Administrar StorageGRID

StorageGRID software

NetApp
December 03, 2025

Índice

Administrar StorageGRID

Administrar StorageGRID

Use estas instruções para configurar e administrar um sistema StorageGRID .

Sobre estas instruções

As principais tarefas para configurar e administrar o StorageGRID permitem que você:

- Use o Grid Manager para configurar grupos e usuários
- Crie contas de locatário para permitir que aplicativos cliente S3 armazenem e recuperem objetos
- Configurar e gerenciar redes StorageGRID
- Configurar AutoSupport
- Gerenciar configurações do nó

Antes de começar

- Você tem uma compreensão geral do sistema StorageGRID .
- Você tem conhecimento bastante detalhado de shells de comando do Linux, redes e configuração e instalação de hardware de servidor.

Comece a usar o Grid Manager

Requisitos do navegador da Web

Você deve usar um navegador da web compatível.

Navegador da web	Versão mínima suportada
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Sign in no Grid Manager

Você acessa a página de login do Grid Manager inserindo o nome de domínio totalmente qualificado (FQDN) ou o endereço IP de um nó de administração na barra de endereços de um navegador da Web compatível.

Cada sistema StorageGRID inclui um nó administrativo primário e qualquer número de nós administrativos não primários. Você pode fazer login no Grid Manager em qualquer nó de administração para gerenciar o sistema StorageGRID . No entanto, alguns procedimentos de manutenção só podem ser executados no nó de administração principal.

Conectar ao grupo HA

Se os nós de administração estiverem incluídos em um grupo de alta disponibilidade (HA), você se conectará usando o endereço IP virtual do grupo de HA ou um nome de domínio totalmente qualificado que mapeie para o endereço IP virtual. O nó de administração principal deve ser selecionado como a interface principal do grupo, para que, ao acessar o Grid Manager, você o acesse no nó de administração principal, a menos que o nó de administração principal não esteja disponível. Ver "Gerenciar grupos de alta disponibilidade" .

Usar SSO

As etapas de login são ligeiramente diferentes se"o logon único (SSO) foi configurado" .

Sign in no Grid Manager no primeiro nó de administração

Antes de começar

- Você tem suas credenciais de login.
- Você está usando um"navegador da web compatível" .
- Os cookies estão habilitados no seu navegador.
- Você pertence a um grupo de usuários que tem pelo menos uma permissão.
- Você tem o URL do Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Você pode usar o nome de domínio totalmente qualificado, o endereço IP de um nó administrativo ou o endereço IP virtual de um grupo HA de nós administrativos.

  Para acessar o Grid Manager em uma porta diferente da porta padrão para HTTPS (443), inclua o número da porta no URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > O SSO não está disponível na porta restrita do Grid Manager. Você deve usar a porta 443.

Passos

1. Inicie um navegador da Web compatível.
2. Na barra de endereço do navegador, digite o URL do Grid Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. Ver "Gerenciar certificados de segurança" .

4. Sign in no Grid Manager.

   A tela de login exibida depende se o logon único (SSO) foi configurado para StorageGRID.

Não usar SSO

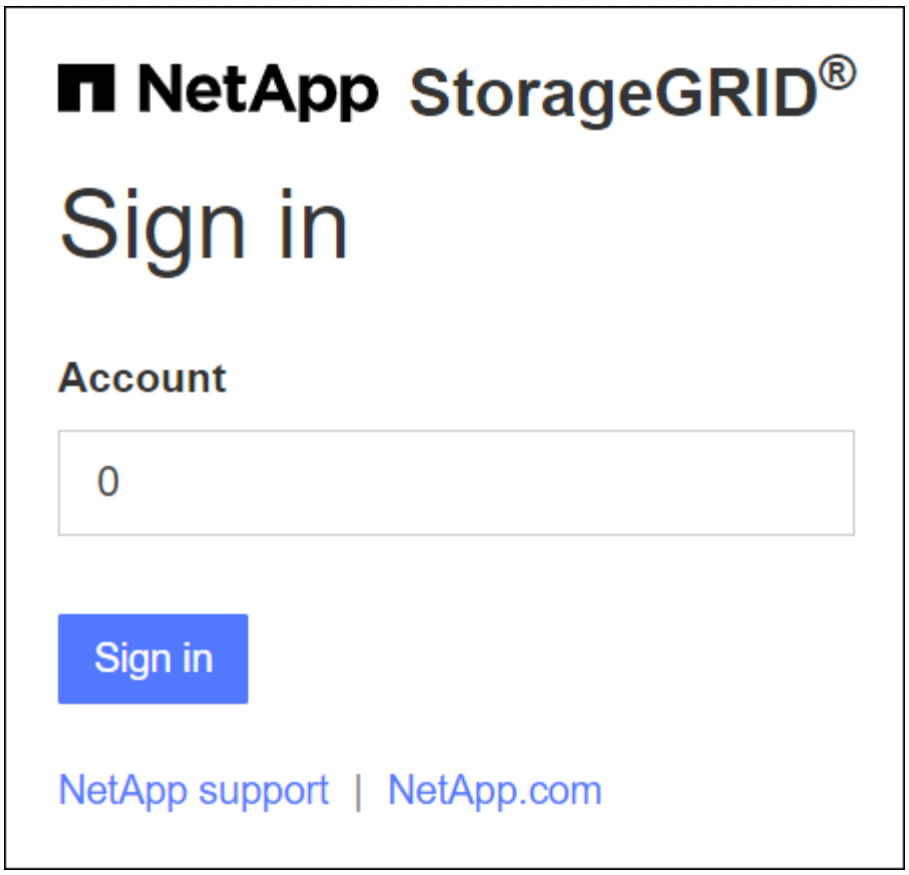
a. Digite seu nome de usuário e senha para o Grid Manager.

b. Selecione **Entrar**.

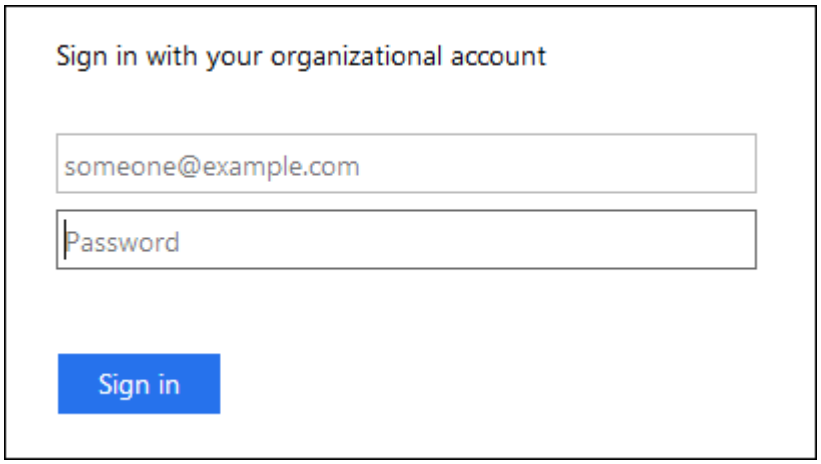
Usando SSO

- Se o StorageGRID estiver usando SSO e esta for a primeira vez que você acessou a URL neste navegador:

  i. Selecione * Sign in*. Você pode deixar o 0 no campo Conta.



ii. Insira suas credenciais SSO padrão na página de login SSO da sua organização. Por exemplo:



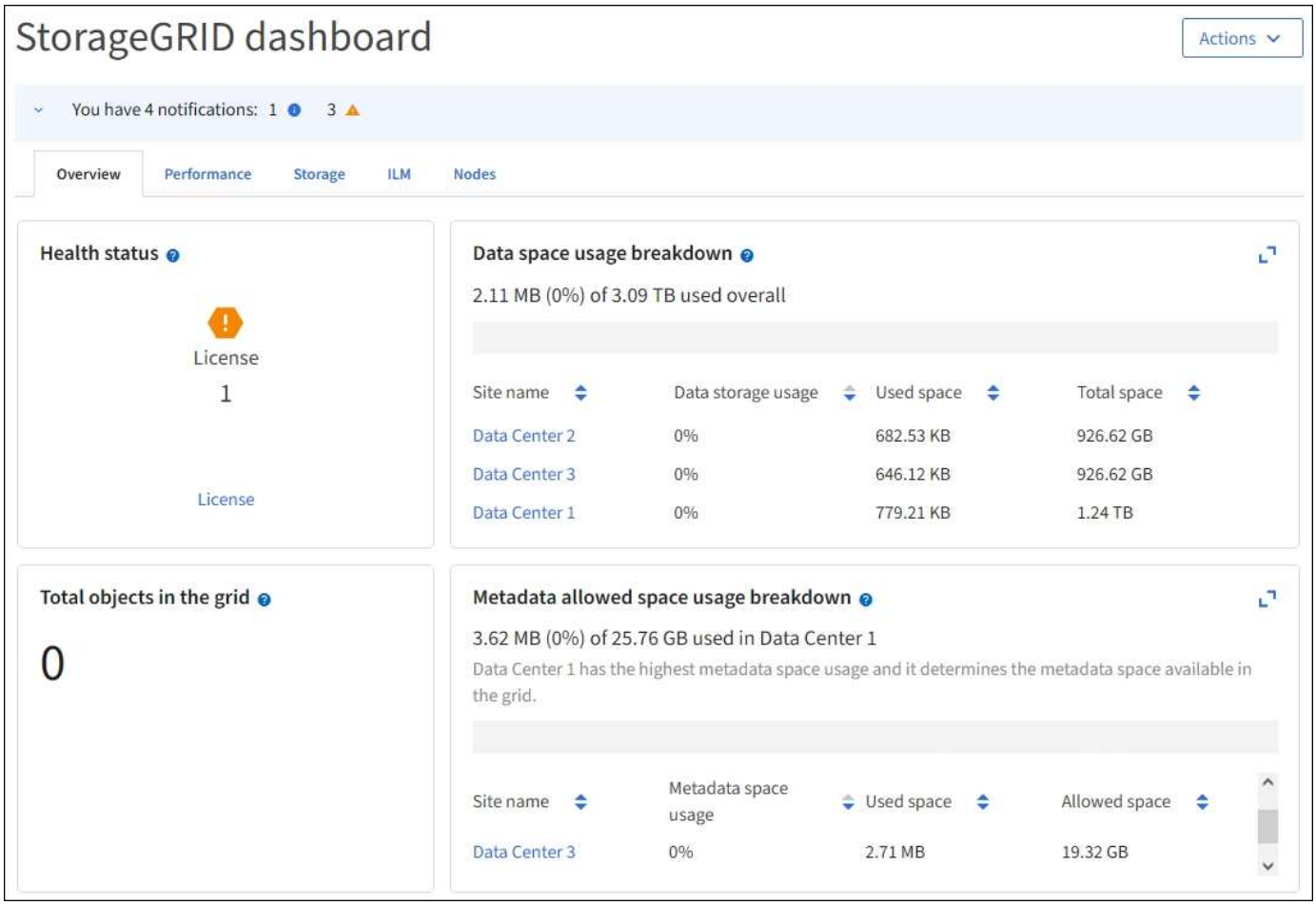
- Se o StorageGRID estiver usando SSO e você tiver acessado anteriormente o Grid Manager ou uma conta de locatário:

  i. Digite **0** (o ID da conta do Grid Manager) ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.

ii. Selecione * Sign in*.

iii. Sign in com suas credenciais SSO padrão na página de login SSO da sua organização.

Quando você estiver conectado, a página inicial do Grid Manager será exibida, incluindo o painel. Para saber quais informações são fornecidas, consulte"Visualizar e gerenciar o painel" .



Entre em outro nó de administração

Siga estas etapas para fazer login em outro nó de administração.

Não usar SSO

Passos

1. Na barra de endereço do navegador, digite o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Inclua o número da porta conforme necessário.
2. Digite seu nome de usuário e senha para o Grid Manager.
3. Selecione **Entrar**.

Usando SSO

Se o StorageGRID estiver usando SSO e você tiver feito login em um nó de administração, poderá acessar outros nós de administração sem precisar fazer login novamente.

Passos

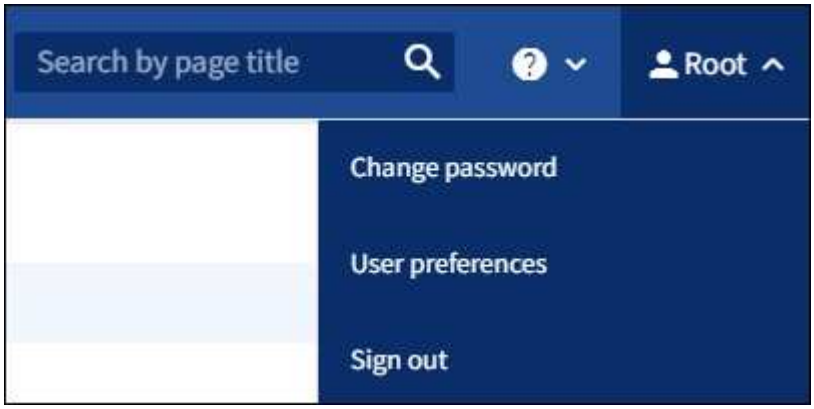
1. Digite o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração na barra de endereços do navegador.
2. Se sua sessão SSO expirou, insira suas credenciais novamente.

Sair do Grid Manager

Quando terminar de trabalhar com o Grid Manager, você deve sair para garantir que usuários não autorizados não possam acessar o sistema StorageGRID . Fechar o navegador pode não desconectar você do sistema, com base nas configurações de cookies do navegador.

Passos

1. Selecione seu nome de usuário no canto superior direito.



2. Selecione **Sair**.

Opção	Descrição
SSO não está em uso	Você está desconectado do nó de administração. A página de login do Grid Manager é exibida. **Observação:** se você tiver entrado em mais de um nó de administração, será necessário sair de cada nó.
SSO habilitado	Você está desconectado de todos os nós de administração que estava acessando. A página de login do StorageGRID é exibida. **Grid Manager** é listado como padrão no menu suspenso **Contas recentes**, e o campo **ID da conta** mostra 0. **Observação:** Se o SSO estiver habilitado e você também estiver conectado ao Gerenciador de locatários, você também deverá"sair da conta do inquilino" para"sair do SSO" .

Alterar sua senha

Se você for um usuário local do Grid Manager, poderá alterar sua própria senha.

Antes de começar

Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Se você fizer login no StorageGRID como um usuário federado ou se o logon único (SSO) estiver habilitado, não será possível alterar sua senha no Grid Manager. Em vez disso, você deve alterar sua senha na fonte de identidade externa, por exemplo, Active Directory ou OpenLDAP.

Passos

1. No cabeçalho do Grid Manager, selecione ***seu nome*** > **Alterar senha**.
2. Digite sua senha atual.
3. Digite uma nova senha.

   Sua senha deve conter no mínimo 8 e no máximo 32 caracteres. As senhas diferenciam maiúsculas de minúsculas.

4. Digite novamente a nova senha.
5. Selecione **Salvar**.

Ver informações da licença do StorageGRID

Você pode visualizar as informações de licença do seu sistema StorageGRID , como a capacidade máxima de armazenamento da sua grade, sempre que necessário.

Antes de começar

Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Se houver um problema com a licença de software para este sistema StorageGRID , o cartão de status de integridade no painel incluirá um ícone de status da licença e um link **Licença**. O número indica o número de problemas relacionados à licença.

Passos

1. Acesse a página de Licença seguindo um destes procedimentos:
   - Selecione **MANUTENÇÃO** > **Sistema** > **Licença**.
   - No cartão Status de integridade no painel, selecione o ícone Status da licença ou o link **Licença**.

     Este link só aparece se houver um problema com a licença.

2. Veja os detalhes somente leitura da licença atual:
    - ID do sistema StorageGRID , que é o número de identificação exclusivo para esta instalação do StorageGRID
    - Número de série da licença
    - Tipo de licença, **Perpétua** ou **Assinatura**
    - Capacidade de armazenamento licenciada da rede
    - Capacidade de armazenamento suportada
    - Data de término da licença. **N/A** aparece para uma licença perpétua.
    - Data de término do suporte

      Esta data é lida do arquivo de licença atual e pode estar desatualizada se você estendeu ou renovou o contrato de serviço de suporte após obter o arquivo de licença. Para atualizar este valor, consulte"Atualizar informações da licença do StorageGRID" . Você também pode visualizar a data real de término do contrato usando o Active IQ.

    - Conteúdo do arquivo de texto da licença

Atualizar informações da licença do StorageGRID

Você deve atualizar as informações da licença do seu sistema StorageGRID sempre que os termos da sua licença forem alterados. Por exemplo, você deve atualizar as informações da licença se comprar capacidade de armazenamento adicional para sua rede.

Antes de começar

- Você tem um novo arquivo de licença para aplicar ao seu sistema StorageGRID .
- Você tem"permissões de acesso específicas" .
- Você tem a senha de provisionamento.

Passos

1. Selecione **MANUTENÇÃO** > **Sistema** > **Licença**.
2. Na seção Atualizar licença, selecione **Procurar**.
3. Localize e selecione o novo arquivo de licença(`.txt`).

   O novo arquivo de licença é validado e exibido.

4. Digite a senha de provisionamento.
5. Selecione **Salvar**.

Use a API

Use a API de gerenciamento de grade

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Grid Management em vez da interface de usuário do Grid Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários,

mais rapidamente.

Recursos de nível superior

A API de gerenciamento de grade fornece os seguintes recursos de nível superior:

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte "Use uma conta de inquilino" .
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

Emitir solicitações de API

A API de gerenciamento de grade usa a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

A interface de usuário do Swagger fornece detalhes completos e documentação para cada operação de API.

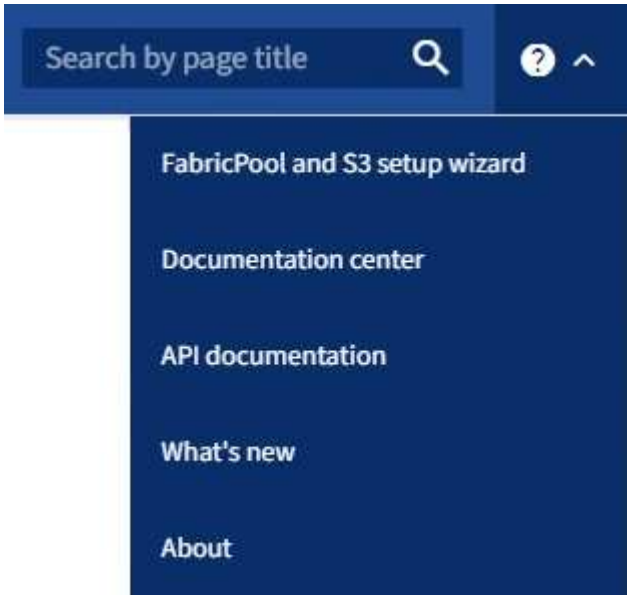
Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

> Todas as operações de API que você realiza usando a página de documentação da API são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. No cabeçalho do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.



2. Para executar uma operação com a API privada, selecione **Ir para a documentação da API privada** na

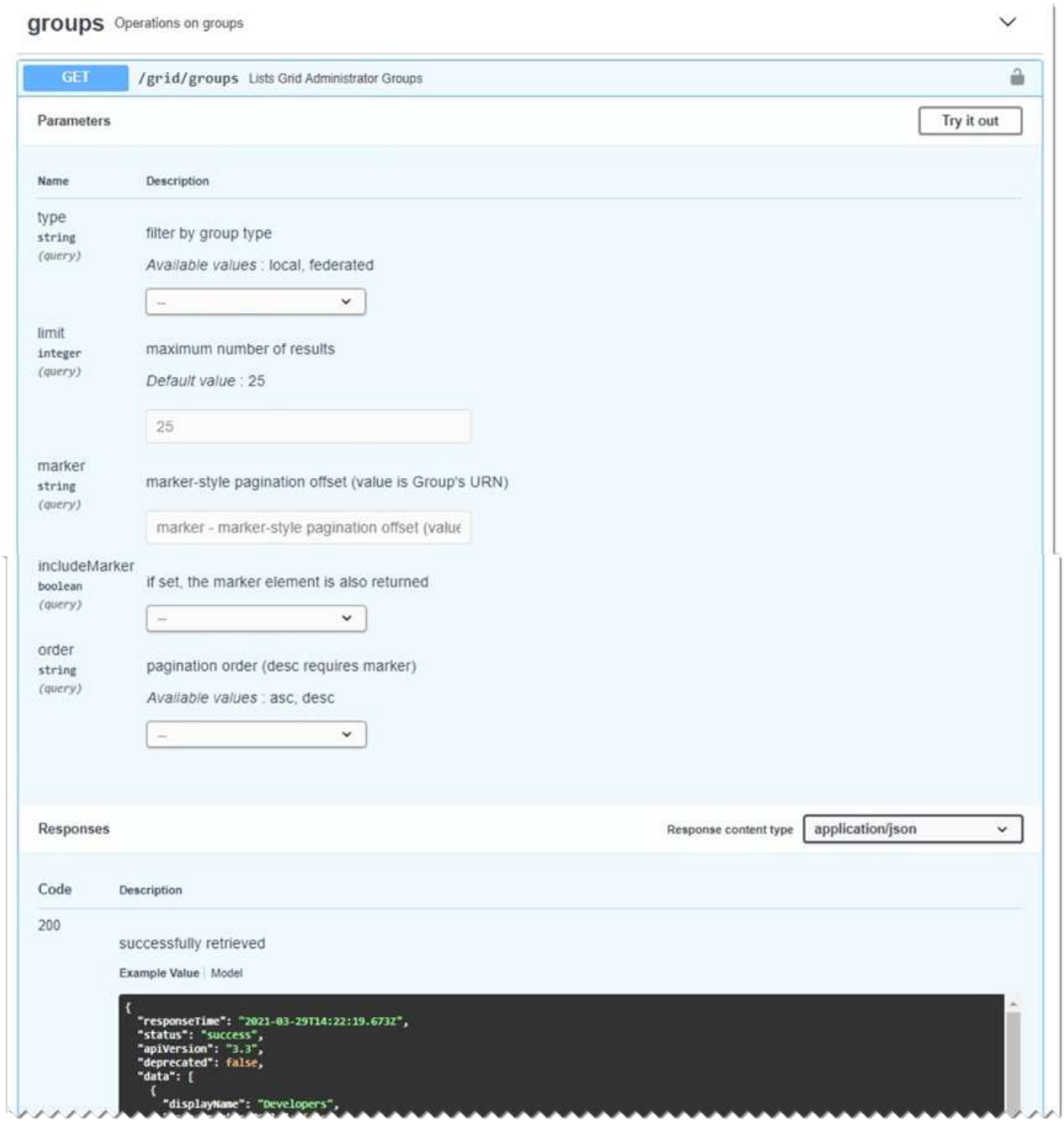
página da API de gerenciamento do StorageGRID .

As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Selecione a operação desejada.

   Ao expandir uma operação de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

4. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo a URL do ponto de extremidade, uma lista de quaisquer parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as respostas possíveis.



5. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou usuário. Então, obtenha esses valores. Talvez seja necessário emitir uma solicitação de API diferente primeiro para obter as informações necessárias.
6. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça quaisquer parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grade

A API de gerenciamento de grade organiza as operações disponíveis nas seguintes seções.

Esta lista inclui apenas operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo a criação de novas contas e a recuperação do uso de armazenamento para uma determinada conta.
- **alert-history**: Operações em alertas resolvidos.
- **alert-receivers**: Operações em receptores de notificação de alerta (e-mail).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **audit**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grade oferece suporte ao esquema de autenticação de token de portador. Para fazer login, você fornece um nome de usuário e uma senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Este token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("Autorização: Token do portador"). O token expira após 16 horas.

  Se o logon único estiver habilitado para o sistema StorageGRID , você deverá executar etapas diferentes para autenticar. Consulte "Autenticação na API se o logon único estiver habilitado".

  Consulte "Proteção contra falsificação de solicitação entre sites" para obter informações sobre como melhorar a segurança da autenticação.

- **client-certificates**: Operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **config**: Operações relacionadas ao lançamento do produto e versões da API de gerenciamento de grade. Você pode listar a versão de lançamento do produto e as principais versões da API de gerenciamento de grade suportadas por essa versão, além de desabilitar versões obsoletas da API.
- **deactivated-features**: Operações para visualizar recursos que podem ter sido desativados.

- **dns-servers**: Operações para listar e alterar servidores DNS externos configurados.
- **drive-details**: Operações em unidades para modelos específicos de dispositivos de armazenamento.
- **endpoint-domain-names**: Operações para listar e alterar nomes de domínio de endpoint S3.
- **erasure-coding**: Operações em perfis de codificação de apagamento.
- **expansão**: Operações de expansão (nível de procedimento).
- **expansion-nodes**: Operações de expansão (nível de nó).
- **expansion-sites**: Operações de expansão (nível de site).
- **grid-networks**: Operações para listar e alterar a Lista de Redes de Grade.
- **grid-passwords**: Operações para gerenciamento de senhas de grade.
- **grupos**: Operações para gerenciar grupos de administradores de grade locais e recuperar grupos de administradores de grade federados de um servidor LDAP externo.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupos federados e usuários.
- **ilm**: Operações em gerenciamento do ciclo de vida da informação (ILM).
- **in-progress-procedures**: Recupera os procedimentos de manutenção que estão em andamento.
- **licença**: Operações para recuperar e atualizar a licença do StorageGRID .
- **logs**: Operações para coleta e download de arquivos de log.v
- **métricas**: Operações em métricas do StorageGRID , incluindo consultas de métricas instantâneas em um único ponto no tempo e consultas de métricas de intervalo ao longo de um intervalo de tempo. A API de gerenciamento de grade usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de backend. Para obter informações sobre como construir consultas do Prometheus, consulte o site do Prometheus.

> ⓘ Métricas que incluem`private` em seus nomes são destinados apenas para uso interno. Essas métricas estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- **node-details**: Operações em detalhes do nó.
- **node-health**: Operações sobre o status de integridade do nó.
- **node-storage-state**: Operações no status de armazenamento do nó.
- **ntp-servers**: Operações para listar ou atualizar servidores externos de Protocolo de Tempo de Rede (NTP).
- **objetos**: Operações em objetos e metadados de objetos.
- **recuperação**: Operações para o procedimento de recuperação.
- **recovery-package**: Operações para baixar o pacote de recuperação.
- **regiões**: Operações para visualizar e criar regiões.
- **s3-object-lock**: Operações nas configurações globais de bloqueio de objetos do S3.
- **server-certificate**: Operações para visualizar e atualizar certificados do servidor do Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **storage-watermarks**: Marcas d'água do nó de armazenamento.
- **traffic-classes**: Operações para políticas de classificação de tráfego.

- **untrusted-client-network**: Operações na configuração de rede de cliente não confiável.
- **usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da API de gerenciamento de grade

A API de gerenciamento de grade usa controle de versão para oferecer suporte a atualizações sem interrupções.

Por exemplo, esta URL de solicitação especifica a versão 4 da API.

`https://hostname_or_ip_address/api/v4/authorize`

A versão principal da API é alterada quando são feitas alterações que *não são compatíveis* com versões mais antigas. A versão secundária da API é alterada quando são feitas alterações que *são compatíveis* com versões mais antigas. Alterações compatíveis incluem a adição de novos pontos de extremidade ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é alterada com base no tipo de alterações feitas.

Tipo de alteração na API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, somente a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID .

> Você pode configurar as versões suportadas. Veja a seção **config** da documentação da API do Swagger para"API de gerenciamento de grade" para mais informações. Você deve desativar o suporte para a versão mais antiga após atualizar todos os clientes da API para usar a versão mais recente.

Solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Obsoleto: verdadeiro"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso obsoleto foi adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinar quais versões de API são suportadas na versão atual

Use o `GET /versions` Solicitação de API para retornar uma lista das principais versões de API suportadas. Esta solicitação está localizada na seção **config** da documentação da API do Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique uma versão de API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho(`/api/v4`) ou um cabeçalho(`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substituirá o valor do caminho.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteja-se contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra o StorageGRID usando tokens CSRF para aprimorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao efetuar login.

Um invasor que pode disparar uma solicitação para um site diferente (como com um formulário HTTP POST) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conectado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro de corpo POST específico.

Para habilitar o recurso, defina o `csrfToken` parâmetro para `true` durante a autenticação. O padrão é `false` .

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando verdadeiro, um `GridCsrfToken` O cookie é definido com um valor aleatório para logins no Grid Manager e o `AccountCsrfToken` O cookie é definido com um valor aleatório para logins no Tenant Manager.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido como o valor do cookie do token CSRF.
- Para terminais que aceitam um corpo codificado em formulário: A `csrfToken` parâmetro do corpo da solicitação codificado em formulário.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.

> Solicitações que tenham um cookie de token CSRF definido também aplicarão o cabeçalho "Content-Type: application/json" para qualquer solicitação que espere um corpo de solicitação JSON como proteção adicional contra ataques CSRF.

Use a API se o logon único estiver habilitado

Use a API se o logon único estiver habilitado (Active Directory)

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o Active Directory como o provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

Estas instruções se aplicam se você estiver usando o Active Directory como provedor de identidade SSO.

Antes de começar

- Você sabe o nome de usuário e a senha do SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` Script Python, que está localizado no diretório de arquivos de instalação do StorageGRID(`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).

- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > ⓘ O fluxo de trabalho curl de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py` Script Python. Vá para o passo 2.
   - Use solicitações curl. Vá para a etapa 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Digite ADFS ou adfs.
   - O nome de usuário do SSO
   - O domínio onde o StorageGRID está instalado
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo usado.

3. Se você quiser usar solicitações curl, use o seguinte procedimento.

   a. Declare as variáveis necessárias para fazer login.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID` .

b. Para receber uma URL de autenticação assinada, emita uma solicitação POST para `/api/v3/authorize-saml` e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma solicitação POST para uma URL de autenticação assinada para `TENANTACCOUNTID` . Os resultados serão repassados para `python -m json.tool` para remover a codificação JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

A resposta para este exemplo inclui uma URL assinada que é codificada por URL, mas não inclui a camada adicional de codificação JSON.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenha uma URL completa que inclua o ID de solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando o URL da resposta anterior.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

A resposta inclui o ID da solicitação do cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salve o ID da solicitação do cliente da resposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envie suas credenciais para a ação do formulário da resposta anterior.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

O AD FS retorna um redirecionamento 302, com informações adicionais nos cabeçalhos.

> Se a autenticação multifator (MFA) estiver habilitada para seu sistema SSO, a postagem do formulário também conterá a segunda senha ou outras credenciais.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salve o `MSISAuth` cookie da resposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envie uma solicitação GET para o local especificado com os cookies do POST de autenticação.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior em caso de logout, e o corpo da resposta conterá o SAMLResponse em um campo de formulário oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salve o `SAMLResponse` do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o salvo `SAMLResponse` , faça um StorageGRID`/api/saml-response` solicitação para gerar

um token de autenticação StorageGRID .

Para `RelayState` , use o ID da conta do locatário ou use 0 se quiser fazer login na API de gerenciamento de grade.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

A resposta inclui o token de autenticação.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salve o token de autenticação na resposta como `MYTOKEN` .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Agora você pode usar `MYTOKEN` para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o Active Directory como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID efetuando logout na página de logout única da sua organização. Ou você pode acionar o logout único (SLO) do StorageGRID, o que requer um token portador do StorageGRID válido.

Passos

1. Para gerar uma solicitação de logout assinada, passe `cookie "sso=true" para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Um URL de logout é retornado:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente da API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Exclua o token portador do StorageGRID .

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `cookie "sso=true" não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UM `204 No Content` a resposta indica que o usuário está desconectado.

```
HTTP/1.1 204 No Content
```

Use a API se o logon único estiver habilitado (Azure)

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o Azure como o provedor de SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatários.

Sign in na API se o logon único do Azure estiver habilitado

Estas instruções se aplicam se você estiver usando o Azure como provedor de identidade SSO

Antes de começar

- Você sabe o endereço de e-mail e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar os seguintes scripts de exemplo:

- O `storagegrid-ssoauth-azure.py` Script Python
- O `storagegrid-ssoauth-azure.js` Script Node.js

Ambos os scripts estão localizados no diretório de arquivos de instalação do StorageGRID(`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).

Para escrever sua própria integração de API com o Azure, consulte o `storagegrid-ssoauth-azure.py` roteiro. O script Python faz duas solicitações diretamente ao StorageGRID (primeiro para obter o SAMLRequest e depois para obter o token de autorização) e também chama o script Node.js para interagir com o Azure para executar as operações de SSO.

As operações de SSO podem ser executadas usando uma série de solicitações de API, mas isso não é simples. O módulo Puppeteer Node.js é usado para extrair dados da interface do Azure SSO.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version` .

Passos

1. Instale as dependências necessárias, da seguinte forma:

a. Instale o Node.js (veja "https://nodejs.org/en/download/").

b. Instale os módulos Node.js necessários (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passe o script Python para o interpretador Python para executá-lo.

   O script Python chamará o script Node.js correspondente para executar as interações do Azure SSO.

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
   - O endereço de e-mail SSO usado para fazer login no Azure
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários
4. Quando solicitado, digite a senha e esteja preparado para fornecer uma autorização MFA ao Azure, se solicitado.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> O script pressupõe que o MFA seja feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para oferecer suporte a outras formas de MFA (como inserir um código recebido em uma mensagem de texto).

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo usado.

Use a API se o logon único estiver habilitado (PingFederate)

Se você tem"configurou e habilitou o logon único (SSO)" e você usa o PingFederate como provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Antes de começar

- Você sabe o nome de usuário e a senha do SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID .
- Se você quiser acessar a API de gerenciamento de locatários, saiba o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` Script Python, que está localizado no diretório de arquivos de instalação do StorageGRID(`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response`.

  > O fluxo de trabalho curl de exemplo não protege a senha de ser vista por outros usuários.

  Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py` Script Python. Vá para o passo 2.
   - Use solicitações curl. Vá para a etapa 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O método SSO. Você pode inserir qualquer variação de "pingfederate" (PINGFEDERATE, pingfederate e assim por diante).
   - O nome de usuário do SSO
   - O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixar em branco ou inserir qualquer valor.
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo usado.
3. Se você quiser usar solicitações curl, use o seguinte procedimento.
   a. Declare as variáveis necessárias para fazer login.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID` .

b. Para receber uma URL de autenticação assinada, emita uma solicitação POST para `/api/v3/authorize-saml` e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma solicitação POST para uma URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para python -m json.tool para remover a codificação JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

A resposta para este exemplo inclui uma URL assinada que é codificada por URL, mas não inclui a camada adicional de codificação JSON.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exporte a resposta e o cookie e faça eco da resposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporte o valor 'pf.adapterId' e repita a resposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporte o valor 'href' (remova a barra final /) e repita a resposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporte o valor 'action':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies junto com as credenciais:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salve o `SAMLResponse` do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o salvo `SAMLResponse` , faça um StorageGRID `/api/saml-response` solicitação para gerar um token de autenticação StorageGRID .

Para `RelayState` , use o ID da conta do locatário ou use 0 se quiser fazer login na API de gerenciamento de grade.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

A resposta inclui o token de autenticação.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salve o token de autenticação na resposta como `MYTOKEN` .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Agora você pode usar `MYTOKEN` para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID efetuando logout na página de logout única da sua organização. Ou você pode acionar o logout único (SLO) do StorageGRID, o que requer um token portador do StorageGRID válido.

Passos

1. Para gerar uma solicitação de logout assinada, passe `cookie "sso=true" para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Um URL de logout é retornado:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente da API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Exclua o token portador do StorageGRID .

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `cookie "sso=true" não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UM `204 No Content` a resposta indica que o usuário está desconectado.

```
HTTP/1.1 204 No Content
```

Desativar recursos com a API

Você pode usar a API de gerenciamento de grade para desativar completamente determinados recursos no sistema StorageGRID . Quando um recurso é desativado, ninguém pode receber permissões para executar as tarefas relacionadas a esse recurso.

Sobre esta tarefa

O sistema Recursos Desativados permite que você impeça o acesso a determinados recursos no sistema StorageGRID . Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administradores com permissão de **acesso root** possam usar esse recurso.

Para entender como essa funcionalidade pode ser útil, considere o seguinte cenário:

_A Empresa A é uma provedora de serviços que aluga a capacidade de armazenamento do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos de seus locatários, a Empresa A quer garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a conta ter sido implantada.

_A empresa A pode atingir esse objetivo usando o sistema Desativar recursos na API de gerenciamento de grade. Ao desativar completamente o recurso **Alterar senha raiz do locatário** no Grid Manager (tanto na IU quanto na API), a Empresa A garante que os usuários administradores — incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **Acesso raiz** — não possam alterar a senha de nenhum usuário raiz da conta do locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. Ver "Use a API de gerenciamento de grade" .
2. Localize o ponto de extremidade Desativar recursos.
3. Para desativar um recurso, como Alterar senha raiz do locatário, envie um corpo para a API como este:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Quando a solicitação for concluída, o recurso Alterar senha raiz do locatário será desabilitado. A permissão de gerenciamento **Alterar senha raiz do locatário** não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falhará com "403 Proibido".

Reativar recursos desativados

Por padrão, você pode usar a API de gerenciamento de grade para reativar um recurso que foi desativado. Entretanto, se você quiser impedir que recursos desativados sejam reativados, você pode desativar o próprio recurso **activateFeatures**.

> O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar este recurso, esteja ciente de que perderá permanentemente a capacidade de reativar quaisquer outros recursos desativados. Você deve entrar em contato com o suporte técnico para restaurar qualquer funcionalidade perdida.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o ponto de extremidade Desativar recursos.
3. Para reativar todos os recursos, envie um corpo para a API como este:

```
{ "grid": null }
```

Quando essa solicitação for concluída, todos os recursos, incluindo o recurso Alterar senha raiz do locatário, serão reativados. A permissão de gerenciamento **Alterar senha raiz do locatário** agora aparece na interface do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário será bem-sucedida, supondo que o usuário tenha a permissão de gerenciamento **Acesso raiz** ou **Alterar senha raiz do locatário**.

> O exemplo anterior faz com que *todos* os recursos desativados sejam reativados. Se outros recursos que devem permanecer desativados tiverem sido desativados, você deverá especificá-los explicitamente na solicitação PUT. Por exemplo, para reativar o recurso Alterar senha raiz do locatário e continuar a desativar a permissão de gerenciamento storageAdmin, envie esta solicitação PUT:
> ```
> { "grid": {"storageAdmin": true} }
> ```

Controle o acesso ao StorageGRID

Controle de acesso ao StorageGRID

Você controla quem pode acessar o StorageGRID e quais tarefas os usuários podem executar criando ou importando grupos e usuários e atribuindo permissões a cada grupo. Opcionalmente, você pode habilitar o logon único (SSO), criar certificados de cliente e alterar senhas de grade.

Controle o acesso ao Grid Manager

Você determina quem pode acessar o Grid Manager e a Grid Management API importando grupos e usuários de um serviço de federação de identidade ou configurando grupos e usuários locais.

Usando"federação de identidade" faz a configuração"grupos" e"Usuários" mais rápido e permite que os usuários façam login no StorageGRID usando credenciais familiares. Você pode configurar a federação de identidade se usar o Active Directory, o OpenLDAP ou o Oracle Directory Server.

> Entre em contato com o suporte técnico se quiser usar outro serviço LDAP v3.

Você determina quais tarefas cada usuário pode executar atribuindo diferentes"permissões" para cada grupo. Por exemplo, você pode querer que usuários em um grupo possam gerenciar regras de ILM e usuários em outro grupo possam executar tarefas de manutenção. Um usuário deve pertencer a pelo menos um grupo para acessar o sistema.

Opcionalmente, você pode configurar um grupo para ser somente leitura. Usuários em um grupo somente leitura podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Grid Manager ou na Grid Management API.

Habilitar logon único

O sistema StorageGRID oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0). Depois de você"configurar e habilitar o SSO" , todos os usuários devem ser autenticados por um provedor de identidade externo antes de poderem acessar o Grid Manager, o Tenant Manager, a Grid Management API ou a Tenant Management API. Usuários locais não podem fazer login no StorageGRID.

Alterar senha de provisionamento

A senha de provisionamento é necessária para muitos procedimentos de instalação e manutenção, e para baixar o Pacote de Recuperação do StorageGRID . A senha também é necessária para baixar backups das informações de topologia de grade e chaves de criptografia para o sistema StorageGRID . Você pode"alterar a senha" conforme necessário.

Alterar senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console do nó, que você precisa para efetuar login no nó como "admin" usando SSH, ou como usuário root em uma conexão de console físico/VM. Conforme necessário, você pode"alterar a senha do console do nó" para cada nó.

Alterar a senha de provisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID . A senha é necessária para procedimentos de recuperação, expansão e manutenção. A senha também é necessária para baixar backups do pacote de recuperação que incluem informações de topologia de grade, senhas de console de nós de grade e chaves de criptografia para o sistema StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem permissões de acesso de manutenção ou root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

A senha de provisionamento é necessária para muitos procedimentos de instalação e manutenção e para"baixando o pacote de recuperação" . A senha de provisionamento não está listada no `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro.

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso**> **Senhas de grade**.
2. Em **Alterar senha de provisionamento**, selecione **Fazer uma alteração**
3. Digite sua senha de provisionamento atual.
4. Digite a nova senha. A senha deve conter no mínimo 8 e no máximo 32 caracteres. As senhas diferenciam maiúsculas de minúsculas.
5. Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.
6. Digite novamente a nova senha e selecione **Salvar**.

   O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento é concluída.

7. Selecione **Pacote de recuperação**.
8. Digite a nova senha de provisionamento para baixar o novo Pacote de Recuperação.

Após alterar a senha de provisionamento, você deve baixar imediatamente um novo Pacote de Recuperação. O arquivo Recovery Package permite restaurar o sistema caso ocorra uma falha.

Alterar senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console do nó, que você precisa para efetuar login no nó. Use estas etapas para alterar a senha exclusiva do console de cada nó na sua grade.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

Use a senha do console do nó para efetuar login em um nó como "admin" usando SSH ou como usuário root em uma conexão de console físico/VM. O processo de alteração de senha do console do nó cria novas senhas para cada nó em sua grade e armazena as senhas em um arquivo atualizado. `Passwords.txt` arquivo no Pacote de Recuperação. As senhas são listadas na coluna Senha no arquivo Passwords.txt.

Há senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. As senhas de acesso SSH não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Senhas de grade**.
2. Em **Alterar senhas do console do nó**, selecione **Fazer uma alteração**.

Digite a senha de provisionamento

Passos

1. Digite a senha de provisionamento para sua grade.
2. Selecione **Continuar**.

Baixe o pacote de recuperação atual

Antes de alterar as senhas do console do nó, baixe o Pacote de Recuperação atual. Você pode usar as senhas neste arquivo se o processo de alteração de senha falhar para qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. Copie o arquivo do pacote de recuperação(`.zip`) para dois locais seguros, protegidos e separados.

O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID .

3. Selecione **Continuar**.
4. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se estiver pronto para começar a alterar as senhas do console do nó.

   Você não pode cancelar este processo depois que ele for iniciado.

Alterar senhas do console do nó

Quando o processo de senha do console do nó é iniciado, um novo Pacote de Recuperação é gerado, incluindo as novas senhas. Em seguida, as senhas são atualizadas em cada nó.

Passos

1. Aguarde a geração do novo Pacote de Recuperação, o que pode levar alguns minutos.
2. Selecione **Baixar novo pacote de recuperação**.
3. Quando o download for concluído:

   a. Abra o `.zip` arquivo.

   b. Confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas senhas do console do nó.

   c. Copie o novo arquivo do pacote de recuperação(`.zip`) para dois locais seguros, protegidos e separados.

   > Não substitua o antigo Pacote de Recuperação.

   O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID .

4. Marque a caixa de seleção para indicar que você baixou o novo Pacote de Recuperação e verificou o conteúdo.
5. Selecione **Alterar senhas do console do nó** e aguarde até que todos os nós sejam atualizados com as novas senhas. Isso pode levar alguns minutos.

   Se as senhas forem alteradas para todos os nós, um banner verde de sucesso será exibido. Vá para o próximo passo.

   Se houver um erro durante o processo de atualização, uma mensagem de banner listará o número de nós que não tiveram suas senhas alteradas. O sistema repetirá automaticamente o processo em qualquer nó cuja senha não tenha sido alterada. Se o processo terminar com alguns nós ainda sem uma senha alterada, o botão **Repetir** será exibido.

   Se a atualização da senha falhar para um ou mais nós:

   a. Revise as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

   > Tentar novamente altera apenas as senhas do console do nó nos nós que falharam durante tentativas anteriores de alteração de senha.

6. Depois que as senhas do console do nó forem alteradas para todos os nós, exclua oprimeiro pacote de recuperação que você baixou .
7. Opcionalmente, use o link **Pacote de recuperação** para baixar uma cópia adicional do novo Pacote de recuperação.

Alterar senhas de acesso SSH para nós de administração

Alterar as senhas de acesso SSH para nós de administração também atualiza os conjuntos exclusivos de chaves SSH internas para cada nó na grade. O nó de administração principal usa essas chaves SSH para acessar nós usando autenticação segura e sem senha.

Use uma chave SSH para efetuar login em um nó como `admin` ou para o usuário root em uma VM ou conexão de console físico.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

As novas senhas de acesso para os nós de administração e as novas chaves internas para cada nó são armazenadas no `Passwords.txt` arquivo no Pacote de Recuperação. As chaves estão listadas na coluna Senha desse arquivo.

Há senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. Elas não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Senhas de grade**.
2. Em **Alterar chaves SSH**, selecione **Fazer uma alteração**.

Baixe o pacote de recuperação atual

Antes de alterar as chaves de acesso SSH, baixe o Pacote de Recuperação atual. Você pode usar as chaves neste arquivo se o processo de alteração de chave falhar para qualquer nó.

Passos

1. Digite a senha de provisionamento para sua grade.
2. Selecione **Baixar pacote de recuperação**.
3. Copie o arquivo do pacote de recuperação(`.zip`) para dois locais seguros, protegidos e separados.

> O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID .

4. Selecione **Continuar**.

5. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se estiver pronto para começar a alterar as chaves de acesso SSH.

   Você não pode cancelar este processo depois que ele for iniciado.

Alterar chaves de acesso SSH

Quando o processo de alteração das chaves de acesso SSH é iniciado, um novo Pacote de Recuperação é gerado, incluindo as novas chaves. Em seguida, as chaves são atualizadas em cada nó.

Passos

1. Aguarde a geração do novo Pacote de Recuperação, o que pode levar alguns minutos.
2. Quando o botão Baixar novo pacote de recuperação estiver habilitado, selecione **Baixar novo pacote de recuperação** e salve o novo arquivo do pacote de recuperação(`.zip`) para dois locais seguros, protegidos e separados.
3. Quando o download for concluído:

   a. Abra o `.zip` arquivo.

   b. Confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas chaves de acesso SSH.

   c. Copie o novo arquivo do pacote de recuperação(`.zip`) para dois locais seguros, protegidos e separados.

      Não substitua o antigo Pacote de Recuperação.

   O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID .

4. Aguarde a atualização das chaves em cada nó, o que pode levar alguns minutos.

   Se as chaves forem alteradas para todos os nós, um banner verde de sucesso será exibido.

   Se houver um erro durante o processo de atualização, uma mensagem de banner listará o número de nós que não tiveram suas chaves alteradas. O sistema repetirá automaticamente o processo em qualquer nó cuja chave não tenha sido alterada. Se o processo terminar com alguns nós ainda sem uma chave alterada, o botão **Repetir** será exibido.

   Se a atualização da chave falhar para um ou mais nós:

   a. Revise as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

      Tentar novamente altera apenas as chaves de acesso SSH nos nós que falharam durante tentativas anteriores de alteração de chave.

5. Após as chaves de acesso SSH terem sido alteradas para todos os nós, exclua oprimeiro pacote de recuperação que você baixou .
6. Opcionalmente, selecione **MANUTENÇÃO** > **Sistema** > **Pacote de recuperação** para baixar uma cópia adicional do novo Pacote de recuperação.

Usar federação de identidade

O uso da federação de identidades agiliza a configuração de grupos e usuários e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configurar federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Grid Manager se quiser que grupos de administradores e usuários sejam gerenciados em outro sistema, como Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você está usando o Active Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

> Se você quiser usar um serviço LDAP v3 que não esteja listado, entre em contato com o suporte técnico.

- Se você planeja usar o OpenLDAP, deverá configurar o servidor OpenLDAP. Ver Diretrizes para configurar um servidor OpenLDAP .
- Se você planeja habilitar o logon único (SSO), você revisou o"requisitos e considerações para logon único" .
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade está usando o TLS 1.2 ou 1.3. Ver "Cifras suportadas para conexões TLS de saída" .

Sobre esta tarefa

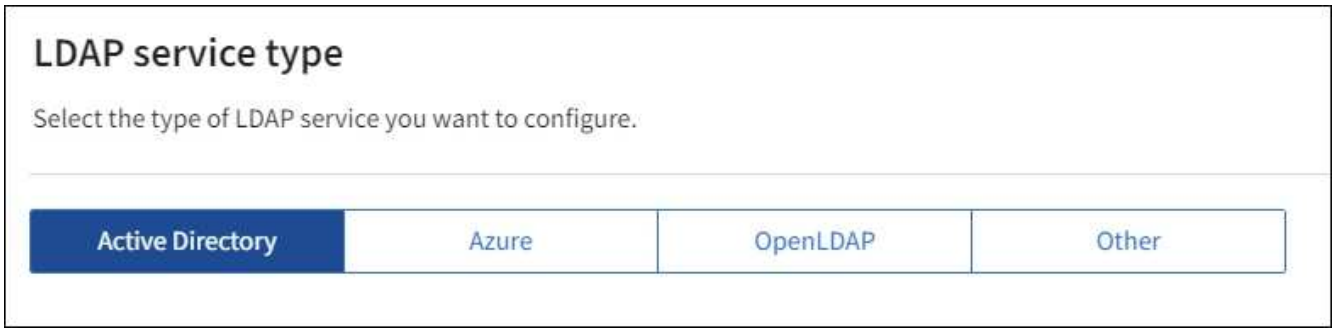
Você pode configurar uma fonte de identidade para o Grid Manager se quiser importar grupos de outro sistema, como Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- Grupos de administradores. Os usuários em grupos de administradores podem entrar no Grid Manager e executar tarefas com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários locatários para locatários que não usam sua própria fonte de identidade. Usuários em grupos de locatários podem entrar no Gerenciador de Locatários e executar tarefas com base nas permissões atribuídas ao grupo no Gerenciador de Locatários. Ver"Criar conta de inquilino" e"Use uma conta de inquilino" para mais detalhes.

Digite a configuração

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Federação de identidade**.
2. Selecione **Ativar federação de identidade**.
3. Na seção Tipo de serviço LDAP, selecione o tipo de serviço LDAP que você deseja configurar.



Selecione **Outro** para configurar valores para um servidor LDAP que usa o Oracle Directory Server.

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para o Active Directory e `uid` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `uid` .
   - **UUID do usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `nsuniqueid` . O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos em formato de 16 bytes ou string, onde hifens são ignorados.
   - **Nome exclusivo do grupo**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para o Active Directory e `cn` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `cn` .
   - **UUID do grupo**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `nsuniqueid` . O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos em formato de 16 bytes ou string, onde hifens são ignorados.
5. Para todos os tipos de serviço LDAP, insira as informações necessárias do servidor LDAP e da conexão de rede na seção Configurar servidor LDAP.
   - **Nome do host**: O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Porta**: A porta usada para conectar ao servidor LDAP.

     A porta padrão para STARTTLS é 389, e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta, desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome distinto (DN) do usuário que se conectará ao servidor LDAP.

     Para o Active Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     O usuário especificado deve ter permissão para listar grupos e usuários e acessar os seguintes atributos:

     - `sAMAccountName`ou `uid`
     - `objectGUID`, `entryUUID` , ou `nsuniqueid`

- `cn`
- `memberOf`ou `isMemberOf`
- **Active Directory**: `objectSid` , `primaryGroupID` , `userAccountControl` , e `userPrincipalName`
- **Azul**: `accountEnabled` e `userPrincipalName`

◦ **Senha**: A senha associada ao nome de usuário.

> Se você alterar a senha no futuro, deverá atualizá-la nesta página.

◦ **DN base do grupo**: O caminho completo do nome distinto (DN) para uma subárvore LDAP na qual você deseja pesquisar grupos. No exemplo do Active Directory (abaixo), todos os grupos cujo Nome Distinto é relativo ao DN base (DC=storagegrid,DC=example,DC=com) podem ser usados como grupos federados.

> Os valores de **Nome exclusivo do grupo** devem ser exclusivos dentro do **DN base do grupo** ao qual pertencem.

◦ **DN base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP na qual você deseja pesquisar usuários.

> Os valores de **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN base do usuário** ao qual pertencem.

◦ **Formato de nome de usuário vinculado** (opcional): O padrão de nome de usuário padrão que o StorageGRID deve usar se o padrão não puder ser determinado automaticamente.

É recomendável fornecer o **formato de nome de usuário de associação** porque ele pode permitir que os usuários efetuem login caso o StorageGRID não consiga se associar à conta de serviço.

Insira um destes padrões:

- **Padrão UserPrincipalName (Active Directory e Azure)**: `[USERNAME]@*example*.com`
- **Padrão de nome de logon de nível inferior (Active Directory e Azure)**: `*example*\[USERNAME]`
- **Padrão de nome distinto**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Inclua **[USERNAME]** exatamente como escrito.

6. Na seção Segurança da Camada de Transporte (TLS), selecione uma configuração de segurança.
   ◦ **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para Active Directory, OpenLDAP ou Outros, mas esta opção não é suportada pelo Azure.
   ◦ **Usar LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar esta opção para o Azure.
   ◦ **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada pelo Azure.

O uso da opção **Não usar TLS** não é suportado se o seu servidor Active Directory impõe assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.
   - **Usar certificado CA do sistema operacional**: Use o certificado CA padrão do Grid instalado no sistema operacional para proteger conexões.
   - **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 de CA.

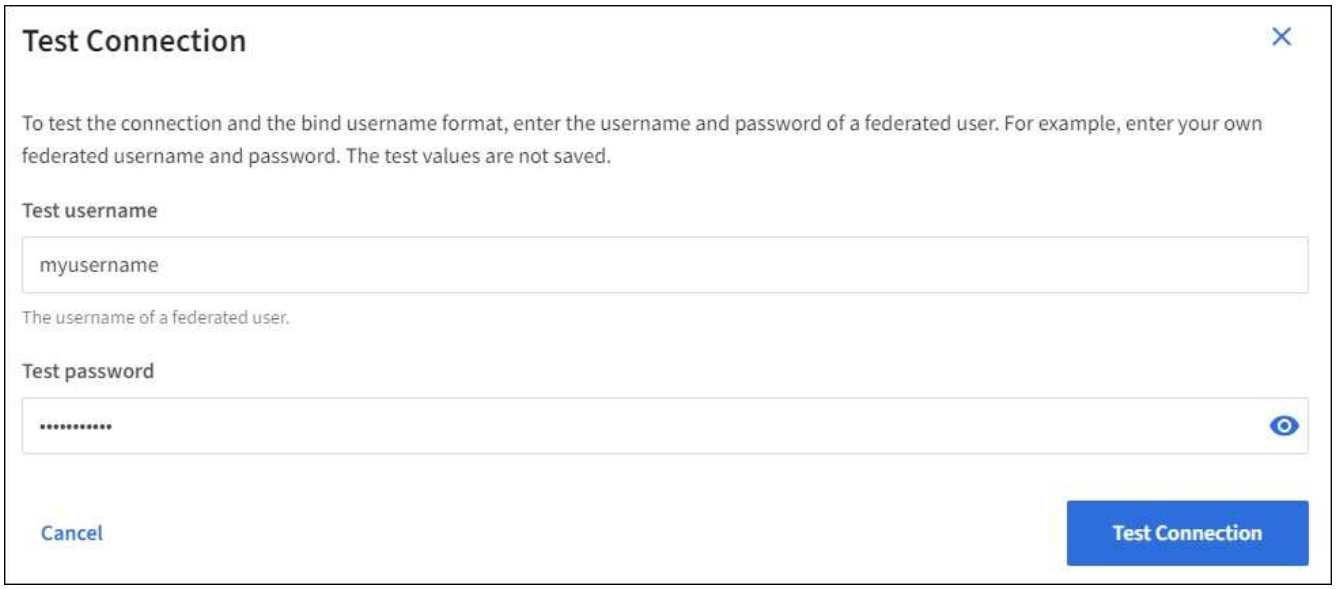
Teste a conexão e salve a configuração

Depois de inserir todos os valores, você deve testar a conexão antes de salvar a configuração. O StorageGRID verifica as configurações de conexão do servidor LDAP e o formato do nome de usuário de vinculação, se você forneceu um.

Passos

1. Selecione **Testar conexão**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
   - A mensagem "Teste de conexão bem-sucedido" será exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
   - A mensagem "não foi possível estabelecer a conexão de teste" aparece se as configurações de conexão forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você forneceu um formato de nome de usuário vinculado, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, digite seu próprio nome de usuário e senha. Não inclua nenhum caractere especial no nome de usuário, como @ ou /.



   - A mensagem "Teste de conexão bem-sucedido" será exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.

- Uma mensagem de erro será exibida se as configurações de conexão, o formato do nome de usuário de vinculação ou o nome de usuário e a senha de teste forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos federados e usuários da fonte de identidade. Você pode forçar o início da sincronização se quiser habilitar ou restringir as permissões do usuário o mais rápido possível.

Passos

1. Acesse a página da Federação de Identidade.
2. Selecione **Servidor de sincronização** no topo da página.

   O processo de sincronização pode levar algum tempo dependendo do seu ambiente.

   O alerta **Falha na sincronização da federação de identidade** é acionado se houver um problema na sincronização de grupos federados e usuários da fonte de identidade.

Desabilitar federação de identidade

Você pode desabilitar temporária ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desabilitada, não há comunicação entre o StorageGRID e a origem da identidade. No entanto, todas as configurações que você definiu serão mantidas, permitindo que você reative facilmente a federação de identidades no futuro.

Sobre esta tarefa

Antes de desabilitar a federação de identidades, você deve estar ciente do seguinte:

- Usuários federados não poderão fazer login.
- Usuários federados que estão conectados no momento manterão acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá, e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidade** será desabilitada se o logon único (SSO) estiver definido como **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desativado** antes que você possa desabilitar a federação de identidades. Ver "Desativar logon único" .

Passos

1. Acesse a página da Federação de Identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

Diretrizes para configurar um servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, deverá configurar definições específicas no servidor OpenLDAP.

Para fontes de identidade que não sejam ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso ao S3 para usuários desabilitados externamente. Para bloquear o acesso ao S3, exclua todas as chaves S3 do usuário ou remova o usuário de todos os grupos.

Sobreposições de membro e reintegração

As sobreposições memberof e refint devem ser habilitadas. Para obter mais informações, consulte as instruções para manutenção de associação de grupo reverso nohttp://www.openldap.org/doc/admin24/index.html["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"^] .

Indexação

Você deve configurar os seguintes atributos OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda para Nome de usuário sejam indexados para desempenho ideal.

Veja as informações sobre manutenção de associação de grupo reverso nohttp://www.openldap.org/doc/admin24/index.html["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"^] .

Gerenciar grupos de administradores

Você pode criar grupos de administradores para gerenciar as permissões de segurança de um ou mais usuários administradores. Os usuários devem pertencer a um grupo para ter acesso ao sistema StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Se você planeja importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na fonte de identidade configurada.

Criar um grupo de administradores

Os grupos de administradores permitem que você determine quais usuários podem acessar quais recursos e operações no Grid Manager e na Grid Management API.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Grupos de administradores**.

2. Selecione **Criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

- Crie um grupo local se quiser atribuir permissões a usuários locais.
- Crie um grupo federado para importar usuários da fonte de identidade.

Grupo local

Passos

1. Selecione **Grupo local**.
2. Insira um nome de exibição para o grupo, que você pode atualizar posteriormente, conforme necessário. Por exemplo, "Usuários de Manutenção" ou "Administradores de ILM".
3. Digite um nome exclusivo para o grupo, que você não poderá atualizar posteriormente.
4. Selecione **Continuar**.

Grupo federado

Passos

1. Selecione **Grupo federado**.
2. Digite o nome do grupo que você deseja importar, exatamente como ele aparece na fonte de identidade configurada.
   - Para o Active Directory e o Azure, use o sAMAccountName.
   - Para OpenLDAP, use o CN (Nome Comum).
   - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **Continuar**.

Gerenciar permissões de grupo

Passos

1. Para **Modo de acesso**, selecione se os usuários do grupo podem alterar as configurações e executar operações no Grid Manager e na Grid Management API ou se eles podem apenas visualizar as configurações e os recursos.
   - **Leitura e gravação** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: os usuários podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Grid Manager ou na Grid Management API. Usuários locais somente leitura podem alterar suas próprias senhas.

   > Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **Somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

2. Selecione um ou mais"permissões do grupo de administração" .

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao

grupo não poderão fazer login no StorageGRID.

3. Se você estiver criando um grupo local, selecione **Continuar**. Se você estiver criando um grupo federado, selecione **Criar grupo** e **Concluir**.

Adicionar usuários (somente grupos locais)

Passos

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.

   Se você ainda não criou usuários locais, você pode salvar o grupo sem adicionar usuários. Você pode adicionar este grupo ao usuário na página Usuários. Ver"Gerenciar usuários" para mais detalhes.

2. Selecione **Criar grupo** e **Concluir**.

Ver e editar grupos de administradores

Você pode visualizar detalhes de grupos existentes, modificar um grupo ou duplicar um grupo.

- Para visualizar informações básicas de todos os grupos, revise a tabela na página Grupos.
- Para visualizar todos os detalhes de um grupo específico ou editar um grupo, use o menu **Ações** ou a página de detalhes.

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do grupo	a. Marque a caixa de seleção do grupo. b. Selecione **Ações** > **Exibir detalhes do grupo**.	Selecione o nome do grupo na tabela.
Editar nome de exibição (somente grupos locais)	a. Marque a caixa de seleção do grupo. b. Selecione **Ações** > **Editar nome do grupo**. c. Digite o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Salvar alterações**.
Editar modo de acesso ou permissões	a. Marque a caixa de seleção do grupo. b. Selecione **Ações** > **Exibir detalhes do grupo**. c. Opcionalmente, altere o Modo de acesso do grupo. d. Opcionalmente, selecione ou desmarque"permissões do grupo de administração" . e. Selecione **Salvar alterações**.	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o Modo de acesso do grupo. c. Opcionalmente, selecione ou desmarque"permissões do grupo de administração" . d. Selecione **Salvar alterações**.

Duplicar um grupo

Passos

1. Marque a caixa de seleção do grupo.
2. Selecione **Ações** > **Duplicar grupo**.
3. Conclua o assistente Duplicar grupo.

Excluir um grupo

Você pode excluir um grupo de administradores quando quiser removê-lo do sistema e remover todas as permissões associadas ao grupo. Excluir um grupo de administradores remove todos os usuários do grupo, mas não exclui os usuários.

Passos

1. Na página Grupos, marque a caixa de seleção de cada grupo que deseja remover.
2. Selecione **Ações** > **Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões do grupo de administração

Ao criar grupos de usuários administradores, você seleciona uma ou mais permissões para controlar o acesso a recursos específicos do Grid Manager. Você pode então atribuir cada usuário a um ou mais desses grupos de administradores para determinar quais tarefas cada usuário pode executar.

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão fazer login no Grid Manager ou na Grid Management API.

Por padrão, qualquer usuário que pertença a um grupo que tenha pelo menos uma permissão pode executar as seguintes tarefas:

- Sign in no Grid Manager
- Ver o painel
- Ver as páginas dos nós
- Ver alertas atuais e resolvidos
- Alterar sua própria senha (somente usuários locais)
- Veja certas informações fornecidas nas páginas de Configuração e Manutenção

Interação entre permissões e modo de acesso

Para todas as permissões, a configuração **Modo de acesso** do grupo determina se os usuários podem alterar as configurações e executar operações ou se eles podem apenas visualizar as configurações e os recursos relacionados. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **Somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

As seções a seguir descrevem as permissões que você pode atribuir ao criar ou editar um grupo de administradores. Qualquer funcionalidade não explicitamente mencionada requer a permissão **Acesso root**.

Acesso root

Esta permissão fornece acesso a todos os recursos de administração da grade.

Alterar senha raiz do locatário

Esta permissão fornece acesso à opção **Alterar senha root** na página Locatários, permitindo que você controle quem pode alterar a senha do usuário root local do locatário. Essa permissão também é usada para migrar chaves S3 quando o recurso de importação de chaves S3 está habilitado. Usuários que não têm essa permissão não podem ver a opção **Alterar senha root**.

> Para conceder acesso à página de locatários, que contém a opção **Alterar senha de root**, atribua também a permissão **Contas de locatários**.

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPORTE** > **Ferramentas** > **Topologia de grade**.

> A página de topologia de grade foi descontinuada e será removida em uma versão futura.

ILM

Esta permissão fornece acesso às seguintes opções de menu **ILM**:

- Regras
- Políticas
- Tags de política
- Pools de armazenamento
- Graus de armazenamento
- Regiões
- Pesquisa de metadados de objetos

> Os usuários devem ter as permissões **Outra configuração de grade** e **Configuração da página de topologia de grade** para gerenciar níveis de armazenamento.

Manutenção

Os usuários devem ter permissão de Manutenção para usar estas opções:

- **CONFIGURAÇÃO** > **Controle de acesso**:
  - Senhas de grade
- **CONFIGURAÇÃO** > **Rede**:
  - Nomes de domínio de endpoint S3
- **MANUTENÇÃO** > **Tarefas**:
  - Descomissionamento
  - Expansão
  - Verificação de existência de objeto
  - Recuperação
- **MANUTENÇÃO** > **Sistema**:

    - Pacote de recuperação
    - Atualização de software
- **SUPORTE** > **Ferramentas**:
    - Registros

Usuários que não têm permissão de Manutenção podem visualizar, mas não editar, estas páginas:

- **MANUTENÇÃO** > **Rede**:
    - Servidores DNS
    - Rede de grade
    - Servidores NTP
- **MANUTENÇÃO** > **Sistema**:
    - Licença
- **CONFIGURAÇÃO** > **Rede**:
    - Nomes de domínio de endpoint S3
- **CONFIGURAÇÃO** > **Segurança**:
    - Certificados
- **CONFIGURAÇÃO** > **Monitoramento**:
    - Servidor de auditoria e syslog

Gerenciar alertas

Esta permissão fornece acesso a opções para gerenciar alertas. Os usuários devem ter essa permissão para gerenciar silêncios, notificações de alerta e regras de alerta.

Consulta de métricas

Esta permissão fornece acesso a:

- **SUPORTE** > **Ferramentas** > página **Métricas**
- Consultas de métricas personalizadas do Prometheus usando a seção **Métricas** da API de gerenciamento de grade
- Cartões do painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM** > **Consulta de metadados do objeto**.

Outra configuração de grade

Esta permissão fornece acesso a opções adicionais de configuração de grade.

> Para ver essas opções adicionais, os usuários também devem ter a permissão **Configuração da página de topologia de grade**.

- **ILM**:

    - Graus de armazenamento
- **CONFIGURAÇÃO** > **Sistema**:
- **SUPORTE** > **Outros**:
    - Custo do link

Administrador do dispositivo de armazenamento

Esta permissão fornece:

- Acesso ao E-Series SANtricity System Manager em dispositivos de armazenamento por meio do Grid Manager.
- A capacidade de executar tarefas de solução de problemas e manutenção na guia Gerenciar unidades para dispositivos que oferecem suporte a essas operações.

Contas de inquilinos

Esta permissão fornece a capacidade de:

- Acesse a página de inquilinos, onde você pode criar, editar e remover contas de inquilinos
- Ver políticas de classificação de tráfego existentes
- Exibir cartões do painel do Grid Manager que contêm detalhes do locatário

Gerenciar usuários

Você pode visualizar usuários locais e federados. Você também pode criar usuários locais e atribuí-los a grupos de administradores locais para determinar quais recursos do Grid Manager esses usuários podem acessar.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Criar um usuário local

Você pode criar um ou mais usuários locais e atribuir cada usuário a um ou mais grupos locais. As permissões do grupo controlam quais recursos do Grid Manager e da Grid Management API o usuário pode acessar.

Você pode criar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários e grupos federados.

O Grid Manager inclui um usuário local predefinido, chamado "root". Você não pode remover o usuário root.

> Se o logon único (SSO) estiver habilitado, os usuários locais não poderão fazer login no StorageGRID.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Usuários administradores**.

2. Selecione **Criar usuário**.

Insira as credenciais do usuário

Passos

1. Digite o nome completo do usuário, um nome de usuário exclusivo e uma senha.
2. Opcionalmente, selecione **Sim** se este usuário não quiser ter acesso ao Grid Manager ou à Grid Management API.
3. Selecione **Continuar**.

