Configurando conexões de cliente S3 e Swift

StorageGRID

NetApp
October 03, 2025

Índice

Configurando conexões de cliente S3 e Swift

Como administrador de grade, você gerencia as opções de configuração que controlam como os locatários S3 e Swift podem conetar aplicativos clientes ao seu sistema StorageGRID para armazenar e recuperar dados. Existem várias opções diferentes para atender a diferentes requisitos de cliente e locatário.

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

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

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

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

Opcionalmente, você pode configurar os seguintes recursos em seu sistema StorageGRID:

- **Serviço de balanceamento de carga**: Você permite que os clientes usem o serviço de balanceamento de carga criando pontos de extremidade do balanceador de carga para conexões de cliente. Ao criar um endpoint de balanceador de carga, você especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).
- **Rede Cliente não confiável**: Você pode tornar a rede Cliente mais segura configurando-a como não confiável. Quando a rede do cliente não é confiável, os clientes só podem se conetar usando pontos de extremidade do balanceador de carga.
- **Grupos de alta disponibilidade**: Você pode criar um grupo de HA de nós de Gateway ou nós de administrador para criar uma configuração de backup ativo ou usar DNS de round-robin ou um balanceador de carga de terceiros e vários grupos de HA para obter uma configuração ativo-ativo. As conexões de cliente são feitas usando os endereços IP virtuais de grupos HA.

Você também pode habilitar o uso de HTTP para clientes que se conetam ao StorageGRID diretamente aos nós de armazenamento ou usando o serviço CLB (obsoleto), e você pode configurar nomes de domínio de endpoint de API S3 para clientes S3.

Resumo: Endereços IP e portas para conexões de clientes

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

Sobre esta tarefa

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os

endereços IP e as portas usadas para cada tipo de conexão. As instruções descrevem como localizar essas informações no Gerenciador de Grade se os pontos de extremidade do balanceador de carga e os grupos de alta disponibilidade (HA) já estiverem configurados.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	• Porta de extremidade do balanceador de carga
Grupo HA	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: • HTTPS:8083 • HTTP:8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	• Porta de extremidade do balanceador de carga
Nó de gateway	CLB **Nota:** o serviço CLB está obsoleto.	Endereço IP do nó de gateway **Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: • HTTPS:8083 • HTTP:8085
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: • HTTPS: 18083 • HTTP:18085

Exemplos

Para conetar um cliente S3 ao ponto de extremidade do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

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

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.5:10443`

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

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

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

- `https://192.0.2.6:10444`

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

Passos

1. Faça login no Gerenciador de Grade usando um navegador compatível.
2. Para localizar o endereço IP de um nó de grade:
   a. Selecione **nós**.
   b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual deseja se conetar.
   c. Selecione a guia **Visão geral**.
   d. Na seção informações do nó, observe os endereços IP do nó.
   e. Clique em **Mostrar mais** para visualizar endereços IPv6 e mapeamentos de interface.

      Você pode estabelecer conexões de aplicativos cliente para qualquer um dos endereços IP na lista:

      - **eth0:** rede de Grade
      - **eth1:** Admin Network (opcional)
      - **eth2:** rede de clientes (opcional)

      > Se você estiver exibindo um nó de administrador ou um nó de gateway e for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de HA será exibido em eth2.

3. Para localizar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.
   b. Na tabela, anote o endereço IP virtual do grupo HA.
4. Para localizar o número da porta de um endpoint do Load Balancer:
   a. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

A página Load Balancer Endpoints é exibida, mostrando a lista de endpoints que já foram configurados.

b. Selecione um endpoint e clique em **Editar endpoint**.

A janela Editar ponto final abre-se e apresenta detalhes adicionais sobre o ponto final.

c. Confirme se o endpoint selecionado está configurado para uso com o protocolo correto (S3 ou Swift) e, em seguida, clique em **Cancelar**.

d. Observe o número da porta do endpoint que você deseja usar para uma conexão de cliente.

> Se o número da porta for 80 ou 443, o endpoint será configurado apenas em nós de Gateway, uma vez que essas portas estão reservadas em nós de administração. Todas as outras portas são configuradas nos nós de Gateway e nos de Admin.

Gerenciamento do balanceamento de carga

Você pode usar as funções de balanceamento de carga do StorageGRID para lidar com cargas de trabalho de ingestão e recuperação de clientes S3 e Swift. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo cargas de trabalho e conexões entre vários nós de storage.

Você pode obter balanceamento de carga em seu sistema StorageGRID das seguintes maneiras:

- Use o serviço Load Balancer, que é instalado em nós de administração e nós de gateway. O serviço Load Balancer fornece balanceamento de carga de camada 7 e executa o encerramento TLS das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage. Este é o mecanismo de balanceamento de carga recomendado.
- Use o serviço CLB (Connection Load Balancer), que é instalado somente em nós de Gateway. O serviço CLB fornece balanceamento de carga da camada 4 e suporta custos de link.

  > O serviço CLB está obsoleto.

- Integre um balanceador de carga de terceiros. Entre em Contato com o representante da sua conta NetApp para obter detalhes.

Como funciona o balanceamento de carga - Serviço do Load Balancer

O serviço Load Balancer distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Para ativar o balanceamento de carga, você deve configurar pontos de extremidade do balanceador de carga usando o Gerenciador de Grade.

Você pode configurar pontos de extremidade do balanceador de carga somente para nós de administrador ou nós de gateway, uma vez que esses tipos de nó contêm o serviço Load Balancer. Não é possível configurar pontos de extremidade para nós de storage ou nós de arquivamento.

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo (HTTP ou HTTPS), um tipo de serviço (S3 ou Swift) e um modo de encadernação. Os endpoints HTTPS requerem um certificado de servidor. Os modos de vinculação permitem restringir a acessibilidade das portas de endpoint a:

- Endereços IP virtuais (VIPs) específicos de alta disponibilidade (HA)
- Interfaces de rede específicas de nós específicos

Considerações de porta

Os clientes podem acessar qualquer um dos pontos de extremidade que você configurar em qualquer nó executando o serviço Load Balancer, com duas exceções: As portas 80 e 443 são reservadas em nós de administração, portanto, os pontos de extremidade configurados nessas portas suportam operações de balanceamento de carga somente em nós de Gateway.

Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

O serviço CLB está obsoleto.

Disponibilidade da CPU

O serviço Load Balancer em cada nó de administração e nó de gateway opera independentemente ao encaminhar tráfego S3 ou Swift para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU. As informações de carga da CPU do nó são atualizadas a cada poucos minutos, mas a ponderação pode ser atualizada com mais frequência. Todos os nós de storage recebem um valor mínimo de peso básico, mesmo que um nó informe a utilização de 100% ou não consiga relatar sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU estão limitadas ao local onde o serviço Load Balancer está localizado.

Informações relacionadas

"Manter recuperar"

Configuração dos pontos de extremidade do balanceador de carga

Você pode criar, editar e remover pontos de extremidade do balanceador de carga.

Criação de pontos de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo de rede (HTTP ou HTTPS) e um tipo de serviço (S3 ou Swift). Se criar um endpoint HTTPS, tem de carregar ou gerar um certificado de servidor.

O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Se você tiver anteriormente as portas remapeadas que pretende usar para o serviço Load Balancer, você deve ter removido os remapes.

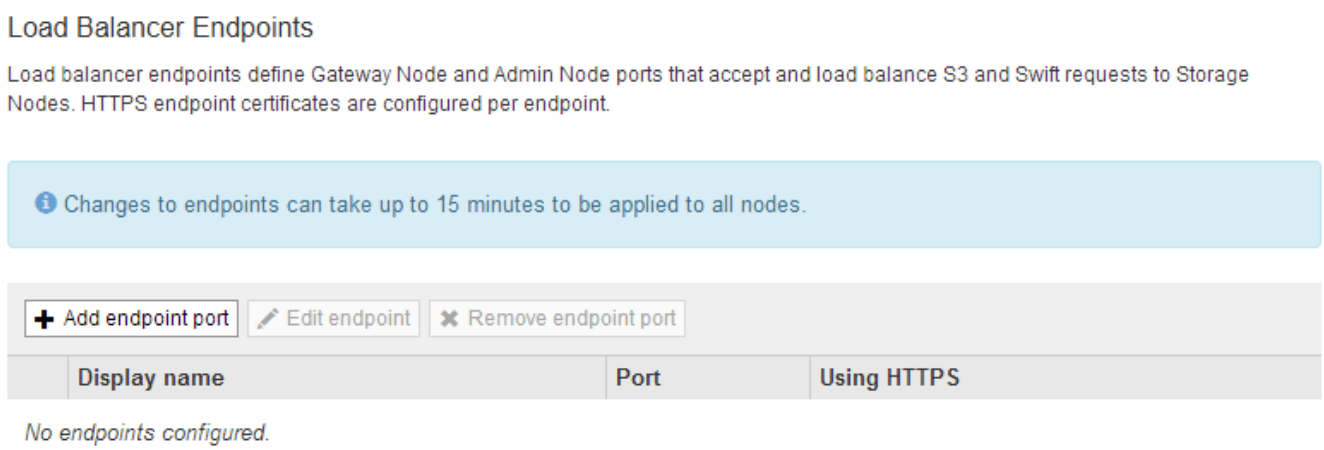
Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

O serviço CLB está obsoleto.

Passos

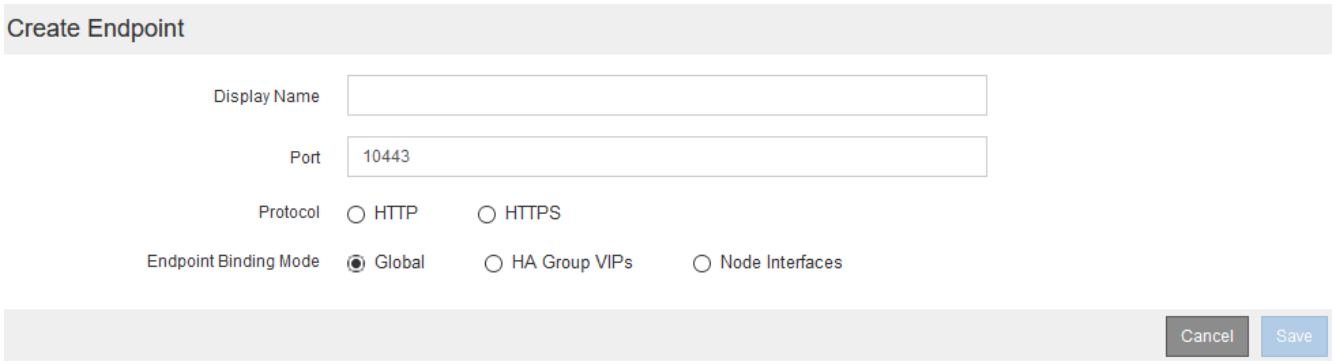
1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida.



2. Selecione **Adicionar endpoint**.

   A caixa de diálogo criar ponto final é exibida.



