Configurar conexões de cliente

StorageGRID

NetApp
March 12, 2025

Índice

Configurar conexões de cliente

Configurar conexões de cliente S3 e Swift: Visão geral

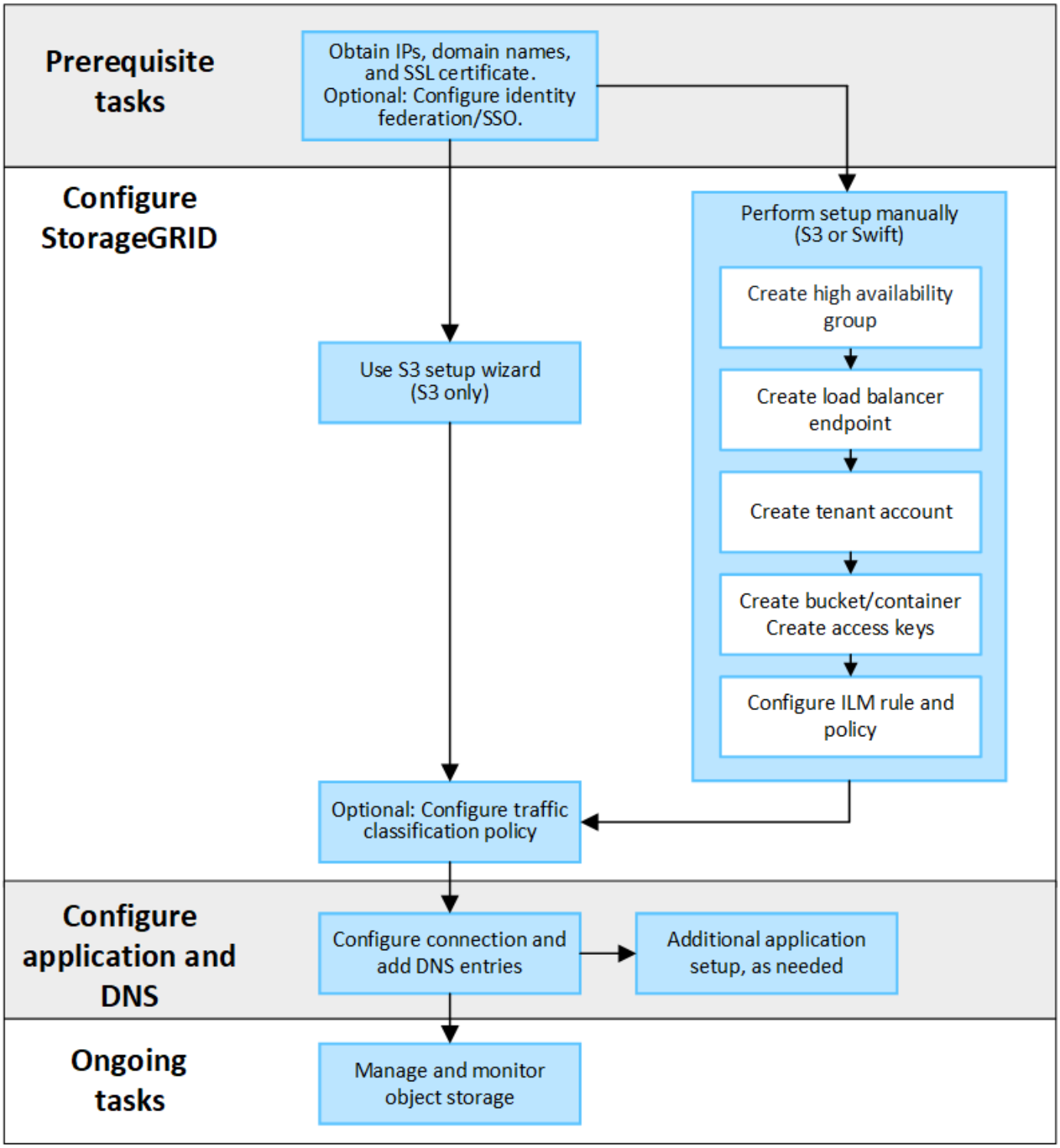
Como administrador de grade, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 e Swift se conetam ao seu sistema StorageGRID para armazenar e recuperar dados.

O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Fluxo de trabalho de configuração

Como mostrado no diagrama de fluxo de trabalho, existem quatro etapas principais para conetar o StorageGRID a qualquer aplicativo S3 ou Swift:

1. Execute tarefas de pré-requisito no StorageGRID, com base na forma como o aplicativo cliente se conetará ao StorageGRID.
2. Use StorageGRID para obter os valores que o aplicativo precisa para se conetar à grade. Você pode usar o assistente de configuração do S3 ou configurar cada entidade do StorageGRID manualmente.
3. Use o aplicativo S3 ou Swift para concluir a conexão com o StorageGRID. Crie entradas DNS para associar endereços IP a qualquer nome de domínio que você pretende usar.
4. Executar tarefas contínuas na aplicação e no StorageGRID para gerenciar e monitorar o storage de objetos ao longo do tempo.



Informações necessárias para anexar o StorageGRID a um aplicativo cliente

Antes de poder anexar o StorageGRID a um aplicativo cliente S3 ou Swift, você deve executar as etapas de configuração no StorageGRID e obter determinado valor.

Quais valores eu preciso?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e onde esses valores são usados pelo aplicativo S3 ou Swift e pelo servidor DNS.

Valor	Onde o valor está configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > grupo HA	Entrada DNS
Porta	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Certificado SSL	StorageGRID > ponto final do balanceador de carga	Aplicação cliente
Nome do servidor (FQDN)	StorageGRID > ponto final do balanceador de carga	• Aplicação cliente • Entrada DNS
S3 ID da chave de acesso e chave de acesso secreta	StorageGRID > locatário e balde	Aplicação cliente
Nome do balde/recipiente	StorageGRID > locatário e balde	Aplicação cliente

Como obtenho esses valores?

Dependendo de seus requisitos, você pode fazer um dos seguintes procedimentos para obter as informações de que precisa:

- **Use o "Assistente de configuração S3"**. O assistente de configuração do S3 ajuda a configurar rapidamente os valores necessários no StorageGRID e gera um ou dois arquivos que você pode usar ao configurar o aplicativo S3. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID.

  > ⓘ Se você estiver configurando um aplicativo S3, é recomendável usar o assistente de configuração S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá uma personalização significativa.

- **Use o "Assistente de configuração do FabricPool"**. Semelhante ao assistente de configuração do S3, o assistente de configuração do FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar um nível de nuvem do FabricPool no ONTAP.

  > ⓘ Se você planeja usar o StorageGRID como o sistema de storage de objetos em uma categoria de nuvem do FabricPool, é recomendável usar o assistente de configuração do FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Configurar itens manualmente**. Se você estiver se conetando a um aplicativo Swift (ou estiver se conetando a um aplicativo S3 e preferir não usar o assistente de configuração S3), você poderá obter os valores necessários executando a configuração manualmente. Siga estes passos:

  a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3 ou Swift. "Configurar grupos de alta disponibilidade"Consulte .

  b. Crie o ponto de extremidade do balanceador de carga que o aplicativo S3 ou Swift usará. "Configurar pontos de extremidade do balanceador de carga"Consulte .

c. Crie a conta de locatário que o aplicativo S3 ou Swift usará. "Crie uma conta de locatário"Consulte .

d. Para um locatário do S3, faça login na conta do locatário e gere uma ID de chave de acesso e chave de acesso secreta para cada usuário que acessará o aplicativo. "Crie suas próprias chaves de acesso"Consulte .

e. Crie um ou mais buckets do S3 ou contentores Swift na conta do locatário. Para S3, "Crie um balde S3D."consulte . Para Swift, use o "COLOQUE o pedido do recipiente".

f. Para adicionar instruções de posicionamento específicas para os objetos pertencentes ao novo locatário ou bucket/container, crie uma nova regra ILM e ative uma nova política ILM para usar essa regra. "Criar regra ILM"Consulte e "Criar política ILM".

Segurança para clientes S3 ou Swift

As contas de locatário do StorageGRID usam aplicativos clientes S3 ou Swift para salvar dados de objeto no StorageGRID. Você deve rever as medidas de segurança implementadas para aplicativos clientes.

Resumo

A tabela a seguir resume como a segurança é implementada para as APIs REST S3 e Swift:

Problema de segurança	Implementação da API REST
Segurança da ligação	TLS
Autenticação do servidor	Certificado de servidor X,509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador
Autenticação de cliente	**S3** S3 conta (ID da chave de acesso e chave de acesso secreta) **Rápido** Conta Swift (nome de utilizador e palavra-passe)
Autorização do cliente	**S3** Propriedade do bucket e todas as políticas de controle de acesso aplicáveis **Rápido** Acesso à função de administrador

Como o StorageGRID fornece segurança para aplicativos clientes

Os aplicativos clientes S3 e Swift podem se conectar ao serviço Load Balancer em nós de Gateway ou nós de administração ou diretamente aos nós de storage.

- Os clientes que se conetam ao serviço Load Balancer podem usar HTTPS ou HTTP, com base em como "configure o ponto final do balanceador de carga"você .

O HTTPS fornece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao endpoint.

O HTTP fornece uma comunicação menos segura e não criptografada e só deve ser usado para grades de teste ou não-produção.

- Os clientes que se conetam a nós de storage também podem usar HTTPS ou HTTP.

  HTTPS é o padrão e é recomendado.

  O HTTP fornece uma comunicação menos segura e não criptografada, mas pode ser opcionalmente "ativado" para grades de teste ou não-produção.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento dentro da grade são criptografadas se o ponto de extremidade do balanceador de carga está configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer cabeçalhos de autenticação HTTP ao StorageGRID para executar operações de API REST. "Autenticar solicitações"Consulte e "Endpoints de API Swift compatíveis".

