



Configurar conexões de cliente S3 e Swift

StorageGRID

NetApp
March 12, 2025

Índice

Configurar conexões de cliente S3 e Swift	1
Sobre as conexões de clientes S3 e Swift	1
Resumo: Endereços IP e portas para conexões de clientes	1
Configurar interfaces VLAN	4
Considerações para interfaces VLAN	4
Crie uma interface VLAN	5
Editar uma interface VLAN	7
Remova uma interface VLAN	8
Gerenciar grupos de alta disponibilidade	8
Gerenciar grupos de alta disponibilidade (HA): Visão geral	8
Como os grupos HA são usados?	11
Opções de configuração para grupos de HA	12
Configurar grupos de alta disponibilidade	14
Gerenciar o balanceamento de carga	20
Gerenciar balanceamento de carga: Visão geral	20
Como funciona o balanceamento de carga - Serviço do Load Balancer	21
Configurar pontos de extremidade do balanceador de carga	22
Como funciona o balanceamento de carga - serviço CLB (obsoleto)	30
Configure os nomes de domínio de endpoint da API S3	31
Ativar HTTP para comunicações de cliente	33
Controle quais operações do cliente são permitidas	34

Configurar conexões de cliente S3 e Swift

Sobre as conexões de clientes S3 e Swift

Como administrador de grade, você gerencia as opções de configuração que controlam como os locatários S3 e Swift podem conectar 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 conectando-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 conectar 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:

- *** Interfaces VLAN*:** Você pode criar interfaces LAN virtual (VLAN) em nós de administração e nós de gateway para isolar e particionar o tráfego de clientes e locatários para segurança, flexibilidade e desempenho. Depois de criar uma interface VLAN, você a adiciona a um grupo de alta disponibilidade (HA).
- **Grupos de alta disponibilidade:** Você pode criar um grupo de HA das interfaces para 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.
- **Serviço de balanceamento de carga:** Você pode habilitar os clientes a usar 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 conectar usando pontos de extremidade do balanceador de carga.

Você também pode habilitar o uso de HTTP para clientes que se conectam 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 conectar 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 conectar usando o endereço IP virtual do grupo HA.

Sobre esta tarefa

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conectar 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 conecta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: <ul style="list-style-type: none"> • HTTPS:8083 • HTTP:8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	<ul style="list-style-type: none"> • Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • HTTPS: 8082 • HTTP: 8084 Portas Swift padrão: <ul style="list-style-type: none"> • HTTPS:8083 • HTTP:8085

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP: 18085

Exemplos

Para conectar 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 conectar ao StorageGRID:

- `https://192.0.2.5:10443`

Para conectar 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 conectar ao StorageGRID:

- `https://192.0.2.6:10444`

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

Passos

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 conectar.
 - 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:

- Selecione **CONFIGURATION > Network > High Availability groups**.
- Na tabela, anote o endereço IP virtual do grupo HA.

4. Para localizar o número da porta de um endpoint do Load Balancer:

- Selecione **CONFIGURATION > Network > Load balancer endpoints**.

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

- Selecione um endpoint e selecione **Editar endpoint**.

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

- Confirme se o endpoint selecionado está configurado para uso com o protocolo correto (S3 ou Swift) e selecione **Cancelar**.

- 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.

Configurar interfaces VLAN

Você pode criar interfaces de LAN virtual (VLAN) em nós de administração e nós de gateway e usá-las em grupos de HA e pontos de extremidade do balanceador de carga para isolar e particionar o tráfego para obter segurança, flexibilidade e desempenho.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo um ID de VLAN e escolhendo uma interface pai em um ou mais nós.
- Uma interface pai deve ser configurada como uma interface de tronco no switch.
- Uma interface pai pode ser a rede de Grade (eth0), a rede de Cliente (eth2) ou uma interface de tronco adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface pai para um determinado nó. Por exemplo, você não pode usar a interface de rede de Grade e a interface de rede de cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego Admin Node, que inclui tráfego relacionado ao Grid Manager e ao

Tenant Manager, selecione interfaces somente em Admin Nodes.

- Se a interface VLAN for para tráfego de clientes S3 ou Swift, selecione interfaces em nós de administração ou nós de gateway.
- Se você precisar adicionar interfaces de tronco, consulte o seguinte para obter detalhes:
 - **VMware (após a instalação do nó):** [VMware: Adicione interfaces de tronco ou acesso a um nó](#)
 - **RHEL ou CentOS (antes de instalar o nó):** [Criar arquivos de configuração de nó](#)
 - * Ubuntu ou Debian (antes de instalar o nó)*: [Criar arquivos de configuração de nó](#)
 - **RHEL, CentOS, Ubuntu ou Debian (após a instalação do nó):** [Linux: Adicione interfaces de tronco ou acesso a um nó](#)

Crie uma interface VLAN

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Uma interface de tronco foi configurada na rede e conectada ao nó VM ou Linux. Você sabe o nome da interface do tronco.
- Você sabe o ID da VLAN que está configurando.

