Gerenciamento de redes e conexões StorageGRID

StorageGRID

NetApp
March 10, 2025

Índice

Gerenciamento de redes e conexões StorageGRID

Você pode usar o Gerenciador de Grade para configurar e gerenciar redes e conexões StorageGRID.

"Configurando conexões de cliente S3 e Swift"Consulte para saber como conetar clientes S3 ou Swift.

- "Diretrizes para redes StorageGRID"
- "Visualização de endereços IP"
- "Cifras suportadas para conexões TLS de saída"
- "Alteração da encriptação de transferência de rede"
- "Configurando certificados de servidor"
- "Configurando as configurações de proxy de armazenamento"
- "Configurando as configurações de proxy Admin"
- "Gerir políticas de classificação de tráfego"
- "Quais são os custos da ligação"

Diretrizes para redes StorageGRID

O StorageGRID suporta até três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual de acordo com seus requisitos de segurança e acesso.

> Para modificar ou adicionar uma rede para um nó de grade, consulte as instruções de recuperação e manutenção. Para obter mais informações sobre a topologia de rede, consulte as instruções de rede.

Rede de rede

Obrigatório. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes.

Rede de administração

Opcional. A rede de administração é normalmente utilizada para administração e manutenção do sistema. Ele também pode ser usado para acesso ao protocolo cliente. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites.

Rede de clientes

Opcional. A rede de clientes é uma rede aberta normalmente usada para fornecer acesso a aplicativos clientes S3 e Swift, para que a rede de Grade possa ser isolada e protegida. A rede do cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

Diretrizes

- Cada nó de grade do StorageGRID requer uma interface de rede dedicada, endereço IP, máscara de sub-rede e gateway para cada rede à qual está atribuído.
- Um nó de grade não pode ter mais de uma interface em uma rede.
- Um único gateway, por rede, por nó de grade é suportado e deve estar na mesma sub-rede que o nó. Você pode implementar roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede mapeia para uma interface de rede específica.

Rede	Nome da interface
Grelha	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conetado a um dispositivo StorageGRID, portas específicas serão usadas para cada rede. Para obter mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se o eth2 estiver ativado, o 0,0.0.0/0 usará a rede do cliente no eth2. Se o eth2 não estiver ativado, o 0,0.0.0/0 usará a rede de Grade no eth0.
- A rede do cliente não se torna operacional até que o nó da grade se junte à grade
- A rede Admin pode ser configurada durante a implantação do nó de grade para permitir o acesso à interface do usuário de instalação antes que a grade esteja totalmente instalada.

Informações relacionadas

"Manter recuperar"

"Diretrizes de rede"

Visualização de endereços IP

Você pode exibir o endereço IP de cada nó de grade em seu sistema StorageGRID. Em seguida, você pode usar esse endereço IP para fazer login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