Atribuir a grupos

Passos

1. Opcionalmente, atribua o usuário a um ou mais grupos para determinar suas permissões.

   Se você ainda não criou grupos, pode salvar o usuário sem selecionar grupos. Você pode adicionar este usuário a um grupo na página Grupos.

   Se um usuário pertencer a vários grupos, as permissões serão cumulativas. Ver"Gerenciar grupos de administradores" para mais detalhes.

2. Selecione **Criar usuário** e selecione **Concluir**.

Visualizar e editar usuários locais

Você pode visualizar detalhes de usuários locais e federados existentes. Você pode modificar um usuário local para alterar seu nome completo, senha ou associação ao grupo. Você também pode impedir temporariamente que um usuário acesse o Grid Manager e a Grid Management API.

Você pode editar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para visualizar informações básicas de todos os usuários locais e federados, revise a tabela na página Usuários.
- Para visualizar todos os detalhes de um usuário específico, editar um usuário local ou alterar a senha de um usuário local, use o menu **Ações** ou a página de detalhes.

  Todas as edições serão aplicadas na próxima vez que o usuário sair e entrar novamente no Grid Manager.

  Usuários locais podem alterar suas próprias senhas usando a opção **Alterar senha** no banner do Grid Manager.

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do usuário	a. Marque a caixa de seleção para o usuário. b. Selecione **Ações** > **Exibir detalhes do usuário**.	Selecione o nome do usuário na tabela.

Tarefa	Menu de ações	Página de detalhes
Editar nome completo (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione **Ações** > **Editar nome completo**. c. Digite o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Salvar alterações**.
Negar ou permitir acesso ao StorageGRID	a. Marque a caixa de seleção para o usuário. b. Selecione **Ações** > **Exibir detalhes do usuário**. c. Selecione a aba Acesso. d. Selecione **Sim** para impedir que o usuário faça login no Grid Manager ou na Grid Management API, ou selecione **Não** para permitir que o usuário faça login. e. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba Acesso. c. Selecione **Sim** para impedir que o usuário faça login no Grid Manager ou na Grid Management API, ou selecione **Não** para permitir que o usuário faça login. d. Selecione **Salvar alterações**.
Alterar senha (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione **Ações** > **Exibir detalhes do usuário**. c. Selecione a aba Senha. d. Digite uma nova senha. e. Selecione **Alterar senha**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba Senha. c. Digite uma nova senha. d. Selecione **Alterar senha**.
Alterar grupos (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione **Ações** > **Exibir detalhes do usuário**. c. Selecione a aba Grupos. d. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. e. Selecione **Editar grupos** para selecionar grupos diferentes. f. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba Grupos. c. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. d. Selecione **Editar grupos** para selecionar grupos diferentes. e. Selecione **Salvar alterações**.

Duplicar um usuário

Você pode duplicar um usuário existente para criar um novo usuário com as mesmas permissões.

Passos

1. Marque a caixa de seleção para o usuário.
2. Selecione **Ações** > **Duplicar usuário**.
3. Conclua o assistente Duplicar usuário.

Excluir um usuário

Você pode excluir um usuário local para removê-lo permanentemente do sistema.

> Você não pode excluir o usuário root.

Passos

1. Na página Usuários, marque a caixa de seleção de cada usuário que deseja remover.
2. Selecione **Ações** > **Excluir usuário**.
3. Selecione **Excluir usuário**.

Use o logon único (SSO)

Configurar logon único

Quando o logon único (SSO) estiver habilitado, os usuários só poderão acessar o Grid Manager, o Tenant Manager, a Grid Management API ou a Tenant Management API se suas credenciais forem autorizadas usando o processo de logon SSO implementado pela sua organização. Usuários locais não podem fazer login no StorageGRID.

Como funciona o logon único

O sistema StorageGRID oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar o logon único (SSO), revise como os processos de login e logout do StorageGRID são afetados quando o SSO está habilitado.

Sign in quando o SSO estiver habilitado

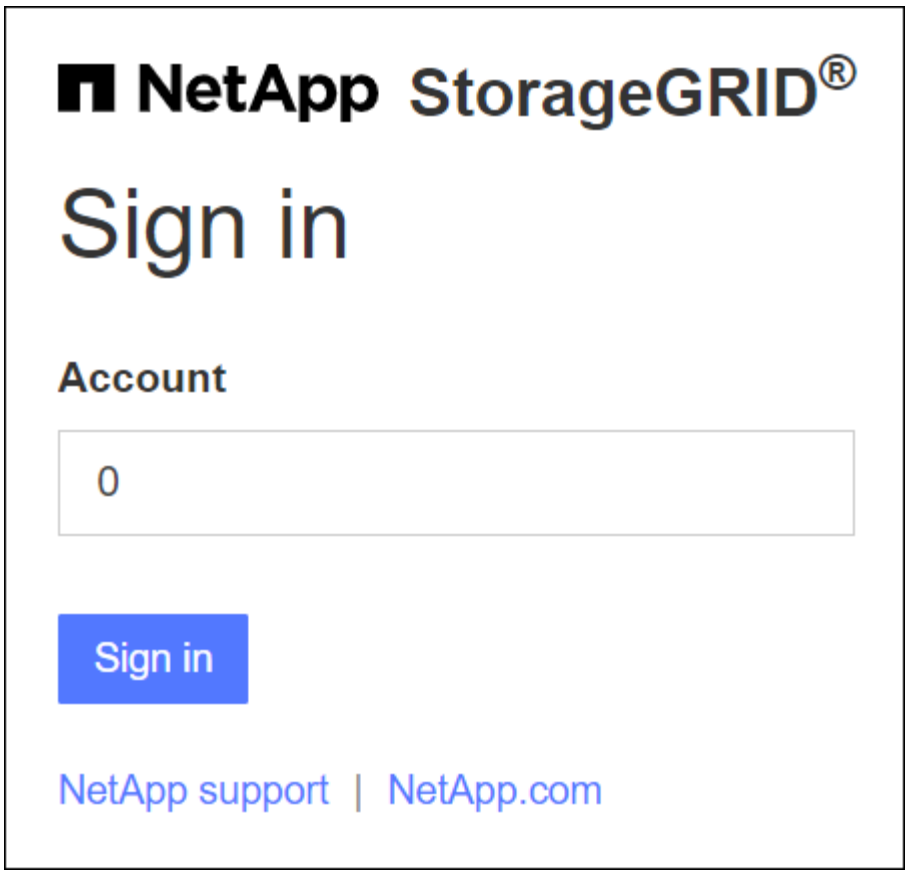
Quando o SSO estiver habilitado e você fizer login no StorageGRID, você será redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

1. Insira o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó de administração do StorageGRID em um navegador da web.

   A página de Sign in do StorageGRID é exibida.

   - Se esta for a primeira vez que você acessa a URL neste navegador, será solicitado um ID de conta:

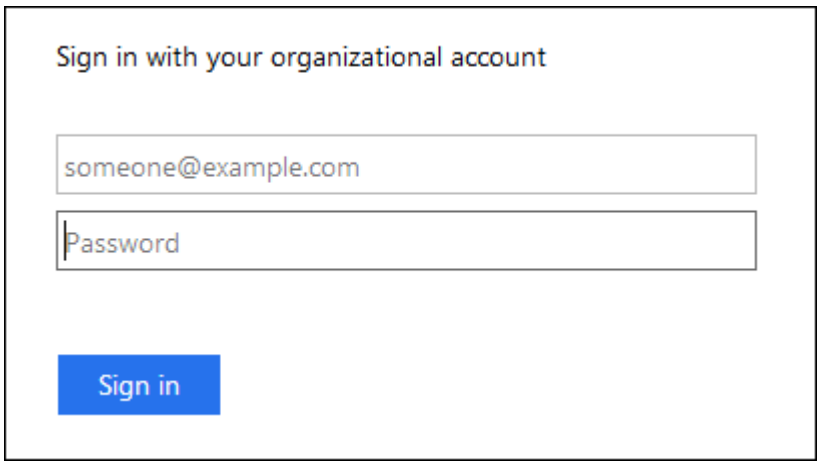


- Se você já acessou o Grid Manager ou o Tenant Manager, será solicitado que você selecione uma conta recente ou insira um ID de conta:

A página de Sign in do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido por `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da sua organização, onde poderáfaça login com suas credenciais SSO .

2. Indique se deseja acessar o Grid Manager ou o Tenant Manager:
   - Para acessar o Grid Manager, deixe o campo **ID da conta** em branco, digite **0** como ID da conta ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.
   - Para acessar o Gerenciador de Inquilinos, insira o ID da conta do inquilino de 20 dígitos ou selecione um inquilino pelo nome se ele aparecer na lista de contas recentes.
3. Selecione * Sign in*

   O StorageGRID redireciona você para a página de login SSO da sua organização. Por exemplo:



4. Sign in com suas credenciais de SSO.

   Se suas credenciais de SSO estiverem corretas:

   a. O provedor de identidade (IdP) fornece uma resposta de autenticação ao StorageGRID.
   b. O StorageGRID valida a resposta de autenticação.
   c. Se a resposta for válida e você pertencer a um grupo federado com permissões de acesso ao StorageGRID , você será conectado ao Grid Manager ou ao Tenant Manager, dependendo da conta selecionada.

   Se a conta de serviço estiver inacessível, você ainda poderá fazer login, desde que seja um usuário existente que pertença a um grupo federado com permissões de acesso ao StorageGRID .

5. Opcionalmente, acesse outros nós de administração ou acesse o Grid Manager ou o Tenant Manager, se você tiver permissões adequadas.

   Você não precisa inserir novamente suas credenciais de SSO.

Sair quando o SSO estiver habilitado

Quando o SSO está habilitado para o StorageGRID, o que acontece quando você sai depende do que você está conectado e de onde você está saindo.

Passos

1. Localize o link **Sair** no canto superior direito da interface do usuário.
2. Selecione **Sair**.

   A página de Sign in do StorageGRID é exibida. O menu suspenso **Contas recentes** foi atualizado para incluir **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conectado a…	E você sai de…	Você está desconectado de…
Gerenciador de grade em um ou mais nós de administração	Gerenciador de grade em qualquer nó de administração	Gerenciador de grade em todos os nós de administração **Observação:** Se você usar o Azure para SSO, poderá levar alguns minutos para sair de todos os nós de administração.
Gerenciador de locatários em um ou mais nós administrativos	Gerenciador de inquilinos em qualquer nó de administração	Gerenciador de inquilinos em todos os nós administrativos
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Somente o Grid Manager. Você também deve sair do Gerenciador de Locatários para sair do SSO.

> A tabela resume o que acontece quando você sai se estiver usando uma única sessão do navegador. Se você estiver conectado ao StorageGRID em várias sessões do navegador, será necessário sair de todas as sessões do navegador separadamente.

Requisitos e considerações para logon único

Antes de habilitar o logon único (SSO) para um sistema StorageGRID , revise os requisitos e considerações.

Requisitos do provedor de identidade

O StorageGRID oferece suporte aos seguintes provedores de identidade SSO (IdP):

- Serviço de Federação do Active Directory (AD FS)
- Diretório Ativo do Azure (Azure AD)
- PingFederate

Você deve configurar a federação de identidade para seu sistema StorageGRID antes de poder configurar um provedor de identidade SSO. O tipo de serviço LDAP que você usa para federação de identidade controla qual tipo de SSO você pode implementar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

Requisitos do AD FS

Você pode usar qualquer uma das seguintes versões do AD FS:

- AD FS do Windows Server 2022
- AD FS do Windows Server 2019
- AD FS do Windows Server 2016

> O Windows Server 2016 deve estar usando o "Atualização KB3201845" , ou superior.

Requisitos adicionais

- Segurança da Camada de Transporte (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Considerações sobre o Azure

Se você usar o Azure como o tipo de SSO e os usuários tiverem nomes principais de usuário que não usam o sAMAccountName como prefixo, poderão ocorrer problemas de login se o StorageGRID perder sua conexão com o servidor LDAP. Para permitir que os usuários efetuem login, você deve restaurar a conexão com o servidor LDAP.

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado de interface de gerenciamento em cada nó de administração para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API. Ao configurar relações de confiança de terceira parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para o StorageGRID, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID .

Se você ainda não o fez"configurou um certificado personalizado para a interface de gerenciamento" , você deve fazer isso agora. Quando você instala um certificado de servidor personalizado, ele é usado para todos os nós de administração e você pode usá-lo em todos os trusts de terceiros confiáveis do StorageGRID , aplicativos empresariais ou conexões SP .

> Não é recomendado usar o certificado de servidor padrão de um nó de administração em uma conexão de confiança de terceira parte, aplicativo empresarial ou SP . Se o nó falhar e você recuperá-lo, um novo certificado de servidor padrão será gerado. Antes de poder fazer login no nó recuperado, você deve atualizar a confiança da parte confiável, o aplicativo empresarial ou a conexão SP com o novo certificado.

Você pode acessar o certificado do servidor de um nó de administração efetuando login no shell de comando

do nó e indo para `/var/local/mgmt-api` diretório. Um certificado de servidor personalizado é denominado `custom-server.crt` . O certificado do servidor padrão do nó é denominado `server.crt` .

Requisitos portuários

O logon único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único. Ver "Controle de acesso em firewall externo" .

Confirme se os usuários federados podem fazer login

Antes de habilitar o logon único (SSO), você deve confirmar se pelo menos um usuário federado pode fazer login no Grid Manager e no Tenant Manager para qualquer conta de locatário existente.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você já configurou a federação de identidade.

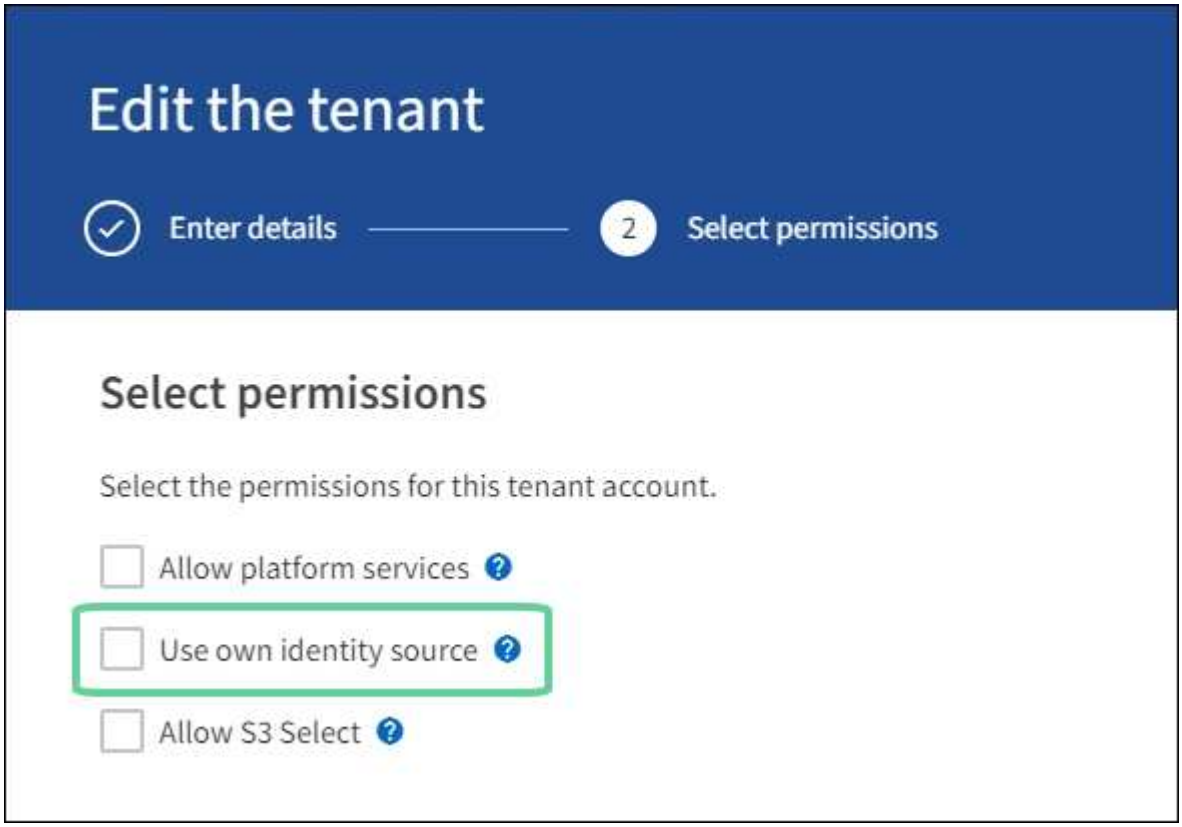
Passos

1. Se houver contas de locatários existentes, confirme se nenhum deles está usando sua própria fonte de identidade.

   > Quando você habilita o SSO, uma fonte de identidade configurada no Tenant Manager é substituída pela fonte de identidade configurada no Grid Manager. Os usuários pertencentes à fonte de identidade do locatário não poderão mais fazer login, a menos que tenham uma conta com a fonte de identidade do Grid Manager.

   a. Sign in no Gerenciador de Inquilinos para cada conta de inquilino.
   b. Selecione **GERENCIAMENTO DE ACESSO** > **Federação de identidade**.
   c. Confirme se a caixa de seleção **Ativar federação de identidade** não está marcada.
   d. Se for o caso, confirme se quaisquer grupos federados que possam estar em uso para esta conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.
2. Confirme se um usuário federado pode acessar o Grid Manager:
   a. No Grid Manager, selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Grupos de administradores**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da fonte de identidade do Active Directory e que tenha recebido a permissão de acesso Root.
   c. Sair.
   d. Confirme se você pode fazer login novamente no Grid Manager como um usuário no grupo federado.
3. Se houver contas de locatário existentes, confirme se um usuário federado com permissão de acesso Root pode fazer login:
   a. No Grid Manager, selecione **LOCATÁRIOS**.
   b. Selecione a conta do locatário e selecione **Ações** > **Editar**.
   c. Na guia Inserir detalhes, selecione **Continuar**.

d. Se a caixa de seleção **Usar fonte de identidade própria** estiver marcada, desmarque a caixa e selecione **Salvar**.



A página do inquilino é exibida.

a. Selecione a conta do locatário, selecione * Sign in* e entre na conta do locatário como usuário root local.
b. No Gerenciador de inquilinos, selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.
c. Certifique-se de que pelo menos um grupo federado do Grid Manager tenha recebido a permissão de acesso Root para este locatário.
d. Sair.
e. Confirme se você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

- "Requisitos e considerações para logon único"
- "Gerenciar grupos de administradores"
- "Use uma conta de inquilino"

Usar o modo sandbox

Você pode usar o modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID . Após o SSO ser habilitado, você pode retornar ao modo sandbox sempre que precisar alterar ou testar novamente a configuração.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Você configurou a federação de identidade para seu sistema StorageGRID .
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou Active Directory ou Azure, com base no provedor de identidade SSO que planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

Sobre esta tarefa

Quando o SSO está habilitado e um usuário tenta fazer login em um nó de administração, o StorageGRID envia uma solicitação de autenticação ao provedor de identidade do SSO. Por sua vez, o provedor de identidade SSO envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autenticação foi bem-sucedida. Para solicitações bem-sucedidas:

- A resposta do Active Directory ou PingFederate inclui um identificador universalmente exclusivo (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal do Usuário (UPN).

Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação do usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. Por fim, você deve retornar ao StorageGRID para habilitar o SSO.

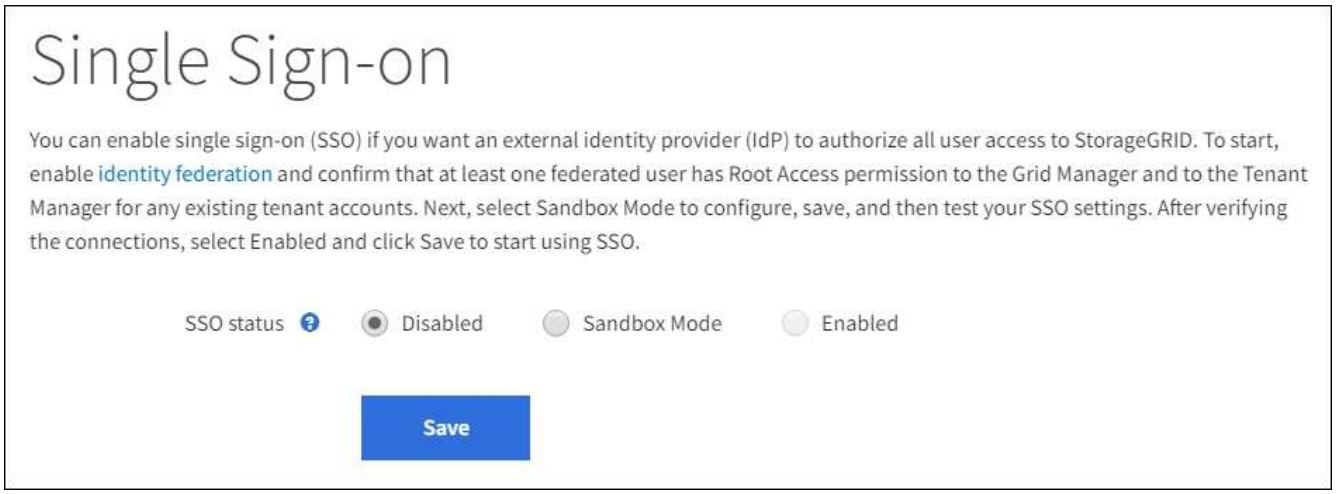
O modo sandbox facilita a execução dessa configuração de ida e volta e o teste de todas as suas configurações antes de habilitar o SSO. Quando você usa o modo sandbox, os usuários não conseguem fazer login usando SSO.

Acessar o modo sandbox

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.

   A página de logon único é exibida, com a opção **Desativado** selecionada.



Se as opções de Status do SSO não aparecerem, confirme se você configurou o provedor de identidade como a fonte de identidade federada. Ver "Requisitos e considerações para logon único" .

2. Selecione **Modo Sandbox**.

   A seção Provedor de Identidade é exibida.

Insira os detalhes do provedor de identidade

Passos

1. Selecione o **tipo de SSO** na lista suspensa.
2. Preencha os campos na seção Provedor de identidade com base no tipo de SSO selecionado.

Diretório ativo

a. Insira o **Nome do serviço de federação** para o provedor de identidade, exatamente como ele aparece no Serviço de Federação do Active Directory (AD FS).

> Para localizar o nome do serviço de federação, acesse o Gerenciador do Windows Server. Selecione **Ferramentas** > **Gerenciamento do AD FS**. No menu Ação, selecione **Editar propriedades do serviço de federação**. O nome do serviço da federação é mostrado no segundo campo.

b. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

c. Na seção Parte Confiável, especifique o **Identificador da parte confiável** para StorageGRID. Este valor controla o nome que você usa para cada parte confiável no AD FS.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra o identificador da parte confiável para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar uma parte confiável para cada nó de administração no seu sistema StorageGRID . Ter uma parte confiável para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

Azul

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do

StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

b. Na seção Aplicativo Corporativo, especifique o **Nome do aplicativo corporativo** para StorageGRID. Este valor controla o nome que você usa para cada aplicativo empresarial no Azure AD.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra um nome de aplicativo corporativo para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar um aplicativo corporativo para cada nó de administração no seu sistema StorageGRID . Ter um aplicativo corporativo para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

c. Siga os passos em"Crie aplicativos corporativos no Azure AD" para criar um aplicativo corporativo para cada nó administrativo listado na tabela.

d. No Azure AD, copie a URL de metadados da federação para cada aplicativo empresarial. Em seguida, cole esta URL no campo **URL de metadados da federação** correspondente no StorageGRID.

e. Depois de copiar e colar uma URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

PingFederate

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.

- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

b. Na seção Provedor de serviços (SP), especifique o * ID de conexão do SP * para StorageGRID. Este valor controla o nome que você usa para cada conexão SP no PingFederate.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra o ID de conexão do SP para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID . Ter uma conexão SP para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

c. Especifique a URL de metadados da federação para cada nó administrativo no campo **URL de metadados da federação**.

Use o seguinte formato:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

Configurar trusts de terceira parte confiável, aplicativos corporativos ou conexões SP

Quando a configuração é salva, o aviso de confirmação do modo Sandbox é exibido. Este aviso confirma que o modo sandbox agora está ativado e fornece instruções gerais.

O StorageGRID pode permanecer no modo sandbox pelo tempo que for necessário. No entanto, quando o **Modo Sandbox** é selecionado na página de logon único, o SSO é desabilitado para todos os usuários do StorageGRID . Somente usuários locais podem fazer login.

Siga estas etapas para configurar confianças de partes confiáveis (Active Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Diretório ativo

Passos

1. Acesse os Serviços de Federação do Active Directory (AD FS).
2. Crie um ou mais trusts de parte confiável para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID .

   Você deve criar uma confiança para cada nó administrativo mostrado na tabela.

   Para obter instruções, acesse"Criar relações de confiança de terceira parte confiável no AD FS" .

Azul

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
   a. Sign in no nó.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Acesse o Portal do Azure.
4. Siga os passos em"Crie aplicativos corporativos no Azure AD" para carregar o arquivo de metadados SAML para cada nó de administração em seu aplicativo empresarial do Azure correspondente.

PingFederate

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
   a. Sign in no nó.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Acesse PingFederate.
4. "Crie uma ou mais conexões de provedor de serviços (SP) para StorageGRID" . Use o ID de conexão SP para cada nó de administração (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administração.

   Você deve criar uma conexão SP para cada nó de administração mostrado na tabela.

Testar conexões SSO

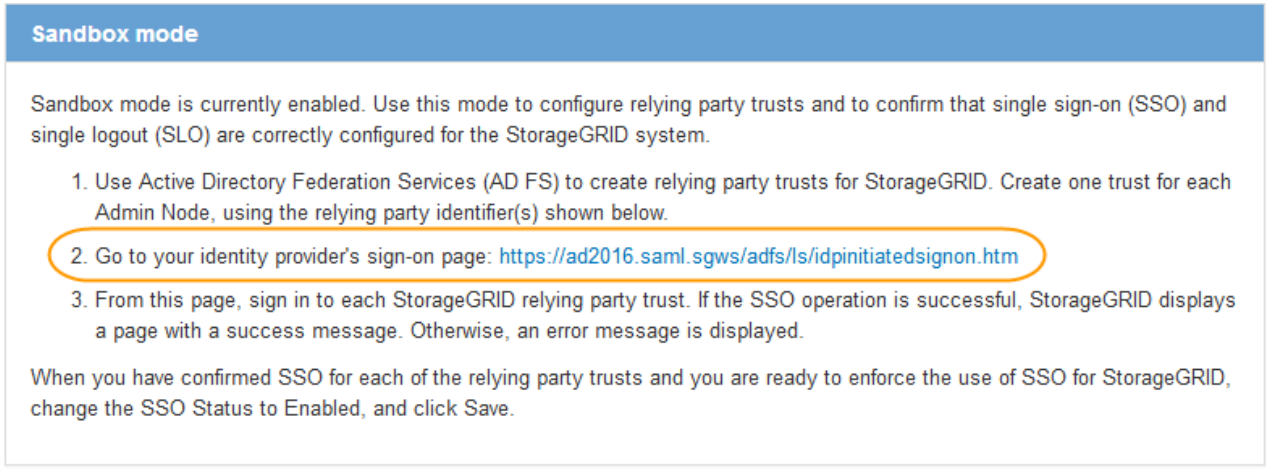
Antes de impor o uso do logon único para todo o seu sistema StorageGRID , você deve confirmar se o logon único e o logout único estão configurados corretamente para cada nó de administração.

Diretório ativo

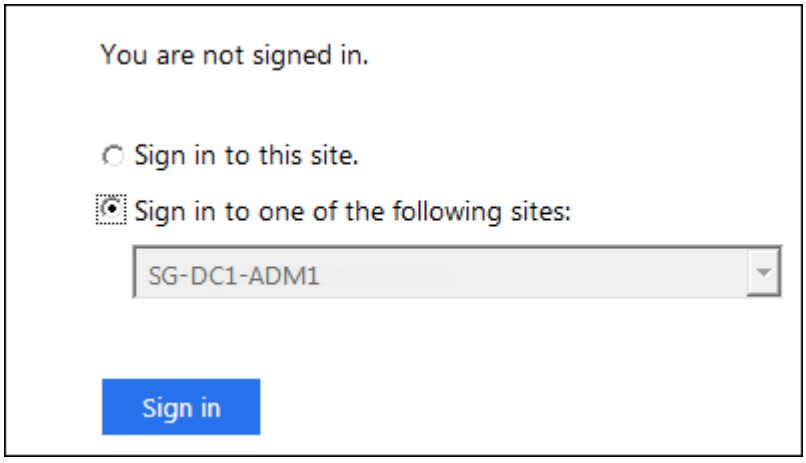
Passos

1. Na página de logon único do StorageGRID , localize o link na mensagem do modo Sandbox.

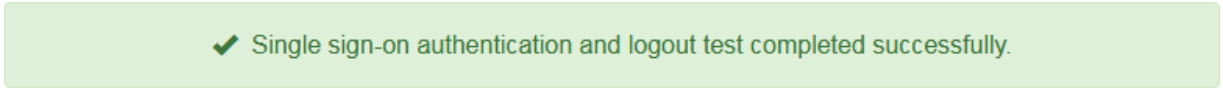
   O URL é derivado do valor inserido no campo **Nome do serviço da federação**.



2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de login do seu provedor de identidade.
3. Para confirmar que você pode usar o SSO para fazer login no StorageGRID, selecione * Sign in em um dos seguintes sites*, selecione o identificador de parte confiável para seu nó de administração principal e selecione * Sign in*.



4. Digite seu nome de usuário e senha federados.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.



   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
5. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

Azul

Passos

1. Acesse a página de logon único no portal do Azure.
2. Selecione **Testar este aplicativo**.
3. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

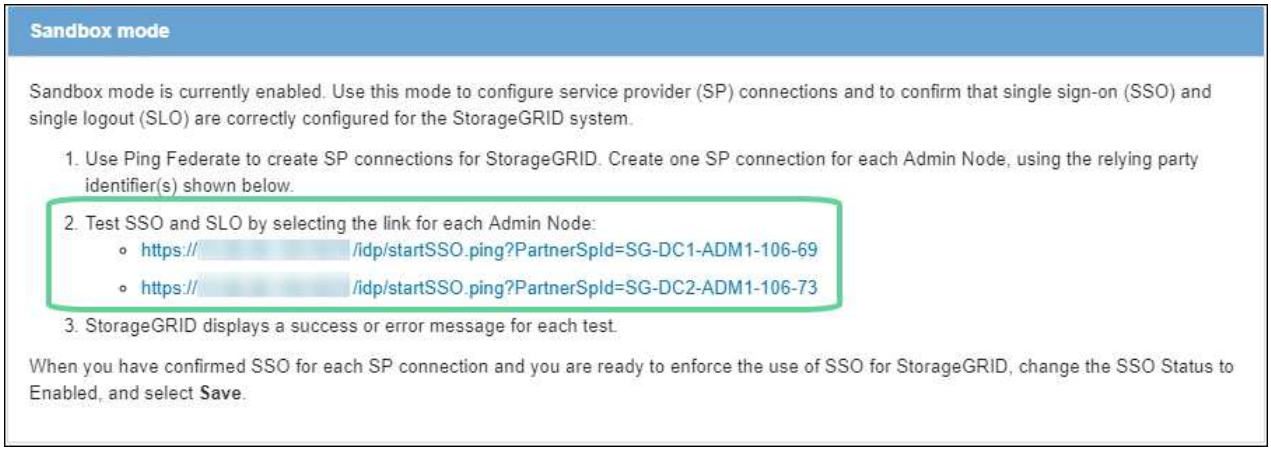
   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
4. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

PingFederate

Passos

1. Na página de logon único do StorageGRID , selecione o primeiro link na mensagem do modo Sandbox.

   Selecione e teste um link por vez.

2. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o próximo link para verificar a conexão SSO para cada nó de administração na sua grade.

   Se você vir uma mensagem de Página expirada, selecione o botão **Voltar** no seu navegador e reenvie suas credenciais.

Habilitar logon único

Depois de confirmar que você pode usar o SSO para fazer login em cada nó de administração, você pode habilitar o SSO para todo o seu sistema StorageGRID .

> Quando o SSO estiver habilitado, todos os usuários deverão usar o SSO para acessar o Grid Manager, o Tenant Manager, a Grid Management API e a Tenant Management API. Usuários locais não podem mais acessar o StorageGRID.

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
2. Altere o status do SSO para **Habilitado**.
3. Selecione **Salvar**.
4. Revise a mensagem de aviso e selecione **OK**.

   O logon único agora está habilitado.

> Se você estiver usando o Portal do Azure e acessar o StorageGRID do mesmo computador que usa para acessar o Azure, certifique-se de que o usuário do Portal do Azure também seja um usuário autorizado do StorageGRID (um usuário em um grupo federado que foi importado para o StorageGRID) ou saia do Portal do Azure antes de tentar entrar no StorageGRID.

Criar relações de confiança de terceira parte confiável no AD FS

Você deve usar os Serviços de Federação do Active Directory (AD FS) para criar uma parte confiável para cada nó de administração no seu sistema. Você pode criar trusts de terceira parte confiável usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador da parte confiável para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID .

  > Você deve criar uma parte confiável para cada nó de administração no seu sistema StorageGRID . Ter uma parte confiável para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

- Você tem experiência na criação de relações de confiança de partes confiáveis no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a confiança da parte confiável manualmente, terá o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou saberá como fazer login em um nó de administração a partir do shell de comando.

Sobre esta tarefa

Estas instruções se aplicam ao AD FS do Windows Server 2016. Se você estiver usando uma versão diferente do AD FS, notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Crie uma confiança de terceira parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais relações de confiança de terceira parte confiável.

Passos

1. No menu Iniciar do Windows, selecione com o botão direito do mouse o ícone do PowerShell e selecione **Executar como Administrador**.
2. No prompt de comando do PowerShell, digite o seguinte comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *`Admin_Node_Identifier`* , insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único. Por exemplo, `SG-DC1-ADM1` .
   - Para *`Admin_Node_FQDN`* , insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)
3. No Gerenciador do Windows Server, selecione **Ferramentas** > **Gerenciamento do AD FS**.

   A ferramenta de gerenciamento do AD FS é exibida.
4. Selecione **AD FS** > **Relying Party Trusts**.

   A lista de trusts de partes confiáveis é exibida.
5. Adicione uma Política de Controle de Acesso à confiança da parte confiável recém-criada:
   a. Localize a parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse no trust e selecione **Editar Política de Controle de Acesso**.
   c. Selecione uma Política de Controle de Acesso.
   d. Selecione **Aplicar** e selecione **OK**
6. Adicione uma Política de Emissão de Reivindicações ao Trust de Parte Confiável recém-criado:
   a. Localize a parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.
   c. Selecione **Adicionar regra**.
   d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.
   e. Na página Configurar regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

f. Para o Attribute Store, selecione **Active Directory**.

g. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.

h. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.

i. Selecione **Concluir** e selecione **OK**.

7. Confirme se os metadados foram importados com sucesso.

a. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.

b. Confirme se os campos nas guias **Endpoints**, **Identifiers** e **Signature** estão preenchidos.

Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

8. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .

9. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo Sandbox" para obter instruções.

Crie uma parte confiável importando metadados da federação

Você pode importar os valores para cada parte confiável acessando os metadados SAML para cada nó de administração.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.

2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.

3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.

4. Selecione **Importar dados sobre a parte confiável publicados on-line ou em uma rede local**.

5. Em **Endereço de metadados da federação (nome do host ou URL)**, digite o local dos metadados SAML para este nó de administração:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`* , insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

6. Conclua o assistente de Relying Party Trust, salve o trust da parte confiável e feche o assistente.

> Ao inserir o nome de exibição, use o Identificador de Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único no Grid Manager. Por exemplo, `SG-DC1-ADM1` .

7. Adicione uma regra de reivindicação:

a. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

b. Selecione **Adicionar regra**:

c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.

d. Na página Configurar regra, insira um nome de exibição para esta regra.

   Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

e. Para o Attribute Store, selecione **Active Directory**.

f. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.

g. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.

h. Selecione **Concluir** e selecione **OK**.

8. Confirme se os metadados foram importados com sucesso.

   a. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.

   b. Confirme se os campos nas guias **Endpoints**, **Identifiers** e **Signature** estão preenchidos.

      Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

9. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .

10. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo Sandbox" para obter instruções.

Crie uma parte confiável manualmente

Se você optar por não importar os dados para as partes confiáveis, poderá inserir os valores manualmente.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.
3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.
4. Selecione **Inserir dados sobre a parte confiável manualmente** e selecione **Avançar**.
5. Conclua o assistente Relying Party Trust:

   a. Insira um nome de exibição para este nó de administração.

      Para consistência, use o Identificador de Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único no Grid Manager. Por exemplo, `SG-DC1-ADM1` .

   b. Ignore a etapa para configurar um certificado de criptografia de token opcional.

   c. Na página Configurar URL, marque a caixa de seleção **Ativar suporte para o protocolo SAML 2.0 WebSSO**.

   d. Digite a URL do ponto de extremidade do serviço SAML para o nó de administração:

      `https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado para o nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

e. Na página Configurar Identificadores, especifique o Identificador de Parte Confiável para o mesmo Nó de Administração:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único. Por exemplo, `SG-DC1-ADM1`.

f. Revise as configurações, salve a confiança da parte confiável e feche o assistente.

A caixa de diálogo Editar política de emissão de reivindicações é exibida.

> Se a caixa de diálogo não aparecer, clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

6. Para iniciar o assistente de Regra de Reivindicação, selecione **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.
   b. Na página Configurar regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

   c. Para o Attribute Store, selecione **Active Directory**.
   d. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
   e. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.
   f. Selecione **Concluir** e selecione **OK**.
7. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
   a. Selecione **Adicionar SAML**.
   b. Selecione **Tipo de endpoint** > **Logout SAML**.
   c. Selecione **Vinculação** > **Redirecionamento**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó de administração:

      `https://Admin_Node_FQDN/api/saml-logout`

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado do nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

   a. Selecione **OK**.

9. Na aba **Assinatura**, especifique o certificado de assinatura para esta parte confiável:
   a. Adicione o certificado personalizado:
      - Se você tiver o certificado de gerenciamento personalizado que carregou no StorageGRID, selecione esse certificado.
      - Se você não tiver o certificado personalizado, faça login no nó de administração, vá para `/var/local/mgmt-api` diretório do nó de administração e adicione o `custom-server.crt` arquivo de certificado.

        Usando o certificado padrão do nó de administração(`server.crt`) não é recomendado. Se o nó de administração falhar, o certificado padrão será regenerado quando você recuperar o nó, e você precisará atualizar a confiança da parte confiável.

   b. Selecione **Aplicar** e selecione **OK**.

      As propriedades da Parte Confiável são salvas e fechadas.

10. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .
11. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo sandbox" para obter instruções.

Crie aplicativos corporativos no Azure AD

Use o Azure AD para criar um aplicativo empresarial para cada nó de administração no seu sistema.

Antes de começar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você tem o **Nome do aplicativo corporativo** para cada nó de administração no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administração na página de logon único do StorageGRID .

  Você deve criar um aplicativo corporativo para cada nó de administração no seu sistema StorageGRID . Ter um aplicativo corporativo para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

- Você tem experiência na criação de aplicativos corporativos no Azure Active Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário da entidade de serviço.

Acessar o Azure AD

Passos

1. Faça login no "Portal do Azure" .
2. Navegar para "Diretório Ativo do Azure" .

3. Selecione "Aplicações empresariais" .

Crie aplicativos corporativos e salve a configuração do StorageGRID SSO

Para salvar a configuração de SSO do Azure no StorageGRID, você deve usar o Azure para criar um aplicativo empresarial para cada nó de administração. Você copiará as URLs de metadados da federação do Azure e as colará nos campos **URL de metadados da federação** correspondentes na página de logon único do StorageGRID .

Passos

1. Repita as etapas a seguir para cada nó de administração.
   a. No painel Aplicativos empresariais do Azure, selecione **Novo aplicativo**.
   b. Selecione **Criar seu próprio aplicativo**.
   c. Para o nome, insira o **Nome do aplicativo corporativo** que você copiou da tabela de detalhes do nó de administração na página de logon único do StorageGRID .
   d. Deixe o botão de opção **Integrar qualquer outro aplicativo que você não encontrar na galeria (Não galeria)** selecionado.
   e. Selecione **Criar**.
   f. Selecione o link **Começar** em **2. Configure a caixa de logon único** ou selecione o link **Logon único** na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o **App Federation Metadata URL**, que você pode encontrar em **Step 3 SAML Signing Certificate**.
   i. Acesse a página de logon único do StorageGRID e cole a URL no campo **URL de metadados da federação** que corresponde ao **Nome do aplicativo corporativo** que você usou.
2. Depois de colar uma URL de metadados de federação para cada nó de administração e fazer todas as outras alterações necessárias na configuração do SSO, selecione **Salvar** na página de logon único do StorageGRID .

Baixe metadados SAML para cada nó de administração

Depois que a configuração do SSO for salva, você poderá baixar um arquivo de metadados SAML para cada nó de administração no seu sistema StorageGRID .

Passos

1. Repita essas etapas para cada nó de administração.
   a. Sign in no StorageGRID a partir do nó de administração.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Selecione o botão para baixar os metadados SAML para esse nó de administração.
   d. Salve o arquivo que você carregará no Azure AD.

Carregar metadados SAML para cada aplicativo empresarial

Depois de baixar um arquivo de metadados SAML para cada nó de administração do StorageGRID , execute as seguintes etapas no Azure AD:

Passos

1. Retorne ao Portal do Azure.
2. Repita estas etapas para cada aplicativo corporativo:

> Talvez seja necessário atualizar a página de aplicativos corporativos para ver os aplicativos adicionados anteriormente na lista.

   a. Acesse a página Propriedades do aplicativo empresarial.
   b. Defina **Atribuição necessária** como **Não** (a menos que você queira configurar as atribuições separadamente).
   c. Acesse a página de login único.
   d. Conclua a configuração SAML.
   e. Selecione o botão **Carregar arquivo de metadados** e selecione o arquivo de metadados SAML que você baixou para o nó de administração correspondente.
   f. Após o carregamento do arquivo, selecione **Salvar** e depois selecione **X** para fechar o painel. Você retornará à página Configurar logon único com SAML.
3. Siga os passos em"Usar o modo sandbox" para testar cada aplicação.

Criar conexões de provedor de serviços (SP) no PingFederate

Use o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administração no seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **Ping Federate** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você tem o * ID de conexão SP * para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID .
- Você baixou os **metadados SAML** para cada nó de administração no seu sistema.
- Você tem experiência na criação de conexões SP no PingFederate Server.
- Você tem ohttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guia de Referência do Administrador"^] para o servidor PingFederate. A documentação do PingFederate fornece instruções e explicações detalhadas passo a passo.
- Você tem o"Permissão de administrador" para o servidor PingFederate.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10.3 como um provedor de SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar estas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas para sua versão.

Pré-requisitos completos no PingFederate

Antes de criar as conexões SP que você usará para o StorageGRID, você deve concluir as tarefas de pré-requisito no PingFederate. Você usará informações desses pré-requisitos ao configurar as conexões SP .

Criar armazenamento de dados

Se ainda não o fez, crie um armazenamento de dados para conectar o PingFederate ao servidor LDAP do AD FS. Use os valores que você usou quando"configurando federação de identidade" em StorageGRID.

- **Tipo**: Diretório (LDAP)
- **Tipo LDAP**: Active Directory
- **Nome do atributo binário**: insira **objectGUID** na guia Atributos binários do LDAP exatamente como mostrado.

Criar validador de credenciais de senha

Caso ainda não tenha feito isso, crie um validador de credenciais de senha.

- **Tipo**: LDAP Nome de usuário Senha Validador de credenciais
- **Armazenamento de dados**: Selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: insira informações do LDAP (por exemplo, DC=saml,DC=sgws).
- **Filtro de pesquisa**: sAMAccountName=${username}
- **Escopo**: Subárvore

Criar instância do adaptador IdP

Se ainda não o fez, crie uma instância do adaptador IdP.

Passos

1. Vá para **Autenticação** > **Integração** > **Adaptadores IdP**.
2. Selecione **Criar nova instância**.
3. Na guia Tipo, selecione **Adaptador IdP de formulário HTML**.
4. Na guia Adaptador IdP, selecione **Adicionar uma nova linha para 'Validadores de credenciais'**.
5. Selecione ovalidador de credenciais de senha você criou.
6. Na guia Atributos do adaptador, selecione o atributo **nome de usuário** para **Pseudônimo**.
7. Selecione **Salvar**.

Criar ou importar certificado de assinatura

Caso ainda não tenha feito isso, crie ou importe o certificado de assinatura.

Passos

1. Vá para **Segurança** > **Chaves e Certificados de Assinatura e Descriptografia**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Ao criar uma conexão SP no PingFederate, você importa os metadados SAML baixados do StorageGRID para o nó de administração. O arquivo de metadados contém muitos dos valores específicos que você precisa.

Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID , para que os usuários possam entrar e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP . Então vá paraCriar conexões SP adicionais para criar quaisquer conexões adicionais que você precisar.

Escolha o tipo de conexão SP

Passos

1. Vá para **Aplicativos** > **Integração** > *Conexões SP *.
2. Selecione **Criar conexão**.
3. Selecione **Não usar um modelo para esta conexão**.
4. Selecione **Perfis SSO do navegador** e **SAML 2.0** como o protocolo.

Importar metadados SP

Passos

1. Na guia Importar metadados, selecione **Arquivo**.
2. Escolha o arquivo de metadados SAML que você baixou da página de logon único do StorageGRID para o nó de administração.
3. Revise o Resumo de Metadados e as informações fornecidas na guia Informações Gerais.

   O ID da entidade do parceiro e o nome da conexão são definidos como o ID da conexão do StorageGRID SP . (por exemplo, 10.96.105.200-DC1-ADM1-105-200). O URL base é o IP do nó de administração do StorageGRID .

4. Selecione **Avançar**.

Configurar SSO do navegador IdP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia Perfis SAML, selecione as opções * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selecione **Avançar**.
4. Na aba Assertion Lifetime, não faça alterações.
5. Na guia Criação de Asserção, selecione **Configurar Criação de Asserção**.
   a. Na guia Mapeamento de Identidade, selecione **Padrão**.
   b. Na guia Contrato de Atributo, use **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para estender o contrato, selecione **Excluir** para remover o `urn:oid` , que não é usado.

Instância do adaptador de mapa

Passos

1. Na guia Mapeamento de fonte de autenticação, selecione **Mapear nova instância do adaptador**.
2. Na guia Instância do adaptador, selecione oinstância do adaptador você criou.

3. Na guia Método de mapeamento, selecione **Recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia Origem do atributo e pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia Armazenamento de dados, forneça uma descrição e selecione oarmazenamento de dados você adicionou.
6. Na guia Pesquisa de diretório LDAP:
   - Insira o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
   - Para o Escopo de pesquisa, selecione **Subárvore**.
   - Para a classe de objeto raiz, procure e adicione um destes atributos: **objectGUID** ou **userPrincipalName**.
7. Na guia Tipos de codificação de atributo binário LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia Filtro LDAP, digite **sAMAccountName=${username}**.
9. Na guia Cumprimento de contrato de atributo, selecione **LDAP (atributo)** no menu suspenso Origem e selecione **objectGUID** ou **userPrincipalName** no menu suspenso Valor.
10. Revise e salve a origem do atributo.
11. Na guia Fonte do atributo Failsave, selecione **Abortar a transação SSO**.
12. Revise o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configurar as definições do protocolo

Passos

1. Na guia * Conexão SP * > * SSO do navegador * > * Configurações do protocolo *, selecione * Definir configurações do protocolo *.
2. Na guia URL do serviço de consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` para URL do ponto de extremidade).
3. Na guia URLs do serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL do ponto de extremidade.
4. Na guia Ligações SAML permitidas, desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são necessários.
5. Na guia Política de Assinatura, deixe as caixas de seleção **Exigir que as solicitações de autenticação sejam assinadas** e **Sempre assinar declaração** marcadas.
6. Na guia Política de Criptografia, selecione **Nenhum**.
7. Revise o resumo e selecione **Concluído** para salvar as configurações do protocolo.
8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia Conexão SP , selecione **Credenciais**.
2. Na guia Credenciais, selecione **Configurar credenciais**.

3. Selecione ocertificado de assinatura que você criou ou importou.
4. Selecione **Avançar** para ir para **Gerenciar configurações de verificação de assinatura**.
   a. Na guia Modelo de confiança, selecione **Não ancorado**.
   b. Na guia Certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID .
5. Revise as telas de resumo e selecione **Salvar** para salvar a conexão SP .

Criar conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada nó de administração na sua grade. Você carrega novos metadados para cada cópia.

> As conexões SP para diferentes nós administrativos usam configurações idênticas, com exceção do ID da entidade do parceiro, URL base, ID da conexão, nome da conexão, verificação de assinatura e URL de resposta do SLO.

Passos

1. Selecione **Ação** > **Copiar** para criar uma cópia da conexão SP inicial para cada nó de administração adicional.
2. Insira o ID da conexão e o nome da conexão para a cópia e selecione **Salvar**.
3. Selecione o arquivo de metadados correspondente ao nó de administração:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **Escolher arquivo** e carregue os metadados.
   c. Selecione **Avançar**.
   d. Selecione **Salvar**.
4. Resolva o erro devido ao atributo não utilizado:
   a. Selecione a nova conexão.
   b. Selecione **Configurar SSO do navegador > Configurar criação de asserção > Contrato de atributo**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Salvar**.

Desativar logon único

Você pode desabilitar o logon único (SSO) se não quiser mais usar essa funcionalidade. Você deve desabilitar o logon único antes de poder desabilitar a federação de identidades.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.

A página de logon único é exibida.

2. Selecione a opção **Desativado**.
3. Selecione **Salvar**.

   Uma mensagem de aviso aparece indicando que usuários locais agora poderão fazer login.

4. Selecione **OK**.

   Na próxima vez que você fizer login no StorageGRID , a página de Sign in do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário local ou federado do StorageGRID .

Desabilitar temporariamente e reabilitar o logon único para um nó de administração

Talvez você não consiga fazer login no Grid Manager se o sistema de logon único (SSO) ficar inativo. Nesse caso, você pode desabilitar temporariamente e reabilitar o SSO para um nó de administração. Para desabilitar e reabilitar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você tem o `Passwords.txt` arquivo.
- Você sabe a senha do usuário root local.

Sobre esta tarefa

Depois de desabilitar o SSO para um nó de administração, você pode entrar no Grid Manager como usuário root local. Para proteger seu sistema StorageGRID , você deve usar o shell de comando do nó para reativar o SSO no nó de administração assim que sair.

> Desabilitar o SSO para um nó administrativo não afeta as configurações de SSO para nenhum outro nó administrativo na grade. A caixa de seleção **Habilitar SSO** na página Login Único no Grid Manager permanece selecionada, e todas as configurações de SSO existentes são mantidas, a menos que você as atualize.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

      Quando você está logado como root, o prompt muda de `$` para `#` .

2. Execute o seguinte comando:`disable-saml`

   Uma mensagem indica que o comando se aplica somente a este nó de administração.

3. Confirme que você deseja desabilitar o SSO.

Uma mensagem indica que o logon único está desabilitado no nó.

4. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.

   A página de login do Grid Manager agora é exibida porque o SSO foi desabilitado.

5. Sign in com o nome de usuário root e a senha do usuário root local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração do SSO:
   a. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Selecione **Salvar**.

      Selecionar **Salvar** na página Login Único reativa automaticamente o SSO para toda a grade.

7. Se você desativou o SSO temporariamente porque precisava acessar o Grid Manager por algum outro motivo:

   a. Execute qualquer tarefa ou tarefas que você precise executar.
   b. Selecione **Sair** e feche o Grid Manager.
   c. Reative o SSO no nó de administração. Você pode executar qualquer uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a este nó de administração.

      Confirme que você deseja habilitar o SSO.

   Uma mensagem indica que o logon único está habilitado no nó.

      - Reinicie o nó da grade: `reboot`

8. Em um navegador da web, acesse o Grid Manager no mesmo nó de administração.
9. Confirme se a página de Sign in do StorageGRID aparece e se você deve inserir suas credenciais de SSO para acessar o Grid Manager.

Usar federação de grade

O que é federação de grade?

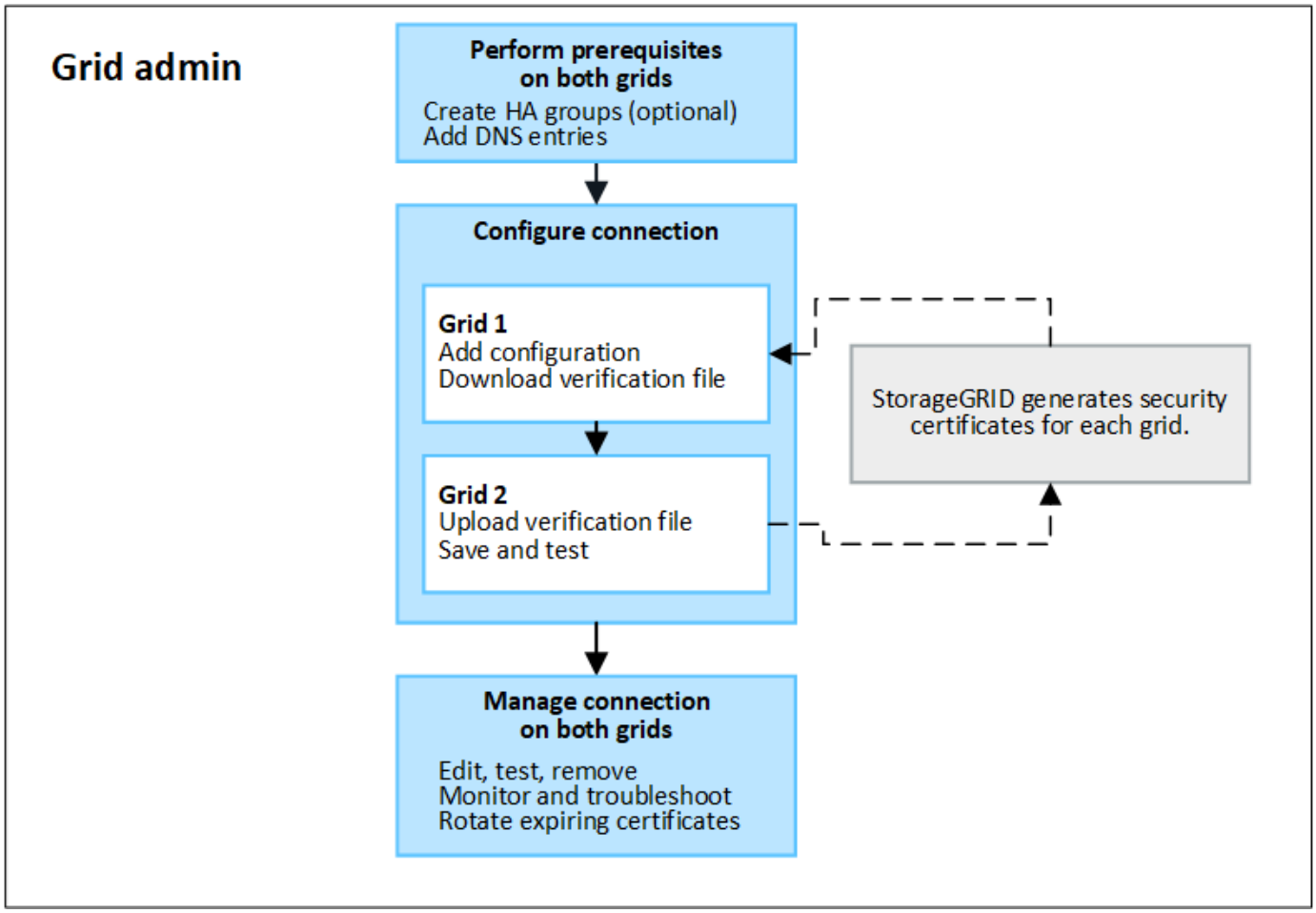
Você pode usar a federação de grade para clonar locatários e replicar seus objetos entre dois sistemas StorageGRID para recuperação de desastres.

O que é uma conexão de federação de rede?

Uma conexão de federação de grade é uma conexão bidirecional, confiável e segura entre nós de administração e gateway em dois sistemas StorageGRID .

Fluxo de trabalho para federação de grade

O diagrama de fluxo de trabalho resume as etapas para configurar uma conexão de federação de grade entre duas grades.



Considerações e requisitos para conexões de federação de rede

- As grades usadas para federação de grade devem executar versões do StorageGRID que sejam idênticas ou não tenham mais de uma diferença de versão principal entre elas.

  Para obter detalhes sobre os requisitos de versão, consulte o"Notas de lançamento" .

- Uma grade pode ter uma ou mais conexões de federação de grade com outras grades. Cada conexão de federação de rede é independente de quaisquer outras conexões. Por exemplo, se a Grade 1 tiver uma conexão com a Grade 2 e uma segunda conexão com a Grade 3, não há conexão implícita entre a Grade 2 e a Grade 3.
- As conexões de federação de rede são bidirecionais. Depois que a conexão for estabelecida, você pode monitorar e gerenciar a conexão de qualquer uma das redes.
- Pelo menos uma conexão de federação de grade deve existir antes que você possa usar"clone de conta" ou"replicação entre grades" .

Requisitos de rede e endereço IP

- As conexões de federação de grade podem ocorrer na Rede de grade, na Rede de administração ou na Rede de cliente.
- Uma conexão de federação de rede conecta uma rede a outra. A configuração de cada grade especifica um ponto de extremidade de federação de grade na outra grade que consiste em nós de administração, nós de gateway ou ambos.
- A melhor prática é conectar"grupos de alta disponibilidade (HA)" de nós de gateway e de administração

em cada grade. O uso de grupos HA ajuda a garantir que as conexões da federação de grade permanecerão online caso os nós fiquem indisponíveis. Se a interface ativa em qualquer grupo HA falhar, a conexão poderá usar uma interface de backup.

- Não é recomendado criar uma conexão de federação de grade que use o endereço IP de um único nó de administração ou nó de gateway. Se o nó ficar indisponível, a conexão da federação de rede também ficará indisponível.
- "Replicação entre grades"de objetos requer que os nós de armazenamento em cada grade sejam capazes de acessar os nós de administração e gateway configurados na outra grade. Para cada grade, confirme se todos os nós de armazenamento têm uma rota de alta largura de banda como nós de administração ou nós de gateway usados para a conexão.

Use FQDNs para balancear a carga da conexão

Para um ambiente de produção, use nomes de domínio totalmente qualificados (FQDNs) para identificar cada grade na conexão. Em seguida, crie as entradas DNS apropriadas, da seguinte forma:

- O FQDN para Grid 1 mapeado para um ou mais endereços IP virtuais (VIP) para grupos HA no Grid 1 ou para o endereço IP de um ou mais nós de administração ou gateway no Grid 1.
- O FQDN para Grid 2 mapeado para um ou mais endereços VIP para Grid 2 ou para o endereço IP de um ou mais nós de administração ou gateway no Grid 2.

Quando você usa várias entradas de DNS, as solicitações para usar a conexão são balanceadas de carga, da seguinte maneira:

- As entradas de DNS mapeadas para os endereços VIP de vários grupos HA são balanceadas de carga entre os nós ativos nos grupos HA.
- As entradas de DNS que mapeiam os endereços IP de vários nós de administração ou nós de gateway são balanceadas de carga entre os nós mapeados.

Requisitos portuários

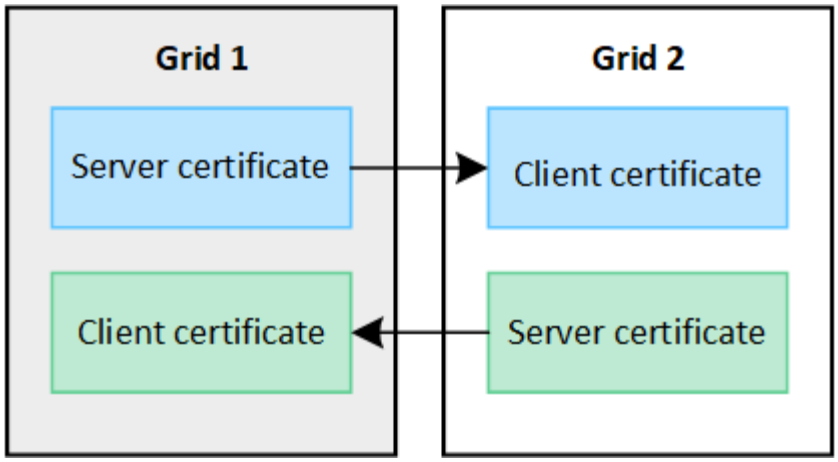
Ao criar uma conexão de federação de grade, você pode especificar qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta.

Você deve garantir que nenhum nó em nenhuma das grades use esta porta para outras conexões.

Requisitos do certificado

Ao configurar uma conexão de federação de grade, o StorageGRID gera automaticamente quatro certificados SSL:

- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grade 1 para a grade 2
- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grade 2 para a grade 1



Por padrão, os certificados são válidos por 730 dias (2 anos). Quando esses certificados estiverem próximos da data de expiração, o alerta **Expiração do certificado de federação de grade** lembrará você de rotacionar os certificados, o que pode ser feito usando o Grid Manager.

> Se os certificados em qualquer extremidade da conexão expirarem, a conexão deixará de funcionar. A replicação de dados ficará pendente até que os certificados sejam atualizados.

Saber mais

- "Criar conexões de federação de grade"
- "Gerenciar conexões de federação de grade"
- "Solucionar erros de federação de grade"

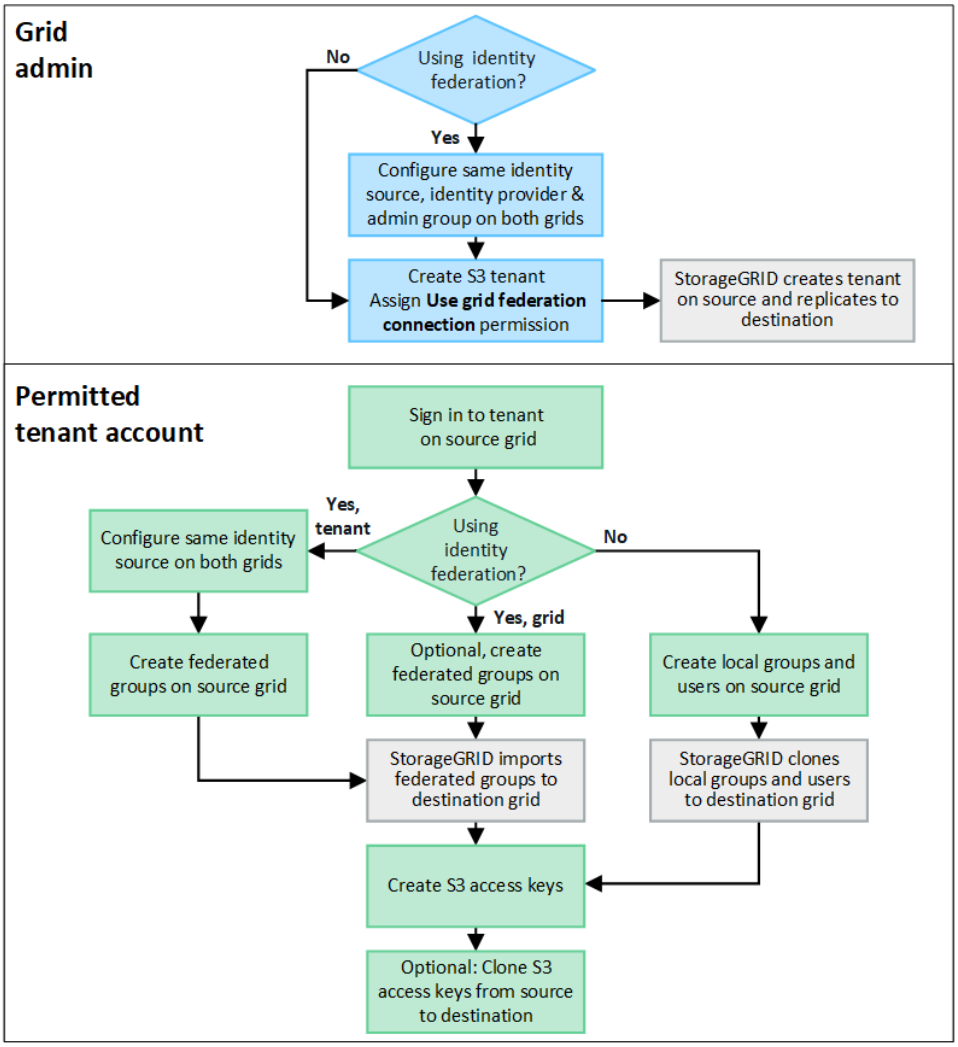
O que é clone de conta?

O clone de conta é a replicação automática de uma conta de locatário, grupos de locatários, usuários de locatários e, opcionalmente, chaves de acesso S3 entre os sistemas StorageGRID em um"conexão de federação de rede" .

É necessário clonar a conta para"replicação entre grades" . A clonagem de informações de conta de um sistema StorageGRID de origem para um sistema StorageGRID de destino garante que usuários e grupos de locatários possam acessar os buckets e objetos correspondentes em qualquer grade.

Fluxo de trabalho para clonagem de conta

O diagrama de fluxo de trabalho mostra as etapas que os administradores de grade e os locatários permitidos executarão para configurar a clonagem da conta. Essas etapas são realizadas após a"a conexão da federação de rede está configurada" .



Fluxo de trabalho de administração de grade

As etapas que os administradores da grade executam dependem se os sistemas StorageGRID no"conexão de federação de rede" use logon único (SSO) ou federação de identidade.

Configurar SSO para clonagem de conta (opcional)

Se qualquer sistema StorageGRID na conexão de federação de grade usar SSO, ambas as grades deverão usar SSO. Antes de criar as contas de locatário para federação de grade, os administradores de grade das grades de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. Ver "Usar federação de identidade" .
2. Configure o mesmo provedor de identidade SSO (IdP) para ambas as grades. Ver "Configurar logon único" .
3. "Crie o mesmo grupo de administração"em ambas as grades importando o mesmo grupo federado.

   Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso Root inicial para as contas do locatário de origem e de destino.

Se esse grupo de administradores não existir em ambas as grades antes de você criar o locatário, o locatário não será replicado para o destino.

Configurar federação de identidade em nível de grade para clone de conta (opcional)

Se qualquer sistema StorageGRID usar federação de identidade sem SSO, ambas as grades deverão usar federação de identidade. Antes de criar as contas de locatário para federação de grade, os administradores de grade das grades de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. Ver "Usar federação de identidade" .
2. Opcionalmente, se um grupo federado tiver permissão de acesso Root inicial para as contas de locatário de origem e de destino,"crie o mesmo grupo de administração" em ambas as grades importando o mesmo grupo federado.

   Se você atribuir permissão de acesso Root a um grupo federado que não existe em ambas as grades, o locatário não será replicado para a grade de destino.

3. Se você não quiser que um grupo federado tenha permissão de acesso root inicial para ambas as contas, especifique uma senha para o usuário root local.

Criar conta de locatário S3 permitida

Depois de configurar opcionalmente o SSO ou a federação de identidade, um administrador de grade executa estas etapas para determinar quais locatários podem replicar objetos de bucket para outros sistemas StorageGRID .

Passos

1. Determine qual grade você deseja que seja a grade de origem do locatário para operações de clonagem de conta.

   A grade onde o locatário é criado originalmente é conhecida como *grade de origem* do locatário. A grade onde o locatário é replicado é conhecida como *grade de destino* do locatário.

2. Nessa grade, crie uma nova conta de locatário do S3 ou edite uma conta existente.
3. Atribua a permissão **Usar conexão de federação de grade**.
4. Se a conta do locatário gerenciar seus próprios usuários federados, atribua a permissão **Usar fonte de identidade própria**.

   Se essa permissão for atribuída, as contas de locatário de origem e de destino deverão configurar a mesma fonte de identidade antes de criar grupos federados. Grupos federados adicionados ao locatário de origem não podem ser clonados para o locatário de destino, a menos que ambas as grades usem a mesma origem de identidade.

5. Selecione uma conexão de federação de rede específica.
6. Salve o inquilino novo ou modificado.

   Quando um novo locatário com a permissão **Usar conexão de federação de grade** é salvo, o StorageGRID cria automaticamente uma réplica desse locatário na outra grade, da seguinte maneira:

   - Ambas as contas de locatário têm o mesmo ID de conta, nome, cota de armazenamento e permissões

atribuídas.

- Se você selecionou um grupo federado para ter permissão de acesso Root para o locatário, esse grupo será clonado para o locatário de destino.
- Se você selecionou um usuário local para ter permissão de acesso Root para o locatário, esse usuário será clonado para o locatário de destino. Entretanto, a senha desse usuário não é clonada.