Certificados de segurança e aplicativos de cliente

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conetam ao serviço do Load Balancer, eles usam o certificado que foi configurado para o endpoint do balanceador de carga. Cada ponto de extremidade do balanceador de carga tem o seu próprio certificado& n.o 8212;um certificado de servidor personalizado carregado pelo administrador da grelha ou um certificado que o administrador da grelha gerou no StorageGRID ao configurar o ponto de extremidade.

  "Considerações para balanceamento de carga"Consulte .

- Quando os aplicativos cliente se conetam diretamente a um nó de armazenamento, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade. "Adicione um certificado de API S3 ou Swift personalizado"Consulte .

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que usam para estabelecer conexões TLS.

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto de conjuntos de codificação que os aplicativos clientes podem usar ao estabelecer uma sessão TLS. Para configurar cifras, vá para **CONFIGURATION** > **Security** > **Security settings** e selecione **TLS e SSH policies**.

Versões suportadas do TLS

O StorageGRID é compatível com TLS 1,2 e TLS 1,3.

SSLv3 e TLS 1,1 (ou versões anteriores) não são mais compatíveis.

Utilize o assistente de configuração S3

Use o assistente de configuração S3: Considerações e requisitos

Você pode usar o assistente de configuração S3 para configurar o StorageGRID como o sistema de armazenamento de objetos para um aplicativo S3.

Quando utilizar o assistente de configuração S3

O assistente de configuração S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você baixa arquivos que você pode usar para inserir valores no aplicativo S3. Use o assistente para configurar o sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID.

Se tiver o "Permissão de acesso à raiz", pode concluir o assistente de configuração do S3 quando começar a utilizar o Gestor de grelha do StorageGRID ou pode aceder e concluir o assistente posteriormente. Dependendo de seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para montar os valores que um aplicativo S3 precisa.

Antes de utilizar o assistente

Antes de utilizar o assistente, confirme que concluiu estes pré-requisitos.

Obtenha endereços IP e configure interfaces VLAN

Se você configurar um grupo de alta disponibilidade (HA), você sabe a quais nós o aplicativo S3 se conetará e a qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de sub-rede, endereço IP de gateway e endereços IP virtual (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, já configurou a interface VLAN. "Configurar interfaces VLAN"Consulte .

Configure a federação de identidade e o SSO

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, ativou esses recursos. Você também sabe qual grupo federado deve ter acesso root para a conta de locatário que o aplicativo S3 usará. "Use a federação de identidade"Consulte e "Configurar o logon único".

Obter e configurar nomes de domínio

Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para o StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA criado usando o assistente.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, você deve ter "Configurados S3 nomes de domínio de endpoint"o . Recomenda-se o uso de solicitações virtuais de estilo hospedado.

Revise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga do StorageGRID, analisou as considerações gerais sobre o balanceamento de carga. Você tem os certificados que você vai carregar ou os valores que você precisa para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (de terceiros), terá o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Configure todas as conexões de federação de grade

Se você quiser permitir que o locatário do S3 clone dados de conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade, confirme o seguinte antes de iniciar o assistente:

- Você "configurada a conexão de federação de grade"tem .
- O estado da ligação é **ligado**.
- Você tem permissão de acesso root.

Acesse e conclua o assistente de configuração do S3

Você pode usar o assistente de configuração S3 para configurar o StorageGRID para uso com um aplicativo S3. O assistente de configuração fornece os valores que o aplicativo precisa para acessar um bucket do StorageGRID e salvar objetos.

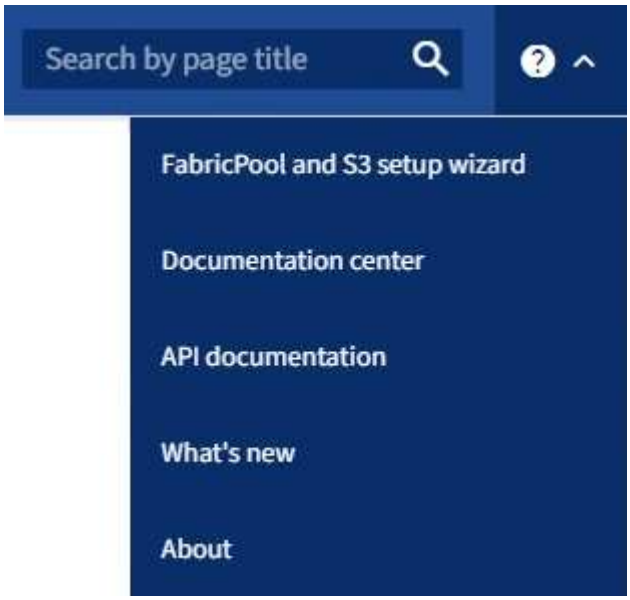
Antes de começar

- Você tem o "Permissão de acesso à raiz".
- Analisou "considerações e requisitos"o para utilizar o assistente.

Acesse o assistente

Passos

1. Faça login no Gerenciador de Grade usando um "navegador da web suportado".
2. Se o banner **FabricPool and S3 setup wizard** for exibido no painel, selecione o link no banner. Se o banner não for mais exibido, selecione o ícone de ajuda na barra de cabeçalho no Gerenciador de Grade e selecione **Assistente de configuração FabricPool e S3**.



3. Na seção S3 da aplicação da página do assistente de configuração FabricPool e S3, selecione **Configurar agora**.

Etapa 1 de 6: Configurar o grupo HA

Um grupo de HA é uma coleção de nós que contêm cada um o serviço StorageGRID Load Balancer. Um grupo de HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de HA para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo de HA falhar, uma interface de backup poderá gerenciar a carga de trabalho com pouco impacto nas operações do S3.

Para obter detalhes sobre esta tarefa, "Gerenciar grupos de alta disponibilidade"consulte .

Passos

1. Se você pretende usar um balanceador de carga externo, não precisa criar um grupo de HA. Selecione **Ignorar este passo** e vá para Etapa 2 de 6: Configurar o ponto final do balanceador de carga.
2. Para usar o balanceador de carga do StorageGRID, você pode criar um novo grupo de HA ou usar um grupo de HA existente.

Criar grupo HA

a. Para criar um novo grupo HA, selecione **criar grupo HA**.

b. Para a etapa **Digite detalhes**, preencha os campos a seguir.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

c. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo HA.

Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

d. Para a etapa **priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para esse grupo de HA.

Arraste linhas para alterar os valores na coluna **Priority Order**.

A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços IP virtual (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup, e assim por diante. Quando as falhas são resolvidas, os endereços VIP voltam para a interface de maior prioridade disponível.

e. Para a etapa **Inserir endereços IP**, preencha os campos a seguir.

Campo	Descrição
CIDR de sub-rede	O endereço da sub-rede VIP na notação CIDR & n.o 8212; um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32). O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.
Endereço IP do gateway (opcional)	Se os S3 endereços IP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Create HA group** e, em seguida, selecione **Finish** para retornar ao assistente de configuração S3.

g. Selecione **continuar** para ir para a etapa do balanceador de carga.

Use o grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA no **Selecione um grupo HA**.

b. Selecione **continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o ponto final do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários nós de storage.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administrador, ou pode se conetar a um balanceador de carga externo (de terceiros). Recomenda-se a utilização do balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, "Considerações para balanceamento de carga"consulte .

Para usar o serviço de balanceador de carga do StorageGRID, selecione a guia **balanceador de carga do StorageGRID** e, em seguida, crie ou selecione o ponto de extremidade do balanceador de carga que deseja usar. Para usar um balanceador de carga externo, selecione a guia **balanceador de carga externo** e forneça detalhes sobre o sistema que você já configurou.

Criar endpoint

Passos

1. Para criar um ponto de extremidade do balanceador de carga, selecione **Create endpoint**.
2. Para a etapa **Digite os detalhes do endpoint**, preencha os campos a seguir.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas em nós de Gateway, porque essas portas serão reservadas em nós de administração. **Observação:** as portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".
Tipo de cliente	Deve ser **S3**.
Protocolo de rede	Selecione **HTTPS**. **Nota**: A comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

3. Para a etapa **Select Binding mode** (Selecionar modo de encadernação), especifique o modo de encadernação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

Modo	Descrição
Global (predefinição)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global** (padrão), a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.

Modo	Descrição
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

4. Para a etapa de Acesso ao locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

5. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use essa opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Consulte "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que introduzir.
Use o certificado StorageGRID S3 e Swift	Utilize esta opção apenas se já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID. "Configure os certificados API S3 e Swift"Consulte para obter detalhes.

6. Selecione **Finish** (concluir) para voltar ao assistente de configuração do S3.
7. Selecione **Continue** para ir para a etapa de locatário e bucket.

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

Use o ponto de extremidade do balanceador de carga existente

Passos

1. Para usar um endpoint existente, selecione seu nome no **Selecione um endpoint do balanceador de carga**.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Use balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os campos a seguir.

Campo	Descrição
FQDN	O nome de domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o aplicativo S3 usará para se conetar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continue** para ir para a etapa de locatário e bucket.

Passo 3 de 6: Crie locatário e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos. Você deve criar o locatário antes de criar o bucket que o aplicativo S3 usará para armazenar seus objetos.

Um bucket é um contentor usado para armazenar os objetos e metadados de objetos de um locatário. Embora alguns inquilinos possam ter muitos buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Você pode usar o Gerenciador do Locatário posteriormente para adicionar quaisquer buckets adicionais que você precisar.

Você pode criar um novo locatário para este aplicativo S3 usar. Opcionalmente, você também pode criar um bucket para o novo locatário. Finalmente, você pode permitir que o assistente crie as chaves de acesso S3 para o usuário raiz do locatário.

