



Gerenciar endpoints de serviços de plataforma

StorageGRID software

NetApp
December 03, 2025

Índice

Gerenciar endpoints de serviços de plataforma	1
Configurar pontos de extremidade de serviços de plataforma	1
O que é um ponto de extremidade de serviços de plataforma?	1
Pontos de extremidade para replicação do CloudMirror	1
Pontos finais para notificações	1
Pontos de extremidade para o serviço de integração de pesquisa	2
Especifique URN para o ponto de extremidade dos serviços de plataforma	2
Elementos URN	2
URNs para serviços hospedados na AWS e GCP	3
URNs para serviços hospedados localmente	3
Criar ponto de extremidade de serviços de plataforma	4
Teste de conexão para ponto de extremidade de serviços de plataforma	9
Editar ponto de extremidade dos serviços da plataforma	10
Excluir ponto de extremidade de serviços de plataforma	11
Solucionar erros de endpoint de serviços de plataforma	12
Determinar se ocorreu um erro	12
Verifique se o erro ainda está presente	12
Resolver erros de endpoint	12
Credenciais de endpoint com permissões insuficientes	13

Gerenciar endpoints de serviços de plataforma

Configurar pontos de extremidade de serviços de plataforma

Antes de configurar um serviço de plataforma para um bucket, você deve configurar pelo menos um endpoint para ser o destino do serviço de plataforma.

O acesso aos serviços da plataforma é habilitado por locatário por um administrador do StorageGRID . Para criar ou usar um ponto de extremidade de serviços de plataforma, você deve ser um usuário locatário com permissão de acesso Gerenciar pontos de extremidade ou Raiz, em uma grade cuja rede foi configurada para permitir que os Nós de Armazenamento acessem recursos de ponto de extremidade externos. Para um único locatário, você pode configurar no máximo 500 pontos de extremidade de serviços de plataforma. Entre em contato com o administrador do StorageGRID para obter mais informações.

O que é um ponto de extremidade de serviços de plataforma?

Um ponto de extremidade de serviços de plataforma especifica as informações que o StorageGRID precisa para acessar o destino externo.

Por exemplo, se você quiser replicar objetos de um bucket do StorageGRID para um bucket do Amazon S3, crie um ponto de extremidade de serviços de plataforma que inclua as informações e credenciais que o StorageGRID precisa para acessar o bucket de destino na Amazon.

Cada tipo de serviço de plataforma requer seu próprio ponto de extremidade, portanto, você deve configurar pelo menos um ponto de extremidade para cada serviço de plataforma que planeja usar. Depois de definir um ponto de extremidade de serviços de plataforma, use o URN do ponto de extremidade como destino no XML de configuração usado para habilitar o serviço.

Você pode usar o mesmo ponto de extremidade como destino para mais de um bucket de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos ao mesmo ponto de extremidade de integração de pesquisa para que você possa realizar pesquisas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite fazer coisas como enviar notificações sobre a criação de objetos para um tópico do Amazon Simple Notification Service (Amazon SNS) e notificações sobre a exclusão de objetos para um segundo tópico do Amazon SNS.

Pontos de extremidade para replicação do CloudMirror

O StorageGRID oferece suporte a endpoints de replicação que representam buckets do S3. Esses buckets podem ser hospedados no Amazon Web Services, na mesma implantação ou em uma implantação remota do StorageGRID ou em outro serviço.

Pontos finais para notificações

O StorageGRID oferece suporte aos endpoints do Amazon SNS e do Kafka. Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Para endpoints do Kafka, o TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido para `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint Kafka.

Pontos de extremidade para o serviço de integração de pesquisa

O StorageGRID oferece suporte a endpoints de integração de pesquisa que representam clusters do Elasticsearch. Esses clusters do Elasticsearch podem estar em um data center local ou hospedados em uma nuvem AWS ou em outro lugar.

O ponto de extremidade de integração de pesquisa refere-se a um índice e tipo específicos do Elasticsearch. Você deve criar o índice no Elasticsearch antes de criar o endpoint no StorageGRID, ou a criação do endpoint falhará. Você não precisa criar o tipo antes de criar o ponto de extremidade. O StorageGRID criará o tipo, se necessário, quando enviar metadados do objeto para o ponto de extremidade.

Informações relacionadas

["Administrar StorageGRID"](#)

Especifique URN para o ponto de extremidade dos serviços de plataforma

Ao criar um ponto de extremidade de serviços de plataforma, você deve especificar um Nome de Recurso Exclusivo (URN). Você usará o URN para referenciar o ponto de extremidade ao criar um XML de configuração para o serviço da plataforma. O URN para cada ponto de extremidade deve ser exclusivo.