Para obter detalhes, consulte "Gerenciar inquilinos permitidos para federação de rede" .

Fluxo de trabalho de conta de inquilino permitido

Depois que um locatário com a permissão **Usar conexão de federação de grade** for replicado para a grade de destino, as contas de locatário permitidas poderão executar estas etapas para clonar grupos de locatários, usuários e chaves de acesso do S3.

Passos

1. Sign in na conta do locatário na grade de origem do locatário.
2. Se permitido, configure a federação de identidade nas contas de locatário de origem e de destino.
3. Crie grupos e usuários no locatário de origem.

   Quando novos grupos ou usuários são criados no locatário de origem, o StorageGRID os clona automaticamente para o locatário de destino, mas nenhuma clonagem ocorre do destino de volta para a origem.

4. Crie chaves de acesso S3.
5. Opcionalmente, clone as chaves de acesso S3 do locatário de origem para o locatário de destino.

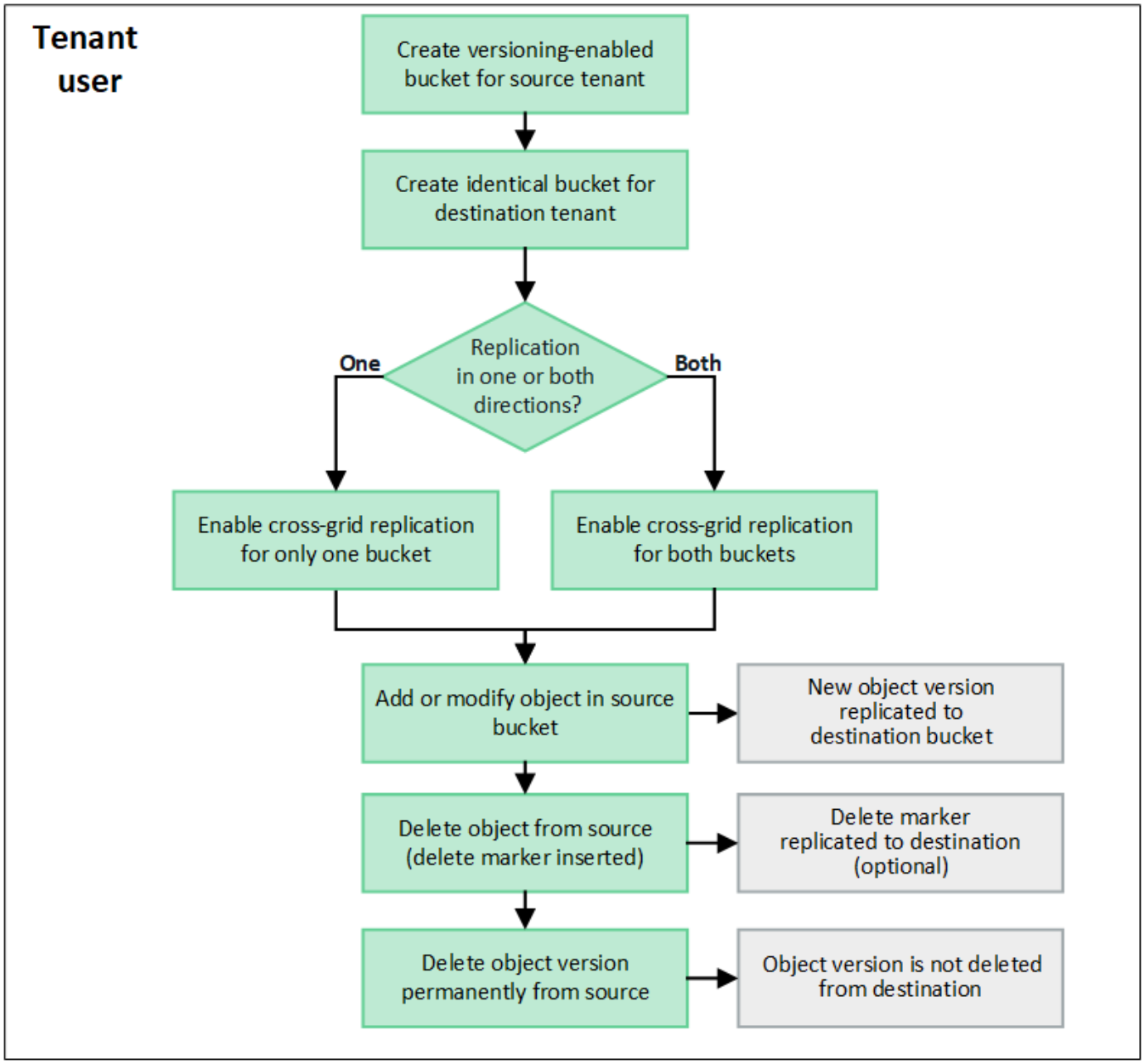
Para obter detalhes sobre o fluxo de trabalho da conta de locatário permitida e saber como grupos, usuários e chaves de acesso S3 são clonados, consulte"Clonar grupos de locatários e usuários" e"Clonar chaves de acesso S3 usando a API" .

O que é replicação entre redes?

A replicação entre grades é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID que estão conectados em um"conexão de federação de rede" . "Clone de conta" é necessário para replicação entre grades.

Fluxo de trabalho para replicação entre grades

O diagrama de fluxo de trabalho resume as etapas para configurar a replicação entre grades entre buckets em duas grades.



Requisitos para replicação entre redes

Se uma conta de locatário tiver a permissão **Usar conexão de federação de grade** para usar um ou mais"conexões de federação de rede" , um usuário locatário com permissão de acesso Root pode criar buckets idênticos nas contas de locatário correspondentes em cada grade. Esses baldes:

- Deve ter o mesmo nome, mas pode ter regiões diferentes
- Deve ter o controle de versão habilitado
- Deve ter o bloqueio de objeto S3 desabilitado
- Deve estar vazio

Depois que ambos os buckets forem criados, a replicação entre grades poderá ser configurada para um ou ambos os buckets.

Saber mais

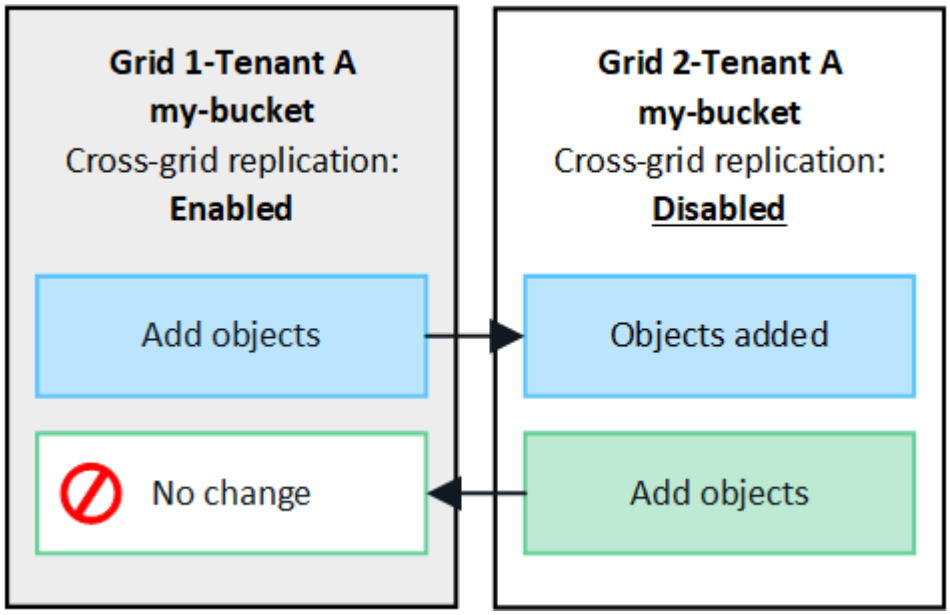
"Gerenciar replicação entre redes"

Como funciona a replicação entre redes

A replicação entre grades pode ser configurada para ocorrer em uma direção ou em ambas as direções.

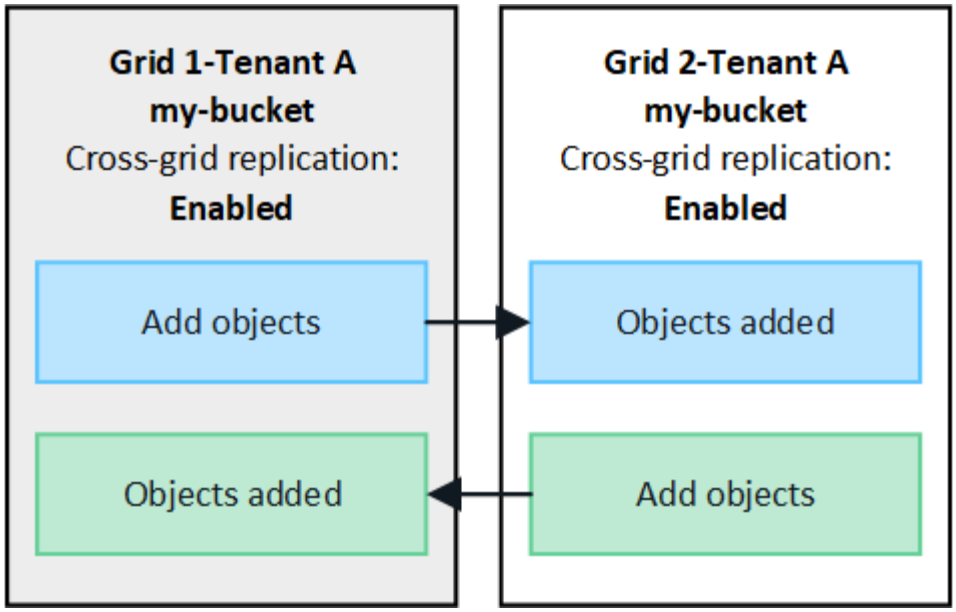
Replicação em uma direção

Se você habilitar a replicação entre grades para um bucket em apenas uma grade, os objetos adicionados a esse bucket (o bucket de origem) serão replicados para o bucket correspondente na outra grade (o bucket de destino). No entanto, os objetos adicionados ao bucket de destino não são replicados de volta para a origem. Na figura, a replicação entre grades está habilitada para `my-bucket` da Grade 1 para a Grade 2, mas não é habilitado na outra direção.



Replicação em ambas as direções

Se você habilitar a replicação entre grades para o mesmo bucket em ambas as grades, os objetos adicionados a qualquer um dos buckets serão replicados para a outra grade. Na figura, a replicação entre grades está habilitada para `my-bucket` em ambas as direções.



O que acontece quando objetos são ingeridos?

Quando um cliente S3 adiciona um objeto a um bucket que tem a replicação entre grades habilitada, acontece o seguinte:

1. O StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo para executar esta operação de replicação em segundo plano depende de vários fatores, incluindo o número de outras operações de replicação pendentes.

   O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject ou HeadObject. A resposta inclui um StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores: O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação GetObject ou HeadObject. A resposta inclui um StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida para todas as conexões de rede. • **PENDENTE**: O objeto não foi replicado para pelo menos uma conexão de grade. • **FALHA**: A replicação não está pendente para nenhuma conexão de rede e pelo menos uma falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	**REPLICA**: O objeto foi replicado da grade de origem.

   O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

2. O StorageGRID usa as políticas de ILM ativas de cada grade para gerenciar os objetos, assim como faria com qualquer outro objeto. Por exemplo, o Objeto A na Grade 1 pode ser armazenado como duas cópias replicadas e retido para sempre, enquanto a cópia do Objeto A que foi replicada na Grade 2 pode ser

armazenada usando codificação de eliminação 2+1 e excluída após três anos.

O que acontece quando objetos são excluídos?

Conforme descrito em"Excluir fluxo de dados" O StorageGRID pode excluir um objeto por qualquer um destes motivos:

- O cliente S3 emite uma solicitação de exclusão.
- Um usuário do Gerenciador de Inquilinos seleciona o"Excluir objetos no bucket" opção para remover todos os objetos de um bucket.
- O bucket tem uma configuração de ciclo de vida, que expira.
- O último período de tempo na regra ILM para o objeto termina e não há mais posicionamentos especificados.

Quando o StorageGRID exclui um objeto devido a uma operação Excluir objetos no bucket, expiração do ciclo de vida do bucket ou expiração do posicionamento do ILM, o objeto replicado nunca é excluído da outra grade em uma conexão de federação de grade. No entanto, os marcadores de exclusão adicionados ao bucket de origem pelas exclusões do cliente S3 podem, opcionalmente, ser replicados para o bucket de destino.

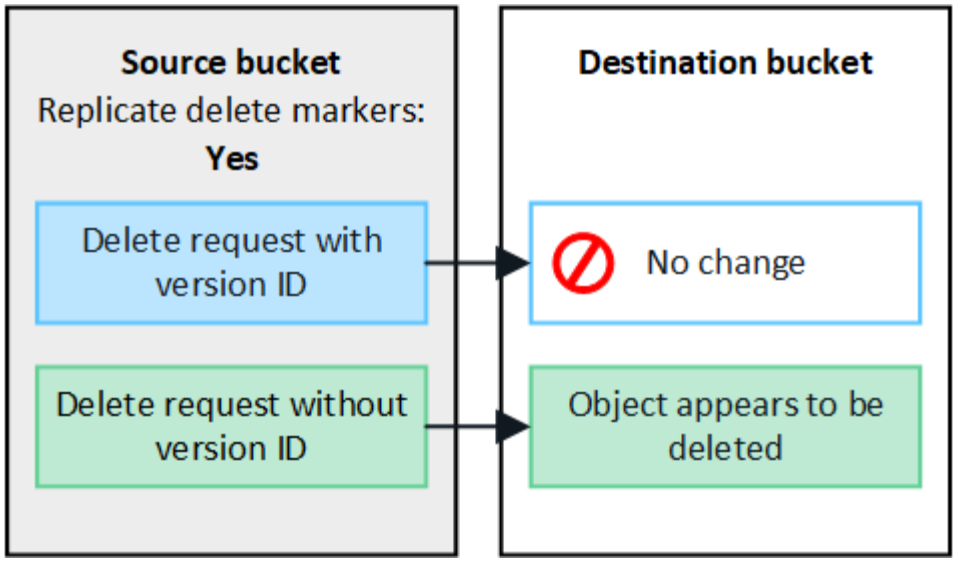
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket que tem a replicação entre grades habilitada, revise como os clientes S3 excluem objetos de buckets que têm o controle de versão habilitado, da seguinte maneira:

- Se um cliente S3 emitir uma solicitação de exclusão que inclua um ID de versão, essa versão do objeto será removida permanentemente. Nenhum marcador de exclusão é adicionado ao bucket.
- Se um cliente S3 emitir uma solicitação de exclusão que não inclua um ID de versão, o StorageGRID não excluirá nenhuma versão de objeto. Em vez disso, ele adiciona um marcador de exclusão ao bucket. O marcador de exclusão faz com que o StorageGRID aja como se o objeto tivesse sido excluído:
  - Uma solicitação GetObject sem um ID de versão falhará com `404 No Object Found`
  - Uma solicitação GetObject com um ID de versão válido será bem-sucedida e retornará a versão do objeto solicitada.

Quando um cliente S3 exclui um objeto de um bucket que tem a replicação entre grades habilitada, o StorageGRID determina se deve replicar a solicitação de exclusão para o destino, da seguinte maneira:

- Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente da grade de origem. No entanto, o StorageGRID não replica solicitações de exclusão que incluem um ID de versão, portanto, a mesma versão do objeto não é excluída do destino.
- Se a solicitação de exclusão não incluir um ID de versão, o StorageGRID poderá, opcionalmente, replicar o marcador de exclusão, com base em como a replicação entre grades estiver configurada para o bucket:
  - Se você optar por replicar marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao bucket de origem e replicado no bucket de destino. Na verdade, o objeto parece ter sido excluído em ambas as grades.
  - Se você optar por não replicar os marcadores de exclusão, um marcador de exclusão será adicionado ao bucket de origem, mas não será replicado no bucket de destino. Na verdade, objetos que são excluídos na grade de origem não são excluídos na grade de destino.

Na figura, **Replicar marcadores de exclusão** foi definido como **Sim** quando"a replicação entre grades foi habilitada" . Solicitações de exclusão para o bucket de origem que incluem um ID de versão não excluirão objetos do bucket de destino. Solicitações de exclusão para o bucket de origem que não incluem um ID de versão aparecerão para excluir objetos no bucket de destino.



Se você deseja manter as exclusões de objetos sincronizadas entre as grades, crie as correspondentes"Configurações do ciclo de vida S3" para os baldes em ambas as grades.

Como os objetos criptografados são replicados

Ao usar a replicação entre grades para replicar objetos entre grades, você pode criptografar objetos individuais, usar a criptografia de bucket padrão ou configurar a criptografia em toda a grade. Você pode adicionar, modificar ou remover configurações de criptografia padrão de bucket ou de toda a grade antes ou depois de habilitar a replicação entre grades para um bucket.

Para criptografar objetos individuais, você pode usar SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID) ao adicionar os objetos ao bucket de origem. Use o `x-amz-server-side-encryption` cabeçalho da solicitação e especificar `AES256` . Ver "Use criptografia do lado do servidor" .

O uso de SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente) não é suportado para replicação entre redes. A operação de ingestão falhará.

Para usar a criptografia padrão para um bucket, use uma solicitação PutBucketEncryption e defina o `SSEAlgorithm` parâmetro para `AES256` . A criptografia em nível de bucket se aplica a todos os objetos ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. Ver "Operações em baldes" .

Para usar a criptografia em nível de grade, defina a opção **Criptografia de objeto armazenado** como **AES-256**. A criptografia em nível de grade se aplica a todos os objetos que não são criptografados no nível do bucket ou que são ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. Ver "Configurar opções de rede e objeto" .

O SSE não suporta AES-128. Se a opção **Criptografia de objeto armazenado** estiver habilitada para a grade de origem usando a opção **AES-128**, o uso do algoritmo AES-128 não será propagado para o objeto replicado. Em vez disso, o objeto replicado usará a configuração de criptografia padrão do bucket ou do nível de grade do destino, se disponível.

Ao determinar como criptografar objetos de origem, o StorageGRID aplica estas regras:

1. Use o `x-amz-server-side-encryption` cabeçalho de ingestão, se presente.
2. Se um cabeçalho de ingestão não estiver presente, use a configuração de criptografia padrão do bucket,

se configurada.

3. Se uma configuração de bucket não estiver configurada, use a configuração de criptografia em toda a grade, se configurada.
4. Se uma configuração para toda a grade não estiver presente, não criptografe o objeto de origem.

Ao determinar como criptografar objetos replicados, o StorageGRID aplica estas regras nesta ordem:

1. Use a mesma criptografia do objeto de origem, a menos que esse objeto use criptografia AES-128.
2. Se o objeto de origem não estiver criptografado ou usar AES-128, use a configuração de criptografia padrão do bucket de destino, se configurada.
3. Se o bucket de destino não tiver uma configuração de criptografia, use a configuração de criptografia em toda a grade do destino, se configurada.
4. Se uma configuração para toda a grade não estiver presente, não criptografe o objeto de destino.

PutObjectTagging e DeleteObjectTagging não são suportados

As solicitações PutObjectTagging e DeleteObjectTagging não são suportadas para objetos em buckets que tenham replicação entre grades habilitada.

Se um cliente S3 emitir uma solicitação PutObjectTagging ou DeleteObjectTagging, `501 Not Implemented` é retornado. A mensagem é `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured.`

Como objetos segmentados são replicados

O tamanho máximo do segmento da grade de origem se aplica a objetos replicados na grade de destino. Quando objetos são replicados para outra grade, a configuração **Tamanho Máximo do Segmento** (**CONFIGURAÇÃO** > **Sistema** > **Opções de armazenamento**) da grade de origem será usada em ambas as grades. Por exemplo, suponha que o tamanho máximo do segmento para a grade de origem seja 1 GB, enquanto o tamanho máximo do segmento da grade de destino seja 50 MB. Se você ingerir um objeto de 2 GB na grade de origem, esse objeto será salvo como dois segmentos de 1 GB. Ele também será replicado para a grade de destino como dois segmentos de 1 GB, embora o tamanho máximo do segmento dessa grade seja 50 MB.

Comparar a replicação entre grades e a replicação do CloudMirror

Ao começar a usar a federação de grade, revise as semelhanças e diferenças entre"replicação entre grades" e o"Serviço de replicação StorageGRID CloudMirror" .

	Replicação entre grades	**Serviço de replicação CloudMirror**
Qual é o objetivo principal?	Um sistema StorageGRID atua como um sistema de recuperação de desastres. Objetos em um bucket podem ser replicados entre as grades em uma ou ambas as direções.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket S3 externo (destino). A replicação do CloudMirror cria uma cópia independente de um objeto em uma infraestrutura S3 independente. Essa cópia independente não é usada como backup, mas geralmente é processada na nuvem.

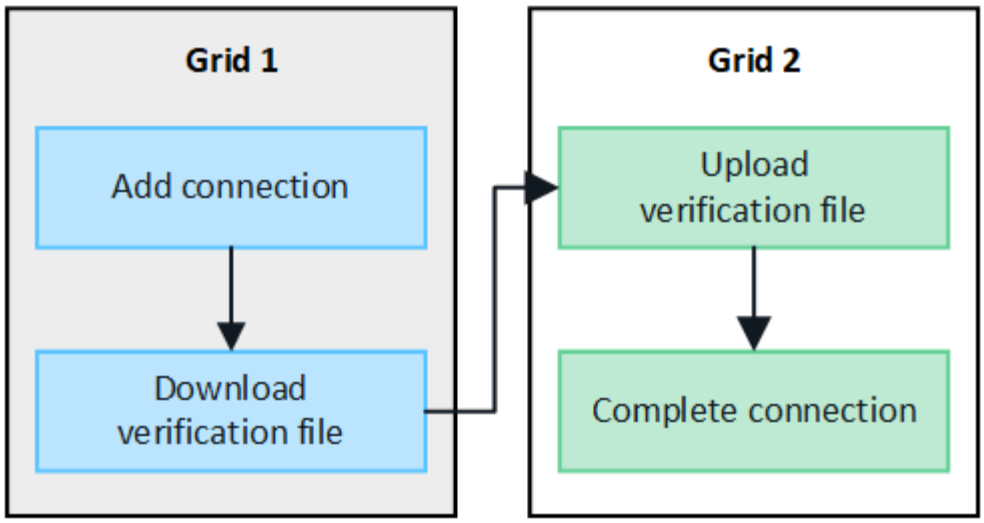
	Replicação entre grades	Serviço de replicação CloudMirror
Como é configurado?	1. Configure uma conexão de federação de grade entre duas grades. 2. Adicione novas contas de locatários, que são clonadas automaticamente para a outra grade. 3. Adicione novos grupos de locatários e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grade e permita que a replicação entre grades ocorra em uma ou ambas as direções.	1. Um usuário locatário configura a replicação do CloudMirror definindo um ponto de extremidade do CloudMirror (endereço IP, credenciais e assim por diante) usando o Gerenciador de Locatários ou a API do S3. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o ponto de extremidade do CloudMirror.
Quem é responsável por configurá-lo?	• Um administrador de grade configura a conexão e os inquilinos. • Os usuários locatários configuram os grupos, usuários, chaves e buckets.	Normalmente, um usuário locatário.
Qual é o destino?	Um bucket S3 correspondente e idêntico no outro sistema StorageGRID na conexão de federação de grade.	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3). • Plataforma de nuvem do Google (GCP)
O controle de versão do objeto é necessário?	Sim, tanto o bucket de origem quanto o de destino devem ter o controle de versão de objetos habilitado.	Não, a replicação do CloudMirror oferece suporte a qualquer combinação de buckets versionados e não versionados na origem e no destino.
O que faz com que os objetos sejam movidos para o destino?	Os objetos são replicados automaticamente quando são adicionados a um bucket que tem a replicação entre grades habilitada.	Os objetos são replicados automaticamente quando são adicionados a um bucket que foi configurado com um endpoint do CloudMirror. Objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são replicados?	A replicação entre grades cria objetos versionados e replica o ID da versão do bucket de origem para o bucket de destino. Isso permite que a ordem das versões seja mantida em ambas as grades.	A replicação do CloudMirror não requer buckets habilitados para controle de versão, portanto, o CloudMirror só pode manter a ordenação de uma chave dentro de um site. Não há garantias de que a ordem será mantida para solicitações de um objeto em um site diferente.
E se um objeto não puder ser replicado?	O objeto é enfileirado para replicação, sujeito aos limites de armazenamento de metadados.	O objeto é enfileirado para replicação, sujeito aos limites dos serviços da plataforma (consulte"Recomendações para uso de serviços de plataforma").

	Replicação entre grades	Serviço de replicação CloudMirror
Os metadados do sistema do objeto são replicados?	Sim, quando um objeto é replicado para outra grade, seus metadados do sistema também são replicados. Os metadados serão idênticos em ambas as grades.	Não, quando um objeto é replicado para o bucket externo, seus metadados do sistema são atualizados. Os metadados serão diferentes entre os locais, dependendo do horário de ingestão e do comportamento da infraestrutura independente do S3.
Como os objetos são recuperados?	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao bucket em qualquer grade.	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao StorageGRID ou ao destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos para uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário usar o StorageGRID .
O que acontece se um objeto for excluído?	• Solicitações de exclusão que incluem um ID de versão nunca são replicadas para a grade de destino. • Solicitações de exclusão que não incluem um ID de versão adicionam um marcador de exclusão ao bucket de origem, que pode ser replicado opcionalmente para a grade de destino. • Se a replicação entre grades for configurada para apenas uma direção, os objetos no bucket de destino poderão ser excluídos sem afetar a origem.	Os resultados variam de acordo com o estado de versão dos buckets de origem e destino (que não precisam ser os mesmos): • Se ambos os buckets forem versionados, uma solicitação de exclusão adicionará um marcador de exclusão em ambos os locais. • Se apenas o bucket de origem for versionado, uma solicitação de exclusão adicionará um marcador de exclusão à origem, mas não ao destino. • Se nenhum dos buckets tiver versão, uma solicitação de exclusão excluirá o objeto da origem, mas não do destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.

Criar conexões de federação de grade

Você pode criar uma conexão de federação de grade entre dois sistemas StorageGRID se quiser clonar detalhes do locatário e replicar dados do objeto.

Conforme mostrado na figura, a criação de uma conexão de federação de grade inclui etapas em ambas as grades. Adicione a conexão em uma grade e complete-a na outra grade. Você pode começar em qualquer grade.



Antes de começar

- Você revisou o"considerações e requisitos" para configurar conexões de federação de grade.
- Se você planeja usar nomes de domínio totalmente qualificados (FQDNs) para cada grade em vez de endereços IP ou VIP, você sabe quais nomes usar e confirmou que o servidor DNS para cada grade tem as entradas apropriadas.
- Você está usando um"navegador da web compatível" .
- Você tem permissão de acesso Root e a senha de provisionamento para ambas as grades.

Adicionar conexão

Execute estas etapas em qualquer um dos dois sistemas StorageGRID .

Passos

1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione **Adicionar conexão**.
4. Insira os detalhes da conexão.

Campo	Descrição
Nome da conexão	Um nome exclusivo para ajudar você a reconhecer essa conexão, por exemplo, "Grade 1-Grade 2".
FQDN ou IP para esta grade	Um dos seguintes: • O FQDN da rede na qual você está conectado no momento • Um endereço VIP de um grupo HA nesta grade • Um endereço IP de um nó de administração ou nó de gateway nesta grade. O IP pode estar em qualquer rede que a grade de destino possa alcançar.

Campo	Descrição
Porta	A porta que você deseja usar para esta conexão. Você pode inserir qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta. Você deve garantir que nenhum nó em nenhuma das grades use esta porta para outras conexões.
Dias de validade do certificado para esta grade	O número de dias que você deseja que os certificados de segurança desta grade na conexão sejam válidos. O valor padrão é 730 dias (2 anos), mas você pode inserir qualquer valor de 1 a 762 dias. O StorageGRID gera automaticamente certificados de cliente e servidor para cada grade quando você salva a conexão.
Senha de provisionamento para esta grade	A senha de provisionamento para a grade na qual você está conectado.
FQDN ou IP para a outra rede	Um dos seguintes: • O FQDN da rede à qual você deseja se conectar • Um endereço VIP de um grupo HA na outra grade • Um endereço IP de um nó de administração ou nó de gateway na outra grade. O IP pode estar em qualquer rede que a grade de origem possa alcançar.

5. Selecione **Salvar e continuar**.
6. Para a etapa Baixar arquivo de verificação, selecione **Baixar arquivo de verificação**.

   Após a conexão ser concluída na outra rede, você não poderá mais baixar o arquivo de verificação de nenhuma delas.

7. Localize o arquivo baixado(*`connection-name`*`.grid-federation`) e salve-o em um local seguro.

   Este arquivo contém segredos (mascarados como *) e outros detalhes confidenciais e devem ser armazenados e transmitidos com segurança.

8. Selecione **Fechar** para retornar à página de federação da grade.
9. Confirme se a nova conexão é exibida e se seu **Status da conexão** é **Aguardando conexão**.
10. Fornecer o *`connection-name`*`.grid-federation` arquivo para o administrador da grade para a outra grade.

Conexão completa

Execute estas etapas no sistema StorageGRID ao qual você está se conectando (a outra grade).

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.

2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de Carregar.
4. Selecione **Carregar arquivo de verificação**. Em seguida, navegue e selecione o arquivo que foi baixado da primeira grade(`connection-name.grid-federation`).

   Os detalhes da conexão são mostrados.

5. Opcionalmente, insira um número diferente de dias válidos para os certificados de segurança desta grade. A entrada **Dias de validade do certificado** assume como padrão o valor inserido na primeira grade, mas cada grade pode usar datas de validade diferentes.

   Em geral, use o mesmo número de dias para os certificados em ambos os lados da conexão.

   > Se os certificados em qualquer extremidade da conexão expirarem, a conexão deixará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

6. Digite a senha de provisionamento da grade na qual você está conectado no momento.
7. Selecione **Salvar e testar**.

   Os certificados são gerados e a conexão é testada. Se a conexão for válida, uma mensagem de sucesso será exibida e a nova conexão será listada na página Federação do Grid. O **Status da conexão** será **Conectado**.

   Se uma mensagem de erro for exibida, resolva quaisquer problemas. Ver "Solucionar erros de federação de grade" .

8. Vá para a página da federação da grade na primeira grade e atualize o navegador. Confirme se o **Status da conexão** agora é **Conectado**.
9. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

   Se você editar esta conexão, um novo arquivo de verificação será criado. O arquivo original não pode ser reutilizado.

Depois que você terminar

- Revise as considerações para"gerenciamento de inquilinos permitidos" .
- "Crie uma ou mais novas contas de inquilino", atribua a permissão **Usar conexão de federação de grade** e selecione a nova conexão.
- "Gerenciar a conexão"conforme necessário. Você pode editar valores de conexão, testar uma conexão, girar certificados de conexão ou remover uma conexão.
- "Monitore a conexão"como parte de suas atividades normais de monitoramento do StorageGRID .
- "Solucionar problemas de conexão", incluindo a resolução de quaisquer alertas e erros relacionados à clonagem de conta e à replicação entre redes.

Gerenciar conexões de federação de grade

O gerenciamento de conexões de federação de grade entre sistemas StorageGRID inclui a edição de detalhes de conexão, a rotação de certificados, a remoção de permissões de locatário e a remoção de conexões não utilizadas.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grades usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" para a grade na qual você está conectado.

Editar uma conexão de federação de grade

Você pode editar uma conexão de federação de grade entrando no nó de administração principal em qualquer grade na conexão. Depois de fazer alterações na primeira grade, você deve baixar um novo arquivo de verificação e enviá-lo para a outra grade.

> ⓘ Enquanto a conexão estiver sendo editada, as solicitações de clonagem de conta ou replicação entre redes continuarão a usar as configurações de conexão existentes. Todas as edições feitas na primeira grade são salvas localmente, mas não são usadas até que sejam carregadas na segunda grade, salvas e testadas.

Comece a editar a conexão

Passos

1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **NÓS** e confirme se todos os outros nós de administração no seu sistema estão online.

   > ⓘ Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Se este arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso aparecerá quando você selecionar **Salvar e testar**.

3. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
4. Edite os detalhes da conexão usando o menu **Ações** na página Federação de grade ou na página de detalhes de uma conexão específica. Ver"Criar conexões de federação de grade" para o que inserir.

   Menu de ações

   a. Selecione o botão de opção para a conexão.
   b. Selecione **Ações** > **Editar**.
   c. Insira as novas informações.

   Página de detalhes

   a. Selecione um nome de conexão para exibir seus detalhes.
   b. Selecione **Editar**.
   c. Insira as novas informações.

5. Digite a senha de provisionamento da grade na qual você está conectado.
6. Selecione **Salvar e continuar**.

   Os novos valores são salvos, mas não serão aplicados à conexão até que você carregue o novo arquivo de verificação na outra grade.

7. Selecione **Baixar arquivo de verificação**.

   Para baixar este arquivo mais tarde, acesse a página de detalhes da conexão.

8. Localize o arquivo baixado(*connection-name*`.grid-federation`) e salve-o em um local seguro.

   > O arquivo de verificação contém segredos e deve ser armazenado e transmitido com segurança.

9. Selecione **Fechar** para retornar à página de federação da grade.
10. Confirme se o **Status da conexão** é **Edição pendente**.

    > Se o status da conexão for diferente de **Conectado** quando você começar a editar a conexão, ele não mudará para **Edição pendente**.

11. Fornecer o *connection-name*`.grid-federation` arquivo para o administrador da grade para a outra grade.

Finalizar edição da conexão

Conclua a edição da conexão carregando o arquivo de verificação na outra grade.

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, navegue e selecione o arquivo que foi baixado da primeira grade.
5. Digite a senha de provisionamento da grade na qual você está conectado no momento.
6. Selecione **Salvar e testar**.

   Se a conexão puder ser estabelecida usando os valores editados, uma mensagem de sucesso será exibida. Caso contrário, uma mensagem de erro será exibida. Revise a mensagem e resolva quaisquer problemas.

7. Feche o assistente para retornar à página Federação de grade.
8. Confirme se o **Status da conexão** é **Conectado**.
9. Vá para a página da federação da grade na primeira grade e atualize o navegador. Confirme se o **Status da conexão** agora é **Conectado**.
10. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Testar uma conexão de federação de grade

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Teste a conexão usando o menu **Ações** na página de federação da grade ou na página de detalhes de uma conexão específica.

Menu de ações

a. Selecione o botão de opção para a conexão.

b. Selecione **Ações** > **Testar**.

Página de detalhes

a. Selecione um nome de conexão para exibir seus detalhes.

b. Selecione **Testar conexão**.

4. Revise o status da conexão:

Status da conexão	Descrição
Conectado	Ambas as redes estão conectadas e se comunicando normalmente.
Erro	A conexão está em estado de erro. Por exemplo, um certificado expirou ou um valor de configuração não é mais válido.
Edição pendente	Você editou a conexão nesta grade, mas a conexão ainda está usando a configuração existente. Para concluir a edição, carregue o novo arquivo de verificação na outra grade.
Aguardando conexão	Você configurou a conexão nesta grade, mas a conexão não foi concluída na outra grade. Baixe o arquivo de verificação desta grade e carregue-o na outra grade.
Desconhecido	A conexão está em um estado desconhecido, possivelmente devido a um problema de rede ou um nó offline.

5. Se o status da conexão for **Erro**, resolva quaisquer problemas. Em seguida, selecione **Testar conexão** novamente para confirmar que o problema foi corrigido.

Rotular certificados de conexão

Cada conexão de federação de grade usa quatro certificados SSL gerados automaticamente para proteger a conexão. Quando os dois certificados de cada grade estiverem próximos da data de expiração, o alerta **Expiração do certificado de federação da grade** lembrará você de rotacionar os certificados.

> Se os certificados em qualquer extremidade da conexão expirarem, a conexão deixará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

Passos

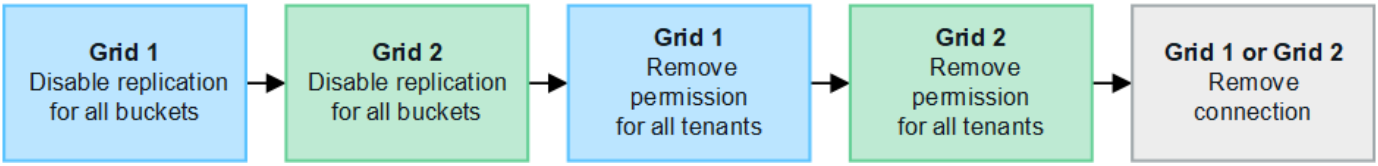
1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Em qualquer uma das guias da página Federação da grade, selecione o nome da conexão para exibir seus detalhes.
4. Selecione a aba **Certificados**.

5. Selecione **Girar certificados**.
6. Especifique por quantos dias os novos certificados devem ser válidos.
7. Digite a senha de provisionamento da grade na qual você está conectado.
8. Selecione **Girar certificados**.
9. Conforme necessário, repita essas etapas na outra grade da conexão.

   Em geral, use o mesmo número de dias para os certificados em ambos os lados da conexão.

Remover uma conexão de federação de grade

Você pode remover uma conexão de federação de grade de qualquer grade na conexão. Conforme mostrado na figura, você deve executar etapas de pré-requisito em ambas as grades para confirmar que a conexão não está sendo usada por nenhum locatário em nenhuma delas.



Antes de remover uma conexão, observe o seguinte:

- Remover uma conexão não exclui nenhum item que já tenha sido copiado entre grades. Por exemplo, usuários, grupos e objetos locatários que existem em ambas as grades não são excluídos de nenhuma delas quando a permissão do locatário é removida. Se você quiser excluir esses itens, deverá excluí-los manualmente de ambas as grades.
- Quando você remove uma conexão, a replicação de todos os objetos com replicação pendente (ingeridos, mas ainda não replicados para a outra grade) falhará permanentemente.

Desabilitar replicação para todos os buckets de locatários

Passos

1. A partir de qualquer grade, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na aba **Inquilinos permitidos**, determine se a conexão está sendo usada por algum inquilino.
5. Se houver algum inquilino listado, instrua todos os inquilinos a"desabilitar replicação entre redes" para todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **Usar conexão de federação de grade** se algum bucket de locatário tiver replicação entre grades habilitada. Cada conta de locatário deve desabilitar a replicação entre grades para seus buckets em ambas as grades.

Remover permissão para cada inquilino

Depois que a replicação entre grades for desabilitada para todos os buckets de locatários, remova a **Permissão de federação de uso de grade** de todos os locatários em ambas as grades.

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
2. Selecione o nome da conexão para exibir seus detalhes.
3. Para cada locatário na guia **Locatários permitidos**, remova a permissão **Usar conexão de federação de grade** de cada locatário. Ver "Gerenciar inquilinos permitidos" .
4. Repita essas etapas para os inquilinos permitidos na outra grade.

Remover conexão

Passos

1. Quando nenhum inquilino em nenhuma das redes estiver usando a conexão, selecione **Remover**.
2. Revise a mensagem de confirmação e selecione **Remover**.
   - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão da federação de rede agora foi removida de ambas as redes.
   - Se a conexão não puder ser removida (por exemplo, se ela ainda estiver em uso ou se houver um erro de conexão), uma mensagem de erro será exibida. Você pode fazer qualquer um dos seguintes:
     - Resolva o erro (recomendado). Ver "Solucionar erros de federação de grade" .
     - Remova a conexão à força. Veja a próxima seção.

Remover uma conexão de federação de grade à força

Se necessário, você pode forçar a remoção de uma conexão que não tenha o status **Conectado**.

A remoção forçada apenas exclui a conexão da rede local. Para remover completamente a conexão, execute os mesmos passos em ambas as grades.

Passos

1. Na caixa de diálogo de confirmação, selecione **Forçar remoção**.

   Uma mensagem de sucesso é exibida. Esta conexão de federação de rede não pode mais ser usada. No entanto, os buckets de locatários ainda podem ter a replicação entre grades habilitada e algumas cópias de objetos podem já ter sido replicadas entre as grades na conexão.

2. Da outra grade na conexão, efetue login no Grid Manager a partir do nó de administração principal.
3. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
4. Selecione o nome da conexão para exibir seus detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **Forçar remoção** para remover a conexão desta grade.

Gerenciar os inquilinos permitidos para federação de rede

Você pode permitir que contas de locatários do S3 usem uma conexão de federação de grade entre dois sistemas StorageGRID . Quando os inquilinos têm permissão para usar uma conexão, etapas especiais são necessárias para editar os detalhes do inquilino ou remover permanentemente a permissão de um inquilino para usar a conexão.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grades usando um"navegador da web

compatível" .

- Você tem o"Permissão de acesso root" para a grade na qual você está conectado.
- Você tem"criou uma conexão de federação de grade" entre duas grades.
- Você revisou os fluxos de trabalho para"clone de conta" e"replicação entre grades" .
- Conforme necessário, você já configurou o logon único (SSO) ou a federação de identidade para ambas as grades na conexão. Ver "O que é clone de conta" .

Criar um inquilino permitido

Se você deseja permitir que uma conta de locatário nova ou existente use uma conexão de federação de grade para clonagem de conta e replicação entre grades, siga as instruções gerais para"criar um novo locatário S3" ou"editar uma conta de inquilino" e observe o seguinte:

- Você pode criar o locatário de qualquer grade na conexão. A grade onde um locatário é criado é a *grade de origem do locatário*.
- O status da conexão deve ser **Conectado**.
- Quando o locatário é criado ou editado para habilitar a permissão **Usar conexão de federação de grade** e depois salvo na primeira grade, um locatário idêntico é replicado automaticamente para a outra grade. A grade onde o locatário é replicado é a *grade de destino do locatário*.
- Os inquilinos em ambas as grades terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões. Opcionalmente, você pode usar o campo **Descrição** para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado na Grade 2: "Este locatário foi criado na Grade 1".
- Por motivos de segurança, a senha de um usuário root local não é copiada para a grade de destino.

> Antes que um usuário root local possa efetuar login no locatário replicado na grade de destino, um administrador de grade para essa grade deve"alterar a senha do usuário root local" .

- Depois que o novo locatário ou o locatário editado estiver disponível em ambas as grades, os usuários locatários poderão executar estas operações:
  - Na grade de origem do locatário, crie grupos e usuários locais, que serão clonados automaticamente na grade de destino do locatário. Ver "Clonar grupos de locatários e usuários" .
  - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para a grade de destino do locatário. Ver "Clonar chaves de acesso S3 usando a API" .
  - Crie buckets idênticos em ambas as grades na conexão e habilite a replicação entre grades em uma direção ou em ambas as direções. Ver "Gerenciar replicação entre redes" .

Ver um inquilino permitido

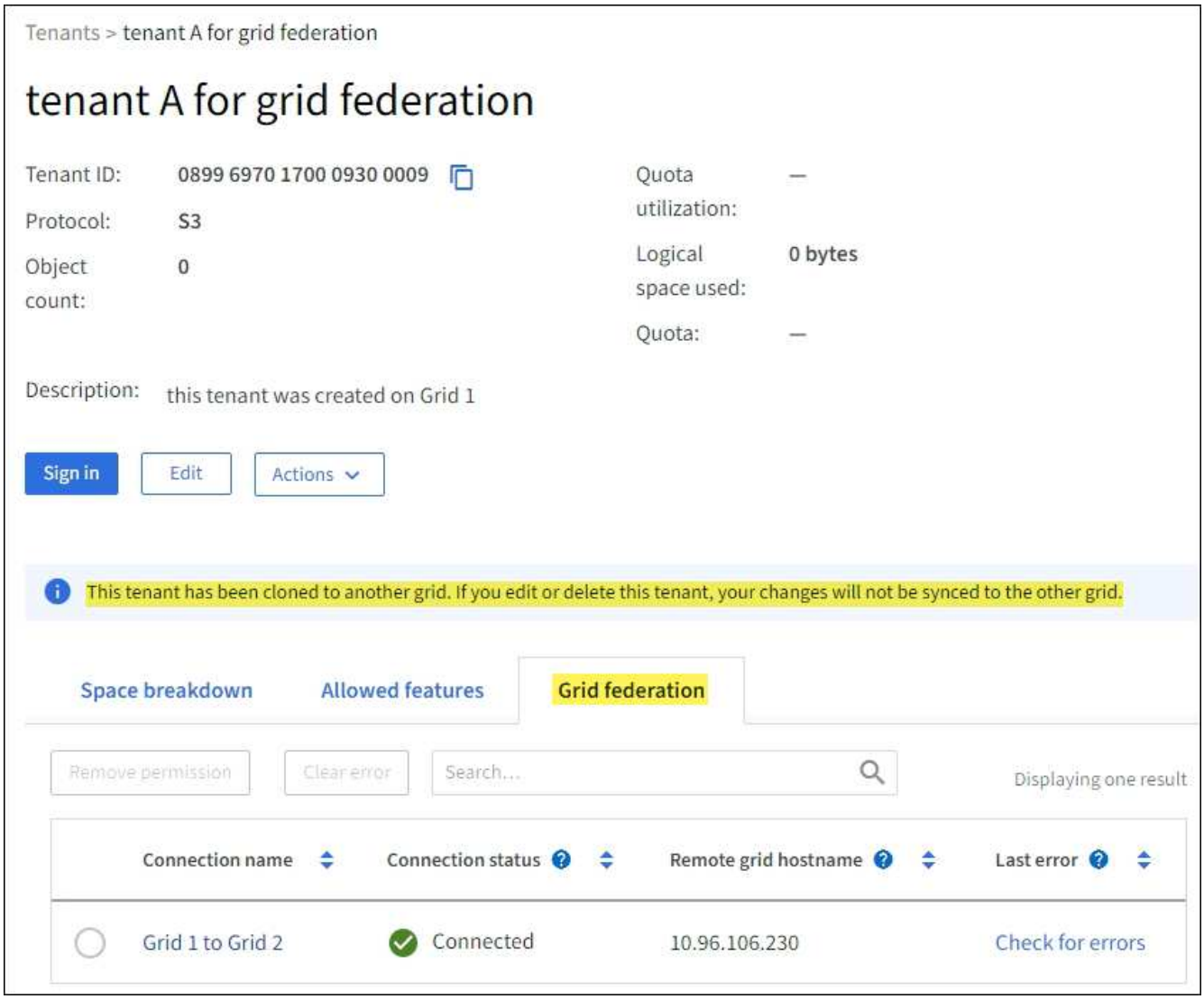
Você pode ver detalhes de um locatário que tem permissão para usar uma conexão de federação de rede.

Passos

1. Selecione **LOCATÁRIOS**.
2. Na página Inquilinos, selecione o nome do inquilino para visualizar a página de detalhes do inquilino.

   Se esta for a grade de origem do locatário (ou seja, se o locatário foi criado nesta grade), um banner

aparecerá para lembrá-lo de que o locatário foi clonado em outra grade. Se você editar ou excluir este locatário, suas alterações não serão sincronizadas com a outra grade.



3. Opcionalmente, selecione a aba **Federação de grade** para"monitorar a conexão da federação de rede" .

Editar um inquilino permitido

Se você precisar editar um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais para"editando uma conta de locatário" e observe o seguinte:

- Se um locatário tiver a permissão **Usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. Entretanto, quaisquer alterações que você fizer não serão copiadas para a outra grade. Se quiser manter os detalhes do inquilino sincronizados entre as grades, você deve fazer as mesmas edições em ambas as grades.
- Não é possível limpar a permissão **Usar conexão de federação de grade** quando você estiver editando um locatário.
- Não é possível selecionar uma conexão de federação de grade diferente ao editar um locatário.

Excluir um inquilino permitido

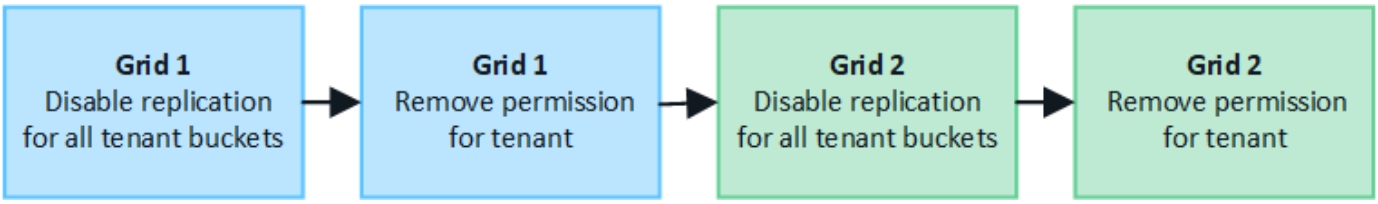
Se você precisar remover um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais para"excluindo uma conta de inquilino" e observe o seguinte:

- Antes de remover o locatário original na grade de origem, você deve remover todos os buckets da conta na grade de origem.
- Antes de remover o locatário clonado na grade de destino, você deve remover todos os buckets da conta na grade de destino.
- Se você remover o locatário original ou clonado, a conta não poderá mais ser usada para replicação entre redes.
- Se você estiver removendo o locatário original na grade de origem, quaisquer grupos de locatários, usuários ou chaves que foram clonados na grade de destino não serão afetados. Você pode excluir o locatário clonado ou permitir que ele gerencie seus próprios grupos, usuários, chaves de acesso e buckets.
- Se você estiver removendo o locatário clonado na grade de destino, ocorrerão erros de clonagem se novos grupos ou usuários forem adicionados ao locatário original.

  Para evitar esses erros, remova a permissão do locatário para usar a conexão de federação da grade antes de excluir o locatário desta grade.

Remover permissão de conexão de federação de grade

Para impedir que um locatário use uma conexão de federação de grade, você deve remover a permissão **Usar conexão de federação de grade**.



Antes de remover a permissão de um locatário para usar uma conexão de federação de grade, observe o seguinte:

- Você não pode remover a permissão **Usar conexão de federação de grade** se algum dos buckets do locatário tiver a replicação entre grades habilitada. A conta do locatário deve primeiro desabilitar a replicação entre redes para todos os seus buckets.
- Remover a permissão **Usar conexão de federação de grade** não exclui nenhum item que já tenha sido replicado entre grades. Por exemplo, quaisquer usuários, grupos e objetos locatários que existam em ambas as grades não serão excluídos de nenhuma delas quando a permissão do locatário for removida. Se você quiser excluir esses itens, deverá excluí-los manualmente de ambas as grades.
- Se você quiser reativar essa permissão com a mesma conexão de federação de grade, exclua esse locatário na grade de destino primeiro; caso contrário, reativar essa permissão resultará em um erro.

> Reativar a permissão **Usar conexão de federação de grade** torna a grade local a grade de origem e aciona a clonagem para a grade remota especificada pela conexão de federação de grade selecionada. Se a conta do locatário já existir na grade remota, a clonagem resultará em um erro de conflito.

Antes de começar

- Você está usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" para ambas as grades.

Desabilitar replicação para buckets de locatários

Como primeira etapa, desabilite a replicação entre grades para todos os buckets de locatários.

Passos

1. A partir de qualquer grade, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na guia **Inquilinos permitidos**, determine se o inquilino está usando a conexão.
5. Se o inquilino estiver listado, instrua-o a"desabilitar replicação entre redes" para todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **Usar conexão de federação de grade** se algum bucket de locatário tiver replicação entre grades habilitada. O locatário deve desabilitar a replicação entre grades para seus buckets em ambas as grades.

Remover permissão para inquilino

Depois que a replicação entre grades for desabilitada para buckets de locatários, você poderá remover a permissão do locatário para usar a conexão de federação de grade.

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Remova a permissão da página de federação do Grid ou da página de Tenants.

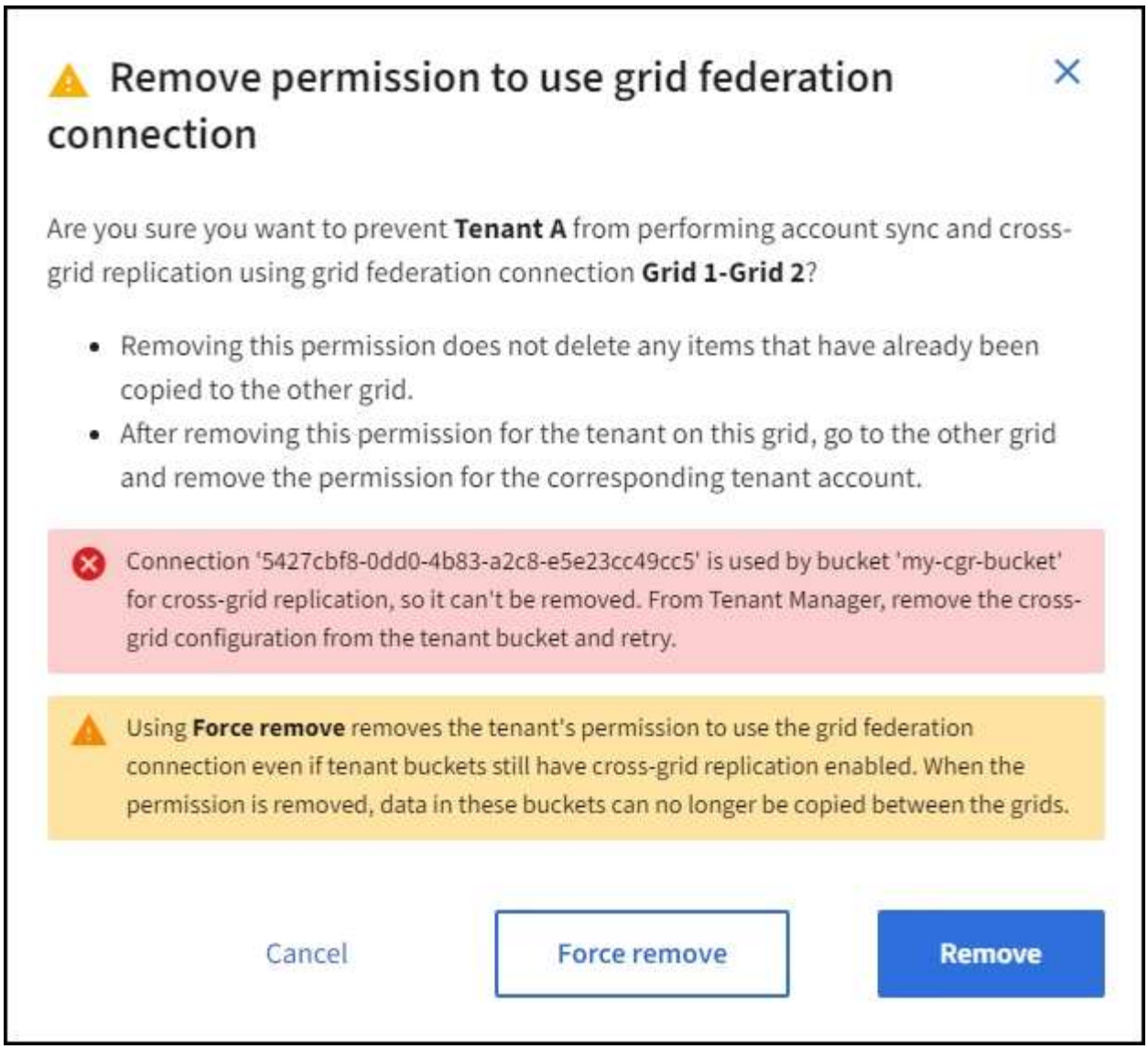
Página da federação da grade

a. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
b. Selecione o nome da conexão para exibir sua página de detalhes.
c. Na aba **Inquilinos permitidos**, selecione o botão de opção para o inquilino.
d. Selecione **Remover permissão**.

Página de inquilinos

a. Selecione **LOCATÁRIOS**.
b. Selecione o nome do inquilino para exibir a página de detalhes.
c. Na aba **Federação de grade**, selecione o botão de opção para a conexão.
d. Selecione **Remover permissão**.

3. Revise os avisos na caixa de diálogo de confirmação e selecione **Remover**.
   - Se a permissão puder ser removida, você retornará à página de detalhes e uma mensagem de sucesso será exibida. Este locatário não pode mais usar a conexão de federação de rede.
   - Se um ou mais buckets de locatários ainda tiverem a replicação entre grades habilitada, um erro será exibido.



Você pode fazer qualquer um dos seguintes:

- (Recomendado.) Sign in no Gerenciador de locatários e desative a replicação para cada um dos buckets do locatário. Ver "Gerenciar replicação entre redes" . Em seguida, repita as etapas para remover a permissão **Usar conexão de rede**.
- Remova a permissão à força. Veja a próxima seção.

4. Vá para a outra grade e repita essas etapas para remover a permissão do mesmo locatário na outra grade.

Remover a permissão à força

Se necessário, você pode forçar a remoção da permissão de um locatário para usar uma conexão de federação de grade, mesmo que os buckets de locatário tenham a replicação entre grades habilitada.

Antes de retirar a permissão de um inquilino à força, observe as considerações gerais pararemovendo a permissão bem como estas considerações adicionais:

- Se você remover a permissão **Usar conexão de federação de grade** à força, todos os objetos que estiverem com replicação pendente para a outra grade (ingeridos, mas ainda não replicados) continuarão sendo replicados. Para evitar que esses objetos em processo cheguem ao bucket de destino, você deve

remover a permissão do locatário na outra grade também.

- Quaisquer objetos ingeridos no bucket de origem após você remover a permissão **Usar conexão de federação de grade** nunca serão replicados para o bucket de destino.

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO** > **Sistema** > **Federação de grade**.
3. Selecione o nome da conexão para exibir sua página de detalhes.
4. Na aba **Inquilinos permitidos**, selecione o botão de opção para o inquilino.
5. Selecione **Remover permissão**.
6. Revise os avisos na caixa de diálogo de confirmação e selecione **Forçar remoção**.

   Uma mensagem de sucesso é exibida. Este locatário não pode mais usar a conexão de federação de rede.

7. Conforme necessário, vá para a outra grade e repita essas etapas para forçar a remoção da permissão para a mesma conta de locatário na outra grade. Por exemplo, você deve repetir essas etapas na outra grade para evitar que objetos em processo cheguem ao bucket de destino.

Solucionar erros de federação de grade

Pode ser necessário solucionar alertas e erros relacionados a conexões de federação de grade, clonagem de conta e replicação entre grades.

Alertas e erros de conexão de federação de rede

Você pode receber alertas ou enfrentar erros com suas conexões de federação de rede.

Depois de fazer qualquer alteração para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne para **Conectado**. Para obter instruções, consulte"Gerenciar conexões de federação de grade" .

Alerta de falha de conexão da federação de rede

Emitir

O alerta **Falha na conexão da federação de rede** foi acionado.

Detalhes

Este alerta indica que a conexão da federação de rede entre as redes não está funcionando.

Ações recomendadas

1. Revise as configurações na página Federação de grade para ambas as grades. Confirme se todos os valores estão corretos. Ver "Gerenciar conexões de federação de grade" .
2. Revise os certificados usados para a conexão. Certifique-se de que não haja alertas para certificados de federação de grade expirados e que os detalhes de cada certificado sejam válidos. Veja as instruções para rotação de certificados de conexão em"Gerenciar conexões de federação de grade" .
3. Confirme se todos os nós de administração e gateway em ambas as grades estão on-line e disponíveis. Resolva quaisquer alertas que possam estar afetando esses nós e tente novamente.
4. Se você forneceu um nome de domínio totalmente qualificado (FQDN) para a grade local ou remota,

confirme se o servidor DNS está online e disponível. Ver"O que é federação de grade?" para requisitos de rede, endereço IP e DNS.

Alerta de expiração do certificado de federação de rede

Emitir

O alerta **Expiração do certificado de federação de rede** foi acionado.

Detalhes

Este alerta indica que um ou mais certificados de federação de grade estão prestes a expirar.

Ações recomendadas

Veja as instruções para rotação de certificados de conexão em"Gerenciar conexões de federação de grade" .

Erro ao editar uma conexão de federação de grade

Emitir

Ao editar uma conexão de federação de grade, você verá a seguinte mensagem de aviso ao selecionar **Salvar e testar**: "Falha ao criar um arquivo de configuração candidato em um ou mais nós."

Detalhes

Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Uma mensagem de aviso será exibida se este arquivo não puder ser salvo em todos os nós administrativos, por exemplo, porque um nó administrativo está offline.

Ações recomendadas

1. Na grade que você está usando para editar a conexão, selecione **NÓS**.
2. Confirme se todos os nós de administração dessa grade estão on-line.
3. Se algum nó estiver offline, coloque-o online novamente e tente editar a conexão novamente.

Erros de clonagem de conta

Não é possível fazer login em uma conta de locatário clonada

Emitir

Você não pode entrar em uma conta de locatário clonada. A mensagem de erro na página de login do Gerenciador de locatários é "Suas credenciais para esta conta eram inválidas. Por favor, tente novamente."

Detalhes

Por motivos de segurança, quando uma conta de locatário é clonada da grade de origem do locatário para a grade de destino do locatário, a senha definida para o usuário raiz local do locatário não é clonada. Da mesma forma, quando um locatário cria usuários locais em sua grade de origem, as senhas dos usuários locais não são clonadas para a grade de destino.

Ações recomendadas

Antes que o usuário root possa efetuar login na grade de destino do locatário, um administrador de grade deve primeiro"alterar a senha do usuário root local" na grade de destino.

Antes que um usuário local clonado possa fazer login na grade de destino do locatário, o usuário raiz do locatário clonado deve adicionar uma senha para o usuário na grade de destino. Para obter instruções, consulte"Gerenciar usuários locais" nas instruções de uso do Gerenciador de Inquilinos.

Inquilino criado sem um clone

Emitir

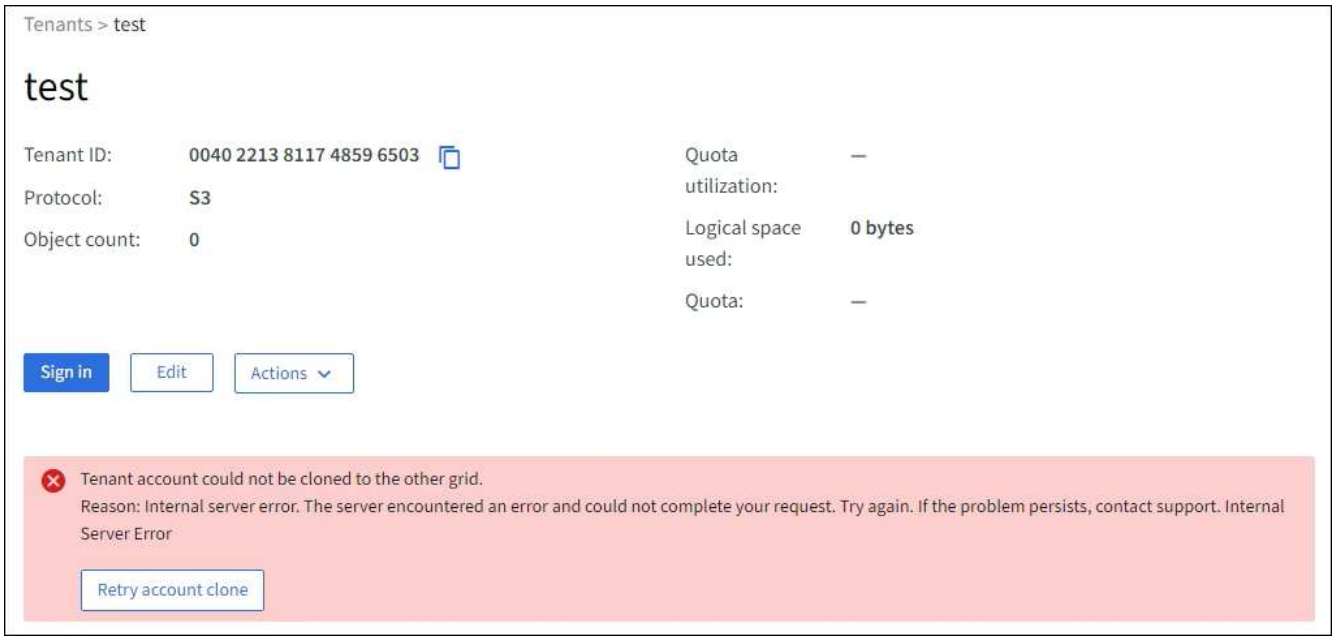
Você vê a mensagem "Locatário criado sem um clone" após criar um novo locatário com a permissão **Usar conexão de federação de grade**.

Detalhes

Esse problema pode ocorrer se as atualizações do status da conexão forem atrasadas, o que pode fazer com que uma conexão não saudável seja listada como **Conectada**.

Ações recomendadas

1. Revise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo o funcionamento da conexão. Ver Alertas e erros de conexão da federação de rede .
2. Siga as instruções para testar uma conexão de federação de rede em"Gerenciar conexões de federação de grade" para confirmar se o problema foi corrigido.
3. Na grade de origem do locatário, selecione **LOCATÁRIOS**.
4. Localize a conta do locatário que não foi clonada.
5. Selecione o nome do inquilino para exibir a página de detalhes.
6. Selecione **Repetir clonagem da conta**.



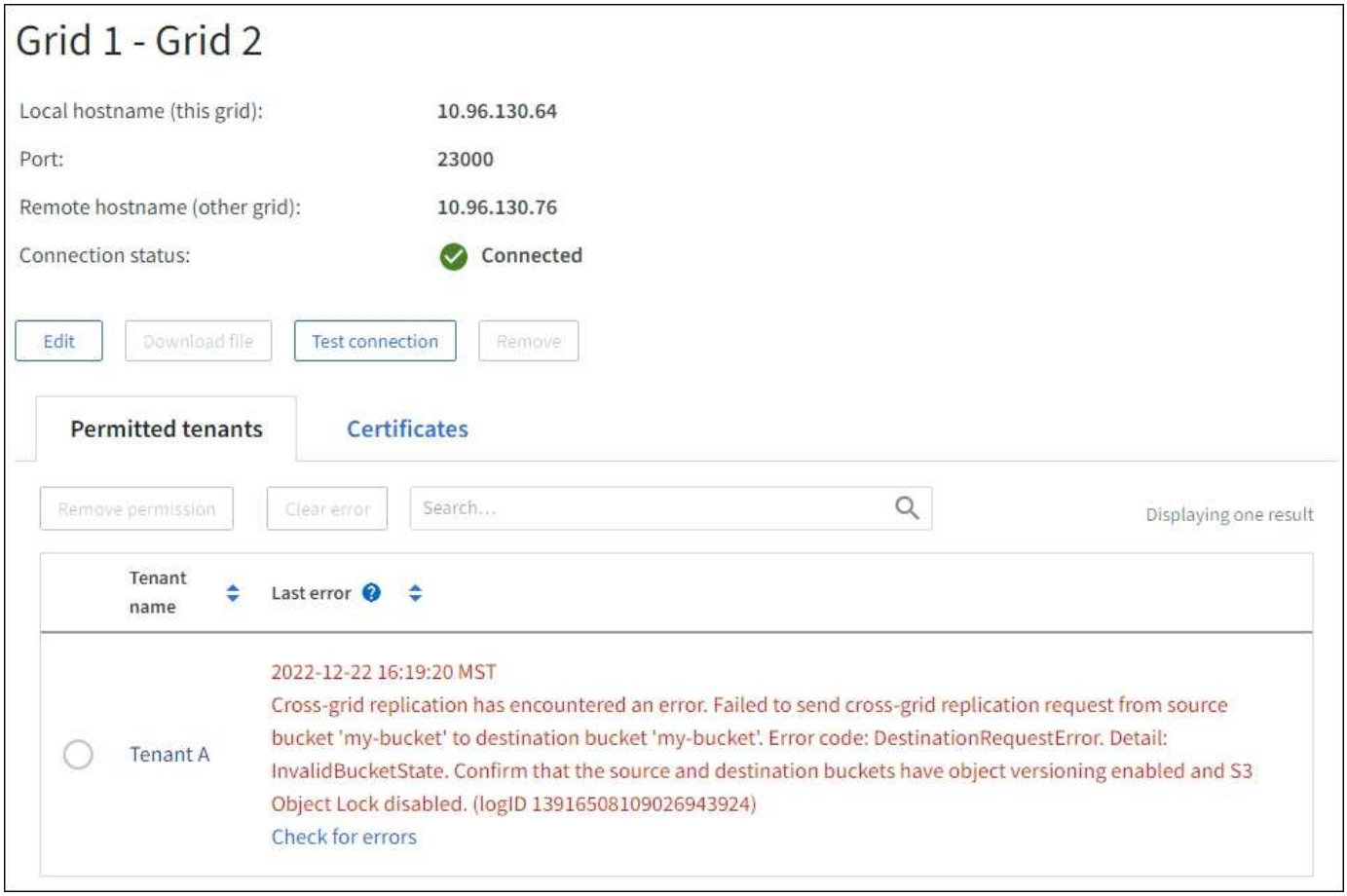
Se o erro tiver sido resolvido, a conta do locatário será clonada para a outra grade.