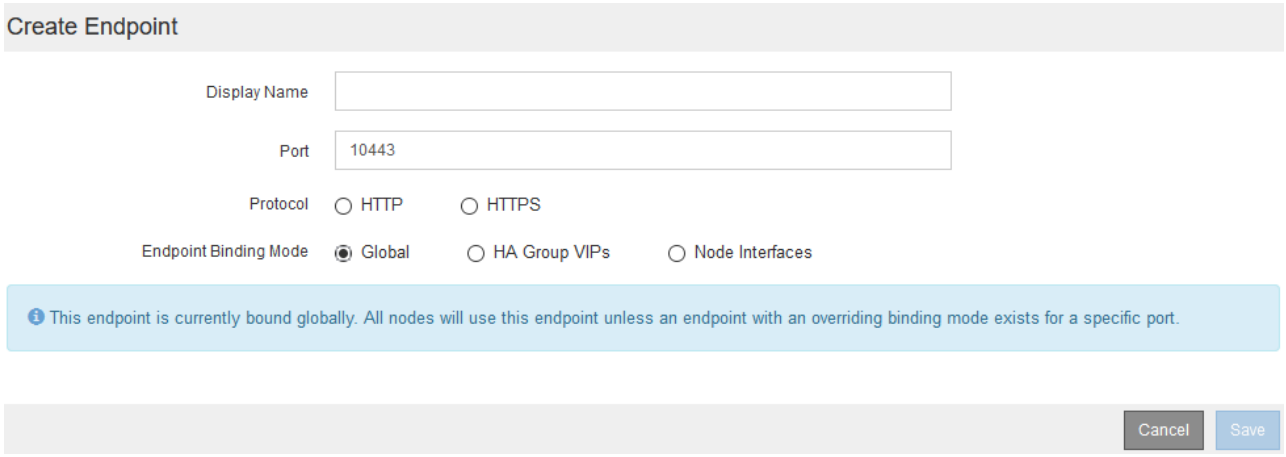
3. Insira um nome de exibição para o endpoint, que aparecerá na lista na página Load Balancer Endpoints.
4. Introduza um número de porta ou deixe o número de porta pré-preenchido como está.

   Se você inserir o número da porta 80 ou 443, o endpoint será configurado somente nos nós do Gateway, uma vez que essas portas serão reservadas nos nós de administração.

   As portas usadas por outros serviços de grade não são permitidas. Consulte as diretrizes de rede para obter uma lista de portas usadas para comunicações internas e externas.

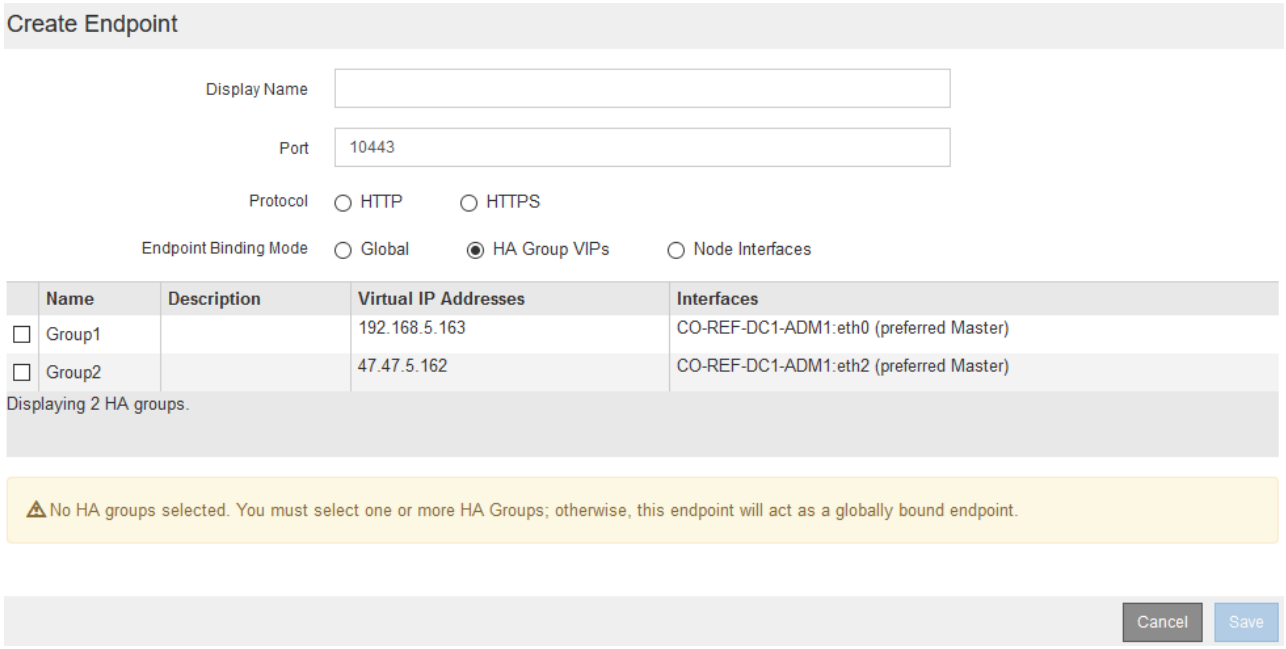
5. Selecione **HTTP** ou **HTTPS** para especificar o protocolo de rede para este endpoint.
6. Selecione um modo de encadernação de endpoint.

   - **Global** (padrão): O endpoint está acessível em todos os nós de Gateway e nós de Admin no número de porta especificado.



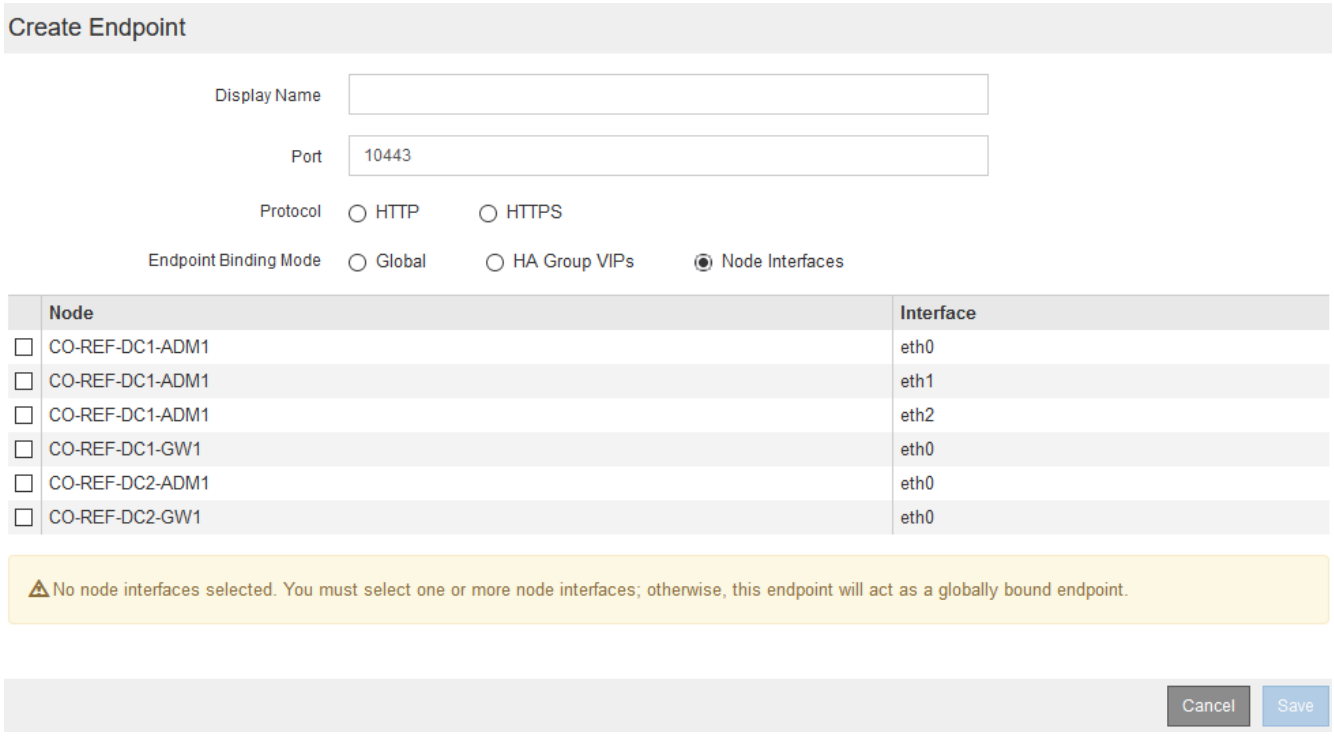
   - **VIPs do grupo HA**: O endpoint só pode ser acessado através dos endereços IP virtuais definidos para os grupos de HA selecionados. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta, desde que os grupos de HA definidos por esses endpoints não se sobreponham entre si.

     Selecione os grupos de HA com os endereços IP virtuais onde deseja que o endpoint apareça.



   - * Interfaces de nó*: O ponto de extremidade é acessível apenas nos nós designados e interfaces de rede. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta desde que essas interfaces não se sobreponham umas às outras.

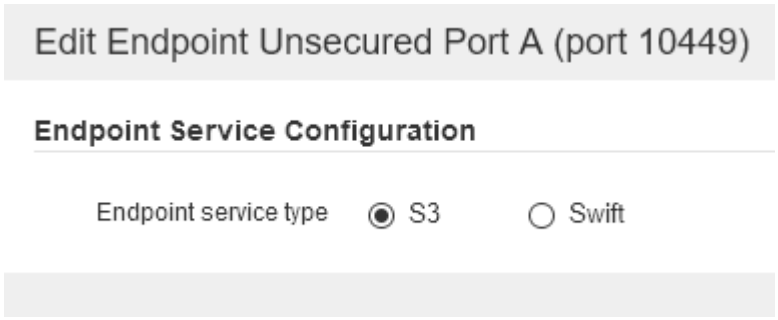
     Selecione as interfaces de nó em que você deseja que o endpoint apareça.



7. Selecione **Guardar**.

   A caixa de diálogo Editar ponto final é exibida.

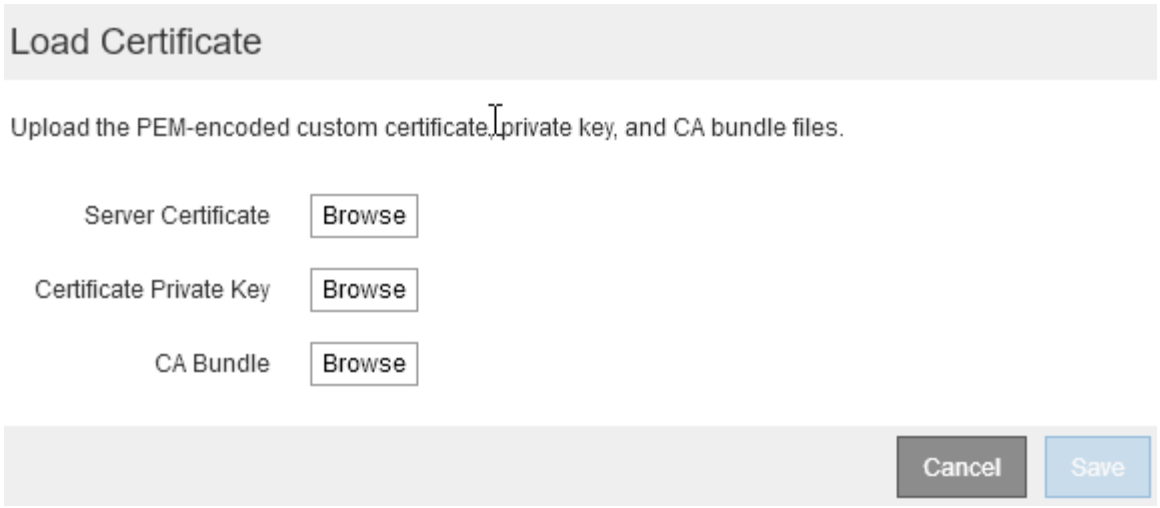
8. Selecione **S3** ou **Swift** para especificar o tipo de tráfego que este endpoint irá servir.