Sobre esta tarefa

O administrador da rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego de cliente ou administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar VLAN 100 para tráfego FabricPool e VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Gerenciador de Grade para criar interfaces de VLAN que permitem que os clientes acessem o StorageGRID em uma VLAN específica. Ao criar interfaces VLAN, você especifica a ID da VLAN e seleciona interfaces pai (tronco) em um ou mais nós.

Acesse o assistente

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Selecione **criar**.

Insira os detalhes das interfaces VLAN

1. Especifique o ID da VLAN na rede. Pode introduzir qualquer valor entre 1 e 4094.

Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar VLAN ID 200 para tráfego de administrador em um local e o mesmo VLAN ID para tráfego de cliente em outro local. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada local. No entanto, duas interfaces VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó.

Se você especificar uma ID que já foi usada, uma mensagem será exibida. Você pode continuar criando outra interface de VLAN para o mesmo ID de VLAN ou pode selecionar **Cancelar** e editar a ID existente.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.

VLAN details

VLAN ID ?

Description (optional) ?

60/64

[Cancel](#)
[Continue](#)

3. Selecione **continuar**.

Escolha interfaces pai

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada local da grade. As interfaces Admin Network (eth1) não podem ser usadas como interfaces pai e não são mostradas.

1. Selecione uma ou mais interfaces pai às quais anexar esta VLAN.

Por exemplo, você pode querer anexar uma VLAN à interface de rede de cliente (eth2) para um nó de gateway e um nó de administrador.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.


Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?	
<input type="checkbox"/>	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
<input checked="" type="checkbox"/>	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
<input type="checkbox"/>	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
<input checked="" type="checkbox"/>	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
<input type="checkbox"/>	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)
[Continue](#)

2. Selecione **continuar**.

Confirme as definições

1. Revise a configuração e faça quaisquer alterações.
 - Se você precisar alterar a ID ou a descrição da VLAN, selecione **Digite os detalhes da VLAN** na parte superior da página.
 - Se você precisar alterar uma interface pai, selecione **escolha interfaces pai** na parte superior da página ou selecione **anterior**.
 - Se for necessário remover uma interface pai, selecione a lixeira .
2. Selecione **Guardar**.
3. Aguarde até 5 minutos para que a nova interface apareça como uma seleção na página grupos de alta disponibilidade e seja listada na tabela **interfaces de rede** para o nó (**NODES > parent interface node > Network**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere a ID ou a descrição da VLAN.
- Adicionar ou remover interfaces pai.

Por exemplo, você pode querer remover uma interface pai de uma interface VLAN se você planeja desativar o nó associado.

Observe o seguinte:

- Não é possível alterar um ID de VLAN se a interface de VLAN for usada em um grupo HA.
- Não é possível remover uma interface pai se essa interface pai for usada em um grupo HA.

Por exemplo, suponha que a VLAN 200 esteja conectada às interfaces pai nos nós A e B. se um grupo de HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você poderá remover a interface pai não utilizada para o nó B, mas não poderá remover a interface pai usada para o nó A.

Passos

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Marque a caixa de seleção da interface VLAN que deseja editar. Em seguida, selecione **ações > Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **continuar**.

Não é possível atualizar um ID de VLAN se a VLAN for usada em um grupo HA.

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **continuar**.
5. Revise a configuração e faça quaisquer alterações.
6. Selecione **Guardar**.

Remova uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela for usada atualmente em um grupo HA. Você deve remover a interface VLAN do grupo HA antes de removê-la.

Para evitar quaisquer interrupções no tráfego do cliente, considere fazer um dos seguintes procedimentos:

- Adicione uma nova interface VLAN ao grupo HA antes de remover essa interface VLAN.
- Crie um novo grupo HA que não use essa interface VLAN.
- Se a interface VLAN que você deseja remover for atualmente a interface ativa, edite o grupo HA. Mova a interface VLAN que você deseja remover para a parte inferior da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e remova a interface antiga do grupo HA. Finalmente, exclua a interface VLAN nesse nó.