Alertas e erros de replicação entre grades

Último erro mostrado para conexão ou locatário

Emitir

Quando"visualizando uma conexão de federação de grade" (ou quando"gerenciando os inquilinos permitidos" para uma conexão), você percebe um erro na coluna **Último erro** na página de detalhes da conexão. Por exemplo:



Detalhes

Para cada conexão de federação de grade, a coluna **Último erro** mostra o erro mais recente ocorrido, se houver, quando os dados de um locatário estavam sendo replicados para a outra grade. Esta coluna mostra apenas o último erro de replicação entre grades que ocorreu; erros anteriores que possam ter ocorrido não serão mostrados. Um erro nesta coluna pode ocorrer por um destes motivos:

- A versão do objeto de origem não foi encontrada.
- O bucket de origem não foi encontrado.
- O bucket de destino foi excluído.
- O bucket de destino foi recriado por uma conta diferente.
- O bucket de destino tem o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora não tem versão.

Ações recomendadas

Se uma mensagem de erro aparecer na coluna **Último erro**, siga estas etapas:

1. Revise o texto da mensagem.
2. Execute todas as ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão para esse bucket.
3. Selecione a conta de conexão ou locatário na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.

6. Espere de 5 a 6 minutos e então ingira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

   Para garantir que a mensagem de erro seja apagada, aguarde pelo menos 5 minutos após o registro de data e hora na mensagem antes de ingerir um novo objeto.

   Depois de limpar o erro, um novo **Último erro** pode aparecer se os objetos forem ingeridos em um bucket diferente que também tenha um erro.

7. Para determinar se algum objeto não foi replicado devido ao erro do bucket, consulte"Identificar e tentar novamente operações de replicação com falha" .

Alerta de falha permanente de replicação entre redes

Emitir

O alerta **Falha permanente de replicação entre grades** foi acionado.

Detalhes

Este alerta indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Esse alerta geralmente é causado por uma alteração no bucket de origem ou de destino.

Ações recomendadas

1. Sign in na grade onde o alerta foi acionado.
2. Vá para **CONFIGURAÇÃO** > **Sistema** > **Federação de grade** e localize o nome da conexão listado no alerta.
3. Na guia Inquilinos permitidos, observe a coluna **Último erro** para determinar quais contas de inquilinos apresentam erros.
4. Para saber mais sobre a falha, consulte as instruções em"Monitorar conexões de federação de rede" para revisar as métricas de replicação entre grades.
5. Para cada conta de locatário afetada:
   a. Veja as instruções em"Monitorar a atividade do inquilino" para confirmar que o locatário não excedeu sua cota na grade de destino para replicação entre grades.
   b. Conforme necessário, aumente a cota do locatário na grade de destino para permitir que novos objetos sejam salvos.
6. Para cada locatário afetado, faça login no Gerenciador de Locatários em ambas as grades para poder comparar a lista de buckets.
7. Para cada bucket que tenha replicação entre grades habilitada, confirme o seguinte:
   - Há um bucket correspondente para o mesmo locatário na outra grade (é necessário usar o nome exato).
   - Ambos os buckets têm o controle de versão de objetos habilitado (o controle de versão não pode ser suspenso em nenhuma das grades).
   - Ambos os buckets têm o bloqueio de objeto S3 desabilitado.
   - Nenhum bucket está no estado **Excluindo objetos: somente leitura**.
8. Para confirmar se o problema foi resolvido, consulte as instruções em"Monitorar conexões de federação de rede" para revisar as métricas de replicação entre grades ou executar estas etapas:

a. Volte para a página da federação Grid.

b. Selecione o inquilino afetado e selecione **Limpar erro** na coluna **Último erro**.

c. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.

d. Espere de 5 a 6 minutos e então ingira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

> Para garantir que a mensagem de erro seja apagada, aguarde pelo menos 5 minutos após o registro de data e hora na mensagem antes de ingerir um novo objeto.

> Pode levar até um dia para que o alerta desapareça após ser resolvido.

a. Vá para"Identificar e tentar novamente operações de replicação com falha" para identificar quaisquer objetos ou excluir marcadores que não foram replicados para a outra grade e tentar replicar novamente conforme necessário.

Alerta de recurso de replicação entre grades indisponível

Emitir

O alerta **Recurso de replicação entre grades indisponível** foi acionado.

Detalhes

Este alerta indica que solicitações de replicação entre grades estão pendentes porque um recurso não está disponível. Por exemplo, pode haver um erro de rede.

Ações recomendadas

1. Monitore o alerta para ver se o problema se resolve sozinho.
2. Se o problema persistir, determine se alguma das grades tem um alerta **Falha na conexão da federação da grade** para a mesma conexão ou um alerta **Não foi possível comunicar com o nó** para um nó. Este alerta pode ser resolvido quando você resolver esses alertas.
3. Para saber mais sobre a falha, consulte as instruções em"Monitorar conexões de federação de rede" para revisar as métricas de replicação entre grades.
4. Se você não conseguir resolver o alerta, entre em contato com o suporte técnico.

A replicação entre redes continuará normalmente após o problema ser resolvido.

Identificar e tentar novamente operações de replicação com falha

Depois de resolver o alerta **Falha permanente de replicação entre grades**, você deve determinar se algum objeto ou marcador de exclusão falhou ao ser replicado para a outra grade. Você pode então reingerir esses objetos ou usar a API de gerenciamento de grade para tentar a replicação novamente.

O alerta **Falha permanente na replicação entre grades** indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Esse alerta geralmente é causado por uma alteração no bucket de origem ou de destino. Para obter detalhes, consulte "Solucionar erros de federação de grade" .

Determinar se algum objeto não foi replicado

Para determinar se algum objeto ou marcador de exclusão não foi replicado para a outra grade, você pode pesquisar no log de auditoria por"CGRR (Solicitação de Replicação Entre Redes)" mensagens. Esta mensagem é adicionada ao log quando o StorageGRID falha ao replicar um objeto, objeto multiparte ou marcador de exclusão para o bucket de destino.

Você pode usar o"ferramenta audit-explain" para traduzir os resultados para um formato mais fácil de ler.

Antes de começar

- Você tem permissão de acesso Root.
- Você tem o `Passwords.txt` arquivo.
- Você sabe o endereço IP do nó de administração principal.

Passos

1. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .
2. Pesquise no audit.log por mensagens CGRR e use a ferramenta audit-explain para formatar os resultados.

   Por exemplo, este comando pesquisa todas as mensagens CGRR nos últimos 30 minutos e usa a ferramenta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Os resultados do comando serão semelhantes a este exemplo, que tem entradas para seis mensagens CGRR. No exemplo, todas as solicitações de replicação entre grades retornaram um erro geral porque o objeto não pôde ser replicado. Os três primeiros erros são para operações de "replicar objeto" e os três últimos erros são para operações de "replicar marcador de exclusão".

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Cada entrada contém as seguintes informações:

Campo	Descrição
Solicitação de replicação entre redes CGRR	O nome da solicitação
inquilino	ID da conta do inquilino
conexão	O ID da conexão da federação de grade
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de exclusão • replicar objeto multiparte
balde	O nome do balde
objeto	O nome do objeto
versão	O ID da versão do objeto

Campo	Descrição
erro	O tipo de erro. Se a replicação entre grades falhar, o erro será "Erro geral".

Tentar novamente as replicações com falha

Depois de gerar uma lista de objetos e marcadores de exclusão que não foram replicados para o bucket de destino e resolver os problemas subjacentes, você pode tentar a replicação novamente de duas maneiras:

- Ingira novamente cada objeto no bucket de origem.
- Use a API privada de gerenciamento de grade, conforme descrito.

Passos

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Selecione **Ir para documentação da API privada**.

> Os pontos de extremidade da API StorageGRID marcados como "Privados" estão sujeitos a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Na seção **cross-grid-replication-advanced**, selecione o seguinte ponto de extremidade:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Selecione **Experimentar**.
5. Na caixa de texto **corpo**, substitua a entrada de exemplo para **versionID** por uma ID de versão do audit.log que corresponda a uma solicitação de replicação entre grades com falha.

   Certifique-se de manter as aspas duplas ao redor da string.

6. Selecione **Executar**.
7. Confirme se o código de resposta do servidor é **204**, indicando que o objeto ou marcador de exclusão foi marcado como pendente para replicação entre grades para a outra grade.

> Pendente significa que a solicitação de replicação entre grades foi adicionada à fila interna para processamento.

Monitorar novas tentativas de replicação

Você deve monitorar as operações de repetição de replicação para garantir que elas sejam concluídas.

> Pode levar várias horas ou mais para que um objeto ou marcador de exclusão seja replicado para a outra grade.

Você pode monitorar operações de repetição de duas maneiras:

- Use um S3"CabeçaObjeto" ou"ObterObjeto" solicitar. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	**REPLICA**: O objeto foi replicado da grade de origem.

- Use a API privada de gerenciamento de grade, conforme descrito.

Passos

1. Na seção **cross-grid-replication-advanced** da documentação da API privada, selecione o seguinte ponto de extremidade:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Selecione **Experimentar**.
3. Na seção Parâmetro, insira o ID da versão que você usou no `cross-grid-replication-retry-failed` solicitar.
4. Selecione **Executar**.
5. Confirme se o código de resposta do servidor é **200**.
6. Revise o status da replicação, que será um dos seguintes:
   - **PENDENTE**: O objeto ainda não foi replicado.
   - **CONCLUÍDO**: A replicação foi bem-sucedida.
   - **FALHOU**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar segurança

Gerenciar segurança

Você pode configurar várias configurações de segurança no Grid Manager para ajudar a proteger seu sistema StorageGRID .

Gerenciar criptografia

O StorageGRID oferece diversas opções para criptografar dados. Você deve"revise os métodos de criptografia disponíveis" para determinar quais atendem aos seus requisitos de proteção de dados.

Gerenciar certificados

Você pode"configurar e gerenciar os certificados do servidor" usado para conexões HTTP ou certificados de cliente usados para autenticar uma identidade de cliente ou usuário no servidor.

Configurar servidores de gerenciamento de chaves

Usando um"servidor de gerenciamento de chaves" permite proteger os dados do StorageGRID mesmo se um

dispositivo for removido do data center. Depois que os volumes do dispositivo forem criptografados, você não poderá acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

> Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **Criptografia de nó** para cada dispositivo durante a instalação, antes que o dispositivo seja adicionado à grade.

Gerenciar configurações de proxy

Se você estiver usando serviços de plataforma S3 ou pools de armazenamento em nuvem, poderá configurar um"servidor proxy de armazenamento" entre os nós de armazenamento e os pontos de extremidade S3 externos. Se você enviar pacotes AutoSupport usando HTTPS ou HTTP, você pode configurar um"servidor proxy de administração" entre nós administrativos e suporte técnico.

Firewalls de controle

Para aumentar a segurança do seu sistema, você pode controlar o acesso aos nós de administração do StorageGRID abrindo ou fechando portas específicas no"firewall externo" . Você também pode controlar o acesso da rede a cada nó configurando seu"firewall interno" . Você pode impedir o acesso em todas as portas, exceto aquelas necessárias para sua implantação.

Revise os métodos de criptografia do StorageGRID

O StorageGRID oferece diversas opções para criptografar dados. Você deve revisar os métodos disponíveis para determinar quais atendem aos seus requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Servidor de gerenciamento de chaves (KMS) no Grid Manager	Você"configurar um servidor de gerenciamento de chaves" para o site StorageGRID e "habilitar criptografia de nó para o dispositivo" . Em seguida, um nó do dispositivo se conecta ao KMS para solicitar uma chave de criptografia de chave (KEK). Esta chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivos que têm **Criptografia de Nó** ativada durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. **Observação**: o gerenciamento de chaves de criptografia com um KMS só é suportado por nós de armazenamento e dispositivos de serviços.

Opção de criptografia	Como funciona	Aplica-se a
Página de Criptografia de Unidade no Instalador do Dispositivo StorageGRID	Se o dispositivo contiver unidades que suportam criptografia de hardware, você poderá definir uma senha para a unidade durante a instalação. Quando você define uma senha para uma unidade, é impossível para qualquer pessoa recuperar dados válidos de unidades que foram removidas do sistema, a menos que saiba a senha. Antes de iniciar a instalação, vá para **Configurar Hardware** > **Criptografia de Unidade** para definir uma senha de unidade que se aplique a todas as unidades autocriptografadas e gerenciadas StorageGRID em um nó.	Dispositivos que contêm unidades de autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas SANtricity. Se você tiver um dispositivo de armazenamento com unidades de autocriptografia e controladores SANtricity , poderá habilitar a segurança da unidade no SANtricity.
Impulsione a segurança no SANtricity System Manager	Se o recurso Drive Security estiver habilitado para seu dispositivo StorageGRID , você poderá usar "Gerente do Sistema SANtricity" para criar e gerenciar a chave de segurança. A chave é necessária para acessar os dados nas unidades protegidas.	Dispositivos de armazenamento que possuem unidades de criptografia completa de disco (FDE) ou unidades de autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com quaisquer dispositivos de serviço.
Criptografia de objetos armazenados	Você habilita o"Criptografia de objetos armazenados" opção no Grid Manager. Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objeto S3 recém-ingeridos. Objetos armazenados existentes não são criptografados. Metadados de objetos e outros dados confidenciais não são criptografados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de bucket S3	Você emite uma solicitação PutBucketEncryption para habilitar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o bucket. Objetos de bucket existentes não são criptografados. Metadados de objetos e outros dados confidenciais não são criptografados. "Operações em baldes"
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o `x-amz-server-side-encryption` cabeçalho da solicitação.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados de objetos e outros dados confidenciais não são criptografados. O StorageGRID gerencia as chaves. "Use criptografia do lado do servidor"
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e inclui três cabeçalhos de solicitação. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados de objetos e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use criptografia do lado do servidor"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de volume externo ou armazenamento de dados	Use um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação oferecer suporte a ele.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou armazenamento de dados seja criptografado. Um método de criptografia externa fornece controle mais rígido sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.
Criptografia de objetos fora do StorageGRID	Use um método de criptografia fora do StorageGRID para criptografar dados de objetos e metadados antes que eles sejam ingeridos no StorageGRID.	Somente dados de objeto e metadados (os dados de configuração do sistema não são criptografados). Um método de criptografia externa fornece controle mais rígido sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do usuário: Protegendo dados usando criptografia do lado do cliente"

Use vários métodos de criptografia

Dependendo de suas necessidades, você pode usar mais de um método de criptografia por vez. Por exemplo:

- Você pode usar um KMS para proteger nós de dispositivos e também usar o recurso de segurança de unidade no SANtricity System Manager para "criptografar duas vezes" dados nas unidades de autocriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados em nós de dispositivos e também usar a opção Criptografia de objetos armazenados para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte dos seus objetos exigir criptografia, considere controlar a criptografia no nível do bucket ou do objeto individual. Habilitar vários níveis de criptografia tem um custo de desempenho adicional.

Gerenciar certificados

Gerenciar certificados de segurança

Certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre componentes do StorageGRID e entre componentes do StorageGRID e sistemas externos.

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam a identidade de um cliente ou usuário no servidor, fornecendo autenticação mais segura do que apenas senhas. Os certificados do cliente não criptografam dados.

Quando um cliente se conecta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica este certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

O StorageGRID funciona como servidor para algumas conexões (como o ponto de extremidade do balanceador de carga) ou como cliente para outras conexões (como o serviço de replicação do CloudMirror).

Certificado Grid CA padrão

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado de CA de grade interno durante a instalação do sistema. O certificado Grid CA é usado, por padrão, para proteger o tráfego interno do StorageGRID . Uma autoridade de certificação (CA) externa pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora você possa usar o certificado Grid CA para um ambiente de não produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não seguras sem certificado também são suportadas, mas não são recomendadas.

- Os certificados CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser aqueles especificados para verificar as conexões do servidor.
- Todos os certificados personalizados devem atender aos"diretrizes de reforço do sistema para certificados de servidor" .
- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados de CA).

> ⓘ O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa no lugar do certificado de CA do sistema operacional.

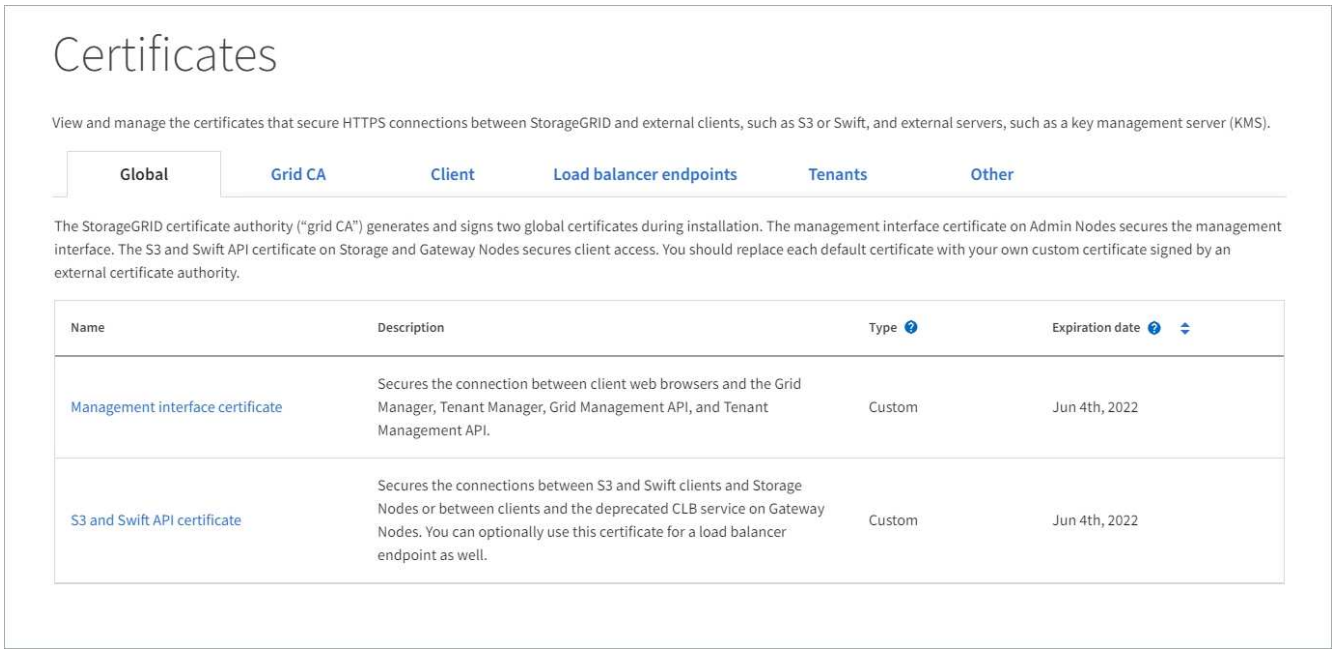
Variantes dos tipos de certificados de servidor e cliente são implementadas de diversas maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Certificados de segurança de acesso

Você pode acessar informações sobre todos os certificados StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.



2. Selecione uma guia na página Certificados para obter informações sobre cada categoria de certificado e acessar as configurações do certificado. Você pode acessar uma aba se tiver a"permissão apropriada" .

   - **Global**: Protege o acesso ao StorageGRID de navegadores da web e clientes de API externos.
   - **Grid CA**: protege o tráfego interno do StorageGRID .
   - **Cliente**: protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - **Pontos de extremidade do balanceador de carga**: protege conexões entre clientes S3 e o balanceador de carga StorageGRID .
   - **Inquilinos**: protege conexões com servidores de federação de identidade ou de pontos de extremidade de serviço de plataforma para recursos de armazenamento S3.
   - **Outro**: Protege conexões StorageGRID que exigem certificados específicos.

     Cada aba é descrita abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso ao StorageGRID de navegadores da web e clientes externos da API S3. Dois certificados globais são gerados inicialmente pela autoridade de certificação StorageGRID durante a instalação. A melhor prática para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- Certificado de interface de gerenciamento: Protege as conexões do navegador da Web do cliente com as interfaces de gerenciamento do StorageGRID .
- Certificado S3 API: Protege conexões de API do cliente com nós de armazenamento, nós de administração e nós de gateway, que os aplicativos cliente S3 usam para carregar e baixar dados de objetos.

As informações sobre os certificados globais instalados incluem:

- **Nome**: Nome do certificado com link para gerenciar o certificado.
- **Descrição**
- **Tipo**: Personalizado ou padrão. + Você deve sempre usar um certificado personalizado para melhorar a segurança da grade.
- **Data de validade**: Se estiver usando o certificado padrão, nenhuma data de validade será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - "Substituir o certificado de interface de gerenciamento gerado pelo StorageGRID padrão"usado para conexões do Grid Manager e do Tenant Manager.
  - "Substituir o certificado da API S3"usado para conexões de nó de armazenamento e ponto de extremidade do balanceador de carga (opcional).
- "Restaurar o certificado da interface de gerenciamento padrão" .
- "Restaurar o certificado padrão da API S3" .
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado" .
- Copie ou baixe o"certificado de interface de gerenciamento" ou"Certificado S3 API" .

Grade CA

OCertificado Grid CA , gerado pela autoridade de certificação do StorageGRID durante a instalação do StorageGRID , protege todo o tráfego interno do StorageGRID .

As informações do certificado incluem a data de validade do certificado e o conteúdo do certificado.

Você pode"copie ou baixe o certificado Grid CA" , mas você não pode alterá-lo.

Cliente

Certificados de cliente, gerado por uma autoridade de certificação externa, protege as conexões entre ferramentas de monitoramento externo e o banco de dados StorageGRID Prometheus.

A tabela de certificados tem uma linha para cada certificado de cliente configurado e indica se o certificado pode ser usado para acesso ao banco de dados do Prometheus, juntamente com a data de expiração do certificado.

Você pode:

- "Carregue ou gere um novo certificado de cliente."
- Selecione um nome de certificado para exibir os detalhes do certificado, onde você pode:
  - "Alterar o nome do certificado do cliente."
  - "Defina a permissão de acesso do Prometheus."
  - "Carregue e substitua o certificado do cliente."
  - "Copie ou baixe o certificado do cliente."
  - "Remova o certificado do cliente."
- Selecione **Ações** para rapidamente"editar" ,"anexar" , ou"remover" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los de uma só vez usando **Ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de ponto de extremidade do balanceador de cargaproteger as conexões entre clientes S3 e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração.

A tabela de ponto de extremidade do balanceador de carga tem uma linha para cada ponto de extremidade do balanceador de carga configurado e indica se o certificado global da API S3 ou um certificado de ponto de extremidade do balanceador de carga personalizado está sendo usado para o ponto de extremidade. A data de validade de cada certificado também é exibida.

> Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- "Exibir um ponto de extremidade do balanceador de carga", incluindo os detalhes do seu certificado.
- "Especifique um certificado de ponto de extremidade do balanceador de carga para FabricPool."
- "Use o certificado global da API S3"em vez de gerar um novo certificado de ponto de extremidade do balanceador de carga.

Inquilinos

Os inquilinos podem usarcertificados de servidor de federação de identidade oucertificados de ponto de extremidade de serviço de plataforma para proteger suas conexões com o StorageGRID.

A tabela de locatários tem uma linha para cada locatário e indica se cada locatário tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- "Selecione um nome de inquilino para fazer login no Gerenciador de Inquilinos"
- "Selecione um nome de locatário para visualizar os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma de locatários"
- "Especifique um certificado de ponto de extremidade de serviço de plataforma durante a criação

do ponto de extremidade"

Outro

O StorageGRID usa outros certificados de segurança para fins específicos. Esses certificados são listados por seu nome funcional. Outros certificados de segurança incluem:

- Certificados de pool de armazenamento em nuvem
- Certificados de notificação de alerta por e-mail
- Certificados de servidor syslog externo
- Certificados de conexão de federação de rede
- Certificados de federação de identidade
- Certificados do servidor de gerenciamento de chaves (KMS)
- Certificados de logon único

As informações indicam o tipo de certificado que uma função usa e as datas de expiração dos certificados de servidor e cliente, conforme aplicável. Selecionar um nome de função abre uma aba do navegador onde você pode visualizar e editar os detalhes do certificado.

> Você só pode visualizar e acessar informações de outros certificados se tiver a permissão"permissão apropriada" .

Você pode:

- "Especifique um certificado de pool de armazenamento em nuvem para S3, C2S S3 ou Azure"
- "Especificar um certificado para notificações de alerta por e-mail"
- "Use um certificado para um servidor syslog externo"
- "Girar certificados de conexão de federação de rede"
- "Visualizar e editar um certificado de federação de identidade"
- "Carregar certificados de servidor e cliente do servidor de gerenciamento de chaves (KMS)"
- "Especificar manualmente um certificado SSO para uma parte confiável"

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre os navegadores da Web do cliente e a interface de gerenciamento do StorageGRID , permitindo que os usuários acessem o Grid Manager e o Tenant Manager sem avisos de segurança. Este certificado também autentica conexões da API de gerenciamento de grade e da API de gerenciamento de locatários. Você pode usar o certificado padrão criado durante a instalação ou carregar um certificado personalizado.	**CONFIGURAÇÃO** > **Segurança** > **Certificados**, selecione a aba **Global** e então selecione **Certificado de interface de gerenciamento**	"Configurar certificados de interface de gerenciamento"

Certificado S3 API

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras do cliente S3 com um nó de armazenamento e com pontos de extremidade do balanceador de carga (opcional).	**CONFIGURAÇÃO** > **Segurança** > **Certificados**, selecione a aba **Global** e então selecione **Certificado S3 API**	"Configurar certificados da API S3"

Certificado Grid CA

Veja oDescrição do certificado CA de grade padrão .

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de clientes externos. • Permite que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**	"Configurar certificados de cliente"

Certificado de ponto de extremidade do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode carregar ou gerar um certificado do balanceador de carga ao configurar um ponto de extremidade do balanceador de carga. Os aplicativos cliente usam o certificado do balanceador de carga ao se conectar ao StorageGRID para salvar e recuperar dados de objetos. Você também pode usar uma versão personalizada do globalCertificado S3 API certificado para autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga. **Observação:** O certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID .	**CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade do balanceador de carga para o FabricPool"

Certificado de ponto de extremidade do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de armazenamento em nuvem do StorageGRID com um local de armazenamento externo, como o S3 Glacier ou o armazenamento de Blobs do Microsoft Azure. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **Pools de armazenamento**	"Criar um pool de armazenamento em nuvem"

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem o Transport Layer Security (TLS), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**ALERTAS** > **Configuração de e-mail**	"Configurar notificações por e-mail para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que registra eventos no StorageGRID. **Observação:** Um certificado de servidor syslog externo não é necessário para conexões TCP, RELP/TCP e UDP com um servidor syslog externo.	**CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**	"Use um servidor syslog externo"

Certificado de conexão de federação de rede

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentique e criptografe as informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grade.	**CONFIGURAÇÃO** > **Sistema** > **Federação de grade**	• "Criar conexões de federação de grade" • "Girar certificados de conexão"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como Active Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, o que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	**CONFIGURAÇÃO** > **Controle de Acesso** > **Federação de Identidade**	"Usar federação de identidade"

Certificado do servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID .	**CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de ponto de extremidade de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID com um recurso de armazenamento S3.	**Gerenciador de inquilinos** > **ARMAZENAMENTO (S3)** > **Pontos de extremidade de serviços de plataforma**	"Criar ponto de extremidade de serviços de plataforma" "Editar ponto de extremidade dos serviços da plataforma"

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como os Serviços de Federação do Active Directory (AD FS) e o StorageGRID , que são usados para solicitações de logon único (SSO).	**CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**	"Configurar logon único"

Exemplos de certificados

Exemplo 1: serviço de balanceador de carga

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.

2. Você configura uma conexão de cliente S3 com o ponto de extremidade do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se conecta ao ponto de extremidade do balanceador de carga usando HTTPS.
4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública, e com uma assinatura baseada na chave privada.
5. O cliente verifica este certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados do objeto para StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externo (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software externo Key Management Server, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Grid Manager, você configura um servidor KMS e carrega os certificados do servidor e do cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura baseada na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

Tipos de certificados de servidor suportados

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica).

> O tipo de cifra da política de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, cifras RSA exigem certificados RSA, e cifras ECDSA exigem certificados ECDSA. Ver "Gerenciar certificados de segurança" . Se você configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, você poderá"reverter temporariamente para a política de segurança padrão" .

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, consulte"Segurança para clientes S3" .

Configurar certificados de interface de gerenciamento

Você pode substituir o certificado de interface de gerenciamento padrão por um único certificado personalizado que permite que os usuários acessem o Grid Manager e o Tenant Manager sem encontrar avisos de segurança. Você também pode reverter para o certificado de interface de gerenciamento padrão ou gerar um novo.

Sobre esta tarefa

Por padrão, cada nó de administração recebe um certificado assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento

personalizado comum e pela chave privada correspondente.

Como um único certificado de interface de gerenciamento personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado curinga ou multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao Grid Manager e ao Tenant Manager. Defina o certificado personalizado de forma que ele corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que estiver usando, os usuários também podem precisar instalar o certificado Grid CA no navegador da Web que usarão para acessar o Grid Manager e o Tenant Manager.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado do servidor para a Interface de Gerenciamento** é acionado quando este certificado do servidor está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado da interface de gerenciamento na guia Global.

> Se você estiver acessando o Grid Manager ou o Tenant Manager usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se ocorrer qualquer uma das seguintes situações:
>
> - Seu certificado de interface de gerenciamento personalizado expira.
> - Você reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão .

Adicionar um certificado de interface de gerenciamento personalizado

Para adicionar um certificado de interface de gerenciamento personalizado, você pode fornecer seu próprio certificado ou gerar um usando o Grid Manager.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
3. Selecione **Usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

- **Certificado do servidor**: O arquivo de certificado do servidor personalizado (codificado em PEM).
- **Chave privada do certificado**: O arquivo de chave privada do certificado do servidor personalizado(`.key`).

> As chaves privadas da EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora intermediária emissora (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

d. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

Gerar certificado

Gere os arquivos de certificado do servidor.

> A melhor prática para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a serem incluídos no certificado.
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Observação**: deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

5. Atualize a página para garantir que o navegador da web esteja atualizado.

> Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página Certificado da interface de gerenciamento exibe informações detalhadas do certificado que está em uso. + Você pode baixar ou copiar o certificado PEM conforme necessário.

Restaurar o certificado da interface de gerenciamento padrão

Você pode voltar a usar o certificado de interface de gerenciamento padrão para conexões do Grid Manager e do Tenant Manager.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
3. Selecione **Usar certificado padrão**.

   Quando você restaura o certificado da interface de gerenciamento padrão, os arquivos de certificado do servidor personalizado que você configurou são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de clientes subsequentes.

4. Atualize a página para garantir que o navegador da web esteja atualizado.

Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação rigorosa do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade de certificação externa.

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó de administração.
2. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

      Quando você está logado como root, o prompt muda de `$` para `#` .

3. Configure o StorageGRID com um novo certificado autoassinado.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Para `--domains` , use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com` .
   - Definir `--type` para `management` para configurar o certificado da interface de gerenciamento, que é usado pelo Grid Manager e pelo Tenant Manager.
   - Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.

O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente de gerenciamento esteja sincronizado com a mesma fonte de tempo que o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

A saída resultante contém o certificado público necessário para seu cliente de API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags BEGIN e END na sua seleção.

5. Saia do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Grid Manager.
   b. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**
   c. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags BEGIN e END.

Baixe ou copie o certificado da interface de gerenciamento

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
3. Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

Baixe o certificado ou pacote de CA `.pem` arquivo. Se você estiver usando um pacote de CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote de CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem` .

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote de CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem` .

   Por exemplo: `storagegrid_certificate.pem`

Configurar certificados da API S3

Você pode substituir ou restaurar o certificado do servidor usado para conexões do cliente S3 com nós de armazenamento ou com pontos de extremidade do balanceador de carga. O certificado de servidor personalizado de substituição é específico para sua organização.

Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "StorageGRID 11.8: Configurar certificados S3 e Swift API" .

Sobre esta tarefa

Por padrão, cada nó de armazenamento recebe um certificado de servidor X.509 assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e pela chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao ponto de extremidade de armazenamento. Defina o certificado personalizado de forma que ele corresponda a todos os nós de armazenamento na grade.

Após concluir a configuração no servidor, talvez você também precise instalar o certificado Grid CA no cliente

S3 API que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que estiver usando.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado de servidor global para API S3** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado da API S3 na guia Global.

Você pode carregar ou gerar um certificado de API S3 personalizado.

Adicionar um certificado de API S3 personalizado

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

- **Certificado do servidor**: O arquivo de certificado do servidor personalizado (codificado em PEM).
- **Chave privada do certificado**: O arquivo de chave privada do certificado do servidor personalizado(`.key`).

> As chaves privadas da EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora emissora intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado de API S3 personalizado que foi carregado. Se você carregou um pacote de CA opcional, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

d. Selecione **Salvar**.

  O certificado de servidor personalizado é usado para novas conexões de cliente S3 subsequentes.

Gerar certificado

Gere os arquivos de certificado do servidor.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a serem incluídos no certificado.

Campo	Descrição
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Observação**: deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM do certificado S3 API personalizado que foi gerado.

   - Selecione **Baixar certificado** para salvar o arquivo de certificado.

     Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**.

   O certificado de servidor personalizado é usado para novas conexões de cliente S3 subsequentes.

5. Selecione uma guia para exibir metadados para o certificado do servidor StorageGRID padrão, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.

   > Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da web esteja atualizado.

7. Depois de adicionar um certificado de API S3 personalizado, a página de certificado de API S3 exibe informações detalhadas do certificado de API S3 personalizado que está em uso. + Você pode baixar ou copiar o certificado PEM conforme necessário.

Restaurar o certificado padrão da API S3

Você pode voltar a usar o certificado padrão da API S3 para conexões de cliente S3 com nós de armazenamento. No entanto, você não pode usar o certificado padrão da API S3 para um ponto de extremidade do balanceador de carga.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado padrão**.

   Quando você restaura a versão padrão do certificado global da API S3, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 será usado para novas conexões de cliente S3 subsequentes com os nós de armazenamento.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3.

   Se você tiver permissão de acesso Root e o certificado de API S3 personalizado tiver sido usado para conexões de ponto de extremidade do balanceador de carga, será exibida uma lista de pontos de extremidade do balanceador de carga que não estarão mais acessíveis usando o certificado de API S3 padrão. Vá para"Configurar pontos de extremidade do balanceador de carga" para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador da web esteja atualizado.

Baixe ou copie o certificado da API S3

Você pode salvar ou copiar o conteúdo do certificado da API S3 para uso em outro lugar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

Baixe o certificado ou pacote de CA `.pem` arquivo. Se você estiver usando um pacote de CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote de CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem` .

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote de CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem` .

   Por exemplo: `storagegrid_certificate.pem`

Informações relacionadas

- "Usar API REST do S3"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado Grid CA

O StorageGRID usa uma autoridade de certificação interna (CA) para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente deverão verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado CA do sistema StorageGRID .

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Grid CA**.

2. Na seção **Certificado PEM**, baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado `.pem` arquivo.

a. Selecione **Baixar certificado**.

b. Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem` .

Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia PEM

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem` .

Por exemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para clientes S3 que realizam validação estrita de nome de host e não oferecem suporte à desabilitação da validação estrita de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Ao criar um ponto de extremidade do balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Certificados assinados por uma CA podem ser rotacionados sem interrupções. Eles também são mais seguros porque oferecem melhor proteção contra ataques do tipo man-in-the-middle.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam o FabricPool. Para obter informações e procedimentos mais detalhados, consulte"Configurar StorageGRID para FabricPool" .

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso pelo FabricPool .
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

   Ao criar um ponto de extremidade do balanceador de carga HTTPS, você será solicitado a carregar seu certificado de servidor, a chave privada do certificado e o pacote de CA opcional.

3. Anexe o StorageGRID como uma camada de nuvem no ONTAP.

   Especifique a porta do ponto de extremidade do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado da CA.

> Se uma CA intermediária emitiu o certificado StorageGRID , você deverá fornecer o certificado da CA intermediária. Se o certificado StorageGRID foi emitido diretamente pela CA raiz, você deve fornecer o certificado da CA raiz.

Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus, fornecendo uma maneira segura para ferramentas externas monitorarem o StorageGRID.

Se precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deverá carregar ou gerar um certificado de cliente usando o Grid Manager e copiar as informações do certificado para a ferramenta externa.

Ver"Gerenciar certificados de segurança" e"Configurar certificados de servidor personalizados" .

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração de certificados de cliente configurados na página Certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO** > **Segurança** > **Certificados** e verificando a data de expiração do certificado do cliente na guia Cliente.

> Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivos especialmente configurados, consulte as informações específicas sobre"carregando um certificado de cliente KMS" .

Antes de começar

- Você tem permissão de acesso Root.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou nome de domínio do nó de administração.
  - Se você configurou o certificado da interface de gerenciamento do StorageGRID , terá a CA, o certificado do cliente e a chave privada usados para configurar o certificado da interface de gerenciamento.
  - Para carregar seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou registrada no momento em que foi criada. Se você não tiver a chave privada original, será necessário criar uma nova.
- Para editar um certificado de cliente:
  - Você tem o endereço IP ou nome de domínio do nó de administração.
  - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no seu computador local.

Adicionar certificados de cliente

Para adicionar o certificado do cliente, use um destes procedimentos:

- Certificado de interface de gerenciamento já configurado
- Certificado de cliente emitido pela CA
- Certificado gerado pelo Grid Manager

Certificado de interface de gerenciamento já configurado

Use este procedimento para adicionar um certificado de cliente se um certificado de interface de gerenciamento já estiver configurado usando uma CA fornecida pelo cliente, um certificado de cliente e uma chave privada.

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
   a. Selecione **Carregar certificado**.
   b. Selecione **Navegar** e selecione o arquivo de certificado da interface de gerenciamento(`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      O novo certificado aparece na aba Cliente.
7. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente de administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para o Prometheus que use um certificado de cliente emitido por uma CA e uma chave privada.

Passos

1. Execute os passos para"configurar um certificado de interface de gerenciamento" .
2. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
3. Selecione **Adicionar**.
4. Digite um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione

Permitir Prometheus.

6. Selecione **Continuar**.
7. Para a etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote da CA:
   a. Selecione **Carregar certificado**.
   b. Selecione **Navegar** e selecione o certificado do cliente, a chave privada e os arquivos do pacote CA(`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      Os novos certificados aparecem na aba Cliente.
8. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente de administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para o Prometheus que use a função de geração de certificado no Grid Manager.

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, selecione **Gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): Assunto X.509 ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
   - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida são adicionadas ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.
8. Selecione **Gerar**.
9. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
- Selecione **Baixar certificado** para salvar o arquivo de certificado.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la em outro lugar.
- Selecione **Baixar chave privada** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo da chave privada e o local do download.

10. Selecione **Criar** para salvar o certificado no Grid Manager.

    O novo certificado aparece na aba Cliente.

11. No Grid Manager, selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Global**.
12. Selecione **Certificado de interface de gerenciamento**.
13. Selecione **Usar certificado personalizado**.
14. Carregue os arquivos certificate.pem e private_key.pem dodetalhes do certificado do cliente etapa. Não há necessidade de fazer upload do pacote CA.
    a. Selecione **Carregar certificado** e depois selecione **Continuar**.
    b. Carregar cada arquivo de certificado(`.pem`).
    c. Selecione **Salvar** para salvar o certificado no Grid Manager.

       O novo certificado aparece na página de certificados da Interface de Gerenciamento.

15. Configurar uma ferramenta de monitoramento externa, como Grafana.

Configurar uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações na sua ferramenta de monitoramento externa, como o Grafana.
    a. **Nome**: Digite um nome para a conexão.

       O StorageGRID não exige essas informações, mas você deve fornecer um nome para testar a conexão.

    b. **URL**: Insira o nome de domínio ou endereço IP do nó de administração. Especifique HTTPS e porta 9091.

       Por exemplo: `https://admin-node.example.com:9091`

    c. Habilite **Autenticação de cliente TLS** e **Com certificado CA**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole:
   - Certificado CA da interface de gerenciamento para **CA Cert**
   - O certificado do cliente para **Client Cert**
   - A chave privada para **Chave do Cliente**
e. **ServerName**: Digite o nome de domínio do nó de administração.

   ServerName deve corresponder ao nome de domínio conforme aparece no certificado da interface de gerenciamento.

2. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

   Agora você pode acessar as métricas do Prometheus do StorageGRID com sua ferramenta de monitoramento externa.

   Para obter informações sobre as métricas, consulte o"instruções para monitorar o StorageGRID" .

Editar certificados de cliente

Você pode editar um certificado de cliente administrador para alterar seu nome, habilitar ou desabilitar o acesso ao Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.

   As datas de expiração dos certificados e as permissões de acesso do Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já tiver expirado, uma mensagem será exibida na tabela e um alerta será disparado.

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione **Editar nome e permissão**
4. Digite um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
6. Selecione **Continuar** para salvar o certificado no Grid Manager.

   O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.

   As datas de expiração dos certificados e as permissões de acesso do Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já tiver expirado, uma mensagem será exibida na tabela e um alerta será disparado.

2. Selecione o certificado que você deseja editar.

3. Selecione **Editar** e depois selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Carregar certificado** e depois selecione **Continuar**.

b. Carregar o nome do certificado do cliente(`.pem`).

   Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   - Selecione **Baixar certificado** para salvar o arquivo de certificado.

     Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem` .

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

c. Selecione **Criar** para salvar o certificado no Grid Manager.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

   - **Assunto** (opcional): Assunto X.509 ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
   - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida são adicionadas ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro

lugar.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la em outro lugar.
- Selecione **Baixar chave privada** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo da chave privada e o local do download.

e. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na aba Cliente.

Baixar ou copiar certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja copiar ou baixar.
3. Baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado `.pem` arquivo.

a. Selecione **Baixar certificado**.

b. Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

Remover certificados de cliente

Se você não precisar mais de um certificado de cliente administrador, poderá removê-lo.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Certificados** e então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja remover.
3. Selecione **Excluir** e depois confirme.

> Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **Ações** > **Excluir**.

Após a remoção de um certificado, os clientes que o utilizaram devem especificar um novo certificado de cliente para acessar o banco de dados StorageGRID Prometheus.

Configurar definições de segurança

Gerenciar a política TLS e SSH

A política TLS e SSH determina quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços internos do StorageGRID .

A política de segurança controla como TLS e SSH criptografam dados em movimento. Em geral, use a política de compatibilidade Moderna (padrão), a menos que seu sistema precise ser compatível com os Critérios Comuns ou você precise usar outras cifras.

> Alguns serviços do StorageGRID não foram atualizados para usar as cifras nessas políticas.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Selecione uma política de segurança

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.

   A aba **Políticas TLS e SSH** mostra as políticas disponíveis. A política atualmente ativa é indicada por uma marca de seleção verde no bloco de políticas.

2. Revise os blocos para saber mais sobre as políticas disponíveis.

Política	Descrição
Compatibilidade moderna (padrão)	Use a política padrão se precisar de criptografia forte e a menos que tenha requisitos especiais. Esta política é compatível com a maioria dos clientes TLS e SSH.
Compatibilidade com legados	Use esta política se precisar de opções adicionais de compatibilidade para clientes mais antigos. As opções adicionais nesta política podem torná-la menos segura do que a política de compatibilidade moderna.
Critérios comuns	Use esta política se precisar da certificação Common Criteria.
FIPS estrito	Use esta política se você precisar de certificação Common Criteria e usar o NetApp Cryptographic Security Module 3.0.8 para conexões de clientes externos com endpoints do balanceador de carga, Tenant Manager e Grid Manager. Usar esta política pode reduzir o desempenho. **Observação**: Depois de selecionar esta política, todos os nós devem ser"reiniciado de forma contínua" para ativar o Módulo de Segurança Criptográfica NetApp . Use **Manutenção** > **Reinicialização contínua** para iniciar e monitorar reinicializações.
Personalizado	Crie uma política personalizada se precisar aplicar suas próprias cifras.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Exibir detalhes**.
4. Para alterar a política atual, selecione **Usar política**.

   Uma marca de seleção verde aparece ao lado de **Política atual** no bloco de políticas.

Crie uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar suas próprias cifras.

Passos

1. No bloco da política mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e depois selecione **Cancelar**.

3. No bloco **Política personalizada**, selecione **Configurar e usar**.
4. Cole o JSON que você copiou e faça as alterações necessárias.
5. Selecione **Usar política**.

   Uma marca de seleção verde aparece ao lado de **Política atual** no bloco Política personalizada.

6. Opcionalmente, selecione **Editar configuração** para fazer mais alterações na nova política personalizada.

Reverter temporariamente para a política de segurança padrão

Se você configurou uma política de segurança personalizada, talvez não consiga fazer login no Grid Manager se a política TLS configurada for incompatível com a"certificado de servidor configurado" .

Você pode reverter temporariamente para a política de segurança padrão.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

      Quando você está logado como root, o prompt muda de `$` para `#` .

2. Execute o seguinte comando:

   ```
   restore-default-cipher-configurations
   ```

3. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.
4. Siga os passos emSelecione uma política de segurança para configurar a política novamente.

Configurar a segurança da rede e do objeto

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, impedir determinadas solicitações do S3 ou permitir que conexões de clientes com nós de armazenamento usem HTTP em vez de HTTPS.

Criptografia de objetos armazenados

A criptografia de objetos armazenados permite a criptografia de todos os dados de objetos à medida que são ingeridos pelo S3. Por padrão, os objetos armazenados não são criptografados, mas você pode optar por criptografar objetos usando o algoritmo de criptografia AES-128 ou AES-256. Quando você ativa a configuração, todos os objetos recém-ingeridos são criptografados, mas nenhuma alteração é feita nos objetos armazenados existentes. Se você desabilitar a criptografia, os objetos criptografados atualmente permanecerão criptografados, mas os objetos recém-ingeridos não serão criptografados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos do S3 que não foram criptografados pela criptografia em nível de bucket ou de objeto.

Para obter mais detalhes sobre os métodos de criptografia StorageGRID , consulte"Revise os métodos de criptografia do StorageGRID" .

Impedir modificação do cliente

Impedir modificação do cliente é uma configuração de todo o sistema. Quando a opção **Impedir modificação do cliente** é selecionada, as seguintes solicitações são negadas.

API REST S3

- Solicitações DeleteBucket
- Quaisquer solicitações para modificar dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

Habilitar HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos cliente usam o protocolo de rede HTTPS para qualquer conexão direta com os nós de armazenamento. Opcionalmente, você pode habilitar HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nós de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente com os nós de armazenamento. Você não precisa usar esta opção para clientes que usam apenas conexões HTTPS ou para clientes que se conectam ao serviço Load Balancer (porque você pode"configurar cada ponto de extremidade do balanceador de carga" para usar HTTP ou HTTPS).

Ver"Resumo: Endereços IP e portas para conexões de clientes" para saber quais portas os clientes S3 usam ao se conectar aos nós de armazenamento usando HTTP ou HTTPS.

Selecionar opções

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem permissão de acesso Root.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.
2. Selecione a aba **Rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **Nenhum** (padrão) se não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **Impedir modificação do cliente** se quiser impedir que clientes S3 façam solicitações específicas.

> Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

5. Opcionalmente, selecione **Habilitar HTTP para conexões de nós de armazenamento** se os clientes se conectarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

> Tenha cuidado ao habilitar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

6. Selecione **Salvar**.

Alterar as configurações de segurança da interface

As configurações de segurança da interface permitem que você controle se os usuários serão desconectados caso fiquem inativos por mais tempo do que o especificado e se um rastreamento de pilha será incluído nas respostas de erro da API.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"Permissão de acesso root" .

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações de **Tempo limite de inatividade do navegador** e **Rastreamento de pilha da API de gerenciamento**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode ficar inativo antes que ele seja desconectado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelo seguinte:

- Um temporizador StorageGRID separado e não configurável, incluído para segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o usuário efetuar login. Quando a autenticação de um usuário expira, esse usuário é desconectado automaticamente, mesmo que o tempo limite de inatividade do navegador esteja desativado ou o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve efetuar login novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja habilitado para StorageGRID.

  Se o SSO estiver habilitado e o navegador do usuário expirar, o usuário deverá inserir novamente suas credenciais de SSO para acessar o StorageGRID novamente. Ver "Configurar logon único" .

Rastreamento de pilha da API de gerenciamento

Controla se um rastreamento de pilha é retornado nas respostas de erro da API do Grid Manager e do Tenant Manager.

Esta opção está desabilitada por padrão, mas talvez você queira habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve deixar o rastreamento de pilha desabilitado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.
2. Selecione a aba **Interface**.
3. Para alterar a configuração de tempo limite de inatividade do navegador:
   a. Expanda o acordeão.
   b. Para alterar o período de tempo limite, especifique um valor entre 60 segundos e 7 dias. O tempo limite padrão é 15 minutos.
   c. Para desativar esse recurso, desmarque a caixa de seleção.
   d. Selecione **Salvar**.

      A nova configuração não afeta os usuários que estão conectados no momento. Os usuários devem fazer login novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.
4. Para alterar a configuração do rastreamento de pilha da API de gerenciamento:
   a. Expanda o acordeão.
   b. Marque a caixa de seleção para retornar um rastreamento de pilha nas respostas de erro da API do Grid Manager e do Tenant Manager.

      > Deixe o rastreamento de pilha desabilitado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

   c. Selecione **Salvar**.

Configurar servidores de gerenciamento de chaves

O que é um servidor de gerenciamento de chaves (KMS)?

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiros que fornece chaves de criptografia para nós do dispositivo StorageGRID no site StorageGRID associado usando o Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP).

O StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista de produtos e versões suportados, use o "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó do dispositivo StorageGRID que tenha a configuração **Criptografia de Nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivos permite que você proteja seus dados mesmo se um dispositivo for removido do data center. Depois que os volumes do dispositivo forem criptografados, você não poderá acessar nenhum dado no dispositivo, a menos que o nó

possa se comunicar com o KMS.

> O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar nós do dispositivo. Se você planeja usar um servidor externo de gerenciamento de chaves para proteger os dados do StorageGRID , você deve entender como configurar esse servidor e como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo destas instruções. Se precisar de ajuda, consulte a documentação do seu servidor de gerenciamento de chaves ou entre em contato com o suporte técnico.

Configuração do KMS e do dispositivo

Antes de poder usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID em nós do dispositivo, você deve concluir duas tarefas de configuração: configurar um ou mais servidores KMS e habilitar a criptografia de nós para os nós do dispositivo. Quando essas duas tarefas de configuração são concluídas, o processo de gerenciamento de chaves ocorre automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger dados do StorageGRID em nós do dispositivo.

O fluxograma mostra a configuração do KMS e a configuração do dispositivo ocorrendo em paralelo; no entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nós para novos nós do dispositivo, com base em seus requisitos.

Configurar o servidor de gerenciamento de chaves (KMS)

A configuração de um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

Etapa	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada KMS ou cluster KMS.	"Configurar o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configurar o StorageGRID como um cliente no KMS"
Adicione o KMS ao Grid Manager, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui as seguintes etapas de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o StorageGRID Appliance Installer para habilitar a configuração **Criptografia de nó** para o dispositivo.

Não é possível habilitar a configuração **Criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não tenham a criptografia de nó habilitada.

2. Execute o instalador do dispositivo StorageGRID . Durante a instalação, uma chave de criptografia de dados aleatória (DEK) é atribuída a cada volume do dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco Linux Unified Key Setup (LUKS) no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). A KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conectar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Ver "Habilitar criptografia de nó" para mais detalhes.

Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível que são executadas automaticamente.

1. Quando você instala um dispositivo com criptografia de nó habilitada na grade, o StorageGRID determina se existe uma configuração KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o dispositivo receberá a configuração do KMS.
   - Se um KMS ainda não tiver sido configurado para o site, os dados no dispositivo continuarão sendo criptografados pela KEK temporária até que você configure um KMS para o site e o dispositivo receba a configuração do KMS.
2. O dispositivo usa a configuração do KMS para se conectar ao KMS e solicitar uma chave de criptografia.
3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui a KEK temporária e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

Todos os dados existentes antes do nó do dispositivo criptografado se conectar ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra remoção do data center até que a chave temporária seja substituída pela chave de criptografia do KMS.

4. Se o dispositivo for ligado ou reiniciado, ele se reconectará ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não sobrevive a uma queda de energia ou a uma reinicialização.

Considerações e requisitos para usar um servidor de gerenciamento de chaves

Antes de configurar um servidor de gerenciamento de chaves externo (KMS), você deve entender as considerações e os requisitos.

Qual versão do KMIP é suportada?

O StorageGRID suporta o KMIP versão 1.4.

"Especificação do Protocolo de Interoperabilidade de Gerenciamento de Chaves Versão 1.4"

Quais são as considerações sobre a rede?

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique por meio da porta usada para comunicações do Key Management Interoperability Protocol (KMIP). A porta KMIP padrão é 5696.

Você deve garantir que cada nó do dispositivo que usa criptografia de nó tenha acesso de rede ao KMS ou cluster KMS que você configurou para o site.

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode oferecer suporte ao protocolo TLS 1.2 ou TLS 1.3 ao fazer conexões KMIP com um cluster KMS ou KMS, com base no que o KMS oferece suporte e em quais"Política de TLS e SSH" você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1.2) ou conjunto de cifras (TLS 1.3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e cifras/conjuntos de cifras estão disponíveis, revise o `tlsOutbound` seção da política TLS e SSH ativa da grade (**CONFIGURAÇÃO** > **Segurança Configurações de segurança**).

Quais aparelhos são suportados?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar chaves de criptografia para qualquer dispositivo StorageGRID em sua grade que tenha a configuração **Criptografia de nó** habilitada. Esta configuração só pode ser ativada durante o estágio de configuração de hardware da instalação do dispositivo usando o StorageGRID Appliance Installer.

> Não é possível habilitar a criptografia de nós depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não tenham a criptografia de nós habilitada.

Você pode usar o KMS configurado para dispositivos e nós de dispositivos StorageGRID .

Não é possível usar o KMS configurado para nós baseados em software (não dispositivos), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em mecanismos de contêiner em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no nível do armazenamento de dados ou do disco.

Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, normalmente você deve configurar um ou mais servidores de gerenciamento de chaves no Grid Manager antes de criar locatários. Essa ordem garante que os nós sejam protegidos antes que quaisquer dados de objeto sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Grid Manager antes ou depois de instalar os nós do dispositivo.

Quantos servidores de gerenciamento de chaves eu preciso?

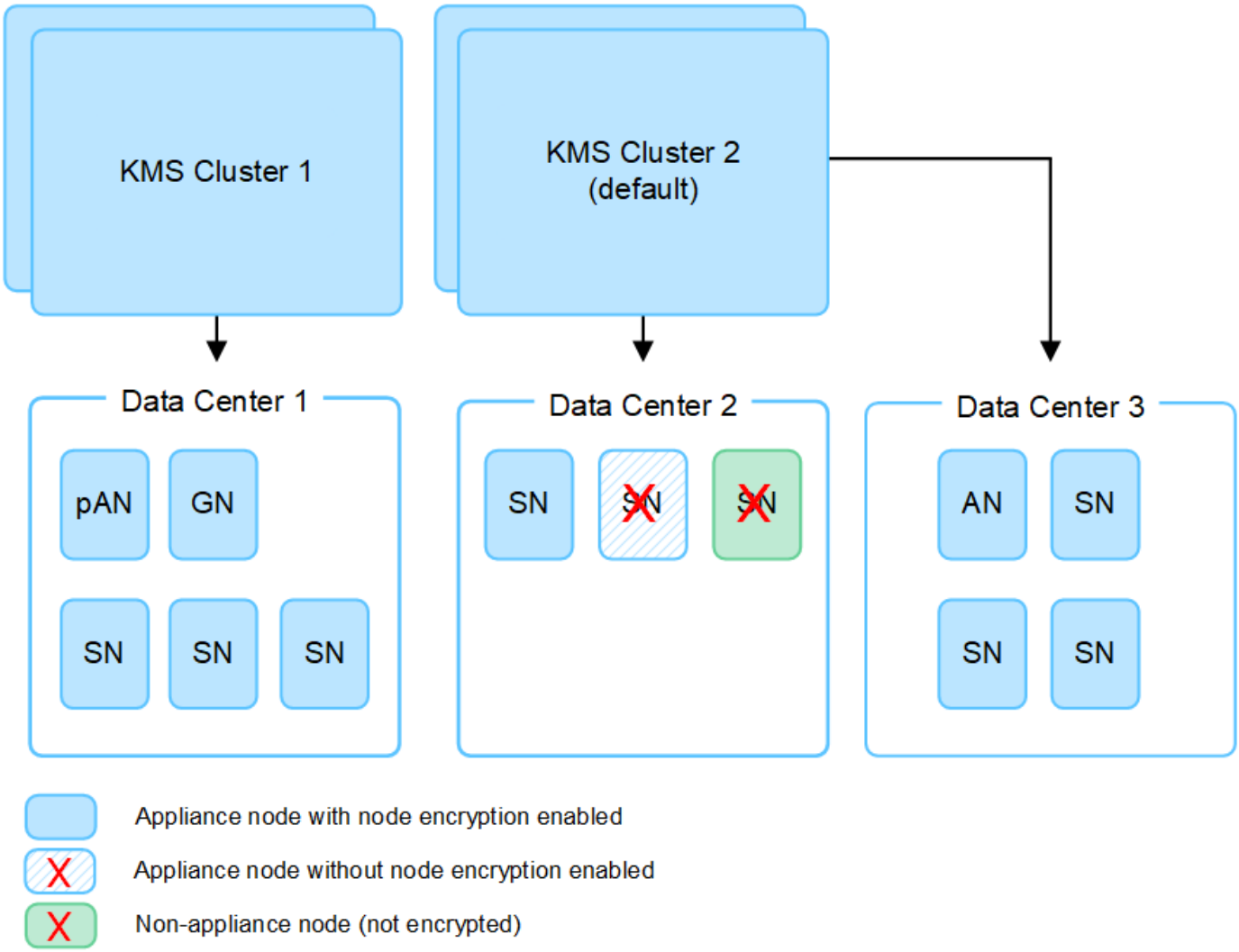
Você pode configurar um ou mais servidores externos de gerenciamento de chaves para fornecer chaves de criptografia aos nós do dispositivo no seu sistema StorageGRID . Cada KMS fornece uma única chave de

criptografia para os nós do dispositivo StorageGRID em um único site ou em um grupo de sites.

O StorageGRID suporta o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham definições de configuração e chaves de criptografia. O uso de clusters KMS para gerenciamento de chaves é recomendado porque melhora os recursos de failover de uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros sites. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que você não pode usar um KMS para nós que não sejam de dispositivo ou para nós de dispositivo que não tenham a configuração **Criptografia de nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como prática recomendada de segurança, você deve periodicamente"gire a chave de criptografia" usado por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós do dispositivo criptografado no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora após a rotação da chave.
- Se o nó do dispositivo criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reinicializado.
- Se a nova versão da chave não puder ser usada para criptografar volumes do dispositivo por qualquer motivo, o alerta **Falha na rotação da chave de criptografia KMS** será acionado para o nó do dispositivo. Talvez seja necessário entrar em contato com o suporte técnico para obter ajuda para resolver este alerta.

Posso reutilizar um nó de dispositivo depois que ele for criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID , primeiro desative o nó da grade para mover os dados do objeto para outro nó. Em seguida, você pode usar o StorageGRID Appliance Installer para "limpar a configuração do KMS" . Limpar a configuração do KMS desabilita a configuração **Criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração do KMS para o site StorageGRID .

> Sem acesso à chave de criptografia do KMS, todos os dados que permanecerem no dispositivo não poderão mais ser acessados e serão bloqueados permanentemente.

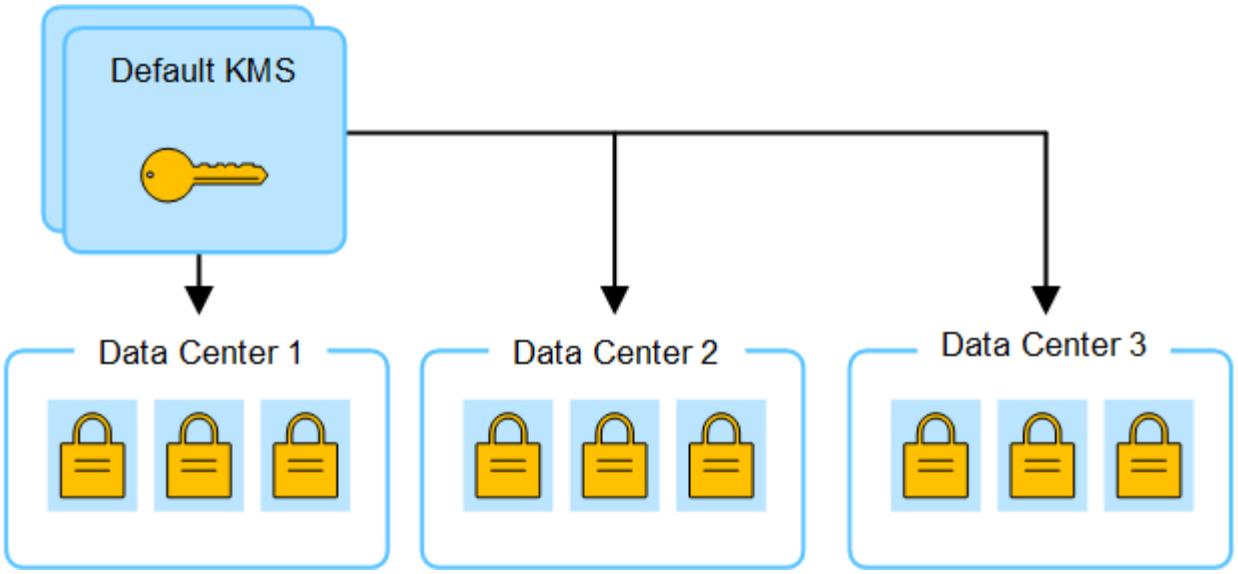
Considerações para alterar o KMS de um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único site ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

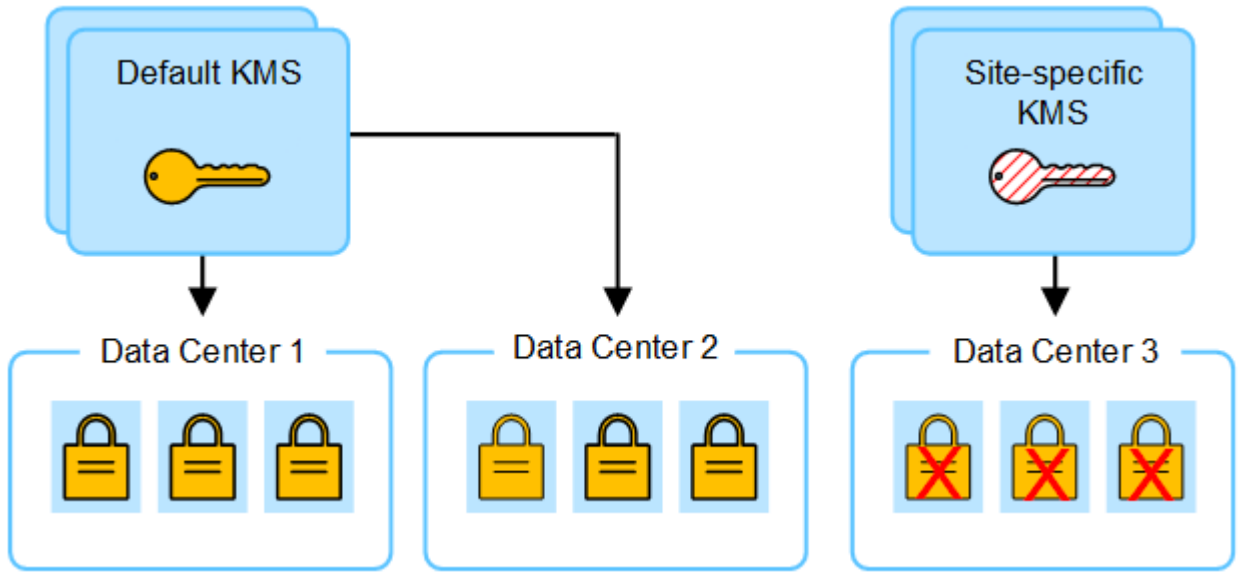
Se você alterar o KMS usado para um site, deverá garantir que os nós do dispositivo criptografados anteriormente naquele site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós do dispositivo criptografados no site.

Por exemplo:

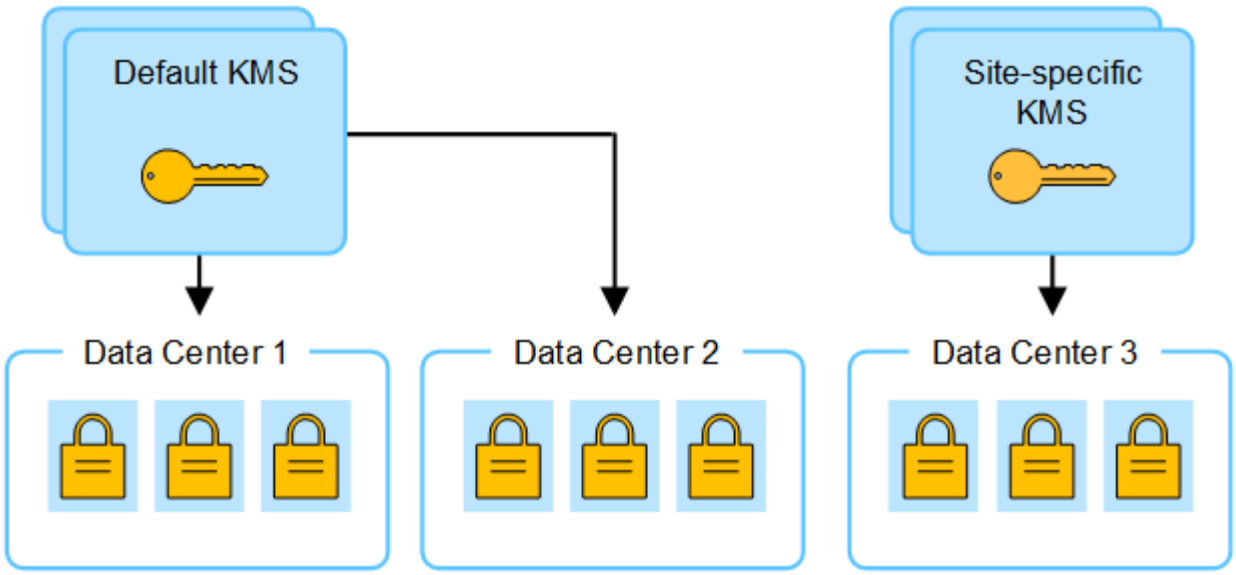
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós do dispositivo que têm a configuração **Criptografia de nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Esta chave é usada para criptografar os nós do dispositivo em todos os sites. Essa mesma chave também deve ser usada para descriptografar esses aparelhos.



3. Você decide adicionar um KMS específico para um site (Data Center 3 na figura). No entanto, como os nós do dispositivo já estão criptografados, ocorre um erro de validação quando você tenta salvar a configuração do KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós naquele site.



4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original se torna uma versão anterior da nova chave.) O KMS específico do site agora tem a chave correta para descriptografar os nós do dispositivo no Data Center 3, para que ela possa ser salva no StorageGRID.



Casos de uso para alterar qual KMS é usado para um site

A tabela resume as etapas necessárias para os casos mais comuns de alteração do KMS de um site.

Caso de uso para alterar o KMS de um site	Etapas necessárias
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como o KMS padrão.	Edite o KMS específico do site. No campo **Gerencia chaves para**, selecione **Sites não gerenciados por outro KMS (KMS padrão)**. O KMS específico do site agora será usado como o KMS padrão. Ele será aplicado a qualquer site que não tenha um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"
Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não quer usar o KMS padrão para o novo site.	1. Se os nós do dispositivo no novo site já tiverem sido criptografados pelo KMS padrão, use o software KMS para copiar a versão atual da chave de criptografia do KMS padrão para um novo KMS. 2. Usando o Grid Manager, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS de um site use um servidor diferente.	1. Se os nós do dispositivo no site já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS. 2. Usando o Grid Manager, edite a configuração do KMS existente e insira o novo nome do host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o StorageGRID como um cliente no KMS

Você deve configurar o StorageGRID como um cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de poder adicionar o KMS ao

StorageGRID.

> Estas instruções se aplicam ao Thales CipherTrust Manager e ao Hashicorp Vault. Para obter uma lista de produtos e versões suportados, use o "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

Passos

1. No software KMS, crie um cliente StorageGRID para cada KMS ou cluster KMS que você planeja usar.

   Cada KMS gerencia uma única chave de criptografia para os nós dos dispositivos StorageGRID em um único site ou em um grupo de sites.

