Administrar o StorageGRID

StorageGRID

NetApp
March 12, 2025

Índice

Administrar o StorageGRID

Administre o StorageGRID: Visão geral

Use estas instruções para configurar e administrar um sistema StorageGRID.

Sobre estas instruções

Essas instruções descrevem como usar o Gerenciador de Grade para configurar grupos e usuários, criar contas de locatário para permitir que aplicativos clientes S3 e Swift armazenem e recuperem objetos, configurem e gerenciem redes StorageGRID, configurem AutoSupport, gerenciem configurações de nó e muito mais.

Estas instruções destinam-se ao pessoal técnico que irá configurar, administrar e dar suporte a um sistema StorageGRID depois de instalado.

Antes de começar

- Você tem uma compreensão geral do sistema StorageGRID.
- Você tem conhecimento bastante detalhado de shells de comando do Linux, rede e configuração e configuração de hardware do 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	107
Microsoft Edge	107
Mozilla Firefox	106

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

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Faça login no Gerenciador de Grade

Você acessa a página de login do Gerenciador de Grade inserindo o nome de domínio

totalmente qualificado (FQDN) ou o endereço IP de um nó Admin na barra de endereços de um navegador da Web compatível.

Visão geral

Cada sistema StorageGRID inclui um nó de administração principal e qualquer número de nós de administração não primários. Você pode entrar no Gerenciador de Grade em qualquer nó de administrador para gerenciar o sistema StorageGRID. No entanto, os nós de administração não são exatamente os mesmos:

- Reconhecimentos de alarmes (sistema legado) feitos em um nó Admin não são copiados para outros nós Admin. Por esse motivo, as informações exibidas para alarmes podem não ter a mesma aparência em cada nó de administração.
- Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Ligar ao grupo HA

Se os nós de administração estiverem incluídos em um grupo de alta disponibilidade (HA), você se conetará usando o endereço IP virtual do grupo de HA ou um nome de domínio totalmente qualificado que mapeia para o endereço IP virtual. O nó de administração principal deve ser selecionado como a interface principal do grupo, de modo que, quando você acessa o Gerenciador de grade, você o acessa no nó de administração principal, a menos que o nó de administração principal não esteja disponível. "Gerenciar grupos de alta disponibilidade"Consulte .

Use SSO

Os passos de início de sessão são ligeiramente diferentes se "Logon único (SSO) foi configurado".

Inicie sessão no Grid Manager no primeiro nó de administração

Antes de começar

- Você tem suas credenciais de login.
- Você está usando um "navegador da web suportado".
- Os cookies são ativados no seu navegador.
- Você pertence a um grupo de usuários que tem pelo menos uma permissão.
- Você tem o URL para o Gerenciador de Grade:

  `https://FQDN_or_Admin_Node_IP/`

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

  Para acessar o Gerenciador de Grade 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 do Gerenciador de Grade restrito. Tem de utilizar a porta 443.

Passos

1. Inicie um navegador da Web compatível.
2. Na barra de endereços do navegador, insira o URL do Gerenciador de Grade.
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. "Gerenciar certificados de segurança"Consulte .
4. Faça login no Gerenciador de Grade.

   O ecrã de início de sessão que aparece depende se o início de sessão único (SSO) foi configurado para o StorageGRID.

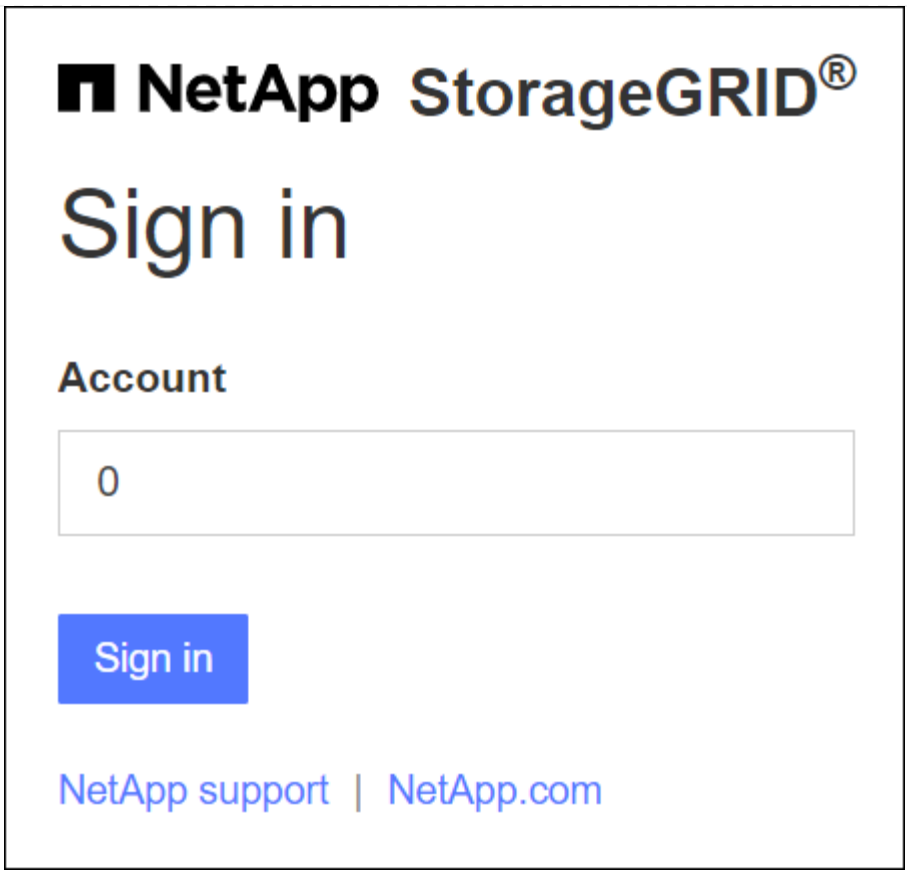
Não está a utilizar SSO

a. Insira seu nome de usuário e senha para o Gerenciador de Grade.

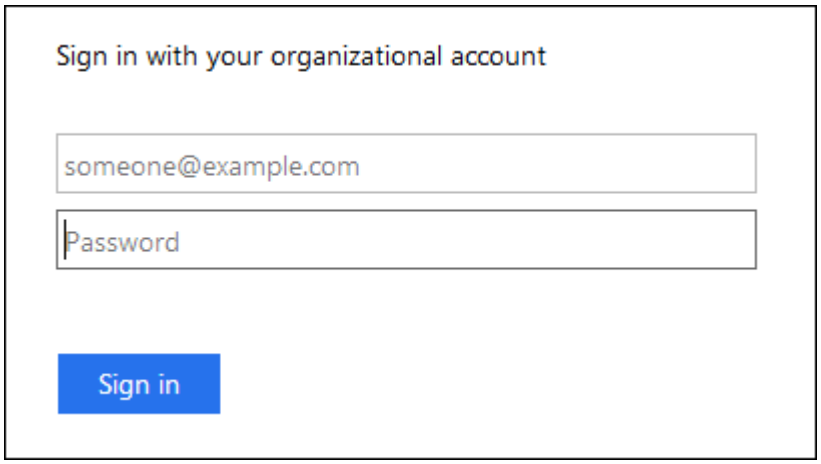
b. Selecione **entrar**.

Usando SSO

- Se o StorageGRID estiver usando SSO e esta é a primeira vez que você acessou o URL neste navegador:
  i. Selecione **entrar**. Você pode deixar o 0 no campo conta.



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

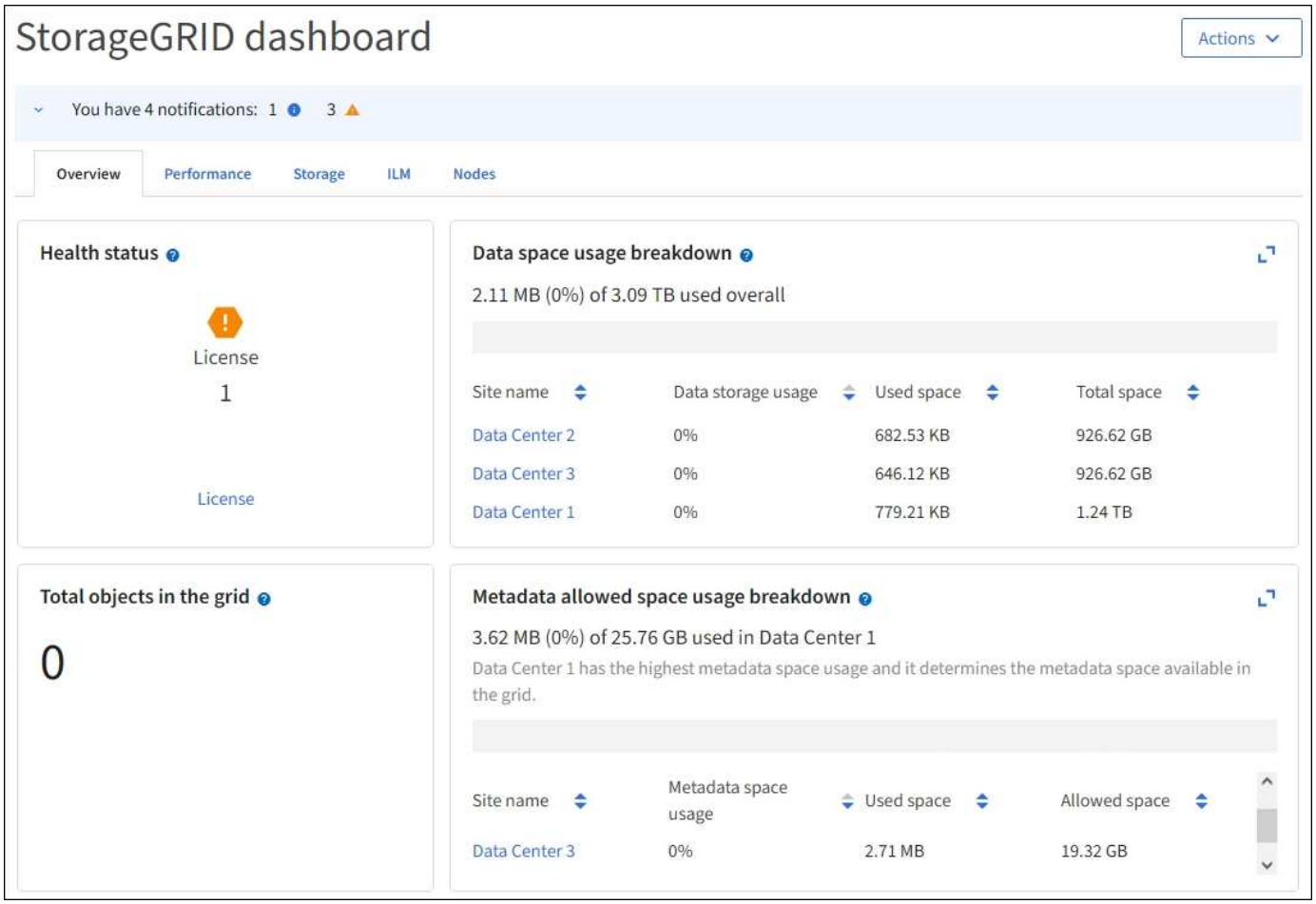


- Se o StorageGRID estiver usando SSO e você tiver acessado anteriormente o Gerenciador de Grade ou uma conta de locatário:
  i. Digite **0** (o ID da conta do Gerenciador de Grade) ou selecione **Gerenciador de Grade** se aparecer na lista de contas recentes.

ii. Selecione **entrar**.

iii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização.

Quando você estiver conetado, a página inicial do Gerenciador de Grade será exibida, que inclui o painel. Para saber quais informações são fornecidas, "Visualizar e gerenciar o painel"consulte .



Entre em outro nó de administração

Siga estes passos para iniciar sessão noutro nó de administração.

Não está a utilizar SSO

Passos

1. Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Inclua o número da porta conforme necessário.
2. Insira seu nome de usuário e senha para o Gerenciador de Grade.
3. Selecione **entrar**.

Usando SSO

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

Passos

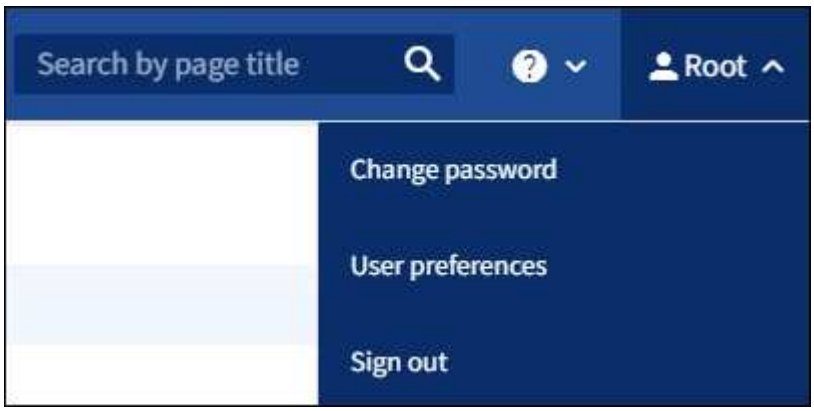
1. Introduza o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração na barra de endereços do browser.
2. Se sua sessão SSO expirou, insira suas credenciais novamente.

Saia do Grid Manager

Quando terminar de trabalhar com o Gerenciador de Grade, você deve sair para garantir que usuários não autorizados não possam acessar o sistema StorageGRID. Fechar seu navegador pode não sair 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 em uso	Você está desconetado do Admin Node. A página de login do Gerenciador de Grade é exibida. **Nota:** se você tiver feito login em mais de um nó Admin, você deve sair de cada nó.
SSO ativado	Você está desconetado de todos os nós de administrador que estava acessando. É apresentada a página de início de sessão do StorageGRID. **Grid Manager** está listado como padrão no menu suspenso **Recent Accounts** e o campo **Account ID** mostra 0. **Observação:** se o SSO estiver ativado e você também estiver conetado ao Gerenciador de Locatário, você também "saia da conta de locatário" deverá entrar "Sair do SSO"no .

Altere a sua palavra-passe

Se você é um usuário local do Gerenciador de Grade, você pode alterar sua própria senha.

Antes de começar

Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

Sobre esta tarefa

Se você entrar no StorageGRID como um usuário federado ou se o logon único (SSO) estiver ativado, não será possível alterar sua senha no Gerenciador de Grade. Em vez disso, você deve alterar sua senha na fonte de identidade externa, por exemplo, ative Directory ou OpenLDAP.

Passos

1. No cabeçalho do Gerenciador de Grade, selecione ***your name*** > **Change password**.
2. Introduza a sua palavra-passe atual.
3. Introduza uma nova palavra-passe.

   Sua senha deve conter pelo menos 8 e não mais de 32 carateres. As senhas diferenciam maiúsculas de minúsculas.
4. Volte a introduzir a nova palavra-passe.
5. Selecione **Guardar**.

Veja as informações da licença do StorageGRID

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

Sobre esta tarefa

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

Passos

1. Acesse a página Licença executando um dos seguintes procedimentos:
   - No cartão de estado de saúde no painel, selecione o ícone de estado da licença ou o link **Licença**. Este link aparece somente se houver um problema com a licença.
   - Selecione **MAINTENANCE** > **System** > **License**.

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, seja **Perpetual** 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 contrato de serviço de suporte

     Essa data é lida a partir do arquivo de licença atual e pode estar desatualizada se você estendeu ou renovou o contrato de serviço de suporte após a obtenção do arquivo de licença. Para atualizar este valor, "Atualizar informações de licença do StorageGRID"consulte a . Você também pode visualizar a data de término real do contrato usando o consultor digital da Active IQ (também conhecido como consultor digital).

   - Conteúdo do arquivo de texto da licença

     > Para as licenças emitidas antes do StorageGRID 10,3, a capacidade de armazenamento licenciada não está incluída no ficheiro de licença e é apresentada uma mensagem "consulte o Contrato de licença" em vez de um valor.

Atualizar informações de licença do StorageGRID

Você deve atualizar as informações de licença do seu sistema StorageGRID a qualquer momento que os termos de sua licença mudarem. Por exemplo, você deve atualizar as informações da licença se adquirir capacidade de armazenamento adicional para sua grade.

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 **MAINTENANCE** > **System** > **License**.
2. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento** e selecione **Procurar**.
3. Na caixa de diálogo abrir, localize e selecione o novo arquivo de licença (`.txt`) e selecione **abrir**.

   O novo ficheiro de licença é validado e apresentado.

4. Selecione **Guardar**.

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, "Use uma conta de locatário"consulte .
- `/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 do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

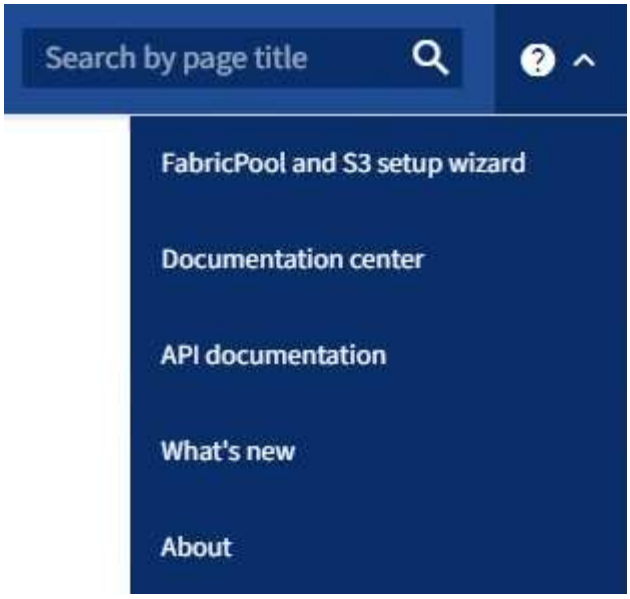
Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

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

Passos

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



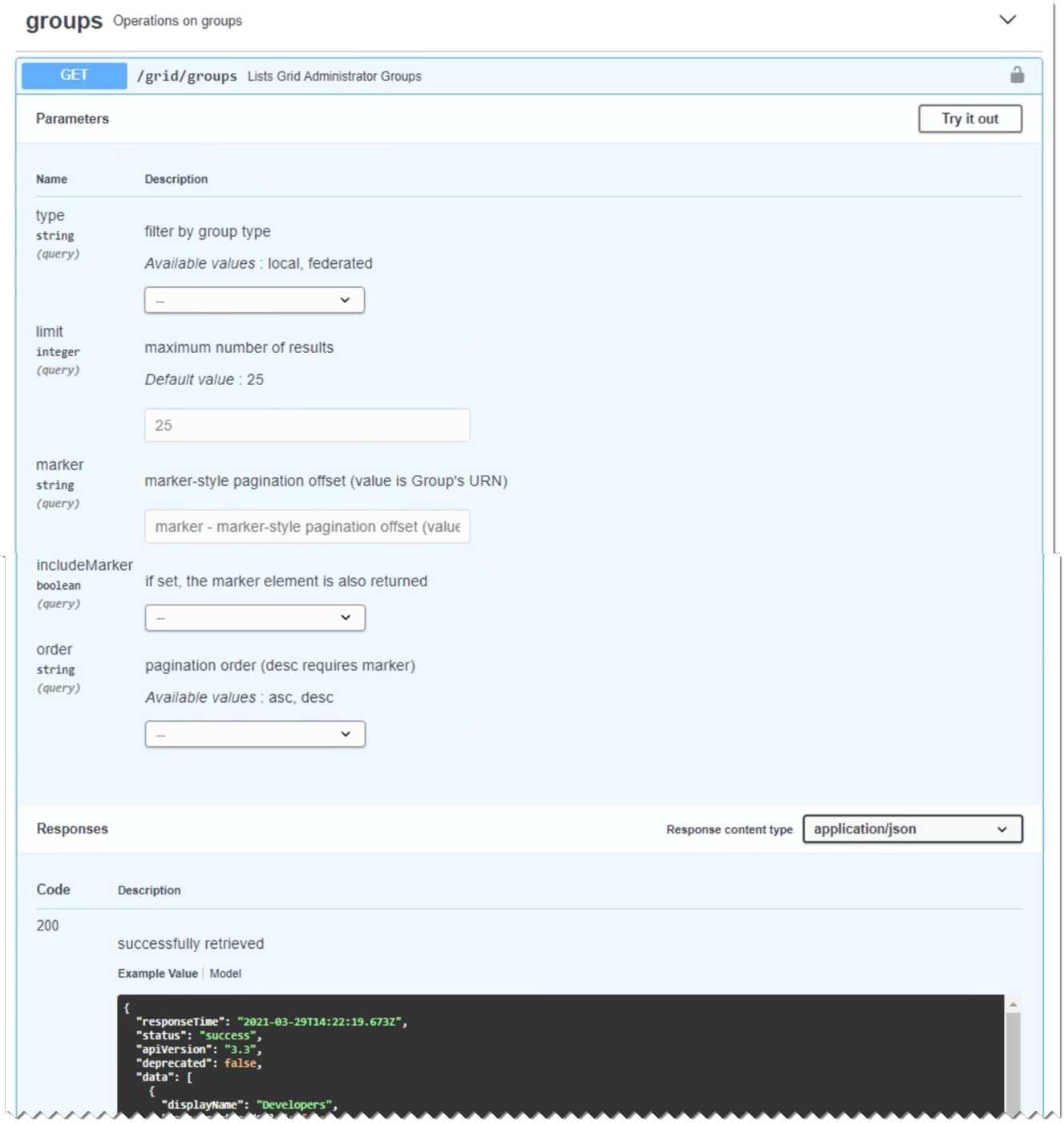
2. Para executar uma operação com a API privada, selecione **ir para a documentação da API privada** na página da API de gerenciamento do StorageGRID.

   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 o URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



5. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.
6. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.
7. Selecione **Experimente**.
8. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API Grid Management

A API Grid Management organiza as operações disponíveis nas seções a seguir.

Esta lista inclui apenas as operações disponíveis na API pública.

- **Contas**: Operações para gerenciar contas de inquilinos de armazenamento, incluindo a criação de novas contas e recuperação de uso de armazenamento para uma determinada conta.
- * Alarmes*: Operações para listar alarmes atuais (sistema legado) e retornar informações sobre a integridade da grade, incluindo os alertas atuais e um resumo dos estados de conexão dos nós.
- **Alert-history**: Operações em alertas resolvidos.
- **Alert-receivers**: Operações em recetores de notificação de alerta (e-mail).
- **Alert-rules**: Operações em regras de alerta.
- **Silêncios de alerta**: Operações em silêncios de alerta.
- **Alertas**: Operações em alertas.
- **Audit**: Operações para listar e atualizar a configuração da auditoria.
- **Auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grade suporta o esquema de autenticação de token do portador. Para fazer login, você fornece um nome de usuário e senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Portador *token*").

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

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

- **Certificados de cliente**: Operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **Config**: Operações relacionadas à versão do produto e versões da API Grid Management. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grade suportadas por essa versão, e você pode desativar versões obsoletas da API.
- **Disabled-features**: Operações para visualizar recursos que podem ter sido desativados.
- **Servidores dns**: Operações para listar e alterar servidores DNS externos configurados.
- * Endpoint-domain-nanos*: Operações para listar e alterar nomes de domínio de endpoint S3.
- **Codificação de apagamento**: Operações em perfis de codificação de apagamento.
- **Expansão**: Operações de expansão (nível de procedimento).
- **Expansion-nonos**: Operações em expansão (nível de nó).
- **Expansão-sites**: Operações em expansão (nível do local).
- **Grid-networks**: Operações para listar e alterar a Grid Network List.
- * Grid-passwords*: Operações para gerenciamento de senhas de grade.

- **Groups**: Operações para gerenciar grupos de Administrador de Grade local e recuperar grupos de Administrador de Grade federados de um servidor LDAP externo.
- **Identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm**: Operações de gerenciamento do ciclo de vida da informação (ILM).
- **Licença**: Operações para recuperar e atualizar a licença StorageGRID.
- **Logs**: Operações para coletar e baixar arquivos de log.
- **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 Grid Management usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de back-end. Para obter informações sobre a construção de consultas Prometheus, consulte o site Prometheus.

> As métricas que `private`incluem em seus nomes são destinadas 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 no status de integridade do nó.
- **Node-storage-State**: Operações no status de armazenamento de nós.
- **ntp-serviders**: Operações para listar ou atualizar servidores NTP (Network Time Protocol) externos.
- * Objetos*: Operações em objetos e metadados de objetos.
- **Recuperação**: Operações para o procedimento de recuperação.
- **Recovery-package**: Operações para baixar o Recovery Package.
- **Regiões**: Operações para visualizar e criar regiões.
- **S3-object-lock**: Operações em configurações globais de bloqueio de objetos S3D.
- **Certificado de servidor**: Operações para visualizar e atualizar certificados de servidor do Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **Classes de tráfego**: Operações para políticas de classificação de tráfego.
- **Não confiável-cliente-rede**: Operações na configuração de rede cliente não confiável.
- **Usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da API Grid Management

A API de gerenciamento de grade usa o controle de versão para suportar atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 3 da API.

`https://hostname_or_ip_address/api/v3/authorize`

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are compatíveis*** com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades. O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para 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, apenas a versão mais recente da API de gerenciamento de grade está ativada. No entanto, quando você atualiza 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 usar a API Grid Management para configurar as versões suportadas. Consulte a seção "config" da documentação da API Swagger para obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes da API Grid Management para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Determine quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

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

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 específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição 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` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

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

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

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

> As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Use a API se o logon único estiver ativado

Use a API se o logon único estiver ativado (ative Directory)

Se você tiver "Logon único configurado e habilitado (SSO)" e usar o ative Directory como provedor SSO, deverá emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe 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 arquivos de instalação do StorageGRID (`./rpms`para Linux ou CentOS, para Ubuntu ou Debian, `./debs` e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho curl pode ter um tempo limite 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. Avance para o passo 2.
   - Use solicitações curl. Avance para o passo 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. Introduza ADFS ou adfs.
   - O nome de usuário 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 do locatário.

```
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, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

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

   a. Declare as variáveis necessárias para iniciar sessão.

```
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 um 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 um URL de autenticação assinada para `TENANTACCOUNTID`. Os resultados serão passados para `python -m json.tool` 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 um URL assinado que é codificado 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 um URL completo 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 de 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 de solicitação do cliente da resposta.

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

f. Envie suas credenciais para a ação de 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 ativada para seu sistema SSO, o post de 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 de logout e o corpo de resposta contém 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 `SAMLResponse` , faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação StorageGRID.

Para `RelayState`, use o ID da conta do locatário ou use 0 se quiser entrar 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.

Saia da API se o logon único estiver ativado

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

Sobre esta tarefa

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

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 devolvida. O local de redirecionamento não é aplicável ao logout somente 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 do portador do StorageGRID.

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

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

Uma `204 No Content` resposta indica que o usuário está desconetado agora.

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

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

Se você tiver "Logon único configurado e habilitado (SSO)" e usar o Azure como provedor 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 do locatário.

Inicie sessão na API se o início de sessão único do Azure estiver ativado

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 SSO e a senha de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe 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 arquivos de instalação do StorageGRID (`./rpms`para Linux ou CentOS, para Ubuntu ou Debian, `./debs` e `./vsphere` para VMware).

Para escrever sua própria integração com a API do Azure, consulte o `storagegrid-ssoauth-azure.py` script. 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 SSO.

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

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 ("https://nodejs.org/en/download/"consulte).
   b. Instale os módulos Node.js necessários (puppeteer e jsdom):

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

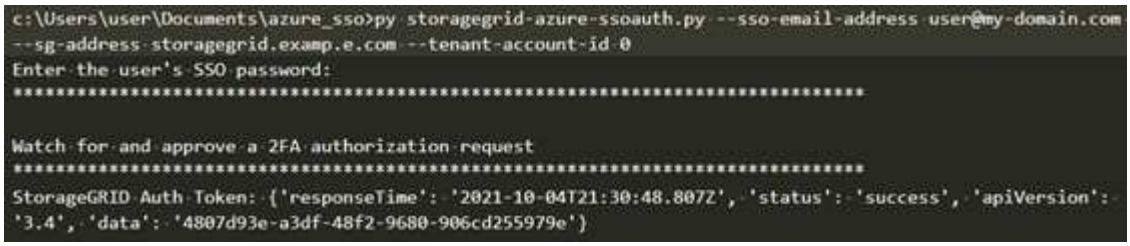
2. Passe o script Python para o interpretador Python para executar o script.

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

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
   - O endereço de e-mail SSO usado para entrar no Azure
   - O endereço para StorageGRID

◦ O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário

4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização de MFA ao Azure, se solicitado.



> O script assume que o MFA é feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para dar 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, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

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

Se você tem "Logon único configurado e habilitado (SSO)" e usa o PingFederate como provedor 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 para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe 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 arquivos de instalação do StorageGRID (`./rpms`para Linux ou CentOS, para Ubuntu ou Debian, `./debs` e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho curl pode ter um tempo limite 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. Avance para o passo 2.
   - Use solicitações curl. Avance para o passo 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 SSO
   - O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
   - O endereço para StorageGRID
   - O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

   ```
   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, semelhante a como você usaria a API se o SSO não estivesse sendo usado.
3. Se você quiser usar solicitações curl, use o procedimento a seguir.
   a. Declare as variáveis necessárias para iniciar sessão.

   ```
   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 um 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 um URL assinado que é codificado 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 ecoe a resposta:

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

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

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

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

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

f. Exporte o valor 'href' (remova a barra à direita /) e faça eco da resposta:

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

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

g. Exportar o valor "ação":

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

h. Enviar cookies juntamente com 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 `SAMLResponse` , faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação StorageGRID.

Para `RelayState`, use o ID da conta do locatário ou use 0 se quiser entrar 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.

Saia da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário. 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 fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

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 devolvida. O local de redirecionamento não é aplicável ao logout somente 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 do portador do StorageGRID.

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

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

   Uma `204 No Content` resposta indica que o usuário está desconetado agora.

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

Desative recursos com a API

Você pode usar a API de gerenciamento de grade para desativar completamente certos 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 de funcionalidades desativadas permite-lhe impedir o acesso a determinadas funcionalidades no sistema StorageGRID. Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administração com permissão **root Access** possam usar esse recurso.

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

A empresa A é um provedor de serviços que aluga a capacidade de armazenamento de seu sistema StorageGRID criando contas de inquilino. Para proteger a segurança dos objetos de seus arrendatários, a empresa A quer garantir que seus próprios funcionários nunca possam acessar qualquer conta de locatário depois que a conta tiver sido implantada.

*A empresa A pode atingir esse objetivo usando o sistema Deactivate Features na API Grid Management. Ao desativar completamente o recurso **alterar senha de root do locatário** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **acesso root** - pode alterar a senha para o usuário raiz de qualquer*

conta de locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. "Use a API de gerenciamento de grade"Consulte .
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como alterar a senha de root do locatário, envie um corpo para a API assim:

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

Quando a solicitação estiver concluída, o recurso alterar senha raiz do locatário é desativado. A permissão de gerenciamento * alterar senha de root do locatário * não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha de raiz de um locatário falhará com "'403 Forbidden.'"

Reativar funcionalidades desativadas

Por padrão, você pode usar a API de Gerenciamento de Grade para reativar um recurso que foi desativado. No entanto, se você quiser impedir que os recursos desativados sejam reativados, você pode desativar o próprio recurso **activateFeatures**.

> O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar esse recurso, esteja ciente de que você 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 endpoint Deactivate Features
3. Para reativar todos os recursos, envie um corpo para a API assim:

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

Quando essa solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento **alterar senha de root do locatário** agora aparece na interface do usuário, e qualquer solicitação de API que tente alterar a senha de root de um locatário terá êxito, assumindo que o usuário tenha a permissão de gerenciamento **acesso root** ou **alterar senha de root do locatário**.

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

Controle o acesso ao StorageGRID

Control StorageGRID Access: Visão geral

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 ativar o logon único (SSO), criar certificados de cliente e alterar senhas de grade.

Controle o acesso ao Gerenciador de Grade

Você determina quem pode acessar o Gerenciador de Grade e a API de Gerenciamento de Grade importando grupos e usuários de um serviço de federação de identidade ou configurando grupos locais e usuários locais.

O uso do "federação de identidade" torna a configuração "grupos" "usuários"mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares. Você pode configurar a federação de identidade se usar o ative Directory, OpenLDAP ou Oracle Directory Server.

> Contacte o suporte técnico se pretender utilizar outro serviço LDAP v3.

Você determina quais tarefas cada usuário pode executar atribuindo diferentes "permissões" a cada grupo. Por exemplo, você pode querer que os usuários de um grupo possam gerenciar regras ILM e usuários de outro grupo para 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. Os usuários em um grupo somente leitura só podem exibir configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade.

Ative o logon único

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Depois de "Configurar e ativar SSO"você , todos os usuários devem ser autenticados por um provedor de identidade externo antes que possam acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatário. Os usuários locais não podem entrar no StorageGRID.

Alterar a frase-passe do aprovisionamento

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 fazer o download de backups das informações de topologia de grade e chaves de criptografia para o sistema StorageGRID. Você pode "altere a frase-passe"como necessário.

Altere as senhas do console do nó

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

Altere a frase-passe de aprovisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A frase-passe 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 nó de grade e chaves de criptografia para o sistema StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

A frase-passe de aprovisionamento é necessária para muitos procedimentos de instalação e manutenção, e para "Transferir o pacote de recuperação"o . 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 e seguro.

Passos

1. Selecione **CONFIGURATION** > **access control**> **Grid passwords**.
2. Em **alterar senha de provisionamento**, selecione **fazer uma alteração**
3. Introduza a sua frase-passe de aprovisionamento atual.
4. Introduza a nova frase-passe. A frase-passe deve conter pelo menos 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e 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 estiver concluída.

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

   Depois de alterar a senha de provisionamento, você deve baixar imediatamente um novo Pacote de recuperação. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

Altere as senhas do console do nó

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

Use a senha do console do nó para fazer login em um nó como "admin" usando SSH, ou para o usuário raiz em uma conexão VM/console físico. 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` no pacote de recuperação. As senhas são listadas na coluna Senha no arquivo Passwords.txt.

> Existem 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 **CONFIGURATION** > **Access control** > **Grid passwords**.
2. Em **alterar senhas de console de nó**, selecione **fazer uma alteração**.

Introduza a frase-passe de aprovisionamento

Passos

1. Introduza a frase-passe de aprovisionamento da grelha.
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 em qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. Copie o arquivo do pacote de recuperação (`.zip`) para dois locais seguros, seguros 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 for exibida, selecione **Sim** se estiver pronto para começar a alterar as senhas do console do nó.

   Não é possível cancelar este processo após o início.

Altere as senhas do console do nó

Quando o processo de senha do console do nó é iniciado, um novo pacote de recuperação é gerado que inclui as novas senhas. Em seguida, as senhas são atualizadas em cada nó.

Passos

1. Aguarde que o novo pacote de recuperação seja gerado, o que pode levar alguns minutos.
2. Selecione **Transferir novo pacote de recuperação**.
3. Quando o download for concluído:

   a. Abra o `.zip` ficheiro.

   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, seguros e separados.

   > Não substitua o pacote de recuperação antigo.

   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 de nós** e aguarde 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 a próxima etapa.

   Se houver um erro durante o processo de atualização, uma mensagem de banner lista o número de nós que não conseguiram alterar suas senhas. O sistema irá tentar novamente automaticamente o processo em qualquer nó que não tenha a sua palavra-passe alterada. Se o processo terminar com alguns nós ainda não tendo uma senha alterada, o botão **Repetir** será exibido.

   Se a atualização da palavra-passe tiver falhado para um ou mais nós:

   a. Reveja as mensagens de erro listadas na tabela.

   b. Resolva os problemas.

   c. Selecione **Repetir**.

   > A tentativa de novo 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 tiverem sido alteradas para todos os nós, exclua o primeiro pacote de recuperação que você baixou.
7. Opcionalmente, use o link **Recovery package** para baixar uma cópia adicional do novo pacote de recuperação.

Use a federação de identidade

O uso da federação de identidade torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configure a federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Gerenciador de Grade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, Azure ative Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Você está usando o ative Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.

  Se pretender utilizar um serviço LDAP v3 que não esteja listado, contacte o suporte técnico.

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Diretrizes para configurar um servidor OpenLDAPConsulte .
- Se você planeja habilitar o logon único (SSO), revisou o "requisitos e considerações para logon único".
- Se você planeja usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1,2 ou 1,3. "Cifras suportadas para conexões TLS de saída"Consulte .

Sobre esta tarefa

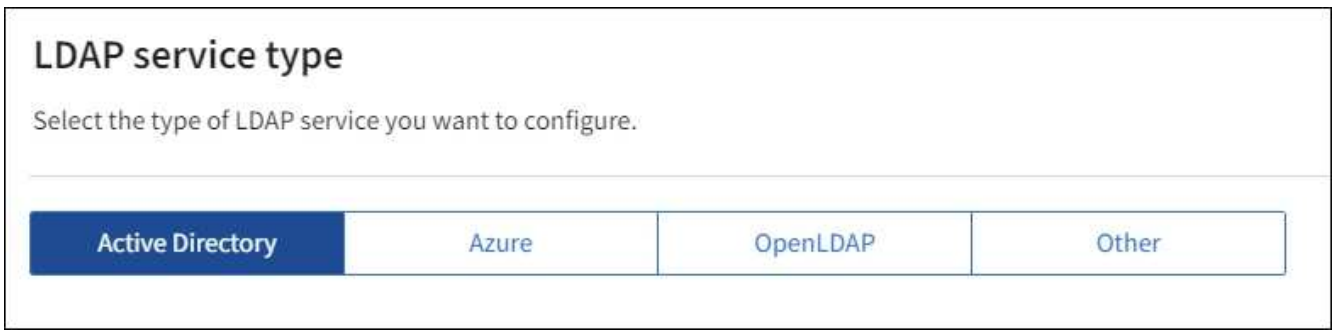
Você pode configurar uma fonte de identidade para o Gerenciador de Grade se quiser importar grupos de outro sistema, como ative Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- Grupos de administração. Os usuários nos grupos de administração podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários que não usam sua própria fonte de identidade. Os usuários em grupos de inquilinos podem entrar no Gerenciador de inquilinos e executar tarefas, com base nas permissões atribuídas ao grupo no Gerenciador de inquilinos. "Crie uma conta de locatário"Consulte e "Use uma conta de locatário" para obter detalhes.

Introduza a configuração

Passos

1. Selecione **CONFIGURATION** > **access control** > **Identity Federation**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.



Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, 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 `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Group Unique Name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
   - **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
5. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.
   - **Nome de host**: O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar 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) para o usuário que se conetará ao servidor LDAP.

     No ative 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 para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`
     - **Ative Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
     - **Azure**: `accountEnabled` E. `userPrincipalName`
   - **Senha**: A senha associada ao nome de usuário.
   - **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

> Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

- **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

> Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN da base de usuários** a que pertencem.

- **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

  É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

  Introduza um destes padrões:

  - **Padrão UserPrincipalName (ative Directory e Azure)**: `[USERNAME]@example.com`
  - * Padrão de nome de logon de nível inferior (ative 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 Transport Layer Security (TLS), selecione uma configuração de segurança.
   - **Use STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para ative Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa 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 para o Azure.

> O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

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

     Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

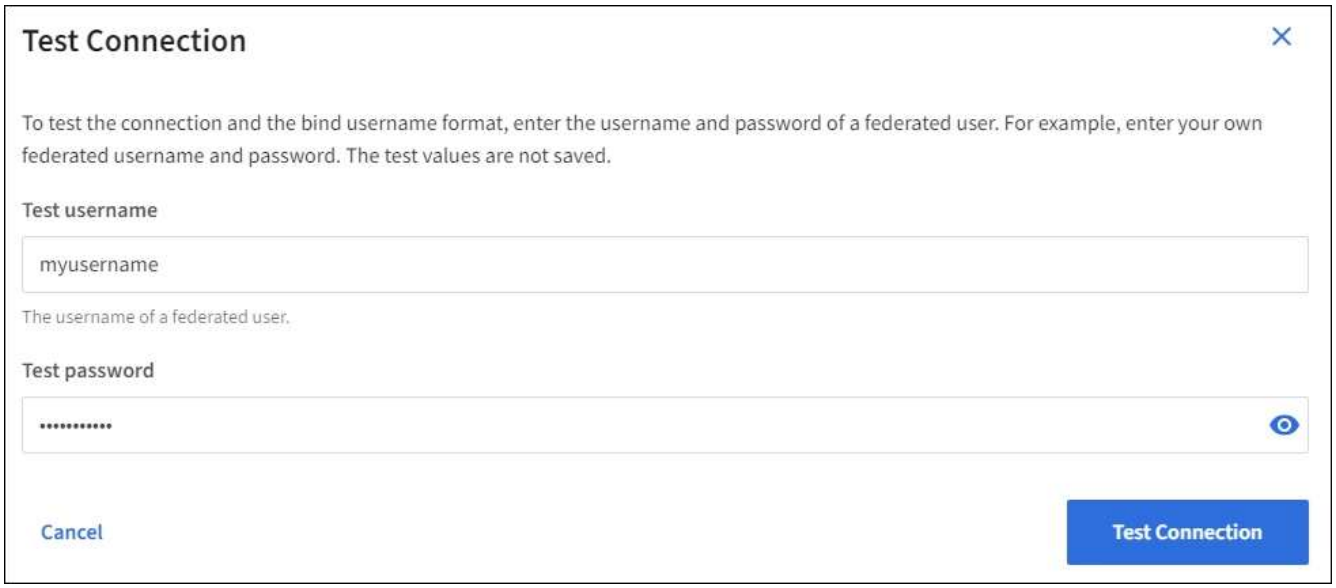
Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

Passos

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem "'test Connection could not be established'" (não foi possível estabelecer ligação) é apresentada se as definições de ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de um usuário federado válido.

   Por exemplo, insira seu próprio nome de usuário e senha. Não inclua carateres especiais no nome de usuário, como em ou /.



   - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
   - Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar a sincronização com a fonte de identidade

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

Passos

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

   O processo de sincronização pode demorar algum tempo, dependendo do ambiente.

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

Desativar a federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desativada, não há comunicação entre o StorageGRID e a fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

Sobre esta tarefa

Antes de desativar a federação de identidade, você deve estar ciente do seguinte:

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o 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 origem da identidade não ocorrerá e os alertas ou alarmes não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Ativar federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. "Desative o logon único"Consulte .

Passos

1. Vá para a página de 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, você deve configurar configurações específicas no servidor OpenLDAP.

Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário ou remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "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 do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no "Documentação do OpenLDAP: Guia do administrador da versão 2,4".

Gerenciar grupos de administradores

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Crie um grupo de administração

Os grupos de administração permitem determinar quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
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 origem da identidade.

Grupo local

Passos

1. Selecione **local group**.
2. Introduza um nome de apresentação para o grupo, que pode atualizar posteriormente, conforme necessário. Por exemplo, "'usuários de Manutenção'" ou "'Administradores de ILM.'"
3. Introduza um nome exclusivo para o grupo, que não pode atualizar mais tarde.
4. Selecione **continuar**.

Grupo federado

Passos

1. Selecione **Federated Group**.
2. Introduza o nome do grupo que pretende importar, exatamente como aparece na origem de identidade configurada.
   - Para o ative Directory e 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 Gerenciador de Grade e na API de Gerenciamento de Grade ou se eles só podem exibir configurações e recursos.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de 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 entrar no StorageGRID.

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

Passos

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

Se ainda não tiver criado utilizadores locais, pode guardar o grupo sem adicionar utilizadores. Pode adicionar este grupo ao utilizador na página utilizadores. "Gerenciar usuários"Consulte para obter detalhes.

2. Selecione **criar grupo** e **concluir**.

Exibir e editar grupos de administração

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

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

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

Duplicar um grupo

Passos

1. Selecione a caixa de verificação para o grupo.
2. Selecione **ações** > **grupo duplicado**.
3. Conclua o assistente de grupo duplicado.

Eliminar um grupo

Você pode excluir um grupo de administração quando quiser remover o grupo do sistema e remover todas as permissões associadas ao grupo. A exclusão de um grupo de administração remove todos os usuários do grupo, mas não exclui os usuários.

Passos

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

Permissões do grupo de administração

Ao criar grupos de usuários admin, você seleciona uma ou mais permissões para controlar o acesso a recursos específicos do Gerenciador de Grade. Em seguida, você pode atribuir cada usuário a um ou mais desses grupos de administração para determinar quais tarefas o usuário pode executar.

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão entrar no Gerenciador de Grade ou na API de Gerenciamento de Grade.

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

- Faça login no Gerenciador de Grade
- Visualizar o painel de instrumentos
- Exibir as páginas de nós
- Monitore a topologia da grade
- Ver alertas atuais e resolvidos
- Visualizar alarmes atuais e históricos (sistema legado)
- Alterar sua própria senha (somente usuários locais)
- Visualize determinadas informações fornecidas nas páginas 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 configurações e executar operações ou se eles podem exibir somente as configurações e 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 mencionada explicitamente requer a permissão **Root Access**.

Acesso à raiz

Essa permissão fornece acesso a todos os recursos de administração de grade.

Reconhecer alarmes (legado)

Esta permissão fornece acesso para reconhecer e responder a alarmes (sistema legado). Todos os usuários conetados podem visualizar alarmes atuais e históricos.

Se você quiser que um usuário monitore a topologia da grade e reconheça somente alarmes, você deve atribuir essa permissão.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página de locatários, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Essa permissão também é usada para migrar chaves S3 quando o recurso de importação de chaves S3 estiver ativado. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

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

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPPORT** > **Tools** > **Grid topology**.

ILM

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

- Regras
- Políticas
- Codificação de apagamento
- Regiões
- Pools de armazenamento

> Os usuários devem ter as permissões **outras configurações de grade** e **Configuração de página de topologia de grade** para gerenciar as notas de armazenamento.

Manutenção

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

- **CONFIGURAÇÃO** > **controlo de acesso**:
  - Senhas de grade
- **CONFIGURAÇÃO** > **rede**:
  - S3 nomes de domínio de endpoint
- **MANUTENÇÃO** > **tarefas**:
  - Descomissionar
  - Expansão
  - Verificação de existência do objeto
  - Recuperação

- **MANUTENÇÃO** > **sistema**:
  - Pacote de recuperação
  - Atualização de software
- **SUPORTE** > **Ferramentas**:
  - Registos

Os usuários que não têm a permissão Manutenção podem visualizar, mas não editar, estas páginas:

- **MANUTENÇÃO** > **rede**:
  - Servidores DNS
  - Rede de rede
  - Servidores NTP
- **MANUTENÇÃO** > **sistema**:
  - Licença
- **CONFIGURAÇÃO** > **rede**:
  - S3 nomes de domínio de endpoint
- **CONFIGURAÇÃO** > **Segurança**:
  - Certificados
- **CONFIGURAÇÃO** > **Monitoramento**:
  - Servidor de auditoria e syslog

Gerenciar alertas

Essa permissão fornece acesso a opções de gerenciamento de 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** > **métricas** página
- Consultas de métricas personalizadas do Prometheus usando a seção **Metrics** da API Grid Management
- Cartões de painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM** > **Object metadata lookup**.

Outra configuração de grade

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

Para ver essas opções adicionais, os usuários também devem ter a permissão **Grid topology page Configuration**.

- **ILM**:

    - Classes de armazenamento
- **CONFIGURAÇÃO** > **sistema**:
    - Opções de armazenamento
- **SUPORTE** > **Alarmes (legado)**:
    - Eventos personalizados
    - Alarmes globais
    - Configuração de e-mail legado
- **SUPORTE** > **outro**:
    - Custo da ligação

Administrador do dispositivo de storage

Essa permissão fornece acesso ao Gerenciador de sistemas do e-Series SANtricity em dispositivos de storage por meio do Gerenciador de Grade.

Contas de inquilino

Essa permissão permite:

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

Gerenciar usuários

Você pode exibir usuários locais e federados. Você também pode criar usuários locais e atribuí-los a grupos de administração locais para determinar quais recursos do Gerenciador de Grade esses usuários podem acessar.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Crie 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 Gerenciador de Grade e da API de Gerenciamento de Grade o usuário pode acessar.

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

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Você não pode remover o usuário raiz.

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

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Access Control** > **Admin Users**.
2. Selecione **criar usuário**.

Introduza as credenciais do utilizador

Passos

1. Introduza o nome completo do utilizador, um nome de utilizador exclusivo e uma palavra-passe.
2. Opcionalmente, selecione **Sim** se esse usuário não tiver acesso ao Gerenciador de Grade ou à API de Gerenciamento de Grade.
3. Selecione **continuar**.

Atribuir a grupos

Passos

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

   Se ainda não tiver criado grupos, pode guardar o utilizador sem selecionar grupos. Você pode adicionar esse usuário a um grupo na página grupos.

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

2. Selecione **Create user** e selecione **Finish**.

Ver e editar utilizadores locais

Você pode exibir detalhes de usuários locais e federados existentes. Você pode modificar um usuário local para alterar o nome completo, a senha ou a associação de grupo do usuário. Você também pode impedir temporariamente que um usuário acesse o Gerenciador de Grade e a API de Gerenciamento de Grade.

Só pode editar utilizadores locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para exibir informações básicas para 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 são aplicadas na próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

> Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do utilizador	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Editar nome completo**. c. Introduza o novo nome. d. Selecione **Salvar alterações**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Salvar alterações**.
Negar ou permitir acesso à StorageGRID	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Acesso. d. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, 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 guia Acesso. c. Selecione **Sim** para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione **não** para permitir que o usuário faça login. d. Selecione **Salvar alterações**.
Alterar palavra-passe (apenas utilizadores locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia Senha. d. Introduza uma nova palavra-passe. e. Selecione **alterar palavra-passe**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Introduza uma nova palavra-passe. d. Selecione **alterar palavra-passe**.

Tarefa	Menu ações	Página de detalhes
Alterar grupos (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione **ações** > **Exibir detalhes do usuário**. c. Selecione a guia grupos. d. Opcionalmente, selecione o link após um nome de grupo para exibir 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 guia grupos. c. Opcionalmente, selecione o link após um nome de grupo para exibir 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. Selecione a caixa de verificação para o utilizador.
2. Selecione **ações** > **usuário duplicado**.
3. Conclua o assistente de usuário duplicado.

Eliminar um utilizador

Você pode excluir um usuário local para remover permanentemente esse usuário do sistema.

Não é possível excluir o usuário raiz.

Passos

1. Na página usuários, marque a caixa de seleção para cada usuário que deseja remover.
2. Selecione **ações** > **Excluir usuário**.
3. Selecione **Eliminar utilizador**.

Usar logon único (SSO)

Configurar o logon único

Quando o logon único (SSO) está ativado, os usuários só podem acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de gerenciamento de grade ou a API de gerenciamento de locatário se suas credenciais forem autorizadas usando o processo de login SSO implementado pela sua organização. Os usuários locais não podem entrar no StorageGRID.

Como o single sign-on funciona

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0).

Antes de ativar o SSO (logon único), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está ativado.

Inicie sessão quando o SSO estiver ativado

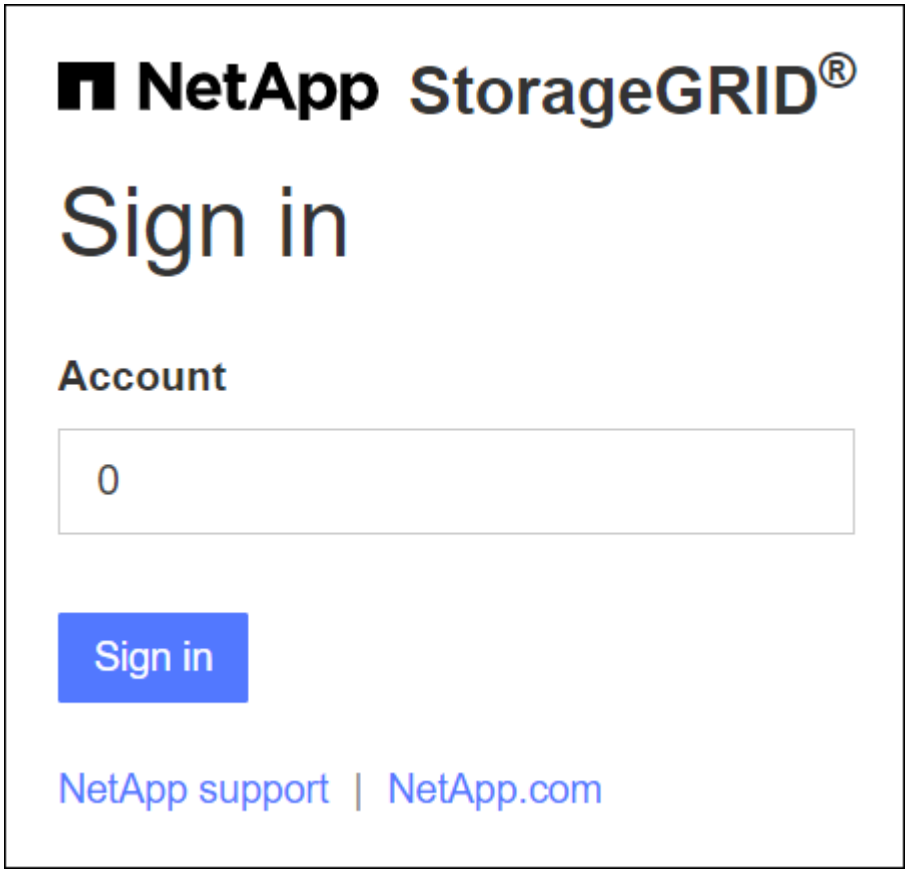
Quando o SSO está ativado e você entra no StorageGRID, você é redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

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

   É apresentada a página de início de sessão do StorageGRID.

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

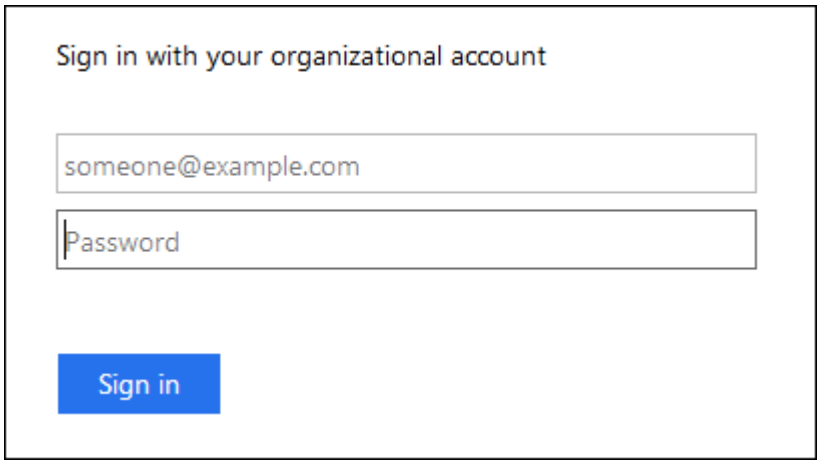


   - Se você acessou anteriormente o Gerenciador de Grade ou o Gerente do Locatário, será solicitado que você selecione uma conta recente ou insira um ID de conta:

A página de login 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 de `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da sua organização, onde você pode Inicie sessão com as suas credenciais SSO.

2. Indique se deseja acessar o Gerenciador de Grade ou o Gerenciador de Locatário:
   - Para acessar o Gerenciador de Grade, deixe o campo **ID de conta** em branco, digite **0** como ID de conta ou selecione **Gerenciador de Grade** se ele aparecer na lista de contas recentes.
   - Para acessar o Gerenciador do Locatário, insira o ID da conta do locatário de 20 dígitos ou selecione um locatário pelo nome se ele aparecer na lista de contas recentes.
3. Selecione **entrar**

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



4. Faça login com suas credenciais SSO.

Se suas credenciais 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 estará conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário, dependendo da conta selecionada.

> Se a conta de serviço estiver inacessível, você ainda poderá fazer login, contanto que você 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 Gerenciador de grade ou o Gerenciador de locatário, se você tiver permissões adequadas.

   Você não precisa reinserir suas credenciais SSO.

Sair quando o SSO estiver ativado

Quando o SSO está ativado para o StorageGRID, o que acontece quando você sai depende do que você está conetado e de onde você está se saindo.

Passos

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

   É apresentada a página de início de sessão do StorageGRID. A lista suspensa **Recent Accounts** (Contas recentes) é atualizada para incluir o **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conetado a…	E você sai de…	Você está logado fora de…
Grid Manager em um ou mais nós de administração	Grid Manager em qualquer nó de administração	Grid Manager em todos os nós de administração **Observação:** se você usar o Azure para SSO, pode levar alguns minutos para ser desconetado de todos os nós de administração.
Gerenciador de locatários em um ou mais nós de administração	Gerente de locatário em qualquer nó de administrador	Gerenciador de locatários em todos os nós de administração
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Apenas o Grid Manager. Você também deve sair do Gerenciador do Locatário para sair do SSO.

A tabela resume o que acontece quando você sai se estiver usando uma única sessão do navegador. Se você estiver conetado 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 ativar 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 ative Directory (AD FS)
- Azure ative Directory (Azure AD)
- PingFederate

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

Requisitos do AD FS

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

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

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

- AD FS 3,0, incluído na atualização do Windows Server 2012 R2 ou superior.

Requisitos adicionais

- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Considerações para o Azure

Se você usar o Azure como o tipo SSO e os usuários tiverem nomes principais de usuário que não usam o sAMAccountName como prefixo, problemas de login podem ocorrer se o StorageGRID perder sua conexão com o servidor LDAP. Para permitir que os utilizadores iniciem sessão, tem de restaurar a ligação ao servidor LDAP.

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado de interface de gerenciamento em cada nó de administrador para proteger o acesso ao Gerenciador de Grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento de locatário. Quando você configura confiança de parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado de servidor como o certificado de assinatura para solicitações StorageGRID.

Se ainda não "configurado um certificado personalizado para a interface de gerenciamento"o fez, deve fazê-lo 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 partes dependentes do StorageGRID, aplicativos empresariais ou conexões SP.

> ⓘ O uso do certificado de servidor padrão de um nó de administrador em uma conexão de confiança de parte confiável, aplicativo empresarial ou SP não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de iniciar sessão no nó recuperado, tem de atualizar a confiança de parte fidedigna, a aplicação empresarial ou a ligação SP com o novo certificado.

Você pode acessar o certificado de servidor de um nó de administrador fazendo login no shell de comando do nó e indo para `/var/local/mgmt-api` o diretório. Um certificado de servidor personalizado é `custom-server.crt` nomeado . O certificado de servidor padrão do nó é `server.crt` nomeado .

Requisitos portuários

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único. "Controle o acesso no firewall externo"Consulte .

Confirme se os usuários federados podem entrar

Antes de ativar o logon único (SSO), você deve confirmar que pelo menos um usuário federado pode entrar no Gerenciador de Grade e entrar no Gerenciador de locatários para quaisquer contas de locatário existentes.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Você já configurou a federação de identidade.

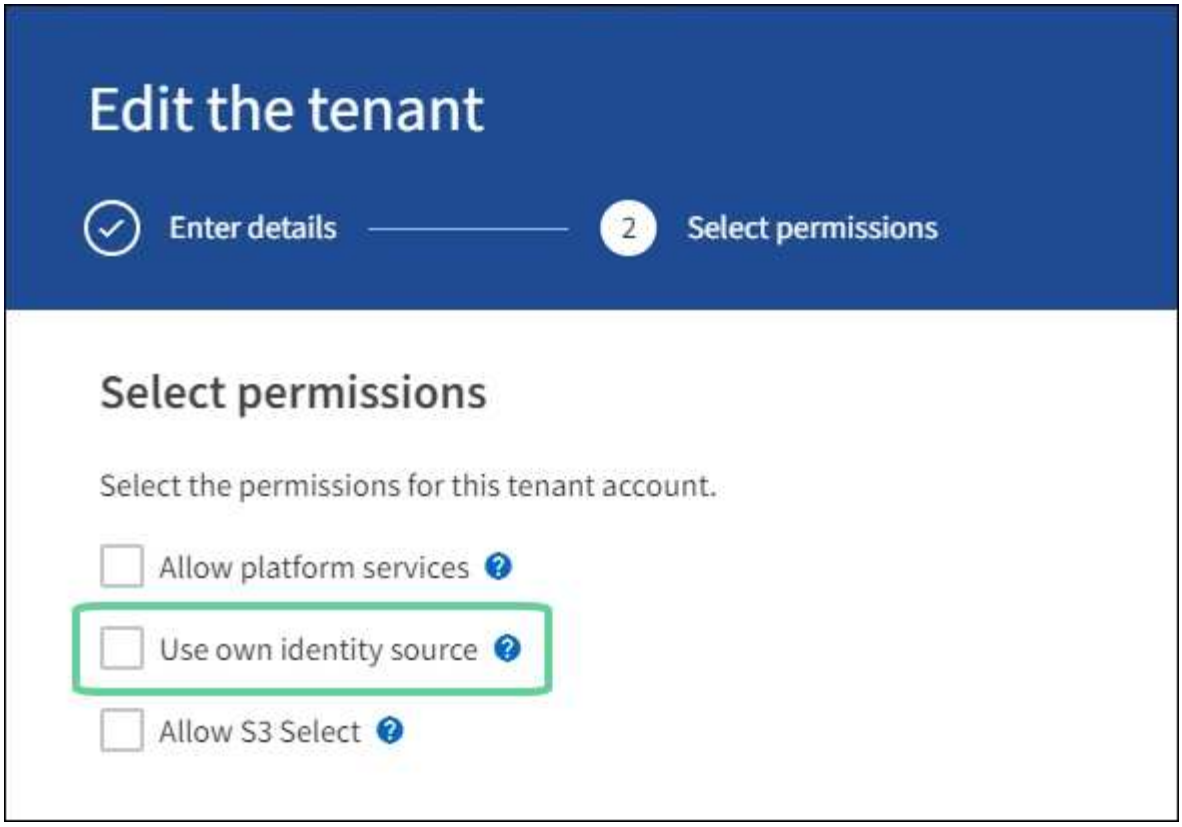
Passos

1. Se houver contas de inquilino existentes, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.

Quando você ativa o SSO, uma fonte de identidade configurada no Gerenciador de locatário é substituída pela origem de identidade configurada no Gerenciador de Grade. Os usuários pertencentes à fonte de identidade do locatário não poderão mais entrar a menos que tenham uma conta com a fonte de identidade do Gerenciador de Grade.

a. Inicie sessão no Gestor do Locatário para cada conta de inquilino.
b. Selecione **GERENCIAMENTO DE ACESSO** > **federação de identidade**.
c. Confirme se a caixa de verificação **Ativar federação de identidade** não está selecionada.
d. Se estiver, confirme se os grupos federados que possam estar em uso para essa conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.

2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
   a. No Gerenciador de Grade, selecione **CONFIGURATION** > **Access Control** > **Admin Groups**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da origem de identidade do ative Directory e de que tenha sido atribuída a permissão de acesso raiz.
   c. Terminar sessão.
   d. Confirme que você pode fazer login novamente no Gerenciador de Grade como um usuário no grupo federado.
3. Se houver contas de locatário existentes, confirme se um usuário federado que tenha permissão de acesso root pode entrar:
   a. No Gerenciador de Grade, selecione **TENANTS**.
   b. Selecione a conta de locatário e selecione **ações** > **Editar**.
   c. Na guia Inserir detalhes, selecione **continuar**.
   d. Se a caixa de seleção **Use own Identity source** estiver selecionada, desmarque a caixa e selecione **Save**.



É apresentada a página do locatário.

a. Selecione a conta de locatário, selecione **entrar** e faça login na conta de locatário como usuário raiz local.
b. No Gerenciador do Locatário, selecione **GERENCIAMENTO DE ACESSO** > **grupos**.
c. Certifique-se de que pelo menos um grupo federado do Gerenciador de Grade recebeu a permissão de acesso raiz para esse locatário.
d. Terminar sessão.
e. Confirme que 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 locatário"

Use 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. Depois que o SSO estiver ativado, você poderá retornar ao modo sandbox sempre que precisar alterar ou testar novamente a configuração.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

- Você configurou a federação de identidade para o seu sistema StorageGRID.
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou o ative Directory ou o Azure, com base no provedor de identidade SSO que você planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ative Directory	• Ative Directory • Azure • PingFederate
Azure	Azure

Sobre esta tarefa

Quando o SSO está ativado e um usuário tenta entrar em um nó de administrador, o StorageGRID envia uma solicitação de autenticação para o provedor de identidade 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 ative Directory ou PingFederate inclui um identificador universal único (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal de 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 de usuário, você deve configurar certas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma confiança de parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. Finalmente, você deve retornar ao StorageGRID para ativar o SSO.

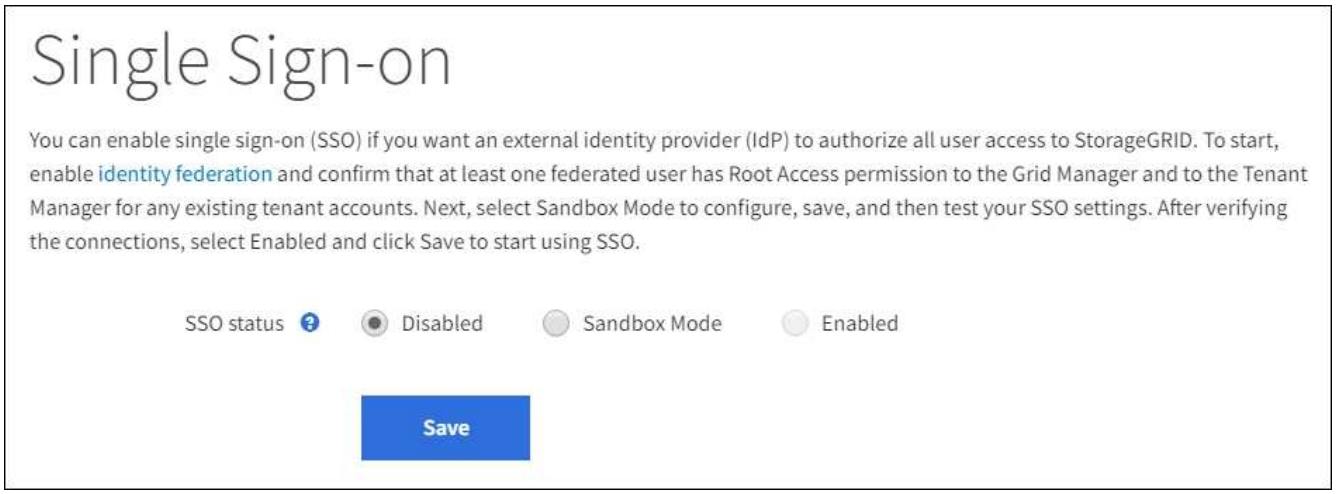
O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO. Quando você está usando o modo sandbox, os usuários não podem entrar usando SSO.

Acesse o modo sandbox

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

   A página Single Sign-On (Início de sessão único) é exibida, com a opção **Disabled** selecionada.



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

2. Selecione **Sandbox Mode**.

   A seção Provedor de identidade é exibida.

Insira os detalhes do provedor de identidade

Passos

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

Ative Directory

1. Digite o nome do serviço **Federation** para o provedor de identidade, exatamente como aparece no ative Directory Federation Service (AD FS).

   Para localizar o nome do serviço de federação, vá para Gerenciador do Windows Server. Selecione **Ferramentas** > **Gerenciamento do AD FS**. No menu Ação, selecione **Editar Propriedades do Serviço de Federação**. O Nome do Serviço de Federação é apresentado no segundo campo.

2. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.
   - **Use o 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 essa 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.
3. Na seção parte dependente, especifique o **identificador de parte dependente** para StorageGRID. Esse valor controla o nome que você usa para cada confiança de parte confiável no AD FS.
   - Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
   - Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra o identificador de parte confiável para cada nó Admin em seu sistema, com base no nome do host do nó.

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

4. Selecione **Guardar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Azure

1. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.
   - **Use o 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 essa 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.

2. Na seção aplicativo empresarial, especifique o **Nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo corporativo no Azure AD.
   - Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
   - Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra um nome de aplicativo corporativo para cada nó Admin em seu sistema, com base no nome do host do nó.

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

3. Siga as etapas em "Crie aplicativos empresariais no Azure AD" para criar um aplicativo corporativo para cada nó de administração listado na tabela.
4. No Azure AD, copie o URL de metadados da federação para cada aplicativo corporativo. Em seguida, cole esse URL no campo **URL de metadados de Federação** correspondente no StorageGRID.
5. Depois de copiar e colar um URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

PingFederate

1. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.
   - **Use o 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 essa 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.
2. Na seção Fornecedor de Serviços (SP), especifique o **ID de conexão SP** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP no PingFederate.
   - Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
   - Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por

exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra o ID de conexão do SP para cada nó de administrador no sistema, com base no nome do host do nó.

> Você deve criar uma conexão SP para cada nó de administração no 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.

3. Especifique o URL de metadados de federação para cada nó Admin no campo **URL de metadados de Federação**.

   Use o seguinte formato:

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

4. Selecione **Guardar**.

   Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.

Configurar trusts de terceiros confiáveis, aplicativos empresariais ou conexões SP

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

O StorageGRID pode permanecer no modo sandbox enquanto necessário. No entanto, quando **modo Sandbox** está selecionado na página de logon único, o SSO é desativado para todos os usuários do StorageGRID. Somente usuários locais podem fazer login.

Siga estas etapas para configurar as trusts de parte confiável (ative Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Ative Directory

Passos

1. Vá para Serviços de Federação do ative Directory (AD FS).
2. Crie uma ou mais confianças de parte confiáveis 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 Admin mostrado na tabela.

   Para obter instruções, vá "Criar confiança de parte confiável no AD FS"para .

Azure

Passos

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para o Portal do Azure.
4. Siga as etapas em "Crie aplicativos empresariais no Azure AD" para carregar o arquivo de metadados SAML para cada nó Admin em seu aplicativo corporativo do Azure correspondente.

PingFederate

Passos

1. Na página de logon único para o nó Admin ao qual você está conetado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Vá para PingFederate.
4. "Crie uma ou mais conexões de provedor de serviços (SP) para o StorageGRID". Use o ID de conexão do SP para cada nó de administrador (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administrador.

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

Testar conexões SSO

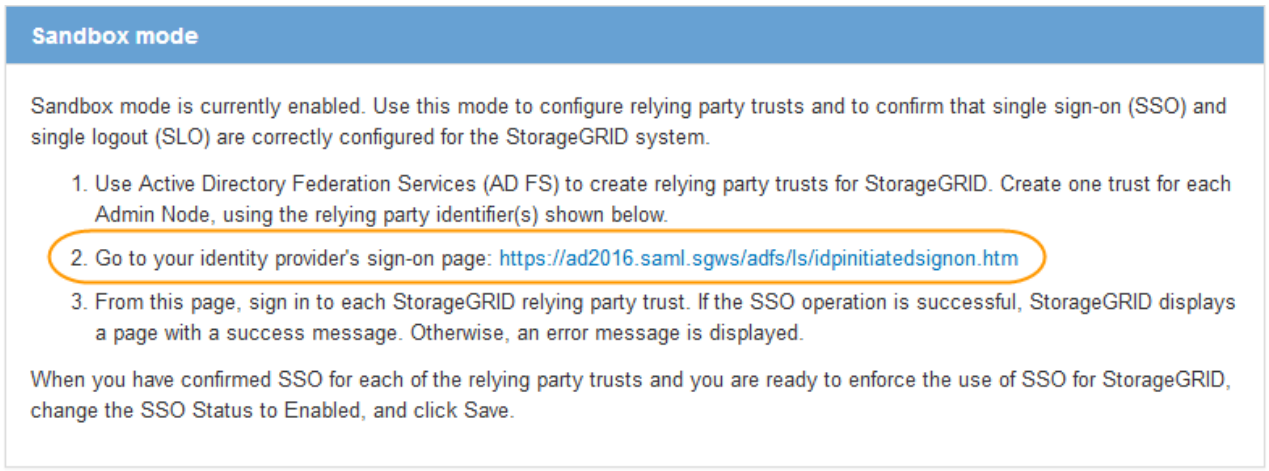
Antes de aplicar o uso de logon único para todo o sistema StorageGRID, você deve confirmar que o logon único e o logout único estão configurados corretamente para cada nó de administração.

Ative Directory

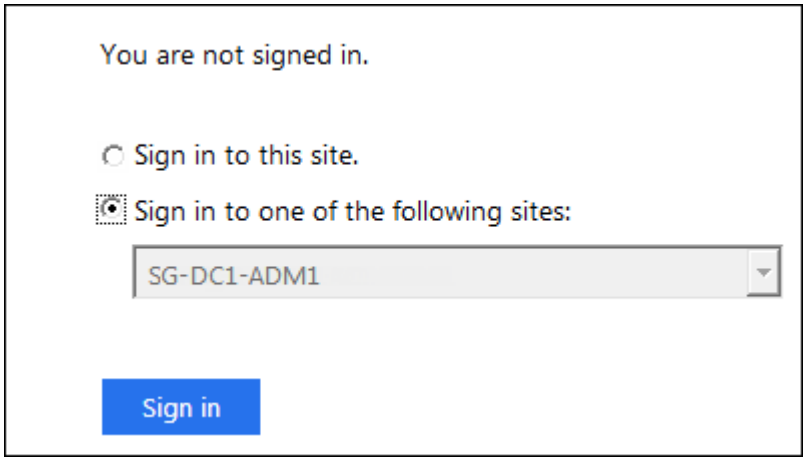
Passos

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

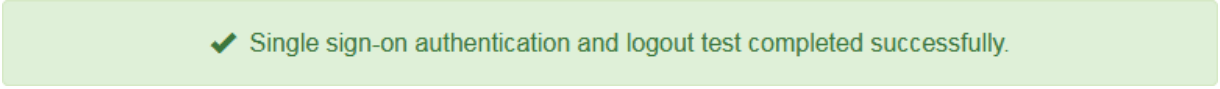
   O URL é derivado do valor inserido no campo **Nome do serviço de Federação**.