Passos

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Marque a caixa de seleção para cada interface VLAN que deseja remover. Em seguida, selecione **ações > Excluir**.
3. Selecione **Sim** para confirmar a sua seleção.

Todas as interfaces VLAN selecionadas são removidas. Um banner verde de sucesso aparece na página interfaces VLAN.

Gerenciar grupos de alta disponibilidade

Gerenciar grupos de alta disponibilidade (HA): Visão geral

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

O que é um grupo HA?

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

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

- Grupos DE HA que incluem nós de gateway, nós de administração ou ambos fornecem conexões de dados altamente disponíveis para clientes S3 e Swift.
- Os GRUPOS DE HA que incluem apenas os nós de Admin fornecem conexões altamente disponíveis ao Gerenciador de Grade e ao Gerente do locatário.
- Um grupo de HA que inclui apenas dispositivos SG100 ou SG1000 e nós de software baseados em VMware pode fornecer conexões altamente disponíveis para [S3 inquilinos que usam S3 Selecto](#) . 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 conectar 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 conectam a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface primária é a interface "ativa" para o grupo.

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

Exibir o status atual do grupo de HA de um nó

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

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

- **Ativo:** O grupo HA está sendo hospedado neste nó.
- **Backup:** O grupo HA não está usando esse nó no momento; essa é uma interface de backup.
- **Stopped:** O grupo HA não pode ser hospedado neste nó porque o serviço de alta disponibilidade (keepalived) foi interrompido manualmente.
- **Falha:** O grupo HA não pode ser hospedado neste nó devido a 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.

DC1-ADM1 (Primary Admin Node) [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Name: DC1-ADM1

Type: Primary Admin Node

ID: ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state: ✔ Connected

Software version: 11.6.0 (build 20211207.1804.614bc17)

HA groups: Admin clients (Active)

FabricPool clients (Backup)

IP addresses: 172.16.1.225 - eth0 (Grid Network)

10.224.1.225 - eth1 (Admin Network)

47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#) ▼

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 conectividade 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.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impacto 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:** 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	<ul style="list-style-type: none">• Nó de administração principal (primário)• Nós de administração não primários <p>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.</p>
Acesso apenas ao Gestor do Locatário	<ul style="list-style-type: none">• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	<ul style="list-style-type: none">• Nós de administração• Nós de gateway

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso de cliente S3 para S3 Seleccione	<ul style="list-style-type: none"> • SG100 ou SG1000 aparelhos • Nós de software baseados em VMware <p>Nota: Os GRUPOS HA são recomendados ao usar o S3 Select, mas não são necessários.</p>
Acesso ao cliente S3 ou Swift — serviço CLB	<ul style="list-style-type: none"> • Nós de gateway <p>Nota: o serviço CLB está obsoleto.</p>

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 conectado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconectado e deverá fazer login novamente para retomar sua tarefa.

Alguns procedimentos de manutenção não podem ser executados quando o nó de administração principal não está disponível. Durante o failover, você pode usar o 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.

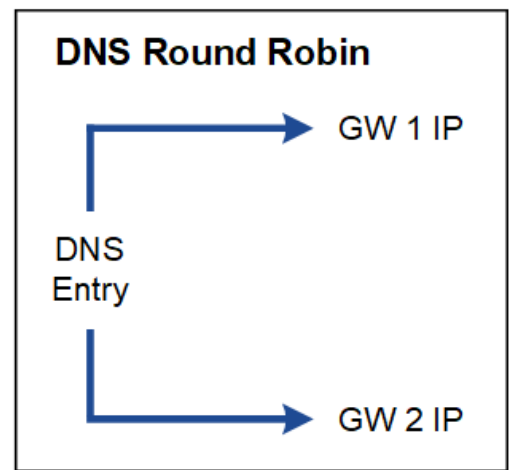
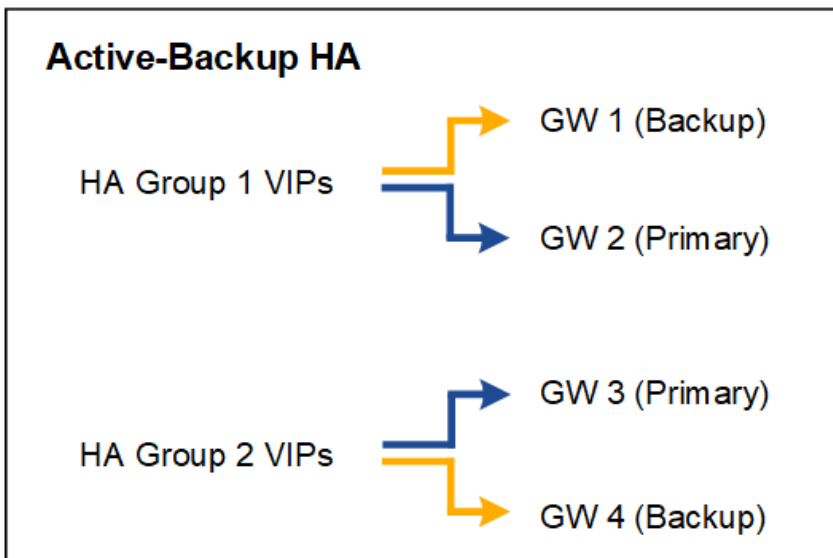


