloque um objeto no recipiente:

```
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. Obtenha o contentor para verificar o objeto:

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

4. Eliminar o 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. Eliminar o recipiente:

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

Informações relacionadas

"Criando e configurando contas de locatário Swift"

"Configurando a segurança para a API REST"

Operações suportadas pela API REST Swift

O sistema StorageGRID dá suporte à maioria das operações na API OpenStack Swift. Antes de integrar clientes API REST do Swift com o StorageGRID, revise os detalhes de implementação para operações de conta, contentor e objeto.

Operações suportadas no StorageGRID

As seguintes operações da API Swift são suportadas:

- "Operações de conta"
- "Operações de contêiner"
- "Operações de objetos"

Cabeçalhos de resposta comuns para todas as operações

O sistema StorageGRID implementa todos os cabeçalhos comuns para operações com suporte, conforme definido pela API de armazenamento de objetos OpenStack Swift v1.

Informações relacionadas

"OpenStack: API de storage de objetos"

Endpoints de API Swift compatíveis

O StorageGRID oferece suporte aos seguintes endpoints da API Swift: O URL de informações, o URL de autenticação e o URL de armazenamento.

URL de informações

Você pode determinar os recursos e limitações da implementação do StorageGRID Swift emitindo uma solicitação GET para o URL base do Swift com o caminho /info.

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

No pedido:

- *FQDN* é o nome de domínio totalmente qualificado.
- *Node IP* É o endereço IP do nó de armazenamento ou do nó de gateway na rede StorageGRID.
- *Swift Port* É o número de porta usado para conexões Swift API no nó de armazenamento ou nó de gateway.

Por exemplo, o seguinte URL de informações solicitaria informações de um nó de armazenamento com o endereço IP de 10.99.106.103 e usando a porta 18083.

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

A resposta inclui os recursos da implementação Swift como um dicionário JSON. Uma ferramenta cliente pode analisar a resposta JSON para determinar os recursos da implementação e usá-los como restrições para operações de armazenamento subsequentes.

A implementação do StorageGRID do Swift permite o acesso não autenticado ao URL de informações.

URL de autenticação

Um cliente pode usar o URL de autenticação Swift para autenticar como usuário de conta de locatário.

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

Você deve fornecer o ID da conta do locatário, o nome de usuário e a senha como parâmetros nos `X-Auth-User` cabeçalhos e `X-Auth-Key` da solicitação, da seguinte forma:

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

X-Auth-Key: Password
```

Nos cabeçalhos de solicitação:

- *Tenant_Account_ID* É o ID de conta atribuído pelo StorageGRID quando o locatário Swift foi criado. Esse é o mesmo ID de conta de locatário usado na página de login do Gerenciador do Locatário.
- *Username* É o nome de um usuário do locatário que foi criado no Gerenciador do Locatário. Esse usuário deve pertencer a um grupo que tenha a permissão Swift Administrator. O usuário raiz do locatário não pode ser configurado para usar a API REST do Swift.

  Se a Federação de identidade estiver ativada para a conta de locatário, forneça o nome de usuário e a senha do usuário federado do servidor LDAP. Em alternativa, forneça o nome de domínio do utilizador LDAP. Por exemplo:

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

- `Password` é a senha para o usuário do locatário. As senhas de usuário são criadas e gerenciadas no Gerenciador do locatário.

A resposta a uma solicitação de autenticação bem-sucedida retorna um URL de armazenamento e um token de autenticação, como segue:

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

X-Auth-Token: token

X-Storage-Token: token
```

Por padrão, o token é válido por 24 horas a partir do tempo de geração.

Os tokens são gerados para uma conta de locatário específica. Um token válido para uma conta não autoriza um usuário a acessar outra conta.

URL de armazenamento

Um aplicativo cliente pode emitir chamadas de API REST Swift para executar operações de conta, contentor e objeto com suporte em um nó de gateway ou nó de storage. As solicitações de armazenamento são endereçadas ao URL de armazenamento retornado na resposta de autenticação. A solicitação também deve incluir o cabeçalho X-Auth-Token e o valor retornado da solicitação de autenticação.

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

[/container][/object]

X-Auth-Token: token
```

Alguns cabeçalhos de resposta de armazenamento que contêm estatísticas de uso podem não refletir números precisos para objetos modificados recentemente. Pode levar alguns minutos para que números precisos apareçam nesses cabeçalhos.