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



4. Introduza o seu nome de utilizador federado e a palavra-passe.
   - Se as operações de login e logout SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.



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

Azure

Passos

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

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

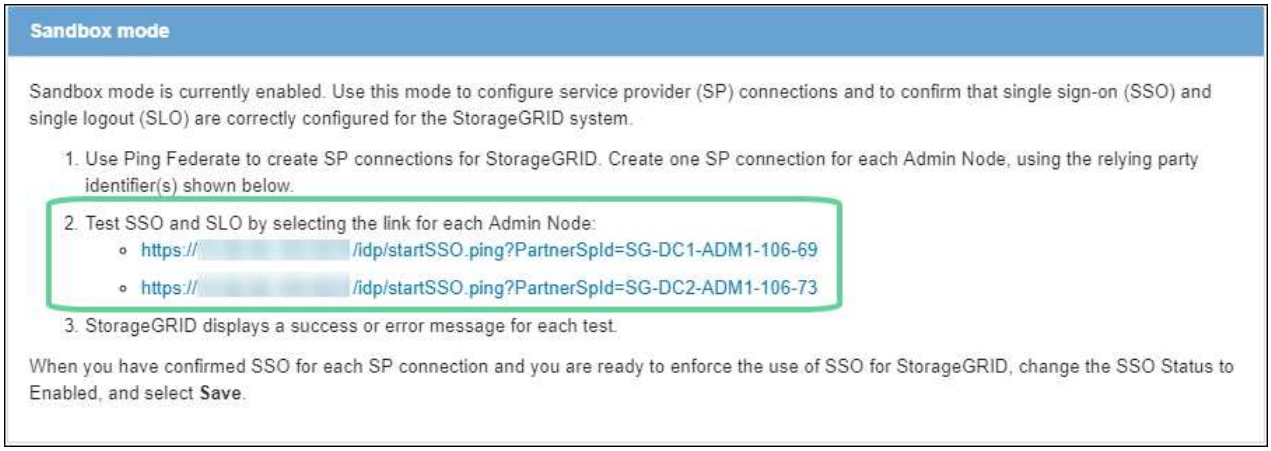
   - Se a operação SSO não for bem-sucedida, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
4. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

PingFederate

Passos

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

   Selecione e teste um link de cada vez.



2. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout 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, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o próximo link para verificar a conexão SSO para cada nó Admin na grade.

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

Ative o logon único

Quando você confirmar que pode usar o SSO para fazer login em cada nó de administrador, você pode ativar o SSO para todo o seu sistema StorageGRID.

> Quando o SSO está ativado, todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade e a API de Gerenciamento de Locatário. Os usuários locais não podem mais acessar o StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
2. Altere o Status SSO para **Enabled**.
3. Selecione **Guardar**.
4. Reveja a mensagem de aviso e selecione **OK**.

   O início de sessão único está agora ativado.

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

Criar confiança de parte confiável no AD FS

Você deve usar os Serviços de Federação do ative Directory (AD FS) para criar uma confiança de parte confiável para cada nó de administração em seu sistema. Você pode criar trusts confiáveis de parte 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 SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de entidade dependente 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 confiança de parte confiável para cada nó de administrador no seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

- Você tem experiência em criar confiança de parte confiável 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 de parte confiável manualmente, você tem o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou sabe como fazer login em um nó de administrador a partir do shell de comando.

Sobre esta tarefa

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

Crie uma confiança de parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais trusts de parte confiáveis.

Passos

1. No menu Iniciar do Windows, selecione o ícone do PowerShell com o botão direito 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 de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, `SG-DC1-ADM1`.
   - Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)
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** > **confiar em parts**.

   É apresentada a lista de confianças de partes dependentes.
5. Adicione uma Política de Controle de Acesso à confiança da entidade dependente recém-criada:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na fidedignidade e selecione **Editar política de controlo de acesso**.
   c. Selecione uma política de controlo de acesso.
   d. Selecione **aplicar** e **OK**
6. Adicione uma Política de emissão de reclamação à recém-criada confiança da parte dependente:
   a. Localize a confiança de quem confia que você acabou de criar.
   b. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
   c. Selecione **Adicionar regra**.
   d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **Avançar**.
   e. Na página Configurar regra, insira um nome de exibição para essa regra.

      Por exemplo, **ObjectGUID to Name ID**.

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

g. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.

h. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

i. Selecione **Finish** e **OK**.

7. Confirme se os metadados foram importados com sucesso.

a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.

b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** 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 confiança de parte confiável para todos os nós de administração no sistema StorageGRID.

9. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo Sandbox"Consulte para obter instruções.

Crie uma confiança de parte confiável importando metadados de federação

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

Passos

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

2. Em ações, selecione **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.

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

5. Em **Endereço de metadados de 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`*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

6. Conclua o assistente confiar na parte confiável, salve a confiança da parte confiável e feche o assistente.

> Ao inserir o nome de exibição, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

7. Adicionar uma regra de reclamação:

a. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.

b. Selecione **Adicionar regra**:

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

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

   Por exemplo, **ObjectGUID to Name ID**.

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

f. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.

g. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.

h. Selecione **Finish** e **OK**.

8. Confirme se os metadados foram importados com sucesso.

   a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.

   b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** 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 confiança de parte confiável para todos os nós de administração no sistema StorageGRID.

10. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo Sandbox"Consulte para obter instruções.

Crie uma confiança de parte confiável manualmente

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

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e **Gerenciamento do AD FS**.
2. Em ações, selecione **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.
4. Selecione **Digite os dados sobre a parte que depende manualmente** e selecione **Next**.
5. Conclua o assistente confiança da parte dependente:

   a. Introduza um nome de apresentação para este nó de administração.

      Para obter consistência, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. 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 o URL do endpoint do serviço SAML para o nó Admin:

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

Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o nó Admin. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

e. Na página Configurar Identificadores, especifique o Identificador da parte de dependência para o mesmo nó de administração:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão 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 reclamação é exibida.

Se a caixa de diálogo não for exibida, clique com o botão direito do Mouse no Trust e selecione **Editar política de emissão de reclamação**.

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

      Por exemplo, **ObjectGUID to Name ID**.

   c. Para o Attribute Store, selecione **ative Directory**.
   d. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   e. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   f. Selecione **Finish** e **OK**.
7. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
   a. Selecione **Adicionar SAML**.
   b. Selecione **Endpoint Type** > **SAML Logout**.
   c. Selecione **Binding** > **Redirect**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó Admin:

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

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

   a. Selecione **OK**.
9. Na guia **assinatura**, especifique o certificado de assinatura para essa confiança de parte confiável:

a. Adicione o certificado personalizado:

   - Se tiver o certificado de gestão personalizado que carregou no StorageGRID, selecione esse certificado.
   - Se você não tiver o certificado personalizado, faça login no Admin Node, vá para `/var/local/mgmt-api` o diretório do Admin Node e adicione o `custom-server.crt` arquivo de certificado.

     Observação: usando o certificado padrão do Admin Node (`server.crt`) não é recomendado. Se o nó Admin falhar, o certificado padrão será regenerado quando você recuperar o nó e você precisará atualizar a confiança da parte confiável.

b. Selecione **aplicar** e **OK**.

   As propriedades da parte dependente são salvas e fechadas.

10. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
11. Quando terminar, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. "Use o modo sandbox"Consulte para obter instruções.

Crie aplicativos empresariais no Azure AD

Você usa o Azure AD para criar um aplicativo corporativo para cada nó de administrador no sistema.

Antes de começar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você tem o **Nome do aplicativo Enterprise** para cada nó Admin no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.

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

- Você tem experiência em criar aplicativos empresariais no Azure ative 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 do responsável do serviço.

Acesse o Azure AD

Passos

1. Inicie sessão no "Portal do Azure".
2. Navegue até "Azure ative Directory".
3. "Aplicações empresariais"Selecione .

Crie aplicativos empresariais e salve a configuração SSO do StorageGRID

Para salvar a configuração SSO para o Azure no StorageGRID, você deve usar o Azure para criar um aplicativo corporativo para cada nó de administração. Você copiará os URLs de metadados da federação do Azure e os 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 Admin.
   a. No painel aplicativos do Azure Enterprise, selecione **novo aplicativo**.
   b. Selecione **Crie seu próprio aplicativo**.
   c. Para o nome, insira o **Nome do aplicativo da empresa** que você copiou da tabela de detalhes do nó de administrador 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 **Get Started** no **2. Configure a caixa Single Sign On** (Início de sessão único) ou selecione o link **Single Sign-On** (Início de sessão único) na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o URL de metadados de Federação de aplicativos*, que você pode encontrar em **Etapa 3 certificado de assinatura SAML**.
   i. Vá para a página de logon único do StorageGRID e cole o URL no campo **URL de metadados da Federação** que corresponde ao nome do aplicativo **empresa** que você usou.
2. Depois de colar um URL de metadados de federação para cada nó de administrador e fazer todas as outras alterações necessárias na configuração SSO, selecione **Salvar** na página de logon único do StorageGRID.

Faça o download dos metadados SAML para cada nó de administração

Depois que a configuração SSO for salva, você pode baixar um arquivo de metadados SAML para cada nó de administrador no sistema StorageGRID.

Passos

1. Repita estas etapas para cada nó Admin.
   a. Inicie sessão no StorageGRID a partir do nó de administração.
   b. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   c. Selecione o botão para baixar os metadados SAML para esse nó Admin.
   d. Salve o arquivo, que você carregará no Azure AD.

Carregue metadados SAML para cada aplicação empresarial

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

Passos

1. Retorne ao Portal do Azure.
2. Repita estes passos para cada aplicação empresarial:

Talvez seja necessário atualizar a página aplicativos empresariais para ver os aplicativos adicionados anteriormente na lista.

a. Vá para a página Propriedades do aplicativo corporativo.
b. Defina **atribuição necessária** como **não** (a menos que você queira configurar atribuições separadamente).
c. Aceda à página de início de sessão único.
d. Conclua a configuração SAML.
e. Selecione o botão **Upload metadata file** e selecione o arquivo de metadados SAML que você baixou para o Admin Node correspondente.
f. Depois que o arquivo for carregado, selecione **Save** e, em seguida, selecione **X** para fechar o painel. Você será retornado à página Configurar logon único com SAML.

3. Siga os passos em "Use o modo sandbox" para testar cada aplicação.

Crie conexões de provedor de serviços (SP) no PingFederate

Você usa o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administrador 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 SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. "Use o modo sandbox"Consulte .
- Você tem o **ID de conexão SP** para cada nó de administrador no 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 Admin no seu sistema.
- Você tem experiência em criar conexões SP no servidor PingFederate.
- Você tem o "Guia de referência do administrador" para PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem a permissão Admin para PingFederate Server.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10,3 como um provedor SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar essas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas sobre o seu lançamento.

Complete pré-requisitos 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 as informações desses pré-requisitos quando configurar as conexões SP.

Criar armazenamento de dados

Se você ainda não o fez, crie um armazenamento de dados para conetar o PingFederate ao servidor LDAP do

AD FS. Use os valores usados "configurando a federação de identidade"no StorageGRID.

- * Tipo*: Diretório (LDAP)
- **Tipo LDAP**: Ative Directory
- **Nome do atributo binário**: Insira **objectGUID** na guia atributos binários LDAP exatamente como mostrado.

Criar validador de credenciais de senha

Se você ainda não o fez, crie um validador de credenciais de senha.

- **Type**: LDAP Username Password Credential Validator
- **Armazenamento de dados**: Selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: Insira informações do LDAP (por exemplo,
- **Filtro de pesquisa**: SAMAccountName
- **Escopo**: Subárvore

Criar instância de adaptador IDP

Se você ainda não o fez, crie uma instância de adaptador IDP.

Passos

1. Aceda a **Autenticação** > **integração** > **adaptadores IDP**.
2. Selecione **criar nova instância**.
3. Na guia tipo, selecione **HTML form IDP Adapter**.
4. Na guia adaptador IDP, selecione **Adicionar uma nova linha a 'Validadores de credenciais'**.
5. Selecione o validador de credenciais de senha que você criou.
6. Na guia Adapter Attributes (atributos do adaptador), selecione o atributo **username** para **pseudônimo**.
7. Selecione **Guardar**.

Criar ou importar certificado de assinatura[[certificado de assinatura]]

Se ainda não o fez, crie ou importe o certificado de assinatura.

Passos

1. Aceda a **Security** > **Signing & Decryption Keys & Certificates**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Quando você cria uma conexão SP no PingFederate, importa os metadados SAML que você baixou do StorageGRID para o nó Admin. O arquivo de metadados contém muitos dos valores específicos que você precisa.

Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID, para que os usuários possam fazer login e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP. Em seguida, aceda a Crie conexões SP adicionais para criar quaisquer ligações adicionais de que necessita.

Escolha o tipo de conexão SP

Passos

1. Aceda a **aplicações** > **integração** > **ligações SP**.
2. Selecione **criar conexão**.
3. Selecione **não utilize um modelo para esta ligação**.
4. Selecione **Browser SSO Profiles** e **SAML 2,0** como protocolo.

Importar metadados do SP

Passos

1. Na guia Importar metadados, selecione **Arquivo**.
2. Escolha o arquivo de metadados SAML que você baixou na 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 ID de conexão 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 **seguinte**.

Configure o SSO do navegador IDP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia perfis SAML, selecione as opções **SSO iniciado por SP**, **SLO inicial por SP**, **SSO iniciado por IDP** e **SLO** iniciado por IDP.
3. Selecione **seguinte**.
4. Na guia Assertion Lifetime, não faça alterações.
5. Na guia criação de asserções, selecione **Configurar criação de asserções**.
   a. Na guia Mapeamento de identidade, selecione **Standard**.
   b. Na guia Contrato de Atributo, use o **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 `urn:oid` o , que não é usado.

Instância do adaptador de mapa

Passos

1. Na guia Mapeamento de origem de autenticação, selecione **Mapear nova instância de adaptador**.
2. Na guia instância do adaptador, selecione o instância do adaptador que 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 o armazenamento de dados que você adicionou.

6. Na guia Pesquisa de diretório LDAP:
   - Digite o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
   - Para o escopo de pesquisa, selecione **subtree**.
   - Para a classe de objeto raiz, procure o atributo **objectGUID** e adicione-o.
7. Na guia tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia filtro LDAP, digite **sAMAccountName**.
9. Na guia execução de contrato de atributo, selecione **LDAP (attribute)** na lista suspensa origem e selecione **objectGUID** na lista suspensa valor.
10. Revise e salve a fonte do atributo.
11. Na guia origem do atributo de salvamento de falha, selecione **Abortar a transação SSO**.
12. Reveja o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configure as definições do protocolo

Passos

1. Na guia **conexão SP** > **SSO do navegador** > **Configurações do protocolo**, selecione **Configurar configurações do protocolo**.
2. Na guia URL do Serviço ao Consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` URL do ponto final).
3. Na guia URLs de serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL de ponto final.
4. Na guia ligações SAML permitidas, desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de assinatura, deixe as caixas de seleção **Require Authn Requests to be signed** e **Always Sign Assertion** selecionadas.
6. Na guia Diretiva de criptografia, selecione **nenhum**.
7. Reveja o resumo e selecione **Concluído** para guardar as definições 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 o certificado de assinatura que você criou ou importou.
4. Selecione **Next** para ir para **Manage Signature Verification Settings**.
   a. Na guia Trust Model (modelo de confiança), selecione **Unancored** (sem ancoragem).
   b. Na guia certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.
5. Reveja os ecrãs de resumo e selecione **Guardar** para guardar a ligação SP.

Crie conexões SP adicionais

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

> As conexões do SP para diferentes nós de administração 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. Introduza a ID da ligação e o nome da ligação para a cópia e selecione **Guardar**.
3. Escolha o arquivo de metadados correspondente ao nó Admin:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **escolha Arquivo** e carregue os metadados.
   c. Selecione **seguinte**.
   d. Selecione **Guardar**.
4. Resolva o erro devido ao atributo não utilizado:
   a. Selecione a nova ligação.
   b. Selecione **Configure Browser SSO > Configure Assertion creation > Attribute Contract**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Guardar**.

Desative o logon único

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.

   É apresentada a página Single Sign-on (Início de sessão único).

2. Selecione a opção **Disabled** (Desativado).
3. Selecione **Guardar**.

   É apresentada uma mensagem de aviso indicando que os utilizadores locais poderão iniciar sessão.

4. Selecione **OK**.

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

Desative e reative temporariamente o logon único para um nó de administração

Talvez você não consiga entrar no Gerenciador de Grade se o sistema de logon único (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um nó de administrador. Para desativar e reativar 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 para o usuário raiz local.

Sobre esta tarefa

Depois de desativar o SSO para um nó Admin, você pode entrar no Gerenciador de Grade como o usuário raiz local. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no nó Admin assim que você sair.

> A desativação do SSO para um nó Admin não afeta as configurações de SSO para quaisquer outros nós Admin na grade. A caixa de seleção **Ativar SSO** na página de logon único no Gerenciador de Grade permanece selecionada e todas as configurações SSO existentes são mantidas, a menos que você as atualize.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

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

   Uma mensagem indica que o comando se aplica somente a esse nó Admin.

3. Confirme que você deseja desativar o SSO.

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

4. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.

   A página de login do Gerenciador de Grade agora é exibida porque o SSO foi desativado.

5. Inicie sessão com a raiz do nome de utilizador e a palavra-passe do utilizador raiz local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração SSO:
   a. Selecione **CONFIGURATION** > **access control** > **Single sign-on**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.

c. Selecione **Guardar**.

Selecionar **Save** na página Single Sign-On (Início de sessão único) reativa automaticamente o SSO para toda a grelha.

7. Se você desativou o SSO temporariamente porque precisava acessar o Gerenciador de Grade por algum outro motivo:

   a. Execute qualquer tarefa ou tarefas que você precisa executar.
   b. Selecione **Sair** e feche o Gerenciador de Grade.
   c. Reative o SSO no nó Admin. Você pode executar uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a esse nó Admin.

      Confirme se você deseja ativar o SSO.

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

      - Reinicie o nó da grade: `reboot`

8. A partir de um navegador da Web, acesse o Gerenciador de Grade a partir do mesmo nó Admin.
9. Confirme se a página de login do StorageGRID é exibida e que você deve inserir suas credenciais SSO para acessar o Gerenciador de Grade.

Use a federação de grade

O que é a federação de grade?

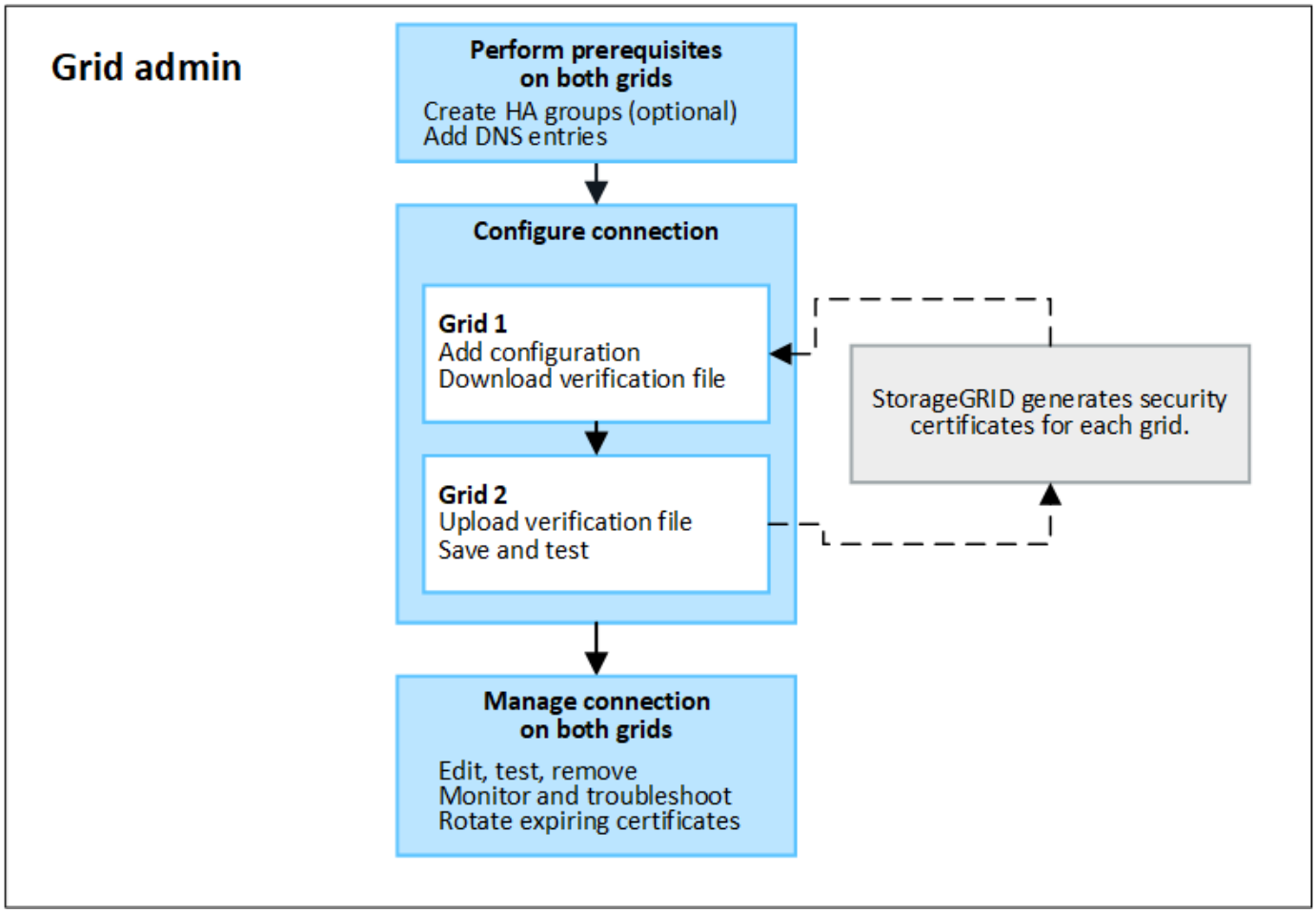
Você pode usar a federação de grade para clonar locatários e replicar seus objetos entre dois sistemas StorageGRID para recuperação de desastres.

O que é uma conexão de federação de grade?

Uma conexão de federação de grade é uma conexão bidirecional, confiável e segura entre os nós de administrador 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 grade

- Ambas as grades usadas para federação de grade devem estar executando o StorageGRID 11,7.
- Uma grade pode ter uma ou mais conexões de federação de grade para outras grades. Cada conexão de federação de grade é independente de quaisquer outras conexões. Por exemplo, se o Grid 1 tiver uma conexão com o Grid 2 e uma segunda conexão com o Grid 3, não haverá conexão implícita entre o Grid 2 e o Grid 3.
- As conexões de federação de grade são bidirecionais. Após a conexão ser estabelecida, você pode monitorar e gerenciar a conexão a partir de qualquer grade.
- Deve existir pelo menos uma ligação de federação de grelha antes de poder utilizar "clone de conta" ou "replicação entre grade".

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 grade coneta uma grade a outra grade. A configuração para cada grade especifica um ponto de extremidade de federação de grade na outra grade que consiste em nós de administrador, nós de gateway ou ambos.
- A prática recomendada é conetar "Grupos de alta disponibilidade (HA)" os nós Gateway e Admin em cada grade. O uso de grupos de HA ajuda a garantir que as conexões de federação de grade permaneçam on-line se os nós ficarem indisponíveis. Se a interface ativa em qualquer um dos grupos HA falhar, a conexão poderá usar uma interface de backup.

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

Use FQDNs para equilibrar a conexão de carga

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

- O FQDN para a Grade 1 mapeou um ou mais endereços IP virtuais (VIP) para grupos de HA na Grade 1 ou para o endereço IP de um ou mais nós de Admin ou Gateway na Grade 1.
- O FQDN para a Grade 2 mapeou um ou mais endereços VIP para a Grade 2 ou para o endereço IP de um ou mais nós de Admin ou Gateway na Grade 2.

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

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

Requisitos portuários

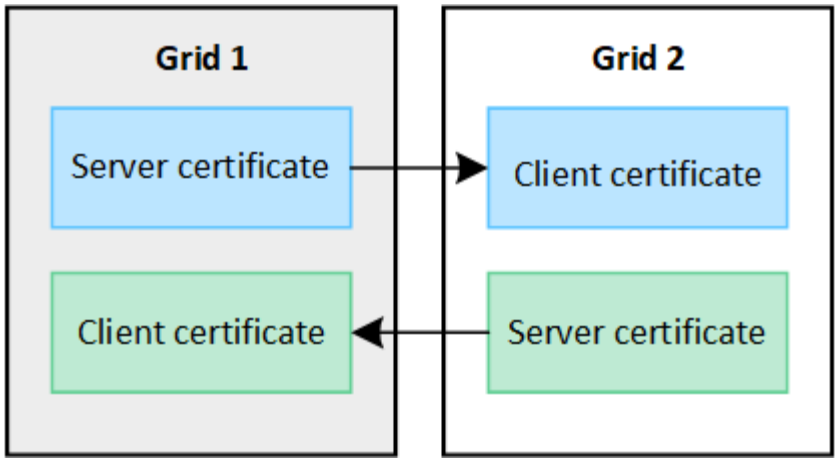
Ao criar uma conexão de federação de grade, você pode especificar qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta.

Você deve garantir que nenhum nó em qualquer grade use essa porta para outras conexões.

Requisitos de certificado

Quando você configura 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 **Expiration of Grid Federation certificate** lembra que você deve girar os certificados, o que você pode fazer usando o Grid Manager.

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

Saiba mais

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

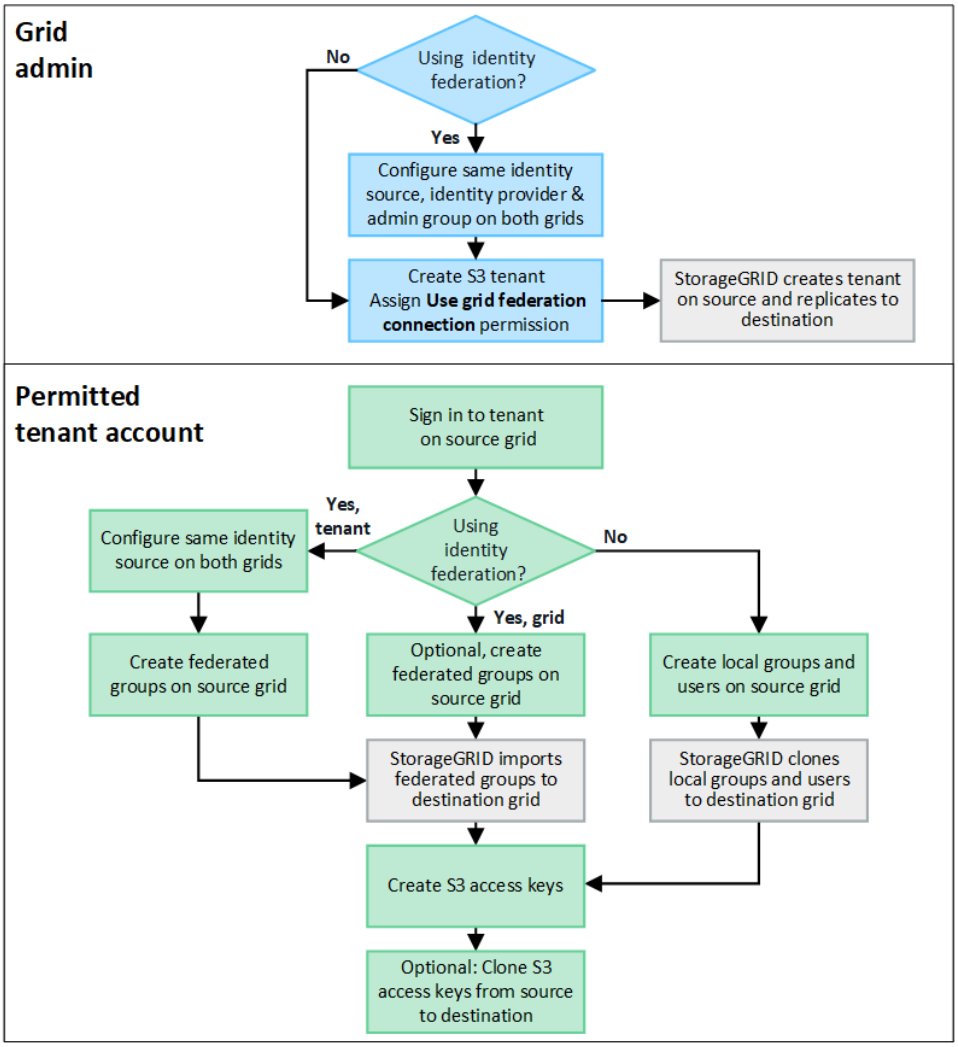
O que é o clone de conta?

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 grade".

O clone de conta é necessário para "replicação entre grade"o . Clonar 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 clone de conta

O diagrama de fluxo de trabalho mostra as etapas que administradores de grade e locatários permitidos executarão para configurar o clone de conta. Estas etapas são executadas após o "a conexão de federação de grade está configurada".



Fluxo de trabalho de administração de grade

As etapas que os administradores de grade executam dependem se os sistemas StorageGRID na "conexão de federação de grade"federação usar logon único (SSO) ou identidade.

Configurar SSO para o clone de conta (opcional)

Se qualquer um dos sistemas StorageGRID na conexão de federação de grade usar SSO, ambas as grades devem usar SSO. Antes de criar as contas de locatário para federação de grade, os administradores de grade para as grades de origem e destino do locatário devem executar essas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. "Use a federação de identidade"Consulte .
2. Configure o mesmo provedor de identidade SSO (IDP) para ambas as grades. "Configurar o logon único"Consulte .
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 raiz inicial para as contas de locatário de origem e destino.

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

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

Se um dos sistemas StorageGRID usar federação de identidade sem SSO, ambas as grades devem usar federação de identidade. Antes de criar as contas de locatário para federação de grade, os administradores de grade para as grades de origem e destino do locatário devem executar essas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. "Use a federação de identidade"Consulte .
2. Opcionalmente, se um grupo federado tiver permissão de acesso raiz inicial para as contas de locatário de origem e 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 raiz inicial para ambas as contas, especifique uma senha para o usuário raiz local.

Crie uma conta de locatário S3 permitida

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

Passos

1. Determine qual grade você deseja ser a grade de origem do locatário para operações de clone de conta.

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

2. Crie uma nova conta de locatário do S3 nessa grade.
3. Atribua a permissão **Use Grid Federation Connection**.
4. Se a conta de locatário gerenciar seus próprios usuários federados, atribua a permissão **Use own Identity source**.

   Se essa permissão for atribuída, as contas de locatário de origem e destino deverão configurar a mesma fonte de identidade antes de criar grupos federados. Os 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 fonte de identidade.

5. Selecione uma conexão de federação de grade específica.
6. Salve o locatário.

   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 forma:

   - Ambas as contas de inquilino 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. No entanto, a senha para esse usuário não é clonada.

Para obter detalhes, "Gerenciar locatários permitidos para federação de grade"consulte .

Fluxo de trabalho de conta de locatário 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 podem executar essas etapas para clonar grupos de locatários, usuários e chaves de acesso S3.

Passos

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

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

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

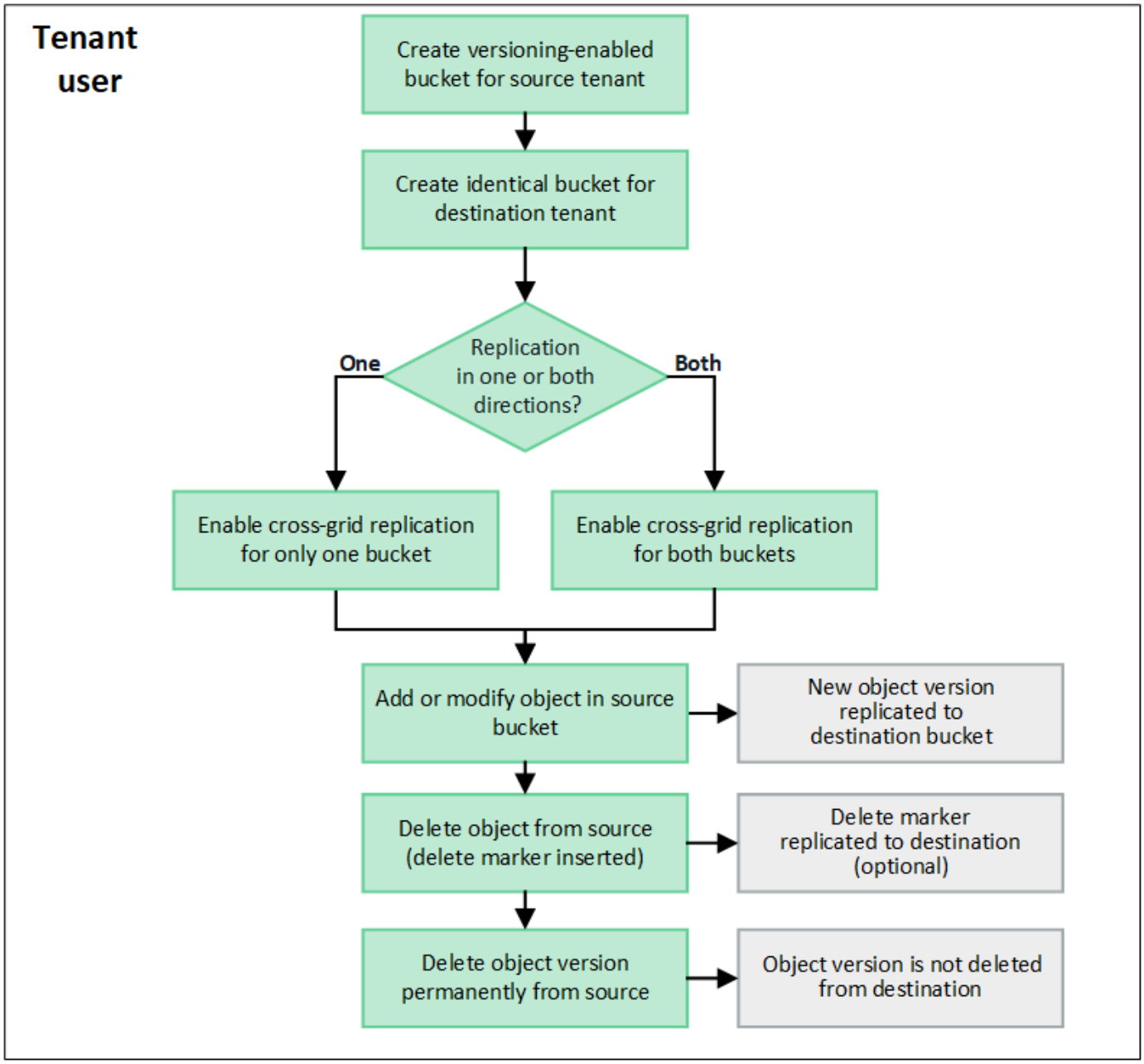
Para obter detalhes sobre o fluxo de trabalho permitido da conta de locatário e saber como grupos, usuários e chaves de acesso S3 são clonados, "Clonar grupos de locatários e usuários"consulte e "Clonar chaves de acesso S3 usando a API".

O que é replicação entre redes?

A replicação entre grade é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID que estão conetados em um "conexão de federação de grade". "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 intervalos em duas grades.



Requisitos para replicação entre grades

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

- Deve ter o mesmo nome e região
- Deve ter o controle de versão habilitado
- Tem de ter o bloqueio de objetos S3 desativado
- Deve estar vazio

Depois que ambos os buckets tiverem sido criados, a replicação entre grades pode ser configurada para um ou ambos os buckets.

Saiba mais

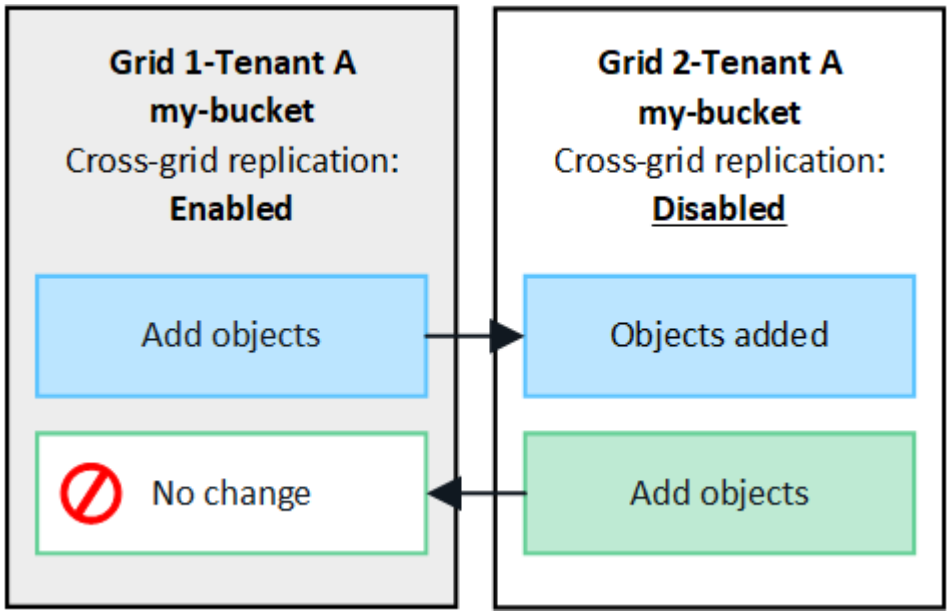
"Gerenciar a replicação entre grades"

Como a replicação entre redes funciona

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

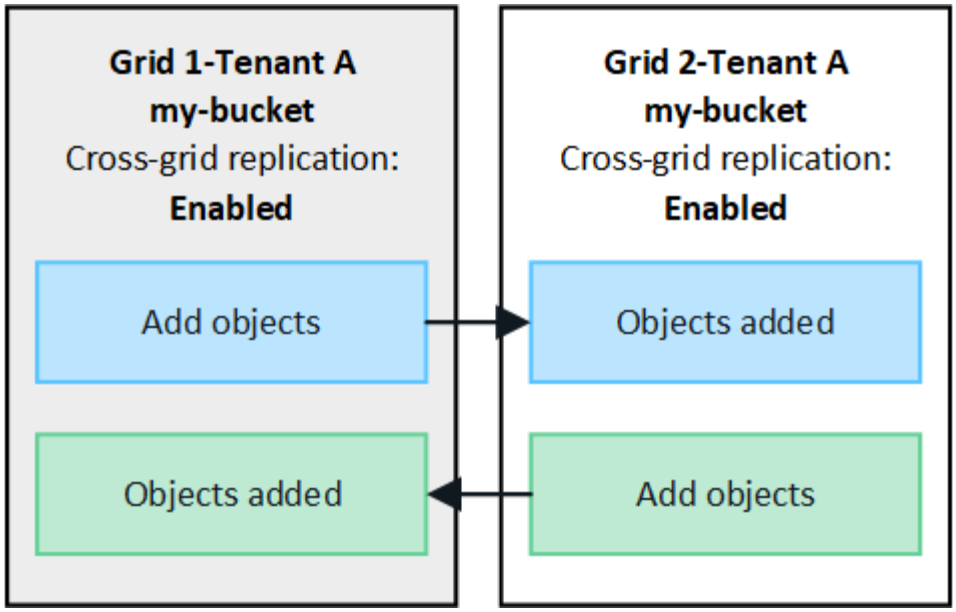
Replicação em uma direção

Se você habilitar a replicação entre grade 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 intervalo de destino não são replicados de volta para a origem. Na figura, a replicação de grade cruzada é ativada para `my-bucket` da grade 1 para a grade 2, mas não é ativada na outra direção.



Replicação em ambas as direções

Se você habilitar a replicação entre grade para o mesmo bucket em ambas as grades, os objetos adicionados a qualquer bucket serão replicados para a outra grade. Na figura, a replicação em grade cruzada é ativada para `my-bucket` em ambas as direções.



O que acontece quando os objetos são ingeridos?

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

1. O StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo para executar essa 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 GET Object ou HEAD Object. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores: O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação GET Object ou HEAD Object. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **SUCCESS**: A replicação foi bem-sucedida para todas as conexões de grade. • **PENDENTE**: O objeto não foi replicado para pelo menos uma conexão de grade. • **FAILURE**: A replicação não está pendente para qualquer conexão de grade e pelo menos uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir da grade de origem.

   O StorageGRID não suporta o `x-amz-replication-status` colhedor.

2. O StorageGRID usa a política ILM ativa de cada grade para gerenciar os objetos, assim como qualquer outro objeto. Por exemplo, Objeto A na Grade 1 pode ser armazenado como duas cópias replicadas e retido para sempre, enquanto a cópia do Objeto A que foi replicado para a Grade 2 pode ser armazenada

usando codificação de apagamento 2-1 e excluída após três anos.

O que acontece quando os objetos são excluídos?

Conforme descrito "Eliminar fluxo de dados"no , o StorageGRID pode excluir um objeto por qualquer um destes motivos:

- O cliente S3 emite uma solicitação de exclusão.
- Um usuário do Tenant Manager seleciona a "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 colocações especificadas.

Quando o StorageGRID exclui um objeto devido a uma operação Excluir objetos na operação de 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 por exclusões do cliente S3 podem ser replicados opcionalmente para o bucket de destino.

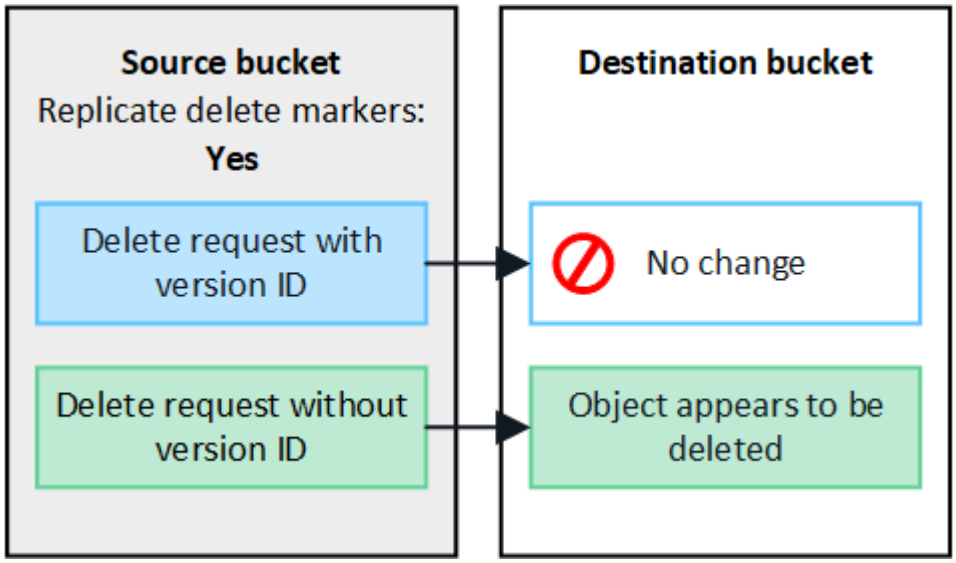
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket que tem replicação entre grade ativada, revise como os clientes S3 excluem objetos de buckets que têm o controle de versão ativado, da seguinte forma:

- 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 eliminação é adicionado ao balde.
- Se um cliente S3 emitir uma solicitação de exclusão que não inclua um ID de versão, o StorageGRID não exclui nenhuma versão de objeto. Em vez disso, ele adiciona um marcador de exclusão ao intervalo. O marcador de exclusão faz com que o StorageGRID atue como se o objeto fosse excluído:
  - Uma solicitação GET sem um ID de versão falhará `404 No Object Found`
  - Uma solicitação GET com uma ID de versão válida será bem-sucedida e retornará a versão do objeto solicitada.

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

- 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 na configuração da replicação entre grade para o bucket:
  - Se você optar por replicar marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao intervalo de origem e replicado ao intervalo de destino. Na verdade, o objeto parece ser excluído em ambas as grades.
  - Se você optar por não replicar marcadores de exclusão, um marcador de exclusão será adicionado ao intervalo de origem, mas não será replicado para o intervalo de destino. Com efeito, os objetos que são excluídos na grade de origem não são excluídos na grade de destino.

Na figura, **Replicate DELETE markers** foi definido como **Yes** quando "a replicação entre redes foi ativada". Excluir solicitações para o bucket de origem que inclua um ID de versão não excluirá objetos do bucket de destino. Excluir solicitações para o bucket de origem que não inclua um ID de versão aparecerão para excluir objetos no bucket de destino.



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

Como os objetos criptografados são replicados

Quando você usa replicação entre grade para replicar objetos entre grades, é possível criptografar objetos individuais, usar criptografia de bucket padrão ou configurar criptografia em toda a grade. Você pode adicionar, modificar ou remover configurações padrão de intervalo ou criptografia em toda a grade antes ou depois de ativar a replicação entre grade para um bucket.

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

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

Para usar a criptografia padrão para um bucket, use uma solicitação de criptografia PUT bucket e defina o `SSEAlgorithm` parâmetro como `AES256`. A criptografia no nível do bucket aplica-se a quaisquer objetos ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. "Operações em baldes"Consulte .

Para usar criptografia no nível da grade, defina a opção **Stored Object Encryption** como **AES-256**. A criptografia no nível da grade se aplica a quaisquer objetos que não sejam criptografados no nível do bucket ou que sejam ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. "Configure as opções de rede e objeto"Consulte .

SSE não suporta AES-128. Se a opção **Stored Object Encryption** estiver ativada 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 o intervalo padrão do destino ou a configuração de criptografia em nível de grade, 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 intervalo, se configurado.
3. Se uma configuração de intervalo não estiver configurada, use a configuração de criptografia em toda a grade, se configurada.
4. Se uma configuração em toda a grade não estiver presente, não criptografe o objeto de origem.

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

1. Use a mesma criptografia que o 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 configurado.
3. Se o intervalo 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 em toda a grade não estiver presente, não criptografe o objeto de destino.

COLOCAR marcação de objeto e EXCLUIR marcação de objeto não são suportados

As solicitações de marcação de objetos PUT e DELETE não são compatíveis com objetos em buckets que têm replicação entre grades ativada.

Se um cliente S3 emitir uma solicitação de marcação PUT Object ou DELETE Object tagging `501 Not Implemented`, será retornado. A mensagem é `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Como os objetos segmentados são replicados

O tamanho máximo do segmento da grade de origem aplica-se a objetos replicados na grade de destino. Quando os objetos são replicados para outra grade, a configuração **tamanho máximo do segmento** (**CONFIGURATION** > **System** > **Storage options**) 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 de 1 GB, enquanto o tamanho máximo do segmento da grade de destino é de 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, mesmo que o tamanho máximo do segmento da grade seja de 50 MB.

Compare a replicação entre redes e a replicação do CloudMirror

À medida que você começar a usar a federação de grade, revise as semelhanças e as diferenças entre "replicação entre grade" e o "Serviço de replicação do StorageGRID CloudMirror".

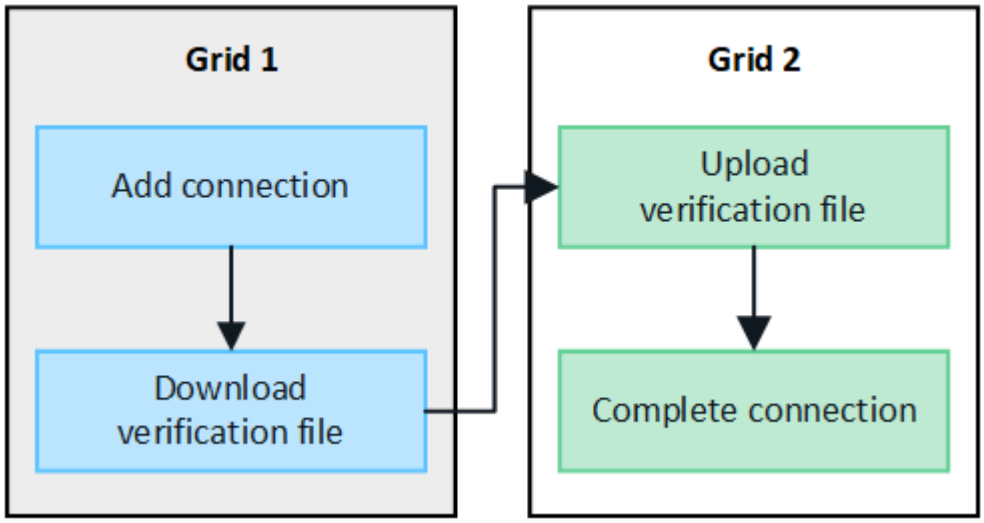
	Replicação entre grade	Serviço de replicação do CloudMirror
Qual é o objetivo principal?	Um sistema StorageGRID atua como um sistema de recuperação de desastres. Os objetos em um bucket podem ser replicados entre as grades em uma ou ambas as direções.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket externo do S3 (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 muitas vezes processada na nuvem.
Como é configurado?	1. Configure uma conexão de federação de grade entre duas grades. 2. Adicione novas contas de inquilino, que são clonadas automaticamente para a outra grade. 3. Adicione novos grupos de inquilinos e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grade e permita que a replicação entre grade ocorra em uma ou ambas as direções.	1. Um usuário de locatário configura a replicação do CloudMirror definindo um endpoint do CloudMirror (endereço IP, credenciais, etc.) usando o Gerenciador do Tenant ou a API S3. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint do CloudMirror.
Quem é responsável por montá-lo?	• Um administrador de grade configura a conexão e os locatários. • Os usuários do locatário 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). • Google Cloud Platform (GCP)
O controle de versão do objeto é necessário?	Sim, os buckets de origem e destino devem ter o controle de versão de objetos habilitado.	Não, a replicação do CloudMirror suporta qualquer combinação de buckets não versionados e 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 replicação entre grade ativada.	Os objetos são replicados automaticamente quando são adicionados a um bucket que foi configurado com um endpoint do CloudMirror. Os 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.

	Replicação entre grade	Serviço de replicação do CloudMirror
Como os objetos são replicados?	A replicação entre grade cria objetos com controle de versão e replica o ID da versão do bucket de origem para o bucket de destino. Isso permite que a ordem da versão seja mantida em ambas as grades.	A replicação do CloudMirror não requer buckets habilitados para controle de versão, portanto, o CloudMirror só pode manter o pedido de uma chave em um site. Não há garantias de que o pedido será mantido para pedidos para um objeto em local diferente.
E se um objeto não puder ser replicado?	O objeto está na fila para replicação, sujeito aos limites de armazenamento de metadados.	O objeto está na fila para replicação, sujeito aos limites dos serviços da plataforma ("Recomendações para o uso de serviços de plataforma"consulte).
Os metadados do sistema do objeto são replicados?	Sim, quando um objeto é replicado para a 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 diferem entre locais, dependendo do tempo 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 para o bucket em qualquer grade.	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação para StorageGRID ou para o destino S3. Por exemplo, suponha que você use a replicação do CloudMirror para espelhar objetos em uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário utilizar o StorageGRID.
O que acontece se um objeto for excluído?	• As solicitações de exclusão que incluem um ID de versão nunca são replicadas para a grade de destino. • Excluir solicitações 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 intervalo de destino podem ser excluídos sem afetar a origem.	Os resultados variam de acordo com o estado de versionamento dos intervalos 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 intervalo de origem for versionado, uma solicitação de exclusão adicionará um marcador de exclusão à origem, mas não ao destino. • Se nenhum intervalo for versionado, uma solicitação de exclusão excluirá o objeto da origem, mas não do destino. Da mesma forma, os objetos no intervalo de destino podem ser excluídos sem afetar a origem.

Crie 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 de objeto.

Como mostrado na figura, a criação de uma conexão de federação de grade inclui etapas em ambas as grades. Você adiciona a conexão em uma grade e a completa na outra grade. Você pode começar a partir de 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 suportado".
- Você deve ter permissão de acesso raiz e a senha de provisionamento para ambas as grades.

Adicionar ligação

Execute estas etapas em um dos dois sistemas StorageGRID.

Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **Adicionar conexão**.
4. Introduza os detalhes da ligação.

Campo	Descrição
Nome da ligação	Um nome exclusivo para ajudá-lo a reconhecer essa conexão, por exemplo, "'Grid 1-Grid 2.'"

Campo	Descrição
FQDN ou IP para esta grade	Uma das seguintes opções: • O FQDN da grade em que você está conetado atualmente • Um endereço VIP de um grupo HA nesta grelha • Um endereço IP de um nó de administrador ou nó de gateway nesta grade. O IP pode estar em qualquer rede que a grade de destino possa alcançar.
Porta	A porta que pretende utilizar para esta ligação. Pode introduzir 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 qualquer grade use essa porta para outras conexões.
Certificado dias válidos para esta grade	O número de dias que deseja que os certificados de segurança para essa grade na conexão sejam válidos. O valor padrão é de 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.
Frase-passe de aprovisionamento para esta grelha	A senha de provisionamento para a grade à qual você está conetado.
FQDN ou IP para a outra grade	Uma das seguintes opções: • O FQDN da grade à qual você deseja se conetar • Um endereço VIP de um grupo HA na outra grade • Um endereço IP de um nó de administrador 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 Download do arquivo de verificação, selecione **Download do arquivo de verificação**.

   Depois que a conexão for concluída na outra grade, você não poderá mais baixar o arquivo de verificação de qualquer grade.

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 sensíveis e deve ser armazenado e transmitido com segurança.

8. Selecione **Fechar** para retornar à página de federação de Grade.
9. Confirme se a nova ligação é apresentada e que o seu **Estado da ligação** é **a aguardar ligação**.

10. Forneça o *connection-name*`.grid-federation` arquivo ao administrador de grade para a outra grade.

Ligação completa

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

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **carregar ficheiro de verificação** para aceder à página carregar.
4. Selecione **carregar ficheiro de verificação**. Em seguida, procure e selecione o arquivo que foi baixado da primeira grade (*connection-name*`.grid-federation`).

   São apresentados os detalhes da ligação.

5. Opcionalmente, insira um número diferente de dias válidos para os certificados de segurança para esta grade. A entrada **Certificate Valid Days** (dias válidos do certificado*) é padrão para o valor inserido na primeira grade, mas cada grade pode usar datas de expiração diferentes.

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

   > ⚠ Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão parará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

6. Insira a senha de provisionamento para a grade à qual você está conetado 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 de federação de Grade. O **Estado da ligação** será **ligado**.

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

8. Vá para a página de federação de Grade na primeira grade e atualize o navegador. Confirme se o **Estado da ligação** é agora **ligado**.
9. Depois que a conexão for estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

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

Depois de terminar

- Reveja as considerações para "gerenciamento de inquilinos permitidos".
- "Crie uma ou mais novas contas de inquilino", Atribua a permissão **Use Grid Federation Connection** e selecione a nova conexão.
- "Gerencie a conexão" conforme necessário. Você pode editar valores de conexão, testar uma conexão, girar certificados de conexão ou remover uma conexão.

- "Monitorize a ligação" Como parte de suas atividades normais de monitoramento do StorageGRID.
- "Solucionar problemas da conexão", incluindo a resolução de quaisquer alertas e erros relacionados ao clone de conta e replicação entre grades.

Gerenciar conexões de federação de grade

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

Antes de começar

- Você está conetado ao Gerenciador de Grade em qualquer grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root para a grade à qual você está conetado.

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 da 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 está sendo editada, as solicitações de replicação entre redes ou clone de conta continuarão a usar as configurações de conexão existentes. Todas as edições feitas na primeira grade são salvas localmente, mas não são usadas até que tenham sido carregadas na segunda grade, salvas e testadas.

Comece a editar a ligação

Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **NÓS** e confirme se todos os outros nós de administrador do 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 esse arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso será exibida quando você selecionar **Salvar e testar**.

3. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
4. Edite os detalhes da conexão usando o menu **ações** na página de federação de Grade ou a página de detalhes de uma conexão específica. Consulte "Crie conexões de federação de grade" para saber o que introduzir.

Menu ações

a. Selecionar o botão do rádio para a ligação.
b. Selecione **ações** > **Editar**.
c. Introduza as novas informações.

Página de detalhes

a. Selecione um nome de ligação para apresentar os respetivos detalhes.
b. Selecione **Editar**.
c. Introduza as novas informações.

5. Insira a senha de provisionamento para a grade à qual você está conetado.
6. Selecione **Salvar e continuar**.

   Os novos valores são salvos, mas eles não serão aplicados à conexão até que você tenha carregado o novo arquivo de verificação na outra grade.

7. Selecione **Transferir ficheiro de verificação**.

   Para transferir este ficheiro posteriormente, aceda à página de detalhes da ligação.

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 de Grade.
10. Confirme se o **Status da conexão** é **Pending edit**.

    Se o status da conexão for diferente de **conectado** quando você começou a editar a conexão, ela não mudará para **Pending edit**.

11. Forneça o *connection-name*`.grid-federation` arquivo ao administrador de grade para a outra grade.

Termine a edição da conexão

Termine a edição da conexão carregando o arquivo de verificação na outra grade.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione **carregar ficheiro de verificação** para aceder à página de carregamento.
4. Selecione **carregar ficheiro de verificação**. Em seguida, procure e selecione o arquivo que foi baixado da primeira grade.
5. Insira a senha de provisionamento para a grade à qual você está conetado 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, é apresentada uma mensagem de erro. Revise a mensagem e solucione quaisquer problemas.

7. Feche o assistente para retornar à página de federação de Grade.
8. Confirme se o **Estado da ligação** é **ligado**.
9. Vá para a página de federação de Grade na primeira grade e atualize o navegador. Confirme se o **Estado da ligação** é agora **ligado**.
10. Depois que a conexão for estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Teste uma conexão de federação de grade

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Teste a conexão usando o menu **ações** na página de federação de Grade ou a página de detalhes para uma conexão específica.

Menu ações

a. Selecionar o botão do rádio para a ligação.
b. Selecione **ações** > **Teste**.

Página de detalhes

a. Selecione um nome de ligação para apresentar os respetivos detalhes.
b. Selecione **Test Connection**.

4. Reveja o estado da ligação:

Estado da ligação	Descrição
Ligado	Ambas as grades estão conetadas e se comunicando normalmente.
Erro	A conexão está em um 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 para a outra grade.
A aguardar ligação	Você configurou a conexão nesta grade, mas a conexão não foi concluída na outra grade. Baixe o arquivo de verificação desta grade e faça o upload para a outra grade.
Desconhecido	A conexão está em um estado desconhecido, possivelmente por causa de um problema de rede ou um nó off-line.

5. Se o status da conexão for **Error**, resolva quaisquer problemas. Em seguida, selecione **Test Connection** novamente para confirmar que o problema foi corrigido.

gire 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 **Expiration of Grid Federation certificate** lembra que você deve girar os certificados.

> Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão parará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

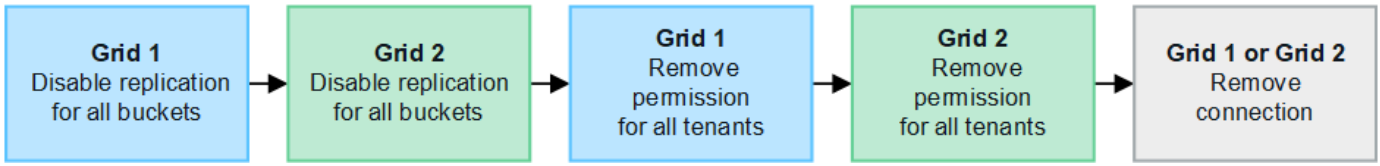
Passos

1. Faça login no Gerenciador de Grade a partir do nó Admin primário em qualquer grade.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Em qualquer guia da página de federação de Grade, selecione o nome da conexão para exibir seus detalhes.
4. Selecione a guia **certificados**.
5. Selecione **Rotate certificates** (rodar certificados).
6. Especifique quantos dias os novos certificados devem ser válidos.
7. Insira a senha de provisionamento para a grade à qual você está conetado.
8. Selecione **Rotate certificates** (rodar certificados).
9. Conforme necessário, repita estas etapas na outra grade na conexão.

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

Remova uma conexão de federação de grade

Você pode remover uma conexão de federação de grade de qualquer grade na conexão. Como 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 qualquer grade.



Antes de remover uma conexão, observe o seguinte:

- A remoção de uma conexão não exclui nenhum item que já tenha sido copiado entre grades. Por exemplo, usuários de locatários, grupos e objetos que existem em ambas as grades não são excluídos de qualquer grade quando a permissão do locatário é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambas as grades.
- Quando você remove uma conexão, quaisquer objetos que estejam pendentes de replicação (ingeridos mas ainda não replicados para a outra grade) terão sua replicação permanentemente falhada.

Desative a replicação para todos os buckets do locatário

Passos

1. A partir de qualquer grade, entre no Gerenciador de Grade a partir do nó Admin primário.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar os respetivos detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), determine se a conexão está sendo usada por quaisquer inquilinos.
5. Se algum inquilino estiver listado, instrua todos os inquilinos para que "desative a replicação entre redes"todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **usar conexão de federação de grade** se qualquer bucket de locatário tiver replicação entre grade ativada. Cada conta de locatário deve desativar a replicação entre grade para seus buckets em ambas as grades.

Remova a permissão para cada locatário

Depois que a replicação entre grades for desativada para todos os buckets do locatário, remova a permissão **Use Grid Federation** de todos os locatários em ambas as grades.

Passos

1. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
2. Selecione o nome da ligação para apresentar os respetivos detalhes.
3. Para cada locatário na guia **inquilinos permitidos**, remova a permissão **usar conexão de federação de grade** de cada locatário. "Gerenciar locatários permitidos"Consulte .
4. Repita estes passos para os inquilinos permitidos na outra grelha.

Remova a conexão

Passos

1. Quando nenhum inquilino em qualquer grade estiver usando a conexão, selecione **Remover**.
2. Reveja a mensagem de confirmação e selecione **Remover**.
   - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão de federação de grade agora é removida de ambas as grades.
   - Se a conexão não puder ser removida (por exemplo, ela ainda está em uso ou há um erro de conexão), uma mensagem de erro será exibida. Você pode fazer um dos seguintes procedimentos:
     - Resolva o erro (recomendado). "Solucionar erros de federação de grade"Consulte .
     - Retire a ligação à força. Consulte a próxima seção.

Remova uma conexão de federação de grade pela força

Se necessário, você pode forçar a remoção de uma conexão que não tenha o status **conectado**.

A remoção forçada apenas elimina a ligação da grelha local. Para remover completamente a conexão, execute as mesmas etapas em ambas as grades.

Passos

1. Na caixa de diálogo de confirmação, selecione **forçar a remoção**.

   É apresentada uma mensagem de sucesso. Essa conexão de federação de grade não pode mais ser usada. No entanto, os buckets do locatário ainda podem ter a replicação entre grade ativada e algumas cópias de objeto podem já ter sido replicadas entre as grades na conexão.

2. A partir da outra grade na conexão, entre no Gerenciador de Grade do nó Admin principal.
3. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
4. Selecione o nome da ligação para apresentar os respetivos detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **forçar a remoção** para remover a conexão desta grade.

Gerenciar os locatários permitidos para a federação de grade

Você pode permitir que novas contas de locatário do S3 usem uma conexão de federação de grade entre dois sistemas StorageGRID. Quando os locatários têm permissão para usar uma conexão, etapas especiais são necessárias para editar os detalhes do locatário ou para remover permanentemente a permissão do locatário para usar a conexão.

Antes de começar

- Você está conetado ao Gerenciador de Grade em qualquer grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root para a grade à qual você está conetado.
- Você "criou uma conexão de federação de grade" tem entre duas grades.
- Analisou os fluxos de trabalho para "clone de conta" e "replicação entre grade".
- Conforme necessário, você já configurou o logon único (SSO) ou identifica a federação para ambas as grades na conexão. "O que é o clone de conta"Consulte .

Crie um locatário permitido

Se você quiser permitir que uma conta de locatário use uma conexão de federação de grade para clone de conta e replicação entre grade, siga as instruções gerais para "Crie um novo locatário do S3" e observe o seguinte:

- Você pode criar o locatário a partir de qualquer grade na conexão. A grade onde um locatário é criado é a grade de origem do *locatário*.
- O estado da ligação tem de ser **ligado**.
- Você só pode selecionar a permissão **usar conexão de federação de grade** quando estiver criando um novo locatário S3; você não pode habilitar essa permissão quando editar um locatário existente.
- Quando o novo locatário é salvo na primeira grade, um locatário idêntico é automaticamente replicado para a outra grade. A grade onde o locatário é replicado é a grade de destino do *locatário*.
- Os locatários em ambas as grades terão o mesmo ID de conta, nome, descrição, cota e permissões de 20 dígitos. Opcionalmente, você pode usar o campo **Description** 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 para a Grade 2: "'este locatário foi criado na Grade 1.'"
- Por motivos de segurança, a senha de um usuário raiz local não é copiada para a grade de destino.

Antes que um usuário raiz local possa fazer login no locatário replicado na grade de destino, um administrador de grade para essa grade deve "altere a senha do usuário raiz local".

- Depois que o novo locatário estiver disponível em ambas as grades, os usuários do locatário poderão executar estas operações:
  - Na grade de origem do locatário, crie grupos e usuários locais, que são clonados automaticamente para a grade de destino do locatário. "Clonar grupos de locatários e usuários"Consulte .
  - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para a grade de destino do locatário. "Clonar chaves de acesso S3 usando a API"Consulte .
  - Crie buckets idênticos em ambas as grades na conexão e habilite a replicação entre grades em uma direção ou em ambas as direções. "Gerenciar a replicação entre grades"Consulte .

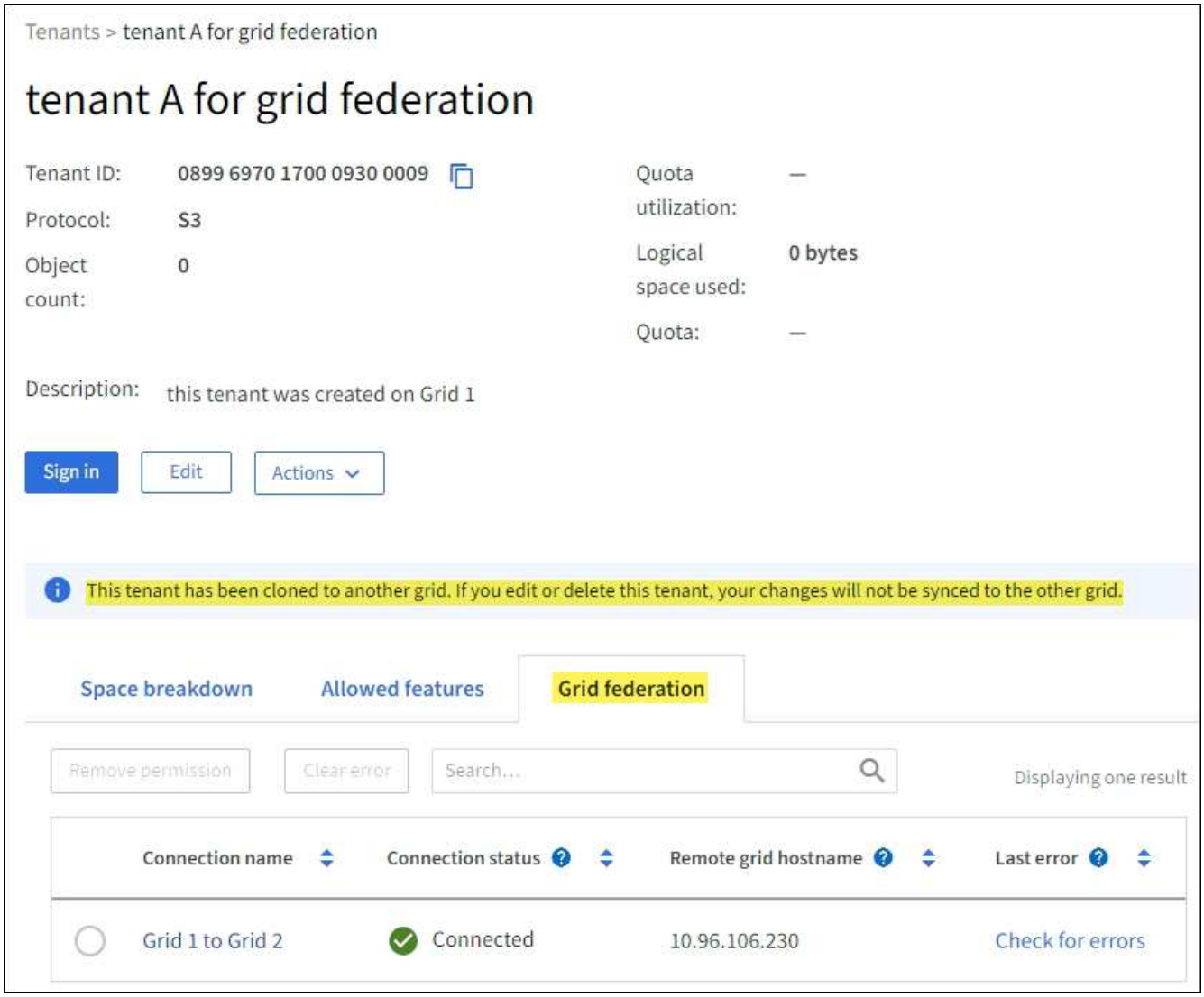
Ver um inquilino permitido

Você pode ver detalhes de um locatário que tem permissão para usar uma conexão de federação de grade.

Passos

1. Selecione **TENANTS**.
2. Na página de locatários, selecione o nome do locatário para exibir a página de detalhes do locatário.

   Se essa for a grade de origem do locatário (ou seja, se o locatário foi criado nessa grade), um banner aparecerá para lembrá-lo de que o locatário foi clonado para outra grade. Se você editar ou excluir esse locatário, suas alterações não serão sincronizadas com a outra grade.



3. Opcionalmente, selecione a guia **Grid Federation** para "monitore a conexão de federação de grade".

Editar um locatário permitido

Se você precisar editar um locatário que tenha a permissão **Use Grid Federation Connection**, 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. No entanto, quaisquer alterações feitas não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário sincronizados entre grades, você deve fazer as mesmas edições em ambas as grades.
- Você não pode limpar a permissão **usar conexão de federação de grade** quando estiver editando um locatário.
- Você não pode selecionar uma conexão de federação de grade diferente quando estiver editando um locatário.

Excluir um locatário permitido

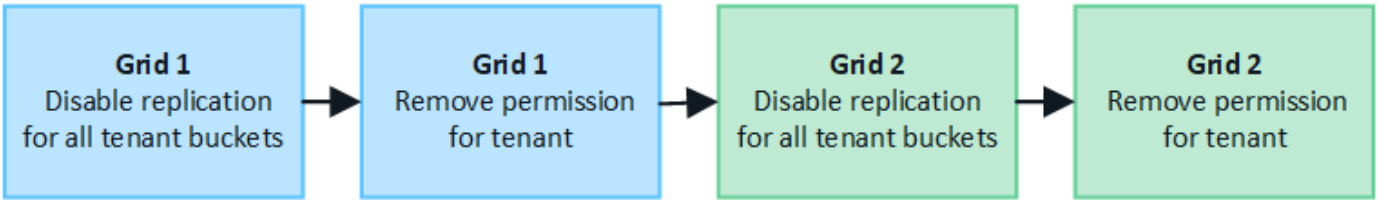
Se você precisar remover um locatário que tenha a permissão **Use Grid Federation Connection**, siga as instruções gerais para "excluindo uma conta de locatário" e observe o seguinte:

- 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 grade.
- Se você estiver removendo o locatário original na grade de origem, todos os grupos de locatários, usuários ou chaves clonadas para a 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, erros de clone ocorrerão 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 de grade antes de excluir o locatário dessa grade.

Remove Use grid Federation Connection permission

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:

- Remover a permissão **usar conexão de federação de grade** de um locatário é uma ação permanente. Não é possível reativar a permissão para este locatário.
- Não é possível remover a permissão **usar conexão de federação de grade** se qualquer um dos buckets do locatário tiver a replicação entre grade ativada. A conta de locatário deve desativar a replicação entre redes para todos os buckets primeiro.
- A remoção da permissão **usar conexão de federação de grade** não exclui nenhum item que já tenha sido replicado entre grades. Por exemplo, os usuários, grupos e objetos de inquilino que existem em ambas as grades não são excluídos de qualquer grade quando a permissão do locatário é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambas as grades.

Antes de começar

- Você está usando um "navegador da web suportado".
- Você tem a permissão de acesso root para ambas as grades.

Desative a replicação para buckets do locatário

Como primeira etapa, desative a replicação entre grade para todos os buckets do locatário.

Passos

1. A partir de qualquer grade, entre no Gerenciador de Grade a partir do nó Admin primário.

2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar os respetivos detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), determine se o locatário está usando a conexão.
5. Se o inquilino estiver listado, instrua-o para "desative a replicação entre redes"todos os seus buckets em ambas as grades na conexão.

> Não é possível remover a permissão **usar conexão de federação de grade** se qualquer bucket de locatário tiver replicação entre grade ativada. O locatário deve desativar a replicação entre grade para seus buckets em ambas as grades.

Remover permissão para locatário

Depois que a replicação entre grades for desativada para buckets do locatário, você poderá remover a permissão do locatário para usar a conexão de federação de grade.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Remova a permissão da página de federação de Grade ou da página de locatários.