O serviço CLB está obsoleto.

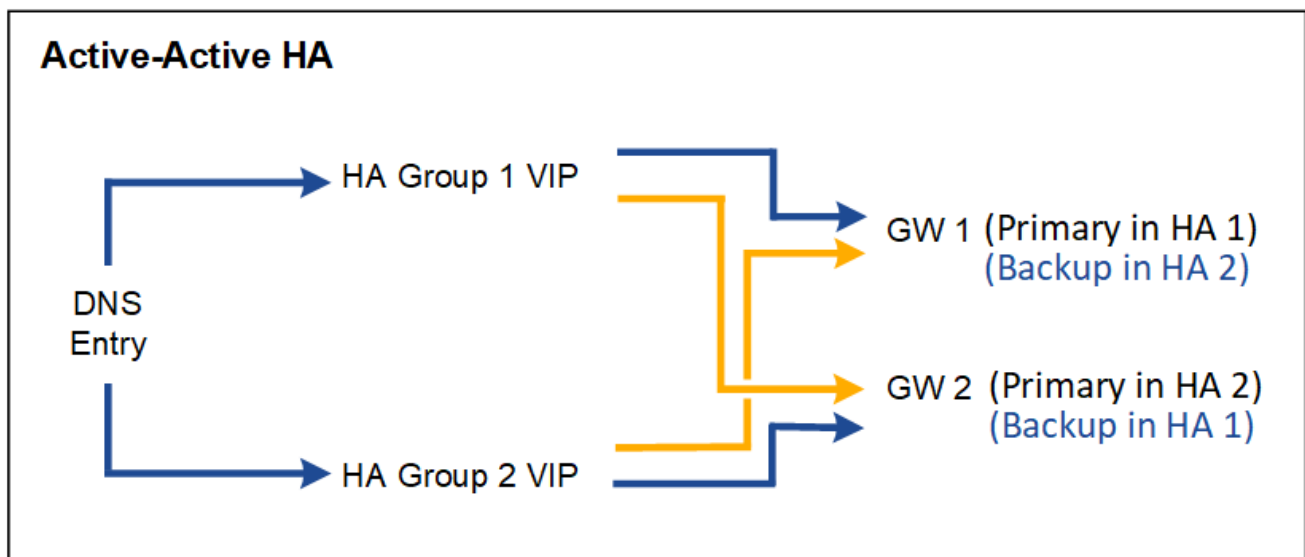
Opções de configuração para grupos de HA

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

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



GW = Gateway Node
VIP = Virtual IP address



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

Configuração	Vantagens	Desvantagens
Active-Backup HA	<ul style="list-style-type: none"> • Gerenciado pelo StorageGRID sem dependências externas. • Failover rápido. 	<ul style="list-style-type: none"> • Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo.
DNS Round Robin	<ul style="list-style-type: none"> • Maior taxa de transferência agregada. • Sem hosts ociosos. 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

O que você vai precisar

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

Crie um grupo de alta disponibilidade

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

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

Acesse o assistente

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

Introduza os detalhes do grupo HA

1. Forneça um nome exclusivo para o grupo HA.

Create a high availability group ✕

1 Enter details — 2 Add interfaces — 3 Prioritize interfaces — 4 Enter IP addresses

Enter details for the HA group

HA group name

Description (optional)

2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **continuar**.