Os cabeçalhos de resposta a seguir para operações de conta e contentor são exemplos daqueles que contêm estatísticas de uso:

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

Informações relacionadas

"Como as conexões do cliente podem ser configuradas"

"Criando e configurando contas de locatário Swift"

"Operações de conta"

"Operações de contêiner"

"Operações de objetos"

Operações de conta

As seguintes operações da API Swift são realizadas em contas.

OBTER conta

Esta operação recupera a lista de contentores associada às estatísticas de uso de conta e conta.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

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

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content" se a conta for encontrada e não tiver contentores ou a lista de contentores estiver vazia; ou uma resposta HTTP/1,1 200 OK se a conta for encontrada e a lista de contentores não estiver vazia:

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

Conta principal

Esta operação recupera informações de conta e estatísticas de uma conta Swift.

É necessário o seguinte parâmetro de pedido:

- `Account`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "'HTTP/1,1 204 no Content'":

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

Informações relacionadas

"Operações rápidas rastreadas nos logs de auditoria"

Operações de contêiner

O StorageGRID suporta um máximo de 1.000 contentores por conta Swift. As seguintes operações da API Swift são executadas em contentores.

ELIMINAR recipiente

Esta operação remove um contentor vazio de uma conta Swift em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

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

PEGUE o recipiente

Esta operação recupera a lista de objetos associada ao contentor juntamente com estatísticas de contentor e metadados em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes parâmetros de consulta de solicitação suportados são opcionais:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 success" ou "HTTP/1,1 204 no content":

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

Recipiente DA cabeça

Esta operação recupera estatísticas de contentor e metadados de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 204 sem conteúdo":

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

COLOQUE o recipiente

Esta operação cria um contentor para uma conta em um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

- `Account`
- `Container`

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado" ou "HTTP/1,1 202 aceito" (se o contentor já existir sob esta conta):

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

Um nome de contêiner deve ser exclusivo no namespace StorageGRID. Se o contentor existir sob outra conta, o seguinte cabeçalho é retornado: "Conflito HTTP/1,1 409".

Informações relacionadas

"Operações rápidas rastreadas nos logs de auditoria"

Operações de objetos

As seguintes operações da API Swift são executadas em objetos.

ELIMINAR objeto

Esta operação exclui o conteúdo e os metadados de um objeto do sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

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

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos de resposta com uma `HTTP/1.1 204 No Content` resposta:

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

Ao processar uma solicitação DE EXCLUSÃO de objetos, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se for bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas dentro de 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID coloca as cópias em fila para remoção e, em seguida, indica sucesso para o cliente.

Para obter mais informações sobre como os objetos são excluídos, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

OBTER objeto

Esta operação recupera o conteúdo do objeto e obtém os metadados do objeto de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

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

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

- `Accept-Encoding`
- `If-Match`

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

Uma execução bem-sucedida retorna os seguintes cabeçalhos com `HTTP/1.1 200 OK` uma resposta:

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

Objeto PRINCIPAL

Esta operação recupera metadados e propriedades de um objeto ingerido a partir de um sistema StorageGRID.

São necessários os seguintes parâmetros de pedido:

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

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 200 OK":

- `Accept-Ranges`
- `Content-Disposition`, retornada somente se `Content-Disposition` os metadados tiverem sido definidos
- `Content-Encoding`, retornada somente se `Content-Encoding` os metadados tiverem sido definidos
- `Content-Length`
- `Content-Type`

- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE o objeto

Essa operação cria um novo objeto com dados e metadados ou substitui um objeto existente por dados e metadados em um sistema StorageGRID.

O StorageGRID suporta objetos de até 5 TB de tamanho.

> As solicitações de clientes conflitantes, como dois clientes escrevendo para a mesma chave, são resolvidas com base em "últimos ganhos". O momento para a avaliação "últimos ganhos" é baseado em quando o sistema StorageGRID completa uma determinada solicitação e não em quando os clientes Swift iniciam uma operação.