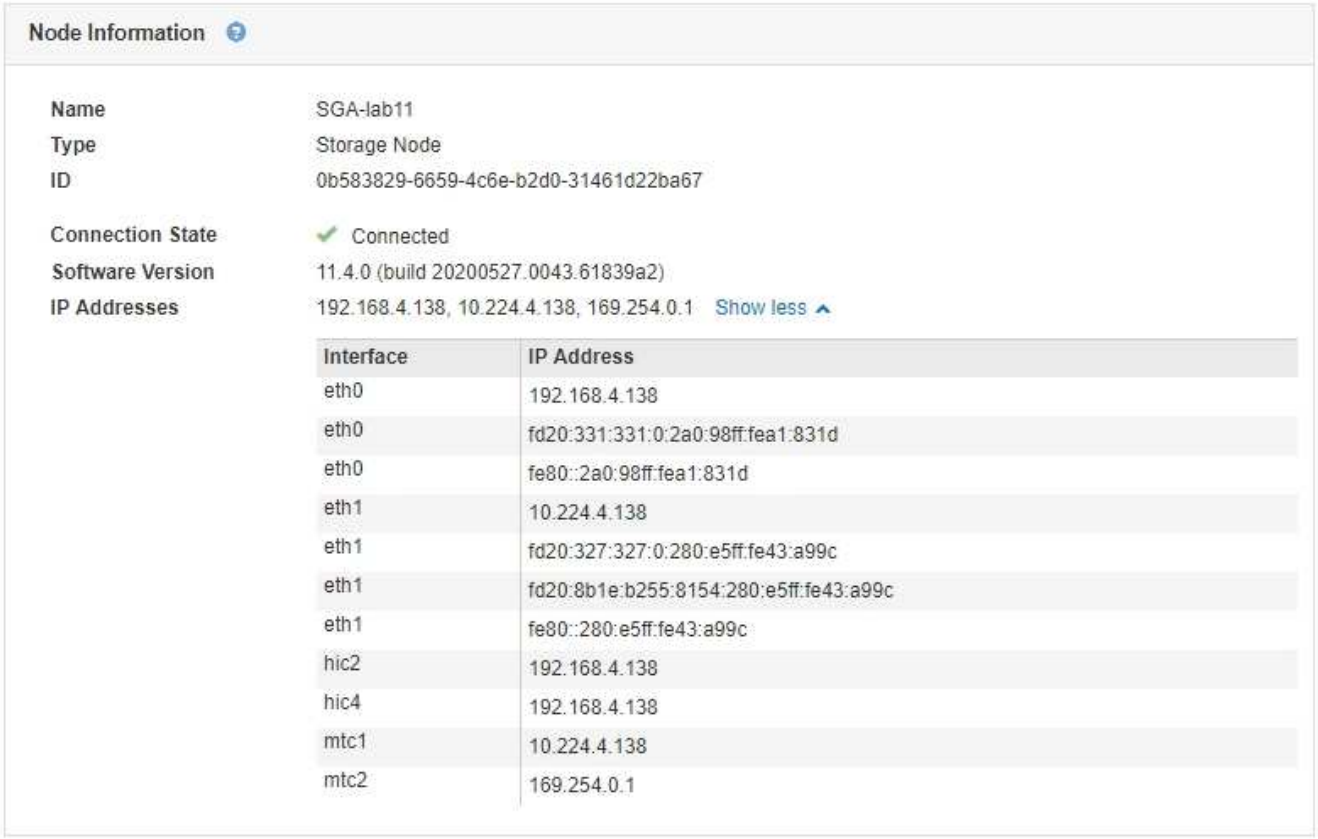
Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte as instruções de recuperação e manutenção.

Passos

1. Selecione **nodes** > ***grid node*** > **Visão geral**.
2. Clique em **Mostrar mais** à direita do título de endereços IP.

   Os endereços IP desse nó de grade são listados em uma tabela.



Informações relacionadas

"Manter recuperar"

Cifras suportadas para conexões TLS de saída

O sistema StorageGRID oferece suporte a um conjunto limitado de conjuntos de codificação para conexões TLS (Transport Layer Security) com os sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

Versões suportadas do TLS

O StorageGRID oferece suporte ao TLS 1,2 e TLS 1,3 para conexões a sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

As cifras TLS que são suportadas para utilização com sistemas externos foram selecionadas para garantir a compatibilidade com uma gama de sistemas externos. A lista é maior do que a lista de cifras que são suportadas para uso com aplicativos cliente S3 ou Swift.

> As opções de configuração TLS, como versões de protocolo, cifras, algoritmos de troca de chaves e algoritmos MAC, não são configuráveis no StorageGRID. Entre em Contato com o representante da sua conta do NetApp se você tiver solicitações específicas sobre essas configurações.

Pacotes de codificação TLS 1,2 suportados

Os seguintes conjuntos de codificação TLS 1,2 são suportados:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Pacotes de codificação TLS 1,3 suportados

Os seguintes conjuntos de codificação TLS 1,3 são suportados:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Alteração da encriptação de transferência de rede

O sistema StorageGRID usa a Segurança da camada de Transporte (TLS) para proteger o tráfego de controle interno entre nós de grade. A opção Network Transfer Encryption (encriptação de transferência de rede) define o algoritmo utilizado pelo TLS para encriptar o tráfego de controlo entre nós de grelha. Esta definição não afeta a encriptação de dados.