Adicionar interfaces ao grupo HA

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.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Search... Total interface count: 4

Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

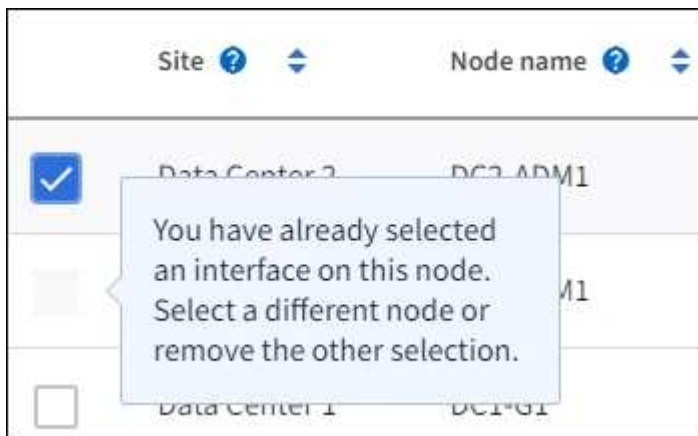
0 interfaces selected



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 o grupo HA for para proteção HA do serviço CLB obsoleto, selecione interfaces somente em nós de Gateway.
- 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 não for possível selecionar uma interface, a caixa de verificação estará 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

1. Determine a interface principal e todas as interfaces de backup (failover) para esse grupo de HA.

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

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order 	Node	Interface 	Node type 
1 (Primary interface)	 DC1-ADM1-104-96 	eth2	Primary Admin Node
2	 DC2-ADM1-104-103 	eth2	Admin Node



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.

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 de HA incluir mais de uma interface e 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.

2. Selecione **continuar**.

Introduza endereços IP

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.

Enter details for the HA group

Subnet CIDR ⓘ

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ⓘ

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ⓘ

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

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 um ou mais **endereços IP virtuais** para o grupo HA. Você pode adicionar até 10 endereços IP. Todos os VIPs devem estar dentro da sub-rede VIP.

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

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

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



Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Próximas etapas

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

Edite um grupo de alta disponibilidade

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

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

Passos

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

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

High availability groups [Learn more about HA groups](#)

You can group the network interfaces of multiple Admin and Gateway Nodes into a high availability (HA) group. If the active interface in the group fails, a backup interface can manage the workload.

Each HA group provides access to the shared services on the selected nodes. Select Gateway Nodes, Admin Nodes, or both for load balancing. Select Admin Nodes for management services. All interfaces in a group must be in the same subnet. You assign one or more virtual IP addresses (VIPs) to each group. Clients use these VIPs to connect to StorageGRID.

- You cannot select an interface if it has a DHCP-assigned IP address.
- Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Create Actions Search... Total HA groups count: 2

<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

← Previous 1 Next →

2. Marque a caixa de seleção do 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 e solte linhas para alterar a ordem de prioridade da interface principal e de quaisquer interfaces de backup para esse grupo de HA.
- d. Opcionalmente, atualize os endereços IP virtuais.
- e. Selecione **Save** e, em seguida, selecione **Finish**.



Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Remova um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de cada vez. No entanto, não é possível remover um grupo de HA se ele estiver vinculado a um ou mais pontos de extremidade do balanceador de carga.

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 conectar 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. Marque a caixa de seleção para cada grupo de HA que deseja remover. Em seguida, selecione **ações > Remover grupo HA**.
3. 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

Gerenciar balanceamento de carga: Visão geral

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 equilibrar a carga de trabalho do cliente 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.

[Como funciona o balanceamento de carga - Serviço do Load Balancer](#) Consulte .

- Use o serviço CLB (Connection Load Balancer) obsoleto, que é instalado apenas em nós de Gateway. O serviço CLB fornece balanceamento de carga da camada 4 e suporta custos de link.

[Como funciona o balanceamento de carga - serviço CLB \(obsoleto\)](#) Consulte .

- 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 de rede (HTTP ou HTTPS), um tipo de cliente (S3 ou Swift) e um modo de ligação. Os endpoints HTTPS requerem um certificado de servidor. Os modos de vinculação permitem restringir a acessibilidade das portas de endpoint a:

- Os endereços IP virtuais (VIPs) de grupos específicos de alta disponibilidade (HA)
- Interfaces de rede específicas de nós específicos de Admin e Gateway

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 em [Remova 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.

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 conectar ao balanceador de carga StorageGRID nos nós de gateway e administrador.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- 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](#) .
- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os GRUPOS HA são recomendados, mas não são necessários. [Gerenciar grupos de alta disponibilidade](#)Consulte .
- Se o ponto final do balanceador de carga for usado [S3 inquilinos para S3 Select](#) pelo , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos SG100 ou SG1000 e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.
- Você configurou todas as interfaces VLAN que planeja usar. [Configurar interfaces VLAN](#)Consulte .
- Se você estiver criando um endpoint HTTPS (recomendado), você terá as informações para o certificado do servidor.



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

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

O certificado 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, `*.storagegrid.example.com` usa o caractere curinga `*` para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`. [Configure os nomes de domínio de endpoint da API S3](#)Consulte .