2. Crie uma chave usando um dos dois métodos a seguir:
   - Use a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada KMS ou cluster KMS.

     A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

   - Faça com que o StorageGRID crie a chave. Você será avisado quando testar e salvar depois"carregando certificados de cliente" .
3. Registre as seguintes informações para cada KMS ou cluster KMS.

   Você precisa dessas informações ao adicionar o KMS ao StorageGRID:

   - Nome do host ou endereço IP para cada servidor.
   - Porta KMIP usada pelo KMS.
   - Alias de chave para a chave de criptografia no KMS.
4. Para cada KMS ou cluster KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contenha cada um dos arquivos de certificado de CA codificados em PEM, concatenados na ordem da cadeia de certificados.

   O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

   - O certificado deve usar o formato X.509 codificado em Base 64 do Privacy Enhanced Mail (PEM).
   - O campo Nome Alternativo do Assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou endereço IP ao qual o StorageGRID se conectará.

     > Ao configurar o KMS no StorageGRID, você deve inserir os mesmos FQDNs ou endereços IP no campo **Nome do host**.

   - O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.
5. Obtenha o certificado de cliente público emitido para o StorageGRID pelo KMS externo e a chave privada para o certificado de cliente.

   O certificado do cliente permite que o StorageGRID se autentique no KMS.

Adicionar um servidor de gerenciamento de chaves (KMS)

Use o assistente do StorageGRID Key Management Server para adicionar cada KMS ou

cluster KMS.

Antes de começar

- Você revisou o"considerações e requisitos para usar um servidor de gerenciamento de chaves" .
- Você tem"configurou o StorageGRID como um cliente no KMS" , e você terá as informações necessárias para cada KMS ou cluster KMS.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

Se possível, configure quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro deverá copiar a versão atual da chave de criptografia do KMS padrão para o novo KMS. Ver"Considerações para alterar o KMS de um site" para mais detalhes.

Etapa 1: detalhes do KMS

Na Etapa 1 (Detalhes do KMS) do assistente Adicionar um Servidor de Gerenciamento de Chaves, você fornece detalhes sobre o KMS ou cluster KMS.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **Criar**.

   A etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. **Observação**: se você não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.

Campo	Descrição
Gerencia chaves para	O site StorageGRID que será associado a este KMS. Se possível, você deve configurar quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um site específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que será aplicado a todos os sites que não tenham um KMS dedicado e a todos os sites que você adicionar em expansões subsequentes. **Observação:** Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas não tiver fornecido a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP para o KMS. **Observação:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **Continuar**.

Etapa 2: Carregar certificado do servidor

Na Etapa 2 (Carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado do servidor (ou pacote de certificados) para o KMS. O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

Passos

1. Na **Etapa 2 (Carregar certificado do servidor)**, navegue até o local do certificado do servidor ou pacote de certificados salvo.
2. Carregue o arquivo do certificado.

   Os metadados do certificado do servidor são exibidos.

Se você carregou um pacote de certificados, os metadados de cada certificado aparecem em sua própria guia.

3. Selecione **Continuar**.

Etapa 3: Carregar certificados de cliente

Na Etapa 3 (Carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado de cliente e a chave privada do certificado de cliente. O certificado do cliente permite que o StorageGRID se autentique no KMS.

Passos

1. Na **Etapa 3 (Carregar certificados do cliente)**, navegue até o local do certificado do cliente.
2. Carregue o arquivo de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até o local da chave privada do certificado do cliente.
4. Carregue o arquivo da chave privada.
5. Selecione **Testar e salvar**.

   Se uma chave não existir, você será solicitado a solicitar que o StorageGRID crie uma.

   As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página Servidor de gerenciamento de chaves.

   Imediatamente após adicionar um KMS, o status do certificado na página Servidor de Gerenciamento de Chaves aparece como Desconhecido. O StorageGRID pode levar até 30 minutos para obter o status real de cada certificado. Você deve atualizar seu navegador para ver o status atual.

6. Se uma mensagem de erro aparecer quando você selecionar **Testar e salvar**, revise os detalhes da mensagem e selecione **OK**.

   Por exemplo, você pode receber um erro 422: Entidade não processável se um teste de conexão falhar.

7. Se precisar salvar a configuração atual sem testar a conexão externa, selecione **Forçar salvamento**.

   Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo com esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós do dispositivo que tenham a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Revise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

   A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Gerenciar um KMS

Gerenciar um servidor de gerenciamento de chaves (KMS) envolve visualizar ou editar detalhes, gerenciar certificados, visualizar nós criptografados e remover um KMS quando ele não for mais necessário.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"permissão de acesso necessária" .

Ver detalhes do KMS

Você pode visualizar informações sobre cada servidor de gerenciamento de chaves (KMS) no seu sistema StorageGRID , incluindo detalhes da chave e o status atual dos certificados do servidor e do cliente.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

   - A guia Detalhes da configuração lista todos os servidores de gerenciamento de chaves que estão configurados.
   - A guia Nós criptografados lista todos os nós que têm a criptografia de nós habilitada.

2. Para visualizar os detalhes de um KMS específico e executar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gerencia chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou **Sites não gerenciados por outro KMS (KMS padrão).**
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS será listado junto com o número de servidores de gerenciamento de chaves adicionais no cluster. Por exemplo: `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others` . Para visualizar todos os nomes de host em um cluster, selecione um KMS e selecione **Editar** ou **Ações** > **Editar**.

3. Selecione uma guia na página de detalhes do KMS para visualizar as seguintes informações:

Aba	Campo	Descrição
Detalhes importantes	Nome da chave	O alias da chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Última modificação
Data e hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (privacy enhanced mail) do certificado.
Certificado de cliente	Metadados	Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.

4. Sempre que exigido pelas práticas de segurança da sua organização, selecione **Girar chave** ou use o software KMS para criar uma nova versão da chave.

   Quando a rotação da chave é bem-sucedida, os campos UID da chave e Última modificação são atualizados.

> Se você girar a chave de criptografia usando o software KMS, gire-a da última versão usada da chave para uma nova versão da mesma chave. Não gire para uma chave totalmente diferente.
>
> Nunca tente rotacionar uma chave alterando o nome da chave (alias) para o KMS. O StorageGRID exige que todas as versões de chaves usadas anteriormente (bem como quaisquer futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias da chave de um KMS configurado, o StorageGRID poderá não conseguir descriptografar seus dados.

Gerenciar certificados

Resolva imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes que eles expirem.

> Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

2. Na tabela, observe o valor de Expiração do certificado para cada KMS.
3. Se a expiração do certificado para qualquer KMS for Desconhecida, aguarde até 30 minutos e atualize seu navegador.
4. Se a coluna Expiração do certificado indicar que um certificado expirou ou está próximo da expiração, selecione o KMS para acessar a página de detalhes do KMS.
   a. Selecione **Certificado do servidor** e verifique o valor do campo "Expira em".
   b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
   c. Repita essas subetapas e selecione **Certificado do cliente** em vez de Certificado do servidor.
5. Quando os alertas **Expiração do certificado da CA KMS**, **Expiração do certificado do cliente KMS** e **Expiração do certificado do servidor KMS** forem acionados, observe a descrição de cada alerta e execute as ações recomendadas.

   Pode levar até 30 minutos para o StorageGRID receber atualizações sobre a expiração do certificado. Atualize seu navegador para ver os valores atuais.

> Se você receber o status **Status do certificado do servidor desconhecido**, certifique-se de que seu KMS permite obter um certificado de servidor sem exigir um certificado de cliente.

Exibir nós criptografados

Você pode visualizar informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **Criptografia de nó** ativada.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de Gerenciamento de Chaves é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. No topo da página, selecione a aba **Nós criptografados**.

   A guia Nós criptografados lista os nós do dispositivo no seu sistema StorageGRID que têm a configuração **Criptografia de nó** ativada.

3. Revise as informações na tabela para cada nó do dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Armazenamento, Administração ou Gateway.
Site	O nome do site StorageGRID onde o nó está instalado.

Coluna	Descrição
Nome da KMS	O nome descritivo do KMS usado para o nó. Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS. "Adicionar um servidor de gerenciamento de chaves (KMS)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para visualizar um UID de chave inteiro, selecione o texto. Um traço (--) indica que o UID da chave é desconhecido, possivelmente devido a um problema de conexão entre o nó do dispositivo e o KMS.
Status	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conectado, o registro de data e hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações na configuração do KMS. **Observação:** Atualize seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema do KMS, resolva o problema imediatamente.

   Durante as operações normais do KMS, o status será **Conectado ao KMS**. Se um nó for desconectado da rede, o estado da conexão do nó será exibido (Administrativamente inativo ou Desconhecido).

   Outras mensagens de status correspondem aos alertas do StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração do KMS
   - Erro de conectividade do KMS
   - Nome da chave de criptografia KMS não encontrado
   - Falha na rotação da chave de criptografia do KMS
   - A chave KMS falhou ao descriptografar um volume do dispositivo
   - O KMS não está configurado

   Execute as ações recomendadas para esses alertas.

> Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

Editar um KMS

Pode ser necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

Antes de começar

- Se você planeja atualizar o site selecionado para um KMS, você revisou o"considerações para alterar o KMS de um site" .

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja editar e selecione **Ações** > **Editar**.

   Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes na **Etapa 1 (Detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.
Gerencia chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione **Sites não gerenciados por outro KMS (KMS padrão)**. Esta seleção converte um KMS específico do site no KMS padrão, que será aplicado a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão. **Observação:** se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP para o KMS. **Observação:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar

um nome de host para cada servidor no cluster.

5. Selecione **Continuar**.

   A etapa 2 (Carregar certificado do servidor) do assistente Editar um servidor de gerenciamento de chaves é exibida.

6. Se precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.
7. Selecione **Continuar**.

   A etapa 3 (Carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se precisar substituir o certificado do cliente e a chave privada do certificado do cliente, selecione **Procurar** e carregue os novos arquivos.
9. Selecione **Testar e salvar**.

   As conexões entre o servidor de gerenciamento de chaves e todos os nós do dispositivo criptografados nos sites afetados são testadas. Se todas as conexões de nós forem válidas e a chave correta for encontrada no KMS, o servidor de gerenciamento de chaves será adicionado à tabela na página Servidor de gerenciamento de chaves.

10. Se uma mensagem de erro for exibida, revise os detalhes da mensagem e selecione **OK**.

    Por exemplo, você pode receber um erro 422: Entidade não processável se o site selecionado para este KMS já for gerenciado por outro KMS ou se um teste de conexão falhar.

11. Se precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Forçar salvamento**.

    > Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo com esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós do dispositivo que tenham a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

    A configuração do KMS é salva.

12. Revise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

    A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, pode ser necessário remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se tiver desativado o site.

Antes de começar

- Você revisou o"considerações e requisitos para usar um servidor de gerenciamento de chaves" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de dispositivo com criptografia de nó habilitada.
- Você pode remover o KMS padrão se já existir um KMS específico do site para cada site que tenha nós de dispositivo com criptografia de nó habilitada.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja remover e selecione **Ações** > **Remover**.

   Você também pode remover um KMS selecionando o nome do KMS na tabela e selecionando **Remover** na página de detalhes do KMS.

3. Confirme se o seguinte é verdadeiro:
   - Você está removendo um KMS específico de um site que não tem nenhum nó de dispositivo com criptografia de nó habilitada.
   - Você está removendo o KMS padrão, mas já existe um KMS específico do site para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS foi removida.

Gerenciar configurações de proxy

Configurar proxy de armazenamento

Se estiver usando serviços de plataforma ou pools de armazenamento em nuvem, você poderá configurar um proxy não transparente entre os nós de armazenamento e os endpoints externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.

> As configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de proxy**.
2. Na guia **Armazenamento**, marque a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
4. Digite o nome do host ou endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para conectar ao servidor proxy.

   Deixe este campo em branco para usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Salvar**.

   Depois que o proxy de armazenamento for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem poderão ser configurados e testados.

   > ⓘ As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço de plataforma do StorageGRID não sejam bloqueadas.
8. Se precisar desabilitar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configurar as definições de proxy do administrador

Se você enviar pacotes do AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre os nós de administração e o suporte técnico (AutoSupport).

Para obter mais informações sobre o AutoSupport, consulte"Configurar AutoSupport" .

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .

Sobre esta tarefa

Você pode configurar as configurações para um único proxy de administrador.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de proxy**.

   A página Configurações de proxy é exibida. Por padrão, Armazenamento é selecionado no menu de guias.

2. Selecione a aba **Admin**.
3. Marque a caixa de seleção **Ativar proxy de administrador**.
4. Digite o nome do host ou endereço IP do servidor proxy.
5. Digite a porta usada para conectar ao servidor proxy.
6. Opcionalmente, insira um nome de usuário e uma senha para o servidor proxy.

   Deixe esses campos em branco se o seu servidor proxy não exigir um nome de usuário ou uma senha.

7. Selecione uma das seguintes opções:

   - Se você quiser proteger a conexão com o proxy do administrador, selecione **Verificar certificado de proxy**. Carregue um pacote de CA para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy do administrador.

     O AutoSupport on Demand, o AutoSupport E-Series por meio do StorageGRID e a determinação do caminho de atualização na página de atualização do StorageGRID não funcionarão se um certificado proxy for verificado.

   Depois de carregar o pacote CA, seus metadados aparecem.

   - Se você não quiser validar certificados ao se comunicar com o servidor proxy do administrador, selecione **Não verificar certificado proxy**.

8. Selecione **Salvar**.

   Depois que o proxy do administrador é salvo, o servidor proxy entre os nós de administração e o suporte técnico é configurado.

   As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se precisar desabilitar o proxy de administrador, desmarque a caixa de seleção **Habilitar proxy de administrador** e selecione **Salvar**.

Firewalls de controle

Controle de acesso em firewall externo

Você pode abrir ou fechar portas específicas no firewall externo.

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode querer impedir que os locatários consigam se conectar ao Grid Manager pelo firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se você quiser configurar o firewall interno do StorageGRID , consulte"Configurar firewall interno" .

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes da API de gerenciamento podem acessar o Grid Manager, a Grid Management API, o Tenant Manager e a Tenant Management API. **Observação:** a porta 443 também é usada para algum tráfego interno.

Porta	Descrição	Se a porta estiver aberta…
8443	Porta do Grid Manager restrita em nós de administração	• Navegadores da Web e clientes da API de gerenciamento podem acessar o Grid Manager e a Grid Management API usando HTTPS. • Navegadores da Web e clientes da API de gerenciamento não podem acessar o Gerenciador de Tenants ou a API de Gerenciamento de Tenants. • Solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Tenant Manager em nós de administração	• Navegadores da Web e clientes da API de gerenciamento podem acessar o Gerenciador de Tenants e a API de Gerenciamento de Tenants usando HTTPS. • Navegadores da Web e clientes da API de gerenciamento não podem acessar o Grid Manager ou a Grid Management API. • Solicitações de conteúdo interno serão rejeitadas.

O logon único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

- "Sign in no Grid Manager"
- "Criar conta de inquilino"
- "Comunicações externas"

Gerenciar controles internos de firewall

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para sua implantação de grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Use as três guias na página de controle do Firewall para personalizar o acesso necessário para sua grade.

- **Lista de endereços privilegiados**: Use esta aba para permitir acesso selecionado a portas fechadas. Você pode adicionar endereços IP ou sub-redes na notação CIDR que podem acessar portas fechadas usando a guia Gerenciar acesso externo.
- **Gerenciar acesso externo**: use esta guia para fechar portas que estão abertas por padrão ou reabrir portas fechadas anteriormente.
- **Rede de cliente não confiável**: use esta guia para especificar se um nó confia no tráfego de entrada da rede de cliente.

  As configurações nesta guia substituem as configurações na guia Gerenciar acesso externo.

- Um nó com uma rede de cliente não confiável aceitará apenas conexões em portas de ponto de extremidade do balanceador de carga configuradas naquele nó (pontos de extremidade globais, de interface de nó e vinculados ao tipo de nó).
- As portas de ponto de extremidade do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
- Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer pontos de extremidade do balanceador de carga abertos na Rede do Cliente.

> As configurações feitas em uma guia podem afetar as alterações de acesso feitas em outra guia. Não deixe de verificar as configurações em todas as abas para garantir que sua rede se comporte da maneira esperada.

Para configurar os controles internos do firewall, consulte"Configurar controles de firewall" .

Para obter mais informações sobre firewalls externos e segurança de rede, consulte"Controle de acesso em firewall externo" .

Lista de endereços privilegiados e guias Gerenciar acesso externo

A guia Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso às portas de rede que estão fechadas. A guia Gerenciar acesso externo permite que você feche o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (portas externas são portas que são acessíveis por nós não pertencentes à grade por padrão). Essas duas guias geralmente podem ser usadas juntas para personalizar o acesso exato à rede que você precisa permitir para sua grade.

> Endereços IP privilegiados não têm acesso à porta de rede interna por padrão.

Exemplo 1: Use um host de salto para tarefas de manutenção

Suponha que você queira usar um host de salto (um host com segurança reforçada) para administração de rede. Você pode usar estas etapas gerais:

1. Use a guia Lista de endereços privilegiados para adicionar o endereço IP do host de salto.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

> Adicione o endereço IP privilegiado antes de bloquear as portas 443 e 8443. Qualquer usuário conectado em uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Depois de salvar sua configuração, todas as portas externas no nó de administração em sua grade serão bloqueadas para todos os hosts, exceto o host de salto. Você pode então usar o jump host para executar tarefas de manutenção na sua rede com mais segurança.

Exemplo 2: Bloquear portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta (por exemplo, SSH na porta 22). Você pode usar as seguintes etapas gerais:

1. Use a guia Lista de endereços privilegiados para conceder acesso somente aos hosts que precisam acessar o serviço.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

Adicione o endereço IP privilegiado antes de bloquear o acesso a quaisquer portas atribuídas para acessar o Grid Manager e o Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado em uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Depois de salvar sua configuração, a porta 22 e o serviço SSH estarão disponíveis para hosts na lista de endereços privilegiados. Todos os outros hosts terão o acesso ao serviço negado, independentemente da interface de onde a solicitação vier.

Exemplo 3: Desabilitar acesso a serviços não utilizados

No nível da rede, você pode desabilitar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego do cliente HTTP S3, você usaria a alternância na guia Gerenciar acesso externo para bloquear a porta 18084.

Guia Redes de clientes não confiáveis

Se estiver usando uma rede de cliente, você pode ajudar a proteger o StorageGRID de ataques hostis aceitando tráfego de cliente de entrada somente em endpoints configurados explicitamente.

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, o StorageGRID confia nas conexões de entrada para cada nó da grade em todos os"portas externas disponíveis" .

Você pode reduzir a ameaça de ataques hostis ao seu sistema StorageGRID especificando que a Rede do Cliente em cada nó seja *não confiável*. Se a rede do cliente de um nó não for confiável, o nó só aceitará conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga. Ver"Configurar pontos de extremidade do balanceador de carga" e"Configurar controles de firewall" .

Exemplo 1: O nó de gateway aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway recuse todo o tráfego de entrada na rede do cliente, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Do"Pontos de extremidade do balanceador de carga" página, configure um ponto de extremidade do balanceador de carga para S3 sobre HTTPS na porta 443.
2. Na página de controle do Firewall, selecione Não confiável para especificar que a Rede do Cliente no Nó do Gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede do cliente do nó do gateway será descartado, exceto solicitações HTTPS S3 na porta 443 e solicitações de eco ICMP (ping).

Exemplo 2: O nó de armazenamento envia solicitações de serviços da plataforma S3

Suponha que você queira habilitar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas deseja impedir qualquer conexão de entrada para esse nó de armazenamento na rede do cliente. Você executaria esta etapa geral:

- Na guia Redes de clientes não confiáveis da página de controle do firewall, indique que a Rede de clientes no nó de armazenamento não é confiável.

Depois de salvar sua configuração, o Nó de Armazenamento não aceita mais nenhum tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para destinos de serviços de plataforma configurados.

Exemplo 3: Limitando o acesso ao Grid Manager a uma sub-rede

Suponha que você queira permitir acesso do Grid Manager somente em uma sub-rede específica. Você executaria os seguintes passos:

1. Anexe a rede do cliente dos seus nós de administração à sub-rede.
2. Use a guia Rede de cliente não confiável para configurar a Rede de cliente como não confiável.
3. Ao criar um ponto de extremidade do balanceador de carga da interface de gerenciamento, insira a porta e selecione a interface de gerenciamento que a porta acessará.
4. Selecione **Sim** para Rede de cliente não confiável.
5. Use a guia Gerenciar acesso externo para bloquear todas as portas externas (com ou sem endereços IP privilegiados definidos para hosts fora dessa sub-rede).

Depois de salvar sua configuração, somente hosts na sub-rede especificada poderão acessar o Grid Manager. Todos os outros hosts estão bloqueados.

Configurar firewall interno

Você pode configurar o firewall StorageGRID para controlar o acesso da rede a portas específicas nos seus nós StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você revisou as informações em"Gerenciar controles de firewall" e"Diretrizes de rede" .
- Se você quiser que um nó de administração ou nó de gateway aceite tráfego de entrada somente em pontos de extremidade explicitamente configurados, você terá definido os pontos de extremidade do balanceador de carga.

> ⓘ Ao alterar a configuração da Rede do Cliente, as conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Sobre esta tarefa

O StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas portas nos nós da sua grade. Você pode usar as guias de controle do Firewall para abrir ou fechar portas que são abertas por padrão na Rede Grid, Rede de Administração e Rede Cliente. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas de grade que estão fechadas. Se estiver usando uma Rede Cliente, você poderá especificar se um nó confia no tráfego de entrada da Rede Cliente e poderá configurar o acesso de portas específicas na Rede Cliente.

Limitar o número de portas abertas para endereços IP fora da sua rede apenas para aquelas que são absolutamente necessárias aumenta a segurança da sua rede. Use as configurações em cada uma das três guias de controle do Firewall para garantir que somente as portas necessárias estejam abertas.

Para obter mais informações sobre o uso de controles de firewall, incluindo exemplos, consulte"Gerenciar controles de firewall" .

Para obter mais informações sobre firewalls externos e segurança de rede, consulte"Controle de acesso em firewall externo" .

Controles de firewall de acesso

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Controle de firewall**.

   As três guias nesta página são descritas em"Gerenciar controles de firewall" .

2. Selecione qualquer aba para configurar os controles do firewall.

   Você pode usar essas guias em qualquer ordem. As configurações definidas em uma guia não limitam o que você pode fazer nas outras guias; no entanto, as alterações de configuração feitas em uma guia podem alterar o comportamento das portas configuradas em outras guias.

Lista de endereços privilegiados

Use a guia Lista de endereços privilegiados para conceder aos hosts acesso a portas que estão fechadas por padrão ou fechadas por configurações na guia Gerenciar acesso externo.

Endereços IP e sub-redes privilegiados não têm acesso à rede interna por padrão. Além disso, os pontos de extremidade do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados podem ser acessados mesmo se bloqueados na guia Gerenciar acesso externo.

> As configurações na guia Lista de endereços privilegiados não podem substituir as configurações na guia Rede de clientes não confiáveis.

Passos

1. Na guia Lista de endereços privilegiados, insira o endereço ou a sub-rede IP à qual você deseja conceder acesso às portas fechadas.
2. Opcionalmente, selecione **Adicionar outro endereço IP ou sub-rede na notação CIDR** para adicionar clientes privilegiados adicionais.

   > Adicione o mínimo possível de endereços à lista privilegiada.

3. Opcionalmente, selecione *Permitir que endereços IP privilegiados acessem as portas internas do StorageGRID *. Ver "Portas internas do StorageGRID" .

   > Esta opção remove algumas proteções para serviços internos. Deixe-o desabilitado, se possível.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, a porta não pode ser acessada por nenhum endereço IP que não seja da rede, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas que estejam abertas por padrão e só pode abrir portas que você tenha fechado.

As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia Rede de cliente não confiável. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede do Cliente, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de cliente não confiável substituem portas fechadas (como 443, 8443, 9443) na Rede de cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós não pertencentes à grade por padrão) para os nós na sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
   - Use o botão de alternância ao lado de cada porta para abrir ou fechar a porta selecionada.
   - Selecione **Abrir todas as portas exibidas** para abrir todas as portas listadas na tabela.
   - Selecione **Fechar todas as portas exibidas** para fechar todas as portas listadas na tabela.

   Se você fechar as portas 443 ou 8443 do Grid Manager, todos os usuários conectados em uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seus endereços IP tenham sido adicionados à lista de endereços privilegiados.

   Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa inserindo um número de porta. Você pode inserir um número de porta parcial. Por exemplo, se você digitar **2**, todas as portas que têm a sequência "2" como parte do nome serão exibidas.

3. Selecione **Salvar**

Rede de clientes não confiáveis

Se a rede do cliente de um nó não for confiável, o nó aceitará somente tráfego de entrada em portas configuradas como pontos de extremidade do balanceador de carga e, opcionalmente, portas adicionais selecionadas nesta guia. Você também pode usar esta guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

As conexões de clientes existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

As alterações de configuração feitas na guia **Rede de cliente não confiável** substituem as configurações na guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de cliente não confiável**.
2. Na seção Definir novo nó padrão, especifique qual deve ser a configuração padrão quando novos nós são adicionados à grade em um procedimento de expansão.
   - **Confiável** (padrão): quando um nó é adicionado em uma expansão, sua Rede de Cliente é confiável.
   - **Não confiável**: quando um nó é adicionado em uma expansão, sua Rede de Cliente não é confiável.

     Conforme necessário, você pode retornar a esta guia para alterar a configuração de um novo nó específico.

Esta configuração não afeta os nós existentes no seu sistema StorageGRID .

3. Use as seguintes opções para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:

   - Selecione **Desconfiar dos nós exibidos** para adicionar todos os nós exibidos na tabela à lista Rede de clientes não confiáveis.
   - Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista Rede de clientes não confiáveis.
   - Use a alternância ao lado de cada nó para definir a Rede do Cliente como Confiável ou Não Confiável para o nó selecionado.

   Por exemplo, você pode selecionar **Desconfiar nos nós exibidos** para adicionar todos os nós à lista Rede de clientes não confiáveis e, em seguida, usar a alternância ao lado de um nó individual para adicionar esse único nó à lista Rede de clientes confiáveis.

   Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó inserindo o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a string "GW" como parte do nome serão exibidos.

4. Selecione **Salvar**.

   As novas configurações de firewall são aplicadas e executadas imediatamente. As conexões de clientes existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Gerenciar inquilinos

O que são contas de inquilino?

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) para armazenar e recuperar objetos em um sistema StorageGRID .

Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "StorageGRID 11.8: Gerenciar locatários" .

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 usam para armazenar e recuperar objetos.

Cada conta de locatário tem grupos federados ou locais, usuários, buckets S3 e objetos.

Contas de locatário podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de locatário podem ser usadas para qualquer um destes casos de uso:

- **Caso de uso corporativo:** Se você estiver administrando um sistema StorageGRID em um aplicativo corporativo, talvez queira segregar o armazenamento de objetos da grade pelos diferentes departamentos da sua organização. Nesse caso, você pode criar contas de locatário para o departamento de Marketing, o departamento de Suporte ao Cliente, o departamento de Recursos Humanos e assim por diante.

Se você usar o protocolo de cliente S3, poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de inquilino. Veja as instruções para implementação"Buckets S3 e políticas de bucket" para mais informações.

- **Caso de uso do provedor de serviços:** Se você estiver administrando um sistema StorageGRID como um provedor de serviços, poderá segregar o armazenamento de objetos da grade pelas diferentes entidades que alugarão o armazenamento na sua grade. Nesse caso, você criaria contas de inquilino para a Empresa A, Empresa B, Empresa C e assim por diante.

Para obter mais informações, consulte "Use uma conta de inquilino" .

Como crio uma conta de inquilino?

Use o Grid Manager para criar uma conta de locatário. Ao criar uma conta de locatário, você especifica as seguintes informações:

- Informações básicas, incluindo nome do locatário, tipo de cliente (S3) e cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar os serviços da plataforma S3, configurar sua própria fonte de identidade, usar o S3 Select ou usar uma conexão de federação de grade.
- O acesso root inicial para o locatário, com base no uso de grupos e usuários locais pelo sistema StorageGRID , federação de identidade ou logon único (SSO).

Além disso, você pode habilitar a configuração de Bloqueio de Objeto S3 para o sistema StorageGRID se as contas de locatário S3 precisarem estar em conformidade com os requisitos regulatórios. Quando o Bloqueio de Objeto S3 está habilitado, todas as contas de locatário S3 podem criar e gerenciar buckets compatíveis.

Para que serve o Tenant Manager?

Depois de criar a conta do locatário, os usuários locatários podem fazer login no Gerenciador de Locatários para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a fonte de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clonagem de conta e replicação entre grades
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select
- Monitorar o uso do armazenamento

Embora os usuários do tenant do S3 possam criar e gerenciar chaves de acesso e buckets do S3 com o Tenant Manager, eles devem usar um aplicativo cliente do S3 para ingerir e gerenciar objetos. Ver"Usar API REST do S3" para mais detalhes.

Criar uma conta de inquilino

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao

armazenamento no seu sistema StorageGRID .

As etapas para criar uma conta de locatário variam dependendo se"federação de identidade" e"login único" estão configurados e se a conta do Grid Manager que você usa para criar a conta do locatário pertence a um grupo de administradores com permissão de acesso Root.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou contas de locatário" .
- Se a conta do locatário usar a fonte de identidade configurada para o Grid Manager e você quiser conceder permissão de acesso Root para a conta do locatário a um grupo federado, você terá importado esse grupo federado para o Grid Manager. Você não precisa atribuir nenhuma permissão do Grid Manager a este grupo de administradores. Ver "Gerenciar grupos de administradores" .
- Se você quiser permitir que um locatário do S3 clone dados da conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade:
  - Você tem"configurou a conexão da federação de grade" .
  - O status da conexão é **Conectado**.
  - Você tem permissão de acesso Root.
  - Você revisou as considerações para"gerenciamento de inquilinos permitidos para federação de rede" .
  - Se a conta do locatário usar a fonte de identidade configurada para o Grid Manager, você importou o mesmo grupo federado para o Grid Manager em ambas as grades.

    Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso Root inicial para as contas do locatário de origem e de destino.

> Se esse grupo de administradores não existir em ambas as grades antes de você criar o locatário, o locatário não será replicado para o destino.

Acesse o assistente

Passos

1. Selecione **LOCATÁRIOS**.
2. Selecione **Criar**.

Insira os detalhes

Passos

1. Insira os detalhes do inquilino.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos inquilinos não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta exclusivo de 20 dígitos.

Campo	Descrição
Descrição (opcional)	Uma descrição para ajudar a identificar o inquilino. Se você estiver criando um locatário que usará uma conexão de federação de grade, opcionalmente, use este campo para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado na Grade 2: "Este locatário foi criado na Grade 1".
Tipo de cliente	O tipo de protocolo de cliente que este locatário usará, **S3** ou **Swift**. **Observação**: O suporte para aplicativos cliente Swift foi descontinuado e será removido em uma versão futura.
Cota de armazenamento (opcional)	Se você quiser que este locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **Continuar**.

Selecionar permissões

Passos

1. Opcionalmente, selecione as permissões básicas que você deseja que este locatário tenha.

> Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, selecione o ícone de ajuda para cada permissão.

Permissão	Se selecionado…
Permitir serviços de plataforma	O locatário pode usar serviços da plataforma S3, como o CloudMirror. Ver "Gerenciar serviços de plataforma para contas de locatários do S3" .
Use sua própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos e usuários federados. Esta opção estará desabilitada se você tiver"SSO configurado" para seu sistema StorageGRID .
Permitir seleção S3	O locatário pode emitir solicitações da API S3 SelectObjectContent para filtrar e recuperar dados do objeto. Ver "Gerenciar S3 Select para contas de locatários" . **Importante**: solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e somente para locatários confiáveis.

2. Opcionalmente, selecione as permissões avançadas que você deseja que este locatário tenha.

Permissão	Se selecionado…
Conexão de federação de rede	O inquilino pode usar uma conexão de federação de rede, que: • Faz com que este locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados desta grade (a *grade de origem*) para a outra grade na conexão selecionada (a *grade de destino*). • Permite que este locatário configure a replicação entre grades entre buckets correspondentes em cada grade. Ver "Gerenciar os inquilinos permitidos para federação de rede" .
Bloqueio de Objeto S3	Permitir que o locatário use recursos específicos do S3 Object Lock: • **Definir período máximo de retenção** define por quanto tempo novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. • **Permitir modo de conformidade** impede que os usuários substituam ou excluam versões de objetos protegidos durante o período de retenção.

3. Selecione **Continuar**.

Definir acesso root e criar locatário

Passos

1. Defina o acesso root para a conta do locatário, com base no uso de federação de identidades pelo seu sistema StorageGRID , logon único (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. Nenhum usuário local pode fazer login.

2. Selecione **Criar inquilino**.

   Uma mensagem de sucesso é exibida e o novo inquilino é listado na página Inquilinos. Para saber como visualizar detalhes do locatário e monitorar a atividade do locatário, consulte"Monitorar a atividade do inquilino" .

A aplicação das configurações do locatário na grade pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

3. Se você selecionou a permissão **Usar conexão de federação de grade** para o locatário:
   a. Confirme se um inquilino idêntico foi replicado para a outra grade na conexão. Os inquilinos em ambas as grades terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões.

      Se você vir a mensagem de erro "Locatário criado sem um clone", consulte as instruções em"Solucionar erros de federação de grade" .

   b. Se você forneceu uma senha de usuário root local ao definir o acesso root,"alterar a senha do usuário root local" para o inquilino replicado.

      Um usuário root local não pode fazer login no Tenant Manager na grade de destino até que a senha seja alterada.

Sign in como inquilino (opcional)

Conforme necessário, você pode entrar no novo locatário agora para concluir a configuração ou pode entrar no locatário mais tarde. As etapas de login dependem se você está conectado ao Grid Manager usando a porta padrão (443) ou uma porta restrita. Ver "Controle de acesso em firewall externo" .

Sign in agora

Se você estiver usando…	Faça isso…
Porta 443 e você define uma senha para o usuário root local	1. Selecione * Sign in como root*. Ao fazer login, aparecem links para configurar buckets, federação de identidades, grupos e usuários. 2. Selecione os links para configurar a conta do locatário. Cada link abre a página correspondente no Gerenciador de Inquilinos. Para completar a página, veja a"instruções para usar contas de inquilinos" .
Porta 443 e você não definiu uma senha para o usuário root local	Selecione * Sign in* e insira as credenciais de um usuário no grupo federado de acesso Root.

Se você estiver usando…	Faça isso…
Uma porta restrita	1. Selecione **Concluir** 2. Selecione **Restrito** na tabela Locatário para saber mais sobre como acessar esta conta de locatário. A URL do Gerenciador de Inquilinos tem este formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ `*port*`é a porta somente para inquilinos ◦ `*20-digit-account-id*`é o ID de conta exclusivo do inquilino

Sign in mais tarde

Se você estiver usando…	Faça uma dessas…
Porta 443	• No Grid Manager, selecione **LOCATÁRIOS** e selecione * Sign in* à direita do nome do locatário. • Digite a URL do locatário em um navegador da web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ `*20-digit-account-id*`é o ID de conta exclusivo do inquilino
Uma porta restrita	• No Grid Manager, selecione **LOCATÁRIOS** e selecione **Restrito**. • Digite a URL do locatário em um navegador da web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `*FQDN_or_Admin_Node_IP*`é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ `*port*`é a porta restrita somente para inquilinos ◦ `*20-digit-account-id*`é o ID de conta exclusivo do inquilino

Configurar o locatário

Siga as instruções em"Use uma conta de inquilino" para gerenciar grupos de locatários e usuários, chaves de acesso S3, buckets, serviços de plataforma, clone de conta e replicação entre redes.

Editar conta de inquilino

Você pode editar uma conta de locatário para alterar o nome de exibição, a cota de armazenamento ou as permissões do locatário.

> Se um locatário tiver a permissão **Usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. Entretanto, quaisquer alterações feitas em uma grade na conexão não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário exatamente sincronizados entre as grades, faça as mesmas edições em ambas as grades. Ver "Gerenciar os inquilinos permitidos para conexão de federação de rede" .

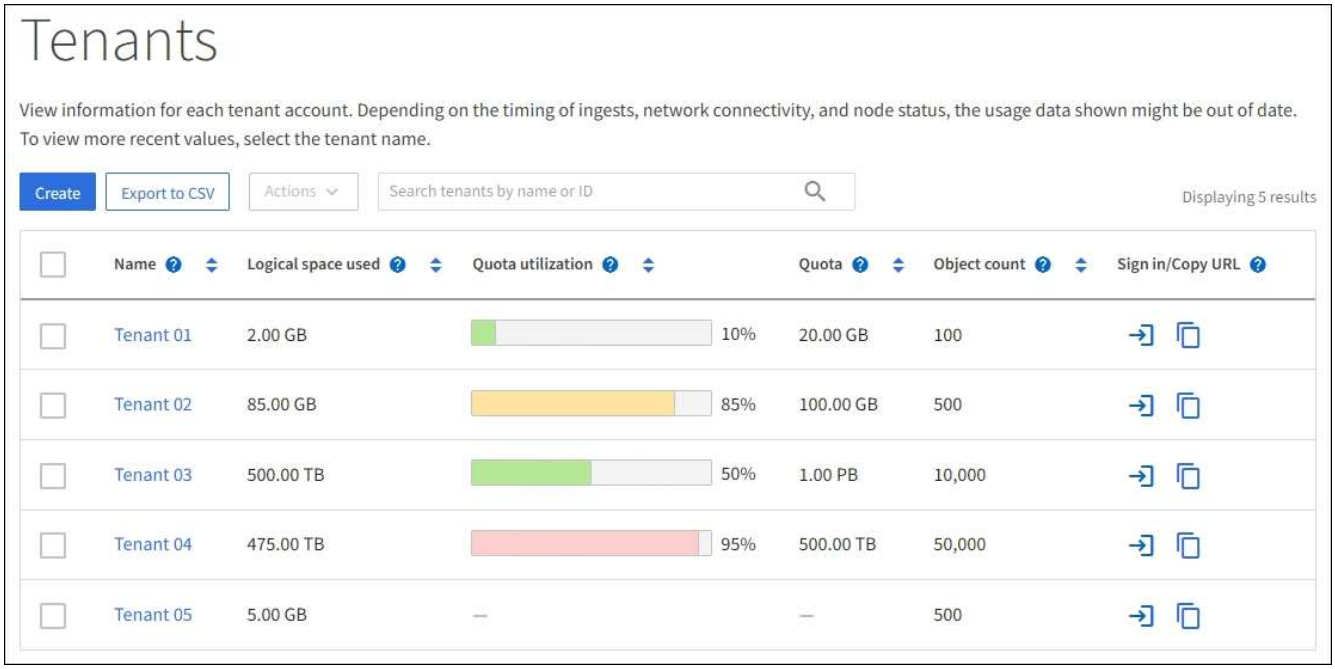
Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou contas de locatário" .

> A aplicação das configurações do locatário na grade pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

Passos

1. Selecione **LOCATÁRIOS**.



2. Localize a conta de locatário que você deseja editar.

   Use a caixa de pesquisa para procurar um inquilino por nome ou ID do inquilino.

3. Selecione o inquilino. Você pode fazer qualquer um dos seguintes:
   - Marque a caixa de seleção do locatário e selecione **Ações** > **Editar**.
   - Selecione o nome do inquilino para exibir a página de detalhes e selecione **Editar**.
4. Opcionalmente, altere os valores destes campos:
   - **Nome**

- **Descrição**
- **Cota de armazenamento**

5. Selecione **Continuar**.
6. Selecione ou desmarque as permissões para a conta do locatário.
   - Se você desabilitar os **Serviços da plataforma** para um locatário que já os esteja usando, os serviços que ele configurou para seus buckets S3 deixarão de funcionar. Nenhuma mensagem de erro é enviada ao locatário. Por exemplo, se o locatário tiver configurado a replicação do CloudMirror para um bucket S3, ele ainda poderá armazenar objetos no bucket, mas cópias desses objetos não serão mais feitas no bucket S3 externo que ele configurou como um ponto de extremidade. Ver "Gerenciar serviços de plataforma para contas de locatários do S3" .
   - Altere a configuração de **Usar fonte de identidade própria** para determinar se a conta do locatário usará sua própria fonte de identidade ou a fonte de identidade que foi configurada para o Grid Manager.

     Se **Usar fonte de identidade própria** for:

     - Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desabilitar sua fonte de identidade antes de poder usar a fonte de identidade que foi configurada para o Grid Manager.
     - Desabilitado e não selecionado, o SSO está habilitado para o sistema StorageGRID . O locatário deve usar a fonte de identidade que foi configurada para o Grid Manager.
   - Selecione ou desmarque a permissão **Permitir seleção S3** conforme necessário. Ver "Gerenciar S3 Select para contas de locatários" .
   - Para remover a permissão **Usar conexão de federação de grade**:
     i. Selecione a aba **Federação de grade**.
     ii. Selecione **Remover permissão**.
   - Para adicionar a permissão **Usar conexão de federação de grade**:
     i. Selecione a aba **Federação de grade**.
     ii. Marque a caixa de seleção **Usar conexão de federação de grade**.
     iii. Opcionalmente, selecione **Clonar usuários e grupos locais existentes** para cloná-los na grade remota. Se desejar, você pode interromper a clonagem em andamento ou tentar clonar novamente se alguns usuários ou grupos locais não puderem ser clonados após a conclusão da última operação de clonagem.
   - Para definir um período máximo de retenção ou permitir o modo de conformidade:

     > O bloqueio de objeto S3 deve ser habilitado na grade antes que você possa usar essas configurações.

     i. Selecione a aba **S3 Object Lock**.
     ii. Para **Definir período máximo de retenção**, insira um valor e selecione o período de tempo no menu suspenso.
     iii. Para **Permitir modo de conformidade**, marque a caixa de seleção.

Alterar senha do usuário root local do locatário

Pode ser necessário alterar a senha do usuário root local de um locatário se o usuário root estiver bloqueado na conta.

Antes de começar

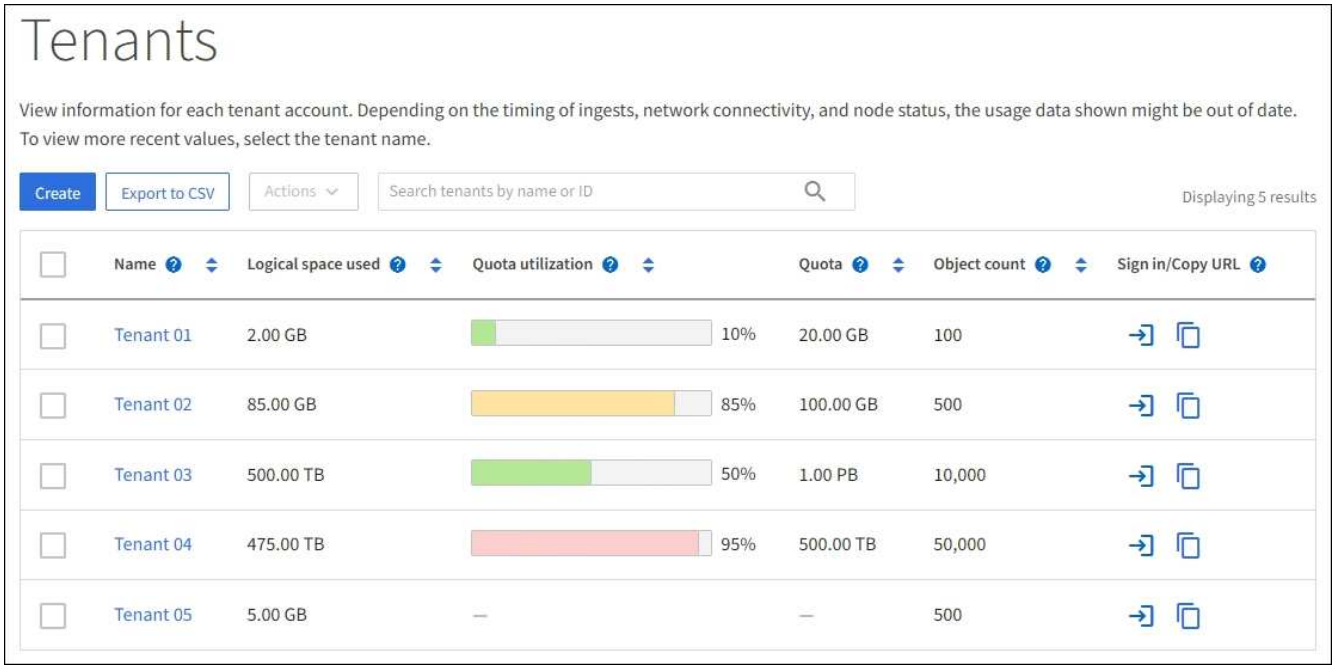
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , o usuário root local não poderá fazer login na conta do locatário. Para executar tarefas de usuário root, os usuários devem pertencer a um grupo federado que tenha permissão de acesso Root para o locatário.

Passos

1. Selecione **LOCATÁRIOS**.



2. Selecione a conta do locatário. Você pode fazer qualquer um dos seguintes:
   - Marque a caixa de seleção do locatário e selecione **Ações** > **Alterar senha root**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **Ações** > **Alterar senha root**.
3. Digite a nova senha para a conta do locatário.
4. Selecione **Salvar**.

Excluir conta de inquilino

Você pode excluir uma conta de locatário se quiser remover permanentemente o acesso do locatário ao sistema.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você removeu todos os buckets e objetos do S3 associados à conta do locatário.
- Se o inquilino tiver permissão para usar uma conexão de federação de rede, você revisou as considerações para"excluindo um locatário com a permissão Usar conexão de federação de grade" .

Passos

1. Selecione **LOCATÁRIOS**.
2. Localize a conta ou contas de locatário que você deseja excluir.

   Use a caixa de pesquisa para procurar um inquilino por nome ou ID do inquilino.

3. Para excluir vários inquilinos, marque as caixas de seleção e selecione **Ações** > **Excluir**.
4. Para excluir um único locatário, faça um dos seguintes:
   - Marque a caixa de seleção e selecione **Ações** > **Excluir**.
   - Selecione o nome do inquilino para exibir a página de detalhes e, em seguida, selecione **Ações** > **Excluir**.
5. Selecione **Sim**.

Gerenciar serviços de plataforma

O que são serviços de plataforma?

Os serviços de plataforma incluem replicação do CloudMirror, notificações de eventos e o serviço de integração de pesquisa.

Se você habilitar serviços de plataforma para contas de locatários do S3, deverá configurar sua grade para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

Replicação do CloudMirror

O serviço de replicação StorageGRID CloudMirror é usado para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

Por exemplo, você pode usar a replicação do CloudMirror para espelhar registros específicos de clientes no Amazon S3 e, em seguida, aproveitar os serviços da AWS para realizar análises em seus dados.

> A replicação do CloudMirror tem algumas semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, consulte"Comparar a replicação entre grades e a replicação do CloudMirror" .

> A replicação do CloudMirror não será suportada se o bucket de origem tiver o S3 Object Lock habilitado.

Notificações

Notificações de eventos por bucket são usadas para enviar notificações sobre ações específicas executadas em objetos para um cluster Kafka externo especificado ou Amazon Simple Notification Service.

Por exemplo, você pode configurar alertas a serem enviados aos administradores sobre cada objeto adicionado a um bucket, onde os objetos representam arquivos de log associados a um evento crítico do sistema.

> Embora a notificação de eventos possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo Retain Until Date e status de retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Serviço de integração de pesquisa

O serviço de integração de pesquisa é usado para enviar metadados de objetos S3 para um índice Elasticsearch especificado, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

Por exemplo, você pode configurar seus buckets para enviar metadados de objetos S3 para um serviço remoto do Elasticsearch. Você pode então usar o Elasticsearch para realizar pesquisas em buckets e realizar análises sofisticadas de padrões presentes nos metadados do seu objeto.

> Embora a integração do Elasticsearch possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo Retain Until Date e status de retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Os serviços de plataforma oferecem aos locatários a capacidade de usar recursos de armazenamento externo, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino dos serviços da plataforma normalmente é externo à sua implantação do StorageGRID , você deve decidir se deseja permitir que os locatários usem esses serviços. Se fizer isso, você deverá habilitar o uso dos serviços da plataforma ao criar ou editar contas de locatários. Você também deve configurar sua rede de modo que as mensagens dos serviços de plataforma geradas pelos locatários possam chegar aos seus destinos.

Recomendações para uso de serviços de plataforma

Antes de utilizar os serviços da plataforma, esteja ciente das seguintes recomendações:

- Se um bucket S3 no sistema StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitados, você também deverá habilitar o controle de versão do bucket S3 para o endpoint de destino. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no ponto de extremidade.
- Você não deve usar mais de 100 locatários ativos com solicitações S3 que exijam replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 locatários ativos pode resultar em desempenho mais lento do cliente S3.
- Solicitações para um endpoint que não podem ser concluídas serão enfileiradas para um máximo de 500.000 solicitações. Esse limite é dividido igualmente entre os inquilinos ativos. Novos inquilinos podem exceder temporariamente esse limite de 500.000 para que os inquilinos recém-criados não sejam penalizados injustamente.

Informações relacionadas

- "Gerenciar serviços de plataforma"
- "Configurar as definições de proxy de armazenamento"
- "Monitorar StorageGRID"

Rede e portas para serviços de plataforma

Se você permitir que um locatário do S3 use serviços de plataforma, deverá configurar a rede para a grade para garantir que as mensagens dos serviços de plataforma possam ser entregues aos seus destinos.

Você pode habilitar serviços de plataforma para uma conta de locatário do S3 ao criar ou atualizar a conta de locatário. Se os serviços da plataforma estiverem habilitados, o locatário poderá criar endpoints que servem como destino para replicação do CloudMirror, notificações de eventos ou mensagens de integração de pesquisa de seus buckets do S3. Essas mensagens de serviços de plataforma são enviadas dos nós de armazenamento que executam o serviço ADC para os pontos de extremidade de destino.

Por exemplo, os locatários podem configurar os seguintes tipos de pontos de extremidade de destino:

- Um cluster Elasticsearch hospedado localmente
- Um aplicativo local que oferece suporte ao recebimento de mensagens do Amazon Simple Notification Service
- Um cluster Kafka hospedado localmente
- Um bucket S3 hospedado localmente na mesma ou em outra instância do StorageGRID
- Um ponto de extremidade externo, como um ponto de extremidade no Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a rede ou redes que contêm os nós de armazenamento do ADC. Você deve garantir que as seguintes portas possam ser usadas para enviar mensagens de serviços de plataforma para os terminais de destino.

Por padrão, as mensagens dos serviços da plataforma são enviadas nas seguintes portas:

- **80**: Para URIs de endpoint que começam com http (a maioria dos endpoints)
- **443**: Para URIs de endpoint que começam com https (a maioria dos endpoints)
- **9092**: Para URIs de endpoint que começam com http ou https (somente endpoints do Kafka)

Os locatários podem especificar uma porta diferente ao criar ou editar um ponto de extremidade.

> Se uma implantação do StorageGRID for usada como destino para replicação do CloudMirror, as mensagens de replicação poderão ser recebidas em uma porta diferente de 80 ou 443. Certifique-se de que a porta usada para o S3 pela implantação do StorageGRID de destino esteja especificada no ponto de extremidade.

Se você usar um servidor proxy não transparente, você também deve"configurar configurações de proxy de armazenamento" para permitir que mensagens sejam enviadas para terminais externos, como um terminal na Internet.

Informações relacionadas

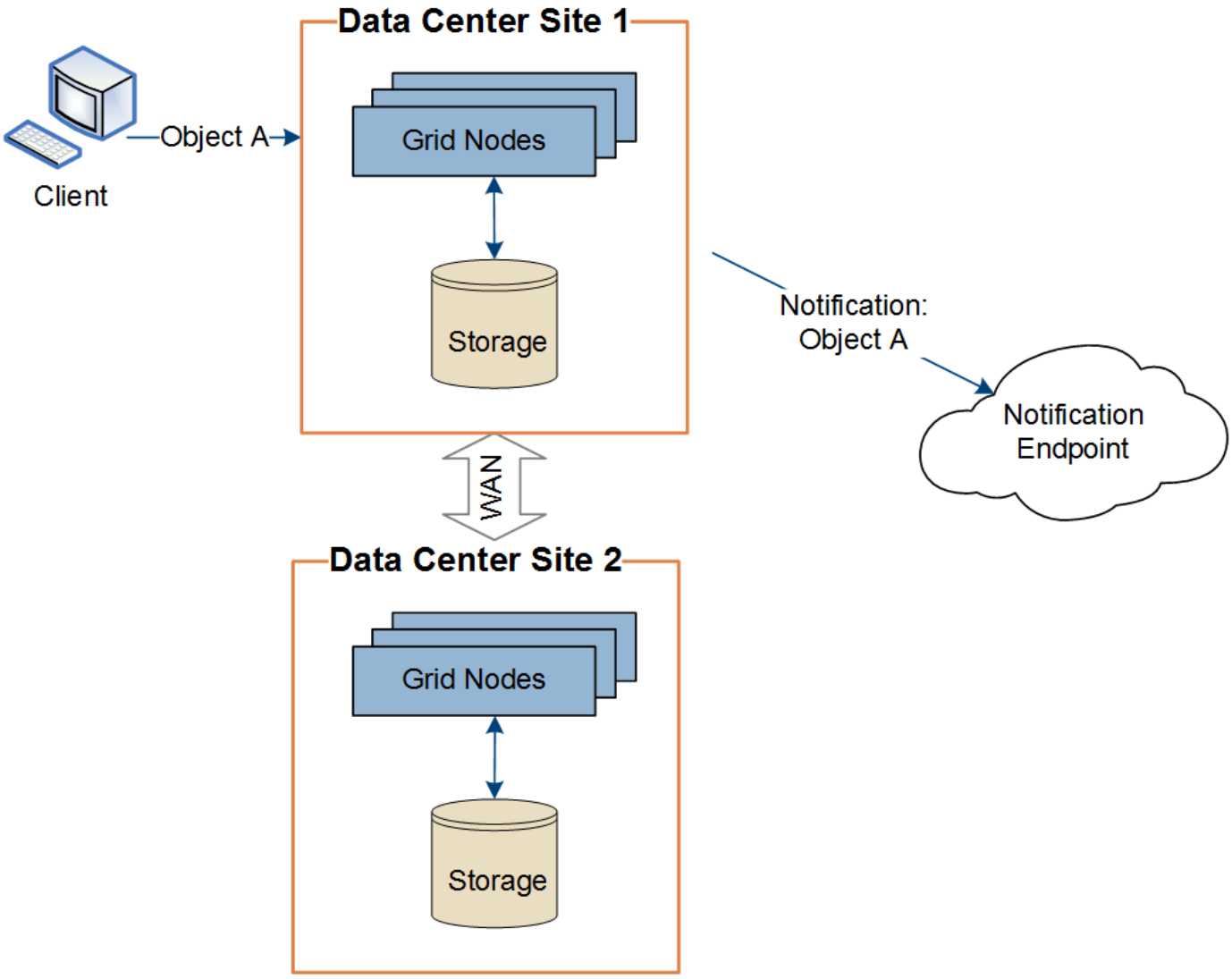
"Use uma conta de inquilino"

Entrega de mensagens de serviços de plataforma por site

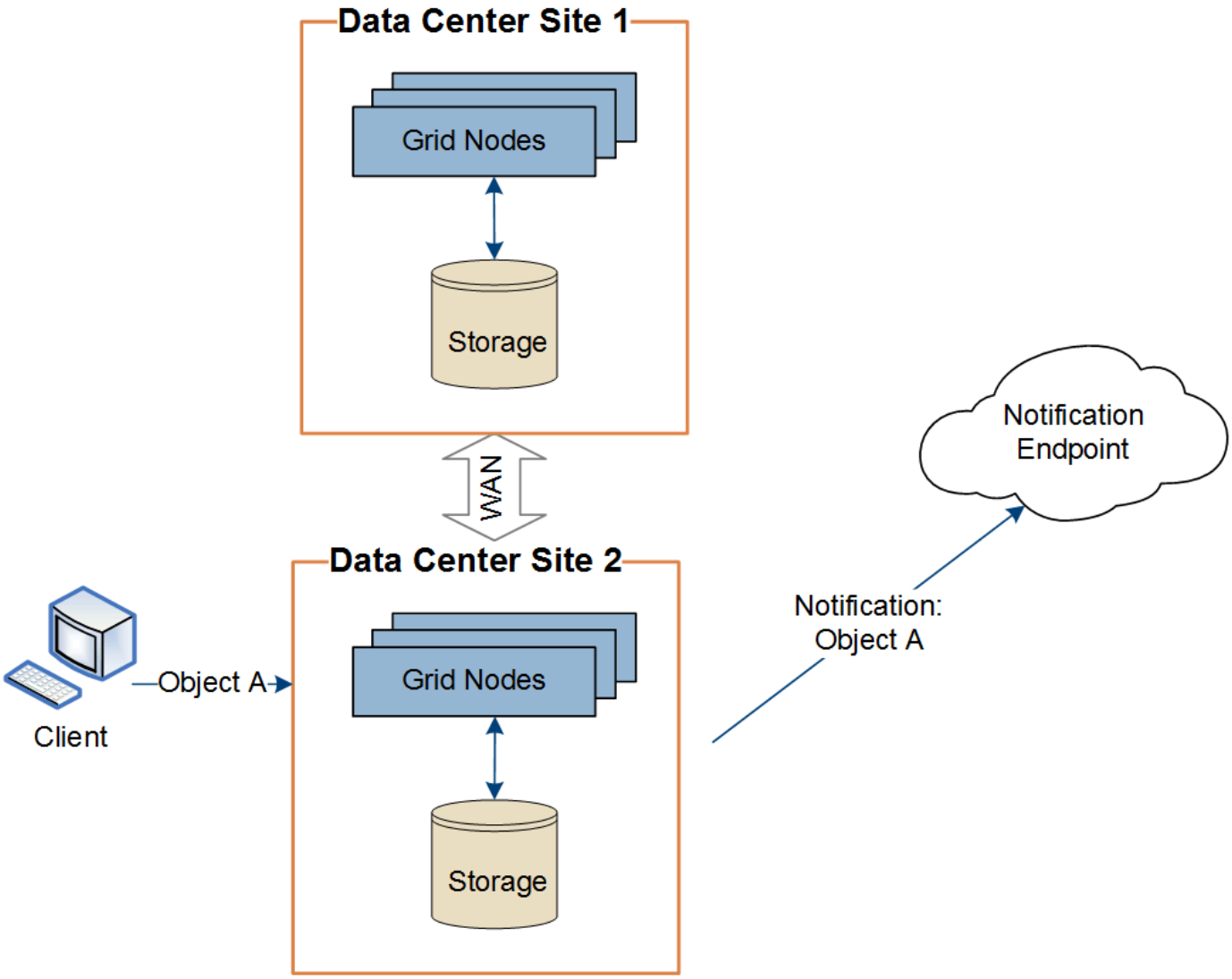
Todas as operações de serviços de plataforma são realizadas por site.

Ou seja, se um locatário usar um cliente para executar uma operação de criação de API do S3 em um objeto conectando-se a um nó de gateway no site do data center 1, a notificação sobre essa ação será acionada e

enviada do site do data center 1.



Se o cliente posteriormente executar uma operação de exclusão da API S3 no mesmo objeto do Site do Data Center 2, a notificação sobre a ação de exclusão será acionada e enviada do Site do Data Center 2.



Certifique-se de que a rede em cada site esteja configurada de forma que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Solucionar problemas de serviços de plataforma

Os pontos de extremidade usados nos serviços da plataforma são criados e mantidos pelos usuários locatários no Gerenciador de Locatários; no entanto, se um locatário tiver problemas para configurar ou usar os serviços da plataforma, você poderá usar o Gerenciador de Grade para ajudar a resolver o problema.

Problemas com novos endpoints

Antes que um locatário possa usar os serviços da plataforma, ele deve criar um ou mais pontos de extremidade usando o Gerenciador de Locatários. Cada ponto de extremidade representa um destino externo para um serviço de plataforma, como um bucket StorageGRID S3, um bucket Amazon Web Services, um tópico Amazon Simple Notification Service, um tópico Kafka ou um cluster Elasticsearch hospedado localmente ou na AWS. Cada ponto de extremidade inclui a localização do recurso externo e as credenciais necessárias para acessar esse recurso.

Quando um locatário cria um ponto de extremidade, o sistema StorageGRID valida que o ponto de extremidade existe e que pode ser acessado usando as credenciais especificadas. A conexão com o ponto de

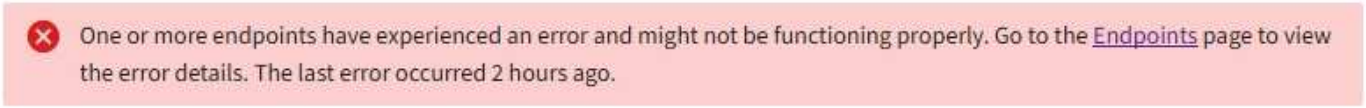
extremidade é validada a partir de um nó em cada site.

Se a validação do ponto de extremidade falhar, uma mensagem de erro explicará o motivo da falha. O usuário locatário deve resolver o problema e tentar criar o endpoint novamente.

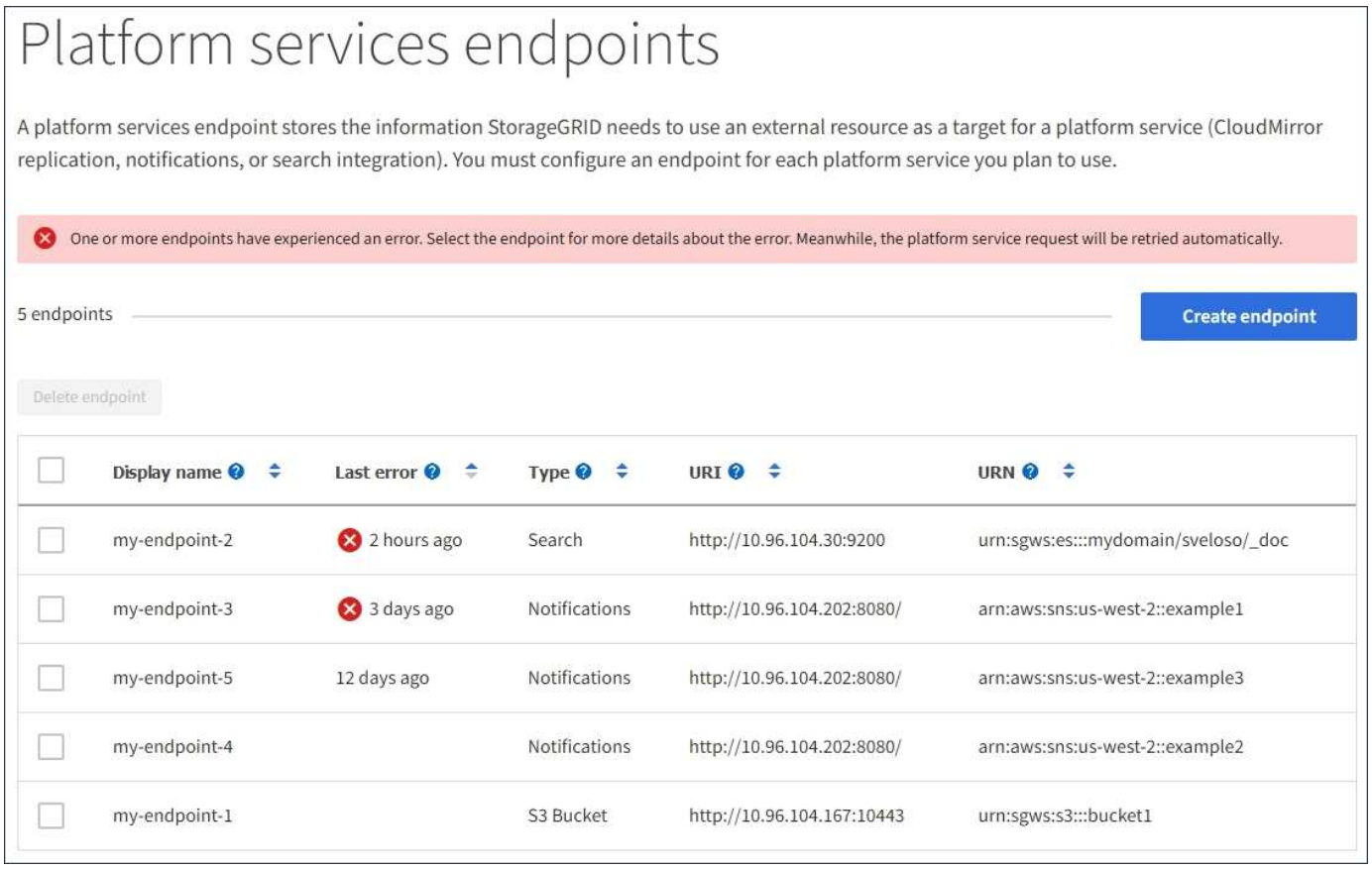
A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do locatário.

Problemas com endpoints existentes

Se ocorrer um erro quando o StorageGRID tentar acessar um ponto de extremidade existente, uma mensagem será exibida no painel do Gerenciador de Tenants.



Os usuários locatários podem acessar a página Endpoints para revisar a mensagem de erro mais recente para cada endpoint e determinar há quanto tempo o erro ocorreu. A coluna **Último erro** exibe a mensagem de erro mais recente para cada ponto de extremidade e indica há quanto tempo o erro ocorreu. Erros que incluem o ícone ocorreu nos últimos 7 dias.



Algumas mensagens de erro na coluna **Último erro** podem incluir um logID entre parênteses. Um administrador de grade ou suporte técnico pode usar esse ID para localizar informações mais detalhadas sobre o erro no bycast.log.

Problemas relacionados a servidores proxy

Se você configurou um"proxy de armazenamento" entre os nós de armazenamento e os pontos de extremidade do serviço de plataforma, podem ocorrer erros se o serviço de proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não estejam bloqueadas.

Determinar se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o painel no Gerenciador de Tenants exibirá uma mensagem de alerta. Você pode acessar a página Endpoints para ver mais detalhes sobre o erro.

As operações do cliente falham

Alguns problemas de serviços de plataforma podem causar falhas nas operações do cliente no bucket S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno da Máquina de Estado Replicado (RSM) parar ou se houver muitas mensagens de serviços de plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**.
2. Selecione ***site*** > ***Nó de Armazenamento*** > **SSM** > **Serviços**.

Erros de endpoint recuperáveis e irrecuperáveis

Após a criação dos endpoints, erros de solicitação de serviço de plataforma podem ocorrer por vários motivos. Alguns erros podem ser recuperados com intervenção do usuário. Por exemplo, erros recuperáveis podem ocorrer pelos seguintes motivos:

- As credenciais do usuário foram excluídas ou expiraram.
- O bucket de destino não existe.
- A notificação não pode ser entregue.

Se o StorageGRID encontrar um erro recuperável, a solicitação de serviço da plataforma será repetida até ser bem-sucedida.

Outros erros são irrecuperáveis. Por exemplo, um erro irrecuperável ocorre se o ponto de extremidade for excluído.

Se o StorageGRID encontrar um erro de endpoint irrecuperável:

- No Grid Manager, acesse **Suporte** > **Ferramentas** > **Métricas** > **Grafana** > **Visão geral dos serviços de plataforma** para visualizar detalhes do erro.
- No Gerenciador de Tenants, acesse **ARMAZENAMENTO (S3)** > **Pontos de extremidade dos serviços de plataforma** para visualizar os detalhes do erro.
- Verifique o `/var/local/log/bycast-err.log` para erros relacionados. Os nós de armazenamento que têm o serviço ADC contêm este arquivo de log.

As mensagens dos serviços da plataforma não podem ser entregues

Se o destino encontrar um problema que o impeça de aceitar mensagens de serviços de plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem de serviços de plataforma não será entregue. Por exemplo, esse erro pode ocorrer se as credenciais forem atualizadas no destino de forma que o

StorageGRID não consiga mais se autenticar no serviço de destino.

Verifique se há alertas relacionados.

Desempenho mais lento para solicitações de serviço de plataforma

O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o ponto de extremidade de destino pode receber as solicitações. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao ponto de extremidade de destino.

