Administrar StorageGRID

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/pt-br/storagegrid-120/admin/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

Índice

Administrar StorageGRID . . . 1
Administrar StorageGRID . . . 1
Sobre estas instruções . . . 1
Antes de começar . . . 1
Comece a usar o Grid Manager . . . 1
Requisitos do navegador web para StorageGRID . . . 1
Faça login no StorageGRID Grid Manager . . . 2
Saia do StorageGRID Grid Manager . . . 4
Altere sua senha do StorageGRID Grid Manager . . . 4
Veja as informações da licença do StorageGRID . . . 5
Atualizar informações de licença do StorageGRID . . . 6
Use o API . . . 6
Controle o acesso ao StorageGRID . . . 28
Controlar o acesso ao StorageGRID . . . 28
Alterar a senha de provisionamento do StorageGRID . . . 29
Alterar senhas do console do nó em StorageGRID . . . 30
Alterar as senhas de acesso SSH para os nós de administração do StorageGRID . . . 32
Use a federação de identidades no StorageGRID . . . 34
Gerenciar grupos de administradores no StorageGRID . . . 39
Permissões do grupo de administradores no StorageGRID . . . 42
Gerenciar usuários no StorageGRID . . . 45
Use o single sign-on (SSO) . . . 49
Use a federação de grid . . . 73
Saiba mais sobre a federação de grids StorageGRID . . . 73
Saiba mais sobre clonagem de contas no StorageGRID . . . 76
Saiba mais sobre replicação entre grids no StorageGRID . . . 79
Compare a replicação entre grades e a replicação CloudMirror no StorageGRID . . . 86
Criar conexões de federação de grids StorageGRID . . . 88
Gerenciar conexões de federação de grids do StorageGRID . . . 91
Gerencie os locatários permitidos para a federação de grids do StorageGRID . . . 96
Solucionar problemas de erros de federação de grid no StorageGRID . . . 102
Identifique e repita operações de replicação do StorageGRID que falharam . . . 107
Gerenciar segurança . . . 111
Gerenciar a segurança no StorageGRID . . . 111
Revise os métodos de criptografia do StorageGRID . . . 112
Gerenciar certificados . . . 115
Configurar as configurações de segurança . . . 148
Configurar os servidores de gerenciamento de chaves . . . 155
Gerenciar configurações de proxy . . . 175
Controlar firewalls . . . 176
Gerenciar locatários . . . 183
Contas de locatário no StorageGRID . . . 183
Crie uma conta de locatário do StorageGRID . . . 185

Editar uma conta de locatário do StorageGRID . . . 190
Alterar a senha do usuário raiz local do StorageGRID tenant . . . 192
Excluir uma conta de locatário do StorageGRID . . . 192
Gerenciar serviços de plataforma . . . 193
Gerenciar o S3 Select para contas de locatário no StorageGRID . . . 202
Configurar conexões de cliente . . . 203
Configurar conexões do cliente S3 ao StorageGRID . . . 203
Segurança para clientes S3 no StorageGRID . . . 206
Use o assistente de instalação S3 . . . 207
Gerenciar grupos de alta disponibilidade . . . 216
Gerenciar balanceamento de carga . . . 227
Configurar os nomes de domínio dos endpoints do S3 no StorageGRID . . . 242
Endereços IP e portas para conexões de clientes StorageGRID . . . 244
Gerenciar redes e conexões . . . 246
Configurar as configurações de rede do StorageGRID . . . 246
Diretrizes para redes StorageGRID . . . 246
Visualizar endereços IP no StorageGRID . . . 248
Configurar interfaces VLAN no StorageGRID . . . 249
Habilite o CORS do StorageGRID para uma interface de gerenciamento . . . 253
Gerenciar políticas de classificação de tráfego . . . 254
Cifras suportadas para conexões TLS de saída no StorageGRID . . . 261
Benefícios das conexões HTTP ativas, ociosas e simultâneas no StorageGRID . . . 262
Gerencie os custos de link no StorageGRID . . . 264
Use o AutoSupport . . . 266
Saiba mais sobre AutoSupport no StorageGRID . . . 266
Configurar AutoSupport em StorageGRID . . . 271
Acionar manualmente um pacote AutoSupport no StorageGRID . . . 275
Solucionar problemas dos pacotes AutoSupport do StorageGRID . . . 276
Envie pacotes E-Series AutoSupport através do StorageGRID . . . 277
Gerenciar nós de armazenamento . . . 281
Use as opções de armazenamento . . . 281
Gerencie o armazenamento de metadados de objetos no StorageGRID . . . 284
Aumente a configuração de Espaço Reservado para Metadados no StorageGRID . . . 291
Compactar objetos armazenados no StorageGRID . . . 293
Gerencie nós de armazenamento completos no StorageGRID . . . 294
Gerenciar nós de administração . . . 294
Use vários nós de administração no StorageGRID . . . 294
Identifique o nó de administração principal no StorageGRID . . . 296

Administrar StorageGRID

Administrar StorageGRID

Utilize estas instruções para configurar e administrar um sistema StorageGRID.

Sobre estas instruções

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

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

Antes de começar

- Você possui um conhecimento geral do sistema StorageGRID.
- Você possui um conhecimento bastante detalhado de shells de comando Linux, rede e configuração e instalação de hardware de servidor.

Comece a usar o Grid Manager

Requisitos do navegador web para StorageGRID

Você precisa usar um navegador web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Defina a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Faça login no StorageGRID Grid Manager

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

Cada sistema StorageGRID inclui um nó administrativo primário e qualquer número de nós administrativos não primários. Você pode acessar o Grid Manager em qualquer nó administrativo para gerenciar o sistema StorageGRID. No entanto, alguns procedimentos de manutenção só podem ser realizados a partir do nó administrativo primário.

Conecte-se ao grupo HA

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

Use o SSO

Os passos para iniciar sessão são ligeiramente diferentes se "O single sign-on (SSO) foi configurado".

Faça login no Grid Manager no primeiro nó de administração

Antes de começar

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

  `https://FQDN_or_Admin_Node_IP/`

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

  Para acessar o Gerenciador de Grade em uma porta diferente da porta padrão para HTTPS (443), inclua o número da porta na URL:

  `https://FQDN_or_Admin_Node_IP:port/`

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

Passos

1. Inicie um navegador web compatível.
2. Na barra de endereços do navegador, digite a URL do Grid Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. Veja "Gerenciar certificados de segurança".

4. Faça login no Grid Manager.

   A tela de login que aparece depende se o single sign-on (SSO) foi configurado para StorageGRID.

   Não usar SSO

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

   b. Selecione **Entrar**.

   Utilizando SSO

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

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

     ii. Insira suas credenciais padrão de SSO na página de SSO da sua organização.

     Por exemplo, se StorageGRID estiver usando SSO e você já tiver acessado o Grid Manager ou uma conta de tenant:

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

     B. Selecione **Sign in**.

     C. Faça login com suas credenciais SSO padrão na página de login SSO da sua organização.

Ao iniciar sessão, a página inicial do Grid Manager é exibida, incluindo o dashboard. Para saber quais informações são fornecidas, consulte "Visualize e gerencie o painel de controle".

Faça login em outro nó de administração

Siga estas etapas para entrar em outro nó de administração.

Não usar SSO

Passos

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

Utilizando SSO

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

Passos

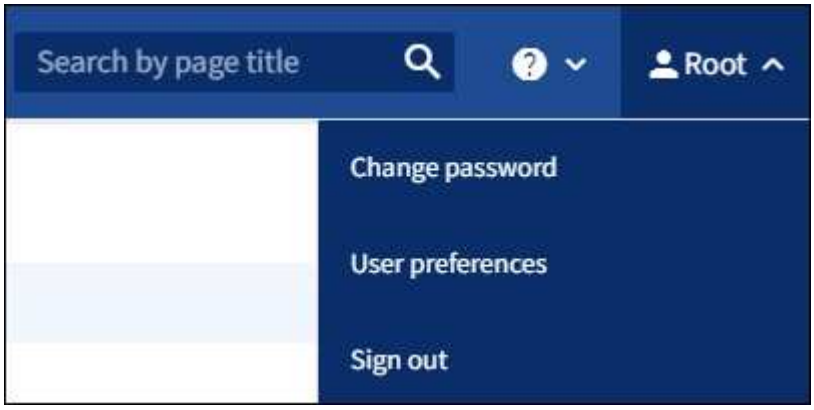
1. Digite o domínio totalmente qualificado ou endereço IP do outro nó de administração na barra de endereços do navegador.
2. Se a sua sessão SSO expirou, insira suas credenciais novamente.

Saia do StorageGRID Grid Manager

Ao terminar de usar o Grid Manager, você deve sair para garantir que usuários não autorizados não acessem o sistema StorageGRID. Fechar o navegador pode não encerrar sua sessão no sistema, dependendo das configurações de cookies do navegador.

Passos

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



2. Selecione **Sair**.

Opção	Descrição
SSO não está em uso	Você foi desconectado do nó de administração. A página de login do Grid Manager é exibida. **Nota:** Se você fez login em mais de um nó de administração, você deve sair de cada um deles.
SSO ativado	Você foi desconectado de todos os Admin Nodes que estava acessando. A página de login do StorageGRID é exibida. **Grid Manager** está listado como padrão na lista suspensa **Contas Recentes**, e o campo **Account ID** mostra 0. **Nota:** Se o SSO estiver ativado e você também estiver conectado ao Gerenciador de Locatários, você também deve "sair da conta do tenant" para "sair do SSO".

Altere sua senha do StorageGRID Grid Manager

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

Antes de começar

Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

Sobre esta tarefa

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

Passos

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

   Sua senha deve conter no mínimo 8 e no máximo 32 caracteres. As senhas diferenciam maiúsculas de minúsculas.
4. Digite novamente a nova senha.
5. Selecione **Salvar**.

Veja as informações da licença do StorageGRID

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

Antes de começar

Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

Sobre esta tarefa

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

Passos

1. Acesse a página de Licença realizando um dos seguintes procedimentos:
   - Selecione **Manutenção** > **Sistema** > **Licença**.
   - No cartão de status de saúde no painel de controle, selecione o ícone de status da licença ou o link **License**.

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

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

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

    - Conteúdo do arquivo de texto da licença

Atualizar informações de licença do StorageGRID

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

Antes de começar

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

Passos

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

   O novo arquivo de licença é validado e exibido.

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

Use o API

Use a API de gerenciamento de grid do StorageGRID

Você pode executar tarefas de gerenciamento do sistema usando a API REST de gerenciamento do Grid 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 alto nível

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

- `/grid`: O acesso é restrito aos usuários do Grid Manager e baseia-se nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte "Use uma conta de tenant".
- `/private`: O acesso é restrito a 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 Grid utiliza a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

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

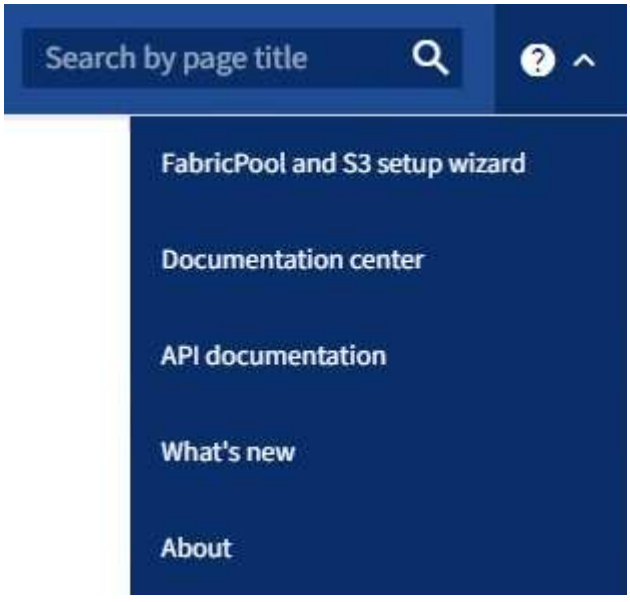
Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

> Qualquer operação de API realizada por meio da página de documentação da API é uma operação em tempo real. 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 **API documentation**.



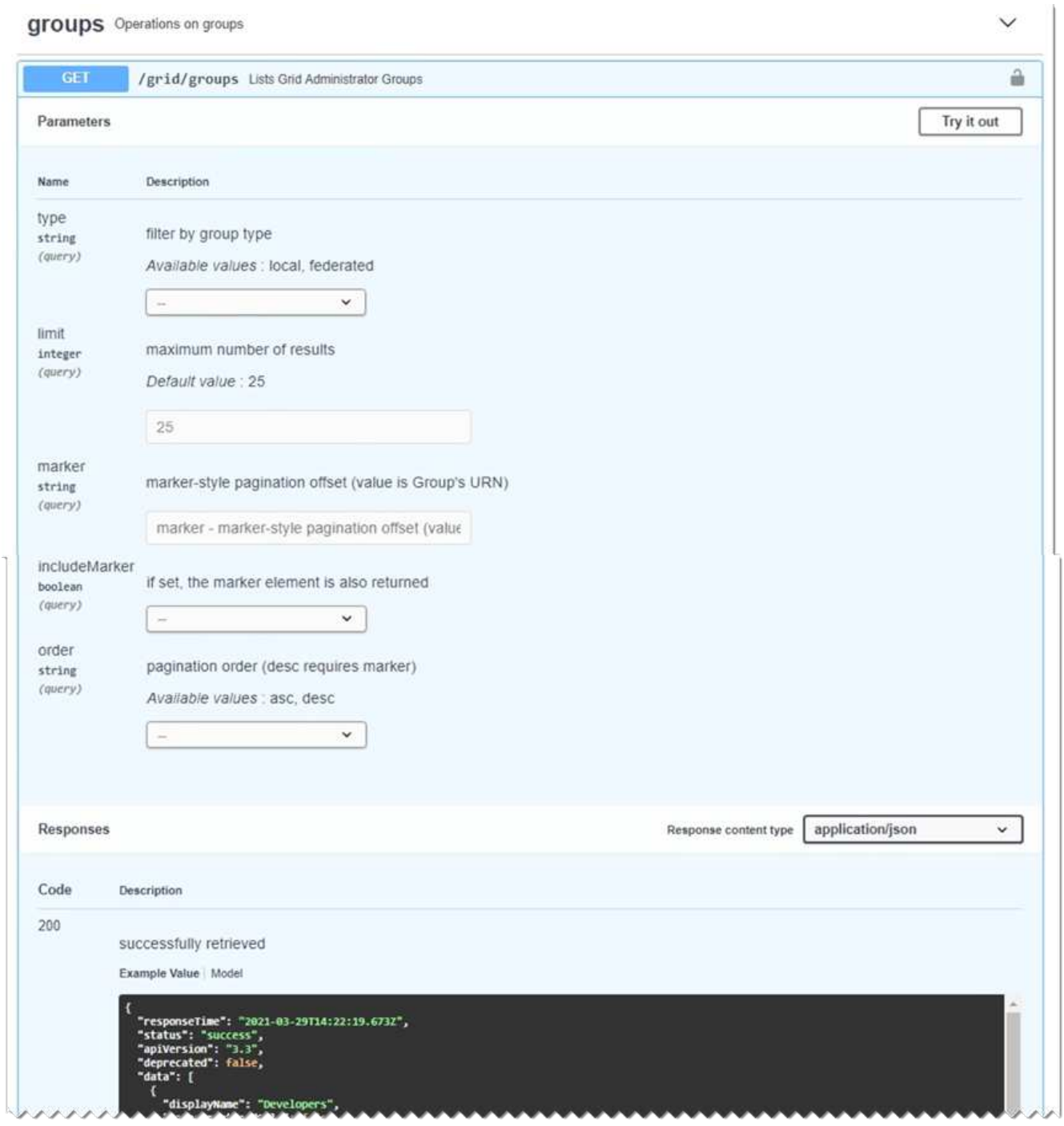
2. Para executar uma operação com a API privada, selecione **Acessar a documentação da API privada** na página da API de gerenciamento do StorageGRID.

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 da API, você pode visualizar 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 parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



5. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou de usuário. Em

seguida, obtenha esses valores. Pode ser necessário fazer uma solicitação de API diferente primeiro para obter as informações de que você precisa.

6. Determine se você precisa modificar o corpo da solicitação de exemplo. Caso precise, selecione **Model** para conhecer os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça todos os parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Analise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grid no StorageGRID

A API de Gerenciamento de Grid organiza as operações disponíveis nas seguintes seções.

> Esta lista inclui apenas as operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo criar novas contas e recuperar o uso de armazenamento para uma determinada conta.
- **histórico de alertas**: operações em alertas resolvidos.
- **receptores de alertas**: Operações em receptores de notificações de alerta (email).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **auditoria**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grid suporta o esquema de autenticação Bearer Token. Para fazer login, você fornece um nome de usuário e uma senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho das solicitações de API subsequentes ("Authorization: Bearer *token*"). O token expira após 16 horas.

  > Se o single sign-on estiver habilitado para o StorageGRID, você deve executar etapas diferentes para autenticar. Consulte "Autenticando na API se o single sign-on estiver habilitado".

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

- **client-certificates**: Operações para configurar certificados de cliente para que StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **config**: Operações relacionadas ao lançamento do produto e às versões da API de Gerenciamento de Grid. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grid suportadas por esse lançamento, além de desativar versões obsoletas da API.
- **recursos-desativados**: operações para visualizar recursos que podem ter sido desativados.
- **servidores-dns**: Operações para listar e alterar servidores DNS externos configurados.

- **drive-details**: Operações em unidades para modelos específicos de dispositivos de storage.
- **endpoint-domain-names**: Operações para listar e alterar nomes de domínio de endpoint do S3.
- **erasure-coding**: Operações em perfis de codificação de apagamento.
- **expansão**: operações de expansão (nível de procedimento).
- **expansion-nodes**: Operações em expansão (nível de nó).
- **locais de expansão**: Operações em expansão (nível do local).
- **grid-networks**: Operações para listar e alterar a Lista de Redes da Grid.
- **grid-passwords**: operações para gerenciamento de senhas em grid.
- **grupos**: Operações para gerenciar grupos de administradores de Grid locais e para recuperar grupos de administradores de Grid federados de um servidor LDAP externo.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo e usuário federados.
- **ilm**: Operações de gerenciamento do ciclo de vida das informações (ILM).
- **procedimentos-em-andamento**: Recupera os procedimentos de manutenção que estão atualmente em andamento.
- **licença**: Operações para recuperar e atualizar a licença do StorageGRID.
- **logs**: Operações para coletar e baixar arquivos de log.v
- **metrics**: Operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas em um ponto único no tempo e consultas de métricas de intervalo ao longo de um período de tempo. A Grid Management API utiliza a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de backend. Para obter informações sobre como construir consultas Prometheus, consulte o site do Prometheus.

  > As métricas que incluem `private` em seus nomes destinam-se apenas ao uso interno. Essas métricas estão sujeitas a alterações entre versões do StorageGRID sem aviso prévio.

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

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

Controle de versão da Grid Management API no StorageGRID

A API de gerenciamento de grid utiliza versionamento para suportar atualizações não disruptivas.

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

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

A versão principal da API é atualizada quando são feitas alterações que *não são compatíveis* com versões anteriores. A versão secundária da API é atualizada quando são feitas alterações que *são compatíveis* com versões anteriores. Alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

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

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

Ao instalar o software StorageGRID pela primeira vez, apenas a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recursos do StorageGRID, você continua tendo acesso à versão anterior da API por pelo menos uma versão de recursos do StorageGRID.

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

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho da resposta é "Deprecated: true"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso de descontinuação é adicionado ao nms.log. Por exemplo:

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

Determine quais versões da API são compatíveis na versão atual

Use a solicitação `GET /versions` à API para retornar uma lista das versões principais da API suportadas. Essa solicitação está localizada na seção **config** da documentação da API Swagger.

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

Especifique uma versão da API para uma solicitação

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

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

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

Proteja contra ataques de falsificação de solicitação entre sites (CSRF) no StorageGRID

Você pode ajudar a proteger contra ataques de Cross-Site Request Forgery (CSRF) ao StorageGRID usando tokens CSRF para aprimorar a autenticação que utiliza cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao fazer login.

Um atacante capaz de enviar uma solicitação para um site diferente (como por meio de um formulário HTTP POST) pode fazer com que determinadas solicitações sejam realizadas usando os cookies do usuário autenticado.

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 no corpo de uma POST.

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

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

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

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

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

Consulte a documentação da API online para obter exemplos e detalhes adicionais.

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

Use a API se o single sign-on estiver ativado

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

Se você tem "configurou e ativou o single sign-on (SSO)" e utiliza o Active Directory como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

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

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

- Um exemplo de fluxo de trabalho com requisições curl.

  O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá 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 seguinte erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py`script Python. Vá para o passo 2.
   - Use requisições curl. Vá 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. Digite ADFS ou adfs.
   - O nome de usuário SSO
   - O domínio onde StorageGRID está instalado
   - O endereço do StorageGRID
   - O ID da conta do locatário, caso você queira acessar a Tenant Management API.

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

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

   a. Declare as variáveis necessárias para efetuar o login.

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

Para acessar a API de Gerenciamento de Grid, use 0 como `TENANTACCOUNTID`.

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

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

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

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

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

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

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

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

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

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

A resposta inclui o ID da solicitação do cliente:

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

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

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

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

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

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

Se a autenticação multifator (MFA) estiver habilitada para o seu sistema SSO, o formulário enviado 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 da autenticação POST.

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

Os cabeçalhos da resposta conterão informações da sessão do AD FS para uso posterior no logout, e o corpo da resposta conterá o SAMLResponse em um campo de formulário oculto.

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

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

i. Salve o `SAMLResponse` do campo oculto:

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

j. Utilizando o valor salvo `SAMLResponse`, faça uma solicitação StorageGRID `/api/saml-response`

para gerar um token de autenticação do StorageGRID.

Para `RelayState`, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da Grid Management API ou da Tenant Management API. Essas instruções se aplicam se você estiver usando Active Directory como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe o 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
```

Uma URL de logout é retornada:

```
{
    "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 a 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 StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via 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 de portador do StorageGRID.

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

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

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

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

Use a API do StorageGRID se o single sign-on estiver ativado (Entra ID)

Se você possui "configurou e ativou o single sign-on (SSO)" e utiliza o Entra ID como provedor de SSO, pode usar dois scripts de exemplo para obter um token de autenticação válido para a Grid Management API ou para a Tenant Management API.

Faça login na API se o single sign-on do Entra ID estiver ativado

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

Antes de começar

- Você conhece o endereço de e-mail e a senha de SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

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

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

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

Para criar sua própria integração de API com o Entra ID, consulte o `storagegrid-ssoauth-azure.py`script. O script em Python faz duas requisições diretamente ao StorageGRID (primeiro para obter o SAMLRequest e, posteriormente, para obter o token de autorização) e também chama o script em Node.js para interagir com o Entra ID e realizar as operações de SSO.

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

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

Passos

1. Instale as dependências necessárias, conforme a seguir:
   a. Instale o Node.js (consulte "https://nodejs.org/en/download/").

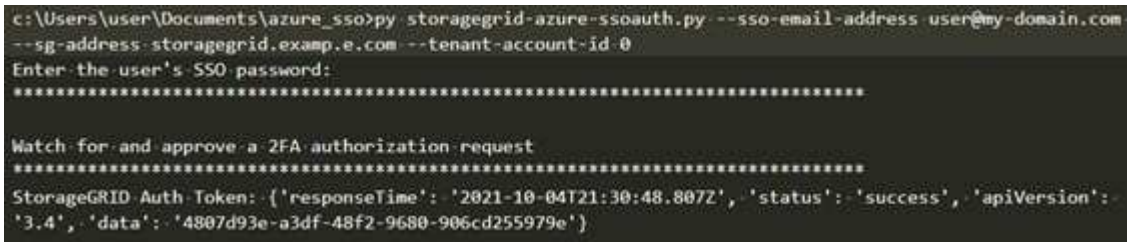
b. Instale os módulos Node.js necessários (puppeteer e jsdom):

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

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

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

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



> O script pressupõe que a autenticação multifator (MFA) seja feita usando o Microsoft Authenticator. Pode ser necessário modificar o script para suportar outras formas de MFA (como inserir um código recebido por mensagem de texto).

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

Use a API do StorageGRID se o login único estiver ativado (PingFederate)

Se você tem "configurou e ativou o single sign-on (SSO)" e utiliza PingFederate como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

Sobre esta tarefa

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

- O `storagegrid-ssoauth.py`script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (./rpms`para RHEL, `./debs`para Ubuntu ou Debian, e `./vsphere`para VMware).
- Um exemplo de fluxo de trabalho com requisições curl.

  O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá 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 seguinte erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py`script Python. Vá para o passo 2.
   - Use requisições curl. Vá 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 StorageGRID está instalado. Este campo não é utilizado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
   - O endereço do StorageGRID
   - O ID da conta do locatário, caso você queira acessar a Tenant Management API.

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

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

   a. Declare as variáveis necessárias para efetuar o login.

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

Para acessar a API de Gerenciamento de Grid, use 0 como `TENANTACCOUNTID`.

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

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

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

A resposta para este exemplo inclui uma URL assinada que está codificada em 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 exiba 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 exiba a resposta:

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

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

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

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

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

g. Exporte o valor de "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. Utilizando o valor salvo `SAMLResponse`, faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação do StorageGRID.

Para `RelayState`, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da API de Gerenciamento de Grid ou da API de Gerenciamento de Locatários. Essas instruções se aplicam se você estiver usando PingFederate como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe o 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
```

Uma URL de logout é retornada:

```
{
    "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 a 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 StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via 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 de portador do StorageGRID.

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

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

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

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

Desative os recursos do StorageGRID com a API

Você pode usar a API de Gerenciamento de Grid 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 Recursos Desativados permite impedir o acesso a determinados recursos no sistema StorageGRID. Desativar um recurso é a única maneira de impedir que o usuário raiz ou usuários pertencentes a grupos de administradores com permissão de **acesso à raiz** possam usar esse recurso.

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

A Company A é uma prestadora de serviços que aluga a capacidade de storage do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos dos seus locatários, a Company A deseja garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a implantação da conta.

A Company A pode atingir esse objetivo usando o sistema Deactivate Features na Grid Management API. Ao desativar completamente o recurso **Change tenant root password** no Grid Manager (tanto na interface de usuário quanto na API), a Company A garante que usuários Admin — incluindo o usuário raiz e usuários pertencentes a grupos com a permissão **Root access** — não possam alterar a senha do usuário raiz de nenhuma conta de tenant.

Passos

1. Acesse a documentação Swagger para a API de Gerenciamento de Grid. Veja "Use a API de gerenciamento de grid".
2. Localize o endpoint Desativar recursos.
3. Para desativar um recurso, como Alterar a senha raiz do locatário, envie um corpo para a API assim:

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

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

Reativar funcionalidades desativadas

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

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

Passos

1. Acesse a documentação Swagger para a API de gerenciamento de Grid.
2. Localize o endpoint Desativar recursos.
3. Para reativar todas as funcionalidades, envie um corpo para a API da seguinte forma:

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

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

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

Controle o acesso ao StorageGRID

Controlar o acesso ao StorageGRID

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

Controle o acesso ao Grid Manager

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

Usar "federação de identidade" torna a configuração de "grupos" e "usuários" mais rápida e permite que os usuários façam login no StorageGRID usando credenciais já conhecidas. Você pode configurar a federação de identidades se usar Active Directory, OpenLDAP ou Oracle Directory Server.

> Contate o suporte técnico se você quiser usar 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 de ILM e os usuários de outro grupo possam executar tarefas de manutenção. Um usuário deve pertencer a pelo menos um grupo para acessar o sistema.

Opcionalmente, você pode configurar um grupo como somente leitura. Usuários em um grupo somente leitura podem apenas visualizar configurações e recursos. Eles não podem fazer alterações nem executar operações no Grid Manager ou na Grid Management API.

Ativar single sign-on

O sistema StorageGRID suporta autenticação única (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0). Após você "configurar e habilitar SSO", todos os usuários devem ser autenticados por um provedor de identidade externo antes de poderem acessar o Grid Manager, o Tenant Manager, a API de gerenciamento do Grid ou a API de gerenciamento do Tenant. Usuários locais não podem fazer login no StorageGRID.

Alterar senha de provisionamento

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

Alterar senhas do console do nó

Cada nó em sua grade possui uma senha de console do nó, que você precisa para fazer login no nó como "admin" usando SSH ou como usuário raiz em uma conexão de console física/VM. Conforme necessário, você pode "alterar a senha do console do nó" para cada nó.

Alterar a senha de provisionamento do StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você possui permissões de acesso de manutenção ou root.
- Você possui a senha de provisionamento atual.

Sobre esta tarefa

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

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Senhas da grade**.
2. Em **Alterar senha de provisionamento**, selecione **Fazer uma alteração**
3. Digite sua senha de provisionamento atual.
4. Digite a nova senha. A senha deve conter no mínimo 8 e no máximo 32 caracteres. Senhas diferenciam maiúsculas de minúsculas.

   Guarde a senha de provisionamento em um local seguro. Ela é necessária para os procedimentos de instalação, expansão e manutenção.

5. Digite novamente a nova senha e selecione **Salvar**.

   O sistema exibe uma faixa verde de sucesso quando a alteração da senha de provisionamento é concluída.

6. Selecione **Recovery Package**.

7. Insira a nova senha de provisionamento para baixar o novo pacote de recuperação.

> Após alterar a senha de provisionamento, você deve baixar imediatamente um novo pacote de recuperação. O arquivo do pacote de recuperação permite restaurar o sistema em caso de falha.

Alterar senhas do console do nó em StorageGRID

Cada nó em sua grade possui uma senha de console do nó, que você usa para fazer login no nó. Por padrão, cada nó tem uma senha única. Você pode alterar cada senha para uma nova senha única ou pode alterar a senha de todos os nós para usar uma senha global. As senhas são armazenadas no pacote de recuperação.

Antes de começar

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

Sobre esta tarefa

Você usa a senha do console do nó para fazer login em um nó como "admin" usando SSH ou como usuário raiz em uma conexão de console de VM/física. Você pode alterar as senhas do console do nó usando uma destas opções:

- Aplicar automaticamente senhas aleatórias a cada nó
- Especifique e aplique uma senha global a todos os nós
- Especifique e aplique uma senha exclusiva a um ou mais nós

As senhas são armazenadas em um arquivo `Passwords.txt`atualizado no pacote de recuperação. As senhas estão listadas na coluna "Senha" no arquivo.

> O "Senhas de acesso SSH" das chaves SSH usadas para comunicação entre os nós é separado das senhas do console do nó. Este procedimento não altera as senhas de acesso SSH.

Acesse o assistente

Passos

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

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 contidas neste arquivo caso o processo de alteração de senha falhe em qualquer nó.

Passos

1. Insira a senha de provisionamento para seu grid.
2. Selecione **Baixar pacote de recuperação**.

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

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

4. Selecione **Continue**.

Forneça novas senhas

1. Selecione o método de alteração de senha que você deseja usar.
   - **Automático**: StorageGRID atribui automaticamente uma nova senha de console aleatória a todos os nós.
   - **Personalizado**: Você fornece as senhas do console.

Automático

1. Selecione **Continue**.

Personalizado

1. Selecione uma das seguintes opções:
   - **Senha global do console**: aplique a mesma senha do console a todos os nós.
   - **Senhas de console exclusivas**: aplique uma senha diferente em um ou mais nós.
2. Se você selecionou **Senha do console global**, insira a senha que você deseja usar para todos os nós.
3. Se você selecionou **Senhas exclusivas do console**, insira uma senha exclusiva para um ou mais nós.
4. Selecione **Continue**.

Conclua a alteração de senha

1. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se você estiver pronto para que StorageGRID comece a alterar as senhas do console do nó.

   Não é possível cancelar esse processo depois que ele for iniciado.

   StorageGRID gera um novo pacote de recuperação contendo a nova senha.

2. Quando o novo pacote de recuperação estiver pronto, selecione **Baixar novo pacote de recuperação** e salve o pacote de recuperação.
3. Abra o arquivo `.zip`.
4. Confirme se você tem acesso ao conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas senhas do console do nó.
5. Copie o novo arquivo do pacote de recuperação (`.zip` para dois locais seguros, protegidos e separados.

   Não sobrescreva o pacote de recuperação antigo.

   Você deve proteger o arquivo de recuperação, pois ele contém chaves de criptografia e senhas que

podem ser usadas para obter dados do sistema StorageGRID.

6. Selecione a caixa de seleção para indicar que você baixou o novo pacote de recuperação e verificou o conteúdo.
7. Selecione **Continue**.

   StorageGRID atualiza a senha de cada nó.

   Se ocorrer um erro durante o processo de atualização, a barra de progresso exibirá o número de nós que não tiveram suas senhas alteradas. O sistema tentará novamente o processo automaticamente em qualquer nó que não teve sua senha alterada. Se o processo terminar com alguns nós ainda sem a senha alterada, o botão **Retry** será exibido.

8. Se a atualização da senha falhar em um ou mais nós:
   a. Analise as mensagens de erro listadas na tabela.
   b. Resolva os problemas.
   c. Selecione **Tentar novamente**.

   > A nova tentativa altera apenas as senhas do console dos nós que falharam durante as tentativas anteriores de alteração de senha.

9. Quando a barra de progresso indicar que não há mais atualizações restantes, selecione **Concluir**.
10. Após alterar as senhas do console de todos os nós, exclua o primeiro pacote de recuperação que você baixou.

Alterar as senhas de acesso SSH para os nós de administração do StorageGRID

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

Utilize uma chave SSH para fazer login em um nó como `admin` ou como usuário raiz em uma máquina virtual ou conexão de console físico.

Antes de começar

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

Sobre esta tarefa

As novas senhas de acesso para os Nós de Administração e as novas chaves internas para cada nó estão armazenadas no `Passwords.txt` arquivo no pacote de recuperação. As chaves estão listadas na coluna Senha desse arquivo.

Existem senhas de acesso SSH separadas para as chaves SSH usadas na comunicação entre os nós. Essas senhas não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Senhas da grid**.
2. Em **Alterar chaves SSH**, selecione **Fazer uma alteração**.

Baixe o pacote de recuperação atual

Antes de alterar as chaves de acesso SSH, baixe o pacote de recuperação atual. Você pode usar as chaves neste arquivo caso o processo de alteração de chaves falhe em qualquer nó.

Passos

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

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

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

   Não é possível cancelar esse processo depois que ele for iniciado.

Alterar chaves de acesso SSH

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

Passos

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

   a. Abra o arquivo `.zip`.

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

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

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

   Se as chaves forem alteradas para todos os nós, uma faixa verde de sucesso aparece.

   Se ocorrer um erro durante o processo de atualização, uma mensagem em destaque lista o número de nós que não tiveram suas chaves alteradas. O sistema tentará automaticamente repetir o processo em qualquer nó que não teve sua chave alterada. Se o processo terminar com alguns nós ainda sem a chave alterada, o botão **Retry** será exibido.

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

   a. Analise as mensagens de erro listadas na tabela.
   b. Resolva os problemas.
   c. Selecione **Tentar novamente**.

      A nova tentativa altera apenas as chaves de acesso SSH nos nós que falharam durante as tentativas anteriores de alteração de chave.

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

Use a federação de identidades no StorageGRID

Utilizar a federação de identidades torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configurar a federação de identidades para o Grid Manager

Você pode configurar a federação de identidades no Grid Manager se você quiser que grupos de administradores e usuários sejam gerenciados em outro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Antes de começar

- Você está conectado ao Grid Manager usando um "navegador web compatível".
- Você "permissões de acesso específicas".
- Você está usando Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server como provedor de identidade.

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

- Se você planeja usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Veja Diretrizes para configurar um servidor OpenLDAP.
- Se você planeja habilitar o login único (SSO), você revisou o "Requisitos e considerações para single sign-on".
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1.2 ou 1.3. Consulte "Cifras suportadas para conexões TLS de

saída".

Sobre esta tarefa

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

- Grupos de administradores. Os usuários em grupos de administradores podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários para locatários que não usam sua própria fonte de identidade. Usuários em grupos de locatários podem fazer login no Tenant Manager e executar tarefas, com base nas permissões atribuídas ao grupo no Tenant Manager. Consulte "Criar conta de locatário" e "Use uma conta de tenant" para obter detalhes.

Insira a configuração

Passos

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

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

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
   - **Nome Único do Usuário**: O nome do atributo que contém o identificador único de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `uid` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `uid`.
   - **UUID do usuário**: O nome do atributo que contém o identificador único permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Nome Único do Grupo**: O nome do atributo que contém o identificador único de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `cn` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `cn`.
   - **UUID do Grupo**: O nome do atributo que contém o identificador único permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou

string, onde os hífens são ignorados.

5. Para todos os tipos de serviço LDAP, insira as informações necessárias do servidor LDAP e da conexão de rede na seção Configurar servidor LDAP.
   - **Nome do host**: O domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
   - **Porta**: A porta usada para conectar ao servidor LDAP.

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

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

     Para o Active Directory, você também pode especificar o Down-Level Logon Name ou o User Principal Name.

     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`
     - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e `userPrincipalName`
     - **Entra ID**: `accountEnabled` e `userPrincipalName`
   - **Senha**: a senha associada ao nome de usuário.

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

   - **DN Base do Grupo**: O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar grupos. No exemplo do Active Directory (abaixo), todos os grupos cujo nome diferenciado é relativo ao DN base (DC=storagegrid,DC=example,DC=com) podem ser usados como grupos federados.

     > Os valores do **Nome único do grupo** devem ser únicos dentro do **DN base do grupo** ao qual pertencem.

   - **DN Base do Usuário**: O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar usuários.

     > Os valores do **Nome único do usuário** devem ser únicos dentro do **DN base do usuário** ao qual pertencem.

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

     É recomendável fornecer o **formato de nome de usuário de vinculação**, pois isso pode permitir que os usuários façam login caso o StorageGRID não consiga se vincular à conta de serviço.

Insira um destes padrões:

- **UserPrincipalName padrão (AD e Entra ID)**: `[USERNAME]@example.com`
- **Padrão de nome de logon de nível inferior (AD e Entra ID)**: `example\[USERNAME]`
- **Padrão de nome diferenciado**: `CN=[USERNAME],CN=Users,DC=example,DC=com`

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

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.
   - **Usar STARTTLS**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para Active Directory, OpenLDAP ou outros, mas esta opção não é compatível com Microsoft Entra ID.
   - **Usar LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar esta opção para Microsoft Entra ID.
   - **Não utilize TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será seguro. Esta opção não é compatível com Microsoft Entra ID.

   > ⓘ A opção **Não usar TLS** não é compatível se o seu servidor Active Directory exigir assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

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

     Se você selecionar esta opção, copie e cole o certificado de segurança personalizado na caixa de texto do certificado da CA.

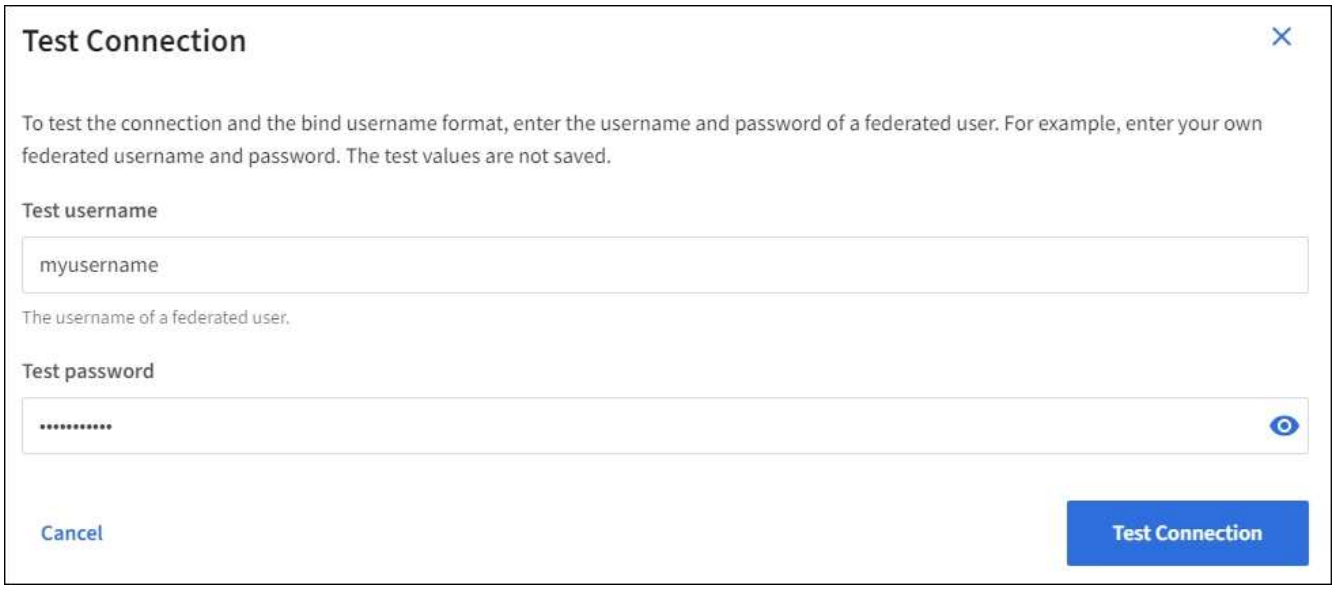
Teste a conexão e salve a configuração

Após inserir todos os valores, você deve testar a conexão antes de salvar a configuração. StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato do nome de usuário de bind, caso você tenha fornecido um.

Passos

1. Selecione **Test connection**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
   - Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
   - A mensagem "Não foi possível estabelecer a conexão de teste" será exibida se as configurações de conexão forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você forneceu um formato de nome de usuário de vinculação, 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 caracteres especiais no nome de usuário, como @ ou /.



- Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
- Uma mensagem de erro será exibida se as configurações de conexão, o formato do nome de usuário de vinculação ou o nome de usuário e senha de teste forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar a sincronização com a fonte de identidade

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

Passos

1. Acesse a página de federação de identidades.
2. Selecione **Sync server** na parte superior da página.

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

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

Desativar federação de identidade

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

Sobre esta tarefa

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

- Usuários federados não poderão fazer login.
- Os usuários federados que estiverem conectados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login após a expiração da sessão.

- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidades** fica desabilitada se o status de logon único (SSO) for **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desabilitado** antes que você possa desabilitar a federação de identidades. Consulte "Desativar single sign-on".

Passos

1. Acesse a página de federação de identidades.
2. Desmarque a caixa de seleção **Ativar federação de identidades**.

Diretrizes para configurar um servidor OpenLDAP

Se você deseja usar um servidor OpenLDAP para federação de identidades, você deve configurar definições específicas no servidor OpenLDAP.

> Para fontes de identidade que não sejam o Active Directory ou o Microsoft Entra ID, StorageGRID não bloqueará automaticamente o acesso S3 para usuários que estejam desabilitados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 do usuário ou remova o usuário de todos os grupos.

Memberof e sobreposições refint

As sobreposições memberof e refint devem estar habilitadas. Para obter mais informações, consulte as instruções para manutenção reversa de associação de grupo no "Documentação do OpenLDAP: Guia do administrador da versão 2.4".

Indexação

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

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

Além disso, certifique-se de que os campos mencionados na ajuda para Username estejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção reversa da associação a grupos no "Documentação do OpenLDAP: Guia do administrador da versão 2.4".

Gerenciar grupos de administradores no StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

- Você tem "permissões de acesso específicas".
- Se você planeja importar um grupo federado, você configurou a federação de identidades e o grupo federado já existe na fonte de identidade configurada.

Criar um grupo de administradores

Os grupos de administradores permitem que você determine quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Grupos de administradores**.
2. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

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

Grupo local

Passos

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

Grupo federado

Passos

1. Selecione **Grupo federado**.
2. Insira o nome do grupo que você deseja importar, exatamente como aparece na fonte de identidade configurada.
   - Para Active Directory e Microsoft Entra ID, use o sAMAccountName.
   - Para o OpenLDAP, use o CN (Common Name).
   - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **Continue**.

Gerenciar permissões de grupo

Passos

1. Em **Modo de acesso**, selecione se os usuários do grupo podem alterar configurações e executar operações no Grid Manager e na Grid Management API ou se podem apenas visualizar configurações e recursos.

- **Leitura e gravação** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
- **Somente leitura**: Os usuários podem apenas visualizar as configurações e os recursos. Eles não podem fazer alterações nem executar operações no Grid Manager ou Grid Management API. Usuários locais com permissão somente leitura podem alterar suas próprias senhas.

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

2. Selecione uma ou mais "permissões do grupo de administradores".

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao grupo não poderão fazer login no StorageGRID.

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

Adicionar usuários (somente grupos locais)

Passos

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

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

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

Visualizar e editar grupos de administradores

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

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

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do grupo	a. Selecione a caixa de seleção do grupo. b. Selecione **Ações** > **Ver detalhes do grupo**.	Selecione o nome do grupo na tabela.
Editar nome de exibição (apenas grupos locais)	a. Selecione a caixa de seleção do grupo. b. Selecione **Ações** > **Editar nome do grupo**. c. Digite o novo nome. d. Selecione **Save changes**.	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Save changes**.

Tarefa	Menu de ações	Página de detalhes
Editar modo de acesso ou permissões	a. Selecione a caixa de seleção do grupo. b. Selecione **Ações** > **Ver detalhes do grupo**. c. Opcionalmente, altere o modo de acesso do grupo. d. Opcionalmente, selecione ou desmarque "permissões do grupo de administradores". e. Selecione **Save changes**.	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o modo de acesso do grupo. c. Opcionalmente, selecione ou desmarque "permissões do grupo de administradores". d. Selecione **Save changes**.

Duplicar um grupo

Passos

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

Excluir um grupo

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

Passos

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

Permissões do grupo de administradores no StorageGRID

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

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

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

- Faça login no Grid Manager
- Veja o dashboard
- Veja as páginas de nós

- Veja os alertas atuais e resolvidos
- Alterar a própria senha (somente para usuários locais)
- Veja determinadas informações fornecidas nas páginas de Configuração e Manutenção

Interação entre permissões e modo de acesso

Para todas as permissões, a configuração **Modo de acesso** do grupo determina se os usuários podem alterar configurações e executar operações ou se podem apenas visualizar as configurações e recursos relacionados. Se um usuário pertencer a vários grupos e algum 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 de **Root access**.

Acesso à raiz

Esta permissão concede acesso a todos os recursos de administração do grid.

Alterar senha raiz do tenant

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

> Para conceder acesso à página Tenants, que contém a opção **Change root password**, atribua também a permissão **Tenant accounts**.

ILM

Esta permissão concede acesso às seguintes opções de menu do **ILM**:

- Regras
- Políticas
- Etiquetas de política
- Pools de storage
- Classes de storage
- Regiões
- Pesquisa de metadados de objetos

> Os usuários devem ter a permissão **Other grid configuration** para gerenciar os storage grades.

Manutenção

Os usuários precisam ter a permissão de Maintenance para usar essas opções:

- **Configuração** > **Controle de acesso**:

    - Senhas do grid
- **Configuração** > **Rede**:
    - Nomes de domínio de endpoint S3
- **Manutenção** > **Tarefas**:
    - Descomissionar
    - Expansão
    - Verificação de existência de objeto
    - Recuperação
- **Manutenção** > **Sistema**:
    - Pacote de recuperação
    - Atualização de software
- **Suporte** > **Ferramentas**:
    - Registros

Usuários que não possuem a permissão de Maintenance podem visualizar, mas não editar, estas páginas:

- **Manutenção** > **Rede**:
    - Servidores DNS
    - Rede de grid
    - Servidores NTP
- **Manutenção** > **Sistema**:
    - Licença
- **Configuração** > **Rede**:
    - Nomes de domínio de endpoint S3
- **Configuração** > **Segurança**:
    - Certificados
- **Configuração** > **Monitoramento**:
    - Servidor de auditoria e syslog

Gerenciar alertas

Essa permissão concede acesso às opções de gerenciamento de alertas. Os usuários precisam dessa permissão para gerenciar silenciamentos, notificações de alerta e regras de alerta.

Consulta de métricas

Esta permissão concede acesso a:

- **Suporte** > **Ferramentas** > **Métricas**
- Consultas de métricas personalizadas do Prometheus usando a seção **Métricas** da Grid Management API
- Cartões do painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão concede acesso à página **ILM** > **Pesquisa de metadados de objetos**.

Outra configuração de grid

Esta permissão concede acesso a estas opções adicionais de configuração da grid:

- **ILM**:
  - Classes de storage
- **Configuração** > **Sistema**:
- **Suporte** > **Outros**:
  - Custo do link

Administrador de appliance de armazenamento

Esta permissão concede:

- Acesso ao E-Series SANtricity System Manager em dispositivos de armazenamento através do Grid Manager.
- A capacidade de executar tarefas de solução de problemas e manutenção na guia Gerenciar unidades para appliances que suportam essas operações.

Contas de locatários

Esta permissão permite:

- Acesse a página de Tenants, onde você pode criar, editar e remover contas de tenant
- Consulte as políticas de classificação de tráfego existentes
- Visualize os cartões do painel do Grid Manager que contêm detalhes do tenant

Gerenciar usuários no StorageGRID

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

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Criar um usuário local

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

Você só pode criar 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 single sign-on (SSO) estiver ativado, os usuários locais não poderão fazer login no StorageGRID.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Usuários administradores**.
2. Selecione **Criar usuário**.

Insira as credenciais do usuário

Passos

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

Atribuir a grupos

Passos

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

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

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

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

Visualizar e editar usuários locais

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

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

- Para visualizar informações básicas sobre todos os usuários locais e federados, consulte 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.

  Quaisquer alterações são aplicadas na próxima vez que o usuário sair e entrar novamente no Grid Manager.

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

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do usuário	a. Selecione a caixa de seleção para o usuário. b. Selecione **Ações** > **Ver detalhes do usuário**.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione **Ações** > **Editar nome completo**. c. Digite o novo nome. d. Selecione **Save changes**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Save changes**.
Negar ou permitir acesso ao StorageGRID	a. Selecione a caixa de seleção para o usuário. b. Selecione **Ações** > **Ver detalhes do usuário**. c. Selecione a guia Acesso. d. Selecione **Sim** para impedir que o usuário faça login no Grid Manager ou na Grid Management API, ou selecione **Não** para permitir que o usuário faça login. e. Selecione **Save changes**.	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 Grid Manager ou na Grid Management API, ou selecione **Não** para permitir que o usuário faça login. d. Selecione **Save changes**.
Alterar senha (somente para usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione **Ações** > **Ver detalhes do usuário**. c. Selecione a guia Senha. d. Digite uma nova senha. e. Selecione **Alterar senha**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Digite uma nova senha. d. Selecione **Alterar senha**.

Tarefa	Menu de ações	Página de detalhes
Alterar grupos (somente usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione **Ações** > **Ver detalhes do usuário**. c. Selecione a guia Grupos. d. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. e. Selecione **Editar grupos** para selecionar grupos diferentes. f. Selecione **Save changes**.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Grupos. c. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. d. Selecione **Editar grupos** para selecionar grupos diferentes. e. Selecione **Save changes**.

Importar usuários federados

Você pode importar um ou mais usuários federados, até um máximo de 100 usuários, diretamente na página Usuários.

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Usuários administradores**.
2. Selecione **Import federated users**.
3. Insira o UUID ou nome de usuário de um ou mais usuários federados.

   Para múltiplas entradas, adicione cada UUID ou nome de usuário em uma nova linha.

4. Selecione **Import**.

   Se a importação para o campo Usuários falhar para um ou mais usuários, execute as seguintes etapas:

   a. Expanda **Usuários não importados** e selecione **Copiar usuários**.
   b. Tente importar novamente selecionando **Anterior** e colando os usuários copiados na caixa de diálogo **Importar usuários federados**.

   Após fechar a caixa de diálogo **Importar usuários federados**, as informações dos usuários federados são exibidas na página Usuários para os usuários importados com sucesso.

Duplicar um usuário

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

Passos

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

Excluir um usuário

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

> Você não pode excluir o usuário raiz.

Passos

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

Use o single sign-on (SSO)

Saiba mais sobre StorageGRID SSO

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

O sistema StorageGRID suporta autenticação única (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar o single sign-on (SSO), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está habilitado.

Faça login quando o SSO estiver ativado

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

Passos

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

   A página de login do StorageGRID é exibida.

   - Se esta for a primeira vez que você acessa a URL neste navegador, será solicitado que você insira um ID de conta.
   - Se você já acessou o Grid Manager ou o Tenant Manager anteriormente, será solicitado que selecione uma conta recente ou insira um ID de conta.

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

2. Indique se você deseja acessar o Grid Manager ou o Tenant Manager:

- Para acessar o Grid Manager, deixe o campo **Account ID** em branco, digite **0** como account ID ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.
- Para acessar o Gerenciador de Inquilinos, insira o ID da conta do inquilino de 20 dígitos ou selecione um inquilino pelo nome se ele aparecer na lista de contas recentes.

3. Selecione **Sign in**

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

4. Faça login com suas credenciais de SSO.

   Se suas credenciais de SSO estiverem corretas:

   a. O provedor de identidade (IdP) fornece uma resposta de autenticação ao StorageGRID.
   b. 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 conectado ao Grid Manager ou ao Tenant Manager, dependendo da conta que você selecionou.

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

5. Opcionalmente, acesse outros Nós de Administração ou acesse o Grid Manager ou o Tenant Manager, caso você tenha permissões adequadas.

   Você não precisa inserir suas credenciais de SSO novamente.

Saia quando o SSO estiver ativado

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

Passos

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

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

   > A tabela resume o que acontece ao sair da sua conta se você estiver usando uma única sessão do navegador. Se você estiver conectado ao StorageGRID em várias sessões do navegador, você deve sair de cada sessão separadamente.

Se você estiver conectado a…	E você sai de…	Você está desconectado(a) de…
Gerenciador de grade em um ou mais nós de administração	Gerenciador de grade em qualquer nó de administração	Gerenciador de grade em todos os nós de administração **Observação:** Se você usar o Entra ID para SSO, pode levar alguns minutos para que a sessão seja encerrada em todos os Admin Nodes.
Gerenciador de locatários em um ou mais nós de administração	Gerenciador de locatários em qualquer nó administrativo	Gerenciador de Inquilinos em todos os nós administrativos
Tanto o Grid Manager quanto o Tenant Manager	Grid Manager	Somente o Grid Manager. Você também precisa sair do Tenant Manager para sair do SSO.

Requisitos e considerações para SSO do StorageGRID

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

Requisitos do provedor de identidade

StorageGRID é compatível com os seguintes provedores de identidade SSO (IdP):

- Serviço de Federação do Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

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

> Windows Server 2016 deve usar a "Atualização KB3201845", ou superior.

Requisitos adicionais

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

Considerações sobre Entra ID

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

Requisitos de certificado do servidor

Por padrão, StorageGRID usa um certificado de interface de gerenciamento em cada nó administrativo para proteger o acesso ao Grid Manager, ao Tenant Manager, à API de Gerenciamento de Grid e à API de Gerenciamento de Locatários. Ao configurar relações de confiança de terceiros (AD FS), aplicativos corporativos (Entra ID) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado do servidor como o certificado de assinatura para as solicitações do StorageGRID.

Se você ainda não "configurou um certificado personalizado para a interface de gerenciamento", deve fazer isso agora. Ao instalar um certificado de servidor personalizado, ele é usado em todos os Admin Nodes e você pode usá-lo em todas as relações de confiança de relying party do StorageGRID, aplicações empresariais ou conexões SP.

> Não é recomendável usar o certificado de servidor padrão de um nó de administração em uma relação de confiança com terceiros, aplicativo corporativo ou conexão SP. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de fazer login no nó recuperado, você deve atualizar a relação de confiança com terceiros, o aplicativo corporativo ou a conexão SP com o novo certificado.

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

Requisitos de porta

O login único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com login único. Consulte "Controle de acesso no firewall externo".

Confirme se os usuários federados podem fazer login no StorageGRID

Antes de ativar o login único (SSO), você deve confirmar que pelo menos um usuário federado consegue acessar o Grid Manager e o Tenant Manager para quaisquer contas de locatário existentes.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você já configurou a federação de identidades.

Passos

1. Caso existam contas de inquilinos, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.

   Ao ativar o SSO, a origem de identidade configurada no Gerenciador de Locatários é substituída pela origem de identidade configurada no Grid Manager. Os usuários pertencentes à origem de identidade do locatário não poderão mais fazer login, a menos que possuam uma conta com a origem de identidade do Grid Manager.

   a. Faça login no Tenant Manager para cada conta de tenant.
   b. Selecione **Gerenciamento de acesso** > **Federação de identidades**.
   c. Confirme se a caixa de seleção **Ativar federação de identidades** não está selecionada.
   d. Caso afirmativo, confirme se os grupos federados que possam estar em uso para esta conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.

2. Confirme se um usuário federado pode acessar o Grid Manager:
   a. No Grid Manager, selecione **Configuração** > **Controle de acesso** > **Grupos de administradores**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da fonte de identidade do Active Directory e que a ele tenha sido atribuída a permissão de acesso raiz.
   c. Sair.
   d. Confirme se você consegue acessar novamente o Grid Manager como um usuário do grupo federado.
3. Caso existam contas de locatário, confirme que um usuário federado com permissão de acesso Root pode fazer login:
   a. No Grid Manager, selecione **Tenants**.
   b. Selecione a conta do locatário e selecione **Ações** > **Editar**.
   c. Na guia Inserir detalhes, selecione **Continuar**.
   d. Se a caixa de seleção **Usar fonte de identidade própria** estiver marcada, desmarque-a e selecione **Salvar**.

      A página do tenant é exibida.

   e. Selecione a conta do locatário, selecione **Entrar** e faça login na conta do locatário como usuário raiz.
   f. No Tenant Manager, selecione **Gerenciamento de Acesso** > **Grupos**.
   g. Certifique-se de que pelo menos um grupo federado do Grid Manager tenha recebido a permissão de acesso Root para este tenant.
   h. Sair.
   i. Confirme se você consegue entrar novamente no tenant como um usuário do grupo federado.

Informações relacionadas

- "Requisitos e considerações para single sign-on"

- "Gerenciar grupos de administradores"
- "Use uma conta de tenant"

Configurar SSO no StorageGRID

Você pode seguir o assistente de configuração do SSO e entrar no modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID. Após o SSO ter sido habilitado, você pode retornar ao modo sandbox quando necessário para alterar ou testar novamente a configuração.

Antes de começar

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Serviço de Federação do Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Sobre esta tarefa

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

- A resposta do Active Directory ou PingFederate inclui um identificador único universal (UUID) para o usuário.
- A resposta do Entra ID inclui um Nome Principal do Usuário (UPN).

Para permitir que StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre as solicitações de autenticação do usuário, você deverá concluir estas tarefas:

1. Configure as configurações no StorageGRID.
2. Use o software do provedor de identidade SSO para criar uma relação de confiança com a parte confiável (AD FS), Aplicativo Empresarial (Entra ID) ou Provedor de Serviços (PingFederate) para cada Admin Node.
3. Retorne ao StorageGRID para ativar o SSO.

O modo sandbox facilita a realização dessa configuração bidirecional e permite testar todas as suas configurações antes de ativar o SSO. Quando você está usando o modo sandbox, os usuários não podem fazer login usando o SSO.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Single sign-on**. A página de Single sign-on é exibida.

   Se o botão Configurar configurações de SSO estiver desativado, confirme se você configurou o provedor de identidade como a fonte de identidade federada. Consulte "Requisitos e considerações para single sign-on".

2. Selecione **Configurar definições de SSO**. A página Fornecer detalhes do provedor de identidade é exibida.

Forneça os detalhes do provedor de identidade

Passos

1. Selecione o **tipo de SSO** na lista suspensa.
2. Se você selecionou o Active Directory como o tipo de SSO, insira o **nome do serviço de federação** para o provedor de identidade, exatamente como aparece no Active Directory Federation Service (AD FS).

   Para localizar o nome do serviço de federação, acesse o Windows Server Manager. Selecione **Tools** > **AD FS Management**. No menu Action, selecione **Edit Federation Service Properties**. O nome do serviço de federação é exibido no segundo campo.

3. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta às solicitações do StorageGRID.
   - **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
   - **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

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

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

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

4. Selecione **Continuar**. A página Fornecer identificador da parte confiável é exibida.

Forneça o identificador da parte confiável

1. Preencha os campos na página "Fornecer identificador da parte confiável" com base no tipo de SSO que você selecionou.

Active Directory

a. Especifique o **Identificador da parte confiável** para StorageGRID. Esse valor controla o nome que você usa para cada relação de confiança com a parte confiável no AD FS.

   - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
   - Se sua grid incluir mais de um Admin Node, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o identificador da relying party para cada Admin Node na grid, com base no hostname do nó.

   > Você deve criar uma relação de confiança de terceiros para cada Nó de Administração no seu sistema StorageGRID. Ter uma relação de confiança de terceiros para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

b. Selecione **Salvar e entrar no modo sandbox**.

Entra ID

a. Na seção Aplicativo Empresarial, especifique o **nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo empresarial no Entra ID.

   - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
   - Se a sua grid incluir mais de um Admin Node, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o nome do aplicativo corporativo para cada Admin Node em seu sistema, com base no hostname do nó.

   > Você deve criar um aplicativo corporativo para cada Nó de Administração em seu sistema StorageGRID. Ter um aplicativo corporativo para cada Nó de Administração garante que os usuários possam entrar e sair de qualquer Nó de Administração com segurança.

b. Siga os passos descritos em "Crie aplicativos empresariais no Entra ID" para criar uma aplicação empresarial para cada Admin Node listado na tabela.

c. No Entra ID, copie a URL dos metadados de federação para cada aplicação empresarial. Em seguida, cole essa URL no campo **Federation metadata URL** correspondente no StorageGRID.

d. Depois de copiar e colar uma URL de metadados de federação para todos os Admin Nodes, selecione **Salvar e entrar no modo sandbox**.

PingFederate

a. Na seção Provedor de Serviços (SP), especifique o **SP connection ID** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP em PingFederate.

   - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
   - Se sua grid incluir mais de um Nó de Administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o ID de conexão do SP para cada Nó de Administração em seu sistema, com base no

hostname do nó.

> Você deve criar uma conexão SP para cada Nó de Administração no seu sistema StorageGRID. Ter uma conexão SP para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

b. Especifique a URL de metadados de federação para cada Nó de Administração no campo **URL de metadados de federação**.

   Utilize o seguinte formato:

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

c. Selecione **Salvar e entrar no modo sandbox**.

Configurar relações de confiança com terceiros confiáveis, aplicativos corporativos ou conexões SP

Após salvar a configuração e entrar no modo sandbox, você pode concluir e testar a configuração do tipo de SSO que você selecionou.

StorageGRID pode permanecer em modo sandbox pelo tempo que for necessário. No entanto, somente usuários federados e usuários locais podem fazer login.

Active Directory

Passos

1. Acesse o Active Directory Federation Services (AD FS).
2. Crie uma ou mais relações de confiança de terceiros para StorageGRID, usando cada identificador de terceiro exibido na tabela na página Configurar SSO.

   Você deve criar uma relação de confiança para cada Admin Node mostrado na tabela.

   Para obter instruções, acesse "Crie relações de confiança de terceiros no AD FS".

Entra ID

Passos

1. Na página de login único do nó de administração em que você está conectado, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração em sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **Configuração** > **Controle de acesso** > **Single sign-on**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Acesse o portal do Azure.
4. Siga os passos em "Crie aplicativos empresariais no Entra ID" para carregar o arquivo de metadados SAML de cada Nó de Administração em seu respectivo aplicativo corporativo Entra ID.

PingFederate

Passos

1. Na página de login único do nó de administração em que você está conectado, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração em sua grade, repita estas etapas:
   a. Faça login no nó.
   b. Selecione **Configuração** > **Controle de acesso** > **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 StorageGRID". Use o ID de conexão do SP para cada Nó de Administração (mostrado na tabela na página Configurar SSO) e os metadados SAML que você baixou para esse Nó de Administração.

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

Testar configuração

Antes de impor o uso de single sign-on para todo o seu sistema StorageGRID, confirme que o single sign-on e o single logout estão configurados corretamente para cada Admin Node.

Active Directory

Passos

1. Na página Configurar SSO, localize o link na etapa Testar configuração do assistente.

   A URL é derivada do valor que você inseriu no campo **Nome do serviço de federação**.

2. Selecione o link ou copie e cole a URL em um navegador para acessar a página de login do seu provedor de identidade.
3. Para confirmar que você pode usar o SSO para entrar no StorageGRID, selecione **Entrar em um dos seguintes sites**, selecione o identificador da parte confiável para seu nó de administração principal e selecione **Entrar**.
4. Insira seu nome de usuário federado e sua senha.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
   - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
5. Repita estes passos para verificar a conexão SSO de cada Admin Node em sua grid.