O StorageGRID valida os pontos de extremidade dos serviços da plataforma conforme você os cria. Antes de criar um ponto de extremidade de serviços de plataforma, confirme se o recurso especificado no ponto de extremidade existe e se pode ser acessado.

Elementos URN

O URN para um ponto de extremidade de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, do seguinte modo:

- Se o serviço estiver hospedado na Amazon Web Services (AWS), use `arn:aws`
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), use `arn:aws`
- Se o serviço estiver hospedado localmente, use `urn:mysite`

Por exemplo, se você estiver especificando o URN para um endpoint do CloudMirror hospedado no StorageGRID, o URN pode começar com `urn:sgws`.

O próximo elemento do URN especifica o tipo de serviço de plataforma, da seguinte forma:

Serviço	Tipo
Replicação do CloudMirror	s3
Notificações	sns ou kafka
Integração de pesquisa	es

Por exemplo, para continuar especificando o URN para um endpoint do CloudMirror hospedado no StorageGRID, você adicionaria `s3` obter `urn:sgws:s3`.

O elemento final do URN identifica o recurso de destino específico no URI de destino.

Serviço	Recurso específico
Replicação do CloudMirror	<code>bucket-name</code>
Notificações	<code>sns-topic-name</code> ou <code>kafka-topic-name</code>
Integração de pesquisa	<code>domain-name/index-name/type-name</code> Observação: se o cluster do Elasticsearch não estiver configurado para criar índices automaticamente, você deverá criar o índice manualmente antes de criar o endpoint.

URNs para serviços hospedados na AWS e GCP

Para entidades AWS e GCP, o URN completo é um ARN AWS válido. Por exemplo:

- Replicação do CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificações:

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

- Integração de pesquisa:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Para um ponto de extremidade de integração de pesquisa da AWS, o `domain-name` deve incluir a string literal `domain/`, como mostrado aqui.

URNs para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar o URN de qualquer maneira que crie um URN válido e exclusivo, desde que o URN inclua os elementos necessários na terceira e última posição. Você pode deixar os elementos indicados como opcionais em branco ou especificá-los de qualquer forma que ajude a identificar o recurso e tornar a URN única. Por exemplo:

- Replicação do CloudMirror:

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

Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar um URN válido que comece com `urn:sgws:`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- **Notificações:**

Especifique um ponto de extremidade do Amazon Simple Notification Service:

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

Especifique um ponto de extremidade do Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- **Integração de pesquisa:**

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



Para pontos de extremidade de integração de pesquisa hospedados localmente, o `domain-name` element pode ser qualquer string, desde que o URN do ponto final seja único.

Criar ponto de extremidade de serviços de plataforma

Você deve criar pelo menos um ponto de extremidade do tipo correto antes de poder habilitar um serviço de plataforma.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID.
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#).
- O recurso referenciado pelo ponto de extremidade dos serviços da plataforma foi criado:
 - Replicação do CloudMirror: bucket S3
 - Notificação de evento: Amazon Simple Notification Service (Amazon SNS) ou tópico Kafka
 - Notificação de pesquisa: índice do Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.

- Você tem as informações sobre o recurso de destino:
 - Host e porta para o Uniform Resource Identifier (URI)



Se você planeja usar um bucket hospedado em um sistema StorageGRID como um ponto de extremidade para replicação do CloudMirror, entre em contato com o administrador da grade para determinar os valores que você precisa inserir.

- Nome de Recurso Único (URN)

"Especifique URN para o ponto de extremidade dos serviços de plataforma"

- Credenciais de autenticação (se necessário):

Pontos de extremidade de integração de pesquisa

Para endpoints de integração de pesquisa, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- HTTP básico: nome de usuário e senha

Pontos de extremidade de replicação do CloudMirror

Para endpoints de replicação do CloudMirror, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- CAP (C2S Access Portal): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada de cliente opcional.

Pontos de extremidade do Amazon SNS

Para endpoints do Amazon SNS, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta

Pontos finais do Kafka

Para endpoints do Kafka, você pode usar as seguintes credenciais:

- SASL/PLAIN: Nome de usuário e senha
- SASL/SCRAM-SHA-256: Nome de usuário e senha
- SASL/SCRAM-SHA-512: Nome de usuário e senha

- Certificado de segurança (se estiver usando um certificado CA personalizado)
- Se os recursos de segurança do Elasticsearch estiverem habilitados, você terá o privilégio de monitorar cluster para testes de conectividade e o privilégio de gravar índice ou os privilégios de indexar e excluir índice para atualizações de documentos.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**. A página de pontos de extremidade dos serviços da plataforma é exibida.
2. Selecione **Criar ponto de extremidade**.
3. Insira um nome de exibição para descrever brevemente o ponto de extremidade e sua finalidade.

O tipo de serviço de plataforma que o endpoint suporta é mostrado ao lado do nome do endpoint quando ele é listado na página Endpoints, portanto você não precisa incluir essa informação no nome.