Para obter detalhes sobre esta tarefa, "Crie uma conta de locatário" consulte e "Crie um balde S3D.".

Passos

1. Selecione **criar inquilino**.
2. Para os passos Enter details (introduzir detalhes), introduza as seguintes informações.

Campo	Descrição
Nome	Um nome para a conta de locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.
Descrição (opcional)	Uma descrição para ajudar a identificar o inquilino.

Campo	Descrição
Tipo de cliente	O tipo de protocolo de cliente que este inquilino usará. Para o assistente de configuração S3, **S3** é selecionado e o campo está desativado.
Cota de armazenamento (opcional)	Se você quiser que esse locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

3. Selecione **continuar**.
4. Opcionalmente, selecione todas as permissões que você deseja que esse locatário tenha.

> Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, selecione o ícone de ajuda para cada permissão.

Permissão	Se selecionado…
Permitir serviços de plataforma	O locatário pode usar serviços de plataforma S3, como o CloudMirror. "Gerencie os serviços de plataforma para contas de inquilino S3"Consulte .
Use a própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos federados e usuários. Esta opção é desativada se tiver "SSO configurado" para o seu sistema StorageGRID.
Permitir S3 Selecione	O locatário pode emitir S3 solicitações de API SelectObjectContent para filtrar e recuperar dados de objeto. "Gerenciar S3 Selecione para contas de inquilino"Consulte . **Importante**: As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.
Use a conexão de federação de grade	O locatário pode usar uma conexão de federação de grade. Selecionar esta opção: • Faz com que esse locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados dessa grade (a *grade de origem*) para a outra grade na conexão selecionada (a *grade de destino*). • Permite que esse locatário configure a replicação entre grade entre intervalos correspondentes em cada grade. "Gerenciar os locatários permitidos para a federação de grade"Consulte .

5. Se você selecionou **usar conexão de federação de grade**, selecione uma das conexões de federação de grade disponíveis.
6. Defina o acesso root para a conta de locatário, com base se o sistema StorageGRID usa "federação de identidade", "Logon único (SSO)"ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver ativada	Especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário raiz local.
Se a federação de identidade e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso root para o locatário. Nenhum usuário local pode entrar.

7. Se você quiser que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário raiz, selecione **Create root user S3 access key automatically**.

   Selecione esta opção se o único usuário para o locatário for o usuário raiz. Se outros usuários usarem esse locatário, use o Gerenciador do Locatário para configurar chaves e permissões.

8. Selecione **continuar**.
9. Para a etapa criar bucket, opcionalmente, crie um bucket para os objetos do locatário. Caso contrário, selecione **criar inquilino sem bucket** para ir para o passo de transferência de dados.

   Se o bloqueio de objeto S3 estiver ativado para a grade, o intervalo criado nesta etapa não terá o bloqueio de objeto S3 ativado. Se você precisar usar um bucket do S3 Object Lock para este aplicativo S3, selecione **criar locatário sem bucket**. Em seguida, use o Gerenciador do Locatário para"crie o balde".

   a. Introduza o nome do intervalo que a aplicação S3 irá utilizar. Por exemplo, `S3-bucket`.

      Não é possível alterar o nome do bucket depois de criar o bucket.

   b. Selecione a **região** para este intervalo.

      Use a região (`us-east-1`padrão) a menos que você espere usar o ILM no futuro para filtrar objetos com base na região do bucket.

   c. Selecione **Ativar controle de versão de objeto** se você quiser armazenar cada versão de cada objeto neste intervalo.

   d. Selecione **criar locatário e bucket** e vá para a etapa de download de dados.

passo 4 de 6: Transferir dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que você acabou de configurar.

Passos

1. Se você selecionou **Create root user S3 access key automatically**, siga um ou ambos os procedimentos a seguir:
   - Selecione **Transferir chaves de acesso** para transferir um `.csv` ficheiro que contenha o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
   - Selecione o ícone de cópia () para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.
2. Selecione **Transferir valores de configuração** para transferir um `.txt` ficheiro que contenha as definições para o terminal do balanceador de carga, locatário, bucket e utilizador raiz.
3. Salve essas informações em um local seguro.

> Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis depois de fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Se solicitado, marque a caixa de seleção para confirmar que você baixou ou copiou as chaves.
5. Selecione **Continue** para ir para a regra ILM e a etapa de política.

Passo 5 de 6: Revise a regra ILM e a política ILM para S3

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos em seu sistema StorageGRID. A política de ILM incluída no StorageGRID faz duas cópias replicadas de todos os objetos. Esta política está em vigor até que você ative pelo menos uma nova política.

Passos

1. Reveja as informações fornecidas na página.
2. Se você quiser adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. "Criar regra ILM"Consulte e "Políticas ILM: Visão geral".
3. Selecione **Reviewei estes passos e compreendi o que preciso fazer**.
4. Marque a caixa de seleção para indicar que você entende o que fazer a seguir.
5. Selecione **continuar** para ir para **Resumo**.

Passo 6 de 6: Rever resumo

Passos

1. Reveja o resumo.
2. Anote os detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de se conetar ao cliente S3. Por exemplo, selecionar **entrar como root** leva-o ao Gerenciador de inquilinos, onde você pode adicionar usuários de inquilinos, criar buckets adicionais e atualizar configurações de bucket.
3. Selecione **Finish**.
4. Configure o aplicativo usando o arquivo baixado do StorageGRID ou os valores obtidos manualmente.

Gerenciar grupos de HA

Gerenciar grupos de alta disponibilidade (HA): Visão geral

Você pode agrupar as interfaces de rede de vários nós de administrador e gateway em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho.

O que é um grupo HA?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift ou para fornecer conexões altamente disponíveis para o Gerenciador de Grade e o Gerenciador de Tenant.

Cada grupo de HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Grupos DE HA que incluem nós de gateway, nós de administração ou ambos fornecem conexões de dados altamente disponíveis para clientes S3 e Swift.
- Os GRUPOS DE HA que incluem apenas os nós de Admin fornecem conexões altamente disponíveis ao Gerenciador de Grade e ao Gerente do locatário.
- Um grupo de HA que inclui apenas dispositivos de serviços e nós de software baseados em VMware pode fornecer conexões altamente disponíveis para "S3 inquilinos que usam S3 Select"o . Os GRUPOS HA são recomendados ao usar S3 Select, mas não são necessários.

Como criar um grupo HA?

1. Você seleciona uma interface de rede para um ou mais nós de administrador ou nós de gateway. Você pode usar uma interface Grid Network (eth0), uma interface Client Network (eth2), uma interface VLAN ou uma interface de acesso que você adicionou ao nó.

   > Não é possível adicionar uma interface a um grupo HA se ele tiver um endereço IP atribuído pelo DHCP.

2. Você especifica uma interface para ser a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.
3. Você determina a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conetar ao StorageGRID.

Para obter instruções, "Configurar grupos de alta disponibilidade"consulte .

O que é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface principal, que é a primeira interface na ordem de prioridade. Enquanto a interface principal permanecer disponível, ela é usada quando os clientes se conetam a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface principal é a interface "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade inferior para o grupo HA funcionam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface principal (atualmente ativa) fique indisponível.

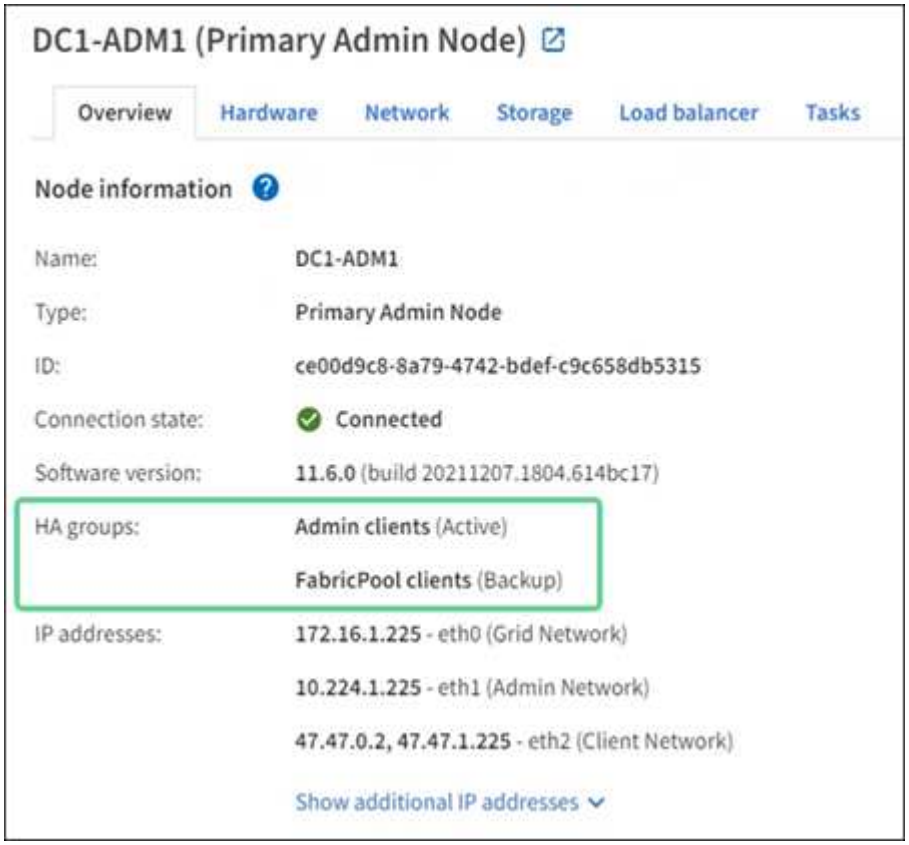
Exibir o status atual do grupo de HA de um nó

Para ver se um nó está atribuído a um grupo de HA e determinar seu status atual, selecione **NÓS** > ***node***.