São necessários os seguintes parâmetros de pedido:

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

É necessário o seguinte cabeçalho de solicitação:

- `X-Auth-Token`

Os seguintes cabeçalhos de solicitação são opcionais:

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

  Não use em pedaços `Content-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Transfer-Encoding`

  Não use compactado ou dividido `Transfer-Encoding` se a regra ILM que se aplica a um objeto filtra objetos com base no tamanho e usa o posicionamento síncrono na ingestão (as opções balanceadas ou rigorosas para o comportamento de ingestão).

- `Content-Length`

  Se uma regra de ILM filtrar objetos por tamanho e usar o posicionamento síncrono na ingestão, você deverá especificar `Content-Length`.

> Se você não seguir estas diretrizes para `Content-Encoding`, `Transfer-Encoding` e `Content-Length`, o StorageGRID deve salvar o objeto antes que ele possa determinar o tamanho do objeto e aplicar a regra ILM. Em outras palavras, o StorageGRID deve criar cópias provisórias de um objeto na ingestão. Ou seja, o StorageGRID deve usar a opção de confirmação dupla para o comportamento de ingestão.

Para obter mais informações sobre o posicionamento síncrono e as regras de ILM, consulte as instruções para gerenciar objetos com o gerenciamento do ciclo de vida das informações.

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

  Se você quiser usar a opção **tempo de criação definido pelo usuário** como tempo de referência para uma regra ILM, você deve armazenar o valor em um cabeçalho definido pelo usuário chamado `X-Object-Meta-Creation-Time`. Por exemplo:

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

  Este campo é avaliado em segundos desde 1 de janeiro de 1970.

- `X-Storage-Class: reduced_redundancy`

  Esse cabeçalho afeta quantas cópias de objeto criadas pelo StorageGRID se a regra ILM que corresponde a um objeto ingerido especificar um comportamento de ingestão de confirmação dupla ou equilibrada.

  - **Commit duplo**: Se a regra ILM especificar a opção de commit duplo para o comportamento de ingestão, o StorageGRID cria uma única cópia provisória à medida que o objeto é ingerido (commit único).
  - **Balanced**: Se a regra ILM especificar a opção Balanced, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito.

    O `reduced_redundancy` cabeçalho é melhor usado quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso, o uso `reduced_redundancy` elimina a criação e exclusão desnecessárias de uma cópia de objeto extra para cada operação de ingestão.

    O uso do `reduced_redundancy` cabeçalho não é recomendado em outras circunstâncias porque aumenta o risco de perda de dados de objetos durante a ingestão. Por exemplo, você pode perder dados se a única cópia for inicialmente armazenada em um nó de armazenamento que falha antes que a avaliação ILM possa ocorrer.

    > Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se houver apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Observe que especificar `reduced_redundancy` apenas afeta quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Ele não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pela política ILM ativa e não faz com que os dados sejam armazenados em níveis mais baixos de redundância no sistema StorageGRID.

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta "HTTP/1,1 201 criado":

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

Informações relacionadas

"Gerenciar objetos com ILM"

"Operações rápidas rastreadas nos logs de auditoria"

Pedido de OPÇÕES

A SOLICITAÇÃO DE OPÇÕES verifica a disponibilidade de um serviço Swift individual. A SOLICITAÇÃO DE OPÇÕES é processada pelo nó de armazenamento ou nó de gateway especificado no URL.

Método de OPÇÕES

Por exemplo, os aplicativos clientes podem emitir uma SOLICITAÇÃO DE OPÇÕES para a porta Swift em um nó de armazenamento, sem fornecer credenciais de autenticação Swift, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de storage está inativo.

Quando usado com o URL info ou o URL de armazenamento, o método OPTIONS retorna uma lista de verbos suportados para o URL dado (por exemplo, HEAD, GET, OPTIONS E PUT). O método DE OPÇÕES não pode ser usado com o URL de autenticação.

É necessário o seguinte parâmetro de pedido:

- `Account`

Os seguintes parâmetros de pedido são opcionais:

- `Container`
- `Object`

Uma execução bem-sucedida retorna os seguintes cabeçalhos com uma resposta HTTP/1,1 204 no content". A SOLICITAÇÃO DE OPÇÕES para o URL de armazenamento não exige que o destino exista.