9. Se você selecionou **HTTP**, selecione **Salvar**.

   O ponto final não protegido é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

10. Se selecionou **HTTPS** e pretende carregar um certificado, selecione **carregar certificado**.



a. Procure o certificado do servidor e a chave privada do certificado.

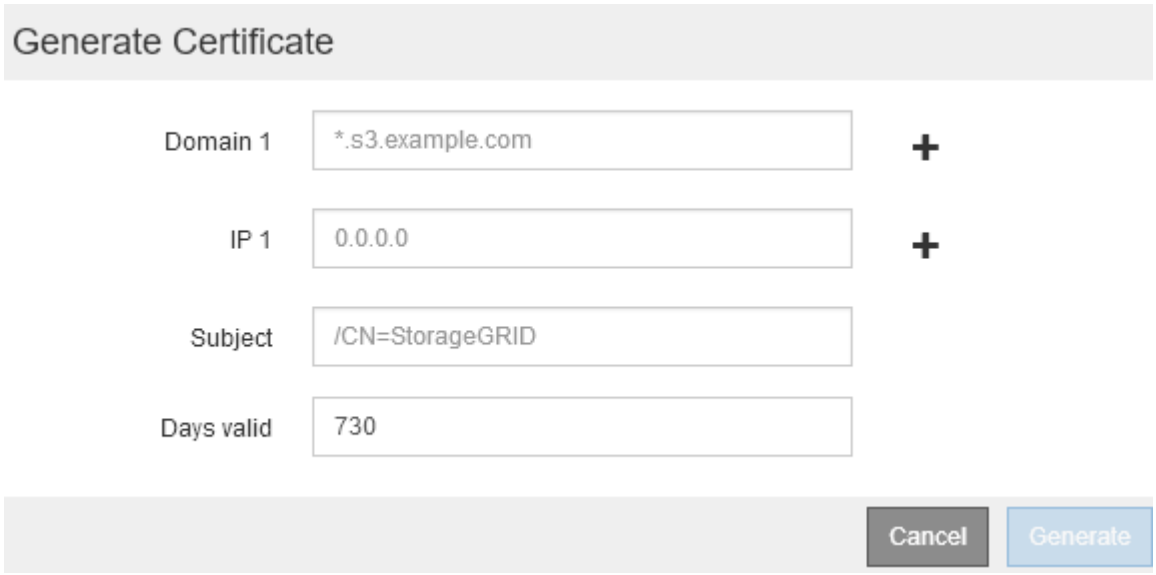
   Para permitir que os clientes S3 se conetem usando um nome de domínio de endpoint da API S3, use um certificado de domínio multidomínio ou curinga que corresponda a todos os nomes de domínio que o cliente possa usar para se conetar à grade. Por exemplo, o certificado do servidor pode usar o nome de domínio `*.example.com` .

"Configurando nomes de domínio de endpoint da API S3"

a. Opcionalmente, procure um pacote de CA.
b. Selecione **Guardar**.

   Os dados de certificado codificados em PEM para o endpoint são exibidos.

11. Se você selecionou **HTTPS** e deseja gerar um certificado, selecione **Generate Certificate**.



a. Introduza um nome de domínio ou um endereço IP.

   Você pode usar wildcards para representar os nomes de domínio totalmente qualificados de todos os nós de administrador e nós de gateway que executam o serviço Load Balancer. Por exemplo, `*.sgws.foo.com` usa o caractere curinga * para representar `gn1.sgws.foo.com` e

`gn2.sgws.foo.com`.

"Configurando nomes de domínio de endpoint da API S3"

a. ➕Selecione para adicionar outros nomes de domínio ou endereços IP.

   Se você estiver usando grupos de alta disponibilidade (HA), adicione os nomes de domínio e endereços IP dos IPs virtuais de HA.

b. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar quem possui o certificado.

c. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.

d. Selecione **Generate**.

   Os metadados do certificado e os dados do certificado codificados em PEM para o endpoint são exibidos.

12. Clique em **Salvar**.

    O endpoint é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

Informações relacionadas

"Manter recuperar"

"Diretrizes de rede"

"Gerenciamento de grupos de alta disponibilidade"

"Gerenciando redes de clientes não confiáveis"

Editar pontos de extremidade do balanceador de carga

Para um endpoint não protegido (HTTP), você pode alterar o tipo de serviço de endpoint entre S3 e Swift. Para um endpoint seguro (HTTPS), você pode editar o tipo de serviço de endpoint e exibir ou alterar o certificado de segurança.

O que você vai precisar

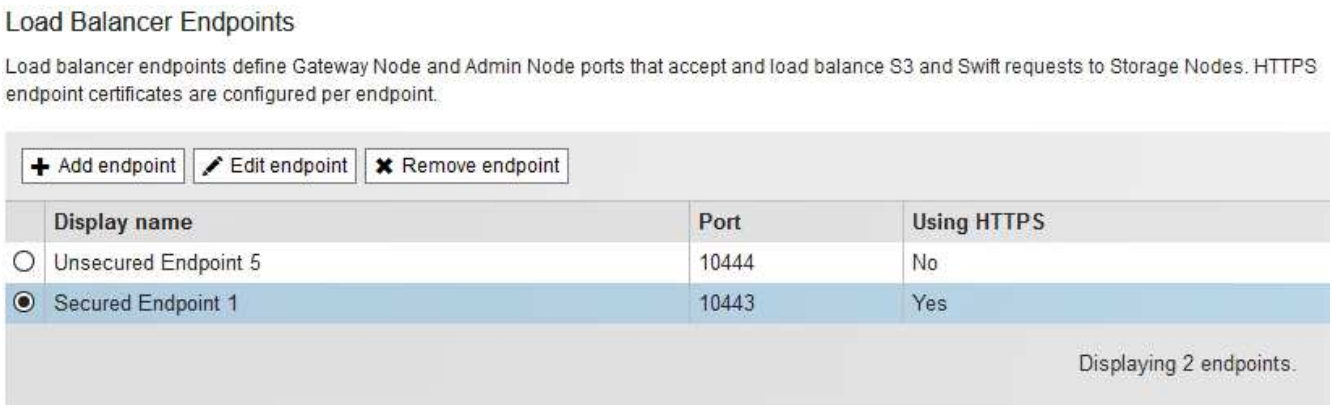
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.

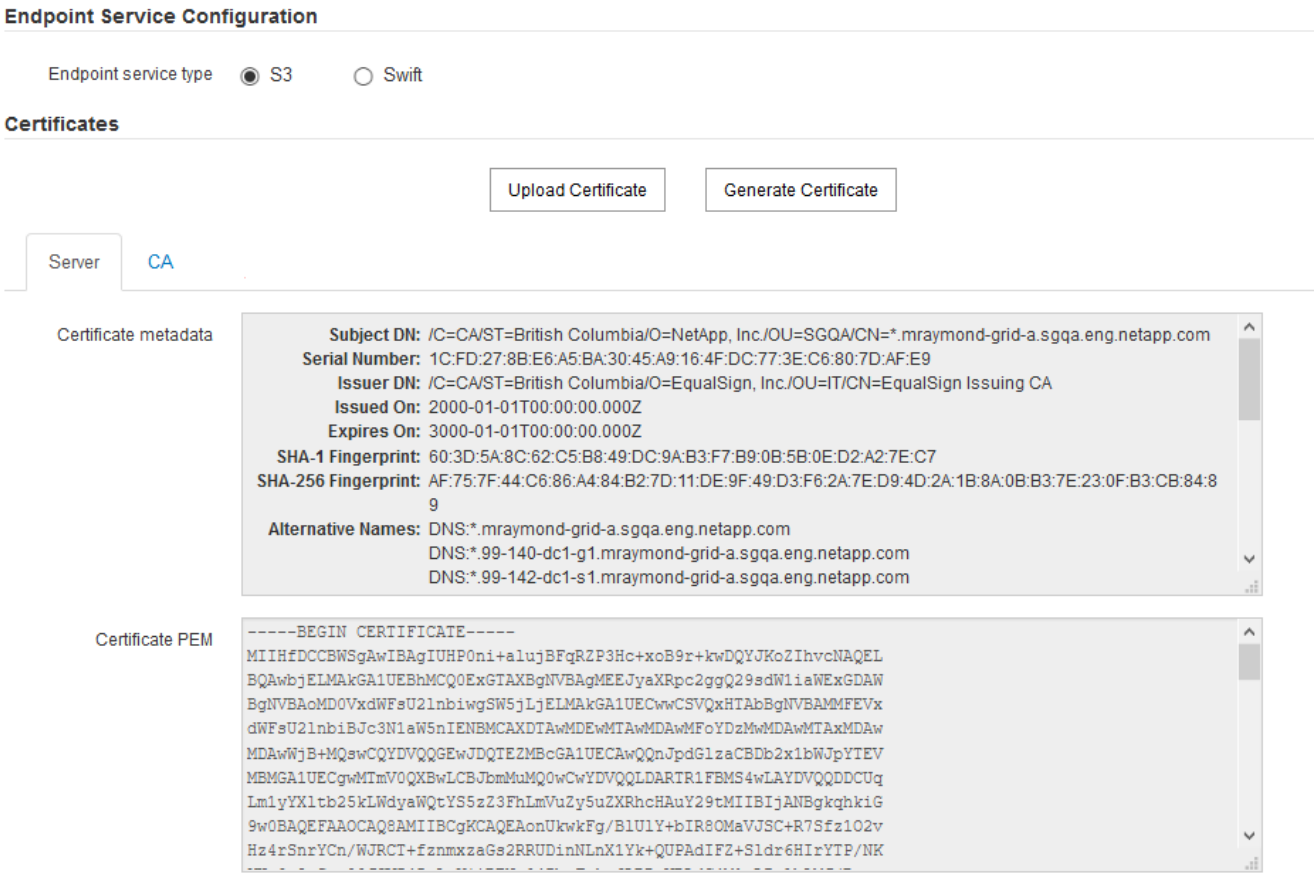
   Endpoints com certificados que expirarão em breve são identificados na tabela.



2. Selecione o ponto de extremidade que pretende editar.
3. Clique em **Editar endpoint**.

   A caixa de diálogo Editar ponto final é exibida.

   Para um ponto de extremidade não protegido (HTTP), apenas a secção Configuração do serviço de extremidade da caixa de diálogo é apresentada. Para um ponto de extremidade seguro (HTTPS), as secções Configuração do serviço de extremidade e certificados da caixa de diálogo são apresentadas, conforme ilustrado no exemplo seguinte.