Se a guia **Visão geral** incluir uma entrada para **grupos de HA**, o nó será atribuído aos grupos de HA listados. O valor após o nome do grupo é o status atual do nó no grupo HA:

- **Ativo**: O grupo HA está sendo hospedado neste nó.
- **Backup**: O grupo HA não está usando esse nó no momento; essa é uma interface de backup.
- **Stopped**: O grupo HA não pode ser hospedado neste nó porque o serviço de alta disponibilidade (keepalived) foi interrompido manualmente.
- **Falha**: O grupo HA não pode ser hospedado neste nó por causa de um ou mais dos seguintes:
  - O serviço do Load Balancer (nginx-gw) não está sendo executado no nó.
  - A interface eth0 ou VIP do nó está inativa.
  - O nó está inativo.

Neste exemplo, o nó de administração principal foi adicionado a dois grupos de HA. Este nó é atualmente a interface ativa para o grupo de clientes administradores e uma interface de backup para o grupo de clientes FabricPool.



O que acontece quando a interface ativa falha?

A interface que atualmente hospeda os endereços VIP é a interface ativa. Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP serão movidos para a primeira interface de backup disponível na ordem de prioridade. Se essa interface falhar, os endereços VIP passam para a próxima interface de backup disponível, e assim por diante.

O failover pode ser acionado por qualquer um destes motivos:

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

> O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pelos serviços do Gerenciador de Grade ou do Gerenciador de Locatário.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impactos e possam confiar em comportamentos normais de repetição para continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta torna-se disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta que está disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões altamente disponíveis ao StorageGRID para dados de objetos e para uso administrativo.

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

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

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

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao Grid Manager	• Nó de administração principal (**primário**) • Nós de administração não primários **Nota:** o nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso apenas ao Gestor do Locatário	• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	• Nós de administração • Nós de gateway
Acesso de cliente S3 para "S3 Selecione"	• Aparelhos de serviços • Nós de software baseados em VMware **Nota**: Os GRUPOS HA são recomendados ao usar o S3 Select, mas não são necessários.

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

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

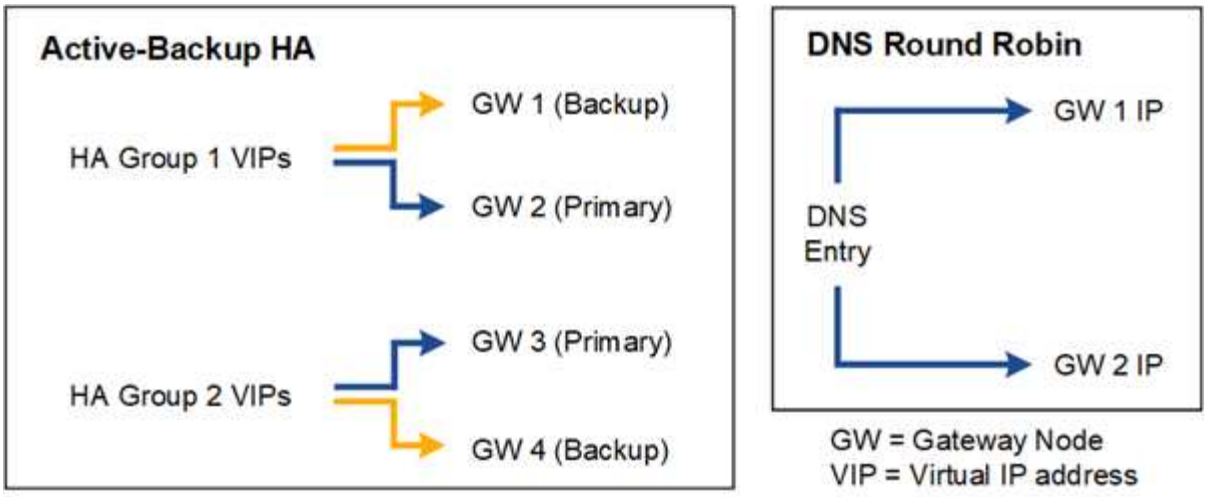
Se você estiver conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconetado e deverá fazer login novamente para retomar sua tarefa.

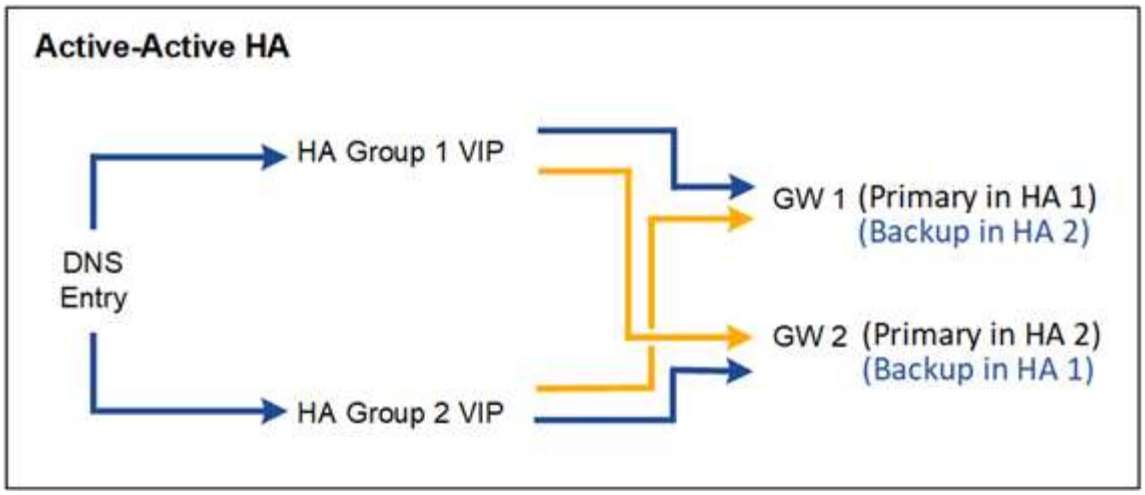
Alguns procedimentos de manutenção não podem ser executados quando o nó Admin principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

Opções de configuração para grupos de HA

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

Nos diagramas, azul indica a interface principal no grupo HA e amarelo indica a interface de backup no grupo HA.





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

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

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

Configurar grupos de alta disponibilidade

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Se você planeja usar uma interface VLAN em um grupo HA, criou a interface VLAN. "Configurar interfaces VLAN"Consulte .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, criou a interface:
  - **Red Hat Enterprise Linux (antes de instalar o nó)**: "Criar arquivos de configuração de nó"
  - * Ubuntu ou Debian (antes de instalar o nó)*: "Criar arquivos de configuração de nó"
  - * Linux (após a instalação do nó)*: "Linux: Adicione interfaces de tronco ou acesso a um nó"
  - **VMware (após a instalação do nó)**: "VMware: Adicione interfaces de tronco ou acesso a um nó"

Crie um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza por ordem de prioridade. Em seguida, atribua um ou mais endereços VIP ao grupo.

Uma interface deve ser incluída em um grupo de HA para um nó de gateway ou um nó de administrador. Um grupo de HA só pode usar uma interface para qualquer nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selecione **criar**.

Introduza os detalhes do grupo HA

Passos

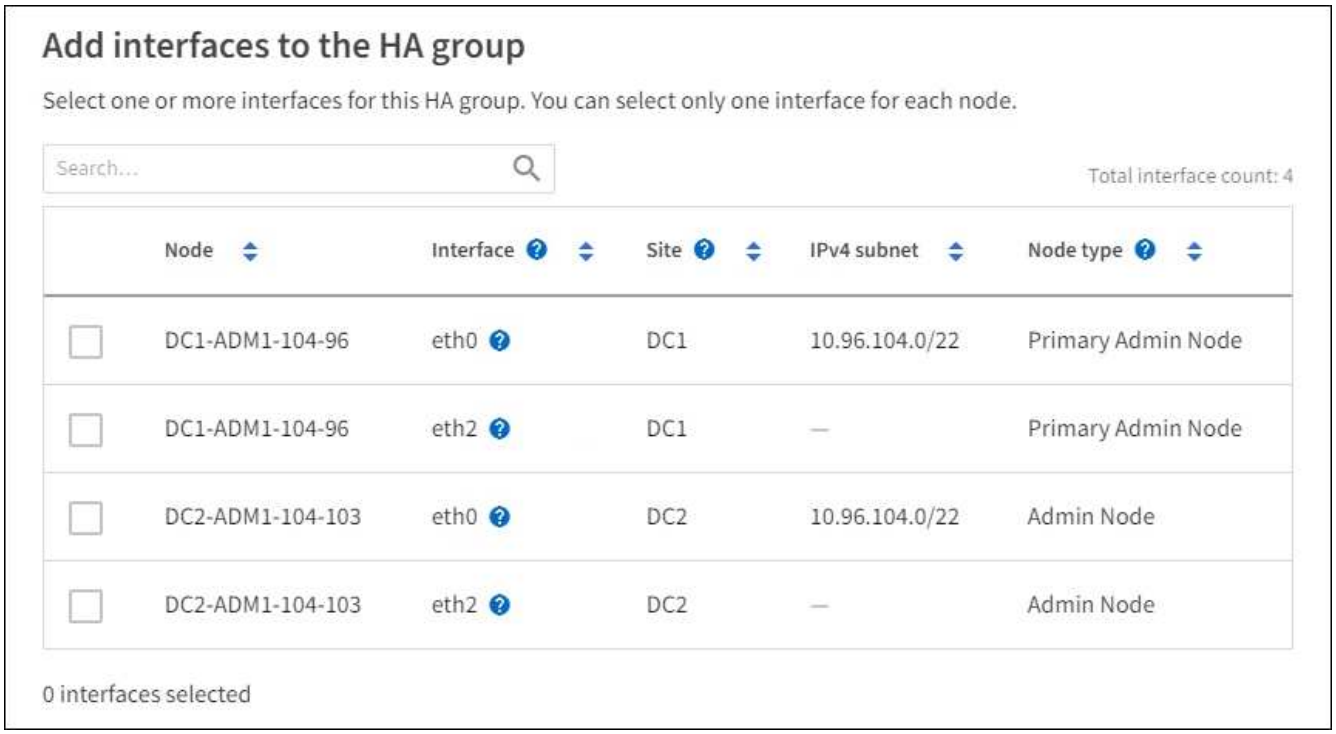
1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **continuar**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a esse grupo de HA.