- `Allow` (Uma lista de verbos suportados para o URL dado, por exemplo, HEAD, GET, OPTIONS e PUT)

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

Informações relacionadas

"Endpoints de API Swift compatíveis"

Respostas de erro às operações da API Swift

Entender as possíveis respostas de erro pode ajudá-lo a solucionar problemas de operações.

Os seguintes códigos de status HTTP podem ser retornados quando erros ocorrem durante uma operação:

Nome de erro Swift	Status HTTP
AccountNameToLong, ContainerNameToLong, HeaderToBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameToLong, MetadataValueToBig, MissingSecurityHeader, ObjectNameToLong, ToManyContainers, ToManyMetadataItems, TotalMetataTooLarge	400 pedido incorreto
AccessDenied	403 proibido
ContainerNotEmpty, ContainerAlreadyExists	409 conflito
InternalError (erro internacional)	500 erro interno do servidor
Intervalo Invalidável	416 intervalo solicitado não satisfatório
MetodNotAlloved	Método 405 não permitido
MissingContentLength	411 comprimento necessário
Não encontrado	404 não encontrado
Sem Implementado	501 não implementado
Pré-condiçãoFailed	412 Pré-condição falhou
ResourceNotFound	404 não encontrado
Não autorizado	401 não autorizado

Nome de erro Swift	Status HTTP
UnprocessableEntity	422 entidade não processável

Operações da API REST do StorageGRID Swift

Há operações adicionadas à API REST do Swift que são específicas do sistema StorageGRID.

OBTER solicitação de consistência de contêiner

O nível de consistência faz uma troca entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós e sites de storage. A solicitação GET Container Consistency permite que você determine o nível de consistência que está sendo aplicado a um contentor específico.

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	Especifica o token de autenticação Swift para a conta a ser usada para a solicitação.
`x-ntap-sg-consistency`	Especifica o tipo de solicitação, onde `true` OBTÉM consistência de contentor e `false` OBTÉM contentor.
`Host`	O nome do host para o qual a solicitação é direcionada.

Exemplo de solicitação

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

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.

Cabeçalho HTTP de resposta	Descrição
`Content-Length`	O comprimento do corpo de resposta.
`x-ntap-sg-consistency`	O nível de controle de consistência que está sendo aplicado ao recipiente. Os seguintes valores são suportados: • **Todos**: Todos os nós recebem os dados imediatamente ou a solicitação falhará. • **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites. • * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site. • **Read-after-novo-write**: Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.

Exemplo de resposta

```
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
```

Informações relacionadas

"Use uma conta de locatário"

COLOQUE o pedido de consistência do recipiente

A solicitação de consistência de contentor PUT permite especificar o nível de consistência a ser aplicado às operações realizadas em um contentor. Por padrão, novos contentores são criados usando o nível de consistência "read-after-new-write".

Pedido

Solicitar cabeçalho HTTP	Descrição
`X-Auth-Token`	O token de autenticação Swift para a conta a ser usada para a solicitação.
`x-ntap-sg-consistency`	O nível de controle de consistência a aplicar às operações no recipiente. Os seguintes valores são suportados: • **Todos**: Todos os nós recebem os dados imediatamente ou a solicitação falhará. • **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites. • * Strong-site*: Garante consistência de leitura-após-gravação para todas as solicitações de clientes dentro de um site. • **Read-after-novo-write**: Fornece consistência de leitura-após-gravação para novos objetos e eventual consistência para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. **Nota**: Se o aplicativo usar SOLICITAÇÕES HEAD em objetos que não existem, você pode receber um número alto de erros de servidor interno 500 se um ou mais nós de armazenamento não estiverem disponíveis. Para evitar esses erros, use o nível "disponível". • **Available** (eventual consistência para OPERAÇÕES DE CABEÇA): Comporta-se da mesma forma que o nível de consistência "read-after-new-write", mas apenas fornece consistência eventual para operações DE CABEÇA. Oferece maior disponibilidade para OPERAÇÕES HEAD do que "read-after-novo-write" se os nós de storage não estiverem disponíveis.

Solicitar cabeçalho HTTP	Descrição
`Host`	O nome do host para o qual a solicitação é direcionada.