4. Faça as alterações desejadas no endpoint.

   Para um endpoint não protegido (HTTP), você pode:

- Altere o tipo de serviço de endpoint entre S3 e Swift.
- Altere o modo de encadernação de endpoint. Para um endpoint seguro (HTTPS), você pode:
- Altere o tipo de serviço de endpoint entre S3 e Swift.
- Altere o modo de encadernação de endpoint.
- Exibir o certificado de segurança.
- Carregue ou gere um novo certificado de segurança quando o certificado atual estiver expirado ou prestes a expirar.

  Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

> Para alterar o protocolo de um endpoint existente, por exemplo, de HTTP para HTTPS, você deve criar um novo endpoint. Siga as instruções para criar pontos de extremidade do balanceador de carga e selecione o protocolo desejado.

5. Clique em **Salvar**.

Informações relacionadas

Criação de pontos de extremidade do balanceador de carga

Remoção dos pontos finais do balanceador de carga

Se você não precisar mais de um ponto de extremidade do balanceador de carga, poderá removê-lo.

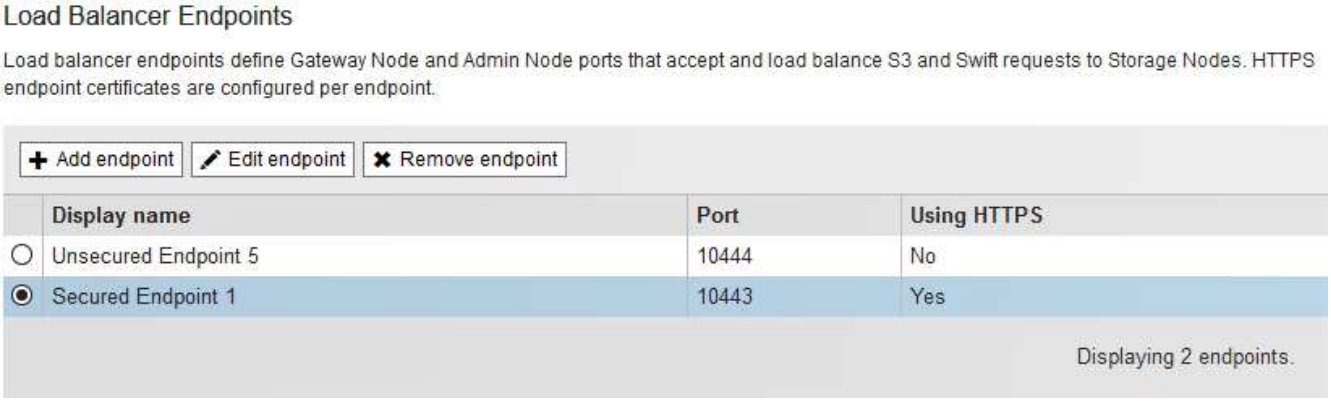
O que você vai precisar

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Passos

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.



2. Selecione o botão de opção à esquerda do ponto de extremidade que pretende remover.
3. Clique em **Remover endpoint**.

   É apresentada uma caixa de diálogo de confirmação.

4. Clique em **OK**.

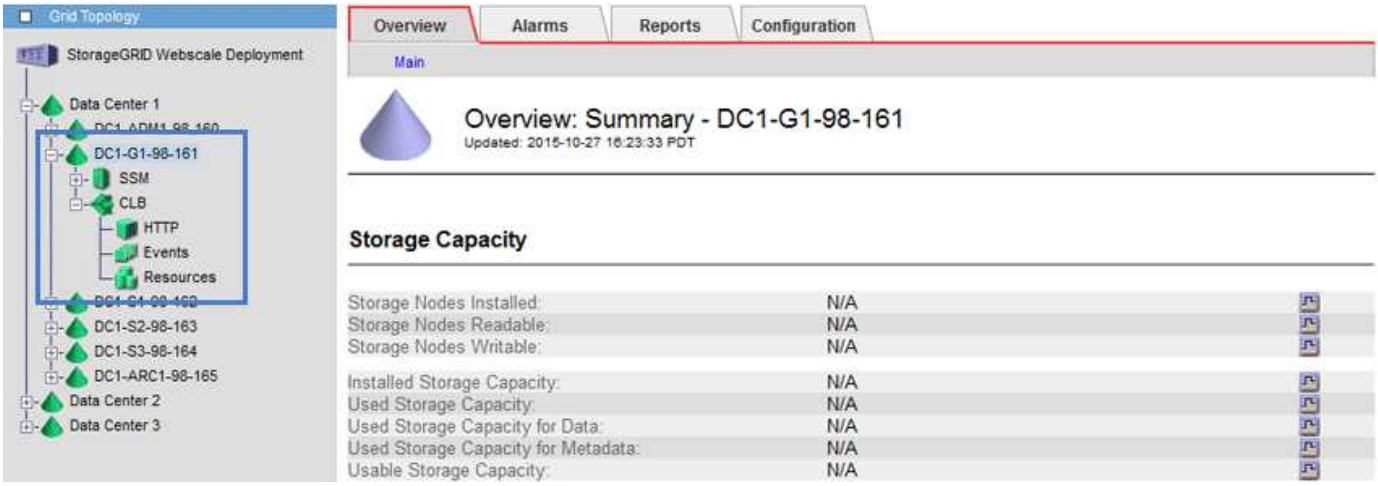
   O ponto final é removido.

Como funciona o balanceamento de carga - serviço CLB

O serviço CLB (Connection Load Balancer) nos nós de Gateway está obsoleto. O serviço Load Balancer é agora o mecanismo de balanceamento de carga recomendado.

O serviço CLB usa o balanceamento de carga da camada 4 para distribuir conexões de rede TCP de entrada de aplicativos clientes para o nó de armazenamento ideal com base na disponibilidade, carga do sistema e custo de link configurado pelo administrador. Quando o nó de armazenamento ideal é escolhido, o serviço CLB estabelece uma conexão de rede bidirecional e encaminha o tráfego de e para o nó escolhido. O CLB não considera a configuração da rede de Grade ao direcionar conexões de rede recebidas.

Para visualizar informações sobre o serviço CLB, selecione **Support** > **Tools** > **Grid Topology** e expanda um Gateway Node até selecionar **CLB** e as opções abaixo.



Se você optar por usar o serviço CLB, considere configurar os custos de link para o seu sistema StorageGRID.

Informações relacionadas

"Quais são os custos da ligação"

"Atualizar custos de link"

Gerenciando redes de clientes não confiáveis

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de clientes de entrada apenas em endpoints configurados explicitamente.

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todas as portas externas disponíveis (consulte as informações sobre comunicações externas nas diretrizes de rede).

Você pode reduzir a ameaça de ataques hostis em seu sistema StorageGRID especificando que a rede de clientes em cada nó seja *não confiável*. Se a rede de cliente de um nó não for confiável, o nó só aceita conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

Exemplo 1: O Gateway Node aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway recuse todo o tráfego de entrada na rede do cliente, exceto para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na página Load Balancer Endpoints, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página redes de clientes não confiáveis, especifique que a rede de cliente no nó de gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede de clientes do nó de Gateway será descartado, exceto para solicitações HTTPS S3 na porta 443 e ICMP echo (ping).

Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma

Suponha que você queira ativar o tráfego de serviço de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede cliente. Você executaria este passo geral:

- Na página redes de clientes não confiáveis, indique que a rede de cliente no nó de armazenamento não é confiável.

Depois de salvar sua configuração, o nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para a Amazon Web Services.

Informações relacionadas

"Diretrizes de rede"

"Configuração dos pontos de extremidade do balanceador de carga"

Especificar a rede cliente de um nó não é confiável

Se você estiver usando uma rede de cliente, poderá especificar se a rede de cliente de cada nó é confiável ou não confiável. Você também pode especificar a configuração padrão para novos nós adicionados em uma expansão.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.

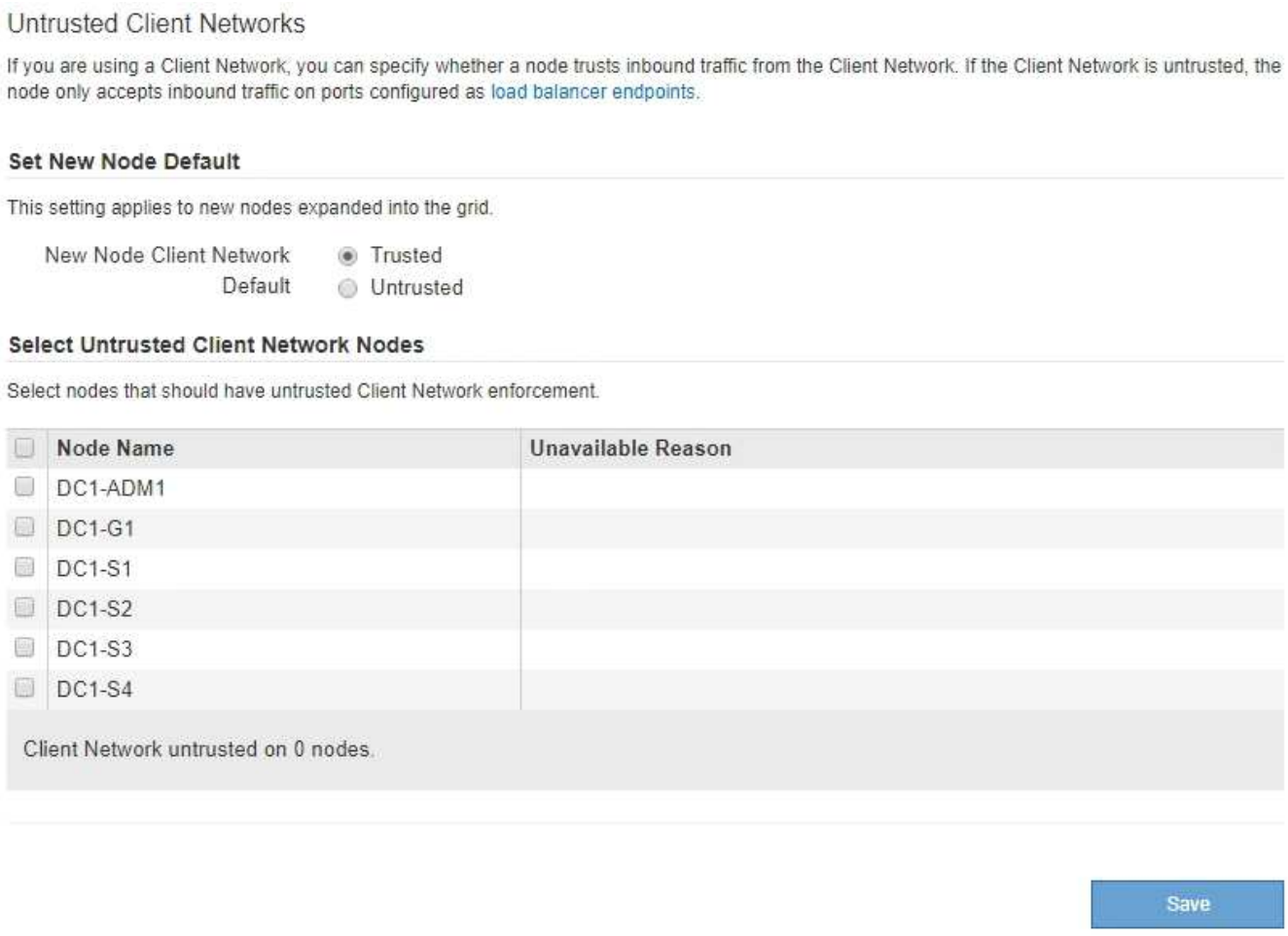
> As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **rede cliente não confiável**.