Entra ID

Passos

1. Acesse a página de logon único no portal do Azure.
2. Selecione **Test this application**.
3. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
   - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
4. Repita estes passos para verificar a conexão SSO de cada Admin Node em sua grid.

PingFederate

Passos

1. Na página Configurar SSO, selecione o primeiro link na mensagem de 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 do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
   - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o link a seguir para verificar a conexão SSO de cada nó de administração em sua grade.

   Se você vir a mensagem "Página Expirada", selecione o botão **Voltar** no seu navegador e envie suas credenciais novamente.

Ativar single sign-on

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

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

Passos

1. Na etapa Test configuration do assistente de configuração de SSO, selecione **Enable SSO**.
2. Analise a mensagem de aviso e selecione **Ativar SSO**.

   O login único agora está ativado. A página de login único é exibida e agora inclui os detalhes do SSO que você acabou de configurar.

3. Para editar a configuração, selecione **Editar**.
4. Para desativar o single sign-on, selecione **Disable SSO**.

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

Crie relações de confiança com terceiros confiáveis no AD FS para StorageGRID

Você deve usar o Active Directory Federation Services (AD FS) para criar uma relação de confiança com outra parte para cada nó administrativo do seu sistema. Você pode criar relações de confiança com outra parte usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para StorageGRID e selecionou **AD FS** como o tipo de SSO.
- Você tem "entrou no modo sandbox" no Grid Manager.
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador da parte confiável para cada Admin Node em seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Admin Nodes na página Configure SSO do StorageGRID.

> Você deve criar uma relação de confiança de terceiros para cada Nó de Administração no seu sistema StorageGRID. Ter uma relação de confiança de terceiros para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

- Você tem experiência na criação de relações de confiança de terceiros no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in de Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a relação de confiança com a parte confiável manualmente, você possui o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID, ou sabe como fazer login em um Admin Node 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, notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se você tiver dúvidas.

Crie uma relação de confiança com terceiros usando Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais relações de confiança com terceiros confiáveis.

Passos

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

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

   - Para *Admin_Node_Identifier*, insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Single Sign-on. Por exemplo, `SG-DC1-ADM1`.
   - Para *Admin_Node_FQDN*, insira o domínio totalmente qualificado para o mesmo Admin Node. (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 deverá atualizar ou recriar essa relying party trust caso esse endereço IP seja alterado.)
3. No Gerenciador do Servidor do Windows Server, selecione **Ferramentas** > **Gerenciamento do AD FS**.

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

   A lista de relying party trusts é exibida.
5. Adicione uma política de controle de acesso à relação de confiança da parte confiável recém-criada:
   a. Localize a relação de confiança da parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse na relação de confiança e selecione **Editar Política de Controle de Acesso**.
   c. Selecione uma política de controle de acesso.
   d. Selecione **Aplicar** e selecione **OK**
6. Adicione uma política de emissão de declarações à nova relação de confiança de terceira parte criada:
   a. Localize a relação de confiança da parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse na trust e selecione **Editar política de emissão de declarações**.
   c. Selecione **Adicionar regra**.
   d. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.
   e. Na página Configurar Regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

f. Para o Repositório de Atributos, selecione **Active Directory**.

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

h. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.

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

7. Confirme se os metadados foram importados com sucesso.

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

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

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

8. Repita estes passos para configurar uma relação de confiança da parte confiável para todos os nós de administração em seu sistema StorageGRID.

9. Ao concluir, retorne ao StorageGRID e "testar todas as relações de confiança de terceiros" para confirmar que estão configurados corretamente.

Crie uma relação de confiança de terceiros importando metadados de federação

Você pode importar os valores para cada relação de confiança com a parte confiável acessando os metadados SAML de cada Admin Node.

Passos

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

2. Em Ações, selecione **Adicionar Relying Party Trust**.

3. Na página de boas-vindas, escolha **Reconhecimento de reivindicações** e selecione **Iniciar**.

4. Selecione **Importar dados sobre a parte confiante publicados online 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 Admin Node:

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

Para *`Admin_Node_FQDN`*, insira o domínio totalmente qualificado para o mesmo Admin Node. (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 deverá atualizar ou recriar essa relying party trust caso esse endereço IP seja alterado.)

6. Conclua o assistente de Relying Party Trust, salve o relying party trust e feche o assistente.

Ao inserir o nome de exibição, use o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Single Sign-on no Grid Manager. Por exemplo, `SG-DC1-ADM1`.

7. Adicione uma regra de reivindicação:

a. Clique com o botão direito do mouse na trust e selecione **Editar política de emissão de declarações**.

b. Selecione **Adicionar regra**:

c. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.

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

   Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

e. Para o Repositório de Atributos, selecione **Active Directory**.

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

g. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.

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

8. Confirme se os metadados foram importados com sucesso.

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

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

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

9. Repita estes passos para configurar uma relação de confiança da parte confiável para todos os nós de administração em seu sistema StorageGRID.

10. Ao concluir, retorne ao StorageGRID e "testar todas as relações de confiança de terceiros" para confirmar se estão configuradas corretamente.

Criar manualmente uma relação de confiança de terceiros

Caso opte por não importar os dados para os relying part trusts, você pode inserir os valores manualmente.

Passos

1. No Gerenciador do Servidor do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
2. Em Ações, selecione **Adicionar Relying Party Trust**.
3. Na página de boas-vindas, escolha **Reconhecimento de reivindicações** e selecione **Iniciar**.
4. Selecione **Inserir manualmente os dados da parte confiante** e selecione **Avançar**.
5. Conclua o assistente de Confiança da Parte Confiável:

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

      Para manter a consistência, use o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Autenticação Única no Gerenciador de Grade. Por exemplo, `SG-DC1-ADM1`.

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

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

d. Digite a URL do endpoint do serviço SAML para o Admin Node:

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

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado do Nó de Administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que será necessário atualizar ou recriar essa relação de confiança com a parte confiável caso esse endereço IP seja alterado.)

e. Na página Configurar Identificadores, especifique o Identificador da Parte Confiável para o mesmo Admin Node:

Admin_Node_Identifier

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

f. Revise as configurações, salve a relação de confiança com a parte confiável e feche o assistente.

A caixa de diálogo Edit Claim Issuance Policy é exibida.

Se a caixa de diálogo não aparecer, clique com o botão direito do mouse na trust e selecione **Editar política de emissão de reivindicações**.

6. Para iniciar o assistente de regras de reivindicação, selecione **Adicionar regra**:
   a. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.
   b. Na página Configurar Regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

   c. Para o Repositório de Atributos, selecione **Active Directory**.
   d. Na coluna Atributo LDAP da tabela de Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
   e. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.
   f. Selecione **Concluir** e selecione **OK**.
7. Clique com o botão direito do mouse na relação de confiança da parte confiável para abrir suas propriedades.
8. Na aba **Endpoints**, configure o endpoint para logout único (SLO):
   a. Selecione **Adicionar SAML**.
   b. Selecione **Tipo de Endpoint** > **Logout SAML**.
   c. Selecione **Associação** > **Redirecionamento**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste Admin Node:

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

Para *Admin_Node_FQDN*, insira o 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 será necessário atualizar ou recriar essa relação de confiança com a outra parte caso esse endereço IP seja alterado.)

   a. Selecione **OK**.

9. Na guia **Assinatura**, especifique o certificado de assinatura para esta relação de confiança com a parte confiável:

   a. Adicione o certificado personalizado:

      - Se você tiver o certificado de gerenciamento personalizado que carregou no StorageGRID, selecione esse certificado.
      - Se você não possui o certificado personalizado, faça login no Nó de Administração, acesse o `/var/local/mgmt-api` diretório do Nó de Administração e adicione o `custom-server.crt` arquivo de certificado.

      > Não é recomendável usar o certificado padrão do nó de administração (`server.crt`. Se o nó de administração falhar, o certificado padrão será regenerado quando você recuperar o nó, e você precisará atualizar a relying party trust.

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

      As propriedades da Relying Party são salvas e fechadas.

10. Repita estes passos para configurar uma relação de confiança da parte confiável para todos os nós de administração em seu sistema StorageGRID.
11. Ao concluir, retorne ao StorageGRID e "testar todas as relações de confiança de terceiros" para confirmar se estão configuradas corretamente.

Crie aplicativos corporativos no Entra ID para StorageGRID

Você usa o Entra ID para criar um aplicativo corporativo para cada Admin Node em seu sistema.

Antes de começar

- Você iniciou a configuração do logon único para StorageGRID e selecionou **Entra ID** como o tipo de SSO.
- Você tem "entrou no modo sandbox" no Grid Manager.
- Você tem o **nome do aplicativo corporativo** para cada Admin Node em seu sistema. Você pode copiar esses valores da tabela de detalhes do Admin Node na página Configurar SSO.

> Você deve criar um aplicativo corporativo para cada Nó de Administração em seu sistema StorageGRID. Ter um aplicativo corporativo para cada Nó de Administração garante que os usuários possam entrar e sair de qualquer Nó de Administração com segurança.

- Você tem experiência na criação de aplicativos corporativos no Entra ID.
- Você possui uma conta Entra ID com uma assinatura ativa.
- Você possui uma das seguintes funções na conta Entra ID: Global Administrator, Cloud Application Administrator, Application Administrator ou owner of the service principal.

Acessar Entra ID

Passos

1. Faça login no "Portal do Azure".
2. Navegue até "Entra ID".
3. Selecione "Aplicações empresariais".

Crie aplicativos corporativos e salve a configuração do StorageGRID SSO

Para salvar a configuração de SSO para o Entra ID no StorageGRID, você deve usar o Entra ID para criar um aplicativo corporativo para cada Admin Node. Você copiará os URLs de metadados de federação do Entra ID e os colará nos campos **URL de metadados de federação** correspondentes na página Configurar SSO.

Passos

1. Repita as seguintes etapas para cada Admin Node.
   a. No painel de aplicações do Entra ID Enterprise, selecione **New application**.
   b. Selecione **Criar sua própria aplicação**.
   c. No campo "Nome", insira o **Nome do aplicativo corporativo** que você copiou da tabela de detalhes do nó de administração na página "Configurar SSO".
   d. Deixe a opção **Integrar qualquer outro aplicativo que você não encontrar na galeria (Não pertencente à galeria)** selecionada.
   e. Selecione **Create**.
   f. Selecione o link **Começar** na **2. Configurar login único** ou selecione o link **Login único** na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o **App Federation Metadata Url**, que você pode encontrar em **Etapa 3 SAML Signing Certificate**.
   i. Acesse a página Configurar SSO e cole a URL no campo **URL de metadados de federação** que corresponde ao **nome do aplicativo corporativo** que você utilizou.
2. Depois de colar uma URL de metadados de federação para cada nó de administração e fazer todas as outras alterações necessárias na configuração do SSO, selecione **Salvar** na página Configurar SSO.

Baixe os metadados SAML para cada nó de administração

Após salvar a configuração do SSO, você pode baixar um arquivo de metadados SAML para cada nó de administração em seu sistema StorageGRID.

Passos

1. Repita estas etapas para cada Admin Node.
   a. Faça login no StorageGRID a partir do nó de administração.
   b. Selecione **Configuração** > **Controle de acesso** > **Single sign-on**.
   c. Selecione o botão para baixar os metadados SAML desse nó administrativo.
   d. Salve o arquivo, que você irá carregar no Entra ID.

Faça o upload dos metadados SAML para cada aplicativo corporativo

Após baixar um arquivo de metadados SAML para cada nó de administração do StorageGRID, execute as

seguintes etapas no Entra ID:

Passos

1. Retorne ao Portal do Azure.
2. Repita estas etapas para cada aplicação empresarial:

   > Pode ser necessário atualizar a página de aplicativos corporativos para ver os aplicativos que você adicionou anteriormente na lista.

   a. Acesse a página Propriedades do aplicativo corporativo.
   b. Defina **Atribuição necessária** como **Não** (a menos que você queira configurar atribuições separadamente).
   c. Vá para a página de login único.
   d. Conclua a configuração SAML.
   e. Selecione o botão **Carregar arquivo de metadados** e selecione o arquivo de metadados SAML que você baixou para o nó de administração correspondente.
   f. Após o carregamento do arquivo, selecione **Salvar** e, em seguida, selecione **X** para fechar o painel. Você retorna à página Configurar Single Sign-On com SAML.
3. "Teste cada aplicação".

Crie conexões de provedor de serviços em PingFederate para StorageGRID

Você usa o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administração em seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

Antes de começar

- Você configurou o logon único para StorageGRID e selecionou **Ping Federate** como o tipo de SSO.
- Você tem "entrou no modo sandbox" no Grid Manager.
- Você possui o **ID de conexão SP** para cada Nó de Administração em seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de Administração na página Configurar SSO.
- Você baixou os **metadados SAML** para cada nó de administração em seu sistema.
- Você tem experiência em criar conexões SP no PingFederate Server.
- Você tem o "Guia de Referência do Administrador" para o PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem o "Permissão de administrador" para o PingFederate Server.

Sobre esta tarefa

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

Conclua os pré-requisitos em PingFederate

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

Criar armazenamento de dados

Se ainda não o fez, crie um armazenamento de dados para conectar PingFederate ao servidor LDAP do AD FS. Use os valores que você usou ao "configurando a federação de identidades" no StorageGRID.

- **Tipo**: Diretório (LDAP)
- **Tipo LDAP**: Active Directory
- **Nome do Atributo Binário**: insira **objectGUID** na guia Atributos Binários do LDAP exatamente como mostrado.

Criar validador de credencial de senha

Se ainda não fez isso, crie um validador de credencial de senha.

- **Tipo**: Validador de credencial LDAP com nome de usuário e senha
- **Armazenamento de dados**: selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: Insira informações do LDAP (por exemplo, DC=saml,DC=sgws).
- **Filtro de pesquisa**: sAMAccountName=${username}
- **Escopo**: Subárvore

Criar instância do adaptador IdP

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

Passos

1. Acesse **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 credencial'**.
5. Selecione o validador de credencial de senha que você criou.
6. Na guia Atributos do Adaptador, selecione o atributo **username** para **Pseudonym**.
7. Selecione **Salvar**.

Criar ou importar certificado de assinatura

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

Passos

1. Acesse **Segurança** > **Chaves e certificados de assinatura e descriptografia**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP em PingFederate

Ao criar uma conexão SP em PingFederate, você importa os metadados SAML que baixou do StorageGRID para o Nó de Administração. O arquivo de metadados contém muitos dos valores específicos de que você precisa.

Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID, para que os usuários possam entrar e sair de qualquer nó com segurança. Use estas instruções para criar a primeira conexão SP. Em seguida, acesse Criar conexões SP adicionais para criar as conexões adicionais necessárias.

Escolha o tipo de conexão SP

Passos

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

Importar metadados do SP

Passos

1. Na guia Importar Metadados, selecione **Arquivo**.
2. Selecione o arquivo de metadados SAML que você baixou da página Configurar SSO para o Admin Node.
3. Analise o Resumo de Metadados e as informações fornecidas na aba Informações Gerais.

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

4. Selecione **Next**.

Configurar SSO do navegador IdP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia Perfis SAML, selecione as opções **SSO iniciado pelo SP**, **SLO iniciado pelo SP**, **SSO iniciado pelo IdP** e **SLO iniciado pelo IdP**.
3. Selecione **Next**.
4. Na aba "Tempo de Vida da Asserção", não faça alterações.
5. Na guia Criação de Asserção, selecione **Configurar Criação de Asserção**.
   a. Na guia Mapeamento de Identidade, selecione **Standard**.
   b. Na guia Contrato de Atributo, use **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para prorrogar o contrato, selecione **Excluir** para remover o `urn:oid`, que não está sendo usado.

Mapear instância do adaptador

Passos

1. Na guia Mapeamento da Fonte de Autenticação, selecione **Mapear nova instância do adaptador**.
2. Na guia Instância do Adaptador, selecione a 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 & Pesquisa de Usuário, selecione **Adicionar Origem do Atributo**.
5. Na aba "Data Store", forneça uma descrição e selecione o armazenamento de dados que você adicionou.
6. Na guia Pesquisa de diretório LDAP:
   - Insira o **DN base**, que deve corresponder exatamente ao valor que você inseriu no StorageGRID para o servidor LDAP.
   - Para o escopo de pesquisa, selecione **Subárvore**.
   - Para a classe de objeto raiz, procure e adicione um destes atributos: **objectGUID** ou **userPrincipalName**.
7. Na guia Tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia Filtro LDAP, insira **sAMAccountName=${username}**.
9. Na guia Cumprimento do Contrato de Atributo, selecione **LDAP (atributo)** na lista suspensa Origem e selecione **objectGUID** ou **userPrincipalName** na lista suspensa Valor.
10. Revise e depois salve a fonte de atributos.
11. Na guia Origem do atributo Failsave, selecione **Abort the SSO Transaction**.
12. Revise o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configurar as configurações do protocolo

Passos

1. Na guia **Conexão SP** > **SSO do navegador** > **Configurações de protocolo**, selecione **Configurar configurações de protocolo**.
2. Na guia URL do serviço de consumo de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para Binding e `/api/saml-response` para Endpoint URL).
3. Na guia URLs do serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para Binding e `/api/saml-logout` para Endpoint URL).
4. Na aba "Associações SAML Permitidas", desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de Assinatura, deixe as caixas de seleção **Exigir que as solicitações de autenticação sejam assinadas** e **Sempre assinar a declaração** marcadas.
6. Na guia Política de Criptografia, selecione **None**.
7. Analise o resumo e selecione **Concluído** para salvar as configurações do protocolo.
8. Analise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia Conexão do SP, selecione **Credenciais**.
2. Na aba Credenciais, selecione **Configurar Credenciais**.
3. Selecione o certificado de assinatura que você criou ou importou.
4. Selecione **Avançar** para ir para **Gerenciar configurações de verificação de assinatura**.

a. Na aba Trust Model, selecione **Unanchored**.

b. Na aba Certificado de Verificação de Assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.

5. Analise as telas de resumo e selecione **Salvar** para salvar a conexão SP.

Criar conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada Nó de Administração em sua grade. Você carrega novos metadados para cada cópia.

> As conexões 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. Insira o ID da conexão e o nome da conexão para a cópia e selecione **Salvar**.
3. Escolha o arquivo de metadados correspondente ao nó de administração:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **Escolher arquivo** e carregue os metadados.
   c. Selecione **Next**.
   d. Selecione **Salvar**.
4. Corrija o erro devido ao atributo não utilizado:
   a. Selecione a nova conexão.
   b. Selecione **Configurar SSO do navegador > Configurar criação de declaração > Contrato de atributo**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Salvar**.

Desativar SSO no StorageGRID

Você pode desativar o single sign-on (SSO) se não quiser mais usar essa funcionalidade. Você deve desativar o single sign-on antes de desativar a federação de identidades.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Passos

1. Selecione **Configuração** > **Controle de acesso** > **Single sign-on**.

   A página de Single Sign-on é exibida.

2. Selecione **Desativar SSO**.

3. Selecione **Sim**.

   Uma mensagem de aviso é exibida indicando que os usuários locais agora poderão fazer login.

Na próxima vez que você acessar o StorageGRID, a página de login do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário local ou federado do StorageGRID.

Desative e reative temporariamente o SSO para um nó de administração do StorageGRID

Você pode não conseguir acessar o Grid Manager se o sistema de autenticação única (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um Admin Node. Para desativar e depois reativar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

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

Sobre esta tarefa

Após desativar o SSO para um Nó de Administração, você pode fazer login no Grid Manager como o usuário raiz. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no Nó de Administração assim que sair.

> Desativar o SSO para um nó de administração não afeta as configurações de SSO de outros nós de administração na grade. A caixa de seleção **Ativar SSO** na página de Single Sign-on do Grid Manager permanece marcada e todas as configurações de SSO existentes são mantidas, a menos que você as atualize.

Passos

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

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

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

   Uma mensagem indica que o comando se aplica somente a este Admin Node.

3. Confirme que você deseja desativar o SSO.

   Uma mensagem indica que o single sign-on está desativado no nó.

4. A partir de um navegador web, acesse o Grid Manager no mesmo Admin Node.

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

5. Faça login com o nome de usuário root e a senha do usuário raiz local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração do SSO:
   a. Selecione **Configuração** > **Controle de acesso** > **Single sign-on**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Selecione **Salvar**.

      Selecionar **Salvar** na página de Single Sign-on reativa automaticamente o SSO para toda a grid.
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 precise executar.
   b. Selecione **Sair** e feche o Grid Manager.
   c. Reative o SSO no nó de administração. Você pode executar uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a este Admin Node.

      Confirme que você deseja ativar o SSO.

      Uma mensagem indica que o single sign-on está ativado no nó.

      - Reinicie o nó da grade: `reboot`
8. A partir de um navegador web, acesse o Grid Manager no mesmo nó de administração.
9. Confirme que a página de login do StorageGRID aparece e que você precisa inserir suas credenciais de SSO para acessar o Grid Manager.

Use a federação de grid

Saiba mais sobre a federação de grids StorageGRID

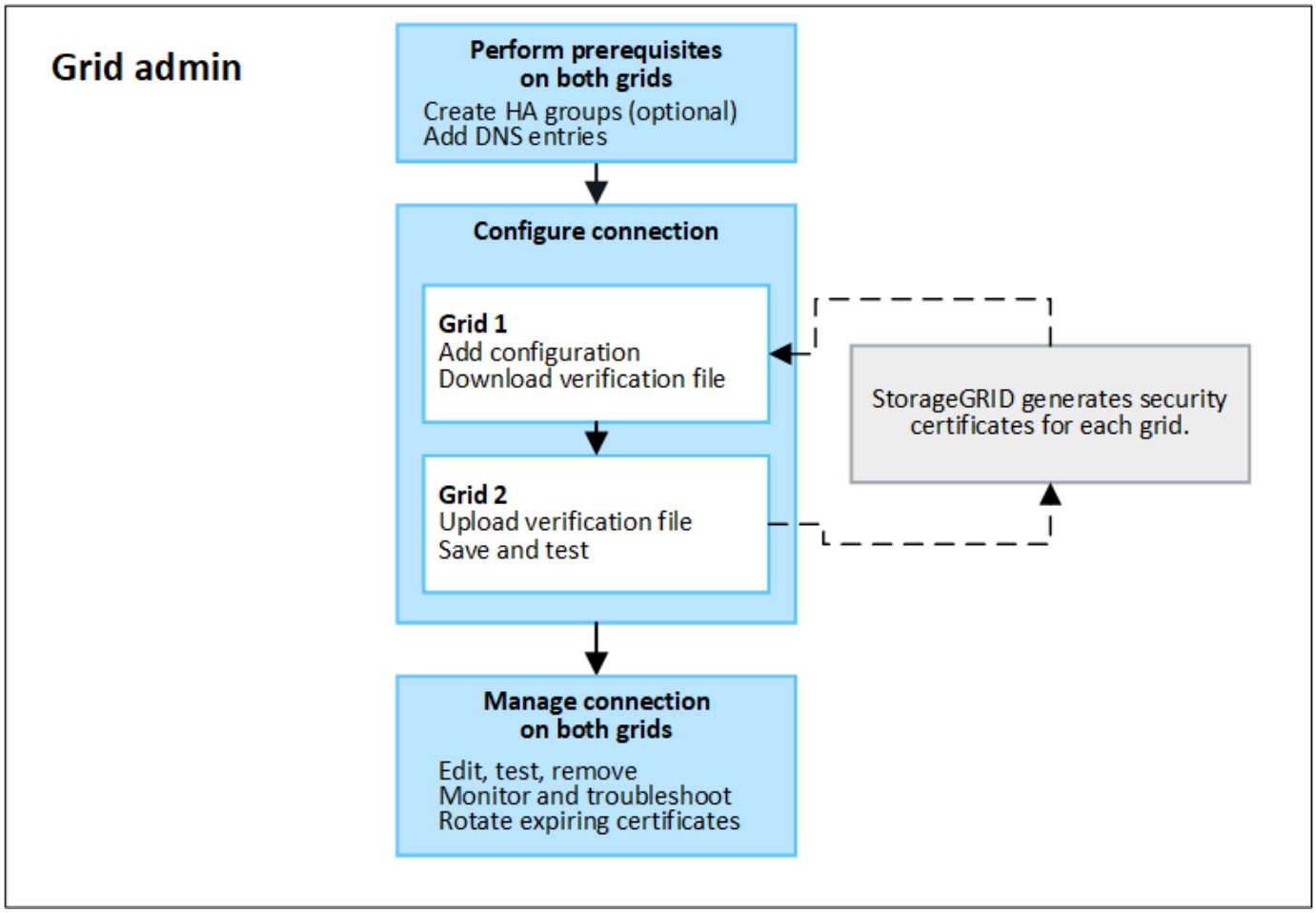
Você pode usar a federação de grids para clonar tenants e replicar seus objetos entre dois sistemas StorageGRID para recuperação de desastres.

O que é uma conexão de federação de grid?

Uma conexão de federação de grid é uma conexão bidirecional, confiável e segura entre Admin Nodes e Gateway Nodes em dois sistemas StorageGRID.

Fluxo de trabalho para federação de grids

O diagrama de fluxo de trabalho resume as etapas para configurar uma conexão de federação de grid entre dois grids.



Considerações e requisitos para conexões de federação de grid

- Os grids usados para a federação de grids devem estar executando versões do StorageGRID que sejam idênticas ou que tenham no máximo uma diferença de uma versão principal entre si.

  Para obter detalhes sobre os requisitos de versão, consulte a "Notas de lançamento". Você precisa fazer login com sua NetApp conta ou criar uma conta para acessar as notas de versão.

- Uma grid pode ter uma ou mais conexões de federação com outras grids. Cada conexão de federação é independente de quaisquer outras conexões. Por exemplo, se a Grid 1 tiver uma conexão com a Grid 2 e uma segunda conexão com a Grid 3, não há nenhuma conexão implícita entre a Grid 2 e a Grid 3.
- As conexões de federação de grids são bidirecionais. Após a conexão ser estabelecida, você pode monitorar e gerenciar a conexão a partir de qualquer um dos grids.
- É necessário que exista pelo menos uma conexão de federação de grade antes de você poder usar "clone de conta" ou "replicação entre grids".

Requisitos de rede e endereço IP

- As conexões de federação de Grid podem ocorrer na Grid Network, na Admin Network ou na Client Network.
- Uma conexão de federação de grids conecta um grid a outro grid. A configuração de cada grid especifica um endpoint de federação de grid no outro grid, que consiste em Admin Nodes, Gateway Nodes ou ambos.
- A melhor prática é conectar "grupos de alta disponibilidade (HA)" os nós de Gateway e de Admin em cada

grid. Usar grupos de HA ajuda a garantir que as conexões de federação de grid permaneçam online se os nós ficarem indisponíveis. Se a interface ativa em qualquer um dos grupos de HA falhar, a conexão pode usar uma interface de backup.

- Não é recomendável criar uma conexão de federação de grid que utilize o endereço IP de um único nó de administração ou nó de gateway. Se o nó ficar indisponível, a conexão de federação de grid também ficará indisponível.
- "Replicação entre grades"O armazenamento de objetos requer que os Nós de Armazenamento em cada grid possam acessar os Nós de Administração e de Gateway configurados no outro grid. Para cada grid, confirme que todos os Nós de Armazenamento tenham uma rota de alta largura de banda até os Nós de Administração ou Nós de Gateway usados para a conexão.

Use FQDNs para balancear a conexão

Para um ambiente de produção, utilize nomes de domínio totalmente qualificados (FQDNs) para identificar cada grid na conexão. Em seguida, crie as entradas DNS apropriadas, conforme descrito a seguir:

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

Ao usar várias entradas DNS, as solicitações para usar a conexão são balanceadas por carga, da seguinte forma:

- As entradas DNS que correspondem aos endereços VIP de vários grupos HA têm sua carga balanceada entre os nós ativos nos grupos HA.
- As entradas DNS que correspondem aos endereços IP de vários Nós de Administração ou Nós de Gateway têm sua carga balanceada entre os nós mapeados.

Requisitos de porta

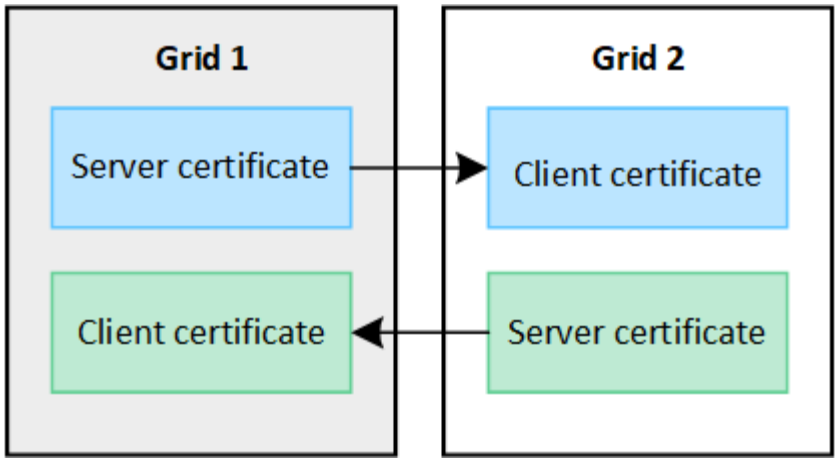
Ao criar uma conexão de federação de grids, você pode especificar qualquer número de porta não utilizado entre 23000 e 23999. Ambos os grids nessa conexão usarão a mesma porta.

Você deve garantir que nenhum nó em nenhuma das grids utilize esta porta para outras conexões.

Requisitos de certificado

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

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



Por padrão, os certificados são válidos por 730 dias (2 anos). Quando esses certificados se aproximam da data de expiração, o alerta **Expiração do certificado de federação de grid** lembra você de rotacionar 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

- "Criar conexões de federação de grid"
- "Gerenciar conexões de federação de grid"
- "Solucionar problemas de erros de federação de grid"

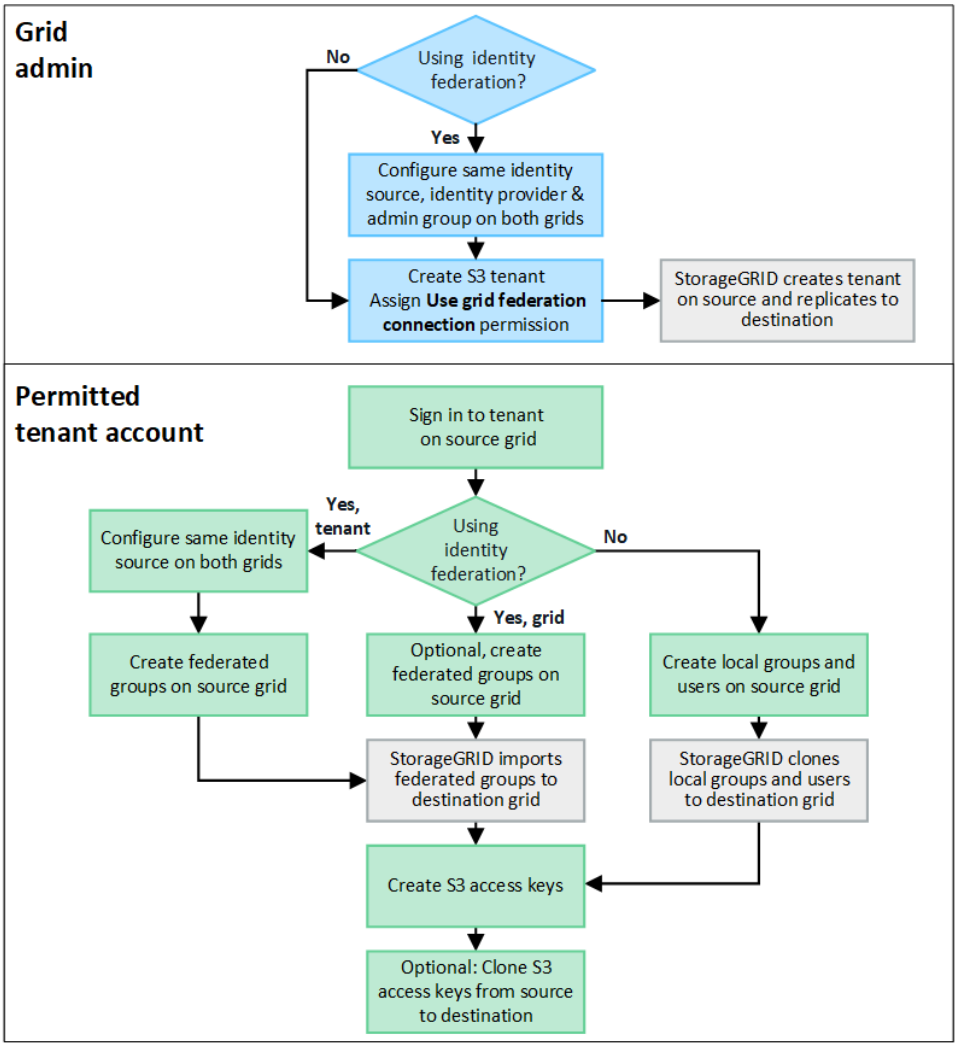
Saiba mais sobre clonagem de contas no StorageGRID

A clonagem 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 grid".

A clonagem de contas é necessária para "replicação entre grids". Clonar as informações da conta de um sistema StorageGRID de origem para um sistema StorageGRID de destino garante que os usuários e grupos do locatário possam acessar os buckets e objetos correspondentes em qualquer um dos grids.

Fluxo de trabalho para clonagem de conta

O diagrama de fluxo de trabalho mostra as etapas que os administradores da grade e os locatários autorizados executarão para configurar a clonagem de contas. Essas etapas são executadas após a "A conexão de federação de grid está configurada".



Fluxo de trabalho de administração do Grid

Os passos que os administradores da grade executam dependem de os sistemas StorageGRID na "conexão de federação de grid" utilizarem autenticação única (SSO) ou federação de identidades.

Configurar SSO para clonagem de conta (opcional)

Se qualquer sistema StorageGRID na conexão de federação de grids usar SSO, ambos os grids devem usar SSO. Antes de criar as contas de locatário para a federação de grids, os administradores dos grids de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grids. Consulte "Use federação de identidades".
2. Configure o mesmo provedor de identidade SSO (IdP) para ambas as grids. Consulte "Configure o single sign-on (SSO)".
3. "Crie o mesmo grupo de administradores" em ambas as grades, importando o mesmo grupo federado.

   Ao criar o locatário, você selecionará este grupo para ter a permissão inicial de acesso à raiz tanto para as contas de locatário de origem quanto de destino.

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

Configurar federação de identidade em nível de grid para account clone (opcional)

Se qualquer um dos sistemas StorageGRID usar federação de identidade sem SSO, ambos os grids devem usar federação de identidade. Antes de criar as contas de locatário para a federação de grids, os administradores dos grids de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grids. Consulte "Use federação de identidades".
2. Opcionalmente, se um grupo federado tiver permissão inicial de acesso Root para ambas as contas de locatário de origem e destino, "crie o mesmo grupo de administradores" em ambos os grids importando o mesmo grupo federado.

   Se você atribuir permissão de acesso de usuário raiz a um grupo federado que não existe em ambas as grids, o locatário não será replicado para a grid de destino.

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

Criar conta de locatário S3 permitida

Após configurar opcionalmente o SSO ou a federação de identidades, um administrador de grid executa estas etapas para determinar quais tenants podem replicar objetos de bucket para outros sistemas StorageGRID.

Passos

1. Determine qual grid você deseja que seja o grid de origem do tenant para operações de clonagem de conta.

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

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

   Se essa permissão for atribuída, tanto as contas de locatário de origem quanto as de destino devem 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 grids usem a mesma fonte de identidade.

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

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

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

- Se você selecionou um grupo federado para ter permissão de acesso de usuário raiz para o locatário, esse grupo é clonado para o locatário de destino.
- Se você selecionou um usuário local com permissão de acesso de usuário raiz para o locatário, esse usuário será clonado para o locatário de destino. No entanto, a senha desse usuário não será clonada.

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

Fluxo de trabalho permitido para conta de tenant

Após um locatário com a permissão **Usar conexão de federação de grid** ser replicado para a grid de destino, as contas de locatário permitidas podem executar estas etapas para clonar grupos de locatários, usuários e chaves de acesso S3.

Passos

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

   Quando novos grupos ou usuários são criados no locatário de origem, StorageGRID os clona automaticamente para o locatário de destino, mas não ocorre clonagem do destino de volta para a origem.
4. Crie chaves de acesso S3.
5. Opcionalmente, clone as chaves de acesso S3 do locatário de origem para o locatário de destino.

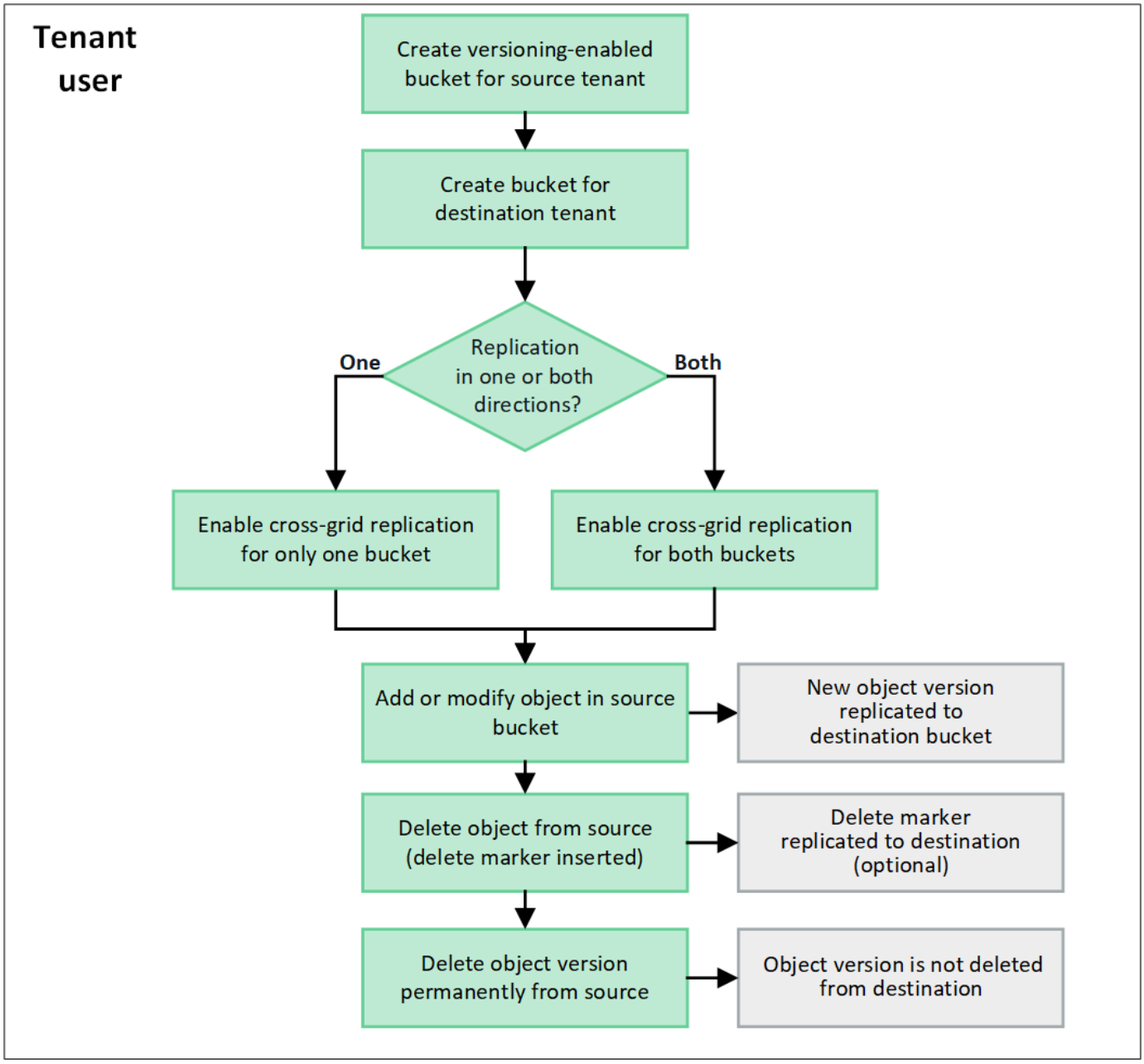
Para obter detalhes sobre o fluxo de trabalho permitido para contas de locatários e para saber como grupos, usuários e chaves de acesso do S3 são clonados, consulte "Clonar grupos de tenants e usuários" e "Clonar chaves de acesso S3 usando a API".

Saiba mais sobre replicação entre grids no StorageGRID

A replicação entre grades é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID conectados em uma "conexão de federação de grid". "Clonagem de conta"é necessário para a replicação entre grades.

Fluxo de trabalho para replicação entre grids

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



Requisitos para replicação entre grids

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

- Podem ter nomes diferentes entre si
- Pode ter regiões diferentes
- É necessário ter o versionamento ativado
- Deve estar vazio

Após a criação de ambos os buckets, a replicação entre grades pode ser configurada para um ou ambos os buckets.

Saiba mais

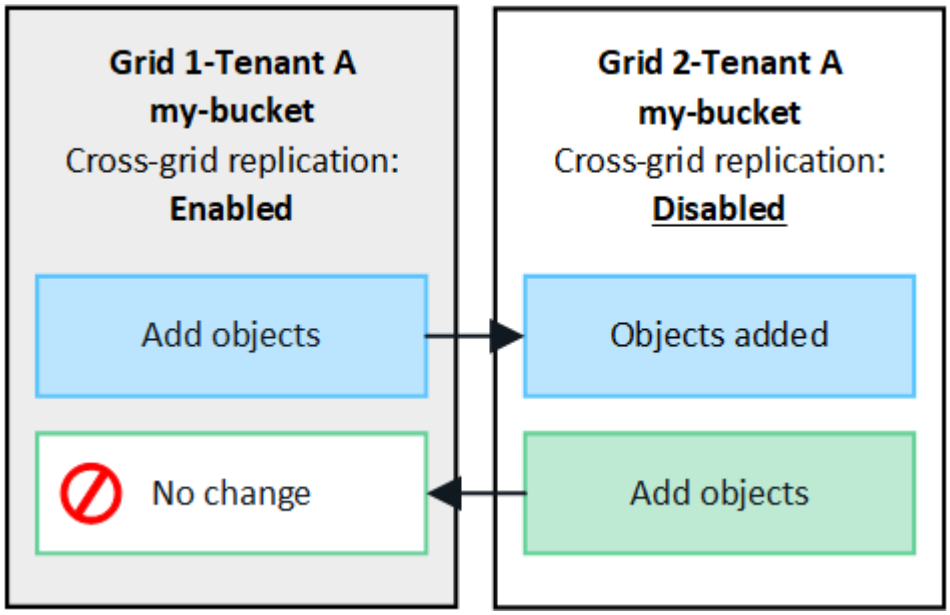
"Gerencie a replicação entre grades"

Como funciona a replicação entre grades

Você pode configurar a replicação entre grades para ocorrer em uma direção ou em ambas as direções.

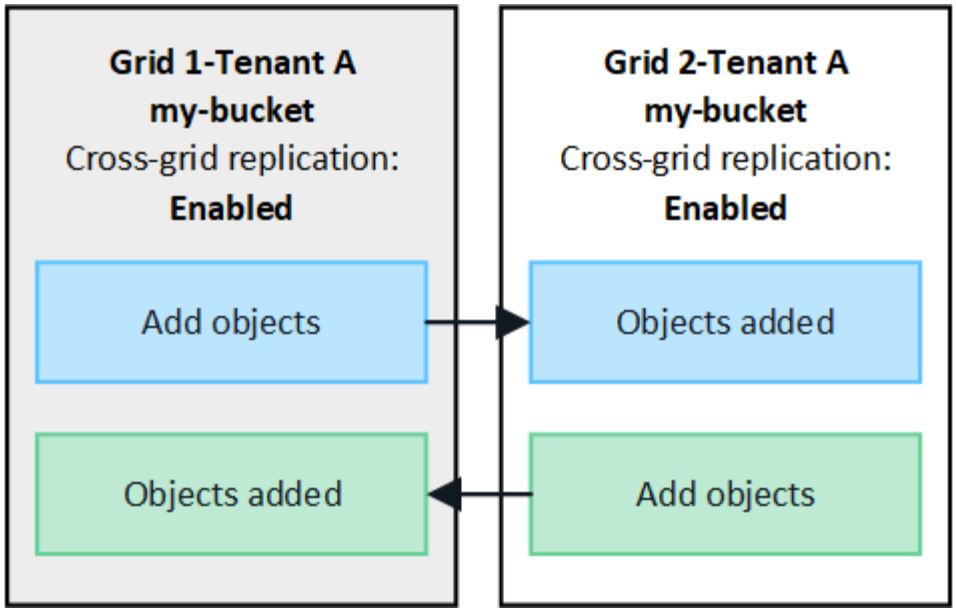
Replicação em uma direção

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



Replicação em ambas as direções

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



O que acontece quando objetos são ingeridos?

Quando um cliente S3 adiciona um objeto a um bucket com replicação entre grades habilitada, ocorre o seguinte:

1. StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo necessário 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 GetObject ou HeadObject. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que possui um dos seguintes valores:

Grid	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida para todas as conexões do grid. • **PENDENTE**: O objeto ainda não foi replicado para pelo menos uma conexão de grid. • **FALHA**: A replicação não está pendente para nenhuma conexão de grid e pelo menos uma falhou com uma falha permanente. Você deve resolver o erro.
Destino	**RÉPLICA**: O objeto foi replicado da grid de origem.

   StorageGRID não suporta o `x-amz-replication-status` cabeçalho.

2. StorageGRID utiliza as políticas ILM ativas de cada grid para gerenciar os objetos, da mesma forma que faria com qualquer outro objeto. Por exemplo, o Objeto A no Grid 1 pode ser armazenado como duas cópias replicadas e mantido indefinidamente, enquanto a cópia do Objeto A que foi replicada para o Grid 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 em "Excluir fluxo de dados", 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 opção "Excluir objetos no bucket" para remover todos os objetos de um bucket.
- O bucket possui uma configuração de ciclo de vida, que expira.
- O último período de tempo na regra ILM para o objeto termina e não há mais posicionamentos especificados.

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

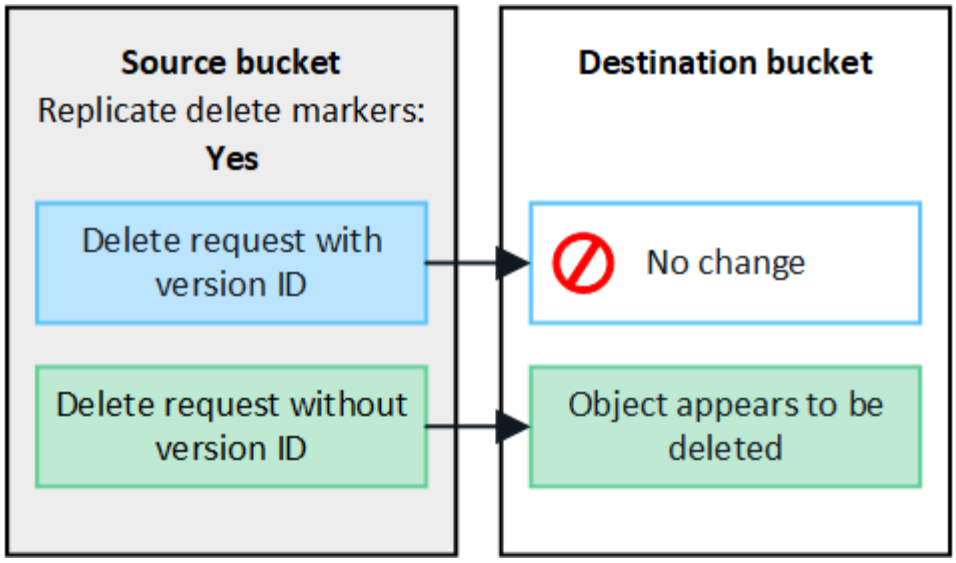
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket com replicação entre grades habilitada, revise como os clientes S3 excluem objetos de buckets com versionamento habilitado, conforme descrito a seguir:

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

Quando um cliente S3 exclui um objeto de um bucket que possui replicação entre grades habilitada, 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 grid de origem. No entanto, 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, StorageGRID pode, opcionalmente, replicar o marcador de exclusão, dependendo de como a replicação entre grids está configurada para o bucket:
  - Se você optar por replicar os marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao bucket de origem e replicado para o bucket de destino. Na prática, o objeto parecerá ter sido excluído em ambas as grids.
  - Se você optar por não replicar os marcadores de exclusão, um marcador de exclusão será adicionado ao bucket de origem, mas não será replicado para o bucket de destino. Na prática, os objetos excluídos na grid de origem não serão excluídos na grid de destino.

Na figura, **Replicar marcadores de exclusão** foi definido como **Sim** quando "A replicação entre grades foi ativada". As solicitações de exclusão para o bucket de origem que incluem um ID de versão não excluem objetos do bucket de destino. As solicitações de exclusão para o bucket de origem que não incluem um ID de versão parecem excluir objetos no bucket de destino.



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

Como os objetos criptografados são replicados

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

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

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

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

Para usar a criptografia em nível de grid, defina a opção **Criptografia de objeto armazenado** como **AES-256**. A criptografia em nível de grid se aplica a quaisquer objetos que não estejam criptografados no nível do bucket ou que sejam ingeridos sem o cabeçalho de solicitação `x-amz-server-side-encryption`. Consulte "Configurar as opções de rede e de objeto".

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

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

1. Use o `x-amz-server-side-encryption`cabeçalho de ingestão, se presente.

2. Caso não haja um cabeçalho de ingestão, utilize a configuração de criptografia padrão do bucket, se configurada.
3. Se uma configuração de bucket não estiver definida, use a configuração de criptografia de toda a grade, se estiver configurada.
4. Se não houver uma configuração para toda a grade, não criptografe o objeto de origem.

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

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

Replicação entre grades com S3 Object Lock

Você pode configurar a replicação entre grids entre buckets do StorageGRID com o S3 Object Lock ativado nas seguintes circunstâncias.

Quando o S3 Object Lock no bucket de origem está…	E o S3 Object Lock no bucket de destino é…
Habilitado	Habilitado
Desabilitado	Habilitado

Quando o S3 Object Lock no bucket de origem estiver ativado:

- Os objetos são bloqueados com configurações de retenção no destino nesta ordem:
  a. Os valores do cabeçalho de retenção do objeto de origem para:

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. A retenção padrão do bucket de origem, se definida.
  c. A retenção padrão do bucket de destino, se definida.

  A configuração de retenção padrão do bucket de destino não substitui as configurações de retenção replicadas do objeto de origem.

- Você pode definir o status de guarda legal para o objeto de destino usando `x-amz-object-lock-legal-hold` ao fazer o upload do objeto.
- Ocorre um erro se o locatário ou bucket de destino não for compatível com as configurações de S3 Object Lock do objeto de origem. Consulte "Alertas e erros de replicação entre grids."

Quando o bloqueio de objeto S3 no bucket de origem está desativado:

- Você pode configurar a retenção padrão no bucket de destino para aplicar as configurações de retenção do S3 Object Lock ao objeto de destino.
- O objeto de destino não pode definir um status de guarda legal.

PutObjectTagging e DeleteObjectTagging não são suportados

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

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

PutObjectRetention e PutObjectLegalHold não são suportados

PutObjectRetention e PutObjectLegalHold solicitações não são totalmente compatíveis com objetos em buckets que têm replicação entre grids ativada.

Se um cliente S3 emitir uma solicitação PutObjectRetention ou PutObjectLegalHold, as configurações do objeto de origem serão modificadas, mas as alterações não serão aplicadas ao destino.

Como os objetos segmentados são replicados

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

Compare a replicação entre grades e a replicação CloudMirror no StorageGRID

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

> Não é possível usar CloudMirror em um bucket replicado por replicação entre grades, e vice-versa.

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

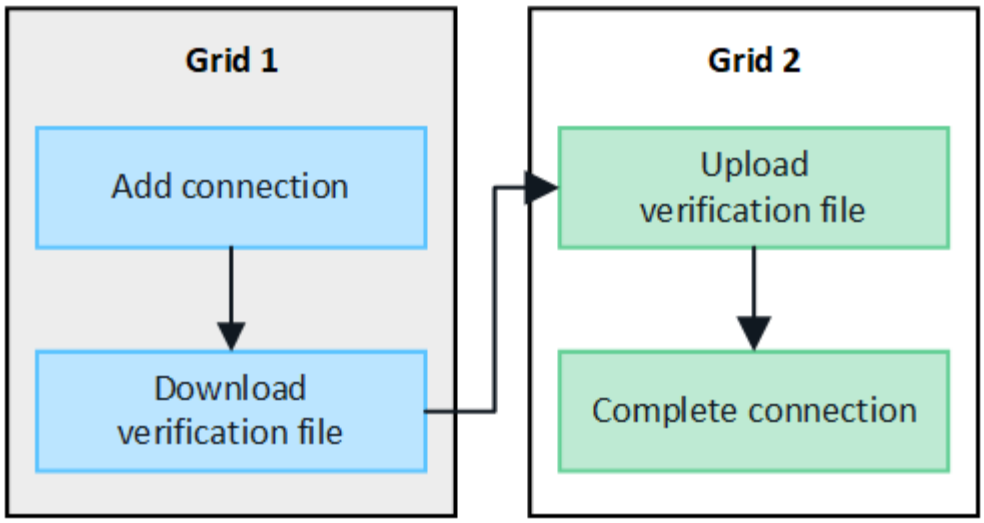
	Replicação entre grades	CloudMirror serviço de replicação
Como é configurado?	1. Configurar uma conexão de federação de grids entre dois grids. 2. Adicione novas contas de locatário, que são clonadas automaticamente para a outra grid. 3. Adicione novos grupos de locatários e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grid e habilite a replicação entre grids para ocorrer em uma ou ambas as direções.	1. Um usuário locatário configura a replicação CloudMirror definindo um endpoint CloudMirror (endereço IP, credenciais e assim por diante) usando o Tenant Manager ou a S3 API. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint CloudMirror.
Quem é responsável por configurá-lo?	• Um administrador de grid configura a conexão e os locatários. • Os usuários locatários configuram os grupos, usuários, chaves e buckets.	Normalmente, um usuário locatário.
Qual é o destino?	Um bucket S3 correspondente e idêntico no outro sistema StorageGRID na conexão de federação de grid.	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3). • Google Cloud Platform (GCP)
O versionamento de objetos é necessário?	Sim, tanto o bucket de origem quanto o de destino devem ter o versionamento de objetos ativado.	Não, a replicação CloudMirror suporta qualquer combinação de buckets não versionados e versionados, tanto na origem quanto no destino.
O que faz com que os objetos sejam movidos para o destino?	Os objetos são replicados automaticamente quando são adicionados a um bucket que tem a replicação entre grades habilitada.	Os objetos são replicados automaticamente quando são adicionados a um bucket que foi configurado com um endpoint CloudMirror. Os objetos que já existiam no bucket de origem antes de o bucket ser configurado com o endpoint CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são replicados?	A replicação entre grids cria objetos versionados e replica o ID da versão do bucket de origem para o bucket de destino. Isso permite que a ordem das versões seja mantida em ambos os grids.	CloudMirror replication não exige buckets com controle de versão habilitado, então o CloudMirror só pode manter a ordem de uma chave dentro de um site. Não há garantias de que a ordem será mantida para solicitações a um objeto em sites diferentes.
E se um objeto não puder ser replicado?	O objeto é enfileirado para replicação, sujeito aos limites de armazenamento de metadados.	O objeto é enfileirado para replicação, sujeito aos limites dos serviços da plataforma (veja "Recomendações para o uso de serviços de plataforma").

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

Criar conexões de federação de grids StorageGRID

Você pode criar uma conexão de federação de grid entre dois sistemas StorageGRID se desejar clonar detalhes de locatários e replicar dados de objetos.

Conforme ilustrado na figura, a criação de uma conexão de federação de grades inclui etapas em ambas as grades. Você adiciona a conexão em uma grade e a conclui na outra. Você pode começar por qualquer uma das grades.



Antes de começar

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

Adicionar conexão

Execute estas etapas em qualquer um dos dois sistemas StorageGRID.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione **Adicionar conexão**.
4. Insira os detalhes da conexão.

Campo	Descrição
Nome da conexão	Um nome único para ajudar você a reconhecer essa conexão, por exemplo, "Grid 1-Grid 2".
FQDN ou IP para esta grid	Uma das seguintes opções: • O FQDN da grid na qual você está conectado no momento • Um endereço VIP de um grupo HA neste grid • Um endereço IP de um Nó de Administração ou Nó de Gateway neste grid. O IP pode estar em qualquer rede que o grid de destino possa alcançar.

Campo	Descrição
Porta	A porta que você deseja usar para esta conexão. Você pode inserir qualquer número de porta não utilizado entre 23000 e 23999. Ambas as grids nesta conexão usarão a mesma porta. Você deve garantir que nenhum nó em nenhuma das grids use esta porta para outras conexões.
Dias de validade do certificado para este grid	O número de dias que você deseja que os certificados de segurança para esta grid na conexão sejam válidos. O valor padrão é 730 dias (2 anos), mas você pode inserir qualquer valor de 1 a 762 dias. StorageGRID gera automaticamente certificados de cliente e servidor para cada grid quando você salva a conexão.
Senha de provisionamento para esta grid	A senha de provisionamento para o grid no qual você está conectado.
FQDN ou IP para a outra grid	Uma das seguintes opções: • O FQDN do grid ao qual você deseja se conectar • Um endereço VIP de um grupo HA em outra grid • Um endereço IP de um Nó de Administração ou Nó de Gateway na outra grid. O IP pode estar em qualquer rede que a grid de origem possa alcançar.

5. Selecione **Salvar e continuar**.
6. Na etapa "Baixar arquivo de verificação", selecione "Baixar arquivo de verificação".

   Após a conexão ser concluída na outra grid, você não poderá mais baixar o arquivo de verificação de nenhuma das grids.

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 da Grid.
9. Confirme que a nova conexão está sendo exibida e que o seu **Status de conexão** é **Aguardando conexão**.
10. Forneça o arquivo *`connection-name`*`.grid-federation` ao administrador da outra grid.

Conexão completa

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

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.

2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de Upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, localize e selecione o arquivo baixado na primeira grade (*`connection-name`*`.grid-federation`).

   Os detalhes da conexão são exibidos.

5. Opcionalmente, insira um número diferente de dias de validade para os certificados de segurança desta grid. A entrada **Dias de validade do certificado** assume por padrão o valor que você inseriu na primeira grid, mas cada grid pode usar datas de expiração diferentes.

   Em geral, utilize 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 deixará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

6. Insira a senha de provisionamento do grid no qual você está conectado.
7. Selecione **Salvar e testar**.

   Os certificados são gerados e a conexão é testada. Se a conexão for válida, uma mensagem de sucesso é exibida e a nova conexão é listada na página de Grid federation. O **Connection status** será **Connected**.

   Se aparecer uma mensagem de erro, resolva os problemas. Consulte "Solucionar problemas de erros de federação de grid".

8. Acesse a página de federação do Grid no primeiro grid e atualize o navegador. Confirme que o **Status da conexão** agora é **Conectado**.
9. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

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

Depois que você terminar

- Analise as considerações para "gerenciando locatários permitidos".
- "Crie uma ou mais novas contas de locatário", atribue a permissão **Usar conexão de federação de grid** e selecione a nova conexão.
- "Gerenciar a conexão" conforme necessário. Você pode editar os valores de conexão, testar uma conexão, rotacionar os certificados de conexão ou remover uma conexão.
- "Monitore a conexão" como parte das suas atividades normais de monitoramento do StorageGRID.
- "Solucione problemas de conexão", incluindo a resolução de quaisquer alertas e erros relacionados à clonagem de contas e à replicação entre grids.

Gerenciar conexões de federação de grids do StorageGRID

O gerenciamento de conexões de federação de grid entre StorageGRID systems inclui editar detalhes da conexão, rotacionar os certificados, remover permissões de tenant e remover conexões não utilizadas.

Antes de começar

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

Editar uma conexão de federação de grid

Você pode editar uma conexão de federação de grids fazendo login no nó de administração principal em qualquer um dos grids da conexão. Depois de fazer alterações no primeiro grid, você deve baixar um novo arquivo de verificação e carregá-lo no outro grid.

> Enquanto a conexão estiver sendo editada, as solicitações de clonagem de conta ou replicação entre grades continuarão usando as configurações de conexão existentes. Quaisquer edições que você fizer na primeira grade serão salvas localmente, mas não serão usadas até que tenham sido carregadas na segunda grade, salvas e testadas.

Comece a editar a conexão

Passos

1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Nós** e confirme se todos os outros Admin Nodes em seu sistema estão online.

   > Ao editar uma conexão de federação de grid, StorageGRID tenta salvar um arquivo de "configuração candidata" em todos os nós de administração do primeiro grid. Se esse arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso aparece ao selecionar **Salvar e testar**.

3. Selecione **Configuração** > **Sistema** > **Grid federation**.
4. Edite os detalhes da conexão usando o menu **Ações** na página de federação do Grid ou na página de detalhes de uma conexão específica. Veja "Criar conexões de federação de grid" o que inserir.

   Menu de ações

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

   Página de detalhes

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

5. Insira a senha de provisionamento da grid na qual você está conectado.
6. Selecione **Salvar e continuar**.

   Os novos valores são salvos, mas não serão aplicados à conexão até que você carregue o novo arquivo de verificação na outra grid.

7. Selecione **Download verification file**.

   Para baixar este arquivo posteriormente, acesse a página de detalhes da conexão.

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

   > O arquivo de verificação contém segredos e deve ser armazenado e transmitido com segurança.

9. Selecione **Fechar** para retornar à página de federação da Grid.
10. Confirme se o **Status da conexão** está como **Edição pendente**.

    > Se o status da conexão era diferente de **Conectado** quando você começou a editar a conexão, ele não mudará para **Edição pendente**.

11. Forneça o arquivo *connection-name*`.grid-federation` ao administrador da outra grid.

Finalize a edição da conexão

Finalize a edição da conexão carregando o arquivo de verificação na outra grid.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, localize e selecione o arquivo que foi baixado do primeiro grid.
5. Insira a senha de provisionamento do grid no qual você está conectado.
6. Selecione **Salvar e testar**.

   Se a conexão puder ser estabelecida usando os valores editados, uma mensagem de sucesso será exibida. Caso contrário, uma mensagem de erro será exibida. Analise a mensagem e resolva quaisquer problemas.

7. Feche o assistente para retornar à página de federação do Grid.
8. Confirme se o **Status da conexão** é **Conectado**.
9. Acesse a página de federação do Grid no primeiro grid e atualize o navegador. Confirme que o **Status da conexão** agora é **Conectado**.
10. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Testar uma conexão de federação de grid

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Teste a conexão usando o menu **Actions** na página de Grid federation ou na página de detalhes de uma conexão específica.

Menu de ações

a. Selecione o botão de opção para a conexão.

b. Selecione **Ações** > **Testar**.

Página de detalhes

a. Selecione o nome da conexão para exibir seus detalhes.

b. Selecione **Test connection**.

4. Verifique o status da conexão:

Status da conexão	Descrição
Conectado	Ambas as grids estão conectadas e comunicando-se normalmente.
Erro	A conexão está em estado de erro. Por exemplo, um certificado expirou ou um valor de configuração não é mais válido.
Edição pendente	Você editou a conexão nesta grid, mas ela ainda está usando a configuração existente. Para concluir a edição, carregue o novo arquivo de verificação na outra grid.
Aguardando conexão	Você configurou a conexão nesta grid, mas a conexão ainda não foi concluída na outra grid. Baixe o arquivo de verificação desta grid e carregue-o na outra grid.
Desconhecido	A conexão está em um estado desconhecido, possivelmente devido a um problema de rede ou a um nó offline.

5. Se o status da conexão for **Erro**, resolva quaisquer problemas. Em seguida, selecione **Testar conexão** novamente para confirmar que o problema foi resolvido.

Rotacionar certificados de conexão

Cada conexão de federação de grids utiliza quatro certificados SSL gerados automaticamente para proteger a conexão. Quando os dois certificados de cada grid estiverem próximos da data de expiração, o alerta **Expiração do certificado de federação de grids** lembra você de rotacionar os certificados.