Como os controles de consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto a sua escolha de controle de consistência quanto a sua regra ILM afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o controle de consistência usado quando um objeto é armazenado afeta o posicionamento inicial dos metadados do objeto, enquanto o comportamento de ingestão selecionado para a regra ILM afeta o posicionamento inicial das cópias do objeto. Como o StorageGRID exige acesso aos metadados de um objeto e aos dados para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para o nível de consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas do sistema mais previsíveis.

Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Strict**: Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja devolvido ao cliente.
- **Balanced**: O StorageGRID tenta fazer todas as cópias especificadas na regra ILM no ingest; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.
- * Commit duplo*: O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

> Antes de selecionar o comportamento de ingestão para uma regra ILM, leia a descrição completa dessas configurações nas instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

Exemplo de como o controle de consistência e a regra ILM podem interagir

Suponha que você tenha uma grade de dois locais com a seguinte regra ILM e a seguinte configuração de nível de consistência:

- **Regra ILM**: Crie duas cópias de objeto, uma no local e outra em um local remoto. O comportamento de ingestão estrita é selecionado.
- **Nível de consistência**: "Trong-global" (metadados de objetos são imediatamente distribuídos para todos os sites.)

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias de objeto e distribui metadados para ambos os sites antes de retornar sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da mensagem de ingestão bem-sucedida. Por exemplo, se o local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existem no local remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usou a mesma regra ILM e o nível de consistência "site-trong", o cliente poderá receber uma mensagem de sucesso depois que os dados do objeto forem replicados para o site remoto, mas antes que os metadados do objeto sejam distribuídos lá. Nesse caso, o nível de proteção dos metadados de objetos não corresponde ao nível de proteção dos dados de objeto. Se o site local for perdido logo após a

ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre níveis de consistência e regras de ILM pode ser complexa. Contacte a NetApp se necessitar de assistência.

Exemplo de solicitação

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

Resposta

Cabeçalho HTTP de resposta	Descrição
`Date`	A data e a hora da resposta.
`Connection`	Se a conexão com o servidor está aberta ou fechada.
`X-Trans-Id`	O identificador de transação exclusivo para a solicitação.
`Content-Length`	O comprimento do corpo de resposta.

Exemplo de resposta

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

Informações relacionadas

"Use uma conta de locatário"

Configurando a segurança para a API REST

Você deve analisar as medidas de segurança implementadas para a API REST e entender como proteger seu sistema.

Como o StorageGRID fornece segurança para a API REST

Você deve entender como o sistema StorageGRID implementa segurança, autenticação e autorização para a API REST.

O StorageGRID usa as seguintes medidas de segurança.

- As comunicações do cliente com o serviço Load Balancer usam HTTPS se o HTTPS estiver configurado para o ponto de extremidade do balanceador de carga.

  Quando você configura um ponto de extremidade do balanceador de carga, o HTTP pode ser habilitado opcionalmente. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

- Por padrão, o StorageGRID usa HTTPS para comunicações de clientes com nós de armazenamento e o serviço CLB em nós de gateway.

  O HTTP pode, opcionalmente, ser habilitado para essas conexões. Por exemplo, você pode querer usar HTTP para testes ou outros fins de não produção. Consulte as instruções para administrar o StorageGRID para obter mais informações.

  > ⓘ O serviço CLB está obsoleto.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer cabeçalhos de autenticação HTTP ao StorageGRID para executar operações de API REST.

Certificados de segurança e aplicativos de cliente

Os clientes podem se conetar ao serviço Load Balancer em nós de gateway ou nós de administrador, diretamente aos nós de storage ou ao serviço CLB em nós de gateway.

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conetam ao serviço do Load Balancer, eles fazem isso usando o certificado que foi configurado para o ponto de extremidade do balanceador de carga específico usado para fazer a conexão. Cada endpoint tem seu próprio certificado, que é um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o endpoint.
- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento ou ao serviço CLB nos nós de gateway, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade.

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Consulte as instruções de administração do StorageGRID para obter informações sobre a configuração de pontos de extremidade do balanceador de carga e para obter instruções sobre como adicionar um único certificado de servidor personalizado para conexões TLS diretamente aos nós de armazenamento ou ao serviço CLB nos nós de gateway.