O que você vai precisar

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

Sobre esta tarefa

Por padrão, a criptografia de transferência de rede usa o algoritmo AES256-SHA. O tráfego de controle também pode ser criptografado usando o algoritmo AES128-SHA.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, altere criptografia de transferência de rede para **AES128-SHA** ou **AES256-SHA** (padrão).

3. Clique em **Salvar**.

Configurando certificados de servidor

Você pode personalizar os certificados de servidor usados pelo sistema StorageGRID.

O sistema StorageGRID usa certificados de segurança para vários fins distintos:

- Certificados de servidor de interface de gerenciamento: Usado para proteger o acesso ao Gerenciador de grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento de locatário.
- Certificados de servidor de API de storage: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos de cliente de API usam para carregar e baixar dados de objeto.

Você pode usar os certificados padrão criados durante a instalação, ou pode substituir qualquer um desses tipos padrão de certificados por seus próprios certificados personalizados.

Tipos suportados de certificado de servidor personalizado

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

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, consulte os guias de implementação S3 ou Swift.

Certificados para pontos de extremidade do balanceador de carga

O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte as instruções para configurar os pontos de extremidade do balanceador de carga.

Informações relacionadas

"Use S3"

"Use Swift"

"Configuração dos pontos de extremidade do balanceador de carga"

Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário

Você pode substituir o certificado de servidor StorageGRID padrão por um único

certificado de servidor personalizado que permite aos usuários acessar o Gerenciador de Grade e o Gerenciador de locatário sem encontrar avisos de segurança.

Sobre esta tarefa

Por padrão, cada nó de administrador é emitido um certificado assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Como um único certificado de servidor personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado de curinga ou de vários domínios se os clientes precisarem verificar o nome do host ao se conetar ao Gerenciador de Grade e ao Gerenciador de locatário. Defina o certificado personalizado de modo que corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da Autoridade de certificação raiz (CA) que você está usando, os usuários também podem precisar instalar o certificado de CA raiz no navegador da Web que eles usarão para acessar o Gerenciador de Grade e o Gerenciador de locatário.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Management Interface** e o alarme legado de expiração de certificado de Interface de Gerenciamento (MCEP) são acionados quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

> Se você estiver acessando o Gerenciador de Grade ou o Gerenciador de locatário usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se uma das seguintes situações ocorrer:
>
> - O certificado do servidor de interface de gerenciamento personalizado expira.
> - Você reverte de um certificado de servidor de interface de gerenciamento personalizado para o certificado de servidor padrão.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção certificado do servidor de interface de gerenciamento, clique em **Instalar certificado personalizado**.
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

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

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

Os certificados de servidor personalizados são usados para todas as novas conexões de cliente subsequentes.

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

> Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

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

Restaurando os certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário

Você pode reverter para o uso dos certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Gerenciar certificado do servidor de interface, clique em **usar certificados padrão**.
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente subsequentes.

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

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

Você pode substituir o certificado do servidor usado para conexões de cliente S3 ou Swift ao nó de armazenamento ou ao serviço CLB (obsoleto) no nó de gateway. O certificado de servidor personalizado de substituição é específico para a sua organização.

Sobre esta tarefa

Por padrão, cada nó de armazenamento é emitido um certificado de servidor X,509 assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao endpoint de armazenamento. Defina o certificado personalizado de modo que corresponda a todos os nós de storage na grade.

Depois de concluir a configuração no servidor, os usuários também podem precisar instalar o certificado CA raiz no cliente API S3 ou Swift que eles usarão para acessar o sistema, dependendo da Autoridade de Certificação raiz (CA) que você estiver usando.

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Storage API Endpoints** e o alarme legacy Storage API Service Endpoints Certificate Expiration (SCEP) são acionados quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

Os certificados personalizados só são usados se os clientes se conetarem ao StorageGRID usando o serviço CLB obsoleto nos nós do gateway ou se eles se conetarem diretamente aos nós de armazenamento. Os clientes S3 ou Swift que se conetam ao StorageGRID usando o serviço de balanceador de carga em nós de administração ou nós de gateway usam o certificado configurado para o ponto de extremidade do balanceador de carga.