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

Passos

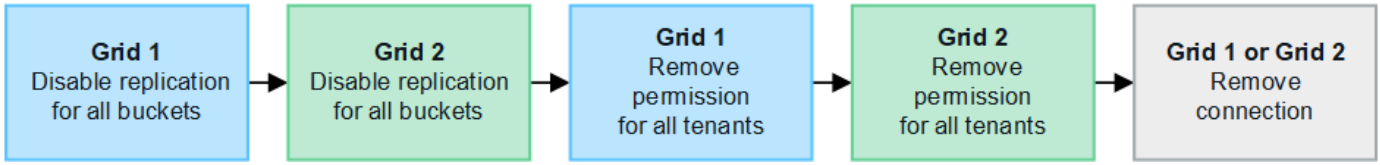
1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Em qualquer uma das abas da página de federação do Grid, selecione o nome da conexão para exibir seus detalhes.

4. Selecione a guia **Certificados**.
5. Selecione **Girar certificados**.
6. Especifique por quantos dias os novos certificados devem ser válidos.
7. Insira a senha de provisionamento da grid na qual você está conectado.
8. Selecione **Girar certificados**.
9. Se necessário, repita estas etapas na outra grid da conexão.

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

Remover uma conexão de federação de grid

Você pode remover uma conexão de federação de grid de qualquer um dos grids na conexão. Como mostrado na figura, você deve executar etapas prévias em ambos os grids para confirmar que a conexão não está sendo usada por nenhum tenant em nenhum dos grids.



Antes de remover uma conexão, observe o seguinte:

- Remover uma conexão não exclui nenhum item que já tenha sido copiado entre grids. Por exemplo, usuários, grupos e objetos do tenant que existem em ambos os grids não são excluídos de nenhum dos grids quando a permissão do tenant é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambos os grids.
- Ao remover uma conexão, quaisquer objetos que estejam com replicação pendente (ingeridos, mas ainda não replicados para a outra grid) terão sua replicação permanentemente falhada.

Desative a replicação para todos os buckets de locatários

Passos

1. A partir de qualquer uma das grades, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na aba **Inquilinos permitidos**, determine se a conexão está sendo usada por algum inquilino.
5. Se houver inquilinos listados, instrua todos os inquilinos a "desativar a replicação entre grids" para todos os seus buckets em ambas as grades da conexão.

> Não é possível remover a permissão **Usar conexão de federação de grid** se algum bucket de locatário tiver a replicação entre grids ativada. Cada conta de locatário deve desativar a replicação entre grids para seus buckets em ambas as grids.

Remover permissão para cada tenant

Após desativar a replicação entre grades para todos os buckets de locatários, remova a permissão **Usar federação de grid** de todos os locatários em ambas as grids.

Passos

1. Selecione **Configuração** > **Sistema** > **Grid federation**.
2. Selecione o nome da conexão para exibir seus detalhes.
3. Para cada locatário na guia **Locatários permitidos**, remova a permissão **Usar conexão de federação de grid** de cada locatário. Consulte "Gerenciar locatários permitidos".
4. Repita estas etapas para os tenants permitidos na outra grid.

Remover conexão

Passos

1. Quando nenhum locatário em nenhuma das grids estiver usando a conexão, selecione **Remover**.
2. Analise a mensagem de confirmação e selecione **Remover**.
   - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão de federação de grids agora foi removida de ambos os grids.
   - Se a conexão não puder ser removida (por exemplo, se ainda estiver em uso ou se houver um erro de conexão), uma mensagem de erro será exibida. Você pode fazer o seguinte:
     - Corrija o erro (recomendado). Consulte "Solucionar problemas de erros de federação de grid".
     - Remova a conexão à força. Veja a próxima seção.

Remova uma conexão de federação de grid à força

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

A remoção forçada exclui apenas a conexão da grid local. Para remover completamente a conexão, execute os mesmos passos em ambas as grids.

Passos

1. Na caixa de diálogo de confirmação, selecione **Forçar remoção**.

   Uma mensagem de sucesso é exibida. Esta conexão de federação de grids não pode mais ser usada. No entanto, os buckets dos tenants ainda podem ter a replicação entre grids habilitada e algumas cópias de objetos podem já ter sido replicadas entre os grids na conexão.

2. A partir da outra grid na conexão, faça login no Grid Manager a partir do nó de administração primário.
3. Selecione **Configuração** > **Sistema** > **Grid federation**.
4. Selecione o nome da conexão para exibir seus detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **Remover à força** para remover a conexão deste grid.

Gerencie os locatários permitidos para a federação de grids do StorageGRID

Você pode permitir que contas de locatários do S3 usem uma conexão de federação de grid 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 de um locatário para usar a conexão.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grids usando um "navegador web compatível".
- Você tem "Permissão de acesso root" para a grid na qual você está conectado.
- Você tem "Criou uma conexão de federação de grid" entre duas grades.
- Você analisou os fluxos de trabalho para "clone de conta" e "replicação entre grids".
- Conforme necessário, você já configurou o login único (SSO) ou a federação de identidade para ambas as grids na conexão. Consulte "O que é clonagem de conta".

Criar um tenant permitido

Se você deseja permitir que uma conta de locatário nova ou existente use uma conexão de federação de grade para clonagem de conta e replicação entre grades, siga as instruções gerais em "crie um novo locatário S3" ou "editar uma conta de tenant" e observe o seguinte:

- Você pode criar o locatário a partir de qualquer uma das grades na conexão. A grade onde um locatário é criado é a *grade de origem do locatário*.
- O status da conexão deve ser **Conectado**.
- Quando o locatário é criado ou editado para habilitar a permissão **Usar conexão de federação de grid** e, em seguida, salvo na primeira grid, um locatário idêntico é replicado automaticamente para a outra grid. A grid na qual o locatário é replicado é a *grid de destino do locatário*.
- Os locatários em ambas as grades terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões. Opcionalmente, você pode usar o campo **Descrição** para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado na Grade 2: "Este locatário foi criado na Grade 1."
- Por motivos de segurança, a senha do usuário raiz local não é copiada para a grid de destino.

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

- Após o novo locatário ou o locatário editado estar disponível em ambas as grades, os usuários do locatário podem realizar estas operações:
  - A partir da grid de origem do tenant, crie grupos e usuários locais, que são clonados automaticamente para a grid de destino do tenant. Consulte "Clonar grupos de tenants e usuários".
  - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para o grid de destino do locatário. Consulte "Clonar chaves de acesso S3 usando a API".
  - Crie buckets idênticos em ambas as grades na conexão e habilite a replicação entre grades em uma direção ou em ambas as direções. Consulte "Gerencie a replicação entre grades".

Visualize um tenant permitido

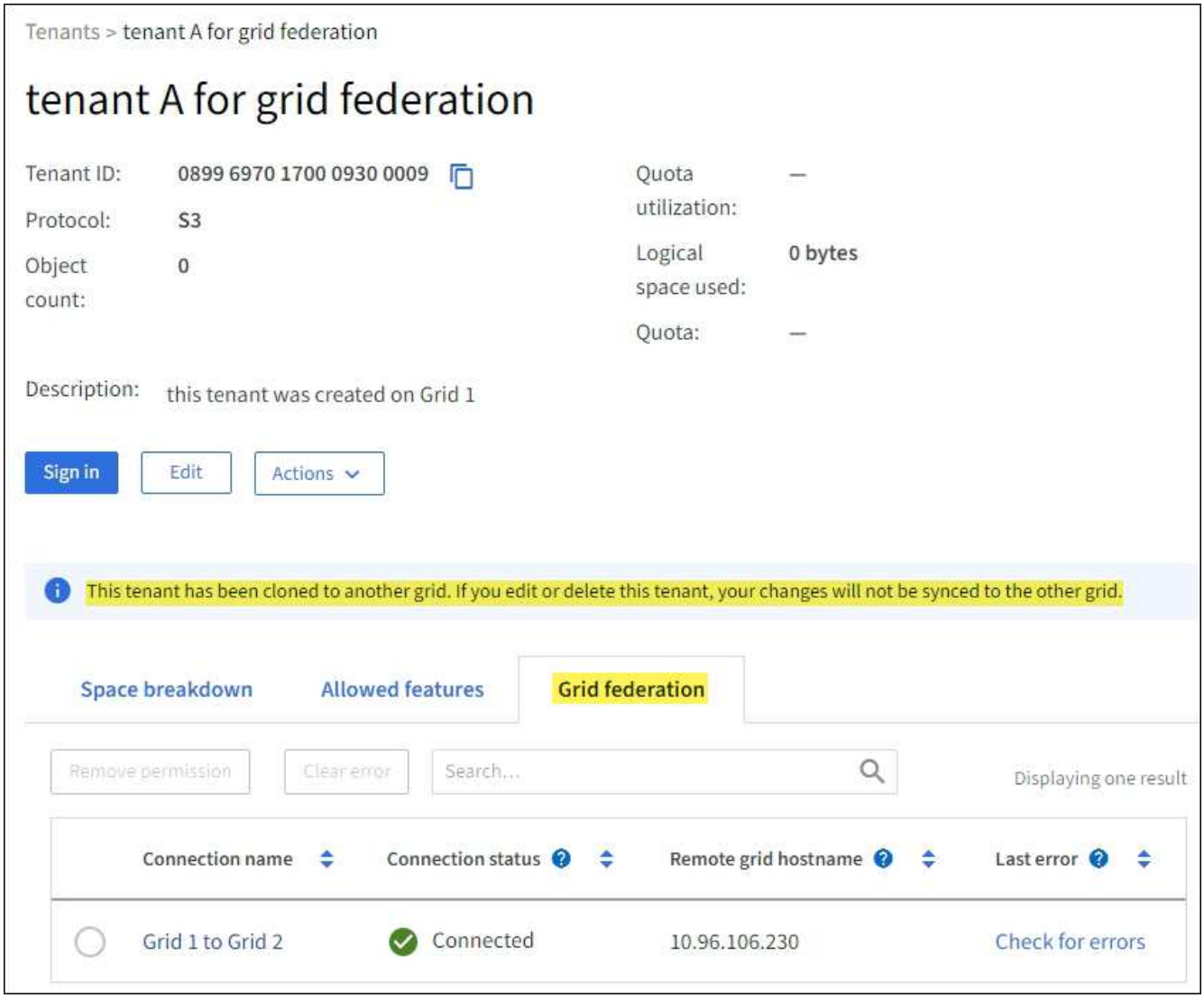
Você pode ver detalhes de um locatário que tem permissão para usar uma conexão de federação de grid.

Passos

1. Selecione **Tenants**.
2. Na página de Tenants, selecione o nome do tenant para visualizar a página de detalhes do tenant.

   Se esta for a grid de origem do tenant (ou seja, se o tenant foi criado nesta grid), um banner será exibido

para lembrar você de que o tenant foi clonado para outra grid. Se você editar ou excluir este tenant, suas alterações não serão sincronizadas com a outra grid.



3. Opcionalmente, selecione a guia **Federação de grade** para "monitorar a conexão da federação da grid".

Editar um tenant permitido

Se precisar editar um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais "editar uma conta de tenant" e observe o seguinte:

- Se um locatário tiver a permissão **Usar conexão de federação de grades**, você pode editar os detalhes do locatário em qualquer uma das grades da conexão. No entanto, quaisquer alterações que você fizer não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário sincronizados entre as grades, deverá fazer as mesmas edições em ambas as grades.
- Você não pode remover a permissão **Usar conexão de federação de grid** ao editar um tenant.
- Não é possível selecionar uma conexão de federação de grid diferente ao editar um tenant.

Excluir um tenant permitido

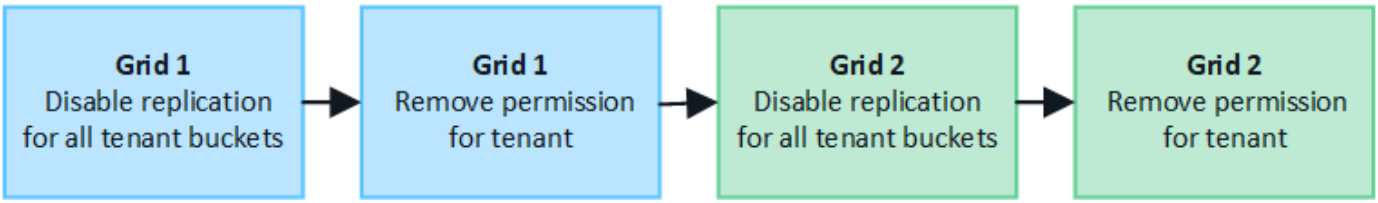
Se precisar remover um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais "Excluindo uma conta de locatário" e observe o seguinte:

- Antes de remover o locatário original na grid de origem, você deve remover todos os buckets da conta na grid de origem.
- Antes de remover o locatário clonado na grid de destino, você deve remover todos os buckets da conta na grid de destino.
- Se você remover o locatário original ou o locatário clonado, a conta não poderá mais ser usada para replicação entre grids.
- Se você estiver removendo o locatário original na grade de origem, quaisquer grupos de locatários, usuários ou chaves que foram clonados para a grade de destino permanecerão inalterados. Você pode excluir o locatário clonado ou permitir que ele gerencie seus próprios grupos, usuários, chaves de acesso e buckets.
- Se você estiver removendo o locatário clonado na grade de destino, ocorrerão erros de clonagem caso novos grupos ou usuários sejam adicionados ao locatário original.

  Para evitar esses erros, remova a permissão do locatário para usar a conexão de federação da grid antes de excluir o locatário desta grid.

Remover permissão Usar conexão de federação de grid

Para impedir que um locatário use uma conexão de federação de grid, você deve remover a permissão **Usar conexão de federação de grid**.



Antes de remover a permissão de um locatário para usar uma conexão de federação de grid, observe o seguinte:

- Não é possível remover a permissão **Usar conexão de federação de grid** se algum dos buckets do locatário tiver a replicação entre grids ativada. A conta do locatário deve desativar a replicação entre grids para todos os seus buckets primeiro.
- Remover a permissão **Usar conexão de federação de grid** não exclui nenhum item que já tenha sido replicado entre os grids. Por exemplo, quaisquer usuários, grupos e objetos do tenant que existam em ambos os grids não são excluídos de nenhum dos grids quando a permissão do tenant é removida. Se você quiser excluir esses itens, deve excluí-los manualmente de ambos os grids.
- Se você deseja reativar essa permissão com a mesma conexão de federação de grid, exclua primeiro esse locatário na grid de destino; caso contrário, reativar essa permissão resultará em um erro.

> Reativar a permissão **Usar conexão de federação de grid** torna o grid local o grid de origem e aciona a clonagem para o grid remoto especificado pela conexão de federação de grid selecionada. Se a conta do tenant já existir no grid remoto, a clonagem resultará em um erro de conflito.

Antes de começar

- Você está usando um "navegador web compatível".
- Você tem o "Permissão de acesso root" para ambas as grades.

Desative a replicação para buckets de locatários

Como primeiro passo, desative a replicação entre grids para todos os buckets de locatários.

Passos

1. A partir de qualquer uma das grades, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na aba **Inquilinos permitidos**, verifique se o inquilino está usando a conexão.
5. Se o inquilino estiver listado, instrua-o a "desativar a replicação entre grids" para todos os seus buckets em ambas as grids na conexão.

Não é possível remover a permissão **Usar conexão de federação de grid** se algum bucket do locatário tiver a replicação entre grids ativada. O locatário deve desativar a replicação entre grids para seus buckets em ambas as grids.

Remover permissão para tenant

Após desativar a replicação entre grids para buckets de locatários, você pode remover a permissão do locatário para usar a conexão de federação de grid.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Remova a permissão da página de federação do Grid ou da página de Tenants.

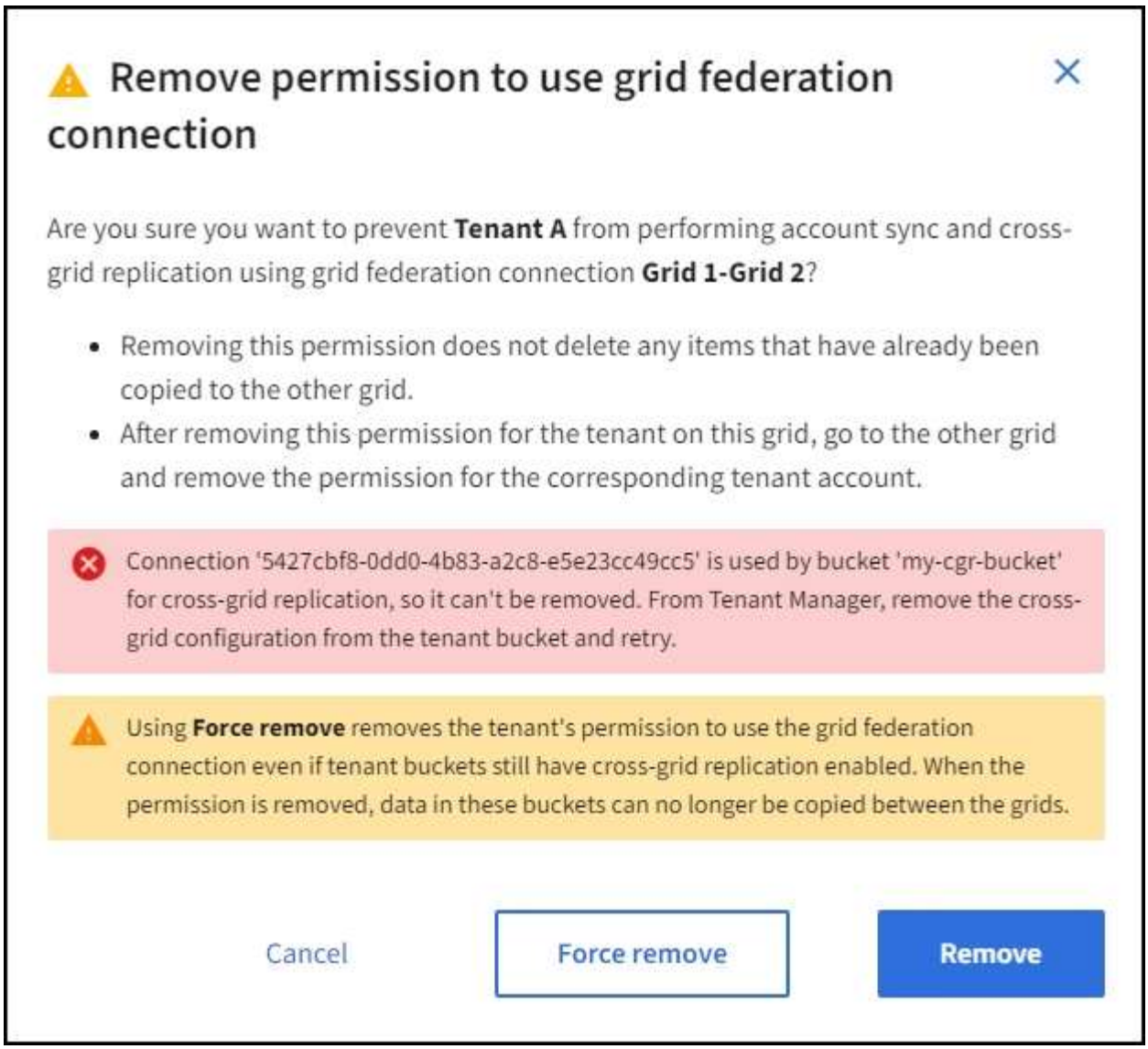
Página de federação de grid

a. Selecione **Configuração** > **Sistema** > **Grid federation**.
b. Selecione o nome da conexão para exibir a página de detalhes.
c. Na aba **Inquilinos permitidos**, selecione o botão de opção correspondente ao tenant.
d. Selecione **Remover permissão**.

Página de locatários

a. Selecione **Tenants**.
b. Selecione o nome do tenant para exibir a página de detalhes.
c. Na aba **Federação de grid**, selecione o botão de opção para a conexão.
d. Selecione **Remover permissão**.

3. Analise os avisos na caixa de diálogo de confirmação e selecione **Remover**.
   - Se a permissão puder ser removida, você retornará à página de detalhes e uma mensagem de sucesso será exibida. Este locatário não poderá mais usar a conexão de federação de grid.
   - Se um ou mais buckets de locatários ainda tiverem a replicação entre grids ativada, um erro será exibido.



Você pode fazer o seguinte:

- (Recomendado.) Faça login no Tenant Manager e desative a replicação para cada um dos buckets do tenant. Veja "Gerencie a replicação entre grades". Em seguida, repita os passos para remover a permissão **Use grid connection**.
- Remova a permissão à força. Veja a próxima seção.

4. Acesse a outra grid e repita estes passos para remover a permissão do mesmo tenant na outra grid.

Remover a permissão à força

Se necessário, você pode forçar a remoção da permissão de um locatário para usar uma conexão de federação de grid, mesmo que os buckets do locatário tenham a replicação entre grids habilitada.

Antes de revogar a permissão de um inquilino à força, observe as considerações gerais para removendo a permissão assim como estas considerações adicionais:

- Se você remover a permissão **Usar conexão de federação de grid** à força, quaisquer objetos que estejam pendentes de replicação para a outra grid (ingeridos, mas ainda não replicados) continuarão sendo replicados. Para impedir que esses objetos em processo cheguem ao bucket de destino, você também deve remover a permissão do locatário na outra grid.

- Quaisquer objetos inseridos no bucket de origem após você remover a permissão **Usar conexão de federação de grid** nunca serão replicados para o bucket de destino.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração** > **Sistema** > **Grid federation**.
3. Selecione o nome da conexão para exibir a página de detalhes.
4. Na aba **Inquilinos permitidos**, selecione o botão de opção correspondente ao tenant.
5. Selecione **Remover permissão**.
6. Analise os avisos na caixa de diálogo de confirmação e selecione **Forçar remoção**.

   Uma mensagem de sucesso é exibida. Este locatário não pode mais usar a conexão de federação de grid.

7. Conforme necessário, acesse a outra grid e repita esses passos para forçar a remoção da permissão para a mesma conta de tenant na outra grid. Por exemplo, você deve repetir esses passos na outra grid para impedir que objetos em processamento cheguem ao bucket de destino.

Solucionar problemas de erros de federação de grid no StorageGRID

Você pode precisar solucionar problemas relacionados a alertas e erros referentes a conexões de federação de grid, clonagem de contas e replicação entre grids.

Alertas e erros de conexão da federação de grid

Você pode receber alertas ou encontrar erros com suas conexões de federação de grid.

Após efetuar quaisquer alterações para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne a **Conectado**. Para obter instruções, consulte "Gerenciar conexões de federação de grid".

Alerta de falha na conexão da federação de grid

Problema

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

Detalhes

Este alerta indica que a conexão de federação de grid entre os grids não está funcionando.

Ações recomendadas

1. Analise as configurações na página de Federação de Grades para ambas as grades. Confirme se todos os valores estão corretos. Consulte "Gerenciar conexões de federação de grid".
2. Analise os certificados usados para a conexão. Certifique-se de que não haja alertas para certificados de federação de grid expirados e que os detalhes de cada certificado sejam válidos. Veja as instruções para rotacionar certificados de conexão em "Gerenciar conexões de federação de grid".
3. Confirme se todos os nós de administração e gateway em ambas as grids estão online e disponíveis. Resolva quaisquer alertas que possam estar afetando esses nós e tente novamente.
4. Se você forneceu um domínio totalmente qualificado (FQDN) para a grid local ou remota, confirme se o servidor DNS está online e disponível. Consulte "O que é federação de grid?" para os requisitos de rede, endereço IP e DNS.

Alerta de expiração do certificado de federação de grid

Problema

O alerta **Expiração do certificado de federação de grid** foi acionado.

Detalhes

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

Ações recomendadas

Consulte as instruções para rotacionar certificados de conexão em "Gerenciar conexões de federação de grid".

Erro ao editar uma conexão de federação de grid

Problema

Ao editar uma conexão de federação de grid, você verá a seguinte mensagem de aviso ao selecionar **Salvar e testar**: "Falha ao criar um arquivo de configuração candidato em um ou mais nós."

Detalhes

Ao editar uma conexão de federação de grid, StorageGRID tenta salvar um arquivo de "configuração candidata" em todos os nós de administração do primeiro grid. Uma mensagem de aviso é 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 **Nodes**.
2. Confirme se todos os nós de administração dessa grid estão online.
3. Se algum nó estiver offline, coloque-o novamente online e tente editar a conexão novamente.

Erros de clonagem de conta

Não é possível iniciar sessão em uma conta de locatário clonada

Problema

Você não pode fazer login em uma conta de locatário clonada. A mensagem de erro na página de login do Tenant Manager é: "Suas credenciais para esta conta são inválidas. Tente novamente."

Detalhes

Por motivos de segurança, quando uma conta de locatário é clonada da grid de origem para a grid de destino, a senha que você definiu para o usuário raiz local do locatário não é clonada. Da mesma forma, quando um locatário cria usuários locais em sua grid de origem, as senhas dos usuários locais não são clonadas para a grid de destino.

Ações recomendadas

Antes que o usuário raiz possa fazer login no grid de destino do locatário, um administrador do grid deve primeiro "alterar a senha do usuário raiz local" no grid de destino.

Antes que um usuário local clonado possa fazer login na grade de destino do locatário, o usuário raiz do locatário clonado deve adicionar uma senha para o usuário na grade de destino. Para obter instruções, consulte "Gerenciar usuários" nas instruções para usar o Tenant Manager.

Tenant criado sem um clone

Problema

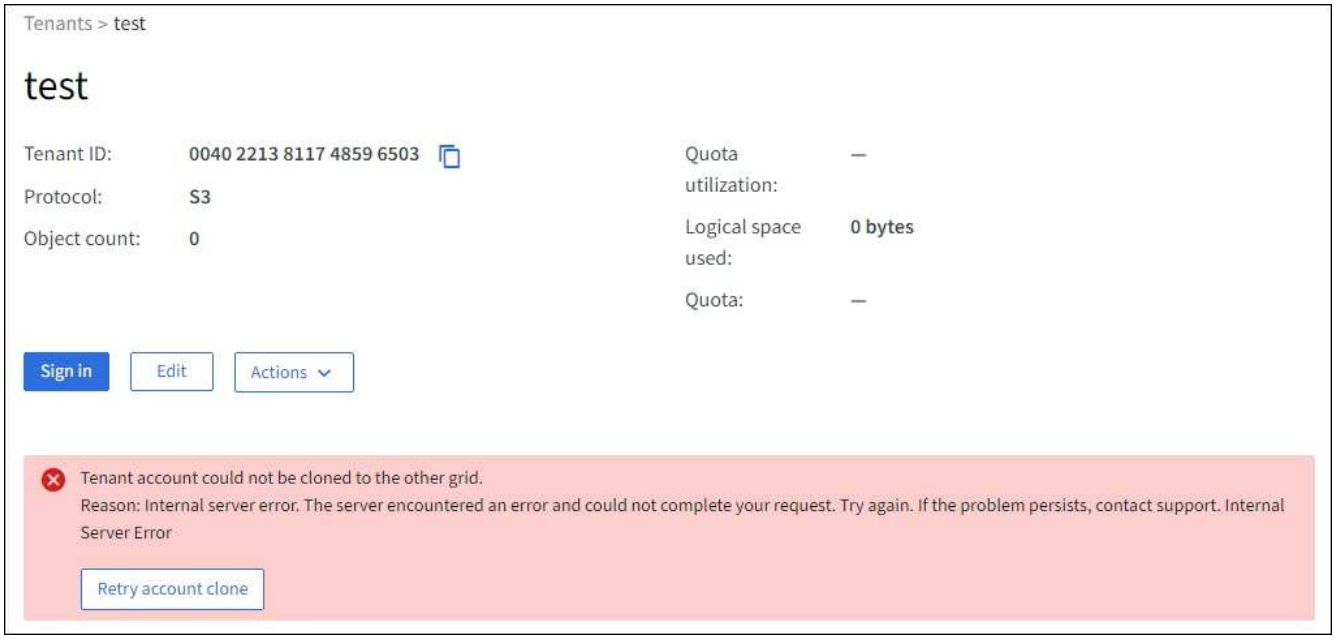
Você vê a mensagem "Tenant created without a clone" após criar um novo tenant com a permissão **Use grid federation connection**.

Detalhes

Esse problema pode ocorrer se as atualizações do status da conexão forem atrasadas, o que pode fazer com que uma conexão instável seja listada como **Connected**.

Ações recomendadas

1. Analise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo a conexão de funcionar. Consulte Alertas e erros de conexão da federação de grid.
2. Siga as instruções para testar uma conexão de federação de grid em "Gerenciar conexões de federação de grid" para confirmar que o problema foi corrigido.
3. Na grid de origem do tenant, selecione **Tenants**.
4. Localize a conta do tenant que não pôde ser clonada.
5. Selecione o nome do tenant para exibir a página de detalhes.
6. Selecione **Retry account clone**.



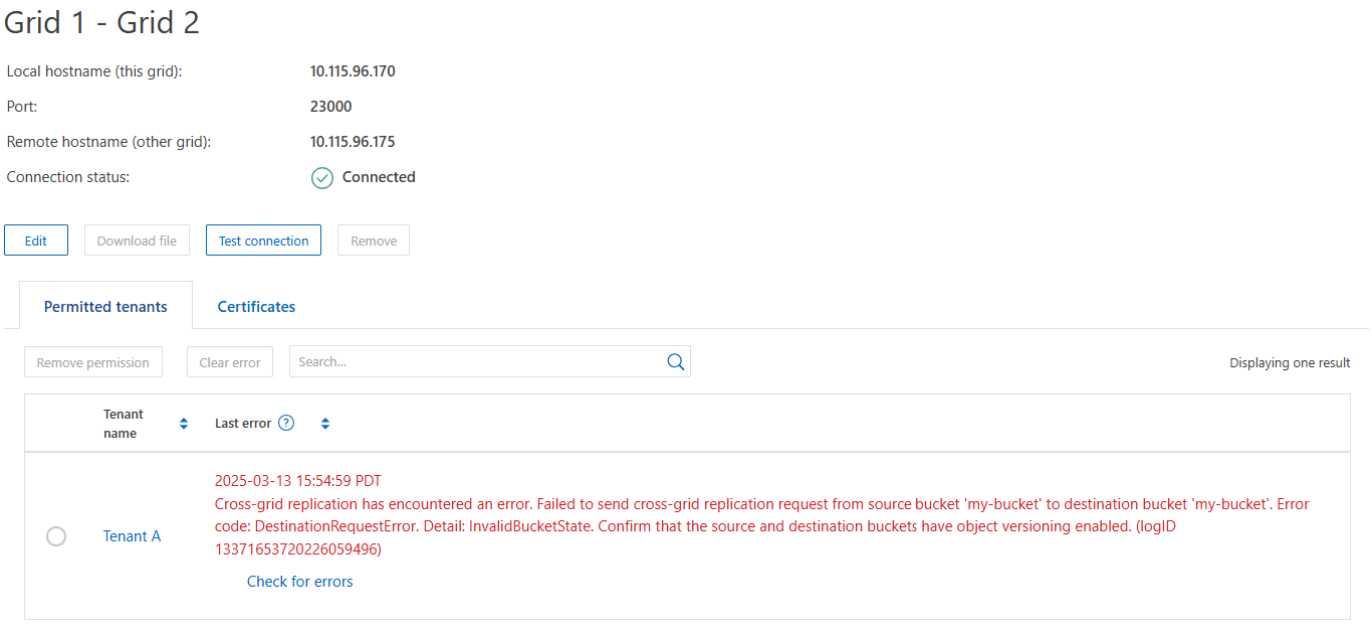
Se o erro tiver sido resolvido, a conta do locatário agora será clonada para a outra grade.

Alertas e erros de replicação entre grids

Último erro exibido para conexão ou locatário

Problema

Quando "Visualizando uma conexão de federação de grid" (ou quando "gerenciando os tenants permitidos" para uma conexão), você nota um erro na coluna **Último erro** na página de detalhes da conexão. Por exemplo:



Detalhes

Para cada conexão de federação de grids, a coluna **Último erro** mostra o erro mais recente ocorrido, se houver, quando os dados de um tenant estavam sendo replicados para o outro grid. Esta coluna exibe apenas o último erro de replicação entre grids; erros anteriores que possam ter ocorrido não são mostrados. Um erro nesta coluna pode ocorrer por um dos seguintes motivos:

- A versão do objeto de origem não foi encontrada.
- O bucket de origem não foi encontrado.
- O bucket de destino foi excluído.
- O bucket de destino foi recriado por uma conta diferente.
- O bucket de destino está com o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora está sem versionamento.
- O objeto de origem possui configurações de bloqueio de objeto S3 que não estão em conformidade com as configurações de retenção em nível de locatário da grade de destino.
- O objeto de origem possui configurações de Bloqueio de Objeto S3 e o Bloqueio de Objeto S3 está desativado no bucket de destino.

Ações recomendadas

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

1. Analise o texto da mensagem.
2. Execute as ações recomendadas. Por exemplo, se o versionamento foi suspenso no bucket de destino para replicação entre grids, reative o versionamento para esse bucket.
3. Selecione a conexão ou a conta de locatário na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
6. Aguarde de 5 a 6 minutos e, em seguida, insira um novo objeto no bucket. Confirme que a mensagem de erro não reaparece.

Para garantir que a mensagem de erro seja eliminada, aguarde pelo menos 5 minutos após o horário indicado na mensagem antes de inserir um novo objeto.

Após a correção do erro, um novo **Último erro** poderá aparecer se objetos forem ingeridos em um bucket diferente que também apresente um erro.

7. Para determinar se algum objeto não foi replicado devido a um erro no bucket, consulte "Identifique e repita operações de replicação com falha".

Alerta de falha permanente de replicação entre grids

Problema

O alerta **Falha permanente na replicação entre grades** foi acionado.

Detalhes

Este alerta indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Normalmente, esse alerta é causado por uma alteração no bucket de origem ou no bucket de destino.

Ações recomendadas

1. Faça login na grid onde o alerta foi acionado.
2. Acesse **Configuração** > **Sistema** > **Federação de grade** e localize o nome da conexão listado no alerta.
3. Na aba "Inquilinos permitidos", observe a coluna "Último erro" para determinar quais contas de inquilinos apresentam erros.
4. Para obter mais informações sobre a falha, consulte as instruções em "Monitorar conexões de federação de grid" para revisar as métricas de replicação entre grades.
5. Para cada conta de inquilino afetada:
   a. Consulte as instruções em "Monitorar a atividade do locatário" para confirmar que o locatário não excedeu sua cota na grid de destino para replicação entre grids.
   b. Conforme necessário, aumente a cota do locatário na grid de destino para permitir que novos objetos sejam salvos.
6. Para cada locatário afetado, faça login no Gerenciador de Locatários em ambas as grids para que você possa comparar a lista de buckets.
7. Para cada bucket com replicação entre grades ativada, confirme o seguinte:
   - Existe um bucket correspondente para o mesmo locatário na outra grid (deve-se usar o nome exato).
   - Ambos os buckets têm o versionamento de objetos ativado (o versionamento não pode ser suspenso em nenhum dos grids).
   - Nenhum dos buckets está no estado **Excluindo objetos: somente leitura**.
8. Para confirmar se o problema foi resolvido, consulte as instruções em "Monitorar conexões de federação de grid" para revisar as métricas de replicação entre grids ou execute estas etapas:
   a. Volte para a página de federação Grid.
   b. Selecione o locatário afetado e selecione **Limpar erro** na coluna **Último erro**.
   c. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
   d. Aguarde de 5 a 6 minutos e, em seguida, insira um novo objeto no bucket. Confirme que a mensagem de erro não reaparece.

Para garantir que a mensagem de erro seja eliminada, aguarde pelo menos 5 minutos após o horário indicado na mensagem antes de inserir um novo objeto.

Pode levar até um dia para o alerta desaparecer após ele ser resolvido.

a. Acesse "Identifique e repita operações de replicação com falha" para identificar quaisquer objetos ou marcadores de exclusão que não foram replicados para a outra grid e para tentar a replicação novamente, se necessário.

Alerta de recurso de replicação entre grades indisponível

Problema

O alerta **Recurso de replicação entre grades indisponível** foi acionado.

Detalhes

Este alerta indica que existem solicitações de replicação entre grades pendentes porque um recurso está indisponível. Por exemplo, pode haver um erro de rede.

Ações recomendadas

1. Monitore o alerta para verificar se o problema se resolve sozinho.
2. Se o problema persistir, verifique se alguma das grades apresenta um alerta de **Falha na conexão de federação da grade** para a mesma conexão ou um alerta de **Não foi possível se comunicar com o nó** para um nó. Esse alerta pode ser resolvido quando você resolver esses alertas.
3. Para obter mais informações sobre a falha, consulte as instruções em "Monitorar conexões de federação de grid" para revisar as métricas de replicação entre grades.
4. Se não conseguir resolver o alerta, entre em contato com o suporte técnico.

A replicação entre grades prosseguirá normalmente após a resolução do problema.

Identifique e repita operações de replicação do StorageGRID que falharam

Após resolver o alerta **Falha permanente na replicação entre grades**, 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 Grid Management API para tentar a replicação novamente.

O alerta **Falha permanente na replicação entre grades** indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Esse alerta geralmente é causado por uma alteração no bucket de origem ou de destino. Para obter detalhes, consulte "Solucionar problemas de erros de federação de grid".

Determine se algum objeto falhou ao ser replicado

Para determinar se algum objeto ou marcador de exclusão não foi replicado para o outro grid, você pode pesquisar o log de auditoria por mensagens "CGRR (Solicitação de Replicação entre Grids)". Essa mensagem é adicionada ao log quando StorageGRID não consegue replicar um objeto, objeto multipart ou marcador de exclusão para o bucket de destino.

Você pode usar o "ferramenta audit-explain" para traduzir os resultados para um formato mais fácil de ler.