Resumo

A tabela a seguir mostra como os problemas de segurança são implementados nas APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS
Autenticação do servidor	Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador
Autenticação de cliente	• S3: Conta S3 (ID da chave de acesso e chave de acesso secreta) • Swift: Conta Swift (nome de usuário e senha)
Autorização do cliente	• S3: Propriedade do bucket e todas as políticas de controle de acesso aplicáveis • Swift: Acesso à função de administrador

Informações relacionadas

"Administrar o StorageGRID"

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto limitado de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão de Segurança da camada de Transporte (TLS).

Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.

SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

Suítes de cifra suportadas

Versão TLS	IANA nome do conjunto de cifra
1,2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1,3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Conjuntos de codificação obsoletos

Os seguintes conjuntos de codificação são obsoletos. O suporte para essas cifras será removido em uma versão futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informações relacionadas

"Como as conexões do cliente podem ser configuradas"

Operações de monitoramento e auditoria

Você pode monitorar workloads e eficiências das operações do cliente visualizando tendências de transações para toda a grade ou para nós específicos. Você pode usar mensagens de auditoria para monitorar operações e transações do cliente.

Monitoramento de taxas de ingestão e recuperação de objetos

Você pode monitorar taxas de ingestão e recuperação de objetos, bem como métricas para contagens de objetos, consultas e verificação. Você pode exibir o número de tentativas bem-sucedidas e com falha por aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID.

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. No painel de instrumentos, localize a secção Protocol Operations (operações de protocolo).

   Esta seção resume o número de operações do cliente realizadas pelo seu sistema StorageGRID. As taxas de protocolo são médias nos últimos dois minutos.

3. Selecione **nós**.
4. Na página inicial dos nós (nível de implantação), clique na guia **Load Balancer**.

   Os gráficos mostram tendências para todo o tráfego do cliente direcionado para pontos de extremidade do balanceador de carga dentro da grade. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

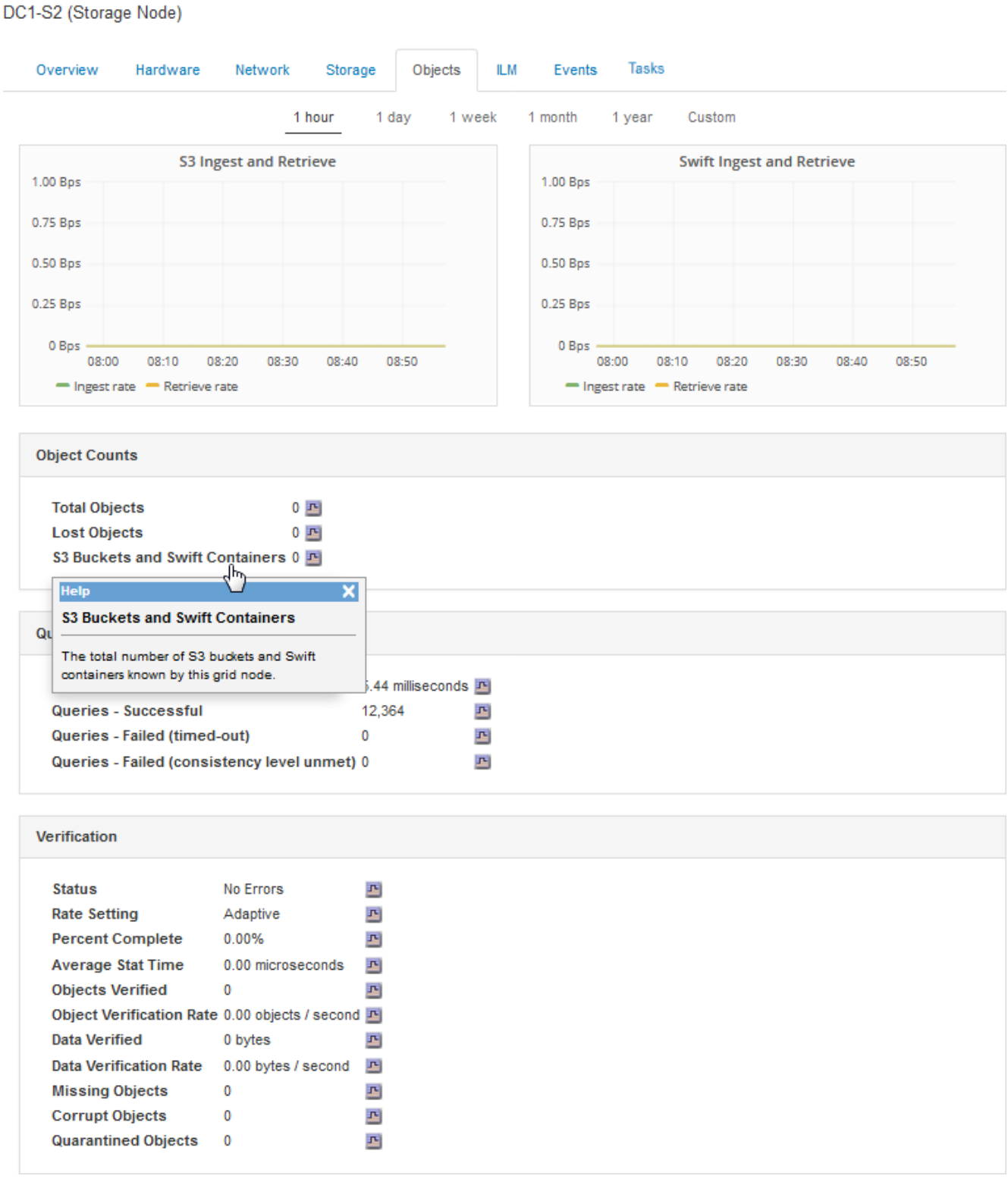
5. Na home page dos nós (nível de implantação), clique na guia **objetos**.