O alerta **Expiration of load balancer endpoint certificate** é acionado para os pontos de extremidade do balanceador de carga que expirarão em breve.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate, clique em **Install Custom Certificate** (Instalar certificado personalizado).
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

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

   - **CA Bundle**: Um único arquivo 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.
4. Clique em **Salvar**.

   O certificado de servidor personalizado é usado para todas as novas conexões de cliente API subsequentes.

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

   Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

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

Informações relacionadas

"Use S3"

"Use Swift"

"Configurando nomes de domínio de endpoint da API S3"

Restaurando os certificados de servidor padrão para os endpoints S3 e Swift REST API

Você pode reverter para o uso dos certificados de servidor padrão para os endpoints da API REST S3 e Swift.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), clique em **Use Default Certificates** (usar certificados padrão).
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão para os endpoints da API de armazenamento de objetos, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente API subsequentes.

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

Copiar o certificado CA do sistema StorageGRID

O StorageGRID usa uma autoridade de certificação (CA) interna para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

O que você vai precisar

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

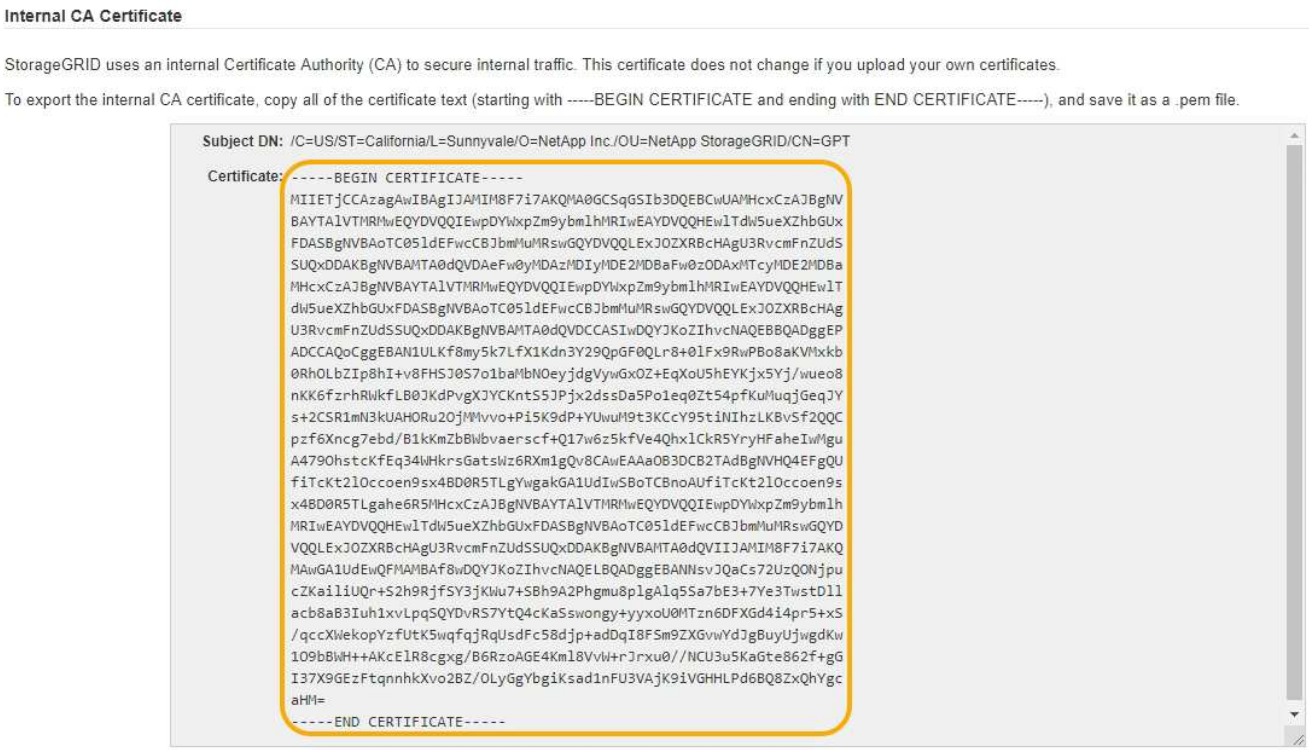
Sobre esta tarefa

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

Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção **certificado de CA interno**, selecione todo o texto do certificado.