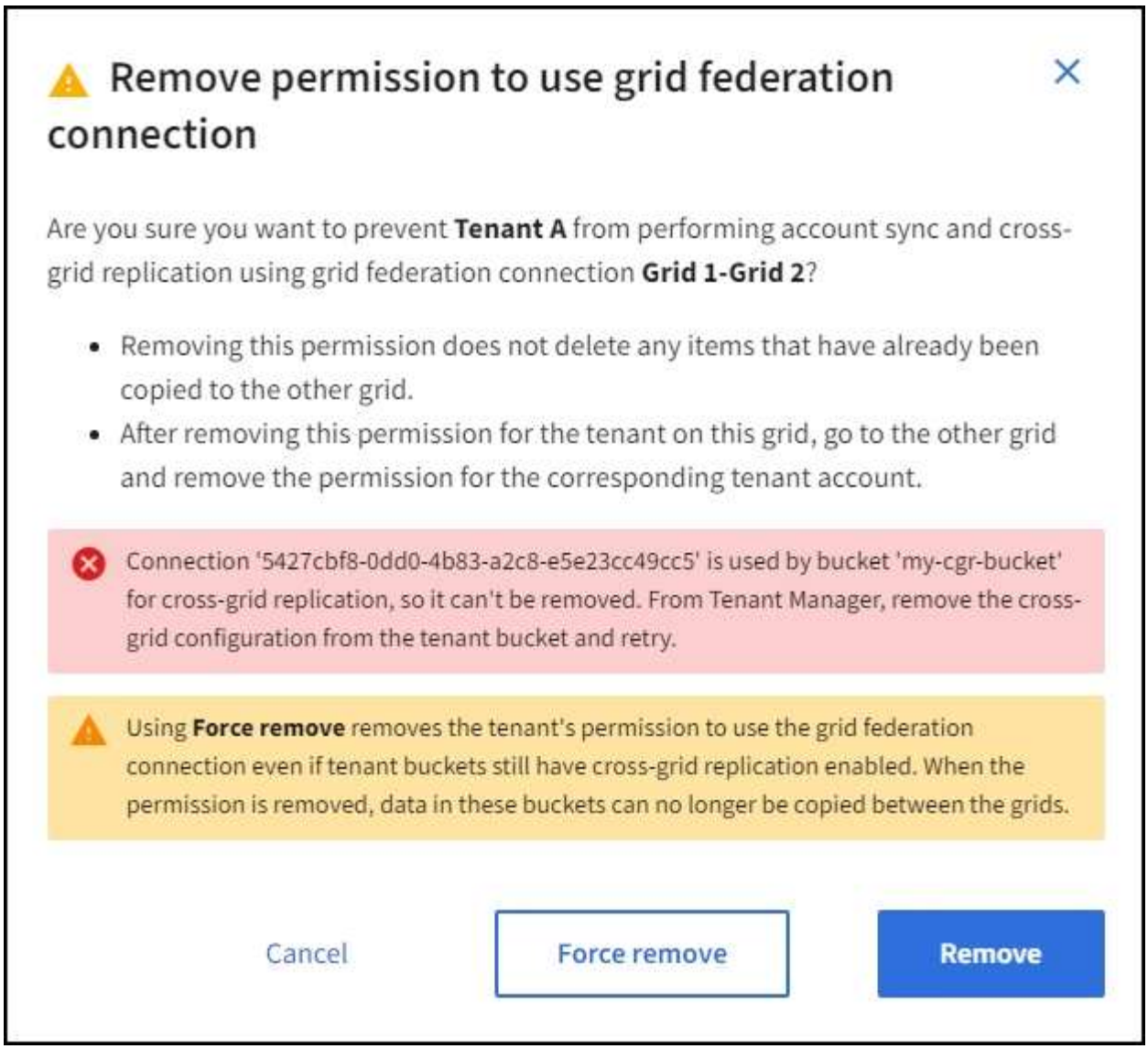
Página de federação de grade

a. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
b. Selecione o nome da ligação para apresentar a respetiva página de detalhes.
c. Na guia **allowed tenants** (inquilinos permitidos), selecione o botão de opção para o locatário.
d. Selecione **Remover permissão**.

Página de inquilinos

a. Selecione **TENANTS**.
b. Selecione o nome do locatário para exibir a página de detalhes.
c. No separador **Grid Federation** (federação de grelha), selecione o botão de opção para a ligação.
d. Selecione **Remover permissão**.

3. Reveja os avisos na caixa de diálogo de confirmação e selecione **Remover**.
   - Se a permissão puder ser removida, você será retornado à página de detalhes e uma mensagem de sucesso será exibida. Esse locatário não pode mais usar a conexão de federação de grade.
   - Se um ou mais buckets de inquilinos ainda tiverem a replicação entre grades ativada, um erro será exibido.



Você pode fazer um dos seguintes procedimentos:

- (Recomendado.) Faça login no Gerenciador do locatário e desative a replicação para cada um dos buckets do locatário. "Gerenciar a replicação entre grades"Consulte . Em seguida, repita as etapas para remover a permissão **Use Grid Connection**.
- Remova a permissão pela força. Consulte a próxima seção.

4. Vá para a outra grade e repita estas etapas para remover a permissão para o mesmo locatário na outra grade.

Remova a permissão pela força

Se necessário, você pode forçar a remoção da permissão de um locatário a usar uma conexão de federação de grade, mesmo se os buckets do locatário tiverem a replicação entre grade ativada.

Antes de remover a permissão de um inquilino por força, observe as considerações gerais remover a permissão, bem como estas considerações adicionais:

- Se você remover a permissão **usar conexão de federação de grade** por força, quaisquer objetos que estejam pendentes de replicação para a outra grade (ingeridos, mas ainda não replicados) continuarão a ser replicados. Para evitar que esses objetos em processo atinjam o intervalo de destino, você também

deve remover a permissão do locatário na outra grade.

- Quaisquer objetos ingeridos no intervalo de origem depois de remover a permissão **usar conexão de federação de grade** nunca serão replicados para o intervalo de destino.

Passos

1. Inicie sessão no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURATION** > **System** > **Grid Federation**.
3. Selecione o nome da ligação para apresentar a respetiva página de detalhes.
4. Na guia **allowed tenants** (inquilinos permitidos), selecione o botão de opção para o locatário.
5. Selecione **Remover permissão**.
6. Reveja os avisos na caixa de diálogo de confirmação e selecione **forçar a remoção**.

   É apresentada uma mensagem de sucesso. Esse locatário não pode mais usar a conexão de federação de grade.

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 atinjam o intervalo de destino.

Solucionar erros de federação de grade

Talvez você precise solucionar alertas e erros relacionados a conexões de federação de grade, clone de conta e replicação entre grade.

alertas e erros de conexão de federação de grade

Você pode receber alertas ou ter erros com suas conexões de federação de grade.

Depois de fazer quaisquer alterações para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne a **conectado**. Para obter instruções, "Gerenciar conexões de federação de grade"consulte .

Alerta de falha de conexão de federação de grade

Problema

O alerta **Falha na conexão da federação de grade** foi acionado.

Detalhes

Este alerta indica que a conexão de federação de grade entre as grades não está funcionando.

Ações recomendadas

1. Revise as configurações na página de Federação de Grade para ambas as grades. Confirme se todos os valores estão corretos. "Gerenciar conexões de federação de grade"Consulte .
2. Reveja os certificados utilizados para a ligação. Certifique-se de que não existem alertas para certificados de federação de grade expirados e de que os detalhes de cada certificado são válidos. Consulte as instruções para obter os certificados de conexão rotativos em "Gerenciar conexões de federação de grade".
3. Confirme se todos os nós Admin e Gateway em ambas as grades estão online 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 on-line e disponível. Consulte "O que é a federação de grade?" para obter informações sobre os requisitos de rede, endereço IP e DNS.

Expiração do alerta de certificado de federação de grade

Problema

O alerta **Expiration of Grid Federation certificate** foi acionado.

Detalhes

Este alerta indica que um ou mais certificados de federação de grade estão prestes a expirar.

Ações recomendadas

Consulte as instruções para obter os certificados de conexão rotativos em "Gerenciar conexões de federação de grade".

Erro ao editar uma conexão de federação de grade

Problema

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 de 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 esse arquivo não puder ser salvo em todos os nós de administração, por exemplo, porque um nó de administração 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 online.
3. Se algum nó estiver offline, coloque-o novamente online e tente editar a conexão novamente.

Erros de clone de conta

Não é possível entrar em uma conta de locatário clonada

Problema

Você não pode entrar em uma conta de locatário clonada. A mensagem de erro na página de início de sessão do Tenant Manager é "as suas credenciais para esta conta eram inválidas. 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 de usuário local não são clonadas para a grade de destino.

Ações recomendadas

Antes que o usuário raiz possa fazer login na grade de destino do locatário, um administrador de grade deve primeiro "altere a senha do usuário raiz local" na grade de destino.

Antes que um usuário local clonado possa entrar 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" as instruções para usar o Gerenciador do Locatário.

Locatário criado sem um clone

Problema

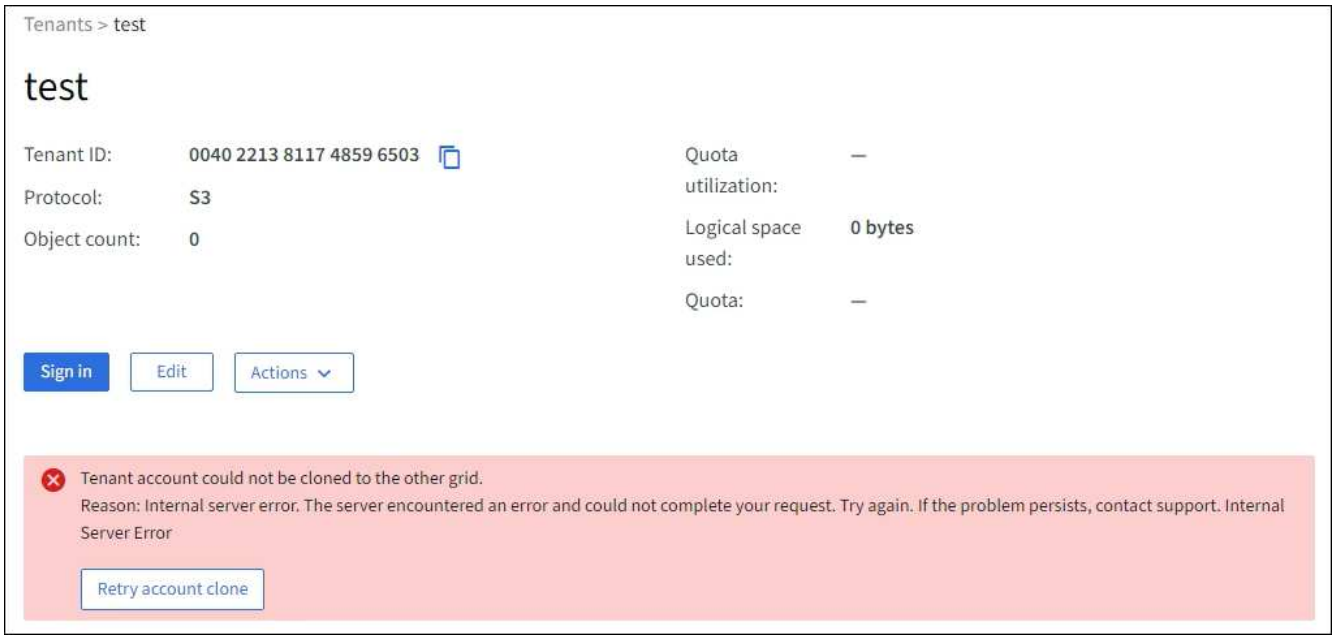
Você verá a mensagem "Tenant created without a clone" depois de criar um novo locatário com a permissão **Use Grid Federation Connection**.

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 **conectado**.

Ações recomendadas

1. Revise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo que a conexão funcione. Alertas e erros de conexão de federação de gradeConsulte .
2. Siga as instruções para testar uma conexão de federação de grade em "Gerenciar conexões de federação de grade"para confirmar que o problema foi corrigido.
3. Na grade de origem do locatário, selecione **TENANTS**.
4. Localize a conta de locatário que não foi clonada.
5. Selecione o nome do locatário para exibir a página de detalhes.
6. Selecione **Repetir clone de conta**.



Se o erro tiver sido resolvido, a conta de locatário será clonada para a outra grade.

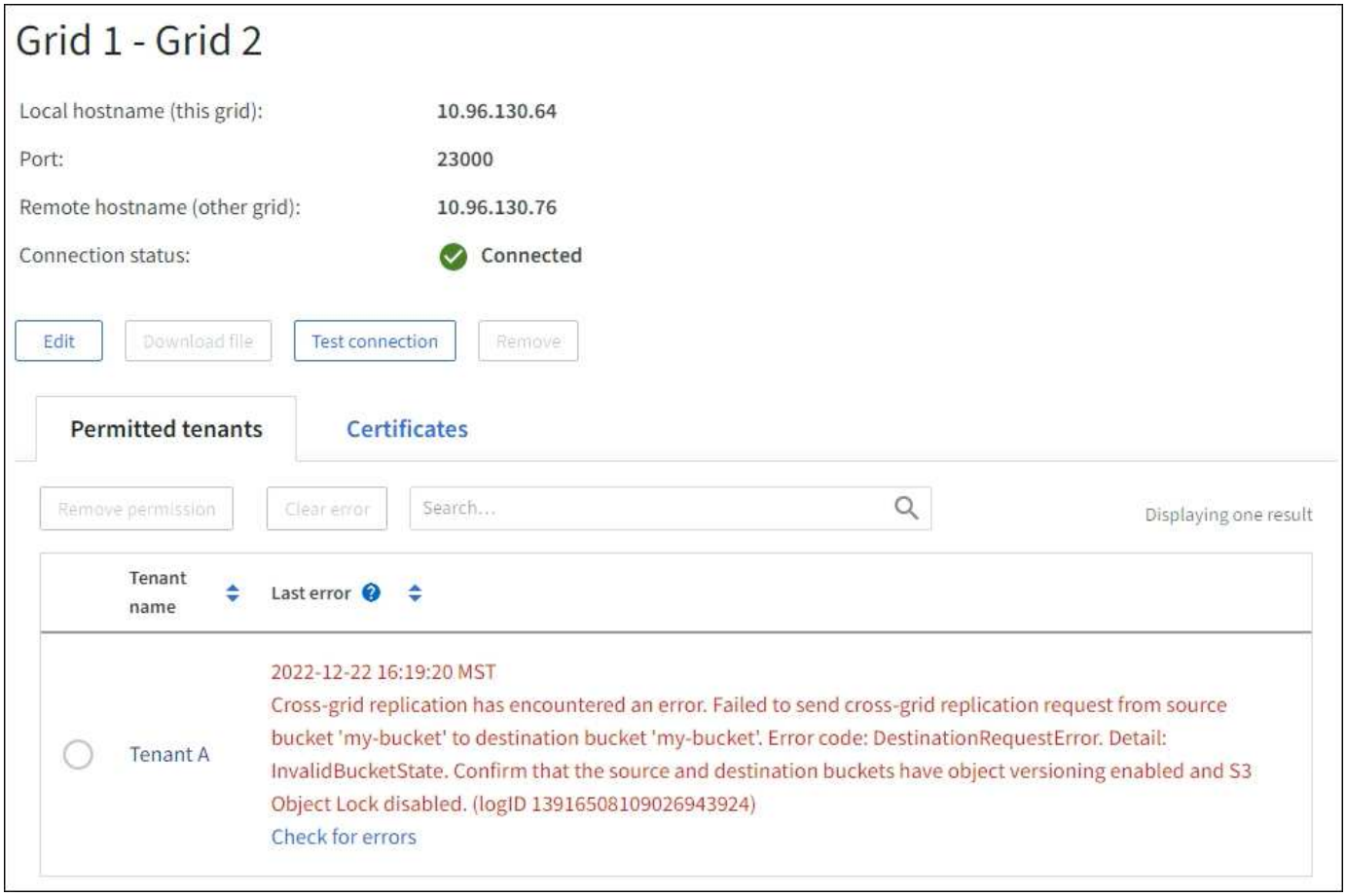
Alertas e erros de replicação entre redes

Último erro mostrado para conexão ou locatário

Problema

Quando "exibindo uma conexão de federação de grade" (ou "gerir os inquilinos permitidos"quando 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 a ocorrer, 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 grelha a ocorrer; os erros anteriores que possam ter ocorrido não serão apresentados. Um erro nesta coluna pode ocorrer por um destes motivos:

- A versão do objeto fonte não foi encontrada.
- O balde de origem não foi encontrado.
- O intervalo de destino foi eliminado.
- O intervalo de destino foi recriado por uma conta diferente.
- O bucket de destino tem controle de versão suspenso.
- O intervalo de destino foi recriado pela mesma conta, mas agora não foi versionado.

Ações recomendadas

Se aparecer uma mensagem de erro na coluna **último erro**, siga estes passos:

1. Reveja o texto da mensagem.
2. Execute quaisquer ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão desse bucket.
3. Selecione a conta de conexão ou locatário na tabela.
4. Selecione **Clear error**.

5. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.
6. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

> Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

> Depois de limpar o erro, um novo **último erro** pode aparecer se os objetos forem ingeridos em um intervalo diferente que também tenha um erro.

7. Para determinar se algum objeto não pôde ser replicado devido ao erro de bucket, "Identificar e tentar novamente operações de replicação com falha"consulte .

Alerta de falha permanente de replicação entre redes

Problema

O alerta **Falha permanente de replicação entre redes** foi acionado.

Detalhes

Esse alerta indica que os objetos de locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer a intervenção do usuário para serem resolvidos. Este alerta é normalmente causado por uma alteração na origem ou no intervalo de destino.

Ações recomendadas

1. Inicie sessão na grelha onde o alerta foi acionado.
2. Aceda a **CONFIGURATION** > **System** > **Grid Federation** e localize o nome da ligação listado no alerta.
3. Na guia inquilinos permitidos, observe a coluna **último erro** para determinar quais contas de locatário têm erros.
4. Para saber mais sobre a falha, consulte as instruções em "Monitorar conexões de federação de grade" para analisar as métricas de replicação entre grades.
5. Para cada conta de locatário afetada:
   a. Consulte as instruções em "Monitorar a atividade do locatário" 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 Tenant Manager em ambas as grades, para que você possa comparar a lista de buckets.
7. Para cada bucket com replicação entre grades ativada, confirme o seguinte:
   - Há um intervalo correspondente para o mesmo inquilino na outra grade (deve usar o nome exato).
   - Ambos os buckets têm o controle de versão de objetos ativado (o controle de versão não pode ser suspenso em nenhuma grade).
   - Ambos os buckets têm o bloqueio de objeto S3 desativado.
   - Nenhum dos buckets está no estado **Deletando objetos: Somente leitura**.
8. Para confirmar que o problema foi resolvido, consulte as instruções em "Monitorar conexões de federação de grade" para rever as métricas de replicação entre redes ou execute estas etapas:

a. Volte para a página de federação de Grade.

b. Selecione o locatário afetado e selecione **Limpar erro** na coluna **último erro**.

c. Selecione **Sim** para limpar a mensagem e atualizar o estado do sistema.

d. Aguarde 5-6 minutos e, em seguida, insira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.

> Para garantir que a mensagem de erro seja limpa, aguarde pelo menos 5 minutos após o carimbo de data/hora na mensagem antes de inserir um novo objeto.

> Pode levar até um dia para que o alerta seja apagado depois que ele for resolvido.

a. Aceda a "Identificar e tentar novamente operações de replicação com falha" para identificar quaisquer objetos ou eliminar marcadores que não foram replicados para a outra grelha e para tentar novamente a replicação conforme necessário.

Alerta de recurso de replicação entre redes indisponível

Problema

O alerta **recurso de replicação entre redes indisponível** foi acionado.

Detalhes

Esse alerta indica que as solicitações de replicação entre grade 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 resolve sozinho.
2. Se o problema persistir, determine se qualquer grade tem um alerta **Falha na conexão de federação de grade** para a mesma conexão ou um alerta **não é possível se comunicar com nó** para um nó. Esse alerta pode ser resolvido quando você resolve esses alertas.
3. Para saber mais sobre a falha, consulte as instruções em "Monitorar conexões de federação de grade" para analisar 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 redes**, você deve determinar se algum objeto ou marcador de exclusão não foi replicado para a outra grade. Em seguida, você pode reingerir esses objetos ou usar a API de Gerenciamento de Grade para repetir a replicação.

O alerta **Falha permanente de replicação entre redes** indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer a intervenção do usuário para serem resolvidos. Este alerta é normalmente causado por uma alteração na origem ou no intervalo de destino. Para obter detalhes, "Solucionar erros de federação de grade"consulte .

Determine se algum objeto não pôde ser replicado

Para determinar se algum objeto ou marcador de exclusão não foram replicados para a outra grade, você pode pesquisar mensagens no log de auditoria"CGRR (solicitação de replicação entre grades)". Essa mensagem é adicionada ao log quando o StorageGRID não consegue replicar um objeto, objeto multiparte ou excluir um marcador para o bucket de destino.

Você pode usar o "ferramenta de auditoria-explicação" para traduzir os resultados em um formato mais fácil de ler.

Antes de começar

- Você tem permissão de acesso root.
- Você tem o `Passwords.txt` arquivo.
- Você conhece o endereço IP do nó de administração principal.

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Procure mensagens CGRR no audit.log e use a ferramenta audit-explain para formatar os resultados.

   Por exemplo, este comando greps para 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 parecidos com este exemplo, que tem entradas para seis mensagens CGRR. No exemplo, todas as solicitações de replicação entre grades retornavam um erro geral porque o objeto não podia 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 Grade CGRR	O nome da solicitação
locatário	ID da conta do locatário
ligação	O ID da conexão de federação de grade
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de eliminação • replique objeto multipart
balde	O nome do intervalo
objeto	O nome do objeto
versão	O ID da versão para o objeto
erro	O tipo de erro. Se a replicação entre redes falhou, o erro é "erro geral".

Repetir repetições falhadas

Depois de gerar uma lista de objetos e excluir marcadores que não foram replicados para o bucket de destino e resolver os problemas subjacentes, você pode repetir a replicação de duas maneiras:

- Reingira cada objeto no intervalo de origem.
- Use a API privada de Gerenciamento de Grade, conforme descrito.

Passos

1. Na parte superior do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Selecione **vá para a 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 endpoint:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Selecione **Experimente**.
5. Na caixa de texto **body**, substitua a entrada de exemplo para **versionID** por uma ID de versão do audit.log que corresponde a uma solicitação de replicação entre grade e 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 grade para a outra grade.

   Pendente significa que a solicitação de replicação entre grade foi adicionada à fila interna para processamento.

Monitorar 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 as operações de repetição de duas maneiras:

- Use um S3 "Objeto HEAD" ou "Objeto GET" pedido. A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes valores:

Grelha	Estado da replicação
Fonte	• **SUCESSO**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FAILURE**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	• RÉPLICA*: O objeto foi replicado a partir 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 endpoint:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Selecione **Experimente**.
3. Na seção parâmetro, insira o ID da versão que você usou na `cross-grid-replication-retry-failed` solicitação.
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.
   - **COMPLETED**: A replicação foi bem-sucedida.
   - **FAILED**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar a segurança

Gerenciar a segurança: Visão geral

Você pode configurar várias configurações de segurança do Gerenciador de Grade para ajudar a proteger seu sistema StorageGRID.

Gerenciar a criptografia

O StorageGRID oferece várias opções para criptografar dados. Você deve "reveja os métodos de encriptação disponíveis"determinar quais atendem aos requisitos de proteção de dados.

Gerenciar certificados

Você pode "configure e gerencie os certificados do servidor" usar para conexões HTTP ou os certificados de cliente usados para autenticar uma identidade de cliente ou usuário no servidor.

Configurar servidores de gerenciamento de chaves

O uso de um "servidor de gerenciamento de chaves" permite proteger os dados do StorageGRID mesmo que

um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode 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 storage em nuvem, poderá configurar um "Servidor proxy de storage" entre nós de storage e os pontos de extremidade externos do S3. Se você enviar mensagens AutoSupport usando HTTPS ou HTTP, poderá configurar um "Servidor proxy Admin" entre nós de administração e suporte técnico.

Controle firewalls

Para melhorar a segurança do 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 à rede a cada nó configurando o respetivo "firewall interno". Você pode impedir o acesso em todas as portas, exceto as necessárias para sua implantação.

Reveja os métodos de encriptação StorageGRID

O StorageGRID oferece várias opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais métodos atendem aos 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	"configurar um servidor de gerenciamento de chaves"Você para o site StorageGRID e "habilite a criptografia de nó para o dispositivo". Em seguida, um nó de dispositivo se coneta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivo que têm **Node Encryption** ativado durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. O gerenciamento de chaves de criptografia com um KMS só é compatível com nós de storage e dispositivos de serviços.

Opção de criptografia	Como funciona	Aplica-se a
Conduza a segurança no Gerenciador de sistemas do SANtricity	Se o recurso Segurança da unidade estiver habilitado para um dispositivo de armazenamento SG5700 ou SG6000, você poderá usar "Gerente do sistema da SANtricity" o para criar e gerenciar a chave de segurança. A chave é necessária para aceder aos dados nas unidades seguras.	Dispositivos de storage com unidades Full Disk Encryption (FDE) ou unidades FIPS. 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 qualquer dispositivo de serviço.
Criptografia de objeto armazenado	Você ativa a "Criptografia de objeto armazenado" opção no Gerenciador de Grade. 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 e Swift recém-ingeridos. Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.
Criptografia de bucket do S3	Você emite uma solicitação de criptografia PUT Bucket 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 objeto S3 recém-ingeridos. A criptografia deve ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os 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 objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. StorageGRID gerencia as chaves. "Use a criptografia do lado do servidor"

Opção de criptografia	Como funciona	Aplica-se a
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 incluir 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 objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use a criptografia do lado do servidor"
Criptografia de volume externo ou datastore	Você usa um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação o suportar.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado. Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.
Criptografia de objetos fora do StorageGRID	Você usa um método de criptografia fora do StorageGRID para criptografar dados e metadados de objetos antes que eles sejam ingeridos no StorageGRID.	Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados). Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente"

Use vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistema do SANtricity para "criptografar" os dados nas unidades de autocriptografia nos mesmos dispositivos.

- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de criptografia de objeto armazenado para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

Gerenciar certificados

Gerenciar certificados de segurança: Visão geral

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 os dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam uma identidade de cliente ou usuário no servidor, fornecendo autenticação mais segura do que senhas sozinhas. Os certificados de cliente não encriptam dados.

Quando um cliente se coneta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica esse 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 o servidor para algumas conexões (como o endpoint do balanceador de carga) ou como o cliente para outras conexões (como o serviço de replicação do CloudMirror).

- Certificado padrão de CA de grade*

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado interno da CA de grade durante a instalação do sistema. O certificado de CA de grade é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora seja possível usar o certificado da CA de Grade para um ambiente que não seja de produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não protegidas sem certificado também são suportadas, mas não são recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser os especificados para verificar conexões de servidor.
- Todos os certificados personalizados devem atender ao "diretrizes de fortalecimento 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 da 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 em vez do certificado CA do sistema operacional.

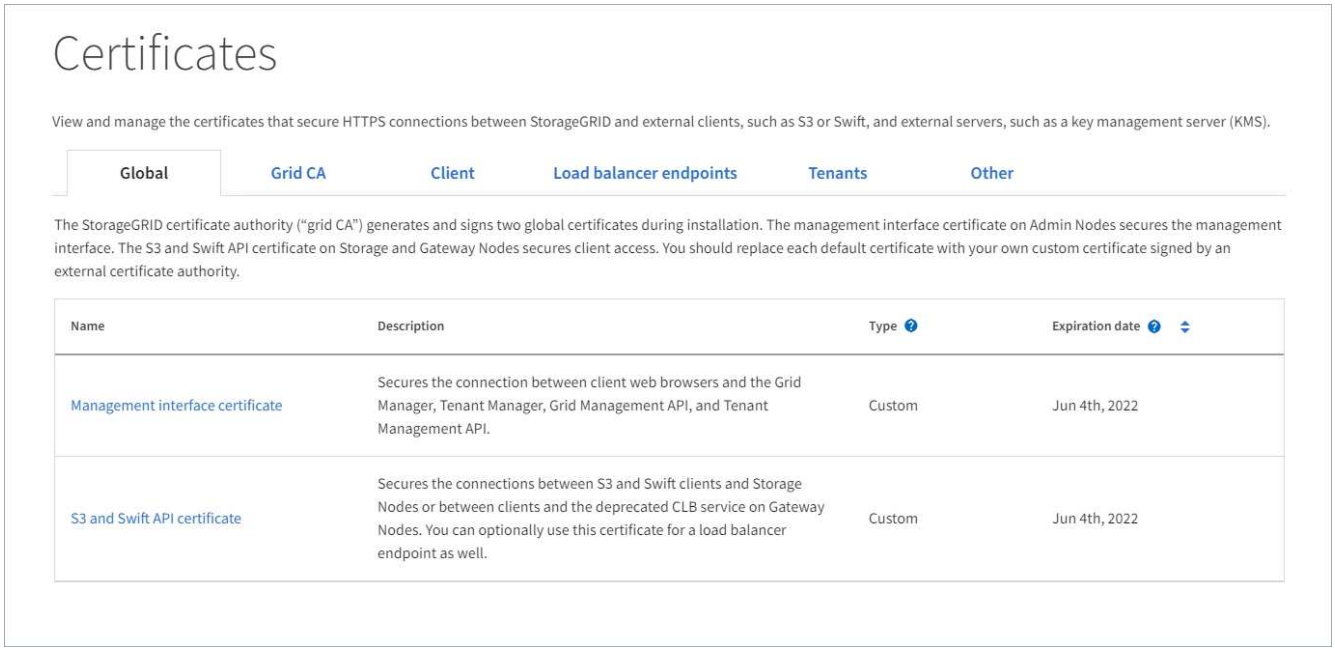
Variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Acesse certificados de segurança

Você pode acessar informações sobre todos os certificados do StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates**.



2. Selecione uma guia na página certificados para obter informações sobre cada categoria de certificado e para acessar as configurações de certificado. Você só pode acessar uma guia se tiver a permissão apropriada.

   - * Global*: Protege o acesso à StorageGRID de navegadores da web e clientes de API externos.
   - * Grade CA*: Protege o tráfego interno do StorageGRID.
   - **Cliente**: Protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - * Terminais de balanceador de carga*: Protege conexões entre clientes S3 e Swift e o balanceador de carga StorageGRID.
   - * Inquilinos*: Protege conexões com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de armazenamento S3.
   - **Outros**: Protege conexões StorageGRID que exigem certificados específicos.

   Cada guia é descrito abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso à StorageGRID a partir de navegadores da Web e clientes externos da API S3 e Swift. Dois certificados globais são inicialmente gerados pela autoridade de certificação StorageGRID durante a instalação. A prática recomendada 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 às interfaces de gerenciamento do StorageGRID.
- Certificado API S3 e Swift: Protege as conexões da API do cliente aos nós de storage, nós de administração e nós de gateway, que os aplicativos clientes S3 e Swift 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 expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - "Substitua o certificado padrão da interface de gerenciamento gerado pelo StorageGRID" Usado para conexões do Grid Manager e do Tenant Manager.
  - "Substitua o certificado API S3 e Swift" Usado para conexões do nó de armazenamento e do ponto de extremidade do balanceador de carga (opcional).
- "Restaure o certificado padrão da interface de gerenciamento."
- "Restaure o certificado padrão da API S3 e Swift."
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado."
- Copie ou transfira a "certificado de interface de gerenciamento" ou "Certificado API S3 e Swift".

CA da grelha

O Certificado CA de grade, gerado pela autoridade de certificação 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 da CA de Grade", mas não pode alterá-lo.

Cliente

Certificados de cliente, Gerado por uma autoridade de certificação externa, proteja as conexões entre ferramentas de monitoramento externas e o banco de dados do 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 Prometheus, juntamente com a data de validade 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:
  - "Altere o nome do certificado do cliente."
  - "Defina a permissão de acesso 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", "fixe", ou "retire" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los ao mesmo tempo usando **ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de terminais do balanceador de carga Proteja as conexões entre clientes S3 e Swift e o serviço de balanceamento de carga StorageGRID em nós de gateway e nós de administração.

A tabela de endpoint do balanceador de carga tem uma linha para cada endpoint do balanceador de carga configurado e indica se o certificado global S3 e Swift API ou um certificado de endpoint do balanceador de carga personalizado está sendo usado para o endpoint. A data de validade de cada certificado também é exibida.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- "Exibir um ponto final do balanceador de carga", incluindo os respetivos detalhes do certificado.
- "Especifique um certificado de endpoint do balanceador de carga para o FabricPool."
- "Use o certificado global S3 e Swift API" em vez de gerar um novo certificado de endpoint do balanceador de carga.

Inquilinos

Os locatários podem usar certificados de servidor de federação de identidade ou certificados de endpoint de serviço de plataformaproteger suas conexões com o StorageGRID.

A tabela de locatário 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 locatário para iniciar sessão no Gestor de inquilinos"
- "Selecione um nome de locatário para exibir os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma do locatário"
- "Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint"

Outros

O StorageGRID usa outros certificados de segurança para fins específicos. Estes certificados são listados pelo seu nome funcional. Outros certificados de segurança incluem:

- Certificados do Cloud Storage Pool
- Certificados de notificação de alerta por e-mail
- Certificados de servidor syslog externos
- Certificados de conexão de federação de grade
- Certificados de federação de identidade
- Certificados de servidor de gerenciamento de chaves (KMS)
- Certificados de logon único

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração do certificado do servidor e do cliente, conforme aplicável. A seleção de um nome de função abre uma guia do navegador onde você pode exibir e editar os detalhes do certificado.

> Você só pode exibir e acessar informações de outros certificados se tiver a permissão apropriada.

Você pode:

- "Especifique um certificado do Cloud Storage Pool para S3, C2S S3 ou Azure"
- "Especifique um certificado para notificações por e-mail de alerta"
- "Especifique um certificado de servidor syslog externo"
- "Girar certificados de conexão de federação de grade"
- "Exibir e editar um certificado de federação de identidade"
- "Carregar certificados de servidor de gerenciamento de chaves (KMS) e cliente"
- "Especifique manualmente um certificado SSO para uma confiança de parte dependente"

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 navegadores da Web cliente e a interface de gerenciamento do StorageGRID, permitindo que os usuários acessem o Gerenciador de Grade e o Gerenciador de locatário sem avisos de segurança. Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário. Pode utilizar o certificado predefinido criado durante a instalação ou carregar um certificado personalizado.	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **Management interface certificate**	"Configurar certificados de interface de gerenciamento"

Certificado API S3 e Swift

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 ou Swift a um nó de storage e a terminais de balanceador de carga (opcional).	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **S3 e Swift API certificate**	"Configure os certificados API S3 e Swift"

Certificado CA de grade

Consulte Descrição do certificado da 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 cliente externo. • Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**CONFIGURATION** > **Security** > **Certificates** e selecione a guia **Client**	"Configurar certificados de cliente"

Certificado de ponto final do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode fazer upload ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos clientes usam o certificado do balanceador de carga ao se conetar ao StorageGRID para salvar e recuperar dados de objeto. Você também pode usar uma versão personalizada do certificado global Certificado API S3 e Swiftpara 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. **Nota:** o certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID.	**CONFIGURATION** > **Network** > **Load balancer endpoints**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade do balanceador de carga para o FabricPool"

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de storage de nuvem do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **conjuntos de armazenamento**	"Crie um pool de storage 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 TLS (Transport Layer Security), 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 do 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. **Nota:** não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP a um servidor syslog externo.	**CONFIGURATION** > **Monitoring** > **Audit and syslog Server** e selecione **Configure External syslog Server**	"Configurar um servidor syslog externo"

certificado de conexão de federação de grade

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.	**CONFIGURATION** > **System** > **Grid Federation**	• "Crie conexões de federação de grade" • "Rode os certificados de ligação"

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 ative Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, que permite que grupos de administração e usuários sejam gerenciados por um sistema externo.	**CONFIGURATION** > **Access Control** > **Identity Federation**	"Use a federação de identidade"

Certificado de 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.	**CONFIGURATION** > **Security** > **Key Management Server**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID a um recurso de storage S3.	**Gerenciador do Locatário** > **ARMAZENAMENTO (S3)** > **terminais de serviços da plataforma**	"Criar endpoint de serviços de plataforma" "Editar endpoint de serviços de 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 AD FS (Serviços de Federação do ative Directory) e StorageGRID usados para solicitações de logon único (SSO).	**CONFIGURATION** > **access control** > **Single sign-on**	"Configurar o logon único"

Exemplos de certificados

Exemplo 1: Serviço do Load Balancer

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 ou Swift para o endpoint do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se coneta ao endpoint 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 esse 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 de objeto para o StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externas (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software servidor de gerenciamento de chaves externo, 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 Gerenciador de Grade, você configura um servidor KMS e carrega os certificados de servidor e 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 com base 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.

Configurar certificados de servidor

Tipos de certificado de servidor suportados

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elítica).

> O tipo de codificação da diretiva de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, as cifras RSA exigem certificados RSA e as cifras ECDSA exigem certificados ECDSA. "Gerenciar certificados de segurança"Consulte . Se configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, pode "reverter temporariamente para a política de segurança padrão".

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, "Configurar a segurança para a API REST do S3"consulte ou "Configure a segurança para a API Swift REST".

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 Gerenciador de Grade e o Gerenciador do locatário 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 administrador é emitido um certificado assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e uma 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 multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao Gerenciador de Grade e ao Gerenciador de locatário. Defina o certificado personalizado de modo que 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 você está usando, os usuários também podem precisar instalar o certificado de CA de grade no navegador da Web que eles usarão para acessar o Gerenciador de Grade e o Gerenciador de locatário.

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Management Interface** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado da interface de gerenciamento na guia Global.

Se você estiver acessando o Gerenciador de Grade ou o Gerenciador de locatário usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se uma das seguintes situações ocorrer:

- O certificado de interface de gerenciamento personalizado expira.
- reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrãoVocê .

Adicione 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 Gerenciador de Grade.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
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 ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas 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 de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, 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 certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

Gerar certificado

Gere os ficheiros de certificado do servidor.

> A prática recomendada para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto 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.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

> Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página de certificado de interface de gerenciamento exibe informações detalhadas de certificado para os certificados que estão em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da interface de gerenciamento

Você pode reverter para o uso do certificado de interface de gerenciamento padrão para conexões do Gerenciador de Grade e do Gerenciador de Tenant.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura o certificado de interface de gerenciamento padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação estrita 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 Admin.
2. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará 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 caractere curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
   - Defina `--type` como `management` para configurar o certificado da interface de gerenciamento, que é usado pelo Gerenciador de Grade e pelo Gerenciador de Locatário.
   - 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 pelo cliente da API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags DE INÍCIO e FIM em sua seleção.

5. Faça logout do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Gerenciador de Grade.
   b. Selecione **CONFIGURATION** > **Security** > **Certificates**
   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 DE INÍCIO e FIM.

Transfira ou copie o certificado da interface de gestão

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote 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 de certificado e o local de 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 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`

Configure os certificados API S3 e Swift

Você pode substituir ou restaurar o certificado de servidor usado para conexões de cliente S3 ou Swift para nós de armazenamento ou para terminais de balanceador de carga. O certificado de servidor personalizado de substituição é específico para a sua organização.

Sobre esta tarefa

Por padrão, cada nó de armazenamento é emitido um certificado de servidor X,509 assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma 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 multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao endpoint de armazenamento. Defina o certificado personalizado de modo que corresponda a todos os nós de storage na grade.

Depois de concluir a configuração no servidor, você também pode precisar instalar o certificado de CA de Grade no cliente API S3 ou Swift que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que você estiver usando.

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of global Server certificate for S3 and Swift API** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de expiração do certificado API S3 e Swift na guia Global.

Você pode fazer upload ou gerar um certificado personalizado de API S3 e Swift.

Adicione um certificado personalizado de API S3 e Swift

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas 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 de certificação de emissão intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado personalizado da API S3 e Swift que foi carregado. Se você carregou um pacote opcional da CA, 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 certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**.

  O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

Gerar certificado

Gere os ficheiros de certificado do servidor.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.

Campo	Descrição
Assunto (opcional)	X,509 Assunto 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.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM para o certificado personalizado da API S3 e Swift que foi gerado.

   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**.

   O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

5. Selecione uma guia para exibir metadados para o certificado padrão do servidor StorageGRID, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.

   Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da Web seja atualizado.

7. Depois de adicionar um certificado personalizado de API S3 e Swift, a página de certificado de API S3 e Swift exibe informações detalhadas de certificado para o certificado personalizado de API S3 e Swift que está em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da API S3 e Swift

Você pode reverter para o uso do certificado padrão S3 e Swift API para conexões de clientes S3 e Swift para nós de storage. No entanto, você não pode usar o certificado padrão S3 e Swift API para um endpoint de balanceador de carga.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura a versão padrão do certificado global S3 e Swift API, os arquivos de certificado de servidor personalizado que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão S3 e Swift API será usado para novas conexões de clientes S3 e Swift subsequentes aos nós de armazenamento.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3 e Swift.

   Se você tiver permissão de acesso root e o certificado personalizado S3 e Swift API foi usado para conexões de endpoint do balanceador de carga, uma lista será exibida de endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão S3 e Swift API. Aceda a "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 seja atualizado.

Faça o download ou copie o certificado API S3 e Swift

Você pode salvar ou copiar o conteúdo do certificado S3 e Swift API para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote 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 de certificado e o local de 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 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

- "USE A API REST DO S3"
- "Use a API Swift REST"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado da CA de Grade

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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente devem verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado da CA do sistema StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificate PEM**, baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado 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 executam validação estrita de nome de host e não suportam a desativação estrita de validação 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".

Sobre esta tarefa

Ao criar um endpoint de 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. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam FabricPool. Para obter informações e procedimentos mais detalhados, "Configurar o StorageGRID para FabricPool"consulte .

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso do FabricPool.
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

Quando você cria um endpoint do balanceador de carga HTTPS, é solicitado que você carregue o certificado do servidor, a chave privada do certificado e o pacote opcional da CA.

3. Anexar o StorageGRID como uma categoria de nuvem no ONTAP.

   Especifique a porta de endpoint do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado CA.

   > Se uma CA intermediária tiver emitido o certificado StorageGRID, você deverá fornecer o certificado de CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.

Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus, fornecendo uma maneira segura para que ferramentas externas monitorem o StorageGRID.

Se você precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deve carregar ou gerar um certificado de cliente usando o Gerenciador de Grade e copiar as informações do certificado para a ferramenta externa.

"Gerenciar certificados de segurança"Consulte 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 ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado do cliente na guia Client.

> Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivo especialmente configurados, consulte as informações específicas sobre "Carregar um certificado de cliente KMS"o .

Antes de começar

- Você tem permissão de acesso root.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Se tiver configurado o certificado da interface de gerenciamento do StorageGRID, você terá a CA, o certificado do cliente e a chave privada usadas para configurar o certificado da interface de gerenciamento.
  - Para carregar o seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou gravada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.
- Para editar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.

- Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no computador local.

Adicionar certificados de cliente

Para adicionar o certificado de 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 Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, 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 **Procurar** e selecione o ficheiro de certificado da interface de gestão (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      O novo certificado é exibido na guia Cliente.
7. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use um certificado de cliente emitido pela CA e uma chave privada.

Passos

1. Execute as etapas para "configurar um certificado de interface de gerenciamento".
2. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

3. Selecione **Adicionar**.
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, 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 CA:
   a. Selecione **carregar certificado**.
   b. Selecione **Procurar** e selecione o certificado do cliente, a chave privada e os ficheiros do pacote CA (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      Os novos certificados aparecem na guia Cliente.
8. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use a função gerar certificado no Gerenciador de Grade.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
5. Selecione **continuar**.
6. Para a etapa **Anexar certificados**, selecione **gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): X,509 Assunto 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 é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

8. Selecione **Generate**.
9. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
   - Selecione **Download private key** para salvar a chave privada como um arquivo.

     Especifique o nome do arquivo de chave privada e o local de download.

10. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

    O novo certificado é exibido na guia Cliente.

11. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Global**.
12. Selecione **certificado de interface de gestão**.
13. Selecione **usar certificado personalizado**.
14. Carregue os arquivos certificate.pem e private_key.pem da detalhes do certificado do cliente etapa. Não há necessidade de carregar o pacote CA.
    a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
    b. Carregar cada ficheiro de certificado (`.pem`).
    c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

       O novo certificado é exibido na guia Cliente.

15. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Configure uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.
   a. **Nome**: Insira um nome para a conexão.

      O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

   b. **URL**: Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

Por exemplo: `https://admin-node.example.com:9091`

c. Ative **TLS Client Auth** e **com CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole
   - A interface de gerenciamento certificado CA para **CA Cert**
   - O certificado de cliente para **Cert de cliente**
   - A chave privada para **chave do cliente**

e. **ServerName**: Insira o nome de domínio do nó Admin.

   Servername deve corresponder ao nome de domínio como 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 Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

   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, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione **Editar nome e permissão**
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
6. Selecione **continuar** para salvar o certificado no Gerenciador de Grade.

   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 **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.

b. Carregue 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 **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

   - **Assunto** (opcional): X,509 Assunto 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 é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo de chave privada e o local de download.

e. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

Baixe ou copie certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende copiar ou transferir.
3. Baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado

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 **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende remover.
3. Selecione **Delete** e confirme.

> Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **ações** > **Excluir**.

Depois que um certificado é removido, os clientes que usaram o certificado devem especificar um novo certificado de cliente para acessar o banco de dados do StorageGRID Prometheus.

Configure as definições de segurança

Gerencie 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 StorageGRID internos.

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 critérios comuns ou que você precise usar outras cifras.

> Alguns serviços do StorageGRID não foram atualizados para usar as cifras nessas políticas.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Selecione uma política de segurança

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.

   A guia **TLS e políticas SSH** mostra as políticas disponíveis. A política atualmente ativa é anotada por uma marca de seleção verde no bloco de política.

2. Revise os blocos para saber mais sobre as políticas disponíveis.

Política	Descrição
Compatibilidade moderna (padrão)	Use a política padrão se você precisar de criptografia forte e a menos que você tenha requisitos especiais. Esta política é compatível com a maioria dos clientes TLS e SSH.
Compatibilidade legada	Use esta política se precisar de opções de compatibilidade adicionais para clientes mais antigos. As opções adicionais desta política podem torná-la menos segura do que a política de compatibilidade moderna.
Critérios comuns	Use esta política se você precisar da certificação Common Criteria.
FIPS rigoroso	Use esta política se você precisar de certificação Common Criteria e precisar usar o módulo de segurança criptográfica NetApp 3.0.0 para conexões de clientes externos para terminais de balanceador de carga, Gerenciador de locatário e Gerenciador de Grade. O uso desta política pode reduzir o desempenho.
Personalizado	Crie uma política personalizada se você precisar aplicar seus próprios cifras.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Exibir detalhes**.
4. Para alterar a política atual, selecione **Use policy**.

   Uma marca de seleção verde aparece ao lado de **política atual** no bloco de política.

Crie uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar suas próprias cifras.

Passos

1. No bloco da política que é o mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e, em seguida, 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 **Use policy**.

   Uma marca de seleção verde aparece ao lado de **Current policy** no mosaico Custom policy (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 tiver configurado uma política de segurança personalizada, talvez não consiga entrar no Gerenciador de Grade se a diretiva TLS configurada for incompatível com o "certificado de servidor configurado".

Você pode reverter temporariamente para a política de segurança padrão.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Execute o seguinte comando:

   ```
   restore-default-cipher-configurations
   ```

3. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.
4. Siga as etapas em Selecione uma política de segurança para configurar a política novamente.

Configurar a segurança de rede e de objetos

Você pode configurar a segurança de rede e objetos para criptografar objetos armazenados, para impedir determinadas solicitações S3 e Swift ou para permitir que conexões de cliente aos nós de armazenamento usem HTTP em vez de HTTPS.

Criptografia de objeto armazenado

A criptografia de objeto armazenado permite a criptografia de todos os dados de objeto à medida que são ingeridos através do 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 aos objetos armazenados existentes. Se desativar a encriptação, os objetos atualmente encriptados permanecem encriptados, mas os objetos recentemente ingeridos não são encriptados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos S3 que não tenham sido criptografados por criptografia no nível do bucket ou no nível do objeto.

Para obter mais detalhes sobre os métodos de criptografia StorageGRID, "Reveja os métodos de encriptação StorageGRID"consulte .

Impedir a modificação do cliente

Impedir a modificação do cliente é uma configuração de todo o sistema. Quando a opção **Prevent client modification** é selecionada, as seguintes solicitações são negadas.

S3 API REST

- Eliminar pedidos de balde
- Quaisquer solicitações para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

Swift REST API

- Eliminar pedidos de contentor
- Solicitações para modificar qualquer objeto existente. Por exemplo, as seguintes operações são negadas: Put Overwrite, Delete, Metadata Update e assim por diante.

Ative HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para quaisquer conexões diretas aos nós de storage. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nó de armazenamento somente se os clientes S3 e Swift precisarem fazer conexões HTTP diretamente aos nós de armazenamento. Não é necessário usar essa opção para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode "configure cada ponto de extremidade do balanceador de carga"usar HTTP ou HTTPS).

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas S3 e clientes Swift usam ao se conetar a nós de armazenamento usando HTTP ou HTTPS.

Selecione as opções

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissão de acesso root.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **nenhum** (padrão) se você não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **Prevent client modification** se você quiser impedir que clientes S3 e Swift façam solicitações específicas.

   Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

5. Opcionalmente, selecione **Ativar HTTP para conexões de nó de armazenamento** se os clientes se conetarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

   Tenha cuidado ao ativar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

6. Selecione **Guardar**.

Alterar o tempo limite de inatividade do navegador

Você pode controlar se os usuários do Grid Manager e do Tenant Manager estão desconetados se estiverem inativos por mais de um determinado período de tempo.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissão de acesso root.

Sobre esta tarefa

O tempo limite de inatividade do navegador é predefinido para 15 minutos. Se o navegador de um usuário não estiver ativo por esse período de tempo, o usuário será desconetado.

Conforme necessário, você pode aumentar ou diminuir o período de tempo limite definindo a opção **Sair de usuários inativos após**.

O tempo limite de inatividade do navegador também é controlado pelo seguinte:

- Um temporizador StorageGRID separado, não configurável, incluído para a segurança do sistema. Por padrão, o token de autenticação de cada usuário expira 16 horas após o login do usuário. Quando a autenticação de um usuário expira, esse usuário é automaticamente desconetado, 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 entrar novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja

ativado para o StorageGRID.

Se o SSO estiver ativado e o navegador de um usuário expirar, o usuário deverá inserir novamente suas credenciais SSO para acessar o StorageGRID novamente. "Configurar o logon único"Consulte .

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **tempo limite de inatividade do navegador**.
3. No campo **Sair de usuários inativos após**, especifique um período de tempo limite do navegador entre 60 segundos e 7 dias.

   Você pode especificar o período de tempo limite do navegador em segundos, minutos, horas ou dias.

4. Selecione **Guardar**. Se um navegador estiver inativo durante o período de tempo especificado, o usuário será desconetado do Gerenciador de Grade ou do Gerenciador de Tenant.

   A nova configuração não afeta os usuários conetados atualmente. Os usuários devem entrar novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.

Configurar servidores de gerenciamento de chaves

Configurar servidores de gerenciamento de chaves: Visão geral

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para proteger os dados em nós de dispositivo especialmente configurados.

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 de dispositivos StorageGRID no site associado do StorageGRID usando o Protocolo de interoperabilidade de Gerenciamento de chaves (KMIP).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó de 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 dispositivo permite que você proteja seus dados mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

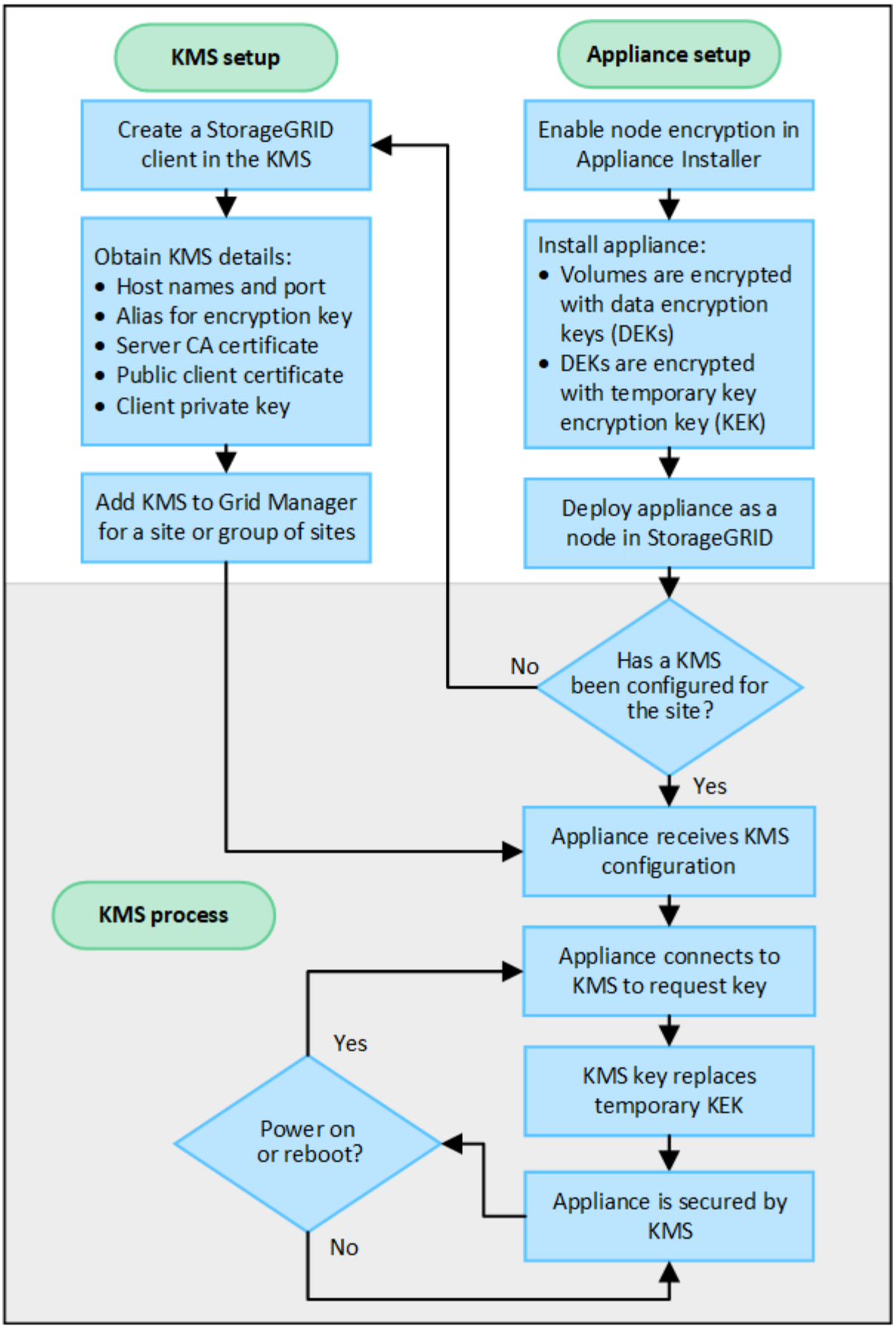
> O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do dispositivo. Se você pretende usar um servidor de gerenciamento de chaves externo para proteger dados do StorageGRID, você deve entender como configurar esse servidor e entender como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo dessas instruções. Se precisar de ajuda, consulte a documentação do servidor de gerenciamento de chaves ou entre em Contato com o suporte técnico.

Visão geral do KMS e da configuração do appliance

Antes de usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID nos 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 os dados do StorageGRID em nós do dispositivo.



O fluxograma mostra a configuração do KMS e a configuração do appliance ocorrendo em paralelo; no

entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nó para novos nós de 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.

Passo	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada cluster KMS ou KMS.	"Configure o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configure o StorageGRID como um cliente no KMS"
Adicione o KMS ao Gerenciador de Grade, 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)"

Configure o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui os seguintes passos de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo.

   > ⓘ Não é possível ativar 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 têm criptografia de nó ativada.

2. Execute o Instalador de dispositivos StorageGRID. Durante a instalação, uma chave de criptografia de dados aleatórios (DEK) é atribuída a cada volume de dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco LUKS (Unified Key Setup) do Linux no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). O KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conetar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

"Habilite a criptografia do nó"Consulte para obter 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 que tem criptografia de nó ativada na grade, o StorageGRID determina se existe uma configuração de KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o appliance receberá a configuração do KMS.

- Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão a ser criptografados pelo KEK temporário até que você configure um KMS para o site e o appliance receba a configuração do KMS.

2. O dispositivo usa a configuração KMS para se conetar 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 o KEK temporário e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

> Todos os dados existentes antes do nó de dispositivo criptografado se conetarem ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra a remoção do data center até que a chave temporária seja substituída pela chave de criptografia KMS.

4. Se o aparelho estiver ligado ou reinicializado, ele se reconeta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não pode sobreviver a uma perda 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.

Quais são os requisitos do KMIP?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID é compatível com as seguintes cifras TLS v1,2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Você deve garantir que cada nó de dispositivo que usa criptografia de nó tenha acesso de rede ao cluster KMS ou KMS configurado para o site.

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique através da porta usada para comunicações KMIP (Key Management Interoperability Protocol). A porta KMIP padrão é 5696.

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** ativada. Esta definição só pode ser ativada durante a fase de configuração de hardware da instalação do dispositivo utilizando o Instalador de dispositivos StorageGRID.

> Não é possível ativar a 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 têm a criptografia de nó ativada.

Você pode usar o KMS configurado para dispositivos StorageGRID e nós de dispositivo.

Não é possível usar o KMS configurado para nós baseados em software (não-appliance), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados nos mecanismos de contêiner em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no armazenamento de dados ou no nível de disco.

Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, você normalmente deve configurar um ou mais servidores de gerenciamento de chaves no Gerenciador de Grade 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 Gerenciador de Grade antes ou depois de instalar os nós do dispositivo.

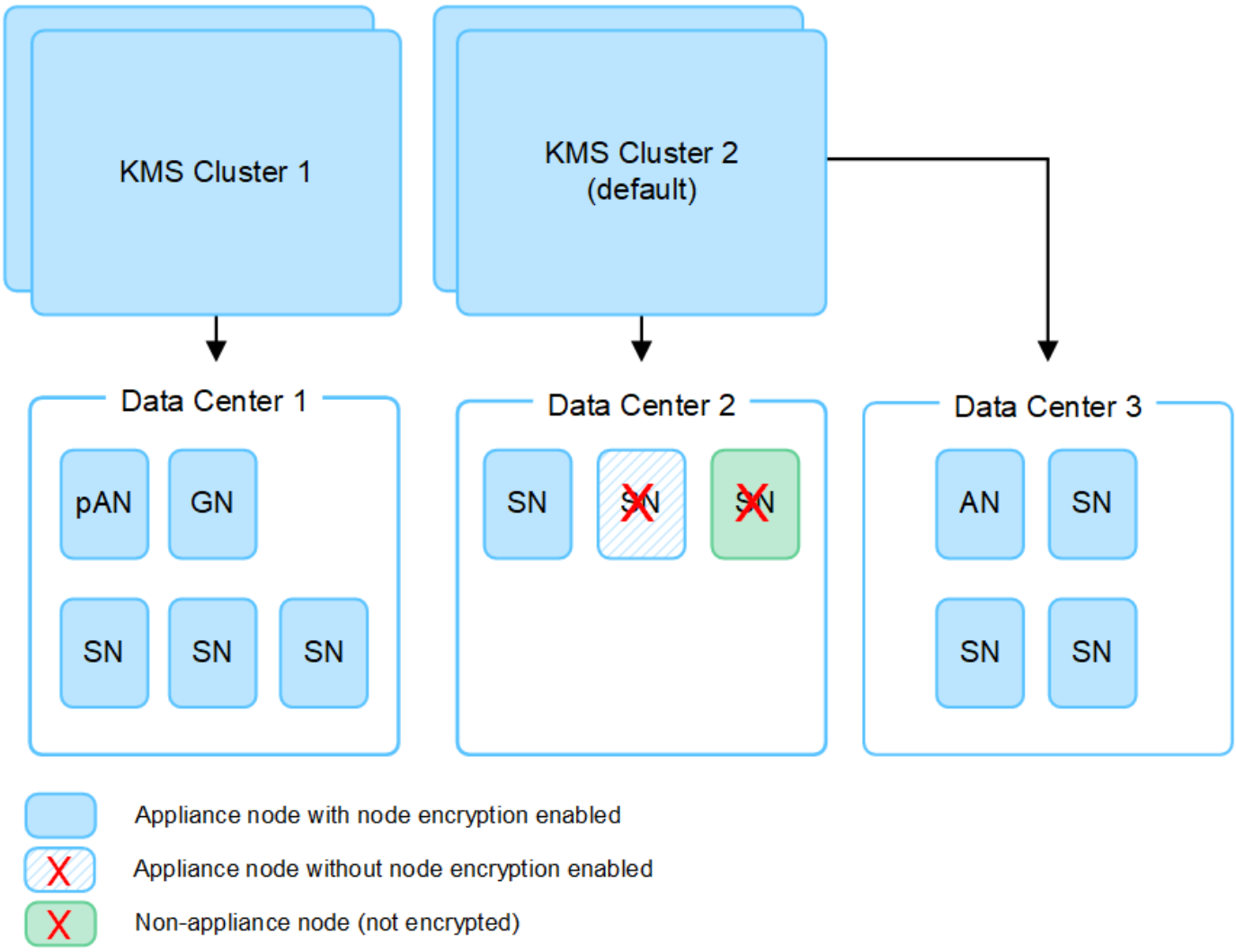
Quantos servidores de gerenciamento de chaves eu preciso?

Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

O StorageGRID é compatível com o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham configurações 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 locais. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que não é possível usar um KMS para nós que não sejam do dispositivo ou para nenhum nó de dispositivo que não tenha a configuração **criptografia do nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como prática recomendada de segurança, você deve girar periodicamente a chave de criptografia usada por cada KMS configurado.

Ao girar a chave de criptografia, use o software KMS para girar da última versão usada da chave para uma nova versão da mesma chave. Não rode para uma chave totalmente diferente.

> Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS no Gerenciador de Grade. Em vez disso, gire a chave atualizando a versão da chave no software KMS. Use o mesmo alias de chave para novas chaves que foi usado para chaves anteriores. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós de dispositivos criptografados no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora de quando a chave é girada.
- 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 reinicializada.

- Se a nova versão de chave não puder ser usada para criptografar volumes de appliance por qualquer motivo, o alerta **rotação da chave de criptografia KMS falhou** é acionado para o nó do appliance. Talvez seja necessário entrar em Contato com o suporte técnico para obter ajuda na resolução desse alerta.

Posso reutilizar um nó de appliance depois que ele foi criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID, primeiro será necessário desativar o nó da grade para mover dados de objeto para outro nó. Em seguida, você pode usar o Instalador de dispositivos StorageGRID para "Limpe a configuração do KMS". A limpeza da configuração KMS desativa a configuração **criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração KMS para o site StorageGRID.

> Sem acesso à chave de criptografia KMS, todos os dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

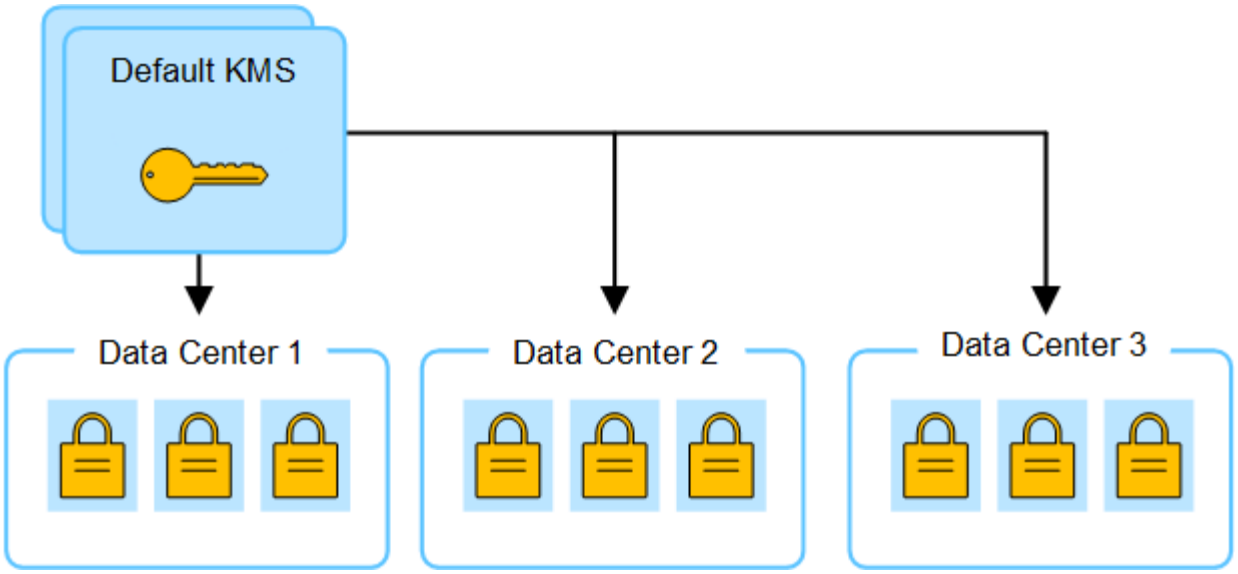
Considerações para alterar o KMS para um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único local 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.

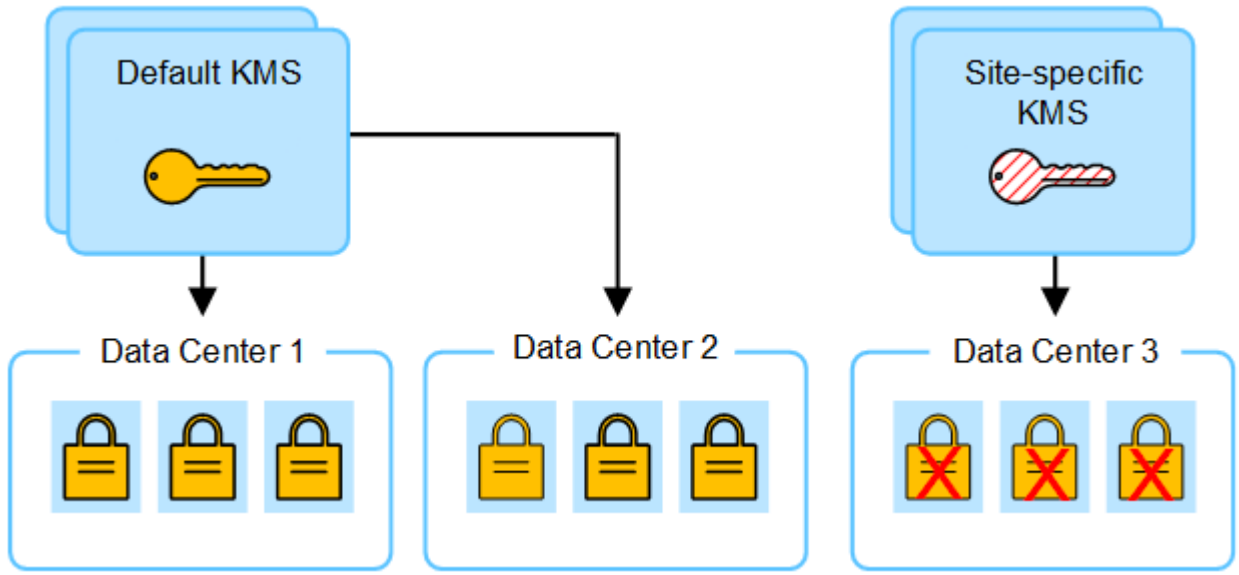
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

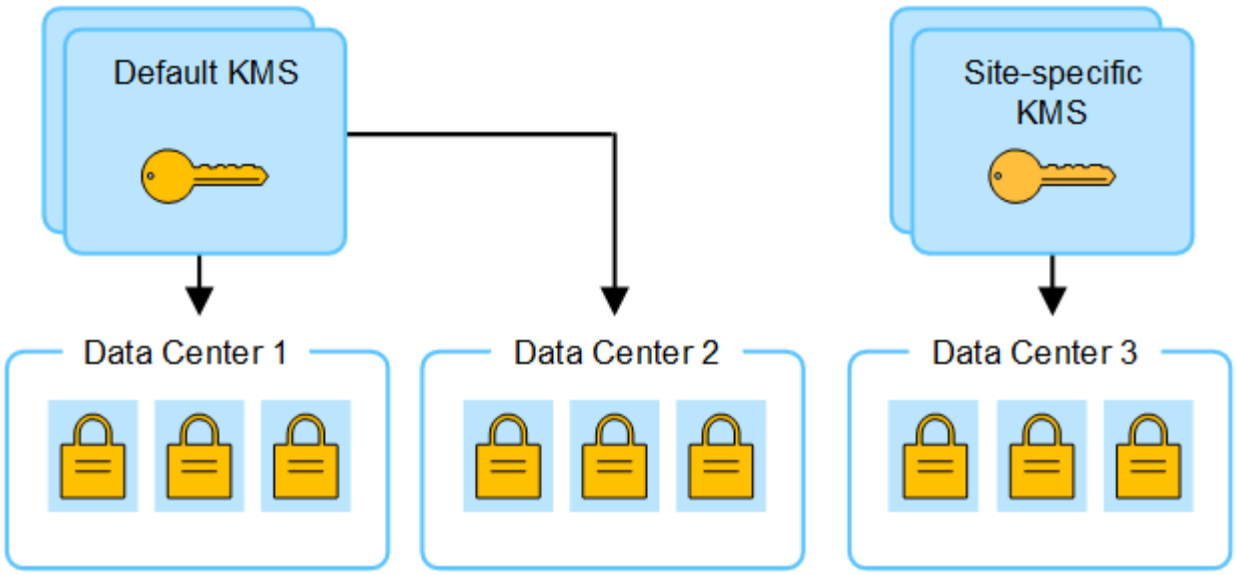
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós do dispositivo em todos os locais. Esta 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 appliance já estão criptografados, um erro de validação ocorre quando você tenta salvar a configuração para o KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós nesse 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 torna-se uma versão anterior da nova chave.) O KMS específico do local agora tem a chave correta para descriptografar os nós do appliance no Data Center 3, para que ele possa ser salvo 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 para alterar o KMS de um site.

Caso de uso para alterar o KMS de um site	Passos necessários
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como 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 se aplicará a quaisquer sites que não tenham 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 de appliance 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 Gerenciador de Grade, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS para um site use um servidor diferente.	1. Se os nós do dispositivo no local 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 Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure 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.

Sobre esta tarefa

Estas instruções aplicam-se ao Thales CipherTrust Manager. Para obter uma lista de versões suportadas, utilize o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Passos

1. A partir do software KMS, crie um cliente StorageGRID para cada cluster KMS ou KMS que você pretende usar.

   Cada KMS gerencia uma única chave de criptografia para os nós do StorageGRID Appliances em um único local ou em um grupo de sites.

2. A partir do software KMS, crie uma chave de criptografia AES para cada cluster KMS ou KMS.

   A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando você adiciona 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.

     > A chave de criptografia já deve existir no KMS. O StorageGRID não cria nem gerencia chaves KMS.

4. Para cada cluster KMS ou KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contém cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de 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 base-64 de Email Avançado de Privacidade (PEM).
   - O campo Nome alternativo do assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP ao qual o StorageGRID se conetará.

     > 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 de cliente permite que o StorageGRID se autentique no KMS.

Adicionar um servidor de gerenciamento de chaves (KMS)

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para

adicionar cada cluster KMS ou KMS.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você tem "Configurado o StorageGRID como um cliente no KMS", e você tem as informações necessárias para cada cluster KMS ou KMS.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

Sobre esta tarefa

Se possível, configure qualquer servidor de gerenciamento de chaves específico 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 copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. "Considerações para alterar o KMS para um site"Consulte para obter detalhes.