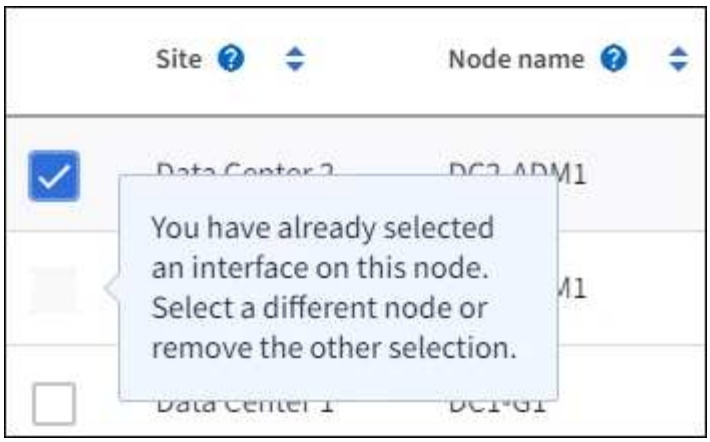
   Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.



> Depois de criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para a seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo de HA for para proteção de HA dos serviços Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione interfaces apenas em nós de administração.
- Se o grupo de HA for para proteção de HA de tráfego de cliente S3 ou Swift, selecione interfaces em nós de administração, nós de gateway ou ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Lembre-se de que, se ocorrer um failover, os serviços fornecidos pelo nó ativo anteriormente podem não estar disponíveis no nó recém-ativo. Por exemplo, um nó de gateway de backup não pode fornecer proteção de HA dos serviços Admin Node. Da mesma forma, um nó Admin de backup não pode executar todos os procedimentos de manutenção que o nó Admin principal pode fornecer.
- Se você não puder selecionar uma interface, sua caixa de seleção será desativada. A dica da ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o seu valor de sub-rede ou gateway entrar em conflito com outra interface selecionada.
- Não é possível selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **continuar**.

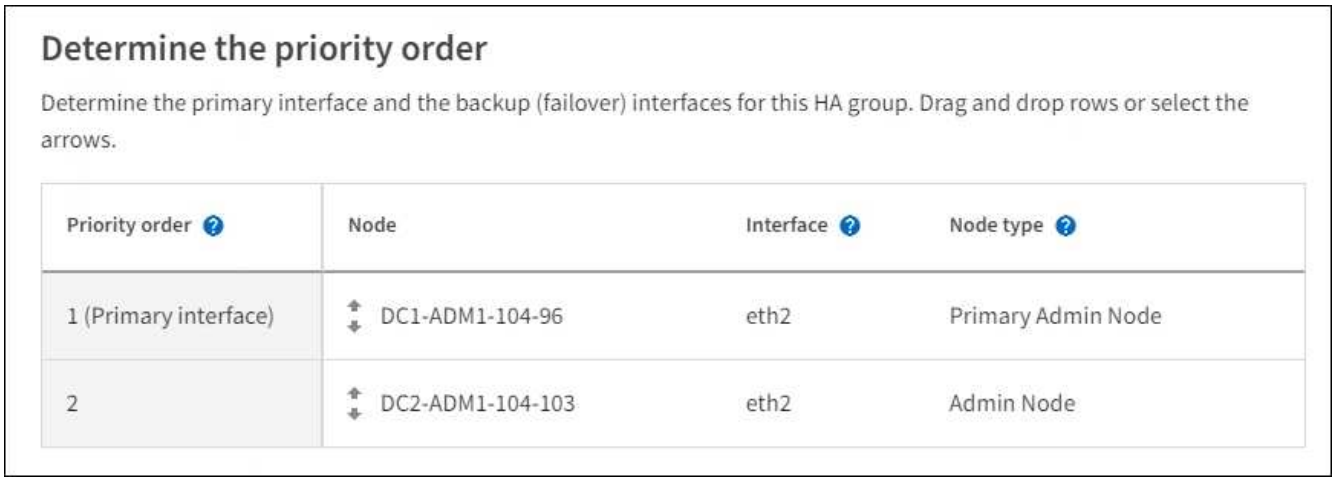
Determine a ordem de prioridade

Se o grupo de HA incluir mais de uma interface, você poderá determinar qual é a interface principal e quais são as interfaces de backup (failover). Se a interface principal falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP passam para a próxima interface de maior prioridade disponível, e assim por diante.

Passos

1. Arraste linhas na coluna **Priority Order** para determinar a interface principal e quaisquer interfaces de backup.

   A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.



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

2. Selecione **continuar**.

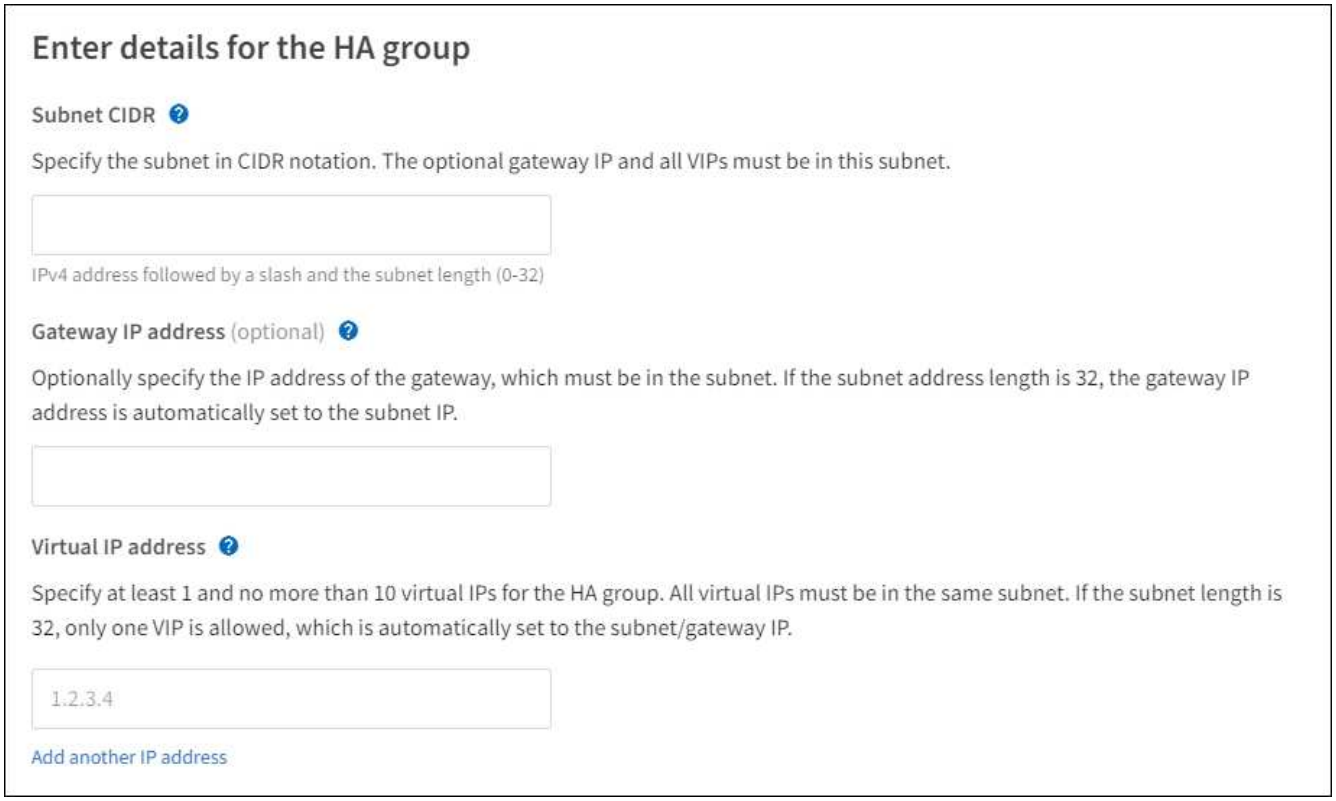
Introduza endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR—um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32).

   O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, `192.16.0.0/22`.

   > Se você usar um prefixo de 32 bits, o endereço de rede VIP também serve como endereço de gateway e endereço VIP.



2. Opcionalmente, se algum cliente S3, Swift, administrativo ou inquilino acessar esses endereços VIP de uma sub-rede diferente, digite o **Endereço IP Gateway**. O endereço de gateway deve estar dentro da sub-rede VIP.

   Os usuários de cliente e administrador usarão esse gateway para acessar os endereços IP virtuais.

3. Introduza pelo menos um e não mais de dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa.

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

4. Selecione **Create HA group** e selecione **Finish**.

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

Próximas etapas

Se você usar esse grupo de HA para balanceamento de carga, crie um ponto de extremidade do balanceador de carga para determinar a porta e o protocolo de rede e para anexar todos os certificados necessários. "Configurar pontos de extremidade do balanceador de carga"Consulte .

Edite um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou atualizar endereços IP virtuais.

Por exemplo, talvez seja necessário editar um grupo de HA se desejar remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.

   A página grupos de alta disponibilidade mostra todos os grupos de HA existentes.