   Você deve incluir `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` em sua seleção.



3. Clique com o botão direito do rato no texto selecionado e selecione **Copiar**.
4. Cole o certificado copiado em um editor de texto.
5. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configurando certificados StorageGRID para FabricPool

Para clientes S3 que executam validação estrita de nome de host e não suportam a desativação estrita de validação de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

O que você vai precisar

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

Sobre esta tarefa

Quando você cria um ponto de extremidade do balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam FabricPool. Para obter informações e procedimentos mais detalhados, consulte as instruções de configuração do StorageGRID for FabricPool.

O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é mais recomendado para uso com o FabricPool.

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso do FabricPool.
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

   Quando você cria um endpoint do balanceador de carga HTTPS, é solicitado que você carregue o certificado do servidor, a chave privada do certificado e o pacote CA.

3. Anexar o StorageGRID como uma categoria de nuvem no ONTAP.

   Especifique a porta de endpoint do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado CA.

   Se uma CA intermediária tiver emitido o certificado StorageGRID, você deverá fornecer o certificado de CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.

Informações relacionadas

"Configurar o StorageGRID para FabricPool"

Gerando um certificado de servidor autoassinado para a interface de gerenciamento

Você pode usar um script para gerar um certificado de servidor auto-assinado para clientes de API de gerenciamento que exigem validação estrita do nome de host.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

Sobre esta tarefa

Em ambientes de produção, você deve usar um certificado assinado por uma autoridade de certificação (CA) conhecida. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó Admin.
2. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   c. Digite o seguinte comando para mudar para root: `su -`
   d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

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

3. Configure o StorageGRID com um novo certificado autoassinado.

   `$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management`

   - Para `--domains`, use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o caractere curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
   - Defina `--type` como `management` para configurar o certificado usado pelo Gerenciador de Grade e pelo Gerenciador de Tenant.
   - Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.

     > O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente da API de gerenciamento esteja sincronizado com a mesma fonte de tempo que o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
     management --days 365
     ```

     A saída resultante contém o certificado público necessário pelo cliente da API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags DE INÍCIO e FIM em sua seleção.

5. Faça logout do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Gerenciador de Grade.
   b. Selecione **Configuração** > **certificados de servidor** > **certificado de servidor de interface de gerenciamento**.
7. Configure seu cliente de API de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

Configurando as configurações de proxy de armazenamento

Se você estiver usando serviços de plataforma ou pools de storage em nuvem, poderá configurar um proxy não transparente entre nós de storage e os pontos de extremidade externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.

O que você vai precisar

- Você deve ter permissões de acesso específicas.

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

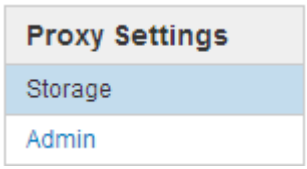
Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

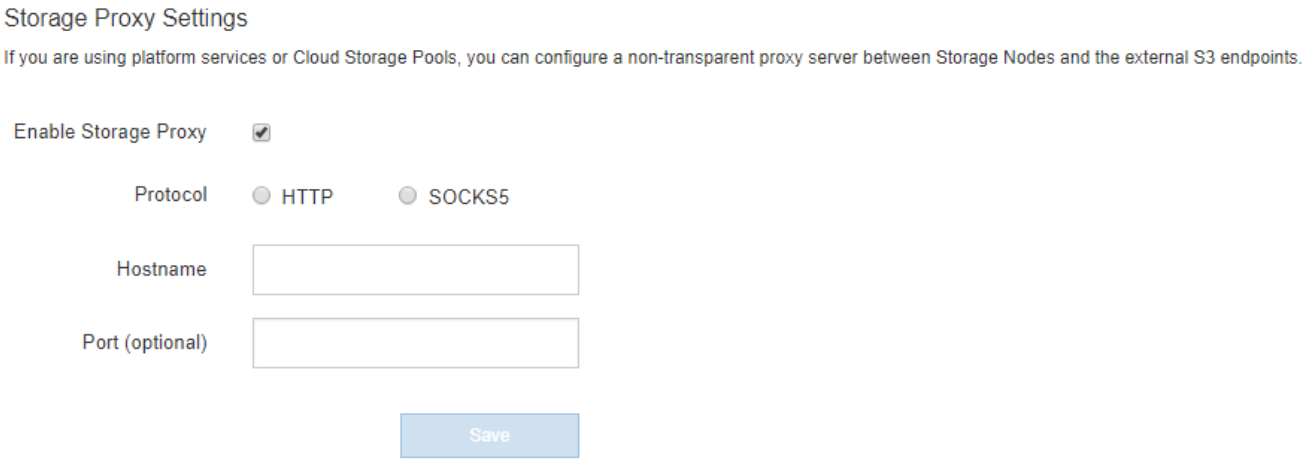
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   A página Configurações do proxy de armazenamento é exibida. Por padrão, **Storage** está selecionado no menu da barra lateral.