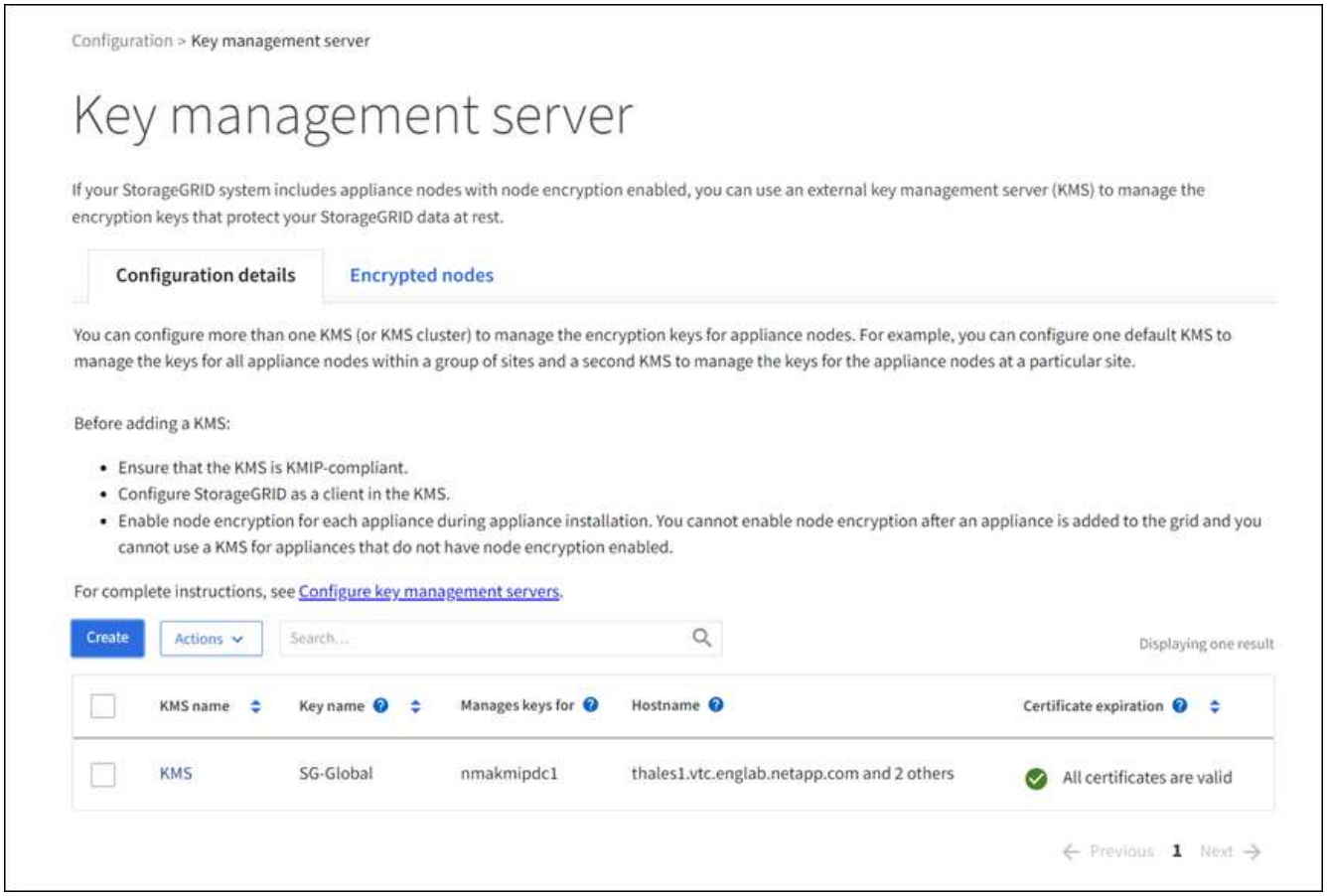
Passo 1: KMS detalhes

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

Passos

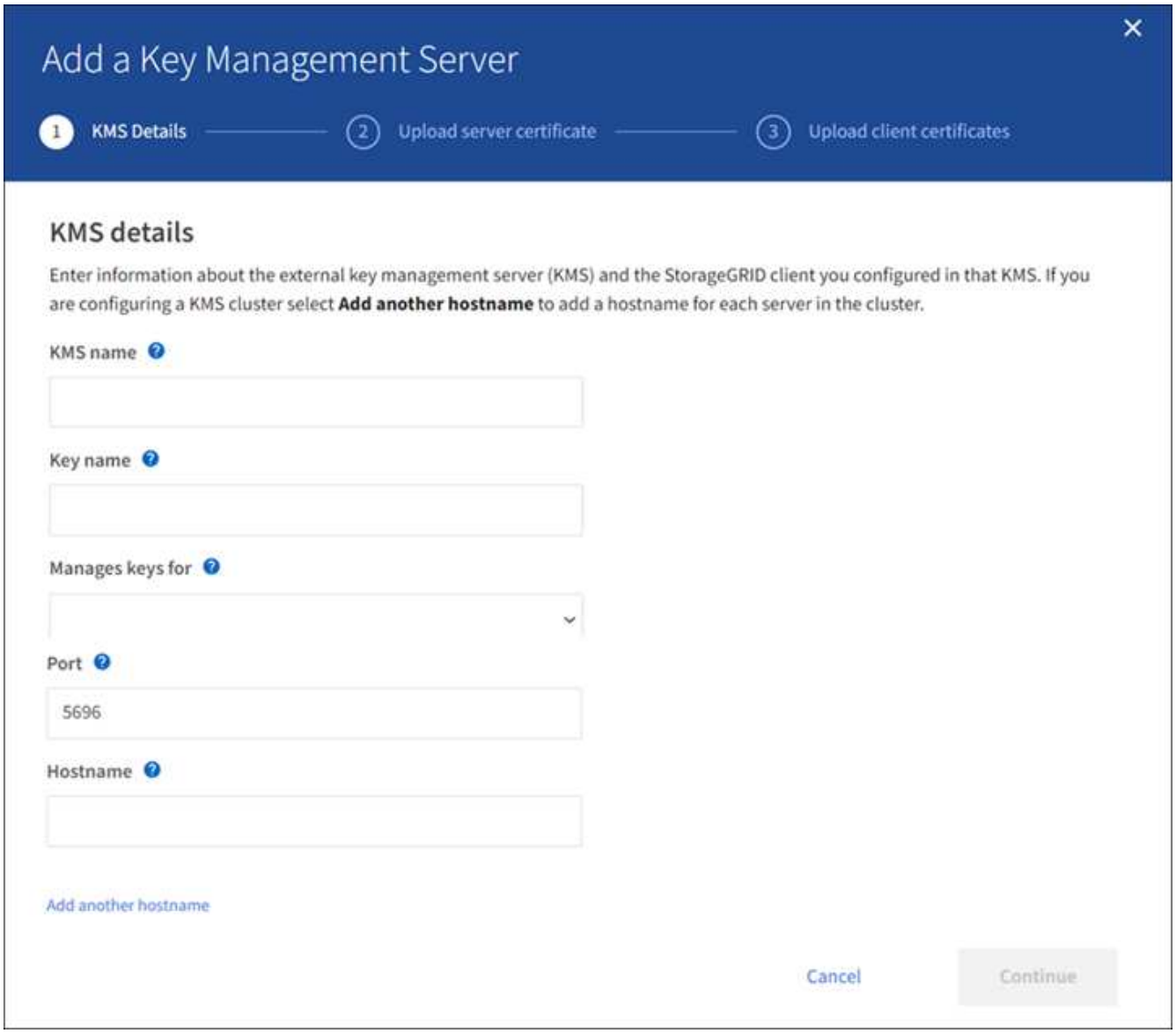
1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página 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
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres.

Campo	Descrição
Gere as chaves para	O site StorageGRID que será associado a este KMS. Se possível, você deve configurar qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplica 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 local específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que se aplicará a quaisquer sites que não tenham um KMS dedicado e a quaisquer sites que você adicionar em expansões subsequentes. **Nota:** 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 você não forneceu a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS.

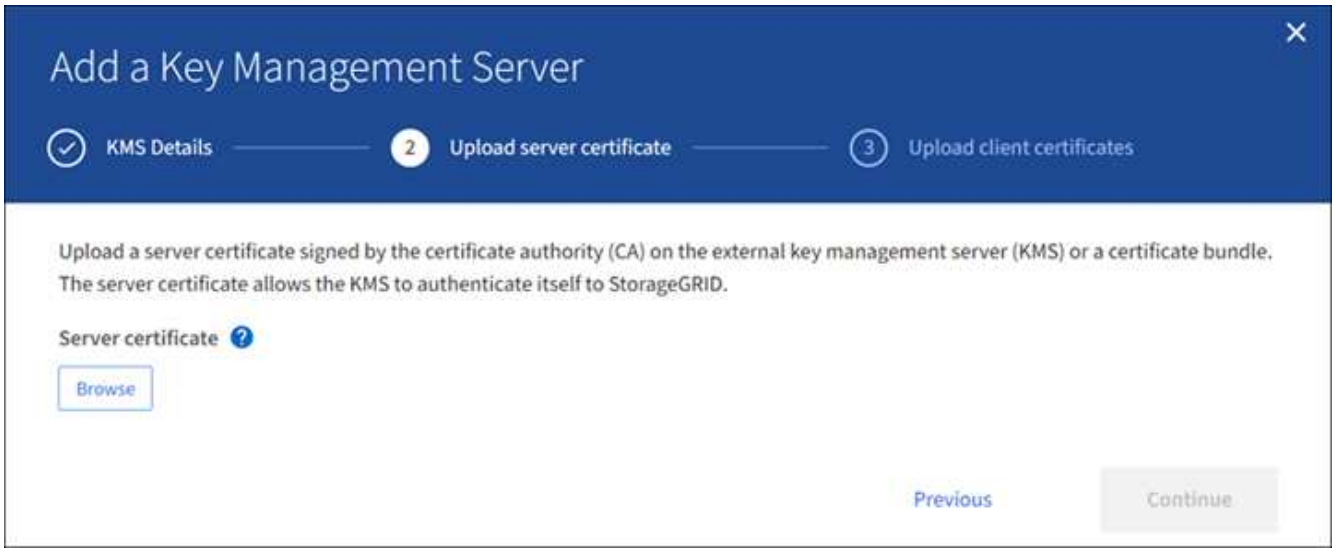
4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **continuar**.

Passo 2: Faça upload do 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.

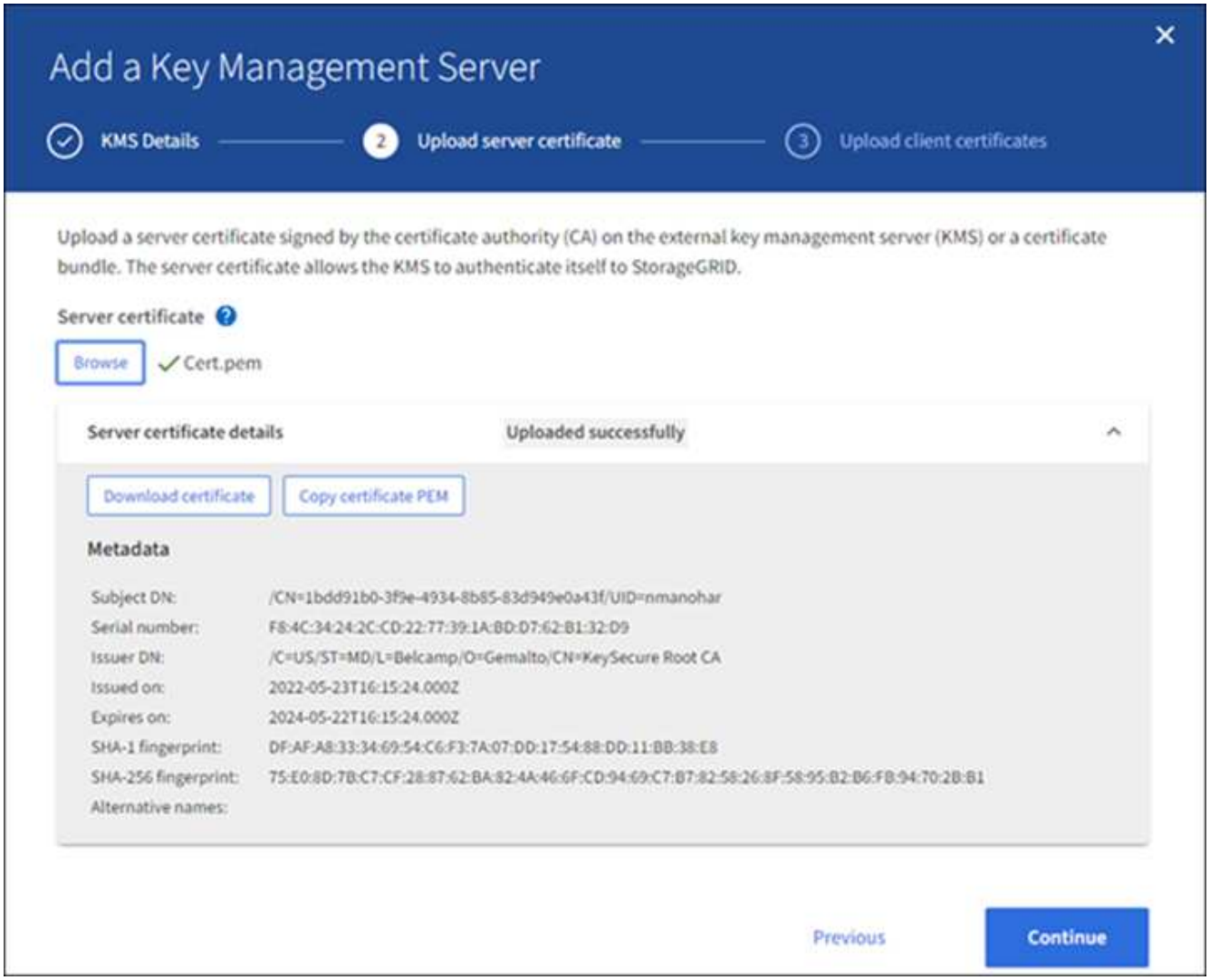
Passos

1. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.



2. Carregue o ficheiro de certificado.

   Os metadados do certificado do servidor são exibidos.



Se você carregou um pacote de certificados, os metadados de cada certificado serão exibidos em sua própria guia.

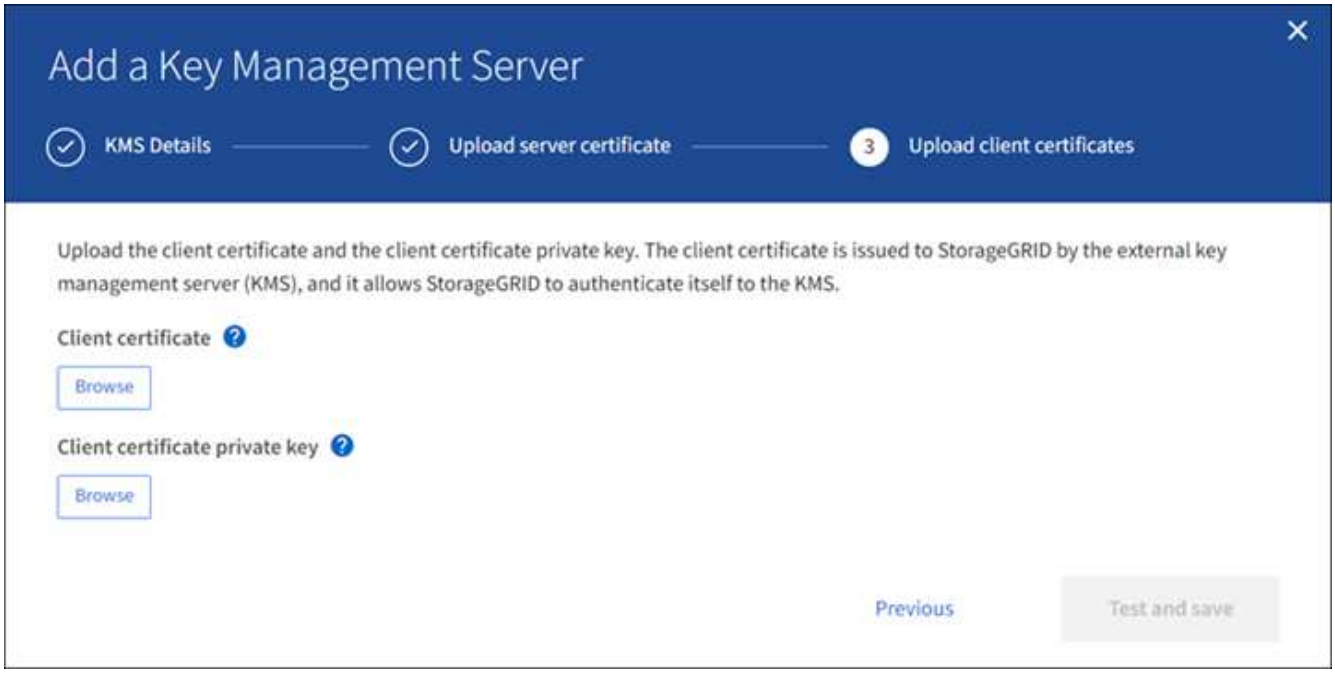
3. Selecione **continuar**.

Passo 3: Faça upload de 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 de cliente permite que o StorageGRID se autentique no KMS.

Passos

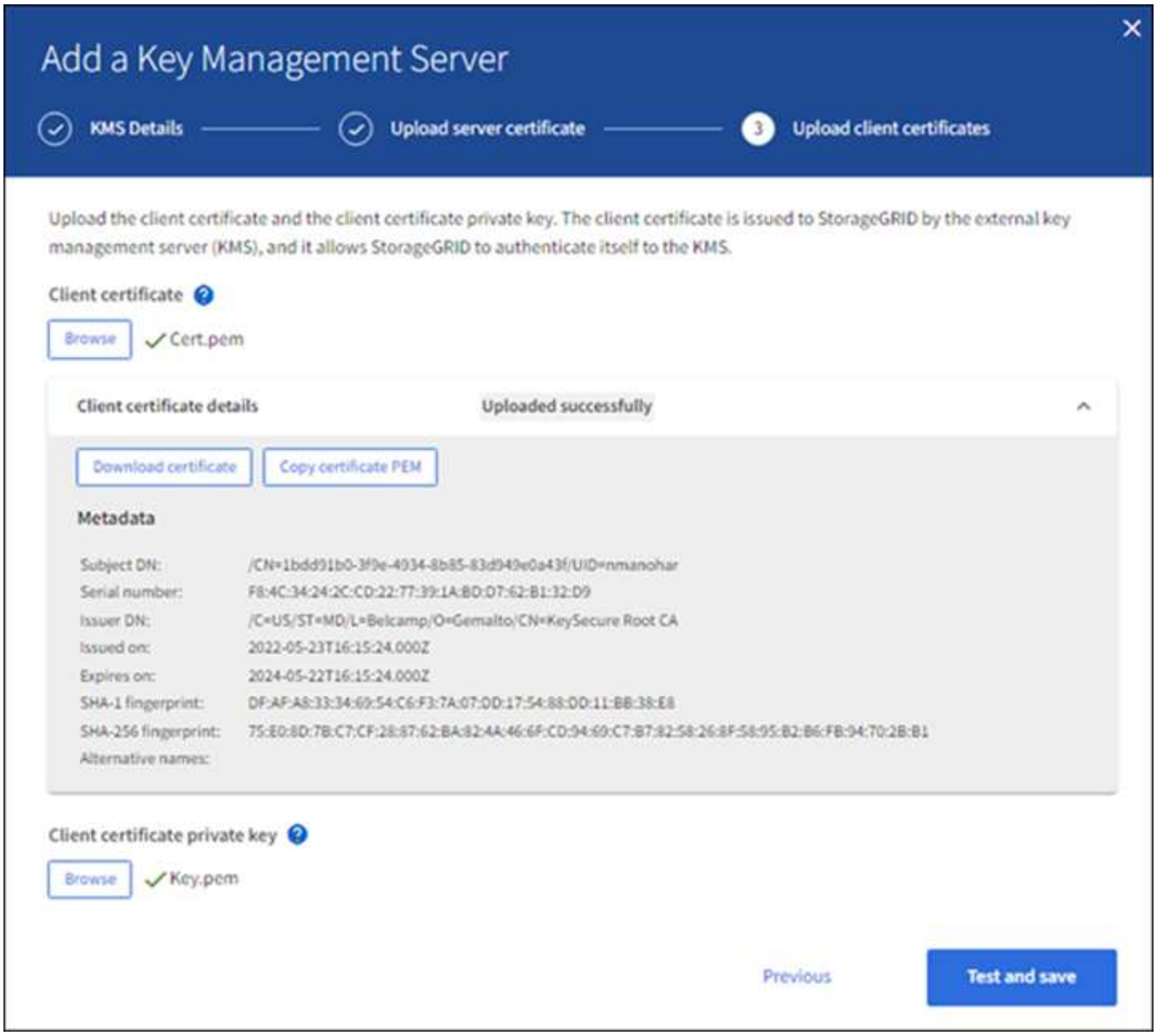
1. A partir de **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.



2. Carregue o ficheiro de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Carregue o ficheiro de chave privada.



5. Selecione **testar e salvar**.

   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 Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status atual.

6. Se uma mensagem de erro for exibida quando você selecionar **Test and save**, revise os detalhes da mensagem e selecione **OK**.

   Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão falhar.

7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **Force save**.

Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

   A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Ver detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo o status atual do servidor e dos certificados de cliente.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves configurados.

2. Reveja as informações na tabela para cada KMS.

Campo	Descrição
KMS nome	O nome descritivo do KMS.
Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
Gere as 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 anfitrião	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 são listados juntamente 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 exibir todos os nomes de host em um cluster, abra um KMS e selecione **Editar** ou **ações** > **Editar**.

Campo	Descrição
Expiração do certificado	Estado atual do certificado do servidor, do certificado da CA opcional e do certificado do cliente: Válido, expirado, próximo da expiração ou desconhecido. **Nota:** pode demorar StorageGRID até 30 minutos para obter atualizações para a expiração do certificado. Você deve atualizar o navegador da Web para ver os valores atuais.

3. Se a expiração do certificado for desconhecida, aguarde até 30 minutos e, em seguida, atualize o navegador da Web.

> Imediatamente após adicionar um KMS, a expiração do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status real.

4. Se a coluna expiração do certificado indicar que um certificado expirou ou está prestes a expirar, solucione o problema o mais rápido possível.

   Quando os alertas **expiração do certificado KMS CA**, **expiração do certificado do cliente KMS** e **expiração do certificado do servidor KMS** forem acionados, anote a descrição de cada alerta e execute as ações recomendadas.

> Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

5. Para exibir os detalhes do certificado para este KMS, selecione o nome do KMS na tabela.
6. Na página de resumo do KMS, revise os metadados e o PEM de certificado para o certificado do servidor e o certificado do cliente. Conforme necessário, selecione **Editar certificado** para substituir um certificado por um novo.

Exibir nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Na parte superior da página, selecione a guia **nós criptografados**.

   A guia nós criptografados lista os nós do dispositivo no sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

3. Revise as informações na tabela para cada nó de dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
KMS nome	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, posicione o cursor sobre a célula. Um traço (--) indica que a chave UID é desconhecida, possivelmente por causa de um problema de conexão entre o nó do aparelho e o KMS.
Estado	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conetado, o carimbo de data/hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações de configuração do KMS. **Observação:** você deve atualizar seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema KMS, solucione o problema imediatamente.

   Durante as operações normais de KMS, o status será **conectado ao KMS**. Se um nó for desconetado da grade, o estado de conexão do nó é mostrado (administrativamente para baixo ou desconhecido).

   Outras mensagens de status correspondem a alertas StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração DE KMS
   - Erro de conetividade DE KMS
   - Nome da chave de encriptação KMS não encontrado
   - Falha na rotação da chave de CRIPTOGRAFIA KMS
   - A chave KMS falhou ao desencriptar um volume de aparelho
   - 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 servidor de gerenciamento de chaves (KMS)

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Se pretende atualizar o site selecionado para um KMS, analisou o "Considerações para alterar o KMS para um site".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   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 em **Etapa 1 (detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. 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. Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. Em vez disso, gire a chave atualizando a versão da chave no software KMS. O StorageGRID requer que todas as versões de chave usadas anteriormente (bem como quaisquer versões futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados. "Considerações e requisitos para usar um servidor de gerenciamento de chaves"

Campo	Descrição
Gere as 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 para o KMS padrão, que se aplicará 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 será possível selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar 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 de cliente e a chave privada do certificado de 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 de dispositivos criptografados por nós nos locais afetados são testadas. Se todas as conexões de nó 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 for apresentada uma mensagem de erro, reveja os detalhes da mensagem e selecione **OK**.

    Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Force save**.

Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm 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. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação 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, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se você tiver desativado o site.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a 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 ativada.
- Você pode remover o KMS padrão se um KMS específico do site já existir para cada site que tenha nós de dispositivo com criptografia de nó ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   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 do site para um site que não tem nó de dispositivo com criptografia de nó ativada.
   - Você está removendo o KMS padrão, mas um KMS específico do site já existe para cada site com criptografia de nó.
4. Selecione **Sim**.

A configuração do KMS é removida.

Gerenciar configurações de proxy

Configure as configurações de proxy de armazenamento

Se você estiver usando serviços de plataforma ou pools de storage em nuvem, poderá configurar um proxy não transparente entre nós de storage e os pontos de extremidade 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.

Antes de começar

- Você tem permissões de acesso específicas.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

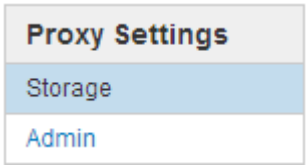
Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

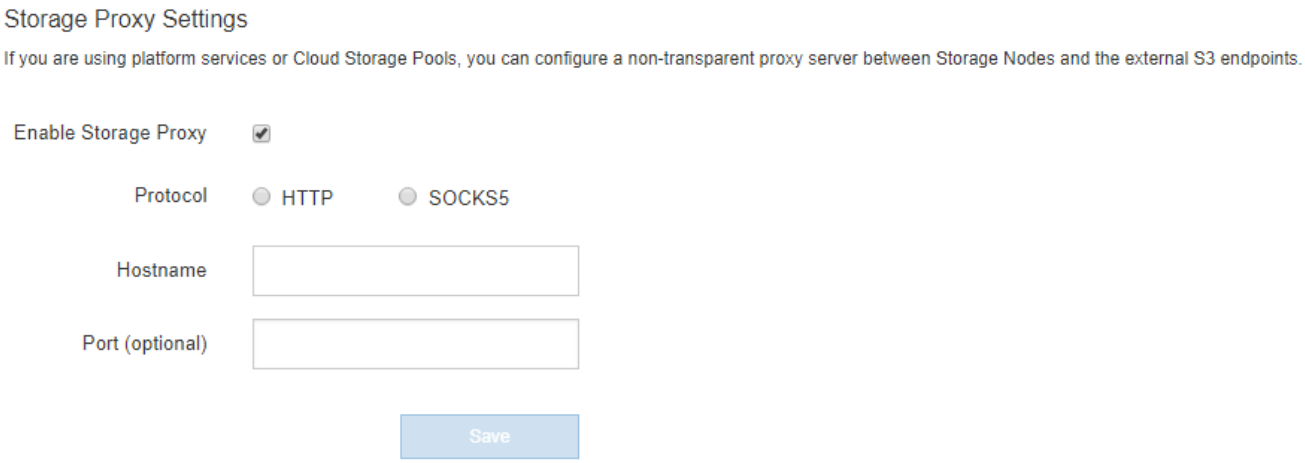
1. Selecione **CONFIGURATION** > **Security** > **Proxy settings**.

   A página Configurações do proxy de armazenamento é exibida. Por padrão, **Storage** está selecionado no menu da barra lateral.

2. Marque a caixa de seleção **Enable Storage Proxy** (Ativar proxy de armazenamento*).

   Os campos para configurar um proxy de armazenamento são exibidos.

3. Selecione o protocolo para o proxy de armazenamento não transparente.

4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para se conetar ao servidor proxy.

   Você pode deixar este campo em branco se usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Guardar**.

   Depois que o proxy Storage for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem podem ser configurados e testados.

   > As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma do StorageGRID não sejam bloqueadas.

Depois de terminar

Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção **Ativar proxy de armazenamento** e selecione **Salvar**.

Informações relacionadas

- "Rede e portas para serviços de plataforma"
- "Gerenciar objetos com ILM"

Configure as configurações do proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS ("Configurar o AutoSupport"consulte), poderá configurar um servidor proxy não transparente entre nós de administração e o suporte técnico (AutoSupport).

Antes de começar

- Você tem permissões de acesso específicas.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

Sobre esta tarefa

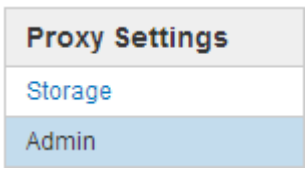
Você pode configurar as configurações para um único proxy Admin.

Passos

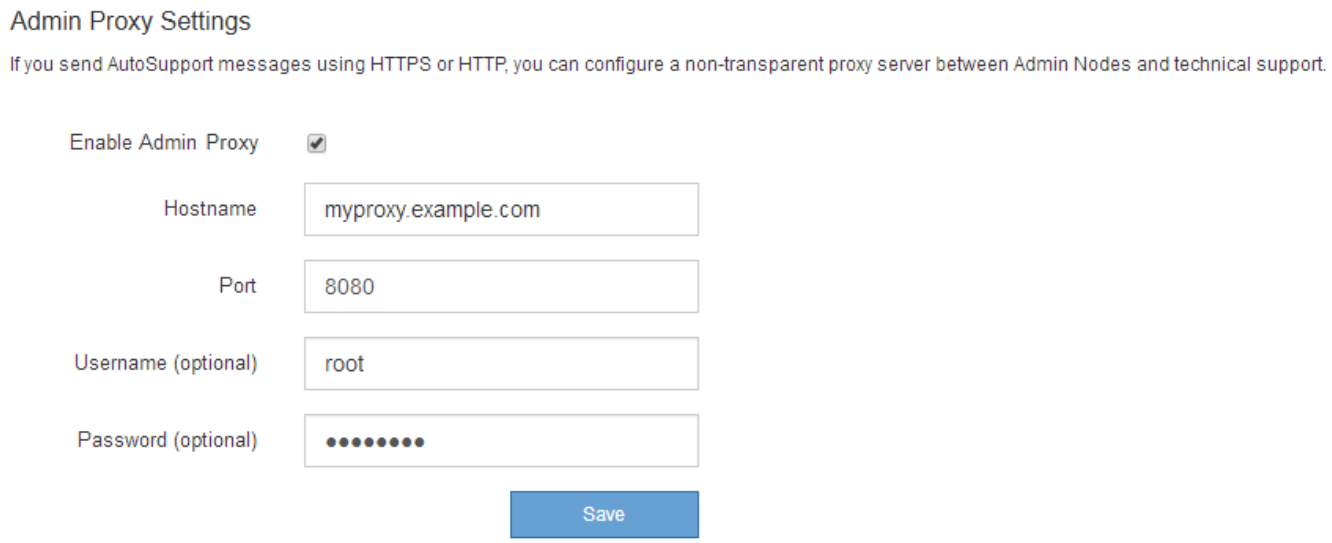
1. Selecione **CONFIGURATION** > **Security** > **Proxy settings**.

   É apresentada a página Admin Proxy Settings (Definições de proxy de administração). Por padrão, **Storage** está selecionado no menu da barra lateral.

2. No menu da barra lateral, selecione **Admin**.



3. Marque a caixa de seleção **Enable Admin Proxy** (Ativar proxy de administrador).



4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Introduza a porta utilizada para ligar ao servidor proxy.
6. Opcionalmente, insira o nome de usuário do proxy.

   Deixe este campo em branco se o servidor proxy não exigir um nome de usuário.

7. Opcionalmente, insira a senha do proxy.

   Deixe este campo em branco se o servidor proxy não exigir uma senha.

8. Selecione **Guardar**.

   Depois que o proxy Admin é salvo, o servidor proxy entre nós Admin e o suporte técnico é configurado.

   As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se você precisar desativar o proxy, desmarque a caixa de seleção **Ativar proxy Admin** e selecione **Salvar**.

Controle firewalls

Controle o acesso no 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 evitar que os locatários sejam capazes de se conetar ao Gerenciador de Grade no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se quiser configurar o firewall interno do StorageGRID, "Configurar firewall interno"consulte .

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade, a API de gerenciamento de grade, o Gerenciador de locatário e a API de gerenciamento do locatário. **Nota:** a porta 443 também é usada para algum tráfego interno.
8443	Porta restrita do Gerenciador de Grade em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS. • Os navegadores da Web e os clientes de API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário. • As solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Gerenciador de inquilinos em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS. • Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade. • As solicitações de conteúdo interno serão rejeitadas.

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

- "Faça login no Gerenciador de Grade"
- "Crie uma conta de locatário"
- "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 as necessárias para a implantação da 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 de que você precisa para sua grade.

- **Lista de endereços privilegiados**: Use esta guia para permitir o 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 abertas por padrão ou reabrir portas previamente fechadas.
- **Rede cliente não confiável**: Use esta guia para especificar se um nó confia no tráfego de entrada da rede cliente.

  Esta guia também fornece a opção de especificar portas adicionais que você deseja abrir quando a rede de cliente não confiável está configurada. Essas portas podem fornecer acesso ao Gerenciador de Grade, ao Gerenciador de Tenant ou a ambos.

  As configurações nesta guia substituem as configurações na guia Gerenciar acesso externo.

  - Um nó com uma rede cliente não confiável aceitará somente conexões em portas de endpoint do balanceador de carga configuradas nesse nó (pontos de extremidade globais, de interface de nó e de tipo de nó).
  - As portas adicionais abertas na guia rede de cliente não confiável estão abertas em todas as redes de clientes não confiáveis, mesmo que nenhum endpoints do balanceador de carga esteja configurado.
  - As portas de endpoint do balanceador de carga e as portas adicionais selecionadas *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
  - Quando confiável, todas as portas abertas na guia Gerenciar acesso externo são acessíveis, bem 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. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporta da maneira que você espera.

Para configurar controles internos de firewall, "Configurar controles de firewall"consulte .

Para obter mais informações sobre firewalls externos e segurança de rede, "Controle o acesso no firewall externo"consulte .

Lista de endereços privilegiados e Gerenciar guias de acesso externo

A guia lista de endereços privilegiados permite que você Registre um ou mais endereços IP que recebem acesso a portas de grade fechadas. A guia Gerenciar acesso externo permite fechar o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (as portas externas são portas que são acessíveis por nós que não são de grade por padrão). Essas duas guias geralmente podem ser usadas em conjunto para personalizar o acesso exato à rede que você precisa para permitir a sua grade.

> Os endereços IP privilegiados não têm acesso interno à porta de grade por padrão.

Exemplo 1: Use um host de salto para tarefas de manutenção

Suponha que você queira usar um host de salto (um host de segurança endurecido) 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. Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão 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 Admin Node em sua grade serão bloqueadas para todos os hosts, exceto o host jump. Em seguida, você pode usar o host jump para executar tarefas de manutenção em sua grade de forma mais segura.

Exemplo 2: Limite o acesso ao Gerenciador de Grade e ao Gerenciador do Locatário

Suponha que você queira limitar o acesso ao Gerenciador de Grade e ao gerente do locatário por motivos de segurança. Você pode usar estas etapas gerais:

1. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 443.
2. Use a opção na guia Gerenciar acesso externo para permitir o acesso à porta 8443.
3. Use a opção na guia Gerenciar acesso externo para permitir o acesso à porta 9443.

Depois de salvar sua configuração, os hosts não poderão acessar a porta 443, mas ainda poderão acessar o Gerenciador de Grade pela porta 8443 e o Gerenciador de Tenant pela porta 9443.

Exemplo 3: 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 as portas 443 e 8443. Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão 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 os hosts na lista de endereços privilegiados. Todos os outros hosts terão acesso negado ao serviço, independentemente da interface da solicitação.

Exemplo 4: Desativar o acesso a serviços não utilizados

Em um nível de rede, você pode desativar alguns serviços que você não pretende usar. Por exemplo, se você não fornecer acesso Swift, você executaria as seguintes etapas gerais:

1. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 18083.
2. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 18085.

Depois de salvar sua configuração, o nó de armazenamento não permite mais a conetividade Swift, mas continua a permitir o acesso a outros serviços em portas desbloqueadas.

Separador redes Cliente não fidedignas

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de clientes de entrada somente em pontos de extremidade configurados explicitamente ou portas adicionais que você selecionar nesta guia.

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todos "portas externas disponíveis".

Você pode reduzir a ameaça de ataques hostis em seu sistema StorageGRID especificando que a rede de clientes em cada nó seja *não confiável*. Se a rede de cliente de um nó não for confiável, o nó só aceita conexões de entrada em portas explicitamente configuradas como endpoints do balanceador de carga e quaisquer portas adicionais que você designar usando a guia rede de cliente não confiável na página de controle do Firewall. "Configurar pontos de extremidade do balanceador de carga"Consulte e "Configurar controles de firewall".

Exemplo 1: O Gateway Node 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 para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na "Pontos de extremidade do balanceador de carga" página, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página de controle do Firewall, selecione não confiável para especificar que a rede do cliente no nó de gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede de clientes do nó de Gateway será descartado, exceto para solicitações HTTPS S3 na porta 443 e ICMP echo (ping).

Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma

Suponha que você queira ativar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede do cliente. Você executaria este passo geral:

- Na guia redes de clientes não confiáveis da página de controle do Firewall, indique que a rede de cliente 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 a permitir solicitações de saída para destinos de serviços de plataforma configurados.

Exemplo 3: Limitando o acesso ao Gerenciador de Grade a uma sub-rede

Suponha que você queira permitir o acesso do Gerenciador de Grade somente em uma sub-rede específica. Você executaria os seguintes passos:

1. Anexe a rede cliente dos seus nós de administrador à sub-rede.

2. Use a guia rede de cliente não confiável para configurar a rede de cliente como não confiável.
3. Na seção **portas adicionais abertas na rede cliente não confiável** da guia, adicione a porta 443 ou 8443.
4. 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 os hosts na sub-rede especificada podem acessar o Gerenciador de Grade. Todos os outros hosts estão bloqueados.

Configurar firewall interno

Você pode configurar o firewall do StorageGRID para controlar o acesso à rede a portas específicas nos nós do StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou as informações em "Gerenciar controles de firewall" e "Diretrizes de rede".
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.

> Ao alterar a configuração da rede do cliente, as conexões de cliente existentes podem falhar se os endpoints 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 das portas nos nós da grade. Você pode usar as guias de controle do Firewall para abrir ou fechar portas abertas por padrão na rede de Grade, na rede Admin e na rede do Cliente. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas de grade fechadas. Se você estiver usando uma rede de cliente, poderá especificar se um nó confia no tráfego de entrada da rede de cliente e configurar o acesso de portas específicas na rede de cliente.

Limitar o número de portas abertas para endereços IP fora da sua grade a apenas aquelas que são absolutamente necessárias aumenta a segurança da sua grade. Você usa 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 como usar controles de firewall, incluindo exemplos, "Gerenciar controles de firewall"consulte .

Para obter mais informações sobre firewalls externos e segurança de rede, "Controle o acesso no firewall externo"consulte .

Aceder aos controlos da firewall

Passos

1. Selecione **CONFIGURATION** > **Security** > **Firewall control**.

   As três guias desta página são descritas em "Gerenciar controles de firewall".

2. Selecione qualquer separador para configurar os controlos da 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 fechadas por padrão ou fechadas por configurações na guia Gerenciar acesso externo.

Endereços IP privilegiados e sub-redes não têm acesso interno à grade por padrão. Além disso, os pontos de extremidade do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados são acessíveis mesmo que estejam bloqueados na guia Gerenciar acesso externo.

As configurações na guia lista de endereços privilegiados não podem substituir as configurações na guia rede cliente não confiável.

Passos

1. Na guia lista de endereços privilegiados, insira o endereço ou a sub-rede IP que deseja conceder acesso a 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 endereços IP privilegiados para acessar portas internas do StorageGRID**. "Portas internas do StorageGRID"Consulte .

   Esta opção remove algumas proteções para serviços internos. Deixe-o desativado, se possível.

4. Selecione **Guardar**.

Gerenciar o 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 grade, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas abertas por padrão e só pode abrir portas fechadas.

As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia rede 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 do cliente não confiável substituem as portas fechadas (como 443, 8443, 9443) na rede do cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não são da grade por padrão) para os nós da grade.
2. Configure as portas que deseja abrir e fechar usando as seguintes opções:

   - Utilize a 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 Gerenciador de Grade, qualquer usuário conetado atualmente em uma porta bloqueada, incluindo você, perderá o acesso ao Gerenciador de Grade, a menos que seu endereço IP tenha sido adicionado 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. Utilize o campo de pesquisa para encontrar as definições de qualquer porta externa introduzindo um número de porta. Pode introduzir um número de porta parcial. Por exemplo, se você inserir um **2**, todas as portas que têm a string "2" como parte de seu nome serão exibidas.

3. Selecione **Guardar**

Rede cliente não confiável

Se a rede do cliente para um nó não for confiável, o nó só aceita o tráfego de entrada em portas configuradas como endpoints do balanceador de carga e, opcionalmente, portas adicionais selecionadas nesta guia. Você também pode usar essa guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

> As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

As alterações de configuração feitas na guia **rede cliente não confiável** substituem as configurações na guia **Gerenciar acesso externo**.

Passos

1. Selecione **rede Cliente não fidedigna**.
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.
   - **Trusted** (padrão): Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável.

     Conforme necessário, você pode retornar a essa guia para alterar a configuração de um novo nó específico.

     > Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Use as opções a seguir para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente ou em portas selecionadas adicionais:
   - Selecione **não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista rede cliente não confiável.
   - Selecione **confiar em nós exibidos** para remover todos os nós exibidos na tabela da lista rede de clientes não confiável.

- Use a alternância ao lado de cada porta para definir a rede do cliente como confiável ou não confiável para o nó selecionado.

  Por exemplo, você pode selecionar **não confiar nos nós exibidos** para adicionar todos os nós à lista rede de clientes não confiável e, em seguida, usar a alternância além de um nó individual para adicionar esse nó único à lista rede de clientes confiáveis.

> Use a barra de rolagem no lado direito da tabela para ter certeza de que você visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó inserindo o nome do nó. Pode introduzir um nome parcial. Por exemplo, se você inserir um **GW**, todos os nós que têm a string "GW" como parte de seu nome serão exibidos.

4. Opcionalmente, selecione quaisquer portas adicionais que você deseja abrir na rede cliente não confiável. Essas portas podem fornecer acesso ao Gerenciador de Grade, ao Gerenciador de Tenant ou a ambos.

   Por exemplo, você pode querer usar essa opção para garantir que o Gerenciador de Grade possa ser acessado na rede do cliente para fins de manutenção.

> Essas portas adicionais estão abertas na rede do cliente, independentemente de estarem fechadas na guia Gerenciar acesso externo.

5. Selecione **Guardar**.

   As novas configurações de firewall são imediatamente aplicadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Gerenciar locatários

Gerenciar locatários: Visão geral

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 e Swift usam para armazenar e recuperar objetos.

> O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

O que são contas de inquilino?

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) ou a API REST Swift para armazenar e recuperar objetos em um sistema StorageGRID.

Cada conta de locatário tem grupos federados ou locais, usuários, buckets do S3 ou contentores Swift e objetos.

As contas de inquilino podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de inquilino podem ser usadas para qualquer um desses casos de uso:

- * Caso de uso corporativo:* se você estiver administrando um sistema StorageGRID em um aplicativo corporativo, talvez queira separar o armazenamento de objetos da grade pelos diferentes departamentos da sua organização. Nesse caso, você pode criar contas de inquilino 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 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 locatário. Consulte as instruções de implementação "Buckets e políticas de buckets do S3" para obter mais informações.

- * Caso de uso do provedor de serviços:* se você estiver administrando um sistema StorageGRID como provedor de serviços, você pode segregar o armazenamento de objetos da grade pelas diferentes entidades que alugarão o armazenamento em sua grade. Neste caso, você criaria contas de inquilino para a empresa A, empresa B, empresa C e assim por diante.

Para obter mais informações, "Use uma conta de locatário"consulte .

Como faço para criar uma conta de locatário?

Ao criar uma conta de locatário, você especifica as seguintes informações:

- Informações básicas, incluindo o nome do locatário, tipo de cliente (S3 ou Swift) e cota de armazenamento opcional.
- Permissões para a conta de locatário, como se a conta de locatário pode usar os serviços da plataforma S3, configurar sua própria origem de identidade, usar S3 Select ou usar uma conexão de federação de grade.
- O acesso raiz inicial para o locatário, com base se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, você pode ativar a configuração bloqueio de objeto S3 para o sistema StorageGRID se as contas de locatário do S3 precisarem cumprir os requisitos regulamentares. Quando o bloqueio de objeto S3 está ativado, todas as contas de locatário do S3 podem criar e gerenciar buckets compatíveis.

Para que é utilizado o Tenant Manager?

Depois de criar a conta de locatário, os usuários do locatário podem entrar no Gerenciador do locatário para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a origem de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clone de conta e replicação entre grade
- Gerenciar S3 chaves de acesso
- Crie e gerencie buckets do S3
- Use os serviços da plataforma S3
- Utilize S3 Select (Selecionar)
- Monitorar o uso do storage

> Embora os usuários de locatários do S3 possam criar e gerenciar chaves de acesso do S3 e buckets com o Gerenciador de locatários, eles precisam usar um aplicativo cliente do S3 para obter e gerenciar objetos. "USE A API REST DO S3"Consulte para obter detalhes.

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

Crie uma conta de locatário

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao storage no sistema StorageGRID.

As etapas para criar uma conta de locatário variam de acordo com "federação de identidade"a configuração e "logon único"se a conta do Gerenciador de Grade que você usa para criar a conta de locatário pertence a um grupo de administração com a permissão de acesso root.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root ou contas do locatário.
- Se a conta de locatário usar a origem de identidade configurada para o Gerenciador de Grade e você quiser conceder permissão de acesso raiz para a conta de locatário a um grupo federado, você importou esse grupo federado para o Gerenciador de Grade. Você não precisa atribuir nenhuma permissão do Gerenciador de Grade a esse grupo de administradores. "Gerenciar grupos de administradores"Consulte .
- Se você quiser permitir que um locatário do S3 clone dados de conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade:
  - Você "configurada a conexão de federação de grade"tem .
  - O estado da ligação é **ligado**.
  - Você tem permissão de acesso root.
  - Você revisou as considerações para "gerenciamento dos locatários permitidos para a federação da grade".
  - Se a conta de locatário usar a origem de identidade configurada para o Gerenciador de Grade, você importou o mesmo grupo federado para o Gerenciador de Grade em ambas as grades.

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

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

Acesse o assistente

Passos

1. Selecione **TENANTS**.
2. Selecione **criar**.

Introduza os detalhes

Passos

1. Insira os detalhes para o locatário.

Campo	Descrição
Nome	Um nome para a conta de locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta exclusivo de 20 dígitos.
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, essa descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado para a Grade 2: "Este locatário foi criado na Grade 1."
Tipo de cliente	O tipo de protocolo de cliente que este locatário usará, seja **S3** ou **Swift**. **Nota**: O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.
Cota de armazenamento (opcional)	Se você quiser que esse locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **continuar**.

Selecione permissões

Passos

1. Opcionalmente, selecione todas as permissões que você deseja que esse 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 de plataforma S3, como o CloudMirror. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
Use a própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos federados e usuários. Esta opção é desativada se tiver "SSO configurado" para o seu sistema StorageGRID.

Permissão	Se selecionado…
Permitir S3 Selecione	O locatário pode emitir S3 solicitações de API SelectObjectContent para filtrar e recuperar dados de objeto. "Gerenciar S3 Selecione para contas de inquilino"Consulte . **Importante**: As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.
Use a conexão de federação de grade	O locatário pode usar uma conexão de federação de grade. Selecionar esta opção: • Faz com que esse locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados dessa grade (a *grade de origem*) para a outra grade na conexão selecionada (a *grade de destino*). • Permite que esse locatário configure a replicação entre grade entre intervalos correspondentes em cada grade. "Gerenciar os locatários permitidos para a federação de grade"Consulte . **Observação**: Você só pode selecionar **usar conexão de federação de grade** quando estiver criando um novo locatário do S3; você não pode selecionar essa permissão para um locatário existente.

2. Se você selecionou **usar conexão de federação de grade**, selecione uma das conexões de federação de grade disponíveis.

3. Selecione **continuar**.

Defina o acesso root e crie o locatário

Passos

1. Defina o acesso root para a conta de locatário, com base se o seu sistema StorageGRID usa federação de identidade, logon único (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.

Opção	Faça isso
Se a federação de identidade estiver ativada	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 raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

2. Selecione **criar inquilino**.

   Uma mensagem de sucesso é exibida e o novo locatário é listado na página de locatários. Para saber como exibir detalhes do locatário e monitorar a atividade do locatário, "Monitorar a atividade do locatário"consulte .

3. Se você selecionou a permissão **usar conexão de federação de grade** para o locatário:
   a. Confirme se um locatário idêntico foi replicado para a outra grade na conexão. Os locatários em ambas as grades terão o mesmo ID de conta, nome, descrição, cota e permissões de 20 dígitos.

      Se você vir a mensagem de erro ""Tenant created without a clone"", consulte as instruções no "Solucionar erros de federação de grade".

   b. Se você forneceu uma senha de usuário raiz local ao definir o acesso root, "altere a senha do usuário raiz local" para o locatário replicado.

      Um usuário raiz local não pode entrar no Gerenciador do locatário na grade de destino até que a senha seja alterada.

Iniciar sessão no locatário (opcional)

Conforme necessário, você pode fazer login no novo locatário agora para concluir a configuração ou entrar no locatário mais tarde. As etapas de login dependem se você está conetado ao Gerenciador de Grade usando a porta padrão (443) ou uma porta restrita. "Controle o acesso no firewall externo"Consulte .

Inicie sessão agora

Se você estiver usando…	Faça isso…
Porta 443 e você define uma senha para o usuário raiz local	1. Selecione **entrar como root**. Quando você faz login, os links são exibidos para configurar buckets, federação de identidade, grupos e usuários. 2. Selecione os links para configurar a conta de locatário. Cada link abre a página correspondente no Gerenciador do Locatário. Para concluir a página, consulte "instruções para o uso de contas de inquilino".

Se você estiver usando…	Faça isso…
Porta 443 e você não definiu uma senha para o usuário raiz local	Selecione **entrar** e insira as credenciais de um usuário no grupo federado de acesso raiz.
Uma porta restrita	1. Selecione **Finish** 2. Selecione **Restricted** na tabela Tenant para saber mais sobre como acessar essa conta de locatário. O URL do Gerenciador do Locatário 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 administrador ◦ *port* é a porta somente locatário ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário

Inicie sessão mais tarde

Se você estiver usando…	Faça um destes…
Porta 443	• No Gerenciador de Grade, selecione **TENANTS** e **Sign in** à direita do nome do locatário. • Insira o 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 administrador ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário
Uma porta restrita	• No Gerenciador de Grade, selecione **TENANTS** e **restricted**. • Insira o 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 administrador ◦ *port* é a porta restrita somente para locatário ◦ *20-digit-account-id* É o ID exclusivo da conta do locatário

Configure o locatário

Siga as instruções em "Use uma conta de locatário" para gerenciar grupos de locatários e usuários, chaves de acesso do S3, buckets, serviços de plataforma e replicação entre grades e clone de contas.

Editar conta de locatário

Você pode editar uma conta de locatário para alterar o nome de exibição, a cota de armazenamento ou as permissões de locatário.

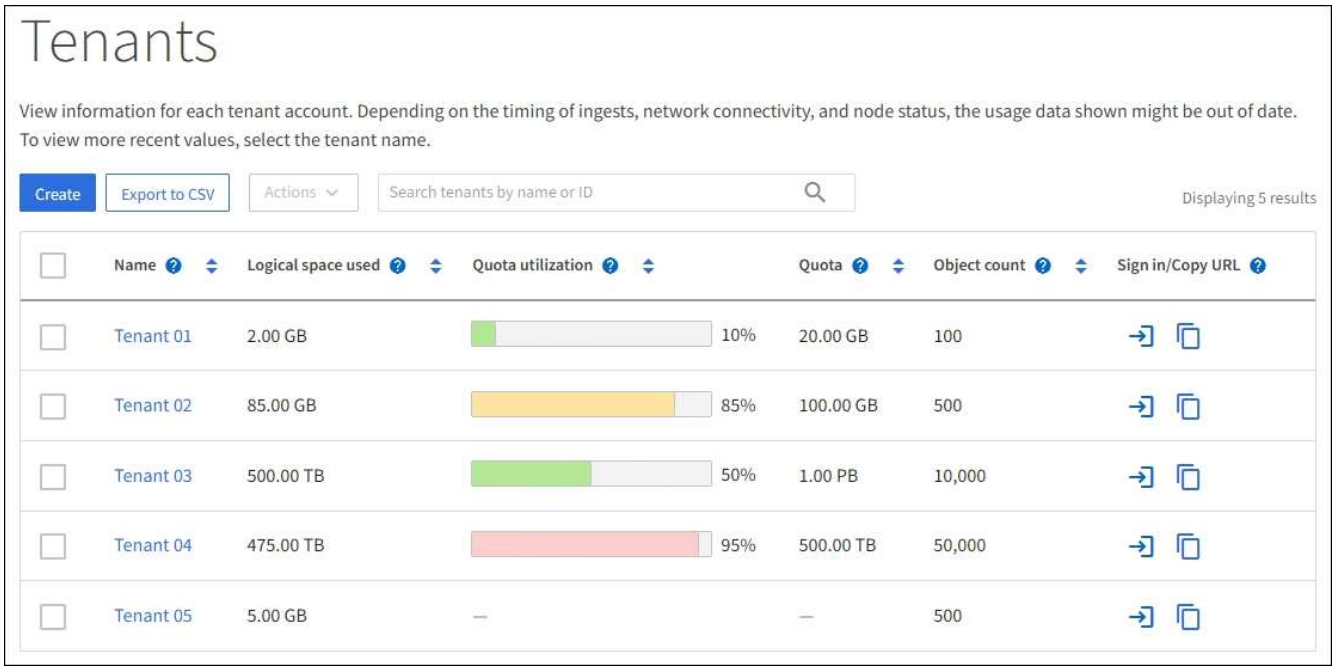
Se um locatário tiver a permissão **usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. No entanto, quaisquer alterações feitas em uma grade na conexão não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário exatamente em sincronia entre grades, faça as mesmas edições em ambas as grades. "Gerenciar os locatários permitidos para conexão de federação de grade"Consulte .

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root ou contas do locatário.

Passos

1. Selecione **TENANTS**.



2. Localize a conta de locatário que você deseja editar.

   Use a caixa de pesquisa para procurar um locatário por nome ou ID de locatário.

3. Selecione o locatário. Você pode fazer um dos seguintes procedimentos:
   - Marque a caixa de seleção para o locatário e selecione **ações** > **Editar**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **Editar**.

4. Opcionalmente, altere os valores para estes campos:
   - **Nome**
   - **Descrição**
   - **Cota de armazenamento**
5. Selecione **continuar**.
6. Selecione ou desmarque as permissões para a conta de locatário.
   - Se você desabilitar **Serviços de plataforma** para um locatário que já os esteja usando, os serviços que eles configuraram para seus buckets do 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 do S3, ele ainda poderá armazenar objetos no bucket, mas as cópias desses objetos não serão mais feitas no bucket externo do S3 configurado como um endpoint. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
   - Altere a configuração de **usa a própria fonte de identidade** para determinar se a conta do locatário usará sua própria fonte de identidade ou a fonte de identidade que foi configurada para o Gerenciador de Grade.

     Se **usa a própria fonte de identidade** for:

     - Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desativar sua origem de identidade antes de poder usar a fonte de identidade que foi configurada para o Gerenciador de Grade.
     - Desativado e não selecionado, SSO está ativado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Gerenciador de Grade.
   - Selecione ou desmarque a permissão **Allow S3 Select** conforme necessário. "Gerenciar S3 Selecione para contas de inquilino"Consulte .
   - Para remover a permissão **Use Grid Federation Connection**, siga as instruções para "removendo a permissão de um locatário para usar a federação de grade".

Altere a senha para o usuário raiz local do locatário

Talvez seja necessário alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado para fora da conta.

Antes de começar

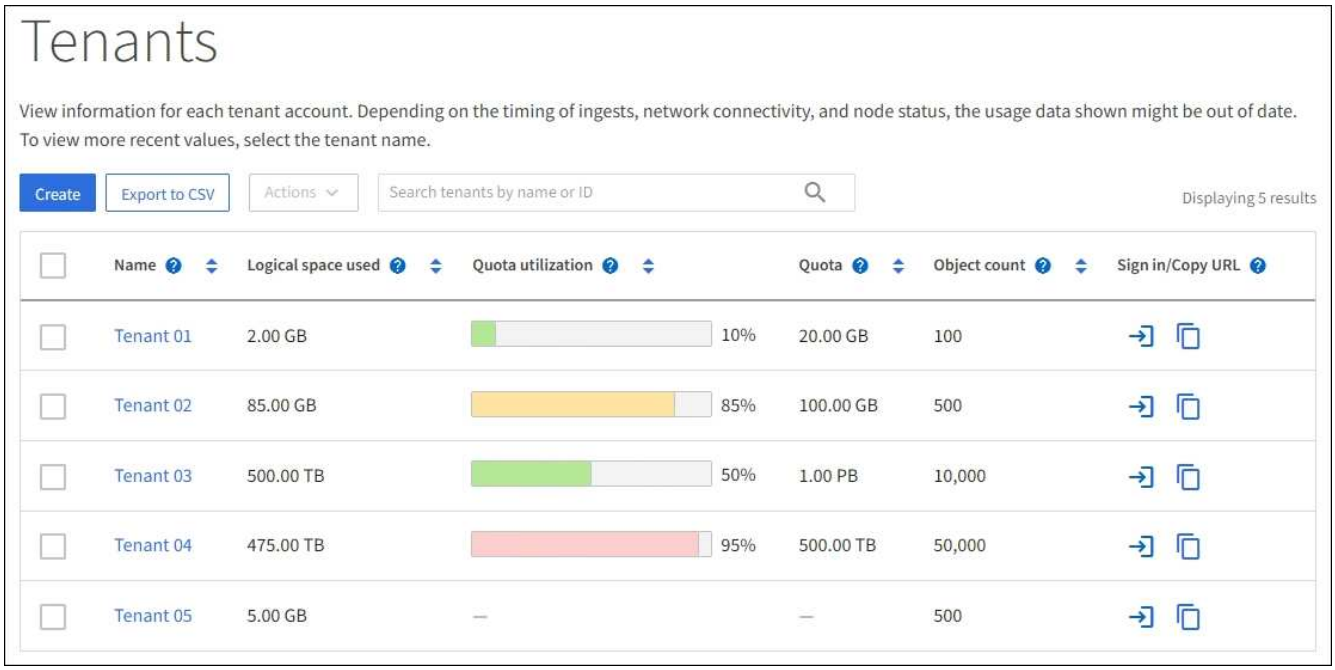
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, o usuário raiz local não poderá entrar na conta de locatário. Para executar tarefas de usuário raiz, os usuários devem pertencer a um grupo federado que tenha a permissão de acesso raiz para o locatário.

Passos

1. Selecione **TENANTS**.



2. Selecione a conta de locatário. Você pode fazer um dos seguintes procedimentos:
   - Marque a caixa de seleção para o locatário e selecione **ações** > **alterar senha de root**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **ações** > **alterar senha de root**.
3. Introduza a nova palavra-passe para a conta de locatário.
4. Selecione **Guardar**.

Eliminar 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Você removeu todos os buckets (S3), contentores (Swift) e objetos associados à conta de locatário.
- Se o locatário tiver permissão para usar uma conexão de federação de grade, você revisou as considerações para "Excluindo um locatário com a permissão usar conexão de federação de grade".

Passos

1. Selecione **TENANTS**.
2. Localize a conta de locatário ou contas que você deseja excluir.

   Use a caixa de pesquisa para procurar um locatário por nome ou ID de locatário.

3. Para excluir vários locatários, marque as caixas de seleção e selecione **ações** > **Excluir**.
4. Para excluir um único locatário, faça um dos seguintes procedimentos:
   - Marque a caixa de seleção e selecione **ações** > **Excluir**.

- Selecione o nome do locatário para exibir a página de detalhes e selecione **ações** > **Excluir**.

5. Selecione **Sim**.

Gerenciar serviços de plataforma

Gerenciar serviços de plataforma para locatários: Visão geral

Se você ativar os serviços de plataforma para contas de locatário do S3, configure sua grade para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

O que são serviços de plataforma?

Os serviços de plataforma incluem replicação do CloudMirror, notificações de eventos e o serviço de integração de pesquisa.

Esses serviços permitem que os locatários usem a seguinte funcionalidade com seus buckets do S3:

- **Replicação do CloudMirror**: O serviço de replicação do 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 aproveitar os serviços da AWS para realizar análises nos seus dados.

  > A replicação do CloudMirror tem algumas semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, "Compare a replicação entre redes e a replicação do CloudMirror"consulte .

  > A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.

- **Notificações**: As notificações de eventos por bucket são usadas para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (Amazon SNS) externo especificado.

  Por exemplo, você pode configurar alertas para 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 evento possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e 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 objeto S3 para um serviço Elasticsearch remoto. Você pode usar o Elasticsearch para realizar pesquisas entre buckets e realizar análises sofisticadas de padrões presentes nos metadados do objeto.

Embora a integração do Elasticsearch possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Com os serviços de plataforma, os locatários têm a capacidade de usar recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino para serviços de plataforma geralmente é externo à implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se o fizer, você deverá habilitar o uso de serviços de plataforma quando criar ou editar contas de locatário. Você também deve configurar sua rede de modo que as mensagens de serviços de plataforma que os locatários geram possam chegar aos destinos deles.

Recomendações para o uso de serviços de plataforma

Antes de usar os serviços da plataforma, esteja ciente das seguintes recomendações:

- Se um bucket do S3 no sistema StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, você também deverá habilitar o controle de versão do bucket do S3 para o endpoint de destino. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.
- Você não deve usar mais de 100 locatários ativos com solicitações do S3 que exigem replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 inquilinos ativos ativos pode resultar em desempenho mais lento do cliente S3.
- As solicitações para um endpoint que não pode ser concluído serão enfileiradas para um máximo de 500.000 solicitações. Esse limite é compartilhado igualmente entre locatários ativos. Novos inquilinos podem exceder temporariamente este limite de 500.000 para que os inquilinos recém-criados não sejam injustamente penalizados.

Informações relacionadas

- "Use uma conta de locatário"
- "Configure as configurações de proxy de armazenamento"
- "Monitore o StorageGRID"

Rede e portas para serviços de plataforma

Se você permitir que um locatário do S3 use serviços de plataforma, você deve configurar a rede para a grade para garantir que as mensagens de serviços de plataforma possam ser entregues aos seus destinos.

Você pode ativar os serviços de plataforma para uma conta de locatário do S3 ao criar ou atualizar a conta de locatário. Se os serviços de plataforma estiverem ativados, o locatário poderá criar endpoints que servem como destino para replicação do CloudMirror, notificações de eventos ou mensagens de integração de pesquisa a partir de seus buckets do S3. Essas mensagens de serviços de plataforma são enviadas de nós de storage que executam o serviço ADC para os endpoints de destino.

Por exemplo, os locatários podem configurar os seguintes tipos de endpoints de destino:

- Um cluster Elasticsearch hospedado localmente
- Um aplicativo local compatível com o recebimento de mensagens do Simple Notification Service (Amazon SNS)
- Um bucket do S3 hospedado localmente na mesma ou em outra instância do StorageGRID

- Um endpoint externo, como um endpoint no Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a rede ou as redes que contêm os nós de armazenamento ADC. Você deve garantir que as portas a seguir possam ser usadas para enviar mensagens de serviços de plataforma para os endpoints de destino.

Por padrão, as mensagens dos serviços da plataforma são enviadas nas seguintes portas:

- **80**: Para URIs de endpoint que começam com http
- **443**: Para URIs de endpoint que começam com https

Os locatários podem especificar uma porta diferente quando criam ou editam um endpoint.

> Se uma implantação do StorageGRID for usada como destino para a replicação do CloudMirror, as mensagens de replicação podem ser recebidas em uma porta diferente de 80 ou 443. Verifique se a porta que está sendo usada para S3 pela implantação do StorageGRID de destino está especificada no endpoint.

Se você usar um servidor proxy não transparente, também deverá "Configure as configurações de proxy de armazenamento"permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

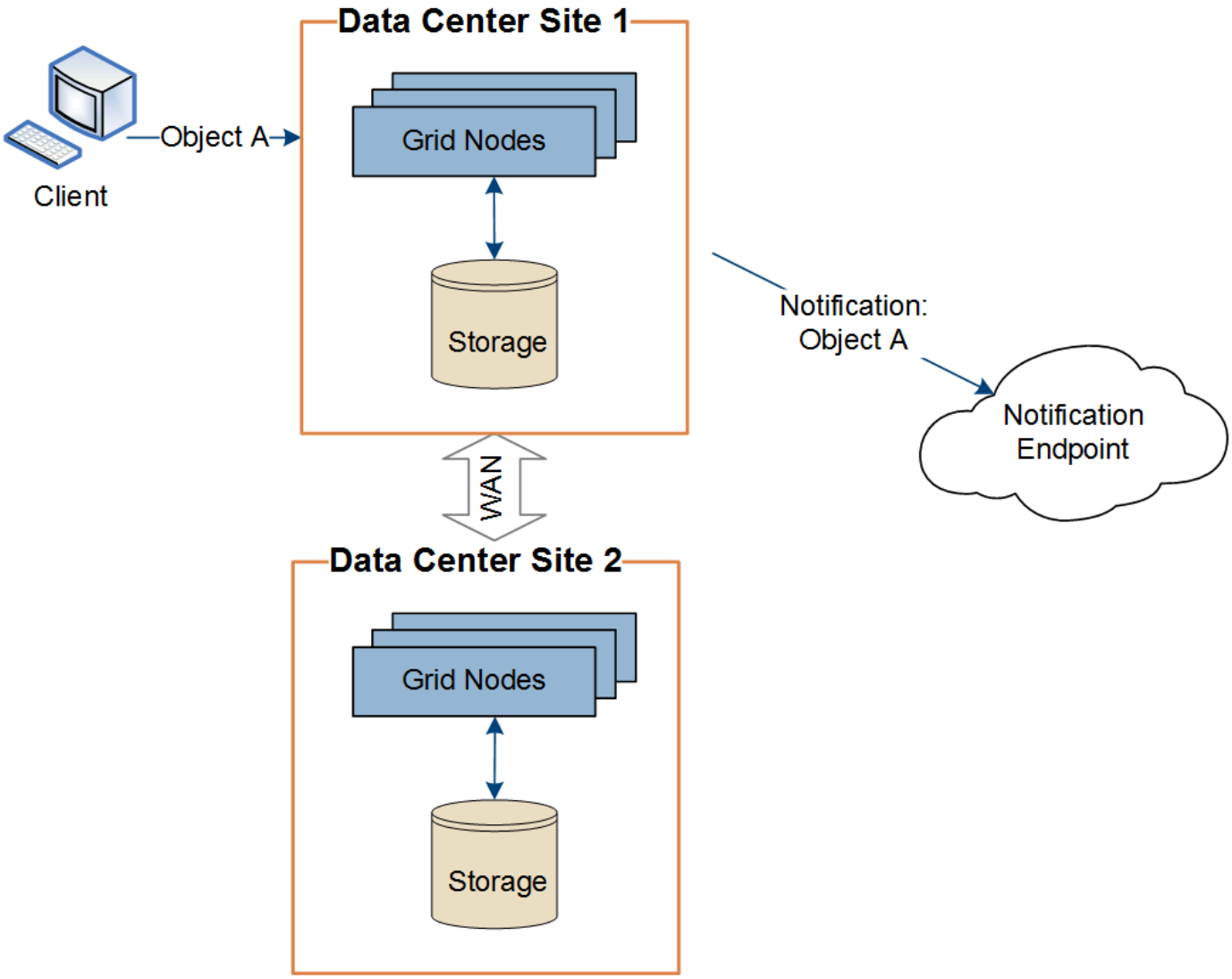
Informações relacionadas

- "Use uma conta de locatário"

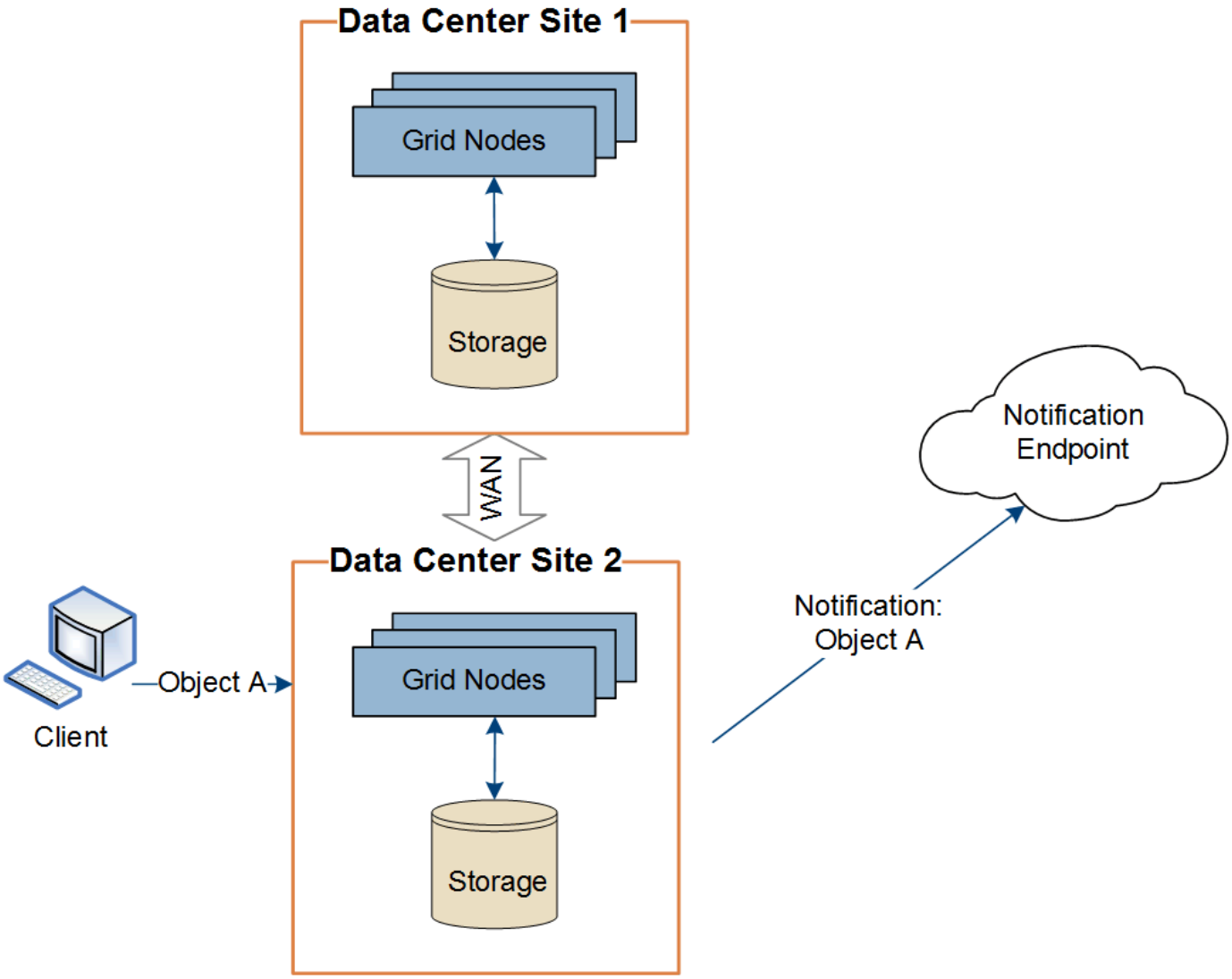
Entrega por local de mensagens de serviços de plataforma

Todas as operações de serviços de plataforma são realizadas por local.

Ou seja, se um locatário usar um cliente para executar uma operação de criação de API S3 em um objeto conetando-se a um nó de gateway no Data Center Site 1, a notificação sobre essa ação será acionada e enviada a partir do Data Center Site 1.



Se o cliente executar posteriormente uma operação de exclusão de API S3 nesse mesmo objeto do Data Center Site 2, a notificação sobre a ação de exclusão será acionada e enviada do Data Center Site 2.



Certifique-se de que a rede em cada local está configurada de forma a que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Solucionar problemas de serviços de plataforma

Os endpoints usados nos serviços de plataforma são criados e mantidos por usuários de inquilinos no Gerenciador de inquilinos; no entanto, se um locatário tiver problemas para configurar ou usar serviços de plataforma, talvez você possa 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 do locatário. Cada endpoint representa um destino externo para um serviço de plataforma, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do serviço de notificação simples ou um cluster do Elasticsearch hospedado localmente ou na AWS. Cada endpoint inclui a localização do recurso externo e as credenciais necessárias para acessar esse recurso.

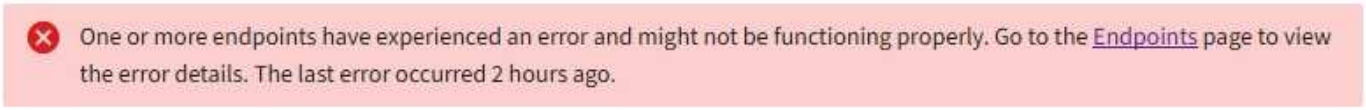
Quando um locatário cria um endpoint, o sistema StorageGRID valida que o endpoint existe e que ele pode ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.

Se a validação do endpoint falhar, uma mensagem de erro explica por que a validação do endpoint falhou. O usuário do locatário deve resolver o problema e tentar criar o endpoint novamente.