2. Marque a caixa de seleção para o grupo HA que deseja editar.
3. Siga um destes procedimentos, com base no que você deseja atualizar:
   - Selecione **ações** > **Editar endereço IP virtual** para adicionar ou remover endereços VIP.
   - Selecione **ações** > **Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
   a. Atualize os endereços IP virtuais do grupo HA.
   b. Selecione **Guardar**.
   c. Selecione **Finish**.
5. Se você selecionou **Edit HA group**:
   a. Opcionalmente, atualize o nome ou a descrição do grupo.
   b. Opcionalmente, selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

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

   c. Opcionalmente, arraste linhas para alterar a ordem de prioridade da interface principal e de quaisquer interfaces de backup para esse grupo de HA.
   d. Opcionalmente, atualize os endereços IP virtuais.
   e. Selecione **Save** e, em seguida, selecione **Finish**.

Remova um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de cada vez.

Não é possível remover um grupo de HA se ele estiver vinculado a um ponto de extremidade do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de todos os pontos de extremidade do balanceador de carga que o usem.

Para evitar interrupções do cliente, atualize quaisquer aplicativos de cliente S3 ou Swift afetados antes de remover um grupo HA. Atualize cada cliente para se conetar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP configurado para uma interface durante a instalação.

Passos

1. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
2. Revise a coluna **Load balancer endpoints** para cada grupo de HA que você deseja remover. Se algum ponto final do balanceador de carga estiver listado:
   a. Aceda a **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Selecione a caixa de verificação para o endpoint.
   c. Selecione **actions** > **Edit endpoint binding mode**
   d. Atualize o modo de encadernação para remover o grupo HA.
   e. Selecione **Salvar alterações**.
3. Se não houver pontos de extremidade do balanceador de carga listados, marque a caixa de seleção para cada grupo de HA que você deseja remover.
4. Selecione **ações** > **Remover grupo HA**.
5. Reveja a mensagem e selecione **Eliminar grupo HA** para confirmar a sua seleção.

   Todos os grupos de HA selecionados são removidos. Um banner verde de sucesso aparece na página grupos de alta disponibilidade.

Gerenciar o balanceamento de carga

Considerações para balanceamento de carga

Você pode usar o balanceamento de carga para lidar com cargas de trabalho de ingestão e recuperação de clientes S3 e Swift.

O que é balanceamento de carga?

Quando um aplicativo cliente salva ou recupera dados de um sistema StorageGRID, o StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de obtenção e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho em vários nós de storage.

O serviço StorageGRID Load Balancer é instalado em todos os nós de administração e em todos os nós de gateway e fornece balanceamento de carga de camada 7. Ele executa o encerramento do TLS (Transport Layer Security) das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage.

O serviço Load Balancer em cada nó opera de forma independente ao encaminhar o tráfego do cliente para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU.

Embora o serviço de balanceamento de carga StorageGRID seja o mecanismo de balanceamento de carga recomendado, você pode querer integrar um balanceador de carga de terceiros. Para obter informações, contacte o representante da sua conta NetApp ou "TR-4626: Balanceadores de carga globais e de terceiros da StorageGRID" consulte .

Quantos nós de balanceamento de carga eu preciso?

Como prática recomendada geral, cada local no seu sistema StorageGRID deve incluir dois ou mais nós com o serviço de balanceador de carga. Por exemplo, um site pode incluir dois nós de Gateway ou um nó de administrador e um nó de gateway. Certifique-se de que há uma infraestrutura adequada de rede, hardware ou virtualização para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um ponto de extremidade do balanceador de carga?

Um ponto de extremidade do balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de aplicativos de cliente de entrada e saída usarão para acessar os nós que contêm o serviço Load Balancer. O endpoint também define o tipo de cliente (S3 ou Swift), o modo de encadernação e, opcionalmente, uma lista de inquilinos permitidos ou bloqueados.

Para criar um ponto de extremidade do balanceador de carga, selecione **CONFIGURATION** > **Network** > **Load balancer endpoints** ou conclua o assistente de configuração do FabricPool e do S3. Para obter instruções:

- "Configurar pontos de extremidade do balanceador de carga"
- "Utilize o assistente de configuração S3"
- "Utilize o assistente de configuração do FabricPool"

Considerações para a porta

A porta de um ponto de extremidade do balanceador de carga é padrão para 10433 para o primeiro ponto de extremidade criado, mas você pode especificar qualquer porta externa não utilizada entre 1 e 65535. Se você usar a porta 80 ou 443, o endpoint usará o serviço Load Balancer somente nos nós do Gateway. Essas portas são reservadas em nós de administração. Se você usar a mesma porta para mais de um endpoint, você deve especificar um modo de encadernação diferente para cada endpoint.

As portas usadas por outros serviços de grade não são permitidas. Consulte "Referência da porta de rede".

Considerações para o protocolo de rede

Na maioria dos casos, as conexões entre aplicativos cliente e StorageGRID devem usar criptografia TLS (Transport Layer Security). A conexão com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga do StorageGRID, deve selecionar **HTTPS**.

Considerações para certificados de endpoint do balanceador de carga

Se selecionar **HTTPS** como protocolo de rede para o ponto de extremidade do balanceador de carga, tem de fornecer um certificado de segurança. Você pode usar qualquer uma dessas três opções ao criar o ponto de extremidade do balanceador de carga:

- **Carregue um certificado assinado (recomendado)**. Este certificado pode ser assinado por uma autoridade de certificação pública ou privada (CA). Usar um certificado de servidor CA publicamente

confiável para proteger a conexão é a melhor prática. Em contraste com os certificados gerados, os certificados assinados por uma CA podem ser girados sem interrupções, o que pode ajudar a evitar problemas de expiração.

Você deve obter os seguintes arquivos antes de criar o ponto de extremidade do balanceador de carga:

- O arquivo de certificado do servidor personalizado.
- O arquivo de chave privada de certificado de servidor personalizado.
- Opcionalmente, um pacote de CA dos certificados de cada autoridade de certificação de emissão intermediária.

- **Gerar um certificado autoassinado**.
- **Use o certificado global StorageGRID S3 e Swift**. Você deve carregar ou gerar uma versão personalizada deste certificado antes de selecioná-lo para o ponto de extremidade do balanceador de carga. "Configure os certificados API S3 e Swift"Consulte .

Quais valores eu preciso?

Para criar o certificado, você deve saber todos os nomes de domínio e endereços IP que os aplicativos cliente S3 ou Swift usarão para acessar o endpoint.

A entrada **Assunto DN** (Nome distinto) do certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para o StorageGRID. Por exemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conforme necessário, o certificado pode usar curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração e nós de gateway que executam o serviço Load Balancer. Por exemplo, `*.storagegrid.example.com` usa o caractere curinga * para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se você planeja usar S3 solicitações virtuais de estilo hospedado, o certificado também deve incluir uma entrada **Nome alternativo** para cada "Nome de domínio do endpoint S3" um que você configurou, incluindo nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se você usar curingas para nomes de domínio, revise o "Diretrizes de fortalecimento para certificados de servidor".

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados expirados?

Se o certificado usado para proteger a conexão entre o aplicativo S3 e o StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente quaisquer alertas que avisem sobre datas de expiração de certificado que estejam se aproximando, como **validade do certificado de endpoint do balanceador de carga** e **expiração do certificado de servidor global para alertas S3 e Swift API**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, você deve substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá substituir certificados que expirarão em breve sem interrupções.
- Se você gerou um certificado StorageGRID auto-assinado e esse certificado está prestes a expirar, você deve substituir manualmente o certificado no StorageGRID e no aplicativo S3 antes que o certificado existente expire.

Considerações para o modo de encadernação

O modo de encadernação permite controlar quais endereços IP podem ser usados para acessar um ponto de extremidade do balanceador de carga. Se um endpoint usar um modo de encadernação, os aplicativos cliente só poderão acessar o endpoint se usarem um endereço IP permitido ou seu nome de domínio totalmente qualificado (FQDN) correspondente. Os aplicativos clientes que usam qualquer outro endereço IP ou FQDN não podem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de encadernação:

- **Global** (padrão): Os aplicativos cliente podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use esta configuração a menos que você precise restringir a acessibilidade de um endpoint.
- **IPs virtuais de grupos HA**. Os aplicativos cliente devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA.
- * Interfaces de nó*. Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó**. Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway.

Considerações para acesso ao locatário

O acesso ao locatário é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um endpoint do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um endpoint (padrão) ou especificar uma lista dos locatários permitidos ou bloqueados para cada endpoint.

Você pode usar esse recurso para fornecer um melhor isolamento de segurança entre os locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que os materiais mais secretos ou altamente classificados de propriedade de um locatário permaneçam completamente inacessíveis para outros inquilinos.

> Para fins de controle de acesso, o locatário é determinado a partir das chaves de acesso usadas na solicitação do cliente, se nenhuma chave de acesso for fornecida como parte da solicitação (como com acesso anônimo) o proprietário do bucket é usado para determinar o locatário.

Exemplo de acesso ao locatário

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade do balanceador de carga, como segue:
   - **Public** endpoint: Usa a porta 10443 e permite o acesso a todos os inquilinos.
   - * Ponto final Top SECRET*: Usa a porta 10444 e permite o acesso apenas ao locatário **Top SECRET**. Todos os outros inquilinos estão bloqueados para acessar este endpoint.
2. O `top-secret.pdf` está em um balde de propriedade do **Top SECRET** inquilino.

Para acessar o `top-secret.pdf`, um usuário no locatário **Top SECRET** pode emitir uma SOLICITAÇÃO GET para `https://w.x.y.z:10444/top-secret.pdf`. Como esse locatário tem permissão para usar o endpoint 10444, o usuário pode acessar o objeto. No entanto, se um usuário pertencente a qualquer outro locatário emitir a mesma solicitação para o mesmo URL, ele receberá uma mensagem de acesso negado imediata. O acesso é negado mesmo que as credenciais e a assinatura sejam válidas.