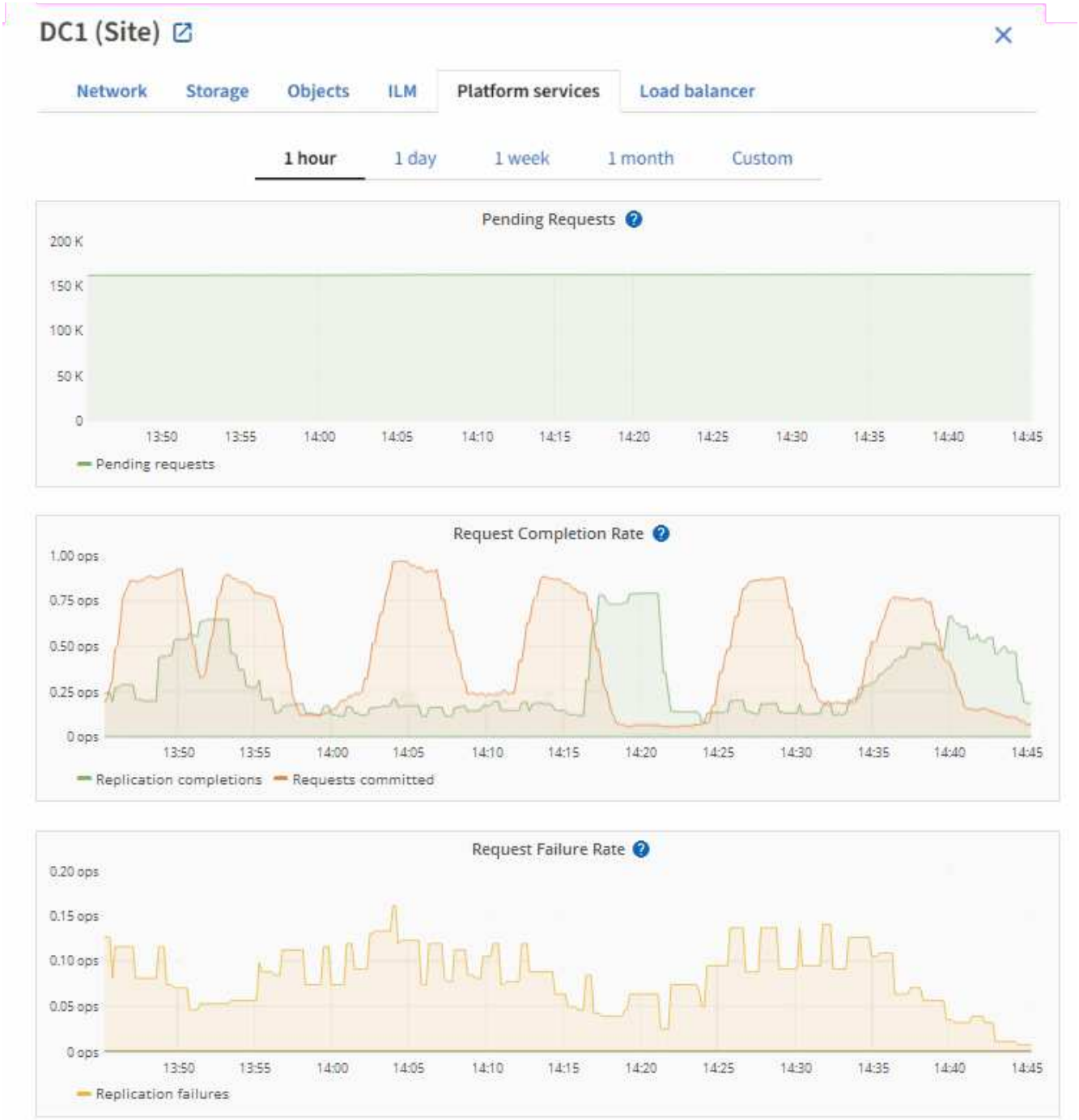
O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, reduza a taxa de ingestão ou use um ponto de extremidade com maior capacidade. Se o acúmulo de solicitações continuar a crescer, as operações do cliente S3 (como solicitações PUT) acabarão falhando.

As solicitações do CloudMirror têm maior probabilidade de serem afetadas pelo desempenho do ponto de extremidade de destino porque essas solicitações geralmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou notificação de eventos.

Falha nas solicitações de serviço da plataforma

Para visualizar a taxa de falha de solicitação para serviços de plataforma:

1. Selecione **NODES**.
2. Selecione ***site*** > **Serviços de plataforma**.
3. Veja o gráfico de taxas de erros de solicitação.



Alerta de serviços de plataforma indisponíveis

O alerta **Serviços de plataforma indisponíveis** indica que nenhuma operação de serviço de plataforma pode ser executada em um site porque poucos nós de armazenamento com o serviço RSM estão em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas aos seus respectivos terminais.

Para resolver esse alerta, determine quais nós de armazenamento no site incluem o serviço RSM. (O serviço RSM está presente em nós de armazenamento que também incluem o serviço ADC.) Em seguida, certifique-se de que a maioria simples desses nós de armazenamento esteja em execução e disponível.

Se mais de um nó de armazenamento que contém o serviço RSM falhar em um site, você perderá todas as solicitações de serviço de plataforma pendentes para esse site.

Orientações adicionais para solução de problemas de endpoints de serviços de plataforma

Para obter informações adicionais, consulte**Use uma conta de locatário › Solucionar problemas de endpoints de serviços de plataforma** .

Informações relacionadas

"Solucionar problemas do sistema StorageGRID"

Gerenciar S3 Select para contas de locatários

Você pode permitir que determinados locatários do S3 usem o S3 Select para emitir solicitações SelectObjectContent em objetos individuais.

O S3 Select oferece uma maneira eficiente de pesquisar grandes quantidades de dados sem precisar implantar um banco de dados e recursos associados para habilitar pesquisas. Também reduz o custo e a latência da recuperação de dados.

O que é o S3 Select?

O S3 Select permite que clientes S3 usem solicitações SelectObjectContent para filtrar e recuperar apenas os dados necessários de um objeto. A implementação do StorageGRID do S3 Select inclui um subconjunto de comandos e recursos do S3 Select.

Considerações e requisitos para usar o S3 Select

Requisitos de administração da rede

O administrador da rede deve conceder aos locatários a capacidade de seleção do S3. Selecione **Permitir seleção S3** quando"criando um inquilino" ou"editando um inquilino" .

Requisitos de formato de objeto

O objeto que você deseja consultar deve estar em um dos seguintes formatos:

- **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
- **Parquet**. Requisitos adicionais para objetos Parquet:
  - O S3 Select suporta apenas compactação em colunas usando GZIP ou Snappy. O S3 Select não oferece suporte à compactação de objetos inteiros para objetos Parquet.
  - O S3 Select não suporta saída Parquet. Você deve especificar o formato de saída como CSV ou JSON.
  - O tamanho máximo do grupo de linhas descompactado é 512 MB.
  - Você deve usar os tipos de dados especificados no esquema do objeto.
  - Você não pode usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.

Requisitos de endpoint

A solicitação SelectObjectContent deve ser enviada para um"Ponto de extremidade do balanceador de carga

StorageGRID" .

Os nós de administração e gateway usados pelo endpoint devem ser um dos seguintes:

- Um nó de dispositivo de serviços
- Um nó de software baseado em VMware
- Um nó bare metal executando um kernel com cgroup v2 habilitado

Considerações gerais

As consultas não podem ser enviadas diretamente para os nós de armazenamento.

> Solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e somente para locatários confiáveis.

Veja o"instruções para usar o S3 Select" .

Para visualizar"Gráficos Grafana" para operações S3 Select ao longo do tempo, selecione **SUPORTE** > **Ferramentas** > **Métricas** no Grid Manager.

Configurar conexões do cliente

Configurar conexões do cliente S3

Como administrador de grade, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 se conectam ao seu sistema StorageGRID para armazenar e recuperar dados.

> Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "StorageGRID 11.8: Configurar conexões de cliente S3 e Swift" .

Tarefas de configuração

1. Execute tarefas de pré-requisito no StorageGRID, com base em como o aplicativo cliente se conectará ao StorageGRID.

Tarefas necessárias

Você deve obter:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Tarefas opcionais

Opcionalmente, configure:

- Federação de identidade
- SSO

1. Use o StorageGRID para obter os valores que o aplicativo precisa para se conectar à grade. Você pode usar o assistente de configuração do S3 ou configurar cada entidade do StorageGRID manualmente.

Use o assistente de configuração do S3

Siga as etapas do assistente de configuração do S3.

Configurar manualmente

1. Criar grupo de alta disponibilidade
2. Criar ponto de extremidade do balanceador de carga
3. Criar conta de inquilino
4. Criar bucket e chaves de acesso
5. Configurar regra e política do ILM

1. Use o aplicativo S3 para concluir a conexão com o StorageGRID. Crie entradas DNS para associar endereços IP a quaisquer nomes de domínio que você planeja usar.

   Conforme necessário, execute configurações adicionais do aplicativo.

2. Execute tarefas contínuas no aplicativo e no StorageGRID para gerenciar e monitorar o armazenamento de objetos ao longo do tempo.

Informações necessárias para anexar o StorageGRID a um aplicativo cliente

Antes de poder anexar o StorageGRID a um aplicativo cliente S3, você deve executar etapas de configuração no StorageGRID e obter determinado valor.

Quais valores eu preciso?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e onde esses valores são usados pelo aplicativo S3 e pelo servidor DNS.

Valor	Onde o valor é configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > grupo HA	Entrada DNS
Porta	StorageGRID > Ponto de extremidade do balanceador de carga	Aplicação do cliente
Certificado SSL	StorageGRID > Ponto de extremidade do balanceador de carga	Aplicação do cliente
Nome do servidor (FQDN)	StorageGRID > Ponto de extremidade do balanceador de carga	• Aplicação do cliente • Entrada DNS
ID da chave de acesso S3 e chave de acesso secreta	StorageGRID > Locatário e bucket	Aplicação do cliente
Nome do balde/recipiente	StorageGRID > Locatário e bucket	Aplicação do cliente

Como obtenho esses valores?

Dependendo de suas necessidades, você pode fazer o seguinte para obter as informações necessárias:

- *Use o"Assistente de configuração do S3" *. O assistente de configuração do S3 ajuda você a configurar rapidamente os valores necessários no StorageGRID e gera um ou dois arquivos que você pode usar ao configurar o aplicativo S3. O assistente orienta você nas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID .

  Se você estiver configurando um aplicativo S3, é recomendável usar o assistente de configuração do S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exija personalização significativa.

- *Use o"Assistente de configuração do FabricPool" *. Semelhante ao assistente de configuração do S3, o assistente de configuração do FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar uma camada de nuvem do FabricPool no ONTAP.

  Se você planeja usar o StorageGRID como o sistema de armazenamento de objetos para uma camada de nuvem do FabricPool , é recomendável usar o assistente de configuração do FabricPool , a menos que você saiba que tem requisitos especiais ou que sua implementação exija personalização significativa.

- **Configurar itens manualmente**. Se você estiver se conectando a um aplicativo S3 e preferir não usar o assistente de configuração do S3, poderá obter os valores necessários executando a configuração manualmente. Siga estes passos:

  a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3. Ver "Configurar grupos de alta disponibilidade" .

  b. Crie o ponto de extremidade do balanceador de carga que o aplicativo S3 usará. Ver "Configurar pontos de extremidade do balanceador de carga" .

c. Crie a conta de locatário que o aplicativo S3 usará. Ver "Criar uma conta de inquilino" .

d. Para um locatário S3, entre na conta do locatário e gere um ID de chave de acesso e uma chave de acesso secreta para cada usuário que acessará o aplicativo. Ver "Crie suas próprias chaves de acesso" .

e. Crie um ou mais buckets S3 na conta do locatário. Para S3, veja"Criar bucket S3" .

f. Para adicionar instruções de posicionamento específicas para os objetos pertencentes ao novo locatário ou bucket/contêiner, crie uma nova regra do ILM e ative uma nova política do ILM para usar essa regra. Ver"Criar regra ILM" e"Criar política de ILM" .

Segurança para clientes S3

As contas de locatário do StorageGRID usam aplicativos cliente S3 para salvar dados de objetos no StorageGRID. Você deve revisar as medidas de segurança implementadas para aplicativos clientes.

Resumo

A lista a seguir resume como a segurança é implementada para a API REST do S3:

Segurança de conexão
TLS

Autenticação do servidor
Certificado de servidor X.509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador

Autenticação do cliente
ID da chave de acesso da conta S3 e chave de acesso secreta

Autorização do cliente
Propriedade do bucket e todas as políticas de controle de acesso aplicáveis

Como o StorageGRID fornece segurança para aplicativos clientes

Os aplicativos cliente S3 podem se conectar ao serviço Load Balancer em nós de gateway ou nós de administração ou diretamente aos nós de armazenamento.

- Os clientes que se conectam ao serviço Load Balancer podem usar HTTPS ou HTTP, dependendo de como você"configurar o ponto de extremidade do balanceador de carga" .

  HTTPS fornece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao ponto de extremidade.

  O HTTP fornece comunicação menos segura e não criptografada e deve ser usado somente para grades de teste ou que não sejam de produção.

- Clientes que se conectam aos nós de armazenamento também podem usar HTTPS ou HTTP.

  HTTPS é o padrão e é recomendado.

  O HTTP fornece comunicação menos segura e não criptografada, mas pode ser opcionalmente"habilitado" para grades de não produção ou de teste.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço do balanceador de carga e os nós de armazenamento na grade são criptografadas, independentemente de o ponto de extremidade do balanceador de carga estar configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer"Cabeçalhos de autenticação HTTP" para StorageGRID para executar operações da API REST.

Certificados de segurança e aplicativos cliente

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 conectam ao serviço do Load Balancer, eles usam o certificado que foi configurado para o ponto de extremidade do balanceador de carga. Cada ponto de extremidade do balanceador de carga tem seu próprio certificado, um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o ponto de extremidade.

  Ver "Considerações para balanceamento de carga" .

- Quando aplicativos cliente se conectam diretamente a um nó de armazenamento, 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. Ver "adicionar um certificado de API S3 personalizado" .

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

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID oferece suporte a um conjunto de conjuntos de cifras que os aplicativos clientes podem usar ao estabelecer uma sessão TLS. Para configurar cifras, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** e selecione **Políticas TLS e SSH**.

Versões suportadas do TLS

O StorageGRID suporta TLS 1.2 e TLS 1.3.

SSLv3 e TLS 1.1 (ou versões anteriores) não são mais suportados.

Use o assistente de configuração do S3

Usar o assistente de configuração do S3: considerações e requisitos

Você pode usar o assistente de configuração do S3 para configurar o StorageGRID como o sistema de armazenamento de objetos para um aplicativo S3.

Quando usar o assistente de configuração do S3

O assistente de configuração do S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você baixa arquivos que podem ser usados para inserir valores no aplicativo S3. Use o assistente para configurar seu sistema mais rapidamente e

garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID .

Se você tem o"Permissão de acesso root" , você pode concluir o assistente de configuração do S3 ao começar a usar o StorageGRID Grid Manager ou pode acessar e concluir o assistente posteriormente. Dependendo dos seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para reunir os valores que um aplicativo S3 precisa.

Antes de usar o assistente

Antes de usar o assistente, confirme se você concluiu estes pré-requisitos.

Obter endereços IP e configurar interfaces VLAN

Se você configurar um grupo de alta disponibilidade (HA), saberá a quais nós o aplicativo S3 se conectará e qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de sub-rede, endereço IP do gateway e endereços IP virtuais (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, você já configurou a interface VLAN. Ver "Configurar interfaces VLAN" .

Configurar federação de identidade e SSO

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID , você habilitou esses recursos. Você também sabe qual grupo federado deve ter acesso root para a conta de locatário que o aplicativo S3 usará. Ver"Usar federação de identidade" e"Configurar logon único" .

Obter e configurar nomes de domínio

Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA que você criar usando o assistente.

Se você planeja usar solicitações de estilo de hospedagem virtual S3, você deve ter"nomes de domínio de endpoint S3 configurados" . É recomendável usar solicitações de estilo de hospedagem virtual.

Revisar os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID , revise as considerações gerais para balanceamento de carga. Você tem os certificados que irá enviar ou os valores necessários para gerar um certificado.

Se você planeja usar um ponto de extremidade de balanceador de carga externo (de terceiros), você tem o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Configurar quaisquer conexões de federação de grade

Se você quiser permitir que o locatário do S3 clone dados da conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade, confirme o seguinte antes de iniciar o assistente:

- Você tem"configurou a conexão da federação de grade" .
- O status da conexão é **Conectado**.
- Você tem permissão de acesso Root.

Acesse e conclua o assistente de configuração do S3

Você pode usar o assistente de configuração do S3 para configurar o StorageGRID para uso com um aplicativo S3. O assistente de configuração fornece os valores que o aplicativo precisa para acessar um bucket do StorageGRID e salvar objetos.

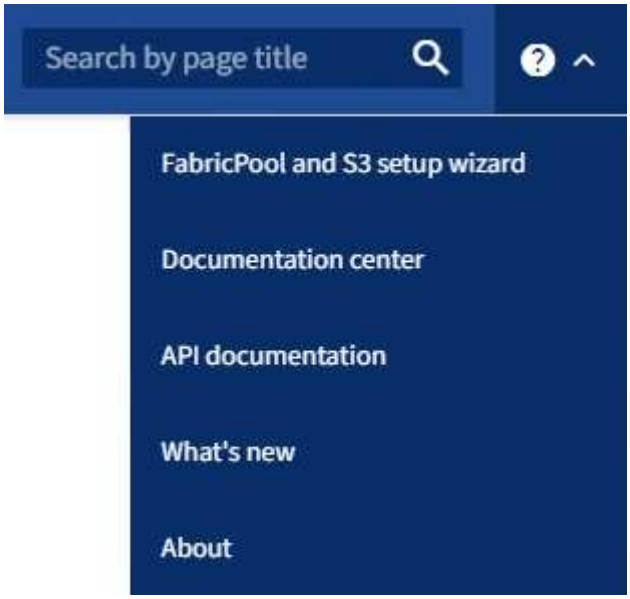
Antes de começar

- Você tem o"Permissão de acesso root" .
- Você revisou o"considerações e requisitos" para usar o assistente.

Acesse o assistente

Passos

1. Sign in no Grid Manager usando um"navegador da web compatível" .
2. Se o banner * Assistente de configuração do FabricPool e do S3* aparecer no painel, selecione o link no banner. Se o banner não aparecer mais, selecione o ícone de ajuda na barra de cabeçalho no Grid Manager e selecione * Assistente de configuração do FabricPool e S3*.



3. Na seção do aplicativo S3 da página do assistente de configuração do FabricPool e do S3, selecione **Configurar agora**.

Etapa 1 de 6: Configurar grupo HA

Um grupo HA é uma coleção de nós que contêm o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo HA para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho com pouco impacto nas operações do S3.

Para obter detalhes sobre esta tarefa, consulte"Gerenciar grupos de alta disponibilidade" .

Passos

1. Se você planeja usar um balanceador de carga externo, não precisa criar um grupo de HA. Selecione **Ignorar esta etapa** e vá paraEtapa 2 de 6: Configurar o ponto de extremidade do balanceador de carga .
2. Para usar o balanceador de carga StorageGRID , você pode criar um novo grupo de HA ou usar um grupo de HA existente.

Criar grupo HA

a. Para criar um novo grupo HA, selecione **Criar grupo HA**.

b. Para a etapa **Inserir detalhes**, preencha os seguintes campos.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

c. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo de HA.

Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas pode selecionar apenas uma interface para cada nó.

d. Para a etapa **Priorizar interfaces**, determine a interface primária e quaisquer interfaces de backup para este grupo de HA.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface na lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços IP virtuais (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup e assim por diante. Quando as falhas são resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

e. Para a etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR: um endereço IPv4 seguido por uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.
Endereço IP do gateway (opcional)	Se os endereços IP do S3 usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID , insira o endereço IP do gateway local VIP do StorageGRID . O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Criar grupo HA** e depois selecione **Concluir** para retornar ao assistente de configuração do S3.

g. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Usar grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA em **Selecionar um grupo HA**.

b. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o ponto de extremidade do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários nós de armazenamento.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administração, ou pode se conectar a um balanceador de carga externo (de terceiros). É recomendado usar o balanceador de carga StorageGRID .

Para obter detalhes sobre esta tarefa, consulte"Considerações para balanceamento de carga" .

Para usar o serviço StorageGRID Load Balancer, selecione a guia * StorageGRID load balancer* e crie ou selecione o ponto de extremidade do balanceador de carga que deseja usar. Para usar um balanceador de carga externo, selecione a aba **Balanceador de carga externo** e forneça detalhes sobre o sistema que você já configurou.

Criar ponto final

Passos

1. Para criar um ponto de extremidade do balanceador de carga, selecione **Criar ponto de extremidade**.
2. Para a etapa **Inserir detalhes do ponto de extremidade**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o ponto de extremidade.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada. Se você digitar 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway, porque essas portas são reservadas em nós de administração. **Observação:** Portas usadas por outros serviços de rede não são permitidas. Veja o"Referência de porta de rede" .
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Observação**: a comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

3. Para a etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.

Modo	Descrição
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

4. Para a etapa de acesso do locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse endpoint para acessar seus buckets.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

5. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Ver"Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que inserir.
Usar certificado StorageGRID S3	Use esta opção somente se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID . Ver"Configurar certificados da API S3" para mais detalhes.

6. Selecione **Concluir** para retornar ao assistente de configuração do S3.
7. Selecione **Continuar** para ir para a etapa do locatário e do bucket.

Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Usar ponto de extremidade do balanceador de carga existente

Passos

1. Para usar um ponto de extremidade existente, selecione seu nome em **Selecionar um ponto de extremidade do balanceador de carga**.
2. Selecione **Continuar** para ir para a etapa do locatário e do bucket.

Usar balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os seguintes campos.

Campo	Descrição
FQDN	O nome de domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o aplicativo S3 usará para se conectar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continuar** para ir para a etapa do locatário e do bucket.

Etapa 3 de 6: criar locatário e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos.

Um bucket é um contêiner usado para armazenar objetos e metadados de objetos de um locatário. Embora os locatários possam ter muitos buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Se precisar adicionar buckets ou definir opções posteriormente, você pode usar o Gerenciador de Tenants.

Para obter detalhes sobre esta tarefa, consulte"Criar conta de inquilino" e"Criar bucket S3" .

Passos

1. Insira um nome para a conta do locatário.

   Os nomes dos inquilinos não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta numérico exclusivo.

2. Defina o acesso root para a conta do locatário, com base no uso do seu sistema StorageGRID"federação de identidade" ,"logon único (SSO)" , ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.

Opção	Faça isso
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter"Permissão de acesso root" para o inquilino. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter"Permissão de acesso root" para o inquilino. Nenhum usuário local pode fazer login.

3. Se você quiser que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário root, selecione **Criar chave de acesso S3 do usuário root automaticamente**.

   Selecione esta opção se o único usuário do locatário for o usuário root. Se outros usuários usarem este locatário,"usar o Gerenciador de Inquilinos" para configurar chaves e permissões.

4. Se você quiser criar um bucket para este locatário agora, selecione **Criar bucket para este locatário**.

   Se o S3 Object Lock estiver habilitado para a grade, o bucket criado nesta etapa não terá o S3 Object Lock habilitado. Se você precisar usar um bucket do S3 Object Lock para este aplicativo S3, não selecione criar um bucket agora. Em vez disso, use o Tenant Manager para"crie o balde" mais tarde.

   a. Insira o nome do bucket que o aplicativo S3 usará. Por exemplo, `s3-bucket` .

      Não é possível alterar o nome do bucket após criá-lo.

   b. Selecione a **Região** para este bucket.

      Use a região padrão(`us-east-1`) a menos que você pretenda usar o ILM no futuro para filtrar objetos com base na região do bucket.

5. Selecione **Criar e continuar**.

Etapa 4 de 6: Baixar dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que acabou de configurar.

Passos

1. Se você selecionou **Criar chave de acesso S3 de usuário root automaticamente**, faça um ou ambos os procedimentos a seguir:
   - Selecione **Baixar chaves de acesso** para baixar um `.csv` arquivo contendo o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
   - Selecione o ícone de cópia ( ) para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.
2. Selecione **Baixar valores de configuração** para baixar um `.txt` arquivo contendo as configurações para o endpoint do balanceador de carga, locatário, bucket e usuário root.
3. Salve essas informações em um local seguro.

Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis depois que você fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID .

4. Se solicitado, marque a caixa de seleção para confirmar que você baixou ou copiou as chaves.
5. Selecione **Continuar** para ir para a etapa de regra e política do ILM.

Etapa 5 de 6: Revise a regra e a política do ILM para o S3

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID . A política ILM incluída no StorageGRID faz duas cópias replicadas de todos os objetos. Esta política estará em vigor até que você ative pelo menos uma nova política.

Passos

1. Revise as informações fornecidas na página.
2. Se você quiser adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. Ver"Criar regra ILM" e"Usar políticas de ILM" .
3. Selecione **Eu revisei estas etapas e entendi o que preciso fazer**.
4. Marque a caixa de seleção para indicar que você entende o que fazer em seguida.
5. Selecione **Continuar** para ir para **Resumo**.

Etapa 6 de 6: Resumo da revisão

Passos

1. Revise o resumo.
2. Anote os detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de se conectar ao cliente S3. Por exemplo, selecionar * Sign in como root* leva você ao Gerenciador de locatários, onde você pode adicionar usuários locatários, criar buckets adicionais e atualizar as configurações de buckets.
3. Selecione **Concluir**.
4. Configure o aplicativo usando o arquivo que você baixou do StorageGRID ou os valores que você obteve manualmente.

Gerenciar grupos de HA

O que são grupos de alta disponibilidade (HA)?

Grupos de alta disponibilidade (HA) fornecem conexões de dados de alta disponibilidade para clientes S3 e conexões de alta disponibilidade para o Grid Manager e o Tenant Manager.

Você pode agrupar as interfaces de rede de vários nós de administração e gateway em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho.

Cada grupo HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Grupos de HA que incluem nós de gateway, nós de administração ou ambos fornecem conexões de dados de alta disponibilidade para clientes S3.
- Grupos de HA que incluem apenas nós de administração fornecem conexões de alta disponibilidade ao Grid Manager e ao Tenant Manager.
- Um grupo HA que inclui apenas dispositivos de serviços e nós de software baseados em VMware pode fornecer conexões de alta disponibilidade para"Locatários do S3 que usam o S3 Select" . Grupos HA são recomendados ao usar o S3 Select, mas não são obrigatórios.

Como criar um grupo HA?

1. Selecione uma interface de rede para um ou mais nós de administração ou nós de gateway. Você pode usar uma interface de rede de grade (eth0), uma interface de rede de cliente (eth2), uma interface de VLAN ou uma interface de acesso que você adicionou ao nó.

   > Não é possível adicionar uma interface a um grupo HA se ela tiver um endereço IP atribuído por DHCP.

2. Você especifica uma interface para ser a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.
3. Você determina a ordem de prioridade para qualquer interface de backup.
4. Você atribui de um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conectar ao StorageGRID.

Para obter instruções, consulte"Configurar grupos de alta disponibilidade" .

O que é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface primária, que é a primeira interface na ordem de prioridade. Enquanto a interface primária permanecer disponível, ela será usada quando os clientes se conectarem a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface primária é a interface "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade mais baixa para o grupo HA atuam como interfaces de "backup". Essas interfaces de backup não são usadas, a menos que a interface primária (atualmente ativa) fique indisponível.

Exibir o status atual do grupo HA de um nó

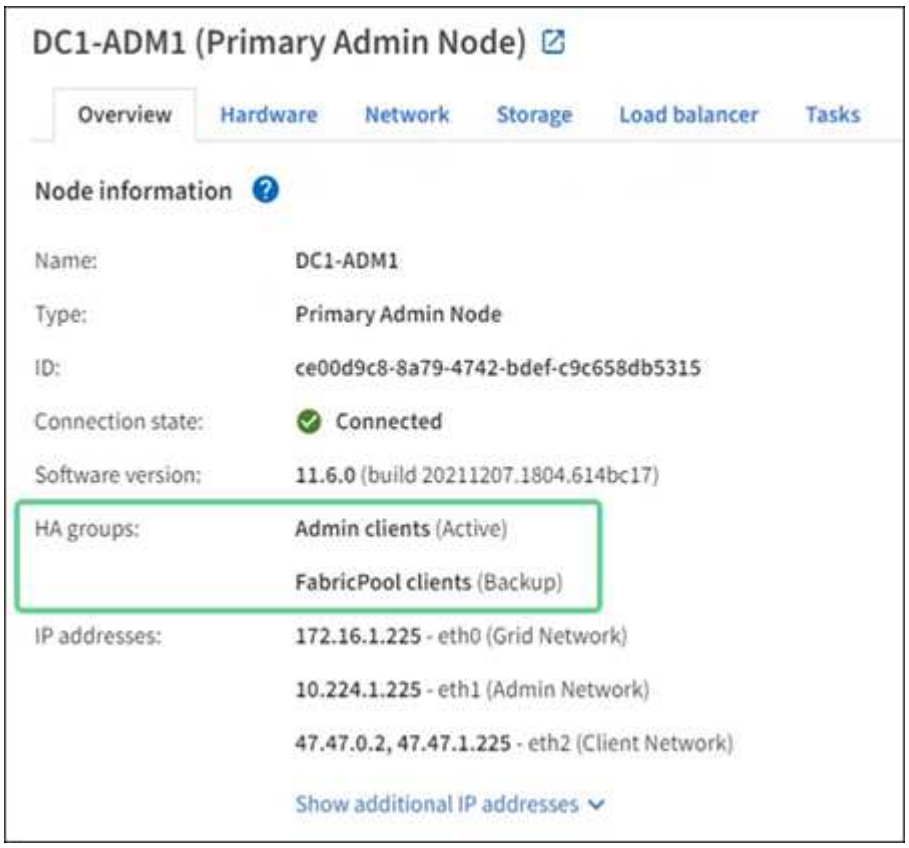
Para ver se um nó está atribuído a um grupo HA e determinar seu status atual, selecione **NODES** > ***node***.

Se a guia **Visão geral** incluir uma entrada para **grupos de HA**, o nó será atribuído aos grupos de HA listados. O valor após o nome do grupo é o status atual do nó no grupo HA:

- **Ativo**: O grupo HA está atualmente hospedado neste nó.
- **Backup**: O grupo HA não está usando este nó no momento; esta é uma interface de backup.
- **Interrompido**: O grupo HA não pode ser hospedado neste nó porque o serviço de Alta Disponibilidade (keepalived) foi interrompido manualmente.
- **Falha**: O grupo HA não pode ser hospedado neste nó devido a um ou mais dos seguintes motivos:
  - O serviço Load Balancer (nginx-gw) não está em execução no nó.
  - A interface eth0 ou VIP do nó está inativa.

◦ O nó está inativo.

Neste exemplo, o nó de administração principal foi adicionado a dois grupos de HA. Este nó é atualmente a interface ativa para o grupo de clientes Admin e uma interface de backup para o grupo de clientes FabricPool .



O que acontece quando a interface ativa falha?

A interface que atualmente hospeda os endereços VIP é a interface ativa. Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP serão movidos para a primeira interface de backup disponível na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup disponível e assim por diante.

O failover pode ser acionado por qualquer um destes motivos:

- O nó no qual a interface está configurada fica inativo.
- O nó no qual a interface está configurada perde a conectividade com todos os outros nós por pelo menos 2 minutos.
- A interface ativa fica inativa.
- O serviço Load Balancer é interrompido.
- O serviço de Alta Disponibilidade é interrompido.

> ⓘ O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pelos serviços do Grid Manager ou do Tenant Manager.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes sofram pouco impacto e possam contar com comportamentos normais de repetição para

continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta fica disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões de alta disponibilidade ao StorageGRID para dados de objetos e para uso administrativo.

- Um grupo HA pode fornecer conexões administrativas de alta disponibilidade ao Grid Manager ou ao Tenant Manager.
- Um grupo HA pode fornecer conexões de dados de alta disponibilidade para clientes S3.
- Um grupo HA que contém apenas uma interface permite que você forneça muitos endereços VIP e defina explicitamente endereços IPv6.

Um grupo HA pode fornecer alta disponibilidade somente se todos os nós incluídos no grupo fornecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços necessários.

- **Nós de administração**: inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Nós de gateway**: inclui o serviço Load Balancer.

Objetivo do grupo HA	Adicionar nós deste tipo ao grupo HA
Acesso ao Grid Manager	• Nó de administração primário (**Primário**) • Nós administrativos não primários **Observação:** O nó de administração principal deve ser a interface primária. Alguns procedimentos de manutenção só podem ser executados no nó de administração principal.
Acesso somente ao Gerenciador de Inquilinos	• Nós administrativos primários ou não primários
Acesso do cliente S3 — serviço de balanceador de carga	• Nós de administração • Nós de gateway
Acesso de cliente S3 para"Seleção S3"	• Aparelhos de serviços • Nós de software baseados em VMware **Observação**: grupos HA são recomendados ao usar o S3 Select, mas não são obrigatórios.

Limitações do uso de grupos HA com o Grid Manager ou o Tenant Manager

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

Se você estiver conectado ao Grid Manager ou ao Tenant Manager quando ocorrer o failover, você será

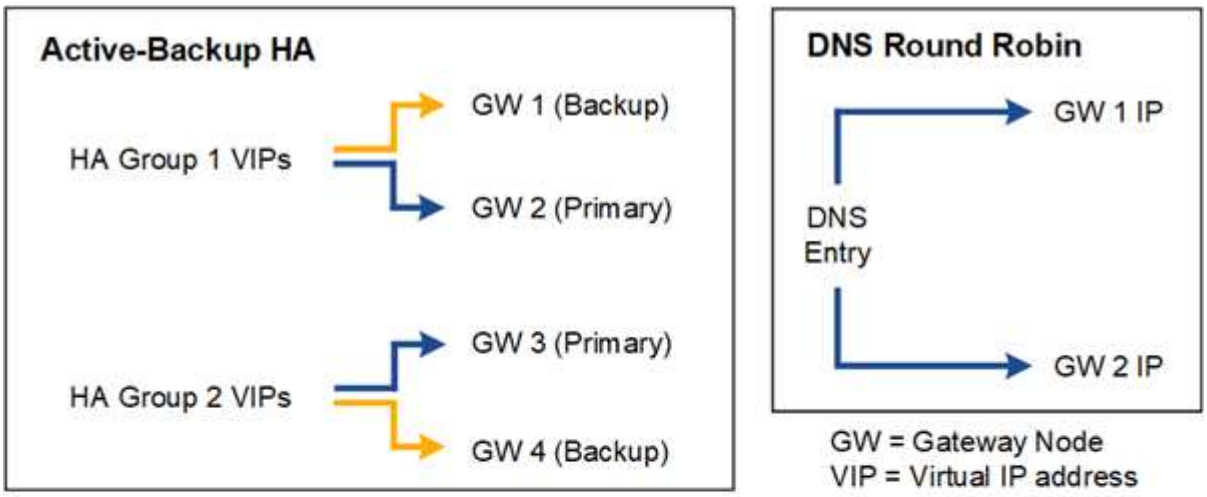
desconectado e deverá fazer login novamente para retomar sua tarefa.

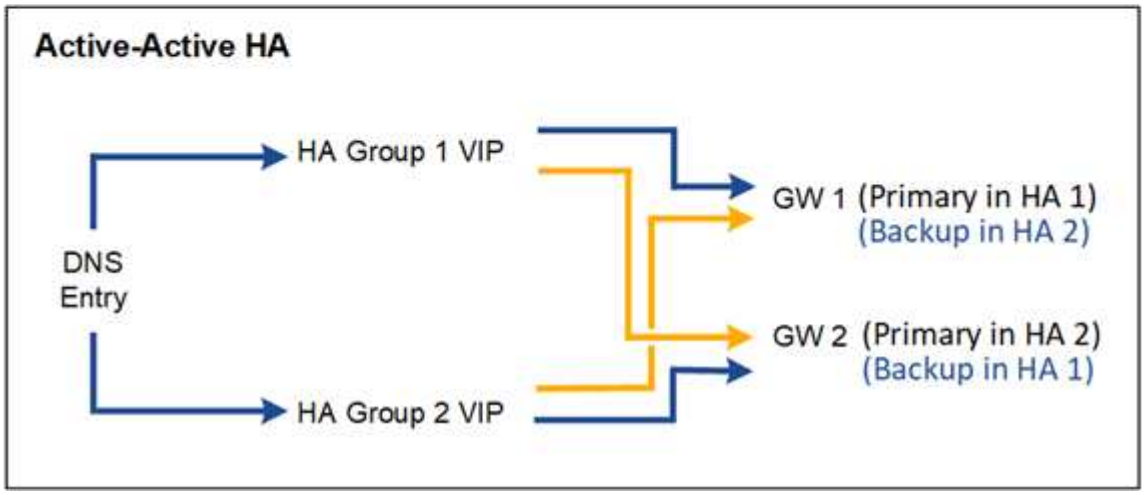
Alguns procedimentos de manutenção não podem ser executados quando o nó de administração principal não está disponível. Durante o failover, você pode usar o Grid Manager para monitorar seu sistema StorageGRID .

Opções de configuração para grupos HA

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de HA. Cada opção tem vantagens e desvantagens.

Nos diagramas, o azul indica a interface primária no grupo HA e o amarelo indica a interface de backup no grupo HA.





A tabela resume os benefícios de cada configuração de HA mostrada no diagrama.

Configuração	Vantagens	Desvantagens
HA de backup ativo	• Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido.	• Somente um nó em um grupo HA está ativo. Pelo menos um nó por grupo HA ficará ocioso.

Configuração	Vantagens	Desvantagens
DNS Round Robin	• Aumento do rendimento agregado. • Nenhum host ocioso.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.
HA ativo-ativo	• O tráfego é distribuído entre vários grupos de HA. • Alto rendimento agregado que pode ser dimensionado com o número de grupos HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade

Você pode configurar grupos de alta disponibilidade (HA) para fornecer acesso de alta disponibilidade aos serviços em nós de administração ou nós de gateway.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Se você planeja usar uma interface VLAN em um grupo HA, você criou a interface VLAN. Ver "Configurar interfaces VLAN" .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, você criou a interface:
  - **Red Hat Enterprise Linux (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **Ubuntu ou Debian (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **Linux (após instalar o nó)**:"Linux: Adicionar interfaces de tronco ou acesso a um nó"
  - **VMware (após instalar o nó)**:"VMware: Adicionar interfaces de tronco ou acesso a um nó"

Criar um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza em ordem de prioridade. Em seguida, você atribui um ou mais endereços VIP ao grupo.

Uma interface deve ser para um nó de gateway ou um nó de administração para ser incluído em um grupo de HA. Um grupo HA só pode usar uma interface para cada nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos HA.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Grupos de alta disponibilidade**.
2. Selecione **Criar**.

Insira detalhes para o grupo HA

Passos

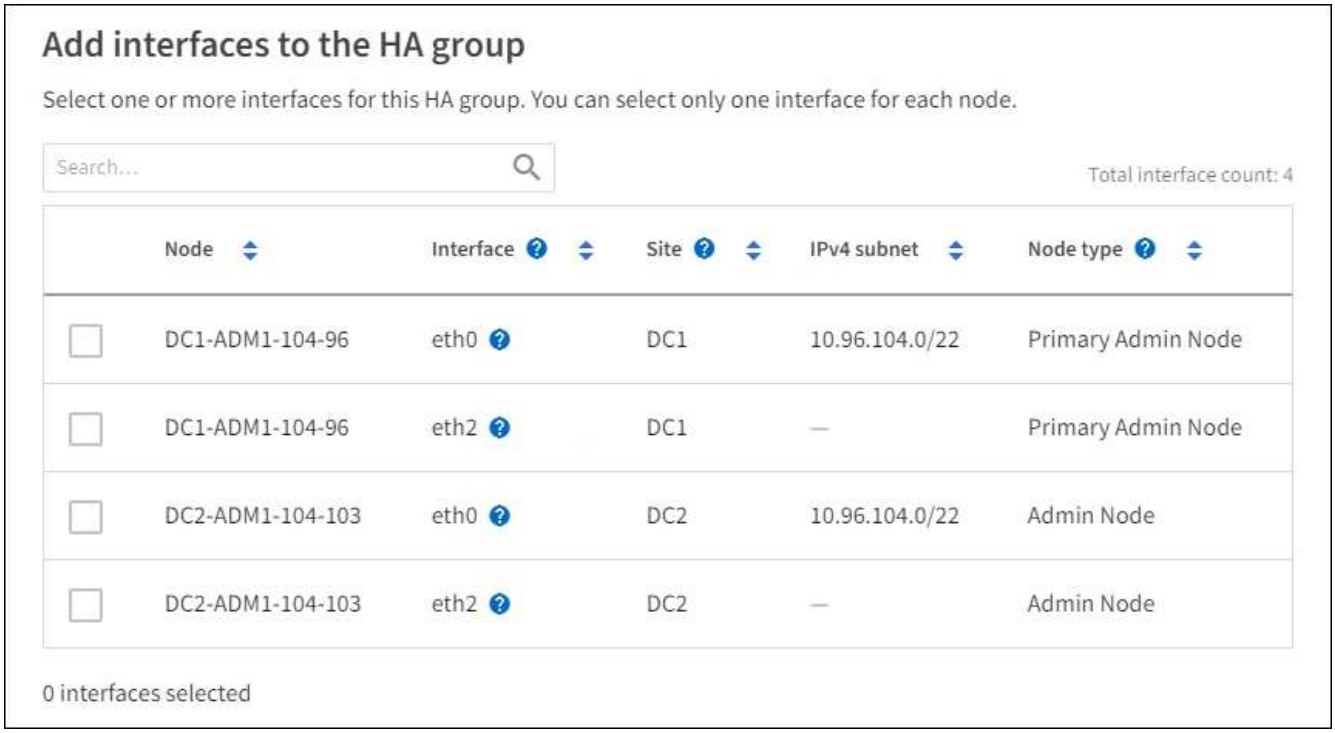
1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **Continuar**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a este grupo HA.

   Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.



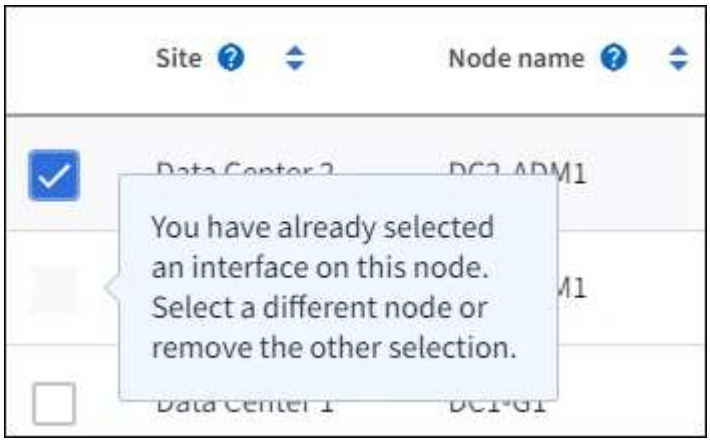
   Após criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo HA for para proteção HA dos serviços do nó administrativo, que incluem o Grid Manager e o Tenant Manager, selecione interfaces somente nos nós administrativos.
- Se o grupo HA for para proteção HA do tráfego do cliente S3, selecione interfaces em nós de administração, nós de gateway ou ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Lembre-se de que, se ocorrer um failover, os serviços fornecidos pelo nó ativo anteriormente podem não estar disponíveis no nó recém-ativo. Por exemplo, um nó de gateway de backup não pode fornecer proteção de alta disponibilidade dos serviços do nó de administração. Da mesma forma, um nó administrativo

de backup não pode executar todos os procedimentos de manutenção que o nó administrativo principal pode fornecer.

- Se você não puder selecionar uma interface, sua caixa de seleção estará desabilitada. A dica de ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o valor da sub-rede ou do gateway estiver em conflito com outra interface selecionada.
- Você não pode selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **Continuar**.

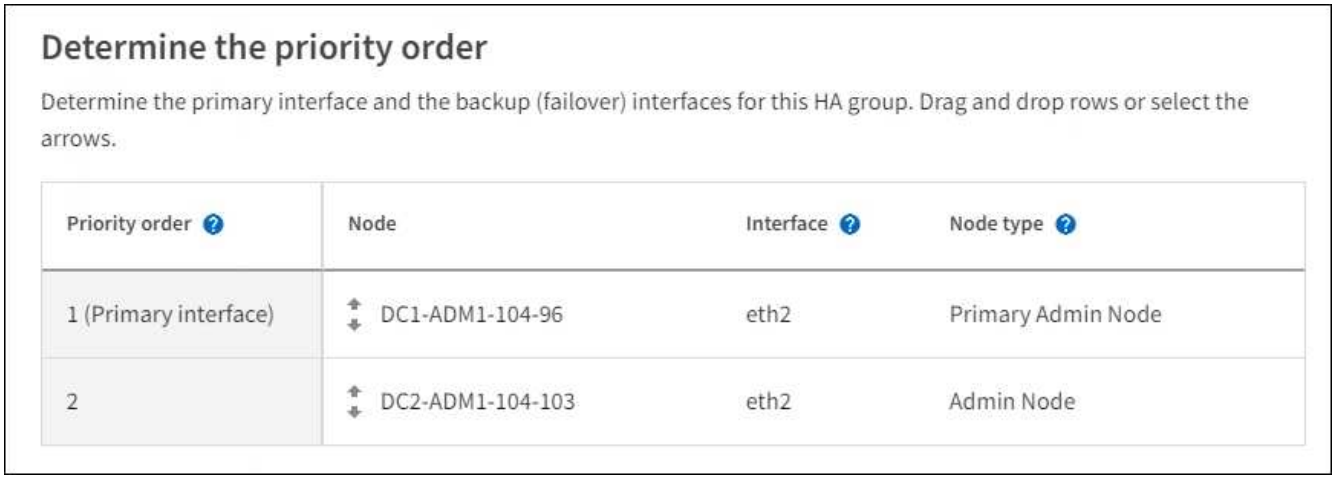
Determinar a ordem de prioridade

Se o grupo HA incluir mais de uma interface, você poderá determinar qual é a interface primária e quais são as interfaces de backup (failover). Se a interface primária falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de maior prioridade disponível, e assim por diante.

Passos

1. Arraste as linhas na coluna **Ordem de prioridade** para determinar a interface primária e quaisquer interfaces de backup.

   A primeira interface na lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.



Se o grupo HA fornecer acesso ao Grid Manager, você deverá selecionar uma interface no nó de administração principal para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados no nó de administração principal.

2. Selecione **Continuar**.

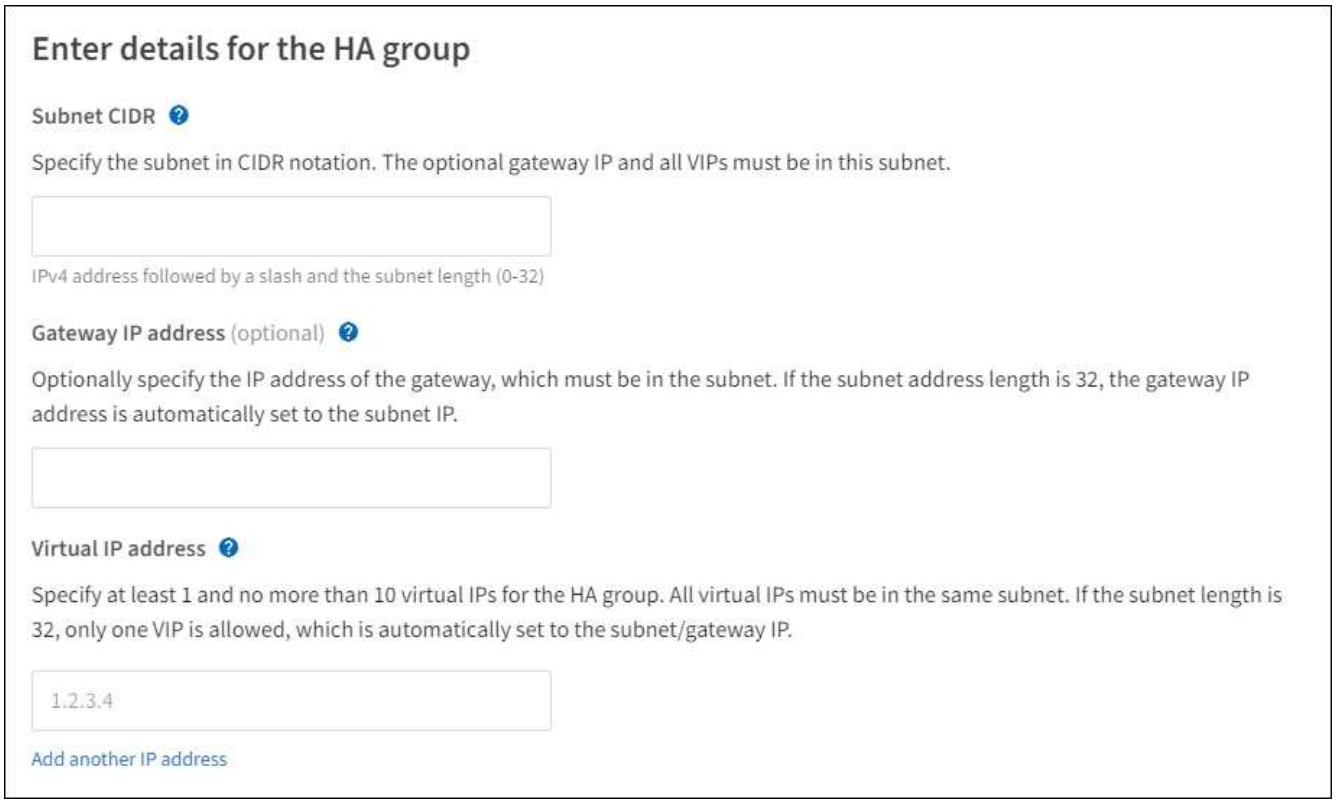
Insira endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR — um endereço IPv4 seguido por uma barra e o comprimento da sub-rede (0-32).

   O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.

   Se você usar um prefixo de 32 bits, o endereço de rede VIP também servirá como endereço de gateway e endereço VIP.



2. Opcionalmente, se algum cliente administrativo ou locatário do S3 acessar esses endereços VIP de uma sub-rede diferente, insira o **Endereço IP do gateway**. O endereço do gateway deve estar dentro da sub-rede VIP.

   Usuários clientes e administradores usarão esse gateway para acessar os endereços IP virtuais.

3. Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

4. Selecione **Criar grupo HA** e selecione **Concluir**.

   O Grupo HA foi criado e agora você pode usar os endereços IP virtuais configurados.

Próximos passos

Se você for usar esse grupo de HA para balanceamento de carga, crie um ponto de extremidade do balanceador de carga para determinar a porta e o protocolo de rede e anexar quaisquer certificados necessários. Ver "Configurar pontos de extremidade do balanceador de carga" .

Editar um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou atualizar endereços IP virtuais.

Por exemplo, talvez seja necessário editar um grupo de HA se você quiser remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Grupos de alta disponibilidade**.

   A página Grupos de alta disponibilidade mostra todos os grupos de alta disponibilidade existentes.

2. Marque a caixa de seleção do grupo HA que você deseja editar.
3. Faça um dos seguintes procedimentos, com base no que você deseja atualizar:
   - Selecione **Ações** > **Editar endereço IP virtual** para adicionar ou remover endereços VIP.
   - Selecione **Ações** > **Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
   a. Atualize os endereços IP virtuais para o grupo HA.
   b. Selecione **Salvar**.
   c. Selecione **Concluir**.
5. Se você selecionou **Editar grupo HA**:
   a. Opcionalmente, atualize o nome ou a descrição do grupo.
   b. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar ou remover interfaces.

      Se o grupo HA fornecer acesso ao Grid Manager, você deverá selecionar uma interface no nó de administração principal para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal

   c. Opcionalmente, arraste as linhas para alterar a ordem de prioridade da interface primária e de quaisquer interfaces de backup para este grupo de HA.
   d. Opcionalmente, atualize os endereços IP virtuais.
   e. Selecione **Salvar** e depois **Concluir**.

Remover um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) por vez.

Não é possível remover um grupo de HA se ele estiver vinculado a um ponto de extremidade do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de todos os pontos de extremidade do balanceador de carga que o utilizam.

Para evitar interrupções no cliente, atualize todos os aplicativos cliente S3 afetados antes de remover um grupo de HA. Atualize cada cliente para se conectar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP que foi configurado para uma interface durante a instalação.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Grupos de alta disponibilidade**.
2. Revise a coluna **Pontos de extremidade do balanceador de carga** para cada grupo de HA que você deseja remover. Se algum ponto de extremidade do balanceador de carga estiver listado:
   a. Vá para **CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga**.
   b. Marque a caixa de seleção do ponto de extremidade.
   c. Selecione **Ações** > **Editar modo de vinculação de ponto de extremidade**.
   d. Atualize o modo de vinculação para remover o grupo HA.
   e. Selecione **Salvar alterações**.
3. Se nenhum ponto de extremidade do balanceador de carga estiver listado, marque a caixa de seleção de cada grupo de HA que você deseja remover.
4. Selecione **Ações** > **Remover grupo HA**.
5. Revise a mensagem e selecione **Excluir grupo HA** para confirmar sua seleção.

   Todos os grupos de HA selecionados serão removidos. Um banner de sucesso verde aparece na página Grupos de alta disponibilidade.

Gerenciar balanceamento de carga

Considerações para balanceamento de carga

Você pode usar o balanceamento de carga para lidar com cargas de trabalho de ingestão e recuperação de clientes S3.

O que é balanceamento de carga?

Quando um aplicativo cliente salva ou recupera dados de um sistema StorageGRID , o StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de ingestão e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho entre vários nós de armazenamento.

O serviço StorageGRID Load Balancer é instalado em todos os nós de administração e todos os nós de gateway e fornece balanceamento de carga da Camada 7. Ele executa o encerramento de solicitações de clientes pelo protocolo TLS (Transport Layer Security), inspeciona as solicitações e estabelece novas conexões seguras com os nós de armazenamento.

O serviço Load Balancer em cada nó opera de forma independente ao encaminhar o tráfego do cliente para os nós de armazenamento. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de armazenamento com maior disponibilidade de CPU.

Embora o serviço StorageGRID Load Balancer seja o mecanismo de balanceamento de carga recomendado, talvez você queira integrar um balanceador de carga de terceiros. Para obter informações, entre em contato com seu representante de conta NetApp ou consulte "TR-4626: balanceadores de carga globais e de terceiros do StorageGRID" .

Quantos nós de balanceamento de carga eu preciso?

Como prática recomendada geral, cada site no seu sistema StorageGRID deve incluir dois ou mais nós com o serviço Load Balancer. Por exemplo, um site pode incluir dois nós de gateway ou um nó de administração e um nó de gateway. Certifique-se de que haja infraestrutura de rede, hardware ou virtualização adequada para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um ponto de extremidade do balanceador de carga?

Um ponto de extremidade do balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de entrada e saída do aplicativo cliente usarão para acessar os nós que contêm o serviço do balanceador de carga. O ponto de extremidade também define o tipo de cliente (S3), o modo de vinculação e, opcionalmente, uma lista de locatários permitidos ou bloqueados.

Para criar um ponto de extremidade do balanceador de carga, selecione **CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga** ou conclua o assistente de configuração do FabricPool e do S3. Para instruções:

- "Configurar pontos de extremidade do balanceador de carga"
- "Use o assistente de configuração do S3"
- "Use o assistente de configuração do FabricPool"

Considerações para o porto

A porta para um ponto de extremidade do balanceador de carga é definida como 10433 para o primeiro ponto de extremidade criado, mas você pode especificar qualquer porta externa não utilizada entre 1 e 65535. Se você usar a porta 80 ou 443, o ponto de extremidade usará o serviço Load Balancer somente nos nós de gateway. Essas portas são reservadas em nós de administração. Se você usar a mesma porta para mais de um ponto de extremidade, deverá especificar um modo de vinculação diferente para cada ponto de extremidade.

Portas usadas por outros serviços de rede não são permitidas. Veja o"Referência de porta de rede" .

Considerações sobre o protocolo de rede

Na maioria dos casos, as conexões entre aplicativos cliente e o StorageGRID devem usar criptografia TLS (Transport Layer Security). A conexão ao StorageGRID sem criptografia TLS é suportada, mas não recomendada, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga StorageGRID , você deve selecionar **HTTPS**.

Considerações sobre certificados de ponto de extremidade do balanceador de carga

Se você selecionar **HTTPS** como o protocolo de rede para o ponto de extremidade do balanceador de carga, deverá fornecer um certificado de segurança. Você pode usar qualquer uma destas três opções ao criar o ponto de extremidade do balanceador de carga:

- **Faça upload de um certificado assinado (recomendado)**. Este certificado pode ser assinado por uma

autoridade de certificação (CA) pública ou privada. Usar um certificado de servidor CA publicamente confiável para proteger a conexão é a melhor prática. Ao contrário dos certificados gerados, os certificados assinados por uma CA podem ser rotacionados sem interrupções, o que pode ajudar a evitar problemas de expiração.

Você deve obter os seguintes arquivos antes de criar o ponto de extremidade do balanceador de carga:

  - O arquivo de certificado do servidor personalizado.
  - O arquivo de chave privada do certificado do servidor personalizado.
  - Opcionalmente, um pacote de CA dos certificados de cada autoridade certificadora emissora intermediária.

- **Gerar um certificado autoassinado**.
- **Use o certificado global StorageGRID S3**. Você deve carregar ou gerar uma versão personalizada deste certificado antes de poder selecioná-lo para o ponto de extremidade do balanceador de carga. Ver "Configurar certificados da API S3" .

Quais valores eu preciso?

Para criar o certificado, você deve saber todos os nomes de domínio e endereços IP que os aplicativos cliente S3 usarão para acessar o ponto de extremidade.

A entrada **Subject DN** (Distinguished Name) do certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para StorageGRID. Por exemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conforme necessário, o certificado pode usar curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração e nós de gateway que executam o serviço do balanceador de carga. Por exemplo, `*.storagegrid.example.com` usa o curinga * para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com` .

Se você planeja usar solicitações de estilo de hospedagem virtual S3, o certificado também deve incluir uma entrada **Nome Alternativo** para cada"Nome de domínio do ponto de extremidade S3" que você configurou, incluindo quaisquer nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Se você usar curingas para nomes de domínio, revise o"Diretrizes de proteção para certificados de servidor" .

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados que estão expirando?

> Se o certificado usado para proteger a conexão entre o aplicativo S3 e o StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente todos os alertas que avisam sobre a aproximação das datas de expiração do certificado, como os alertas **Expiração do certificado de ponto de extremidade do balanceador de carga** e **Expiração do certificado do servidor global para a API S3**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá substituir certificados prestes a expirar sem interrupções.
- Se você gerou um certificado StorageGRID autoassinado e esse certificado estiver prestes a expirar, você deverá substituí-lo manualmente no StorageGRID e no aplicativo S3 antes que o certificado existente expire.

Considerações sobre o modo de ligação

O modo de vinculação permite controlar quais endereços IP podem ser usados para acessar um ponto de extremidade do balanceador de carga. Se um ponto de extremidade usar um modo de vinculação, os aplicativos clientes só poderão acessar o ponto de extremidade se usarem um endereço IP permitido ou seu nome de domínio totalmente qualificado (FQDN) correspondente. Aplicativos clientes que usam qualquer outro endereço IP ou FQDN não conseguem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de vinculação:

- **Global** (padrão): Os aplicativos cliente podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use esta configuração, a menos que você precise restringir a acessibilidade de um ponto de extremidade.
- **IPs virtuais de grupos HA**. Os aplicativos cliente devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA.
- **Interfaces de nó**. Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó**. Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway.

Considerações sobre acesso de inquilinos

O acesso do locatário é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um ponto de extremidade do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um ponto de extremidade (padrão) ou pode especificar uma lista de locatários permitidos ou bloqueados para cada ponto de extremidade.

Você pode usar esse recurso para fornecer melhor isolamento de segurança entre locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que os materiais ultrassecretos ou altamente confidenciais de propriedade de um inquilino permaneçam completamente inacessíveis a outros inquilinos.

Para fins de controle de acesso, o locatário é determinado a partir das chaves de acesso usadas na solicitação do cliente. Se nenhuma chave de acesso for fornecida como parte da solicitação (como no caso de acesso anônimo), o proprietário do bucket será usado para determinar o locatário.

Exemplo de acesso do inquilino

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade do balanceador de carga, como segue:
   - Ponto de extremidade **público**: usa a porta 10443 e permite acesso a todos os locatários.
   - Ponto de extremidade **Top Secret**: usa a porta 10444 e permite acesso somente ao locatário **Top Secret**. Todos os outros inquilinos estão bloqueados de acessar este ponto de extremidade.
2. O `top-secret.pdf` está em um balde de propriedade do inquilino **ultrassecreto**.

Para acessar o `top-secret.pdf` , um usuário no locatário **Top secret** pode emitir uma solicitação GET para `https://w.x.y.z:10444/top-secret.pdf` . Como esse locatário tem permissão para usar o ponto de extremidade 10444, o usuário pode acessar o objeto. Entretanto, se um usuário pertencente a qualquer outro locatário emitir a mesma solicitação para o mesmo URL, ele receberá imediatamente uma mensagem de Acesso Negado. O acesso é negado mesmo que as credenciais e a assinatura sejam válidas.

Disponibilidade da CPU

O serviço Load Balancer em cada nó de administração e nó de gateway opera de forma independente ao encaminhar o tráfego S3 para os nós de armazenamento. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de armazenamento com maior disponibilidade de CPU. As informações de carga da CPU do nó são atualizadas a cada poucos minutos, mas a ponderação pode ser atualizada com mais frequência. Todos os nós de armazenamento recebem um valor mínimo de peso base, mesmo que um nó relate 100% de utilização ou não relate sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU são limitadas ao site onde o serviço Load Balancer está localizado.

Configurar pontos de extremidade do balanceador de carga

Os pontos de extremidade do balanceador de carga determinam as portas e os protocolos de rede que os clientes S3 podem usar ao se conectar ao balanceador de carga StorageGRID nos nós de gateway e de administração. Você também pode usar endpoints para acessar o Grid Manager, o Tenant Manager ou ambos.

Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "Configurar conexões de cliente S3 e Swift" .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Você revisou o"considerações para balanceamento de carga" .
- Se você remapeou anteriormente uma porta que pretende usar para o ponto de extremidade do balanceador de carga, você tem"removeu o remapeamento da porta" .

- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Grupos HA são recomendados, mas não obrigatórios. Ver "Gerenciar grupos de alta disponibilidade" .
- Se o ponto de extremidade do balanceador de carga for usado por"Inquilinos S3 para S3 Select" , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos de serviços e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.
- Você configurou todas as interfaces VLAN que planeja usar. Ver "Configurar interfaces VLAN" .
- Se estiver criando um ponto de extremidade HTTPS (recomendado), você terá as informações para o certificado do servidor.

> Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

  - Para carregar um certificado, você precisa do certificado do servidor, da chave privada do certificado e, opcionalmente, de um pacote de CA.
  - Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 usarão para acessar o ponto de extremidade. Você também deve conhecer o assunto (Nome Distinto).
  - Se você quiser usar o certificado StorageGRID S3 API (que também pode ser usado para conexões diretas com nós de armazenamento), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. Ver "Configurar certificados da API S3" .

Criar um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga do cliente S3 especifica uma porta, um tipo de cliente (S3) e um protocolo de rede (HTTP ou HTTPS). Os pontos de extremidade do balanceador de carga da interface de gerenciamento especificam uma porta, um tipo de interface e uma rede de cliente não confiável.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga**.
2. Para criar um ponto de extremidade para um cliente S3 ou Swift, selecione a guia **Cliente S3 ou Swift**.
3. Para criar um ponto de extremidade para acesso ao Grid Manager, ao Tenant Manager ou a ambos, selecione a guia **Interface de gerenciamento**.
4. Selecione **Criar**.

Insira os detalhes do ponto de extremidade

Passos

1. Selecione as instruções apropriadas para inserir detalhes sobre o tipo de ponto de extremidade que você deseja criar.

Cliente S3 ou Swift

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página Endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você digitar **80** ou **8443**, o ponto de extremidade será configurado somente em nós de gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um ponto de extremidade S3, e a porta será configurada nos nós de gateway e de administração.
Tipo de cliente	O tipo de aplicativo cliente que usará este ponto de extremidade, **S3** ou **Swift**.
Protocolo de rede	O protocolo de rede que os clientes usarão ao se conectar a este ponto de extremidade. • Selecione **HTTPS** para comunicação segura e criptografada por TLS (recomendado). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione **HTTP** para comunicação menos segura e não criptografada. Use HTTP somente para uma grade não produtiva.

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página Endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Grid Manager, o Tenant Manager ou ambos. • Gerente de grade: **8443** • Gerente de inquilinos: **9443** • Gerente de Rede e Gerente de Inquilino: **443** **Observação**: Você pode usar essas portas predefinidas ou outras portas disponíveis.
Tipo de interface	Selecione o botão de opção para a interface StorageGRID que você acessará usando este ponto de extremidade.

Campo	Descrição
Rede de clientes não confiáveis	Selecione **Sim** se este ponto de extremidade deve ser acessível a redes de clientes não confiáveis. Caso contrário, selecione **Não**. Quando você seleciona **Sim**, a porta é aberta em todas as redes de clientes não confiáveis. **Observação**: você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis ao criar o ponto de extremidade do balanceador de carga.

1. Selecione **Continuar**.

Selecione um modo de encadernação

Passos

1. Selecione um modo de vinculação para o ponto de extremidade para controlar como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

   Alguns modos de vinculação estão disponíveis para terminais de cliente ou terminais de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints do cliente)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global**, a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó (somente terminais do cliente)	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

Modo	Descrição
Todos os nós de administração (padrão para terminais de interface de gerenciamento)	Os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração para acessar este ponto de extremidade.

Se mais de um ponto de extremidade usar a mesma porta, o StorageGRID usará esta ordem de prioridade para decidir qual ponto de extremidade usar: **IPs virtuais de grupos de HA** > **Interfaces de nó** > **Tipo de nó** > **Global**.

Se você estiver criando pontos de extremidade de interface de gerenciamento, somente nós de administração serão permitidos.

2. Se você selecionou **IPs virtuais de grupos HA**, selecione um ou mais grupos HA.

   Se você estiver criando endpoints de interface de gerenciamento, selecione VIPs associados somente a nós de administração.

3. Se você selecionou **Interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administração ou nó de gateway que deseja associar a este ponto de extremidade.
4. Se você selecionou **Tipo de nó**, selecione Nós de administração, que inclui o Nó de administração primário e quaisquer Nós de administração não primários, ou Nós de gateway.

Controlar o acesso do inquilino

Um ponto de extremidade da interface de gerenciamento pode controlar o acesso do locatário somente quando o ponto de extremidade tem otipo de interface do Gerenciador de Inquilinos .

Passos

1. Para a etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse endpoint para acessar seus buckets. Você deve selecionar esta opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o ponto de extremidade do balanceador de carga para permitir ou bloquear contas específicas.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

2. Se você estiver criando um ponto de extremidade **HTTP**, não precisará anexar um certificado. Selecione

Criar para adicionar o novo ponto de extremidade do balanceador de carga. Então vá paraDepois que você terminar . Caso contrário, selecione **Continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um ponto de extremidade **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao ponto de extremidade.

   O certificado protege as conexões entre clientes S3 e o serviço Load Balancer no nó de administração ou nos nós de gateway.

   - **Carregar certificado**. Selecione esta opção se você tiver certificados personalizados para carregar.
   - **Gerar certificado**. Selecione esta opção se você tiver os valores necessários para gerar um certificado personalizado.
   - **Use o certificado StorageGRID S3**. Selecione esta opção se quiser usar o certificado global da API S3, que também pode ser usado para conexões diretas com nós de armazenamento.

     Você não pode selecionar esta opção a menos que tenha substituído o certificado padrão da API S3, que é assinado pela CA da grade, por um certificado personalizado assinado por uma autoridade de certificação externa. Ver "Configurar certificados da API S3" .

   - **Usar certificado de interface de gerenciamento**. Selecione esta opção se quiser usar o certificado da interface de gerenciamento global, que também pode ser usado para conexões diretas com nós de administração.
2. Se você não estiver usando o certificado StorageGRID S3, carregue ou gere o certificado.

Carregar certificado

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

- **Certificado do servidor**: O arquivo de certificado do servidor personalizado na codificação PEM.
- **Chave privada do certificado**: O arquivo de chave privada do certificado do servidor personalizado(`.key`).

> As chaves privadas da EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora intermediária emissora (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem` .

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

d. Selecione **Criar**. + O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e o ponto de extremidade.

Gerar certificado

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a serem incluídos no certificado.
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).

Campo	Descrição
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Observação**: deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

  Especifique o nome do arquivo do certificado e o local do download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Criar**.

O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e este ponto de extremidade.

Depois que você terminar

Passos

1. Se você usar um DNS, certifique-se de que o DNS inclua um registro para associar o nome de domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para fazer conexões.

   O endereço IP inserido no registro DNS depende se você está usando um grupo HA de nós de balanceamento de carga:

   - Se você tiver configurado um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
   - Se você não estiver usando um grupo HA, os clientes se conectarão ao serviço StorageGRID Load Balancer usando o endereço IP de um nó de gateway ou nó de administrador.