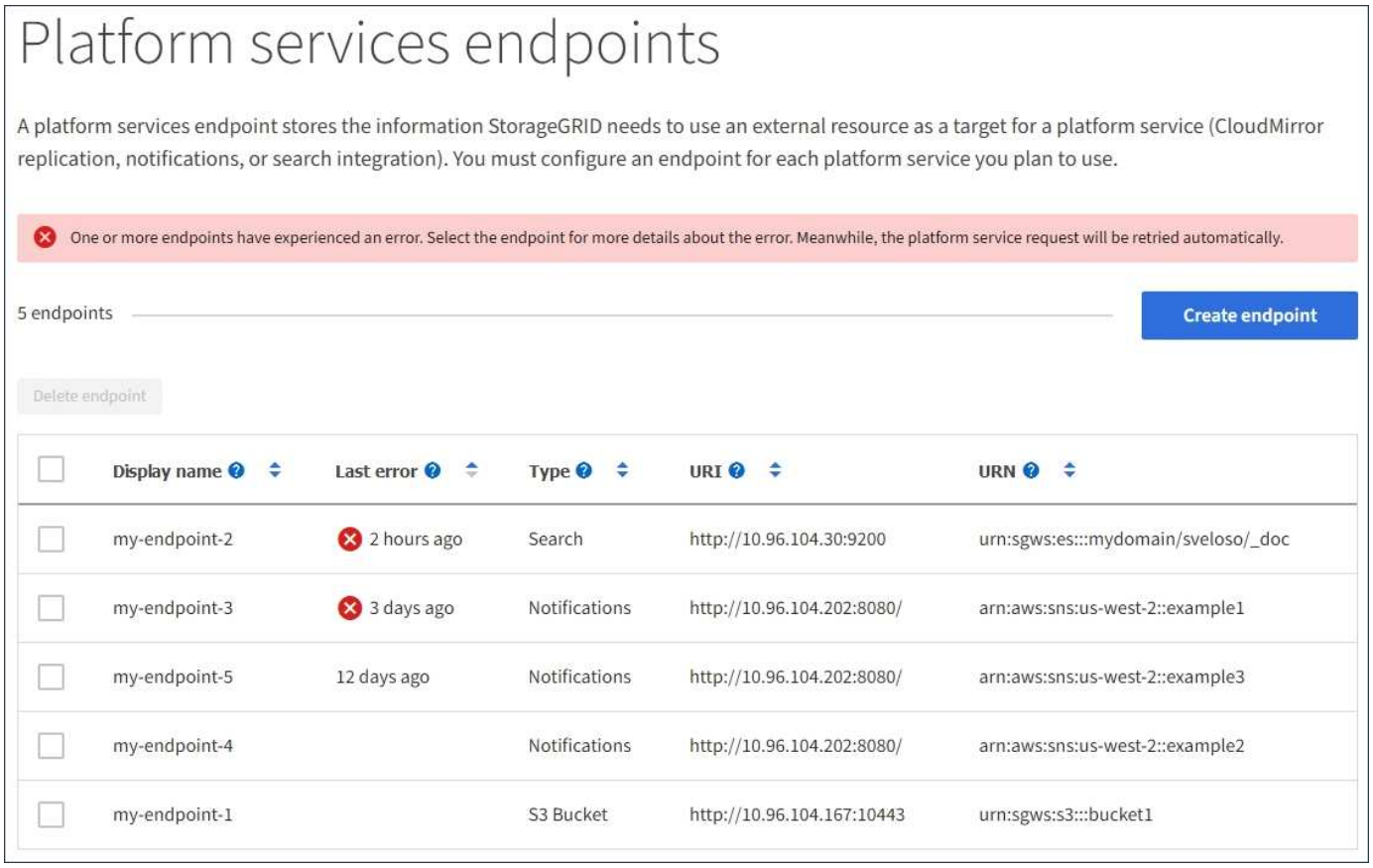
A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do locatário.

Problemas com endpoints existentes

Se ocorrer um erro quando o StorageGRID tenta alcançar um endpoint existente, uma mensagem é exibida no painel no Gerenciador de inquilinos.



Os usuários do locatário podem ir para a página Endpoints para revisar a mensagem de erro mais recente para cada endpoint e determinar quanto tempo atrás o erro ocorreu. A coluna **último erro** exibe a mensagem de erro mais recente para cada endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone ocorreram 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 aos servidores proxy

Se você tiver configurado um "Proxy de storage" entre nós de storage e endpoints de serviço da plataforma, poderão ocorrer erros se o serviço proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não sejam bloqueadas.

Determine se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o painel no Gerenciador de inquilinos exibirá uma mensagem de alerta. Pode aceder à página Endpoints para ver mais detalhes sobre o erro.

Falha nas operações do cliente

Alguns problemas de serviços de plataforma podem causar falha nas operações do cliente no bucket do 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 **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > ***Storage Node*** > **SSM** > **Serviços**.

Erros de endpoint recuperáveis e irrecuperáveis

Após a criação de endpoints, os erros de solicitação de serviço da plataforma podem ocorrer por vários motivos. Alguns erros são recuperáveis com a intervenção do usuário. Por exemplo, erros recuperáveis podem ocorrer pelos seguintes motivos:

- As credenciais do usuário foram excluídas ou expiraram.
- O intervalo de destino não existe.
- A notificação não pode ser entregue.

Se o StorageGRID encontrar um erro recuperável, a solicitação de serviço da plataforma será tentada novamente até que seja bem-sucedida.

Outros erros são irrecuperáveis. Por exemplo, um erro irrecuperável ocorre se o endpoint for excluído.

Se o StorageGRID encontrar um erro de endpoint irrecuperável, o alarme legado de Eventos totais (SMTT) é acionado no Gerenciador de Grade. Para visualizar o alarme legado Total de Eventos:

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > ***node*** > **SSM** > **Eventos**.
3. Veja o último evento na parte superior da tabela.

   As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

4. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
5. Selecione a guia **Configuração** para redefinir contagens de eventos.
6. Notificar o locatário dos objetos cujas mensagens de serviços da plataforma não foram entregues.
7. Instrua o locatário a reativar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto.

O locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

As mensagens dos serviços da plataforma não podem ser entregues

Se o destino encontrar um problema que o impeça de aceitar mensagens de serviços da plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem de serviços da plataforma não será entregue. Por exemplo, esse erro pode acontecer se as credenciais forem atualizadas no destino, de modo que o StorageGRID não possa mais se autenticar no serviço de destino.

Se as mensagens dos serviços da plataforma não puderem ser entregues devido a um erro irrecuperável, o alarme legado de Eventos totais (SMTT) será acionado no Grid Manager.

Desempenho mais lento para solicitações de serviço de plataforma

O software StorageGRID pode controlar as solicitações recebidas do S3 para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o endpoint de destino pode receber as solicitações. O estrangulamento só ocorre quando há um backlog de solicitações aguardando para serem enviadas para o endpoint de destino.

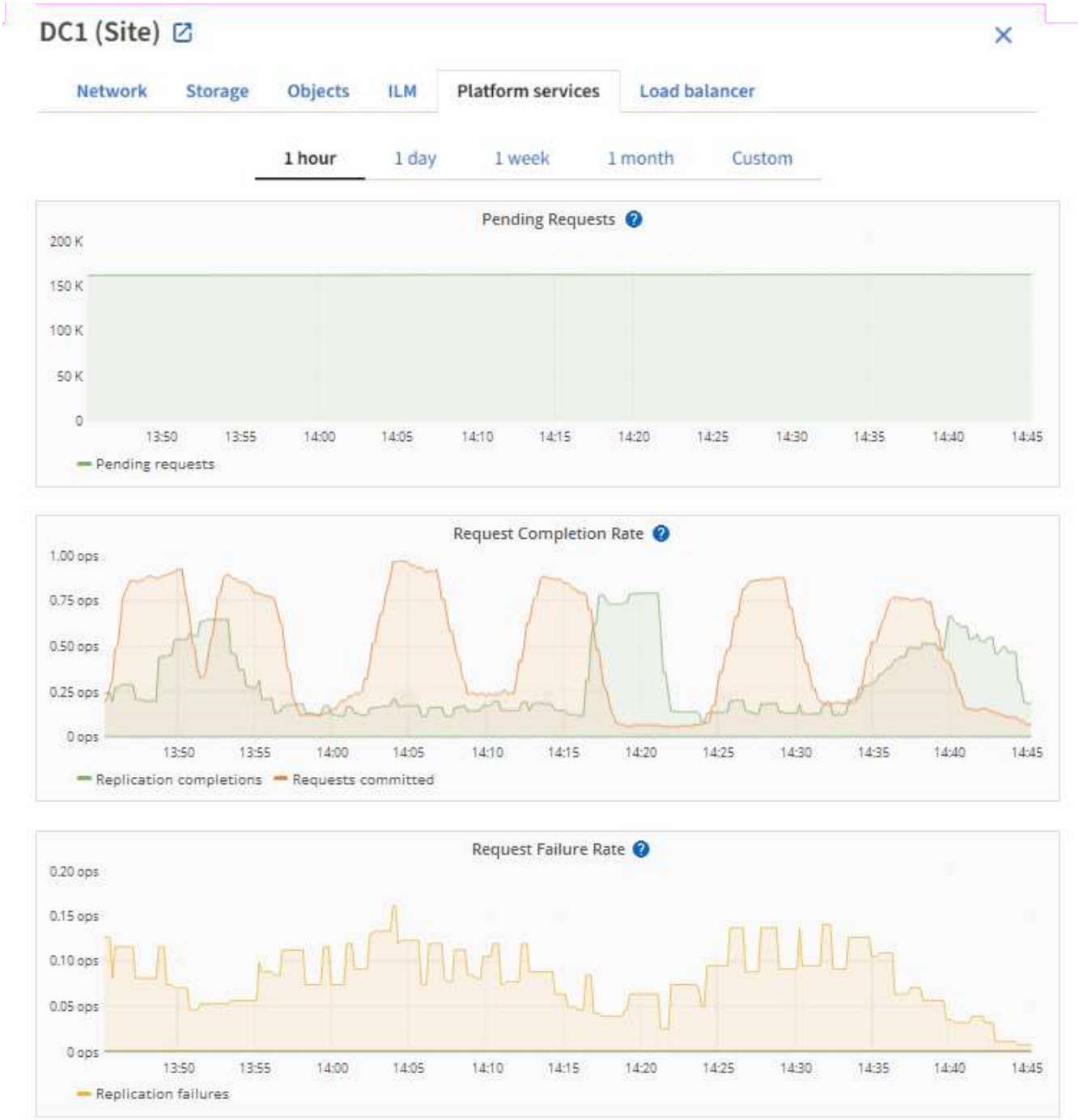
O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detetar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as operações do cliente S3 (como SOLICITAÇÕES PUT) acabarão falhando.

As solicitações do CloudMirror são mais propensas a serem afetadas pelo desempenho do endpoint de destino, pois essas solicitações geralmente envolvem mais transferência de dados do que solicitações de integração de pesquisa ou notificação de eventos.

As solicitações de serviço da plataforma falham

Para visualizar a taxa de falha da solicitação para serviços de plataforma:

1. Selecione **NODES**.
2. Selecione ***site*** > **Serviços de Plataforma**.
3. Veja o gráfico de taxa de erro de solicitação.



Alerta de serviços de plataforma indisponíveis

O alerta **Platform services unavailable** indica que nenhuma operação de serviço de plataforma pode ser executada em um local porque poucos nós de storage com o serviço RSM estão em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas para seus respetivos endpoints.

Para resolver esse alerta, determine quais nós de storage no local incluem o serviço RSM. (O serviço RSM está presente nos nós de storage que também incluem o serviço ADC.) Em seguida, certifique-se de que uma maioria simples desses nós de storage esteja em execução e disponível.

Se mais de um nó de storage que contém o serviço RSM falhar em um local, você perderá quaisquer solicitações de serviço de plataforma pendentes para esse site.

Orientação adicional para solução de problemas para endpoints de serviços de plataforma

Para obter informações adicionais, **Usar uma conta de locatário › solucionar problemas de endpoints de serviços de plataforma**consulte .

Informações relacionadas

- "Solucionar problemas do sistema StorageGRID"

Gerenciar S3 Selecione para contas de inquilino

Você pode permitir que certos locatários do S3 usem o S3 Select para emitir solicitações SelectObjectContent em objetos individuais.

S3 Select fornece uma maneira eficiente de pesquisar grandes quantidades de dados sem ter que implantar um banco de dados e recursos associados para habilitar pesquisas. Ele também reduz o custo e a latência da recuperação de dados.

O que é o S3 Select?

S3 Select permite que os clientes S3 usem as 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 grade

O administrador da grade deve conceder aos locatários S3 Select Ability. Selecione **permitir S3 Selecionar** quando "criando um locatário" ou "editando um locatário".

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 comprimido em arquivos GZIP ou bzip2.
- **Parquet**. Requisitos adicionais para objetos em Parquet:
  - S3 Select suporta apenas compactação colunar usando GZIP ou Snappy. S3 Select não suporta compactação de objetos inteiros para objetos Parquet.
  - S3 a seleção não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
  - O tamanho máximo do grupo de linhas não comprimidas é de 512 MB.
  - Você deve usar os tipos de dados especificados no esquema do objeto.
  - Você não pode usar os tipos lógicos INTERVALO, JSON, LISTA, HORA ou UUID.

Requisitos de endpoint

A solicitação SelectObjectContent deve ser enviada para um "Ponto de extremidade do balanceador de carga

StorageGRID".

Os nós Admin e Gateway usados pelo endpoint devem ser um dos seguintes:

- Um nó de dispositivo SG100 ou SG1000
- 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 nós de storage.

> As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.

Consulte "Instruções para utilizar o S3 Select".

Para visualizar "Gráficos de Grafana" as operações S3 Select ao longo do tempo, selecione **SUPPORT** > **Tools** > **Metrics** no Grid Manager.

Configurar conexões de cliente

Configurar conexões de cliente S3 e Swift: Visão geral

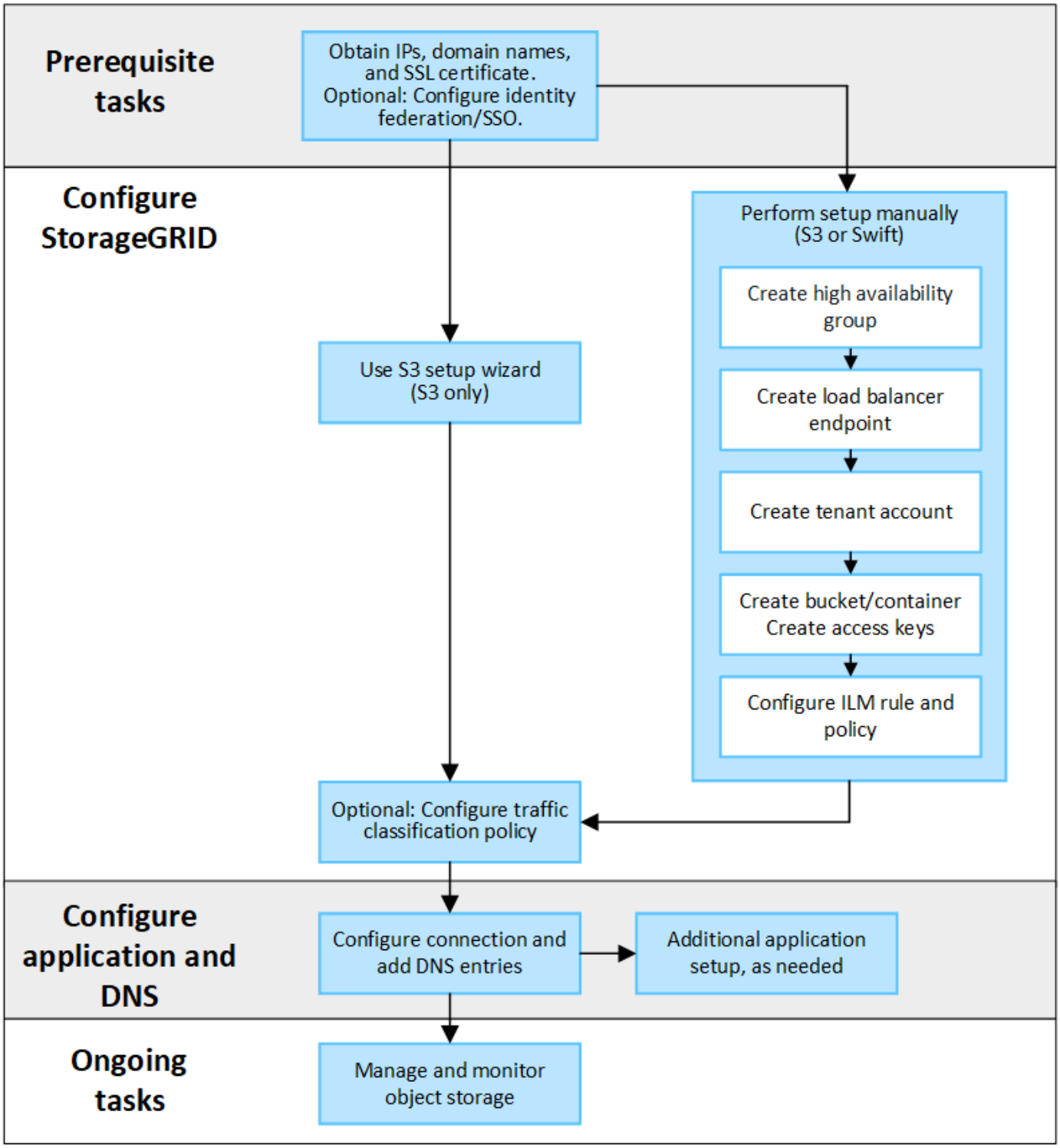
Como administrador de grade, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 e Swift se conetam ao seu sistema StorageGRID para armazenar e recuperar dados.

> O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Fluxo de trabalho de configuração

Como mostrado no diagrama de fluxo de trabalho, existem quatro etapas principais para conetar o StorageGRID a qualquer aplicativo S3 ou Swift:

1. Execute tarefas de pré-requisito no StorageGRID, com base na forma como o aplicativo cliente se conetará ao StorageGRID.
2. Use StorageGRID para obter os valores que o aplicativo precisa para se conetar à grade. Você pode usar o assistente de configuração do S3 ou configurar cada entidade do StorageGRID manualmente.
3. Use o aplicativo S3 ou Swift para concluir a conexão com o StorageGRID. Crie entradas DNS para associar endereços IP a qualquer nome de domínio que você pretende usar.
4. Executar tarefas contínuas na aplicação e no StorageGRID para gerenciar e monitorar o storage 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 ou Swift, você deve executar as 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 ou Swift e pelo servidor DNS.

Valor	Onde o valor está configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > grupo HA	Entrada DNS
Porta	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Certificado SSL	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Nome do servidor (FQDN)	StorageGRID > ponto final do balanceador de carga	• Aplicação cliente • Entrada DNS
S3 ID da chave de acesso e chave de acesso secreta	StorageGRID > locatário e balde	Aplicação cliente
Nome do balde/recipiente	StorageGRID > locatário e balde	Aplicação cliente

Como obtenho esses valores?

Dependendo de seus requisitos, você pode fazer um dos seguintes procedimentos para obter as informações de que precisa:

- **Use o "Assistente de configuração S3"**. O assistente de configuração do S3 ajuda 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 pelas 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 S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá uma 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 um nível de nuvem do FabricPool no ONTAP.

  > ⓘ Se você planeja usar o StorageGRID como o sistema de storage de objetos em uma categoria 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 exigirá personalização significativa.

- **Configurar itens manualmente**. Se você estiver se conetando a um aplicativo Swift (ou estiver se conetando a um aplicativo S3 e preferir não usar o assistente de configuração S3), você 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 ou Swift. "Configurar grupos de alta disponibilidade"Consulte .

  b. Crie o ponto de extremidade do balanceador de carga que o aplicativo S3 ou Swift usará. "Configurar pontos de extremidade do balanceador de carga"Consulte .

c. Crie a conta de locatário que o aplicativo S3 ou Swift usará. "Crie uma conta de locatário"Consulte .

d. Para um locatário do S3, faça login na conta do locatário e gere uma ID de chave de acesso e chave de acesso secreta para cada usuário que acessará o aplicativo. "Crie suas próprias chaves de acesso"Consulte .

e. Crie um ou mais buckets do S3 ou contentores Swift na conta do locatário. Para S3, "Crie um balde S3D."consulte . Para Swift, use o "COLOQUE o pedido do recipiente".

f. Para adicionar instruções de posicionamento específicas para os objetos pertencentes ao novo locatário ou bucket/container, crie uma nova regra ILM e ative uma nova política ILM para usar essa regra. "Criar regra ILM"Consulte e "Criar política ILM".

Utilize o assistente de configuração S3

Use o assistente de configuração S3: Considerações e requisitos

Você pode usar o assistente de configuração S3 para configurar o StorageGRID como o sistema de armazenamento de objetos para um aplicativo S3.

Quando utilizar o assistente de configuração S3

O assistente de configuração 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 você pode usar para inserir valores no aplicativo S3. Use o assistente para configurar o sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID.

Se você tiver a permissão de acesso root, poderá concluir o assistente de configuração do S3 quando começar a usar o Gerenciador de Grade do StorageGRID ou acessar e concluir o assistente posteriormente. Dependendo de seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para montar os valores que um aplicativo S3 precisa.

Antes de utilizar o assistente

Antes de utilizar o assistente, confirme que concluiu estes pré-requisitos.

Obtenha endereços IP e configure interfaces VLAN

Se você configurar um grupo de alta disponibilidade (HA), você sabe a quais nós o aplicativo S3 se conetará e a qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de sub-rede, endereço IP de gateway e endereços IP virtual (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, já configurou a interface VLAN. "Configurar interfaces VLAN"Consulte .

Configure a federação de identidade e o SSO

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, ativou esses recursos. Você também sabe qual grupo federado deve ter acesso root para a conta de locatário que o aplicativo S3 usará. "Use a federação de identidade"Consulte e "Configurar o logon único".

Obter e configurar nomes de domínio

Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para o StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA

criado usando o assistente.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, você deve ter "Configurados S3 nomes de domínio de endpoint"o . Recomenda-se o uso de solicitações virtuais de estilo hospedado.

Revise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga do StorageGRID, analisou as considerações gerais sobre o balanceamento de carga. Você tem os certificados que você vai carregar ou os valores que você precisa para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (de terceiros), terá o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Configure todas as conexões de federação de grade

Se você quiser permitir que o locatário do S3 clone dados de 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 "configurada a conexão de federação de grade"tem .
- O estado da ligação é **ligado**.
- Você tem permissão de acesso root.

Acesse e conclua o assistente de configuração do S3

Você pode usar o assistente de configuração 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.

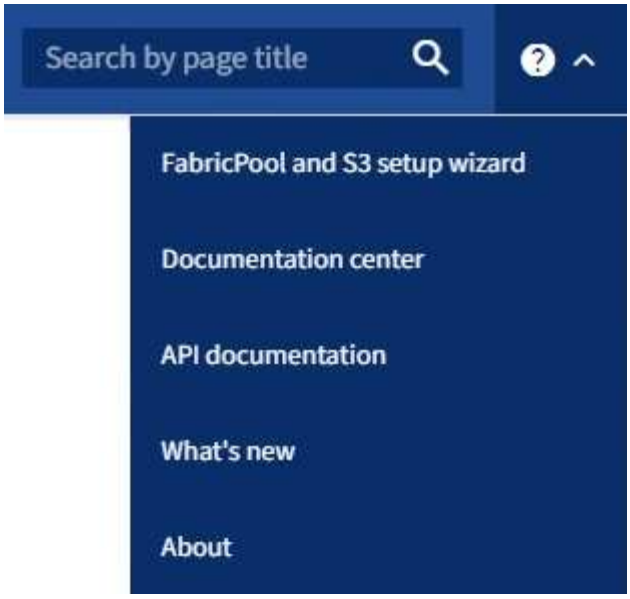
Antes de começar

- Você tem o "Permissão de acesso à raiz".
- Analisou "considerações e requisitos"o para utilizar o assistente.

Acesse o assistente

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Se o banner **FabricPool and S3 setup wizard** for exibido no painel, selecione o link no banner. Se o banner não for mais exibido, selecione o ícone de ajuda na barra de cabeçalho no Gerenciador de Grade e selecione **Assistente de configuração FabricPool e S3**.



3. Na seção S3 da aplicação da página do assistente de configuração FabricPool e S3, selecione **Configurar agora**.

Etapa 1 de 6: Configurar o grupo HA

Um grupo de HA é uma coleção de nós que contêm cada um o serviço StorageGRID Load Balancer. Um grupo de HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de HA para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo de 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, "Gerenciar grupos de alta disponibilidade"consulte .

Passos

1. Se você pretende usar um balanceador de carga externo, não precisa criar um grupo de HA. Selecione **Ignorar este passo** e vá para Etapa 2 de 6: Configurar o ponto final do balanceador de carga.
2. Para usar o balanceador de carga do 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 **Digite detalhes**, preencha os campos a seguir.

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 HA.

Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

d. Para a etapa **priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para esse grupo de HA.

Arraste linhas para alterar os valores na coluna **Priority Order**.

A primeira interface na lista é a interface principal. A interface principal 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 virtual (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 voltam para a interface de maior prioridade disponível.

e. Para a etapa **Inserir endereços IP**, preencha os campos a seguir.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR & n.o 8212; um endereço IPv4 seguido de 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 S3 endereços IP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Introduza pelo menos um e não mais de 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 **Create HA group** e, em seguida, selecione **Finish** para retornar ao assistente de configuração S3.

g. Selecione **continuar** para ir para a etapa do balanceador de carga.

Use o grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA no **Selecione um grupo HA**.

b. Selecione **continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o ponto final 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 em vários nós de storage.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administrador, ou pode se conetar a um balanceador de carga externo (de terceiros). Recomenda-se a utilização do balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, "Considerações para balanceamento de carga"consulte .

Para usar o serviço de balanceador de carga do StorageGRID, selecione a guia **balanceador de carga do StorageGRID** e, em seguida, crie ou selecione o ponto de extremidade do balanceador de carga que deseja usar. Para usar um balanceador de carga externo, selecione a guia **balanceador de carga externo** e forneça detalhes sobre o sistema que você já configurou.

Criar endpoint

Passos

1. Para criar um ponto de extremidade do balanceador de carga, selecione **Create endpoint**.
2. Para a etapa **Digite os detalhes do endpoint**, preencha os campos a seguir.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas serão reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

3. Para a etapa **Select Binding mode** (Selecionar modo de encadernação), especifique o modo de encadernação. O modo de encadernação controla a forma como o ponto de extremidade é acedido&n.o 8212;utilizando qualquer endereço IP ou utilizando endereços IP específicos e interfaces de rede.

Opção	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, 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 endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.

Opção	Descrição
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

4. Para a etapa de Acesso ao locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

5. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use essa 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. Consulte "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que introduzir.
Use o certificado StorageGRID S3 e Swift	Utilize esta opção apenas se já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID. "Configure os certificados API S3 e Swift"Consulte para obter detalhes.

6. Selecione **Finish** (concluir) para voltar ao assistente de configuração do S3.
7. Selecione **Continue** para ir para a etapa de locatário e bucket.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Use o ponto de extremidade do balanceador de carga existente

Passos

1. Para usar um endpoint existente, selecione seu nome no **Selecione um endpoint do balanceador de carga**.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Use balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os campos a seguir.

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 conetar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Passo 3 de 6: Crie 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. Você deve criar o locatário antes de criar o bucket que o aplicativo S3 usará para armazenar seus objetos.

Um bucket é um contentor usado para armazenar os objetos e metadados de objetos de um locatário. Embora alguns inquilinos possam ter muitos buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Você pode usar o Gerenciador do Locatário posteriormente para adicionar quaisquer buckets adicionais que você precisar.

Você pode criar um novo locatário para este aplicativo S3 usar. Opcionalmente, você também pode criar um bucket para o novo locatário. Finalmente, você pode permitir que o assistente crie as chaves de acesso S3 para o usuário raiz do locatário.

Para obter detalhes sobre esta tarefa, "Crie uma conta de locatário" consulte e "Crie um balde S3D.".

Passos

1. Selecione **criar inquilino**.
2. Para os passos Enter details (introduzir detalhes), introduza as seguintes informações.

Campo	Descrição
Nome	Um nome para a conta de locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.
Descrição (opcional)	Uma descrição para ajudar a identificar o inquilino.

Campo	Descrição
Tipo de cliente	O tipo de protocolo de cliente que este inquilino usará. Para o assistente de configuração S3, **S3** é selecionado e o campo está desativado.
Cota de armazenamento (opcional)	Se você quiser que esse locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

3. Selecione **continuar**.
4. Opcionalmente, selecione todas as permissões que você deseja que esse 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 de plataforma S3, como o CloudMirror. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
Use a própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos federados e usuários. Esta opção é desativada se tiver "SSO configurado" para o seu sistema StorageGRID.
Permitir S3 Selecione	O locatário pode emitir S3 solicitações de API SelectObjectContent para filtrar e recuperar dados de objeto. "Gerenciar S3 Selecione para contas de inquilino"Consulte . **Importante**: As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.
Use a conexão de federação de grade	O locatário pode usar uma conexão de federação de grade. Selecionar esta opção: • Faz com que esse locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados dessa grade (a *grade de origem*) para a outra grade na conexão selecionada (a *grade de destino*). • Permite que esse locatário configure a replicação entre grade entre intervalos correspondentes em cada grade. "Gerenciar os locatários permitidos para a federação de grade"Consulte . **Observação**: Você só pode selecionar **usar conexão de federação de grade** quando estiver criando um novo locatário do S3; você não pode selecionar essa permissão para um locatário existente.

5. Se você selecionou **usar conexão de federação de grade**, selecione uma das conexões de federação de grade disponíveis.

6. Defina o acesso root para a conta de locatário, com base se o sistema StorageGRID usa "federação de identidade", "Logon único (SSO)"ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade estiver ativada	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 raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

7. Se você quiser que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário raiz, selecione **Create root user S3 access key automatically**.

   Selecione esta opção se o único usuário para o locatário for o usuário raiz. Se outros usuários usarem esse locatário, use o Gerenciador do Locatário para configurar chaves e permissões.

8. Selecione **continuar**.
9. Para a etapa criar bucket, opcionalmente, crie um bucket para os objetos do locatário. Caso contrário, selecione **criar inquilino sem bucket** para ir para o passo de transferência de dados.

   Se o bloqueio de objeto S3 estiver ativado para a grade, o intervalo criado nesta etapa não terá o bloqueio de objeto S3 ativado. Se você precisar usar um bucket do S3 Object Lock para este aplicativo S3, selecione **criar locatário sem bucket**. Em seguida, use o Gerenciador do Locatário para"crie o balde".

   a. Introduza o nome do intervalo que a aplicação S3 irá utilizar. Por exemplo, `S3-bucket`.

      Não é possível alterar o nome do bucket depois de criar o bucket.

   b. Selecione a **região** para este intervalo.

      Use a região padrão (US-East-1) a menos que você espere usar o ILM no futuro para filtrar objetos com base na região do bucket.

   c. Selecione **Ativar controle de versão de objeto** se você quiser armazenar cada versão de cada objeto neste intervalo.

   d. Selecione **criar locatário e bucket** e vá para a etapa de download de dados.

passo 4 de 6: Transferir dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que você acabou de configurar.

Passos

1. Se você selecionou **Create root user S3 access key automatically**, siga um ou ambos os procedimentos a seguir:
   - Selecione **Transferir chaves de acesso** para transferir um `.csv` ficheiro que contenha 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 **Transferir valores de configuração** para transferir um `.txt` ficheiro que contenha as definições para o terminal do balanceador de carga, locatário, bucket e utilizador raiz.
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 de 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 **Continue** para ir para a regra ILM e a etapa de política.

Passo 5 de 6: Revise a regra ILM e a política ILM para 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 em seu sistema StorageGRID. A política de ILM incluída no StorageGRID faz duas cópias replicadas de todos os objetos. Esta política está em vigor até que você crie uma nova política proposta e ative-a.

Passos

1. Reveja 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. "Criar regra ILM"Consulte e "Criar política ILM: Visão geral".
3. Selecione **Reviewei estes passos e compreendi o que preciso fazer**.
4. Marque a caixa de seleção para indicar que você entende o que fazer a seguir.
5. Selecione **continuar** para ir para **Resumo**.

Passo 6 de 6: Rever resumo

Passos

1. Reveja o resumo.
2. Anote os detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de se conetar ao cliente S3. Por exemplo, selecionar **entrar como root** leva-o ao Gerenciador de inquilinos, onde você pode adicionar usuários de inquilinos, criar buckets adicionais e atualizar configurações de bucket.
3. Selecione **Finish**.
4. Configure o aplicativo usando o arquivo baixado do StorageGRID ou os valores obtidos manualmente.

Gerenciar grupos de HA

Gerenciar grupos de alta disponibilidade (HA): Visão geral

Você pode agrupar as interfaces de rede de vários nós de administrador 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.

O que é um grupo HA?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift ou para fornecer conexões altamente disponíveis para o Gerenciador de Grade e o Gerenciador de Tenant.

Cada grupo de 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 altamente disponíveis para clientes S3 e Swift.
- Os GRUPOS DE HA que incluem apenas os nós de Admin fornecem conexões altamente disponíveis ao Gerenciador de Grade e ao Gerente do locatário.
- Um grupo de HA que inclui apenas dispositivos SG100 ou SG1000 e nós de software baseados em VMware pode fornecer conexões altamente disponíveis para "S3 inquilinos que usam S3 Select"o . Os GRUPOS HA são recomendados ao usar S3 Select, mas não são necessários.

Como criar um grupo HA?

1. Você seleciona uma interface de rede para um ou mais nós de administrador ou nós de gateway. Você pode usar uma interface Grid Network (eth0), uma interface Client Network (eth2), uma interface VLAN ou uma interface de acesso que você adicionou ao nó.

   > ⓘ Não é possível adicionar uma interface a um grupo HA se ele tiver um endereço IP atribuído pelo DHCP.

2. Você especifica uma interface para ser a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.
3. Você determina a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conetar ao StorageGRID.

Para obter instruções, "Configurar grupos de alta disponibilidade"consulte .

O que é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface principal, que é a primeira interface na ordem de prioridade. Enquanto a interface principal permanecer disponível, ela é usada quando os clientes se conetam 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 inferior para o grupo HA funcionam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface principal (atualmente ativa) fique indisponível.

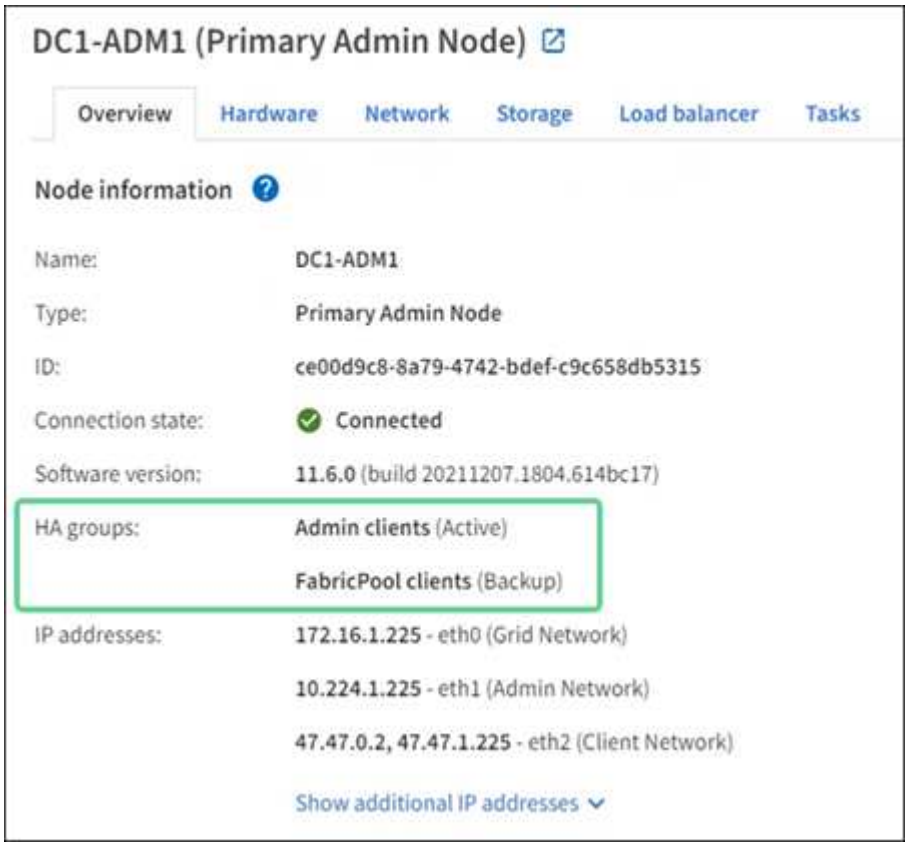
Exibir o status atual do grupo de HA de um nó

Para ver se um nó está atribuído a um grupo de HA e determinar seu status atual, selecione **NÓS** > ***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 sendo hospedado neste nó.
- **Backup**: O grupo HA não está usando esse nó no momento; essa é uma interface de backup.
- **Stopped**: 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 por causa de um ou mais dos seguintes:
  - O serviço do Load Balancer (nginx-gw) não está sendo executado 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 administradores 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 passam 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 é desativado.
- O nó no qual a interface está configurada perde a conetividade com todos os outros nós por pelo menos 2 minutos.
- A interface ativa desce.
- O serviço Load Balancer pára.
- O serviço de alta disponibilidade pára.

> 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 Gerenciador de Grade ou do Gerenciador de Locatário.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impactos e possam confiar em comportamentos normais de repetição para continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta torna-se disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta que está disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões altamente disponíveis ao StorageGRID para dados de objetos e para uso administrativo.

- Um grupo de HA pode fornecer conexões administrativas altamente disponíveis ao Gerenciador de Grade ou ao Gerente do Locatário.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3 e Swift.
- Um grupo de HA que contém apenas uma interface permite fornecer muitos endereços VIP e definir explicitamente endereços IPv6.

Um grupo de HA poderá fornecer alta disponibilidade somente se todos os nós incluídos no grupo oferecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços de que você precisa.

- **Admin Nodes**: Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Gateway Nodes**: Inclua o serviço Load Balancer.

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao Grid Manager	• Nó de administração principal (**primário**) • Nós de administração não primários **Nota:** o nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso apenas ao Gestor do Locatário	• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	• Nós de administração • Nós de gateway
Acesso de cliente S3 para "S3 Selecione"	• SG100 ou SG1000 aparelhos • Nós de software baseados em VMware **Nota**: Os GRUPOS HA são recomendados ao usar o S3 Select, mas não são necessários.

Limitações do uso de grupos de HA com Grid Manager ou Tenant Manager

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

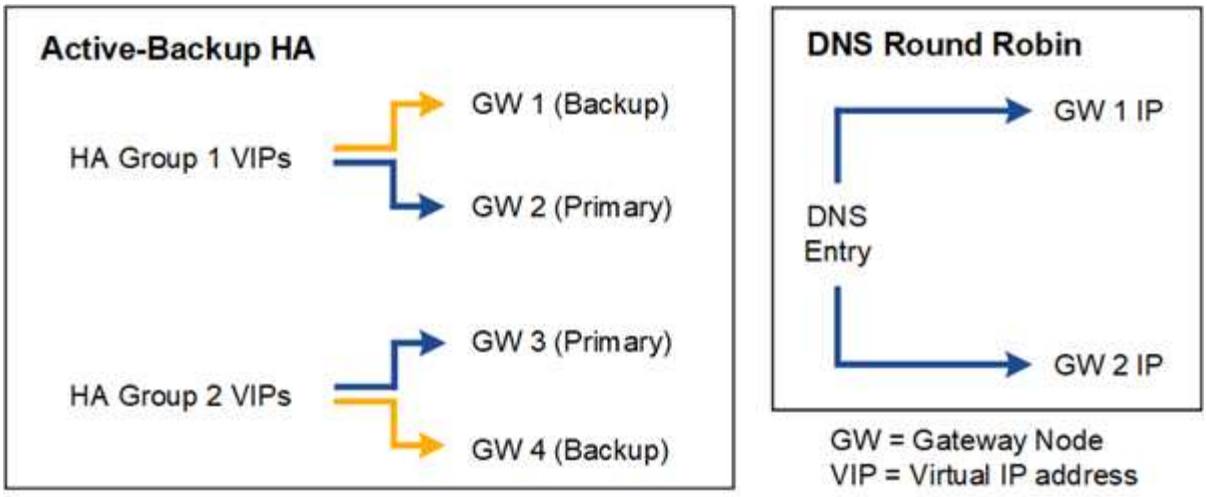
Se você estiver conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconetado e deverá fazer login novamente para retomar sua tarefa.

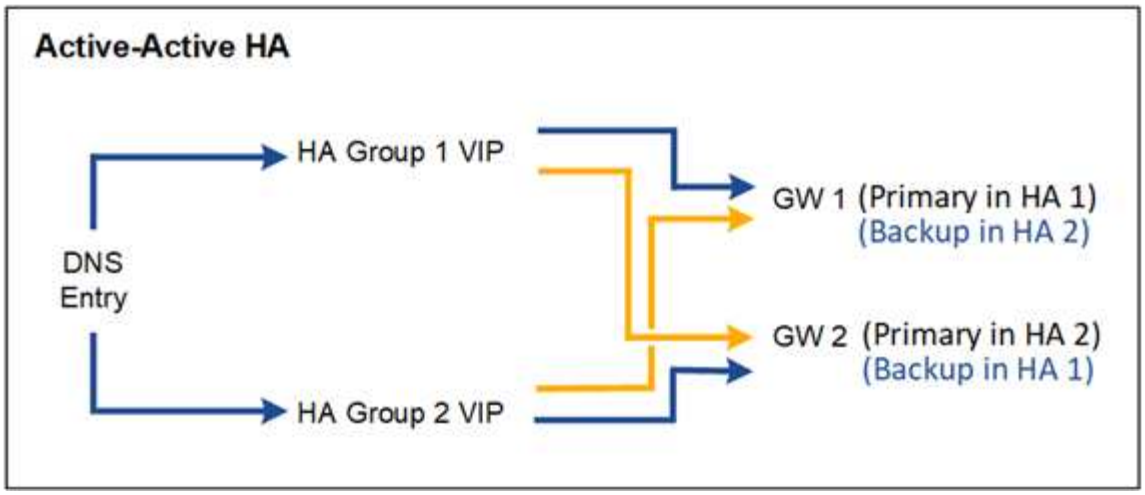
Alguns procedimentos de manutenção não podem ser executados quando o nó Admin principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

Opções de configuração para grupos de HA

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de HA. Cada opção tem vantagens e desvantagens.

Nos diagramas, azul indica a interface principal no grupo HA e 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
Active-Backup HA	• Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido.	• Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo.
DNS Round Robin	• Maior taxa de transferência agregada. • Sem hosts ociosos.	• 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.

Configuração	Vantagens	Desvantagens
Ha ativo-ativo	• O tráfego é distribuído em vários grupos de HA. • Alta taxa de transferência agregada que é dimensionada com o número de grupos de 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 altamente disponível aos serviços em nós de administração ou nós de gateway.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.
- Se você planeja usar uma interface VLAN em um grupo HA, criou a interface VLAN. "Configurar interfaces VLAN"Consulte .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, criou a interface:
  - **Red Hat Enterprise Linux ou CentOS (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 a instalação do nó)*: "Linux: Adicione interfaces de tronco ou acesso a um nó"
  - **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"

Crie um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza por ordem de prioridade. Em seguida, atribua um ou mais endereços VIP ao grupo.

Uma interface deve ser incluída em um grupo de HA para um nó de gateway ou um nó de administrador. Um grupo de HA só pode usar uma interface para qualquer nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selecione **criar**.

Introduza os detalhes do grupo HA

Passos

1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.

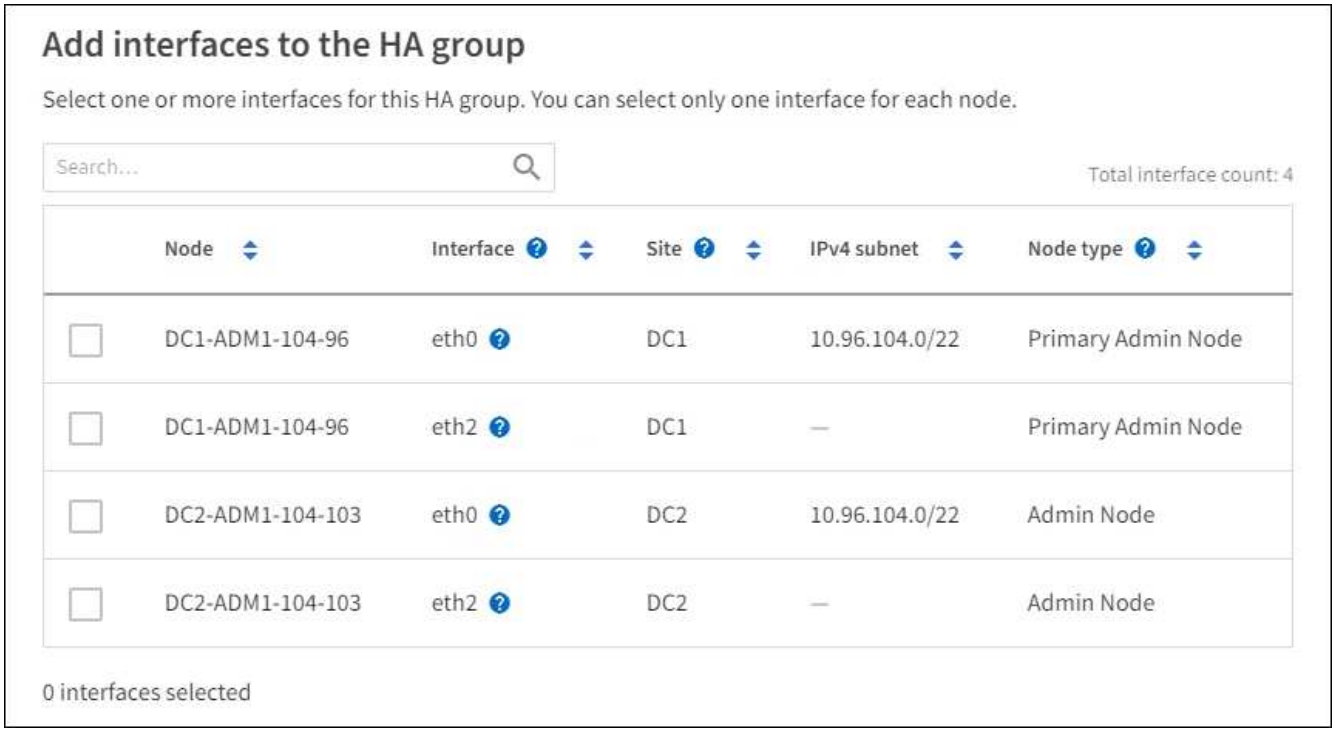
3. Selecione **continuar**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a esse grupo de HA.

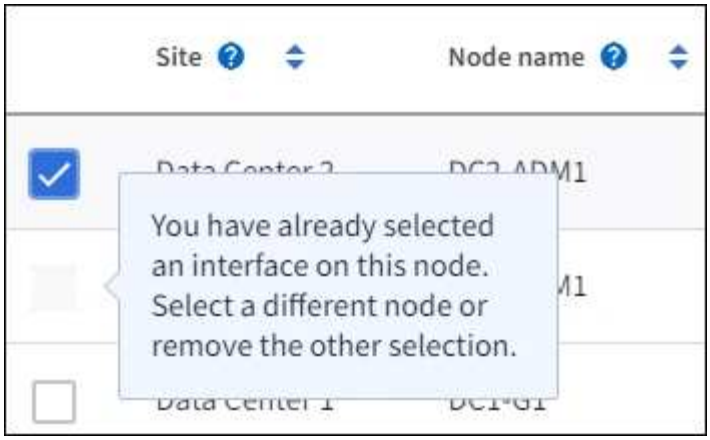
   Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.



> Depois de criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para a seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo de HA for para proteção de HA dos serviços Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione interfaces apenas em nós de administração.
- Se o grupo de HA for para proteção de HA de tráfego de cliente S3 ou Swift, 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 HA dos serviços Admin Node. Da mesma forma, um nó Admin de backup não pode executar todos os procedimentos de manutenção que o nó Admin principal pode fornecer.
- Se você não puder selecionar uma interface, sua caixa de seleção será desativada. A dica da ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o seu valor de sub-rede ou gateway entrar em conflito com outra interface selecionada.
- Não é possível selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **continuar**.

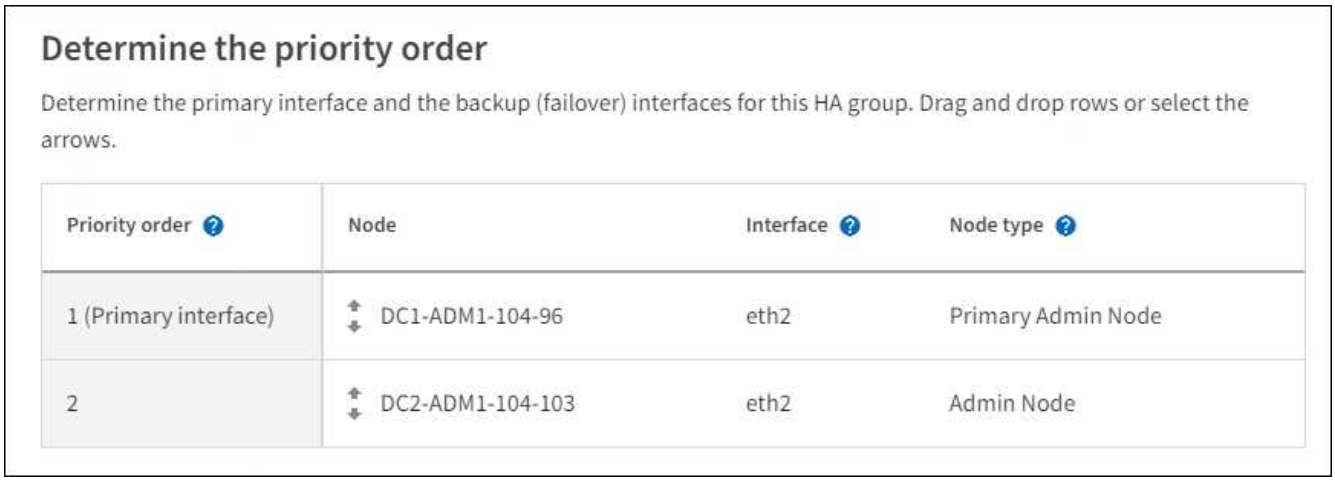
Determine a ordem de prioridade

Se o grupo de HA incluir mais de uma interface, você poderá determinar qual é a interface principal e quais são as interfaces de backup (failover). Se a interface principal falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP passam para a próxima interface de maior prioridade disponível, e assim por diante.

Passos

1. Arraste linhas na coluna **Priority Order** para determinar a interface principal e quaisquer interfaces de backup.

   A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.



Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deverá selecionar uma interface no nó Admin primário para ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

2. Selecione **continuar**.

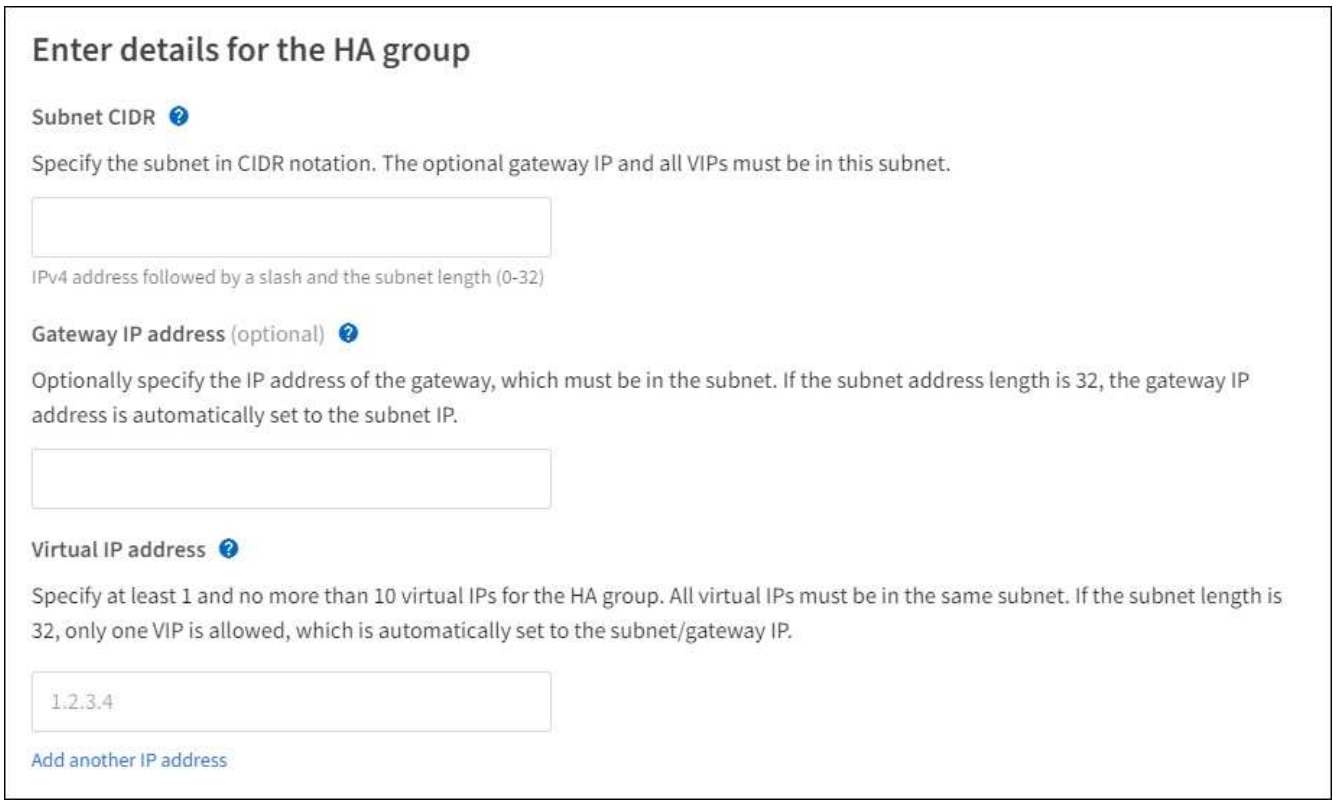
Introduza endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR—um endereço IPv4 seguido de 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 serve como endereço de gateway e endereço VIP.



2. Opcionalmente, se algum cliente S3, Swift, administrativo ou inquilino acessar esses endereços VIP de uma sub-rede diferente, digite o **Endereço IP Gateway**. O endereço de gateway deve estar dentro da sub-rede VIP.

   Os usuários de cliente e administrador usarão esse gateway para acessar os endereços IP virtuais.

3. Introduza pelo menos um e não mais de 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 **Create HA group** e selecione **Finish**.

   O Grupo HA é criado e agora você pode usar os endereços IP virtuais configurados.

Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Próximas etapas

Se você 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 para anexar todos os certificados necessários. "Configurar pontos de extremidade do balanceador de carga"Consulte .

Edite 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 desejar remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.

   A página grupos de alta disponibilidade mostra todos os grupos de HA existentes.

2. Marque a caixa de seleção para o grupo HA que deseja editar.
3. Siga um destes 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 do grupo HA.
   b. Selecione **Guardar**.
   c. Selecione **Finish**.
5. Se você selecionou **Edit HA group**:
   a. Opcionalmente, atualize o nome ou a descrição do grupo.
   b. Opcionalmente, selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

      Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deverá selecionar uma interface no nó Admin primário para ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal

   c. Opcionalmente, arraste linhas para alterar a ordem de prioridade da interface principal e de quaisquer interfaces de backup para esse grupo de HA.
   d. Opcionalmente, atualize os endereços IP virtuais.
   e. Selecione **Save** e, em seguida, selecione **Finish**.

Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Remova um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de cada 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 usem.

Para evitar interrupções do cliente, atualize quaisquer aplicativos de cliente S3 ou Swift afetados antes de remover um grupo HA. Atualize cada cliente para se conetar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP configurado para uma interface durante a instalação.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Revise a coluna **Load balancer endpoints** para cada grupo de HA que você deseja remover. Se algum ponto final do balanceador de carga estiver listado:
   a. Aceda a **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Selecione a caixa de verificação para o endpoint.
   c. Selecione **actions** > **Edit endpoint binding mode**
   d. Atualize o modo de encadernação para remover o grupo HA.
   e. Selecione **Salvar alterações**.
3. Se não houver pontos de extremidade do balanceador de carga listados, marque a caixa de seleção para cada grupo de HA que você deseja remover.
4. Selecione **ações** > **Remover grupo HA**.
5. Reveja a mensagem e selecione **Eliminar grupo HA** para confirmar a sua seleção.

   Todos os grupos de HA selecionados são removidos. Um banner verde de sucesso aparece na página grupos de alta disponibilidade.

Gerenciar o 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 e Swift.

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 obtenção e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho em vários nós de storage.

O serviço StorageGRID Load Balancer é instalado em todos os nós de administração e em todos os nós de gateway e fornece balanceamento de carga de camada 7. Ele executa o encerramento do TLS (Transport Layer Security) das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage.

O serviço Load Balancer em cada nó opera de forma independente ao encaminhar o tráfego do cliente para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU.

> Embora o serviço de balanceamento de carga StorageGRID seja o mecanismo de balanceamento de carga recomendado, você pode querer integrar um balanceador de carga de terceiros. Para obter informações, contacte o representante da sua conta NetApp ou "TR-4626: Balanceadores de carga globais e de terceiros da StorageGRID" consulte .

Quantos nós de balanceamento de carga eu preciso?

Como prática recomendada geral, cada local no seu sistema StorageGRID deve incluir dois ou mais nós com o serviço de balanceador de carga. Por exemplo, um site pode incluir dois nós de Gateway ou um nó de administrador e um nó de gateway. Verifique se há infraestrutura adequada de rede, hardware ou virtualização para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços SG100 ou SG1000, 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 aplicativos de cliente de entrada e saída usarão para acessar os nós que contêm o serviço Load Balancer. O endpoint também define o tipo de cliente (S3 ou Swift), o modo de encadernação e, opcionalmente, uma lista de inquilinos permitidos ou bloqueados.

Para criar um ponto de extremidade do balanceador de carga, selecione **CONFIGURATION** > **Network** > **Load balancer endpoints** ou conclua o assistente de configuração do FabricPool e do S3. Para obter instruções:

- "Configurar pontos de extremidade do balanceador de carga"
- "Utilize o assistente de configuração S3"
- "Utilize o assistente de configuração do FabricPool"

Considerações para a porta

A porta de um ponto de extremidade do balanceador de carga é padrão para 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 endpoint usará o serviço Load Balancer somente nos nós do Gateway. Essas portas são reservadas em nós de administração. Se você usar a mesma porta para mais de um endpoint, você deve especificar um modo de encadernação diferente para cada endpoint.

As portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".

Considerações para o protocolo de rede

Na maioria dos casos, as conexões entre aplicativos cliente e StorageGRID devem usar criptografia TLS (Transport Layer Security). A conexão com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga do StorageGRID, deve selecionar **HTTPS**.

Considerações para certificados de endpoint do balanceador de carga

Se selecionar **HTTPS** como protocolo de rede para o ponto de extremidade do balanceador de carga, tem de fornecer um certificado de segurança. Você pode usar qualquer uma dessas três opções ao criar o ponto de

extremidade do balanceador de carga:

- **Carregue um certificado assinado (recomendado)**. Este certificado pode ser assinado por uma autoridade de certificação pública ou privada (CA). Usar um certificado de servidor CA publicamente confiável para proteger a conexão é a melhor prática. Em contraste com os certificados gerados, os certificados assinados por uma CA podem ser girados 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 de certificado de servidor personalizado.
  - Opcionalmente, um pacote de CA dos certificados de cada autoridade de certificação de emissão intermediária.
- **Gerar um certificado autoassinado**.
- **Use o certificado global StorageGRID S3 e Swift**. Você deve carregar ou gerar uma versão personalizada deste certificado antes de selecioná-lo para o ponto de extremidade do balanceador de carga. "Configure os certificados API S3 e Swift"Consulte .

Quais valores eu preciso?

Para criar o certificado, você deve saber todos os nomes de domínio e endereços IP que os aplicativos cliente S3 ou Swift usarão para acessar o endpoint.

A entrada **Assunto DN** (Nome distinto) do certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para o 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 Load Balancer. Por exemplo, `*.storagegrid.example.com` usa o caractere curinga * para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, o certificado também deve incluir uma entrada **Nome alternativo** para cada "Nome de domínio do endpoint S3" um que você configurou, incluindo nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Se você usar curingas para nomes de domínio, revise o "Diretrizes de fortalecimento para certificados de servidor".

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados expirados?

> 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 quaisquer alertas que avisem sobre datas de expiração de certificado que estejam se aproximando, como **validade do certificado de endpoint do balanceador de carga** e **expiração do certificado de servidor global para alertas S3 e Swift API**.
- 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, você deve 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 que expirarão em breve sem interrupções.
- Se você gerou um certificado StorageGRID auto-assinado e esse certificado está prestes a expirar, você deve substituir manualmente o certificado no StorageGRID e no aplicativo S3 antes que o certificado existente expire.

Considerações para o modo de encadernação

O modo de encadernação permite controlar quais endereços IP podem ser usados para acessar um ponto de extremidade do balanceador de carga. Se um endpoint usar um modo de encadernação, os aplicativos cliente só poderão acessar o endpoint se usarem um endereço IP permitido ou seu nome de domínio totalmente qualificado (FQDN) correspondente. Os aplicativos clientes que usam qualquer outro endereço IP ou FQDN não podem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de encadernação:

- **Global** (padrão): Os aplicativos cliente podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, 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 endpoint.
- **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 Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway.

Considerações para acesso ao locatário

O acesso ao locatário é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um endpoint do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um endpoint (padrão) ou especificar uma lista dos locatários permitidos ou bloqueados para cada endpoint.

Você pode usar esse recurso para fornecer um melhor isolamento de segurança entre os locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que os materiais mais secretos ou altamente classificados de propriedade de um locatário permaneçam completamente inacessíveis para 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 com acesso anônimo) o proprietário do bucket é usado para determinar o locatário.

Exemplo de acesso ao locatário

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:
   - **Public** endpoint: Usa a porta 10443 e permite o acesso a todos os inquilinos.
   - * Ponto final Top SECRET*: Usa a porta 10444 e permite o acesso apenas ao locatário **Top SECRET**. Todos os outros inquilinos estão bloqueados para acessar este endpoint.
2. O `top-secret.pdf` está em um balde de propriedade do **Top SECRET** inquilino.

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 endpoint 10444, o usuário pode acessar o objeto. No entanto, se um usuário pertencente a qualquer outro locatário emitir a mesma solicitação para o mesmo URL, ele receberá uma mensagem de acesso negado imediata. 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 independentemente ao encaminhar tráfego S3 ou Swift para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage 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 storage recebem um valor mínimo de peso básico, mesmo que um nó informe a utilização de 100% ou não consiga relatar sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU estão limitadas ao local 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 S3 e os clientes Swift podem usar ao se conetar ao balanceador de carga StorageGRID nos nós de gateway e administrador.

O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a 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 "removido o remapeamento da porta"o .
- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os GRUPOS HA são recomendados, mas não são necessários. "Gerenciar grupos de alta disponibilidade"Consulte .

- Se o ponto final do balanceador de carga for usado "S3 inquilinos para S3 Select"pelo , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos SG100 ou SG1000 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. "Configurar interfaces VLAN"Consulte .
- Se você estiver criando um endpoint HTTPS (recomendado), você terá as informações para o certificado do servidor.

> As alterações a um certificado de endpoint 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 ou Swift usarão para acessar o endpoint. Você também deve conhecer o assunto (Nome distinto).
  - Se você quiser usar o certificado StorageGRID S3 e Swift API (que também pode ser usado para conexões diretamente aos nós de armazenamento), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API S3 e Swift"Consulte .

Crie um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um tipo de cliente (S3 ou Swift) e um protocolo de rede (HTTP ou HTTPS).

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
2. Selecione **criar**.

Introduza os detalhes do endpoint

Passos

1. Insira os detalhes do endpoint.

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada entre 1 e 65535. Se você digitar **80** ou **443**, o endpoint será configurado somente em nós de Gateway. Essas portas são reservadas em nós de administração.
Tipo de cliente	O tipo de aplicativo cliente que usará esse endpoint, **S3** ou **Swift**.

Campo	Descrição
Protocolo de rede	O protocolo de rede que os clientes utilizarão ao ligar a este ponto final. • Selecione **HTTPS** para comunicação segura e criptografada TLS (recomendada). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione **HTTP** para comunicação menos segura e não criptografada. Use HTTP apenas para uma grade não-produção.

2. Selecione **continuar**.

Selecione um modo de encadernação

Passos

1. Selecione um modo de encadernação para o endpoint para controlar como o endpoint é acessado& n.o 8212;usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

Opção	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, 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 endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

> Se mais de um ponto de extremidade utilizar a mesma porta, o StorageGRID utiliza esta ordem de prioridade para decidir qual ponto de extremidade utilizar: **IPs virtuais de grupos de HA** > **interfaces de nó** > **tipo de nó** > **Global**.

2. Se você selecionou **IPs virtuais de grupos de HA**, selecione um ou mais grupos de HA.
3. Se você selecionou **interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administrador ou nó de gateway que você deseja associar a esse ponto de extremidade.
4. Se você selecionou **tipo de nó**, selecione os nós de administrador, que incluem o nó de administrador

principal e quaisquer nós de administrador não primários ou nós de gateway.

Controle o acesso do locatário

Passos

1. Para a etapa **Acesso ao locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets. Você deve selecionar essa opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o endpoint do balanceador de carga para permitir ou bloquear contas específicas.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

2. Se você estiver criando um endpoint **HTTP**, não será necessário anexar um certificado. Selecione **Create** para adicionar o novo ponto de extremidade do balanceador de carga. Em seguida, vá Depois de terminarpara . Caso contrário, selecione **continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um endpoint **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao endpoint.

   O certificado protege as conexões entre clientes S3 e Swift e o serviço Load Balancer no nó Admin ou nos nós Gateway.

   - * Carregar certificado*. Selecione esta opção se tiver certificados personalizados para carregar.
   - **Gerar certificado**. Selecione esta opção se tiver os valores necessários para gerar um certificado personalizado.
   - **Use o certificado StorageGRID S3 e Swift**. Selecione essa opção se quiser usar o certificado global S3 e Swift API, que também pode ser usado para conexões diretamente aos nós de storage.

     Não é possível selecionar essa opção a menos que você tenha substituído o certificado padrão S3 e Swift API, que é assinado pela CA de grade, por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API S3 e Swift"Consulte .

2. Se você não estiver usando o certificado StorageGRID S3 e Swift, carregue ou gere o certificado.

Carregar certificado

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado do servidor**: O arquivo de certificado do servidor personalizado na codificação PEM.
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

> As chaves privadas 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 de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, 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 certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar 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 e Swift e o endpoint.

Gerar certificado

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto 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.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **criar**.

O ponto final do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift e este endpoint.

Depois de terminar

Passos

1. Se você usar um DNS, verifique se o DNS inclui 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 conetarão aos endereços IP virtuais desse grupo HA.
   - Se você não estiver usando um grupo de HA, os clientes se conetarão ao serviço do 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 de curinga.

2. Forneça aos clientes S3 e Swift as informações necessárias para se conetar ao endpoint:
   - Número da porta

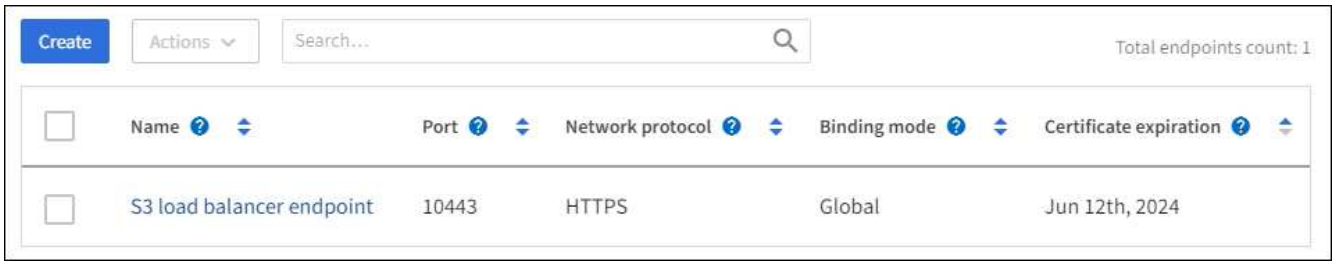
- Nome de domínio ou endereço IP totalmente qualificado
- Todos os detalhes necessários do certificado

Visualize e edite pontos de extremidade do balanceador de carga

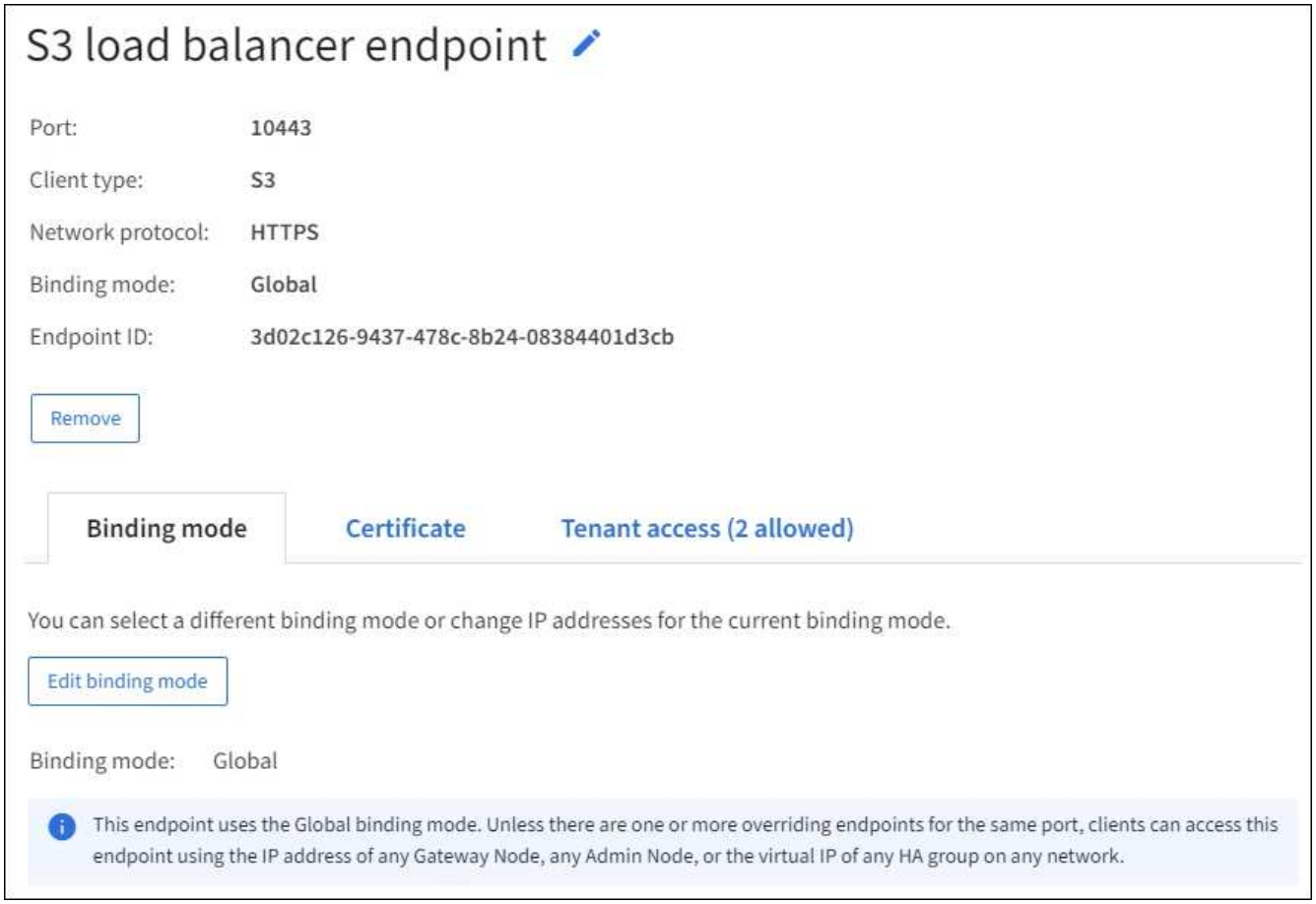
Você pode exibir detalhes dos endpoints existentes do balanceador de carga, incluindo os metadados do certificado para um endpoint seguro. Você também pode alterar o nome ou o modo de vinculação de um endpoint e atualizar quaisquer certificados associados.

Não é possível alterar o tipo de serviço (S3 ou Swift), a porta ou o protocolo (HTTP ou HTTPS).

- Para exibir informações básicas de todos os pontos de extremidade do balanceador de carga, revise a tabela na página pontos de extremidade do balanceador de carga.



- Para exibir todos os detalhes sobre um endpoint específico, incluindo metadados de certificado, selecione o nome do endpoint na tabela.



- Para editar um endpoint, use o menu **ações** na página terminais do balanceador de carga ou a página de detalhes de um endpoint específico.

Depois de editar um endpoint, você pode precisar esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu ações	Página de detalhes
Edite o nome do endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar nome do endpoint**. c. Introduza o novo nome. d. Selecione **Guardar**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Guardar**.
Editar o modo de encadernação de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **actions** > **Edit endpoint binding mode** c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione **Editar modo de encadernação**. c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.
Editar certificado de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar certificado de endpoint**. c. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **certificado**. c. Selecione **Editar certificado**. d. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. e. Selecione **Salvar alterações**.
Editar acesso ao locatário	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar acesso ao locatário**. c. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **Acesso ao locatário**. c. Selecione **Editar acesso ao locatário**. d. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. e. Selecione **Salvar alterações**.

Remova os pontos finais do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **ações** ou remover um único endpoint da página de detalhes.