Disponibilidade da CPU

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

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

Configurar pontos de extremidade do balanceador de carga

Os pontos de extremidade do balanceador de carga determinam as portas e os protocolos de rede S3 e os clientes Swift podem usar ao se conetar ao balanceador de carga StorageGRID nos nós de gateway e administrador. Você também pode usar endpoints para acessar o Gerenciador de Grade, o Gerenciador de Tenant ou ambos.

O suporte para aplicativos cliente Swift foi obsoleto e será removido em uma versão futura.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".
- Você revisou o "considerações para balanceamento de carga".
- Se você remapeou anteriormente uma porta que pretende usar para o ponto de extremidade do balanceador de carga, você tem "removido o remapeamento da porta"o .
- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os GRUPOS HA são recomendados, mas não são necessários. "Gerenciar grupos de alta disponibilidade"Consulte .
- Se o ponto final do balanceador de carga for usado "S3 inquilinos para S3 Select"pelo , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos de serviços e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.

- Você configurou todas as interfaces VLAN que planeja usar. "Configurar interfaces VLAN"Consulte .
- Se você estiver criando um endpoint HTTPS (recomendado), você terá as informações para o certificado do servidor.

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

  - Para carregar um certificado, você precisa do certificado do servidor, da chave privada do certificado e, opcionalmente, de um pacote de CA.
  - Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 ou Swift usarão para acessar o endpoint. Você também deve conhecer o assunto (Nome distinto).
  - Se você quiser usar o certificado StorageGRID S3 e Swift API (que também pode ser usado para conexões diretamente aos nós de armazenamento), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API S3 e Swift"Consulte .

Crie um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga do cliente S3 ou Swift especifica uma porta, um tipo de cliente (S3 ou Swift) e um protocolo de rede (HTTP ou HTTPS). Os pontos de extremidade do balanceador de carga da interface de gerenciamento especificam uma porta, tipo de interface e rede cliente não confiável.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
2. Para criar um endpoint para um cliente S3 ou Swift, selecione a guia **S3 ou Swift client**.
3. Para criar um endpoint para acesso ao Gerenciador de Grade, Gerenciador de Tenant ou ambos, selecione a guia **Interface de Gerenciamento**.
4. Selecione **criar**.

Introduza os detalhes do endpoint

Passos

1. Selecione as instruções apropriadas para inserir detalhes do tipo de endpoint que você deseja criar.

Cliente S3 ou Swift

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo é padrão para 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você digitar **80** ou **8443**, o endpoint será configurado somente em nós de Gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um endpoint S3 e a porta será configurada nos nós Gateway e Admin.
Tipo de cliente	O tipo de aplicativo cliente que usará esse endpoint, **S3** ou **Swift**.
Protocolo de rede	O protocolo de rede que os clientes utilizarão ao ligar a este ponto final. • Selecione **HTTPS** para comunicação segura e criptografada TLS (recomendada). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione **HTTP** para comunicação menos segura e não criptografada. Use HTTP apenas para uma grade não-produção.

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Gerenciador de Grade, o Gerenciador do Locatário ou ambos. • Grid Manager: **8443** • Gerente de inquilino: **9443** • Gerente de Grade e Gerente de Locatário: **443** **Nota**: Você pode usar essas portas predefinidas ou outras portas disponíveis.
Tipo de interface	Selecione o botão de opção para a interface do StorageGRID que você acessará usando este endpoint.

Campo	Descrição
Rede cliente não confiável	Selecione **Sim** se este endpoint estiver acessível a redes de clientes não confiáveis. Caso contrário, selecione **não**. Quando você seleciona **Sim**, a porta é aberta em todas as redes de clientes não confiáveis. **Observação**: Você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis quando estiver criando o endpoint do balanceador de carga.

1. Selecione **continuar**.

Selecione um modo de encadernação

Passos

1. Selecione um modo de encadernação para o endpoint controlar como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP específicos e interfaces de rede.

   Alguns modos de vinculação estão disponíveis para endpoints de cliente ou endpoints de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints do cliente)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer nó de gateway ou nó de administrador, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração **Global**, a menos que você precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos de HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo de HA para acessar esse endpoint. Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nós	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar esse endpoint.
Tipo de nó (somente endpoints do cliente)	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin ou o endereço IP (ou FQDN correspondente) de qualquer nó Gateway para acessar esse ponto final.

Modo	Descrição
Todos os nós de administração (padrão para endpoints de interface de gerenciamento)	Os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó Admin para acessar esse endpoint.

Se mais de um ponto de extremidade utilizar a mesma porta, o StorageGRID utiliza esta ordem de prioridade para decidir qual ponto de extremidade utilizar: **IPs virtuais de grupos de HA** > **interfaces de nó** > **tipo de nó** > **Global**.

Se você estiver criando endpoints de interface de gerenciamento, somente os nós de administrador serão permitidos.

2. Se você selecionou **IPs virtuais de grupos de HA**, selecione um ou mais grupos de HA.

   Se estiver a criar endpoints de interface de gestão, selecione VIPs associados apenas a nós de administração.

3. Se você selecionou **interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administrador ou nó de gateway que você deseja associar a esse ponto de extremidade.
4. Se você selecionou **tipo de nó**, selecione os nós de administrador, que incluem o nó de administrador principal e quaisquer nós de administrador não primários ou nós de gateway.

Controle o acesso do locatário

> Um endpoint de interface de gerenciamento pode controlar o acesso do locatário somente quando o endpoint tiver o Tipo de interface do Gerenciador de inquilinos.

Passos

1. Para a etapa **Acesso ao locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de inquilino podem usar esse endpoint para acessar seus buckets. Você deve selecionar essa opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o endpoint do balanceador de carga para permitir ou bloquear contas específicas.
Permitir inquilinos selecionados	Somente as contas de locatário selecionadas podem usar esse endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar esse endpoint para acessar seus buckets. Todos os outros inquilinos podem usar este endpoint.

2. Se você estiver criando um endpoint **HTTP**, não será necessário anexar um certificado. Selecione **Create**

para adicionar o novo ponto de extremidade do balanceador de carga. Em seguida, vá Depois de terminarpara . Caso contrário, selecione **continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um endpoint **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao endpoint.

   O certificado protege as conexões entre clientes S3 e Swift e o serviço Load Balancer no nó Admin ou nos nós Gateway.

   - * Carregar certificado*. Selecione esta opção se tiver certificados personalizados para carregar.
   - **Gerar certificado**. Selecione esta opção se tiver os valores necessários para gerar um certificado personalizado.
   - **Use o certificado StorageGRID S3 e Swift**. Selecione essa opção se quiser usar o certificado global S3 e Swift API, que também pode ser usado para conexões diretamente aos nós de storage.

     Não é possível selecionar essa opção a menos que você tenha substituído o certificado padrão S3 e Swift API, que é assinado pela CA de grade, por um certificado personalizado assinado por uma autoridade de certificação externa. "Configure os certificados API S3 e Swift"Consulte .

   - **Use o certificado de interface de gerenciamento**. Selecione esta opção se pretender utilizar o certificado de interface de gestão global, que também pode ser utilizado para ligações diretas a nós de administração.
2. Se você não estiver usando o certificado StorageGRID S3 e Swift, carregue ou gere o certificado.

Carregar certificado

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

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

> As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

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

  Por exemplo: `storagegrid_certificate.pem`

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

d. Selecione **criar**. O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift ou a interface de gerenciamento e o endpoint.

Gerar certificado

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

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).

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

c. Selecione **Generate**.

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

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

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

  Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **criar**.

O ponto final do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift ou a interface de gerenciamento e este endpoint.

Depois de terminar

Passos

1. Se você usar um DNS, verifique se o DNS inclui um Registro para associar o nome de domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para fazer conexões.

   O endereço IP inserido no Registro DNS depende se você está usando um grupo HA de nós de balanceamento de carga:

   - Se você tiver configurado um grupo HA, os clientes se conetarão aos endereços IP virtuais desse grupo HA.
   - Se você não estiver usando um grupo de HA, os clientes se conetarão ao serviço do StorageGRID Load Balancer usando o endereço IP de um nó de gateway ou nó de administrador.

     Você também deve garantir que o Registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes de curinga.