4. No campo **URI**, especifique o Identificador de Recurso Único (URI) do ponto de extremidade.

Use um dos seguintes formatos:

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

Se você não especificar uma porta, as seguintes portas padrão serão usadas:

- Porta 443 para URIs HTTPS e porta 80 para URIs HTTP (a maioria dos endpoints)
- Porta 9092 para HTTPS e URIs HTTP (somente endpoints do Kafka)

Por exemplo, o URI para um bucket hospedado no StorageGRID pode ser:

```
https://s3.example.com:10443
```

Neste exemplo, `s3.example.com` representa a entrada DNS para o IP virtual (VIP) do grupo de alta disponibilidade (HA) do StorageGRID e `10443` representa a porta definida no ponto de extremidade do balanceador de carga.



Sempre que possível, você deve se conectar a um grupo HA de nós de balanceamento de carga para evitar um único ponto de falha.

Da mesma forma, o URI para um bucket hospedado na AWS pode ser:

```
https://s3-aws-region.amazonaws.com
```



Se o ponto de extremidade for usado para o serviço de replicação do CloudMirror, não inclua o nome do bucket no URI. Inclua o nome do bucket no campo **URN**.

5. Insira o Nome de Recurso Exclusivo (URN) para o ponto de extremidade.



Não é possível alterar o URN de um endpoint depois que ele for criado.

6. Selecione **Continuar**.

7. Selecione um valor para **Tipo de autenticação**.

Pontos de extremidade de integração de pesquisa

Insira ou carregue as credenciais para um ponto de extremidade de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
HTTP básico	Usa um nome de usuário e uma senha para autenticar conexões com o destino.	• Nome de usuário • Senha

Pontos de extremidade de replicação do CloudMirror

Insira ou carregue as credenciais para um ponto de extremidade de replicação do CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
CAP (Portal de Acesso C2S)	Usa certificados e chaves para autenticar conexões com o destino.	• URL de credenciais temporárias • Certificado CA do servidor (upload de arquivo PEM) • Certificado do cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografada) • Senha da chave privada do cliente (opcional)

Pontos de extremidade do Amazon SNS

Insira ou carregue as credenciais para um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornecer acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta

Pontos finais do Kafka

Insira ou carregue as credenciais para um ponto de extremidade do Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornecer acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
SASL/SIM	Usa um nome de usuário e uma senha com texto simples para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-256	Usa um nome de usuário e uma senha usando um protocolo de desafio-resposta e hash SHA-256 para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-512	Usa um nome de usuário e uma senha usando um protocolo de desafio-resposta e hash SHA-512 para autenticar conexões com o destino.	• Nome de usuário • Senha

Selecione **Usar autenticação de delegação** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **Continuar**.

9. Selecione um botão de opção para **Verificar servidor** para escolher como a conexão TLS com o ponto de extremidade será verificada.

Tipo de verificação do certificado	Descrição
Usar certificado CA personalizado	Use um certificado de segurança personalizado. Se você selecionar esta configuração, copie e cole o certificado de segurança personalizado na caixa de texto Certificado CA .
Usar certificado CA do sistema operacional	Use o certificado Grid CA padrão instalado no sistema operacional para proteger conexões.
Não verificar certificado	O certificado usado para a conexão TLS não foi verificado. Esta opção não é segura.

10. Selecione **Testar e criar ponto de extremidade**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Retornar aos detalhes do endpoint** e atualize as informações. Em seguida, selecione **Testar e criar endpoint**.



A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para sua conta de locatário. Entre em contato com o administrador do StorageGRID .

Depois de configurar um ponto de extremidade, você pode usar seu URN para configurar um serviço de plataforma.

Informações relacionadas

- ["Especifique URN para o ponto de extremidade dos serviços de plataforma"](#)
- ["Configurar a replicação do CloudMirror"](#)
- ["Configurar notificações de eventos"](#)
- ["Configurar serviço de integração de pesquisa"](#)

Teste de conexão para ponto de extremidade de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você poderá testar a conexão do ponto de extremidade para validar se o recurso de destino existe e se pode ser acessado usando as credenciais especificadas.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#) .

Sobre esta tarefa

O StorageGRID não valida se as credenciais têm as permissões corretas.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Selecione o ponto de extremidade cuja conexão você deseja testar.

A página de detalhes do endpoint é exibida.

3. Selecione **Testar conexão**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **Testar e salvar alterações**.

Editar ponto de extremidade dos serviços da plataforma

Você pode editar a configuração de um ponto de extremidade de serviços de plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, talvez você precise atualizar credenciais expiradas ou alterar o URI para apontar para um índice de backup do Elasticsearch para failover. Não é possível alterar o URN de um ponto de extremidade de serviços de plataforma.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#).