Para evitar interrupções do cliente, atualize os aplicativos de cliente S3 ou Swift afetados antes de remover um ponto de extremidade do balanceador de carga. Atualize cada cliente para se conetar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Certifique-se de atualizar todas as informações de certificado necessárias também.

- Para remover um ou mais pontos finais:
  a. Na página Load balancer, marque a caixa de seleção para cada ponto final que deseja remover.
  b. Selecione **ações** > **Remover**.
  c. Selecione **OK**.
- Para remover um endpoint da página de detalhes:
  a. Na página Load balancer. Selecione o nome do endpoint.
  b. Selecione **Remover** na página de detalhes.
  c. Selecione **OK**.

Configurar nomes de domínio de endpoint S3

Para oferecer suporte a S3 solicitações de estilo hospedado virtual, você deve usar o Gerenciador de Grade para configurar a lista de S3 nomes de domínio de endpoint aos quais os clientes S3 se conetam.

O uso de um endereço IP para um nome de domínio de endpoint não é suportado. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você confirmou que uma atualização de grade não está em andamento.

Não faça alterações 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 endpoint S3, você deve fazer todas as seguintes ações:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o "Certificado que o cliente usa para conexões HTTPS com o StorageGRID" está assinado para todos os nomes de domínio que o cliente requer.

  Por exemplo, se o endpoint for `s3.company.com`, você deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo do assunto universal (SAN) do endpoint: `*.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 verifique se os Registros fazem referência a todos os nomes de domínio de

endpoint S3 necessários, incluindo quaisquer nomes de curinga.

> Os clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administrador ou um nó de armazenamento, ou conetando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conetam à grade para incluir os endereços IP corretos nos Registros DNS.

Os clientes que usam conexões HTTPS (recomendadas) para a grade podem usar qualquer um destes certificados:

- Os clientes que se conetam 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 endpoint S3.
- Os clientes que se conetam a um ponto de extremidade do balanceador de carga ou diretamente a um nó de armazenamento podem personalizar o certificado global S3 e Swift API para incluir todos os nomes de domínio de endpoint S3 necessários.

> Se você não adicionar nomes de domínio de endpoint S3 e a lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

Adicione um nome de domínio de endpoint S3

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Introduza o nome de domínio no campo **Domain Name 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.
3. Selecione **Guardar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint S3 necessários.
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use seu próprio certificado"atualize o certificado associado ao endpoint", .
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use o certificado global S3 e Swift API ou diretamente aos nós de storage, "Atualize o certificado global S3 e Swift API".
5. Adicione os Registros DNS necessários para garantir que as solicitações de nome de domínio de endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o endpoint `bucket.s3.company.com`, o servidor DNS resolve para o endpoint correto e o certificado autentica o endpoint como esperado.

Renomeie um nome de domínio de endpoint S3

Se você alterar um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.

2. Selecione o campo de nome de domínio que deseja editar e faça as alterações necessárias.
3. Selecione **Guardar**.
4. Selecione **Sim** para confirmar a alteração.

Exclua um nome de domínio de endpoint S3

Se você remover um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Selecione o ícone de exclusão ✕ ao lado do nome de domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- "USE A 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 e Swift se conetam ao serviço Load Balancer, que está incluído em todos os nós Admin e nós Gateway, ou ao serviço LDR (roteador de distribuição local), que está incluído em todos os nós de armazenamento.

Os aplicativos clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de grade e o número da porta do serviço nesse nó. Como opção, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões altamente disponíveis que usam endereços IP virtual (VIP). Se você quiser se conetar 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 conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Se você já criou endpoints do balanceador de carga e grupos de alta disponibilidade (HA), consulte Onde encontrar endereços IP para localizar esses valores no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	Porta atribuída ao ponto de extremidade do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: • HTTPS: 18083 • HTTP:18085

Exemplos de URLs

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

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

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta do endpoint do balanceador de carga for 10443, um aplicativo poderá usar o seguinte URL para se conetar ao StorageGRID:

`https://192.0.2.5:10443`

Onde encontrar endereços IP

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Para localizar 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 deseja se conetar.
   c. Selecione a guia **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 cliente para qualquer um dos endereços IP na lista:

      - **eth0:** rede de Grade
      - **eth1:** Admin Network (opcional)
      - **eth2:** rede de clientes (opcional)

      Se você estiver exibindo um nó de administrador ou um nó de gateway e for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de HA será exibido em eth2.

3. Para localizar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Na tabela, anote o endereço IP virtual do grupo HA.
4. Para localizar o número da porta de um endpoint do Load Balancer:
   a. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Observe o número da porta do endpoint que você deseja usar.

   > Se o número da porta for 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas estão reservadas em nós de administração. Todas as outras portas são configuradas nos nós de Gateway e nos de Admin.

   c. Selecione o nome do endpoint na tabela.
   d. Confirme se o **Client type** (S3 ou Swift) corresponde ao aplicativo cliente que usará o endpoint.

Gerencie redes e conexões

Configurar definições de rede: Visão geral

Você pode configurar várias configurações de rede do Gerenciador de Grade para ajustar a operação do sistema StorageGRID.

Configurar interfaces VLAN

Você pode "Crie interfaces de LAN virtual (VLAN)"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 endpoints 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 gerenciar 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 na limitação e monitoramento de tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Gerenciador de Grade para configurar e gerenciar redes e conexões StorageGRID.

"Configurar conexões de cliente S3 e Swift"Consulte para saber como conetar clientes S3 ou Swift.

Redes StorageGRID predefinidas

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 de acordo com seus requisitos de segurança e acesso.

Para obter mais informações sobre a topologia de rede, "Diretrizes de rede"consulte .

Rede de rede

Obrigatório. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes.

Rede de administração

Opcional. A rede de administração é normalmente utilizada para administração e manutenção do sistema. Ele também pode ser usado para acesso ao protocolo cliente. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites.

Rede de clientes

Opcional. A rede de clientes é uma rede aberta normalmente usada para fornecer acesso a aplicativos clientes S3 e Swift, para que a rede de Grade possa ser isolada e protegida. A rede do cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

Diretrizes

- Cada nó de grade do StorageGRID requer uma interface de rede dedicada, endereço IP, máscara de sub-rede e gateway para cada rede à qual está 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 roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede mapeia para uma interface de rede específica.

Rede	Nome da interface
Grelha	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conetado a um dispositivo StorageGRID, portas específicas serão usadas para cada rede. Para obter mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se o eth2 estiver ativado, o 0,0.0.0/0 usará a rede do cliente no eth2. Se o eth2 não estiver ativado, o 0,0.0.0/0 usará a rede de Grade no eth0.
- A rede do cliente não se torna operacional até que o nó da grade se junte à grade
- A rede Admin pode ser configurada durante a implantação do nó de grade para permitir o 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 Admin ou Gateway, para que você possa usar "Interfaces VLAN" para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou, talvez você queira adicionar uma interface de acesso a ser usada em um "Grupo de alta disponibilidade (HA)".

Para adicionar interfaces de tronco ou acesso, consulte o seguinte:

- **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"
  - **RHEL ou CentOS (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, CentOS, Ubuntu ou Debian (após a instalação do nó)**: "Linux: Adicione interfaces de tronco ou acesso a um nó"

Ver endereços IP

Você pode exibir o endereço IP de cada nó de grade em seu sistema StorageGRID. Em seguida, você pode usar esse endereço IP para fazer login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

Antes de começar

Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".

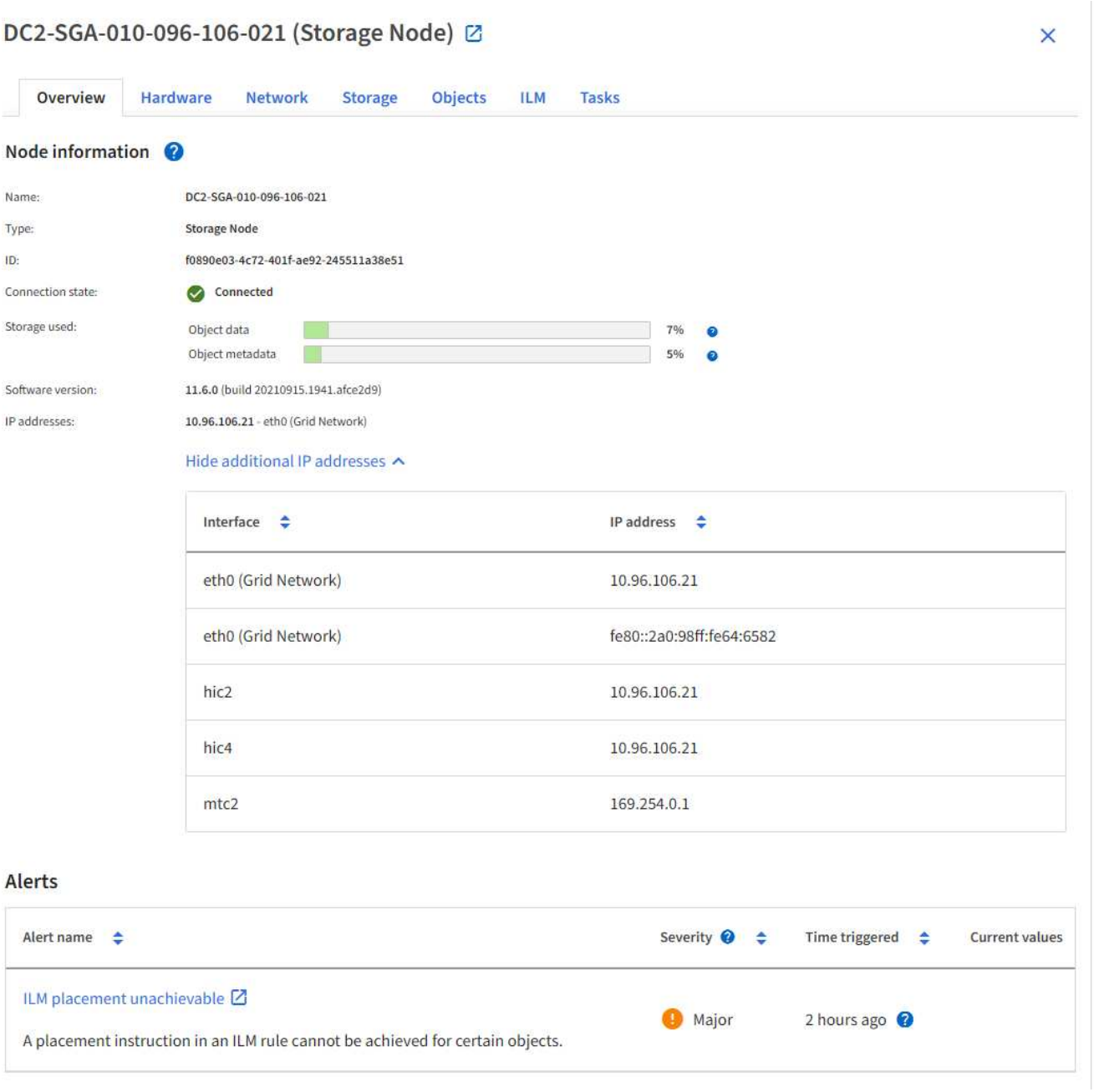
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, "Configurar endereços IP"consulte .

Passos

1. Selecione **NODES** > ***grid node*** > **Visão geral**.
2. Selecione **Mostrar mais** à direita do título dos endereços IP.

   Os endereços IP desse nó de grade são listados em uma tabela.



Cifras suportadas para conexões TLS de saída

O sistema StorageGRID oferece suporte a um conjunto limitado de conjuntos de codificação para conexões TLS (Transport Layer Security) com os sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

Versões suportadas do TLS

O StorageGRID oferece suporte ao TLS 1,2 e TLS 1,3 para conexões a sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

As cifras TLS que são suportadas para utilização com sistemas externos foram selecionadas para garantir a compatibilidade com uma gama de sistemas externos. A lista é maior do que a lista de cifras que são suportadas para uso com aplicativos cliente S3 ou Swift. Para configurar cifras, vá para **CONFIGURATION** >

Security > **Security settings** e selecione **TLS e SSH policies**.

> As opções de configuração TLS, como versões de protocolo, cifras, algoritmos de troca de chaves e algoritmos MAC, não são configuráveis no StorageGRID. Entre em Contato com o representante da sua conta do NetApp se você tiver solicitações específicas sobre essas configurações.

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 obter segurança, flexibilidade e desempenho.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo um 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 de 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 de cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego Admin Node, que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces somente em Admin Nodes.
- Se a interface VLAN for para tráfego de clientes S3 ou Swift, selecione interfaces em nós de administração ou nós de gateway.
- Se você precisar adicionar interfaces de tronco, consulte o seguinte para obter detalhes:
  - **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"
  - **RHEL ou CentOS (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, CentOS, Ubuntu ou Debian (após a instalação do nó)**: "Linux: Adicione interfaces de tronco ou acesso a um nó"

Crie uma interface VLAN

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.
- Uma interface de tronco foi configurada na rede e conetada ao nó VM ou 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 de cliente ou administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar VLAN 100 para tráfego FabricPool e

VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Gerenciador de Grade para criar interfaces de VLAN que permitem que os clientes acessem o StorageGRID em uma VLAN específica. Ao criar interfaces VLAN, você especifica a ID da VLAN e seleciona interfaces pai (tronco) em um ou mais nós.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selecione **criar**.

Insira os detalhes das interfaces VLAN

Passos

1. Especifique o ID da VLAN na rede. Pode introduzir qualquer valor entre 1 e 4094.

   Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar VLAN ID 200 para tráfego de administrador em um local e o mesmo VLAN ID para tráfego de cliente em outro local. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada local. No entanto, duas interfaces VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó. Se você especificar uma ID que já foi usada, uma mensagem será exibida.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **continuar**.

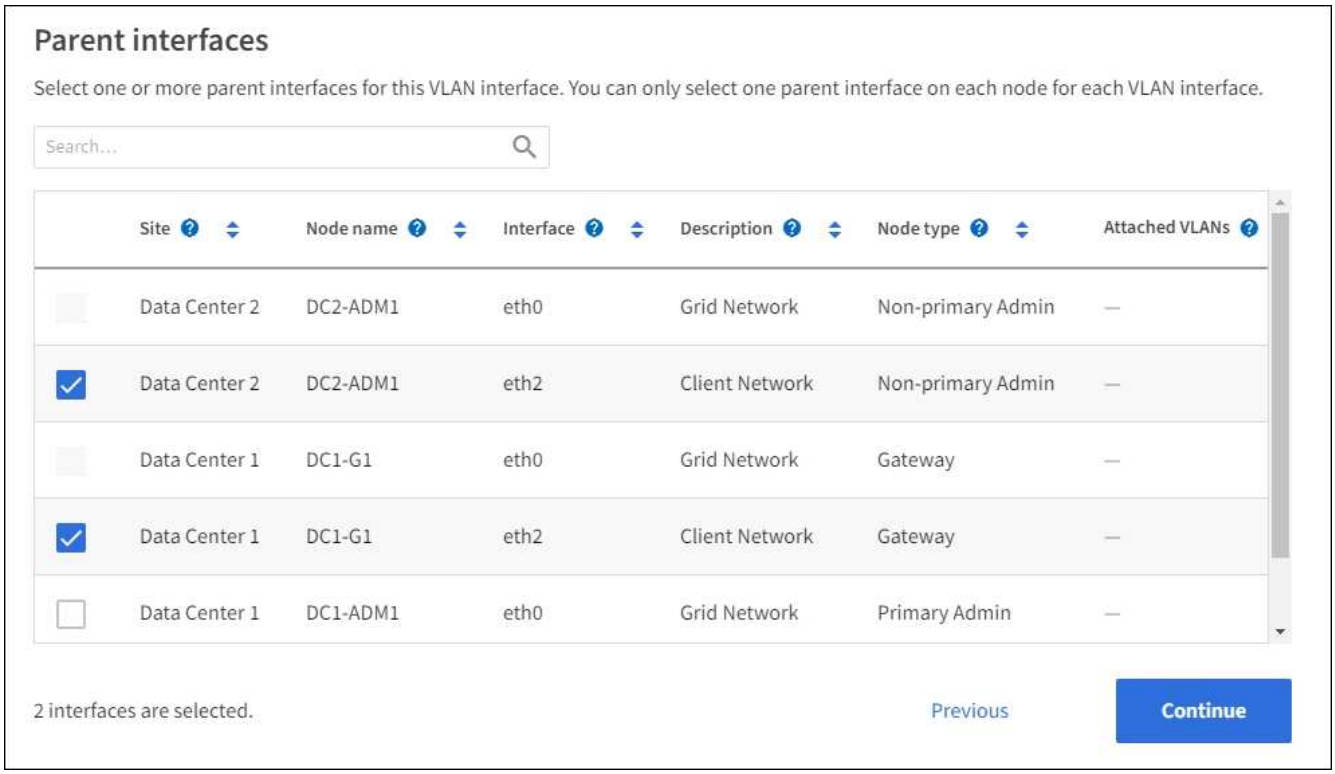
Escolha interfaces pai

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada local da grade. As interfaces Admin Network (eth1) não podem ser usadas como interfaces pai e não são mostradas.

Passos

1. Selecione uma ou mais interfaces pai às quais anexar esta VLAN.

   Por exemplo, você pode querer anexar uma VLAN à interface de rede de cliente (eth2) para um nó de gateway e um nó de administrador.



2. Selecione **continuar**.

Confirme as definições

Passos

1. Revise a configuração e faça quaisquer alterações.
   - Se você precisar alterar a ID ou a descrição da VLAN, selecione **Digite os detalhes da VLAN** na parte superior da página.
   - Se você precisar alterar uma interface pai, selecione **escolha interfaces pai** na parte superior da página ou selecione **anterior**.
   - Se for necessário remover uma interface pai, selecione a lixeira .
2. Selecione **Guardar**.
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** para o nó (**NODES** > ***parent interface node*** > **Network**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere a 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 você 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 essa interface pai for usada em um grupo HA.

  Por exemplo, suponha que a VLAN 200 esteja conetada às interfaces pai nos nós A e B. se um grupo de 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 **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Marque a caixa de seleção para a interface VLAN que 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 um 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 quaisquer alterações.
6. Selecione **Guardar**.

Remova uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela for usada atualmente em um grupo HA. Você deve remover a interface VLAN do grupo HA antes de removê-la.

Para evitar quaisquer interrupções no tráfego do cliente, considere fazer um dos seguintes procedimentos:

- Adicione uma nova interface VLAN ao grupo HA antes de remover essa interface VLAN.
- Crie um novo grupo HA que não use essa interface VLAN.
- Se a interface VLAN que você deseja remover for atualmente a interface ativa, edite o grupo HA. Mova a interface VLAN que você deseja remover para a parte inferior da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e remova a interface antiga do grupo HA. Finalmente, exclua a interface VLAN nesse nó.

Passos

1. Selecione **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Marque a caixa de seleção para cada interface VLAN que você deseja remover. Em seguida, selecione **ações** > **Excluir**.
3. Selecione **Sim** para confirmar a sua seleção.

   Todas as interfaces VLAN selecionadas são removidas. Um banner verde de sucesso aparece na página interfaces VLAN.

Gerenciar políticas de classificação de tráfego

Gerenciar políticas de classificação de tráfego: Visão geral

Para aprimorar suas ofertas de qualidade de serviço (QoS), você pode criar políticas de classificação de tráfego para identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e monitoramento de tráfego.

As políticas de classificação de tráfego são aplicadas a pontos de extremidade no serviço de balanceador de carga do StorageGRID 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 correspondentes

Cada política de classificação de tráfego contém uma ou mais regras correspondentes para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Baldes
- Sub-rede
- Locatário
- 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 de agregado
- Largura de banda por solicitação
- Solicitações simultâneas
- Taxa de solicitação

Os valores-limite são impostos por balanceador de carga. Se o tráfego for distribuído simultaneamente em vários balanceadores de carga, as taxas máximas totais são vários dos limites de taxa especificados.

> Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

Para limites de largura de banda agregada ou por solicitação, as solicitações são transmitidas ou enviadas pela taxa definida. O StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo matcher, é a aplicada. A largura de banda consumida pela solicitação não conta com outras políticas de correspondência menos específicas que contenham políticas de limite de largura de banda agregada. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta de retardo 503 para solicitações que excedem qualquer limite de política correspondente.

No Gerenciador de Grade, 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 aplicar acordos de nível de serviço (SLAs) que fornecem detalhes sobre 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 alcançar 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 copiar regra ILM	25 K solicitações/seg Largura de banda de 5 GB/seg (40 Gbps)	dólares por mês
Prata	250 TB de armazenamento permitido	2 copiar regra ILM	10 K solicitações/seg Largura de banda de 1,25 GB/seg (10 Gbps)	dólares por mês
Bronze	100 TB de armazenamento permitido	2 copiar regra ILM	5 K solicitações/seg Largura de banda de 1 GB/seg (8 Gbps)	dólares por mês

Crie 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, endpoint 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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.
- Você criou todos os pontos de extremidade do balanceador de carga que deseja corresponder.
- Você criou quaisquer inquilinos que você deseja combinar.

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.

2. Selecione **criar**.
3. Introduza um nome e uma descrição (opcional) para a política e selecione **continuar**.

   Por exemplo, descreva ao que esta política de classificação de tráfego se aplica e ao 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 correspondente se aplica. Os tipos de tráfego são bucket, bucket regex, CIDR, terminal balanceador de carga e locatário.
Corresponder valor	Introduza o valor que corresponde ao tipo selecionado. • Balde: Introduza um ou mais nomes de intervalo. • Regex do 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 coincidir no início do nome do bucket e use a âncora para coincidir no final do nome. A correspondência regular de expressões suporta um subconjunto da sintaxe PCRE (Perl compatible regular expression). • CIDR: Insira uma ou mais sub-redes IPv4, na notação CIDR, que corresponda 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 definidos no "Configurar pontos de extremidade do balanceador de carga". • Inquilino: A correspondência de inquilino 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 intervalo acessado será usada para determinar o locatário.
Correspondência inversa	Se você quiser corresponder todo tráfego de rede *exceto* tráfego consistente com o valor tipo e correspondência definido, marque a caixa de seleção **correspondência inversa**. Caso contrário, deixe a caixa de seleção marcada. Por exemplo, se você quiser que essa política se aplique a todos os pontos finais do balanceador de carga, especifique o ponto final do balanceador de carga a ser excluído e selecione **correspondência inversa**. Para uma política que contenha vários matchers em que pelo menos um é um matcher inverso, tenha 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 que você não adicione limites, para que você possa entender as tendências de tráfego.

Campo	Descrição
Tipo	O tipo de limite que você deseja aplicar ao tráfego de rede correspondente à regra. Por exemplo, você pode limitar a largura de banda ou a taxa de solicitação. **Nota**: 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. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no 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 tem uma política que limita o tráfego em apenas uma direção, então 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 correspondências "melhores" para limites de largura de banda na seguinte ordem: • Endereço IP exato (/máscara 32) • Nome exato do balde • Regex do balde • Locatário • Endpoint • 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, digite 10 e selecione MIB/s para evitar que o tráfego de rede combinado por esta regra exceda 10 MIB/s. **Nota**: Dependendo da configuração de unidades, as unidades disponíveis serão binárias (por exemplo, GiB) ou decimais (por exemplo, GB). Para alterar a configuração unidades, selecione a lista suspensa usuário no canto superior direito do Gerenciador de Grade e selecione **Preferências do usuário**.
Unidade	A unidade que descreve o valor introduzido.

Por exemplo, se você quiser criar um limite de largura de banda de 40 GB/s para um nível 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 reveja a política de classificação de tráfego. Use o botão **anterior** para voltar e fazer alterações conforme necessário. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

   O tráfego de clientes S3 e Swift agora é Tratado de acordo com a política de classificação de tráfego.

Depois de terminar

"Exibir métricas de tráfego de rede" para verificar se as políticas estão aplicando os limites de tráfego que você espera.

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 conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.

   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. Consulte "crie políticas de classificação de tráfego" para saber o que introduzir.

   Menu ações

   a. Selecione a caixa de verificação 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 Digite o nome da política, edite opcionalmente o nome ou a descrição da política e selecione **continuar**.
4. Para a etapa Adicionar regras de correspondência, adicione uma regra ou edite o **tipo** e **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 é agora Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Eliminar 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 certa porque uma política não pode ser recuperada quando excluída.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION** > **Network** > **Traffic Classification**.

   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 ações

   a. Selecione a caixa de verificação 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 é eliminada.

Exibir métricas de tráfego de rede

Pode monitorizar o tráfego de rede visualizando os gráficos disponíveis na página políticas de classificação de tráfego.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root ou a permissão Contas do Locatário.

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode exibir métricas para o serviço de balanceador de carga para determinar se a política está limitando com êxito o tráfego na rede. Os dados nos gráficos podem ajudá-lo a determinar se você precisa ajustar a política.

Mesmo que nenhum limite seja definido 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 **CONFIGURATION** > **Network** > **Traffic Classification**.

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 o qual deseja exibir as métricas.
3. Selecione a guia **Metrics**.

   São apresentados os gráficos da política de classificação de tráfego. Os gráficos exibem métricas apenas 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 que corresponde a essa política tratada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho de dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho de dados do corpo de resposta para solicitações que incluem dados do corpo na resposta.

     > Quando as solicitações são concluídas, este gráfico mostra somente o uso da largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode diferir dos valores relatados neste gráfico.

   - Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual as solicitações correspondentes a esta política estão retornando erros (código de status HTTP > 400) para clientes.
   - Duração média da solicitação (não-erro): Este gráfico fornece uma duração média de solicitações bem-sucedidas correspondentes a essa política.
   - Uso de largura de banda da política: Este gráfico fornece a quantidade de largura de banda que corresponde a essa política tratada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho de dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho de dados do corpo de 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 Grafana** logo abaixo do título Metrics para visualizar todos os gráficos de uma política. Além dos quatro gráficos da guia **Metrics**, você pode ver mais dois gráficos:
   - Taxa de solicitação de gravação por tamanho do objeto: A taxa de solicitações DE PUT/POST/DELETE que correspondem a essa política. Posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na exibição de hover são truncadas para contagens de inteiros e podem reportar 0 quando há solicitações não zero no intervalo.
   - Ler taxa de solicitação por tamanho do objeto: A taxa de SOLICITAÇÕES GET/HEAD correspondentes a essa política. Posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na exibição de hover são truncadas para contagens de inteiros e podem reportar 0 quando há solicitações não zero no intervalo.
6. Em alternativa, aceda aos gráficos a partir do menu **SUPPORT**.
   a. Selecione **SUPPORT** > **Tools** > **Metrics**.
   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 de objetos que são agregados na contagem e o número de solicitações por segundo durante esse período de tempo.

As políticas de classificação de tráfego são identificadas pelo 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 ajustar a política.

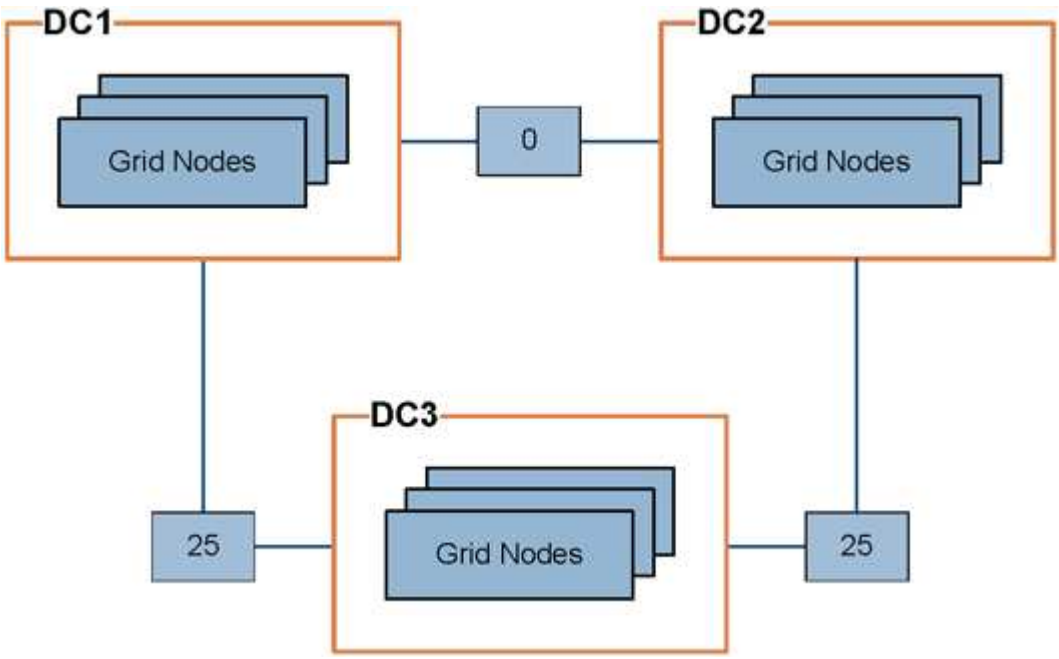
Gerenciar custos de link

Os custos de link permitem que você priorize qual local do data center fornece um serviço solicitado quando existem dois ou mais locais de data center. Você pode ajustar os custos de link para refletir a latência entre sites.

O que são custos de link?

- Os custos de link são usados para priorizar qual cópia de objeto é usada para cumprir recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatário para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço Load Balancer em nós de administração e nós de gateway para direcionar as conexões do cliente. "Considerações para balanceamento de carga"Consulte .

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço Load Balancer em nós de administração e nós de gateway distribui igualmente as conexões de clientes para todos os nós de storage no mesmo local do data center e para qualquer local do data center com um custo de link de 0.

  No exemplo, um nó de gateway no local do data center 1 (DC1) distribui igualmente as conexões de cliente para nós de storage em DC1 e para nós de storage em DC2. Um nó de gateway em DC3 envia conexões de cliente somente para nós de storage em 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 em DC2 recupera um objeto que é armazenado em DC1 e DC3, o objeto é recuperado de DC1, porque o custo do link de DC1 para DC2 é 0, o que é menor do que o custo do link de DC3 para DC2 (25).

Os custos de ligação são números relativos arbitrários sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado menos preferencialmente do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

Link	Custo da ligação	Notas
Entre locais de data center físico	25 (predefinição)	Data centers conectados por um link WAN.
Entre locais lógicos de data center no mesmo local físico	0	Data centers lógicos no mesmo prédio físico ou campus conetados por uma LAN.

Atualizar custos de link

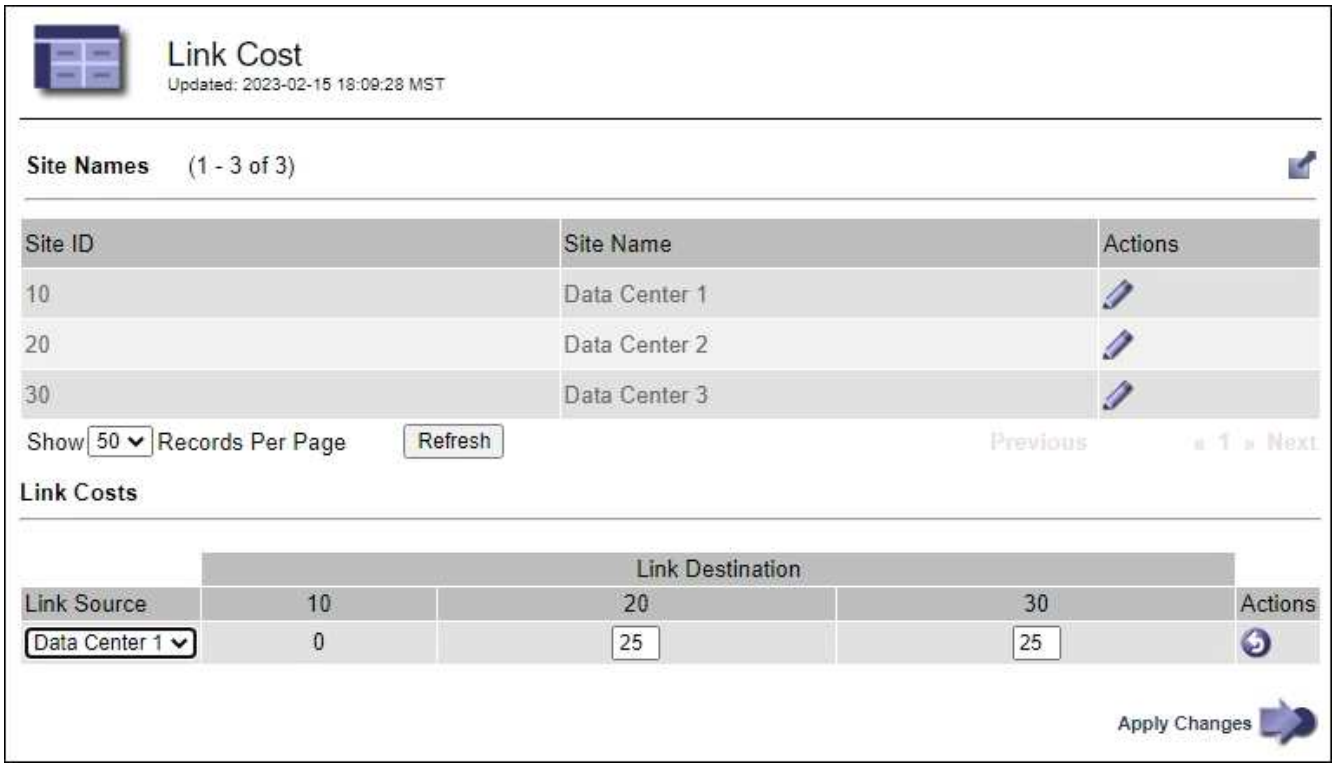
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de configuração de página de topologia de grade".

Passos

1. Selecione **SUPPORT** > **Other** > **Link Cost**.



2. Selecione um site em **Link Source** e insira um valor de custo entre 0 e 100 em **Link Destination**.

Não é possível alterar o custo do link se a origem for a mesma do destino.

Para cancelar as alterações, selecione **Revert**.

3. Selecione **aplicar alterações**.

Use o AutoSupport

Use AutoSupport: Visão geral

O recurso AutoSupport permite que o sistema StorageGRID envie mensagens de status e integridade para o suporte técnico.

O uso do AutoSupport pode acelerar significativamente a determinação e resolução de problemas. O suporte técnico também pode monitorar as necessidades de storage do seu sistema e ajudá-lo a determinar se precisa adicionar novos nós ou sites. Opcionalmente, você pode configurar as mensagens do AutoSupport para serem enviadas para um destino adicional.

Você deve configurar o StorageGRID AutoSupport somente no nó de administração principal. No entanto, você deve configurar Hardware AutoSupport em cada dispositivo.

Informações incluídas nas mensagens do AutoSupport

As mensagens do AutoSupport incluem informações como as seguintes:

- Versão do software StorageGRID
- Versão do sistema operativo
- Informações sobre atributos no nível do sistema e no nível da localização
- Alertas e alarmes recentes (sistema legado)
- Status atual de todas as tarefas de grade, incluindo dados históricos
- Utilização da base de dados do Admin Node
- Número de objetos perdidos ou perdidos
- Definições de configuração da grelha
- Entidades NMS
- Política ILM ativa
- Arquivo de especificação de grade provisionada
- Métricas de diagnóstico

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente. Se o AutoSupport não estiver ativado, uma mensagem será exibida no painel Gerenciador de Grade. 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 que é o Digital Advisor?

O consultor digital é baseado na nuvem e aproveita as análises preditivas e o conhecimento da comunidade fornecidos pela base instalada da NetApp. Suas avaliações de risco contínuas, alertas preditivos, orientações prescritivas e ações automatizadas ajudam a evitar problemas antes que eles ocorram, levando a uma melhor integridade do sistema e maior disponibilidade do sistema.

Você deve habilitar o AutoSupport se quiser usar os painéis e a funcionalidade do consultor digital no site de suporte da NetApp.

"Documentação do Digital Advisor"

Protocolos para envio de mensagens AutoSupport

Você pode escolher um dos três protocolos para enviar mensagens AutoSupport:

- HTTPS
- HTTP
- SMTP

Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP.

Opções de AutoSupport

Você pode usar qualquer combinação das seguintes opções para enviar mensagens do AutoSupport para o suporte técnico:

- **Semanal**: Enviar automaticamente mensagens AutoSupport uma vez por semana. Predefinição: Activado.
- **Event-dispolled**: Envie automaticamente mensagens AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Predefinição: Activado.
- **Sob demanda**: Permita que o suporte técnico solicite que seu sistema StorageGRID envie mensagens AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Predefinição: Desativada.
- **Ativado pelo usuário**: Envie mensagens AutoSupport manualmente a qualquer momento.

AutoSupport para aparelhos

O AutoSupport for Appliances relata problemas de hardware do StorageGRID, enquanto o StorageGRID AutoSupport relata problemas de software do StorageGRID (exceto o SGF6112 em que o StorageGRID AutoSupport relata problemas de hardware e software). Você deve configurar o AutoSupport em cada dispositivo, exceto para o SGF6112 que não requer configuração adicional. O AutoSupport é implementado de maneira diferente para serviços e dispositivos de storage.

É necessário habilitar o AutoSupport no SANtricity para cada dispositivo de storage. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou depois que um dispositivo tiver sido instalado:

- Para aparelhos SG6000 e SG5700, "Configure o AutoSupport no Gerenciador de sistemas do SANtricity"

As mensagens do AutoSupport de dispositivos e-Series podem ser incluídas no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy no "Gerente do sistema da SANtricity".

O StorageGRID AutoSupport não relata problemas de hardware, como falhas de DIMM ou placa de interface do host (HIC). No entanto, algumas falhas de componentes podem acionar "alertas de hardware". Para dispositivos StorageGRID com um controlador de gerenciamento de placa base (BMC), como o SG100, SG1000, SG6060 ou SGF6024, você pode configurar traps de e-mail e SNMP para relatar falhas de hardware:

- "Configurar notificações por e-mail para alertas"
- "Configurar definições SNMP" Para o controlador SG6000-CN ou para os aparelhos de serviços SG100 e SG1000

Informações relacionadas

"Suporte à NetApp"

Configurar o AutoSupport

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root ou outra configuração de grade.
- Se você usar HTTPS para enviar mensagens AutoSupport, você forneceu acesso de saída à Internet para o nó de administração principal, diretamente ou "usando um servidor proxy" (conexões de entrada não necessárias).
- Se HTTP estiver selecionado na página StorageGRID AutoSupport, você configurou um servidor proxy para encaminhar mensagens AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitarão mensagens enviadas usando HTTP.

  "Saiba mais sobre como configurar as configurações de proxy de administrador".

- Se utilizar SMTP como protocolo para mensagens AutoSupport, configurou um servidor de correio SMTP. A mesma configuração do servidor de e-mail é usada para notificações de e-mail de alarme (sistema legado).

Especifique o protocolo para mensagens AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar mensagens AutoSupport:

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. Este protocolo utiliza a porta 443. Se pretender Ative o recurso AutoSupport On Demand, tem de utilizar HTTPS.
- * HTTP*: Se você selecionar HTTP, você deve configurar um servidor proxy para encaminhar mensagens AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam mensagens enviadas usando HTTP. Este protocolo utiliza a porta 80.
- **SMTP**: Use esta opção se quiser que as mensagens do AutoSupport sejam enviadas por e-mail. Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP na página Configuração de e-mail legado (**SUPPORT** > **Alarmes (legacy)** > **Configuração de e-mail legado**).

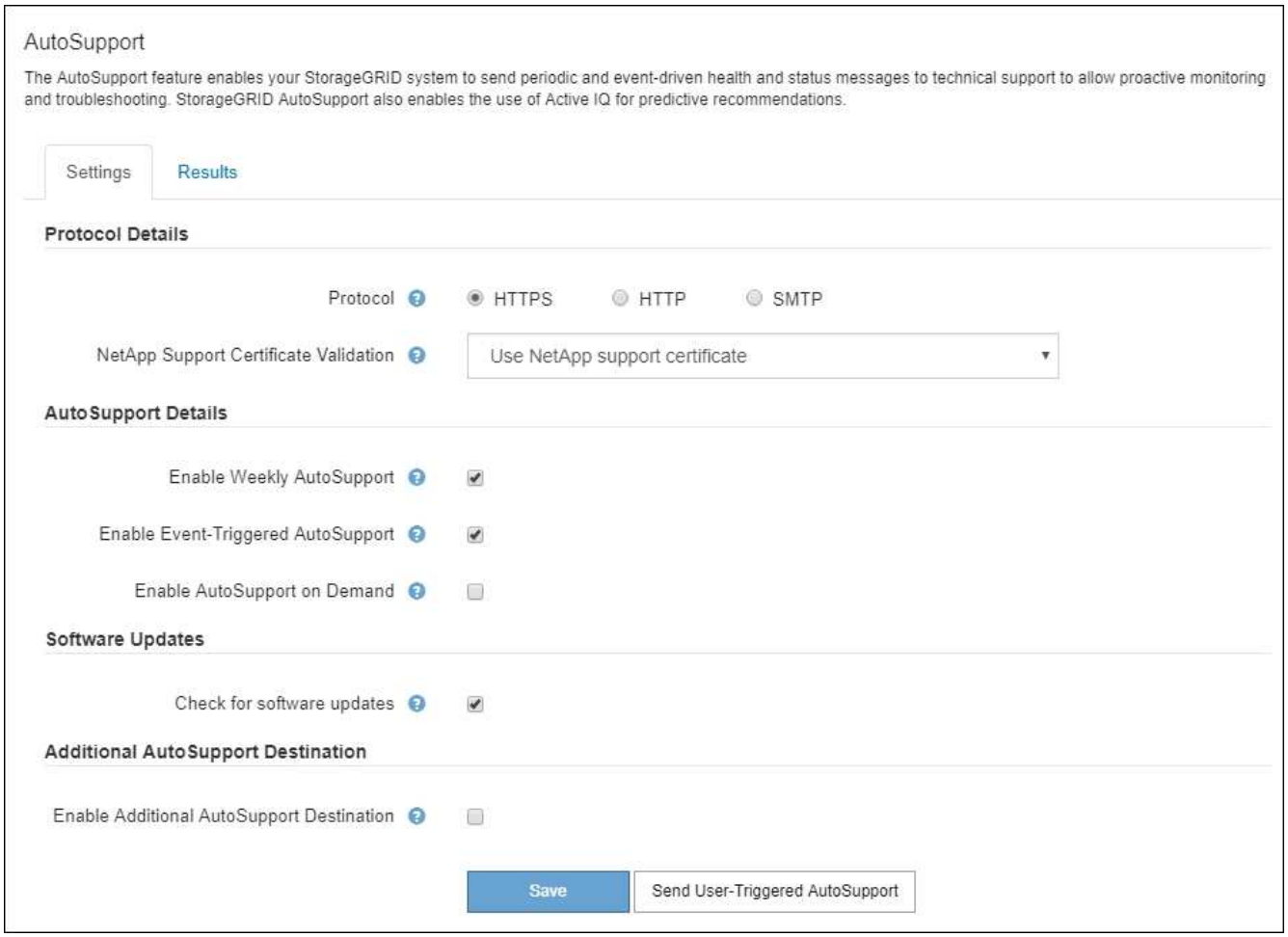
O SMTP era o único protocolo disponível para mensagens AutoSupport antes do lançamento do StorageGRID 11,2. Se você instalou uma versão anterior do StorageGRID inicialmente, o SMTP pode ser o protocolo selecionado.

O protocolo definido é utilizado para enviar todos os tipos de mensagens AutoSupport.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.

   A página AutoSupport é exibida e a guia **Configurações** é selecionada.



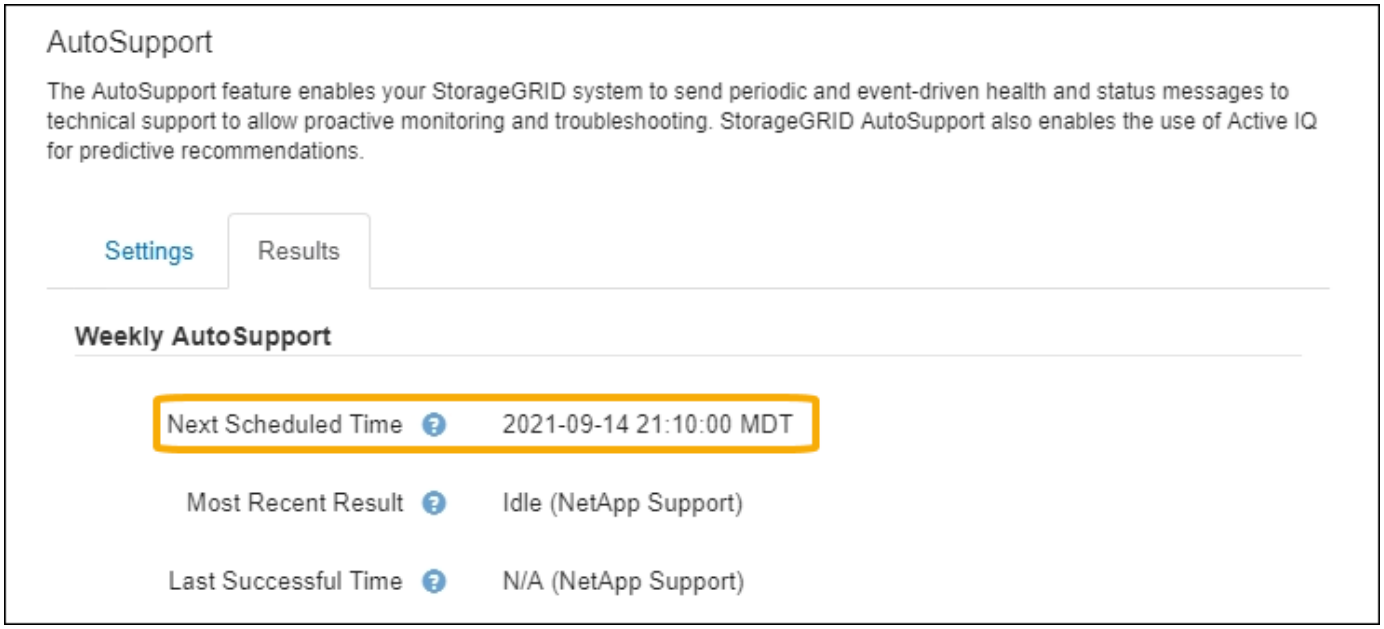
2. Selecione o protocolo que pretende utilizar para enviar mensagens AutoSupport.
3. Se você selecionou **HTTPS**, selecione se deseja usar um certificado TLS para proteger a conexão com o servidor de suporte da NetApp.
   - **Use o certificado de suporte NetApp** (padrão): A validação do certificado garante que a transmissão de mensagens AutoSupport seja segura. O certificado de suporte do NetApp já está instalado com o software StorageGRID.
   - **Não verifique o certificado**: Selecione esta opção somente quando tiver um bom motivo para não usar a validação do certificado, como quando houver um problema temporário com um certificado.
4. Selecione **Guardar**.

   Todas as mensagens semanais, acionadas pelo utilizador e acionadas por eventos são enviadas utilizando o protocolo selecionado.

Desativar mensagens AutoSupport semanais

Por padrão, o sistema StorageGRID está configurado para enviar uma mensagem AutoSupport para o suporte da NetApp uma vez por semana.

Para determinar quando a mensagem AutoSupport semanal será enviada, vá para a guia **AutoSupport** > **resultados**. Na seção **Weekly AutoSupport**, observe o valor para **Next Scheduled Time**.



Pode desativar o envio automático de mensagens AutoSupport semanais a qualquer momento.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desmarque a caixa de seleção **Enable Weekly** (Ativar AutoSupport semanal*).
3. Selecione **Guardar**.

Desative mensagens AutoSupport acionadas por evento

Por padrão, o sistema StorageGRID é configurado para enviar uma mensagem AutoSupport para o suporte da NetApp quando ocorre um alerta importante ou outro evento significativo do sistema.

Você pode desativar as mensagens AutoSupport acionadas por eventos a qualquer momento.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desmarque a caixa de seleção **Enable Event-Triggered** (Ativar AutoSupport ativado por evento*).
3. Selecione **Guardar**.

Habilite o 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. A ativação deste recurso permite que o suporte técnico solicite que o sistema StorageGRID envie mensagens AutoSupport automaticamente. O suporte

técnico também pode definir o intervalo de tempo de polling para consultas AutoSupport On Demand.

O suporte técnico não pode ativar ou desativar o AutoSupport sob demanda.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Selecione **HTTPS** para o protocolo.
3. Marque a caixa de seleção **Enable Weekly** (Ativar AutoSupport semanal*).
4. Marque a caixa de seleção **Enable on Demand** (Ativar AutoSupport on Demand*).
5. Selecione **Guardar**.

   O AutoSupport On Demand está ativado e o suporte técnico pode enviar solicitações AutoSupport On Demand para o StorageGRID.

Desativar verificações para atualizações de software

Por predefinição, o StorageGRID contacta o NetApp para determinar se estão disponíveis atualizações de software para o seu sistema. Se estiver disponível um hotfix do StorageGRID ou uma nova versão, a nova versão será exibida na página Atualização do StorageGRID.

Conforme necessário, você pode opcionalmente desativar a verificação de atualizações de software. Por exemplo, se o sistema não tiver acesso à WAN, desative a verificação para evitar erros de download.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Desmarque a caixa de verificação **verificar atualizações de software**.
3. Selecione **Guardar**.

Adicione um destino AutoSupport adicional

Quando você ativa o AutoSupport, as mensagens de estado e de saúde são enviadas para o suporte da NetApp. Você pode especificar um destino adicional para todas as mensagens do AutoSupport.

Para verificar ou alterar o protocolo usado para enviar mensagens AutoSupport, consulte as instruções para Especifique o protocolo para mensagens AutoSupport.

> Não é possível usar o protocolo SMTP para enviar mensagens AutoSupport para um destino adicional.

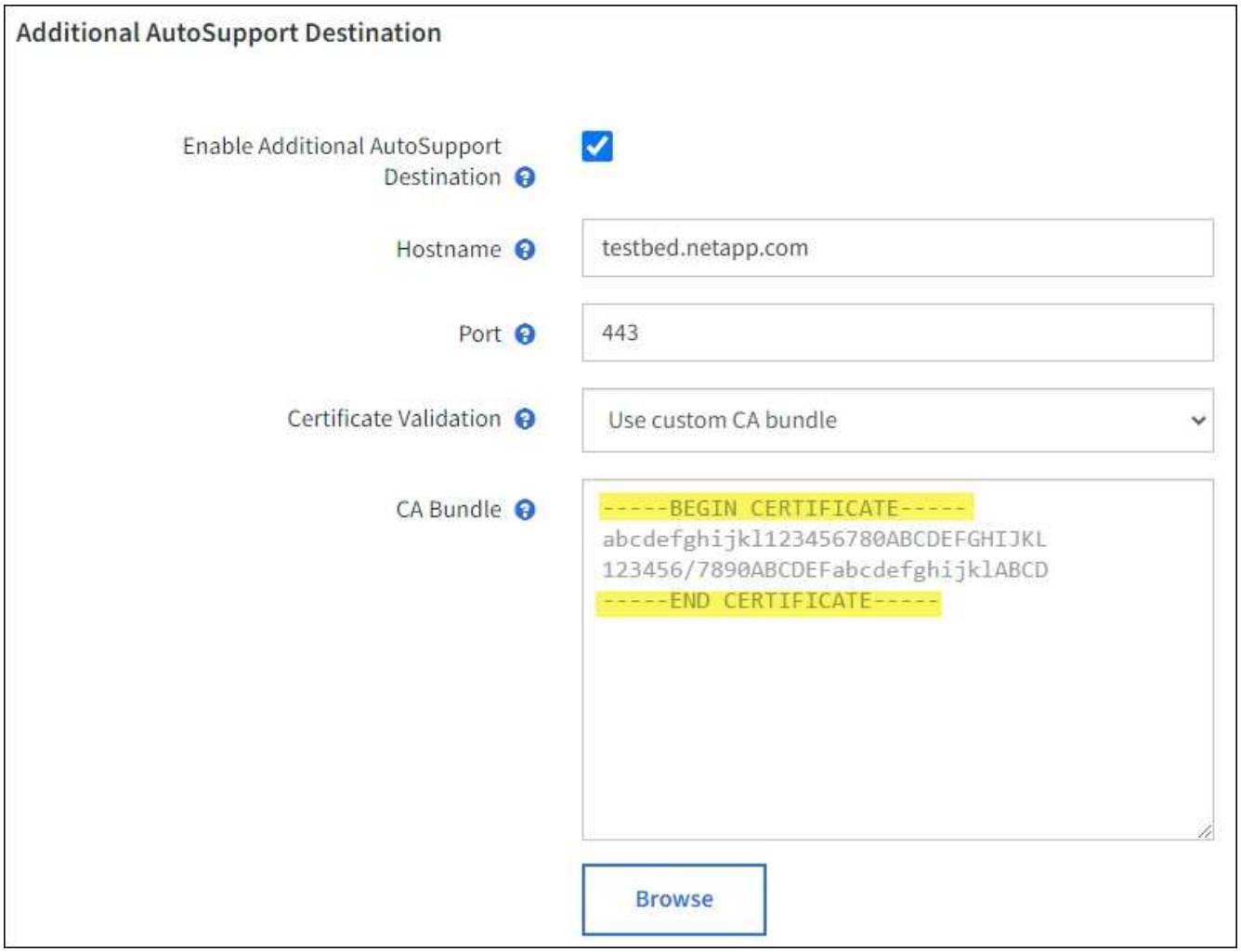
Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Selecione **Ativar destino AutoSupport Adicional**.
3. Especifique o seguinte:

Campo	Descrição
Nome do anfitrião	O nome do host do servidor ou endereço IP de um servidor de destino AutoSupport adicional. **Nota**: Pode introduzir apenas um destino adicional.
Porta	A porta usada para se conetar a um servidor de destino AutoSupport adicional. A predefinição é a porta 80 para HTTP ou a porta 443 para HTTPS.
Validação da certificação	Se um certificado TLS é usado para proteger a conexão com o destino adicional. • Selecione **não verificar o certificado** para enviar as mensagens do AutoSupport sem validação do certificado. Selecione esta opção apenas quando tiver um bom motivo para não utilizar a validação do certificado, como por exemplo, quando houver um problema temporário com um certificado. • Selecione **Use o pacote CA personalizado** para usar a validação do certificado.

4. Se você selecionou **Use o pacote CA personalizado**, siga um destes procedimentos:
   - Selecione **Procurar**, navegue até o arquivo que contém os certificados e selecione **abrir** para carregar o arquivo.
   - Use uma ferramenta de edição para copiar e colar todo o conteúdo de cada um dos arquivos de certificado CA codificados em PEM no campo **CA Bundle**, concatenado em ordem de cadeia de certificados.

     Você deve incluir `----BEGIN CERTIFICATE----` e `----END CERTIFICATE----` em sua seleção.



5. Selecione **Guardar**.

   Todas as futuras mensagens AutoSupport semanais, acionadas por eventos e acionadas pelo usuário serão enviadas para o destino adicional.

Acione manualmente uma mensagem AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente uma mensagem AutoSupport a ser enviada.

Antes de começar

- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT** > **Tools** > **AutoSupport**.
2. Na guia **Configurações**, selecione **Enviar AutoSupport acionado pelo usuário**.

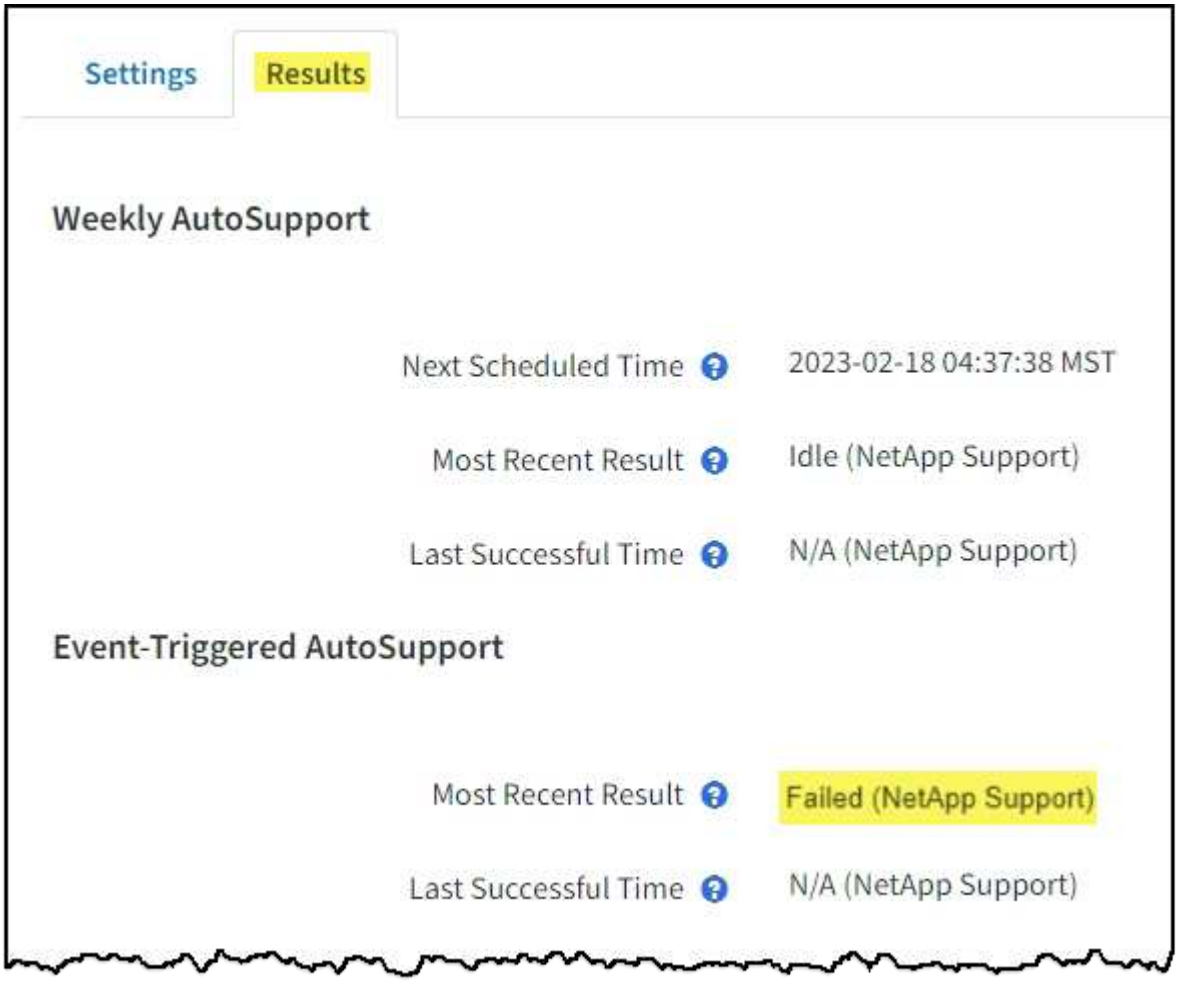
   O StorageGRID tenta enviar uma mensagem do AutoSupport para o suporte técnico. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar a mensagem AutoSupport novamente.

Depois de enviar uma mensagem AutoSupport acionada pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Solucionar problemas de mensagens do AutoSupport

Se uma tentativa de enviar uma mensagem AutoSupport falhar, o sistema StorageGRID executa ações diferentes dependendo do tipo de mensagem AutoSupport. Pode verificar o estado das mensagens do AutoSupport selecionando **SUPPORT** > **Tools** > **AutoSupport** > **results**.

Quando a mensagem AutoSupport não é enviada, "'Falha'" aparece na guia **resultados** da página **AutoSupport**.



Se você configurou um servidor proxy para encaminhar mensagens do AutoSupport para o NetApp, você deve "verifique se as configurações do servidor proxy estão corretas".

Falha semanal da mensagem AutoSupport

Se uma mensagem AutoSupport semanal não for enviada, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo de resultado mais recente para tentar novamente.

2. Tenta reenviar a mensagem AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas de envio, atualiza o atributo de resultado mais recente para Falha.
4. Tenta enviar uma mensagem AutoSupport novamente na próxima hora programada.
5. Mantém a programação regular do AutoSupport se a mensagem falhar porque o serviço NMS não está disponível e se uma mensagem for enviada antes de sete dias passar.
6. Quando o serviço NMS estiver disponível novamente, envia uma mensagem AutoSupport imediatamente se uma mensagem não tiver sido enviada por sete dias ou mais.

Falha de mensagem AutoSupport acionada pelo usuário ou por evento

Se uma mensagem AutoSupport acionada pelo usuário ou por um evento não for enviada, 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 corretas de e-mail, o seguinte erro é exibido: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tenta enviar a mensagem novamente.
3. Regista o erro no `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 servidor de e-mail está em execução (**SUPPORT** > **Alarmes (legacy)** > **> Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda a "configure as definições do servidor de correio eletrónico".

Corrija uma falha de mensagem do AutoSupport

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 servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envie mensagens AutoSupport do e-Series através do StorageGRID

Você pode enviar mensagens 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 storage.

```
https://docs.netapp.com/us-en/e-series-santricity/sm-support/autosupport-feature-overview.html["AutoSupport de hardware e-Series"^]Consulte para obter mais informações sobre como usar o AutoSupport com dispositivos e-Series.
```

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de administrador do Storage Appliance ou a permissão de acesso à raiz.
- Você configurou o SANtricity AutoSupport:
  - Para aparelhos SG6000 e SG5700, "Configure o AutoSupport no Gerenciador de sistemas do SANtricity"

> Você deve ter o firmware SANtricity 8,70 ou superior para acessar o Gerenciador de sistema do SANtricity usando o Gerenciador de Grade.

Sobre esta tarefa

As mensagens AutoSupport do e-Series contêm detalhes do hardware de armazenamento e são mais específicas do que outras mensagens AutoSupport enviadas pelo sistema StorageGRID.

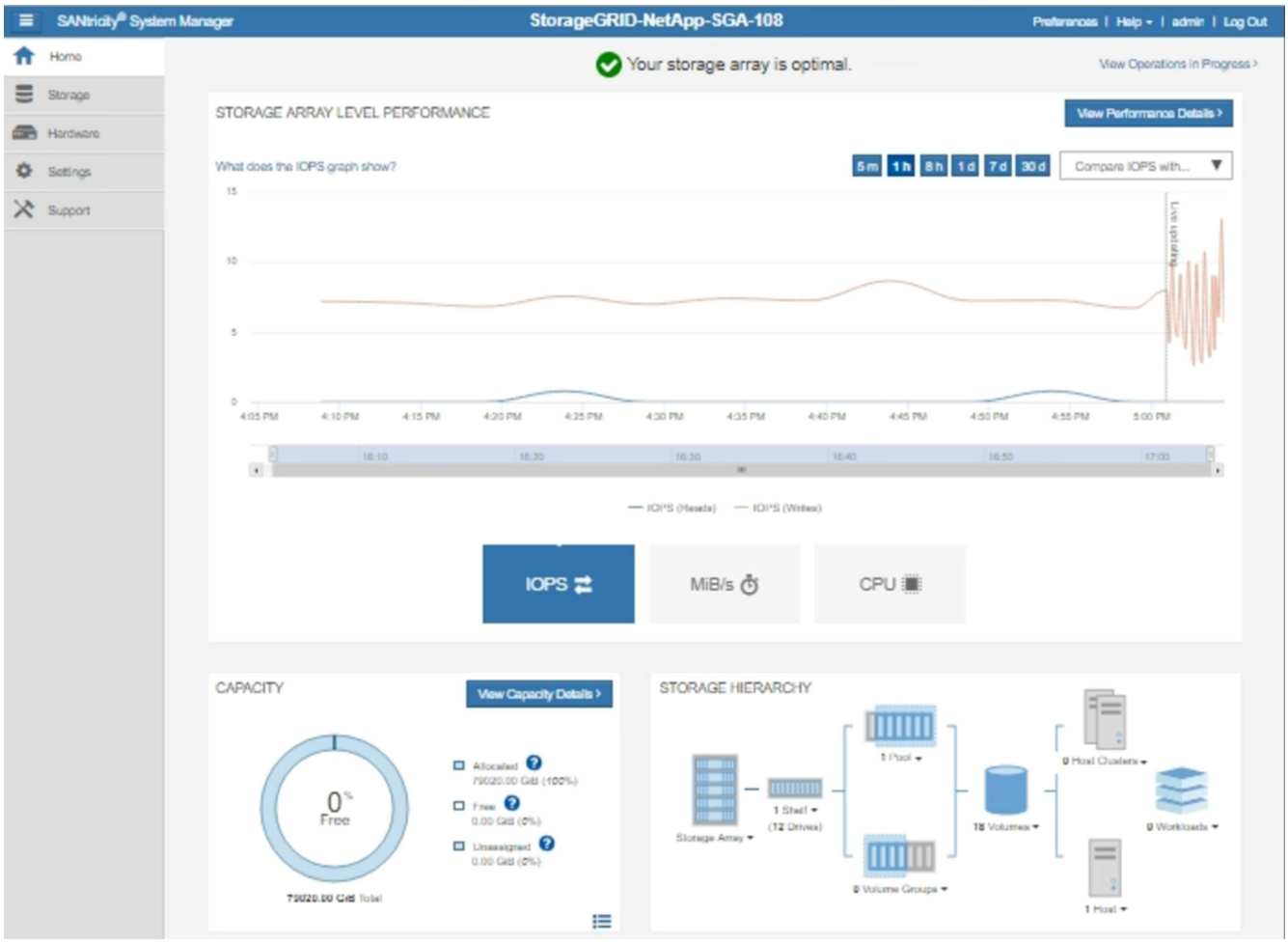
Você pode configurar um endereço de servidor proxy especial no Gerenciador de sistema do SANtricity para transmitir mensagens do AutoSupport por meio de um nó de administração do StorageGRID sem o uso da porta de gerenciamento do dispositivo. As mensagens AutoSupport transmitidas desta forma são enviadas pelo "Nó Admin. Remetente preferido", e usam qualquer "Configurações de proxy de administrador" uma que tenha sido configurada no Gerenciador de Grade.

> Este procedimento destina-se apenas à configuração de um servidor proxy StorageGRID para mensagens AutoSupport e-Series. Para obter detalhes adicionais sobre a configuração do e-Series AutoSupport, consulte "Documentação do NetApp e-Series e do SANtricity".

Passos

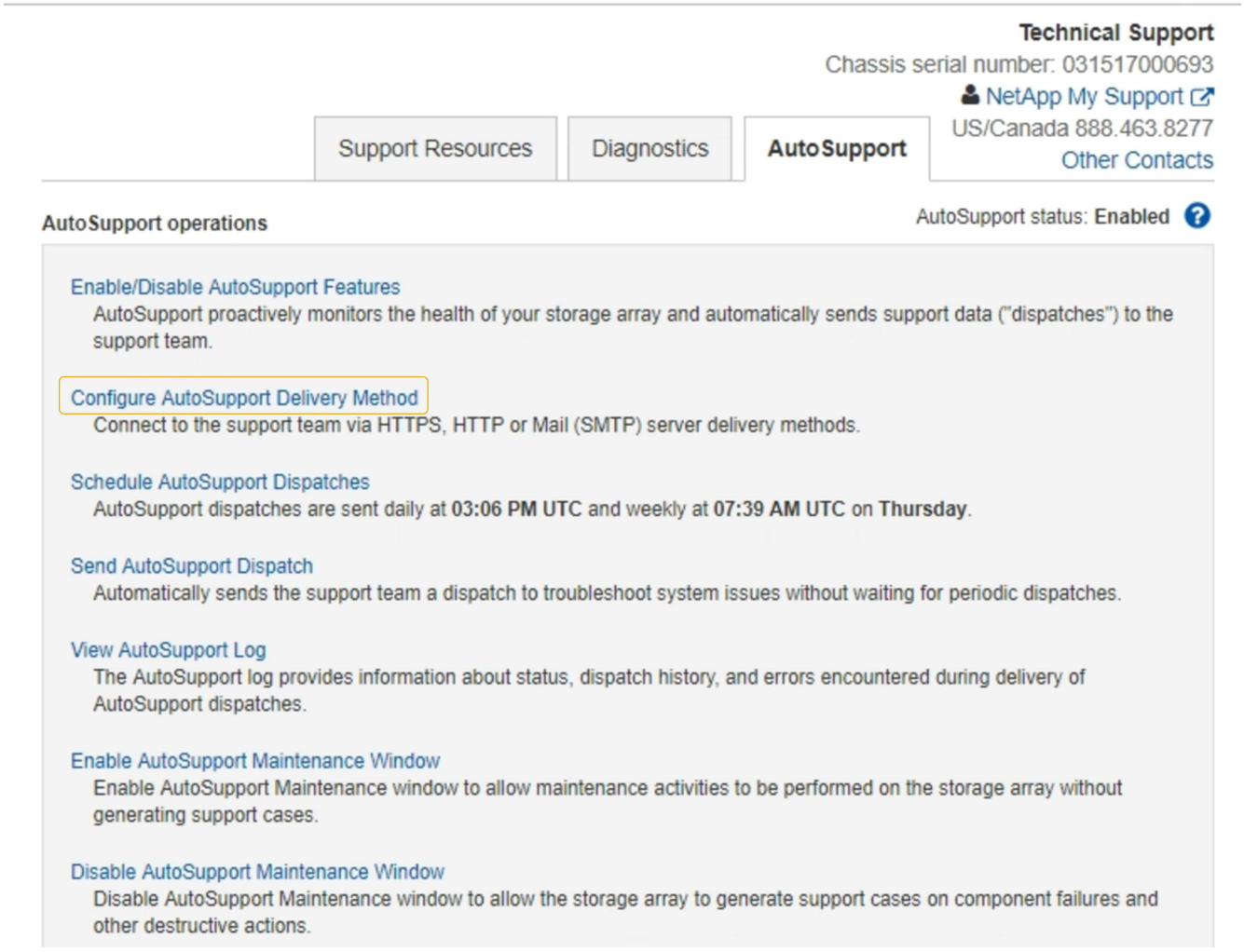
1. No Gerenciador de Grade, selecione **NÓS**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de storage que deseja configurar.
3. Selecione **Gerenciador do sistema SANtricity**.

   É apresentada a página inicial do Gestor do sistema SANtricity.



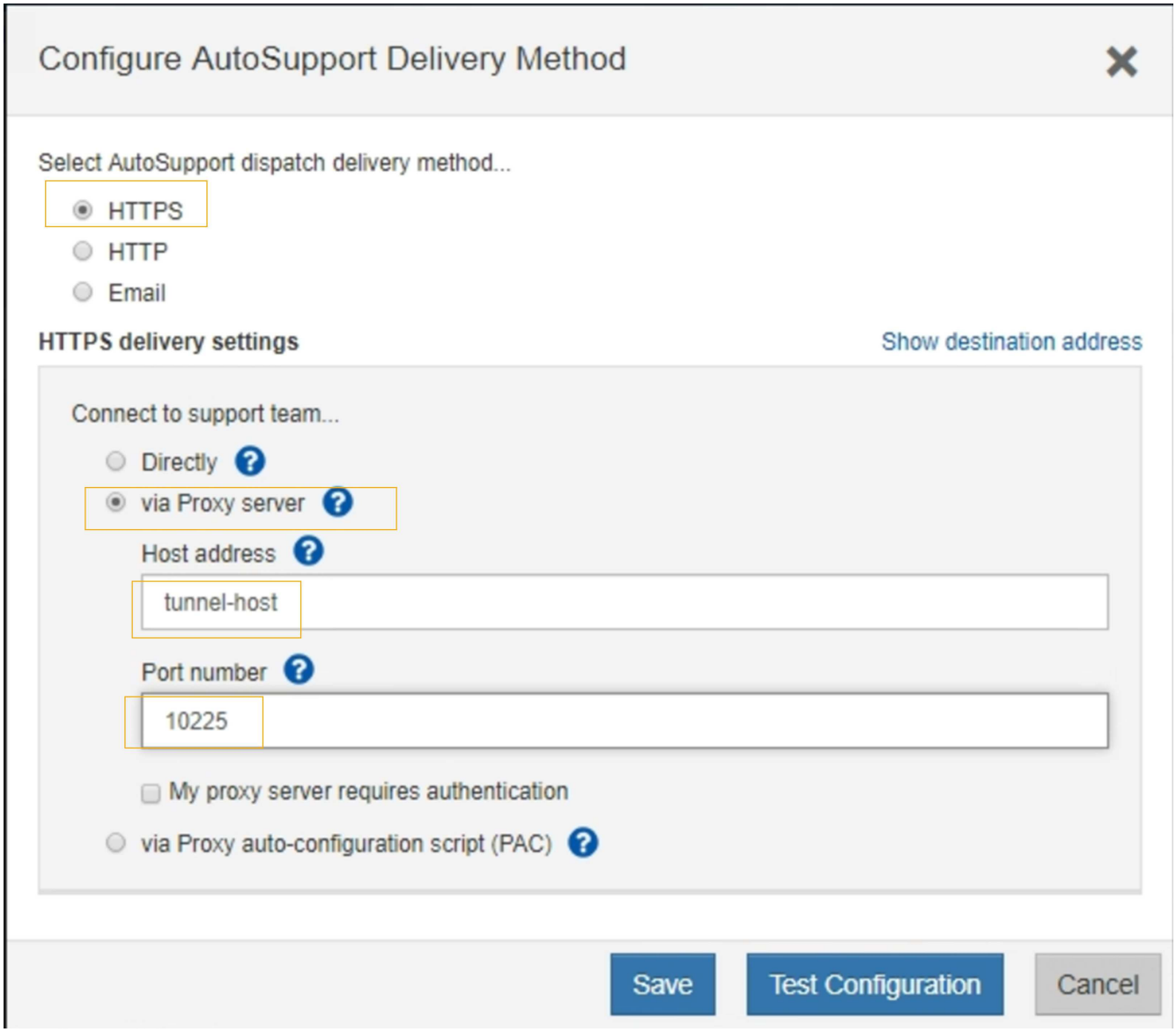
4. Selecione **SUPPORT** > **SUPPORT Center** > **AutoSupport**.