   A página redes de clientes não confiáveis é exibida.

   Esta página lista todos os nós no seu sistema StorageGRID. A coluna motivo indisponível inclui uma entrada se a rede do cliente no nó tiver de ser fidedigna.



2. Na seção **Definir novo padrão de nó**, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grade em um procedimento de expansão.
   - **Trusted**: Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável. Conforme necessário, você pode retornar a esta página para alterar a configuração de um novo nó específico.

Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Na seção **Selecione nós de rede de cliente não confiáveis**, selecione os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente.

   Você pode selecionar ou desmarcar a caixa de seleção no título para selecionar ou desmarcar todos os nós.

4. Clique em **Salvar**.

   As novas regras de firewall são imediatamente adicionadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Informações relacionadas

"Configuração dos pontos de extremidade do balanceador de carga"

Gerenciamento de grupos de alta disponibilidade

Grupos de alta disponibilidade (HA) podem ser usados para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift. Os GRUPOS HA também podem ser usados para fornecer conexões altamente disponíveis ao Gerenciador de Grade e ao Gerenciador de Locatário.

- "O que é um grupo HA"
- "Como os grupos de HA são usados"
- "Opções de configuração para grupos de HA"
- "Criando um grupo de alta disponibilidade"
- "Edição de um grupo de alta disponibilidade"
- "Removendo um grupo de alta disponibilidade"

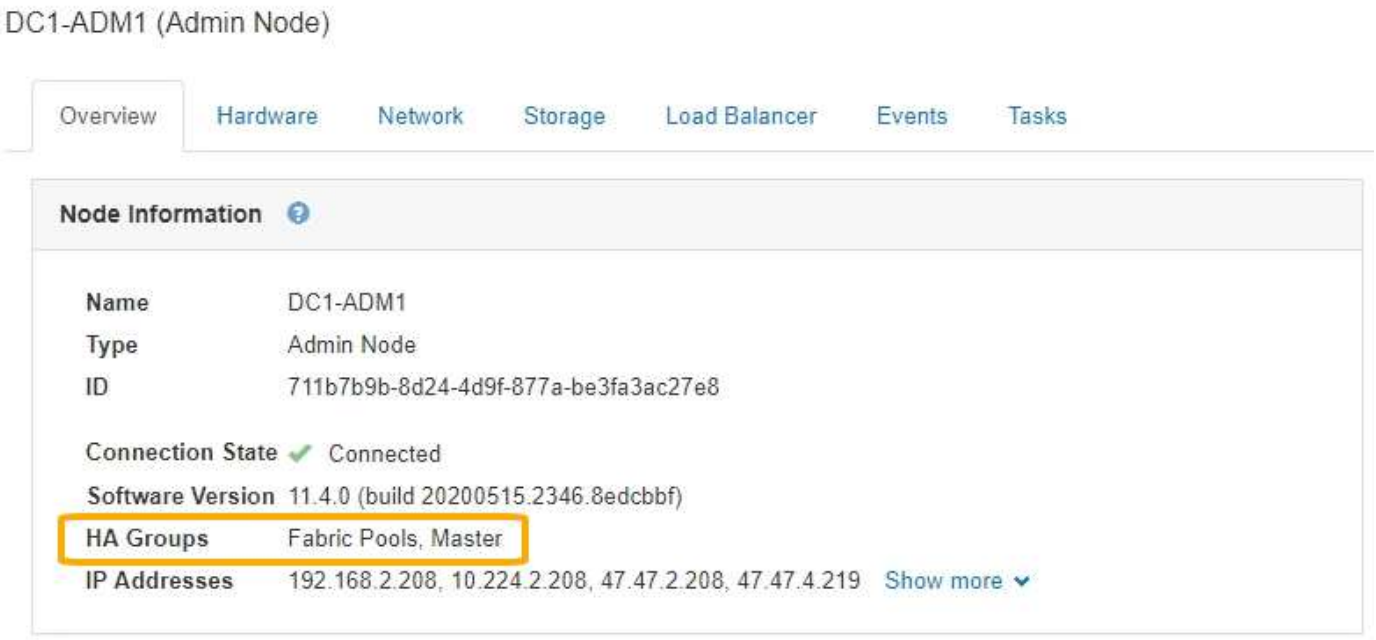
O que é um grupo HA

Os grupos de alta disponibilidade usam endereços IP virtuais (VIPs) para fornecer acesso de backup ativo aos serviços do nó de gateway ou nó de administrador.

Um grupo de HA consiste em uma ou mais interfaces de rede em nós de administração e nós de gateway. Ao criar um grupo HA, você seleciona interfaces de rede pertencentes à rede Grid (eth0) ou à rede Client (eth2). Todas as interfaces de um grupo HA devem estar dentro da mesma sub-rede de rede.

Um grupo de HA mantém um ou mais endereços IP virtuais que são adicionados à interface ativa no grupo. Se a interface ativa ficar indisponível, os endereços IP virtuais serão movidos para outra interface. Esse processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impactos e possam confiar em comportamentos normais de repetição para continuar a operação.

A interface ativa em um grupo HA é designada como Master. Todas as outras interfaces são designadas como Backup. Para visualizar estas designações, selecione **nodes** > ***node*** > **Overview**.



Ao criar um grupo HA, você especifica uma interface para ser o mestre preferido. O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup. Quando a falha é resolvida, os endereços VIP são automaticamente movidos de volta para o Master preferido.

O failover pode ser acionado por qualquer um destes motivos:

- O nó no qual a interface está configurada é desativado.
- O nó no qual a interface está configurada perde a conetividade com todos os outros nós por pelo menos 2 minutos
- A interface ativa desce.
- O serviço Load Balancer pára.
- O serviço de alta disponibilidade pára.

> O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pela falha do serviço CLB (obsoleto) ou serviços para o Gerenciador de Grade ou o Gerenciador de Tenant.

Se o grupo de HA incluir interfaces de mais de dois nós, a interface ativa poderá ser movida para a interface de qualquer outro nó durante o failover.

Como os grupos de HA são usados

Você pode querer usar grupos de alta disponibilidade (HA) por vários motivos.

- Um grupo de HA pode fornecer conexões administrativas altamente disponíveis ao Gerenciador de Grade ou ao Gerente do Locatário.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3 e Swift.
- Um grupo de HA que contém apenas uma interface permite fornecer muitos endereços VIP e definir explicitamente endereços IPv6.

Um grupo de HA poderá fornecer alta disponibilidade somente se todos os nós incluídos no grupo oferecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços de que você precisa.

- **Admin Nodes**: Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Gateway Nodes**: Incluem o serviço Load Balancer e o serviço CLB (obsoleto).

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao Grid Manager	• Nó de administração principal (**Mestre preferido**) • Nós de administração não primários **Nota:** o nó de administração principal deve ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.
Acesso apenas ao Gestor do Locatário	• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	• Nós de administração • Nós de gateway
Acesso ao cliente S3 ou Swift — serviço CLB **Nota:** o serviço CLB está obsoleto.	• Nós de gateway

Limitações do uso de grupos de HA com Grid Manager ou Tenant Manager

A falha de serviços para o Gerenciador de Grade ou o Gerenciador de locatário não aciona o failover dentro do grupo de HA.

Se você estiver conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconetado e deverá fazer login novamente para retomar sua tarefa.

Alguns procedimentos de manutenção não podem ser executados quando o nó de administração principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

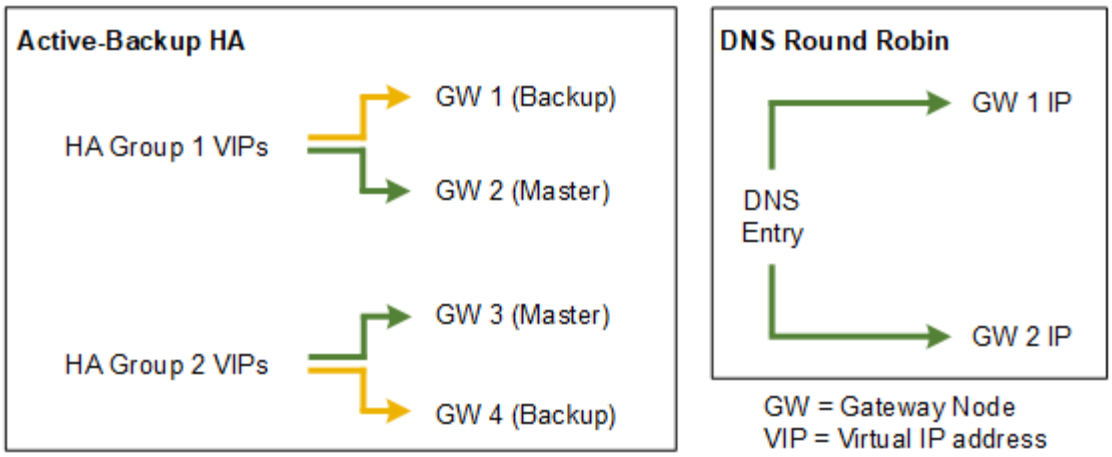
Limitações do uso de grupos HA com o serviço CLB

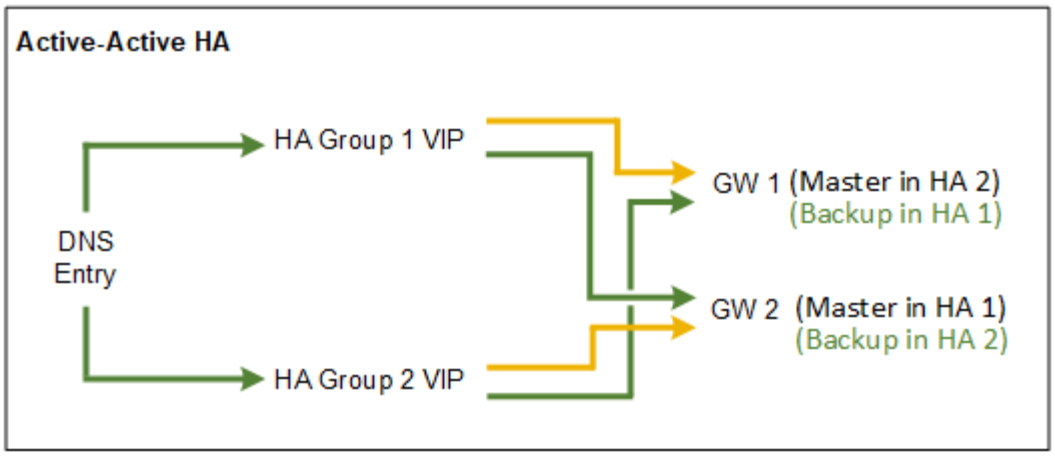
A falha do serviço CLB não aciona o failover no grupo HA.