2. Marque a caixa de seleção **Enable Storage Proxy** (Ativar proxy de armazenamento*).

   Os campos para configurar um proxy de armazenamento são exibidos.



3. Selecione o protocolo para o proxy de armazenamento não transparente.
4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para se conetar ao servidor proxy.

   Você pode deixar este campo em branco se usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Clique em **Salvar**.

   Depois que o proxy Storage for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem podem ser configurados e testados.

   As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma do StorageGRID não sejam bloqueadas.

Depois de terminar

Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção **Ativar proxy de armazenamento** e clique em **Salvar**.

Informações relacionadas

"Rede e portas para serviços de plataforma"

"Gerenciar objetos com ILM"

Configurando as configurações de proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico (AutoSupport).

O que você vai precisar

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

Sobre esta tarefa

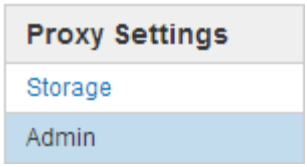
Você pode configurar as configurações para um único proxy Admin.

Passos

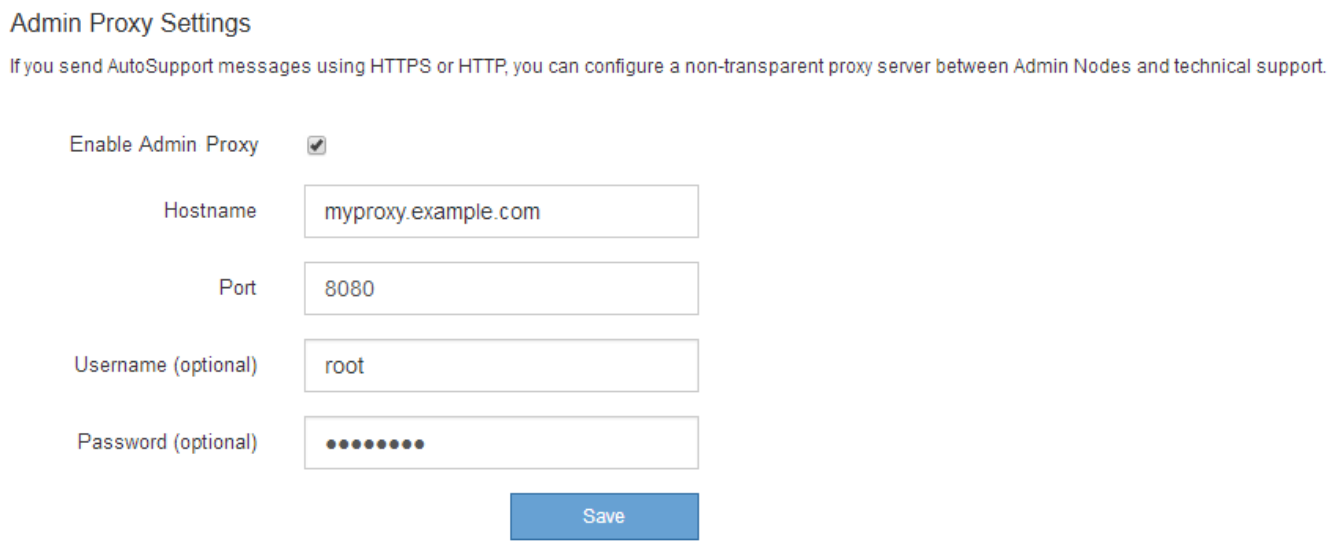
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   É apresentada a página Admin Proxy Settings (Definições de proxy de administração). Por padrão, **Storage** está selecionado no menu da barra lateral.