Antes de começar

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

Passos

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

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

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

   Por exemplo, este comando busca todas as mensagens CGRR dos últimos 30 minutos e utiliza a ferramenta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Os resultados do comando serão semelhantes a este exemplo, que contém entradas para seis mensagens CGRR. No exemplo, todas as solicitações de replicação entre grades retornaram um erro geral porque o objeto não pôde ser replicado. Os três primeiros erros são de operações de "replicate object" e os três últimos erros são de operações de "replicate delete marker".

```
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 grades CGRR	O nome da solicitação
inquilino	O ID da conta do tenant
conexão	O ID da conexão da federação de grid
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de exclusão • replicar objeto multipart
bucket	O nome do bucket
objeto	O nome do objeto
versão	O ID da versão do objeto

Campo	Descrição
erro	O tipo de erro. Se a replicação entre grades falhar, o erro será "Erro geral".

Tentar novamente as replicações com falha

Após gerar uma lista de objetos e marcadores de exclusão que não foram replicados para o bucket de destino e resolver os problemas subjacentes, você pode tentar a replicação novamente de duas maneiras:

- Reingira cada objeto no bucket de origem.
- Utilize a API privada de Gerenciamento de Grid, conforme descrito.

Passos

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **API documentation**.
2. Selecione **Ir para a documentação da API privada**.

> Os endpoints 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 **Experimentar**.
5. Na caixa de texto **body**, substitua a entrada de exemplo para **versionID** por um ID de versão do log de auditoria que corresponda a uma solicitação de replicação entre grades com falha.

   Certifique-se de manter as aspas duplas em torno da string.

6. Selecione **Executar**.
7. Confirme se o código de resposta do servidor é **204**, indicando que o objeto ou marcador de exclusão foi marcado como pendente para replicação entre grades para a outra grade.

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

Monitorar novas tentativas de replicação

Você deve monitorar as operações de repetição de replicação para garantir que elas sejam concluídas.

> Pode levar várias horas ou mais para que um objeto ou marcador de exclusão seja replicado para a outra grid.

Você pode monitorar as operações de repetição de duas maneiras:

- Use uma solicitação S3 "HeadObject" ou "GetObject". A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes

valores:

Grid	Status de replicação
Fonte	• **CONCLUÍDO**: A replicação foi bem-sucedida. • **PENDENTE**: O objeto ainda não foi replicado. • **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	**RÉPLICA**: O objeto foi replicado da grid de origem.

- Utilize a API privada de Gerenciamento de Grid, 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 **Experimentar**.
3. Na seção Parâmetros, 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. Verifique o status da replicação, que será um dos seguintes:
   - **PENDENTE**: O objeto ainda não foi replicado.
   - **CONCLUÍDO**: A replicação foi bem-sucedida.
   - **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar segurança

Gerenciar a segurança no StorageGRID

Você pode configurar diversas opções de segurança no Gerenciador de Grade para ajudar a proteger seu sistema StorageGRID.

Gerenciar criptografia

StorageGRID oferece diversas opções para criptografar dados. Você deve "revise os métodos de criptografia disponíveis" determinar quais delas atendem aos seus requisitos de proteção de dados.

Gerenciar certificados

Você pode "configurar e gerenciar os certificados do servidor" usá-los para conexões HTTP ou os certificados de cliente usados para autenticar a identidade de um cliente ou usuário no servidor.

Configurar os servidores de gerenciamento de chaves

O uso de um "servidor de gerenciamento de chaves" permite proteger os dados do StorageGRID mesmo se um appliance for removido do data center. Depois que os volumes do appliance são criptografados, você não pode acessar nenhum dado no appliance, a menos que o nó consiga se comunicar com o KMS.

> Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **Criptografia de Nó** para cada appliance durante a instalação, antes que o appliance seja adicionado à grid.

Gerenciar configurações de proxy

Se você estiver usando os serviços da plataforma S3 ou os Cloud Storage Pools, pode configurar um "servidor proxy de storage" entre os Storage Nodes e os endpoints externos do S3. Se você enviar pacotes AutoSupport usando HTTPS ou HTTP, pode configurar um "servidor proxy de administração" entre os Admin Nodes e o suporte técnico.

Controlar firewalls

Para aumentar a segurança do seu sistema, você pode controlar o acesso aos StorageGRID Admin Nodes abrindo ou fechando portas específicas no "firewall externo". Você também pode controlar o acesso à rede de cada nó configurando seu "firewall interno". Você pode bloquear o acesso em todas as portas, exceto aquelas necessárias para sua implantação.

Revise os métodos de criptografia do StorageGRID

StorageGRID oferece diversas opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais atendem aos seus requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Servidor de gerenciamento de chaves (KMS) no Grid Manager	Você "configurar um servidor de gerenciamento de chaves" para o site do StorageGRID e "Ative a criptografia de nó para o dispositivo". Em seguida, um nó do dispositivo se conecta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivos com **Criptografia de Nó** ativada durante a instalação. Todos os dados no dispositivo estão protegidos contra perda física ou remoção do data center. **Nota**: Gerenciar chaves de criptografia com um KMS é compatível apenas com Storage Nodes e dispositivos de serviço.

Opção de criptografia	Como funciona	Aplica-se a
Página de Criptografia de Unidade no Instalador do Dispositivo StorageGRID	Se o dispositivo contiver unidades que suportam criptografia de hardware, você pode definir uma senha de unidade durante a instalação. Ao definir uma senha de unidade, é impossível para qualquer pessoa recuperar dados válidos de unidades que foram removidas do sistema, a menos que saiba a senha. Antes de iniciar a instalação, acesse **Configurar Hardware** > **Criptografia de Unidade** para definir uma senha de unidade que se aplique a todas as unidades autocriptografáveis gerenciadas pelo StorageGRID em um nó.	Dispositivos que contêm unidades de armazenamento com criptografia automática. Todos os dados nessas unidades seguras são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas pelo SANtricity. Se você tiver um dispositivo de storage com unidades de autocriptografia e controladores SANtricity, poderá ativar a segurança da unidade no SANtricity.
Segurança de unidade no SANtricity System Manager	Se o recurso Drive Security estiver ativado para o seu StorageGRID appliance, você pode usar "SANtricity System Manager" para criar e gerenciar a chave de segurança. A chave é necessária para acessar os dados nas unidades protegidas.	Dispositivos de storage que possuem unidades de Full Disk Encryption (FDE) ou unidades com criptografia automática. Todos os dados nas unidades protegidas estão protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de storage ou com nenhum dispositivo de serviço.
Criptografia de objeto armazenado	Você habilita a opção "Criptografia de objeto armazenado" no Grid Manager. Quando habilitada, quaisquer novos objetos que não estejam criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objetos S3 recém-ingeridos. Os objetos armazenados existentes não são criptografados. Os metadados dos objetos e outros dados confidenciais não são criptografados.
Criptografia de bucket S3	Você emite uma solicitação PutBucketEncryption para habilitar a criptografia para o bucket. Quaisquer novos objetos que não estejam criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o bucket. Os objetos de bucket existentes não são criptografados. Os metadados dos objetos e outros dados confidenciais não são criptografados. "Operações em buckets"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia do lado do servidor (SSE) de objetos S3	Você emite uma solicitação S3 para armazenar um objeto e inclui o `x-amz-server-side-encryption` cabeçalho da solicitação.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados do objeto e outros dados confidenciais não são criptografados. StorageGRID gerencia as chaves. "Use criptografia do lado do servidor"
Criptografia do lado do servidor S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e inclui três cabeçalhos de solicitação. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados do objeto e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use criptografia do lado do servidor"
Criptografia de volume externo ou datastore	Você usa um método de criptografia externo ao StorageGRID para criptografar um volume ou datastore inteiro, se sua plataforma de implantação oferecer suporte a isso.	Todos os dados de objetos, metadados e dados de configuração do sistema, assumindo que cada volume ou datastore esteja criptografado. Um método de criptografia externa proporciona um controle mais rigoroso sobre os algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de objetos fora do StorageGRID	Você utiliza um método de criptografia externo ao StorageGRID para criptografar os dados e metadados antes que sejam inseridos no StorageGRID.	Apenas dados de objetos e metadados (os dados de configuração do sistema não são criptografados). Um método de criptografia externa proporciona um controle mais rigoroso sobre os algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do Usuário: Protegendo dados usando criptografia do lado do cliente"

Use vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia ao mesmo tempo. Por exemplo:

- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança de unidade no SANtricity System Manager para "duplamente criptografar" os dados nas unidades de criptografia automática nos mesmos dispositivos.
- Você pode usar um KMS para proteger os dados nos nós do dispositivo e também usar a opção de criptografia de objeto armazenado para criptografar todos os objetos quando forem inseridos.

Se apenas uma pequena parte dos seus objetos requer criptografia, considere controlar a criptografia no nível do bucket ou do objeto individual. Habilitar vários níveis de criptografia acarreta um custo adicional de desempenho.

Informações relacionadas

"Conheça as opções de criptografia com certificação FIPS"

Gerenciar certificados

Gerenciar certificados de segurança no StorageGRID

Os certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre os componentes do StorageGRID e entre os componentes do StorageGRID e sistemas externos.

StorageGRID utiliza dois tipos de certificados de segurança:

- Os **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 possuem cada um uma cópia do certificado.

- **Certificados de cliente** autenticam a identidade de um cliente ou usuário no servidor, proporcionando uma autenticação mais segura do que apenas senhas. Certificados de cliente não criptografam dados.

Quando um cliente se conecta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente compara a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas coincidirem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

StorageGRID funciona como servidor para algumas conexões (como o endpoint do balanceador de carga) ou como cliente para outras conexões (como o serviço de replicação CloudMirror).

Certificado CA padrão do Grid

StorageGRID possui uma autoridade de certificação (CA) incorporada que gera um certificado interno do Grid CA durante a instalação do sistema. O certificado Grid CA é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação (CA) externa pode emitir certificados personalizados que estejam totalmente em conformidade com as políticas de segurança da informação da sua organização.

Use o certificado da Autoridade Certificadora (CA) do Grid para ambientes que não sejam de produção. Para produção, use certificados personalizados assinados por uma autoridade certificadora externa. Conexões não seguras sem certificado são suportadas, mas não recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser aqueles especificados para verificar as conexões do servidor.
- Todos os certificados personalizados devem atender aos "Diretrizes de reforço do sistema para certificados de servidor".
- StorageGRID suporta o agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados de CA).

> ⓘ StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todos os grids. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa no lugar do certificado de CA do sistema operacional.

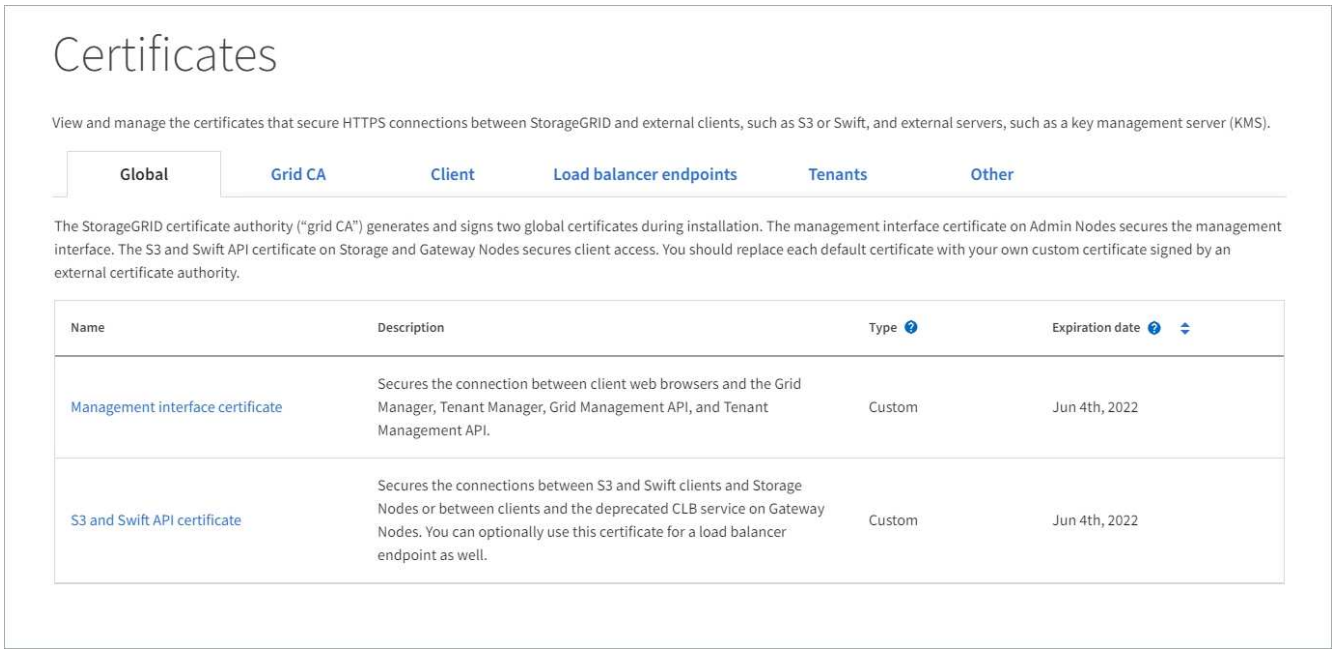
As variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter todos os certificados necessários para a sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Certificados de segurança de acesso

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 Grid Manager, selecione **Configuração** > **Segurança** > **Certificados**.



2. Selecione uma aba na página Certificados para obter informações sobre cada categoria de certificado e acessar as configurações do certificado. Você pode acessar uma aba se tiver o "permissão apropriada".

   - **Global**: protege o acesso ao StorageGRID a partir de navegadores web e clientes de API externos.
   - **Grid CA**: protege o tráfego interno do StorageGRID.
   - **Cliente**: Garante a segurança das conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - **Pontos de extremidade do balanceador de carga**: Garante a segurança das conexões entre os clientes S3 e o Load Balancer do StorageGRID.
   - **Inquilinos**: Garante conexões seguras com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de storage.
   - **Outros**: Protege as conexões StorageGRID que exigem certificados específicos.

     Cada aba é descrita abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso ao StorageGRID a partir de navegadores web e clientes externos da API S3. Dois certificados globais são gerados inicialmente pela autoridade de certificação do StorageGRID durante a instalação. A melhor prática para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- Certificado da interface de gerenciamento: Protege as conexões do navegador web do cliente com as interfaces de gerenciamento do StorageGRID.
- Certificado da API S3: Protege as conexões da API do cliente com os Nós de Armazenamento, Nós de Administração e Nós de Gateway, que os aplicativos cliente do S3 usam para fazer upload e download de 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 grid.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração é exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade certificadora externa para melhorar a segurança do grid:
  - "Substitua o certificado de interface de gerenciamento padrão gerado pelo StorageGRID" Usado para conexões do Grid Manager e do Tenant Manager.
  - "Substitua o certificado da API S3" Usado para conexões com o Storage Node e o endpoint do load balancer (opcional).
- "Restaurar o certificado padrão da interface de gerenciamento".
- "Restaurar o certificado padrão da API S3".
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado".
- Copie ou baixe o "certificado da interface de gerenciamento" ou "Certificado da API S3".

Grid CA

O Certificado CA da Grid gerado pela autoridade de certificação do StorageGRID durante a instalação do StorageGRID protege todo o tráfego interno do StorageGRID.

As informações do certificado incluem a data de expiração do certificado e o conteúdo do certificado.

Você pode "Copie ou faça o download do certificado Grid CA", mas não pode mudar.

Cliente

Certificados de cliente, gerados por uma autoridade de certificação externa, protegem as conexões entre ferramentas de monitoramento externas e o banco de dados StorageGRID Prometheus.

A tabela de certificados possui 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 expiração do certificado.

Você pode:

- "Faça o upload ou gere um novo certificado de cliente."
- Selecione o nome do certificado para exibir os detalhes do certificado, onde você pode:
  - "Altere o nome do certificado do cliente."
  - "Defina a permissão de acesso do Prometheus."
  - "Faça o upload e substitua o certificado do cliente."
  - "Copie ou faça o download do certificado do cliente."
  - "Remova o certificado do cliente."
- Selecione **Ações** para rapidamente "editar", "anexar" ou "remover" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los de uma só vez usando **Ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de endpoint do balanceador de carga Proteja as conexões entre os clientes S3 e o serviço StorageGRID Load Balancer nos nós de gateway e nos nós de administração.

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

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

Você pode:

- "Visualizar um endpoint de balanceador de carga", incluindo os detalhes do certificado.
- "Especifique um certificado de endpoint do balanceador de carga para FabricPool."
- "Use o certificado global da API S3" em vez de gerar um novo certificado de endpoint do balanceador de carga.

Locatários

Os inquilinos podem usar certificados do servidor de federação de identidades ou certificados de endpoint de serviço da plataforma para proteger suas conexões com StorageGRID.

A tabela de inquilinos possui uma linha para cada inquilino e indica se cada inquilino tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- "Selecione um nome de inquilino para entrar no Tenant Manager"
- "Selecione um nome de locatário para visualizar os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para ver os detalhes dos serviços da plataforma do locatário"
- "Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint"

Outro

StorageGRID utiliza outros certificados de segurança para fins específicos. Esses certificados estão listados por seu nome funcional. Outros certificados de segurança incluem:

- Certificados do Cloud Storage Pool
- Certificados de notificação de alerta por e-mail
- Certificados externos do servidor syslog
- Certificados de conexão de grid federation
- Certificados de federação de identidade
- Certificados do servidor de gerenciamento de chaves (KMS)
- Certificados de single sign-on

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração dos certificados de servidor e cliente, quando aplicável. Selecionar o nome de uma função abre uma aba do navegador onde você pode visualizar e editar os detalhes do certificado.

> Você só pode visualizar e acessar informações de outros certificados se tiver o "permissão apropriada".

Você pode:

- "Especifique um certificado de Cloud Storage Pool para S3, C2S S3 ou Azure"
- "Especifique um certificado para notificações de alerta por e-mail"
- "Use um certificado para um servidor syslog externo"
- "Girar certificados de conexão da federação de grid"
- "Visualizar e editar um certificado de federação de identidades"
- "Carregar certificados do servidor de gerenciamento de chaves (KMS) e do cliente"
- "Especifique manualmente um certificado SSO para uma relação de confiança de terceiros"

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado da interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre os navegadores web do cliente e a interface de gerenciamento do StorageGRID, permitindo que você acesse o Grid Manager e o Tenant Manager sem avisos de segurança. Este certificado também autentica as conexões da Grid Management API e da Tenant Management API. Você pode usar o certificado padrão criado durante a instalação ou carregar um certificado personalizado.	Em **Configuração** > **Segurança** > **Certificados**, selecione a guia **Global** e, em seguida, selecione **Certificado da interface de gerenciamento**	"Configurar certificados da interface de gerenciamento"

Certificado da API S3

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 a um nó de armazenamento e a endpoints de balanceamento de carga (opcional).	**Configuração** > **Segurança** > **Certificados**, selecione a guia **Global** e, em seguida, selecione **S3 API certificate**	"Configurar certificados da API S3"

Certificado CA da Grid

Consulte o Descrição padrão do certificado CA do Grid.

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que StorageGRID autentique o acesso de clientes externos. • Permite que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**Configuração** > **Segurança** > **Certificados** e então selecione a guia **Cliente**	"Configurar certificados de cliente"

Certificado de endpoint do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 e o serviço StorageGRID Load Balancer nos nós de gateway e nós de administração. Você pode carregar ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos cliente usam o certificado do balanceador de carga ao se conectarem ao StorageGRID para salvar e recuperar dados de objetos. Você também pode usar uma versão personalizada do Certificado da API S3 certificado global para autenticar conexões com o serviço de Load Balancer. Se o certificado global for usado para autenticar conexões com o Load Balancer, você não precisa carregar ou gerar um certificado separado para cada endpoint do Load Balancer. **Nota:** O certificado usado para autenticação do balanceador de carga é o certificado mais utilizado durante a operação normal do StorageGRID.	**Configuração** > **Rede** > **Pontos de extremidade do balanceador de carga**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade de balanceamento de carga para FabricPool"

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um StorageGRID Cloud Storage Pool para um local de armazenamento externo, como S3 Glacier ou Microsoft Azure Blob storage. É necessário um certificado diferente para cada tipo de provedor de nuvem.	**ILM** > **Pools de armazenamento**	"Criar um Cloud Storage Pool"

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 StorageGRID usado para notificações de alerta. • Se a comunicação com o servidor SMTP exigir Segurança da Camada de Transporte (TLS), você deve especificar o certificado da Autoridade Certificadora (CA) do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**Alertas** > **Configuração de e-mail**	"Configure 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 com um servidor syslog externo.	**Configuração** > **Monitoramento** > **Servidor de auditoria e syslog**	"Use um servidor syslog externo"

Certificado de conexão de federação de grid

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autenticar e criptografar informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grades.	**Configuração** > **Sistema** > **Grid federation**	• "Criar conexões de federação de grid" • "Rotacionar certificados de conexão"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre StorageGRID e um provedor de identidade externo, como Active Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidades, que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	**Configuração** > **Controle de acesso** > **Federação de identidades**	"Use federação de identidades"

Certificado do servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	**Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID com um recurso de armazenamento S3.	**Gerenciador de Locatários** > **ARMAZENAMENTO (S3)** > **Pontos de extremidade de serviços da plataforma**	"Criar endpoint de serviços de plataforma" "Editar endpoint de serviços da plataforma"

Certificado de single sign-on (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como Active Directory Federation Services (AD FS), e StorageGRID que são usados para solicitações de logon único (SSO).	**Configuração** > **Controle de acesso** > **Autenticação única**	"Configure o single sign-on (SSO)"

Exemplos de certificados

Exemplo 1: serviço de balanceador de carga

Neste exemplo, StorageGRID atua como o servidor.

1. Você configura um endpoint de balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 com o endpoint do balanceador de carga e carrega o mesmo certificado no cliente.

3. Quando o cliente deseja salvar ou recuperar dados, ele se conecta ao endpoint do balanceador de carga usando HTTPS.
4. StorageGRID responde com o certificado do servidor, que contém uma chave pública, e com uma assinatura baseada na chave privada.
5. O cliente compara a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas coincidirem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objetos para StorageGRID.

Exemplo 2: servidor externo de gerenciamento de chaves (KMS)

Neste exemplo, StorageGRID atua como o cliente.

1. Utilizando um software externo de Key Management Server, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado por uma autoridade certificadora (CA), um certificado de cliente público e a chave privada para o certificado de cliente.
2. Utilizando o Grid Manager, você configura um servidor KMS e faz upload dos certificados do servidor e do cliente, além da chave privada do cliente.
3. Quando um nó do StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura baseada na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

Tipos de certificados de servidor suportados no StorageGRID

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica).

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

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, consulte "Segurança para clientes S3".

Configurar certificados da interface de gerenciamento no StorageGRID

Você pode substituir o certificado padrão da interface de gerenciamento por um único certificado personalizado que permite aos usuários acessar o Grid Manager e o Tenant Manager sem encontrar avisos de segurança. Você também pode reverter para o certificado padrão da interface de gerenciamento ou gerar um novo.

Sobre esta tarefa

Por padrão, cada nó administrativo recebe um certificado assinado pela CA da grid. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e a 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 de vários domínios se os clientes precisarem verificar o nome do host ao se conectarem ao Grid Manager e ao Tenant Manager. Defina o certificado personalizado de forma que ele corresponda a todos os Nós de Administração na grid.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que estiver usando, os usuários também podem precisar instalar o certificado da CA do Grid no navegador da web que usarão para acessar o Grid Manager e o Tenant Manager.

Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração do certificado do servidor para a interface de gerenciamento** é acionado quando este certificado está prestes a expirar. Se necessário, você pode verificar quando o certificado atual expira selecionando **Configuração** > **Segurança** > **Certificados** e consultando a data de expiração do certificado da interface de gerenciamento na guia Global.

Se você estiver acessando o Grid Manager ou o Tenant Manager usando um nome de domínio em vez de um endereço IP, o navegador exibirá um erro de certificado sem opção para ignorá-lo caso ocorra uma das seguintes situações:

- Seu certificado de interface de gerenciamento personalizada expirou.
- Você reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão.

Adicionar um certificado de interface de gerenciamento personalizado

Para adicionar um certificado de interface de gerenciamento personalizado, você pode fornecer seu próprio certificado ou gerar um usando o Grid Manager.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione **Usar certificado personalizado**.
4. Faça o upload ou gere o certificado.

Carregar certificado

Faça o upload dos arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

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

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote de CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora (CA) intermediária. O arquivo deve conter cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado é exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

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

  Por exemplo: `storagegrid_certificate.pem`

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

d. Selecione **Salvar**. + O certificado da interface de gerenciamento personalizada é usado para todas as novas conexões subsequentes com o Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

Gerar certificado

Gere os arquivos de certificado do servidor.

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

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

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

Campo	Descrição
IP	Um ou mais endereços IP para incluir no certificado.
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Salvar**. + O certificado da interface de gerenciamento personalizada é usado para todas as novas conexões subsequentes com o Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

5. Atualize a página para garantir que o navegador web esteja atualizado.

> Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam resolvidos.

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

Restaurar o certificado padrão da interface de gerenciamento

Você pode voltar a usar o certificado de interface de gerenciamento padrão para conexões do Grid Manager e do Tenant Manager.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione **Usar certificado padrão**.

   Ao restaurar o certificado da interface de gerenciamento padrão, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado da interface de gerenciamento padrão é usado para todas as novas conexões de clientes subsequentes.

4. Atualize a página para garantir que o navegador web esteja atualizado.

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

Caso seja necessária uma validação rigorosa do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

Antes de começar

- Você tem "permissões de acesso específicas".
- Você tem o arquivo `Passwords.txt`.

Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade certificadora externa.

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó administrativo.
2. Faça login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no arquivo `Passwords.txt`.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no arquivo `Passwords.txt`.

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

3. Configurar 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 Admin Nodes. Por exemplo, `*.ui.storagegrid.example.com` usa o curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
   - Defina `--type` para `management` configurar o certificado da interface de gerenciamento, que é usado pelo Grid Manager e pelo Tenant Manager.
   - Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.

O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente de gerenciamento esteja sincronizado com a mesma fonte de tempo que StorageGRID; caso contrário, o cliente pode rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

O resultado obtido contém o certificado público necessário para o seu cliente da API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags BEGIN e END na sua seleção.

5. Saia do terminal de comandos. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Grid Manager.
   b. Selecione **Configuração** > **Segurança** > **Certificados**
   c. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags BEGIN e END.

Baixe ou copie o certificado da interface de gerenciamento

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

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione a guia **Servidor** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Baixe o arquivo de certificado ou o pacote de CA

Faça o download do arquivo de certificado ou do pacote de CA `.pem`. Se você estiver usando um pacote de CA opcional, cada certificado do pacote é exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote de CA**.

   Se você estiver baixando um pacote de certificados de autoridade certificadora (CA bundle), todos os certificados nas guias secundárias do pacote de certificados de autoridade certificadora serão baixados como um único arquivo.

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

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote PEM da CA

Copie o texto do certificado para colar em outro local. Se você estiver usando um pacote de CA opcional, cada certificado do pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar CA bundle PEM**.

   Se você estiver copiando um pacote de certificados de autoridade de certificação (CA bundle), todos os certificados nas guias secundárias do pacote de CA são copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configurar os certificados da API S3 no StorageGRID

Você pode substituir ou restaurar o certificado do servidor usado para conexões de clientes S3 com nós de armazenamento ou com endpoints de balanceadores de carga. O certificado de servidor personalizado de substituição é específico para sua organização.

Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja "StorageGRID 11.8: Configurar certificados das APIs S3 e Swift".

Sobre esta tarefa

Por padrão, cada Storage Node recebe um certificado de servidor X.509 assinado pela CA da grid. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e a chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os Storage Nodes, então você deve especificar o certificado como um curinga ou multi-domain certificate se os clientes precisarem verificar o hostname ao se conectarem ao endpoint de armazenamento. Defina o certificado personalizado de forma que ele corresponda a todos os Storage Nodes na grid.

Após concluir a configuração no servidor, você também poderá precisar instalar o certificado da Autoridade Certificadora (CA) do Grid no cliente da API S3 que você usará para acessar o sistema, dependendo da autoridade certificadora raiz (CA) que você estiver utilizando.

> Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração do certificado global do servidor para a API do S3** é acionado quando o certificado raiz do servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **Configuração** > **Segurança** > **Certificados** e consultando a data de expiração do certificado da API do S3 na guia Global.

Você pode carregar ou gerar um certificado de API S3 personalizado.

Adicionar um certificado de API S3 personalizado

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione **Usar certificado personalizado**.
4. Faça o upload ou gere o certificado.

Carregar certificado

Faça o upload dos arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

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

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote de CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora intermediária. O arquivo deve conter cada um dos arquivos de certificado de CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM de cada certificado personalizado da API S3 que foi carregado. Se você carregou um pacote de CA opcional, cada certificado é exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

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

  Por exemplo: `storagegrid_certificate.pem`

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

d. Selecione **Salvar**.

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

Gerar certificado

Gere os arquivos de certificado do servidor.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

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

Campo	Descrição
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Salvar**.

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

5. Selecione uma aba para exibir metadados do certificado padrão do servidor StorageGRID, de um certificado assinado por uma CA que foi carregado ou de um certificado personalizado que foi gerado.

> Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam resolvidos.

6. Atualize a página para garantir que o navegador web esteja atualizado.
7. Após adicionar um certificado de API S3 personalizado, a página de certificados da API S3 exibe informações detalhadas sobre o certificado personalizado em uso. Você pode baixar ou copiar o arquivo PEM do certificado conforme necessário.

Restaurar o certificado padrão da API S3

Você pode voltar a usar o certificado padrão da API S3 para conexões de clientes S3 com os nós de armazenamento. No entanto, você não pode usar o certificado padrão da API S3 para um endpoint de balanceador de carga.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione **Usar certificado padrão**.

   Ao restaurar a versão padrão do certificado global da API S3, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 será usado para novas conexões de cliente S3 subsequentes com os Storage Nodes.

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

   Se você tiver permissão de acesso Root e o certificado personalizado da API S3 tiver sido usado para conexões de endpoints do balanceador de carga, será exibida uma lista dos endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão da API S3. Vá para "Configurar pontos de extremidade do balanceador de carga" para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador web esteja atualizado.

Baixe ou copie o certificado da API S3

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

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione a guia **Servidor** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Baixe o arquivo de certificado ou o pacote de CA

Faça o download do arquivo de certificado ou do pacote de CA `.pem`. Se você estiver usando um pacote de CA opcional, cada certificado do pacote é exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote de CA**.

   Se você estiver baixando um pacote de certificados de autoridade certificadora (CA bundle), todos os certificados nas guias secundárias do pacote de certificados de autoridade certificadora serão baixados como um único arquivo.

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

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote PEM da CA

Copie o texto do certificado para colar em outro local. Se você estiver usando um pacote de CA opcional, cada certificado do pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar CA bundle PEM**.

   Se você estiver copiando um pacote de certificados de autoridade de certificação (CA bundle), todos os certificados nas guias secundárias do pacote de CA são 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

- "Utilize a API REST S3"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado CA do StorageGRID Grid

StorageGRID utiliza uma autoridade de certificação (CA) interna para proteger o tráfego interno. Este certificado não se altera caso você carregue seus próprios certificados.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Sobre esta tarefa

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

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificado PEM**, faça o download ou copie o certificado.

Baixar arquivo de certificado

Baixe o arquivo de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo do 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`

Configure os certificados do StorageGRID para FabricPool

Para clientes S3 que realizam validação rigorosa de nome de host e não suportam a desativação dessa validação, como clientes ONTAP que utilizam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o endpoint do balanceador de carga.

Antes de começar

- Você tem "permissões de acesso específicas".
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

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 certificadora (CA) reconhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA reconhecida. Certificados assinados por uma CA podem ser rotacionados sem interrupção. Eles também são mais seguros porque oferecem melhor proteção contra ataques man-in-the-middle.

Os passos a seguir fornecem diretrizes gerais para clientes S3 que utilizam FabricPool. Para obter informações e procedimentos mais detalhados, consulte "Configurar o StorageGRID para FabricPool".

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para o FabricPool usar.
2. Crie um endpoint de balanceador de carga S3 para FabricPool usar.

Ao criar um endpoint de balanceador de carga HTTPS, você será solicitado a carregar seu certificado do servidor, a chave privada do certificado e, opcionalmente, o pacote de CA.

3. Anexe StorageGRID como uma camada de nuvem no ONTAP.

   Especifique a porta do 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 da CA.

> Se o certificado StorageGRID foi emitido por uma autoridade certificadora intermediária, você deve fornecer o certificado dessa autoridade certificadora intermediária. Se o certificado StorageGRID foi emitido diretamente pela autoridade certificadora raiz, você deve fornecer o certificado dessa autoridade certificadora raiz.

Configurar certificados de cliente no StorageGRID

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus, fornecendo uma maneira segura para ferramentas externas monitorarem o StorageGRID.

Se você precisar acessar StorageGRID usando uma ferramenta de monitoramento externa, deverá carregar ou gerar um certificado de cliente usando o Grid Manager e copiar as informações do certificado para a ferramenta externa.

Veja "Gerenciar certificados de segurança" e "Configurar certificados de servidor personalizados".

> Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração dos certificados do cliente configurados na página Certificados** é acionado quando este certificado do servidor está prestes a expirar. Se necessário, você pode verificar quando o certificado atual expira selecionando **Configuração** > **Segurança** > **Certificados** e consultando a data de expiração do certificado do cliente na guia Cliente.

> Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivos especialmente configurados, consulte as informações específicas sobre "Carregando um certificado de cliente KMS".

Antes de começar

- Você tem permissão de acesso root.
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Para configurar um certificado de cliente:
  - Você possui o endereço IP ou nome de domínio do Admin Node.
  - Se você configurou o certificado da interface de gerenciamento do StorageGRID, você possui a CA, o certificado do cliente e a chave privada usados para configurar o certificado da interface de gerenciamento.
  - Para carregar seu próprio certificado, a chave privada do certificado está disponível em seu computador local.
  - A chave privada deve ter sido salva ou registrada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.

- Para editar um certificado de cliente:
  - Você possui o endereço IP ou nome de domínio do Admin Node.
  - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se utilizada) estão disponíveis em seu computador local.

Adicionar certificados de cliente

Para adicionar o certificado do cliente, utilize um destes procedimentos:

- O certificado da interface de gerenciamento já está configurado
- Certificado de cliente emitido pela CA
- Certificado gerado pelo Grid Manager

O certificado da interface de gerenciamento já está configurado

Utilize este procedimento para adicionar um certificado de cliente caso um certificado de interface de gerenciamento já esteja configurado utilizando uma CA fornecida pelo cliente, certificado de cliente e chave privada.

Passos

1. No Grid Manager, selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Add**.
3. Insira um nome de certificado.
4. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
5. Selecione **Continue**.
6. Na etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
   a. Selecione **Carregar certificado**.
   b. Selecione **Procurar** e selecione o arquivo de certificado da interface de gerenciamento (`.pem`.
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      O novo certificado aparece na guia Cliente.
7. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador caso um certificado de interface de gerenciamento não tenha sido configurado e você planeje adicionar um certificado de cliente para o Prometheus que utilize um certificado de cliente e uma chave privada emitidos por uma Autoridade Certificadora (CA).

Passos

1. Execute os passos para "configurar um certificado de interface de gerenciamento".
2. No Grid Manager, selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
3. Selecione **Add**.
4. Insira um nome de certificado.
5. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
6. Selecione **Continue**.
7. Na etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote de certificados da autoridade certificadora (CA):
   a. Selecione **Carregar certificado**.
   b. Selecione **Procurar** e selecione o certificado do cliente, a chave privada e os arquivos do pacote da CA (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.
      - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **Criar** para salvar o certificado no Grid Manager.

      Os novos certificados aparecem na guia Cliente.
8. Configurar uma ferramenta de monitoramento externa, como Grafana.

Certificado gerado pelo Grid Manager

Utilize este procedimento para adicionar um certificado de cliente administrador caso um certificado de interface de gerenciamento não tenha sido configurado e você planeje adicionar um certificado de cliente para o Prometheus que utilize a função de gerar certificado no Grid Manager.

Passos

1. No Grid Manager, selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Add**.
3. Insira um nome de certificado.
4. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
5. Selecione **Continue**.
6. Na etapa **Anexar certificados**, selecione **Gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): assunto X.509 ou nome diferenciado (DN) do proprietário do certificado.
   - **Dias de validade**: o número de dias 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), as extensões de uso de chave e de uso de chave estendido são adicionadas ao certificado gerado.

Essas extensões definem a finalidade da chave contida no certificado.

Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

8. Selecione **Gerar**.
9. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   - Selecione **Baixar certificado** para salvar o arquivo de certificado.

     Especifique o nome do arquivo do 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 **Baixar chave privada** para salvar a chave privada como um arquivo.

     Especifique o nome do arquivo da chave privada e o local de download.

10. Selecione **Criar** para salvar o certificado no Grid Manager.

    O novo certificado aparece na guia Cliente.

11. No Grid Manager, selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Global**.
12. Selecione **certificado da interface de gerenciamento**.
13. Selecione **Usar certificado personalizado**.
14. Faça o upload dos arquivos certificate.pem e private_key.pem da detalhes do certificado do cliente etapa. Não é necessário fazer o upload do CA bundle.
    a. Selecione **Carregar certificado** e depois selecione **Continuar**.
    b. Faça o upload de cada arquivo de certificado (`.pem`).
    c. Selecione **Salvar** para salvar o certificado no Grid Manager.

       O novo certificado aparece na página de certificados da interface de gerenciamento.

15. Configurar uma ferramenta de monitoramento externa, como Grafana.

Configurar uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações na sua ferramenta de monitoramento externa, como o Grafana.
   a. **Nome**: Insira um nome para a conexão.

StorageGRID não exige essas informações, mas você precisa fornecer um nome para testar a conexão.

b. **URL**: Insira o nome de domínio ou endereço IP do Admin Node. Especifique HTTPS e a porta 9091.

   Por exemplo: `https://admin-node.example.com:9091`

c. Ative **Autenticação de Cliente TLS** e **Com Certificado CA**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole:
   - O certificado CA da interface de gerenciamento para **CA Cert**
   - O certificado do cliente para **Client Cert**
   - A chave privada para a **Client Key**

e. **ServerName**: insira o nome de domínio do nó de administração.

   ServerName deve corresponder ao nome de domínio conforme aparece no certificado da interface de gerenciamento.

2. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

   Agora você pode acessar as métricas do Prometheus do StorageGRID com sua ferramenta de monitoramento externa.

   Para obter informações sobre as métricas, consulte o "Instruções para monitoramento do StorageGRID".

Editar certificados de cliente

Você pode editar um certificado de cliente administrador para alterar seu nome, habilitar ou desabilitar o acesso do Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.

   As datas de expiração dos certificados e as permissões de acesso do Prometheus são listadas na tabela. Se um certificado estiver prestes a expirar ou já estiver expirado, uma mensagem aparece na tabela e um alerta é acionado.

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione **Editar nome e permissão**
4. Insira um nome de certificado.
5. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
6. Selecione **Continuar** para salvar o certificado no Grid Manager.

   O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode enviar um novo certificado quando o atual expirar.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.

   As datas de expiração dos certificados e as permissões de acesso do Prometheus são listadas na tabela. Se um certificado estiver prestes a expirar ou já estiver expirado, uma mensagem aparece na tabela e um alerta é acionado.

2. Selecione o certificado que você deseja 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 depois selecione **Continuar**.

b. Faça upload do nome do certificado do cliente (`.pem`).

   Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.

   - Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

   Por exemplo: `storagegrid_certificate.pem`

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

c. Selecione **Criar** para salvar o certificado no Grid Manager.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

   - **Assunto** (opcional): assunto X.509 ou nome diferenciado (DN) do proprietário do certificado.
   - **Dias de validade**: o número de dias 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), as extensões de uso de chave e de uso de chave estendido são adicionadas ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.

   Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

   - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro

lugar.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

  Especifique o nome do arquivo do 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 **Baixar chave privada** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo da chave privada e o local de download.

e. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na guia Cliente.

Baixe ou copie os certificados do cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro local.

Passos

1. Selecione **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione o certificado que você deseja copiar ou baixar.
3. Faça o download ou copie o certificado.

Baixar arquivo de certificado

Baixe o arquivo de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo do 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 **Configuração** > **Segurança** > **Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione o certificado que você deseja remover.
3. Selecione **Excluir** e confirme.

> Para remover até 10 certificados, selecione cada certificado que deseja remover na guia Cliente e selecione **Ações** > **Excluir**.

Após a remoção de um certificado, os clientes que o utilizavam devem especificar um novo certificado de cliente para acessar o banco de dados StorageGRID Prometheus.

Configurar as configurações de segurança

Gerencie a política de TLS e SSH no StorageGRID

A política de TLS e SSH determina quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços internos do StorageGRID.

A política de segurança controla como o TLS e o SSH criptografam os dados em trânsito. Em geral, use a política de compatibilidade Modern (padrão), a menos que seu sistema precise estar em conformidade com Common Criteria ou que você precise usar outros cifradores.

> Alguns serviços do StorageGRID ainda não foram atualizados para usar as cifras presentes nessas políticas.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Selecione uma política de segurança

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de segurança**.

   A aba **Políticas de TLS e SSH** mostra as políticas disponíveis. A política atualmente ativa é indicada por uma marca de seleção verde no bloco da política.

2. Consulte as abas para saber mais sobre as políticas disponíveis.

Compatibilidade moderna (padrão)

Use a política padrão se precisar de criptografia forte e não tiver requisitos especiais. Essa política é compatível com a maioria dos clientes TLS e SSH.

Compatibilidade com versões anteriores

Use a política de compatibilidade Legado se você 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

Utilize a política de Common Criteria se você precisar de certificação Common Criteria.

FIPS estrito

Use a política FIPS estrita se você precisar de certificação Common Criteria e precisar usar o NetApp Cryptographic Security Module (NCSM) 3.0.8 ou o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para conexões de clientes externos com os endpoints do balanceador de carga, Tenant Manager e Grid Manager. O uso dessa política pode reduzir o desempenho.

O NCSM 3.0.8 e o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 são usados nas seguintes operações:

- NCSM
  - Conexões TLS entre os seguintes serviços: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw e cache-svc
  - Conexões TLS entre clientes e o serviço nginx-gw (endpoints do balanceador de carga)
  - Conexões TLS entre clientes e o serviço LDR
  - Criptografia de conteúdo de objeto para SSE-S3, SSE-C e a configuração de criptografia de objeto armazenado
  - Conexões SSH

  Para obter mais informações, consulte o Programa de Validação de Algoritmos Criptográficos do NIST "Certificado nº 4838".

- NetApp StorageGRID módulo da API de criptografia do kernel

  O módulo StorageGRID Kernel Crypto API da NetApp está presente apenas nas plataformas de VM e appliance StorageGRID.

  - Coleta de entropia
  - Criptografia de nó

  Para obter mais informações, consulte o Programa de Validação de Algoritmos Criptográficos do NIST "Certificados nº A6242 a nº A6257" e "Certificado de Entropia nº E223".

Nota: Após selecionar esta política, "execute uma reinicialização gradual" para todos os nós para ativar o NCSM. Use **Manutenção** > **reinicialização em andamento** para iniciar e monitorar as reinicializações.

Personalizado

Crie uma política personalizada se você precisar aplicar seus próprios cifradores.

Opcionalmente, se o seu StorageGRID tiver requisitos de criptografia FIPS 140, habilite o recurso de modo FIPS para usar o NCSM 3.0.8 e o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

a. Defina o `fipsMode`parâmetro para `true`.

b. Quando solicitado, "execute uma reinicialização gradual" ative os módulos de criptografia em todos os nós. Use **Manutenção** > **reinicialização contínua** para iniciar e monitorar as reinicializações.

c. Selecione **Suporte** > **Diagnóstico** para visualizar as versões ativas do módulo FIPS.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Ver detalhes**.
4. Para alterar a política atual, selecione **Usar política**.

   Uma marca de seleção verde aparece ao lado de **Current policy** no bloco de políticas.

Criar uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar seus próprios cifradores.

Passos

1. Na aba da política mais semelhante à política personalizada que você deseja criar, selecione **Ver 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 **Usar política**.

   Uma marca de seleção verde aparece ao lado de **Política atual** no bloco Política personalizada.

6. Opcionalmente, selecione **Editar configuração** para fazer mais alterações na nova política personalizada.

Reverter temporariamente para a política de segurança padrão

Se você configurou uma política de segurança personalizada, poderá não conseguir fazer login no Grid Manager se a política TLS configurada for incompatível com a "certificado de servidor configurado".

Você pode reverter temporariamente para a política de segurança padrão.

Passos

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

   Quando você está logado como root, o prompt muda de `$` para `#`.
2. Execute o seguinte comando:

   ```
   restore-default-cipher-configurations
   ```
3. A partir de um navegador web, acesse o Grid Manager no mesmo Admin Node.
4. Siga os passos em Selecione uma política de segurança para configurar a política novamente.

Configurar a segurança de rede e de objetos do StorageGRID

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, impedir determinadas solicitações S3 ou permitir que as conexões de clientes com os Storage Nodes usem HTTP em vez de HTTPS.

Criptografia de objeto armazenado

A criptografia de objetos armazenados permite a criptografia de todos os dados dos objetos à medida que são ingeridos pelo S3. Por padrão, os objetos armazenados não são criptografados, mas você pode optar por criptografar objetos usando o algoritmo de criptografia AES-128 ou AES-256. Quando você habilita essa configuração, todos os objetos recém-ingeridos são criptografados, mas nenhuma alteração é feita nos objetos armazenados existentes. Se você desabilitar a criptografia, os objetos atualmente criptografados permanecerão criptografados, mas os objetos recém-ingeridos não serão criptografados.

A configuração de criptografia de objetos armazenados aplica-se somente a objetos S3 que não foram criptografados por criptografia no nível do bucket ou no nível do objeto.

Para obter mais detalhes sobre os métodos de criptografia do StorageGRID, consulte "Revise os métodos de criptografia do StorageGRID".

Impedir modificação do cliente

Impedir modificação do cliente é uma configuração de todo o sistema. Quando a opção **Impedir modificação do cliente** está selecionada, as seguintes solicitações são negadas.

S3 API REST

- DeleteBucket solicitações
- Qualquer solicitação para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objetos S3

Habilitar HTTP para conexões de nós de armazenamento

Por padrão, os aplicativos cliente usam o protocolo de rede HTTPS para quaisquer conexões diretas com os Storage Nodes. Você pode habilitar o HTTP opcionalmente para essas conexões, por exemplo, ao testar uma grid que não seja de produção.

Use HTTP para conexões com nós de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente com os nós de armazenamento. Você não precisa usar essa opção para clientes que usam apenas conexões HTTPS ou para clientes que se conectam ao serviço de Load Balancer (porque você pode "configurar cada endpoint do balanceador de carga" usar HTTP ou HTTPS).

Consulte "Resumo: endereços IP e portas para conexões de clientes" para saber quais portas os clientes S3 usam ao se conectar aos nós de armazenamento usando HTTP ou HTTPS.

Selecione opções

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem permissão de acesso root.

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de segurança**.
2. Selecione a guia **Rede e objetos**.
3. Para a criptografia de objetos armazenados, use a configuração **Nenhuma** (padrão) se você não quiser que os objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar os objetos armazenados.
4. Opcionalmente, selecione **Impedir modificação pelo cliente** se você quiser impedir que os clientes S3 façam solicitações específicas.

   Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e escalabilidade.

5. Opcionalmente, selecione **Habilitar HTTP para conexões de nós de armazenamento** se os clientes se conectarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

   Tenha cuidado ao habilitar HTTP para uma grade de produção, pois as solicitações serão enviadas sem criptografia.

6. Selecione **Salvar**.

Alterar as configurações de segurança da interface StorageGRID

As configurações de segurança da interface permitem que você controle se os usuários serão desconectados caso fiquem inativos por mais tempo do que o período

especificado e se um rastreamento de pilha será incluído nas respostas de erro da API.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "Permissão de acesso root".

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações **Tempo limite de inatividade do navegador** e **Rastreamento de pilha da Management API**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode ficar inativo antes que o usuário seja desconectado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelos seguintes:

- Um timer StorageGRID separado e não configurável, incluído para a segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o usuário fazer login. Quando a autenticação de um usuário expira, esse usuário é desconectado automaticamente, mesmo que o tempo limite de inatividade do navegador esteja desativado ou que o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve fazer login novamente.
- Configurações de tempo limite para o provedor de identidade, assumindo que o logon único (SSO) esteja habilitado para StorageGRID.

  Se o SSO estiver ativado e o navegador de um usuário expirar, o usuário deverá inserir novamente suas credenciais de SSO para acessar o StorageGRID. Consulte "Como funciona o SSO".

Rastreamento de pilha da Management API

Controla se um rastreamento de pilha é retornado nas respostas de erro da API do Grid Manager e do Tenant Manager.

Essa opção está desativada por padrão, mas você pode querer habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve manter o rastreamento de pilha desativado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de segurança**.
2. Selecione a guia **Interface**.
3. Para alterar a configuração de tempo limite de inatividade do navegador:
   a. Expanda o acordeão.
   b. Para alterar o período de tempo limite, especifique um valor entre 60 segundos e 7 dias. O tempo limite padrão é de 15 minutos.
   c. Para desativar essa função, desmarque a caixa de seleção.
   d. Selecione **Salvar**.

      A nova configuração não afeta os usuários que já estão conectados. Os usuários precisam fazer login novamente ou atualizar o navegador para que a nova configuração de timeout entre em vigor.
4. Para alterar a configuração do rastreamento de pilha da Management API:

a. Expanda o acordeão.

b. Selecione a caixa de seleção para retornar um rastreamento de pilha nas respostas de erro da API do Grid Manager e do Tenant Manager.

> Deixe o rastreamento de pilha desativado em ambientes de produção para evitar a divulgação de detalhes internos do software quando ocorrerem erros na API.

c. Selecione **Salvar**.

Gerenciar o acesso SSH externo no StorageGRID

Gerencie o acesso SSH para tráfego de entrada na grid bloqueando ou permitindo acesso externo. O gerenciamento do acesso SSH externo não afeta o tráfego entre os nós na grid.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "Permissão de acesso root".

Sobre esta tarefa

Para aumentar a segurança do sistema, o acesso SSH externo é bloqueado por padrão. Se você precisar realizar tarefas que exigem acesso SSH de entrada, como solucionar problemas, permita temporariamente o acesso externo. Quando você terminar a tarefa, bloqueie o acesso externo.

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de segurança**.
2. Selecione a guia **Bloquear SSH**.
3. Use a opção **Bloquear acesso SSH de entrada** para gerenciar acesso SSH externo:
   a. Selecione a caixa de seleção para bloquear o acesso (padrão).
   b. Desmarque a caixa de seleção para permitir o acesso.

> É necessário acesso à porta 22 entre o laptop de serviço e todos os outros nós da grade. Remova o acesso à porta 22 ao concluir a tarefa de manutenção.

4. Selecione **Salvar**.

Configurar os servidores de gerenciamento de chaves

Saiba mais sobre os principais servidores de gerenciamento no StorageGRID

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiro que fornece chaves de criptografia para os nós de appliance StorageGRID no site StorageGRID associado, usando o Key Management Interoperability Protocol (KMIP).

StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista dos produtos e versões suportados, use o "NetApp Ferramenta de Matriz de Interoperabilidade (IMT)".

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia

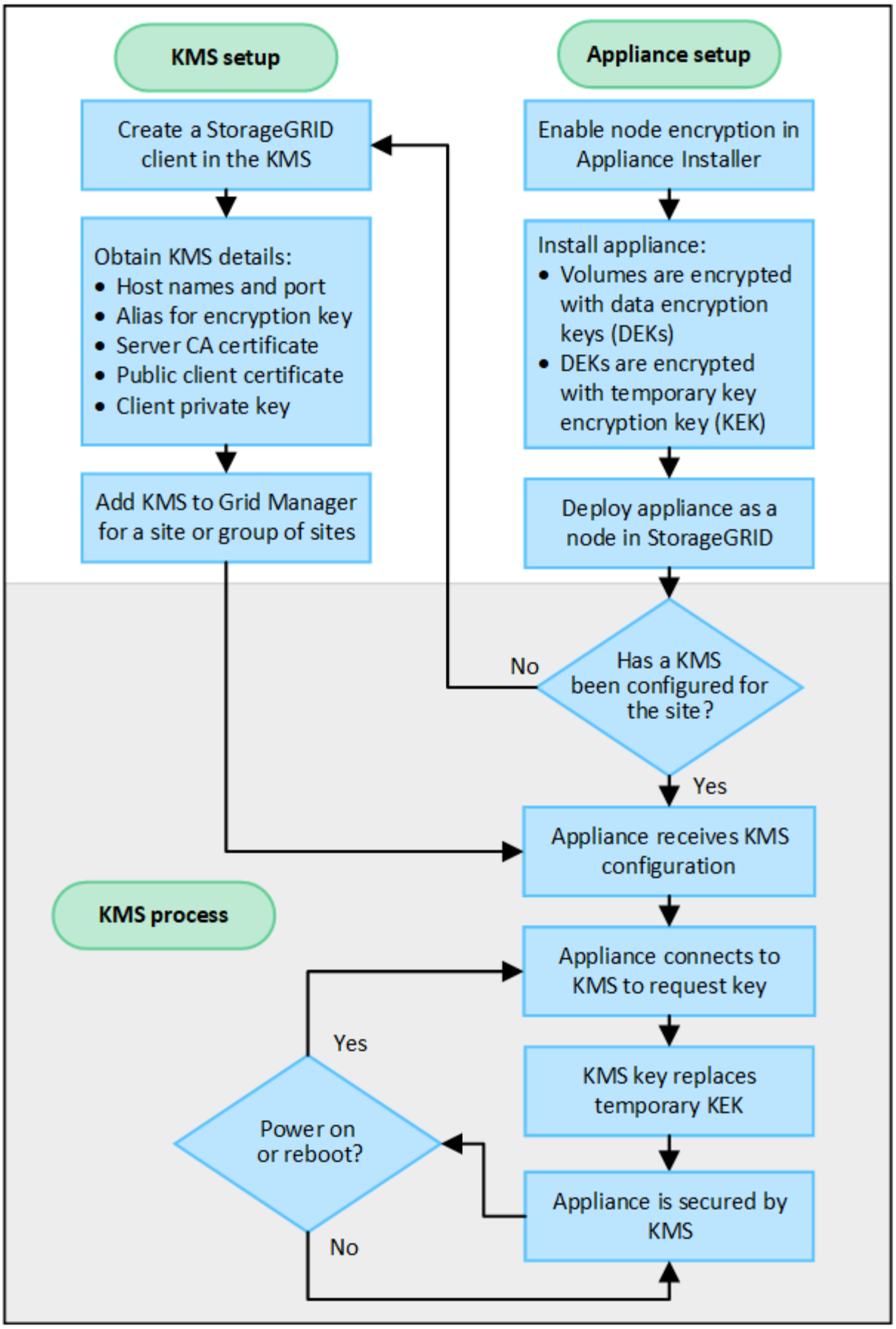
de nós para quaisquer nós de dispositivo StorageGRID que tenham a configuração **Criptografia de Nó** habilitada durante a instalação. Usar servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo se um dispositivo for removido do data center. Depois que os volumes do dispositivo forem criptografados, você não poderá acessar nenhum dado no dispositivo, a menos que o nó consiga se comunicar com o KMS.

> StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do appliance. Se você planeja usar um servidor de gerenciamento de chaves externo para proteger os dados do StorageGRID, você precisa entender como configurar esse servidor e como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo destas instruções. Se você precisar de ajuda, consulte a documentação do seu servidor de gerenciamento de chaves ou entre em contato com o suporte técnico.

Configuração do servidor de gerenciamento de chaves e do dispositivo StorageGRID

Antes de você poder usar um servidor de gerenciamento de chaves (KMS) para proteger os dados do StorageGRID nos nós do appliance, é necessário concluir duas tarefas de configuração: configurar um ou mais servidores KMS e habilitar a criptografia de nó para os nós do appliance. Quando essas duas tarefas de configuração estiverem concluídas, o processo de gerenciamento de chaves ocorrerá automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger os dados do StorageGRID nos nós do appliance.



O fluxograma mostra a configuração do KMS e a configuração do dispositivo ocorrendo em paralelo; no

entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia para novos nós do dispositivo, com base em suas necessidades.

Configurar o servidor de gerenciamento de chaves (KMS)

Configurar um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

Etapa	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada KMS ou cluster KMS.	"Configurar o StorageGRID como cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configurar o StorageGRID como cliente no KMS"
Adicione o KMS ao Grid Manager, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o appliance

Configurar um nó de appliance para uso com o KMS inclui as seguintes etapas de alto nível.

1. Durante a fase de configuração de hardware da instalação do appliance, use o StorageGRID Appliance Installer para ativar a configuração **Criptografia de Nó** para o appliance.

   > Não é possível ativar a configuração **Criptografia de Nó** depois que um appliance é adicionado à grid, e não é possível usar o gerenciamento de chaves externas para appliances que não têm criptografia de nó ativada.

2. Execute o StorageGRID Appliance Installer. Durante a instalação, uma chave de criptografia de dados (DEK) aleatória é atribuída a cada volume do dispositivo, da seguinte forma:
   - As DEKs são usadas para criptografar os dados em cada volume. Essas chaves são geradas usando Linux Unified Key Setup (LUKS) criptografia de disco no sistema operacional do appliance e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). A KEK inicial é uma chave temporária que criptografa os DEKs até que o appliance possa se conectar ao KMS.
3. Adicione o nó do appliance ao StorageGRID.

Veja "Habilitar criptografia do nó" para obter detalhes.

Processo de criptografia com gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível, que são executadas automaticamente.

1. Ao instalar um dispositivo com criptografia de nó habilitada na grade, StorageGRID determina se existe uma configuração KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o appliance recebe a configuração do KMS.

- Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão criptografados pela KEK temporária até que você configurar um KMS para o site e o appliance receba a configuração do KMS.

2. O dispositivo utiliza a configuração KMS para se conectar ao KMS e solicitar uma chave de criptografia.
3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui a KEK temporária e agora é usada para criptografar e descriptografar as DEKs dos volumes do dispositivo.

> Quaisquer dados existentes antes da conexão do nó do appliance criptografado ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do appliance não devem ser considerados protegidos contra remoção do data center até que a chave temporária seja substituída pela chave de criptografia do KMS.

4. Se o dispositivo for ligado ou reiniciado, ele se reconecta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não sobrevive a uma perda de energia ou a uma reinicialização.

Requisitos e considerações do servidor de gerenciamento de chaves do StorageGRID

Antes de configurar um servidor de gerenciamento de chaves (KMS) externo, você deve entender as considerações e os requisitos.

Qual versão do KMIP é suportada?

StorageGRID é compatível com a versão 1.4 do KMIP.