Crie um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um tipo de cliente (S3 ou Swift) e um protocolo de rede (HTTP ou HTTPS).

Acesse o assistente

1. Selecione **CONFIGURATION > Network > Load balancer endpoints**.
2. Selecione **criar**.

Introduza os detalhes do endpoint

1. Insira os detalhes do endpoint.

Create a load balancer endpoint ✕

1 Enter endpoint details — 2 Select binding mode — 3 Attach certificate

Endpoint details

Name ?

Port ?

Enter an unused port or accept the suggested port.

Client type ?

Select the type of client application that will use this endpoint.

S3 Swift

Network protocol ?

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

HTTPS (recommended) HTTP

Cancel Continue

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	Os clientes de porta serão usados para se conectar ao serviço Load Balancer em nós de administração e nós de gateway. Aceite o número de porta sugerido ou insira qualquer porta externa que não seja usada por outro serviço de grade. Introduza um valor entre 1 e 65535. Se você digitar 80 ou 443 , o endpoint será configurado somente em nós de Gateway. Essas portas são reservadas em nós de administração. Consulte Diretrizes de rede para obter informações sobre portas externas.
Tipo de cliente	O tipo de aplicativo cliente que usará esse endpoint, S3 ou Swift .

Campo	Descrição
Protocolo de rede	<p>O protocolo de rede que os clientes utilizarão ao ligar a este ponto final.</p> <ul style="list-style-type: none"> • Selecione HTTPS para comunicação segura e criptografada TLS (recomendada). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione HTTP para comunicação menos segura e não criptografada. Use HTTP apenas para uma grade não-produção.

2. Selecione **continuar**.

Selecione o modo de encadernação

1. Selecione um modo de encadernação para o endpoint controlar como o endpoint é acessado.

Opção	Descrição
Global (predefinição)	<p>Os clientes podem acessar o endpoint usando um nome de domínio totalmente qualificado (FQDN), o endereço IP de qualquer nó de gateway ou nó de administrador ou o endereço IP virtual de qualquer grupo de HA em qualquer rede.</p> <p>Use a configuração Global (padrão), a menos que você precise restringir a acessibilidade deste endpoint.</p>
Interfaces de nós	<p>Os clientes devem usar o endereço IP de um nó e interface de rede selecionados para acessar esse endpoint.</p>
IPs virtuais de grupos de HA	<p>Os clientes devem usar um endereço IP virtual de um grupo de HA para acessar esse endpoint.</p> <p>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.</p> <p>Os endpoints com este modo podem usar o mesmo número de porta, desde que as interfaces selecionadas para os endpoints não se sobreponham.</p>



Se você usar a mesma porta para mais de um endpoint, um endpoint usando o modo **Virtual IPs de grupos de HA** substitui um endpoint usando o modo **Node interfaces**, que substitui um endpoint usando o modo **Global**.

2. 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.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

Global Node interfaces Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search... Total interface count: 3

<input type="checkbox"/>	Node ?	Node interface ?	Site ?	IP address ?	Node type ?
<input type="checkbox"/>	DC1-ADM1	eth0 ?	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth1 ?	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth2 ?	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

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

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

Global Node interfaces Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search... Total interface count: 2

<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. 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 terminar](#) para . Caso contrário, selecione **continuar** para anexar o certificado.

Anexar certificado

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, assinado pela CA de grade, por um certificado personalizado assinado por uma autoridade de certificação externa. [Configure os certificados API S3 e Swift](#) Consulte .

2. Se você não estiver usando o certificado StorageGRID S3 e Swift, carregue ou gere o certificado.

Carregar certificado

- a. Selecione **carregar certificado**.
- b. Carregue os ficheiros de certificado do servidor necessários:
 - **Certificado do servidor:** O arquivo de certificado do servidor personalizado na codificação PEM.
 - **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (.key).



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

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.
- c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.
 - Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- d. Selecione **criar**. O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift e o endpoint.

Gerar certificado

- a. Selecione **Generate certificate** (gerar certificado).
- b. Especifique as informações do certificado:
 - **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:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
 - **Dias válidos:** Número de dias após a criação em que o certificado expira.
- c. Selecione **Generate**.
- d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

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

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

Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **criar**.