     Você também deve garantir que o registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes curinga.

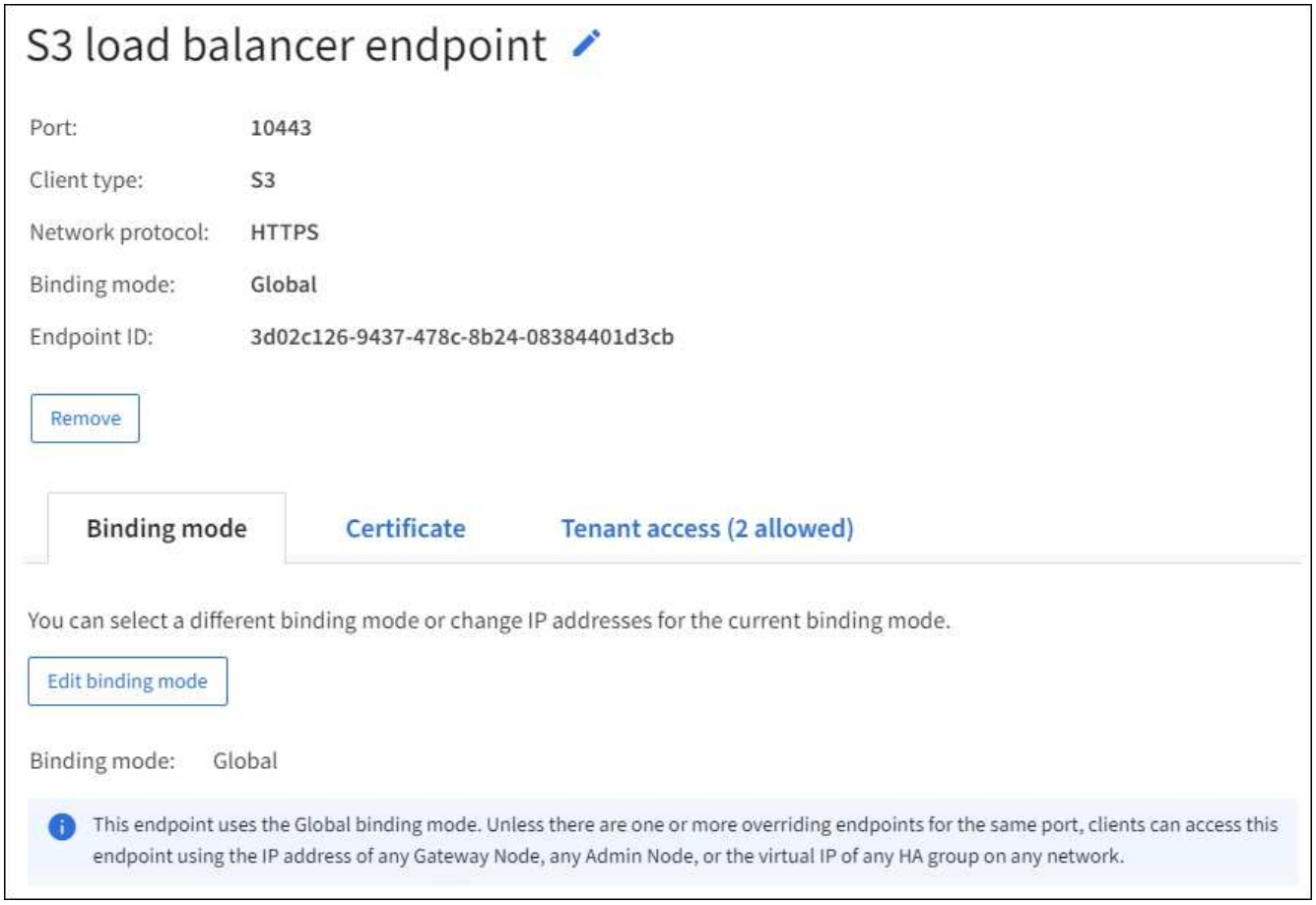
2. Forneça aos clientes S3 as informações necessárias para se conectar ao ponto de extremidade:

- Número da porta
- Nome de domínio totalmente qualificado ou endereço IP
- Quaisquer detalhes do certificado necessários

Visualizar e editar pontos de extremidade do balanceador de carga

Você pode visualizar detalhes dos pontos de extremidade do balanceador de carga existentes, incluindo os metadados do certificado para um ponto de extremidade protegido. Você pode alterar determinadas configurações de um ponto de extremidade.

- Para visualizar informações básicas de todos os pontos de extremidade do balanceador de carga, revise as tabelas na página Pontos de extremidade do balanceador de carga.
- Para visualizar todos os detalhes sobre um ponto de extremidade específico, incluindo metadados do certificado, selecione o nome do ponto de extremidade na tabela. As informações mostradas variam dependendo do tipo de endpoint e de como ele está configurado.



- Para editar um endpoint, use o menu **Ações** na página Endpoints do balanceador de carga.

> Se você perder o acesso ao Grid Manager ao editar a porta de um ponto de extremidade da interface de gerenciamento, atualize o URL e a porta para recuperar o acesso.

> Depois de editar um ponto de extremidade, pode ser necessário esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu de ações	Página de detalhes
Editar nome do ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione **Ações** > **Editar nome do ponto de extremidade**. c. Digite o novo nome. d. Selecione **Salvar**.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Salvar**.
Editar porta do ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione **Ações** > **Editar porta do ponto de extremidade** c. Digite um número de porta válido. d. Selecione **Salvar**.	*n / D*
Editar modo de vinculação de ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione **Ações** > **Editar modo de vinculação de ponto de extremidade**. c. Atualize o modo de vinculação conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione **Editar modo de vinculação**. c. Atualize o modo de vinculação conforme necessário. d. Selecione **Salvar alterações**.
Editar certificado de ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione **Ações** > **Editar certificado de ponto de extremidade**. c. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione a aba **Certificado**. c. Selecione **Editar certificado**. d. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. e. Selecione **Salvar alterações**.

Tarefa	Menu de ações	Página de detalhes
Editar acesso do locatário	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione **Ações** > **Editar acesso do locatário**. c. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça as duas coisas. d. Selecione **Salvar alterações**.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione a aba **Acesso do locatário**. c. Selecione **Editar acesso do locatário**. d. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça as duas coisas. e. Selecione **Salvar alterações**.

Remover pontos de extremidade do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **Ações** ou pode remover um único endpoint da página de detalhes.

> Para evitar interrupções no cliente, atualize todos os aplicativos cliente S3 afetados antes de remover um ponto de extremidade do balanceador de carga. Atualize cada cliente para se conectar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Não se esqueça de atualizar também todas as informações necessárias do certificado.

> Se você perder o acesso ao Grid Manager ao remover um ponto de extremidade da interface de gerenciamento, atualize o URL.

- Para remover um ou mais pontos de extremidade:
  a. Na página Balanceador de carga, marque a caixa de seleção de cada endpoint que deseja remover.
  b. Selecione **Ações** > **Remover**.
  c. Selecione **OK**.
- Para remover um ponto de extremidade da página de detalhes:
  a. Na página Balanceador de carga, selecione o nome do endpoint.
  b. Selecione **Remover** na página de detalhes.
  c. Selecione **OK**.

Configurar nomes de domínio de endpoint S3

Para dar suporte a solicitações de estilo de hospedagem virtual do S3, você deve usar o Grid Manager para configurar a lista de nomes de domínio de endpoint do S3 aos quais os clientes do S3 se conectam.

> Não há suporte para o uso de um endereço IP para um nome de domínio de ponto de extremidade. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você confirmou que uma atualização de rede não está em andamento.

> Não faça nenhuma alteração na configuração do nome de domínio quando uma atualização de grade estiver em andamento.

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de ponto de extremidade S3, você deve fazer tudo o seguinte:

- Use o Grid Manager para adicionar os nomes de domínio do endpoint S3 ao sistema StorageGRID .
- Assegurar que o"certificado que o cliente usa para conexões HTTPS com o StorageGRID" é assinado para todos os nomes de domínio que o cliente requer.

  Por exemplo, se o ponto final for `s3.company.com` , você deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` ponto de extremidade e o nome alternativo do assunto (SAN) curinga do ponto de extremidade: `*.s3.company.com` .

- Configure o servidor DNS usado pelo cliente. Inclua registros DNS para os endereços IP que os clientes usam para fazer conexões e garanta que os registros façam referência a todos os nomes de domínio de ponto de extremidade S3 necessários, incluindo quaisquer nomes curinga.

> Os clientes podem se conectar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administração ou um nó de armazenamento, ou conectando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos clientes se conectam à grade para incluir os endereços IP corretos nos registros DNS.

Clientes que usam conexões HTTPS (recomendado) para a grade podem usar qualquer um destes certificados:

- Clientes que se conectam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de ponto de extremidade S3.
- Os clientes que se conectam a um ponto de extremidade do balanceador de carga ou diretamente a um nó de armazenamento podem personalizar o certificado global da API do S3 para incluir todos os nomes de domínio de ponto de extremidade do S3 necessários.

> Se você não adicionar nomes de domínio de ponto de extremidade S3 e a lista estiver vazia, o suporte para solicitações de estilo de hospedagem virtual S3 será desabilitado.

Adicionar um nome de domínio de ponto de extremidade S3

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Nomes de domínio de ponto de extremidade S3**.
2. Digite o nome do domínio no campo **Nome de domínio 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.

3. Selecione **Salvar**.
4. Certifique-se de que os certificados do servidor usados pelos clientes correspondam aos nomes de domínio do ponto de extremidade S3 necessários.
   - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que usa seu próprio certificado,"atualizar o certificado associado ao ponto de extremidade" .
   - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que usa o certificado global da API S3 ou diretamente aos nós de armazenamento,"atualizar o certificado global da API S3" .
5. Adicione os registros DNS necessários para garantir que as solicitações de nome de domínio do endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o ponto de extremidade `bucket.s3.company.com` , o servidor DNS resolve para o ponto de extremidade correto e o certificado autentica o ponto de extremidade conforme o esperado.

Renomear um nome de domínio de ponto de extremidade S3

Se você alterar um nome usado pelos aplicativos S3, as solicitações no estilo de hospedagem virtual falharão.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Nomes de domínio de ponto de extremidade S3**.
2. Selecione o campo de nome de domínio que deseja editar e faça as alterações necessárias.
3. Selecione **Salvar**.
4. Selecione **Sim** para confirmar sua alteração.

Excluir um nome de domínio de ponto de extremidade S3

Se você remover um nome usado por aplicativos S3, as solicitações no estilo de hospedagem virtual falharão.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Nomes de domínio de ponto de extremidade S3**.
2. Selecione o ícone de exclusão ❌ ao lado do nome do domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- "Usar API REST do S3"
- "Ver endereços IP"
- "Configurar grupos de alta disponibilidade"

Resumo: Endereços IP e portas para conexões de clientes

Para armazenar ou recuperar objetos, os aplicativos cliente S3 se conectam ao serviço Load Balancer, que está incluído em todos os nós de administração e nós de gateway, ou ao serviço Local Distribution Router (LDR), que está incluído em todos os nós de armazenamento.

Os aplicativos cliente podem se conectar ao StorageGRID usando o endereço IP de um nó de grade e o

número da porta do serviço nesse nó. Opcionalmente, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões de alta disponibilidade que usam endereços IP virtuais (VIP). Se você quiser se conectar ao StorageGRID usando um nome de domínio totalmente qualificado (FQDN) em vez de um endereço IP ou VIP, você pode configurar entradas de DNS.

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conectar ao StorageGRID e os endereços IP e portas usados para cada tipo de conexão. Se você já criou endpoints do balanceador de carga e grupos de alta disponibilidade (HA), consulteOnde encontrar endereços IP para localizar esses valores no Grid Manager.

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de administração	Balanceador de carga	Endereço IP do nó de administração	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de armazenamento	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

URLs de exemplo

Para conectar um aplicativo cliente ao ponto de extremidade do balanceador de carga de um grupo HA de nós de gateway, use uma URL estruturada conforme mostrado abaixo:

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

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta do ponto de extremidade do balanceador de carga for 10443, um aplicativo poderá usar a seguinte URL para se conectar ao StorageGRID:

`https://192.0.2.5:10443`

Onde encontrar endereços IP

1. Sign in no Grid Manager usando um"navegador da web compatível" .
2. Para encontrar o endereço IP de um nó de grade:
   a. Selecione **NODES**.
   b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual você deseja se conectar.

c. Selecione a aba **Visão geral**.

d. Na seção Informações do nó, observe os endereços IP do nó.

e. Selecione **Mostrar mais** para visualizar endereços IPv6 e mapeamentos de interface.

Você pode estabelecer conexões de aplicativos clientes para qualquer um dos endereços IP na lista:

- **eth0:** Rede de grade
- **eth1:** Rede de administração (opcional)
- **eth2:** Rede do cliente (opcional)

> Se você estiver visualizando um nó de administração ou um nó de gateway e ele for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de alta disponibilidade será mostrado em eth2.

3. Para encontrar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **CONFIGURAÇÃO** > **Rede** > **Grupos de alta disponibilidade**.
   b. Na tabela, observe o endereço IP virtual do grupo HA.
4. Para encontrar o número da porta de um ponto de extremidade do Load Balancer:
   a. Selecione **CONFIGURAÇÃO** > **Rede** > **Pontos de extremidade do balanceador de carga**.
   b. Anote o número da porta do ponto de extremidade que você deseja usar.

> Se o número da porta for 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway, porque essas portas são reservadas em nós de administração. Todas as outras portas são configuradas nos nós de gateway e nos nós de administração.

   c. Selecione o nome do ponto de extremidade na tabela.
   d. Confirme se o **Tipo de cliente** (S3) corresponde ao aplicativo cliente que usará o ponto de extremidade.

Gerenciar redes e conexões

Configurar as configurações de rede

Você pode configurar várias configurações de rede no Grid Manager para ajustar a operação do seu sistema StorageGRID .

Configurar interfaces VLAN

Você pode"criar interfaces de LAN virtual (VLAN)" para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Cada interface VLAN está associada a uma ou mais interfaces pai em nós de administração e nós de gateway. Você pode usar interfaces VLAN em grupos de HA e em pontos de extremidade do balanceador de carga para segregar o tráfego de cliente ou administrador por aplicativo ou locatário.

Políticas de classificação de tráfego

Você pode usar"políticas de classificação de tráfego" para identificar e manipular diferentes tipos de tráfego de rede, incluindo tráfego relacionado a buckets específicos, locatários, sub-redes de clientes ou pontos de extremidade do balanceador de carga. Essas políticas podem ajudar a limitar e monitorar o tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Grid Manager para configurar e gerenciar redes e conexões do StorageGRID .

Ver"Configurar conexões do cliente S3" para aprender como conectar clientes S3.

Redes StorageGRID padrão

Por padrão, o StorageGRID oferece suporte a três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual para atender aos seus requisitos de segurança e acesso.

Para obter mais informações sobre topologia de rede, consulte"Diretrizes de rede" .

Rede de grade

Obrigatório. A Grid Network é usada para todo o tráfego interno do StorageGRID . Ele fornece conectividade entre todos os nós na grade, em todos os sites e sub-redes.

Rede de administração

Opcional. A rede de administração é normalmente usada para administração e manutenção do sistema. Ele também pode ser usado para acesso ao protocolo do cliente. A rede de administração normalmente é uma rede privada e não precisa ser roteável entre sites.

Rede de clientes

Opcional. A Rede do Cliente é uma rede aberta normalmente usada para fornecer acesso a aplicativos cliente S3, para que a Rede Grid possa ser isolada e protegida. A Rede do Cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

Diretrizes

- Cada nó StorageGRID requer uma interface de rede dedicada, endereço IP, máscara de sub-rede e gateway para cada rede à qual é atribuído.
- Um nó de grade não pode ter mais de uma interface em uma rede.
- Um único gateway, por rede, por nó de grade é suportado e deve estar na mesma sub-rede que o nó. Você pode implementar um roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede é mapeada para uma interface de rede específica.

Rede	Nome da interface
Grade	eth0
Administrador (opcional)	eth1

Rede	Nome da interface
Cliente (opcional)	eth2

- Se o nó estiver conectado a um dispositivo StorageGRID , portas específicas serão usadas para cada rede. Para mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se eth2 estiver habilitado, então 0.0.0.0/0 usa a Rede do Cliente em eth2. Se eth2 não estiver habilitado, então 0.0.0.0/0 usa a Grid Network em eth0.
- A Rede do Cliente não se torna operacional até que o nó da rede se junte à rede
- A rede de administração pode ser configurada durante a implantação do nó da grade para permitir acesso à interface do usuário de instalação antes que a grade esteja totalmente instalada.

Interfaces opcionais

Opcionalmente, você pode adicionar interfaces extras a um nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó de administração ou gateway, para que possa usar"Interfaces VLAN" para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou você pode querer adicionar uma interface de acesso para usar em um"grupo de alta disponibilidade (HA)" .

Para adicionar interfaces de tronco ou acesso, consulte o seguinte:

- **VMware (após instalar o nó)**:"VMware: Adicionar interfaces de tronco ou acesso a um nó"
  - **Red Hat Enterprise Linux (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **Ubuntu ou Debian (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **RHEL, Ubuntu ou Debian (após instalar o nó)**:"Linux: Adicionar interfaces de tronco ou acesso a um nó"

Ver endereços IP

Você pode visualizar o endereço IP de cada nó de grade no seu sistema StorageGRID . Você pode então usar esse endereço IP para efetuar login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

Antes de começar

Você está conectado ao Grid Manager usando um"navegador da web compatível" .

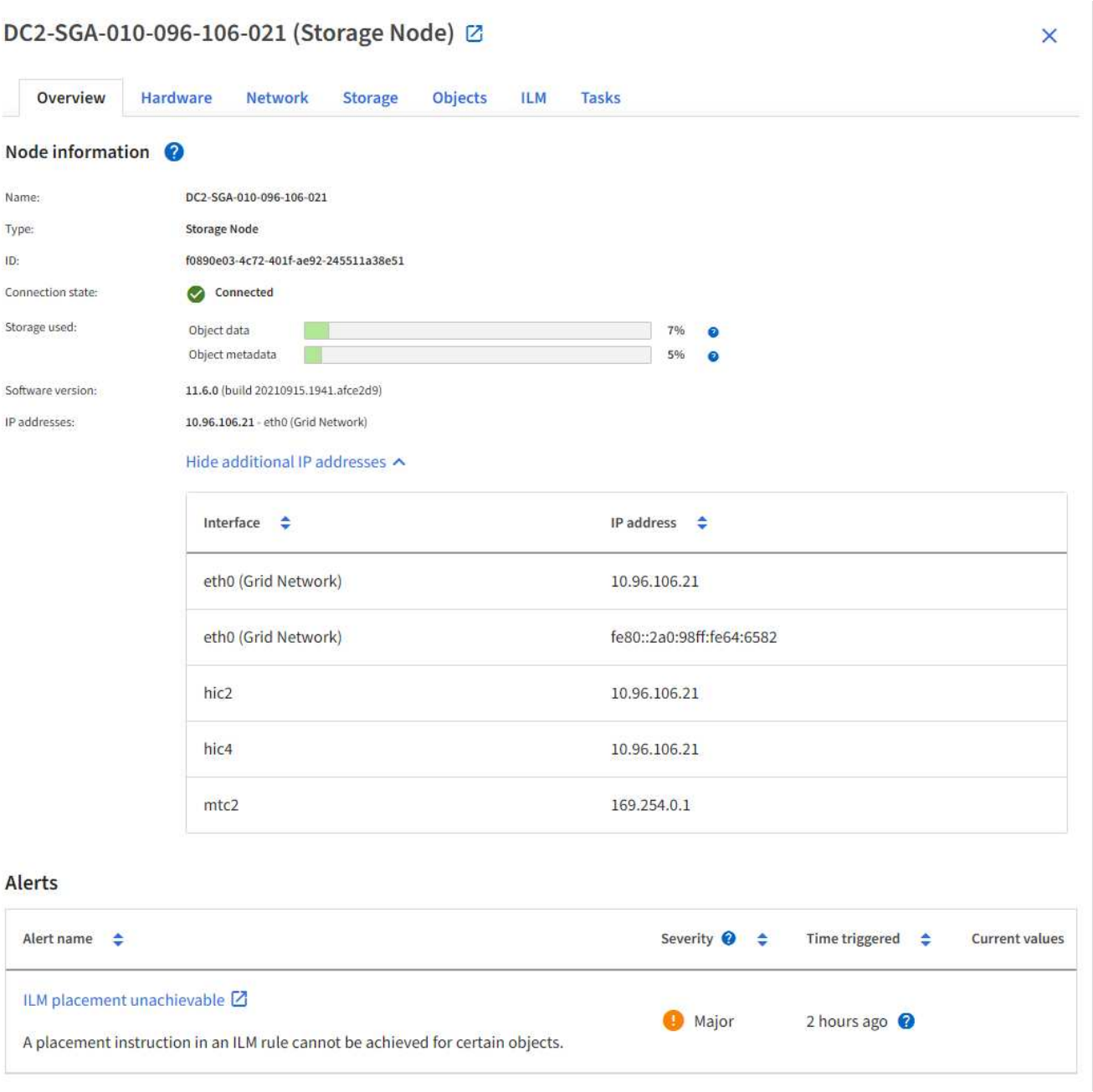
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte"Configurar endereços IP" .

Passos

1. Selecione **NÓS** > ***nó da grade*** > **Visão geral**.
2. Selecione **Mostrar mais** à direita do título Endereços IP.

   Os endereços IP para esse nó de grade são listados em uma tabela.



Configurar interfaces VLAN

Você pode criar interfaces de LAN virtual (VLAN) em nós de administração e nós de gateway e usá-las em grupos de HA e pontos de extremidade do balanceador de carga para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Os nós selecionados no grupo HA podem usar as interfaces VLAN para compartilhar até 10 endereços IP virtuais, de modo que, se um nó cair, outro nó assume o tráfego de e para os endereços IP virtuais.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo uma ID de VLAN e escolhendo uma interface pai em um ou mais nós.

- Uma interface pai deve ser configurada como uma interface de tronco no switch.
- Uma interface pai pode ser a Rede de Grade (eth0), a Rede do Cliente (eth2) ou uma interface de tronco adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface pai para um determinado nó. Por exemplo, você não pode usar a interface de rede de grade e a interface de rede do cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego do nó de administração, o que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces somente nos nós de administração.
- Se a interface VLAN for para tráfego de cliente S3, selecione interfaces em Nós de administração ou Nós de gateway.
- Se você precisar adicionar interfaces de tronco, veja o seguinte para obter detalhes:
  - **VMware (após instalar o nó)**:"VMware: Adicionar interfaces de tronco ou acesso a um nó"
  - **RHEL (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **Ubuntu ou Debian (antes de instalar o nó)**:"Criar arquivos de configuração de nó"
  - **RHEL, Ubuntu ou Debian (após instalar o nó)**:"Linux: Adicionar interfaces de tronco ou acesso a um nó"

Criar uma interface VLAN

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Uma interface de tronco foi configurada na rede e anexada à VM ou ao nó Linux. Você sabe o nome da interface do tronco.
- Você sabe o ID da VLAN que está configurando.

Sobre esta tarefa

O administrador da rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego do cliente ou do administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar a VLAN 100 para tráfego do FabricPool e a VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Grid Manager para criar interfaces de VLAN que permitem que clientes acessem o StorageGRID em uma VLAN específica. Ao criar interfaces de VLAN, você especifica o ID da VLAN e seleciona interfaces pai (tronco) em um ou mais nós.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Interfaces VLAN**.
2. Selecione **Criar**.

Insira detalhes para as interfaces VLAN

Passos

1. Especifique o ID da VLAN na sua rede. Você pode inserir qualquer valor entre 1 e 4094.

   Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar a ID de VLAN 200 para

tráfego de administrador em um site e a mesma ID de VLAN para tráfego de cliente em outro site. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada site. No entanto, duas interfaces VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó. Se você especificar um ID que já foi usado, uma mensagem será exibida.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **Continuar**.

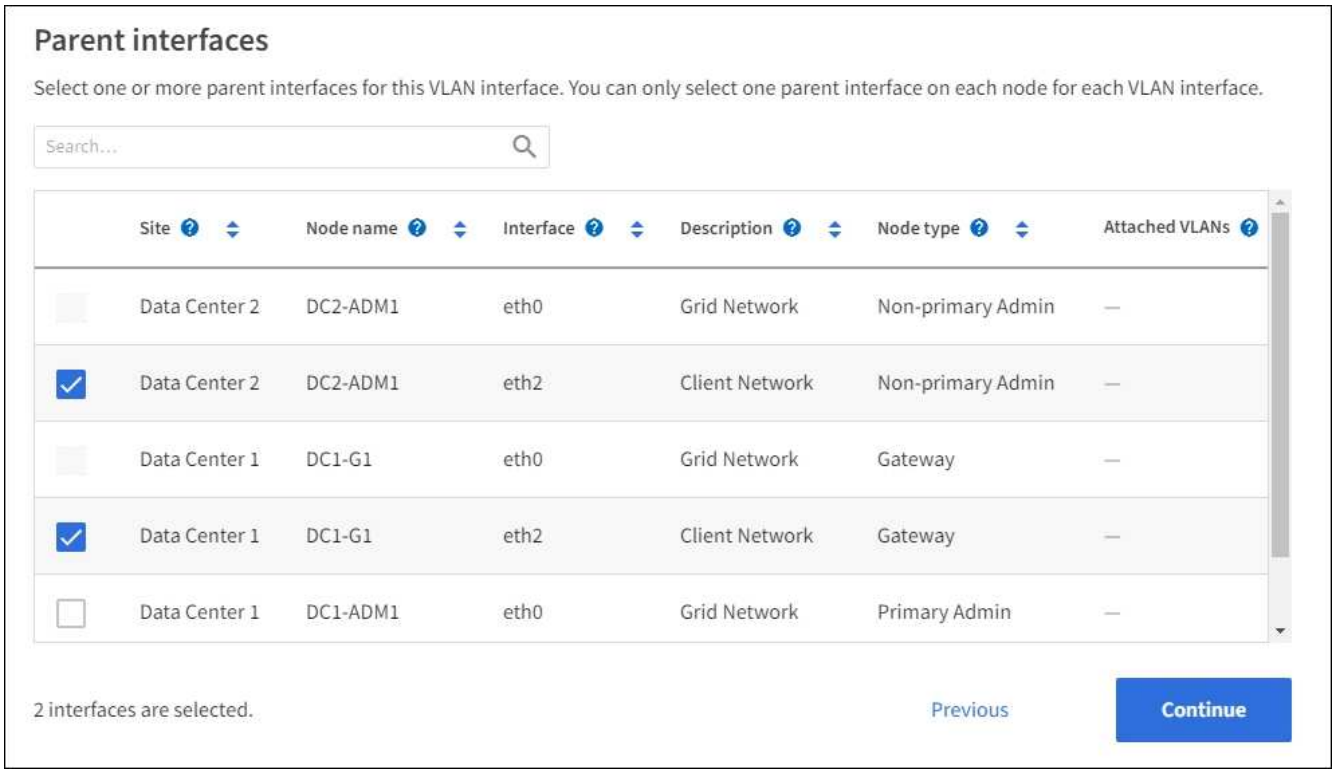
Escolha as interfaces dos pais

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada site da sua grade. As interfaces de rede de administração (eth1) não podem ser usadas como interfaces pai e não são exibidas.

Passos

1. Selecione uma ou mais interfaces pai para anexar esta VLAN.

   Por exemplo, você pode querer anexar uma VLAN à interface de rede do cliente (eth2) para um nó de gateway e um nó de administração.



2. Selecione **Continuar**.

Confirme as configurações

Passos

1. Revise a configuração e faça as alterações necessárias.
   - Se precisar alterar o ID ou a descrição da VLAN, selecione **Inserir detalhes da VLAN** na parte superior da página.
   - Se precisar alterar uma interface pai, selecione **Escolher interfaces pai** na parte superior da página ou selecione **Anterior**.

◦ Se você precisar remover uma interface pai, selecione a lixeira .

2. Selecione **Salvar**.
3. Aguarde até 5 minutos para que a nova interface apareça como uma seleção na página Grupos de alta disponibilidade e seja listada na tabela **Interfaces de rede** do nó (**NÓS** > ***nó da interface pai*** > **Rede**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere o ID ou a descrição da VLAN.
- Adicionar ou remover interfaces pai.

Por exemplo, você pode querer remover uma interface pai de uma interface VLAN se planeja desativar o nó associado.

Observe o seguinte:

- Não é possível alterar um ID de VLAN se a interface de VLAN for usada em um grupo HA.
- Não é possível remover uma interface pai se ela for usada em um grupo HA.

  Por exemplo, suponha que a VLAN 200 esteja anexada às interfaces pai nos nós A e B. Se um grupo HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você poderá remover a interface pai não utilizada para o nó B, mas não poderá remover a interface pai usada para o nó A.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Interfaces VLAN**.
2. Marque a caixa de seleção da interface VLAN que você deseja editar. Em seguida, selecione **Ações** > **Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **Continuar**.

   Não é possível atualizar uma ID de VLAN se a VLAN for usada em um grupo HA.

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **Continuar**.
5. Revise a configuração e faça as alterações necessárias.
6. Selecione **Salvar**.

Remover uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela estiver sendo usada em um grupo HA. Você deve remover a interface VLAN do grupo HA antes de poder removê-la.

Para evitar interrupções no tráfego de clientes, considere fazer uma das seguintes ações:

- Adicione uma nova interface VLAN ao grupo HA antes de remover esta interface VLAN.
- Crie um novo grupo HA que não use esta interface VLAN.
- Se a interface VLAN que você deseja remover for a interface ativa no momento, edite o grupo HA. Mova a interface VLAN que você deseja remover para o final da lista de prioridades. Aguarde até que a

comunicação seja estabelecida na nova interface primária e, em seguida, remova a interface antiga do grupo HA. Por fim, exclua a interface VLAN nesse nó.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Interfaces VLAN**.
2. Marque a caixa de seleção de cada interface VLAN que você deseja remover. Em seguida, selecione **Ações** > **Excluir**.
3. Selecione **Sim** para confirmar sua seleção.

   Todas as interfaces VLAN selecionadas serão removidas. Um banner verde de sucesso aparece na página de interfaces de VLAN.

Gerenciar políticas de classificação de tráfego

O que são políticas de classificação de tráfego?

As políticas de classificação de tráfego permitem identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar a limitar e monitorar o tráfego para melhorar suas ofertas de qualidade de serviço (QoS).

As políticas de classificação de tráfego são aplicadas aos endpoints no serviço StorageGRID Load Balancer para nós de gateway e nós de administração. Para criar políticas de classificação de tráfego, você já deve ter criado pontos de extremidade do balanceador de carga.

Regras de correspondência

Cada política de classificação de tráfego contém uma ou mais regras de correspondência para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Baldes
- Sub-rede
- Inquilino
- Pontos de extremidade do balanceador de carga

O StorageGRID monitora o tráfego que corresponde a qualquer regra dentro da política de acordo com os objetivos da regra. Qualquer tráfego que corresponda a qualquer regra de uma política é tratado por essa política. Por outro lado, você pode definir regras para corresponder a todo o tráfego, exceto uma entidade especificada.

Limitação de tráfego

Opcionalmente, você pode adicionar os seguintes tipos de limite a uma política:

- Largura de banda agregada
- Largura de banda por solicitação
- Solicitações simultâneas
- Taxa de solicitação

Os valores limite são aplicados por balanceador de carga. Se o tráfego for distribuído simultaneamente entre vários balanceadores de carga, as taxas máximas totais serão um múltiplo dos limites de taxa especificados.

Você pode criar políticas para limitar a largura de banda agregada ou para limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Limites agregados de largura de banda podem impor um impacto menor adicional no desempenho do tráfego não limitado.

Para limites de largura de banda agregados ou por solicitação, as solicitações entram ou saem na taxa que você definir. O StorageGRID só pode impor uma velocidade, portanto, a correspondência de política mais específica, por tipo de correspondente, é a que é imposta. A largura de banda consumida pela solicitação não é contabilizada em outras políticas de correspondência menos específicas que contêm políticas agregadas de limite de largura de banda. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta 503 Slow Down para solicitações que excedem qualquer limite de política correspondente.

No Grid Manager, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Use políticas de classificação de tráfego com SLAs

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para impor acordos de nível de serviço (SLAs) que fornecem especificações para capacidade, proteção de dados e desempenho.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para atingir os objetivos de desempenho de cada nível de SLA.

Nível de serviço	Capacidade	Proteção de Dados	Desempenho máximo permitido	Custo
Ouro	1 PB de armazenamento permitido	3 cópias da regra ILM	25 K solicitações/seg Largura de banda de 5 GB/seg (40 Gbps)	$$$ por mês
Prata	250 TB de armazenamento permitido	2 cópias da regra ILM	10 K solicitações/seg Largura de banda de 1,25 GB/seg (10 Gbps)	$$ por mês
Bronze	100 TB de armazenamento permitido	2 cópias da regra ILM	5 K solicitações/seg Largura de banda de 1 GB/seg (8 Gbps)	$ por mês

Criar políticas de classificação de tráfego

Você pode criar políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por bucket, regex de bucket, CIDR, ponto de

extremidade do balanceador de carga ou locatário. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Você criou todos os pontos de extremidade do balanceador de carga que deseja corresponder.
- Você criou todos os inquilinos que deseja corresponder.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.
2. Selecione **Criar**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.

   Por exemplo, descreva a que esta política de classificação de tráfego se aplica e o que ela limitará.

4. Selecione **Adicionar regra** e especifique os seguintes detalhes para criar uma ou mais regras correspondentes para a política. Qualquer política que você criar deve ter pelo menos uma regra correspondente. Selecione **Continuar**.

Campo	Descrição
Tipo	Selecione os tipos de tráfego aos quais a regra de correspondência se aplica. Os tipos de tráfego são bucket, regex de bucket, CIDR, ponto de extremidade do balanceador de carga e locatário.
Valor da partida	Insira o valor que corresponde ao Tipo selecionado. • Bucket: insira um ou mais nomes de bucket. • Expressão regular de bucket: insira uma ou mais expressões regulares usadas para corresponder a um conjunto de nomes de bucket. A expressão regular não está ancorada. Use a âncora ^ para corresponder ao início do nome do bucket e use a âncora $ para corresponder ao final do nome. A correspondência de expressões regulares oferece suporte a um subconjunto da sintaxe PCRE (expressão regular compatível com Perl). • CIDR: insira uma ou mais sub-redes IPv4, em notação CIDR, que correspondam à sub-rede desejada. • Ponto de extremidade do balanceador de carga: selecione um nome de ponto de extremidade. Estes são os pontos de extremidade do balanceador de carga que você definiu no"Configurar pontos de extremidade do balanceador de carga" . • Locatário: a correspondência de locatários usa o ID da chave de acesso. Se a solicitação não contiver um ID de chave de acesso (por exemplo, acesso anônimo), a propriedade do bucket acessado será usada para determinar o locatário.

Campo	Descrição
Correspondência inversa	Se você quiser corresponder todo o tráfego de rede *exceto* o tráfego consistente com o Tipo e o Valor de correspondência recém-definidos, marque a caixa de seleção **Correspondência inversa**. Caso contrário, deixe a caixa de seleção desmarcada. Por exemplo, se você quiser que esta política se aplique a todos os endpoints do balanceador de carga, exceto um, especifique o endpoint do balanceador de carga a ser excluído e selecione **Correspondência inversa**. Para uma política que contém vários correspondentes, onde pelo menos um é um correspondente inverso, tome cuidado para não criar uma política que corresponda a todas as solicitações.

5. Opcionalmente, selecione **Adicionar um limite** e selecione os seguintes detalhes para adicionar um ou mais limites para controlar o tráfego de rede correspondido por uma regra.

> O StorageGRID coleta métricas mesmo se você não adicionar nenhum limite, para que você possa entender as tendências de tráfego.

Campo	Descrição
Tipo	O tipo de limite que você deseja aplicar ao tráfego de rede correspondido pela regra. Por exemplo, você pode limitar a largura de banda ou a taxa de solicitação. **Observação**: você pode criar políticas para limitar a largura de banda agregada ou para limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Quando a largura de banda agregada está em uso, a largura de banda por solicitação não está disponível. Por outro lado, quando a largura de banda por solicitação está em uso, a largura de banda agregada não está disponível. Limites agregados de largura de banda podem impor um impacto menor adicional no desempenho do tráfego não limitado. Para limites de largura de banda, o StorageGRID aplica a política que melhor corresponde ao tipo de limite definido. Por exemplo, se você tiver uma política que limita o tráfego em apenas uma direção, o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais que tenham limites de largura de banda. O StorageGRID implementa as "melhores" correspondências para limites de largura de banda na seguinte ordem: • Endereço IP exato (máscara /32) • Nome exato do bucket • Expressão regular de balde • Inquilino • Ponto final • Correspondências CIDR não exatas (não /32) • Correspondências inversas
Aplica-se a	Se esse limite se aplica a solicitações de leitura do cliente (GET ou HEAD) ou solicitações de gravação (PUT, POST ou DELETE).
Valor	O valor ao qual o tráfego de rede será limitado, com base na Unidade selecionada. Por exemplo, insira 10 e selecione MiB/s para evitar que o tráfego de rede correspondido por esta regra exceda 10 MiB/s. **Observação**: Dependendo da configuração das unidades, as unidades disponíveis serão binárias (por exemplo, GiB) ou decimais (por exemplo, GB). Para alterar a configuração das unidades, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.
Unidade	A unidade que descreve o valor inserido.

Por exemplo, se você quiser criar um limite de largura de banda de 40 GB/s para uma camada de SLA, crie dois limites de largura de banda agregados: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selecione **Continuar**.

7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

   O tráfego do cliente S3 agora é tratado de acordo com a política de classificação de tráfego.

Depois que você terminar

"Exibir métricas de tráfego de rede"para verificar se as polícias estão aplicando os limites de tráfego esperados.

Editar política de classificação de tráfego

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.

   A página Políticas de classificação de tráfego é exibida e as políticas existentes são listadas em uma tabela.

2. Edite a política usando o menu Ações ou a página de detalhes. Ver"criar políticas de classificação de tráfego" para o que inserir.

   Menu de ações

   a. Marque a caixa de seleção da política.

   b. Selecione **Ações** > **Editar**.

   Página de detalhes

   a. Selecione o nome da política.

   b. Selecione o botão **Editar** ao lado do nome da política.

3. Para a etapa Inserir nome da política, edite opcionalmente o nome ou a descrição da política e selecione **Continuar**.
4. Para a etapa Adicionar regras de correspondência, opcionalmente adicione uma regra ou edite o **Tipo** e o **Valor de correspondência** da regra existente e selecione **Continuar**.
5. Para a etapa Definir limites, opcionalmente adicione, edite ou exclua um limite e selecione **Continuar**.
6. Revise a política atualizada e selecione **Salvar e continuar**.

   As alterações feitas na política são salvas e o tráfego de rede agora é tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de trânsito e verificar se as polícias estão aplicando os limites de tráfego esperados.

Excluir uma política de classificação de tráfego

Você pode excluir uma política de classificação de tráfego se não precisar mais dela. Certifique-se de excluir a política correta porque uma política não pode ser recuperada quando excluída.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.

   A página Políticas de classificação de tráfego é exibida com as políticas existentes listadas em uma tabela.

2. Exclua a política usando o menu Ações ou a página de detalhes.

   Menu de ações

   a. Marque a caixa de seleção da política.

   b. Selecione **Ações** > **Remover**.

   Página de detalhes da política

   a. Selecione o nome da política.

   b. Selecione o botão **Remover** ao lado do nome da política.

3. Selecione **Sim** para confirmar que deseja excluir a política.

   A política foi excluída.

Exibir métricas de tráfego de rede

Você pode monitorar o tráfego de rede visualizando os gráficos disponíveis na página Políticas de classificação de tráfego.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou contas de locatário" .

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode visualizar métricas do serviço do balanceador de carga para determinar se a política está limitando o tráfego na rede com sucesso. Os dados nos gráficos podem ajudar você a determinar se precisa ajustar a política.

Mesmo que não haja limites definidos para uma política de classificação de tráfego, as métricas são coletadas e os gráficos fornecem informações úteis para entender as tendências de tráfego.

Passos

1. Selecione **CONFIGURAÇÃO** > **Rede** > **Classificação de tráfego**.

   A página Políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

2. Selecione o nome da política de classificação de tráfego para a qual você deseja visualizar as métricas.
3. Selecione a aba **Métricas**.

   Os gráficos da política de classificação de tráfego são exibidos. Os gráficos exibem métricas somente para o tráfego que corresponde à política selecionada.

   Os gráficos a seguir estão incluídos na página.

   - Taxa de solicitação: este gráfico fornece a quantidade de largura de banda correspondente a esta política manipulada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho dos dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho dos dados do corpo da resposta para solicitações que incluem dados do corpo na resposta.

     > Quando as solicitações são concluídas, este gráfico mostra apenas o uso da largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode ser diferente dos valores relatados neste gráfico.

   - Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual solicitações que correspondem a esta política estão retornando erros (código de status HTTP >= 400) aos clientes.
   - Duração média da solicitação (sem erro): Este gráfico fornece uma duração média de solicitações bem-sucedidas que correspondem a esta política.
   - Uso de largura de banda da política: este gráfico fornece a quantidade de largura de banda correspondente a esta política manipulada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho dos dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho dos dados do corpo da resposta para solicitações que incluem dados do corpo na resposta.
4. Posicione o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.
5. Selecione **Painel do Grafana** logo abaixo do título Métricas para visualizar todos os gráficos de uma política. Além dos quatro gráficos da aba **Métricas**, você pode visualizar mais dois gráficos:
   - Taxa de solicitação de gravação por tamanho do objeto: a taxa de solicitações PUT/POST/DELETE que correspondem a esta política. O posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na visualização instantânea são truncadas para contagens inteiras e podem reportar 0 quando há solicitações diferentes de zero no bucket.
   - Taxa de solicitação de leitura por tamanho do objeto: a taxa de solicitações GET/HEAD que correspondem a esta política. O posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na visualização instantânea são truncadas para contagens inteiras e podem reportar 0 quando há solicitações diferentes de zero no bucket.
6. Alternativamente, acesse os gráficos no menu **SUPORTE**.
   a. Selecione **SUPORTE** > **Ferramentas** > **Métricas**.
   b. Selecione **Política de Classificação de Tráfego** na seção **Grafana**.
   c. Selecione a política no menu no canto superior esquerdo da página.
   d. Posicione o cursor sobre um gráfico para ver um pop-up que mostra a data e a hora da amostra, os tamanhos dos objetos que são agregados na contagem e o número de solicitações por segundo

durante esse período.

As políticas de classificação de tráfego são identificadas por seu ID. Os IDs de política são listados na página Políticas de classificação de tráfego.

7. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustá-la.

Cifras suportadas para conexões TLS de saída

O sistema StorageGRID oferece suporte a um conjunto limitado de conjuntos de criptografia para conexões TLS (Transport Layer Security) com sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

Versões suportadas do TLS

O StorageGRID oferece suporte a TLS 1.2 e TLS 1.3 para conexões com sistemas externos usados para federação de identidades e pools de armazenamento em nuvem.

As cifras TLS suportadas para uso com sistemas externos foram selecionadas para garantir compatibilidade com uma variedade de sistemas externos. A lista é maior que a lista de cifras suportadas para uso com aplicativos cliente S3. Para configurar cifras, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** e selecione **Políticas TLS e SSH**.

> Opções de configuração de TLS, como versões de protocolo, cifras, algoritmos de troca de chaves e algoritmos MAC, não são configuráveis no StorageGRID. Entre em contato com seu representante de conta NetApp se tiver solicitações específicas sobre essas configurações.

Benefícios de conexões HTTP ativas, ociosas e simultâneas

A maneira como você configura as conexões HTTP pode afetar o desempenho do sistema StorageGRID . As configurações variam dependendo se a conexão HTTP está ativa ou ociosa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

Benefícios de manter conexões HTTP inativas abertas

Você deve manter as conexões HTTP abertas mesmo quando os aplicativos clientes estiverem ociosos para permitir que os aplicativos clientes realizem transações subsequentes na conexão aberta. Com base nas medições do sistema e na experiência de integração, você deve manter uma conexão HTTP inativa aberta por no máximo 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que seja mantida aberta e ociosa por mais de 10 minutos.

Conexões HTTP abertas e ociosas oferecem os seguintes benefícios:

- Latência reduzida desde o momento em que o sistema StorageGRID determina que precisa executar uma transação HTTP até o momento em que o sistema StorageGRID pode executar a transação

A latência reduzida é a principal vantagem, especialmente pelo tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados ao preparar o algoritmo de inicialização lenta do TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de várias classes de condições de falha que interrompem a conectividade entre o aplicativo cliente e o sistema StorageGRID

Determinar por quanto tempo manter uma conexão ociosa aberta é uma compensação entre os benefícios do início lento associado à conexão existente e a alocação ideal da conexão aos recursos internos do sistema.

Benefícios das conexões HTTP ativas

Para conexões diretas com nós de armazenamento, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP execute transações continuamente.

Determinar a duração máxima que uma conexão deve ser mantida aberta é uma compensação entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de clientes com nós de armazenamento, limitar conexões HTTP ativas oferece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID .

  Com o tempo, uma conexão HTTP pode não ser mais ideal, pois os requisitos de balanceamento de carga mudam. O sistema executa seu melhor balanceamento de carga quando os aplicativos clientes estabelecem uma conexão HTTP separada para cada transação, mas isso anula os ganhos muito mais valiosos associados às conexões persistentes.

- Permite que aplicativos clientes direcionem transações HTTP para serviços LDR que tenham espaço disponível.
- Permite iniciar procedimentos de manutenção.

  Alguns procedimentos de manutenção começam somente depois que todas as conexões HTTP em andamento são concluídas.

Para conexões de clientes com o serviço Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção sejam iniciados imediatamente. Se a duração das conexões do cliente não for limitada, poderá levar vários minutos para que as conexões ativas sejam encerradas automaticamente.

Benefícios das conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP abertas com o sistema StorageGRID para permitir o paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de uma variedade de fatores.

Conexões HTTP simultâneas fornecem os seguintes benefícios:

- Latência reduzida

  As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Aumento da produtividade

O sistema StorageGRID pode executar transações paralelas e aumentar o rendimento agregado de transações.

Os aplicativos clientes devem estabelecer várias conexões HTTP. Quando um aplicativo cliente precisa executar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID tem um pico de rendimento diferente para transações e conexões simultâneas antes que o desempenho comece a cair. O pico de rendimento depende de fatores como recursos de computação, recursos de rede, recursos de armazenamento e links WAN. O número de servidores e serviços e o número de aplicativos que o sistema StorageGRID suporta também são fatores.

Os sistemas StorageGRID geralmente oferecem suporte a vários aplicativos clientes. Você deve ter isso em mente ao determinar o número máximo de conexões simultâneas usadas por um aplicativo cliente. Se o aplicativo cliente consistir em várias entidades de software, cada uma estabelecendo conexões com o sistema StorageGRID , você deverá somar todas as conexões entre as entidades. Pode ser necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do sistema StorageGRID afeta o número máximo de transações e conexões simultâneas que o sistema pode suportar.
- Os aplicativos clientes que interagem com o sistema StorageGRID por meio de uma rede com largura de banda limitada podem ter que reduzir o grau de simultaneidade para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos cliente compartilham o sistema StorageGRID , pode ser necessário reduzir o grau de simultaneidade para evitar exceder os limites do sistema.

Separação de pools de conexão HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar a quantidade de um pool a ser usada para cada uma. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos cliente podem criar cargas que são dominantes em recuperação (leitura) ou dominantes em armazenamento (gravação). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar quanto de cada pool será dedicado para transações de leitura ou gravação.

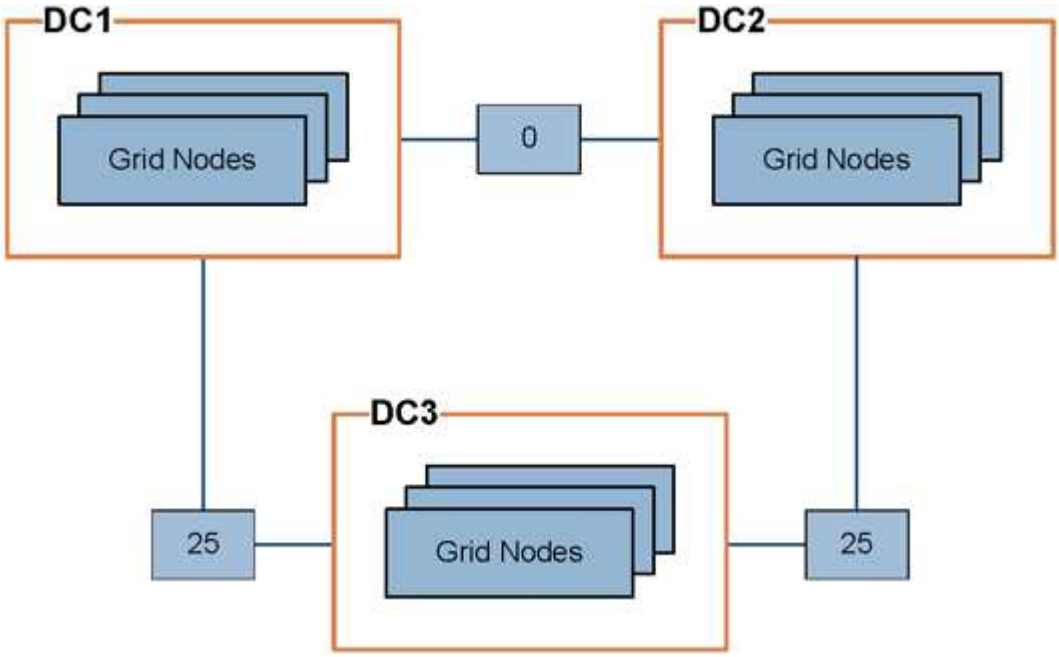
Gerenciar custos de link

Os custos de link permitem que você priorize qual site de data center fornece um serviço solicitado quando existem dois ou mais sites de data center. Você pode ajustar os custos dos links para refletir a latência entre os sites.

O que são custos de link?

- Os custos de link são usados para priorizar qual cópia de objeto é usada para atender às recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatários para determinar quais serviços internos do StorageGRID usar.
- Os custos de link são usados pelo serviço Load Balancer em nós de administração e nós de gateway para direcionar conexões de clientes. Ver "Considerações para balanceamento de carga" .

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço Load Balancer nos nós de administração e nos nós de gateway distribui igualmente as conexões do cliente para todos os nós de armazenamento no mesmo site do data center e para quaisquer sites do data center com um custo de link de 0.

  No exemplo, um nó de gateway no site do data center 1 (DC1) distribui igualmente conexões de clientes para nós de armazenamento no DC1 e para nós de armazenamento no DC2. Um nó de gateway no DC3 envia conexões de cliente somente para nós de armazenamento no DC3.

- Ao recuperar um objeto que existe como várias cópias replicadas, o StorageGRID recupera a cópia no data center que tem o menor custo de link.

  No exemplo, se um aplicativo cliente no DC2 recupera um objeto armazenado tanto no DC1 quanto no DC3, o objeto é recuperado do DC1, porque o custo do link do DC1 para o DC2 é 0, que é menor que o custo do link do DC3 para o DC2 (25).

Os custos de link são números relativos arbitrários, sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado com menos preferência do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

Link	Custo do link	Notas
Entre locais de data center físico	25 (padrão)	Data centers conectados por um link WAN.
Entre sites de data center lógicos no mesmo local físico	0	Data centers lógicos no mesmo prédio físico ou campus conectados por uma LAN.

Atualizar custos de link

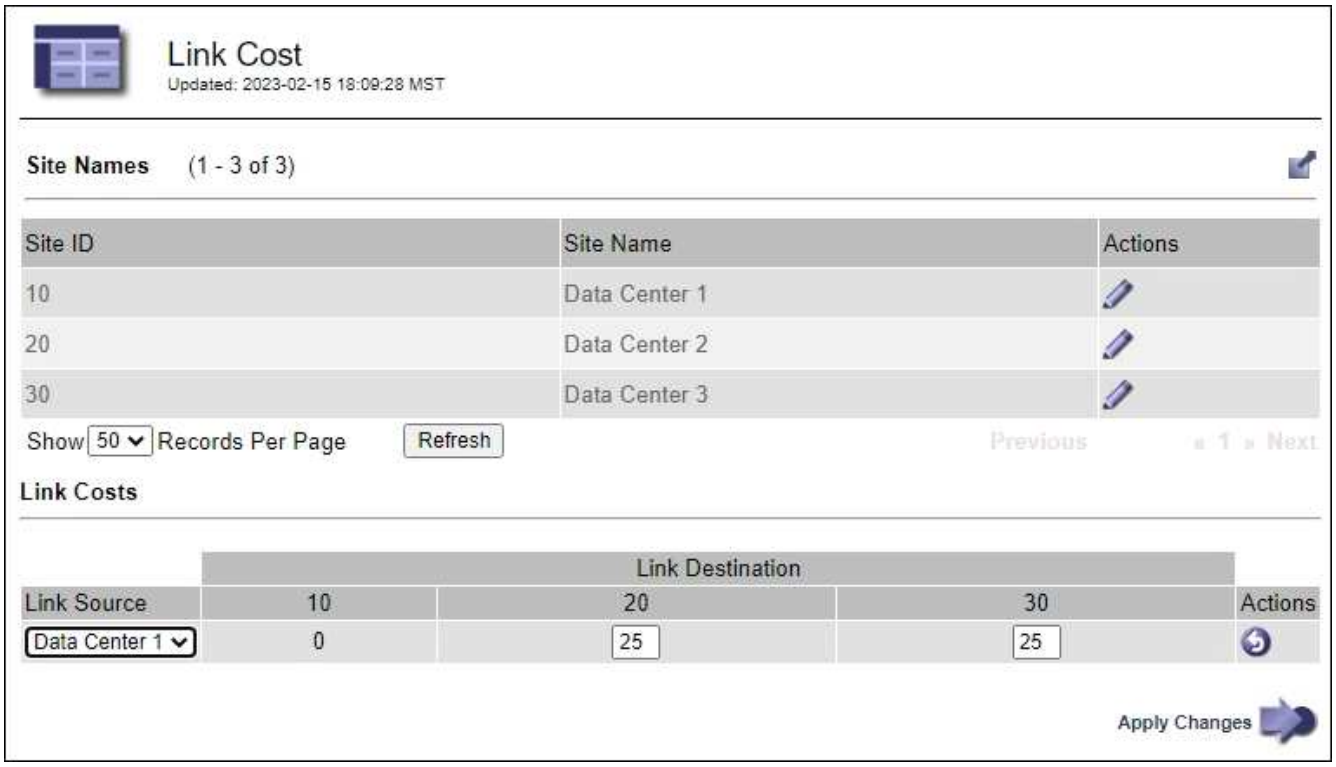
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de configuração da página de topologia de grade" .

Passos

1. Selecione **SUPORTE** > **Outro** > **Custo do link**.



2. Selecione um site em **Origem do link** e insira um valor de custo entre 0 e 100 em **Destino do link**.

   Você não pode alterar o custo do link se a origem for a mesma que o destino.

   Para cancelar as alterações, selecione **Reverter**.

3. Selecione **Aplicar alterações**.

Usar AutoSupport

O que é AutoSupport?

O recurso AutoSupport permite que o StorageGRID envie pacotes de integridade e status ao suporte técnico da NetApp .

Usar o AutoSupport pode acelerar significativamente a determinação e a resolução de problemas. O suporte técnico também pode monitorar as necessidades de armazenamento do seu sistema e ajudar você a determinar se precisa adicionar novos nós ou sites. Opcionalmente, você pode configurar os pacotes do AutoSupport para serem enviados para um destino adicional.

O StorageGRID tem dois tipos de AutoSupport:

- * StorageGRID AutoSupport* relata problemas de software StorageGRID . Ativado por padrão quando você instala o StorageGRID pela primeira vez. Você pode"alterar a configuração padrão do AutoSupport" se necessário.

> Se o StorageGRID AutoSupport não estiver habilitado, uma mensagem será exibida no painel do Grid Manager. A mensagem inclui um link para a página de configuração do AutoSupport . Se você fechar a mensagem, ela não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

- * O AutoSupport de hardware do dispositivo* relata problemas no dispositivo StorageGRID . Você deve"configurar o AutoSupport de hardware em cada dispositivo" .

O que é Active IQ?

O Active IQ é um consultor digital baseado em nuvem que aproveita a análise preditiva e a sabedoria da comunidade da base instalada da NetApp. Suas avaliações contínuas de risco, alertas preditivos, orientação prescritiva e ações automatizadas ajudam a prevenir problemas antes que eles ocorram, resultando em melhor integridade do sistema e maior disponibilidade do sistema.

Se quiser usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp , você deve habilitar o AutoSupport.

"Documentação do Digital Advisor Active IQ"

Informações incluídas no pacote AutoSupport

Um pacote AutoSupport contém os seguintes arquivos e detalhes.

Nome do arquivo	Campos	Descrição
AUTOSUPPORT-HISTORY.XML	Número de sequência do AutoSupport + Destino para este AutoSupport + Status da entrega + Tentativas de entrega + Assunto do AutoSupport + URI de entrega + Último erro + Nome do arquivo PUT do AutoSupport + Hora da geração + Tamanho compactado do AutoSupport + Tamanho descompactado do AutoSupport + Tempo total de coleta (ms)	Arquivo de histórico do AutoSupport .

Nome do arquivo	Campos	Descrição
AUTOSUPPORT.XML	Nó + Protocolo para contato com o suporte + URL de suporte para HTTP/HTTPS + Endereço de suporte + Estado do AutoSupport OnDemand + URL do servidor do AutoSupport OnDemand + Intervalo de pesquisa do AutoSupport OnDemand	Arquivo de status do AutoSupport . Fornece detalhes do protocolo usado, URL e endereço de suporte técnico, intervalo de pesquisa e OnDemand AutoSupport , se ativado ou desativado.
BUCKETS.XML	ID do bucket + ID da conta + Versão da compilação + Configuração de restrição de local + Conformidade habilitada + Configuração de conformidade + Bloqueio de objeto S3 habilitado + Configuração de bloqueio de objeto S3 + Configuração de consistência + CORS habilitado + Configuração do CORS + Hora do último acesso habilitada + Política habilitada + Configuração da política + Notificações habilitadas + Configuração de notificações + Cloud Mirror habilitado + Configuração do Cloud Mirror + Pesquisa habilitada + Configuração de pesquisa + Marcação de bucket habilitada + Configuração de marcação de bucket + Configuração de controle de versão	Fornece detalhes de configuração e estatísticas no nível do bucket. Exemplos de configurações de bucket incluem serviços de plataforma, conformidade e consistência de bucket.
CONFIGURAÇÕES DE GRADE.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de configuração de toda a rede. Contém informações sobre certificados de grade, espaço reservado de metadados, definições de configuração de toda a grade (conformidade, bloqueio de objeto S3, compactação de objeto, alertas, syslog e configuração de ILM), detalhes do perfil de codificação de eliminação, nome DNS e"Nome da NMS" .

Nome do arquivo	Campos	Descrição
ESPECIFICAÇÃO DE GRADE.XML	Especificações de grade, XML bruto	Usado para configurar e implantar o StorageGRID. Contém especificações de grade, IP do servidor NTP, IP do servidor DNS, topologia de rede e perfis de hardware dos nós.
GRID-TASKS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de status de tarefas de grade (procedimentos de manutenção). Fornece detalhes das tarefas ativas, encerradas, concluídas, com falha e pendentes da grade.
GRADE.JSON	Grade + Revisão + Versão do Software + Descrição + Licença + Senhas + DNS + NTP + Sites + Nós	Informações da grade.
ILM-CONFIGURAÇÃO.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Lista de atributos para configurações de ILM.
ILM-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de métricas do ILM. Contém taxas de avaliação de ILM para cada nó e métricas de toda a grade.
ILM.XML	XML bruto do ILM	Arquivo de política ativa do ILM. Contém detalhes sobre as políticas ativas do ILM, como ID do pool de armazenamento, comportamento de ingestão, filtros, regras e descrição.
LOG.TGZ	*n / D*	Arquivo de log para download. Contém `bycast-err.log` e `servermanager.log` de cada nó.
MANIFESTO.XML	Ordem de coleta + Nome do arquivo de conteúdo do AutoSupport para esses dados + Descrição deste item de dados + Número de bytes coletados + Tempo gasto na coleta + Status deste item de dados + Descrição do erro + Tipo de conteúdo do AutoSupport para esses dados	Contém metadados do AutoSupport e breves descrições de todos os arquivos do AutoSupport .

Nome do arquivo	Campos	Descrição
NMS-ENTIDADES.XML	Índice de atributo + OID da entidade + ID do nó + ID do modelo do dispositivo + Versão do modelo do dispositivo + Nome da entidade	Entidades de grupo e de serviço no"Árvore NMS" . Fornece detalhes da topologia da grade. O nó pode ser determinado com base nos serviços em execução no nó.
OBJETOS-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Status do objeto, incluindo status de verificação em segundo plano, transferência ativa, taxa de transferência, transferências totais, taxa de exclusão, fragmentos corrompidos, objetos perdidos, objetos ausentes, tentativa de reparo, taxa de verificação, período estimado de verificação e status de conclusão do reparo.
STATUS-DO-SERVIDOR.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Configurações do servidor. Contém estes detalhes para cada nó: tipo de plataforma, sistema operacional, memória instalada, memória disponível, conectividade de armazenamento, número de série do chassi do dispositivo de armazenamento, contagem de unidades com falha do controlador de armazenamento, temperatura do chassi do controlador de computação, hardware de computação, número de série do controlador de computação, fonte de alimentação, tamanho da unidade e tipo de unidade.
STATUS-DO-SERVIÇO.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações do nó de serviço. Contém detalhes como espaço de tabela alocado, espaço de tabela livre, métricas do Reaper do banco de dados, duração do reparo do segmento, duração do trabalho de reparo, reinicializações automáticas do trabalho e encerramento automático do trabalho.
ARMAZENAMENTO-GRADES.XML	ID do nível de armazenamento + Nome do nível de armazenamento + ID do nó de armazenamento + Caminho do nó de armazenamento	Arquivo de definições de nível de armazenamento para cada nó de armazenamento.

Nome do arquivo	Campos	Descrição
RESUMO-ATRIBUTOS.XML	OID do grupo + Caminho do grupo + ID do atributo de resumo + Nome do atributo de resumo + Valor + Índice + ID da tabela + Nome da tabela	Dados de status do sistema de alto nível que resumem as informações de uso do StorageGRID . Fornece detalhes como nome da grade, nomes dos sites, número de nós de armazenamento por grade e por site, tipo de licença, capacidade e uso da licença, termos de suporte de software e detalhes das operações do S3.
ALERTAS-DO-SISTEMA.XML	Nome + Gravidade + Nome do nó + Status do alerta + Nome do site + Hora de acionamento do alerta + Hora de resolução do alerta + ID da regra + ID do nó + ID do site + Silenciado + Outras anotações + Outros rótulos	Alertas atuais do sistema que indicam possíveis problemas no sistema StorageGRID .
AGENTES DO USUÁRIO.XML	Agente do usuário + Número de dias + Total de solicitações HTTP + Total de bytes ingeridos + Total de bytes recuperados + Solicitações PUT + Solicitações GET + Solicitações DELETE + Solicitações HEAD + Solicitações POST + Solicitações OPTIONS + Tempo médio de solicitação (ms) + Tempo médio de solicitação PUT (ms) + Tempo médio de solicitação GET (ms) + Tempo médio de solicitação DELETE (ms) + Tempo médio de solicitação HEAD (ms) + Tempo médio de solicitação POST (ms) + Tempo médio de solicitação OPTIONS (ms)	Estatísticas baseadas nos agentes de usuários do aplicativo. Por exemplo, o número de operações PUT/GET/DELETE/HEAD por agente de usuário e o tamanho total de bytes de cada operação.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	Dados do cabeçalho do AutoSupport .

Configurar AutoSupport

Por padrão, o recurso StorageGRID AutoSupport é habilitado quando você instala o StorageGRID pela primeira vez. No entanto, você deve configurar o AutoSupport de hardware em cada dispositivo. Conforme necessário, você pode alterar a configuração do AutoSupport .

Se você quiser alterar a configuração do StorageGRID AutoSupport, faça suas alterações somente no nó de administração principal. Você deveconfigurar hardware AutoSupport em cada aparelho.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Se você usar HTTPS para enviar pacotes de AutoSupport , você forneceu acesso de saída à Internet para o nó de administração principal, diretamente ou"usando um servidor proxy" (conexões de entrada não são necessárias).
- Se HTTP for selecionado na página StorageGRID AutoSupport , você terá"configurou um servidor proxy" para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitarão pacotes enviados via HTTP.
- Se você usar SMTP como protocolo para pacotes AutoSupport , você terá configurado um servidor de e-mail SMTP.

Sobre esta tarefa

Você pode usar qualquer combinação das seguintes opções para enviar pacotes do AutoSupport ao suporte técnico:

- **Semanal**: Envie automaticamente pacotes de AutoSupport uma vez por semana. Configuração padrão: Ativado.
- **Acionado por evento**: envie automaticamente pacotes de AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Configuração padrão: Ativado.
- **Sob demanda**: permita que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Configuração padrão: Desativado.
- **Acionado pelo usuário**: envie manualmente pacotes do AutoSupport a qualquer momento.

Especifique o protocolo para pacotes AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar pacotes do AutoSupport :

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. Este protocolo usa a porta 443. Se você quiserhabilitar o recurso AutoSupport on Demand , você deve usar HTTPS.
- **HTTP**: Se você selecionar HTTP, deverá configurar um servidor proxy para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam pacotes enviados via HTTP. Este protocolo usa a porta 80.
- **SMTP**: Use esta opção se quiser que os pacotes do AutoSupport sejam enviados por e-mail.

O protocolo definido é usado para enviar todos os tipos de pacotes do AutoSupport .

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Selecione o protocolo que você deseja usar para enviar pacotes do AutoSupport .
3. Se você selecionou **HTTPS**, selecione se deseja usar um certificado de suporte NetApp (certificado TLS) para proteger a conexão com o servidor de suporte técnico.
   - **Verificar certificado** (padrão): garante que a transmissão de pacotes do AutoSupport seja segura. O certificado de suporte da NetApp já está instalado com o software StorageGRID .
   - **Não verificar certificado**: Selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.
4. Selecione **Salvar**. Todos os pacotes semanais, acionados pelo usuário e por eventos são enviados usando o protocolo selecionado.

Desativar o AutoSupport semanal

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport ao suporte técnico uma vez por semana.

Para determinar quando o pacote semanal de AutoSupport será enviado, vá para a aba * AutoSupport* > **Resultados**. Na seção * AutoSupport semanal*, observe o valor de **Próximo horário agendado**.

Você pode desativar o envio automático de pacotes semanais do AutoSupport a qualquer momento.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Desmarque a caixa de seleção **Ativar AutoSupport semanal**.
3. Selecione **Salvar**.

Desabilitar AutoSupport acionado por evento

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport ao suporte técnico a cada hora.

Você pode desabilitar o AutoSupport acionado por evento a qualquer momento.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Desmarque a caixa de seleção **Habilitar AutoSupport Acionado por Evento**.
3. Selecione **Salvar**.

Habilitar AutoSupport sob Demanda

O AutoSupport on Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport on Demand está desativado. Habilitar esse recurso permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes do AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de pesquisa para consultas do AutoSupport on Demand.

O suporte técnico não pode ativar ou desativar o AutoSupport on Demand.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Selecione **HTTPS** para o protocolo.
3. Marque a caixa de seleção **Ativar AutoSupport semanal**.
4. Marque a caixa de seleção **Ativar AutoSupport sob demanda**.
5. Selecione **Salvar**.

   O AutoSupport on Demand está habilitado e o suporte técnico pode enviar solicitações do AutoSupport on Demand para o StorageGRID.

Desativar verificações de atualizações de software

Por padrão, o StorageGRID entra em contato com a NetApp para determinar se há atualizações de software disponíveis para o seu sistema. Se um hotfix ou uma nova versão do StorageGRID estiver disponível, a nova versão será exibida na página de atualização do StorageGRID .

Conforme necessário, você pode opcionalmente desabilitar a verificação de atualizações de software. Por exemplo, se o seu sistema não tiver acesso WAN, você deve desabilitar a verificação para evitar erros de download.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Desmarque a caixa de seleção **Verificar atualizações de software**.
3. Selecione **Salvar**.

Adicionar um destino adicional de AutoSupport

Quando você habilita o AutoSupport, os pacotes de saúde e status são enviados ao suporte técnico. Você pode especificar um destino adicional para todos os pacotes do AutoSupport .