"Especificação do Protocolo de Interoperabilidade de Gerenciamento de Chaves Versão 1.4"

Quais são as considerações de rede?

As configurações do firewall de rede devem permitir que cada nó do appliance se comunique pela porta usada para comunicações do Key Management Interoperability Protocol (KMIP). A porta KMIP padrão é 5696.

Você deve garantir que cada nó do dispositivo que usa criptografia de nó tenha acesso à rede ao KMS ou cluster KMS que você configurou para o site.

Quais versões do TLS são suportadas?

A comunicação entre os nós do dispositivo e o KMS configurado utiliza conexões TLS seguras. StorageGRID pode suportar o protocolo TLS 1.2 ou TLS 1.3 ao estabelecer conexões KMIP com um KMS ou cluster KMS, dependendo do que o KMS suporta e de qual "Política de TLS e SSH" você está utilizando.

StorageGRID negocia o protocolo e a cifra (TLS 1.2) ou o conjunto de cifras (TLS 1.3) com o KMS ao estabelecer a conexão. Para verificar quais versões de protocolo e cifras/conjuntos de cifras estão disponíveis, consulte a seção `tlsOutbound` da política ativa de TLS e SSH do grid (**Configuração** > **Segurança** > **Configurações de segurança**).

Quais appliances são compatíveis?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar as chaves de criptografia de qualquer appliance StorageGRID em sua grid que tenha a configuração **Criptografia de Nó** ativada. Essa configuração só pode ser ativada durante a etapa de configuração de hardware da instalação do appliance usando o StorageGRID Appliance Installer.

Você não pode ativar a criptografia de nó depois que um appliance é adicionado ao grid, e não pode usar o gerenciamento externo de chaves para appliances que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para StorageGRID appliances e nós de appliances.

Não é possível usar o KMS configurado para nós baseados em software (não appliance), incluindo os seguintes:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em mecanismos de contêiner em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no nível do datastore ou do disco.

Quando devo configurar os servidores de gerenciamento de chaves?

Para uma nova instalação, geralmente é recomendável configurar um ou mais servidores de gerenciamento de chaves no Grid Manager antes de criar tenants. Essa ordem garante que os nós estejam protegidos antes que quaisquer dados de objetos sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Grid Manager antes ou depois de instalar os nós do appliance.

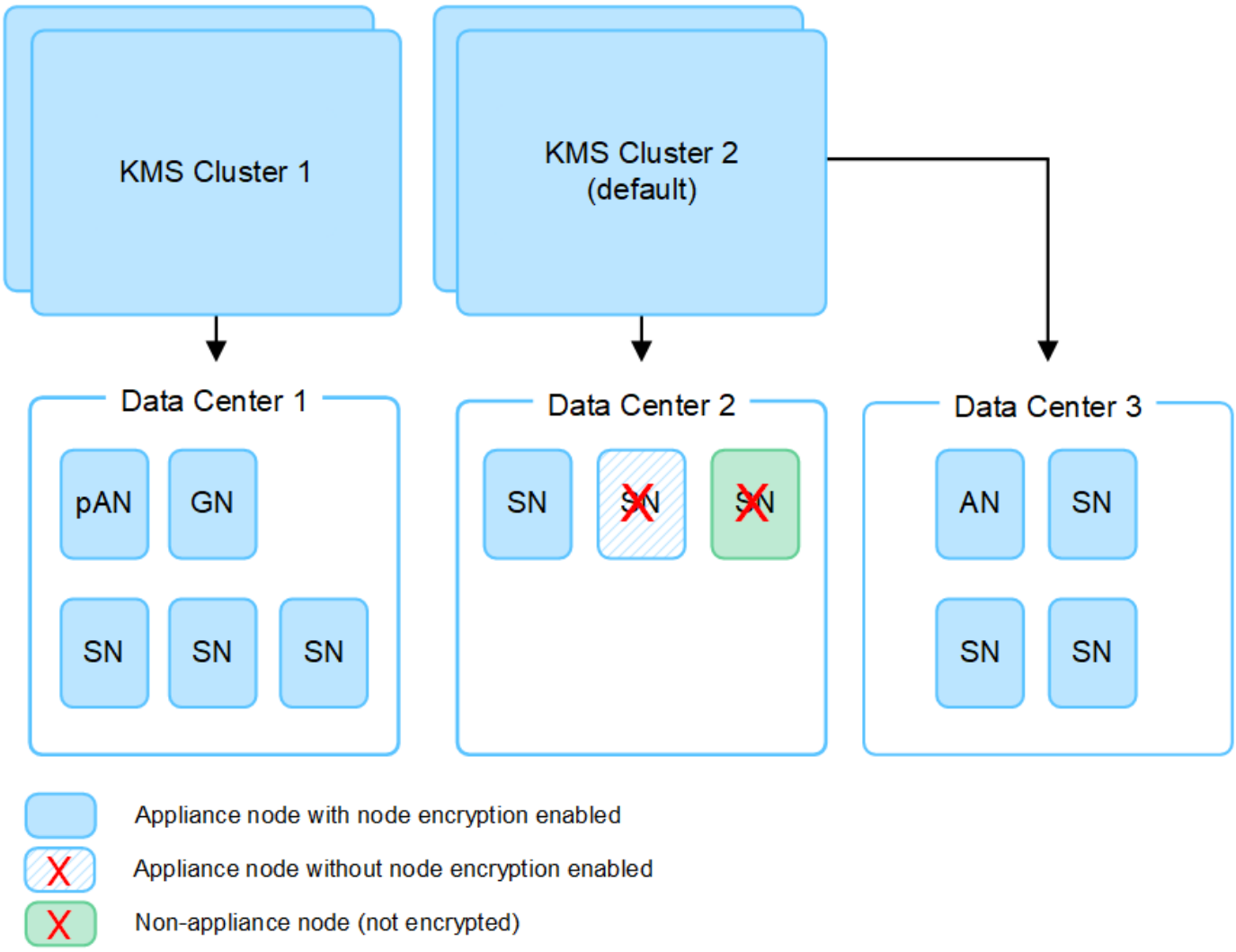
De quantos servidores de gerenciamento de chaves você precisa?

Você pode configurar um ou mais servidores externos de gerenciamento de chaves para fornecer chaves de criptografia aos nós do appliance em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do appliance StorageGRID em um único site ou em um grupo de sites.

StorageGRID suporta 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 a capacidade de failover em uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três sites de data center. Você pode configurar um cluster KMS para fornecer uma chave a todos os nós de appliance no Data Center 1 e um segundo cluster KMS para fornecer uma chave a todos os nós de appliance em todos os outros sites. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que você não pode usar um KMS para nós que não sejam appliance ou para quaisquer nós appliance que não tenham a configuração **Criptografia de Nó** ativada durante a instalação.



O que acontece quando uma chave é rotacionada?

Como prática recomendada de segurança, você deve periodicamente "girar a chave de criptografia" usado por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ela é distribuída automaticamente para os nós de appliance criptografados no(s) site(s) associado(s) ao KMS. A distribuição deve ocorrer dentro de uma hora após a rotação da chave.
- Se o nó do appliance criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reiniciado.
- Se a nova versão da chave não puder ser usada para criptografar volumes do appliance por qualquer motivo, o alerta **KMS encryption key rotation failed** será 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 após ele ter sido criptografado?

Se você precisar instalar um appliance criptografado em outro sistema StorageGRID, primeiro deve descomissionar o nó de grid para mover os dados de objeto para outro nó. Em seguida, você pode usar o StorageGRID Appliance Installer para "Limpar a configuração do KMS". Limpar a configuração do KMS desativa a configuração **Node Encryption** e remove a associação entre o nó do appliance e a configuração

do KMS para o site StorageGRID.

Sem acesso à chave de criptografia KMS, quaisquer dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

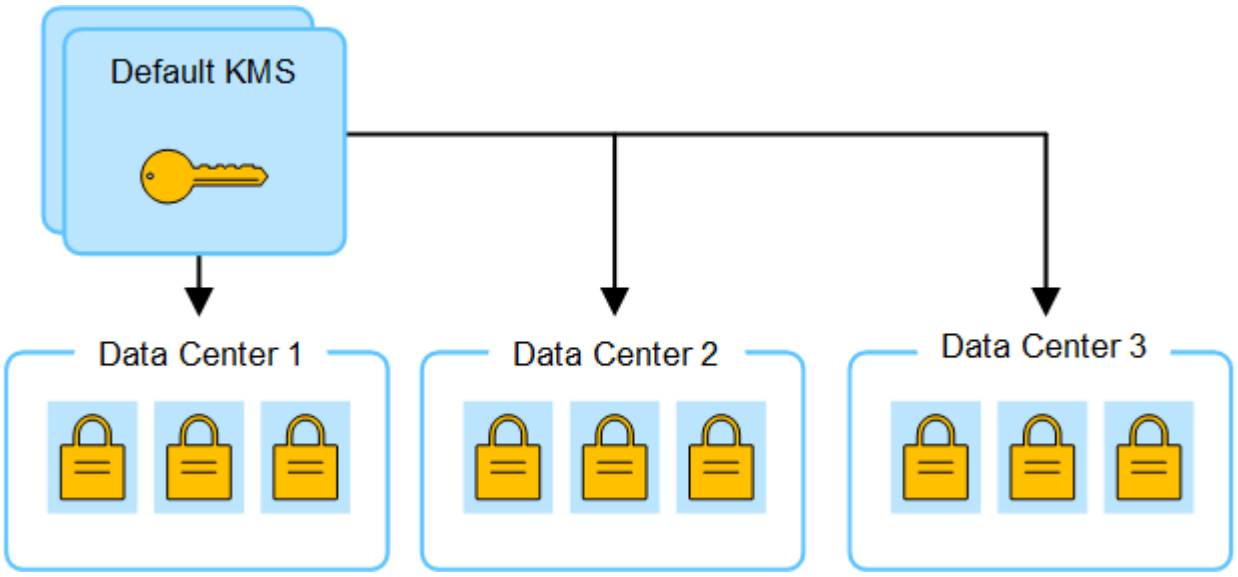
Considerações para a alteração do KMS em um site StorageGRID

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do appliance em um único site ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

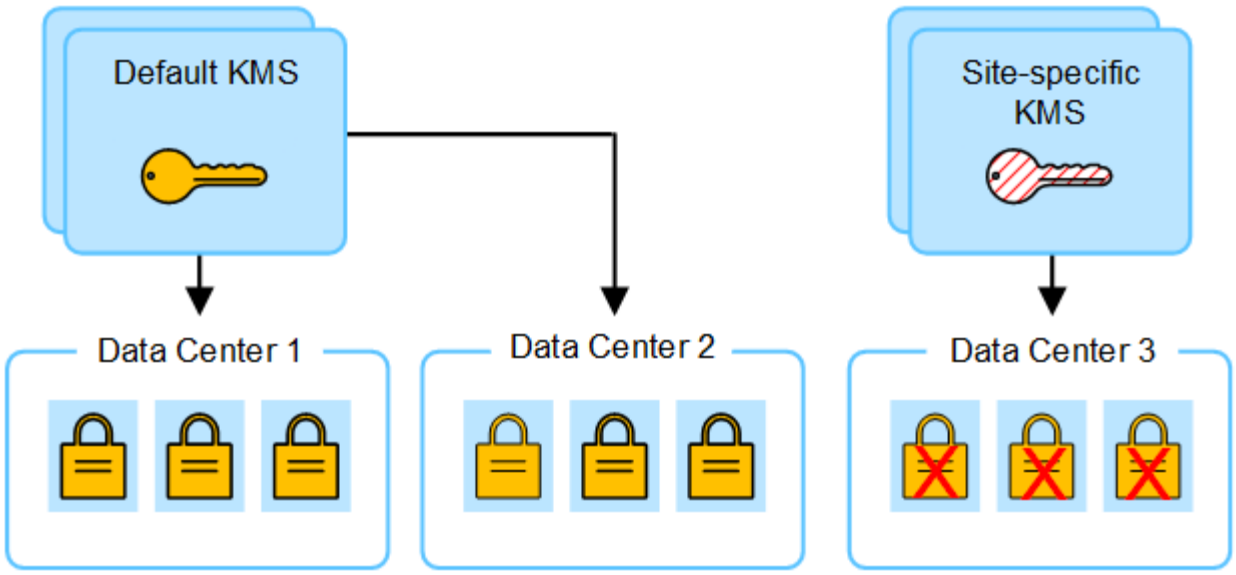
Se você alterar o KMS usado em um site, deverá garantir que os nós de appliance criptografados anteriormente nesse site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de appliance criptografados no site.

Por exemplo:

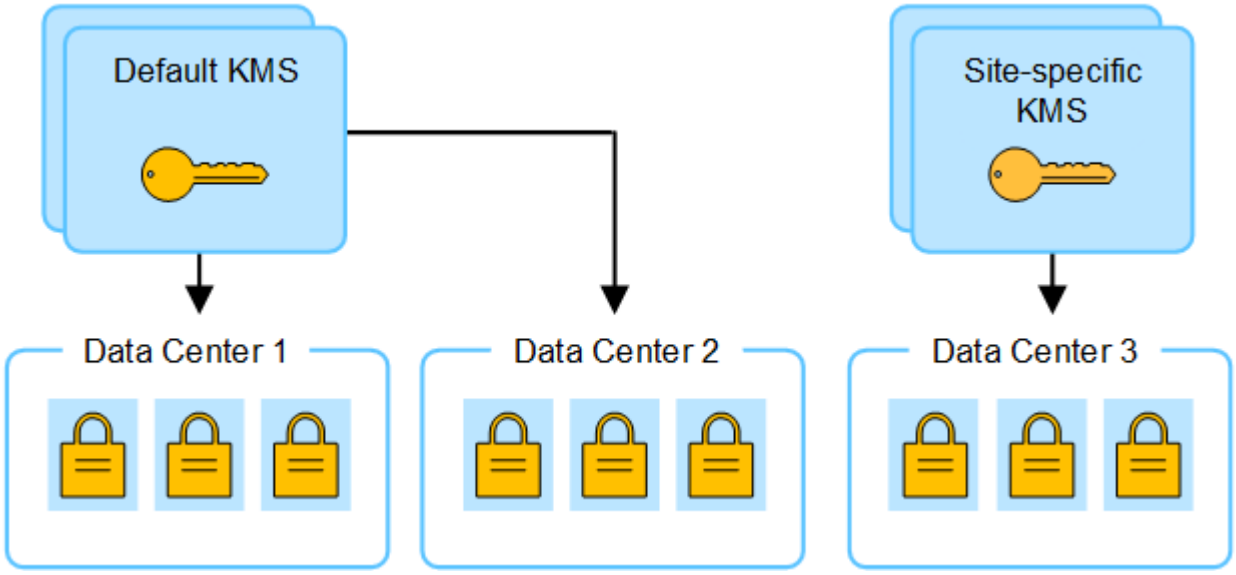
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não possuem um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de appliance que têm a configuração **Criptografia de Nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós de appliance em todos os sites. Essa mesma chave também deve ser usada para descriptografar esses appliances.



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, ocorre um erro de validação ao tentar salvar a configuração do KMS específico para o site. O erro ocorre porque o KMS específico para o site não possui a chave correta para descriptografar os nós nesse site.



4. Para resolver o problema, você copia a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original se torna uma versão anterior da nova chave.) O KMS específico do site agora possui a chave correta para descriptografar os nós do appliance no data center 3, então ela pode ser salva no StorageGRID.



Casos de uso para alterar qual KMS é usado para um site

A tabela resume as etapas necessárias para os casos mais comuns de alteração do KMS de um site.

Caso de uso para alterar o KMS de um site	Etapas necessárias
Você possui 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 será aplicado a qualquer site que não tenha um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"
Você possui um KMS padrão e adiciona um novo site em uma expansão. Você não deseja usar o KMS padrão para o novo site.	1. Se os nós do 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 Grid Manager, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você deseja que o KMS de um site utilize 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. Utilizando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome do host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o StorageGRID como cliente no KMS

Você deve configurar StorageGRID como cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de adicionar o KMS ao StorageGRID.

Estas instruções aplicam-se ao Thales CipherTrust Manager e ao Hashicorp Vault. Para obter uma lista de produtos e versões compatíveis, utilize o "NetApp Ferramenta de Matriz de Interoperabilidade (IMT)".

Passos

1. A partir do software KMS, crie um cliente StorageGRID para cada KMS ou cluster KMS que você planeja usar.

   Cada KMS gerencia uma única chave de criptografia para os nós dos appliances StorageGRID em um único site ou em um grupo de sites.

2. Crie uma chave usando um dos dois métodos a seguir:
   - Utilize a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada KMS ou cluster KMS.

     A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

   - Peça para o StorageGRID criar a chave. Você será solicitado quando testar e salvar após "Carregando certificados de cliente".
3. Registre as seguintes informações para cada KMS ou cluster KMS.

Você precisa dessas informações ao adicionar o KMS ao StorageGRID:

- Nome do host ou endereço IP para cada servidor.
- Porta KMIP usada pelo KMS.
- Alias da chave de criptografia no KMS.

4. Para cada KMS ou cluster KMS, obtenha um certificado de servidor assinado por uma autoridade certificadora (CA) ou um pacote de certificados que contenha cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da cadeia de certificados.

   O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

   - O certificado deve usar o formato X.509 codificado em Base-64 Privacy Enhanced Mail (PEM).
   - O campo Nome Alternativo do Assunto (SAN) em cada certificado de servidor deve incluir o domínio totalmente qualificado (FQDN) ou endereço IP ao qual o StorageGRID se conectará.

     > Ao configurar o KMS no StorageGRID, você deve inserir os mesmos domínios totalmente qualificados ou endereços IP no campo **Hostname**.

   - O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.

5. Obtenha o certificado público do cliente emitido para o StorageGRID pelo KMS externo e a chave privada do certificado do cliente.

   O certificado do cliente permite que o StorageGRID se autentique no KMS.

Adicionar um servidor de gerenciamento de chaves no StorageGRID

Você usa o assistente do StorageGRID Key Management Server para adicionar cada KMS ou cluster KMS.

Antes de começar

- Você revisou o "Considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você tem "configurou StorageGRID como cliente no KMS" e as informações necessárias para cada KMS ou cluster KMS.
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Sobre esta tarefa

Se possível, configure quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os appliances criptografados no nível do nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site depois, será necessário primeiro copiar a versão atual da chave de criptografia do KMS padrão para o novo KMS. Consulte "Considerações para alterar o KMS de um site" para obter detalhes.

Etapa 1: detalhes do KMS

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um Servidor de Gerenciamento de Chaves, você fornece detalhes sobre o KMS ou cluster KMS.

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **Create**.

   A etapa 1 (detalhes do KMS) do assistente Adicionar um Key Management Server é exibida.

3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. **Observação**: Se você ainda não criou uma chave usando seu produto KMS, será solicitado que StorageGRID crie a chave.
Gerencia chaves para	O site do StorageGRID que será associado a este KMS. Se possível, você deve configurar quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS for gerenciar as chaves de criptografia para os nós do dispositivo em um site específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que será aplicado a qualquer site que não tenha um KMS dedicado e a qualquer site que você adicionar em expansões subsequentes. **Nota:** Ocorrerá um erro de validação ao salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas não forneceu a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. **Nota:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o domínio totalmente qualificado ou endereço IP inserido aqui. Caso contrário, StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **Continue**.

Etapa 2: Carregar o 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 da **Etapa 2 (Carregar certificado do servidor)**, navegue até o local onde o certificado do servidor ou a cadeia de certificados foi salva.
2. Faça o upload do arquivo de certificado.

   Os metadados do certificado do servidor são exibidos.

   > Se você carregou um pacote de certificados, os metadados de cada certificado aparecem em sua própria guia.

3. Selecione **Continue**.

Etapa 3: Carregar certificados do 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 da **Etapa 3 (Carregar certificados do cliente)**, navegue até o local do certificado do cliente.
2. Faça upload do arquivo de certificado do cliente.

   Os metadados do certificado do cliente aparecem.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Faça o upload do arquivo de chave privada.
5. Selecione **Test and save**.

   Se uma chave não existir, você será solicitado a permitir que o StorageGRID crie uma.

   As conexões entre o servidor de gerenciamento de chaves e os nós do appliance são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves é adicionado à tabela na página Key Management Server.

   > Imediatamente após você adicionar um KMS, o status do certificado na página Key Management Server aparece como Desconhecido. O StorageGRID pode levar até 30 minutos para obter o status real de cada certificado. Você deve atualizar seu navegador para ver o status atual.

6. Se uma mensagem de erro aparecer ao selecionar **Test and save**, revise os detalhes da mensagem e selecione **OK**.

Por exemplo, você pode receber um erro 422: entidade não processável se um teste de conexão falhar.

7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **Forçar salvamento**.

> Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada appliance com esse KMS. Se houver algum problema com a configuração, você pode não conseguir reinicializar os nós de appliance que têm criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Analise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

   A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Gerencie um servidor de gerenciamento de chaves no StorageGRID

Gerenciar um servidor de gerenciamento de chaves (KMS) envolve visualizar ou editar detalhes, gerenciar certificados, visualizar nós criptografados e remover um KMS quando ele não for mais necessário.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "permissão de acesso necessária".

Ver detalhes do KMS

Você pode visualizar informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo detalhes da chave e o status atual dos certificados do servidor e do cliente.

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

   - A aba Detalhes da configuração lista todos os servidores de gerenciamento de chaves que estão configurados.
   - A aba "Nós criptografados" lista todos os nós que têm criptografia de nó ativada.

2. Para visualizar os detalhes de um KMS específico e realizar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gerencia chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou **Sites não gerenciados por outro KMS (KMS padrão).**

Campo	Descrição
Nome do host	O domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o domínio totalmente qualificado ou endereço IP de ambos os servidores será listado. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o domínio totalmente qualificado ou endereço IP do primeiro KMS será listado 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 visualizar todos os nomes de host em um cluster, selecione um KMS e selecione **Editar** ou **Ações** > **Editar**.

3. Selecione uma aba na página de detalhes do KMS para visualizar as seguintes informações:

Aba	Campo	Descrição
Detalhes principais	Nome da chave	O alias principal para o cliente StorageGRID no KMS.
UID da chave	O identificador único da versão mais recente da chave.	Última modificação
A data e a hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de expiração e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (privacy enhanced mail) do certificado.
Certificado do cliente	Metadados	Os metadados do certificado, como número de série, data e hora de expiração e o PEM do certificado.

4. Sempre que as práticas de segurança da sua organização exigirem, selecione **Girar chave** ou use o software KMS para criar uma nova versão da chave.

   Quando a rotação de chaves é bem-sucedida, os campos UID da chave e Última modificação são atualizados.

Se você rotacionar a chave de criptografia usando o software KMS, rotacione-a da última versão usada da chave para uma nova versão da mesma chave. Não rotacione para uma chave completamente diferente.

Nunca tente rotacionar uma chave alterando o nome da chave (alias) no KMS. StorageGRID exige 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, StorageGRID pode não conseguir descriptografar seus dados.

Gerenciar certificados

Resolva prontamente quaisquer problemas com certificados de servidor ou cliente. Se possível, substitua os certificados antes que expirem.

Você deve resolver quaisquer problemas com certificados o mais rápido possível para manter o acesso aos dados.

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.
2. Na tabela, observe o valor de validade do certificado para cada KMS.
3. Se a data de expiração do certificado de qualquer KMS for desconhecida, aguarde até 30 minutos e atualize seu navegador.
4. Se a coluna Validade do certificado indicar que um certificado expirou ou está perto de expirar, selecione o KMS para acessar a página de detalhes do KMS.
   a. Selecione **Certificado do servidor** e verifique o valor do campo "Expira em".
   b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
   c. Repita esses subpassos e selecione **Certificado do cliente** em vez de Certificado do servidor.
5. Quando os alertas **Expiração do certificado da CA do KMS**, **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.

   Pode levar até 30 minutos para o StorageGRID obter atualizações sobre a expiração do certificado. Atualize seu navegador para ver os valores atuais.

Se você receber o status **Status do certificado do servidor desconhecido**, verifique se o seu KMS permite obter um certificado de servidor sem exigir um certificado de cliente.

Visualizar nós criptografados

Você pode visualizar informações sobre os nós de appliance em seu sistema StorageGRID que têm a configuração **Criptografia de Nó** ativada.

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do Servidor de Gerenciamento de Chaves é exibida. A guia Detalhes da Configuração mostra quaisquer servidores de gerenciamento de chaves que foram configurados.

2. Na parte superior da página, selecione a guia **Nós criptografados**.

   A aba "Nós criptografados" lista os nós do appliance no seu sistema StorageGRID que têm a configuração **Criptografia de nó** ativada.

3. Analise as informações na tabela para cada nó do appliance.

Coluna	Descrição
Nome do nó	O nome do nó do appliance.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Site	O nome do site StorageGRID onde o nó está instalado.
Nome da KMS	O nome descritivo do KMS usado para o nó. Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS. "Adicionar um servidor de gerenciamento de chaves (KMS)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do appliance. Para visualizar o UID completo de uma chave, selecione o texto. Um traço (--) indica que o UID da chave é desconhecido, possivelmente devido a um problema de conexão entre o nó do appliance e o KMS.
Status	O status da conexão entre o KMS e o nó do appliance. Se o nó estiver conectado, o registro de data e hora é atualizado a cada 30 minutos. Pode levar alguns minutos para o status da conexão ser atualizado após alterações na configuração do KMS. **Nota:** Atualize seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema com o KMS, resolva o problema imediatamente.

   Durante as operações normais do KMS, o status será **Conectado ao KMS**. Se um nó estiver desconectado do grid, o estado de conexão do nó será exibido (Administrativamente Inativo ou Desconhecido).

   Outras mensagens de status correspondem a alertas do StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração do KMS
   - Erro de conectividade KMS
   - Nome da chave de criptografia KMS não encontrado
   - Falha na rotação da chave de criptografia KMS
   - A chave KMS não conseguiu descriptografar um volume do appliance.
   - KMS não está configurado

Execute as ações recomendadas para esses alertas.

> Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

Editar um KMS

Pode ser necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

Antes de começar

- Se você planeja atualizar o site selecionado para um KMS, você revisou o "Considerações para a alteração do KMS de um site".
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que você deseja editar e selecione **Ações** > **Editar**.

   Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes na **Etapa 1 (detalhes do KMS)** do assistente Edit a Key Management Server.

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.

Campo	Descrição
Gerencia chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, selecione opcionalmente **Sites não gerenciados por outro KMS (KMS padrão)**. Essa seleção converte o KMS específico do site no KMS padrão, que será aplicado a todos os sites que não possuem um KMS dedicado e a quaisquer sites adicionados em uma expansão. **Observação:** Se você estiver editando um KMS específico de um site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. **Nota:** O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o domínio totalmente qualificado ou endereço IP inserido aqui. Caso contrário, StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **Continue**.

   A etapa 2 (Carregar certificado do servidor) do assistente Editar um Key Management Server é exibida.

6. Se você precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.
7. Selecione **Continue**.

   A etapa 3 (Carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se você precisar substituir o certificado do cliente e a chave privada do certificado do cliente, selecione **Procurar** e carregue os novos arquivos.
9. Selecione **Test and save**.

   As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados nos sites 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 é adicionado à tabela na página Key Management Server.

10. Se aparecer uma mensagem de erro, revise os detalhes da mensagem e selecione **OK**.

    Por exemplo, você pode receber um erro 422: Entidade não processável se o site que você selecionou para este KMS já for gerenciado por outro KMS ou se um teste de conexão falhar.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Forçar salvamento**.

Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada appliance com esse KMS. Se houver algum problema com a configuração, você pode não conseguir reinicializar os nós de appliance que têm 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 foi salva.

12. Analise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

    A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se o site tiver sido desativado.

Antes de começar

- Você revisou o "Considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Sobre esta tarefa

Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de appliance com criptografia de nó ativada.
- Você pode remover o KMS padrão se já existir um KMS específico para cada site que possua nós de appliance com criptografia ativada.

Passos

1. Selecione **Configuração** > **Segurança** > **Servidor de gerenciamento de chaves**.

   A página do servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que você 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 possui nenhum nó de appliance com criptografia de nó ativada.
   - Você está removendo o KMS padrão, mas já existe um KMS específico para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS foi removida.

Gerenciar configurações de proxy

Configurar um proxy de armazenamento StorageGRID

Se você estiver usando serviços de plataforma ou Cloud Storage Pools, poderá configurar um proxy não transparente entre os Storage Nodes e os endpoints externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens dos serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na internet.

> As configurações de proxy de armazenamento configuradas não se aplicam aos endpoints dos serviços da plataforma Kafka.

Antes de começar

- Você tem "permissões de acesso específicas".
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

Sobre esta tarefa

Você pode configurar as definições para um único servidor proxy de armazenamento.

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de proxy**.
2. Na guia **Armazenamento**, selecione a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
4. Digite o nome do host ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para conectar-se ao servidor proxy.

   Deixe este campo em branco para usar a porta padrão do protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Salvar**.

   Após salvar o proxy de armazenamento, novos endpoints para serviços de plataforma ou Cloud Storage Pools podem ser configurados e testados.

   > As alterações de proxy podem levar até 10 minutos para entrar em vigor.

7. Verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma StorageGRID não sejam bloqueadas.
8. Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configurar as definições de proxy de administrador no StorageGRID

Se você enviar pacotes AutoSupport usando HTTP ou HTTPS, pode configurar um servidor proxy não transparente entre os Nós de Administração e o suporte técnico (AutoSupport).

Para obter mais informações sobre AutoSupport, consulte "Configurar AutoSupport".

Antes de começar

- Você tem "permissões de acesso específicas".
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

Sobre esta tarefa

Você pode configurar as configurações para um único proxy de administrador.

Passos

1. Selecione **Configuração** > **Segurança** > **Configurações de proxy**.

   A página Configurações de Proxy é exibida. Por padrão, Storage está selecionado no menu de abas.

2. Selecione a aba **Admin**.
3. Selecione a caixa de seleção **Enable Admin Proxy**.
4. Digite o nome do host ou o endereço IP do servidor proxy.
5. Digite a porta usada para conectar ao servidor proxy.
6. Opcionalmente, insira um nome de usuário e uma senha para o servidor proxy.

   Deixe esses campos em branco se o seu servidor proxy não exigir um nome de usuário ou uma senha.

7. Selecione uma das seguintes opções:

   - Se você deseja proteger a conexão com o proxy administrativo, selecione **Verificar certificado de proxy**. Carregue um pacote de certificados de autoridade certificadora (CA) para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy administrativo.

     AutoSupport on Demand, E-Series AutoSupport através do StorageGRID e a determinação do caminho de atualização na página de upgrade do StorageGRID não funcionarão se um certificado de proxy for verificado.

   Após o upload do pacote CA, seus metadados aparecem.

   - Se você não quiser validar certificados ao se comunicar com o servidor proxy, selecione **Não verificar certificado de proxy**.

8. Selecione **Salvar**.

   Após salvar o proxy administrativo, o servidor proxy entre os nós administrativos e o suporte técnico é configurado.

   As alterações de proxy podem levar até 10 minutos para entrar em vigor.

9. Se você precisar desativar o proxy administrativo, desmarque a caixa de seleção **Ativar proxy administrativo** e selecione **Salvar**.

Controlar firewalls

Controlar o acesso ao StorageGRID em um firewall externo

Você pode abrir ou fechar portas específicas no firewall externo.

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode querer impedir que os tenants se conectem ao Grid Manager no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se você deseja configurar o firewall interno do StorageGRID, consulte "Configurar firewall interno".

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para Admin Nodes	Navegadores web e clientes de API de gerenciamento podem acessar o Grid Manager, a Grid Management API, o Tenant Manager e a Tenant Management API. **Nota:** A porta 443 também é usada para algum tráfego interno.
8443	Porta do Grid Manager restrita em nós de administração	• Navegadores web e clientes da API de gerenciamento podem acessar o Grid Manager e a Grid Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Tenant Manager nem a Tenant Management API. • Solicitações de conteúdo interno serão rejeitadas.
9443	Porta do Tenant Manager restrita em Admin Nodes	• Navegadores web e clientes da API de gerenciamento podem acessar o Tenant Manager e a Tenant Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Grid Manager nem a Grid Management API. • Solicitações de conteúdo interno serão rejeitadas.

O login único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com login único.

Informações relacionadas

- "Faça login no Grid Manager"
- "Criar conta de locatário"
- "Comunicação externa"

Gerencie os controles internos do firewall no StorageGRID

StorageGRID inclui um firewall interno em cada nó que aumenta a segurança do seu

grid, permitindo que você controle o acesso à rede do nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para a sua implementação específica do grid. As alterações de configuração que você faz na página de controle do firewall são aplicadas a cada nó.

Utilize as três abas na página de controle do Firewall para personalizar o acesso necessário para seu grid.

- **Lista de endereços privilegiados**: Use esta aba para permitir acesso selecionado a portas fechadas. Você pode adicionar endereços IP ou sub-redes na notação CIDR que podem acessar portas fechadas usando a aba Gerenciar acesso externo.
- **Gerenciar acesso externo**: Use esta aba para fechar portas que estão abertas por padrão ou reabrir portas previamente fechadas.
- **Rede de cliente não confiável**: Use esta aba para especificar se um nó confia no tráfego de entrada da rede de cliente.

  As configurações desta guia substituem as configurações da guia Gerenciar acesso externo.

  - Um nó com uma Client Network não confiável aceitará apenas conexões nas portas de endpoint do balanceador de carga configuradas nesse nó (globais, de interface de nó e vinculadas ao tipo de nó).
  - As portas dos endpoints do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Manage external networks.
  - Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer endpoints de balanceamento de carga abertos na Client Network.

> As configurações que você define em uma guia podem afetar as alterações de acesso que você faz em outra guia. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporte da maneira que você espera.

Para configurar os controles internos do firewall, consulte "Configurar controles de firewall".

Para obter mais informações sobre firewalls externos e segurança de rede, consulte "Controle de acesso no firewall externo".

Guias Lista de endereços privilegiados e Gerenciar acesso externo

A aba Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso a portas do grid que estão fechadas. A aba Gerenciar acesso externo permite que você feche o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (portas externas são portas acessíveis por nós que não fazem parte do grid por padrão). Essas duas abas geralmente podem ser usadas juntas para personalizar exatamente o acesso à rede que você precisa permitir para seu grid.

> Endereços IP privilegiados não possuem acesso à porta interna da grid por padrão.

Exemplo 1: use um servidor de salto para tarefas de manutenção

Suponha que você queira usar um jump host (um host com segurança reforçada) para administração de rede. Você pode seguir estes passos gerais:

1. Utilize a aba Lista de endereços privilegiados para adicionar o endereço IP do jump host.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

Adicione o endereço IP privilegiado antes de bloquear as portas 443 e 8443. Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, todas as portas externas no Admin Node do seu grid serão bloqueadas para todos os hosts, exceto o jump host. Você poderá então usar o jump host para realizar tarefas de manutenção no seu grid com mais segurança.

Exemplo 2: bloqueio de portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta. Você pode seguir os seguintes passos gerais:

1. Use a guia Lista de endereços privilegiados para conceder acesso somente aos hosts que precisam acessar o serviço.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

Adicione o endereço IP privilegiado antes de bloquear o acesso a quaisquer portas atribuídas ao Grid Manager e ao Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, a porta sensível e o serviço nessa porta ficam disponíveis para os hosts na lista de endereços privilegiados. Todos os outros hosts são impedidos de acessar o serviço, independentemente da interface de origem da solicitação.

Exemplo 3: desativar o acesso a serviços não utilizados

Em nível de rede, você pode desativar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego de cliente HTTP S3, você usaria a opção na guia Gerenciar acesso externo para bloquear a porta 18084.

Aba Redes de Clientes Não Confiáveis

Se você estiver usando uma Client Network, poderá ajudar a proteger o StorageGRID contra ataques hostis, aceitando o tráfego de entrada de clientes somente em endpoints explicitamente configurados.

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, StorageGRID confia nas conexões de entrada para cada nó da grade em todos os "portas externas disponíveis".

Você pode reduzir a ameaça de ataques hostis ao seu StorageGRID especificando que a Client Network em cada nó seja *não confiável*. Se a Client Network de um nó for não confiável, o nó aceita apenas conexões de entrada em portas explicitamente configuradas como endpoints do balanceador de carga. Consulte "Configurar pontos de extremidade do balanceador de carga" e "Configurar controles de firewall".

Exemplo 1: o nó de gateway aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway rejeite todo o tráfego de entrada na Client Network, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Na página "Pontos de extremidade do balanceador de carga", configure um endpoint de balanceador de carga para S3 sobre HTTPS na porta 443.

2. Na página de controle do Firewall, selecione Não confiável para especificar que a Client Network no Gateway Node não é confiável.

Após salvar sua configuração, todo o tráfego de entrada na rede cliente do nó de gateway é bloqueado, exceto as solicitações HTTPS S3 na porta 443 e as solicitações de eco ICMP (ping).

Exemplo 2: nó de armazenamento envia solicitações de serviços da plataforma S3

Suponha que você queira habilitar o tráfego de saída dos serviços da plataforma S3 a partir de um Storage Node, mas queira impedir quaisquer conexões de entrada para esse Storage Node na Client Network. Você executaria esta etapa geral:

- Na guia "Redes de Clientes Não Confiáveis" da página de controle do Firewall, indique que a Rede de Clientes no Nó de Armazenamento não é confiável.

Após salvar sua configuração, o Nó de Armazenamento deixa de aceitar qualquer tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para os destinos de serviços de plataforma configurados.

Exemplo 3: limitar o acesso ao Grid Manager a uma sub-rede

Suponha que você queira permitir o acesso do Grid Manager apenas em uma sub-rede específica. Você executaria os seguintes passos:

1. Conecte a rede do cliente dos seus nós de administração à subnet.
2. Utilize a guia Rede de Cliente Não Confiável para configurar a Rede de Cliente como não confiável.
3. Ao criar um endpoint de balanceador de carga da interface de gerenciamento, insira a porta e selecione a interface de gerenciamento que a porta acessará.
4. Selecione **Sim** para Rede de Cliente Não Confiável.
5. Use a guia Gerenciar acesso externo para bloquear todas as portas externas (com ou sem endereços IP privilegiados definidos para hosts fora dessa sub-rede).

Após salvar sua configuração, somente os hosts na sub-rede que você especificou poderão acessar o Grid Manager. Todos os outros hosts são bloqueados.

Configurar o firewall interno do StorageGRID

Você pode configurar o firewall do StorageGRID para controlar o acesso à rede a portas específicas nos seus nós do StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você analisou as informações em "Gerenciar controles de firewall" e "Diretrizes de networking".
- Se você deseja que um Nó de Administração ou um Nó de Gateway aceite tráfego de entrada somente em endpoints explicitamente configurados, você definiu os endpoints do balanceador de carga.

> ⓘ Ao alterar a configuração da Rede do Cliente, as conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

Sobre esta tarefa

StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas portas nos nós da sua grade. Você pode usar as abas de controle do Firewall para abrir ou fechar portas que estão abertas por padrão na Grid Network, Admin Network e Client Network. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas da grade que estão fechadas. Se você estiver usando uma Client Network, pode especificar se um nó confia no tráfego de entrada da Client Network e configurar o acesso a portas específicas na Client Network.

Limitar o número de portas abertas para endereços IP externos à sua grid apenas àquelas absolutamente necessárias aumenta a segurança da sua grid. 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 os controles de firewall, incluindo exemplos, consulte "Gerenciar controles de firewall".

Para obter mais informações sobre firewalls externos e segurança de rede, consulte "Controle de acesso no firewall externo".

Acessar controles de firewall

Passos

1. Selecione **Configuração** > **Segurança** > **Controle de firewall**.

   As três abas desta página são descritas em "Gerenciar controles de firewall".

2. Selecione qualquer aba para configurar os controles do firewall.

   Você pode usar essas abas em qualquer ordem. As configurações definidas em uma aba não limitam o que você pode fazer nas outras abas; no entanto, as alterações de configuração feitas em uma aba podem alterar o comportamento das portas configuradas em outras abas.

Lista de endereços privilegiados

Você usa a guia Lista de endereços privilegiados para conceder acesso a hosts a portas que estão fechadas por padrão ou fechadas pelas configurações na guia Gerenciar acesso externo.

Endereços IP e sub-redes privilegiados não têm acesso interno à grid por padrão. Além disso, os endpoints 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 de cliente não confiável.

Passos

1. Na guia Lista de endereços privilegiados, insira o endereço ou a sub-rede IP à qual você deseja conceder acesso às portas fechadas.
2. Opcionalmente, selecione **Adicionar outro endereço IP ou sub-rede na notação CIDR** para adicionar clientes privilegiados adicionais.

   > Adicione o mínimo possível de endereços à lista de privilegiados.

3. Opcionalmente, selecione **Permitir que endereços IP privilegiados acessem as portas internas do StorageGRID**. Consulte "Portas internas do StorageGRID".

Esta opção remove algumas proteções para serviços internos. Se possível, deixe-a desativada.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, ela não pode ser acessada por nenhum endereço IP fora da grid, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas que estejam abertas por padrão e só pode abrir portas que você tenha fechado.

As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia Rede de clientes não confiáveis. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede de clientes, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de clientes não confiáveis substituem as portas fechadas (como 443, 8443, 9443) na Rede de clientes.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não fazem parte da grade por padrão) para os nós em sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
   - Utilize o botão ao lado de cada porta para abrir ou fechar a porta selecionada.
   - Selecione **Abrir todas as portas exibidas** para abrir todas as portas listadas na tabela.
   - Selecione **Fechar todas as portas exibidas** para fechar todas as portas listadas na tabela.

Se você fechar as portas 443 ou 8443 do Grid Manager, todos os usuários atualmente conectados a uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Use a barra de rolagem à direita da tabela para garantir que você visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa digitando um número de porta. Você pode digitar um número de porta parcial. Por exemplo, se você digitar **2**, todas as portas que têm a sequência "2" como parte do nome serão exibidas.

3. Selecione **Save**

Rede de cliente não confiável

Se a Rede Cliente de um nó não for confiável, o nó aceitará tráfego de entrada apenas nas portas configuradas como endpoints do balanceador de carga e, opcionalmente, em portas adicionais que você selecionar nesta guia. Você também pode usar esta guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

As conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

As alterações de configuração que você faz na guia **Rede de Clientes Não Confiáveis** substituem as

configurações da guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de Cliente Não Confiável**.
2. Na seção Definir padrão para novos nós, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grid em um procedimento de expansão.

   - **Confiável** (padrão): Quando um nó é adicionado em uma expansão, sua Client Network é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede de clientes é não confiável.

     Se necessário, você pode retornar a esta aba para alterar a configuração de um novo nó específico.

   Essa configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Utilize as seguintes opções para selecionar os nós que devem permitir conexões de clientes somente em endpoints de balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:

   - Selecione **Não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista de Rede de Cliente Não Confiável.
   - Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista de Rede de Cliente Não Confiável.
   - Use o botão ao lado de cada nó para definir a Client Network 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 de Rede de Clientes Não Confiáveis e, em seguida, usar a opção ao lado de um nó individual para adicionar esse nó específico à lista de Rede de Clientes Confiáveis.

   Use a barra de rolagem à direita da tabela para garantir que você visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó digitando o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a sequência "GW" como parte do nome serão exibidos.

4. Selecione **Salvar**.

   As novas configurações do firewall são aplicadas e entram em vigor imediatamente. As conexões de cliente existentes podem falhar se os endpoints do balanceador de carga não tiverem sido configurados.

Gerenciar locatários

Contas de locatário no StorageGRID

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) para armazenar e recuperar objetos em um sistema StorageGRID.

Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja "StorageGRID 11.8: gerenciar locatários".

Como administrador de grid, você cria e gerencia as contas de locatário que os clientes S3 usam para armazenar e recuperar objetos.

Cada conta de locatário possui grupos federados ou locais, usuários, buckets S3 e objetos.

As contas de locatário podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de locatário podem ser usadas para qualquer um destes casos de uso:

- **Caso de uso empresarial:** Se você administra um sistema StorageGRID em uma aplicação empresarial, pode ser interessante segregar o storage de objetos pelos diferentes departamentos da sua organização. Nesse caso, você poderia criar contas de locatário para o departamento de Marketing, o departamento de Suporte ao Cliente, o departamento de Recursos Humanos e assim por diante.

  > Se você utiliza o protocolo de cliente S3, pode usar buckets e políticas de buckets do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de locatário. Consulte as instruções para implementar "Buckets S3 e políticas de bucket" para obter mais informações.

- **Caso de uso do provedor de serviços:** Se você está administrando um sistema StorageGRID como provedor de serviços, pode segregar o storage de objetos pelas diferentes entidades que irão alugar o storage na sua grid. Nesse caso, você criaria contas de locatário para Company A, Company B, Company C e assim por diante.

Para obter mais informações, consulte "Use uma conta de tenant".

Como faço para criar uma conta de locatário?

Use o Grid manager para criar uma conta de tenant. Ao criar uma conta de tenant, você especifica as seguintes informações:

- Informações básicas, incluindo o nome do locatário, o tipo de cliente (S3) e a cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar serviços de plataforma S3, configurar sua própria fonte de identidade, usar S3 Select ou usar uma conexão de federação de grid.
- O acesso inicial à raiz para o locatário, dependendo se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, você pode habilitar a configuração de S3 Object Lock para o StorageGRID se as contas de locatário do S3 precisarem atender a requisitos regulatórios. Quando o S3 Object Lock está habilitado, todas as contas de locatário do S3 podem criar e gerenciar buckets em conformidade.

Para que serve o Tenant Manager?

Após você criar a conta de locatário, os usuários do locatário podem fazer login no Tenant Manager para executar tarefas como as seguintes:

- Configure a federação de identidades (a menos que a fonte de identidade seja compartilhada com o grid)
- Gerenciar grupos e usuários
- Use a federação de grids para clonagem de contas e replicação entre grids
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select

- Monitorar o uso de armazenamento

> Embora os usuários de locatários do S3 possam criar e gerenciar chaves de acesso e buckets do S3 com o Gerenciador de Locatários, eles precisam usar um aplicativo cliente S3 para ingerir e gerenciar objetos. Veja "Utilize a API REST S3" para mais detalhes.

Crie uma conta de locatário do StorageGRID

Você precisa criar pelo menos uma conta de locatário para controlar o acesso ao armazenamento no seu sistema StorageGRID.

Os passos para criar uma conta de locatário variam dependendo de "federação de identidade" e "autenticação única" estarem configurados e se a conta do Grid Manager que você usa para criar a conta de locatário pertence a um grupo de administradores com a permissão de acesso à raiz.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Acesso à raiz ou permissão para contas de locatário".
- Se a conta do locatário usar a fonte de identidade configurada para o Grid Manager e você quiser conceder permissão de acesso à raiz para a conta do locatário a um grupo federado, você já importou esse grupo federado para o Grid Manager. Você não precisa atribuir nenhuma permissão do Grid Manager a esse grupo de administradores. Consulte "Gerenciar grupos de administradores".
- Se você deseja permitir que um locatário do S3 clone dados de conta e replique objetos de bucket para outra grid usando uma conexão de federação de grids:
  - Você tem "configurou a conexão de federação de grid".
  - O status da conexão é **Conectado**.
  - Você tem permissão de acesso root.
  - Você analisou as considerações para "Gerenciando os tenants permitidos para a federação de grid".
  - Se a conta do locatário usar a fonte de identidade que foi configurada para o Grid Manager, você importou o mesmo grupo federado para o Grid Manager em ambas as grids.

    Ao criar o locatário, você selecionará este grupo para ter a permissão inicial de acesso à raiz tanto para as contas de locatário de origem quanto de destino.

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

Acesse o assistente

Passos

1. Selecione **Tenants**.
2. Selecione **Create**.

Insira os detalhes

Passos

1. Insira os detalhes do tenant.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos locatários não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta exclusivo de 20 dígitos.
Descrição (opcional)	Uma descrição para ajudar a identificar o tenant. Se você estiver criando um locatário que usará uma conexão de federação de grid, opcionalmente, use este campo para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado no Grid 1 também aparecerá para o locatário replicado no Grid 2: "Este locatário foi criado no Grid 1."
Tipo de cliente	Deve ser **S3**.
Cota de armazenamento (opcional)	Se você deseja que este tenant tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **Continue**.

Selecione permissões

Passos

1. Opcionalmente, selecione as permissões básicas que você deseja que este locatário tenha.

> Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, selecione o ícone de ajuda para cada permissão.

Permissão	Se selecionado…
Permitir serviços de plataforma	O locatário pode usar serviços da plataforma S3, como CloudMirror. Veja "Gerencie serviços de plataforma para contas de locatário do S3".
Use sua própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos e usuários federados. Essa opção fica desabilitada se você tiver "SSO configurado" para o seu sistema StorageGRID.
Permitir S3 Select	O locatário pode emitir solicitações de API S3 SelectObjectContent para filtrar e recuperar dados de objetos. Consulte "Gerencie o S3 Select para contas de locatário". **Importante**: as solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e apenas para locatários confiáveis.

2. Opcionalmente, selecione as permissões avançadas que você deseja que este locatário tenha.

Permissão	Se selecionado…
Conexão de federação de grid	O tenant pode usar uma conexão de federação de grid, que: • Faz com que este locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados desta grid (a *grid de origem*) para a outra grid na conexão selecionada (a *grid de destino*). • Permite que este locatário configure a replicação entre grades (cross-grid) entre buckets correspondentes em cada grade. Consulte "Gerenciar os inquilinos permitidos para a federação de grid".
Bloqueio de objeto S3	Permitir que o locatário utilize recursos específicos do S3 Object Lock: • **Definir período máximo de retenção** define por quanto tempo os novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. • **Permitir modo de conformidade** impede que os usuários sobrescrevam ou excluam versões de objetos protegidos durante o período de retenção.

3. Selecione **Continue**.

Defina acesso à raiz e crie um locatário

Passos

1. Defina acesso à raiz para a conta do locatário, com base em se o seu sistema StorageGRID usa federação de identidade, single sign-on (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. Nenhum usuário local pode fazer login.

2. Selecione **Criar locatário**.

   Uma mensagem de sucesso é exibida e o novo tenant é listado na página de Tenants. Para saber como visualizar os detalhes do tenant e monitorar a atividade do tenant, consulte "Monitorar a atividade do locatário".

A aplicação das configurações de locatário em toda a grid pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

3. Se você selecionou a permissão **Usar conexão de federação de grid** para o locatário:
   a. Confirme se um locatário idêntico foi replicado para a outra grid na conexão. Os locatários em ambas as grids terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões.

      Se você vir a mensagem de erro "Tenant created without a clone", consulte as instruções em "Solucionar problemas de erros de federação de grid".

   b. Se você forneceu uma senha de usuário raiz local ao definir acesso à raiz, "alterar a senha do usuário raiz local" para o locatário replicado.

      Um usuário raiz local não consegue fazer login no Tenant Manager na grade de destino até que a senha seja alterada.

Faça login no tenant (opcional)

Conforme necessário, você pode entrar no novo locatário agora para concluir a configuração ou pode entrar no locatário mais tarde. As etapas de login dependem se você está conectado ao Grid Manager usando a porta padrão (443) ou uma porta restrita. Consulte "Controle de acesso no firewall externo".

Faça login agora

Se você estiver usando…	Faça isso…
Porta 443 e você define uma senha para o usuário raiz local	1. Selecione **Entrar como root**. Ao iniciar sessão, aparecem links para configurar buckets, federação de identidade, grupos e usuários. 2. Selecione os links para configurar a conta do locatário. Cada link abre a página correspondente no Tenant Manager. Para concluir a página, consulte o "Instruções para usar contas de tenant".
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 à raiz.

Se você estiver usando…	Faça isso…
Uma porta restrita	1. Selecione **Concluir** 2. Selecione **Restrito** na tabela de tenant para saber mais sobre como acessar esta conta de tenant. A URL do Tenant Manager tem este formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ *`port`* é a porta exclusiva para tenants ◦ *`20-digit-account-id`* é o ID de conta exclusivo do locatário

Entrar mais tarde

Se você estiver usando…	Faça uma destas opções…
Porta 443	• No Grid Manager, selecione **Tenants** e, em seguida, selecione **Sign in** à direita do nome do tenant. • Digite a URL do locatário em um navegador da web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ *`20-digit-account-id`* é o ID de conta exclusivo do locatário
Uma porta restrita	• No Grid Manager, selecione **Inquilinos** e selecione **Restrito**. • Digite a URL do locatário em um navegador da web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *`FQDN_or_Admin_Node_IP`* é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ `*port*` é a porta restrita exclusiva para tenant ◦ *`20-digit-account-id`* é o ID de conta exclusivo do locatário

Configurar o locatário

Siga as instruções em "Use uma conta de tenant" para gerenciar grupos de locatários e usuários, chaves de

acesso S3, buckets, serviços de plataforma, clonagem de contas e replicação entre grids.

Editar uma conta de locatário do StorageGRID

Você pode editar uma conta de locatário para alterar o nome de exibição, a cota de armazenamento ou as permissões do locatário.

Se um locatário tiver a permissão **Usar conexão de federação de grid**, você pode editar os detalhes do locatário em qualquer uma das grids da conexão. No entanto, quaisquer alterações que você fizer em uma grid da conexão não serão copiadas para a outra grid. Se você quiser manter os detalhes do locatário exatamente sincronizados entre as grids, faça as mesmas edições em ambas as grids. Consulte "Gerencie os locatários permitidos para conexão de federação de grid".

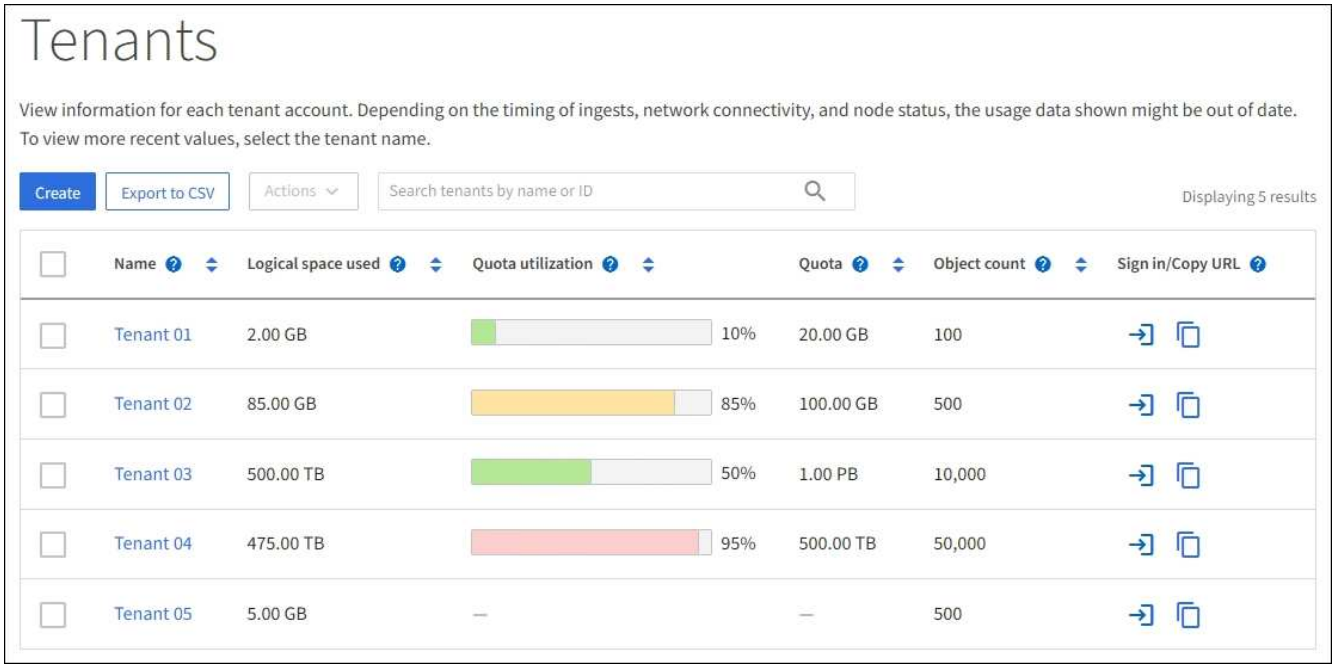
Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Acesso à raiz ou permissão para contas de locatário".

A aplicação das configurações de locatário em toda a grid pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

Passos

1. Selecione **Tenants**.



2. Localize a conta do locatário que você deseja editar.

   Utilize a caixa de pesquisa para procurar um tenant pelo nome ou pelo ID do tenant.

3. Selecione o tenant. Você pode fazer uma das seguintes ações:
   - Selecione a caixa de seleção do tenant e selecione **Actions** > **Edit**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **Editar**.

4. Opcionalmente, altere os valores destes campos:
   - **Nome**
   - **Descrição**
   - **Cota de armazenamento**
5. Selecione **Continue**.
6. Selecione ou limpe as permissões da conta do tenant.
   - Se você desativar os **Serviços da Plataforma** para um locatário que já os utiliza, os serviços que ele configurou para seus buckets S3 deixarão de funcionar. Nenhuma mensagem de erro é enviada ao locatário. Por exemplo, se o locatário configurou a replicação CloudMirror para um bucket S3, ele ainda poderá armazenar objetos no bucket, mas cópias desses objetos não serão mais feitas no bucket S3 externo que ele configurou como endpoint. Consulte "Gerencie serviços de plataforma para contas de locatário do S3".
   - Altere a configuração de **Usar a própria fonte de identidade** para determinar se a conta do locatário usará sua própria fonte de identidade ou a fonte de identidade configurada para o Grid Manager.

     Se **Usar a própria fonte de identidade** estiver:

     - Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desativar sua fonte de identidade antes de poder usar a fonte de identidade configurada para o Grid Manager.
     - Desativado e não selecionado, o SSO está habilitado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Grid Manager.
   - Selecione ou desmarque a permissão **Permitir seleção S3** conforme necessário. Consulte "Gerencie o S3 Select para contas de locatário".
   - Para remover a permissão **Usar conexão de federação de grid**:
     i. Selecione a guia **Federação de grid**.
     ii. Selecione **Remover permissão**.
   - Para adicionar a permissão **Usar conexão de federação de grid**:
     i. Selecione a guia **Federação de grid**.
     ii. Selecione a caixa de seleção **Usar conexão de federação de grid**.
     iii. Opcionalmente, selecione **Clonar usuários e grupos locais existentes** para cloná-los para a grid remota. Se desejar, você pode interromper a clonagem em andamento ou tentar novamente a clonagem caso alguns usuários ou grupos locais não tenham sido clonados após a conclusão da última operação de clonagem.
   - Para definir um período máximo de retenção ou permitir o modo de conformidade:

     > O bloqueio de objetos S3 deve estar ativado na grid antes que você possa usar essas configurações.

     i. Selecione a aba **Bloqueio de Objeto S3**.
     ii. Em **Definir período máximo de retenção**, insira um valor e selecione o período de tempo no menu suspenso.
     iii. Para **Permitir modo de conformidade**, selecione a caixa de seleção.

Alterar a senha do usuário raiz local do StorageGRID tenant

Você pode precisar alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado na conta.

Antes de começar

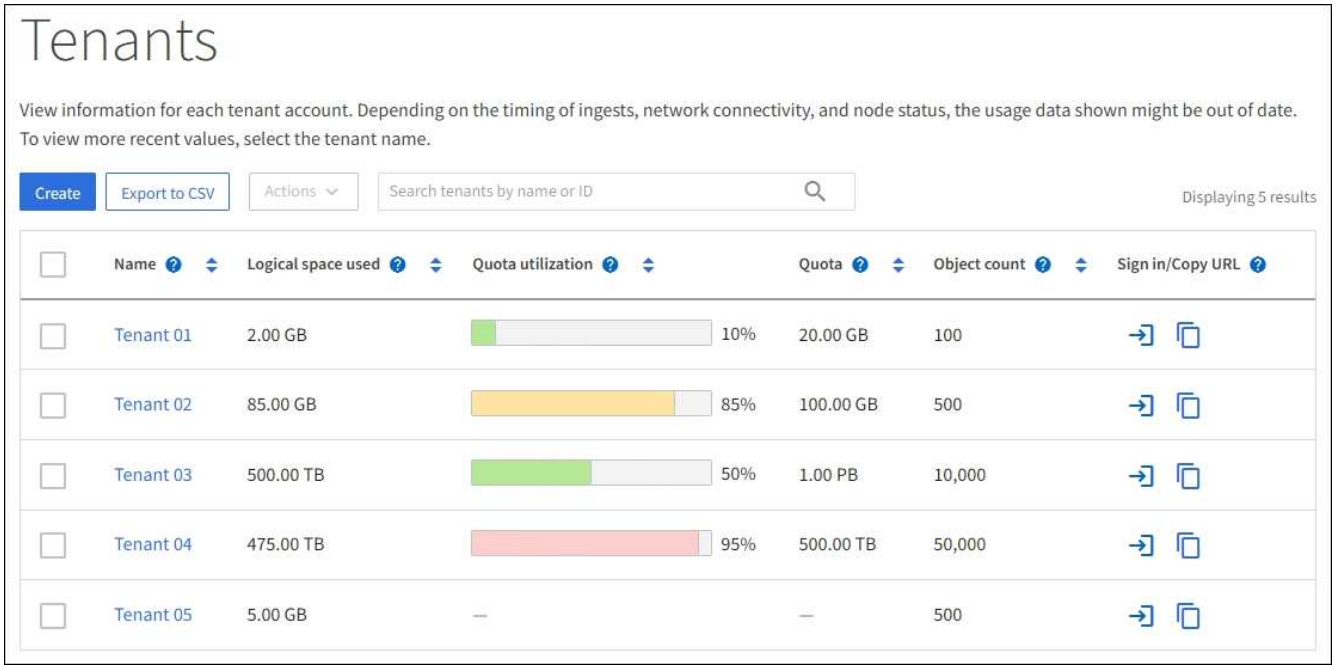
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Sobre esta tarefa

Se o login único (SSO) estiver habilitado para o seu sistema StorageGRID, o usuário raiz não poderá acessar a conta do tenant. Para executar tarefas de usuário raiz, os usuários devem pertencer a um grupo federado que tenha permissão de acesso root para o tenant.

Passos

1. Selecione **Tenants**.



2. Selecione a conta do locatário. Você pode fazer uma das seguintes ações:
   - Selecione a caixa de seleção do locatário e selecione **Ações** > **Alterar senha de root**.
   - Selecione o nome do locatário para exibir a página de detalhes e selecione **Ações** > **Alterar senha root**.
3. Digite a nova senha para a conta do tenant.
4. Selecione **Salvar**.

Excluir uma conta de locatário do StorageGRID

Você pode excluir a conta de um locatário se desejar remover permanentemente o acesso desse locatário ao sistema.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você removeu todos os buckets e objetos S3 associados à conta do locatário.
- Se o inquilino tiver permissão para usar uma conexão de federação de grid, você analisou as considerações para "excluindo um locatário com a permissão "Usar conexão de federação de grid"".

Passos

1. Selecione **Tenants**.
2. Localize a(s) conta(s) do locatário que você deseja excluir.

   Utilize a caixa de pesquisa para procurar um tenant pelo nome ou pelo ID do tenant.

3. Para excluir vários tenants, selecione as caixas de seleção e selecione **Ações** > **Excluir**.
4. Para excluir um único locatário, faça um dos seguintes:
   - Selecione a caixa de seleção e selecione **Ações** > **Excluir**.
   - Selecione o nome do locatário para exibir a página de detalhes e, em seguida, selecione **Actions** > **Delete**.
5. Selecione **Sim**.

Gerenciar serviços de plataforma

Saiba mais sobre os serviços da plataforma StorageGRID

Os serviços da plataforma incluem CloudMirror replicação, notificações de eventos e o serviço de integração de pesquisa.

Se você habilitar os serviços de plataforma para contas de locatários do S3, deverá configurar sua grid para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

Os serviços de plataforma não são suportados para "buckets de branch".

CloudMirror replicação

O serviço de replicação CloudMirror do StorageGRID é usado para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

Por exemplo, você pode usar a replicação CloudMirror para espelhar registros específicos de clientes no Amazon S3 e, em seguida, aproveitar os serviços da AWS para realizar análises em seus dados.

CloudMirror replication apresenta algumas semelhanças e diferenças importantes em relação ao recurso de replicação entre grades. Para saber mais, consulte "Compare a replicação entre grades e a replicação CloudMirror".

CloudMirror replication 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 realizadas em objetos para um cluster Kafka externo especificado, um endpoint de webhook ou o Amazon Simple Notification Service.

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 seja possível configurar a notificação de eventos em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) 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 específico, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

Por exemplo, você pode configurar seus buckets para enviar metadados de objetos S3 para um serviço Elasticsearch remoto. Em seguida, você pode usar o Elasticsearch para realizar buscas em todos os buckets e executar análises sofisticadas de padrões presentes nos metadados dos seus objetos.

> Embora a integração com o Elasticsearch possa ser configurada em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) dos objetos não serão incluídos nas mensagens de notificação.

Os serviços de plataforma permitem que os locatários usem recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino dos serviços de plataforma geralmente é externo à sua implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se permitir, você deve habilitar o uso dos serviços de plataforma ao criar ou editar contas de locatário. Você também deve configurar sua rede para que as mensagens dos serviços de plataforma geradas pelos locatários possam chegar aos seus destinos.

Recomendações para o uso de serviços de plataforma

Antes de utilizar os serviços da plataforma, esteja ciente das seguintes recomendações:

- Se um bucket S3 no sistema StorageGRID tiver tanto o versionamento quanto a replicação CloudMirror ativados, você também deve ativar o versionamento do bucket S3 para o endpoint de destino. Isso permite que a replicação CloudMirror gere versões de objetos semelhantes no endpoint.
- Você não deve usar mais de 100 tenants ativos com solicitações S3 que exigem CloudMirror para replicação, notificações e integração de pesquisa. Ter mais de 100 tenants ativos pode resultar em desempenho mais lento do cliente S3.
- As solicitações para um endpoint que não puderem ser concluídas serão enfileiradas até um máximo de 500.000 solicitações. Esse limite é compartilhado igualmente entre os tenants ativos. Novos tenants podem exceder temporariamente esse limite de 500.000 para que não sejam penalizados injustamente.

Informações relacionadas

- "Gerenciar serviços de plataforma"
- "Configurar as configurações de proxy de storage"
- "Monitorar o StorageGRID"

Rede e portas para serviços de plataforma StorageGRID

Se você permitir que um locatário do S3 use os serviços da plataforma, deverá

configurar a rede do grid para garantir que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Você pode habilitar os serviços de plataforma para uma conta de locatário S3 ao criar ou atualizar a conta do locatário. Se os serviços de plataforma estiverem habilitados, o locatário pode criar endpoints que servem como destino para replicação CloudMirror, notificações de eventos ou mensagens de integração de pesquisa de seus buckets S3. Essas mensagens de serviços de plataforma são enviadas dos Storage Nodes 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 que oferece suporte ao recebimento de mensagens do Amazon Simple Notification Service
- Um cluster Kafka hospedado localmente
- Um endpoint webhook externo ou hospedado localmente que suporta solicitações de notificação HTTP POST.

  Este endpoint pode ser hospedado em diversos servidores web, frameworks ou ferramentas de processamento de dados, como o Fluentd.

- Um bucket S3 hospedado localmente na mesma instância ou em outra instância do StorageGRID
- Um endpoint externo, como um endpoint na Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a(s) rede(s) que contém(êm) os Nós de Armazenamento do ADC. Você deve garantir que as seguintes portas possam ser usadas para enviar mensagens dos serviços da plataforma aos 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 (a maioria dos endpoints)
- **443**: Para URIs de endpoint que começam com https (a maioria dos endpoints)
- **9092**: Para URIs de endpoint que começam com http ou https (somente endpoints Kafka)

Os locatários podem especificar uma porta diferente ao criar ou editar um endpoint.

> Se uma implementação do StorageGRID for usada como destino para a replicação do CloudMirror, as mensagens de replicação poderão ser recebidas em uma porta diferente de 80 ou 443. Certifique-se de que a porta usada para o S3 pela implementação do StorageGRID de destino esteja especificada no endpoint.

Se você utiliza um servidor proxy não transparente, também precisa "configurar as configurações de proxy de armazenamento" permitir que mensagens sejam enviadas para endpoints externos, como um endpoint na internet.

Informações relacionadas

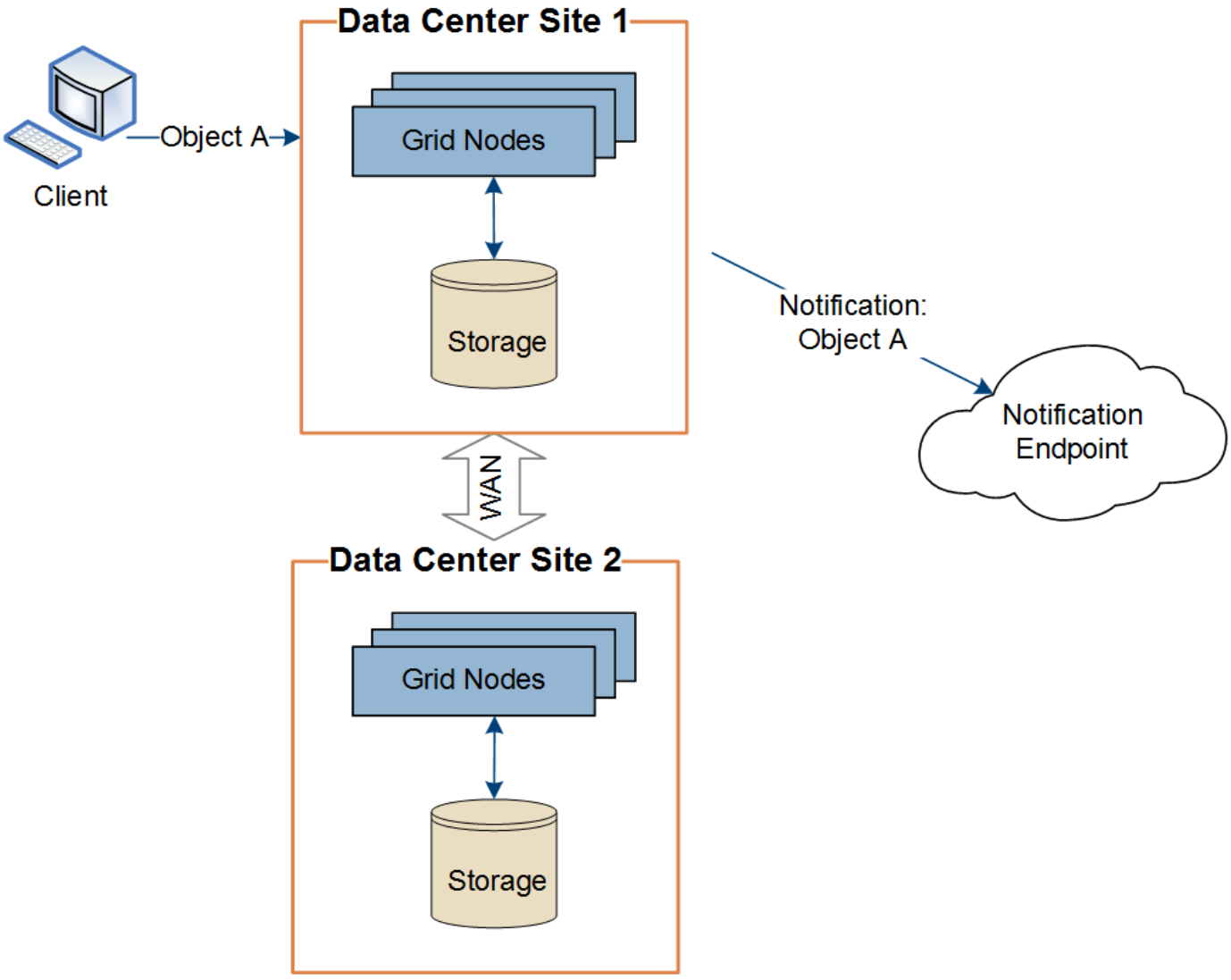
"Use uma conta de tenant"

Entrega por local de mensagens dos serviços da plataforma StorageGRID

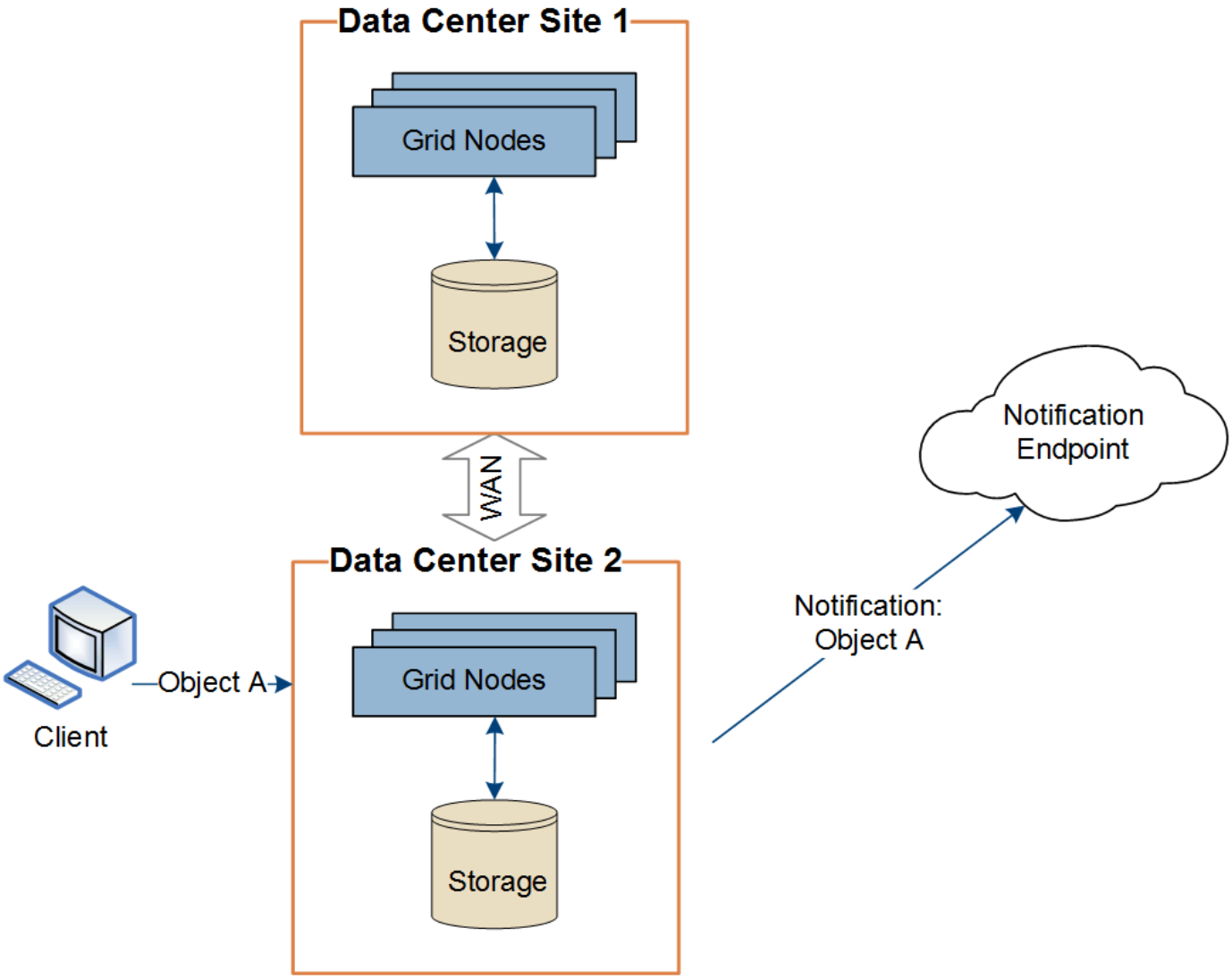
Todas as operações de serviços da plataforma são realizadas individualmente em cada

site.

Ou seja, se um locatário usar um cliente para executar uma operação Create da API S3 em um objeto, conectando-se a um Gateway Node no Data Center Site 1, a notificação sobre essa ação será acionada e enviada do Data Center Site 1.



Se o cliente posteriormente executar uma operação de exclusão da API S3 nesse mesmo objeto a partir 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 esteja configurada de forma que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Solucione problemas dos serviços da plataforma StorageGRID

Os endpoints usados nos serviços da plataforma são criados e mantidos pelos usuários do tenant no Tenant Manager. No entanto, se um tenant tiver problemas para configurar ou usar os serviços da plataforma, você pode usar o Grid Manager 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 endpoints usando o Tenant Manager. Cada endpoint representa um destino externo para um serviço da plataforma, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon Simple Notification Service, um tópico do Kafka ou um cluster do Elasticsearch hospedado localmente ou na AWS. Cada endpoint inclui tanto a localização do recurso externo quanto as credenciais necessárias para acessar esse recurso.

Quando um locatário cria um endpoint, o StorageGRID valida se o endpoint existe e se pode ser acessado 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.

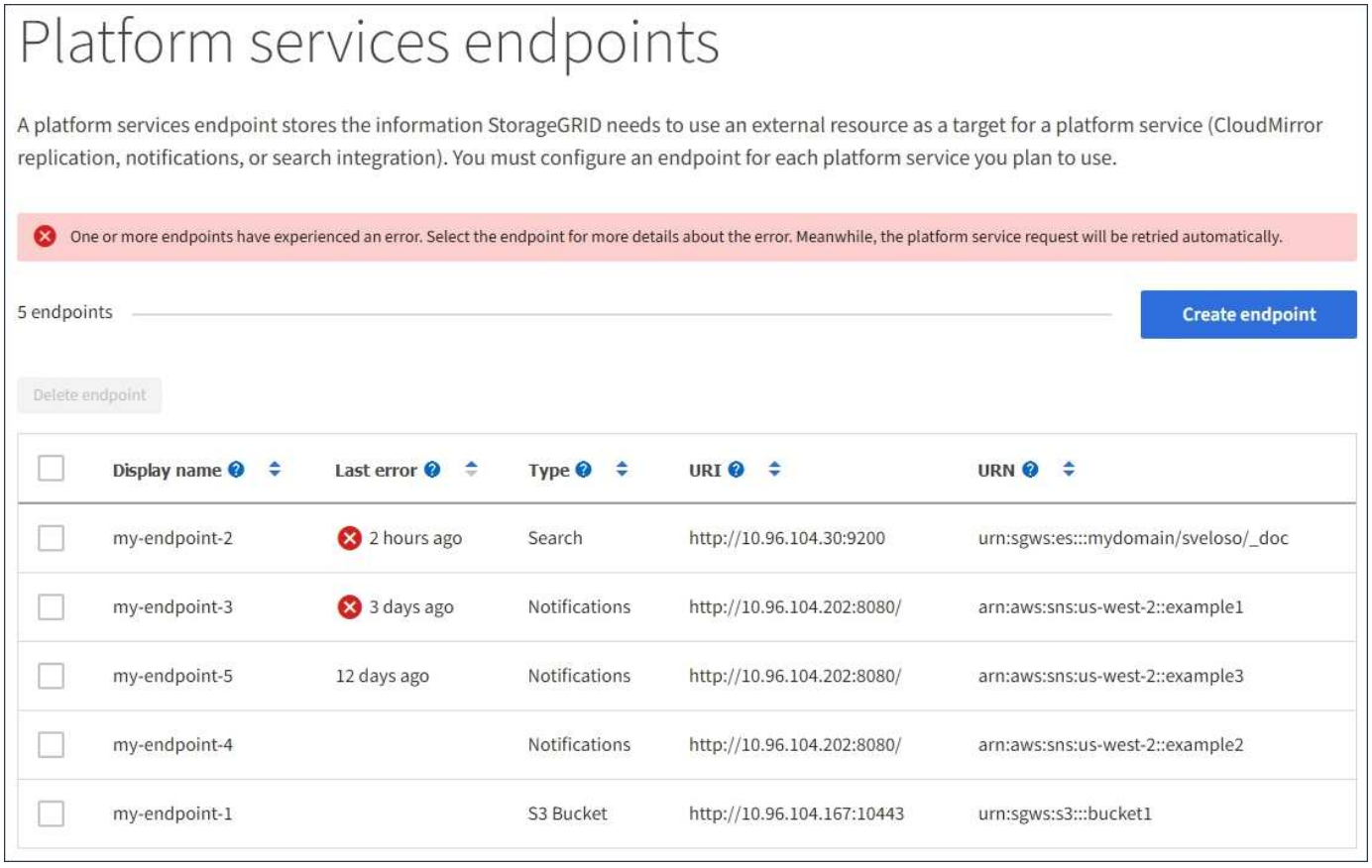
> A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do tenant.

Problemas com os endpoints existentes

Se ocorrer um erro quando StorageGRID tentar acessar um endpoint existente, uma mensagem será exibida no painel do Tenant Manager.

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

Os usuários locatários podem acessar a página de Endpoints para revisar a mensagem de erro mais recente de cada endpoint e determinar há quanto tempo o erro ocorreu. A coluna **Último erro** exibe a mensagem de erro mais recente de cada endpoint e indica há quanto tempo 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 da grade ou suporte técnico pode usar esse ID para localizar informações mais detalhadas sobre o erro no bycast.log.

Problemas relacionados a servidores proxy

Se você configurou um "proxy de armazenamento" entre os nós de armazenamento e os endpoints do serviço da plataforma, podem ocorrer erros se o seu serviço de proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não estejam sendo bloqueadas.

Determine se ocorreu um erro

Se ocorrerem erros de endpoint nos últimos 7 dias, o painel do Tenant Manager exibirá uma mensagem de alerta. Você pode acessar a página Endpoints para ver mais detalhes sobre o erro.

As operações do cliente falham

Alguns problemas nos serviços da plataforma podem causar falhas nas operações do cliente no bucket S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno de Replicated State Machine (RSM) for interrompido ou se houver muitas mensagens dos serviços da plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **Nós** > ***site*** > ***Nó de armazenamento*** > **Visão geral**.
2. Verifique se há alertas ativos na tabela de Alertas.
3. Resolva quaisquer alertas ativos. Se necessário, entre em contato com o suporte técnico.

Erros de endpoint recuperáveis e irrecuperáveis

Após a criação dos endpoints, erros nas solicitações de serviço da plataforma podem ocorrer por diversos 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 bucket de destino não existe.
- A notificação não pôde ser entregue.

Caso StorageGRID encontre um erro recuperável, a solicitação de serviço da plataforma será repetida até que seja bem-sucedida.

Outros erros são irrecuperáveis. Por exemplo, erros irrecuperáveis podem ocorrer pelos seguintes motivos:

- O endpoint foi excluído.
- Um endpoint de webhook destino responde a uma solicitação de notificação com um `400 Bad Request` erro.

Se StorageGRID encontrar um erro de endpoint irrecuperável:

- No Grid Manager, acesse **Suporte** > **Ferramentas** > **Métricas** > **Grafana** > **Platform Services Overview** para visualizar os detalhes do erro.
- No Gerenciador de Locatários, vá para **STORAGE (S3)** > **Platform Services Endpoints** para visualizar os detalhes do erro.