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

depois de terminar

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

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

- Se você tiver configurado um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo de HA, os clientes se conectarão ao serviço do StorageGRID Load Balancer usando o endereço IP de qualquer 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 conectar ao endpoint:

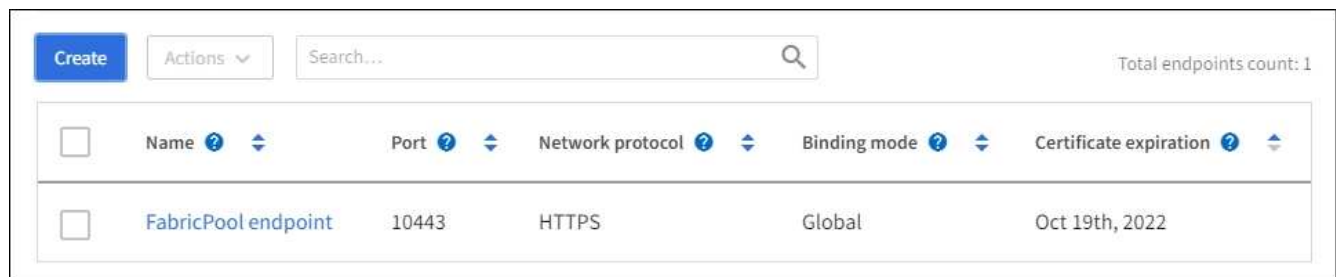
- Número da porta
- Nome de domínio ou endereço IP totalmente qualificado
- Todos os detalhes necessários do certificado

Visualize e edite pontos de extremidade do balanceador de carga

Você pode exibir detalhes dos endpoints existentes do balanceador de carga, incluindo os metadados do certificado para um endpoint seguro. Você também pode alterar o nome ou o modo de vinculação de um endpoint e atualizar quaisquer certificados associados.

Não é possível alterar o tipo de serviço (S3 ou Swift), a porta ou o protocolo (HTTP ou HTTPS).

- Para exibir informações básicas de todos os pontos de extremidade do balanceador de carga, revise a tabela na página pontos de extremidade do balanceador de carga.



<input type="checkbox"/>	Name ? ↕	Port ? ↕	Network protocol ? ↕	Binding mode ? ↕	Certificate expiration ? ↕
<input type="checkbox"/>	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022

- Para exibir todos os detalhes sobre um endpoint específico, incluindo metadados de certificado, selecione o nome do endpoint na tabela.

FabricPool endpoint

Port: 10443

Client type: S3

Network protocol: HTTPS

Binding mode: Global

Endpoint ID: c2b6feb3-c567-449d-b717-4fed98c4a411

[Remove](#)

Binding Mode
Certificate

You can select a different binding mode or change IP addresses for the current binding mode.

[Edit binding mode](#)

Binding mode: Global

This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Para editar um endpoint, use o menu **ações** na página terminais do balanceador de carga ou a página de detalhes de um endpoint específico.



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

Tarefa	Menu ações	Página de detalhes
Edite o nome do endpoint	a. Marque a caixa de seleção do 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 .

Tarefa	Menu ações	Página de detalhes
Editar o modo de encadernação de endpoint	<ol style="list-style-type: none"> Marque a caixa de seleção do endpoint. Selecione actions > Edit endpoint binding mode Atualize o modo de encadernação conforme necessário. Selecione Salvar alterações. 	<ol style="list-style-type: none"> Selecione o nome do endpoint para exibir os detalhes. Selecione Editar modo de encadernação. Atualize o modo de encadernação conforme necessário. Selecione Salvar alterações.
Editar certificado de endpoint	<ol style="list-style-type: none"> Marque a caixa de seleção do endpoint. Selecione ações > Editar certificado de endpoint. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. Selecione Salvar alterações. 	<ol style="list-style-type: none"> Selecione o nome do endpoint para exibir os detalhes. Selecione a guia certificado. Selecione Editar certificado. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. 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 conectar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Certifique-se de atualizar todas as informações de certificado necessárias também.