   É apresentada a página operations (operações de AutoSupport).



5. Selecione **Configurar método de entrega AutoSupport**.

   A página Configurar método de entrega AutoSupport é exibida.



6. Selecione **HTTPS** para o método de entrega.

   O certificado que ativa o HTTPS está pré-instalado.

7. Selecione **via servidor Proxy**.
8. Introduza `tunnel-host` o **Endereço anfitrião**.

   `tunnel-host` É o endereço especial para usar um nó de administrador para enviar mensagens AutoSupport da série e.

9. Introduza `10225` o **número da porta**.

   `10225` É o número da porta no servidor proxy StorageGRID que recebe mensagens AutoSupport do controlador e-Series no dispositivo.

10. Selecione **Configuração de teste** para testar o roteamento e a configuração do servidor proxy AutoSupport.

    Se estiver correto, uma mensagem em um banner verde será exibida: ""sua configuração do AutoSupport

foi verificada."

Se o teste falhar, uma mensagem de erro será exibida em um banner vermelho. Verifique as configurações de DNS e a rede do StorageGRID, verifique se o "Nó Admin. Remetente preferido" pode se conetar ao site de suporte da NetApp e tente o teste novamente.

11. Selecione **Guardar**.

    A configuração é salva e uma mensagem de confirmação aparece: ""o método de entrega AutoSupport foi configurado."

Gerenciar nós de storage

Gerenciar nós de storage: Visão geral

Os nós de storage fornecem capacidade e serviços de storage em disco. O gerenciamento de nós de storage implica o seguinte:

- Gerenciamento de opções de armazenamento
- Compreender quais são as marcas d'água do volume de storage 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
- Configuração de configurações globais para objetos armazenados
- Aplicando as configurações do nó de armazenamento
- Gerenciamento de nós de storage completos

O que é um nó de storage?

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Cada sistema StorageGRID precisa ter pelo menos três nós de storage. Se você tiver vários locais, cada local no sistema StorageGRID também precisará ter três nós de storage.

Um nó de armazenamento inclui os serviços e processos necessários para armazenar, mover, verificar e recuperar dados de objetos e metadados no disco. Você pode exibir informações detalhadas sobre os nós de storage na página **NÓS**.

O que é o serviço ADC?

O serviço controlador de domínio administrativo (ADC) autentica os nós de grade e suas conexões entre si. O serviço ADC é hospedado em cada um dos três primeiros nós de storage em um local.

O serviço ADC mantém informações de topologia, incluindo a localização e disponibilidade dos serviços. Quando um nó de grade requer informações de outro nó de grade ou uma ação a ser executada por outro nó de grade, ele entra em Contato com um serviço ADC para encontrar o melhor nó de grade para processar sua solicitação. Além disso, o serviço ADC retém uma cópia dos pacotes de configuração da implantação do StorageGRID, permitindo que qualquer nó de grade recupere informações de configuração atuais.você pode visualizar informações ADC para um nó de armazenamento na página topologia de Grade (**SUPPORT** > **Grid topology**).

Para facilitar operações distribuídas e desembarcadas, cada serviço ADC sincroniza certificados, pacotes de

configuração e informações sobre serviços e topologia com os outros serviços ADC no sistema StorageGRID.

Em geral, todos os nós de grade mantêm uma conexão com pelo menos um serviço ADC. Isso garante que os nós de grade estejam sempre acessando as informações mais recentes. Quando os nós de grade se conetam, eles armazenam em cache certificados de outros nós de grade, permitindo que os sistemas continuem funcionando com nós de grade conhecidos, mesmo quando um serviço ADC não está disponível. Novos nós de grade só podem estabelecer conexões usando um serviço ADC.

A conexão de cada nó de grade permite que o serviço ADC colete informações de topologia. Essas informações de nó de grade incluem a carga da CPU, o espaço disponível em disco (se ele tiver armazenamento), os serviços suportados e o ID do site do nó de grade. Outros serviços pedem ao serviço ADC informações de topologia por meio de consultas de topologia. O serviço ADC responde a cada consulta com as informações mais recentes recebidas do sistema StorageGRID.

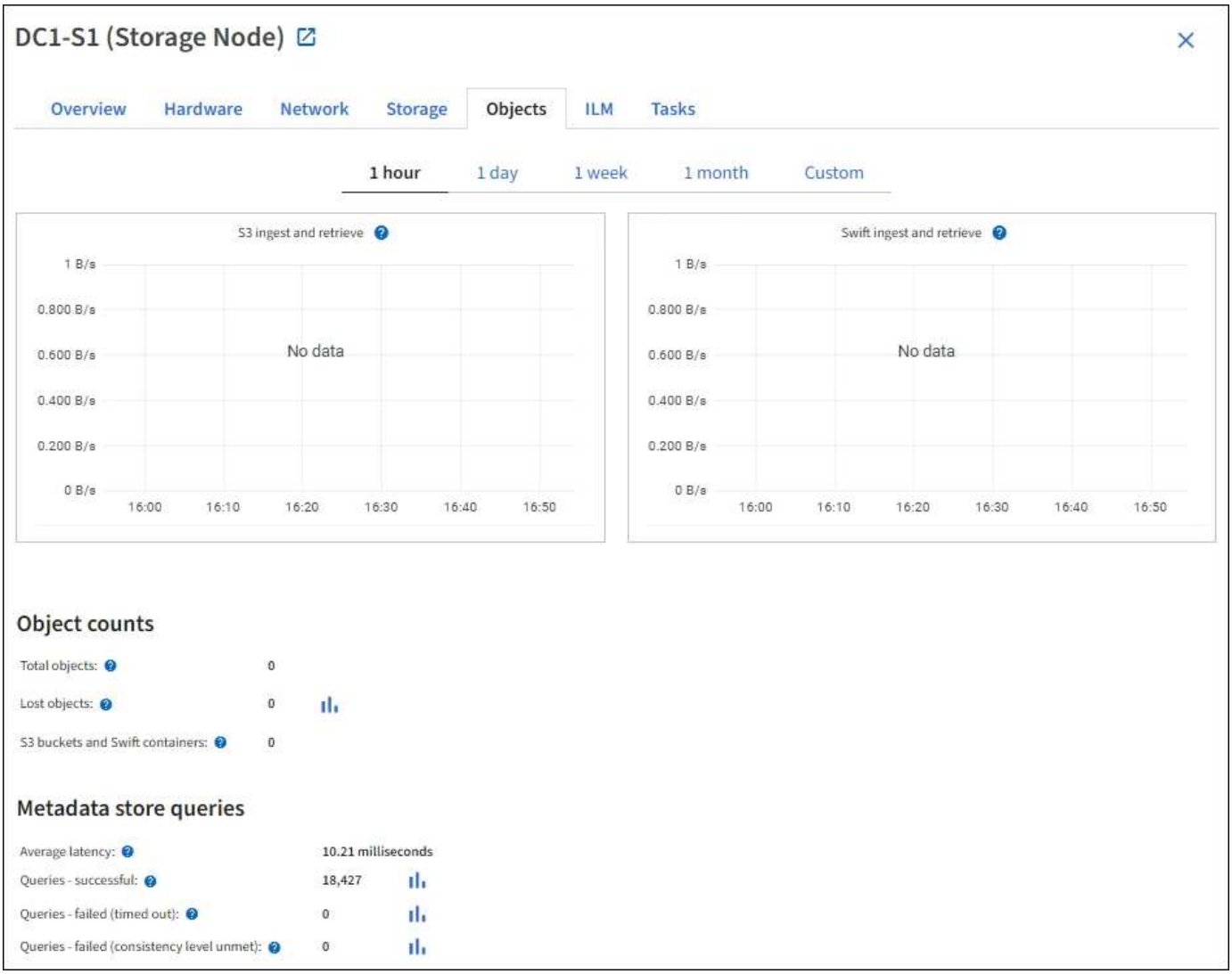
O que é o serviço DDS?

Hospedado por um nó de armazenamento, o serviço armazenamento de dados distribuído (DDS) faz interface com o banco de dados Cassandra para executar tarefas em segundo plano nos metadados de objetos armazenados no sistema StorageGRID.

Contagens de objetos

O serviço DDS rastreia o número total de objetos ingeridos no sistema StorageGRID, bem como o número total de objetos ingeridos através de cada uma das interfaces suportadas do sistema (S3 ou Swift).

Você pode ver a contagem total de objetos na página nós > guia objetos para qualquer nó de storage.



Consultas

Você pode identificar o tempo médio que leva para executar uma consulta contra o armazenamento de metadados através do serviço DDS específico, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode querer revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, Cassandra, que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é realizada através do serviço DDS específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "Execute o diagnóstico"Consulte .

Garantias de consistência e controles

O StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer operação GET após uma operação PUT concluída com êxito poderá ler os dados recém-gravados. As

substituições de objetos existentes, atualizações de metadados e exclusões permanecem, eventualmente, consistentes.

O que é o serviço LDR?

Hospedado por cada nó de armazenamento, o serviço de roteador de distribuição local (LDR) lida com o transporte de conteúdo para o sistema StorageGRID. O transporte de conteúdo abrange muitas tarefas, incluindo armazenamento de dados, roteamento e manuseio de solicitações. O serviço LDR faz a maior parte do trabalho árduo do sistema StorageGRID, manipulando cargas de transferência de dados e funções de tráfego de dados.

O serviço LDR lida com as seguintes tarefas:

- Consultas
- Atividade de gerenciamento do ciclo de vida das informações (ILM)
- Exclusão de objeto
- Storage de dados de objetos
- Transferências de dados de objeto de outro serviço LDR (Storage Node)
- Gerenciamento de storage de dados
- Interfaces de protocolo (S3 e Swift)

O serviço LDR também gerencia o mapeamento de objetos S3 e Swift para os "manipuladores de conteúdo" exclusivos que o sistema StorageGRID atribui a cada objeto ingerido.

Consultas

As consultas LDR incluem consultas para localização de objetos durante operações de recuperação e arquivamento. Você pode identificar o tempo médio que leva para executar uma consulta, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, o que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é executada através do serviço LDR específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "Execute o diagnóstico"Consulte .

Atividade ILM

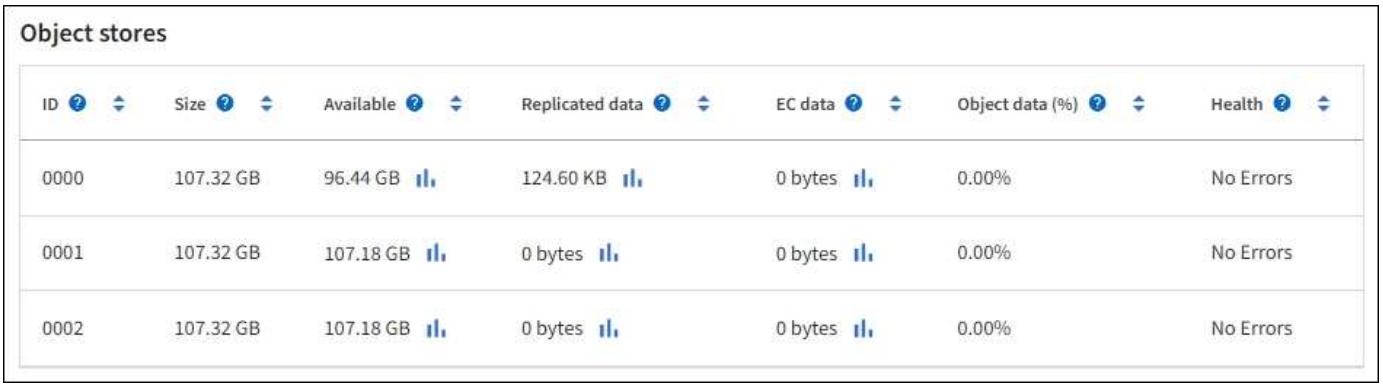
As métricas de gerenciamento do ciclo de vida das informações (ILM) permitem monitorar a taxa na qual os objetos são avaliados para a implementação do ILM. Você pode visualizar essas métricas no painel ou em **NÓS** > ***Storage Node*** > **ILM**.

Armazenamentos de objetos

O armazenamento de dados subjacente de um serviço LDR é dividido em um número fixo de armazenamentos de objetos (também conhecidos como volumes de armazenamento). Cada armazenamento

de objetos é um ponto de montagem separado.

Você pode ver os armazenamentos de objetos para um nó de storage na página nós > guia armazenamento.



Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Os armazenamentos de objetos em um nó de armazenamento são identificados por um número hexadecimal de 0000 a 002F, que é conhecido como ID de volume. O espaço é reservado no primeiro armazenamento de objetos (volume 0) para metadados de objetos em um banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objeto. Todos os outros armazenamentos de objetos são usados exclusivamente para dados de objetos, o que inclui cópias replicadas e fragmentos codificados por apagamento.

Para garantir até mesmo o uso de espaço para cópias replicadas, os dados de objeto de um determinado objeto são armazenados em um armazenamento de objetos com base no espaço de storage disponível. Quando um ou mais objetos armazenam preenchimento até a capacidade, os armazenamentos de objetos restantes continuam armazenando objetos até que não haja mais espaço no nó de armazenamento.

Proteção de metadados

Metadados de objeto são informações relacionadas ou uma descrição de um objeto; por exemplo, tempo de modificação de objeto ou local de armazenamento. O StorageGRID armazena metadados de objetos em um banco de dados Cassandra, que faz interface com o serviço LDR.

Para garantir redundância e, portanto, proteção contra perda, três cópias dos metadados de objetos são mantidas em cada local. Esta replicação não é configurável e executada automaticamente.

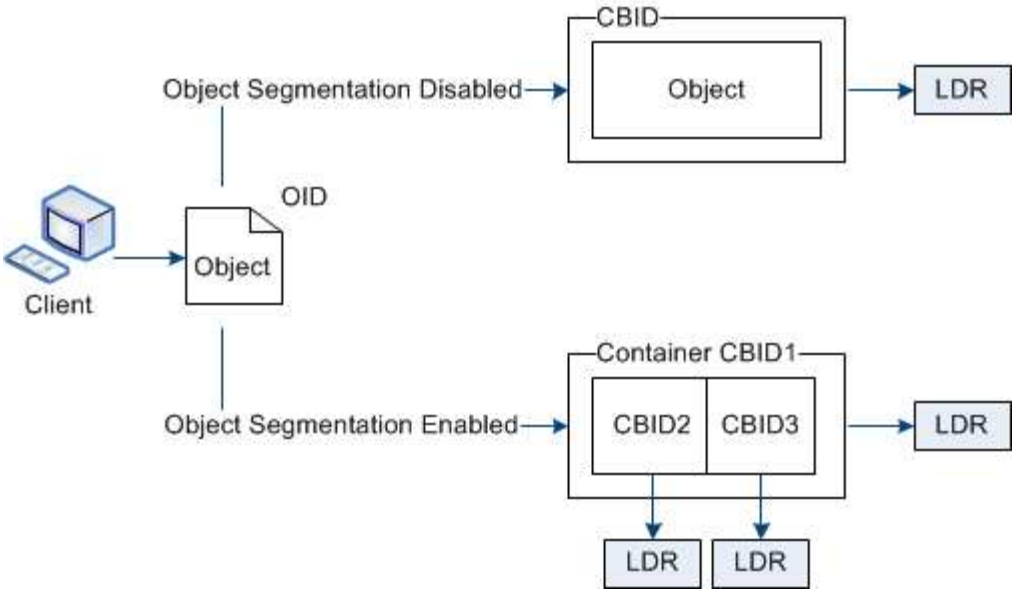
"Gerenciar o storage de metadados de objetos"

Use as opções de armazenamento

O que é segmentação de objetos?

A 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 de várias partes 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 contentor de segmento que lista as informações do cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contentor de segmento, o serviço LDR monta o objeto original de seus segmentos e retorna o objeto ao cliente.

O contentor e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contentor e os segmentos podem ser armazenados em qualquer nó de armazenamento dentro do conjunto 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 de objetos gerenciados aumentará em três após a ingestão ser concluída, da seguinte forma:

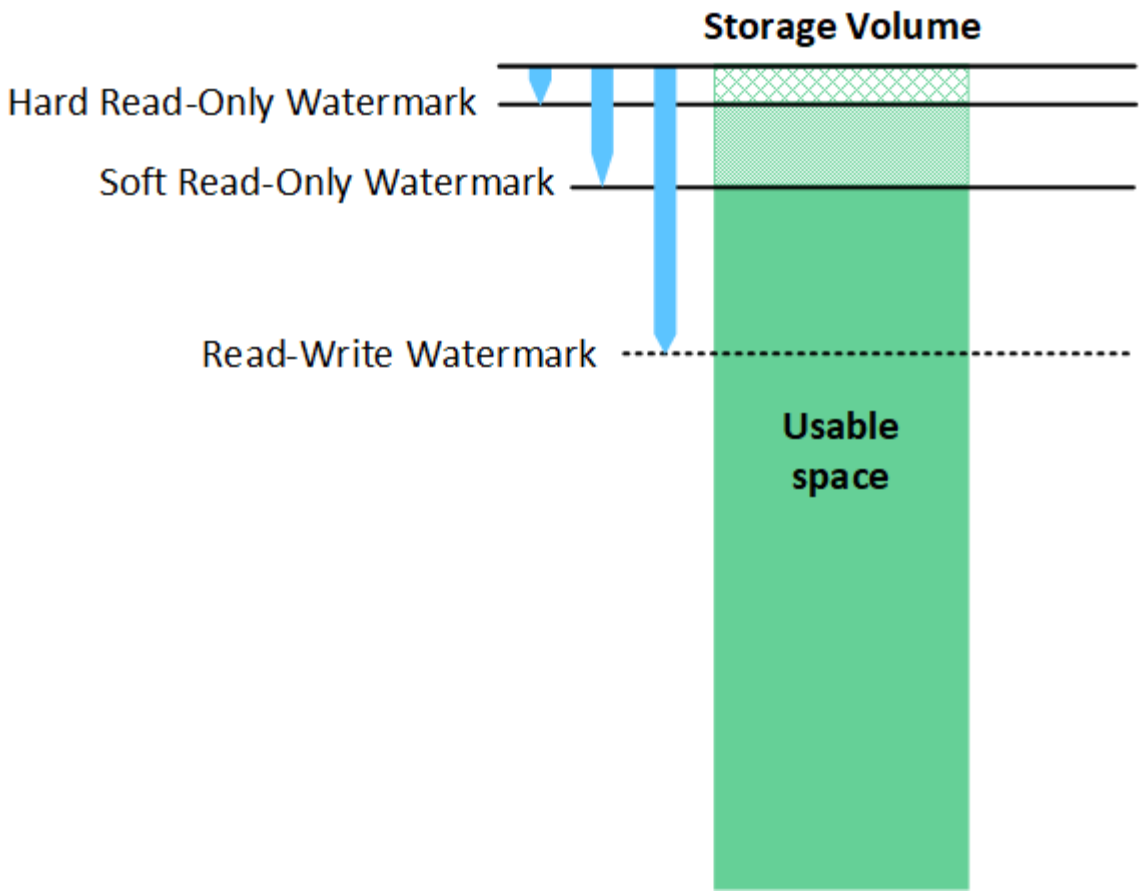
```
segment container + segment 1 + segment 2 = three stored objects
```

Você pode melhorar o desempenho ao lidar com objetos grandes, garantindo que:

- Cada Gateway e nó de armazenamento tem largura de banda de rede suficiente para a taxa de transferência necessária. Por exemplo, configure redes Grid e Client separadas em interfaces Ethernet de 10 Gbps.
- Nós de Gateway e storage suficientes são implantados para a taxa de transferência necessária.
- Cada nó de storage tem desempenho de e/S de disco suficiente para a taxa de transferência necessária.

O que são marcas d'água de volume de armazenamento?

O StorageGRID usa três marcas d'água de volume de storage para garantir que os nós de storage sejam transferidos com segurança para um estado somente leitura antes que eles sejam executados com muito pouco espaço e para permitir que os nós de storage que foram transferidos para um estado somente leitura sejam novamente lidos.



As marcas d'água do volume de armazenamento aplicam-se apenas ao espaço utilizado para dados de objetos replicados e codificados por apagamento. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, vá para "Gerenciar o storage de metadados de objetos".

O que é o Soft Read-Only Watermark?

O **Storage volume Soft Read-Only Watermark** é a primeira marca d'água a indicar que o espaço utilizável de um nó de armazenamento para dados de objetos está se tornando cheio.

Se cada volume em um nó de armazenamento tiver menos espaço livre do que o Watermark Soft Read-Only desse volume, o nó de armazenamento muda para *read-only mode*. O modo somente leitura significa que o nó de storage anuncia serviços somente leitura para o resto 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 de água somente leitura suave de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o nó de armazenamento passa para o modo somente leitura suave.

O que é a marca d'água Hard Read-Only?

O **Storage volume Hard Read-Only Watermark** é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio.

Se o espaço livre em um volume for menor do que a marca de água Hard Read-Only desse volume, as gravações no volume falharão. As gravações em outros volumes podem continuar, no entanto, até que o espaço livre nesses volumes seja menor do que suas marcas de água somente leitura dura.

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 aceita mais nenhuma solicitação de gravação.

A marca d'água Hard Read-Only é sempre inferior à marca d'água Soft Read-Only.

O que é a marca d'água Read-Write?

O **marca d'água de leitura e gravação de volume de armazenamento** aplica-se apenas a nós de armazenamento que tenham feito 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 é maior do que a marca de água de leitura e gravação desse volume, o nó automaticamente faz a transição de volta para o estado de leitura e gravação.

Por exemplo, suponha que o nó de armazenamento tenha sido transferido para o modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura-escrita de 30 GB. Assim que o espaço livre para qualquer volume aumentar para 30 GB, o nó torna-se leitura-gravação novamente.

A marca d'água de leitura-escrita é sempre maior do que a marca d'água Soft Read-Only e a marca d'água Hard Read-Only.

Ver marcas de água do volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados pelo sistema. Se não estiverem a ser utilizadas marcas de água otimizadas, pode determinar se pode ou deve ajustar as definições.

Antes de começar

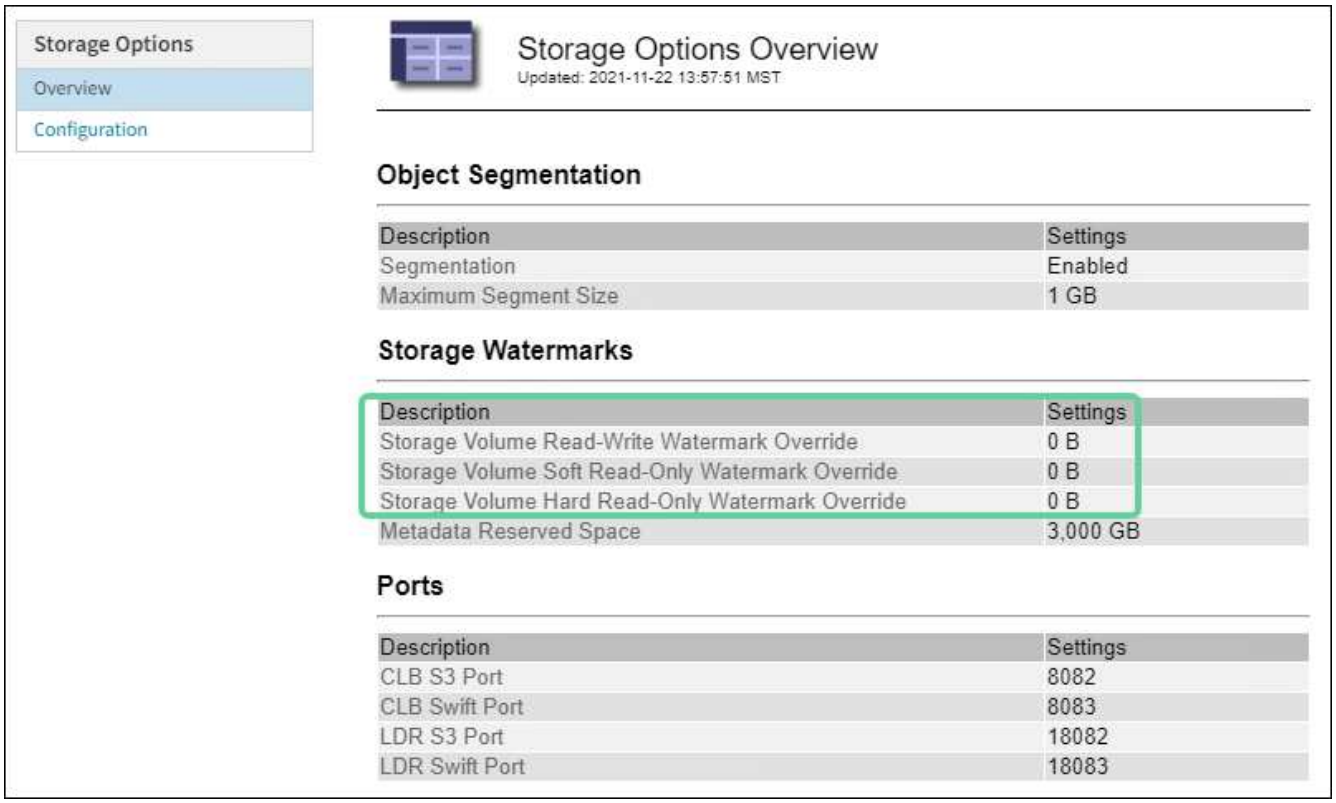
- Concluiu a atualização para o StorageGRID 11,6 ou superior.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem a permissão de acesso root.

Ver as definições atuais da marca d'água

Você pode exibir as configurações atuais de marca d'água de armazenamento no Gerenciador de Grade.

Passos

1. Selecione **CONFIGURATION** > **System** > **Storage options**.
2. Na seção marcas d'água de armazenamento, observe as configurações para as três substituições de marca d'água de volume de armazenamento.



- Se as substituições da marca d'água forem **0**, todas as três marcas d'água são 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. Você não deve atualizar esses valores. Conforme necessário, você pode opcionalmente Ver marcas de água de armazenamento otimizadas.

- Se as substituições da marca d'água forem valores não 0, marcas d'água personalizadas (não otimizadas) estão sendo usadas. Não é recomendável usar configurações personalizadas de marca d'água. Use as instruções para "Solução de problemas de baixa substituição de marca d'água somente leitura alertas"determinar se você pode ou deve ajustar as configurações.

Ver marcas de água de armazenamento otimizadas

O StorageGRID usa duas métricas Prometheus para mostrar os valores otimizados que calculou para a marca d'água **volume de armazenamento Soft Read-Only**. Você pode visualizar os valores otimizados mínimo e máximo para cada nó de storage em sua grade.

1. Selecione **SUPPORT** > **Tools** > **Metrics**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário Prometheus.
3. Para ver a marca d'água mínima de leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor mínimo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para o **Storage volume Soft Read-Only Watermark**, o alerta **Low read-only Watermark** (Sobreposição de marca d'água somente leitura baixa) será acionado para o Storage Node.

4. Para ver a marca d'água somente leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor máximo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento.

Gerenciar o storage 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 os metadados de objetos.

O que é metadados de objetos?

Metadados de objetos são qualquer informação que descreva 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.

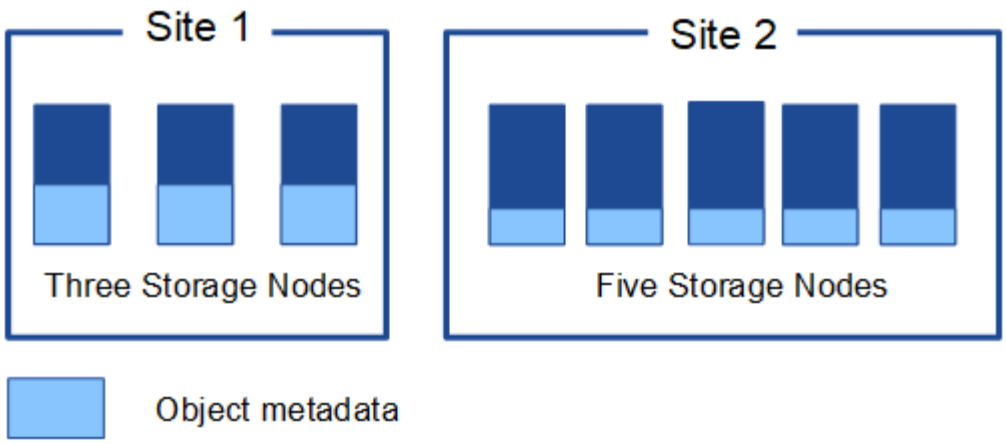
Para um objeto no StorageGRID, os metadados de objeto incluem os seguintes tipos de informações:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3 ou do contentor Swift, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.
- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
- Para cópias de objetos replicadas, o local de storage atual de cada cópia.
- Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, 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 de objetos são armazenados?

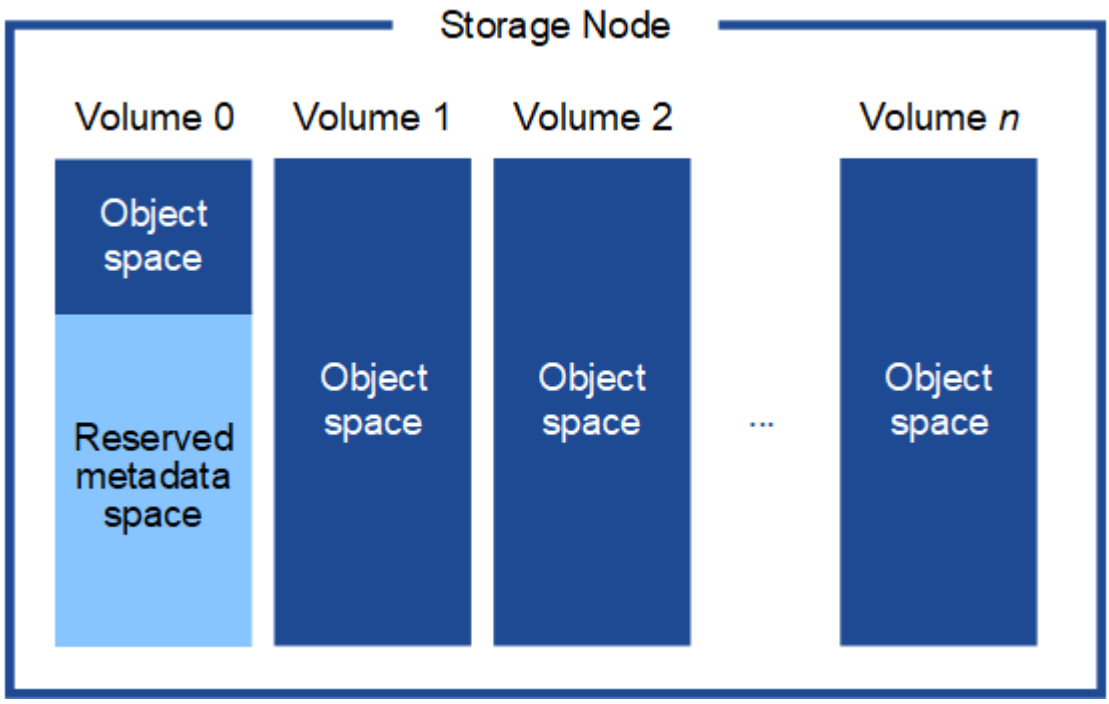
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local.

Essa figura representa os nós de storage em dois locais. Cada local tem a mesma quantidade de metadados de objetos, e os metadados de cada local são subdivididos entre todos os nós de storage nesse local.



Onde os metadados de objetos são armazenados?

Essa figura representa os volumes de storage de um único nó de storage.



Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Ele usa o espaço reservado para armazenar metadados de objetos e executar operações essenciais de banco de dados. Qualquer espaço restante no volume de storage 0 e todos os outros volumes de storage no nó de storage são usados exclusivamente para dados de objetos (cópias replicadas e fragmentos codificados por apagamento).

A quantidade de espaço reservada para metadados de objetos em um nó de storage específico depende de vários fatores, os quais são descritos abaixo.

Definição de espaço reservado metadados

O *Metadata Reserved Space* é uma configuração em todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada nó de armazenamento. Como mostrado na tabela, o valor padrão dessa configuração é baseado em:

- A versão de software que você estava usando quando você instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

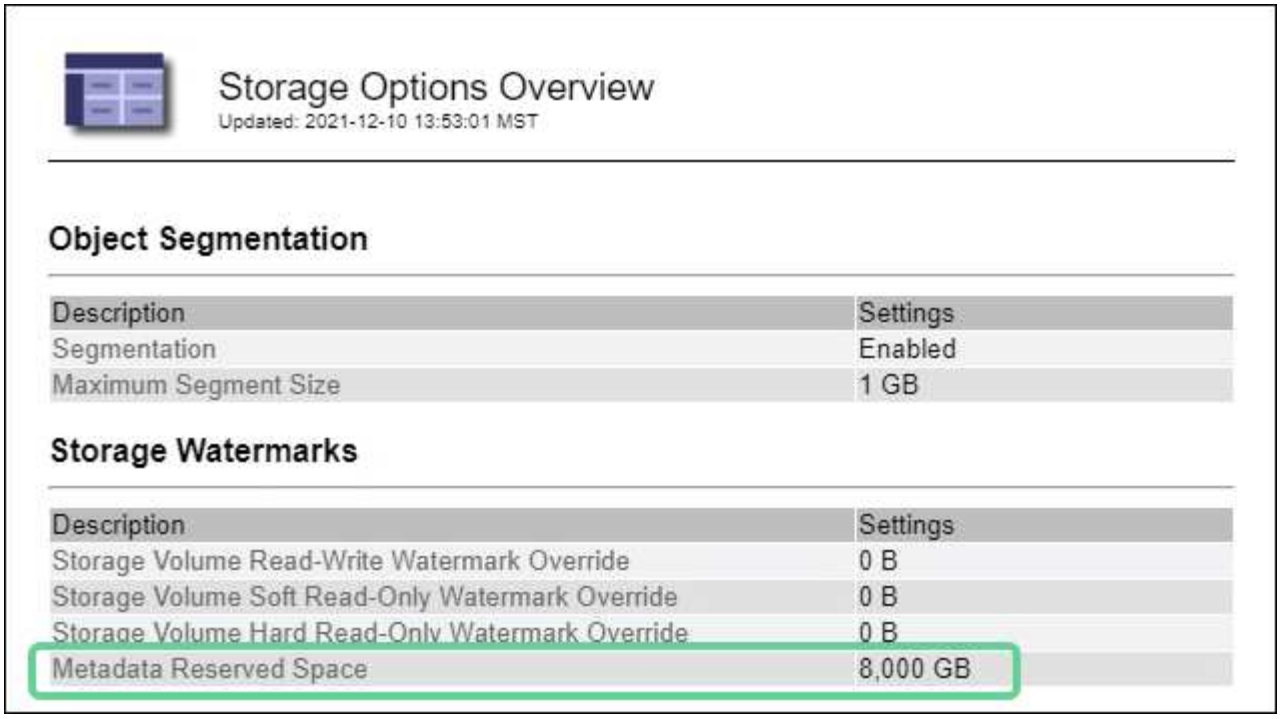
Versão utilizada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de storage	Predefinição Metadata Reserved Space
11,5 a 11,7	128 GB ou mais em cada nó de storage na grade	8 TB (8.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento na grade	3 TB (3.000 GB)
11,1 a 11,4	128 GB ou mais em cada nó de armazenamento em qualquer local	4 TB (4.000 GB)
	Menos de 128 GB em qualquer nó de storage em cada local	3 TB (3.000 GB)
11,0 ou anterior	Qualquer valor	2 TB (2.000 GB)

Exibir a configuração espaço reservado metadados

Siga estas etapas para visualizar a configuração espaço reservado metadados para o seu sistema StorageGRID.

Passos

1. Selecione **CONFIGURATION** > **System** > **Storage options**.
2. Na tabela Storage Watermarks (marcas de água de armazenamento), localize **Metadata Reserved Space** (espaço reservado de metadados).



Na captura de tela, o valor **espaço reservado de metadados** é de 8.000 GB (8 TB). Esta é 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.

Espaço reservado real para metadados

Em contraste com a configuração espaço reservado de metadados em todo o sistema, o *espaço reservado real* para metadados de objetos 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 **espaço reservado de metadados** em todo o sistema.

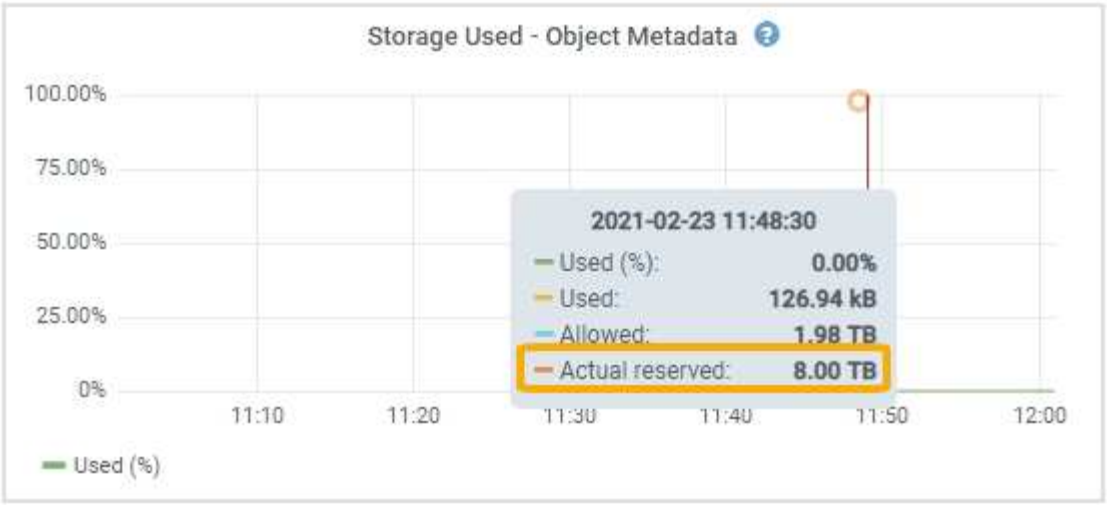
Tamanho do volume 0 para o nó	Espaço reservado real para metadados
Menos de 500 GB (uso não produção)	10% do volume 0
500 GB ou mais	O menor desses valores: • Volume 0 • Definição de espaço reservado metadados

Veja o espaço reservado real para metadados

Siga estas etapas para exibir o espaço reservado real para metadados em um nó de armazenamento específico.

Passos

1. No Gerenciador de Grade, selecione **NÓS** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Posicione o cursor sobre o gráfico armazenamento usado - metadados de objetos e localize o valor **Real reservado**.



Na captura de tela, o valor **atual reservado** é de 8 TB. Esta captura de tela é para um nó de armazenamento grande em uma nova instalação do StorageGRID 11,6. Como a configuração 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 espaço reservado de metadados.

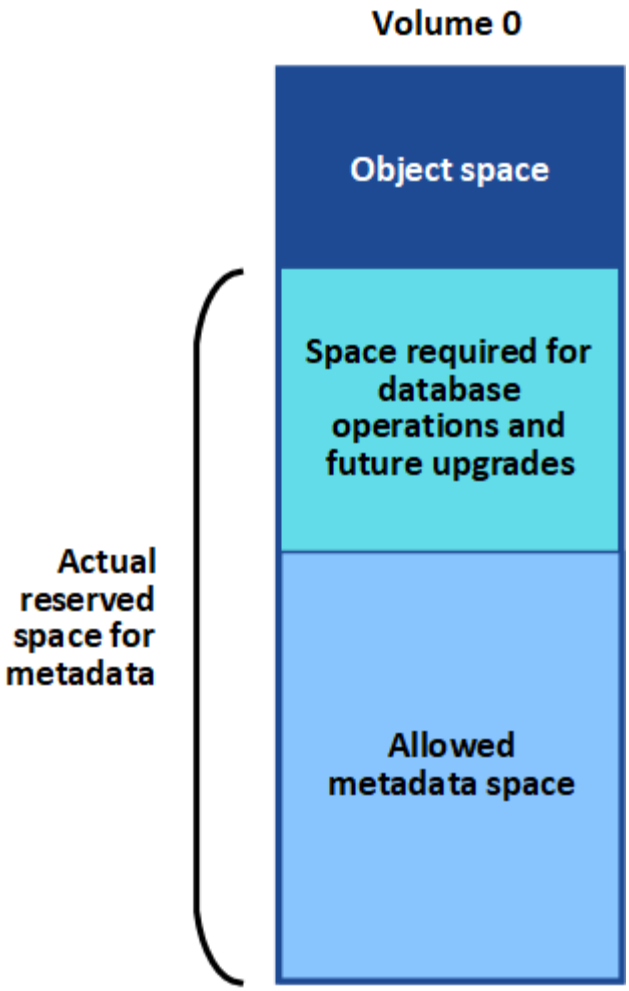
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11,7. Para este exemplo, suponha que cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **Metadata Reserved Space** em todo o sistema está definido para 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 reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)

Espaço de metadados permitido

O espaço reservado real de cada nó de storage para metadados é subdividido no espaço disponível para metadados de objetos (o espaço de metadados permitido_) e no espaço necessário para operações essenciais de banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço de metadados permitido rege 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 reservado real para metadados.

		Quantidade de memória no nó de armazenamento	
	≪ 128 GB	≫ 128 GB	**Espaço reservado real para metadados**
≪ 4 TB	60% do espaço reservado real para metadados, até um máximo de 1,32 TB	60% do espaço reservado real para metadados, até um máximo de 1,98 TB	≫ 4 TB

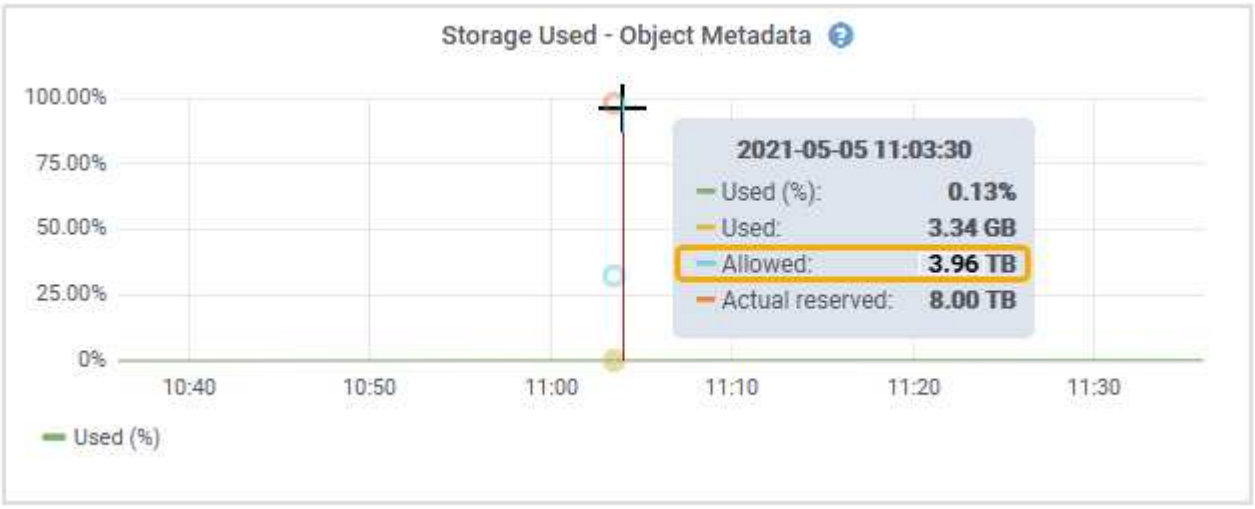
Exibir espaço permitido de metadados

Siga estas etapas para exibir o espaço de metadados permitido para um nó de armazenamento.

Passos

1. No Gerenciador de Grade, selecione **NÓS**.

2. Selecione o nó de armazenamento.
3. Selecione a guia **armazenamento**.
4. Posicione o cursor sobre o gráfico armazenamento usado - metadados de objetos e localize o valor **permitido**.



Na captura de tela, o valor **permitido** é de 3,96 TB, que é o valor máximo para um nó de armazenamento cujo espaço reservado real para metadados é superior a 4 TB.

O valor **allowed** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemplo de espaço permitido de metadados

Suponha que você instale um sistema StorageGRID usando a versão 11,6. Para este exemplo, suponha que cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **Metadata Reserved Space** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11,6 ou superior quando cada nó de armazenamento tem mais de 128 GB de RAM.)
- O espaço reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado no tabela para espaço permitido para metadados: (espaço reservado real para metadados - 1 TB) x 60%, até um máximo de 3,96 TB.

Como os nós de storage de diferentes tamanhos afetam a capacidade do objeto

Como descrito acima, o StorageGRID distribui uniformemente os metadados de objetos nos nós de storage em cada local. Por esse motivo, se um site contiver nós de storage de tamanhos diferentes, o menor nó do local determinará a capacidade de metadados do local.

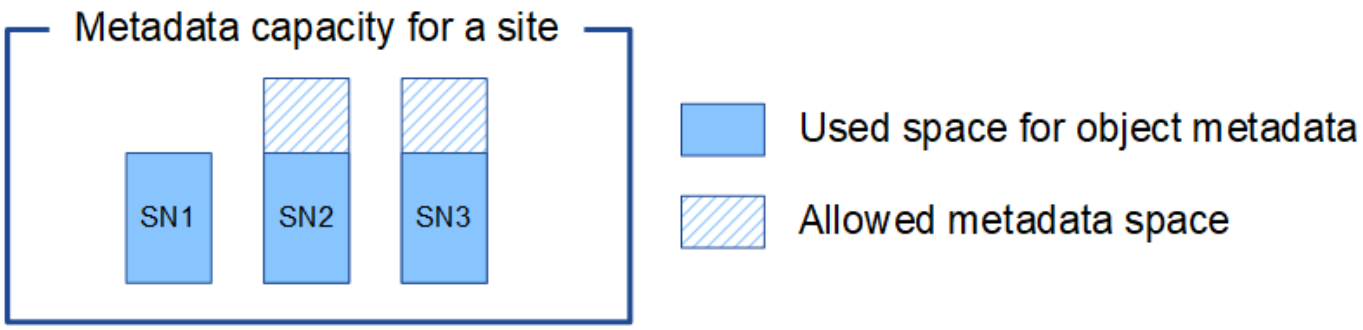
Considere o seguinte exemplo:

- Você tem uma grade de local único que contém três nós de storage de tamanhos diferentes.

- A configuração **Metadata Reserved Space** é de 4 TB.
- Os nós de storage têm os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de storage	Tamanho do volume 0	Espaço reservado real de metadados	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 de objetos são distribuídos uniformemente pelos nós de storage em um local, cada nó neste exemplo pode conter apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço permitido de metadados para SN2 e SN3 não podem ser usados.



Da mesma forma, como o StorageGRID mantém todos os metadados de objetos para um sistema StorageGRID em cada local, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objetos do menor local.

E como a capacidade de metadados de objetos 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 de objetos para cada nó de armazenamento, consulte as instruções para "Monitorização do StorageGRID".
- Para aumentar a capacidade dos metadados de objetos do seu sistema, "expanda sua grade"adicionando novos nós de storage.

Comprimir objetos armazenados

Você pode ativar a compactação de objetos para reduzir o tamanho dos objetos armazenados no StorageGRID, para que os objetos consumam menos storage.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Por padrão, a compactação de objetos está desativada. Se você ativar a compactação, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando a compactação sem perda.

> Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

Antes de ativar a compressão de objetos, tenha em atenção o seguinte:

- Você não deve selecionar **Compress Stored Objects** a menos que você saiba que os dados que estão sendo armazenados são compressíveis.
- Os 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 essa opção não reduzirá ainda mais o tamanho de um objeto.
- Não selecione **Compress Stored Objects** se você estiver usando o NetApp FabricPool com o StorageGRID.
- Se **Compress Stored Objects** estiver selecionado, os aplicativos cliente S3 e Swift devem evitar executar operações GET Object que especificam um intervalo de bytes serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB a partir de um objeto compactado de 50 GB.

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

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

Passos

1. Selecione **CONFIGURATION** > **System** > **Object Compression**.
2. Marque a caixa de seleção **Compress Stored Objects**.
3. Selecione **Guardar**.

Configurações do nó de storage

Cada nó de armazenamento usa várias configurações e contadores. Talvez seja necessário exibir as configurações atuais ou redefinir contadores para apagar alarmes (sistema legado).

> Exceto quando especificamente instruído na documentação, você deve consultar o suporte técnico antes de modificar qualquer configuração do nó de armazenamento. Conforme necessário, você pode redefinir contadores de eventos para limpar alarmes legados.

Siga estes passos para aceder às definições e contadores de configuração de um nó de armazenamento.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > ***Storage Node***.
3. Expanda o nó de armazenamento e selecione o serviço ou componente.

4. Selecione a guia **Configuração**.

As tabelas a seguir resumem as configurações do nó de armazenamento.

LDR

Nome do atributo	Código	Descrição
Estado HTTP	HSTE	O estado atual de HTTP para S3, Swift e outro tráfego interno de StorageGRID: • Offline: Não são permitidas operações e qualquer aplicativo cliente que tente abrir uma sessão HTTP para o serviço LDR recebe uma mensagem de erro. As sessões ativas estão graciosamente fechadas. • Online: A operação continua normalmente
Auto-Iniciar HTTP	HTAS	• Se selecionado, o estado do sistema ao reiniciar depende do estado do componente **LDR** > **Storage**. Se o componente **LDR** > **Storage** for somente leitura ao reiniciar, a interface HTTP também será somente leitura. Se o componente **LDR** > **Storage** estiver Online, o HTTP também estará Online. Caso contrário, a interface HTTP permanece no estado Offline. • Se não estiver selecionada, a interface HTTP permanece Offline até explicitamente ativada.

LDR > armazenamento de dados

Nome do atributo	Código	Descrição
Repor contagem de objetos perdidos	RCOR	Redefina o contador para o número de objetos perdidos neste serviço.

LDR > armazenamento

Nome do atributo	Código	Descrição
Estado de armazenamento — desejado	SSDS	Uma configuração configurável pelo usuário para o estado desejado do componente de armazenamento. O serviço LDR lê este valor e tenta corresponder ao estado indicado por este atributo. O valor é persistente entre as reinicializações. Por exemplo, você pode usar essa configuração para forçar o armazenamento a se tornar somente leitura, mesmo quando houver amplo espaço de armazenamento disponível. Isso pode ser útil para a solução de problemas. O atributo pode ter um dos seguintes valores: • Offline: Quando o estado desejado é Offline, o serviço LDR coloca o componente **LDR** > **Storage** offline. • Somente leitura: Quando o estado desejado é somente leitura, o serviço LDR move o estado de armazenamento para somente leitura e pára de aceitar novo conteúdo. Observe que o conteúdo pode continuar sendo salvo no nó de armazenamento por um curto período de tempo até que as sessões abertas sejam fechadas. • Online: Deixe o valor em Online durante as operações normais do sistema. O estado de armazenamento — a corrente do componente de armazenamento será definida dinamicamente pelo serviço com base na condição do serviço LDR, como a quantidade de espaço de armazenamento de objetos disponível. Se o espaço for baixo, o componente torna-se somente leitura.
Tempo limite de verificação de integridade	SHCT	O limite de tempo em segundos no qual um teste de verificação de integridade deve ser concluído para que um volume de armazenamento seja considerado saudável. Altere este valor apenas quando direcionado para o fazer pelo suporte.

LDR > Verificação

Nome do atributo	Código	Descrição
Repor contagem de objetos em falta	VCMI	Redefine a contagem de objetos perdidos detetados (OMIS). Use somente depois que a verificação existência do objeto for concluída. Os dados de objeto replicado em falta são restaurados automaticamente pelo sistema StorageGRID.

Nome do atributo	Código	Descrição
Taxa de verificação	VPRI	Defina a taxa em que a verificação de fundo ocorre. Consulte informações sobre como configurar a taxa de verificação em segundo plano.
Repor contagem de objetos corrompidos	VCCR	Redefina o contador para obter dados de objeto replicado corrompidos encontrados durante a verificação em segundo plano. Esta opção pode ser usada para limpar a condição de alarme objetos corrompidos detetados (OCOR).
Excluir objetos em quarentena	OQRT	Exclua objetos corrompidos do diretório de quarentena, redefina a contagem de objetos em quarentena para zero e limpe o alarme objetos em quarentena detetados (OQRT). Esta opção é usada depois que objetos corrompidos foram restaurados automaticamente pelo sistema StorageGRID. Se um alarme de objetos perdidos for acionado, o suporte técnico pode querer acessar os objetos em quarentena. Em alguns casos, objetos em quarentena podem ser úteis para a recuperação de dados ou para depurar os problemas subjacentes que causaram as cópias de objetos corrompidas.

LDR > codificação de apagamento

Nome do atributo	Código	Descrição
Repor gravações contagem de falhas	RSWF	Redefina o contador para falhas de gravação de dados de objetos codificados por apagamento no nó de storage.
A reinicialização lê a contagem de falhas	RSRF	Redefina o contador para falhas de leitura de dados de objetos codificados por apagamento a partir do nó de armazenamento.
A reposição elimina a contagem de falhas	RSDF	Redefina o contador para falhas de exclusão de dados de objetos codificados por apagamento do nó de storage.
Repor contagem de cópias corrompidas detetadas	RSCC	Redefina o contador para o número de cópias corrompidas de dados de objetos codificados por apagamento no nó de storage.
Repor a contagem de fragmentos corrompidos detetados	RSCD	Redefina o contador de fragmentos corrompidos de dados de objetos codificados por apagamento no nó de storage.

Nome do atributo	Código	Descrição
Repor contagem de fragmentos detetados em falta	RSMD	Redefina o contador de fragmentos ausentes de dados de objetos codificados por apagamento no nó de storage. Use somente depois que a verificação existência do objeto for concluída.

LDR > replicação

Nome do atributo	Código	Descrição
Repor contagem de falhas de replicação de entrada	RICR	Redefina o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicação de entrada — Falha).
Repor contagem de falhas de replicação efetuada	ROCR	Redefina o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed).
Desativar replicação de entrada	DSIR	Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal. Quando a replicação de entrada é desativada, os objetos podem ser recuperados do nó de armazenamento para cópia para outros locais no sistema StorageGRID, mas os objetos não podem ser copiados para este nó de armazenamento a partir de outros locais: O serviço LDR é somente leitura.
Desativar replicação efetuada	DSOR	Selecione para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal. Quando a replicação de saída é desativada, os objetos podem ser copiados para este nó de armazenamento, mas os objetos não podem ser recuperados do nó de armazenamento para serem copiados para outros locais no sistema StorageGRID. O serviço LDR é apenas de escrita.

Gerencie nós de storage completos

À medida que os nós de storage atingem a capacidade, você precisa expandir o sistema StorageGRID com a adição de um novo storage. Há três opções disponíveis: Adicionar volumes de storage, adicionar compartimentos de expansão de storage e adicionar nós de storage.

Adicione volumes de armazenamento

Cada nó de storage oferece suporte a um número máximo de volumes de storage. 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, pode adicionar volumes para aumentar a sua capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

Adicione compartimentos de expansão de storage

Alguns nós de storage de dispositivos StorageGRID, como o SG6060, podem dar suporte a gavetas de storage adicionais. Se você tiver dispositivos StorageGRID com funcionalidades de expansão que ainda não foram expandidas para a capacidade máxima, poderá adicionar compartimentos de storage para aumentar a capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

Adicionar nós de storage

Você pode aumentar a capacidade de storage adicionando nós de storage. Deve-se ter em consideração cuidadosamente as regras de ILM e os requisitos de capacidade atualmente ativos ao adicionar armazenamento. Consulte as instruções para "Expandindo um sistema StorageGRID".

Gerenciar nós de administração

O que é um nó de administração?

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Cada grade deve ter um nó de administração principal e pode ter qualquer número de nós de administração não primários para redundância.

Quando você entra no Gerenciador de Grade ou no Gerenciador de Tenant, você está se conetando a um nó Admin. Você pode se conetar a qualquer nó de administrador e cada nó de administrador exibe uma exibição semelhante do sistema StorageGRID. No entanto, os procedimentos de manutenção devem ser executados usando o nó de administração principal.

Os nós Admin também podem ser usados para equilibrar o tráfego de clientes S3 e Swift.

Qual é o remetente preferido

Se a sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal é o remetente preferido para notificações de alerta, mensagens AutoSupport, traps e informes SNMP e notificações de alarme herdadas.

Em operações normais do sistema, apenas o remetente preferido envia notificações. No entanto, todos os outros nós de administração monitoram o remetente preferido. Se um problema for detetado, outros nós de administração agem como *remetentes de reserva*.

Várias notificações podem ser enviadas nesses casos:

- Se os nós de administração ficarem "isaterizados" uns dos outros, tanto o remetente preferido como os remetentes de reserva tentarão enviar notificações, e várias cópias de notificações podem ser recebidas.
- Se o remetente em espera detetar problemas com o remetente preferido e começar a enviar notificações, o remetente preferido pode recuperar sua capacidade de enviar notificações. Se isso ocorrer, notificações duplicadas podem ser enviadas. O remetente em espera deixará de enviar notificações quando não detetar mais erros no remetente preferido.

Quando você testa mensagens do AutoSupport, todos os nós de administração enviam o e-mail de teste. Ao testar notificações de alerta, você deve entrar em cada nó de administração para verificar a conetividade.

Serviços primários para nós de administração

A tabela a seguir mostra os serviços primários para nós de administração; no entanto, essa tabela não lista todos os serviços de nó.

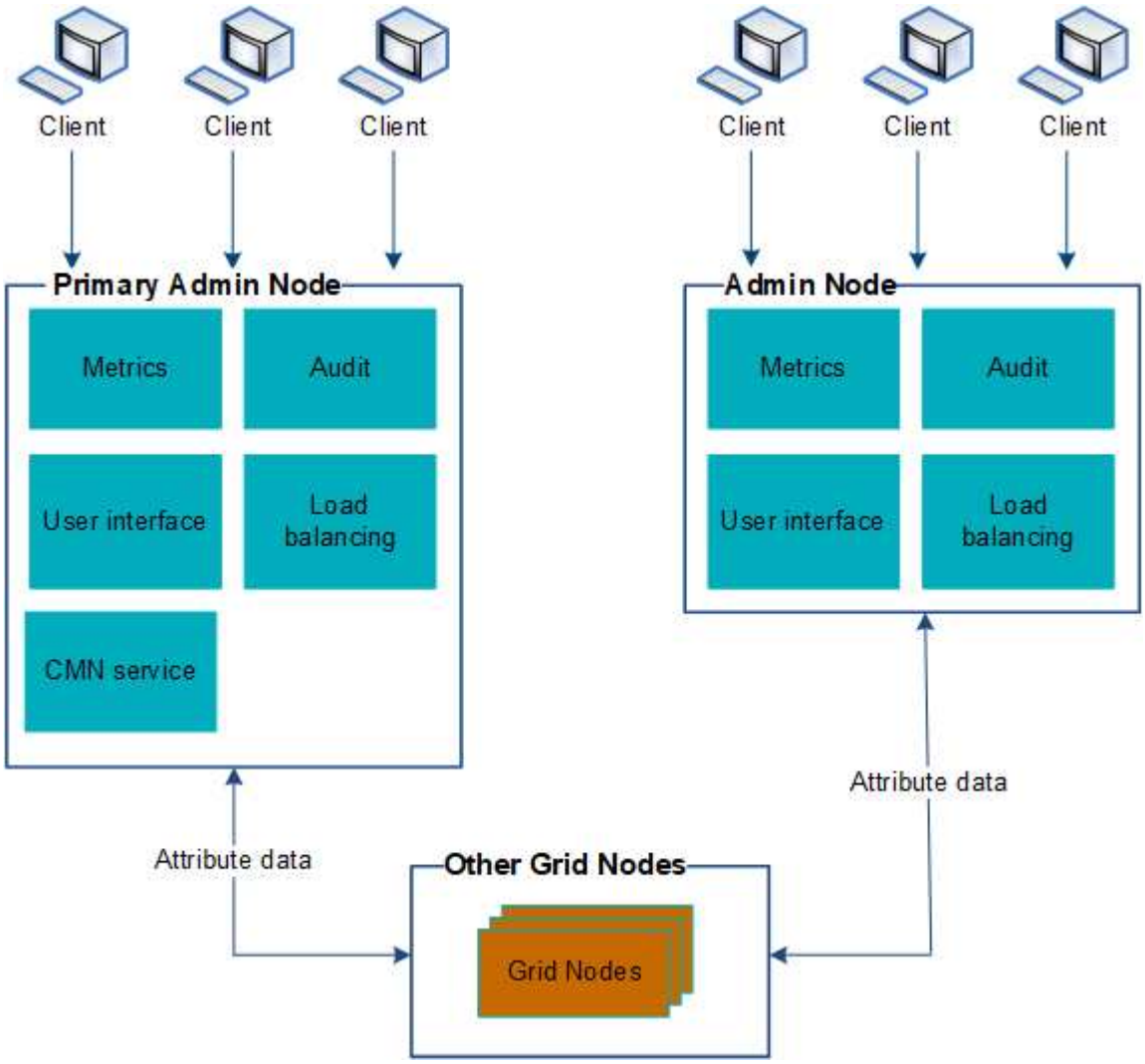
Serviço	Função de chave
Sistema de Gestão de Auditoria (AMS)	Monitoriza a atividade e os eventos do sistema.
Nó de gerenciamento de configuração (CMN)	Gerencia a configuração em todo o sistema. Somente nó de administração principal.
Interface do programa de aplicação de gerenciamento (mgmt-api)	Processa solicitações da API de gerenciamento de grade e da API de gerenciamento do locatário.
Alta disponibilidade	Gerencia endereços IP virtuais de alta disponibilidade para grupos de nós de administração e nós de gateway. **Nota:** este serviço também é encontrado em nós de Gateway.
Balanceador de carga	Fornece balanceamento de carga de tráfego S3 e Swift de clientes para nós de storage. **Nota:** este serviço também é encontrado em nós de Gateway.
Sistema de gerenciamento de rede (NMS)	Fornece funcionalidade para o Gerenciador de Grade.
Prometheus	Coleta e armazena métricas de séries temporais dos serviços em todos os nós.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

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 Admin ficar indisponível, o processamento de atributos continuará, alertas e alarmes (sistema legado) ainda serão acionados e notificações de e-mail e mensagens AutoSupport ainda serão enviadas. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto notificações e mensagens AutoSupport. Em particular, os reconhecimentos de alarmes feitos de um nó Admin não são

copiados para outros nós Admin.



Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administrador falhar:

- Os clientes da Web podem se reconetar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de nós de administração de alta disponibilidade, os clientes da Web poderão continuar a aceder ao Gestor de grelha ou ao Gestor de inquilinos utilizando o endereço IP virtual do grupo HA. "Gerenciar grupos de alta disponibilidade"Consulte .

> Ao usar um grupo de HA, o acesso é interrompido se o nó Admin ativo falhar. Os usuários devem fazer login novamente após o failover do endereço IP virtual do grupo HA para outro nó Admin no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó de administração principal falhar, ele deve ser recuperado antes que o sistema StorageGRID esteja totalmente funcional novamente.

Identifique o nó de administração principal

O nó de administração principal hospeda o serviço CMN. Alguns procedimentos de manutenção só podem ser executados usando o nó de administração principal.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***site*** > **Admin Node** e, em seguida, ➕ selecione para expandir a árvore de topologia e mostrar os serviços hospedados neste Admin Node.

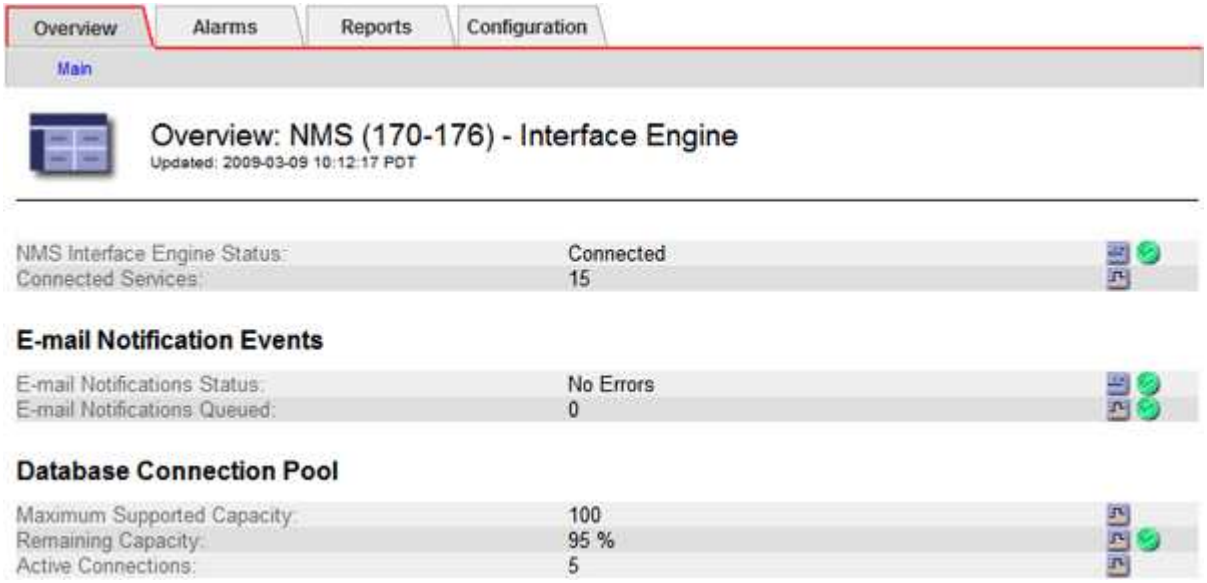
   O nó de administração principal hospeda o serviço CMN.

3. Se este nó Admin não hospedar o serviço CMN, verifique os outros nós Admin.

Exibir status de notificação e filas

O serviço do sistema de gerenciamento de rede (NMS) nos nós de administração envia notificações para o servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho de sua fila de notificações na página mecanismo de interface.

Para acessar a página mecanismo de interface, selecione **SUPPORT** > **Tools** > **Grid topoly**. Finalmente, selecione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



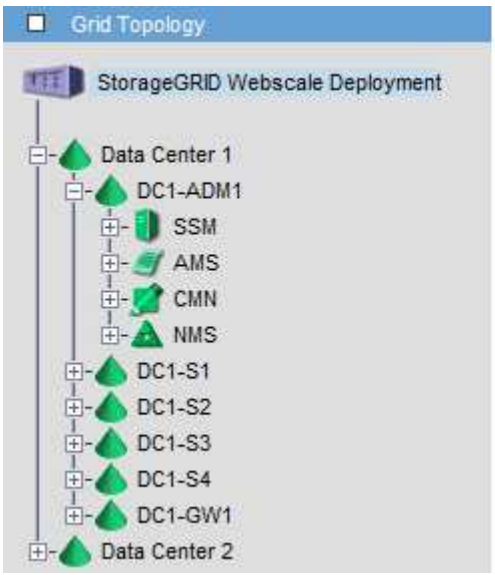
As notificações são processadas através da fila de notificações de e-mail e são enviadas para o servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando a tentativa for feita para enviar a notificação, uma tentativa de reenviar a notificação para o servidor de e-mail continuará por um período de 60 segundos. Se a notificação não for enviada para o servidor de correio após 60 segundos, a notificação será retirada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila.

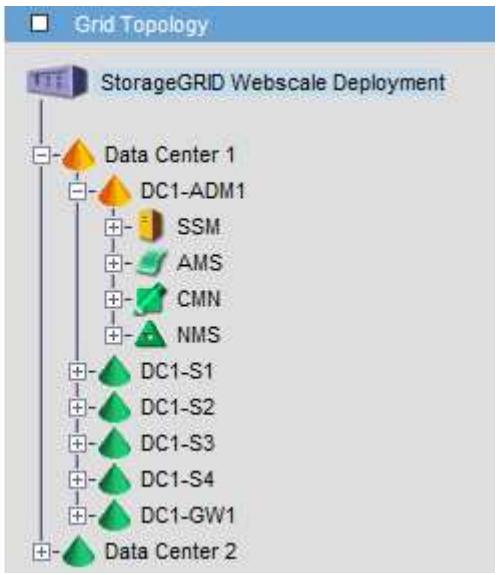
Como as notificações podem ser retiradas da fila de notificações sem serem enviadas, é possível que um alarme possa ser acionado sem que uma notificação seja enviada. Se uma notificação for descartada da fila sem ser enviada, o alarme menor MINS (Status da notificação de e-mail) será acionado.

Como os nós de administração mostram alarmes reconhecidos (sistema legado)

Quando você reconhece um alarme em um nó Admin, o alarme reconhecido não é copiado para nenhum outro nó Admin. Como os reconhecimentos não são copiados para outros nós de administração, a árvore de topologia de grade pode não ter a mesma aparência para cada nó de administração.

Essa diferença pode ser útil ao conetar clientes da Web. Os clientes da Web podem ter visualizações diferentes do sistema StorageGRID com base nas necessidades do administrador.





Observe que as notificações são enviadas do nó Admin onde a confirmação ocorre.

Configurar acesso de cliente de auditoria

Configurar acesso de cliente de auditoria para NFS

O Admin Node, por meio do serviço do Audit Management System (AMS), Registra todos os eventos do sistema auditados em um arquivo de log disponível por meio do compartilhamento de auditoria, que é adicionado a cada Admin Node na instalação. O compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

Para acessar logs de auditoria, você pode configurar o acesso do cliente a compartilhamentos de auditoria para NFS. Ou, você pode "use um servidor syslog externo".

O sistema StorageGRID usa reconhecimento positivo para evitar a perda de mensagens de auditoria antes de serem gravadas no arquivo de log. Uma mensagem permanece na fila em um serviço até que o serviço AMS ou um serviço de relé de auditoria intermediária tenha reconhecido o controle dele. Para obter mais informações, "Rever registos de auditoria"consulte .

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).
- O cliente de auditoria está usando o NFS versão 3 (NFSv3).

Sobre esta tarefa

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

   Se algum serviço não estiver listado como em execução ou verificado, resolva problemas antes de continuar.

3. Retorne à linha de comando. Pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração NFS. Introduza: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Adicione o cliente de auditoria: `add-audit-share`
   a. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: `client_IP_address`
   b. Quando solicitado, pressione **Enter**.
6. Se mais de um cliente de auditoria tiver permissão para acessar o compartilhamento de auditoria, adicione o endereço IP do usuário adicional: `add-ip-to-share`
   a. Introduza o número da partilha de auditoria: *`audit_share_number`*
   b. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

c. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

d. Repita essas subetapas para cada cliente de auditoria adicional que tenha acesso ao compartilhamento de auditoria.

7. Opcionalmente, verifique sua configuração.

   a. Introduza o seguinte: `validate-config`

      Os serviços são verificados e exibidos.

   b. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

   c. Feche o utilitário de configuração NFS: `exit`

8. Determine se você deve habilitar compartilhamentos de auditoria em outros sites.
   - Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
   - Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:
     i. Inicie sessão remotamente no Admin Node do site:
        A. Introduza o seguinte comando: `ssh admin@grid_node_IP`
        B. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
        C. Digite o seguinte comando para mudar para root: `su -`
        D. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
     ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.
     iii. Feche o login de shell seguro remoto para o Admin Node remoto. Introduza: `exit`

9. Faça logout do shell de comando: `exit`

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento ou remova um cliente de auditoria existente removendo seu endereço IP.

Adicione um cliente de auditoria NFS a um compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento de auditoria.

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha da conta root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).
- O cliente de auditoria está usando o NFS versão 3 (NFSv3).

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

      Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Introduza: `add-ip-to-share`

   Uma lista de compartilhamentos de auditoria NFS habilitados no Admin Node é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número da partilha de auditoria: *`audit_share_number`*
5. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

   O cliente de auditoria é adicionado ao compartilhamento de auditoria.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Repita as etapas para cada cliente de auditoria que deve ser adicionado ao compartilhamento de auditoria.
8. Opcionalmente, verifique sua configuração: `validate-config`

   Os serviços são verificados e exibidos.

   a. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

9. Feche o utilitário de configuração NFS: `exit`
10. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

Caso contrário, se a implantação do StorageGRID incluir nós de administração em outros sites, ative opcionalmente esses compartilhamentos de auditoria, conforme necessário:

a. Faça login remotamente no Admin Node de um site:
   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   iii. Digite o seguinte comando para mudar para root: `su -`
   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

11. Faça logout do shell de comando: `exit`

Verificar a integração da auditoria NFS

Depois de configurar um compartilhamento de auditoria e adicionar um cliente de auditoria NFS, você pode montar o compartilhamento de cliente de auditoria e verificar se os arquivos estão disponíveis no compartilhamento de auditoria.

Passos

1. Verifique a conetividade (ou variante para o sistema cliente) usando o endereço IP do lado do cliente do nó Admin que hospeda o serviço AMS. Introduza: `ping IP_address`

   Verifique se o servidor responde, indicando conetividade.

2. Monte o compartilhamento de auditoria somente leitura usando um comando apropriado ao sistema operacional cliente. Um exemplo de comando Linux é (Enter em uma linha):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Use o endereço IP do nó de administração que hospeda o serviço AMS e o nome de compartilhamento predefinido para o sistema de auditoria. O ponto de montagem pode ser qualquer nome selecionado pelo cliente (por exemplo, `myAudit` no comando anterior).