- Verifique o `/var/local/log/bycast-err.log` para erros relacionados. Os nós de armazenamento que possuem o serviço ADC contêm este arquivo de log.

Não foi possível entregar as mensagens dos serviços da plataforma

Se o destino encontrar um problema que o impeça de aceitar mensagens dos serviços da plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem dos serviços da plataforma não será entregue. Por exemplo, esse erro pode ocorrer se as credenciais forem atualizadas no destino de forma que StorageGRID não consiga mais se autenticar no serviço de destino.

Verifique se há alertas relacionados.

Desempenho mais lento para solicitações de serviço da plataforma

O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa de envio das solicitações exceder a taxa na qual o endpoint de destino pode recebê-las. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao endpoint de destino.

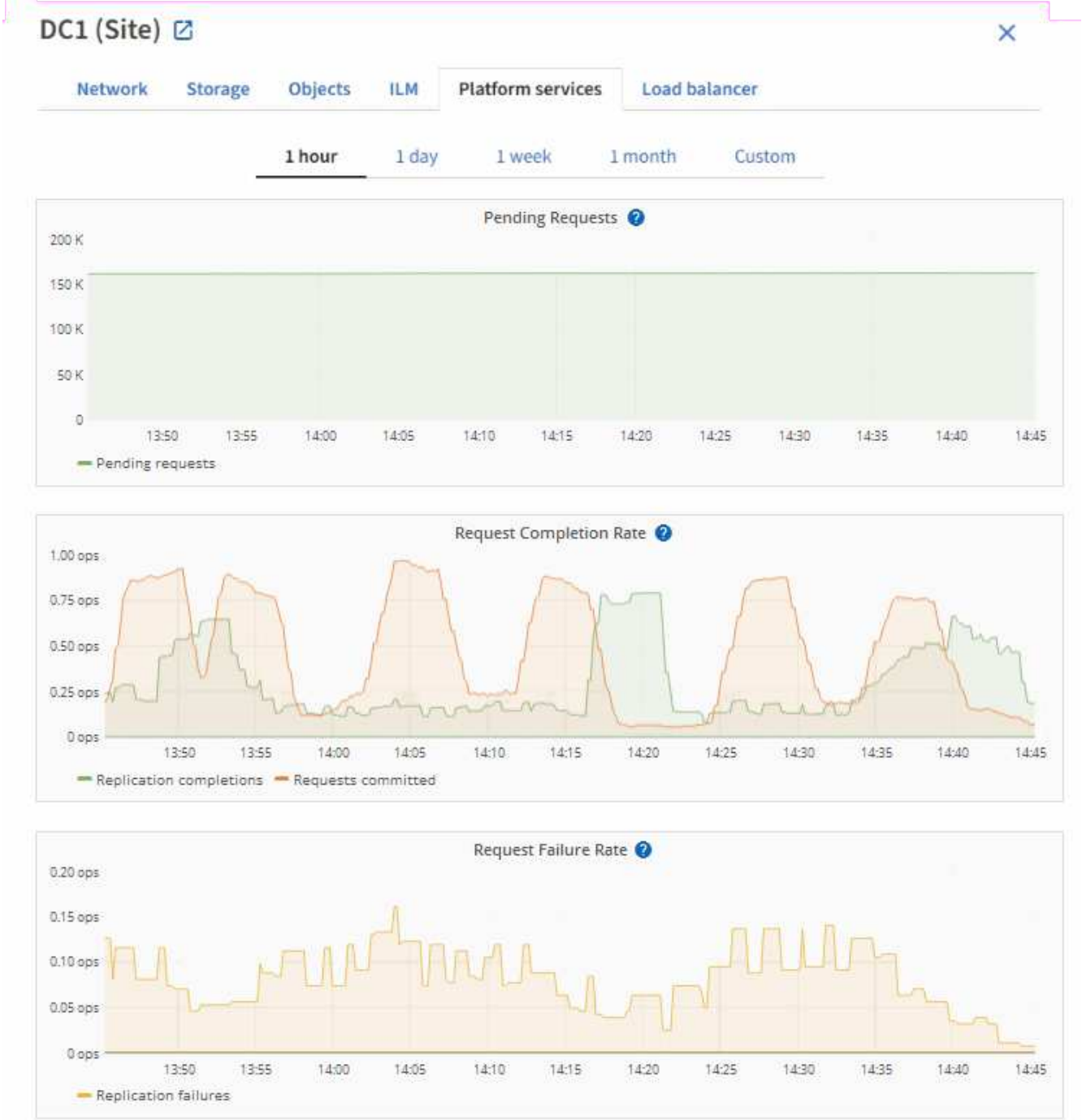
O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o acúmulo de solicitações continuar crescendo, as operações do cliente S3 (como solicitações PUT) eventualmente falharão.

As solicitações do CloudMirror têm mais probabilidade de serem afetadas pelo desempenho do endpoint de destino, porque normalmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou de notificação de eventos.

As solicitações de serviço da plataforma falham

Para visualizar a taxa de falha de solicitações para serviços da plataforma:

1. Selecione **Nós**.
2. Selecione ***site*** > **Serviços da Plataforma**.
3. Veja o gráfico da taxa de erros de solicitação.



Alerta de indisponibilidade dos serviços da plataforma

O alerta **Serviços da plataforma indisponíveis** indica que nenhuma operação de serviço da plataforma pode ser executada em um site porque há poucos Storage Nodes com o serviço RSM em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas aos seus respectivos endpoints.

Para resolver este alerta, determine quais Storage Nodes no site incluem o serviço RSM. (O serviço RSM está presente nos Storage Nodes que também incluem o serviço ADC.) Em seguida, certifique-se de que a maioria simples desses Storage Nodes esteja em execução e disponível.

Se mais de um nó de armazenamento que contenha o serviço RSM falhar em um site, você perderá quaisquer solicitações de serviço de plataforma pendentes para esse site.

Orientações adicionais para resolução de problemas nos endpoints dos serviços da plataforma

Para obter informações adicionais, consulte **Usar uma conta de locatário › Solucionar problemas de endpoints de serviços da plataforma**.

Informações relacionadas

"Solucione problemas do sistema StorageGRID"

Gerenciar o S3 Select para contas de locatário no StorageGRID

Você pode permitir que determinados tenants do S3 usem o S3 Select para emitir solicitações SelectObjectContent em objetos individuais.

O S3 Select oferece uma maneira eficiente de pesquisar grandes quantidades de dados sem a necessidade de implantar um banco de dados e os recursos associados para viabilizar as pesquisas. Ele também reduz o custo e a latência da recuperação de dados.

O que é S3 Select?

O S3 Select permite que os clientes S3 usem solicitações SelectObjectContent para filtrar e recuperar apenas os dados necessários de um objeto. A implementação do S3 Select no StorageGRID inclui um subconjunto de comandos e recursos do S3 Select.

Considerações e requisitos para usar o S3 Select

Requisitos de administração do grid

O administrador da grade deve conceder aos locatários a permissão S3 Select. Selecione **Permitir S3 Select** quando "criando um tenant" ou "editar um tenant".

Requisitos de formato de objeto

O objeto que você deseja consultar deve estar em um dos seguintes formatos:

- **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
- **Parquet**. Requisitos adicionais para objetos Parquet:
  - O S3 Select suporta apenas compressão colunar usando GZIP ou Snappy. O S3 Select não suporta compressão de objeto inteiro para objetos Parquet.
  - O S3 Select não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
  - O tamanho máximo de um grupo de linhas não compactadas é de 512 MB.
  - Você deve usar os tipos de dados especificados no esquema do objeto.
  - Não é possível usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.

Requisitos do endpoint

A solicitação SelectObjectContent deve ser enviada para um "Endpoint do balanceador de carga

StorageGRID".

Os nós de administração e de gateway usados pelo endpoint devem ser um dos seguintes:

- Um nó de appliance de serviços
- Um nó de software baseado em VMware
- Um nó bare metal executando um kernel com cgroup v2 habilitado

Considerações gerais

Não é possível enviar consultas diretamente para os Storage Nodes.

> SelectObjectContent requests podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e apenas para locatários confiáveis.

Consulte o "Instruções para usar o S3 Select".

Para visualizar "Gráficos do Grafana" para operações do S3 Select ao longo do tempo, selecione **Suporte** > **Ferramentas** > **Métricas** no Gerenciador de Grade.

Configurar conexões de cliente

Configurar conexões do cliente S3 ao StorageGRID

Como administrador de grid, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 se conectam ao seu sistema StorageGRID para armazenar e recuperar dados.

> Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja "StorageGRID 11.8: Configurar conexões de cliente S3 e Swift".

Tarefas de configuração

1. Execute as tarefas pré-requisito no StorageGRID, com base em como o aplicativo cliente se conectará ao StorageGRID.

Tarefas necessárias

Você deve obter:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Tarefas opcionais

Opcionalmente, configure:

- Federação de identidades
- SSO

1. Use StorageGRID para obter os valores necessários para que o aplicativo se conecte à grid. Você pode usar o assistente de instalação S3 ou configurar cada entidade do StorageGRID manualmente.

Use o assistente de instalação S3

Siga os passos no assistente de instalação S3.

Configurar manualmente

1. Criar grupo de alta disponibilidade
2. Criar endpoint de balanceador de carga
3. Criar conta de locatário
4. Criar bucket e chaves de acesso
5. Configurar regra e política do ILM

1. Utilize o aplicativo S3 para concluir a conexão com StorageGRID. Crie entradas DNS para associar endereços IP a quaisquer nomes de domínio que você planeje usar.

   Se necessário, realize configurações adicionais do aplicativo.

2. Execute tarefas contínuas no aplicativo e no StorageGRID para gerenciar e monitorar storage de objetos ao longo do tempo.

Informações necessárias para conectar StorageGRID a um aplicativo cliente

Antes de conectar StorageGRID a um aplicativo cliente S3, você deve executar etapas de configuração no StorageGRID e obter determinados valores.

Quais valores você precisa?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e onde esses valores são usados pelo aplicativo S3 e pelo servidor DNS.

Valor	Onde o valor é configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > Grupo HA	Entrada DNS
Porta	StorageGRID > Ponto final do balanceador de carga	Aplicativo do cliente
Certificado SSL	StorageGRID > Ponto final do balanceador de carga	Aplicativo do cliente
Nome do servidor (FQDN)	StorageGRID > Ponto final do balanceador de carga	• Aplicativo do cliente • Entrada DNS
ID da chave de acesso S3 e chave de acesso secreta	StorageGRID > Locatário e bucket	Aplicativo do cliente
Nome do bucket/container	StorageGRID > Locatário e bucket	Aplicativo do cliente

Como obtenho esses valores?

Dependendo das suas necessidades, você pode fazer o seguinte para obter as informações de que precisa:

- **Use o "Assistente de instalação S3"**. O assistente de instalação S3 ajuda você a configurar rapidamente os valores necessários no StorageGRID e gera um ou dois arquivos que você pode usar ao configurar o aplicativo S3. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID.

  > Se você estiver configurando um aplicativo S3, recomenda-se usar o assistente de instalação do S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Use o "FabricPool assistente de instalação"**. Semelhante ao assistente de instalação S3, o assistente de instalação FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar uma camada de nuvem FabricPool no ONTAP.

  > Se você planeja usar StorageGRID como o storage de objetos para uma camada de nuvem FabricPool, é recomendado usar o assistente de instalação FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Configurar itens manualmente**. Se você estiver se conectando a um aplicativo S3 e preferir não usar o assistente de instalação, você pode obter os valores necessários realizando a configuração manualmente. Siga estas etapas:

  a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3. Consulte "Configurar grupos de alta disponibilidade".

  b. Crie o endpoint do balanceador de carga que o aplicativo S3 usará. Consulte "Configurar pontos de extremidade do balanceador de carga".

  c. Crie a conta de locatário que o aplicativo S3 usará. Consulte "Crie uma conta de locatário".

d. Para um locatário S3, faça login na conta do locatário e gere um ID de chave de acesso e uma chave de acesso secreta para cada usuário que acessará o aplicativo. Consulte "Crie suas próprias chaves de acesso".

e. Crie um ou mais buckets do S3 na conta do locatário. Para S3, veja "Criar bucket S3".

f. Para adicionar instruções específicas de posicionamento 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. Consulte "Criar regra ILM" e "Criar política de ILM".

Segurança para clientes S3 no StorageGRID

As contas de tenant do StorageGRID usam aplicativos cliente S3 para salvar dados de objetos no StorageGRID. Você deve revisar as medidas de segurança implementadas para aplicativos cliente.

Resumo

A lista a seguir resume como a segurança é implementada para a S3 API REST:

Segurança da conexão
TLS

Autenticação do servidor
Certificado de servidor X.509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador

Autenticação do cliente
ID da chave de acesso da conta S3 e chave de acesso secreta

Autorização do cliente
Propriedade do bucket e todas as políticas de controle de acesso aplicáveis

Como StorageGRID fornece segurança para aplicativos de cliente

Os aplicativos cliente S3 podem se conectar ao serviço Load Balancer em Gateway Nodes, Admin Nodes ou diretamente aos Storage Nodes.

- Os clientes que se conectam ao serviço Load Balancer podem usar HTTPS ou HTTP, dependendo de como você "configurar o endpoint do balanceador de carga".

  O HTTPS oferece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao endpoint.

  O HTTP oferece comunicação menos segura e não criptografada, devendo ser usado apenas para grids de teste ou que não sejam de produção.

- Os clientes que se conectam aos nós de armazenamento também podem usar HTTPS ou HTTP.

  O HTTPS é o padrão e é recomendado.

  O HTTP oferece comunicação menos segura e não criptografada, mas pode ser opcionalmente "habilitado" para grids de teste ou que não sejam de produção.

- As comunicações entre StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento na grade são criptografadas, independentemente de o endpoint do Load Balancer estar configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer "Cabeçalhos de autenticação HTTP" ao StorageGRID para executar operações da API REST.

Certificados de segurança e aplicativos de cliente

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

- Quando os aplicativos cliente se conectam ao serviço Load Balancer, eles usam o certificado que foi configurado para o endpoint do balanceador de carga. Cada endpoint do balanceador de carga tem seu próprio certificado—seja um certificado de servidor personalizado carregado pelo administrador do grid ou um certificado que o administrador do grid gerou no StorageGRID ao configurar o endpoint.

  Consulte "Considerações sobre balanceamento de carga".

- Quando os aplicativos cliente se conectam diretamente a um Nó de Armazenamento, eles usam os certificados de servidor gerados pelo sistema para os Nós de Armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade certificadora do sistema), ou um único certificado de servidor personalizado fornecido para a grid por um administrador da grid. Consulte "Adicionar um certificado de API S3 personalizado".

Os clientes devem ser configurados para confiar na autoridade certificadora que assinou o certificado que utilizam para estabelecer conexões TLS.

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto de suítes de cifras que os aplicativos cliente podem usar ao estabelecer uma sessão TLS. Para configurar as cifras, vá em **Configuração** > **Segurança** > **Configurações de segurança** e selecione **Políticas de TLS e SSH**.

Versões compatíveis do TLS

StorageGRID suporta TLS 1.2 e TLS 1.3.

SSLv3 e TLS 1.1 (ou versões anteriores) não são mais suportados.

Use o assistente de instalação S3

Considerações e requisitos do assistente de instalação do StorageGRID S3

Você pode usar o assistente de instalação S3 para configurar o StorageGRID como o storage de objetos para um aplicativo S3.

Quando usar o assistente de instalação S3

O assistente de instalação S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você faz o download de arquivos que pode usar para inserir valores no aplicativo S3. Use o assistente para configurar seu sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID.

Se você tiver "Permissão de acesso root", poderá concluir o assistente de instalação do S3 ao começar a usar o StorageGRID Grid Manager ou poderá acessá-lo e concluí-lo posteriormente. Dependendo dos seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para reunir os valores que um aplicativo S3 precisa.

Antes de usar o assistente

Antes de usar o assistente, confirme que você concluiu esses pré-requisitos.

Obtenha endereços IP e configure interfaces VLAN

Se você for configurar um grupo de alta disponibilidade (HA), saberá a quais nós o aplicativo S3 se conectará e qual rede StorageGRID será usada. Você também saberá quais valores inserir para o CIDR da sub-rede, endereço IP do gateway e endereços IP virtuais (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, você já configurou a interface VLAN. Consulte "Configurar interfaces VLAN".

Configurar a federação de identidades e o SSO (Single Sign-On)

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, você habilitou esses recursos. Você também sabe qual grupo federado deve ter acesso à raiz para a conta do tenant que o aplicativo S3 usará. Consulte "Use federação de identidades" e "Configure o single sign-on (SSO)".

Obtenha e configure nomes de domínio

Você sabe qual domínio totalmente qualificado (FQDN) usar para StorageGRID. As entradas do servidor de nomes (DNS) mapearão esse FQDN para os endereços VIP do grupo de HA que você criar usando o assistente.

Se você planeja usar solicitações virtuais no estilo de hospedagem do S3, você deve ter "nomes de domínio de endpoint S3 configurados". O uso de solicitações virtuais no estilo de hospedagem é recomendado.

Analise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID, já deve ter revisado as considerações gerais sobre balanceamento de carga. Você já possui os certificados que irá carregar ou os valores necessários para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (terceiro), você precisa ter o domínio totalmente qualificado (FQDN), a porta e o certificado desse balanceador de carga.

Configurar quaisquer conexões de federação de grid

Se você deseja permitir que o locatário do S3 clone dados da conta e replique objetos do bucket para outra grid usando uma conexão de federação de grid, confirme o seguinte antes de iniciar o assistente:

- Você tem "configurou a conexão de federação de grid".
- O status da conexão é **Conectado**.
- Você tem permissão de acesso root.

Acesse e conclua o assistente de instalação no StorageGRID

Você pode usar o assistente de instalação S3 para configurar StorageGRID para uso com um aplicativo S3. O assistente de instalação fornece os valores necessários para

que o aplicativo acesse um bucket do StorageGRID e salve objetos.

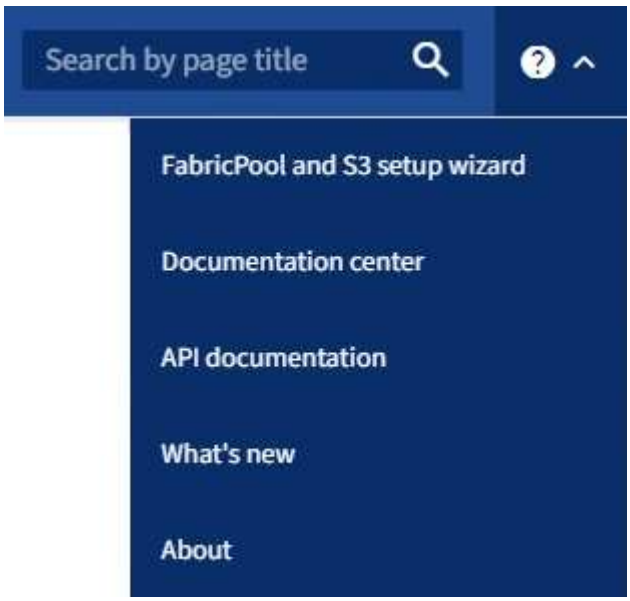
Antes de começar

- Você tem o "Permissão de acesso root".
- Você já revisou as "Considerações e requisitos" instruções para usar o assistente.

Acesse o assistente

Passos

1. Faça login no Grid Manager usando um "navegador web compatível".
2. Se o banner **FabricPool and S3 assistente de instalação** aparecer no painel, selecione o link no banner. Se o banner não aparecer mais, selecione o ícone de ajuda na barra de cabeçalho no Grid Manager e selecione **FabricPool and S3 assistente de instalação**.



3. Na seção de aplicativos S3 da página do assistente de instalação do FabricPool e S3, selecione **Configurar agora**.

Etapa 1 de 6: configurar grupo de alta disponibilidade

Um grupo de alta disponibilidade (HA) é uma coleção de nós, cada um contendo o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de alta disponibilidade (HA) para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho com pouco impacto nas operações do S3.

Para obter detalhes sobre esta tarefa, consulte "Gerenciar grupos de alta disponibilidade".

Passos

1. Se você planeja usar um balanceador de carga externo, não precisa criar um grupo de alta disponibilidade. Selecione **Ignorar esta etapa** e vá para Etapa 2 de 6: Configurar o endpoint do balanceador de carga.
2. Para usar o balanceador de carga StorageGRID, você pode criar um novo grupo de alta disponibilidade (HA) ou usar um grupo HA existente.

Criar grupo HA

a. Para criar um novo grupo HA, selecione **Criar grupo HA**.

b. Na etapa **Inserir detalhes**, preencha os seguintes campos.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

c. Na etapa **Adicionar interfaces**, selecione as interfaces de nó que você deseja usar neste grupo de alta disponibilidade.

Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

d. Na etapa **Priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para este grupo de alta disponibilidade.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP (VIP) são movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP são movidos para a próxima interface de backup e assim por diante. Quando as falhas forem resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

e. Na etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR da sub-rede	O endereço da sub-rede VIP na notação CIDR — um endereço IPv4 seguido por uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.
Endereço IP do gateway (opcional)	Se os endereços IP do S3 usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do VIP do StorageGRID. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Criar grupo HA** e, em seguida, selecione **Concluir** para retornar ao assistente de instalação do S3.

g. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Usar grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA em **Selecionar um grupo HA**.

b. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o endpoint do balanceador de carga

StorageGRID utiliza um balanceador de carga para gerenciar a carga de trabalho dos aplicativos cliente. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários Storage Nodes.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós Gateway e Admin, ou pode se conectar a um balanceador de carga externo (de terceiro). Recomenda-se usar o balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, consulte "Considerações sobre balanceamento de carga".

Para usar o serviço StorageGRID Load Balancer, selecione a guia **StorageGRID load balancer** e, em seguida, crie ou selecione o endpoint do balanceador de carga que você deseja usar. Para usar um balanceador de carga externo, selecione a guia **External load balancer** e forneça detalhes sobre o sistema que você já configurou.

Criar endpoint

Passos

1. Para criar um endpoint de balanceador de carga, selecione **Criar endpoint**.
2. Na etapa **Inserir detalhes do endpoint**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta do StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como padrão 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 nos nós de Gateway, pois essas portas são reservadas nos nós de Admin. **Nota:** Portas usadas por outros serviços de grid não são permitidas. Consulte "Portas internas do StorageGRID".
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com StorageGRID sem criptografia TLS é suportada, mas não recomendada.

3. Na etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.

Modo	Descrição
Tipo de nó	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

4. Na etapa de acesso do locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

5. Na etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Fazer upload do certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado por uma CA, a chave privada do certificado e, opcionalmente, um pacote de CA.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Veja "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que inserir.
Use o certificado StorageGRID S3	Use esta opção somente se você já tiver carregado ou gerado uma versão personalizada do certificado global do StorageGRID. Veja "Configurar certificados da API S3" para detalhes.

6. Selecione **Concluir** para retornar ao assistente de instalação do S3.
7. Selecione **Continuar** para ir para a etapa de tenant e bucket.

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

Usar o endpoint do balanceador de carga existente

Passos

1. Para usar um endpoint existente, selecione o nome dele em **Selecionar um endpoint do balanceador de carga**.
2. Selecione **Continuar** para ir para a etapa de tenant e bucket.

Use um balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os seguintes campos.

Campo	Descrição
FQDN	O domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o aplicativo S3 usará para se conectar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continuar** para ir para a etapa de tenant e bucket.

Etapa 3 de 6: criar locatário e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário possui seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos.

Um bucket é um contêiner usado para armazenar os objetos e os metadados de um locatário. Embora os locatários possam ter vários buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Se você precisar adicionar buckets ou definir opções depois, pode usar o Tenant Manager.

Para obter detalhes sobre esta tarefa, consulte "Criar conta de locatário" e "Criar bucket S3".

Passos

1. Insira um nome para a conta do locatário.

   Os nomes dos inquilinos não precisam ser únicos. Quando a conta do inquilino é criada, ela recebe um ID de conta numérico exclusivo.

2. Defina acesso à raiz para a conta do locatário, com base em se o seu sistema StorageGRID usa "federação de identidade", "autenticação única (SSO)" ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para "Permissão de acesso root" para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.

Opção	Faça isso
Se a federação de identidades 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 fazer login.

3. Se você deseja que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário raiz, selecione **Criar chave de acesso S3 do usuário raiz automaticamente**.

   Selecione esta opção se o único usuário do locatário for o usuário raiz. Se outros usuários utilizarem este locatário, "Use o Tenant Manager" para configurar as chaves e permissões.

4. Se você deseja criar um bucket para este tenant agora, selecione **Create bucket for this tenant**.

   Se o S3 Object Lock estiver habilitado para a grid, o bucket criado nesta etapa não terá o S3 Object Lock habilitado. Se você precisar usar um bucket com S3 Object Lock para este aplicativo S3, não selecione criar um bucket agora. Em vez disso, use o Tenant Manager para "criar o bucket" mais tarde.

   a. Insira o nome do bucket que o aplicativo S3 usará. Por exemplo, `s3-bucket`.

      Não é possível alterar o nome do bucket depois de criá-lo.

   b. Selecione a **Região** para este bucket.

      Use a região padrão (`us-east-1`) a menos que você pretenda usar o ILM no futuro para filtrar objetos com base na região do bucket.

5. Selecione **Criar e continuar**.

Etapa 4 de 6: baixar dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que você acabou de configurar.

Passos

1. Se você selecionou **Criar chave de acesso S3 do usuário raiz automaticamente**, faça um ou ambos os seguintes procedimentos:
   - Selecione **Baixar chaves de acesso** para baixar um arquivo `.csv` contendo o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
   - Selecione o ícone de copiar ( ) para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.
2. Selecione **Baixar valores de configuração** para baixar um arquivo `.txt` contendo as configurações do endpoint do balanceador de carga, tenant, bucket e do usuário raiz.
3. Guarde essas informações em um local seguro.

   Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis após você fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Caso seja solicitado, selecione a caixa de seleção para confirmar que você baixou ou copiou as chaves.
5. Selecione **Continuar** para ir para a etapa de regra e política do ILM.

Etapa 5 de 6: Revisar a regra ILM e a política ILM para S3

As regras de gerenciamento de ciclo de vida da informação (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID. A política de ILM incluída com o StorageGRID cria duas cópias replicadas de todos os objetos. Essa política permanece em vigor até que você ative pelo menos uma nova política.

Passos

1. Analise as informações fornecidas na página.
2. Se você deseja adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. Consulte "Criar regra ILM" e "Use políticas ILM".
3. Selecione **Eu revisei essas etapas e entendi o que preciso fazer**.
4. Selecione a caixa de seleção para indicar que você entende o que fazer a seguir.
5. Selecione **Continuar** para ir para **Resumo**.

Etapa 6 de 6: revisar o resumo

Passos

1. Analise o resumo.
2. Preste atenção aos detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de você se conectar ao cliente S3. Por exemplo, selecionar **Entrar como root** leva você ao Tenant Manager, onde você pode adicionar usuários do tenant, criar buckets adicionais e atualizar as configurações do bucket.
3. Selecione **Concluir**.
4. Configure o aplicativo usando o arquivo que você baixou do StorageGRID ou os valores que você obteve manualmente.

Gerenciar grupos de alta disponibilidade

Saiba mais sobre os grupos de alta disponibilidade do StorageGRID

Os grupos de alta disponibilidade (HA) fornecem conexões de dados altamente disponíveis para clientes S3 e conexões altamente disponíveis para o Grid Manager e o Tenant Manager.

Você pode agrupar as interfaces de rede de vários nós de administração e gateway em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho.

Cada grupo HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Grupos de HA que incluem Gateway Nodes, Admin Nodes ou ambos fornecem conexões de dados altamente disponíveis para clientes S3.
- Grupos de HA que incluem apenas Admin Nodes fornecem conexões altamente disponíveis para o Grid Manager e o Tenant Manager.

- Um grupo de alta disponibilidade (HA) que inclua apenas appliances de serviços e nós de software baseados em VMware pode fornecer conexões de alta disponibilidade para "Locatários S3 que usam o S3 Select". Os grupos de HA são recomendados ao usar S3 Select, mas não são obrigatórios.

Como você cria um grupo de alta disponibilidade?

1. Você seleciona uma interface de rede para um ou mais Admin Nodes ou Gateway Nodes. Você pode usar uma interface Grid Network (eth0), interface Client Network (eth2), interface VLAN ou uma interface de acesso que você adicionou ao nó.

   > Você não pode adicionar uma interface a um grupo HA se ela tiver um endereço IP atribuído por DHCP.

2. Você especifica uma interface para ser a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.
3. Você define a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui de um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos cliente podem usar qualquer um desses endereços IP virtuais (VIP) para se conectar ao StorageGRID.

Para obter instruções, consulte "Configurar grupos de alta disponibilidade".

Qual é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface Primária, que é a primeira interface na ordem de prioridade. Enquanto a interface Primária permanecer disponível, ela será usada quando os clientes se conectarem a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface Primária é a "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade mais baixa para o grupo HA atuam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface Primária (atualmente ativa) fique indisponível.

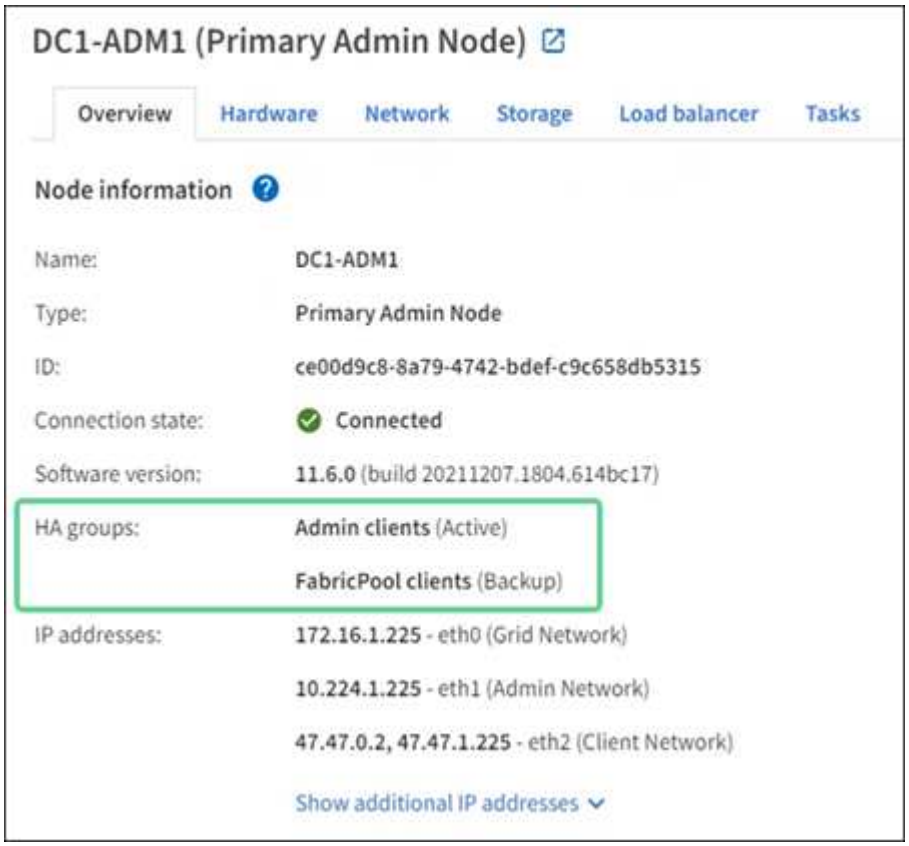
Visualize o status atual do grupo HA de um nó

Para verificar se um nó está atribuído a um grupo HA e determinar seu status atual, selecione **Nós** > ***nó***.

Se a aba **Visão geral** incluir uma entrada para **HA groups**, o nó será atribuído aos HA groups listados. O valor após o nome do grupo representa o status atual do nó no HA group:

- **Ativo**: O grupo HA está atualmente hospedado neste nó.
- **Backup**: O grupo HA não está usando este nó no momento; esta é uma interface de backup.
- **Parado**: O grupo HA não pode ser hospedado neste nó porque o serviço de Alta Disponibilidade (keepalived) foi interrompido manualmente.
- **Falha**: O grupo HA não pode ser hospedado neste nó devido a um ou mais dos seguintes motivos:
  - O serviço Load Balancer (nginx-gw) não está em execução no nó.
  - A interface eth0 ou VIP do nó está inativa.
  - O nó está inativo.

Neste exemplo, o nó de administração principal foi adicionado a dois grupos de HA. Este nó é atualmente a interface ativa para o grupo de clientes de administração 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 transferidos para a primeira interface de backup disponível, seguindo a ordem de prioridade. Se essa interface falhar, os endereços VIP serão transferidos para a próxima interface de backup disponível, e assim por diante.

O failover pode ser acionado por qualquer um destes motivos:

- O nó no qual a interface está configurada fica inativo.
- O nó no qual a interface está configurada perde a conectividade com todos os outros nós por pelo menos 2 minutos.
- A interface ativa fica inativa.
- O serviço Load Balancer é interrompido.
- O serviço de Alta Disponibilidade é interrompido.

> ⓘ O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pelos serviços do Grid Manager ou do Tenant Manager.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos cliente sofram pouco impacto e possam contar com os comportamentos normais de repetição para continuar operando.

Quando a falha é resolvida e uma interface de prioridade mais alta volta a ficar disponível, os endereços VIP são automaticamente movidos para a interface de maior prioridade que estiver disponível.

Como os grupos de alta disponibilidade do StorageGRID proporcionam alta disponibilidade

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 HA pode fornecer conexões administrativas altamente disponíveis ao Grid Manager ou ao Tenant Manager.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3.
- Um grupo HA que contém apenas uma interface permite que você forneça vários endereços VIP e defina explicitamente endereços IPv6.

Um grupo de alta disponibilidade (HA) só pode fornecer alta disponibilidade se todos os nós incluídos no grupo fornecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços que você precisa.

- **Nós de administração**: Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Nós de Gateway**: Incluem o serviço Load Balancer.

Objetivo do grupo HA	Adicione nós deste tipo ao grupo HA
Acesso ao Grid Manager	• Nó de administração principal (**Primary**) • Nós Admin não primários **Nota:** O nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser realizados a partir do nó de administração principal.
Acesso somente ao Tenant Manager	• Nós de administração primários ou não primários
Acesso do cliente S3—serviço de balanceador de carga	• Nós de administração • Nós de gateway
Acesso do cliente S3 para "S3 Select"	• Appliances de serviços • Nós de software baseados em VMware **Nota**: Grupos de alta disponibilidade (HA) são recomendados ao usar o S3 Select, mas não são obrigatórios.

Limitações do uso de grupos de alta disponibilidade com o Grid Manager ou o Tenant Manager

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

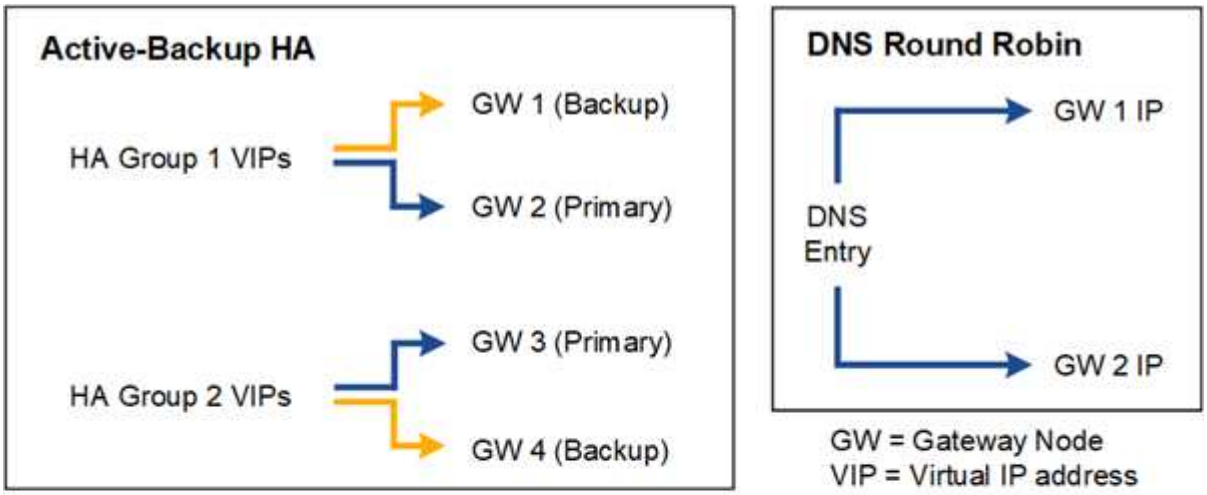
Se você estiver conectado ao Grid Manager ou ao Tenant Manager quando ocorrer uma falha, você será desconectado e precisará entrar novamente para retomar sua tarefa.

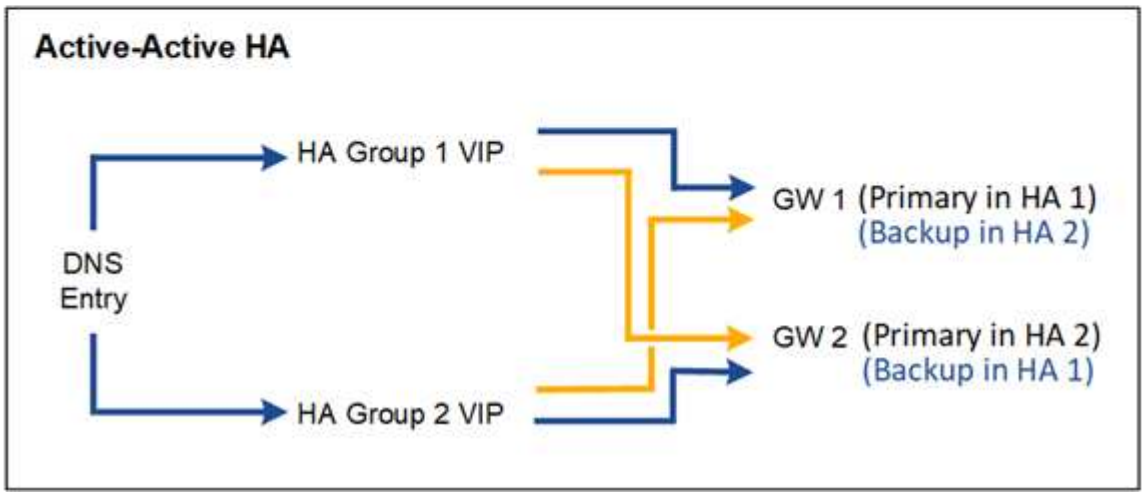
Alguns procedimentos de manutenção não podem ser executados quando o nó de administração primário está indisponível. Durante o failover, você pode usar o Grid Manager para monitorar seu sistema StorageGRID.

Opções de configuração para grupos de alta disponibilidade do StorageGRID

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de alta disponibilidade (HA). Cada opção tem vantagens e desvantagens.

Nos diagramas, azul indica a interface primária no grupo HA e amarelo indica a interface de backup no grupo HA.





A tabela resume os benefícios de cada configuração de alta disponibilidade (HA) mostrada no diagrama.

Configuração	Vantagens	Desvantagens
HA Active-Backup	• Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido.	• Apenas um nó em um grupo HA está ativo. Pelo menos um nó por grupo HA ficará ocioso.

Configuração	Vantagens	Desvantagens
DNS Round Robin	• Aumento da taxa de transferência agregada. • Não há hosts ociosos.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Necessita de uma verificação de integridade implementada pelo cliente.
HA ativo-ativo	• O tráfego é distribuído por vários grupos de HA. • Alto rendimento agregado que escala com o número de grupos HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Necessita de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade no StorageGRID

Você pode configurar grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em Admin Nodes ou Gateway Nodes.

Um sistema StorageGRID pode ter no máximo 255 grupos de HA.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".
- Se você planeja usar uma interface VLAN em um grupo HA, você criou a interface VLAN. Consulte "Configurar interfaces VLAN".
- Se você planeja usar uma interface de acesso para um nó em um grupo de alta disponibilidade (HA), você criou a interface:
  - **Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - **Linux (após instalar o nó)**: "Adicione interfaces de tronco ou de acesso a um nó"
  - **VMware (após a instalação do nó)**: "Adicione interfaces de tronco ou de acesso a um nó"

"Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade (IMT)".

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, você atribui um ou mais endereços VIP ao grupo.

Para que uma interface seja incluída em um grupo de alta disponibilidade (HA), ela deve ser de um nó de Gateway ou de um nó de Admin. Um grupo de HA só pode usar uma interface por nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Rede** > **Grupos de alta disponibilidade**.
2. Selecione **Create**.

Insira os detalhes do grupo HA

Passos

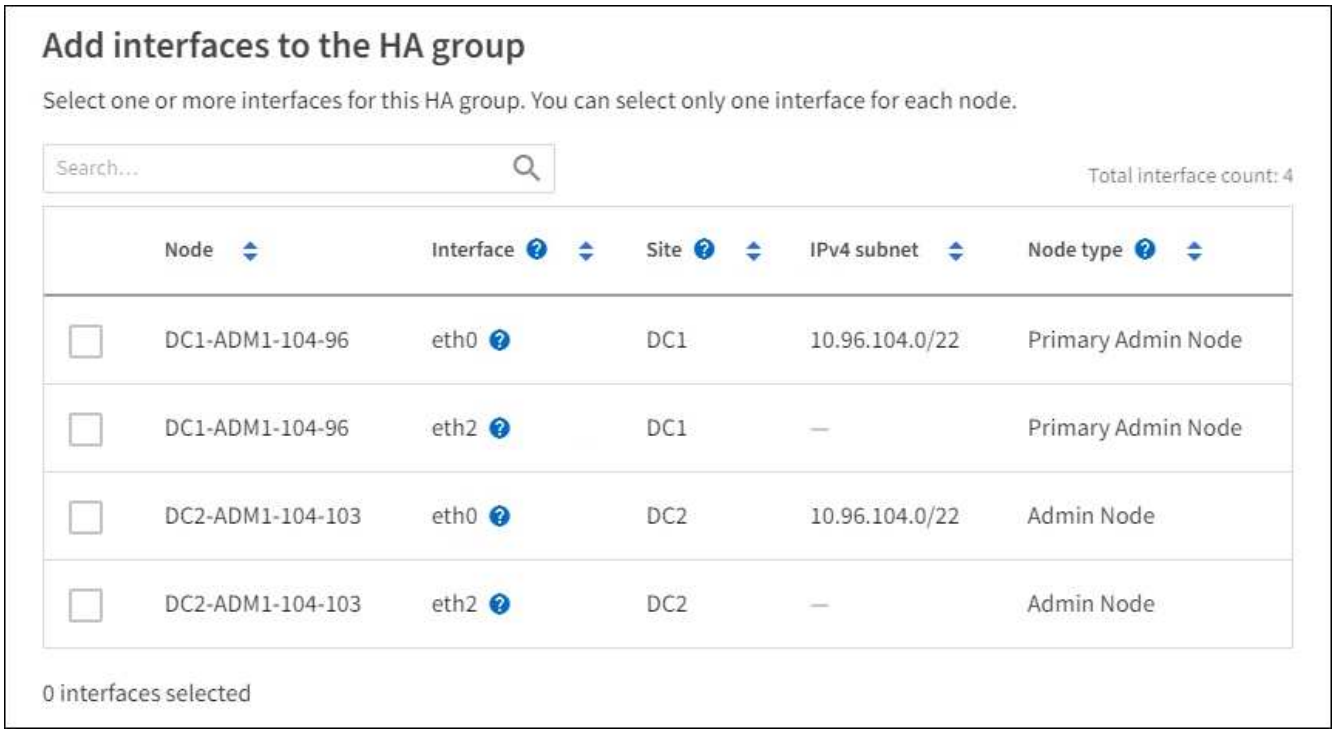
1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **Continue**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a este grupo de HA.

   Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

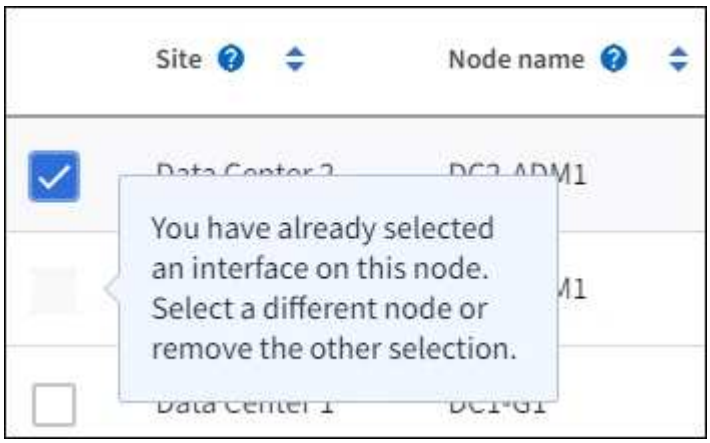


> Após criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo HA for para proteção de alta disponibilidade dos serviços do Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione apenas as interfaces nos Admin Nodes.

- Se o grupo HA for para proteção de alta disponibilidade do tráfego de clientes S3, selecione interfaces em nós de administração, nós de gateway ou em ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Você é lembrado de que, se ocorrer um failover, os serviços fornecidos pelo nó anteriormente ativo podem não estar disponíveis no novo nó ativo. Por exemplo, um nó Gateway de backup não pode fornecer proteção HA dos serviços do nó Admin. Da mesma forma, um nó Admin de backup não pode executar todos os procedimentos de manutenção que o nó Admin primário pode fornecer.
- Se não for possível selecionar uma interface, a caixa de seleção correspondente estará desativada. A dica de ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o valor da sub-rede ou o gateway entrar em conflito com outra interface selecionada.
- Você não pode selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **Continue**.

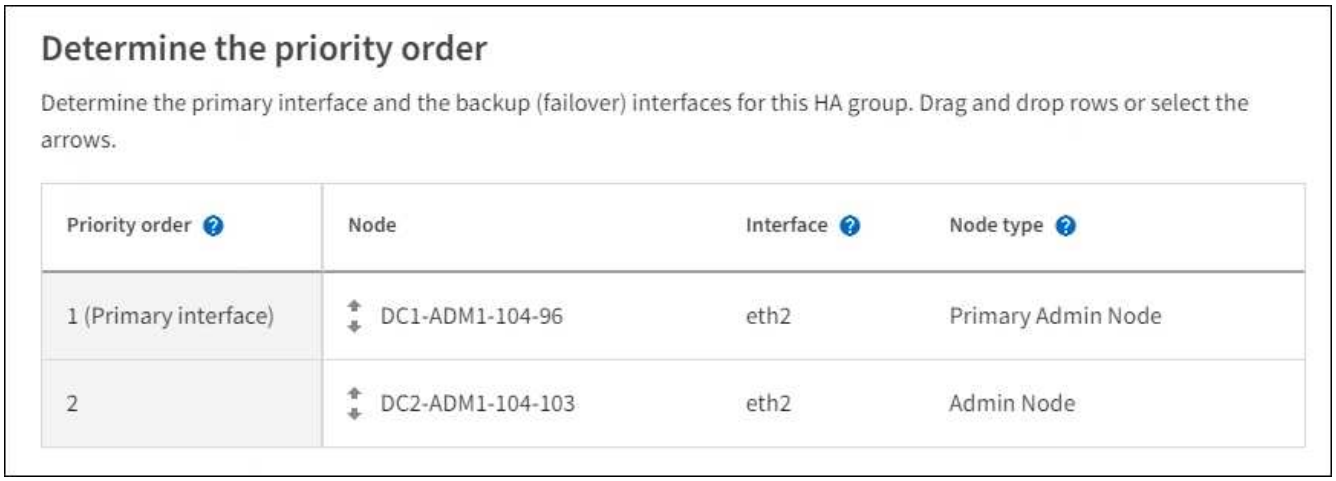
Determine a ordem de prioridade

Se o grupo HA incluir mais de uma interface, você pode determinar qual é a interface Primária e quais são as interfaces de Backup (failover). Se a interface Primária falhar, os endereços VIP são transferidos para a interface disponível de maior prioridade. Se essa interface falhar, os endereços VIP são transferidos para a próxima interface disponível de maior prioridade, e assim por diante.

Passos

1. Arraste as linhas na coluna **Ordem de prioridade** para determinar a interface primária e quaisquer interfaces de backup.

   A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.



Se o grupo HA fornecer acesso ao Grid Manager, você deve selecionar uma interface no Nó de Administração primário para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do Nó de Administração primário.

2. Selecione **Continue**.

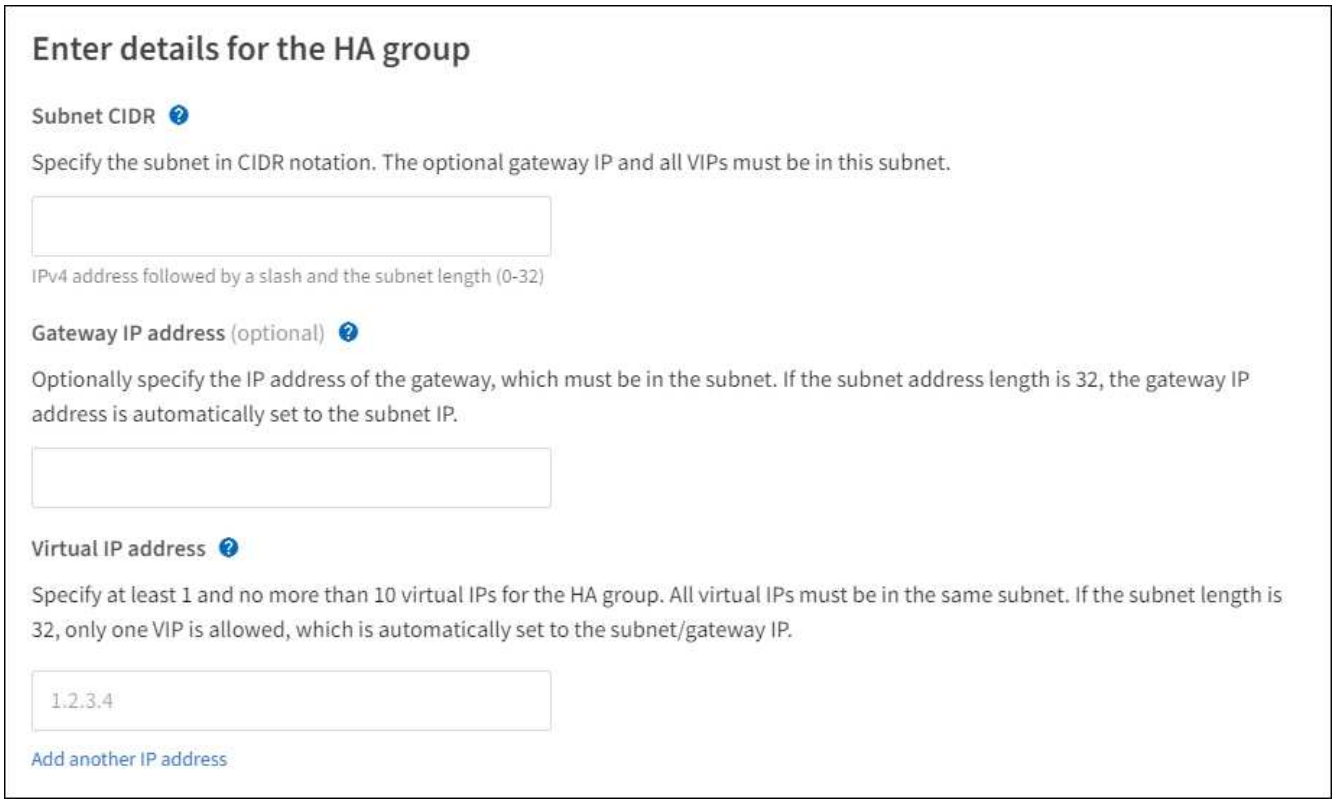
Insira endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR: um endereço IPv4 seguido por uma barra e o comprimento da sub-rede (0-32).

   O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.

   Se você usar um prefixo de 32 bits, o endereço de rede VIP também servirá como endereço de gateway e endereço VIP.



2. Opcionalmente, se algum cliente administrativo ou locatário S3 acessar esses endereços VIP a partir de uma sub-rede diferente, insira o **endereço IP do gateway**. O endereço do gateway deve estar dentro da sub-rede VIP.

   Usuários clientes e administradores usarão este gateway para acessar os endereços IP virtuais.

3. Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

4. Selecione **Criar grupo HA** e selecione **Concluir**.

   O grupo HA foi criado e agora você pode usar os endereços IP virtuais configurados.

Próximos passos

Se você for usar este grupo HA para balanceamento de carga, crie um endpoint de balanceador de carga para determinar a porta e o protocolo de rede e para anexar quaisquer certificados necessários. Consulte "Configurar pontos de extremidade do balanceador de carga".

Editar um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou atualizar endereços IP virtuais.

Por exemplo, pode ser necessário editar um grupo de HA se você quiser remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **Configuração** > **Rede** > **Grupos de alta disponibilidade**.

   A página Grupos de alta disponibilidade mostra todos os grupos de alta disponibilidade existentes.

2. Selecione a caixa de seleção do grupo HA que você deseja editar.
3. Faça uma das seguintes opções, dependendo do que você deseja atualizar:
   - Selecione **Ações** > **Editar endereço IP virtual** para adicionar ou remover endereços VIP.
   - Selecione **Ações** > **Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
   a. Atualize os endereços IP virtuais para o grupo HA.
   b. Selecione **Salvar**.
   c. Selecione **Concluir**.
5. Se você selecionou **Editar grupo HA**:
   a. Opcionalmente, atualize o nome ou a descrição do grupo.
   b. Opcionalmente, selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

      Se o grupo HA fornecer acesso ao Grid Manager, você deve selecionar uma interface no Nó de Administração primário para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do Nó de Administração primário.

   c. Opcionalmente, arraste as linhas para alterar a ordem de prioridade da interface primária e de quaisquer interfaces de backup para este grupo de alta disponibilidade.
   d. Opcionalmente, atualize os endereços IP virtuais.
   e. Selecione **Salvar** e depois selecione **Concluir**.

Remover um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de uma só vez.

Não é possível remover um grupo de alta disponibilidade (HA) se ele estiver vinculado a um endpoint do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de qualquer endpoint do balanceador de carga que o utilize.

Para evitar interrupções nos clientes, atualize todos os aplicativos cliente S3 afetados antes de remover um grupo HA. Atualize cada cliente para se conectar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP que foi configurado para uma interface durante a instalação.

Passos

1. Selecione **Configuração** > **Rede** > **Grupos de alta disponibilidade**.
2. Analise a coluna **Pontos de extremidade do balanceador de carga** para cada grupo de alta disponibilidade que você deseja remover. Se algum ponto de extremidade do balanceador de carga estiver listado:
   a. Acesse **Configuração** > **Rede** > **Pontos de extremidade do balanceador de carga**.
   b. Selecione a caixa de seleção do endpoint.

c. Selecione **Actions** > **Edit endpoint binding mode**.

d. Atualize o modo de vinculação para remover o grupo HA.

e. Selecione **Save changes**.

3. Se nenhum ponto de extremidade do balanceador de carga estiver listado, selecione a caixa de seleção para cada grupo de HA que você deseja remover.
4. Selecione **Ações** > **Remover grupo HA**.
5. Analise a mensagem e selecione **Excluir grupo HA** para confirmar sua seleção.

   Todos os grupos de alta disponibilidade que você selecionou foram removidos. Uma faixa verde de sucesso aparece na página de grupos de alta disponibilidade.

Gerenciar balanceamento de carga

Saiba mais sobre o balanceamento de carga do StorageGRID

Você pode usar o balanceamento de carga para lidar com as cargas de trabalho de ingestão e recuperação de clientes S3.

O que é balanceamento de carga?

Quando um aplicativo cliente salva ou recupera dados de um sistema StorageGRID, StorageGRID utiliza um balanceador de carga para gerenciar a carga de trabalho de ingestão e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão ao distribuir a carga de trabalho entre vários Storage Nodes.

O serviço StorageGRID Load Balancer está instalado em todos os Nós de Administração e em todos os Nós de Gateway e fornece balanceamento de carga na Camada 7. Ele realiza a terminação TLS das solicitações dos clientes, inspeciona as solicitações e estabelece novas conexões seguras com os Nós de Armazenamento.

O serviço de balanceamento de carga em cada nó opera de forma independente ao encaminhar o tráfego do cliente para os nós de armazenamento. Por meio de um processo de ponderação, o serviço de balanceamento de carga direciona mais solicitações para os nós de armazenamento com maior disponibilidade de CPU.

> Embora o serviço StorageGRID Load Balancer seja o mecanismo de balanceamento de carga recomendado, você pode optar por integrar um balanceador de carga de terceiro. Para obter informações, entre em contato com seu representante de contas da NetApp ou consulte "Use balanceadores de carga de terceiros com StorageGRID".

Quantos nós de balanceamento de carga você precisa?

Como prática recomendada geral, cada site em seu StorageGRID deve incluir dois ou mais nós com o serviço Load Balancer. Por exemplo, um site pode incluir dois Gateway Nodes ou tanto um Admin Node quanto um Gateway Node. Certifique-se de que haja infraestrutura de rede, hardware ou virtualização adequada para cada nó de balanceamento de carga, independentemente de você estar usando appliances de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um endpoint de balanceador de carga?

Um endpoint de balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de aplicativos cliente de entrada e saída usarão para acessar os nós que contêm o serviço de Load Balancer. O endpoint também define o tipo de cliente (S3), o modo de vinculação e, opcionalmente, uma lista de tenants permitidos ou bloqueados.

Para criar um endpoint de balanceador de carga, use o Grid Manager ou conclua os assistentes de configuração do S3 e FabricPool:

- "Configurar pontos de extremidade do balanceador de carga"
- "Use o assistente de instalação S3"
- "Utilize o assistente de instalação do FabricPool"

Considerações sobre armazenamento em cache do balanceador de carga

O armazenamento em cache melhora significativamente o desempenho quando uma carga de trabalho opera em um subconjunto de dados e acessa objetos várias vezes. Além disso, o armazenamento em cache fornece acesso remoto ao storage de objetos sem a necessidade de uma implantação completa de grid. O armazenamento em cache do balanceador de carga está disponível apenas para Gateway Nodes.

Ao criar endpoints de balanceamento de carga:

- Habilite armazenamento em cache apenas para cargas de trabalho que são armazenáveis em cache. Cargas de trabalho que acessam dados não armazenados em cache com mais frequência do que dados em cache terão desempenho pior do que se não tivessem sido atendidas pelo cache. Em alguns casos, cargas de trabalho com altas taxas de sobrescrita e remoção também podem exceder a resistência à gravação garantida da unidade.
- Considere adicionar endpoints ou nós adicionais para armazenamento em cache de cargas de trabalho individuais que sejam boas candidatas ao armazenamento em cache.
- Utilize endpoints distintos para cargas de trabalho armazenáveis em cache e não armazenáveis em cache. Essa separação garante que os mecanismos de armazenamento em cache sejam aplicados adequadamente e não interfiram no processamento de dados não armazenáveis em cache.
- Avalie uma carga de trabalho potencialmente armazenável em cache direcionando-a para o endpoint habilitado para cache. Monitore e verifique a taxa de acerto do cache para determinar a adequação da carga de trabalho ao armazenamento em cache. Essa avaliação ajuda a otimizar o desempenho e a garantir o uso eficiente dos recursos de cache.
- "Analisar registros de auditoria" para determinar se uma carga de trabalho existente seria uma boa candidata para armazenamento em cache. Para um determinado período, determine qual porcentagem de GETs é para objetos únicos. Para ser adequada para armazenamento em cache, esse valor deve ser inferior a 50%.

Exemplos de cargas de trabalho que podem ser boas candidatas ao armazenamento em cache

- Lagos de dados
- Computação de alto desempenho (HPC)
- Treinamento de IA/ML
- Rede de entrega de conteúdo (CDN)
- Gerenciamento de ativos de mídia
- Produção de vídeo

- É possível armazenar em cache várias versões de um objeto.
- Operações de leitura de intervalo são suportadas.

Exemplos de cargas de trabalho que não são boas candidatas para armazenamento em cache

- FabricPool
- Aplicativos de backup
- Tierização de storage

Se algum conteúdo a ser servido pelo cache exigir criptografia em repouso, "Ativar criptografia de nó ou unidade"no nó de cache.

Tipos de objetos e solicitações que não serão armazenados em cache

- O `response-content-encoding` parâmetro de consulta
- O `partNumber` parâmetro de consulta
- Cabeçalhos condicionais
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- Solicitações que foram criptografadas em repouso com qualquer um dos seguintes:
  - SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID)
  - SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)
  - Criptografia de objeto armazenado

Qualquer solicitação que não esteja armazenada em cache é encaminhada para um LDR upstream como se o armazenamento em cache não estivesse ativado.

Informações relacionadas

- "Solucione problemas de armazenamento em cache do balanceador de carga"
- Para obter mais informações sobre armazenamento em cache do balanceador de carga, entre em contato com o suporte técnico.

Considerações para a porta

A porta para um endpoint de balanceador de carga é definida como 10433 por padrão para o primeiro endpoint que você criar, 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 de Load Balancer apenas nos Gateway Nodes. Essas portas são reservadas nos Admin Nodes. Se você usar a mesma porta para mais de um endpoint, você deve especificar um modo de vinculação diferente para cada endpoint.

Portas utilizadas por outros serviços da rede não são permitidas. Consulte "Portas internas do StorageGRID".

Considerações sobre o protocolo de rede

Na maioria dos casos, as conexões entre os aplicativos cliente e o StorageGRID devem usar criptografia TLS (Transport Layer Security). Conectar-se ao StorageGRID sem criptografia TLS é suportado, mas não é recomendado, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o endpoint do balanceador de carga do StorageGRID, você deve selecionar **HTTPS**.

Considerações sobre certificados de endpoint de balanceador de carga

Se você selecionar **HTTPS** como protocolo de rede para o ponto de extremidade do balanceador de carga, deverá fornecer um certificado de segurança. Você pode usar qualquer uma destas três opções ao criar o ponto de extremidade do balanceador de carga:

- **Faça o upload de um certificado assinado (recomendado)**. Este certificado pode ser assinado por uma autoridade certificadora (AC) pública ou privada. Usar um certificado de servidor de uma AC pública para proteger a conexão é a melhor prática. Ao contrário dos certificados gerados, os certificados assinados por uma AC podem ser rotacionados sem interrupção, o que pode ajudar a evitar problemas de expiração.

  Você precisa obter os seguintes arquivos antes de criar o endpoint do balanceador de carga:

  - O arquivo de certificado de servidor personalizado.
  - O arquivo de chave privada do certificado de servidor personalizado.
  - Opcionalmente, um pacote de certificados das autoridades certificadoras intermediárias.
- **Gerar um certificado autoassinado**.
- **Use o certificado global do StorageGRID S3**. Você precisa carregar ou gerar uma versão personalizada deste certificado antes de poder selecioná-lo para o endpoint do balanceador de carga. Consulte "Configurar certificados da API S3".

Quais valores você precisa?

Para criar o certificado, você precisa saber todos os nomes de domínio e endereços IP que os aplicativos cliente do S3 usarão para acessar o endpoint.

A entrada **DN do Assunto** (Nome Distinto) para o certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para StorageGRID. Por exemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conforme necessário, o certificado pode usar curingas para representar os nomes de domínio totalmente qualificados de todos os Nós de Administração e Nós de Gateway que executam o serviço de Balanceador de Carga. Por exemplo, `*.storagegrid.example.com` usa o curinga * para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se você planeja usar solicitações no estilo de hospedagem virtual do S3, o certificado também deve incluir uma entrada de **Nome Alternativo** para cada "Nome de domínio do endpoint S3" que você configurou, incluindo quaisquer nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se você usa curingas para nomes de domínio, revise o "Diretrizes de reforço para certificados de servidor".

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados que estão expirando?

Se o certificado usado para proteger a conexão entre o aplicativo S3 e StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas com a expiração do certificado, siga estas boas práticas:

- Monitore atentamente quaisquer alertas que avisem sobre a proximidade da expiração de certificados, como os alertas **Expiração do certificado do endpoint do balanceador de carga** e **Expiração do certificado global do servidor para S3 API**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um endpoint do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de uma Autoridade Certificadora (CA) com assinatura pública. Se você usar um certificado assinado por uma CA, você pode substituir certificados prestes a expirar sem interrupções.
- Se você gerou um certificado StorageGRID autoassinado e esse certificado está prestes a expirar, você deve substituí-lo manualmente tanto no StorageGRID quanto no aplicativo S3 antes que o certificado existente expire.

Considerações sobre o modo de binding

O modo de vinculação permite que você controle quais endereços IP podem ser usados para acessar um endpoint do balanceador de carga. Se um endpoint usa o modo de vinculação, os aplicativos cliente só podem acessá-lo se usarem um endereço IP permitido ou seu respectivo domínio totalmente qualificado (FQDN). Aplicativos cliente que usam qualquer outro endereço IP ou FQDN não podem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de vinculação:

- **Global** (padrão): Os aplicativos cliente podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço 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 domínio totalmente qualificado correspondente) de um grupo HA.
- **Interfaces de nó**. Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó**. Dependendo do tipo de nó selecionado, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway.

Considerações para o acesso do tenant

O acesso de locatários 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 de locatários permitidos ou bloqueados para cada endpoint.

Você pode usar esse recurso para proporcionar um melhor isolamento de segurança entre os locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que materiais ultrassecretos ou altamente confidenciais pertencentes a um locatário permaneçam completamente inacessíveis a outros locatários.

> Para fins de controle de acesso, o locatário é determinado pelas chaves de acesso usadas na solicitação do cliente. Se nenhuma chave de acesso for fornecida como parte da solicitação (como no acesso anônimo), o proprietário do bucket é usado para determinar o locatário.

Exemplo de acesso do tenant

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade de balanceamento de carga, conforme descrito a seguir:
   - Endpoint **público**: utiliza a porta 10443 e permite acesso a todos os locatários.
   - Endpoint **ultrassecreto**: utiliza a porta 10444 e permite acesso somente ao tenant **ultrassecreto**. Todos os outros tenants estão bloqueados de acessar este endpoint.
2. O `top-secret.pdf` está em um bucket pertencente ao tenant **Top secret**.

Para acessar o `top-secret.pdf`, um usuário do tenant **Top secret** pode enviar uma requisição GET para `https://w.x.y.z:10444/top-secret.pdf`. Como esse tenant tem permissão para usar o endpoint 10444, o usuário pode acessar o objeto. No entanto, se um usuário de qualquer outro tenant enviar a mesma requisição para a mesma URL, receberá imediatamente uma mensagem de acesso negado. O acesso é negado mesmo que as credenciais e a assinatura sejam válidas.

Disponibilidade da CPU

O serviço Load Balancer em cada Admin Node e Gateway Node opera de forma independente ao encaminhar o tráfego S3 para os Storage Nodes. Por meio de um processo de ponderação, o serviço Load Balancer direciona mais solicitações para Storage Nodes 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 Storage Nodes recebem um valor de peso base mínimo, mesmo que um nó relate 100% de utilização ou não reporte sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU ficam limitadas ao site onde o serviço Load Balancer está localizado.

Configurar os endpoints do balanceador de carga do StorageGRID

Os endpoints do balanceador de carga determinam as portas e os protocolos de rede que os clientes S3 podem usar ao se conectar ao balanceador de carga do StorageGRID nos nós de Gateway e de Administração. Você também pode usar endpoints para acessar o Grid Manager, o Tenant Manager ou ambos.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".
- Você revisou o "Considerações sobre balanceamento de carga".
- Se você já remapeou uma porta que pretende usar para o endpoint do balanceador de carga, você tem "removeu o remapeamento de porta".

- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os grupos de HA são recomendados, mas não obrigatórios. Consulte "Gerenciar grupos de alta disponibilidade".
- Se o endpoint do balanceador de carga for usado por "Locatários S3 para S3 Select", ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente appliances de serviços e nós de software baseados em VMware são permitidos para os endpoints do balanceador de carga usados para S3 Select.
- Você configurou todas as interfaces VLAN que pretende usar. Consulte "Configurar interfaces VLAN".
- Se você estiver criando um endpoint HTTPS (recomendado), você tem as informações do certificado do servidor.

> As alterações em 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 CA bundle.
  - Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 usarão para acessar o endpoint. Você também precisa saber o assunto (Distinguished Name).
  - Se você deseja usar o certificado da API S3 do StorageGRID (que também pode ser usado para conexões diretas com os Storage Nodes), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. Consulte "Configurar certificados da API S3".

Crie um endpoint de balanceador de carga

Cada endpoint do balanceador de carga do cliente S3 especifica uma porta, um tipo de cliente (S3) e um protocolo de rede (HTTP ou HTTPS). Os endpoints do balanceador de carga da interface de gerenciamento especificam uma porta, um tipo de interface e uma Client Network não confiável.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Rede** > **Pontos de extremidade do balanceador de carga**.
2. Para criar um endpoint para um cliente S3, selecione a guia **Cliente S3**.
3. Para criar um ponto de extremidade para acesso ao Grid Manager, Tenant Manager ou a ambos, selecione a guia **Interface de gerenciamento**.
4. Selecione **Create**.

Insira os detalhes do endpoint

Passos

1. Selecione as instruções apropriadas para inserir os detalhes do tipo de endpoint que você deseja criar.

Cliente S3

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página de endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como valor padrão 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você inserir **80** ou **8443**, o endpoint será configurado apenas nos nós de gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um endpoint S3, e a porta será configurada tanto nos nós de gateway quanto nos nós de administração.
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	O protocolo de rede que os clientes usarão ao se conectar a este endpoint. • Selecione **HTTPS** para comunicação segura e criptografada por TLS (recomendado). Você precisa anexar um certificado de segurança antes de salvar o endpoint. • Selecione **HTTP** para comunicação menos segura e não criptografada. Use HTTP somente para uma grid que não seja de produção.
Ativar armazenamento em cache	Ativar ou desativar "armazenamento em cache nos nós de gateway" para este endpoint do balanceador de carga. Se ocorrerem problemas com armazenamento em cache, consulte "Solucione problemas de armazenamento em cache do balanceador de carga".

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página de endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Grid Manager, o Tenant Manager ou ambos. • Grid Manager: **8443** • Tenant Manager: **9443** • Tanto o Grid Manager quanto o Tenant Manager: **443** **Nota**: Você pode usar essas portas predefinidas ou outras portas disponíveis.

Campo	Descrição
Tipo de interface	Selecione o botão de opção para a interface StorageGRID que você acessará usando este endpoint.
Rede de cliente não confiável	Selecione **Sim** se este endpoint deve ser acessível a redes de clientes não confiáveis. Caso contrário, selecione **Não**. Ao selecionar **Sim**, a porta fica aberta em todas as redes de clientes não confiáveis. **Nota**: Você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis ao criar o endpoint do balanceador de carga.

1. Selecione **Continue**.

Selecione um modo de vinculação

Passos

1. Selecione um modo de vinculação para o endpoint para controlar como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

   Alguns modos de vinculação estão disponíveis tanto para endpoints de cliente quanto para endpoints de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints de cliente)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global**, a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.
Tipo de nó (somente endpoints de cliente)	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

Modo	Descrição
Todos os nós de administração (padrão para endpoints da interface de gerenciamento)	Os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer nó administrativo para acessar este endpoint.

Se mais de um ponto de extremidade usar a mesma porta, StorageGRID usa esta ordem de prioridade para decidir qual ponto de extremidade usar: **IPs virtuais de grupos HA** > **Interfaces de nó** > **Tipo de nó** > **Global**.

Se você estiver criando endpoints de interface de gerenciamento, somente Admin Nodes são permitidos.

2. Se você selecionou **IPs virtuais de grupos HA**, selecione um ou mais grupos HA.

   Se você estiver criando endpoints de interface de gerenciamento, selecione apenas os VIPs associados aos Admin Nodes.

3. Se você selecionou **Interfaces de nó**, selecione uma ou mais interfaces de nó para cada Nó de Administração ou Nó de Gateway que você deseja associar a este endpoint.
4. Se você selecionou **Tipo de nó**, selecione Nós de administração, que inclui tanto o nó de administração principal quanto quaisquer nós de administração não primários, ou Nós de gateway.

Controlar o acesso do tenant

> Um endpoint de interface de gerenciamento só pode controlar o acesso do locatário quando o endpoint tiver a tipo de interface do Tenant Manager.

Passos

1. Na etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets. Você deve selecionar esta opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o endpoint do balanceador de carga para permitir ou bloquear contas específicas.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

2. Se você estiver criando um endpoint **HTTP**, não precisa anexar um certificado. Selecione **Criar** para adicionar o novo endpoint do balanceador de carga. Em seguida, acesse Depois que você terminar. 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 associar ao endpoint.

   O certificado protege as conexões entre os clientes S3 e o serviço Load Balancer no Admin Node ou nos Gateway Nodes.

   - **Carregar certificado**. Selecione esta opção se você tiver certificados personalizados para carregar.
   - **Gerar certificado**. Selecione esta opção se você tiver os valores necessários para gerar um certificado personalizado.
   - **Usar certificado StorageGRID S3**. Selecione esta opção se você quiser usar o certificado global da API S3, que também pode ser usado para conexões diretas com os Storage Nodes.

     Você não pode selecionar esta opção a menos que tenha substituído o certificado padrão da API S3, que é assinado pela CA do grid, por um certificado personalizado assinado por uma autoridade de certificação externa. Consulte "Configurar certificados da API S3".

   - **Usar certificado da interface de gerenciamento**. Selecione esta opção se você quiser usar o certificado global da interface de gerenciamento, que também pode ser usado para conexões diretas com os Admin Nodes.
2. Se você não estiver usando o certificado StorageGRID S3, faça o upload ou gere o certificado.

Carregar certificado

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

- **Certificado do servidor**: o arquivo de certificado personalizado do servidor em codificação PEM.
- **Chave privada do certificado**: O arquivo de chave privada do certificado personalizado do servidor (`.key`).

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote de CA**: Um único arquivo opcional contendo os certificados de cada autoridade certificadora (CA) intermediária. O arquivo deve conter cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado é exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificados.

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

  Por exemplo: `storagegrid_certificate.pem`

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

d. Selecione **Criar**. + O endpoint do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre os clientes S3 ou a interface de gerenciamento e o endpoint.

Gerar certificado

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados para incluir no certificado. Use um * como caractere curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP para incluir no certificado.
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).

Campo	Descrição
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Create**.

O endpoint do balanceador de carga foi criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre os clientes S3 ou a interface de gerenciamento e esse endpoint.

Depois que você terminar

Passos

1. Se você utiliza um DNS, certifique-se de que o DNS inclua um registro para associar o domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para se conectar.

   O endereço IP que você insere no registro DNS depende de você estar usando um grupo HA de nós de balanceamento de carga:

   - Se você configurou um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
   - Se você não estiver usando um grupo de alta disponibilidade (HA), os clientes se conectarão ao serviço StorageGRID Load Balancer usando o endereço IP de um Gateway Node ou Admin Node.

     Você também deve garantir que o registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes curinga.

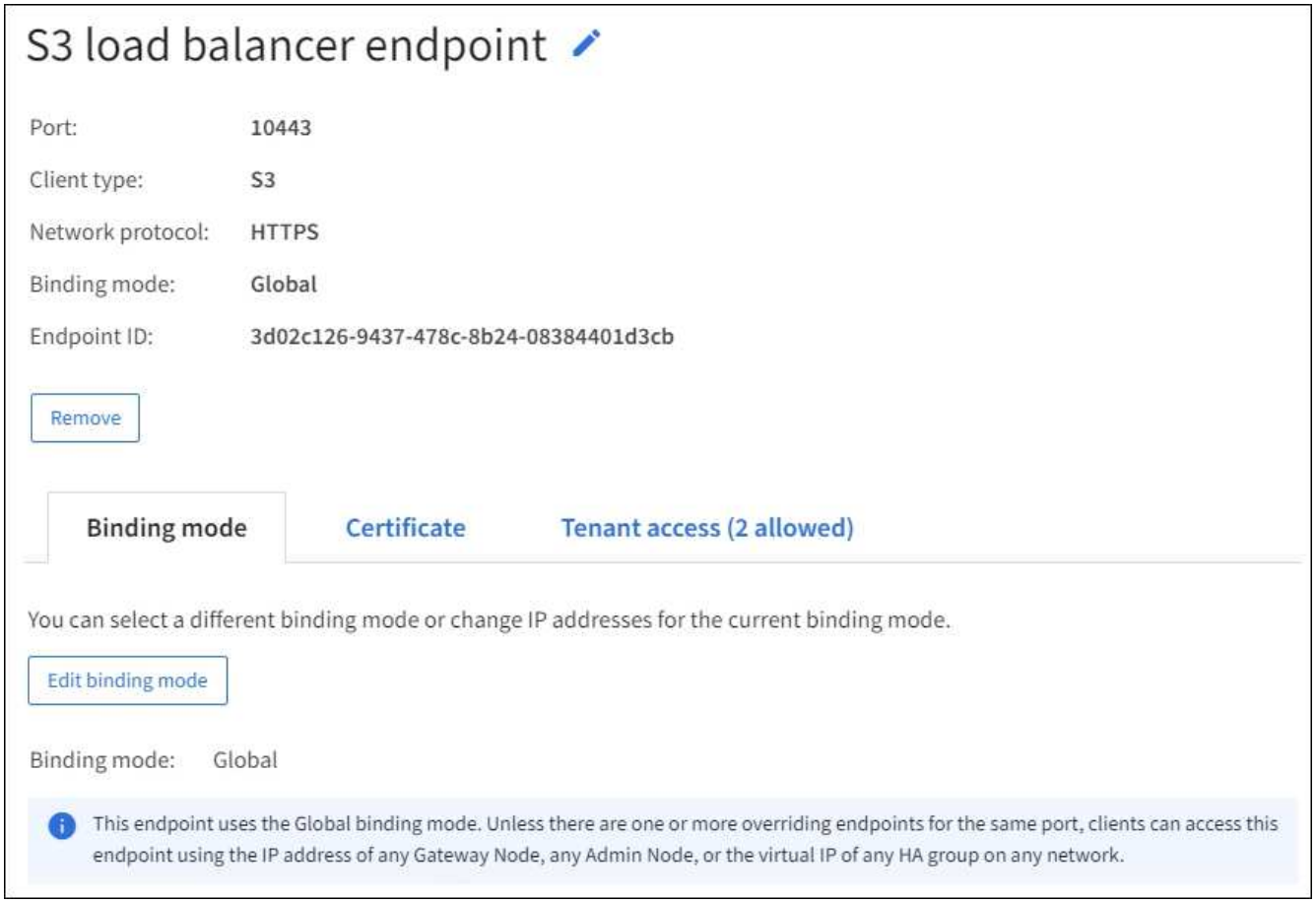
2. Forneça aos clientes S3 as informações necessárias para se conectar ao endpoint:

- Número da porta
- Domínio totalmente qualificado ou endereço IP
- Quaisquer detalhes de certificado necessários

Visualizar e editar endpoints do balanceador de carga

Você pode visualizar detalhes dos endpoints de balanceamento de carga existentes, incluindo os metadados do certificado para um endpoint seguro. Você pode alterar determinadas configurações de um endpoint.

- Para visualizar informações básicas sobre todos os pontos de extremidade do balanceador de carga, consulte as tabelas na página Pontos de extremidade do balanceador de carga.
- Para visualizar todos os detalhes sobre um endpoint específico, incluindo metadados do certificado, selecione o nome do endpoint na tabela. As informações exibidas variam dependendo do tipo de endpoint e de como ele está configurado.



- Para editar um endpoint, use o menu **Ações** na página de endpoints do load balancer.

> Se você perder o acesso ao Grid Manager enquanto estiver editando a porta de um endpoint da interface de gerenciamento, atualize a URL e a porta para recuperar o acesso.

> Após editar um endpoint, pode ser necessário aguardar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu de ações	Página de detalhes
Editar nome do endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione **Ações** > **Editar nome do endpoint**. c. Digite o novo nome. d. Selecione **Salvar**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione **Salvar**.
Editar porta do endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione **Ações** > **Editar porta do endpoint** c. Insira um número de porta válido. d. Selecione **Salvar**.	*n/a*
Editar modo de vinculação de endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione **Actions** > **Edit endpoint binding mode**. c. Atualize o modo de vinculação conforme necessário. d. Selecione **Save changes**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione **Editar modo de vinculação**. c. Atualize o modo de vinculação conforme necessário. d. Selecione **Save changes**.
Editar certificado de endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione **Ações** > **Editar certificado do endpoint**. c. Faça o upload ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. d. Selecione **Save changes**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **Certificate**. c. Selecione **Editar certificado**. d. Faça o upload ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. e. Selecione **Save changes**.
Editar acesso do locatário	a. Selecione a caixa de seleção do endpoint. b. Selecione **Ações** > **Editar acesso do tenant**. c. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça ambos. d. Selecione **Save changes**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **Acesso do locatário**. c. Selecione **Editar acesso do tenant**. d. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça ambos. e. Selecione **Save changes**.

Remover endpoints do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **Ações** ou pode remover um único endpoint na página de detalhes.

> Para evitar interrupções nos clientes, atualize todos os aplicativos cliente S3 afetados antes de remover um endpoint do balanceador de carga. Atualize cada cliente para se conectar usando uma porta atribuída a outro endpoint do balanceador de carga. Certifique-se também de atualizar todas as informações de certificado necessárias.

> Se você perder o acesso ao Grid Manager ao remover um endpoint da interface de gerenciamento, atualize a URL.

- Para remover um ou mais endpoints:
  a. Na página do balanceador de carga, selecione a caixa de seleção para cada endpoint que você deseja remover.
  b. Selecione **Ações** > **Remover**.