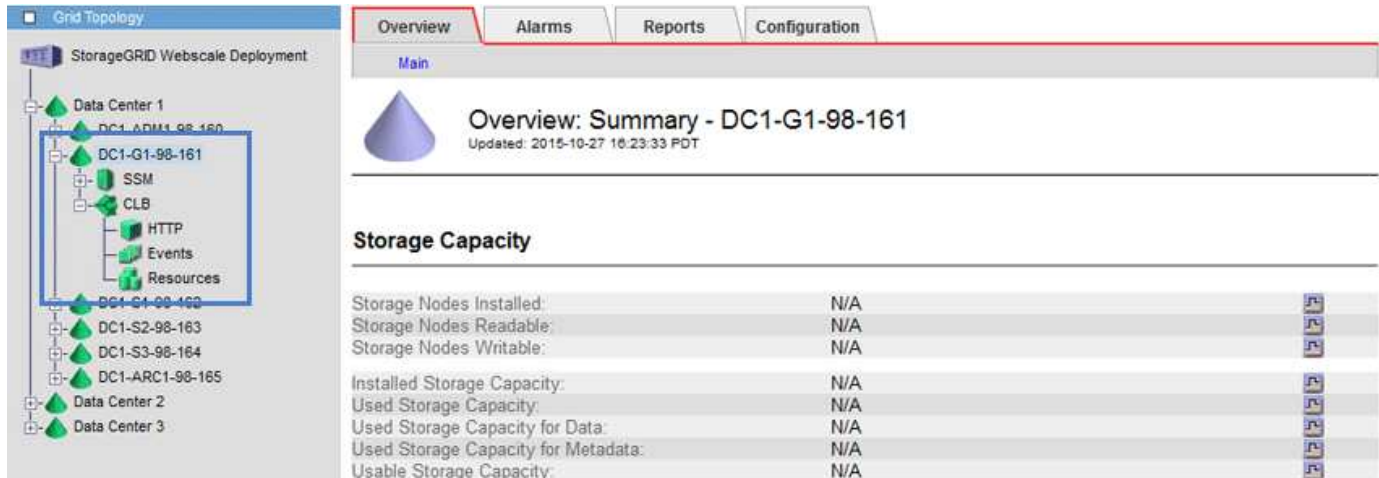
- Para remover um ou mais pontos finais:
 - Na página balanceador de carga, marque a caixa de seleção para cada ponto final que deseja remover.
 - Selecione **ações > Remover**.
 - Selecione **OK**.
- Para remover um endpoint da página de detalhes:
 - Na página Load balancer. Selecione o nome do endpoint.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

Como funciona o balanceamento de carga - serviço CLB (obsoleto)

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, em seguida, expanda um Gateway Node até selecionar **CLB** e as opções abaixo dele.



The screenshot shows the 'Grid Topology' interface. On the left, a tree view displays the hierarchy: StorageGRID Webscale Deployment > Data Center 1 > DC1-G1-98-161 > CLB. The CLB node is highlighted with a blue box. On the right, the 'Overview' tab is active, showing a summary for 'DC1-G1-98-161' updated on 2015-10-27. Below the summary is a 'Storage Capacity' table with the following data:

Storage Capacity	
Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

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

- [Quais são os custos da ligação](#)
- [Atualizar custos de link](#)

Configure os 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 conectam.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- 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 necessários, incluindo quaisquer nomes de curinga.



Os clientes podem se conectar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administrador ou um nó de armazenamento, ou conectando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conectam 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 conectam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.
- Os clientes que se conectam a um ponto de extremidade do balanceador de carga, diretamente a um nó de armazenamento, ou diretamente ao serviço CLB obsoleto em um nó de gateway podem personalizar o certificado global S3 e Swift API para incluir todos os nomes de domínio de endpoint necessários.

Passos

1. Selecione **CONFIGURATION > Network > Domain Names**.

A página nomes de domínio do endpoint é exibida.

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: `s3.example.com`, `s3.example.co.uk`, `s3-east.example.com`

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕

2. Digite a lista de nomes de domínio de endpoint da API S3 nos campos **Endpoint**. Utilize o **+** ícone para adicionar campos adicionais.

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

3. Selecione **Guardar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint necessários.

- Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que use seu próprio certificado, atualize o certificado associado ao ponto de extremidade.
 - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que use o certificado global S3 e Swift API, diretamente aos nós de armazenamento ou ao serviço CLB nos nós de Gateway, 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.

Informações relacionadas

- [Use S3](#)
- [Ver endereços IP](#)
- [Configurar grupos de alta disponibilidade](#)
- [Configure os certificados API S3 e Swift](#)
- [Configurar pontos de extremidade do balanceador de carga](#)

Ativar HTTP para comunicações de 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 conectam 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 conectar 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 **CONFIGURATION > System > Grid options**.

2. Na seção Opções de rede, marque a caixa de seleção **Ativar conexão HTTP** .

Network Options



3. Selecione **Guardar**.

Informações relacionadas

- [Configurar pontos de extremidade do balanceador de carga](#)
- [Use S3](#)
- [Use Swift](#)

Controle 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 **CONFIGURATION > System > Grid options**.

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

Network Options

Prevent Client Modification



Enable HTTP Connection



Network Transfer Encryption



AES128-SHA

AES256-SHA

3. Selecione **Guardar**.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.