O serviço CLB está obsoleto.

Opções de configuração para grupos de HA

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de HA. Cada opção tem vantagens e desvantagens.





Ao criar vários grupos de HA sobrepostos, como mostrado no exemplo de HA ativo-ativo, a taxa de transferência total é dimensionada com o número de nós e grupos de HA. Com três ou mais nós e três ou mais grupos de HA, você também pode continuar as operações usando qualquer um dos VIPs, mesmo durante procedimentos de manutenção que exigem que você coloque um nó off-line.

A tabela resume os benefícios de cada configuração de HA mostrada no diagrama.

Configuração	Vantagens	Desvantagens
Active-Backup HA	• Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido.	• Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo.
DNS Round Robin	• Maior taxa de transferência agregada. • Sem hosts ociosos.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Configuração	Vantagens	Desvantagens
Ativo-ativo	• O tráfego é distribuído em vários grupos de HA. • Alta taxa de transferência agregada que é dimensionada com o número de grupos de HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Criando um grupo de alta disponibilidade

Você pode criar um ou mais grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em nós de administração ou nós de gateway.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

Uma interface deve atender às seguintes condições para ser incluída em um grupo HA:

- A interface deve ser para um nó de gateway ou um nó de administrador.
- A interface deve pertencer à rede de Grade (eth0) ou à rede de Cliente (eth2).
- A interface deve ser configurada com endereçamento IP fixo ou estático, não com DHCP.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

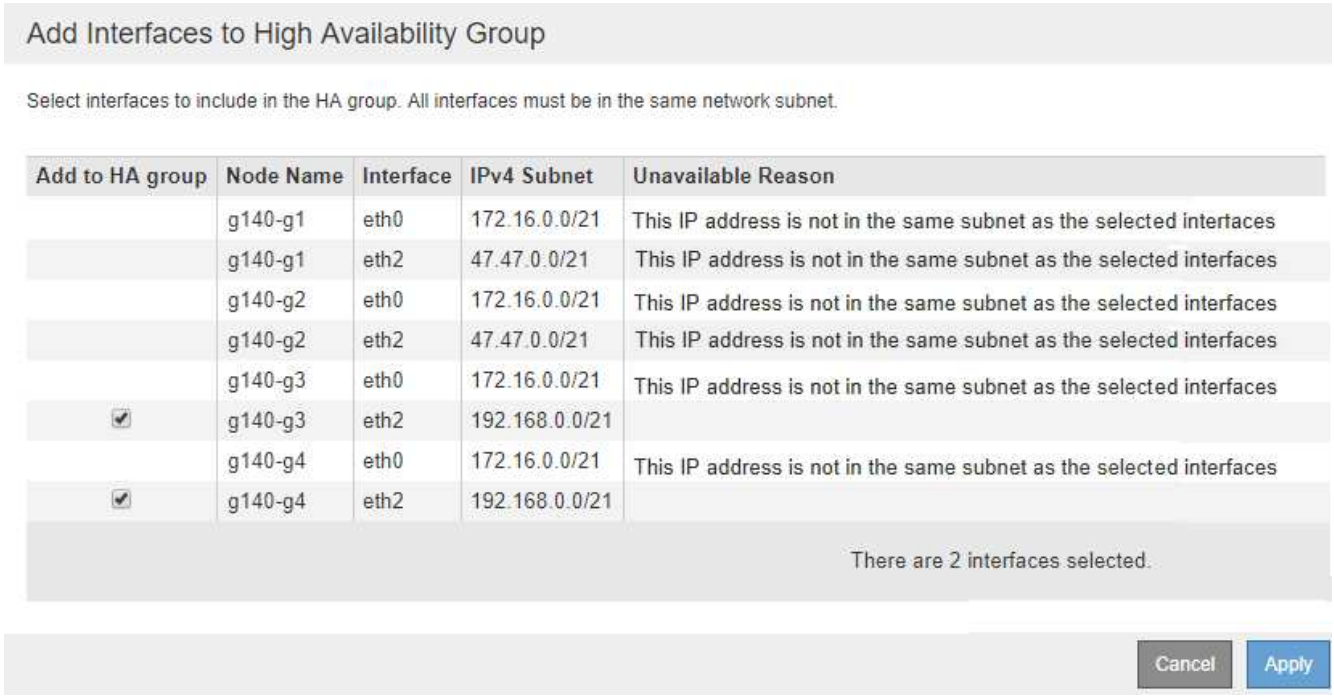
   A página grupos de alta disponibilidade é exibida.

2. Clique em **criar**.

   A caixa de diálogo criar Grupo de alta disponibilidade é exibida.

3. Digite um nome e, se desejado, uma descrição para o grupo HA.
4. Clique em **Select interfaces**.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida. A tabela lista nós, interfaces e sub-redes IPv4 elegíveis.



Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Na coluna **Adicionar ao grupo HA**, marque a caixa de seleção da interface que deseja adicionar ao grupo HA.

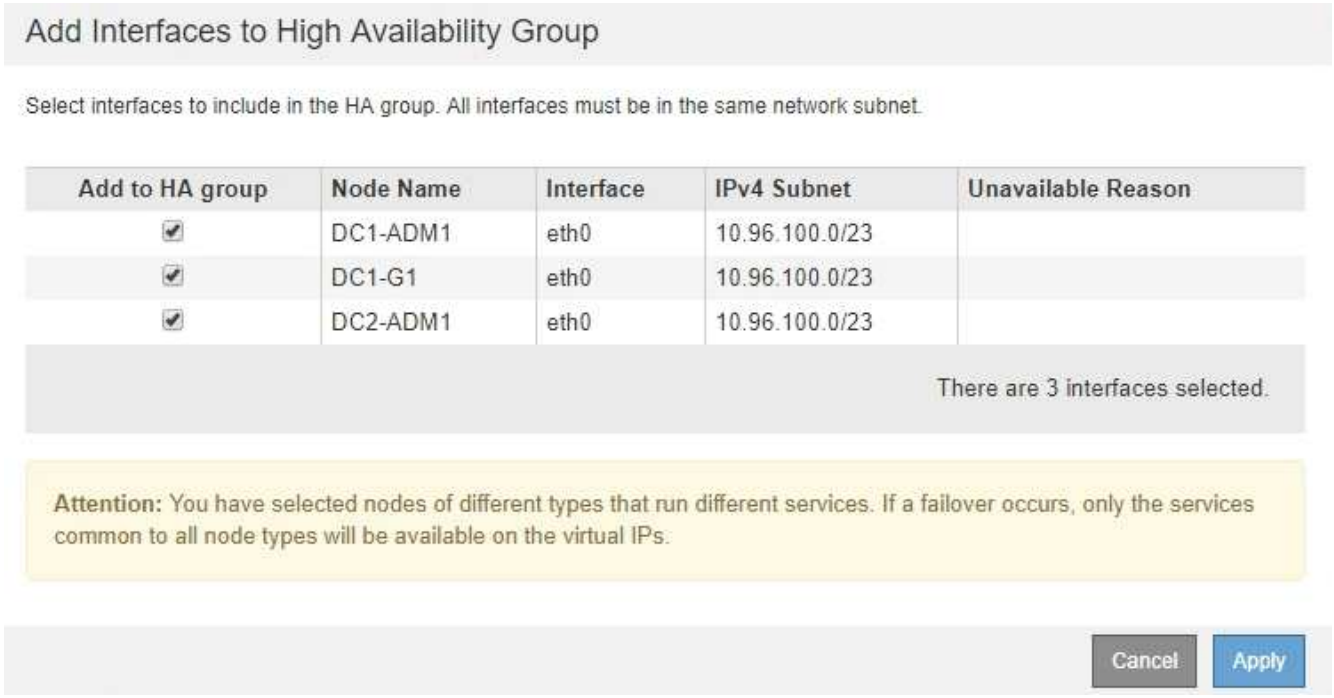
   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

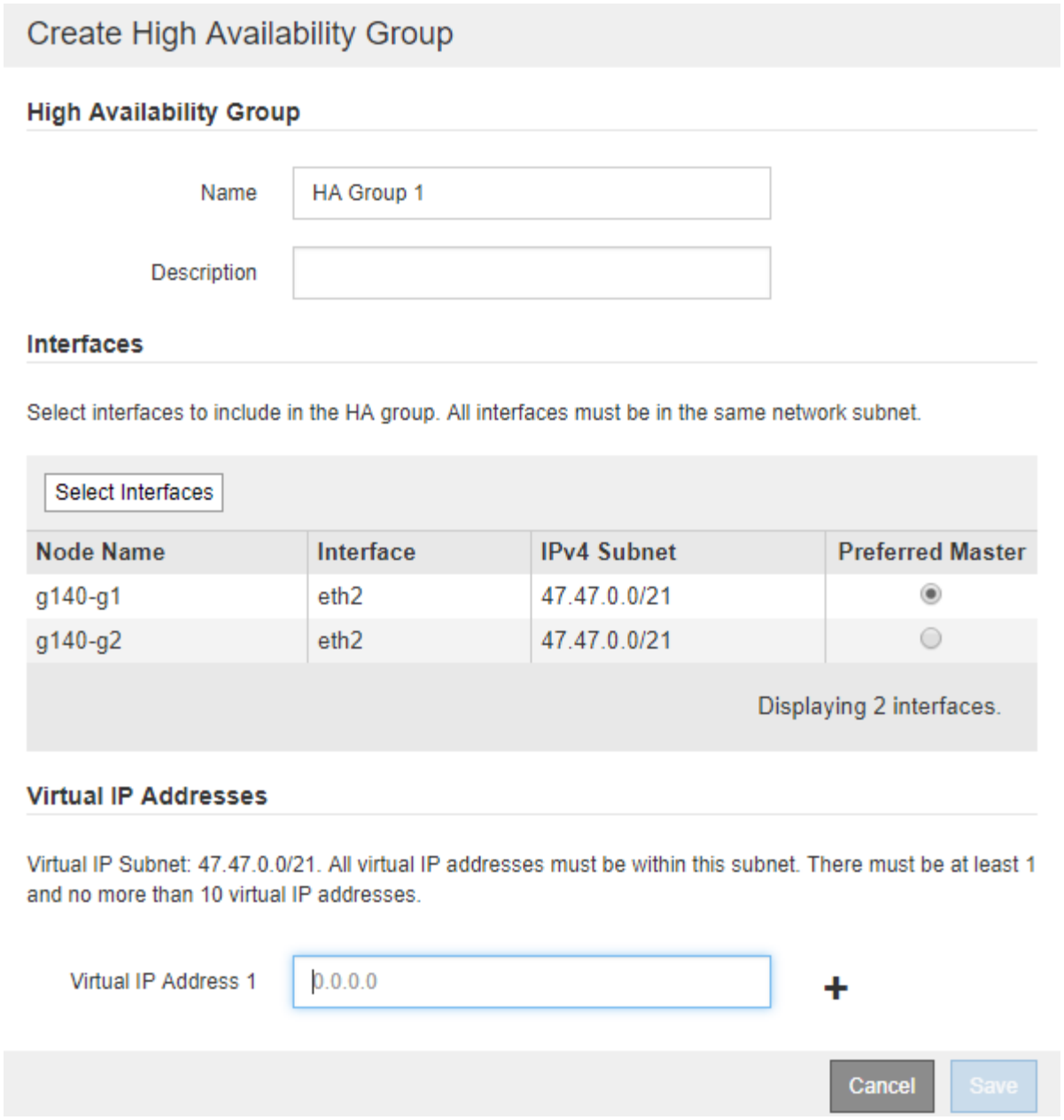
   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.