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Selecione o ponto de extremidade que você deseja editar.

A página de detalhes do endpoint é exibida.

3. Selecione **Configuração**.

4. Conforme necessário, altere a configuração do ponto de extremidade.



Não é possível alterar o URN de um endpoint depois que ele for criado.

- a. Para alterar o nome de exibição do ponto de extremidade, selecione o ícone de edição
- b. Conforme necessário, altere o URI.
- c. Conforme necessário, altere o tipo de autenticação.
 - Para autenticação de chave de acesso, altere a chave conforme necessário selecionando **Editar**

chave S3 e colando uma nova ID de chave de acesso e uma chave de acesso secreta. Se precisar cancelar suas alterações, selecione **Reverter edição da chave S3**.

- Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha da chave privada do cliente opcional e carregue novos arquivos de certificado e chave conforme necessário.



A chave privada do cliente deve estar no formato criptografado OpenSSL ou no formato de chave privada não criptografada.

d. Conforme necessário, altere o método de verificação do servidor.

5. Selecione **Testar e salvar alterações**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é verificada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto de extremidade para corrigir o erro e selecione **Testar e salvar alterações**.

Excluir ponto de extremidade de serviços de plataforma

Você pode excluir um ponto de extremidade se não quiser mais usar o serviço de plataforma associado.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#).

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Marque a caixa de seleção de cada ponto de extremidade que você deseja excluir.



Se você excluir um ponto de extremidade de serviços de plataforma que está em uso, o serviço de plataforma associado será desabilitado para todos os buckets que usarem o ponto de extremidade. Quaisquer solicitações que ainda não tenham sido concluídas serão descartadas. Quaisquer novas solicitações continuarão a ser geradas até que você altere a configuração do seu bucket para não fazer mais referência ao URN excluído. O StorageGRID relatará essas solicitações como erros irre recuperáveis.

3. Selecione **Ações > Excluir ponto de extremidade**.

Uma mensagem de confirmação é exibida.

4. Selecione **Excluir ponto de extremidade**.

Solucionar erros de endpoint de serviços de plataforma

Se ocorrer um erro quando o StorageGRID tentar se comunicar com um ponto de extremidade de serviços da plataforma, uma mensagem será exibida no painel. Na página Pontos de extremidade dos serviços da plataforma, a coluna Último erro indica há quanto tempo o erro ocorreu. Nenhum erro será exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determinar se ocorreu um erro

Se algum erro de ponto de extremidade de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador de Tenants exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

O mesmo erro que aparece no painel também aparece na parte superior da página de pontos de extremidade dos serviços da plataforma. Para ver uma mensagem de erro mais detalhada:

Passos

1. Na lista de endpoints, selecione o endpoint que apresenta o erro.
2. Na página de detalhes do endpoint, selecione **Conexão**. Esta guia exibe apenas o erro mais recente de um ponto de extremidade e indica há quanto tempo o erro ocorreu. Erros que incluem o ícone X vermelho  ocorreu nos últimos 7 dias.

Verifique se o erro ainda está presente

Alguns erros podem continuar a ser exibidos na coluna **Último erro** mesmo depois de serem resolvidos. Para verificar se um erro é atual ou para forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o ponto final.

A página de detalhes do endpoint é exibida.

2. Selecione **Conexão > Testar conexão**.

Selecionar **Testar conexão** faz com que o StorageGRID valide se o ponto de extremidade dos serviços da plataforma existe e se pode ser acessado com as credenciais atuais. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.

Resolver erros de endpoint

Você pode usar a mensagem **Último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por exemplo, um erro de CloudMirroring pode ocorrer se o StorageGRID não conseguir acessar o bucket S3 de destino porque não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "As credenciais do endpoint ou o acesso ao destino precisam ser atualizados" e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver um erro, selecionar **Testar e salvar alterações** fará com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser acessado com as credenciais atuais. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.

Passos

1. Selecione o ponto final.
2. Na página de detalhes do endpoint, selecione **Configuração**.
3. Edite a configuração do endpoint conforme necessário.
4. Selecione **Conexão > Testar conexão**.

Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um ponto de extremidade de serviços de plataforma, ele confirma que as credenciais do ponto de extremidade podem ser usadas para entrar em contato com o recurso de destino e realiza uma verificação básica de permissões. No entanto, o StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços da plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço de plataforma (como "403 Forbidden"), verifique as permissões associadas às credenciais do endpoint.

Informações relacionadas

- [Administrar StorageGRID > Solucionar problemas de serviços de plataforma](#)
- ["Criar ponto de extremidade de serviços de plataforma"](#)
- ["Teste de conexão para ponto de extremidade de serviços de plataforma"](#)
- ["Editar ponto de extremidade dos serviços da plataforma"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.