3. Verifique se os arquivos estão disponíveis no compartilhamento de auditoria. Introduza: `ls myAudit /*`

   ```
   `_myAudit_`onde está o ponto de montagem da partilha de auditoria. Deve
   haver pelo menos um arquivo de log listado.
   ```

Remover um cliente de auditoria NFS do compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Você pode remover um cliente de auditoria existente removendo seu endereço IP.

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha da conta root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).

Sobre esta tarefa

Não é possível remover o último endereço IP permitido para acessar o compartilhamento de auditoria.

Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Remova o endereço IP do compartilhamento de auditoria: `remove-ip-from-share`

   Uma lista numerada de compartilhamentos de auditoria configurados no servidor é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número correspondente à partilha de auditoria: *`audit_share_number`*

   É apresentada uma lista numerada de endereços IP permitidos para aceder à partilha de auditoria.

5. Introduza o número correspondente ao endereço IP que pretende remover.

   O compartilhamento de auditoria é atualizado e o acesso não é mais permitido a partir de qualquer cliente de auditoria com este endereço IP.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Feche o utilitário de configuração NFS: `exit`
8. Se a implantação do StorageGRID for uma implantação de vários locais de data center com nós de administração adicionais nos outros sites, desative esses compartilhamentos de auditoria conforme

necessário:

a. Faça login remotamente no Admin Node de cada site:

   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

   iii. Digite o seguinte comando para mudar para root: `su -`

   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.

c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

9. Faça logout do shell de comando: `exit`

Altere o endereço IP de um cliente de auditoria NFS

Conclua estas etapas se precisar alterar o endereço IP de um cliente de auditoria NFS.

Passos

1. Adicione um novo endereço IP a um compartilhamento de auditoria NFS existente.
2. Remova o endereço IP original.

Informações relacionadas

- "Adicione um cliente de auditoria NFS a um compartilhamento de auditoria"
- "Remover um cliente de auditoria NFS do compartilhamento de auditoria"

Gerenciar nós de arquivamento

O que é um nó de arquivo?

Opcionalmente, cada local de data center do StorageGRID pode ser implantado com um nó de arquivo, que permite que você se conete a um sistema de armazenamento de arquivamento externo direcionado, como o Gerenciador de armazenamento do Tivoli (TSM).

> O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.
>
> Consulte:
>
> - "Migre objetos para um Cloud Storage Pool"
> - "Use Cloud Storage Pools"
>
> Além disso, você deve remover nós de arquivamento da política ILM ativa no StorageGRID 11,7 ou anterior. A remoção de dados de objetos armazenados nos nós de arquivamento simplificará futuras atualizações. "Trabalhando com regras de ILM e políticas de ILM"Consulte .

O Archive Node fornece uma interface através da qual você pode segmentar um sistema de storage de arquivamento externo para o armazenamento de dados de objetos a longo prazo. O nó de arquivo também monitora essa conexão e a transferência de dados de objetos entre o sistema StorageGRID e o sistema de armazenamento de arquivamento externo direcionado.

Depois de configurar as ligações ao destino externo, pode configurar o nó de arquivo para otimizar o desempenho do TSM, colocar um nó de arquivo offline quando um servidor TSM estiver a aproximar-se da capacidade ou indisponível, e configurar as definições de replicação e recuperação. Também pode definir alarmes personalizados para o nó de arquivo.

Os dados de objetos que não podem ser excluídos, mas não são acessados regularmente, podem, a qualquer momento, ser movidos dos discos giratórios de um nó de storage e para um storage de arquivamento externo, como a nuvem ou a fita. Este arquivamento de dados de objetos é realizado através da configuração do nó de arquivo de um site de data center e, em seguida, a configuração de regras ILM em que este nó de arquivo é selecionado como o "destino" para instruções de posicionamento de conteúdo. O nó de arquivo não gerencia os dados de objeto arquivados em si; isso é obtido pelo dispositivo de arquivamento externo.

Os metadados de objetos não são arquivados, mas permanecem em nós de storage.

O que é o serviço ARC

O serviço de arquivamento (ARC) em nós de arquivamento fornece a interface de gerenciamento que você pode usar para configurar conexões com armazenamento de arquivamento externo, como fita por meio do middleware TSM.

É o serviço ARC que interage com um sistema de armazenamento de arquivos externo, enviando dados de objetos para armazenamento near-line e realizando recuperações quando um aplicativo cliente solicita um objeto arquivado. Quando um aplicativo cliente solicita um objeto arquivado, um nó de armazenamento solicita os dados do objeto do serviço ARC. O serviço ARC faz uma solicitação para o sistema de armazenamento de arquivos externo, que recupera os dados de objeto solicitados e os envia para o serviço ARC. O serviço ARC verifica os dados do objeto e os encaminha para o nó de armazenamento, que por sua vez retorna o objeto para o aplicativo cliente solicitante.

As solicitações de dados de objetos arquivados em fita por meio do middleware TSM são gerenciadas para eficiência de recuperações. As solicitações podem ser solicitadas para que os objetos armazenados em ordem sequencial na fita sejam solicitados na mesma ordem sequencial. As solicitações são então enfileiradas para envio para o dispositivo de armazenamento. Dependendo do dispositivo de arquivamento, várias solicitações de objetos em diferentes volumes podem ser processadas simultaneamente.

Arquive para a nuvem por meio da API S3

Você pode configurar um nó de arquivo para se conetar diretamente à Amazon Web Services (AWS) ou a qualquer outro sistema que possa fazer interface com o sistema StorageGRID por meio da API S3.

O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.

"Use Cloud Storage Pools"Consulte .

Configure as configurações de conexão para a API S3

Se você estiver se conetando a um nó de Arquivo usando a interface S3, você deverá configurar as configurações de conexão para a API S3. Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o sistema de armazenamento de arquivos externo.

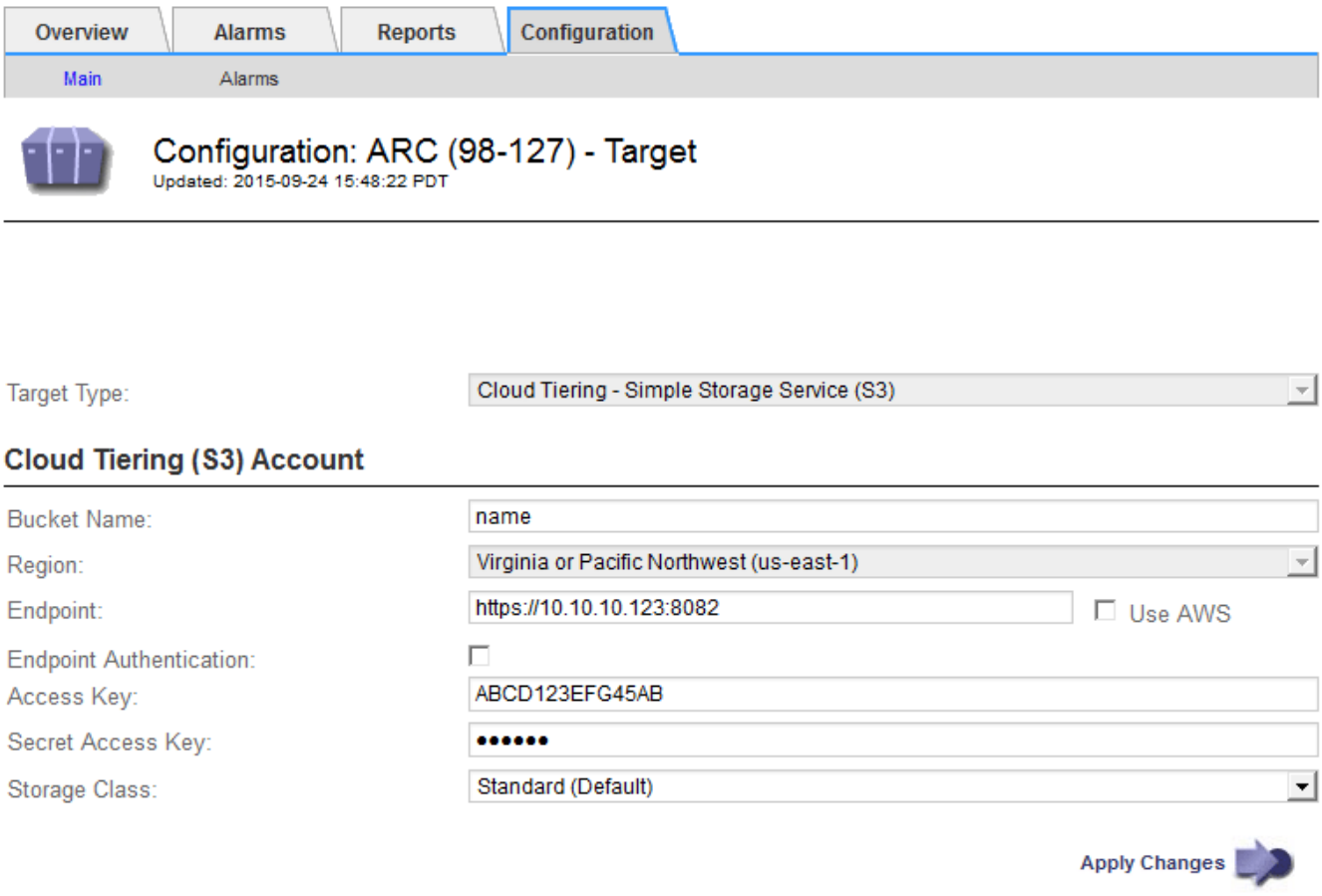
> O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.
>
> "Use Cloud Storage Pools"Consulte .

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Você criou um bucket no sistema de storage de arquivamento de destino:
  - O bucket é dedicado a um único nó de arquivo. Ele não pode ser usado por outros nós de arquivamento ou outras aplicações.
  - O balde tem a região apropriada selecionada para a sua localização.
  - O bucket deve ser configurado com o controle de versão suspenso.
- A Segmentação de objetos está ativada e o tamanho máximo do segmento é menor ou igual a 4,5 GiB (4.831.838.208 bytes). S3 solicitações de API que excederem esse valor falharão se S3 for usado como sistema de armazenamento de arquivamento externo.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione **Archive Node** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Selecione **disposição em camadas na nuvem - Serviço de armazenamento simples (S3)** na lista suspensa tipo de destino.

   As configurações ficam indisponíveis até que você selecione um tipo de destino.

5. Configurar a conta Cloud Tiering (S3) através da qual o Archive Node se conetará ao sistema de storage de arquivamento externo de destino com capacidade para S3.

   A maioria dos campos nesta página são auto-explicativos. A seguir descreve os campos para os quais você pode precisar de orientação.

   - **Região**: Disponível somente se **usar AWS** estiver selecionado. A região selecionada tem de corresponder à região do balde.
   - **Endpoint** e **Use AWS**: Para Amazon Web Services (AWS), selecione **Use AWS**. **Endpoint** é então preenchido automaticamente com um URL de endpoint baseado nos atributos Nome do bucket e região. Por exemplo:

     ```
     https://bucket.region.amazonaws.com
     ```

     Para um destino que não seja AWS, insira o URL do sistema que hospeda o bucket, incluindo o número da porta. Por exemplo:

```
https://system.com:1080
```

   - **Autenticação de ponto final**: Ativada por padrão. Se a rede para o sistema de armazenamento de arquivos externo for confiável, você pode desmarcar a caixa de seleção para desativar o certificado SSL de endpoint e a verificação de hostname para o sistema de armazenamento de arquivos externo

de destino. Se outra instância de um sistema StorageGRID for o dispositivo de armazenamento de arquivamento de destino e o sistema estiver configurado com certificados assinados publicamente, você poderá manter a caixa de seleção selecionada.

- **Classe de armazenamento**: Selecione **Standard (padrão)** para armazenamento regular. Selecione **redundância reduzida** apenas para objetos que possam ser facilmente recriados. **Redundância reduzida** fornece armazenamento de menor custo com menos confiabilidade. Se o sistema de armazenamento de arquivos de destino for outra instância do sistema StorageGRID, **Classe de armazenamento** controla quantas cópias provisórias do objeto são feitas na ingestão no sistema de destino, se a confirmação dupla for usada quando os objetos forem ingeridos lá.

6. Selecione **aplicar alterações**.

   As configurações especificadas são validadas e aplicadas ao seu sistema StorageGRID. Uma vez configurado, o destino não pode ser alterado.

Modifique as configurações de conexão para a API S3

Depois que o nó de arquivo é configurado para se conetar a um sistema de armazenamento de arquivos externo através da API S3, você pode modificar algumas configurações caso a conexão seja alterada.

Antes de começar

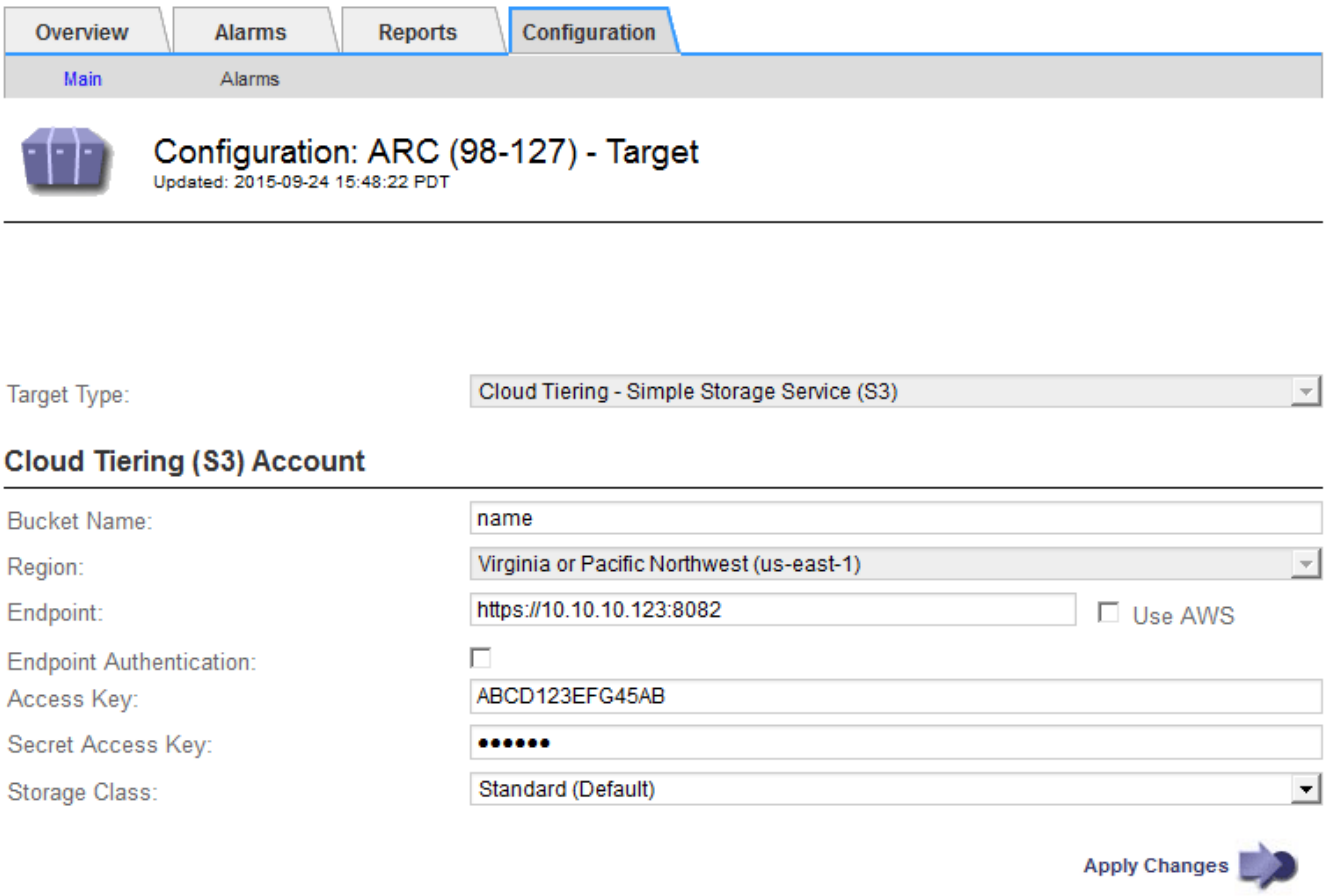
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Se você alterar a conta do Cloud Tiering (S3), deverá garantir que as credenciais de acesso do usuário tenham acesso de leitura/gravação ao bucket, incluindo todos os objetos que foram ingeridos anteriormente pelo Archive Node ao bucket.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as informações da conta, conforme necessário.

   Se você alterar a classe de armazenamento, os novos dados de objeto serão armazenados com a nova classe de armazenamento. O objeto existente continua a ser armazenado sob o conjunto de classes de armazenamento quando ingerido.

   Nome do bucket, região e ponto final, use valores da AWS e não pode ser alterado.

5. Selecione **aplicar alterações**.

Modifique o estado Cloud Tiering Service

Você pode controlar a capacidade de leitura e gravação do nó de arquivamento no sistema de storage de arquivamento externo de destino que se conecta pela API S3, alterando o estado do Cloud Tiering Service.

Antes de começar

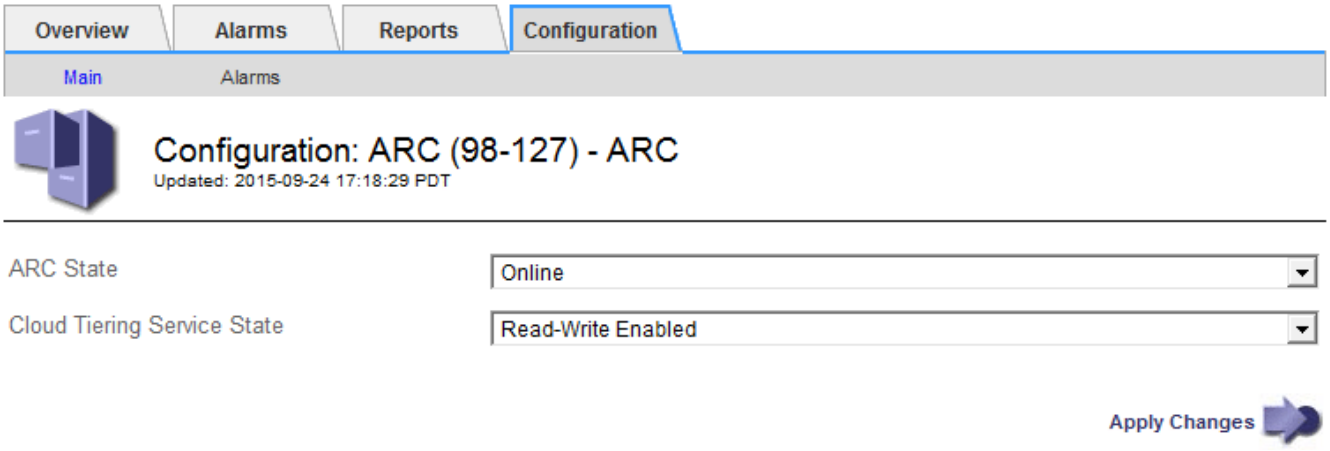
- Você deve estar conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você deve ter permissões de acesso específicas.
- O nó de arquivo deve ser configurado.

Sobre esta tarefa

Você pode efetivamente colocar o nó de arquivo offline alterando o estado do Serviço de disposição em categorias na nuvem para **leitura-escrita desativada**.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC**.
3. Selecione **Configuração** > **Principal**.



4. Selecione um **Estado do Serviço de disposição em camadas na nuvem**.
5. Selecione **aplicar alterações**.

Redefina a contagem de falhas de armazenamento para conexão API S3

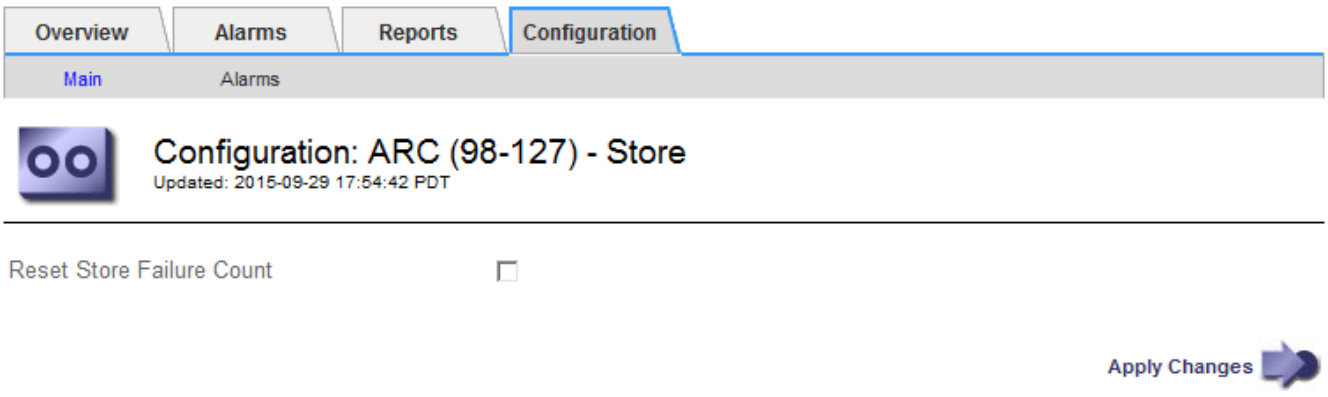
Se o seu nó de arquivo se conetar a um sistema de armazenamento de arquivos por meio da API S3, você poderá redefinir a contagem de falhas de armazenamento, que pode ser usada para limpar o alarme ARVF (falhas de armazenamento).

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.



4. Selecione **Repor contagem de falhas de armazenamento**.

5. Selecione **aplicar alterações**.

   O atributo Store Failures (falhas de armazenamento) é reposto a zero.

Migre objetos do Cloud Tiering - S3 para um Cloud Storage Pool

Se você estiver usando o recurso **Cloud Tiering - Simple Storage Service (S3)** para categorizar dados de objetos em um bucket do S3, você deve migrar seus objetos para um pool de armazenamento em nuvem. Os pools de storage em nuvem fornecem uma abordagem dimensionável que aproveita todos os nós de storage do seu sistema StorageGRID.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.
- Você já armazenou objetos no bucket do S3 configurado para o Cloud Tiering.

> Antes de migrar dados de objeto, entre em Contato com o representante da conta do NetApp para entender e gerenciar quaisquer custos associados.

Sobre esta tarefa

Do ponto de vista do ILM, um Cloud Storage Pool é semelhante a um pool de storage. No entanto, embora os pools de storage consistam em nós de storage ou nós de arquivamento no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo do S3.

Antes de migrar objetos do Cloud Tiering - S3 para um pool de armazenamento em nuvem, primeiro você deve criar um bucket do S3 e, em seguida, criar o pool de armazenamento em nuvem no StorageGRID. Em seguida, você pode criar uma nova política de ILM e substituir a regra ILM usada para armazenar objetos no bucket do Cloud Tiering por uma regra ILM clonada que armazena os mesmos objetos no Cloud Storage Pool.

> Quando os objetos são armazenados em um pool de armazenamento em nuvem, as cópias desses objetos também não podem ser armazenadas no StorageGRID. Se a regra ILM que você está usando atualmente para o Cloud Tiering estiver configurada para armazenar objetos em vários locais ao mesmo tempo, considere se você ainda deseja executar essa migração opcional porque perderá essa funcionalidade. Se você continuar com essa migração, crie novas regras em vez de clonar as existentes.

Passos

1. Crie um pool de storage em nuvem.

   Use um novo bucket do S3 para o Cloud Storage Pool para garantir que ele contenha apenas os dados gerenciados pelo Cloud Storage Pool.

2. Localize quaisquer regras de ILM na política de ILM ativa que façam com que os objetos sejam armazenados no bucket do Cloud Tiering.
3. Clone cada uma dessas regras.
4. Nas regras clonadas, altere o local de posicionamento para o novo Cloud Storage Pool.
5. Salve as regras clonadas.

6. Crie uma nova política que use as novas regras.
7. Simule e ative a nova política.

   Quando a nova política é ativada e a avaliação ILM ocorre, os objetos são movidos do bucket do S3 configurado para o bucket do Cloud Tiering para o bucket do S3 configurado para o pool de armazenamento em nuvem. O espaço utilizável na grade não é afetado. Depois que os objetos são movidos para o Cloud Storage Pool, eles são removidos do bucket do Cloud Tiering.

Informações relacionadas

"Gerenciar objetos com ILM"

Arquive para fita através do middleware TSM

Você pode configurar um nó de arquivo para segmentar um servidor Tivoli Storage Manager (TSM) que fornece uma interface lógica para armazenar e recuperar dados de objetos em dispositivos de armazenamento de acesso aleatório ou sequencial, incluindo bibliotecas de fitas.

O serviço ARC do Archive Node atua como um cliente para o servidor TSM, usando o Tivoli Storage Manager como middleware para comunicação com o sistema de armazenamento de arquivos.

> O suporte para nós de arquivamento (tanto para arquivamento na nuvem usando a API S3 como para arquivamento em fita usando middleware TSM) está obsoleto e será removido em uma versão futura. Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo foi substituído pelo ILM Cloud Storage Pools, que oferece mais funcionalidade.
>
> "Use Cloud Storage Pools"Consulte .

Classes de gestão TSM

As classes de gerenciamento definidas pelo middleware TSM descrevem como as operações de backup e arquivamento do TSMs funcionam e podem ser usadas para especificar regras para conteúdo que são aplicadas pelo servidor TSM. Essas regras operam independentemente da política ILM do sistema StorageGRID e devem ser consistentes com o requisito do sistema StorageGRID de que os objetos são armazenados permanentemente e estão sempre disponíveis para recuperação pelo nó de arquivo. Depois que os dados do objeto são enviados para um servidor TSM pelo nó de arquivo, as regras de ciclo de vida e retenção do TSM são aplicadas enquanto os dados do objeto são armazenados em fita gerenciada pelo servidor TSM.

A classe de gerenciamento TSM é usada pelo servidor TSM para aplicar regras de localização ou retenção de dados depois que os objetos são enviados para o servidor TSM pelo nó de arquivamento. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

Configurar conexões com middleware TSM

Antes que o Archive Node possa se comunicar com o middleware Tivoli Storage Manager (TSM), você deve configurar várias configurações.

Antes de começar

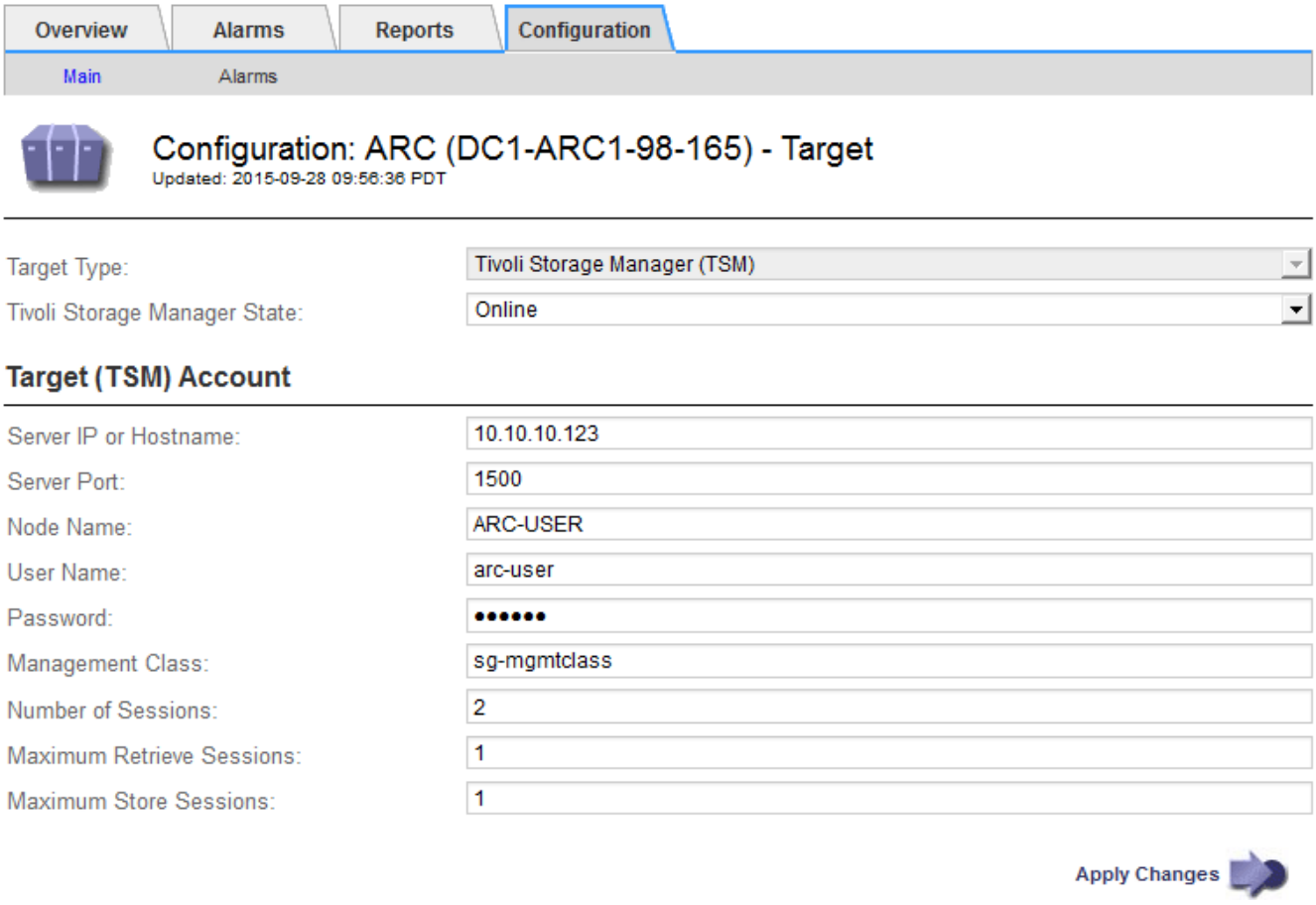
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o Tivoli Storage Manager.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.



4. Na lista suspensa **tipo de destino**, selecione **Tivoli Storage Manager (TSM)**.
5. Para o **Tivoli Storage Manager State**, selecione **Offline** para evitar recuperações do servidor de middleware TSM.

   Por padrão, o Tivoli Storage Manager State é definido como Online, o que significa que o Archive Node é capaz de recuperar dados de objetos do servidor middleware TSM.

6. Preencha as seguintes informações:

   - **IP do servidor ou Nome de host**: Especifique o endereço IP ou nome de domínio totalmente qualificado do servidor middleware TSM usado pelo serviço ARC. O endereço IP padrão é 127,0.0,1.

- **Server Port**: Especifique o número da porta no servidor middleware TSM ao qual o serviço ARC se conetará. A predefinição é 1500.
- **Nome do nó**: Especifique o nome do nó de arquivo. Você deve inserir o nome (usuário ARC) registrado no servidor de middleware TSM.
- **Nome de usuário**: Especifique o nome de usuário que o serviço ARC usa para fazer login no servidor TSM. Introduza o nome de utilizador predefinido (ARC-user) ou o utilizador administrativo que especificou para o nó de arquivo.
- **Senha**: Especifique a senha usada pelo serviço ARC para fazer login no servidor TSM.
- **Classe de gerenciamento**: Especifique a classe de gerenciamento padrão a ser usada se uma classe de gerenciamento não for especificada quando o objeto estiver sendo salvo no sistema StorageGRID, ou a classe de gerenciamento especificada não estiver definida no servidor de middleware TSM.
- **Número de sessões**: Especifique o número de unidades de fita no servidor middleware TSM que são dedicadas ao nó de arquivo. O nó de arquivo cria simultaneamente um máximo de uma sessão por ponto de montagem mais um pequeno número de sessões adicionais (menos de cinco).

  Tem de alterar este valor para ser o mesmo que o valor definido para MAXNUMMP (número máximo de pontos de montagem) quando o nó de arquivo foi registado ou atualizado. (No comando register, o valor predefinido de MAXNUMMP utilizado é 1, se nenhum valor estiver definido.)

Você também deve alterar o valor de MAXSESSIONS para o servidor TSM para um número que seja pelo menos tão grande quanto o número de sessões definido para o serviço ARC. O valor padrão de MAXSESSIONS no servidor TSM é 25.

- * Sessões de recuperação máxima*: Especifique o número máximo de sessões que o serviço ARC pode abrir para o servidor middleware TSM para operações de recuperação. Na maioria dos casos, o valor apropriado é o número de sessões menos sessões de armazenamento máximo. Se você precisar compartilhar uma unidade de fita para armazenamento e recuperação, especifique um valor igual ao número de sessões.
- **Maximum Store Sessions**: Especifique o número máximo de sessões simultâneas que o serviço ARC pode abrir para o servidor middleware TSM para operações de arquivamento.

  Esse valor deve ser definido como um, exceto quando o sistema de armazenamento de arquivos de destino estiver cheio e somente recuperações podem ser executadas. Defina esse valor como zero para usar todas as sessões para recuperações.

7. Selecione **aplicar alterações**.

Otimize um nó de arquivo para sessões de middleware TSM

Você pode otimizar o desempenho de um nó de arquivo que se coneta ao Tivoli Server Manager (TSM) configurando as sessões do nó de arquivo.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

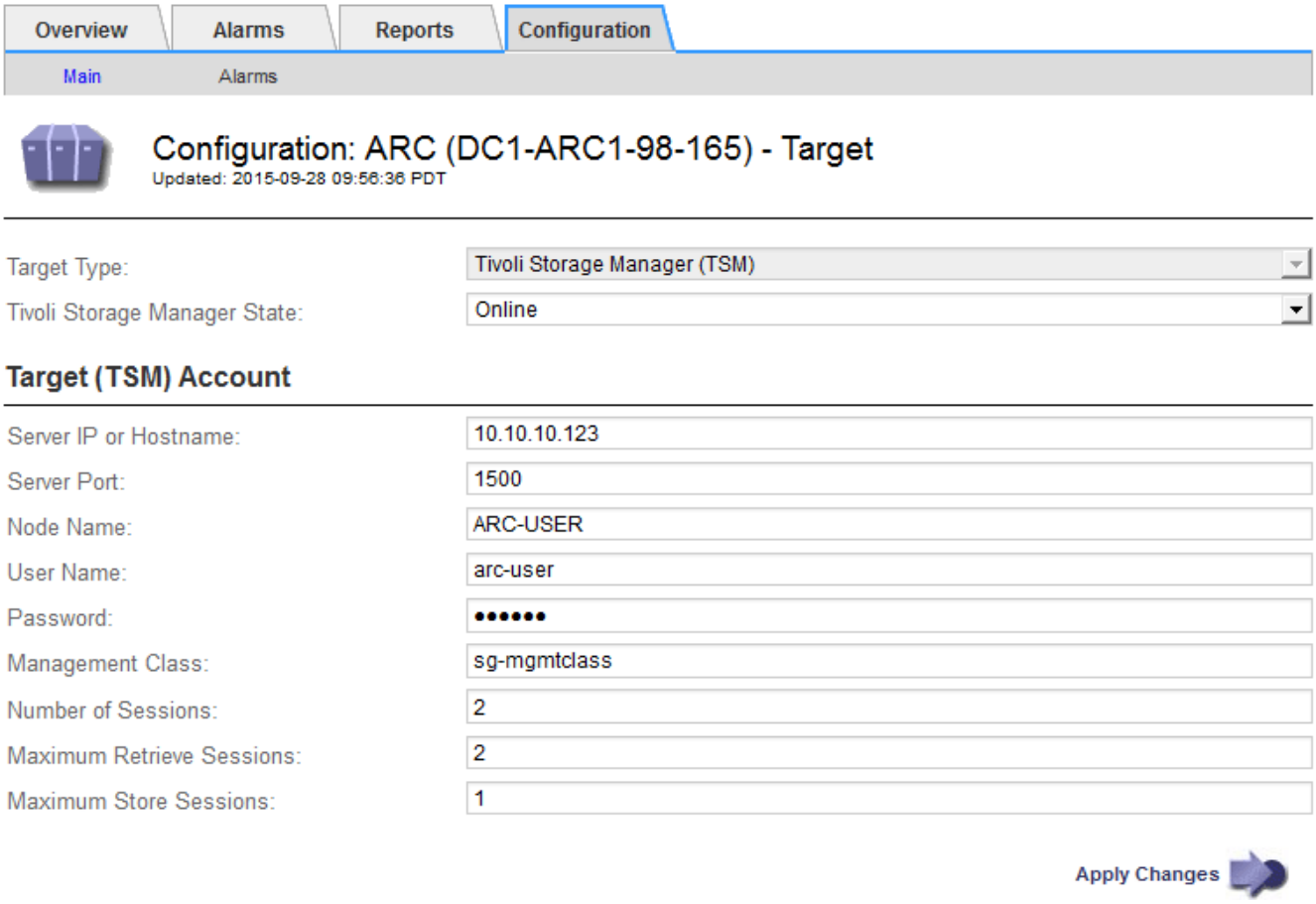
Sobre esta tarefa

Normalmente, o número de sessões simultâneas que o Archive Node tem aberto ao servidor middleware TSM é definido para o número de unidades de fita que o servidor TSM dedicou ao Archive Node. Uma unidade de fita é alocada para armazenamento enquanto o resto é alocado para recuperação. No entanto, em situações em que um nó de armazenamento está sendo reconstruído a partir de cópias do nó de arquivo ou o nó de

arquivo está operando no modo somente leitura, você pode otimizar o desempenho do servidor TSM definindo o número máximo de sessões de recuperação para ser o mesmo que o número de sessões simultâneas. O resultado é que todas as unidades podem ser usadas simultaneamente para recuperação e, no máximo, uma dessas unidades também pode ser usada para armazenamento, se aplicável.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.
4. Altere **sessões de recuperação máxima** para ser o mesmo que **número de sessões**.



5. Selecione **aplicar alterações**.

Configure o estado do arquivo e os contadores para o TSM

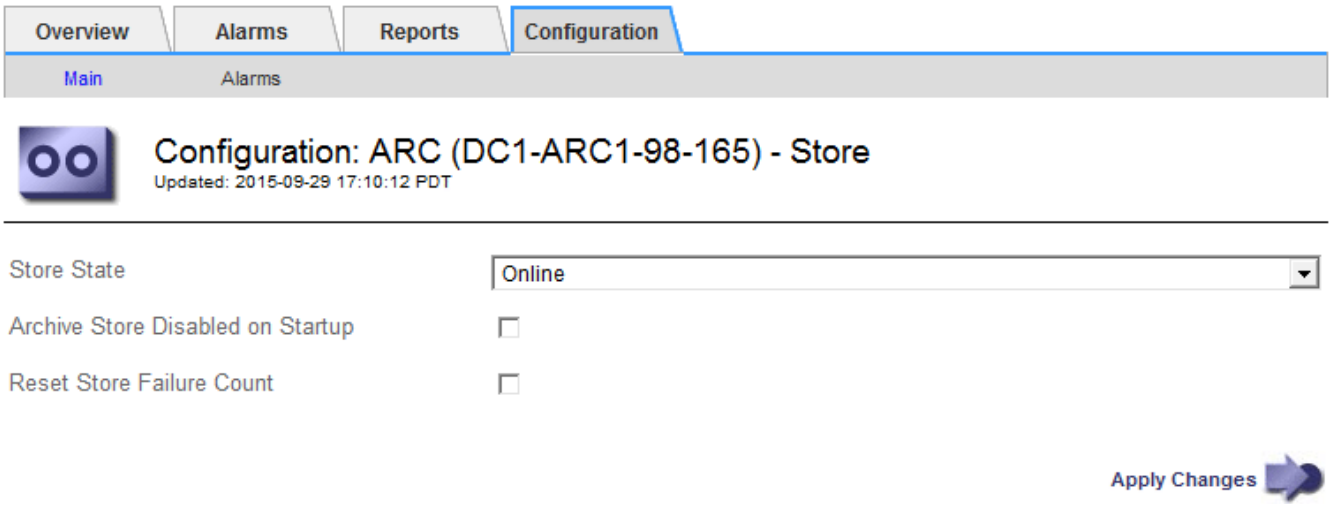
Se o seu Archive Node se conetar a um servidor middleware TSM, você poderá configurar o estado de armazenamento de arquivo de um Archive Node para Online ou Offline. Você também pode desativar o armazenamento de arquivos quando o nó de arquivo é iniciado pela primeira vez ou redefinir a contagem de falhas sendo rastreada para o alarme associado.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - Estado da loja: Defina o estado do componente para:
     - On-line: O Archive Node está disponível para processar dados de objetos para armazenamento no sistema de armazenamento de arquivamento.
     - Offline: O nó de arquivo não está disponível para processar dados de objeto para armazenamento no sistema de armazenamento de arquivo.
   - Archive Store Disabled on Startup (armazenamento de arquivo desativado na inicialização): Quando selecionado, o componente Archive Store (armazenamento de arquivo) permanece no estado Read-Only (somente leitura) quando reiniciado. Usado para desativar persistentemente o armazenamento para o sistema de armazenamento de arquivo visado. Útil quando o sistema de armazenamento de arquivos visado não consegue aceitar conteúdo.
   - Repor contagem de falhas de armazenamento: Reponha o contador para falhas de armazenamento. Isso pode ser usado para limpar o alarme ARVF (falha de armazenamento).
5. Selecione **aplicar alterações**.

Informações relacionadas

"Gerencie um nó de arquivo quando o servidor TSM atingir a capacidade"

Gerencie um nó de arquivo quando o servidor TSM atingir a capacidade

O servidor TSM não tem como notificar o nó de arquivo quando o banco de dados TSM ou o armazenamento de Mídia de arquivamento gerenciado pelo servidor TSM estiver próximo da capacidade. Esta situação pode ser evitada através do monitoramento proativo do servidor TSM.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Sobre esta tarefa

O nó de arquivo continua a aceitar dados de objeto para transferência para o servidor TSM depois que o servidor TSM parar de aceitar novo conteúdo. Este conteúdo não pode ser escrito em Mídia gerenciada pelo servidor TSM. Um alarme é acionado se isso acontecer.

Impedir que o serviço ARC envie conteúdo para o servidor TSM

Para evitar que o serviço ARC envie mais conteúdo para o servidor TSM, você pode colocar o nó de Arquivo offline, colocando o componente **ARC** > **Store** offline. Este procedimento também pode ser útil na prevenção de alarmes quando o servidor TSM não estiver disponível para manutenção.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.

4. Altere **Estado de armazenamento** para `Offline`.
5. Selecione **Archive Store Disabled on Startup**.
6. Selecione **aplicar alterações**.

Defina Archive Node como somente leitura se o middleware TSM atingir a capacidade

Se o servidor de middleware TSM visado atingir a capacidade, o nó de arquivo pode ser otimizado para executar apenas recuperações.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.
4. Altere as sessões de recuperação máxima para ser igual ao número de sessões simultâneas listadas em número de sessões.
5. Altere o máximo de sessões de armazenamento para 0.

> Não é necessário alterar o máximo de sessões de armazenamento para 0 se o nó de arquivo for apenas leitura. As sessões de armazenamento não serão criadas.

6. Selecione **aplicar alterações**.

Configurar as definições de recuperação do nó de arquivo

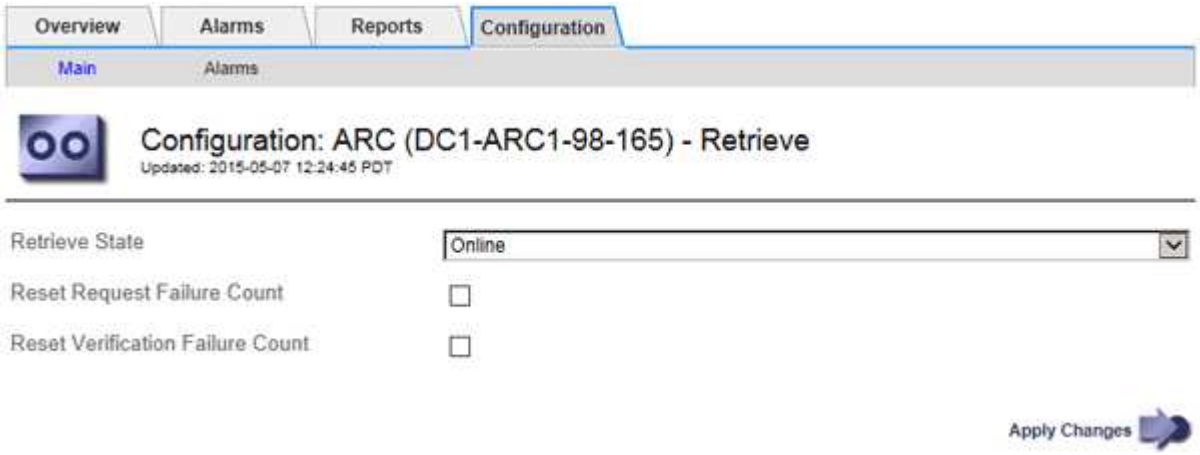
Você pode configurar as configurações de recuperação de um nó de arquivo para definir o estado como Online ou Offline, ou redefinir as contagens de falhas que estão sendo rastreadas para os alarmes associados.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione **Archive Node** > **ARC** > **Retrieve**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - **Retrieve State**: Defina o estado do componente para:
     - On-line: O nó de grade está disponível para recuperar dados de objeto do dispositivo de Mídia de arquivamento.
     - Offline: O nó de grade não está disponível para recuperar dados de objeto.
   - Reset Request Failures Count (Redefinir contagem de falhas de pedido): Selecione a caixa de verificação para repor o contador para falhas de pedido. Isso pode ser usado para limpar o alarme ARRF (falhas de solicitação).
   - Redefinir contagem de falhas de verificação: Marque a caixa de seleção para redefinir o contador para falhas de verificação em dados de objetos recuperados. Isso pode ser usado para limpar o alarme ARRV (falhas de verificação).
5. Selecione **aplicar alterações**.

Configurar a replicação do nó de arquivo

Você pode configurar as configurações de replicação para um nó de arquivo e desativar a replicação de entrada e saída ou redefinir as contagens de falha que estão sendo

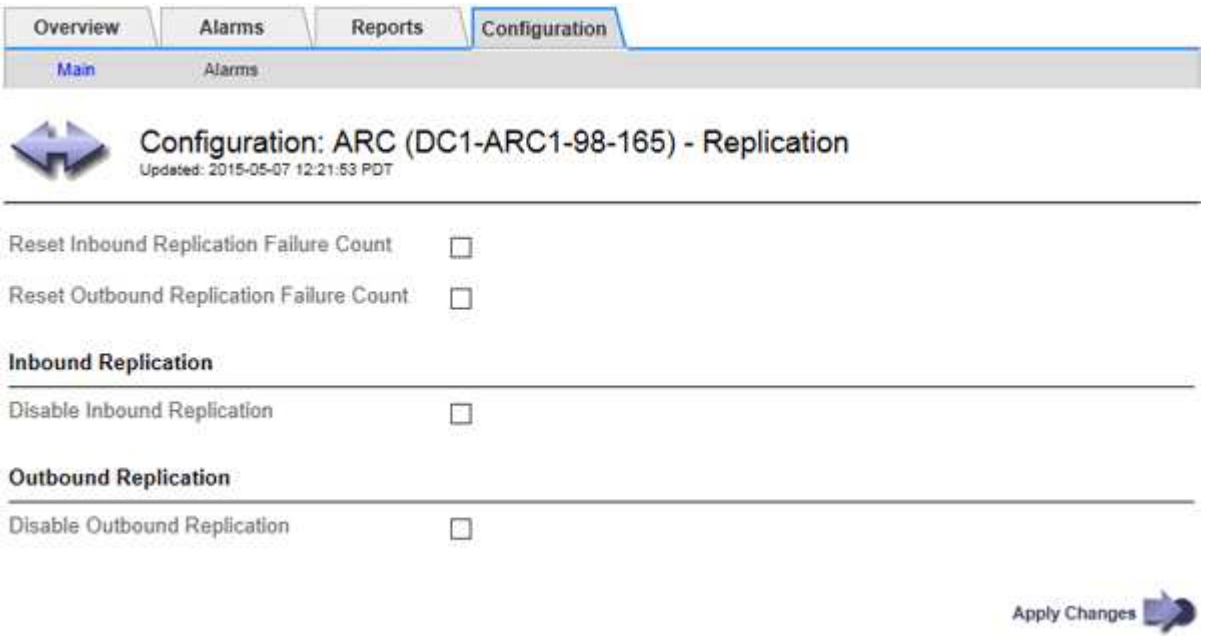
rastreadas para os alarmes associados.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT** > **Tools** > **Grid topology**.
2. Selecione ***Archive Node*** > **ARC** > **Replication**.
3. Selecione **Configuração** > **Principal**.



4. Modifique as seguintes definições, conforme necessário:
   - **Redefinir contagem de falhas de replicação de entrada**: Selecione para redefinir o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicações embutidas — Failed).
   - **Redefinir contagem de falhas de replicação de saída**: Selecione para redefinir o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed).
   - **Desativar replicação de entrada**: Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe limpo durante o funcionamento normal.

     Quando a replicação de entrada é desativada, os dados de objeto podem ser recuperados do serviço ARC para replicação para outros locais no sistema StorageGRID, mas os objetos não podem ser replicados para este serviço ARC a partir de outros locais do sistema. O serviço ARC é apenas de leitura.

   - **Desativar replicação de saída**: Marque a caixa de seleção para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.

     Quando a replicação de saída é desativada, os dados de objeto podem ser copiados para este serviço ARC para satisfazer as regras ILM, mas os dados de objeto não podem ser recuperados do serviço

ARC para serem copiados para outros locais no sistema StorageGRID. O serviço ARC é apenas de escrita.

5. Selecione **aplicar alterações**.

Definir alarmes personalizados para o nó de arquivo

Você deve estabelecer alarmes personalizados para os atributos ARQL e ARRL que são usados para monitorar a velocidade e eficiência da recuperação de dados de objetos do sistema de armazenamento de arquivos pelo nó Archive.

- ARQL: Comprimento médio da fila. O tempo médio, em microssegundos, em que os dados do objeto são enfileirados para recuperação do sistema de armazenamento de arquivamento.
- ARRL: Latência média da solicitação. O tempo médio, em microssegundos, necessário pelo nó de arquivo para recuperar dados de objetos do sistema de armazenamento de arquivamento.

Os valores aceitáveis para esses atributos dependem de como o sistema de armazenamento de arquivos é configurado e usado. (Vá para **ARC** > **Retrieve** > **Overview** > **Main**.) Os valores definidos para tempos limite de solicitação e o número de sessões disponibilizadas para solicitações de recuperação são particularmente influentes.

Depois que a integração estiver concluída, monitorize as recuperações de dados de objetos do nó de Arquivo para estabelecer valores para tempos de recuperação normais e comprimentos de fila. Em seguida, crie alarmes personalizados para ARQL e ARRL que serão acionados se surgir uma condição operacional anormal. Consulte as instruções para "gerenciamento de alarmes (sistema legado)".

Integre o Tivoli Storage Manager

Configuração e operação do nó de arquivamento

Seu sistema StorageGRID gerencia o nó de arquivo como um local onde os objetos são armazenados indefinidamente e são sempre acessíveis.

Quando um objeto é ingerido, cópias são feitas em todos os locais necessários, incluindo nós de arquivo, com base nas regras de gerenciamento do ciclo de vida da informação (ILM) definidas para o seu sistema StorageGRID. O nó de arquivo atua como um cliente para um servidor TSM, e as bibliotecas de cliente TSM são instaladas no nó de arquivo pelo processo de instalação do software StorageGRID. Os dados do objeto direcionados para o nó de arquivo para armazenamento são salvos diretamente no servidor TSM à medida que são recebidos. O nó de arquivo não armazena os dados do objeto antes de salvá-los no servidor TSM, nem realiza agregação de objetos. No entanto, o nó de arquivo pode enviar várias cópias para o servidor TSM em uma única transação quando as taxas de dados são garantidas.

Depois que o nó de arquivo salva os dados do objeto no servidor TSM, os dados do objeto são gerenciados pelo servidor TSM usando suas políticas de ciclo de vida/retenção. Essas políticas de retenção devem ser definidas para serem compatíveis com a operação do nó de arquivo. Ou seja, os dados de objeto salvos pelo nó de arquivo devem ser armazenados indefinidamente e devem sempre ser acessíveis pelo nó de arquivo, a menos que sejam excluídos pelo nó de arquivo.

Não há conexão entre as regras de ILM do sistema StorageGRID e as políticas de ciclo de vida/retenção do servidor TSM. Cada um opera independentemente do outro; no entanto, à medida que cada objeto é ingerido no sistema StorageGRID, você pode atribuir a ele uma classe de gerenciamento TSM. Essa classe de gerenciamento é passada para o servidor TSM junto com os dados do objeto. A atribuição de diferentes classes de gerenciamento a diferentes tipos de objetos permite configurar o servidor TSM para colocar dados

de objetos em diferentes pools de armazenamento ou aplicar diferentes políticas de migração ou retenção, conforme necessário. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

O nó de arquivo pode ser integrado a um servidor TSM novo ou existente; ele não requer um servidor TSM dedicado. Os servidores TSM podem ser compartilhados com outros clientes, desde que o servidor TSM seja dimensionado adequadamente para a carga máxima esperada. O TSM deve ser instalado em um servidor ou máquina virtual separado do nó de arquivo.

É possível configurar mais de um nó de arquivo para gravar no mesmo servidor TSM; no entanto, esta configuração só é recomendada se os nós de arquivo gravarem conjuntos diferentes de dados no servidor TSM. A configuração de mais de um nó de arquivo para gravação no mesmo servidor TSM não é recomendada quando cada nó de arquivo grava cópias dos mesmos dados de objeto no arquivo. No último cenário, ambas as cópias estão sujeitas a um único ponto de falha (o servidor TSM) para o que é suposto ser cópias independentes e redundantes de dados de objeto.

Os nós de arquivamento não fazem uso do componente HSM (Hierarchical Storage Management) do TSM.

Práticas recomendadas de configuração

Quando você está dimensionando e configurando seu servidor TSM, existem práticas recomendadas que você deve aplicar para otimizá-lo para trabalhar com o nó de Arquivo.

Ao dimensionar e configurar o servidor TSM, você deve considerar os seguintes fatores:

- Como o nó de arquivo não agrega objetos antes de salvá-los no servidor TSM, o banco de dados TSM deve ser dimensionado para conter referências a todos os objetos que serão gravados no nó de arquivo.
- O software Archive Node não pode tolerar a latência envolvida na gravação de objetos diretamente na fita ou em outra Mídia removível. Portanto, o servidor TSM deve ser configurado com um pool de armazenamento de disco para o armazenamento inicial de dados salvos pelo nó de arquivo sempre que Mídia removível for usada.
- Você deve configurar políticas de retenção de TSM para usar a retenção baseada em eventos. O nó de arquivo não suporta políticas de retenção de TSM baseadas na criação. Use as seguintes configurações recomendadas de retmin.0 e retver.0 na política de retenção (que indica que a retenção começa quando o nó de arquivamento aciona um evento de retenção e é mantido por 0 dias depois disso). No entanto, esses valores para retmin e retver são opcionais.

O pool de discos deve ser configurado para migrar dados para o pool de fitas (ou seja, o pool de fitas deve ser o NXTSTGPOOL do pool de discos). O pool de fitas não deve ser configurado como um pool de cópias do pool de discos com gravação simultânea em ambos os pools (ou seja, o pool de fitas não pode ser um COPYSTGPOOL para o pool de discos). Para criar cópias off-line das fitas que contêm dados do Archive Node, configure o servidor TSM com um segundo pool de fitas que é um pool de cópias do pool de fitas usado para dados do Archive Node.

Conclua a configuração do nó de arquivo

O nó de arquivo não funciona depois de concluir o processo de instalação. Antes que o sistema StorageGRID possa salvar objetos no nó de arquivo TSM, você deve concluir a instalação e configuração do servidor TSM e configurar o nó de arquivo para se comunicar com o servidor TSM.

Consulte a seguinte documentação da IBM, conforme necessário, enquanto prepara o servidor TSM para integração com o nó de arquivo em um sistema StorageGRID:

- "Guia de instalação e do usuário dos drivers de dispositivo de fita IBM"
- "Referência de programação de drivers de dispositivo de fita IBM"

Instale um novo servidor TSM

Você pode integrar o nó de arquivo a um servidor TSM novo ou existente. Se você estiver instalando um novo servidor TSM, siga as instruções na documentação do TSM para concluir a instalação.

Um nó de arquivo não pode ser co-hospedado com um servidor TSM.

Configure o servidor TSM

Esta seção inclui instruções de exemplo para preparar um servidor TSM seguindo as práticas recomendadas do TSM.

As instruções a seguir o orientam durante o processo de:

- Definir um pool de armazenamento em disco e um pool de armazenamento em fita (se necessário) no servidor TSM
- Definir uma política de domínio que utilize a classe de gestão TSM para os dados guardados a partir do nó de arquivo e registar um nó para utilizar esta política de domínio

Estas instruções são fornecidas apenas para a sua orientação; não se destinam a substituir a documentação do TSM ou a fornecer instruções completas e abrangentes adequadas para todas as configurações. Instruções específicas de implantação devem ser fornecidas por um administrador do TSM que esteja familiarizado com seus requisitos detalhados e com o conjunto completo de documentação do TSM Server.

Defina conjuntos de armazenamento em disco e fita TSM

O nó de arquivamento grava em um pool de armazenamento em disco. Para arquivar conteúdo em fita, você deve configurar o pool de armazenamento em disco para mover o conteúdo para um pool de armazenamento em fita.

Sobre esta tarefa

Para um servidor TSM, você deve definir um pool de armazenamento em fita e um pool de armazenamento em disco no Tivoli Storage Manager. Depois que o pool de discos for definido, crie um volume de disco e atribua-o ao pool de discos. Não é necessário um pool de fitas se o servidor TSM usar storage somente em disco.

Você deve concluir várias etapas em seu servidor TSM antes de criar um pool de armazenamento de fita. (Crie uma biblioteca de fitas e pelo menos uma unidade na biblioteca de fitas. Defina um caminho do servidor para a biblioteca e do servidor para as unidades e, em seguida, defina uma classe de dispositivo para as unidades.) Os detalhes dessas etapas podem variar dependendo da configuração de hardware e dos requisitos de armazenamento do site. Para obter mais informações, consulte a documentação do TSM.

O seguinte conjunto de instruções ilustra o processo. Você deve estar ciente de que os requisitos para o seu site podem ser diferentes, dependendo dos requisitos da sua implantação. Para obter detalhes de

configuração e instruções, consulte a documentação do TSM.

Você deve fazer login no servidor com Privileges administrativo e usar a ferramenta dsmadmc para executar os seguintes comandos.

Passos

1. Crie uma biblioteca de fitas.

   `define library tapelibrary libtype=scsi`

   `_tapelibrary_`Onde é escolhido um nome arbitrário para a biblioteca de fitas, e o valor de `libtype` pode variar dependendo do tipo de biblioteca de fitas.

2. Defina um caminho do servidor para a biblioteca de fitas.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* É o nome do servidor TSM
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu
   - *lib-devicename* é o nome do dispositivo para a biblioteca de fitas

3. Defina uma unidade para a biblioteca.

   `define drive tapelibrary drivename`

   - *drivename* é o nome que você deseja especificar para a unidade
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu

     Você pode querer configurar uma unidade ou unidades adicionais, dependendo da configuração do hardware. (Por exemplo, se o servidor TSM estiver conetado a um switch Fibre Channel que tenha duas entradas de uma biblioteca de fitas, talvez você queira definir uma unidade para cada entrada.)

4. Defina um caminho do servidor para a unidade definida.

   `define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname`

   - *drive-dname* é o nome do dispositivo para a unidade
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu

     Repita para cada unidade definida para a biblioteca de fitas, usando uma unidade *drivename* separada e *drive-dname* para cada unidade.

5. Defina uma classe de dispositivo para as unidades.

   `define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype`

- *DeviceClassName* é o nome da classe de dispositivo
- *lto* é o tipo de unidade conetada ao servidor
- *tapelibrary* é o nome da biblioteca de fitas que você definiu
- *tapetype* é o tipo de fita; por exemplo, ultrium3

6. Adicione volumes de fita ao inventário da biblioteca.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary é o nome da biblioteca de fitas que você definiu.

7. Crie o pool de armazenamento de fita primário.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* É o nome do conjunto de armazenamento de fita do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento de fita (desde que o nome use as convenções de sintaxe esperadas pelo servidor TSM).
   - *DeviceClassName* é o nome do nome da classe do dispositivo para a biblioteca de fitas.
   - *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo: "'conjunto de armazenamento de fita para o nó de arquivo.'"
   - *collocate=filespace* Especifica que o servidor TSM deve gravar objetos do mesmo espaço de arquivo em uma única fita.
   - `XX` é um dos seguintes:
     - O número de fitas vazias na biblioteca de fitas (caso o nó de arquivo seja o único aplicativo que usa a biblioteca).
     - O número de fitas alocadas para uso pelo sistema StorageGRID (nos casos em que a biblioteca de fitas é compartilhada).

8. Em um servidor TSM, crie um pool de armazenamento em disco. Na consola administrativa do servidor TSM, introduza

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* É o nome do conjunto de discos do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento em disco (desde que o nome use as convenções de sintaxe esperadas pelo TSM).
   - *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo, ""conjunto de armazenamento em disco para o nó de arquivo".
   - *maximum_file_size* força objetos maiores do que esse tamanho a serem gravados diretamente na fita, em vez de serem armazenados em cache no pool de discos. Recomenda-se definir *maximum_file_size* para 10 GB.
   - *nextstgpool=SGWSTapePool* Refere o pool de armazenamento em disco ao pool de

armazenamento em fita definido para o nó de arquivo.

- *percent_high* define o valor no qual o pool de discos começa a migrar seu conteúdo para o pool de fitas. Recomenda-se definir *percent_high* como 0 para que a migração de dados comece imediatamente
- *percent_low* define o valor no qual a migração para o conjunto de fitas pára. Recomenda-se definir *percent_low* como 0 para limpar o pool de discos.

9. Em um servidor TSM, crie um volume de disco (ou volumes) e atribua-o ao pool de discos.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* é o nome do pool de discos.
- *volume_name* É o caminho completo para o local do volume (por exemplo, `/var/local/arc/stage6.dsm`) no servidor TSM onde grava o conteúdo do pool de discos em preparação para transferência para fita.
- *size* É o tamanho, em MB, do volume do disco.

  Por exemplo, para criar um único volume de disco de modo que o conteúdo de um pool de discos preencha uma única fita, defina o valor de tamanho como 200000 quando o volume da fita tiver uma capacidade de 200 GB.

  No entanto, pode ser desejável criar vários volumes de disco de um tamanho menor, já que o servidor TSM pode gravar em cada volume no pool de discos. Por exemplo, se o tamanho da fita for de 250 GB, crie 25 volumes de disco com um tamanho de 10 GB (10000) cada.

O servidor TSM prealoca espaço no diretório para o volume de disco. Isso pode levar algum tempo para ser concluído (mais de três horas para um volume de disco de 200 GB).

Defina uma política de domínio e Registre um nó

Você precisa definir uma política de domínio que use a classe de gerenciamento TSM para os dados salvos do nó de arquivamento e, em seguida, Registrar um nó para usar essa diretiva de domínio.

> Os processos do nó de arquivamento podem vazar memória se a senha do cliente para o nó de arquivamento no Tivoli Storage Manager (TSM) expirar. Certifique-se de que o servidor TSM está configurado para que o nome de utilizador/palavra-passe do cliente para o nó de arquivo nunca expire.

Ao Registrar um nó no servidor TSM para o uso do nó de arquivo (ou atualizar um nó existente), você deve especificar o número de pontos de montagem que o nó pode usar para operações de gravação especificando o parâmetro MAXNUMMP para o comando DE NÓ DE REGISTRO. O número de pontos de montagem é normalmente equivalente ao número de cabeças de unidade de fita alocadas ao nó de arquivo. O número especificado para MAXNUMMP no servidor TSM deve ser pelo menos tão grande quanto o valor definido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para o Archive Node, que é definido para um valor de 0 ou 1, já que as sessões de armazenamento simultâneas não são suportadas pelo Archive Node.

O valor de MAXSESSIONS definido para o servidor TSM controla o número máximo de sessões que podem ser abertas para o servidor TSM por todos os aplicativos clientes. O valor de MAXSESSIONS especificado no TSM deve ser pelo menos tão grande quanto o valor especificado para **ARC** > **Target** > **Configuration** >

Main > **Number of Sessions** no Grid Manager para o Archive Node. O nó de arquivo cria simultaneamente, no máximo, uma sessão por ponto de montagem, mais um pequeno número (inferior a 5) de sessões adicionais.

O nó TSM atribuído ao nó de arquivo usa uma política de domínio personalizada `tsm-domain` . A `tsm-domain` política de domínio é uma versão modificada da política de domínio "sandard", configurada para gravar em fita e com o destino do arquivo definido como o pool de armazenamento do sistema StorageGRID (*`SGWSDiskPool`*).

> Você deve fazer login no servidor TSM com Privileges administrativo e usar a ferramenta dsmadmc para criar e ativar a diretiva de domínio.

Crie e ative a política de domínio

Você deve criar uma política de domínio e ativá-la para configurar o servidor TSM para salvar os dados enviados do nó de Arquivo.

Passos

1. Crie uma política de domínio.

   ```
   copy domain standard tsm-domain
   ```

2. Se você não estiver usando uma classe de gerenciamento existente, insira uma das seguintes opções:

   ```
   define policyset tsm-domain standard

   define mgmtclass tsm-domain standard default
   ```

   `default` é a classe de gerenciamento padrão para a implantação.

3. Crie um copygroup para o pool de armazenamento apropriado. Introduza (numa linha):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` É a classe de gerenciamento padrão para o nó de arquivo. Os valores de `retinit`, `retmin` e `retver` foram escolhidos para refletir o comportamento de retenção atualmente utilizado pelo nó de arquivo

   > Não defina `retinit` para `retinit=create`. A configuração `retinit=create` impede que o nó de arquivamento exclua conteúdo, porque os eventos de retenção são usados para remover conteúdo do servidor TSM.

4. Atribua a classe de gerenciamento como padrão.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Defina o novo conjunto de políticas como ativo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore o aviso "'no backup copy group'" que aparece quando você digita o comando Activate.

6. Registre um nó para usar o novo conjunto de políticas no servidor TSM. No servidor TSM, introduza (numa linha):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   ARC-user e ARC-password são o mesmo nome de nó de cliente e palavra-passe definidos no nó de arquivo, e o valor de MAXNUMMP é definido para o número de unidades de fita reservadas para sessões de armazenamento de nó de arquivo.

   > Por padrão, o Registro de um nó cria uma ID de usuário administrativo com autoridade de proprietário do cliente, com a senha definida para o nó.

Migrar dados para o StorageGRID

É possível migrar grandes quantidades de dados para o sistema StorageGRID e, simultaneamente, usar o sistema StorageGRID para operações diárias.

Use este guia para Planejar a migração de grandes quantidades de dados para o sistema StorageGRID. Ele não é um guia geral para a migração de dados e não inclui etapas detalhadas para a execução de uma migração. Siga as diretrizes e instruções nesta seção para garantir que os dados sejam migrados com eficiência para o sistema StorageGRID sem interferir nas operações diárias e que os dados migrados sejam tratados adequadamente pelo sistema StorageGRID.

Confirme a capacidade do sistema StorageGRID

Antes de migrar grandes quantidades de dados para o sistema StorageGRID, confirme se o sistema StorageGRID tem a capacidade de disco para lidar com o volume esperado.

Se o sistema StorageGRID incluir um nó de arquivo e uma cópia de objetos migrados tiver sido salva em armazenamento near-line (como fita), verifique se o armazenamento do nó de arquivamento tem capacidade suficiente para o volume esperado de dados migrados.

Como parte da avaliação de capacidade, observe o perfil de dados dos objetos que você planeja migrar e calcule a quantidade de capacidade de disco necessária. Para obter detalhes sobre como monitorar a capacidade de disco do sistema StorageGRID, consulte "Gerenciar nós de storage" e as instruções para "Monitorização do StorageGRID".

Determine a política de ILM para dados migrados

A política ILM do sistema StorageGRID determina quantas cópias são feitas, os locais para os quais as cópias são armazenadas e por quanto tempo essas cópias são mantidas. Uma política ILM consiste em um conjunto de regras ILM que descrevem como filtrar objetos e gerenciar dados de objetos ao longo do tempo.

Dependendo de como os dados migrados são usados e de seus requisitos de dados migrados, talvez você queira definir regras exclusivas de ILM para dados migrados que são diferentes das regras de ILM usadas para operações diárias. Por exemplo, se houver requisitos regulatórios diferentes para o gerenciamento diário de dados do que os dados incluídos na migração, talvez você queira um número diferente de cópias dos dados migrados em um nível diferente de storage.

Você pode configurar regras que se aplicam exclusivamente aos dados migrados se for possível distinguir de forma exclusiva entre dados migrados e dados de objetos salvos de operações diárias.

Se você puder distinguir de forma confiável entre os tipos de dados usando um dos critérios de metadados, use esses critérios para definir uma regra de ILM que se aplica apenas aos dados migrados.

Antes de iniciar a migração de dados, certifique-se de que compreende a política de ILM do sistema StorageGRID e de que forma será aplicada aos dados migrados e de que fez e testou quaisquer alterações à política ILM. "Gerenciar objetos com ILM"Consulte .

> Uma política de ILM que foi incorretamente especificada pode causar perda de dados irrecuperável. Revise cuidadosamente todas as alterações feitas em uma política ILM antes de ativá-la para garantir que a política funcionará conforme pretendido.

Avaliar o impactos da migração nas operações

O sistema StorageGRID foi desenvolvido para fornecer operações eficientes de storage e recuperação de objetos, além de fornecer excelente proteção contra a perda de dados por meio da criação otimizada de cópias redundantes de dados de objetos e metadados.

No entanto, a migração de dados deve ser cuidadosamente gerenciada de acordo com as instruções deste guia para evitar ter impacto nas operações diárias do sistema ou, em casos extremos, colocar os dados em risco de perda em caso de falha no sistema StorageGRID.

A migração de grandes quantidades de dados coloca carga adicional no sistema. Quando o sistema StorageGRID está muito carregado, ele responde mais lentamente às solicitações para armazenar e recuperar objetos. Isso pode interferir com as solicitações de armazenamento e recuperação que são parte integrante das operações diárias. A migração também pode causar outros problemas operacionais. Por exemplo, quando um nó de armazenamento está próximo da capacidade, a carga intermitente pesada devido à ingestão de lote pode fazer com que o nó de armazenamento alterne entre somente leitura e leitura-gravação, gerando notificações.

Se o carregamento pesado persistir, as filas podem se desenvolver para várias operações que o sistema StorageGRID deve executar para garantir a redundância total dos dados e metadados do objeto.

A migração de dados deve ser cuidadosamente gerenciada de acordo com as diretrizes deste documento para garantir o funcionamento seguro e eficiente do sistema StorageGRID durante a migração. Ao migrar dados, ingira objetos em lotes ou controle continuamente a ingestão. Em seguida, monitore continuamente o sistema StorageGRID para garantir que vários valores de atributo não sejam excedidos.

Agendar e monitorar a migração de dados

A migração de dados deve ser agendada e monitorada conforme necessário para garantir que os dados sejam colocados de acordo com a política de ILM dentro do prazo exigido.

Agendar a migração de dados

Evite migrar dados durante o horário operacional principal. Limite a migração de dados para noites, fins de semana e outras ocasiões em que o uso do sistema é baixo.

Se possível, não programe a migração de dados durante períodos de alta atividade. No entanto, se não for prático evitar completamente o período de atividade elevada, é seguro prosseguir desde que monitorize de perto os atributos relevantes e tome medidas se excederem os valores aceitáveis.

Monitorar a migração de dados

Esta tabela lista os atributos que você deve monitorar durante a migração de dados e os problemas que eles representam.

Se você usar políticas de classificação de tráfego com limites de taxa para reduzir a ingestão, poderá monitorar a taxa observada em conjunto com as estatísticas descritas na tabela a seguir e reduzir os limites, se necessário.

Monitorar	Descrição
Número de objetos aguardando avaliação ILM	1. Selecione **SUPPORT** > **Tools** > **Grid topology**. 2. Selecione ***deployment*** > **Overview** > **Main**. 3. Na seção ILM Activity, monitore o número de objetos mostrados para os seguintes atributos: ◦ **Aguardando - todos (XQUZ)**: O número total de objetos aguardando avaliação ILM. ◦ **Aguardando - Cliente (XCQZ)**: O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest). 4. Se o número de objetos mostrados para qualquer um desses atributos exceder 100.000, diminua a taxa de ingestão de objetos para reduzir a carga no sistema StorageGRID.
Capacidade de armazenamento do sistema de arquivamento direcionado	Se a política de ILM salvar uma cópia dos dados migrados para um sistema de armazenamento de arquivamento de destino (fita ou nuvem), monitore a capacidade do sistema de armazenamento de arquivamento de destino para garantir que haja capacidade suficiente para os dados migrados.
Archive Node > **ARC** > **Store**	Se um alarme para o atributo **Store Failures (ARVF)** for acionado, o sistema de armazenamento de arquivos alvo pode ter atingido a capacidade. Verifique o sistema de armazenamento de arquivos alvo e resolva quaisquer problemas que acionaram um alarme.

Informações sobre direitos autorais

Informações sobre marcas comerciais