6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página criar Grupo de alta disponibilidade. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.



7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   > Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Na seção endereços IP virtuais da página, insira um a 10 endereços IP virtuais para o grupo HA. Clique no sinal de mais (+) para adicionar vários endereços IP.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

   Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é criado e agora você pode usar os endereços IP virtuais configurados.

Informações relacionadas

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale o VMware"

"Instale Ubuntu ou Debian"

"Gerenciamento do balanceamento de carga"

Edição de um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces ou adicionar ou atualizar um endereço IP virtual.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

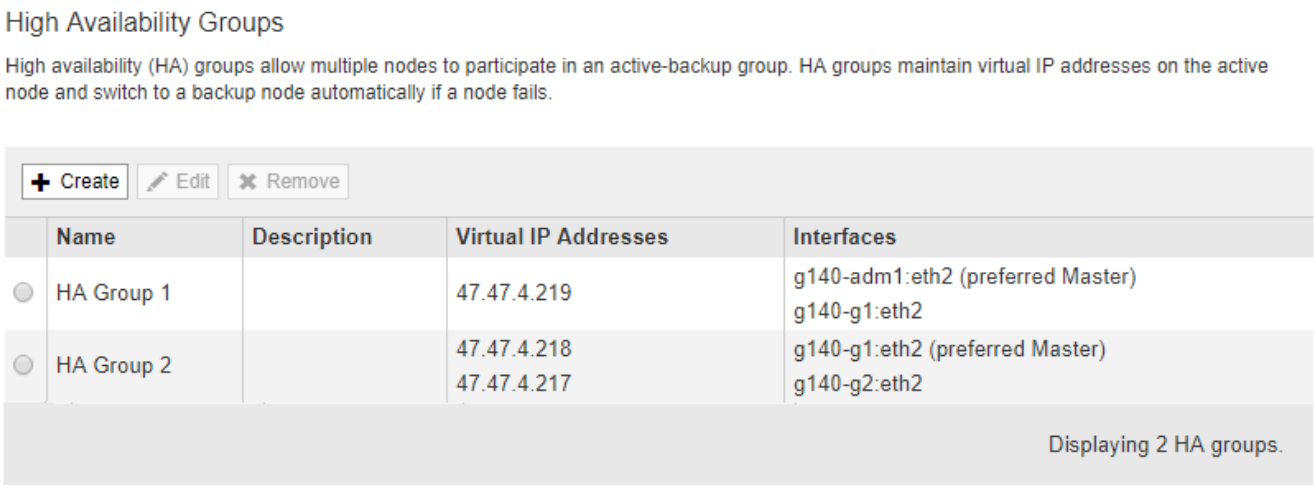
Algumas das razões para editar um grupo HA incluem o seguinte:

- Adicionando uma interface a um grupo existente. O endereço IP da interface deve estar dentro da mesma sub-rede que outras interfaces já atribuídas ao grupo.
- Remover uma interface de um grupo de HA. Por exemplo, você não pode iniciar um procedimento de desativação de site ou nó se a interface de um nó para a rede de Grade ou a rede de cliente for usada em um grupo HA.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.

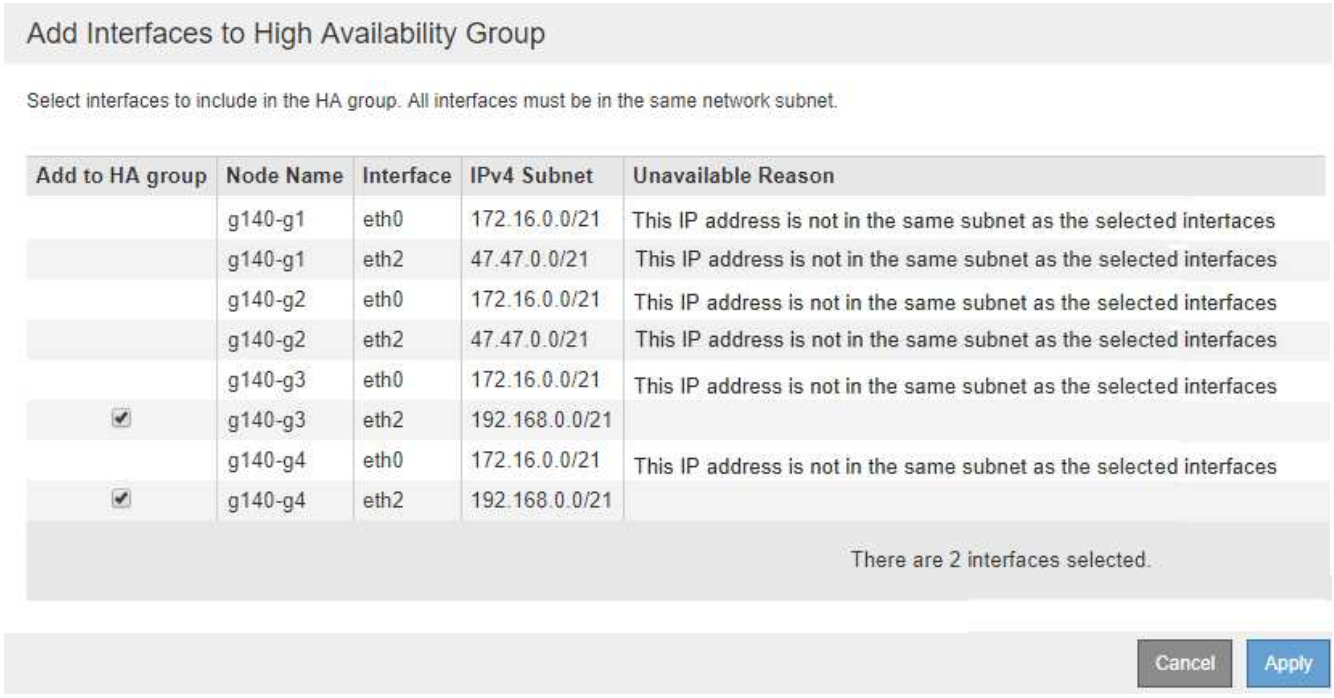


2. Selecione o grupo HA que deseja editar e clique em **Editar**.

   A caixa de diálogo Editar Grupo de alta disponibilidade é exibida.

3. Opcionalmente, atualize o nome ou a descrição do grupo.
4. Opcionalmente, clique em **Select interfaces** para alterar as interfaces do Grupo HA.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida.



   Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

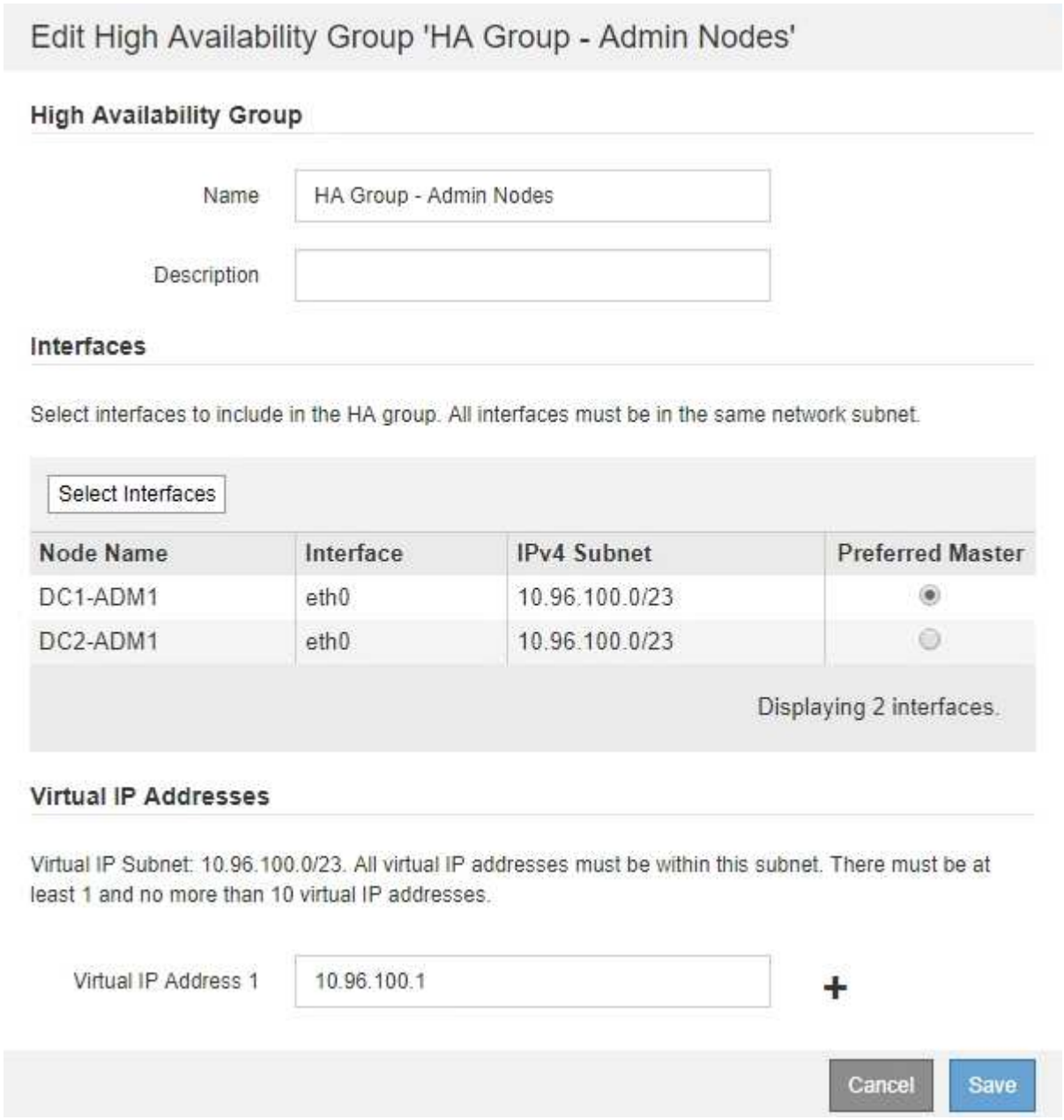
     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.

6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.



7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Opcionalmente, atualize os endereços IP virtuais para o grupo HA.

Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é atualizado.