  c. Selecione **OK**.
- Para remover um endpoint da página de detalhes:
  a. Na página do balanceador de carga, selecione o nome do endpoint.
  b. Selecione **Remover** na página de detalhes.
  c. Selecione **OK**.

Configurar os nomes de domínio dos endpoints do S3 no StorageGRID

Para dar suporte a solicitações no estilo de hospedagem virtual do S3, você deve usar o Grid Manager para configurar a lista de nomes de domínio de endpoint do S3 aos quais os clientes S3 se conectam.

> O uso de um endereço IP como nome de domínio de endpoint não é suportado. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você confirmou que uma atualização do grid não está em andamento.

> Não faça nenhuma alteração na configuração do nome de domínio enquanto uma atualização da grid estiver em andamento.

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de endpoints do S3, você deve fazer todas as seguintes ações:

- Utilize o Grid Manager para adicionar os nomes de domínio dos endpoints S3 ao sistema StorageGRID.
- Certifique-se de que o "certificado que o cliente usa para conexões HTTPS com o StorageGRID" esteja

assinado para todos os nomes de domínio que o cliente necessita.

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 wildcard Subject Alternative Name (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 se conectar e certifique-se de que os registros façam referência a todos os nomes de domínio de endpoint S3 necessários, incluindo quaisquer nomes curinga.

> Os clientes podem se conectar ao StorageGRID usando o endereço IP de um Gateway Node, um Admin Node ou um Storage Node, ou conectando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conectam à grid para incluir os endereços IP corretos nos registros DNS.

Os clientes que utilizam conexões HTTPS (recomendado) com a grid podem usar qualquer um destes certificados:

- Os clientes que se conectam a um endpoint do balanceador de carga podem usar um certificado personalizado para esse endpoint. Cada endpoint do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de endpoint S3.
- Os clientes que se conectam a um endpoint de balanceador de carga ou diretamente a um Storage Node podem personalizar o certificado global da API S3 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 no estilo virtual-hosted do S3 será desativado.

Adicionar um nome de domínio de endpoint S3

Passos

1. Selecione **Configuração** > **Rede** > **Nomes de domínio de endpoint S3**.
2. Insira o nome de domínio no campo **Nome de domínio 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.
3. Selecione **Salvar**.
4. Certifique-se de que os certificados de servidor que os clientes usam correspondam aos nomes de domínio dos endpoints S3 necessários.
   - Se os clientes se conectarem a um endpoint de balanceador de carga que usa seu próprio certificado, "Atualize o certificado associado ao endpoint".
   - Se os clientes se conectarem a um endpoint de balanceador de carga que usa o certificado da API global do S3 ou diretamente aos nós de armazenamento, "Atualize o certificado global da API S3".
5. Adicione os registros DNS necessários para garantir que as solicitações de nome de domínio dos endpoints 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 conforme o esperado.

Renomear um nome de domínio de endpoint S3

Se você alterar um nome usado por aplicativos S3, as solicitações no estilo virtual-hosted falharão.

Passos

1. Selecione **Configuração** > **Rede** > **Nomes de domínio de endpoint S3**.
2. Selecione o campo do nome de domínio que você deseja editar e faça as alterações necessárias.
3. Selecione **Salvar**.
4. Selecione **Sim** para confirmar sua alteração.

Excluir um nome de domínio de endpoint S3

Se você remover um nome usado por aplicativos S3, as solicitações no estilo virtual-hosted falharão.

Passos

1. Selecione **Configuração** > **Rede** > **Nomes de domínio de endpoint S3**.
2. Selecione o ícone de exclusão ✕ ao lado do nome de domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- "Utilize a API REST S3"
- "Ver endereços IP"
- "Configurar grupos de alta disponibilidade"

Endereços IP e portas para conexões de clientes StorageGRID

Para armazenar ou recuperar objetos, os aplicativos cliente do S3 se conectam ao serviço Load Balancer, que está incluído em todos os Admin Nodes e Gateway Nodes, ou ao serviço Local Distribution Router (LDR), que está incluído em todos os Storage Nodes.

Os aplicativos cliente podem se conectar ao StorageGRID usando o endereço IP de um nó da grade e o número da porta do serviço nesse nó. Opcionalmente, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões altamente disponíveis que usam endereços IP virtuais (VIP). Se você quiser se conectar ao StorageGRID usando um domínio totalmente qualificado (FQDN) em vez de um endereço IP ou VIP, você pode configurar entradas de DNS.

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conectar ao StorageGRID e os endereços IP e portas usados para cada tipo de conexão. Se você já criou endpoints de balanceamento de carga e grupos de alta disponibilidade (HA), consulte Onde encontrar endereços IP para localizar esses valores no Gerenciador de Grid.

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	Porta atribuída ao endpoint do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Nó de administração	Balanceador de carga	Endereço IP do nó de administração	Porta atribuída ao endpoint do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao endpoint do balanceador de carga
Nó de armazenamento	LDR	Endereço IP do Storage Node	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

URLs de exemplo

Para conectar um aplicativo cliente ao endpoint do balanceador de carga de um grupo HA de nós de gateway, use uma URL estruturada conforme mostrado abaixo:

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

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta do endpoint do balanceador de carga for 10443, um aplicativo pode usar a seguinte URL para se conectar ao StorageGRID:

`https://192.0.2.5:10443`

Onde encontrar endereços IP

1. Faça login no Gerenciador de Grade usando um "navegador web compatível".
2. Para encontrar o endereço IP de um nó da grid:
   a. Selecione **Nós**.
   b. Selecione o nó de administração, o nó de gateway ou o nó de armazenamento ao qual você deseja se conectar.
   c. Selecione a guia **Visão geral**.
   d. Na seção Informações do Nó, anote os endereços IP do nó.
   e. Selecione **Mostrar mais** para visualizar os endereços IPv6 e os mapeamentos de interface.

      Você pode estabelecer conexões de aplicativos cliente para qualquer um dos endereços IP da lista:

      - **eth0:** Rede Grid
      - **eth1:** Rede Administrativa (opcional)
      - **eth2:** Rede do cliente (opcional)

      Se você estiver visualizando um Nó de Administração ou um Nó de Gateway e ele for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de alta disponibilidade será exibido em eth2.

3. Para encontrar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **Configuração** > **Rede** > **Grupos de alta disponibilidade**.
   b. Na tabela, observe o endereço IP virtual do grupo HA.
4. Para encontrar o número da porta de um endpoint do Load Balancer:
   a. Selecione **Configuração** > **Rede** > **Pontos de extremidade do balanceador de carga**.
   b. Anote o número da porta do endpoint que você deseja usar.

> Se o número da porta for 80 ou 443, o endpoint é configurado apenas nos Nós de Gateway, porque essas portas estão reservadas nos Nós de Administração. Todas as outras portas são configuradas tanto nos Nós de Gateway quanto nos Nós de Administração.

   c. Selecione o nome do endpoint na tabela.
   d. Confirme se o **Tipo de cliente** (S3) corresponde ao aplicativo cliente que irá utilizar o endpoint.

Gerenciar redes e conexões

Configurar as configurações de rede do StorageGRID

Você pode configurar diversas opções de rede no Grid Manager para otimizar o funcionamento do seu sistema StorageGRID.

Configurar interfaces VLAN

Você pode "criar 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 Admin Nodes e Gateway Nodes. Você pode usar interfaces VLAN em grupos de HA e em endpoints de balanceador de carga para segregar o tráfego de clientes ou de administração 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, tenants, sub-redes de clientes ou endpoints de balanceadores de carga. Essas políticas podem auxiliar na limitação e no monitoramento do tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Grid Manager para configurar e gerenciar redes e conexões do StorageGRID.

Veja "Configurar conexões do cliente S3" para saber como conectar clientes S3.

Redes padrão do StorageGRID

Por padrão, StorageGRID suporta três interfaces de rede por nó de grid, permitindo que você configure a rede para cada nó de grid individual de acordo com seus requisitos de segurança e acesso.

Para obter mais informações sobre topologia de rede, consulte "Diretrizes de networking".

Rede de grid

Obrigatório. A Rede Grid é usada para todo o tráfego interno do StorageGRID. Ela fornece conectividade entre todos os nós da grid, em todos os sites e sub-redes.

Rede de administração

Opcional. A Rede Administrativa é normalmente usada para administração e manutenção do sistema. Também pode ser usada para acesso a protocolo do cliente. A Rede Administrativa é normalmente uma rede privada e não precisa ser roteável entre sites.

Rede de cliente

Opcional. A Client Network é uma rede aberta, normalmente usada para fornecer acesso a aplicativos cliente S3, permitindo que a Grid Network seja isolada e protegida. A Client Network pode se comunicar com qualquer sub-rede acessível por meio do gateway local.

Diretrizes

- Cada nó 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 grid não pode ter mais de uma interface em uma rede.
- É suportado um único gateway por rede, por nó de grid, e ele deve estar na mesma sub-rede que o nó. Você pode implementar roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede é mapeada para uma interface de rede específica.

Rede	Nome da interface
Grid	eth0
Administrador (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conectado a um appliance StorageGRID, portas específicas serão usadas para cada rede. Para obter detalhes, consulte as instruções de instalação do seu appliance.
- A rota padrão é gerada automaticamente para cada nó. Se eth2 estiver habilitada, então 0.0.0.0/0 usa a Rede do Cliente em eth2. Se eth2 não estiver habilitada, então 0.0.0.0/0 usa a Rede Grid em eth0.
- A rede de clientes só se torna operacional depois que o nó da grade se junta à grade
- A Rede Administrativa pode ser configurada durante a implantação do nó da grade para permitir o acesso à interface de 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 trunk a um nó Admin ou Gateway, para poder usar "Interfaces VLAN" para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou, você pode querer adicionar uma interface de acesso para usar em um "grupo de alta disponibilidade (HA)".

Para adicionar interfaces de tronco ou de acesso, consulte o seguinte:

- **VMware (após a instalação do nó)**: "VMware: adicionar interfaces de tronco ou de acesso a um nó"
  - **Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - **Linux (após instalar o nó)**: "Adicione interfaces de tronco ou de acesso a um nó"

> "Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade (IMT)".

Visualizar endereços IP no StorageGRID

Você pode visualizar o endereço IP de cada nó da grade no seu sistema StorageGRID. Em seguida, você pode usar esse endereço IP para fazer login no nó da grade pela linha de comando e executar diversos procedimentos de manutenção.

Antes de começar

Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".

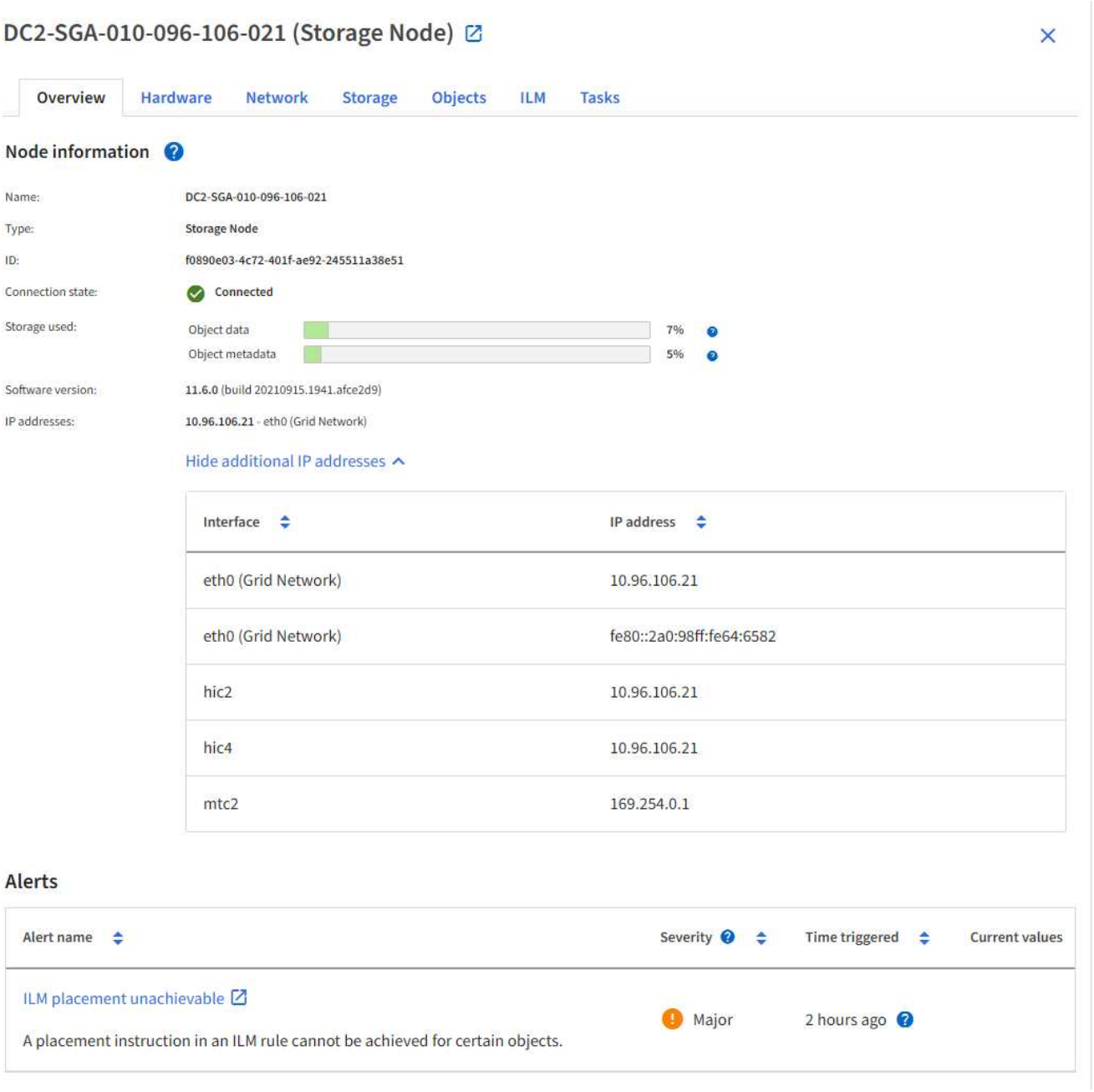
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte "Configurar endereços IP".

Passos

1. Selecione **Nodes** > ***grid node*** > **Overview**.
2. Selecione **Mostrar mais** à direita do título IP Addresses.

   Os endereços IP para esse nó da grid estão listados em uma tabela.



Configurar interfaces VLAN no StorageGRID

Crie interfaces de VLAN (Rede Local Virtual) nos Nós de Administração e Nós de Gateway e use-as em grupos de HA e endpoints de balanceador de carga para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Os nós selecionados no grupo de HA podem usar as interfaces de VLAN para compartilhar até 10 endereços IP virtuais, assim, se um nó falhar, outro nó assume o tráfego de e para os endereços IP virtuais.

Considerações sobre interfaces VLAN

- Você cria uma interface VLAN inserindo um ID de VLAN e escolhendo uma interface principal em um ou mais nós.

- Uma interface principal deve ser configurada como uma interface trunk no switch.
- Uma interface principal pode ser a Grid Network (eth0), a Client Network (eth2) ou uma interface trunk adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface principal para um determinado nó. Por exemplo, você não pode usar tanto a interface Grid Network quanto a interface Client Network no mesmo Gateway Node como interface principal para a mesma VLAN.
- Se a interface VLAN for para tráfego do Nó Administrativo, que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces apenas nos Nós Administrativos.
- Se a interface VLAN for para tráfego de cliente S3, selecione interfaces em Admin Nodes ou Gateway Nodes.
- Se você precisar adicionar interfaces de tronco, consulte os detalhes a seguir:
  - **VMware (após a instalação do nó)**: "VMware: adicionar interfaces de tronco ou de acesso a um nó"
  - **Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - **Linux (após instalar o nó)**: "Adicione interfaces de tronco ou de acesso a um nó"

"Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o "NetApp Ferramenta de Matriz de Interoperabilidade (IMT)".

Criar uma interface VLAN

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".
- Uma interface trunk foi configurada na rede e conectada à máquina virtual ou ao nó Linux. Você sabe o nome da interface trunk.
- Você conhece o ID da VLAN que está configurando.

Sobre esta tarefa

Seu administrador de rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego de cliente ou de administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar a VLAN 100 para tráfego de FabricPool e a VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Gerenciador de Grid para criar interfaces VLAN que permitem que os clientes acessem StorageGRID em uma VLAN específica. Ao criar interfaces VLAN, você especifica o ID da VLAN e seleciona as interfaces pai (trunk) em um ou mais nós.

Acesse o assistente

Passos

1. Selecione **Configuração** > **Rede** > **Interfaces VLAN**.
2. Selecione **Create**.

Insira os detalhes das interfaces VLAN

Passos

1. Especifique o ID da VLAN em sua rede. Você pode inserir qualquer valor entre 1 e 4094.

Os IDs de VLAN não precisam ser únicos. Por exemplo, você pode usar o ID de VLAN 200 para tráfego administrativo em um site e o mesmo ID de VLAN para tráfego de cliente em outro site. Você pode criar interfaces de VLAN separadas com diferentes conjuntos de interfaces pai em cada site. No entanto, duas interfaces de VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó. Se você especificar um ID que já foi usado, uma mensagem aparece.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **Continue**.

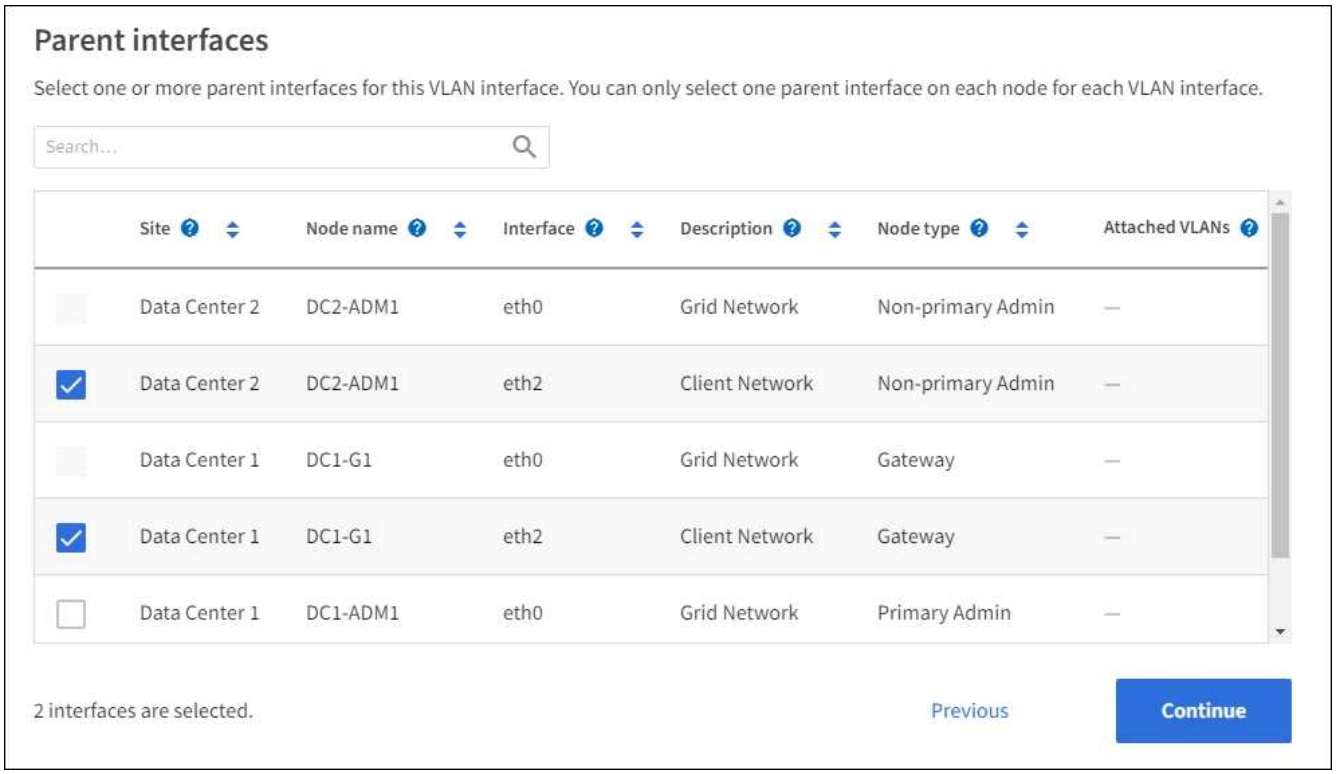
Escolha as interfaces principais

A tabela lista as interfaces disponíveis para todos os Nós de Administração e Nós de Gateway em cada site da sua grid. As interfaces da Admin Network (eth1) não podem ser usadas como interfaces pai e não são exibidas.

Passos

1. Selecione uma ou mais interfaces principais às quais deseja conectar esta VLAN.

   Por exemplo, você pode querer associar uma VLAN à interface Client Network (eth2) para um Gateway Node e um Admin Node.



2. Selecione **Continue**.

Confirme as configurações

Passos

1. Revise a configuração e faça as alterações necessárias.
   - Se você precisar alterar o ID ou a descrição da VLAN, selecione **Inserir detalhes da VLAN** na parte superior da página.

- Se você precisar alterar uma interface principal, selecione **Escolher interfaces principais** na parte superior da página ou selecione **Anterior**.
- Se você precisar remover uma interface principal, selecione a lixeira .

2. Selecione **Salvar**.
3. Aguarde até 5 minutos para que a nova interface apareça como uma opção na página Grupos de alta disponibilidade e seja listada na tabela **Interfaces de rede** para o nó (**Nós** > ***nó interface pai*** > **Rede**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere o ID da VLAN ou a descrição.
- Adicionar ou remover interfaces pai.

Por exemplo, você pode querer remover uma interface principal de uma interface VLAN se planeja desativar o nó associado.

Observe o seguinte:

- Não é possível alterar o ID de uma VLAN se a interface VLAN estiver sendo usada em um grupo HA.
- Não é possível remover uma interface principal se essa interface principal estiver sendo usada em um grupo de alta disponibilidade (HA).

  Por exemplo, suponha que a VLAN 200 esteja associada às interfaces pai nos nós A e B. Se um grupo HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você pode remover a interface pai não utilizada do nó B, mas não pode remover a interface pai utilizada do nó A.

Passos

1. Selecione **Configuração** > **Rede** > **Interfaces VLAN**.
2. Selecione a caixa de seleção da interface VLAN que você deseja editar. Em seguida, selecione **Ações** > **Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **Continuar**.

   Você não pode atualizar um ID de VLAN se a VLAN estiver sendo usada em um grupo de HA.

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **Continuar**.
5. Revise a configuração e faça as alterações necessárias.
6. Selecione **Salvar**.

Remover uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela estiver sendo usada em um grupo HA. Você precisa remover a interface VLAN do grupo HA antes de poder removê-la.

Para evitar interrupções no tráfego de clientes, considere uma das seguintes opções:

- Adicione uma nova interface VLAN ao grupo HA antes de remover esta interface VLAN.

- Crie um novo grupo HA que não utilize esta 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 o final da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e, em seguida, remova a interface antiga do grupo HA. Por fim, exclua a interface VLAN nesse nó.

Passos

1. Selecione **Configuração** > **Rede** > **Interfaces VLAN**.
2. Selecione a caixa de seleção para cada interface VLAN que você deseja remover. Em seguida, selecione **Ações** > **Excluir**.
3. Selecione **Sim** para confirmar sua seleção.

   Todas as interfaces VLAN que você selecionou foram removidas. Uma faixa verde de sucesso aparece na página de interfaces VLAN.

Habilite o CORS do StorageGRID para uma interface de gerenciamento

Como administrador de grid, você pode habilitar o compartilhamento de recursos entre origens (CORS) para solicitações de API de gerenciamento ao StorageGRID, caso deseje que os dados no StorageGRID sejam acessíveis por meio de APIs de gerenciamento em outro domínio.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- O "Permissão de acesso root" fornece acesso a todas as solicitações de configuração CORS.

Sobre esta tarefa

CORS é um mecanismo de segurança que permite que aplicativos web cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você queira criar um painel de monitoramento para StorageGRID no domínio `http://www.example.com`. Ao habilitar o CORS no StorageGRID para `http://www.example.com` e "Grid Manager", o domínio StorageGRID responde às solicitações da API de gerenciamento de grid de `http://www.example.com`.

As solicitações da Management API (mgmt-api) com `application/json` ou `multipart/formdata` solicitações para `Content-Type` são compatíveis com CORS.

Passos

1. No Grid Manager, vá para **CONFIGURAÇÃO** > **Rede** > **Configurações CORS da interface de gerenciamento**.
2. Selecione **Grid Manager**, **Tenant Manager** ou ambas as opções.
   - **Gerenciador de Grid**: Habilita CORS para solicitações de API de gerenciamento de Grid entre domínios diferentes.
   - **Gerenciador de Locatários**: Habilita o CORS para solicitações de API de gerenciamento de locatários entre domínios.
3. Insira a URL do outro domínio no campo **Domínios**.

   Selecione **Adicionar outro domínio** se você quiser ativar o CORS no StorageGRID para mais de um domínio.

4. Selecione **Salvar**.

Informações relacionadas

"Configurar o CORS do StorageGRID para buckets e objetos"

Gerenciar políticas de classificação de tráfego

Políticas de classificação de tráfego no StorageGRID

As políticas de classificação de tráfego permitem que você identifique e monitore diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e no monitoramento do tráfego para aprimorar suas ofertas de qualidade de serviço (QoS).

As políticas de classificação de tráfego são aplicadas aos endpoints no serviço StorageGRID Load Balancer para Gateway Nodes e Admin Nodes. Para criar políticas de classificação de tráfego, você deve já ter criado endpoints de balanceador de carga.

Regras de correspondência

Cada política de classificação de tráfego contém uma ou mais regras de correspondência para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Buckets
- Sub-rede
- Locatário
- Pontos de extremidade do balanceador de carga

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 a uma entidade específica.

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 aplicados individualmente a cada balanceador de carga. Se o tráfego for distribuído simultaneamente entre vários balanceadores de carga, as taxas máximas totais serão um múltiplo dos limites de taxa que você especificar.

> Você pode criar políticas para limitar a largura de banda de agregado ou para limitar a largura de banda por solicitação. No entanto, StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda de agregado podem impor um pequeno impacto adicional no desempenho do tráfego não limitado.

Para limites de largura de banda de agregado ou por solicitação, as solicitações fluem de entrada ou saída na taxa que você definir. StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo de correspondência, é a que será aplicada. A largura de banda consumida pela solicitação não é contabilizada em outras políticas de correspondência menos específicas que contenham políticas de limite de largura de banda de agregado. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta 503 Slow Down para solicitações que excedam qualquer limite de política correspondente.

No Grid Manager, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego que você espera.

Utilize políticas de classificação de tráfego com SLAs

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para impor acordos de nível de serviço (SLAs) que fornecem especificações para capacidade, proteção de dados e desempenho.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para atingir os objetivos de desempenho de cada nível do SLA.

Nível de serviço	Capacidade	Proteção de dados	Desempenho máximo permitido	Custo
Gold	1 PB de armazenamento permitido	Regra de 3 cópias ILM	25 mil solicitações/segundo 5 GB/s (40 Gbps) largura de banda	$$$ por mês
Prata	250 TB de armazenamento permitido	Regra de 2 cópias ILM	10 mil solicitações/segundo 1,25 GB/s (10 Gbps) largura de banda	$$ por mês
Bronze	100 TB de armazenamento permitido	Regra de 2 cópias ILM	5 mil solicitações/segundo 1 GB/s (8 Gbps) largura de banda	$ por mês

Criar políticas de classificação de tráfego do StorageGRID

Você pode criar políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por bucket, expressão regular de bucket, CIDR, endpoint do balanceador de carga ou tenant. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".
- Você criou todos os endpoints de balanceamento de carga que deseja corresponder.
- Você criou todos os tenants que deseja corresponder.

Passos

1. Selecione **Configuração** > **Rede** > **Classificação de tráfego**.
2. Selecione **Create**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.

   Por exemplo, descreva a que se aplica esta política de classificação de tráfego e o que ela vai limitar.

4. Selecione **Adicionar regra** e especifique os seguintes detalhes para criar uma ou mais regras correspondentes para a política. Qualquer política que você criar deve ter pelo menos uma regra correspondente. Selecione **Continuar**.

Campo	Descrição
Tipo	Selecione os tipos de tráfego aos quais a regra de correspondência se aplica. Os tipos de tráfego são bucket, expressão regular de bucket, CIDR, endpoint de balanceador de carga e tenant.
Valor correspondente	Insira o valor que corresponde ao tipo selecionado. • Bucket: insira um ou mais nomes de bucket. • Expressão regular para buckets: insira uma ou mais expressões regulares usadas para corresponder a um conjunto de nomes de buckets. A expressão regular não possui âncora. Use a âncora ^ para corresponder ao início do nome do bucket e a âncora $ para corresponder ao final do nome. A correspondência por expressão regular suporta um subconjunto da sintaxe PCRE (expressão regular compatível com Perl). • CIDR: insira uma ou mais sub-redes IPv4, na notação CIDR, que correspondam à sub-rede desejada. • Ponto de extremidade do balanceador de carga: selecione um nome para o ponto de extremidade. Estes são os pontos de extremidade do balanceador de carga que você definiu no "Configurar pontos de extremidade do balanceador de carga". • Tenant: A correspondência de tenant utiliza o ID da chave de acesso. Se a solicitação não contiver um ID de chave de acesso (por exemplo, acesso anônimo), a propriedade do bucket acessado será usada para determinar o tenant.

Campo	Descrição
Correspondência inversa	Se você deseja corresponder todo o tráfego de rede, *exceto* o tráfego consistente com o Tipo e o Valor de Correspondência que você acabou de definir, selecione a caixa de seleção **Correspondência inversa**. Caso contrário, deixe a caixa de seleção desmarcada. Por exemplo, se você quiser que essa política se aplique a todos os endpoints do balanceador de carga, exceto um, especifique o endpoint do balanceador de carga a ser excluído e selecione **Correspondência inversa**. Para uma política que contenha vários correspondentes, onde pelo menos um seja um correspondente inverso, tome cuidado para não criar uma política que corresponda a todas as solicitações.

5. Opcionalmente, selecione **Adicionar um limite** e selecione os detalhes a seguir para adicionar um ou mais limites para controlar o tráfego de rede correspondente a uma regra.

> ⓘ StorageGRID coleta métricas mesmo que você não adicione nenhum limite, assim você pode 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 largura de banda ou taxa de requisições. **Nota**: Você pode criar políticas para limitar a largura de banda de agregado ou para limitar a largura de banda por solicitação. No entanto, StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Quando a largura de banda de agregado está em uso, a largura de banda por solicitação fica indisponível. Da mesma forma, quando a largura de banda por solicitação está em uso, a largura de banda de agregado fica indisponível. Os limites de largura de banda de agregado podem impor um pequeno impacto adicional no desempenho do tráfego não limitado. Para limites de largura de banda, o StorageGRID aplica a política que melhor corresponde ao tipo de limite definido. Por exemplo, se você tiver uma política que limita o tráfego em apenas uma direção, o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais com limites de largura de banda. O StorageGRID implementa as "melhores" correspondências para limites de largura de banda na seguinte ordem: • Endereço IP (máscara /32) • Nome exato do bucket • Expressão regular de bucket • Locatário • Endpoint • Correspondências CIDR não exatas (não /32) • Correspondências inversas

Campo	Descrição
Aplica-se a	Se este limite se aplica a solicitações de leitura do cliente (GET ou HEAD) ou a solicitações de escrita (PUT, POST ou DELETE).
Valor	O valor ao qual o tráfego de rede será limitado, com base na unidade que você selecionar. Por exemplo, insira 10 e selecione MiB/s para impedir que o tráfego de rede correspondente a 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 de unidades, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e, em seguida, selecione **User Preferences**.
Unidade	A unidade que descreve o valor que você inseriu.

Por exemplo, se você quiser criar um limite de largura de banda de 4 GB/s para um nível de SLA, crie dois limites de largura de banda de agregado: GET/HEAD em 4 GB/s e PUT/POST/DELETE em 4 GB/s.

6. Selecione **Continue**.
7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando você estiver satisfeito com a política, selecione **Salvar e continuar**.

   O tráfego de cliente S3 agora é tratado de acordo com a política de classificação de tráfego.

Depois que você terminar

"Visualizar métricas de tráfego de rede"para verificar se as políticas estão aplicando os limites de tráfego que você espera.

Editar uma política de classificação de tráfego do StorageGRID

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Passos

1. Selecione **Configuração** > **Rede** > **Classificação de tráfego**.

   A página de políticas de classificação de tráfego aparece e as políticas existentes são listadas em uma tabela.

2. Edite a política usando o menu Ações ou a página de detalhes. Veja "criar políticas de classificação de tráfego" o que inserir.

Menu de ações

a. Selecione a caixa de seleção da política.

b. Selecione **Ações** > **Editar**.

Página de detalhes

a. Selecione o nome da política.

b. Selecione o botão **Editar** ao lado do nome da policy.

3. Na etapa "Inserir nome da política", você pode opcionalmente editar o nome ou a descrição da política e selecionar "Continuar".
4. Na etapa Adicionar regras de correspondência, opcionalmente adicione uma regra ou edite o **Tipo** e o **Valor de correspondência** da regra existente e selecione **Continuar**.
5. Na etapa Definir limites, opcionalmente, adicione, edite ou exclua um limite e selecione **Continuar**.
6. Analise a política atualizada e selecione **Salvar e continuar**.

   As alterações feitas na política foram salvas e o tráfego de rede agora é gerenciado 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 que você espera.

Excluir uma política de classificação de tráfego do StorageGRID

Você pode excluir uma política de classificação de tráfego se não precisar mais dela. Certifique-se de excluir a política correta, pois uma política não pode ser recuperada quando excluída.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Passos

1. Selecione **Configuração** > **Rede** > **Classificação de tráfego**.

   A página de políticas de classificação de tráfego aparece com as políticas existentes listadas em uma tabela.

2. Exclua a política usando o menu Ações ou a página de detalhes.

Menu de ações

a. Selecione a caixa de seleção da política.

b. Selecione **Ações** > **Remover**.

Página de detalhes da política

a. Selecione o nome da política.

b. Selecione o botão **Remover** ao lado do nome da política.

3. Selecione **Sim** para confirmar que você deseja excluir a política.

   A política foi excluída.

Visualize métricas de tráfego de rede no StorageGRID

Você pode monitorar o tráfego de rede visualizando os gráficos disponíveis na página de políticas de classificação de tráfego.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Acesso à raiz ou permissão para contas de locatário".

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode visualizar métricas do serviço de balanceador de carga para determinar se a política está limitando o tráfego na rede com sucesso. Os dados nos gráficos podem ajudar você a determinar se é necessário ajustar a política.

Mesmo que não sejam definidos limites para uma política de classificação de tráfego, métricas são coletadas e os gráficos fornecem informações úteis para a compreensão das tendências de tráfego.

Passos

1. Selecione **Configuração** > **Rede** > **Classificação de tráfego**.

   A página de políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

2. Selecione o nome da política de classificação de tráfego para a qual você deseja visualizar métricas.
3. Selecione a guia **Métricas**.

   Os gráficos da política de classificação de tráfego são exibidos. Os gráficos mostram métricas apenas para o tráfego que corresponde à política selecionada.

   Os seguintes gráficos estão incluídos na página.

   - Taxa de requisições: Este gráfico mostra a quantidade de largura de banda correspondente a esta política, gerenciada por todos os balanceadores de carga. Os dados recebidos incluem os cabeçalhos de todas as requisições e o tamanho dos dados do corpo para as respostas que têm dados no corpo. Os dados enviados incluem os cabeçalhos de resposta de todas as requisições e o tamanho dos dados do corpo de resposta para as requisições que incluem dados no corpo da resposta.

     > Quando as solicitações são concluídas, este gráfico mostra apenas a utilização de largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode ser diferente dos valores apresentados neste gráfico.

   - Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual as solicitações que correspondem a esta política estão retornando erros (código de status HTTP >= 400) aos clientes.
   - Duração média das solicitações (sem erros): este gráfico fornece a duração média das solicitações bem-sucedidas que correspondem a esta política.
   - Utilização de largura de banda da política: Este gráfico mostra a quantidade de largura de banda correspondente a esta política, gerenciada por todos os balanceadores de carga. Os dados recebidos incluem os cabeçalhos de todas as requisições e o tamanho do corpo das respostas que contêm

dados no corpo. Os dados enviados incluem os cabeçalhos de todas as requisições e o tamanho do corpo das respostas que contêm dados no corpo.

4. Posicione o cursor sobre um gráfico de linhas para ver um pop-up com os valores de uma parte específica do gráfico.
5. Selecione **Grafana dashboard** logo abaixo do título Métricas para visualizar todos os gráficos de uma política. Além dos quatro gráficos da guia **Métricas**, você pode visualizar mais dois gráficos:
   - Taxa de requisições de escrita por tamanho do objeto: a taxa para requisições PUT/POST/DELETE que correspondem a esta política. O posicionamento em uma célula individual mostra as taxas por segundo. As taxas exibidas na visualização ao passar o mouse são truncadas para contagens inteiras e podem mostrar 0 quando houver requisições diferentes de zero no bucket.
   - Taxa de requisições de leitura por tamanho do objeto: a taxa para requisições GET/HEAD que correspondem a esta política. O posicionamento em uma célula individual mostra as taxas por segundo. As taxas exibidas na visualização ao passar o mouse são truncadas para contagens inteiras e podem mostrar 0 quando houver requisições diferentes de zero no bucket.
6. Alternativamente, acesse os gráficos no menu **Suporte**.
   a. Selecione **Suporte** > **Ferramentas** > **Métricas**.
   b. Selecione **Política de Classificação de Tráfego** na seção **Grafana**.
   c. Selecione a política no menu no canto superior esquerdo da página.
   d. Posicione o cursor sobre um gráfico para ver uma janela pop-up que mostra a data e a hora da amostra, os tamanhos dos objetos que são agregados na contagem e o número de solicitações por segundo durante esse período.

      As políticas de classificação de tráfego são identificadas por seus IDs. Os IDs das políticas estão listados na página de 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.

Cifras suportadas para conexões TLS de saída no StorageGRID

O sistema StorageGRID suporta um conjunto limitado de suítes de cifras para conexões Transport Layer Security (TLS) com os sistemas externos usados para federação de identidades e Cloud Storage Pools.

Versões compatíveis do TLS

StorageGRID oferece suporte a TLS 1.2 e TLS 1.3 para conexões com sistemas externos usados para federação de identidades e Cloud Storage Pools.

Os algoritmos de criptografia TLS suportados para uso com sistemas externos foram selecionados para garantir a compatibilidade com uma ampla gama de sistemas externos. A lista é maior do que a lista de algoritmos de criptografia suportados para uso com aplicativos cliente S3. Para configurar os algoritmos de criptografia, acesse **Configuração** > **Segurança** > **Configurações de segurança** e selecione **Políticas de TLS e SSH**.

> 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 seu representante de conta da NetApp se você tiver solicitações específicas sobre essas configurações.

Benefícios das conexões HTTP ativas, ociosas e simultâneas no StorageGRID

A forma como você configura as conexões HTTP pode afetar o desempenho do sistema StorageGRID. As configurações variam dependendo se a conexão HTTP está ativa ou ociosa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

Benefícios de manter conexões HTTP ociosas abertas

Mantenha as conexões HTTP abertas quando os aplicativos cliente estiverem ociosos para permitir transações posteriores. Mantenha uma conexão HTTP ociosa aberta por no máximo 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que permanecer aberta e ociosa por mais de 10 minutos.

Conexões HTTP abertas e ociosas oferecem os seguintes benefícios:

- Latência reduzida desde o momento em que o sistema StorageGRID determina que precisa realizar uma transação HTTP até o momento em que o sistema StorageGRID pode realizar a transação

  A principal vantagem é a latência reduzida, especialmente considerando o tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados ao preparar o algoritmo de inicialização lenta do TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de diversas classes de falhas que interrompem a conectividade entre o aplicativo cliente e o sistema StorageGRID

Decida por quanto tempo manter uma conexão ociosa aberta, equilibrando os benefícios do slow start e a alocação de recursos.

Benefícios das conexões HTTP ativas

Para conexões diretas com Storage Nodes, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP execute transações continuamente.

Determinar a duração máxima em que uma conexão deve permanecer aberta é um equilíbrio entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de clientes com Storage Nodes, limitar as conexões HTTP ativas oferece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

  Com o tempo, uma conexão HTTP pode deixar de ser a ideal à medida que os requisitos de balanceamento de carga mudam. O sistema apresenta o melhor desempenho em balanceamento de carga quando os aplicativos cliente estabelecem uma conexão HTTP separada para cada transação, mas esse método anula os valiosos ganhos associados às conexões persistentes.

- Permite que aplicativos cliente direcionem transações HTTP para serviços LDR que tenham espaço disponível.
- Permite o início dos procedimentos de manutenção.

  Alguns procedimentos de manutenção só começam depois que todas as conexões HTTP em andamento forem concluídas.

Para conexões de cliente com o serviço de Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção comecem prontamente. Se a duração das conexões de cliente não for limitada, pode levar vários minutos para que as conexões ativas sejam encerradas automaticamente.

Benefícios das conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP abertas com o sistema StorageGRID para permitir o paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de diversos fatores.

As conexões HTTP simultâneas oferecem os seguintes benefícios:

- Latência reduzida

  As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Aumento da taxa de transferência

  O sistema StorageGRID pode executar transações paralelas e aumentar a capacidade de processamento agregada de transações.

Os aplicativos cliente devem estabelecer múltiplas conexões HTTP. Quando um aplicativo cliente precisa realizar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID apresenta uma taxa de transferência máxima diferente para transações e conexões simultâneas. A taxa de transferência máxima depende de computação, rede, recursos de storage, links WAN e do número de servidores, serviços e aplicativos que o sistema StorageGRID suporta.

Os sistemas StorageGRID geralmente suportam vários aplicativos cliente. Leve isso em consideração ao determinar o número máximo de conexões simultâneas. Se o aplicativo cliente consistir em várias entidades de software que estabelecem conexões com o sistema StorageGRID, some todas as conexões entre as entidades. Talvez seja necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do StorageGRID afeta o número máximo de transações e conexões simultâneas que o sistema pode suportar.
- Aplicações cliente que interagem com o sistema StorageGRID através de uma rede com largura de banda limitada podem ter que reduzir o grau de concorrência para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos cliente compartilham o sistema StorageGRID, pode ser necessário reduzir o grau de concorrência para evitar exceder os limites do sistema.

Separação de pools de conexões HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar quanto do pool usar para cada uma. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos cliente podem gerar cargas de trabalho com predominância de recuperação (leitura) ou de armazenamento (gravação). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar a quantidade de cada pool dedicada a transações de leitura ou gravação.

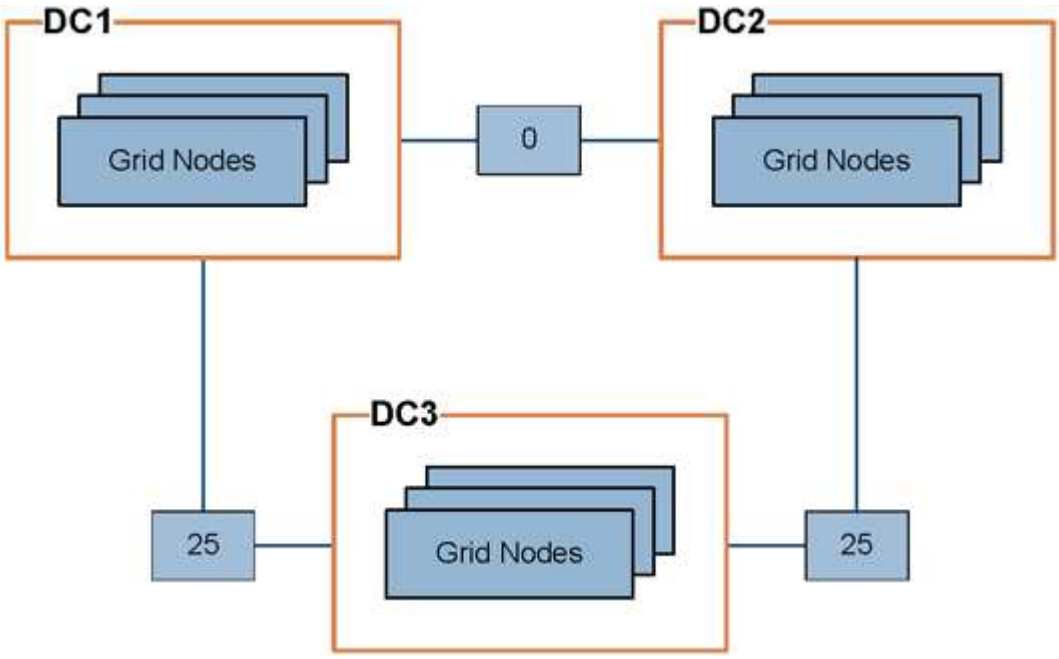
Gerencie os custos de link no StorageGRID

Os custos de enlace permitem que você priorize qual site de data center fornece um serviço solicitado quando existem dois ou mais sites de data center. Você pode ajustar os custos de enlace para refletir a latência entre os sites.

O que são custos de enlace?

- Os custos de enlace são usados para priorizar qual cópia do objeto é usada para realizar a recuperação do objeto.
- Os custos de conexão são usados pela API de Gerenciamento de Grid e pela API de Gerenciamento de Inquilinos para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço Load Balancer nos nós de administração e nos nós de gateway para direcionar as conexões dos clientes. Consulte "Considerações sobre balanceamento de carga".

O diagrama mostra uma grade de três sites com custos de enlace configurados entre os sites:



- O serviço Load Balancer nos nós de administração e nos nós de gateway distribui igualmente as conexões dos clientes para todos os nós de armazenamento no mesmo site do data center e para quaisquer sites de data center com um custo de link de 0.

  No exemplo, um nó de gateway no data center site 1 (DC1) distribui igualmente as conexões de clientes para os nós de armazenamento no DC1 e para os nós de armazenamento no DC2. Um nó de gateway no

DC3 envia conexões de clientes apenas para os nós de armazenamento no DC3.

- Ao recuperar um objeto que existe em múltiplas cópias replicadas, StorageGRID recupera a cópia no data center que possui o menor custo de link.

  No exemplo, se um aplicativo cliente no DC2 recuperar um objeto que está armazenado tanto no DC1 quanto no DC3, o objeto será recuperado do DC1, porque o custo do link do DC1 para o DC2 é 0, que é menor que o custo do link do DC3 para o DC2 (25).

Os custos de enlace são números relativos arbitrários, sem uma unidade de medida específica. Por exemplo, um custo de enlace de 50 é usado menos preferencialmente do que um custo de enlace de 25. A tabela mostra os custos de enlace mais comuns.

Link	Custo do link	Notas
Entre sites físicos de data center	25 (padrão)	Data centers conectados por um link WAN.
Entre sites de data center lógicos na mesma localização física	0	Centros de dados lógicos no mesmo edifício físico ou campus conectados por uma LAN.

Atualizar custos do link

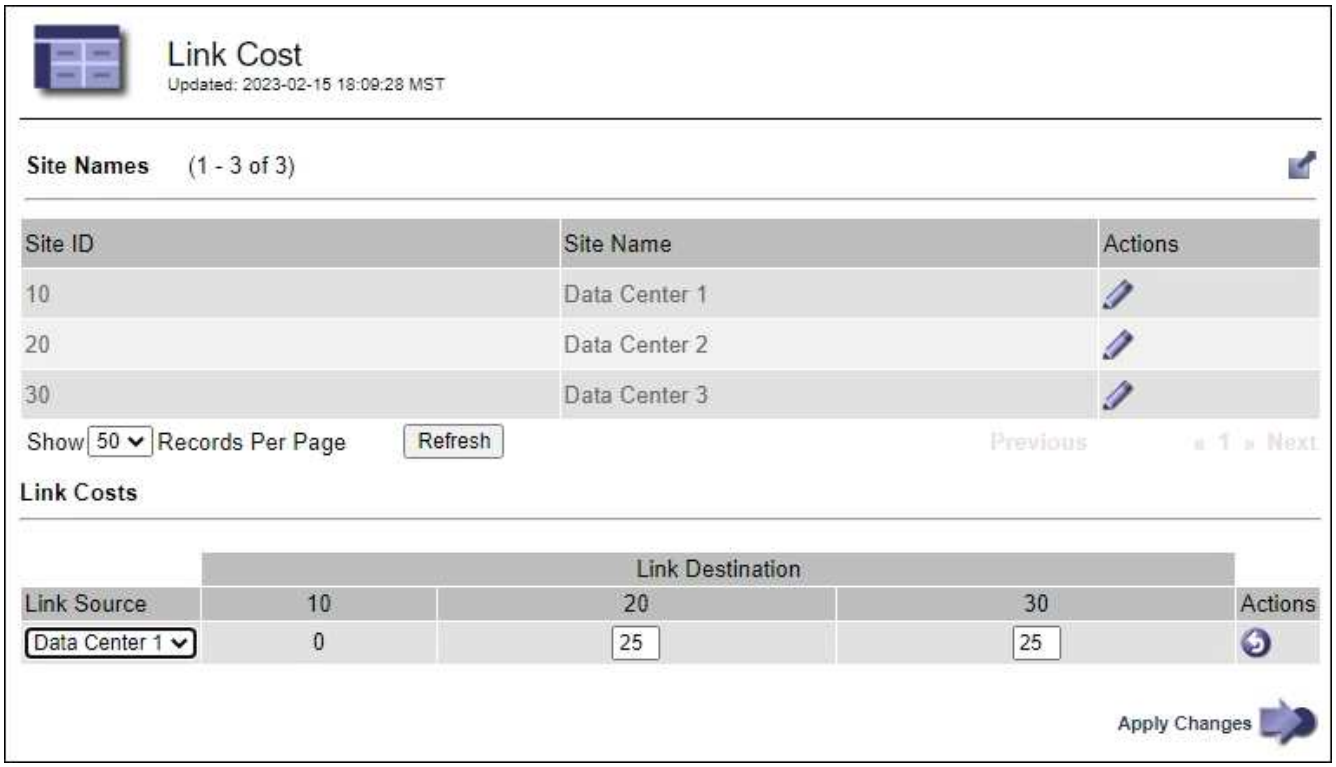
Você pode atualizar os custos de conexão entre sites do data center para refletir a latência entre eles.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Outra permissão de configuração da grid".

Passos

1. Selecione **Support** > **Other** > **Link cost**.



2. Selecione um site em **Origem do link** e insira um valor de custo entre 0 e 100 em **Destino do link**.

   Não é possível alterar o custo do link se a origem for a mesma que o destino.

   Para cancelar as alterações, selecione **Reverter**.

3. Selecione **Aplicar alterações**.

Use o AutoSupport

Saiba mais sobre AutoSupport no StorageGRID

O recurso AutoSupport permite que o StorageGRID envie pacotes de integridade e status para o suporte técnico da NetApp.

Usar o AutoSupport ajuda a resolver problemas mais rapidamente. O suporte técnico pode monitorar as necessidades de storage do seu sistema e ajudar a determinar se você precisa adicionar novos nós ou sites. Opcionalmente, o AutoSupport pode enviar pacotes para um destino adicional.

StorageGRID possui dois tipos de AutoSupport:

- **StorageGRID AutoSupport** relata problemas de software do StorageGRID. Ativado por padrão quando você instala o StorageGRID pela primeira vez. Você pode "alterar a configuração padrão do AutoSupport" se necessário.

> Se StorageGRID AutoSupport não estiver ativado, uma mensagem será exibida no painel do 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 seu navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

- **O hardware do appliance AutoSupport** relata problemas no appliance StorageGRID. Você deve "configurar hardware AutoSupport em cada appliance".

O que é Active IQ?

Active IQ é um consultor digital baseado na nuvem que aproveita a análise preditiva e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações contínuas de risco, alertas preditivos, orientações prescritivas e ações automatizadas ajudam você a prevenir problemas antes que eles ocorram, resultando em melhor saúde do sistema e maior disponibilidade do sistema.

Se você deseja usar os painéis e funcionalidades do Active IQ no site de suporte da NetApp, você deve habilitar o AutoSupport.

"Documentação do Active IQ Digital Advisor"

Informações incluídas no pacote AutoSupport

Um pacote AutoSupport contém os seguintes arquivos e detalhes.

Nome do arquivo	Campos	Descrição
AUTOSUPPORT-HISTORY.XML	AutoSupport Número de sequência + Destino para este AutoSupport + Status da entrega + Tentativas de entrega + AutoSupport Assunto + URI da entrega + Último erro + AutoSupport Nome do arquivo PUT + Hora de geração + Tamanho compactado do Autosupport + Tamanho descompactado do Autosupport + Tempo total de coleta (ms)	AutoSupport arquivo de histórico.
AUTOSUPPORT.XML	Nó + Protocolo para contatar o suporte + URL de suporte para HTTP/HTTPS + Endereço de suporte + AutoSupport OnDemand State + AutoSupport OnDemand Server URL + AutoSupport OnDemand Polling Interval	Arquivo de status do AutoSupport. Fornece detalhes do protocolo usado, URL e endereço do suporte técnico, intervalo de sondagem e se o OnDemand AutoSupport está ativado ou desativado.

Nome do arquivo	Campos	Descrição
BUCKETS.XML	ID do bucket + ID da conta + versão da build + configuração de restrição de localização + conformidade ativada + configuração de conformidade + S3 Object Lock ativado + configuração de S3 Object Lock + configuração de consistência + CORS ativado + configuração de CORS + último horário de acesso ativado + política ativada + configuração de política + notificações ativadas + configuração de notificações + Cloud Mirror ativado + configuração de Cloud Mirror + busca ativada + configuração de busca + marcação de bucket ativada + configuração de marcação de bucket + configuração de versionamento	Fornece detalhes de configuração e estatísticas no nível do bucket. Exemplos de configurações de bucket incluem serviços de plataforma, conformidade e consistência do bucket.
GRID-CONFIGURATIONS.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de configuração de toda a grid. Contém informações sobre certificados da grid, espaço reservado de metadados, configurações de toda a grid (conformidade, S3 Object Lock, compactação de objetos, alertas, syslog e configuração ILM), detalhes do perfil de codificação de apagamento, nome DNS e "Nome da NMS".
GRID-SPEC.XML	Especificações do grid, XML bruto	Utilizado para configurar e implementar StorageGRID. Contém especificações da grid, endereço IP do servidor NTP, endereço IP do servidor DNS, topologia de rede e perfis de hardware dos nós.
GRID-TASKS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de status das tarefas da grade (procedimentos de manutenção). Fornece detalhes das tarefas ativas, finalizadas, concluídas, com falha e pendentes da grade.
GRID.JSON	Grid + Revisão + Versão do Software + Descrição + Licença + Senhas + DNS + NTP + Sites + Nós	Informações do grid.

Nome do arquivo	Campos	Descrição
ILM-CONFIGURATION.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Lista de atributos para configurações ILM.
ILM-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de métricas do ILM. Contém as taxas de avaliação do ILM para cada nó e métricas em toda a grid.
ILM.XML	XML bruto do ILM	Arquivo de política ativa do ILM. Contém detalhes sobre as políticas ativas do ILM, como ID do pool de storage, comportamento de ingestão, filtros, regras e descrição.
LOG.TGZ	*n/a*	Arquivo de log para download. Contém `bycast-err.log` e `servermanager.log` de cada nó.
MANIFEST.XML	Ordem de coleta + AutoSupport content filename para esses dados + descrição deste item de dados + número de bytes coletados + tempo gasto na coleta + status deste item de dados + descrição do erro + AutoSupport tipo de conteúdo para esses dados	Contém metadados do AutoSupport e breves descrições de todos os arquivos AutoSupport.
NMS-ENTITIES.XML	Índice de atributo + OID da entidade + ID do nó + ID do modelo do dispositivo + Versão do modelo do dispositivo + Nome da entidade	Agrupa entidades e serviços no "Árvore NMS". Fornece detalhes da topologia da grade. O nó pode ser determinado com base nos serviços em execução no nó.
OBJECTS-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Estado do objeto, incluindo o estado da verificação em segundo plano, transferência ativa, taxa de transferência, total de transferências, taxa de exclusão, fragmentos corrompidos, objetos perdidos, objetos ausentes, tentativa de reparo, taxa de verificação, período estimado de verificação e estado de conclusão do reparo.

Nome do arquivo	Campos	Descrição
SERVER-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Configurações do servidor. Contém estes detalhes para cada nó: tipo de plataforma, sistema operacional, memória instalada, memória disponível, conectividade de storage, número de série do chassi do dispositivo de storage, quantidade de unidades com falha no controlador de storage, temperatura do chassi do controlador de computação, hardware de computação, número de série do controlador de computação, fonte de alimentação, tamanho da unidade e tipo de unidade.
SERVICE-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações do nó de serviço. Contém detalhes como espaço de tabela alocado, espaço de tabela livre, métricas Reaper do banco de dados, duração do reparo do segmento, duração da tarefa de reparo, reinicializações automáticas de tarefas e encerramento automático de tarefas.
STORAGE-GRADES.XML	ID da classe de armazenamento + Nome da classe de armazenamento + ID do nó de armazenamento + Caminho do nó de armazenamento	Arquivo de definições de storage grade para cada Storage Node.
SUMMARY-ATTRIBUTES.XML	OID do grupo + Caminho do grupo + ID do atributo de resumo + Nome do atributo de resumo + Valor + Índice + ID da tabela + Nome da tabela	Dados de status de alto nível do sistema que resumem as informações de uso do StorageGRID. Fornece detalhes como nome da grid, nomes dos sites, número de Storage Nodes por grid e por site, tipo de licença, capacidade e uso da licença, termos de suporte do software e detalhes das operações S3.
SYSTEM-ALERTS.XML	Nome + Gravidade + Nome do nó + Status do alerta + Nome do site + Hora de disparo do alerta + Hora de resolução do alerta + ID da regra + ID do nó + ID do site + Silenciado + Outras anotações + Outros rótulos	Alertas atuais do sistema que indicam possíveis problemas no sistema StorageGRID.

Nome do arquivo	Campos	Descrição
USERAGENTS.XML	Agente do usuário + Número de dias + Total de requisições HTTP + Total de bytes ingeridos + Total de bytes recuperados + Requisições PUT + Requisições GET + Requisições DELETE + Requisições HEAD + Requisições POST + Requisições OPTIONS + Tempo médio de requisição (ms) + Tempo médio de requisição PUT (ms) + Tempo médio de requisição GET (ms) + Tempo médio de requisição DELETE (ms) + Tempo médio de requisição HEAD (ms) + Tempo médio de requisição POST (ms) + Tempo médio de requisição OPTIONS (ms)	Estatísticas baseadas nos agentes de usuário do aplicativo. Por exemplo, o número de operações PUT/GET/DELETE/HEAD por agente de usuário e o tamanho total em bytes de cada operação.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport dados do cabeçalho.

Configurar AutoSupport em StorageGRID

Por padrão, o recurso AutoSupport do StorageGRID é ativado quando você instala o StorageGRID pela primeira vez. No entanto, você deve configurar o hardware AutoSupport em cada appliance. Se necessário, você pode alterar a configuração do AutoSupport.

Se você deseja alterar a configuração do StorageGRID AutoSupport, faça as alterações somente no nó de administração primário. Você deve configurar hardware AutoSupport em cada appliance.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".
- Se você for usar HTTPS para enviar AutoSupport pacotes, você terá fornecido acesso de saída à internet para o nó de administração principal, seja diretamente ou "usando um servidor proxy" (conexões de entrada não são necessárias).
- Se o HTTP for selecionado na página do AutoSupport do StorageGRID, você tem "configurou um servidor proxy" para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp

rejeitarão pacotes enviados usando HTTP.

- Se você for usar SMTP como protocolo para pacotes do AutoSupport, você configurou um servidor de e-mail SMTP.

Sobre esta tarefa

Você pode usar qualquer combinação das seguintes opções para enviar pacotes AutoSupport para o suporte técnico:

- **Semanal**: Enviar pacotes AutoSupport automaticamente uma vez por semana. Configuração padrão: Ativado.
- **Acionado por evento**: Enviar automaticamente pacotes AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Configuração padrão: Ativado.
- **Sob Demanda**: Permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer o protocolo de transmissão AutoSupport HTTPS). Configuração padrão: Desativado.
- **Acionado pelo usuário**: Envie pacotes AutoSupport manualmente a qualquer momento.
- **Coleta de logs**: "coletar manualmente arquivos de log e dados do sistema e enviar um pacote AutoSupport".

Especifique o protocolo para pacotes AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar pacotes AutoSupport:

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. Este protocolo utiliza a porta 443. Se você quiser Ative o recurso AutoSupport on Demand, deve usar HTTPS.
- **HTTP**: se você selecionar HTTP, deverá configurar um servidor proxy para encaminhar pacotes AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam pacotes enviados usando HTTP. Este protocolo usa a porta 80.
- **SMTP**: Use esta opção se você quiser que os pacotes AutoSupport sejam enviados por e-mail.

O protocolo que você definir será usado para o envio de todos os tipos de pacotes AutoSupport.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Selecione o protocolo que você deseja usar para enviar pacotes AutoSupport.
3. Se você selecionou **HTTPS**, escolha se deseja usar um certificado de suporte NetApp (certificado TLS) para proteger a conexão com o servidor de suporte técnico.
   - **Verificar certificado** (padrão): Garante que a transmissão de pacotes AutoSupport seja segura. O certificado de suporte NetApp já está instalado com o software StorageGRID.
   - **Não verificar certificado**: selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.
4. Selecione **Salvar**. Todos os pacotes semanais, acionados pelo usuário e acionados por eventos são enviados usando o protocolo selecionado.

Desativar AutoSupport semanal

Por padrão, o sistema StorageGRID está configurado para enviar um pacote AutoSupport para o suporte técnico uma vez por semana.

Para determinar quando o pacote semanal do AutoSupport será enviado, vá até a guia **AutoSupport** > **Resultados**. Na seção **Semanal AutoSupport**, verifique o valor de **Próximo horário agendado**.

Você pode desativar o envio automático de pacotes semanais do AutoSupport a qualquer momento.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Desmarque a caixa de seleção **Ativar semanalmente AutoSupport**.
3. Selecione **Salvar**.

Desativar AutoSupport acionado por evento

Por padrão, o sistema StorageGRID está configurado para enviar um pacote AutoSupport para o suporte técnico a cada hora.

Você pode desativar o acionamento por eventos AutoSupport a qualquer momento.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Desmarque a caixa de seleção **Ativar acionamento por evento AutoSupport**.
3. Selecione **Salvar**.

Ativar AutoSupport sob demanda

AutoSupport on Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport Sob Demanda está desativado. Habilitar esse recurso permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de sondagem para consultas AutoSupport Sob Demanda.

O suporte técnico não pode ativar ou desativar AutoSupport on Demand.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Selecione **HTTPS** para o protocolo.
3. Selecione a caixa de seleção **Ativar semanalmente AutoSupport**.
4. Selecione a caixa de seleção **Ativar AutoSupport sob demanda**.
5. Selecione **Salvar**.

   AutoSupport On Demand está ativado e o suporte técnico pode enviar solicitações AutoSupport On Demand para o StorageGRID.

Desative as verificações de atualizações de software

Por padrão, StorageGRID entra em contato com a NetApp para verificar se há atualizações de software disponíveis para o seu sistema. Se uma hotfix do StorageGRID ou uma nova versão estiver disponível, a nova versão será exibida na página de upgrade do StorageGRID.

Se necessário, você pode opcionalmente desativar a verificação de atualizações de software. Por exemplo, se

seu sistema não tiver acesso à WAN, você deve desativar a verificação para evitar erros de download.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Desmarque a caixa de seleção **Verificar atualizações de software**.
3. Selecione **Salvar**.

Adicionar um destino adicional do AutoSupport

Quando você ativa o AutoSupport, os pacotes de integridade e status são enviados para o suporte técnico. Você pode especificar um destino adicional para todos os pacotes do AutoSupport.

Para verificar ou alterar o protocolo usado para enviar pacotes AutoSupport, consulte as instruções para especifique o protocolo para pacotes AutoSupport.

> Não é possível usar o protocolo SMTP para enviar pacotes AutoSupport para um destino adicional.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport** > **Configurações**.
2. Selecione **Ativar destino adicional do AutoSupport**.
3. Especifique o seguinte:

   Nome do host
   O nome do host ou endereço IP de um servidor de destino AutoSupport adicional.

   > Você pode inserir apenas um destino adicional.

   Porta
   A porta usada para conectar a um servidor de destino AutoSupport adicional. O padrão é a porta 80 para HTTP ou a porta 443 para HTTPS.

   Validação de certificado
   Indica se um certificado TLS é usado para proteger a conexão com o destino adicional.

   - Selecione **Verificar certificado** para usar a validação de certificado.
   - Selecione **Não verificar certificado** para enviar seus AutoSupport pacotes sem validação de certificado.

     Selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.

4. Se você selecionou **Verificar certificado**, faça o seguinte:
   a. Navegue até a localização do certificado da CA.
   b. Faça o upload do arquivo de certificado da CA.

   Os metadados do certificado CA são exibidos.

5. Selecione **Salvar**.

Todos os futuros pacotes semanais, acionados por eventos e acionados pelo usuário de AutoSupport serão enviados para o destino adicional.

Configurar AutoSupport para dispositivos de storage

AutoSupport para dispositivos reporta problemas de hardware do StorageGRID, e StorageGRID AutoSupport reporta problemas de software do StorageGRID, com uma exceção: para o SGF6112, StorageGRID AutoSupport reporta problemas tanto de hardware quanto de software. Você deve configurar AutoSupport em cada dispositivo, exceto o SGF6112, que não requer configuração adicional. AutoSupport é implementado de forma diferente para dispositivos de serviço e dispositivos de storage.

Você utiliza SANtricity para habilitar o AutoSupport para cada dispositivo de storage. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou após a instalação do dispositivo:

- Para os dispositivos SG6000 e SG5700, "configurar AutoSupport no SANtricity System Manager"

AutoSupport pacotes de dispositivos E-Series podem ser incluídos no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy em "SANtricity System Manager".

StorageGRID AutoSupport não reporta problemas de hardware, como falhas em módulos DIMM ou placas de interface de host (HIC). No entanto, algumas falhas de componentes podem gerar "alertas de hardware". Para dispositivos de storage StorageGRID com um controlador de gerenciamento de placa-mãe (BMC), você pode configurar e-mail e traps SNMP para reportar falhas de hardware:

- "Configure notificações por e-mail para alertas do BMC"
- "Configurar as definições de SNMP para BMC"

Informações relacionadas

"Suporte da NetApp"

Acionar manualmente um pacote AutoSupport no StorageGRID

Para ajudar o suporte técnico a solucionar problemas com seu sistema StorageGRID, você pode acionar manualmente o envio de um pacote AutoSupport.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você possui acesso de root ou permissão de configuração de outra grid.

Passos

1. Selecione **Suporte** > **Ferramentas** > **AutoSupport**.
2. Na aba **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

   StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **Resultado Mais Recente** e **Última Vez Bem-Sucedida** na aba **Resultados** são atualizados. Se houver um problema, o valor **Resultado Mais Recente** é atualizado para "Falha" e o StorageGRID não tenta enviar o pacote AutoSupport novamente.

3. Após 1 minuto, atualize a página AutoSupport no seu navegador para acessar os resultados mais recentes.

Além disso, você pode "coletar arquivos de log e dados do sistema mais extensos" e enviá-los para o site de suporte da NetApp.

Solucionar problemas dos pacotes AutoSupport do StorageGRID

Se uma tentativa de envio de um pacote AutoSupport falhar, o sistema StorageGRID tomará ações diferentes dependendo do tipo de pacote AutoSupport. Você pode verificar o status dos pacotes AutoSupport selecionando **Suporte** > **Ferramentas** > **AutoSupport** > **Resultados**.

Quando o pacote AutoSupport falha ao ser enviado, "Falha" aparece na guia **Resultados** da página **AutoSupport**.

Se você configurou um servidor proxy para encaminhar pacotes AutoSupport para NetApp, você deve "Verifique se as configurações do servidor proxy estão corretas.".

Falha semanal no pacote AutoSupport

Se um pacote semanal do AutoSupport falhar ao ser enviado, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo Resultado Mais Recente para Tentando Novamente.
2. O sistema tenta reenviar o pacote AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas no envio, atualiza o atributo "Resultado Mais Recente" para "Falha".
4. Tenta enviar novamente um pacote AutoSupport no próximo horário agendado.
5. Mantém a programação regular do AutoSupport caso o pacote falhe devido à indisponibilidade do serviço NMS e se um pacote for enviado antes de sete dias.
6. Quando o serviço NMS estiver disponível novamente, envia um pacote AutoSupport imediatamente se nenhum pacote tiver sido enviado por sete dias ou mais.

Falha de pacote AutoSupport acionada pelo usuário ou por evento

Se um pacote AutoSupport acionado pelo usuário ou por um evento não for enviado, o sistema StorageGRID executa as seguintes ações:

1. Exibe uma mensagem de erro se o erro for conhecido. Por exemplo, se um usuário selecionar o protocolo SMTP sem fornecer as configurações de e-mail corretas, o seguinte erro será exibido: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tenta enviar o pacote novamente.
3. Registra o erro em `nms.log`.

Se ocorrer uma falha e o protocolo selecionado for SMTP, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução (**Suporte** > **Alarmes (legado)** > **Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Saiba como "configurar as configurações do servidor de e-mail".

Corrigir uma falha no pacote AutoSupport

Se ocorrer uma falha e o protocolo selecionado for SMTP, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envie pacotes E-Series AutoSupport através do StorageGRID

Você pode enviar pacotes AutoSupport do E-Series SANtricity System Manager para o suporte técnico por meio de um nó Admin do StorageGRID, em vez da porta de gerenciamento do dispositivo de storage.

Consulte "Hardware E-Series AutoSupport" para obter mais informações sobre o uso do AutoSupport com dispositivos de storage E-Series.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de administrador do dispositivo de storage ou acesso root".
- Você configurou SANtricity AutoSupport:
  - Para os dispositivos SG6000 e SG5700, "configurar AutoSupport no SANtricity System Manager"

> Você precisa ter firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

Sobre esta tarefa

Os pacotes E-Series AutoSupport contêm detalhes do hardware de storage e são mais específicos do que outros pacotes AutoSupport enviados pelo sistema StorageGRID.

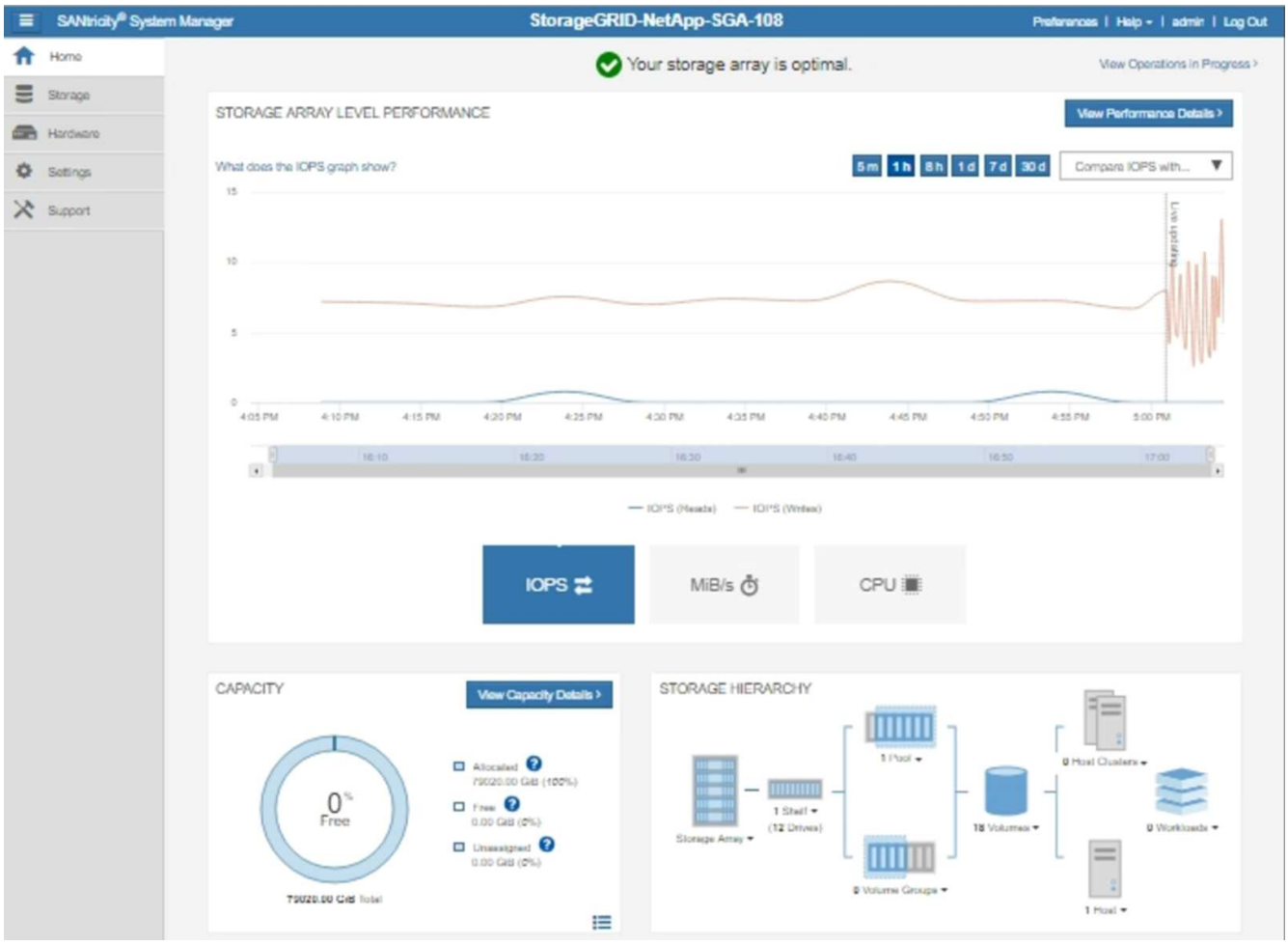
Você pode configurar um endereço de servidor proxy especial no SANtricity System Manager para transmitir pacotes AutoSupport através de um StorageGRID Admin Node sem usar a porta de gerenciamento do appliance. Pacotes AutoSupport transmitidos dessa forma são enviados pelo "Nó de administração remetente preferencial" e utilizam qualquer "configurações de proxy do admin" que tenha sido configurado no Grid Manager.

> Este procedimento é apenas para configurar um servidor proxy StorageGRID para pacotes AutoSupport do E-Series. Para obter detalhes adicionais sobre a configuração do E-Series AutoSupport, consulte o "NetApp E-Series e documentação do SANtricity".

Passos

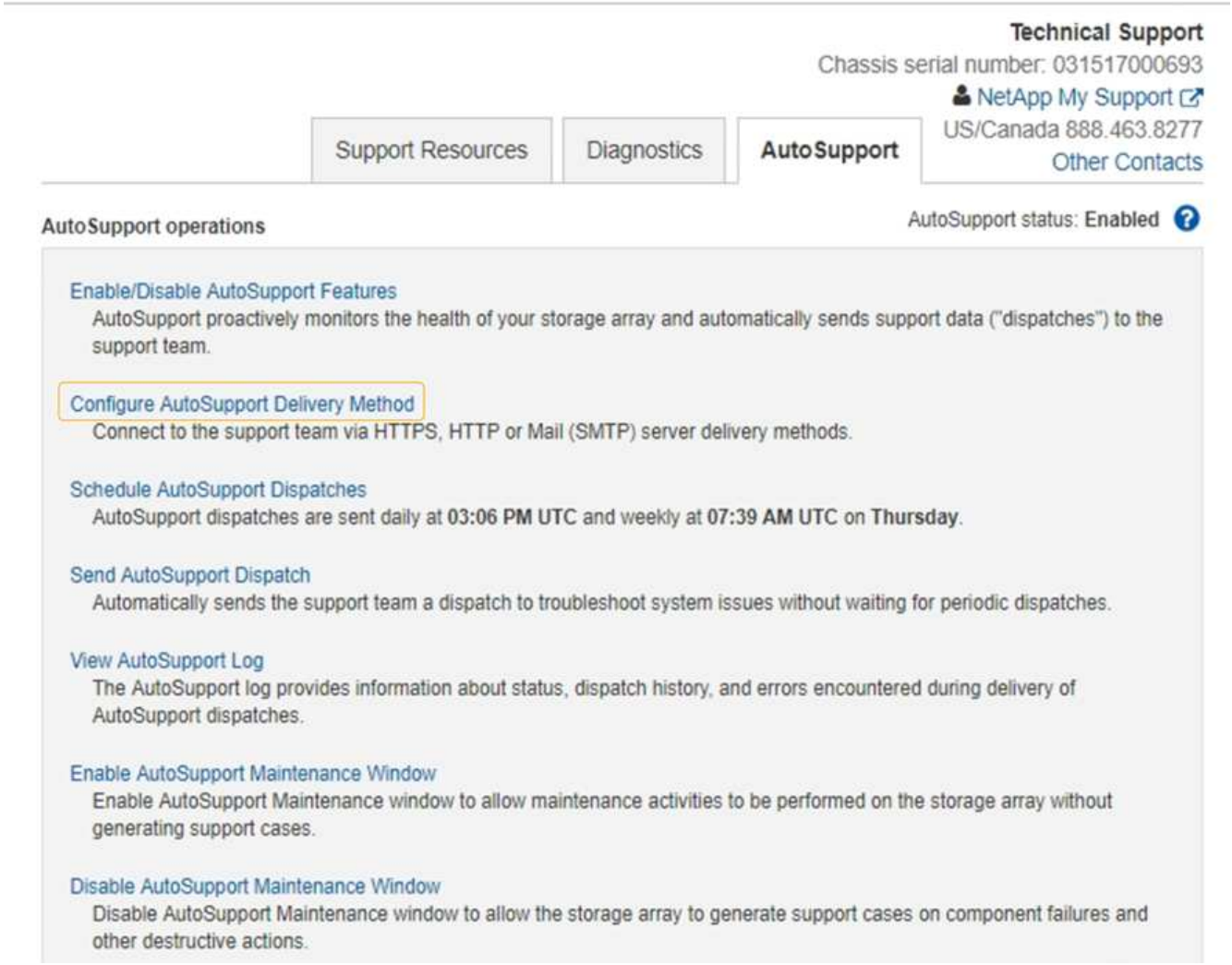
1. No Gerenciador de Grade, selecione **Nós**.
2. Na lista de nós à esquerda, selecione o dispositivo de storage que você deseja configurar.
3. Selecione **SANtricity System Manager**.

   A página inicial do SANtricity System Manager é exibida.



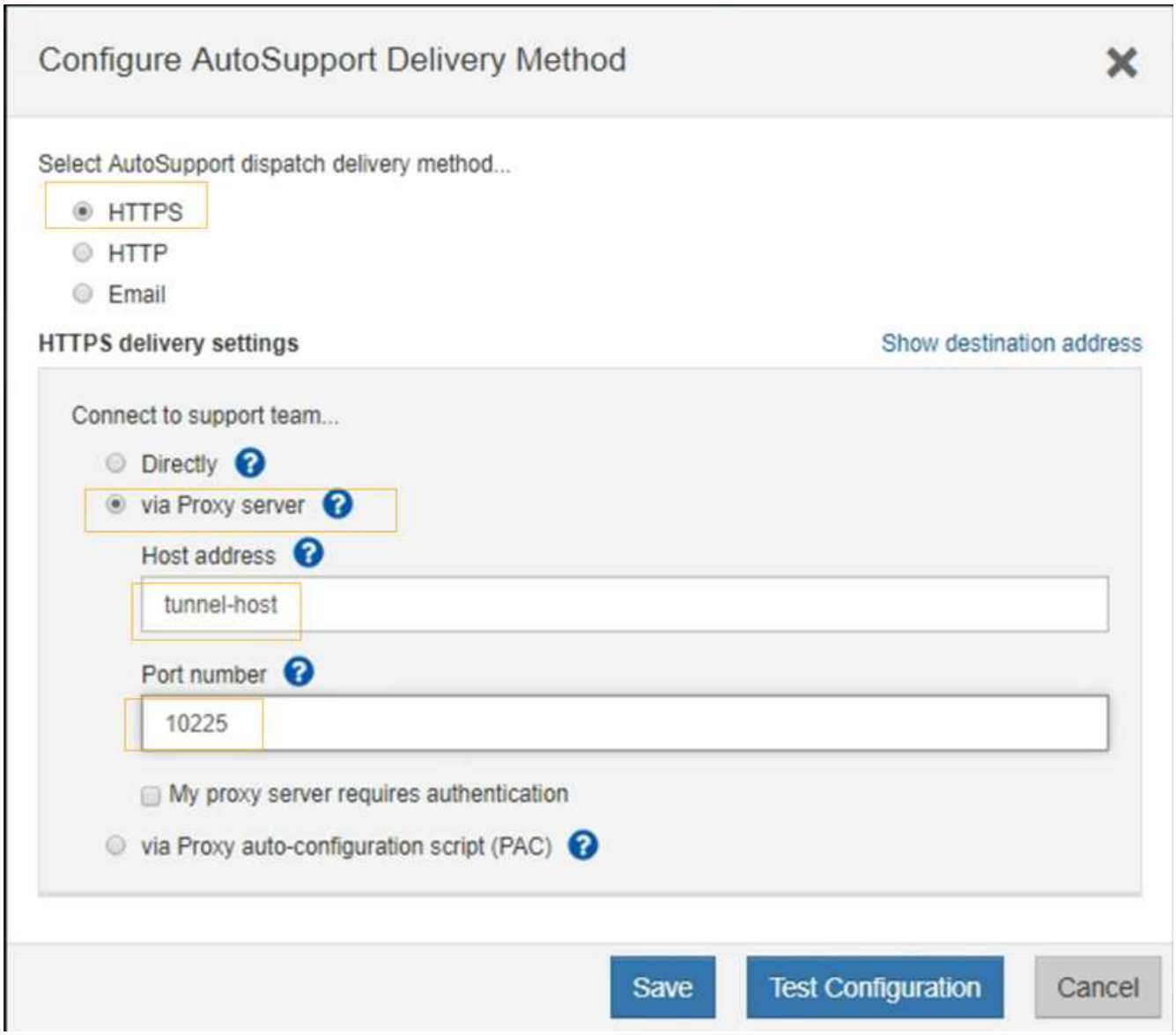
4. Selecione **Suporte** > **Central de suporte** > **AutoSupport**.

   A página de operações do AutoSupport é exibida.



5. Selecione **Configurar AutoSupport Delivery Method**.

   A página Configurar AutoSupport Método de Entrega é exibida.



6. Selecione **HTTPS** como método de entrega.

   O certificado que habilita o HTTPS já está pré-instalado.

7. Selecione **via servidor proxy**.
8. Insira `tunnel-host` para o **Endereço do host**.

   `tunnel-host` é o endereço especial para usar um Nó de Administração para enviar pacotes E-Series AutoSupport.

9. Digite `10225` para o **número da porta**.

   `10225` é o número da porta no servidor proxy do StorageGRID que recebe pacotes AutoSupport do controlador E-Series no dispositivo.

10. Selecione **Testar Configuração** para testar o roteamento e a configuração do seu servidor proxy AutoSupport.

Se estiver correta, uma mensagem em uma faixa verde aparecerá: "Sua configuração do AutoSupport foi verificada."

Se o teste falhar, uma mensagem de erro aparecerá em uma faixa vermelha. Verifique suas configurações de DNS do StorageGRID e de rede, certifique-se de que "Nó de administração remetente preferencial" pode se conectar ao site de suporte da NetApp e tente o teste novamente.

11. Selecione **Salvar**.

    A configuração é salva e uma mensagem de confirmação aparece: "AutoSupport delivery method foi configurado."

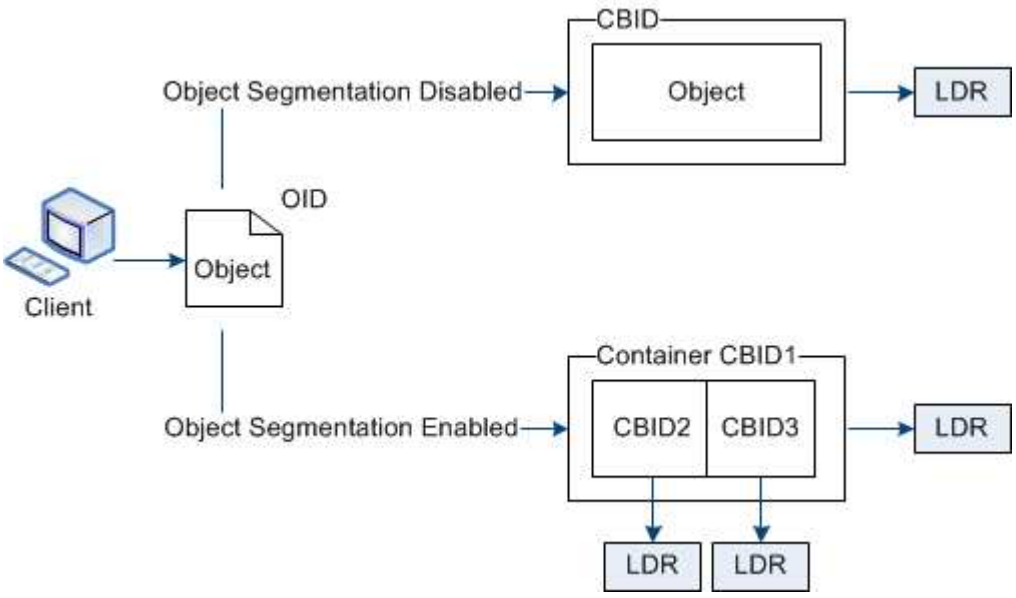
Gerenciar nós de armazenamento

Use as opções de armazenamento

Saiba mais sobre segmentação de objetos no StorageGRID

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 multipartes do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é inserido no sistema StorageGRID, o serviço LDR divide o objeto em segmentos e cria um contêiner de segmentos que lista as informações de cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contêiner de segmento, o serviço LDR monta o objeto original a partir de seus segmentos e retorna o objeto ao cliente.

O contêiner e os segmentos não precisam estar armazenados no mesmo Storage Node. O contêiner e os segmentos podem estar armazenados em qualquer Storage Node dentro do pool de storage especificado na regra ILM.

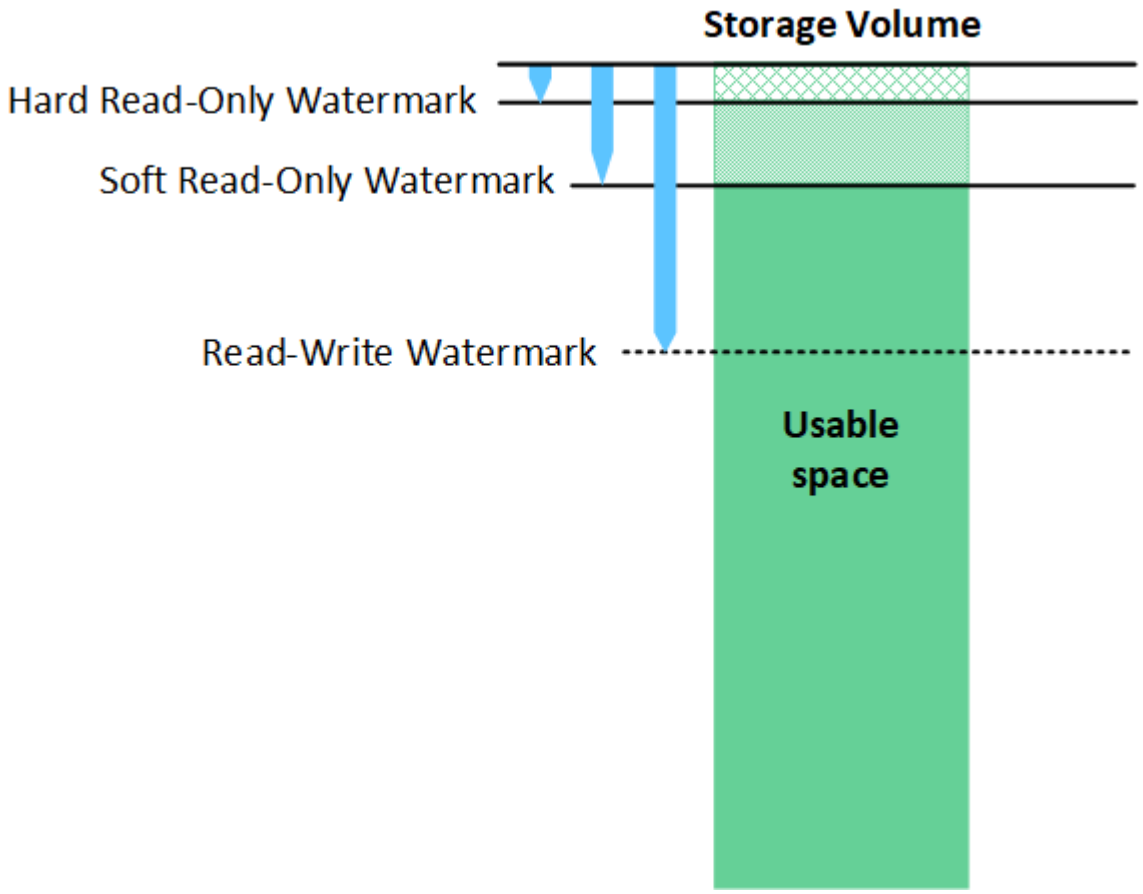
Cada segmento é tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de

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 conclusão da ingestão, conforme a seguir:

```
segment container + segment 1 + segment 2 = three stored objects
```

Saiba mais sobre marcas d'água de volume de armazenamento no StorageGRID

StorageGRID utiliza três marcas d'água de volume de armazenamento para garantir que os nós de armazenamento sejam transferidos com segurança para um estado somente leitura antes que fiquem criticamente sem espaço e para permitir que os nós de armazenamento que foram transferidos para um estado somente leitura voltem a ser de leitura e gravação.



As marcas d'água de volume de armazenamento aplicam-se apenas ao espaço usado para dados de objetos replicados e codificados por apagamento. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, acesse "Gerencie o armazenamento de metadados de objetos".

O que é a marca d'água "somente leitura" suave?

A **marca d'água somente leitura flexível do volume de storage** é a primeira marca d'água a indicar que o espaço utilizável de um Storage Node para dados de objetos está ficando cheio.

Se cada volume em um Nó de Armazenamento tiver menos espaço livre do que a marca d'água de leitura

flexível desse volume, o Nó de Armazenamento entra no modo somente leitura. O modo somente leitura significa que o Nó de Armazenamento anuncia serviços somente leitura para o restante do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Por exemplo, suponha que cada volume em um Storage Node tenha uma marca d'água de leitura flexível de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o Storage Node entra no modo de leitura flexível.

O que é o watermark rígido de somente leitura?

A **marca d'água rígida de somente leitura do volume de storage** é a próxima marca d'água a indicar que o espaço utilizável de um nó para dados de objetos está ficando cheio.

Se o espaço livre em um volume for menor que a marca d'água de leitura obrigatória desse volume, as gravações nesse volume falharão. No entanto, as gravações em outros volumes podem continuar até que o espaço livre nesses volumes seja menor que suas respectivas marcas d'água de leitura obrigatória.

Por exemplo, suponha que cada volume em um Storage Node tenha uma marca d'água rígida de somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o Storage Node não aceitará mais solicitações de gravação.

A marca d'água rígida de somente leitura é sempre menor que a marca d'água flexível de somente leitura.

O que é a marca d'água de leitura/gravação?

A **marca d'água de leitura/gravação do volume de storage** aplica-se somente aos Storage Nodes que passaram para o modo somente leitura. Ela determina quando o nó pode voltar a ser leitura/gravação. Quando o espaço livre em qualquer volume de storage em um Storage Node for maior que a marca d'água de leitura/gravação desse volume, o nó retorna automaticamente ao estado de leitura/gravação.

Por exemplo, suponha que o Storage Node tenha entrado em modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura/gravação de 30 GB. Assim que o espaço livre em qualquer volume aumentar para 30 GB, o nó volta a ser leitura/gravação.

A marca d'água de leitura/gravação é sempre maior do que tanto a marca d'água de leitura flexível quanto a marca d'água de leitura rígida.

Exibir marcas d'água de volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados pelo sistema. Caso as marcas d'água otimizadas não estejam sendo utilizadas, você pode determinar se é possível ou recomendável ajustar as configurações.

Antes de começar

- Você concluiu a atualização para StorageGRID 11.6 ou superior.
- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem o "Permissão de acesso root".

Ver as configurações atuais da marca d'água

Você pode visualizar as configurações atuais da marca d'água de storage no Grid Manager.

Passos

1. Selecione **Support** > **Other** > **Storage watermarks**.

2. Na página de marcas d'água de storage, verifique a caixa de seleção "Usar valores otimizados".
   - Se a caixa de seleção estiver marcada, todas as três marcas d'água serão otimizadas para cada volume de storage em cada Storage Node, com base no tamanho do Storage Node e na capacidade relativa do volume.

     Esta é a configuração padrão e recomendada. Não altere esses valores. Opcionalmente, você pode Visualizar marcas d'água de storage otimizadas.

   - Se a caixa de seleção "Usar valores otimizados" estiver desmarcada, marcas d'água personalizadas (não otimizadas) estão sendo usadas. Não é recomendável usar configurações de marca d'água personalizadas. Use as instruções para "Solução de problemas de alertas de sobreposição de marca d'água somente leitura baixa" determinar se você pode ou deve ajustar as configurações.

     Ao especificar configurações de marca d'água personalizadas, você deve inserir valores maiores que 0.

Visualizar marcas d'água de storage otimizadas

StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que calculou para a marca d'água de leitura somente leitura suave do volume de storage. Você pode visualizar os valores otimizados mínimo e máximo para cada Storage Node em sua grid.

1. Selecione **Suporte** > **Ferramentas** > **Métricas**.
2. Na seção Prometheus, selecione o link para acessar a interface de usuário do Prometheus.
3. Para visualizar a marca d'água mínima recomendada para leitura somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor mínimo otimizado da marca d'água de leitura somente leitura flexível para todos os volumes de armazenamento em cada Storage Node. Se esse valor for maior que a configuração personalizada para a marca d'água de leitura somente leitura flexível do volume de armazenamento, o alerta **Low read-only watermark override** será acionado para o Storage Node.

4. Para visualizar a marca d'água máxima recomendada para leitura somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   A última coluna mostra o valor máximo otimizado da marca d'água de leitura somente leitura flexível para todos os volumes de armazenamento em cada Storage Node.

Gerencie o armazenamento de metadados de objetos no StorageGRID

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 suficiente para armazenar novos objetos, você precisa entender onde e como o StorageGRID armazena os metadados dos objetos.

O que são metadados de objeto?

Metadados de objeto são quaisquer informações que descrevem um objeto. StorageGRID usa metadados de objeto para rastrear as localizações de todos os objetos na grid e para gerenciar o ciclo de vida de cada objeto ao longo do tempo.

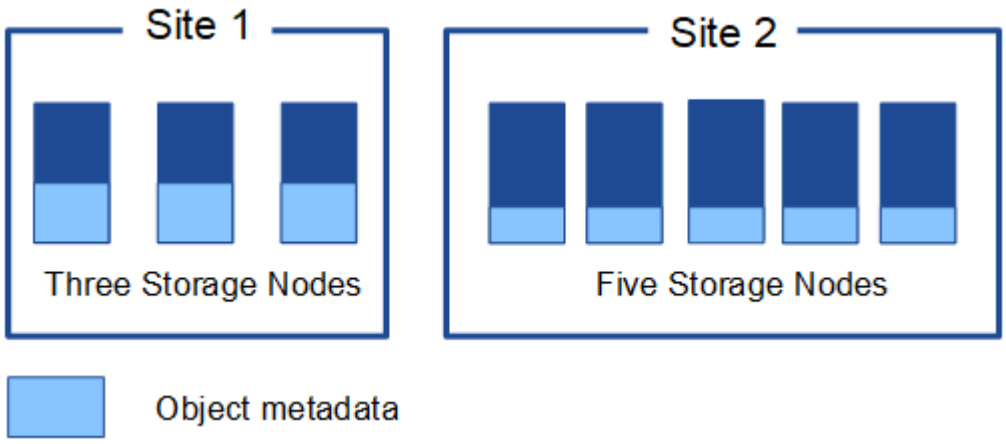
Para um objeto no StorageGRID, os metadados do objeto incluem os seguintes tipos de informações:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket S3, o nome ou ID da conta do tenant, 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 chave-valor de metadados de usuário personalizados associados ao objeto.
- Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
- Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.
- Para cópias de objetos com código de apagamento, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, a localização 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 objeto são armazenados?

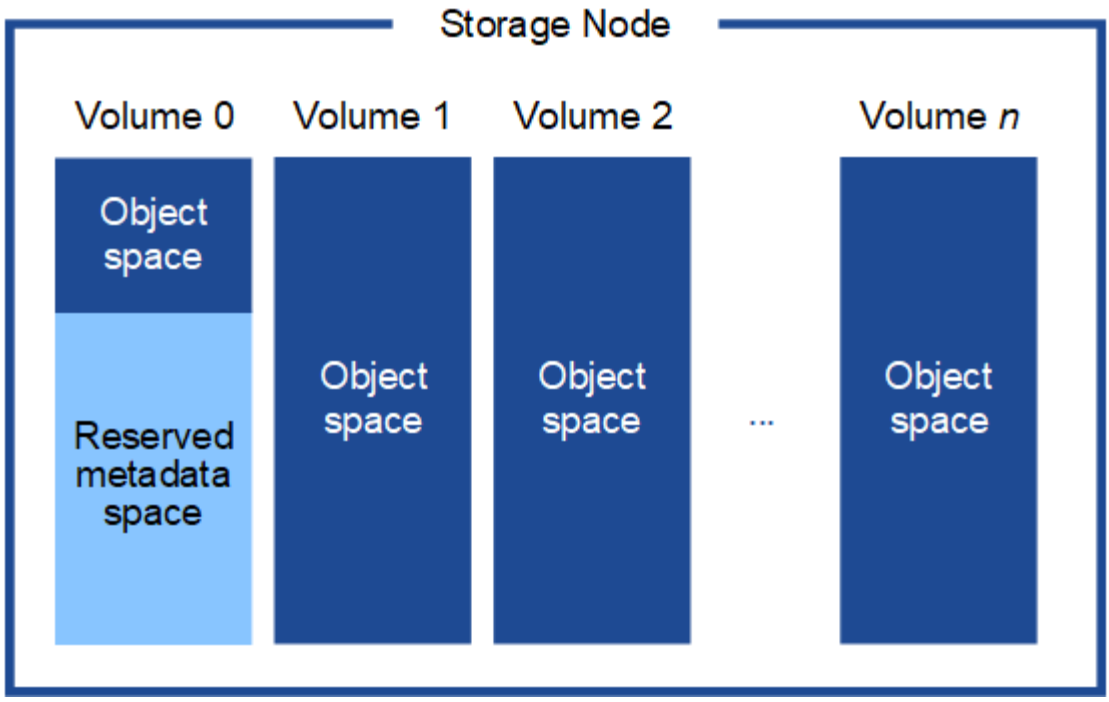
StorageGRID mantém os metadados dos objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados dos objetos. Para garantir a redundância e proteger os metadados dos objetos contra perda, StorageGRID armazena três cópias dos metadados para todos os objetos do sistema em cada site.

Esta figura representa os nós de armazenamento em dois locais. Cada local possui a mesma quantidade de metadados de objetos, e os metadados de cada local são subdivididos entre todos os nós de armazenamento desse local.



Onde os metadados do objeto são armazenados?

Esta figura representa os volumes de armazenamento para um único Storage Node.



Conforme ilustrado na figura, StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada Nó de Armazenamento. Ele utiliza o espaço reservado para armazenar metadados de objetos e para executar operações essenciais do banco de dados. Qualquer espaço restante no volume de armazenamento 0 e em todos os outros volumes de armazenamento do Nó de Armazenamento é utilizado exclusivamente para dados de objetos (cópias replicadas e fragmentos codificados por eliminação).

A quantidade de espaço reservada para metadados de objetos em um determinado Nó de Armazenamento depende de vários fatores, que são descritos abaixo.

Configuração de espaço reservado para metadados

O *Espaço reservado para metadados* é uma configuração de todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada Storage Node. Conforme mostrado na tabela, o valor padrão dessa configuração é baseado em:

- A versão do software que você estava usando quando instalou StorageGRID.
- A quantidade de RAM em cada Storage Node.

Versão usada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado para metadados
11,5 a 12,0	128 GB ou mais em cada nó de armazenamento na grade	8 TB (8.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento na grade	3 TB (3.000 GB)
11.1 a 11.4	128 GB ou mais em cada nó de armazenamento em qualquer local	4 TB (4.000 GB)

Versão usada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado para metadados
	Menos de 128 GB em qualquer nó de armazenamento em cada local	3 TB (3.000 GB)
11.0 ou anterior	Qualquer quantidade	2 TB (2.000 GB)

Visualizar configuração de espaço reservado de metadados

Siga estas etapas para visualizar a configuração de espaço reservado para metadados do seu sistema StorageGRID.

Passos

1. Selecione **Configuração** > **Sistema** > **Configurações de armazenamento**.
2. Na página Configurações de armazenamento, expanda a seção **Espaço reservado para metadados**.

Para StorageGRID 11.8 ou superior, o valor do espaço reservado para metadados deve ser de pelo menos 100 GB e no máximo 1 PB.

A configuração padrão para uma nova instalação do StorageGRID 11.6 ou superior, na qual cada nó de armazenamento possui 128 GB ou mais de RAM, é de 8.000 GB (8 TB).

Espaço reservado real para metadados

Em contraste com a configuração de espaço reservado para metadados em todo o sistema, o espaço reservado real para metadados de objetos é determinado para cada Storage Node. Para qualquer Storage Node, o espaço reservado real para metadados depende do tamanho do volume 0 do nó e da configuração de espaço reservado para metadados em todo o sistema.

Tamanho do volume 0 para o nó	Espaço reservado real para metadados
Menos de 500 GB (uso não produtivo)	10% do volume 0
500 GB ou mais + ou + Nós de armazenamento somente de metadados	O menor desses valores: • Volume 0 • Configuração de espaço reservado para metadados **Nota**: Apenas um rangedb é necessário para nós de armazenamento somente de metadados.

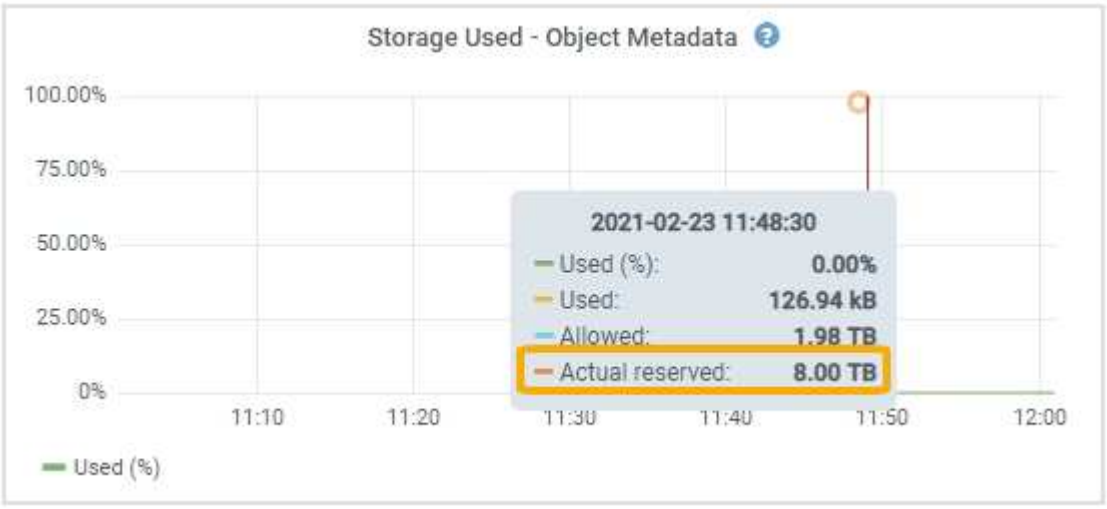
Veja o espaço reservado real para metadados

Siga estes passos para visualizar o espaço reservado para metadados em um determinado Storage Node.

Passos

1. No Gerenciador de Grade, selecione **Nós** > ***Nó de Armazenamento***.
2. Selecione a guia **Storage**.

3. Posicione o cursor sobre o gráfico "Armazenamento Utilizado - Metadados do Objeto" e localize o valor "**Reservado de fato**".



Na captura de tela, o valor **Reservado real** é 8 TB. Esta captura de tela é de um Storage Node grande em uma nova instalação do StorageGRID 11.6. Como a configuração de espaço reservado para metadados em todo o sistema é menor que o volume 0 para este Storage Node, o espaço reservado real para este nó é igual à configuração de espaço reservado para metadados.

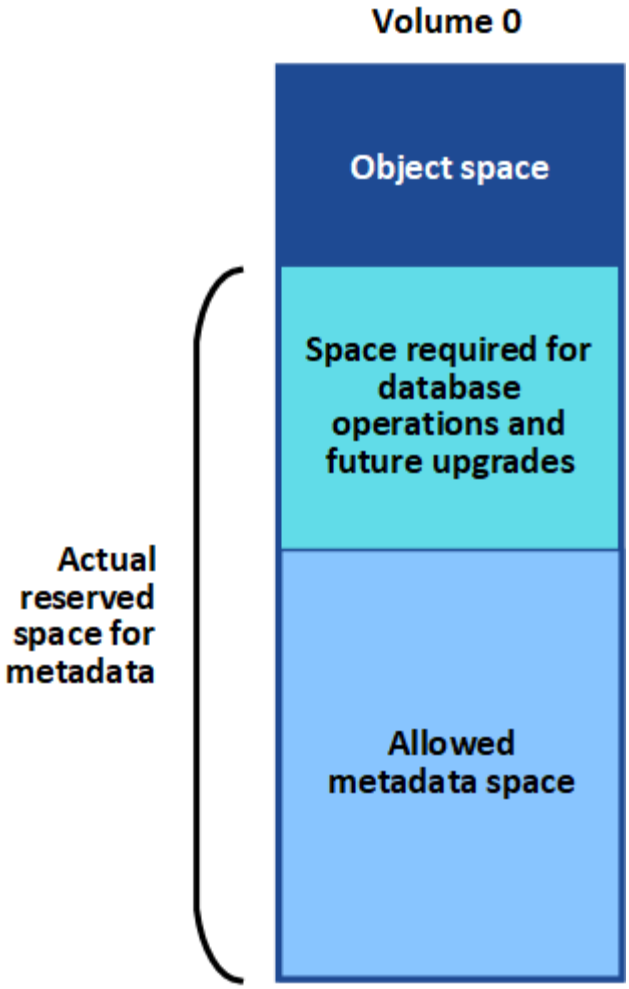
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11.7 ou posterior. Para este exemplo, suponha que cada Storage Node tenha mais de 128 GB de RAM e que o volume 0 do Storage Node 1 (SN1) tenha 6 TB. Com base nesses valores:

- O **espaço reservado de metadados** em todo o sistema está definido como 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11.6 ou superior se cada Storage Node tiver mais de 128 GB de RAM.)
- O espaço reservado real para metadados no SN1 é de 6 TB. (Todo o volume está reservado porque o volume 0 é menor que a configuração **Espaço reservado para metadados**.)

Espaço de metadados permitido

O espaço reservado real de cada Storage Node para metadados é subdividido no espaço disponível para metadados de objeto (o *espaço de metadados permitido*) e no espaço necessário para operações essenciais do banco de dados (como compactação e reparo) e upgrades futuros de hardware e software. O espaço de metadados permitido controla a capacidade geral de objetos.



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 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

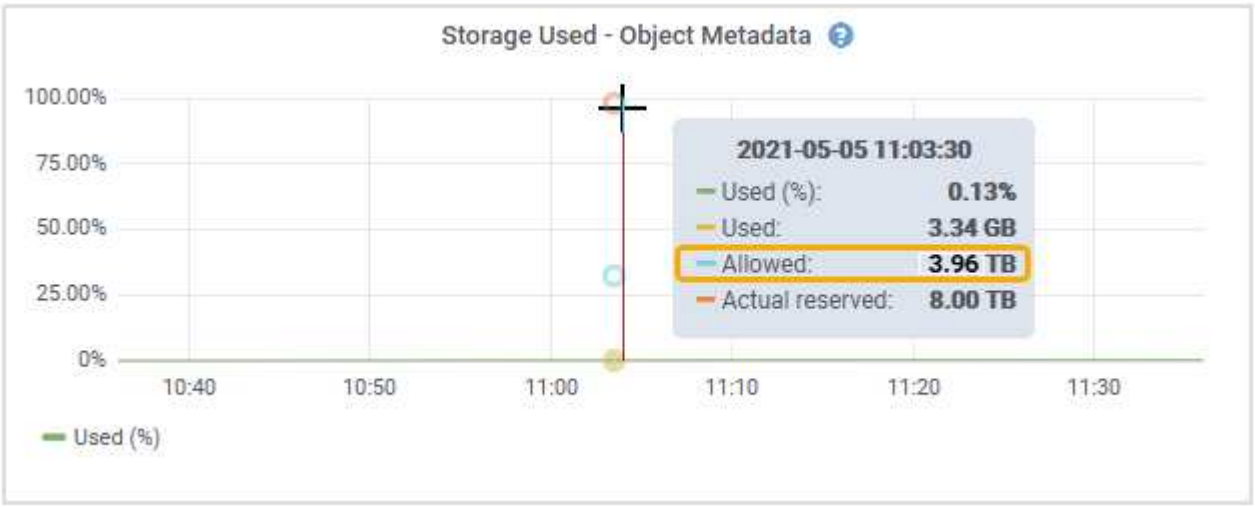
Exibir espaço de metadados permitido

Siga estas etapas para visualizar o espaço de metadados permitido para um Storage Node.

Passos

1. No Gerenciador de Grade, selecione **Nós**.

2. Selecione o nó de armazenamento.
3. Selecione a guia **Storage**.
4. Posicione o cursor sobre o gráfico "Storage used - object metadata" e localize o valor **Allowed**.



Na captura de tela, o valor **Permitido** é 3,96 TB, que é o valor máximo para um Storage Node cujo espaço reservado para metadados é superior a 4 TB.

O valor **Permitido** corresponde a esta métrica do Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemplo de espaço de metadados permitido

Suponha que você instale um StorageGRID usando a versão 11.6. Para este exemplo, considere que cada Storage Node possui mais de 128 GB de RAM e que o volume 0 do Storage Node 1 (SN1) tem 6 TB. Com base nesses valores:

- O **espaço reservado de metadados** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11.6 ou superior quando cada Storage Node tem mais de 128 GB de RAM.)
- O espaço reservado real para metadados no SN1 é de 6 TB. (Todo o volume está reservado porque o volume 0 é menor que a configuração **Espaço reservado para metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado na tabela de espaço permitido para metadados: (espaço reservado para metadados − 1 TB) × 60%, até um máximo de 3,96 TB.

Como os nós de armazenamento de diferentes tamanhos afetam a capacidade de objetos

Conforme descrito acima, StorageGRID distribui uniformemente os metadados de objetos entre os Storage Nodes em cada site. Por esse motivo, se um site contiver Storage Nodes de tamanhos diferentes, o menor node do site determinará a capacidade de metadados do site.

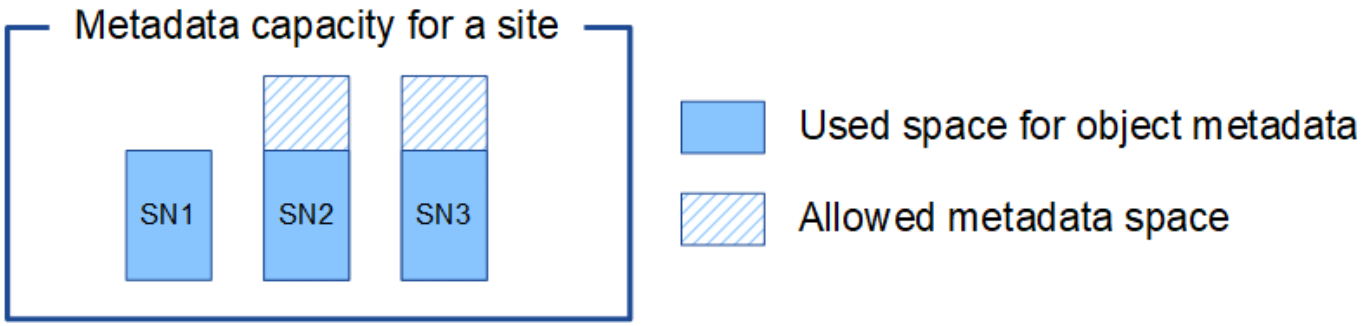
Considere o seguinte exemplo:

- Você possui uma grid de site único contendo três Storage Nodes de tamanhos diferentes.

- A configuração **Espaço reservado para metadados** é de 4 TB.
- Os nós de armazenamento possuem os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de armazenamento	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 entre os Storage Nodes em um site, cada nó neste exemplo pode armazenar apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço de metadados permitido para SN2 e SN3 não podem ser usados.



Da mesma forma, como o StorageGRID mantém todos os metadados de objetos de um sistema StorageGRID em cada site, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objetos do menor site.

E como a capacidade de metadados do objeto controla a quantidade máxima de objetos, quando um nó fica sem capacidade de metadados, a grid fica efetivamente cheia.

Informações relacionadas

- Para aprender como monitorar a capacidade de metadados de objetos para cada Storage Node, consulte as instruções para "Monitorando o StorageGRID".
- Para aumentar a capacidade de metadados de objetos do seu sistema, "expandir uma grid" adicione novos Storage Nodes.

Aumente a configuração de Espaço Reservado para Metadados no StorageGRID

Você poderá aumentar a configuração de Espaço Reservado para Metadados se seus nós de armazenamento atenderem a requisitos específicos de RAM e espaço disponível.

O que você vai precisar

- Você está conectado ao Grid Manager usando um "navegador web compatível".
- Você tem o "Permissão de acesso root ou permissão de outra configuração da grid".

Sobre esta tarefa

Você pode aumentar manualmente a configuração de Espaço Reservado para Metadados em todo o sistema para até 8 TB.

Você só pode aumentar o valor da configuração de Espaço Reservado para Metadados em todo o sistema se ambas as afirmações a seguir forem verdadeiras:

- Os nós de armazenamento em qualquer site do seu sistema possuem 128 GB ou mais de RAM.
- Os nós de armazenamento em qualquer site do seu sistema têm espaço disponível suficiente no volume de armazenamento 0.

Tenha em mente que, ao aumentar essa configuração, você reduzirá simultaneamente o espaço disponível para storage de objetos no volume de armazenamento 0 de todos os Storage Nodes. Por esse motivo, talvez seja melhor definir o Espaço Reservado para Metadados para um valor inferior a 8 TB, com base nos seus requisitos esperados de metadados de objetos.

> Em geral, é melhor usar um valor mais alto do que um valor mais baixo. Se a configuração de Espaço Reservado para Metadados for muito grande, você pode diminuí-la depois. Por outro lado, se você aumentar o valor depois, o sistema pode precisar mover dados de objetos para liberar espaço.

Para uma explicação detalhada de como a configuração Espaço Reservado para Metadados afeta o espaço permitido para armazenamento de metadados de objetos em um determinado Storage Node, consulte "Gerencie o armazenamento de metadados de objetos".

Passos

1. Determine a configuração atual de Espaço Reservado para Metadados.
   a. Selecione **Configuração** > **Sistema** > **Configurações de armazenamento**.
   b. Observe o valor de **Espaço Reservado para Metadados**.
2. Certifique-se de que você tem espaço disponível suficiente no volume de armazenamento 0 de cada Storage Node para aumentar esse valor.
   a. Selecione **Nós**.
   b. Selecione o primeiro nó de armazenamento na grid.
   c. Selecione a guia Armazenamento.
   d. Na seção Volumes, localize a entrada **/var/local/rangedb/0**.
   e. Confirme que o valor Disponível é igual ou maior que a diferença entre o novo valor que você deseja usar e o valor atual do Espaço Reservado para Metadados.

      Por exemplo, se a configuração de Espaço Reservado para Metadados estiver atualmente em 4 TB e você quiser aumentá-la para 6 TB, o valor Disponível deve ser de 2 TB ou superior.

   f. Repita estas etapas para todos os Storage Nodes.
      - Se um ou mais nós de armazenamento não tiverem espaço disponível suficiente, o valor de Espaço Reservado para Metadados não poderá ser aumentado. Não prossiga com este procedimento.
      - Se cada nó de armazenamento tiver espaço disponível suficiente no volume 0, passe para a próxima etapa.
3. Certifique-se de ter pelo menos 128 GB de RAM em cada Storage Node.

a. Selecione **Nós**.

b. Selecione o primeiro nó de armazenamento na grid.

c. Selecione a guia **Hardware**.

d. Posicione o cursor sobre o gráfico de Uso de Memória. Certifique-se de que a **Memória Total** seja de pelo menos 128 GB.

e. Repita estas etapas para todos os Storage Nodes.

- Se um ou mais nós de armazenamento não tiverem memória total disponível suficiente, o valor do Espaço Reservado para Metadados não poderá ser aumentado. Não prossiga com este procedimento.
- Se cada nó de armazenamento tiver pelo menos 128 GB de memória total, vá para a próxima etapa.

4. Atualize a configuração de Espaço Reservado para Metadados.

a. Selecione **Configuração** > **Sistema** > **Configurações de armazenamento**.

b. Selecione **Espaço Reservado para Metadados**.

c. Insira o novo valor.

Por exemplo, para inserir 8 TB, que é o valor máximo suportado, digite **8000000000000** (8, seguido de 12 zeros)

d. Selecione **Salvar**.

Compactar objetos armazenados no StorageGRID

Você pode habilitar a compactação de objetos para reduzir o tamanho dos objetos armazenados no StorageGRID, para que os objetos consumam menos armazenamento.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Sobre esta tarefa

Por padrão, a compressão de objetos está desativada. Se você ativar a compressão, StorageGRID tenta comprimir cada objeto ao salvá-lo, usando compressão sem perdas.

Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e escalabilidade.

Antes de ativar a compactação de objetos, esteja ciente do seguinte:

- Você não deve selecionar **Comprimir objetos armazenados** a menos que saiba que os dados armazenados são compressíveis.
- Aplicações que salvam objetos no StorageGRID podem compactar os objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, selecionar esta opção não reduzirá ainda mais o tamanho do objeto.
- Não selecione **Comprimir objetos armazenados** se você estiver usando NetApp FabricPool com StorageGRID.

- Se a opção **Comprimir objetos armazenados** estiver selecionada, os aplicativos cliente do S3 devem evitar realizar operações GetObject que especifiquem um intervalo de bytes a ser retornado. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar os objetos para acessar os bytes solicitados. Operações GetObject que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB de um objeto compactado de 50 GB.

  Se intervalos forem lidos de objetos compactados, 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 do aplicativo.

Passos

1. Selecione **Configuração** > **Sistema** > **Configurações de armazenamento** > **Compressão de objetos**.
2. Selecione a caixa de seleção **Comprimir objetos armazenados**.
3. Selecione **Salvar**.

Gerencie nós de armazenamento completos no StorageGRID

À medida que os nós de armazenamento atingem a capacidade, você deve expandir o sistema StorageGRID por meio da adição de novo storage. Existem três opções disponíveis: adicionar volumes de storage, adicionar prateleiras de expansão de storage e adicionar nós de armazenamento.

Adicionar volumes de storage

Cada Storage Node suporta um número máximo de volumes de storage. O máximo definido varia de acordo com a plataforma. Se um Storage Node contiver menos do que o número máximo de volumes de storage, você pode adicionar volumes para aumentar sua capacidade. Veja as instruções para "Expandindo um sistema StorageGRID".

Adicionar prateleiras de expansão de storage

Alguns StorageGRID appliance Storage Nodes, como o SG6060 ou o SG6160, podem suportar prateleiras de armazenamento adicionais. Se você tiver StorageGRID appliances com capacidade de expansão que ainda não foram expandidos ao máximo, pode adicionar prateleiras de armazenamento para aumentar a capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

Adicionar nós de armazenamento

Você pode aumentar a capacidade de storage adicionando Storage Nodes. Ao adicionar storage, é necessário considerar cuidadosamente as regras ILM ativas e os requisitos de capacidade. Consulte as instruções para "Expandindo um sistema StorageGRID".

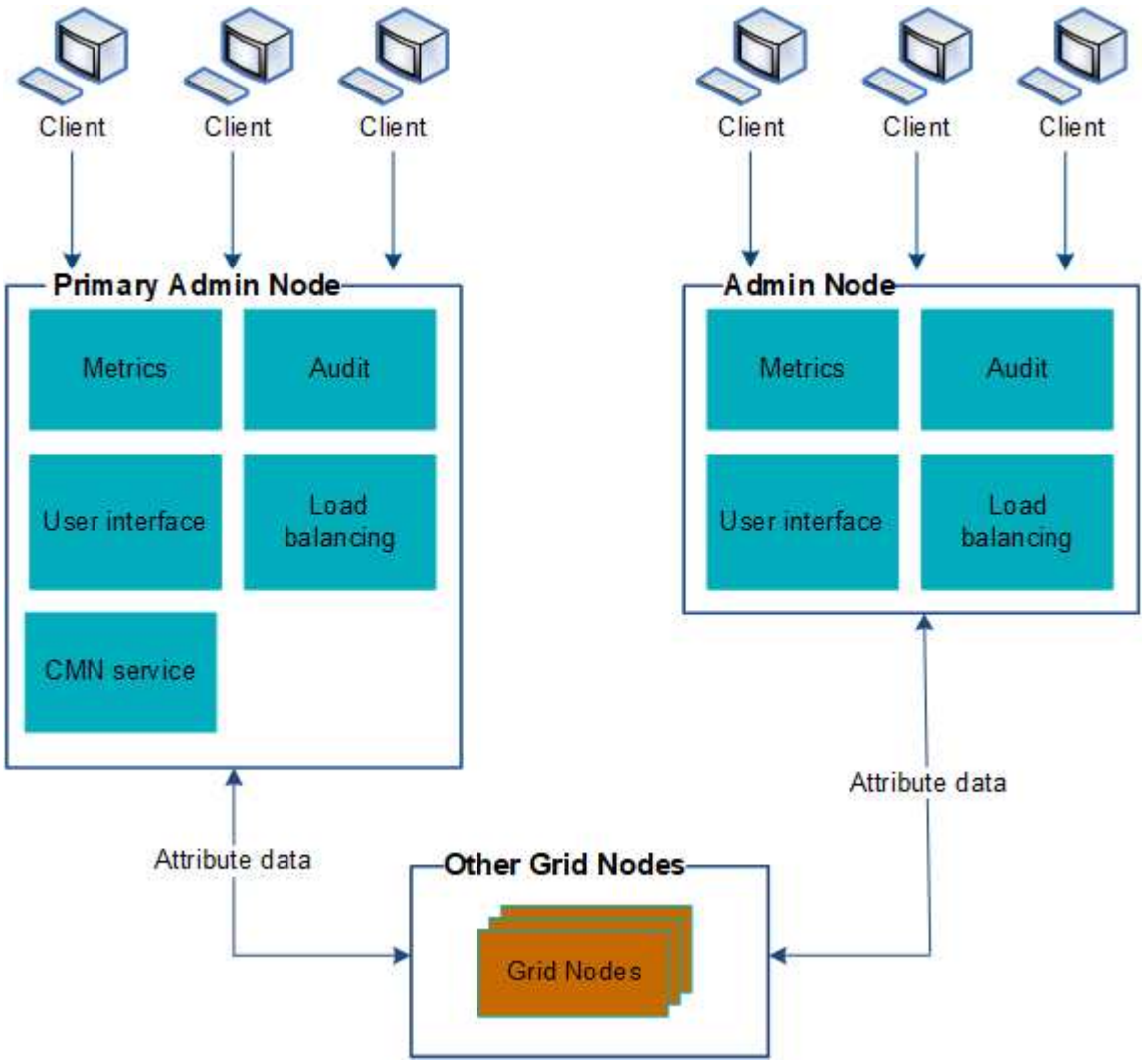
Gerenciar nós de administração

Use vários nós de administração no StorageGRID

Um sistema StorageGRID pode incluir vários nós de administração para que você possa monitorar e configurar seu sistema StorageGRID continuamente, mesmo que um nó de

administração falhe.

Se um nó administrativo ficar indisponível, o processamento de atributos continua, os alertas ainda são acionados e as notificações por e-mail e os pacotes AutoSupport ainda são enviados. No entanto, ter vários nós administrativos não oferece proteção contra falhas, exceto para notificações e pacotes AutoSupport.



Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID caso um nó de administração falhe:

- Os clientes web podem se reconectar a qualquer outro Admin Node disponível.
- Se um administrador do sistema tiver configurado um grupo de alta disponibilidade de Nós de Administração, os clientes web podem continuar a acessar o Grid Manager ou o Tenant Manager usando o endereço IP virtual do grupo de alta disponibilidade. Consulte "Gerenciar grupos de alta disponibilidade".

> Ao usar um grupo de alta disponibilidade (HA), o acesso é interrompido se o nó de administração ativo falhar. Os usuários precisam fazer login novamente depois que o endereço IP virtual do grupo HA for transferido para outro nó de administração do grupo.

Algumas tarefas de manutenção só podem ser realizadas usando o nó de administração primário. Se o nó de administração primário falhar, ele deverá ser recuperado antes que o sistema StorageGRID volte a funcionar plenamente.

Identifique o nó de administração principal no StorageGRID

O nó de administração principal oferece mais funcionalidades do que os nós de administração não principais. Por exemplo, alguns procedimentos de manutenção devem ser realizados usando o nó de administração principal.

Para obter mais informações sobre nós de administração, consulte "O que é um nó de administração".

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".

Passos

1. Selecione **Nós**.
2. Digite **principal** na caixa de pesquisa.

   Nos resultados da pesquisa, identifique o nó com "Primary Admin Node" exibido na coluna Tipo. Um Primary Admin Node deve ser listado.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

Informações sobre marcas comerciais

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