Para verificar ou alterar o protocolo usado para enviar pacotes AutoSupport , consulte as instruções paraespecifique o protocolo para pacotes AutoSupport .

> Você não pode usar o protocolo SMTP para enviar pacotes do AutoSupport para um destino adicional.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport* > **Configurações**.
2. Selecione **Ativar destino de AutoSupport adicional**.
3. Especifique o seguinte:

   Nome do host

   O nome do host do servidor ou endereço IP de um servidor de destino AutoSupport adicional.

   > Você pode inserir apenas um destino adicional.

   Porta

   A porta usada para conectar a um servidor de destino AutoSupport adicional. O padrão é a porta 80 para HTTP ou a porta 443 para HTTPS.

Validação de certificado

Se um certificado TLS é usado para proteger a conexão com o destino adicional.

- Selecione **Verificar certificado** para usar a validação do certificado.
- Selecione **Não verificar certificado** para enviar seus pacotes do AutoSupport sem validação de certificado.

  Selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.

4. Se você selecionou **Verificar certificado**, faça o seguinte:
   a. Navegue até o local do certificado da CA.
   b. Carregue o arquivo do certificado da CA.

   Os metadados do certificado da CA são exibidos.
5. Selecione **Salvar**.

   Todos os pacotes futuros do AutoSupport semanais, acionados por eventos e acionados pelo usuário serão enviados para o destino adicional.

Configurar AutoSupport para aparelhos

O AutoSupport para dispositivos relata problemas de hardware do StorageGRID , e o StorageGRID AutoSupport relata problemas de software do StorageGRID , com uma exceção: para o SGF6112, o StorageGRID AutoSupport relata problemas de hardware e software. Você deve configurar o AutoSupport em cada dispositivo, exceto o SGF6112, que não requer configuração adicional. O AutoSupport é implementado de forma diferente para dispositivos de serviços e dispositivos de armazenamento.

Use o SANtricity para habilitar o AutoSupport para cada dispositivo de armazenamento. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou após a instalação do dispositivo:

- Para aparelhos SG6000 e SG5700, "configurar AutoSupport no SANtricity System Manager"

Os pacotes AutoSupport dos dispositivos E-Series podem ser incluídos no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy em"Gerente do Sistema SANtricity" .

O StorageGRID AutoSupport não relata problemas de hardware, como falhas no DIMM ou na placa de interface do host (HIC). No entanto, algumas falhas de componentes podem desencadear"alertas de hardware" . Para dispositivos StorageGRID com um controlador de gerenciamento de placa base (BMC), você pode configurar interceptações de e-mail e SNMP para relatar falhas de hardware:

- "Configurar notificações por e-mail para alertas do BMC"
- "Configurar definições SNMP para BMC"

Informações relacionadas

"Suporte NetApp"

Acionar manualmente um pacote AutoSupport

Para auxiliar o suporte técnico na solução de problemas com seu sistema StorageGRID ,

você pode acionar manualmente o envio de um pacote AutoSupport .

Antes de começar

- Você deve estar conectado ao Grid Manager usando um"navegador da web compatível" .
- Você deve ter acesso Root ou permissão para Outra configuração de grade.

Passos

1. Selecione **SUPORTE** > **Ferramentas** > * AutoSupport*.
2. Na guia **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar um pacote de AutoSupport para o site de suporte da NetApp . Se a tentativa for bem-sucedida, os valores **Resultado mais recente** e **Última hora bem-sucedida** na guia **Resultados** serão atualizados. Se houver um problema, o valor **Resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.

   Após enviar um pacote de AutoSupport acionado pelo usuário, atualize a página de AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Solucionar problemas de pacotes AutoSupport

Se uma tentativa de enviar um pacote AutoSupport falhar, o sistema StorageGRID tomará ações diferentes dependendo do tipo de pacote AutoSupport . Você pode verificar o status dos pacotes do AutoSupport selecionando **SUPPORT** > **Tools** > * AutoSupport* > **Results**.

Quando o pacote AutoSupport falha ao enviar, "Falha" aparece na guia **Resultados** da página * AutoSupport*.

Se você configurou um servidor proxy para encaminhar pacotes do AutoSupport para o NetApp, você deve"verifique se as configurações do servidor proxy estão corretas" .

Falha no pacote AutoSupport semanal

Se um pacote semanal do AutoSupport não for enviado, o sistema StorageGRID tomará as seguintes ações:

1. Atualiza o atributo Resultado Mais Recente para Tentando Novamente.
2. Tenta reenviar o pacote AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas de envio, atualiza o atributo Resultado Mais Recente para Falha.
4. Tenta enviar um pacote AutoSupport novamente no próximo horário agendado.
5. Mantém o cronograma regular do AutoSupport se o pacote falhar porque o serviço NMS não está disponível e se um pacote for enviado antes de sete dias.
6. Quando o serviço NMS estiver disponível novamente, envie um pacote AutoSupport imediatamente se um pacote não tiver sido enviado por sete dias ou mais.

Falha do pacote AutoSupport acionada pelo usuário ou por evento

Se um pacote AutoSupport acionado pelo usuário ou por evento não for enviado, o sistema StorageGRID executará as seguintes ações:

1. Exibe uma mensagem de erro se o erro for conhecido. Por exemplo, se um usuário selecionar o protocolo SMTP sem fornecer as configurações de e-mail corretas, o seguinte erro será exibido: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tente enviar o pacote novamente.
3. Registra o erro em `nms.log` .

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução (**SUPORTE** > **Alarmes (antigos)** > **Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Saiba como "configurar as configurações do servidor de e-mail" .

Corrigir uma falha no pacote AutoSupport

Se ocorrer uma falha e SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se seu servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Enviar pacotes E-Series AutoSupport por meio do StorageGRID

Você pode enviar pacotes do E-Series SANtricity System Manager AutoSupport para o suporte técnico por meio de um nó de administração do StorageGRID em vez da porta de gerenciamento do dispositivo de armazenamento.

Ver "AutoSupport de hardware da série E" para obter mais informações sobre como usar o AutoSupport com dispositivos da Série E.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou de administrador do dispositivo de armazenamento" .
- Você configurou o SANtricity AutoSupport:
  - Para aparelhos SG6000 e SG5700, "configurar AutoSupport no SANtricity System Manager"

> Você deve ter o firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

Sobre esta tarefa

Os pacotes AutoSupport da Série E contêm detalhes do hardware de armazenamento e são mais específicos do que outros pacotes AutoSupport enviados pelo sistema StorageGRID .

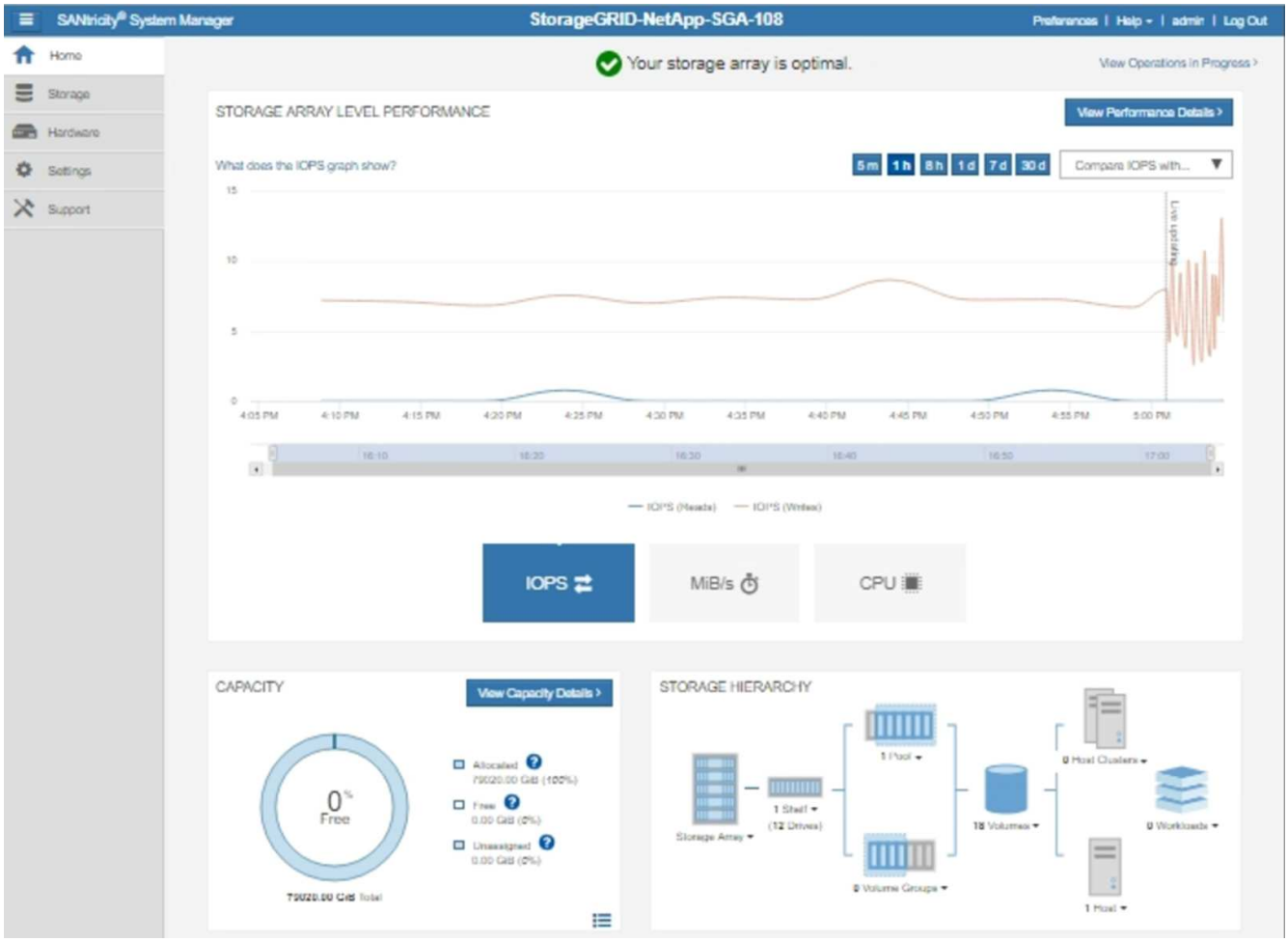
Você pode configurar um endereço de servidor proxy especial no SANtricity System Manager para transmitir pacotes do AutoSupport por meio de um nó de administração do StorageGRID sem usar a porta de gerenciamento do dispositivo. Os pacotes AutoSupport transmitidos desta forma são enviados pelo"nó de administração do remetente preferencial" , e eles usam qualquer"configurações de proxy do administrador" que foram configurados no Grid Manager.

Este procedimento serve apenas para configurar um servidor proxy StorageGRID para pacotes E-Series AutoSupport . Para obter detalhes adicionais sobre a configuração do E-Series AutoSupport , consulte o "Documentação do NetApp E-Series e SANtricity" .

Passos

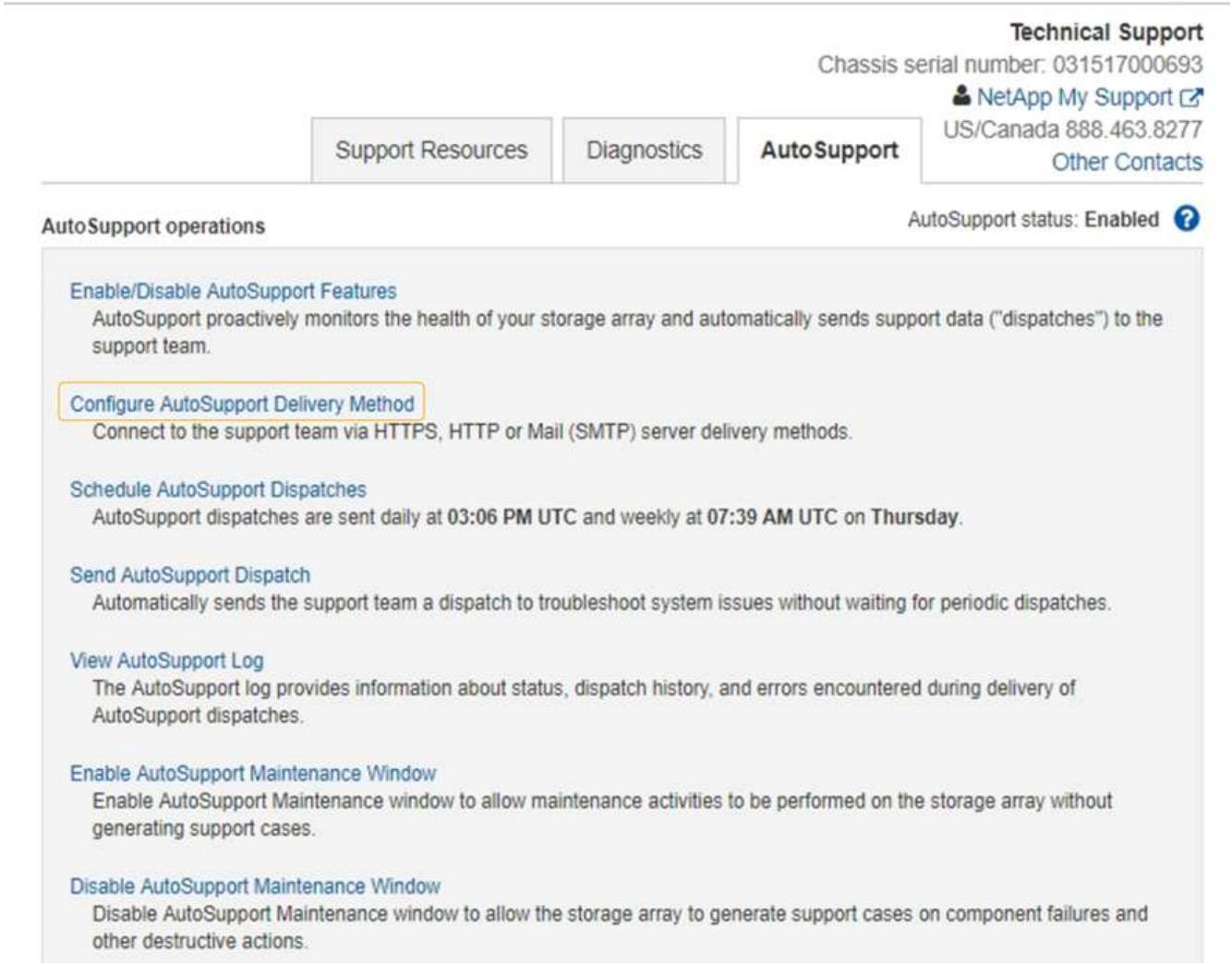
1. No Grid Manager, selecione **NODES**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de armazenamento que você deseja configurar.
3. Selecione * SANtricity System Manager*.

   A página inicial do SANtricity System Manager é exibida.



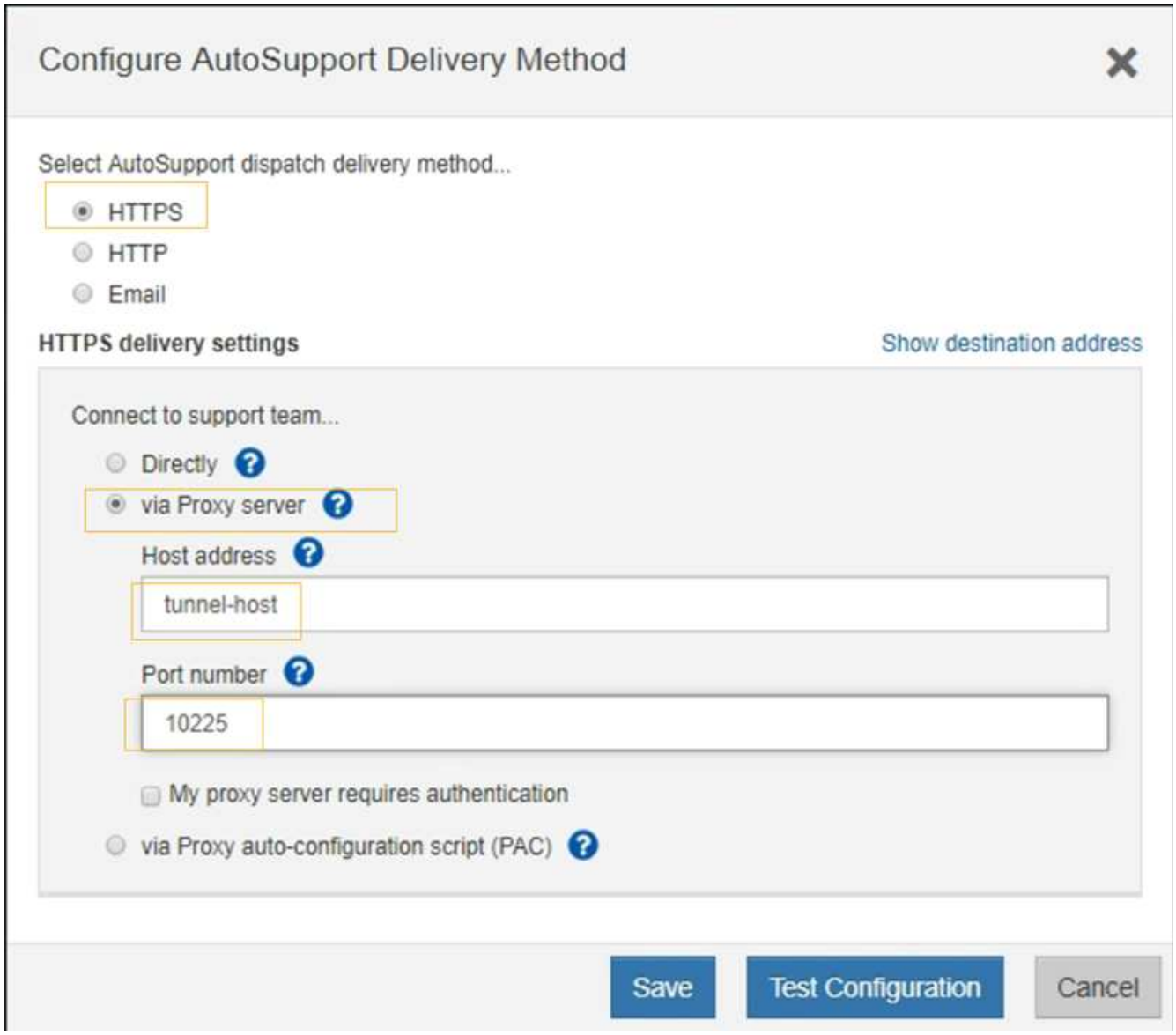
4. Selecione **SUPORTE** > **Centro de suporte** > * AutoSupport*.

   A página de operações do AutoSupport é exibida.



5. Selecione *Configurar método de entrega do AutoSupport *.

   A página Configurar método de entrega do AutoSupport é exibida.



6. Selecione **HTTPS** como método de entrega.

   O certificado que habilita HTTPS está pré-instalado.

7. Selecione **via servidor proxy**.
8. Digitar `tunnel-host` para o **Endereço do host**.

   `tunnel-host`é o endereço especial para usar um nó de administração para enviar pacotes do E-Series AutoSupport .

9. Digitar `10225` para o **Número da porta**.

   `10225`é o número da porta no servidor proxy StorageGRID que recebe pacotes AutoSupport do controlador E-Series no dispositivo.

10. Selecione **Testar configuração** para testar o roteamento e a configuração do seu servidor proxy AutoSupport .

    Se estiver correto, uma mensagem em um banner verde aparecerá: "Sua configuração do AutoSupport foi

verificada".

Se o teste falhar, uma mensagem de erro aparecerá em um banner vermelho. Verifique as configurações de DNS e rede do StorageGRID , certifique-se de que"nó de administração do remetente preferencial" você pode se conectar ao site de suporte da NetApp e tentar o teste novamente.

11. Selecione **Salvar**.

    A configuração é salva e uma mensagem de confirmação é exibida: "O método de entrega do AutoSupport foi configurado."

Gerenciar nós de armazenamento

Gerenciar nós de armazenamento

Os nós de armazenamento fornecem capacidade e serviços de armazenamento em disco. O gerenciamento de nós de armazenamento envolve o seguinte:

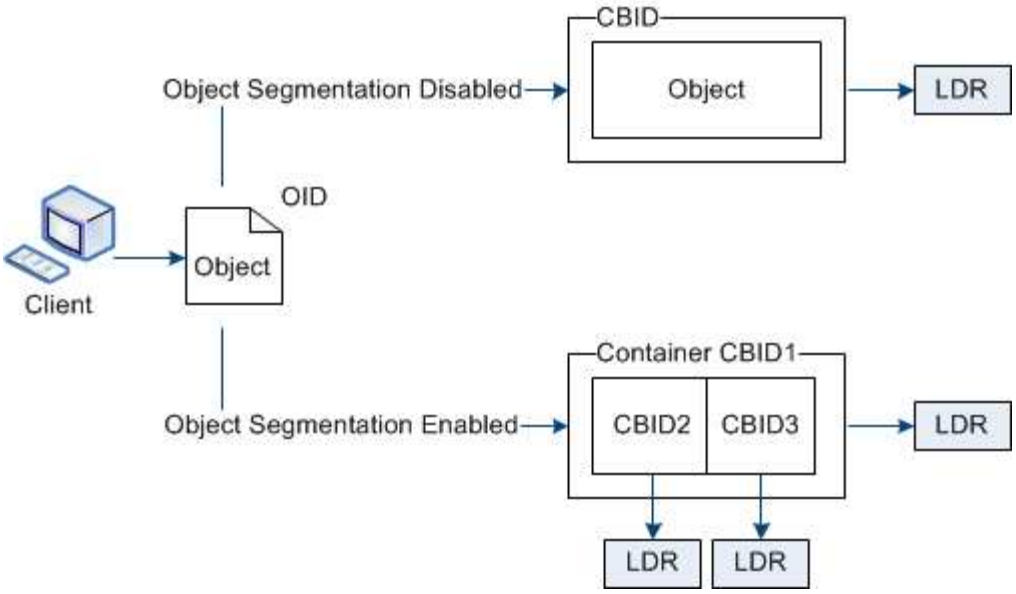
- Gerenciando opções de armazenamento
- Entendendo o que são marcas d'água de volume de armazenamento e como você pode usar substituições de marca d'água para controlar quando os nós de armazenamento se tornam somente leitura
- Monitoramento e gerenciamento do espaço usado para metadados de objetos
- Configurando configurações globais para objetos armazenados
- Aplicando as configurações do nó de armazenamento
- Gerenciando nós de armazenamento completos

Usar opções de armazenamento

O que é segmentação de objetos?

Segmentação de objetos é o processo de dividir um objeto em uma coleção de objetos menores de tamanho fixo para otimizar o armazenamento e o uso de recursos para objetos grandes. O upload multiparte do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é ingerido no sistema StorageGRID , o serviço LDR divide o objeto em segmentos e cria um contêiner de segmentos que lista as informações de cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contêiner de segmento, o serviço LDR monta o objeto original a partir de seus segmentos e retorna o objeto ao cliente.

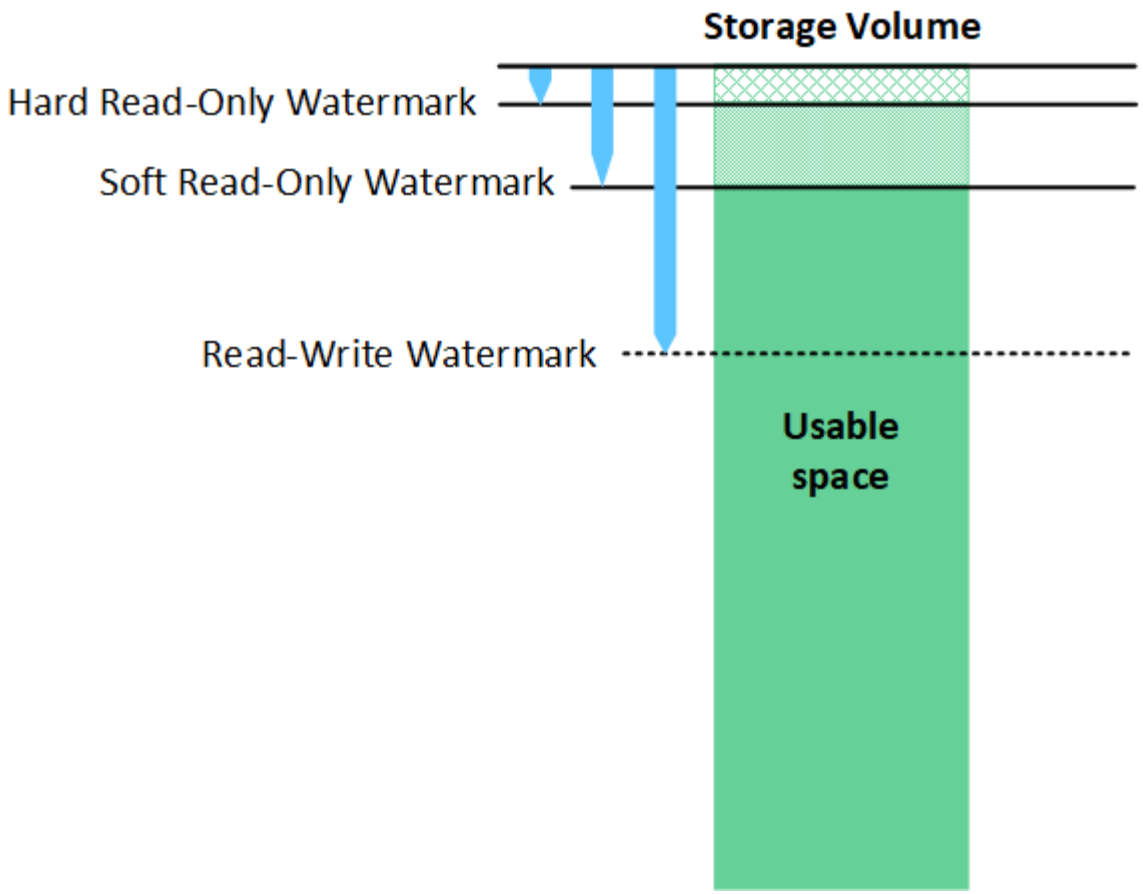
O contêiner e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contêiner e os segmentos podem ser armazenados em qualquer nó de armazenamento dentro do pool de armazenamento especificado na regra ILM.

Cada segmento é tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de atributos, como Objetos Gerenciados e Objetos Armazenados. Por exemplo, se um objeto armazenado no sistema StorageGRID for dividido em dois segmentos, o valor dos Objetos Gerenciados aumentará em três após a conclusão da ingestão, da seguinte forma:

```
segment container + segment 1 + segment 2 = three stored objects
```

O que são marcas d'água de volume de armazenamento?

O StorageGRID usa três marcas d'água de volume de armazenamento para garantir que os nós de armazenamento sejam transferidos com segurança para um estado somente leitura antes de ficarem com espaço criticamente baixo e para permitir que os nós de armazenamento que foram transferidos para um estado somente leitura se tornem leitura-gravação novamente.



As marcas d'água do volume de armazenamento se aplicam somente ao espaço usado para dados de objetos replicados e codificados para eliminação. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, acesse"Gerenciar armazenamento de metadados de objetos" .

O que é a marca d'água suave somente leitura?

A **marca d'água de somente leitura do volume de armazenamento** é a primeira marca d'água a indicar que o espaço utilizável de um Nó de Armazenamento para dados de objeto está ficando cheio.

Se cada volume em um nó de armazenamento tiver menos espaço livre do que a marca d'água somente leitura do volume, o nó de armazenamento fará a transição para o *modo somente leitura*. O modo somente leitura significa que o nó de armazenamento anuncia serviços somente leitura para o restante do sistema StorageGRID , mas atende a todas as solicitações de gravação pendentes.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o nó de armazenamento passará para o modo somente leitura suave.

O que é a marca d'água somente leitura?

A **marca d'água de somente leitura do volume de armazenamento** é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está ficando cheio.

Se o espaço livre em um volume for menor que a marca d'água de somente leitura desse volume, as gravações no volume falharão. No entanto, as gravações em outros volumes podem continuar até que o espaço livre nesses volumes seja menor que suas marcas d'água de somente leitura.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o nó de armazenamento não aceitará mais nenhuma solicitação de gravação.

A marca d'água somente leitura rígida é sempre menor que a marca d'água somente leitura flexível.

O que é a marca d'água de leitura e gravação?

A **marca d'água de leitura/gravação do volume de armazenamento** se aplica somente aos nós de armazenamento que fizeram a transição para o modo somente leitura. Ele determina quando o nó pode se tornar leitura-gravação novamente. Quando o espaço livre em qualquer volume de armazenamento em um nó de armazenamento for maior que a marca d'água de leitura e gravação desse volume, o nó retornará automaticamente ao estado de leitura e gravação.

Por exemplo, suponha que o nó de armazenamento tenha passado para o modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura e gravação de 30 GB. Assim que o espaço livre para qualquer volume aumenta para 30 GB, o nó se torna novamente de leitura e gravação.

A marca d'água de leitura e gravação é sempre maior que a marca d'água somente leitura suave e a marca d'água somente leitura forte.

Exibir marcas d'água do volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados do sistema. Se marcas d'água otimizadas não estiverem sendo usadas, você pode determinar se pode ou deve ajustar as configurações.

Antes de começar

- Você concluiu a atualização para o StorageGRID 11.6 ou superior.
- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Ver configurações atuais de marca d'água

Você pode visualizar as configurações atuais da marca d'água de armazenamento no Grid Manager.

Passos

1. Selecione **SUPORTE** > **Outros** > **Marcas d'água de armazenamento**.
2. Na página Marcas d'água de armazenamento, marque a caixa de seleção Usar valores otimizados.
   - Se a caixa de seleção estiver marcada, todas as três marcas d'água serão otimizadas para cada volume de armazenamento em cada nó de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

     Esta é a configuração padrão e recomendada. Não atualize esses valores. Opcionalmente, você podeExibir marcas d'água de armazenamento otimizadas .

   - Se a caixa de seleção Usar valores otimizados estiver desmarcada, marcas d'água personalizadas (não otimizadas) serão usadas. Não é recomendado usar configurações de marca d'água personalizadas. Use as instruções para"solução de problemas de alertas de substituição de marca d'água somente leitura" para determinar se você pode ou deve ajustar as configurações.

     Ao especificar configurações de marca d'água personalizadas, você deve inserir valores maiores que 0.

Ver marcas d'água de armazenamento otimizadas

O StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que ele calculou para a marca d'água somente leitura do volume de armazenamento. Você pode visualizar os valores mínimos e máximos otimizados para cada nó de armazenamento na sua grade.

1. Selecione **SUPORTE** > **Ferramentas** > **Métricas**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário do Prometheus.
3. Para ver a marca d'água mínima recomendada somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor mínimo otimizado da marca d'água somente leitura para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para a marca d'água somente leitura do volume de armazenamento, o alerta **Substituição de marca d'água somente leitura baixa** será acionado para o Nó de Armazenamento.

4. Para ver a marca d'água máxima recomendada para somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor máximo otimizado da marca d'água somente leitura para todos os volumes de armazenamento em cada nó de armazenamento.

Gerenciar armazenamento de metadados de objetos

A capacidade de metadados de objetos de um sistema StorageGRID controla o número máximo de objetos que podem ser armazenados nesse sistema. Para garantir que seu sistema StorageGRID tenha espaço adequado para armazenar novos objetos, você deve entender onde e como o StorageGRID armazena metadados de objetos.

O que são metadados de objeto?

Metadados de objeto são quaisquer informações que descrevem um objeto. O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Para um objeto no StorageGRID, os metadados do objeto incluem os seguintes tipos de informações:

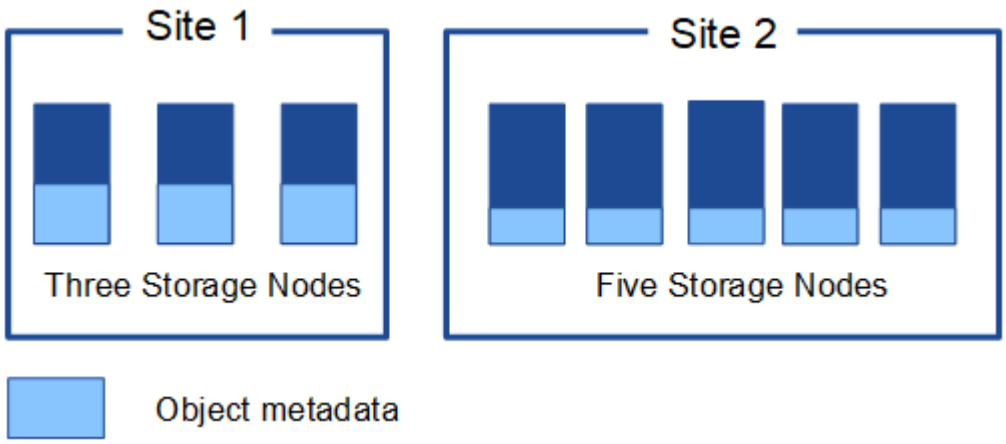
- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e a hora em que o objeto foi criado pela primeira vez e a data e a hora em que o objeto foi modificado pela última vez.
- Quaisquer pares de chave-valor de metadados de usuário personalizados associados ao objeto.
- Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
- Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.
- Para cópias de objetos codificadas por eliminação, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um pool de armazenamento em nuvem, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.

- Para objetos segmentados e objetos multipartes, identificadores de segmento e tamanhos de dados.

Como os metadados do objeto são armazenados?

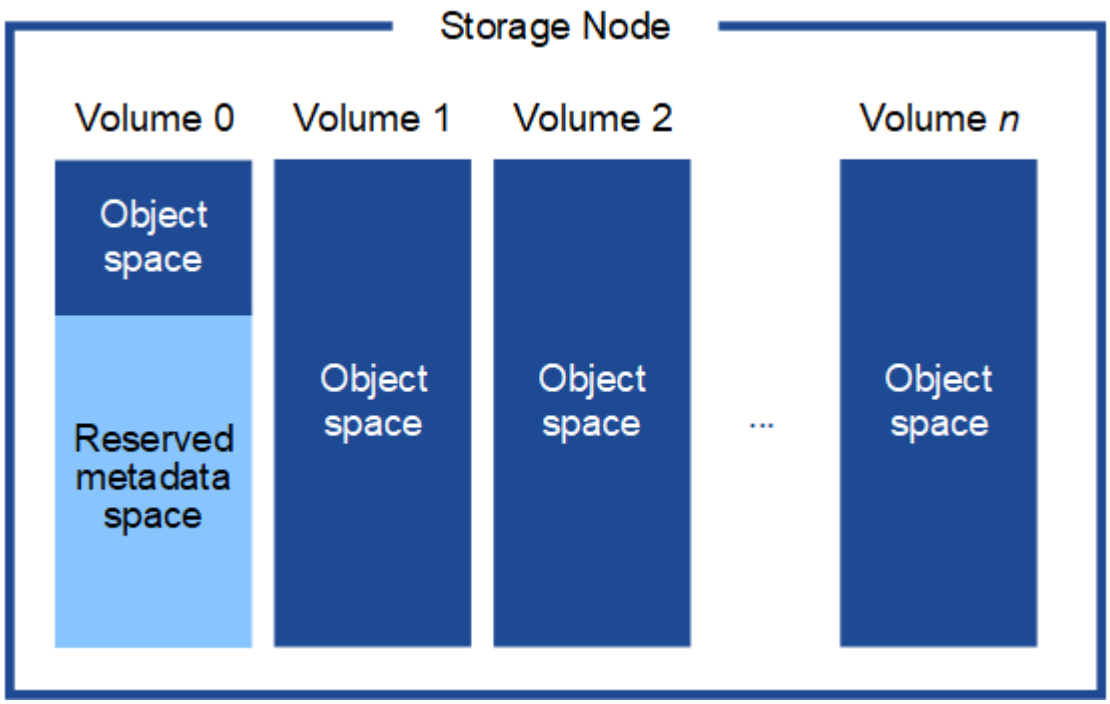
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados do objeto contra perdas, o StorageGRID armazena três cópias dos metadados para todos os objetos no sistema em cada site.

Esta figura representa os nós de armazenamento em dois locais. Cada site tem a mesma quantidade de metadados de objeto, e os metadados de cada site são subdivididos entre todos os nós de armazenamento naquele site.



Onde os metadados do objeto são armazenados?

Esta figura representa os volumes de armazenamento de um único nó de armazenamento.



Conforme mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada nó de armazenamento. Ele usa o espaço reservado para armazenar metadados de

objetos e executar operações essenciais do banco de dados. Qualquer espaço restante no volume de armazenamento 0 e todos os outros volumes de armazenamento no Nó de Armazenamento são usados exclusivamente para dados de objeto (cópias replicadas e fragmentos codificados para eliminação).

A quantidade de espaço reservada para metadados de objetos em um nó de armazenamento específico depende de vários fatores, descritos abaixo.

Configuração de espaço reservado de metadados

O *Espaço reservado para metadados* é uma configuração de todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada nó de armazenamento. Conforme mostrado na tabela, o valor padrão desta configuração é baseado em:

- A versão do software que você estava usando quando instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

Versão usada para instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado de metadados
11,5 a 11,9	128 GB ou mais em cada nó de armazenamento na grade	8 TB (8.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento na grade	3 TB (3.000 GB)
11.1 a 11.4	128 GB ou mais em cada nó de armazenamento em qualquer site	4 TB (4.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento em cada site	3 TB (3.000 GB)
11.0 ou anterior	Qualquer quantia	2 TB (2.000 GB)

Exibir configuração de espaço reservado de metadados

Siga estas etapas para visualizar a configuração de espaço reservado de metadados para seu sistema StorageGRID .

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Configurações de armazenamento**.
2. Na página Configurações de armazenamento, expanda a seção **Espaço reservado para metadados**.

Para StorageGRID 11.8 ou superior, o valor do espaço reservado de metadados deve ser de pelo menos 100 GB e não mais que 1 PB.

A configuração padrão para uma nova instalação do StorageGRID 11.6 ou superior, na qual cada nó de armazenamento tem 128 GB ou mais de RAM, é 8.000 GB (8 TB).

Espaço real reservado para metadados

Em contraste com a configuração de espaço reservado de metadados em todo o sistema, o *espaço reservado*

real para metadados de objeto é determinado para cada nó de armazenamento. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração de espaço reservado de metadados em todo o sistema.

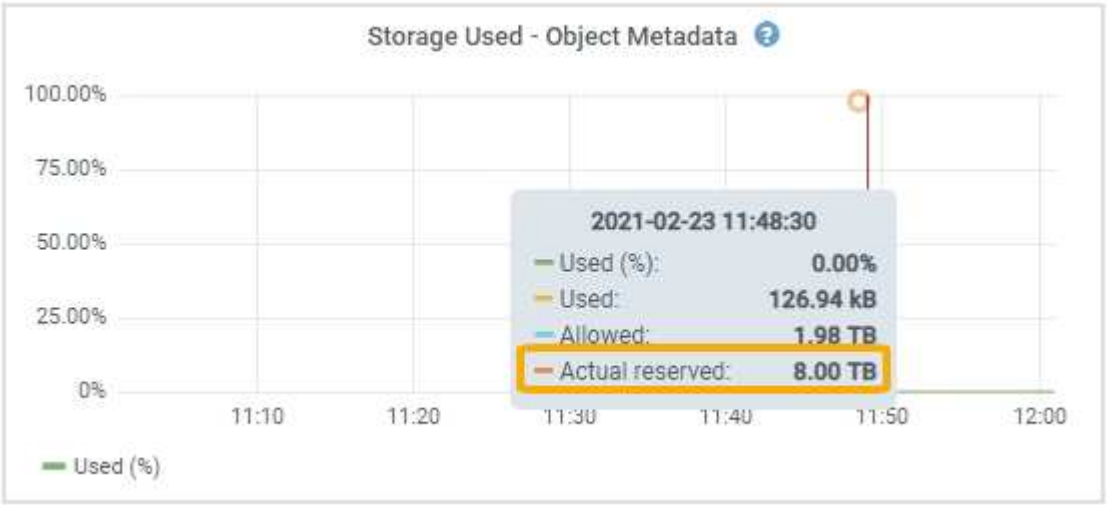
Tamanho do volume 0 para o nó	Espaço real reservado para metadados
Menos de 500 GB (uso não produtivo)	10% do volume 0
500 GB ou mais + ou + Nós de armazenamento somente de metadados	O menor desses valores: • Volume 0 • Configuração de espaço reservado de metadados **Observação**: somente um rangedb é necessário para nós de armazenamento somente de metadados.

Ver espaço reservado real para metadados

Siga estas etapas para visualizar o espaço real reservado para metadados em um nó de armazenamento específico.

Passos

1. No Grid Manager, selecione **NODES** > ***Storage Node***.
2. Selecione a aba **Armazenamento**.
3. Posicione o cursor sobre o gráfico Armazenamento usado - Metadados do objeto e localize o valor **Realmente reservado**.



Na captura de tela, o valor **Realmente reservado** é 8 TB. Esta captura de tela é de um grande nó de armazenamento em uma nova instalação do StorageGRID 11.6. Como a configuração de espaço reservado de metadados em todo o sistema é menor que o volume 0 para este nó de armazenamento, o espaço reservado real para este nó é igual à configuração de espaço reservado de metadados.

Exemplo de espaço de metadados reservado real

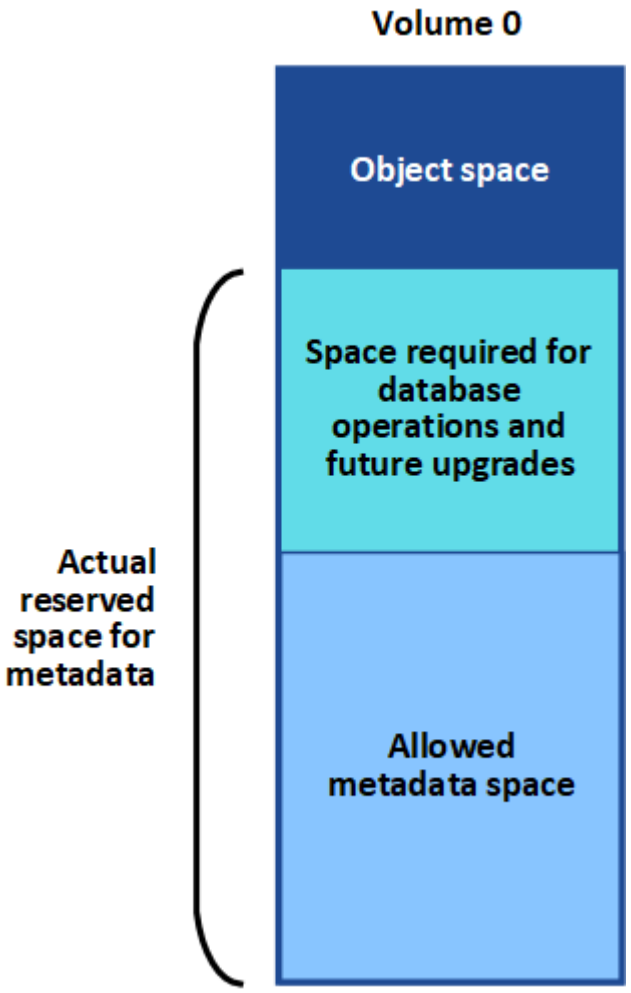
Suponha que você instale um novo sistema StorageGRID usando a versão 11.7 ou posterior. Para este

exemplo, suponha que cada nó de armazenamento tenha mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) seja de 6 TB. Com base nestes valores:

- O **espaço reservado de metadados** em todo o sistema está definido como 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11.6 ou superior se cada nó de armazenamento tiver mais de 128 GB de RAM.)
- O espaço real reservado para metadados para SN1 é de 6 TB. (O volume inteiro é reservado porque o volume 0 é menor que a configuração **Espaço reservado de metadados**.)

Espaço de metadados permitido

O espaço real reservado de cada nó de armazenamento para metadados é subdividido no espaço disponível para metadados de objetos (o *espaço de metadados permitido*) e no espaço necessário para operações essenciais do banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço de metadados permitido controla a capacidade geral do objeto.



A tabela a seguir mostra como o StorageGRID calcula o **espaço de metadados permitido** para diferentes nós de armazenamento, com base na quantidade de memória do nó e no espaço real reservado para metadados.

		Quantidade de memória no nó de armazenamento	

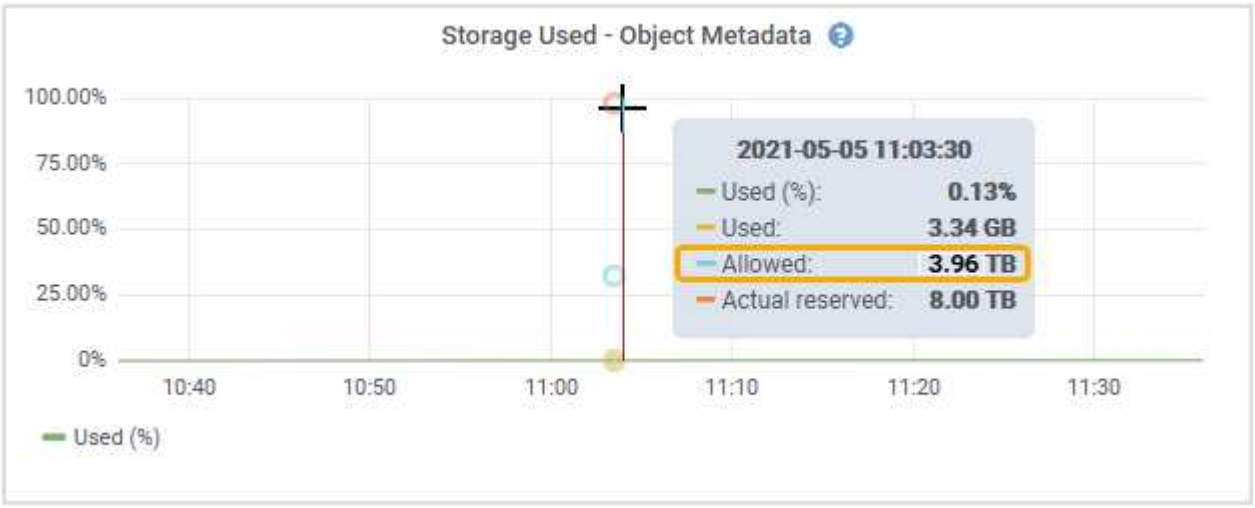
	< 128 GB	>= 128 GB	**Espaço reservado real para metadados**
⇐ 4 TB	60% do espaço real reservado para metadados, até um máximo de 1,32 TB	60% do espaço real reservado para metadados, até um máximo de 1,98 TB	4 TB

Exibir espaço de metadados permitido

Siga estas etapas para visualizar o espaço de metadados permitido para um nó de armazenamento.

Passos

1. No Grid Manager, selecione **NODES**.
2. Selecione o nó de armazenamento.
3. Selecione a aba **Armazenamento**.
4. Posicione o cursor sobre o gráfico Armazenamento usado - metadados do objeto e localize o valor **Permitido**.



Na captura de tela, o valor **Permitido** é 3,96 TB, que é o valor máximo para um Nó de Armazenamento cujo espaço real reservado para metadados é maior que 4 TB.

O valor **Permitido** corresponde a esta métrica do Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemplo de espaço de metadados permitido

Suponha que você instale um sistema StorageGRID usando a versão 11.6. Para este exemplo, suponha que cada nó de armazenamento tenha mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) seja de 6 TB. Com base nestes valores:

- O **espaço reservado de metadados** em todo o sistema está definido como 8 TB. (Este é o valor padrão para StorageGRID 11.6 ou superior quando cada nó de armazenamento tem mais de 128 GB de RAM.)
- O espaço real reservado para metadados para SN1 é de 6 TB. (O volume inteiro é reservado porque o volume 0 é menor que a configuração **Espaço reservado de metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado notabela para espaço permitido para metadados : (Espaço reservado real para metadados − 1 TB) × 60%, até um máximo de 3,96 TB.

Como nós de armazenamento de tamanhos diferentes afetam a capacidade do objeto

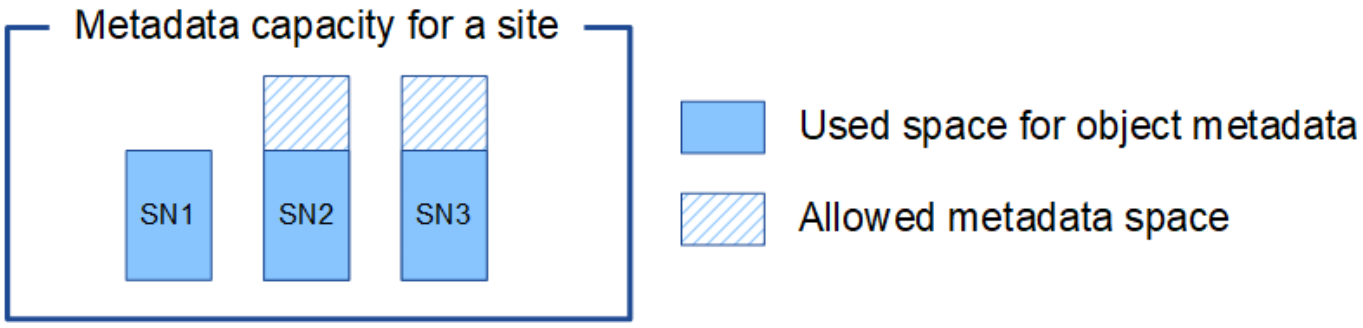
Conforme descrito acima, o StorageGRID distribui uniformemente os metadados dos objetos entre os nós de armazenamento em cada site. Por esse motivo, se um site contiver nós de armazenamento de tamanhos diferentes, o menor nó no site determinará a capacidade de metadados do site.

Considere o seguinte exemplo:

- Você tem uma grade de site único contendo três nós de armazenamento de tamanhos diferentes.
- A configuração **Espaço reservado para metadados** é 4 TB.
- Os nós de armazenamento têm os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de armazenamento	Tamanho do volume 0	Espaço de metadados reservado real	Espaço de metadados permitido
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Como os metadados do objeto são distribuídos uniformemente entre os nós de armazenamento em um site, cada nó neste exemplo pode conter apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço de metadados permitido para SN2 e SN3 não podem ser usados.



Da mesma forma, como o StorageGRID mantém todos os metadados de objeto para um sistema StorageGRID em cada site, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objeto do menor site.

E como a capacidade de metadados do objeto controla a contagem máxima de objetos, quando um nó fica sem capacidade de metadados, a grade fica efetivamente cheia.

Informações relacionadas

- Para saber como monitorar a capacidade de metadados do objeto para cada nó de armazenamento, consulte as instruções para"Monitoramento StorageGRID" .
- Para aumentar a capacidade de metadados de objetos do seu sistema,"expandir uma grade" adicionando novos nós de armazenamento.

Aumentar a configuração do Espaço Reservado de Metadados

Você poderá aumentar a configuração do sistema Espaço Reservado de Metadados se seus Nós de Armazenamento atenderem a requisitos específicos de RAM e espaço disponível.

O que você vai precisar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root ou permissões de configuração da página de topologia de grade e outras configurações de grade" .

> A página de topologia de grade foi descontinuada e será removida em uma versão futura.

Sobre esta tarefa

Você pode aumentar manualmente a configuração de Espaço Reservado de Metadados em todo o sistema para até 8 TB.

Você só poderá aumentar o valor da configuração Espaço Reservado de Metadados em todo o sistema se ambas as afirmações forem verdadeiras:

- Os nós de armazenamento em qualquer local do seu sistema têm 128 GB ou mais de RAM.
- Os nós de armazenamento em qualquer site do seu sistema têm espaço disponível suficiente no volume de armazenamento 0.

Esteja ciente de que se você aumentar essa configuração, você reduzirá simultaneamente o espaço disponível para armazenamento de objetos no volume de armazenamento 0 de todos os Nós de Armazenamento. Por esse motivo, você pode preferir definir o Espaço Reservado de Metadados para um valor menor que 8 TB, com base nos requisitos esperados de metadados do objeto.

> Em geral, é melhor usar um valor mais alto em vez de um valor mais baixo. Se a configuração do Espaço Reservado de Metadados for muito grande, você poderá diminuí-la mais tarde. Por outro lado, se você aumentar o valor posteriormente, o sistema poderá precisar mover dados do objeto para liberar espaço.

Para obter uma explicação detalhada de como a configuração do Espaço Reservado de Metadados afeta o espaço permitido para armazenamento de metadados de objetos em um nó de armazenamento específico, consulte"Gerenciar armazenamento de metadados de objetos" .

Passos

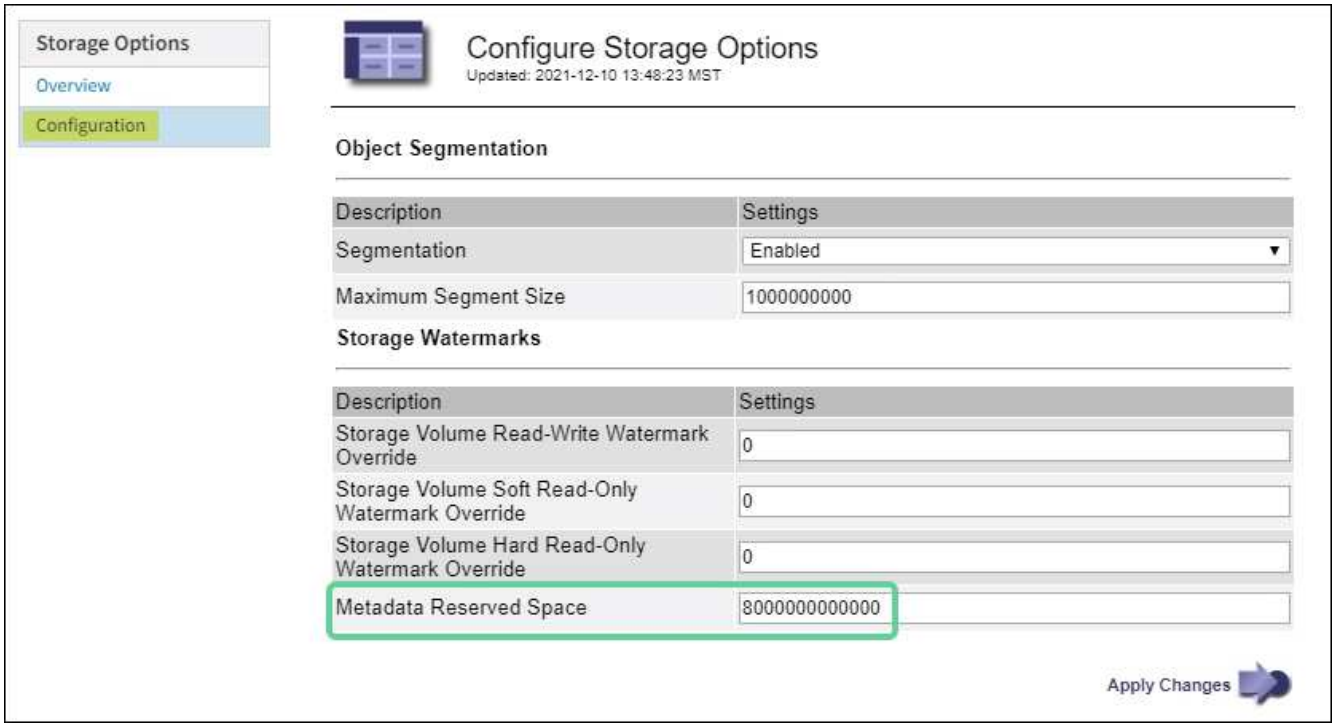
1. Determine a configuração atual do Espaço Reservado de Metadados.
   a. Selecione **CONFIGURAÇÃO** > **Sistema** > **Opções de armazenamento**.
   b. Na seção Marcas d'água de armazenamento, observe o valor de **Espaço reservado para metadados**.

2. Certifique-se de ter espaço disponível suficiente no volume de armazenamento 0 de cada nó de armazenamento para aumentar esse valor.
   a. Selecione **NODES**.
   b. Selecione o primeiro nó de armazenamento na grade.
   c. Selecione a aba Armazenamento.
   d. Na seção Volumes, localize a entrada **/var/local/rangedb/0**.
   e. Confirme se o valor Disponível é igual ou maior que a diferença entre o novo valor que você deseja usar e o valor atual do Espaço Reservado de Metadados.

      Por exemplo, se a configuração do Espaço Reservado de Metadados for atualmente 4 TB e você quiser aumentá-la para 6 TB, o valor Disponível deverá ser 2 TB ou maior.

   f. Repita essas etapas para todos os nós de armazenamento.
      - Se um ou mais nós de armazenamento não tiverem espaço disponível suficiente, o valor do espaço reservado de metadados não poderá ser aumentado. Não continue com este procedimento.
      - Se cada nó de armazenamento tiver espaço disponível suficiente no volume 0, vá para a próxima etapa.
3. Certifique-se de ter pelo menos 128 GB de RAM em cada nó de armazenamento.
   a. Selecione **NODES**.
   b. Selecione o primeiro nó de armazenamento na grade.
   c. Selecione a aba **Hardware**.
   d. Passe o cursor sobre o gráfico de uso de memória. Certifique-se de que a **Memória Total** seja de pelo menos 128 GB.
   e. Repita essas etapas para todos os nós de armazenamento.
      - Se um ou mais nós de armazenamento não tiverem memória total disponível suficiente, o valor do espaço reservado de metadados não poderá ser aumentado. Não continue com este procedimento.
      - Se cada nó de armazenamento tiver pelo menos 128 GB de memória total, vá para a próxima etapa.
4. Atualize a configuração do Espaço Reservado de Metadados.
   a. Selecione **CONFIGURAÇÃO** > **Sistema** > **Opções de armazenamento**.
   b. Selecione a aba Configuração.
   c. Na seção Marcas d'água de armazenamento, selecione **Espaço reservado para metadados**.
   d. Digite o novo valor.

      Por exemplo, para inserir 8 TB, que é o valor máximo suportado, insira **8000000000000** (8, seguido de 12 zeros)



a. Selecione **Aplicar alterações**.

Compactar objetos armazenados

Você pode habilitar a compactação de objetos para reduzir o tamanho dos objetos armazenados no StorageGRID, para que os objetos consumam menos armazenamento.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Sobre esta tarefa

Por padrão, a compactação de objetos está desabilitada. Se você habilitar a compactação, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando compactação sem perdas.

> Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

Antes de habilitar a compactação de objetos, esteja ciente do seguinte:

- Você não deve selecionar **Compactar objetos armazenados** a menos que saiba que os dados armazenados são compactáveis.
- Aplicativos que salvam objetos no StorageGRID podem compactar objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, selecionar esta opção não reduzirá ainda mais o tamanho do objeto.
- Não selecione **Compactar objetos armazenados** se estiver usando o NetApp FabricPool com StorageGRID.
- Se **Compactar objetos armazenados** for selecionado, os aplicativos cliente S3 deverão evitar executar

operações GetObject que especifiquem um intervalo de bytes a serem retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar efetivamente os objetos para acessar os bytes solicitados. Operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

Se os intervalos forem lidos de objetos compactados, as solicitações do cliente poderão expirar.

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Sistema** > **Configurações de armazenamento** > **Compactação de objetos**.
2. Marque a caixa de seleção **Compactar objetos armazenados**.
3. Selecione **Salvar**.

Gerenciar nós de armazenamento completos

À medida que os nós de armazenamento atingem a capacidade, você deve expandir o sistema StorageGRID por meio da adição de novo armazenamento. Há três opções disponíveis: adicionar volumes de armazenamento, adicionar prateleiras de expansão de armazenamento e adicionar nós de armazenamento.

Adicionar volumes de armazenamento

Cada nó de armazenamento suporta um número máximo de volumes de armazenamento. O máximo definido varia de acordo com a plataforma. Se um nó de armazenamento contiver menos do que o número máximo de volumes de armazenamento, você poderá adicionar volumes para aumentar sua capacidade. Veja as instruções para"expandindo um sistema StorageGRID" .

Adicionar prateleiras de expansão de armazenamento

Alguns nós de armazenamento do dispositivo StorageGRID , como o SG6060 ou o SG6160, podem suportar prateleiras de armazenamento adicionais. Se você tiver dispositivos StorageGRID com recursos de expansão que ainda não foram expandidos para a capacidade máxima, você pode adicionar prateleiras de armazenamento para aumentar a capacidade. Veja as instruções para"expandindo um sistema StorageGRID" .

Adicionar nós de armazenamento

Você pode aumentar a capacidade de armazenamento adicionando nós de armazenamento. É preciso considerar cuidadosamente as regras de ILM atualmente ativas e os requisitos de capacidade ao adicionar armazenamento. Veja as instruções para"expandindo um sistema StorageGRID" .

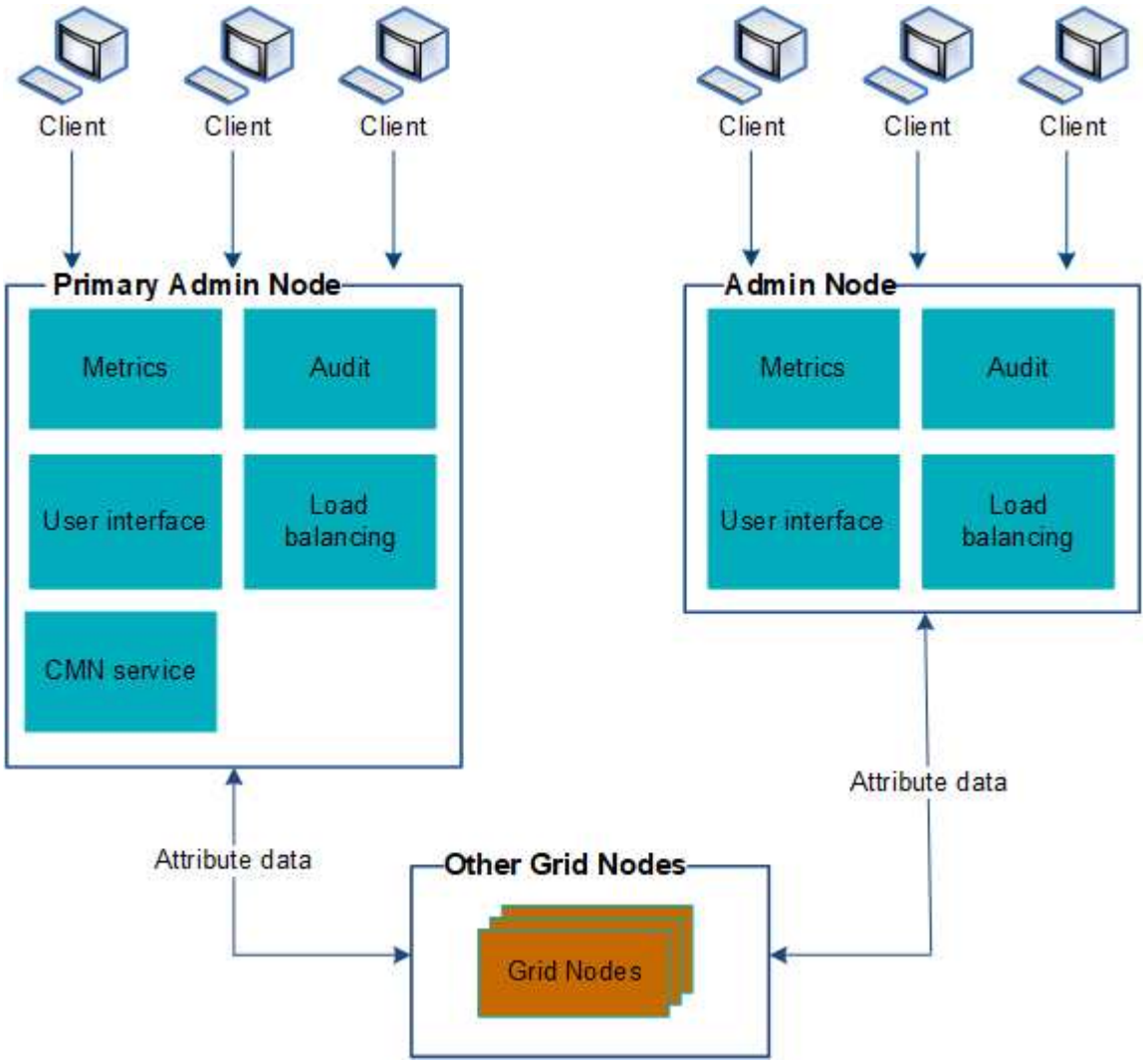
Gerenciar nós de administração

Use vários nós de administração

Um sistema StorageGRID pode incluir vários nós de administração para permitir que

você monitore e configure continuamente seu sistema StorageGRID , mesmo se um nó de administração falhar.

Se um nó de administração ficar indisponível, o processamento de atributos continuará, os alertas ainda serão acionados e as notificações por e-mail e os pacotes de AutoSupport ainda serão enviados. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto para notificações e pacotes de AutoSupport .



Há duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administração falhar:

- Os clientes da Web podem se reconectar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de alta disponibilidade de nós de administração, os clientes da Web poderão continuar acessando o Grid Manager ou o Tenant Manager usando o endereço IP virtual do grupo HA. Ver "Gerenciar grupos de alta disponibilidade" .

> Ao usar um grupo HA, o acesso é interrompido se o nó de administração ativo falhar. Os usuários devem efetuar login novamente depois que o endereço IP virtual do grupo HA falhar para outro nó de administração no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó

de administração primário falhar, ele deverá ser recuperado antes que o sistema StorageGRID esteja totalmente funcional novamente.

Identifique o nó de administração principal

O nó administrativo primário fornece mais funcionalidades do que os nós administrativos não primários. Por exemplo, alguns procedimentos de manutenção devem ser executados usando o nó de administração principal.

Para obter mais informações sobre nós de administração, consulte"O que é um nó de administração" .

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Passos

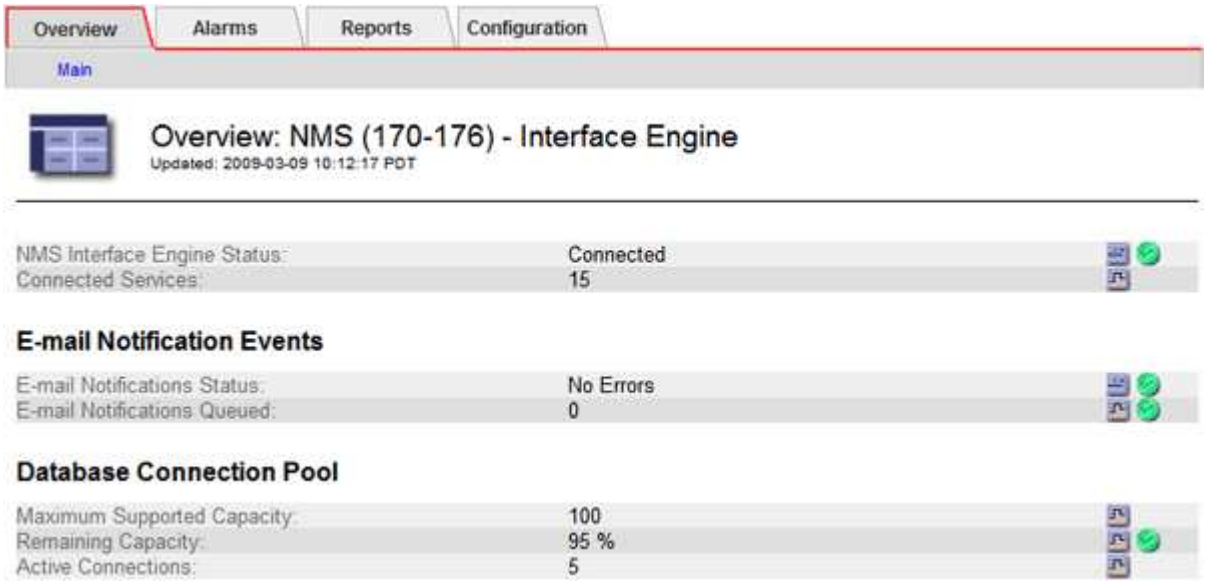
1. Selecione **NODES**.
2. Digite **primário** na caixa de pesquisa.

   Nos resultados da pesquisa, identifique o nó com "Nó de administração principal" exibido na coluna Tipo. Um nó de administração primário deve ser listado.

Ver status de notificação e filas

O serviço do Sistema de Gerenciamento de Rede (NMS) nos Nós de Administração envia notificações ao servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho da fila de notificações na página Interface Engine.

Para acessar a página Interface Engine, selecione **SUPORTE** > **Ferramentas** > **Topologia de grade**. Em seguida, selecione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



As notificações são processadas pela fila de notificações por e-mail e enviadas ao servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando for feita a tentativa de enviar a notificação, uma

tentativa de reenviar a notificação ao servidor de e-mail continuará por um período de 60 segundos. Se a notificação não for enviada ao servidor de e-mail após 60 segundos, ela será descartada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila.

Informações sobre direitos autorais

Informações sobre marcas comerciais