   O gráfico mostra as taxas de ingestão e recuperação de todo o seu sistema StorageGRID em bytes por segundo e total de bytes. Você pode selecionar um intervalo de tempo em horas, dias, semanas, meses ou anos, ou pode aplicar um intervalo personalizado.

6. Para ver as informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e clique na guia **Objects**.

   O gráfico mostra as taxas de ingestão e recuperação de objetos para este nó de armazenamento. A guia também inclui métricas para contagens de objetos, consultas e verificação. Você pode clicar nos rótulos

para ver as definições dessas métricas.



7. Se você quiser ainda mais detalhes:
   a. Selecione **Support** > **Tools** > **Grid Topology**.
   b. Selecione ***site* Visão geral Principal**.

      A seção operações da API exibe informações resumidas para toda a grade.

c. Selecione ***Storage Node* LDR *client Application* Overview Main**

A seção operações exibe informações resumidas para o nó de armazenamento selecionado.

Acesso e revisão de logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. As mensagens de auditoria específicas da API nos logs de auditoria fornecem dados críticos de monitoramento de segurança, operação e desempenho que podem ajudá-lo a avaliar a integridade do sistema.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

Sobre esta tarefa

O arquivo de log de auditoria ativo é `audit.log` chamado , e é armazenado em nós de administração.

Uma vez por dia, o arquivo audit.log ativo é salvo e um novo arquivo audit.log é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato `yyyy-mm-dd.txt`.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz`, que preserva a data original.

Este exemplo mostra o arquivo audit.log ativo, o arquivo do dia anterior (2018-04-15.txt) e o arquivo compactado para o dia anterior (`2018-04-14.txt.gz`).

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

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh *admin@primary_Admin_Node_IP*`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:`cd /var/local/audit/export`
3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

Informações relacionadas

"Rever registos de auditoria"

Operações rápidas rastreadas nos logs de auditoria

Todas as operações bem-sucedidas de EXCLUSÃO, RECEBIMENTO, CABEÇALHO, POST e PUT DE armazenamento são rastreadas no log de auditoria do StorageGRID. As falhas não são registradas, nem são solicitações de informações, autenticação ou OPÇÕES.

Consulte *Entendendo mensagens de auditoria* para obter detalhes sobre as informações rastreadas para as seguintes operações do Swift.

Operações de conta

- OBTER conta
- Conta principal

Operações de contêiner

- ELIMINAR recipiente
- PEGUE o recipiente
- Recipiente DA cabeça
- COLOQUE o recipiente

Operações de objetos

- ELIMINAR objeto
- OBTER objeto
- Objeto PRINCIPAL
- COLOQUE o objeto

Informações relacionadas

"Rever registos de auditoria"

"Operações de conta"

"Operações de contêiner"

"Operações de objetos"

Informações sobre direitos autorais

Informações sobre marcas comerciais