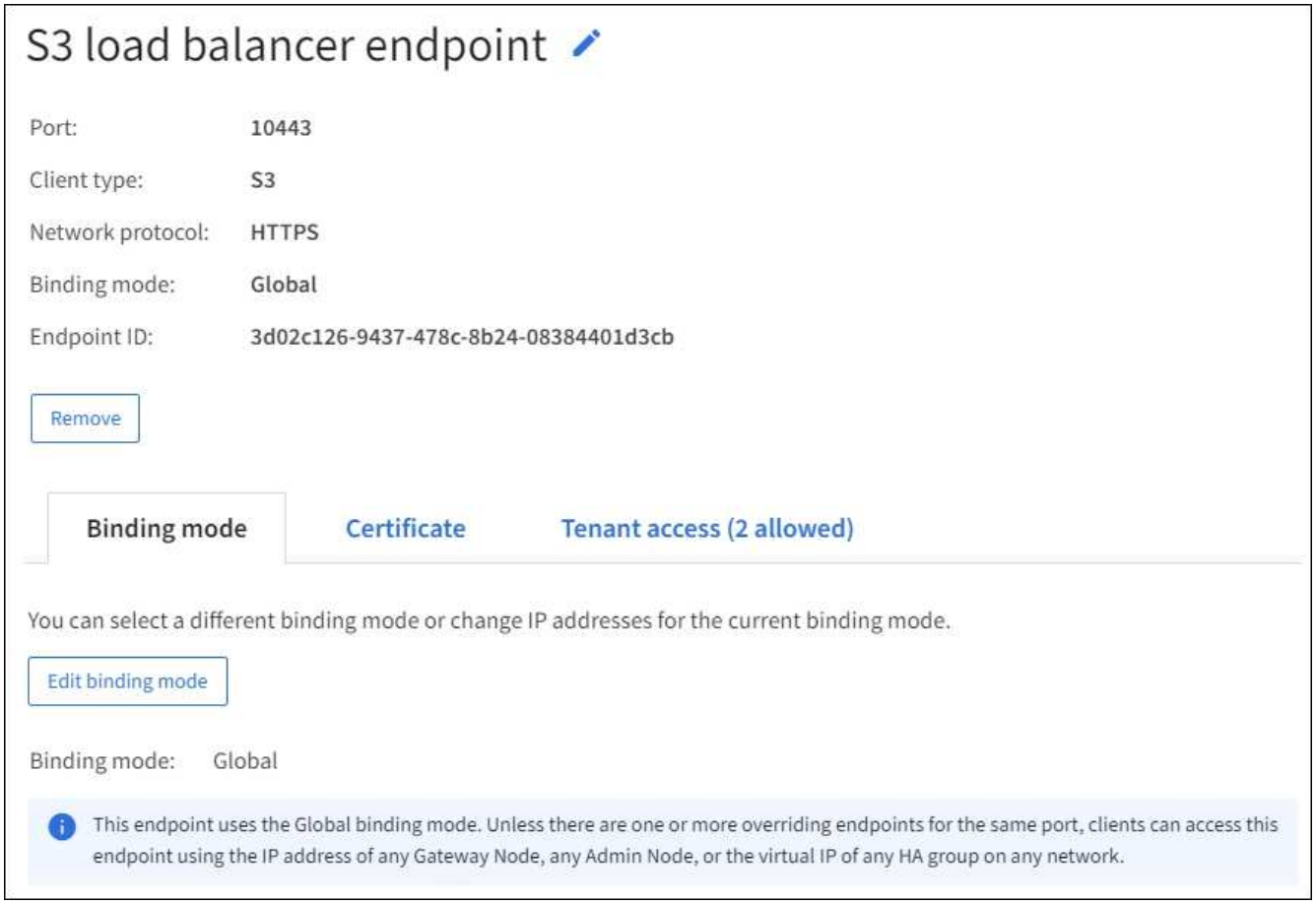
2. Forneça aos clientes S3 e Swift as informações necessárias para se conetar ao endpoint:

- Número da porta
- Nome de domínio ou endereço IP totalmente qualificado
- Todos os detalhes necessários do certificado

Visualize e edite pontos de extremidade do balanceador de carga

Você pode exibir detalhes dos endpoints existentes do balanceador de carga, incluindo os metadados do certificado para um endpoint seguro. Você pode alterar certas configurações para um endpoint.

- Para exibir informações básicas de todos os pontos de extremidade do balanceador de carga, revise as tabelas na página pontos de extremidade do balanceador de carga.
- Para exibir todos os detalhes sobre um endpoint específico, incluindo metadados de certificado, selecione o nome do endpoint na tabela. As informações apresentadas variam consoante o tipo de ponto de extremidade e a forma como são configuradas.



- Para editar um endpoint, use o menu **ações** na página pontos de extremidade do balanceador de carga.

Se você perder o acesso ao Gerenciador de Grade ao editar a porta de um endpoint de interface de gerenciamento, atualize o URL e a porta para recuperar o acesso.

Depois de editar um endpoint, você pode precisar esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu ações	Página de detalhes
Edite o nome do endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar nome do endpoint**. c. Introduza o novo nome. d. Selecione **Guardar**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione o ícone de edição . c. Introduza o novo nome. d. Selecione **Guardar**.
Editar porta de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar porta de endpoint** c. Introduza um número de porta válido. d. Selecione **Guardar**.	*n/a*
Editar o modo de encadernação de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **actions** > **Edit endpoint binding mode** c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione **Editar modo de encadernação**. c. Atualize o modo de encadernação conforme necessário. d. Selecione **Salvar alterações**.
Editar certificado de endpoint	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar certificado de endpoint**. c. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **certificado**. c. Selecione **Editar certificado**. d. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. e. Selecione **Salvar alterações**.
Editar acesso ao locatário	a. Selecione a caixa de verificação para o endpoint. b. Selecione **ações** > **Editar acesso ao locatário**. c. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. d. Selecione **Salvar alterações**.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia **Acesso ao locatário**. c. Selecione **Editar acesso ao locatário**. d. Escolha uma opção de acesso diferente, selecione ou remova locatários da lista ou faça ambos. e. Selecione **Salvar alterações**.

Remova os pontos finais do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **ações** ou remover um único endpoint da página de detalhes.

> Para evitar interrupções do cliente, atualize os aplicativos de cliente S3 ou Swift afetados antes de remover um ponto de extremidade do balanceador de carga. Atualize cada cliente para se conetar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Certifique-se de atualizar todas as informações de certificado necessárias também.

> Se você perder o acesso ao Gerenciador de Grade ao remover um endpoint de interface de gerenciamento, atualize o URL.

- Para remover um ou mais pontos finais:
  a. Na página Load balancer, marque a caixa de seleção para cada ponto final que deseja remover.
  b. Selecione **ações** > **Remover**.
  c. Selecione **OK**.
- Para remover um endpoint da página de detalhes:
  a. Na página Load balancer. Selecione o nome do endpoint.
  b. Selecione **Remover** na página de detalhes.
  c. Selecione **OK**.

Configurar nomes de domínio de endpoint S3

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

> O uso de um endereço IP para um nome de domínio de endpoint não é suportado. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você confirmou que uma atualização de grade não está em andamento.

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

Sobre esta tarefa

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

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.

- Certifique-se de que o "Certificado que o cliente usa para conexões HTTPS com o StorageGRID" está assinado para todos os nomes de domínio que o cliente requer.

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

- Configure o servidor DNS usado pelo cliente. Inclua Registros DNS para os endereços IP que os clientes usam para fazer conexões e verifique se os Registros fazem referência a todos os nomes de domínio de endpoint S3 necessários, incluindo quaisquer nomes de curinga.

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

Os clientes que usam conexões HTTPS (recomendadas) para a grade podem usar qualquer um destes certificados:

- Os clientes que se conetam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de endpoint S3.
- Os clientes que se conetam a um ponto de extremidade do balanceador de carga ou diretamente a um nó de armazenamento podem personalizar o certificado global S3 e Swift API para incluir todos os nomes de domínio de endpoint S3 necessários.

> ⓘ Se você não adicionar nomes de domínio de endpoint S3 e a lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

Adicione um nome de domínio de endpoint S3

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Introduza o nome de domínio no campo **Domain Name 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.
3. Selecione **Guardar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint S3 necessários.
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use seu próprio certificado"atualize o certificado associado ao endpoint", .
   - Se os clientes se conetarem a um ponto de extremidade do balanceador de carga que use o certificado global S3 e Swift API ou diretamente aos nós de storage, "Atualize o certificado global S3 e Swift API".
5. Adicione os Registros DNS necessários para garantir que as solicitações de nome de domínio de endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o endpoint *`bucket.s3.company.com`*, o servidor DNS resolve para o

endpoint correto e o certificado autentica o endpoint como esperado.

Renomeie um nome de domínio de endpoint S3

Se você alterar um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Selecione o campo de nome de domínio que deseja editar e faça as alterações necessárias.
3. Selecione **Guardar**.
4. Selecione **Sim** para confirmar a alteração.

Exclua um nome de domínio de endpoint S3

Se você remover um nome usado por aplicativos S3, as solicitações de estilo hospedado virtual falharão.

Passos

1. Selecione **CONFIGURATION** > **Network** > **S3 endpoint domain names**.
2. Selecione o ícone de exclusão ✕ ao lado do nome de domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- "USE A API REST DO S3"
- "Ver endereços IP"
- "Configurar grupos de alta disponibilidade"

Resumo: Endereços IP e portas para conexões de clientes

Para armazenar ou recuperar objetos, os aplicativos cliente S3 e Swift se conetam ao serviço Load Balancer, que está incluído em todos os nós Admin e nós Gateway, ou ao serviço LDR (roteador de distribuição local), que está incluído em todos os nós de armazenamento.

Os aplicativos clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de grade e o número da porta do serviço nesse nó. Como opção, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões altamente disponíveis que usam endereços IP virtual (VIP). Se você quiser se conetar ao StorageGRID usando um nome de domínio totalmente qualificado (FQDN) em vez de um endereço IP ou VIP, você pode configurar entradas de DNS.

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. Se você já criou endpoints do balanceador de carga e grupos de alta disponibilidade (HA), consulte Onde encontrar endereços IP para localizar esses valores no Gerenciador de Grade.

Onde a conexão é feita	Serviço ao qual o cliente se coneta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: • HTTPS: 18083 • HTTP:18085

Exemplos de URLs

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

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

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

`https://192.0.2.5:10443`

Onde encontrar endereços IP

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

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

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

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

3. Para localizar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Na tabela, anote o endereço IP virtual do grupo HA.
4. Para localizar o número da porta de um endpoint do Load Balancer:
   a. Selecione **CONFIGURATION** > **Network** > **Load balancer endpoints**.
   b. Observe o número da porta do endpoint que você deseja usar.

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

   c. Selecione o nome do endpoint na tabela.
   d. Confirme se o **Client type** (S3 ou Swift) corresponde ao aplicativo cliente que usará o endpoint.

Informações sobre direitos autorais

Informações sobre marcas comerciais