Removendo um grupo de alta disponibilidade

Você pode remover um grupo de alta disponibilidade (HA) que não esteja mais usando.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

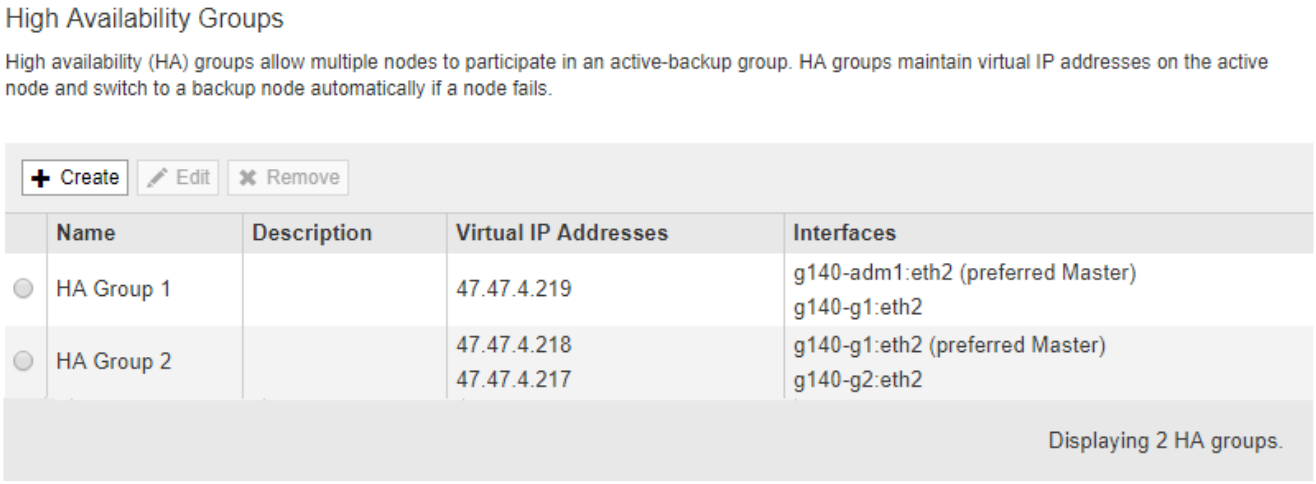
Aborde esta tarefa

Se você remover um grupo HA, qualquer cliente S3 ou Swift configurado para usar um dos endereços IP virtuais do grupo não poderá mais se conetar ao StorageGRID. Para evitar interrupções do cliente, você deve atualizar todos os aplicativos clientes S3 ou Swift afetados antes de remover um grupo HA. Atualize cada cliente para se conetar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP configurado para uma interface durante a instalação ou usando DHCP.

Passos

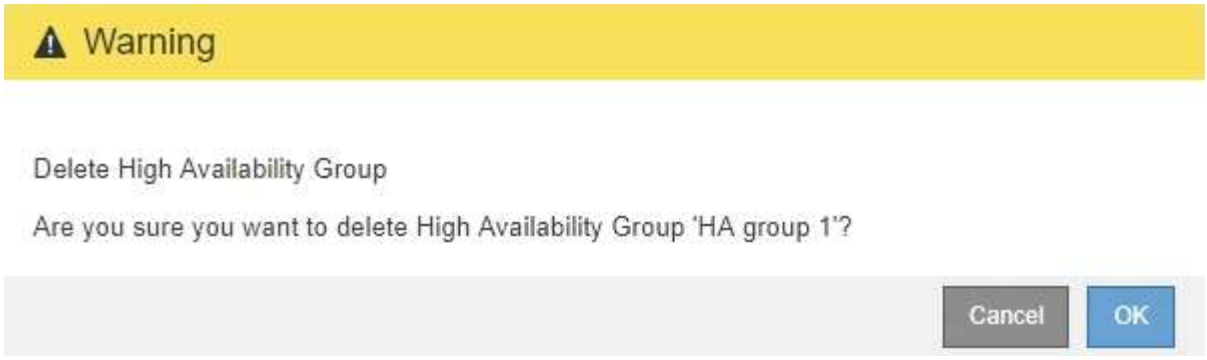
1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.



2. Selecione o grupo HA que deseja remover e clique em **Remover**.

   O aviso Excluir Grupo de alta disponibilidade é exibido.



3. Clique em **OK**.

   O grupo HA é removido.

Configurando nomes de domínio de endpoint da API S3

Para oferecer suporte a solicitações de estilo hospedado virtual S3, você deve usar o Gerenciador de Grade para configurar a lista de nomes de domínio de endpoint aos quais os clientes S3 se conetam.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter confirmado que uma atualização de grade não está em andamento.

> Não faça alterações na configuração do nome de domínio quando uma atualização de grade estiver em andamento.

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de endpoint S3, você deve executar todas as seguintes tarefas:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o certificado que o cliente usa para conexões HTTPS com o StorageGRID está assinado para todos os nomes de domínio que o cliente requer.

  Por exemplo, se o endpoint for `s3.company.com`, você deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo do assunto universal (SAN) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente. Inclua Registros DNS para os endereços IP que os clientes usam para fazer conexões e verifique se os Registros fazem referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes de curinga.

Os clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administrador ou um nó de armazenamento, ou conetando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conetam à grade para incluir os endereços IP corretos nos Registros DNS.

O certificado que um cliente usa para conexões HTTPS depende de como o cliente se coneta à grade:

- Se um cliente se conetar usando o serviço Load Balancer, ele usará o certificado para um ponto de extremidade específico do balanceador de carga.

  Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

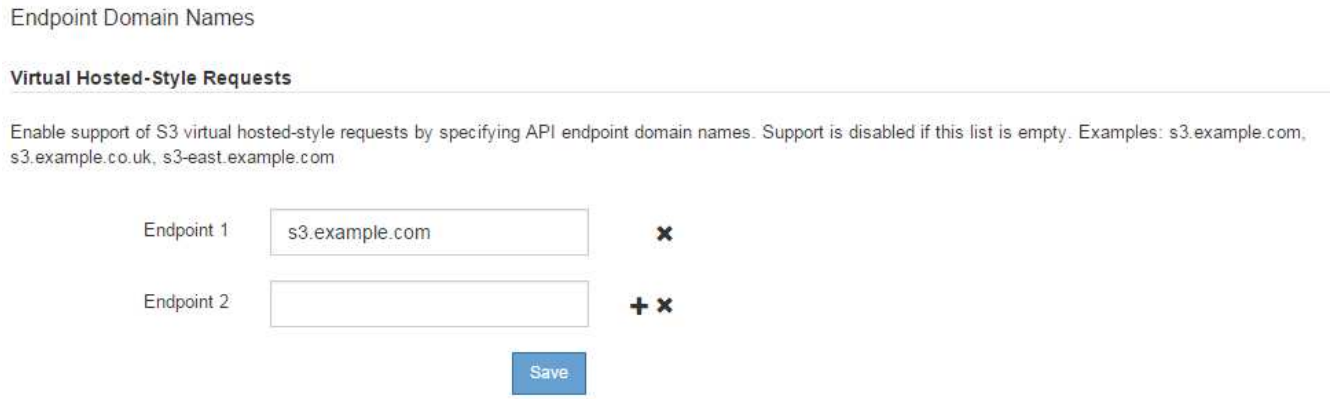
- Se o cliente se conetar a um nó de armazenamento ou ao serviço CLB em um nó de gateway, o cliente usará um certificado de servidor personalizado de grade que foi atualizado para incluir todos os nomes de domínio de endpoint necessários.

  O serviço CLB está obsoleto.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **nomes de domínio**.

   A página nomes de domínio do endpoint é exibida.



2. Para adicionar campos adicionais, insira a lista de nomes de domínio de endpoint da API S3 nos campos **Endpoint**.

   Se esta lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

3. Clique em **Salvar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint necessários.
   - Para clientes que usam o serviço Load Balancer, atualize o certificado associado ao ponto de extremidade do balanceador de carga ao qual o cliente se coneta.
   - Para clientes que se conetam diretamente aos nós de storage ou que usam o serviço CLB nos nós de Gateway, atualize o certificado de servidor personalizado para a grade.

5. Adicione os Registros DNS necessários para garantir que as solicitações de nome de domínio de endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o endpoint `bucket.s3.company.com`, o servidor DNS resolve para o endpoint correto e o certificado autentica o endpoint como esperado.

Informações relacionadas

"Use S3"

"Visualização de endereços IP"

"Criando um grupo de alta disponibilidade"

"Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB"

"Configuração dos pontos de extremidade do balanceador de carga"

Ativar HTTP para comunicações cliente

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para todas as conexões com nós de armazenamento ou para o serviço CLB obsoleto em nós de gateway. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Conclua esta tarefa somente se os clientes S3 e Swift precisarem fazer conexões HTTP diretamente aos nós de armazenamento ou ao serviço CLB obsoleto nos nós de Gateway.

Não é necessário concluir essa tarefa para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode configurar cada ponto de extremidade do Load Balancer para usar HTTP ou HTTPS). Consulte as informações sobre como configurar pontos de extremidade do balanceador de carga para obter mais informações.

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas S3 e clientes Swift usam ao se conetar a nós de armazenamento ou ao serviço CLB obsoleto usando HTTP ou HTTPS

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

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, marque a caixa de seleção **Ativar conexão HTTP** .

3. Clique em **Salvar**.

Informações relacionadas

"Configuração dos pontos de extremidade do balanceador de carga"

"Use S3"

"Use Swift"

Controlar quais operações do cliente são permitidas

Você pode selecionar a opção Prevent Client Modification grid (impedir a modificação do cliente) para negar operações específicas do cliente HTTP.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Impedir Modificação do Cliente é uma configuração de todo o sistema. Quando a opção impedir modificação de cliente é selecionada, as seguintes solicitações são negadas:

- **S3 API REST**
  - Eliminar pedidos de balde
  - Quaisquer solicitações para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

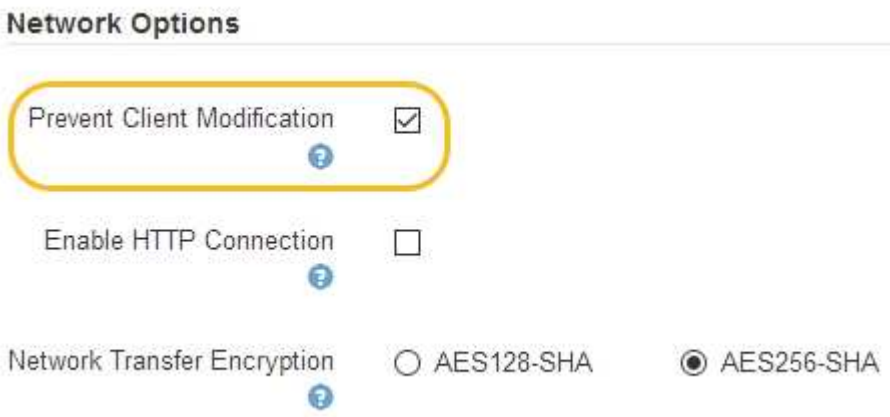
> Esta configuração não se aplica a buckets com controle de versão ativado. O controle de versão já impede modificações nos dados do objeto, metadados definidos pelo usuário e marcação de objetos.

- * Swift REST API*
  - Eliminar pedidos de contentor
  - Solicitações para modificar qualquer objeto existente. Por exemplo, as seguintes operações são negadas: Put Overwrite, Delete, Metadata Update e assim por diante.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.

2. Na seção Opções de rede, marque a caixa de seleção **impedir modificação de cliente**.



3. Clique em **Salvar**.

Informações sobre direitos autorais

Informações sobre marcas comerciais