2. No menu da barra lateral, selecione **Admin**.



3. Marque a caixa de seleção **Enable Admin Proxy** (Ativar proxy de administrador).



4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Introduza a porta utilizada para ligar ao servidor proxy.
6. Opcionalmente, insira o nome de usuário do proxy.

   Deixe este campo em branco se o servidor proxy não exigir um nome de usuário.

7. Opcionalmente, insira a senha do proxy.

   Deixe este campo em branco se o servidor proxy não exigir uma senha.

8. Clique em **Salvar**.

   Depois que o proxy Admin é salvo, o servidor proxy entre nós Admin e o suporte técnico é configurado.

   > As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se você precisar desativar o proxy, desmarque a caixa de seleção **Ativar proxy Admin** e clique em **Salvar**.

Informações relacionadas

"Especificando o protocolo para mensagens AutoSupport"

Gerir políticas de classificação de tráfego

Para aprimorar suas ofertas de qualidade de serviço (QoS), você pode criar políticas de classificação de tráfego para identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e monitoramento de tráfego.

As políticas de classificação de tráfego são aplicadas a pontos de extremidade no serviço de balanceador de carga do StorageGRID para nós de gateway e nós de administração. Para criar políticas de classificação de tráfego, você já deve ter criado pontos de extremidade do balanceador de carga.

Regras de correspondência e limites opcionais

Cada política de classificação de tráfego contém uma ou mais regras correspondentes para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Baldes
- Inquilinos
- Sub-redes (IPv4 sub-redes contendo o cliente)
- Pontos finais (pontos finais do balanceador de carga)

O StorageGRID monitora o tráfego que corresponde a qualquer regra dentro da política de acordo com os objetivos da regra. Qualquer tráfego que corresponda a qualquer regra de uma política é Tratado por essa política. Por outro lado, você pode definir regras para corresponder a todo o tráfego, exceto uma entidade especificada.

Opcionalmente, você pode definir limites para uma política com base nos seguintes parâmetros:

- Agregar largura de banda em
- Agregar largura de banda para fora
- Solicitações de leitura simultânea
- Solicitações de gravação simultânea
- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

Limitação de tráfego

Quando você criou políticas de classificação de tráfego, o tráfego é limitado de acordo com o tipo de regras e limites definidos. Para limites de largura de banda agregada ou por solicitação, as solicitações são transmitidas ou enviadas pela taxa definida. O StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo matcher, é a aplicada. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta de retardo 503 para solicitações que excedem qualquer limite de política correspondente.

No Gerenciador de Grade, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Usando políticas de classificação de tráfego com SLAs

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para aplicar acordos de nível de serviço (SLAs) que fornecem detalhes sobre capacidade, proteção de dados e desempenho.

Os limites de classificação de tráfego são implementados por balanceador de carga. Se o tráfego for distribuído simultaneamente em vários balanceadores de carga, as taxas máximas totais são vários dos limites de taxa especificados.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para alcançar os objetivos de desempenho de cada nível de SLA.

Nível de serviço	Capacidade	Proteção de dados	Desempenho	Custo
Ouro	1 PB de armazenamento permitido	3 copiar regra ILM	25 K solicitações/seg Largura de banda de 5 GB/seg (40 Gbps)	dólares por mês
Prata	250 TB de armazenamento permitido	2 copiar regra ILM	10 K solicitações/seg Largura de banda de 1,25 GB/seg (10 Gbps)	dólares por mês
Bronze	100 TB de armazenamento permitido	2 copiar regra ILM	5 K solicitações/seg Largura de banda de 1 GB/seg (8 Gbps)	dólares por mês

Criando políticas de classificação de tráfego

Você cria políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por intervalo, locatário, sub-rede IP ou ponto de extremidade do balanceador de carga. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

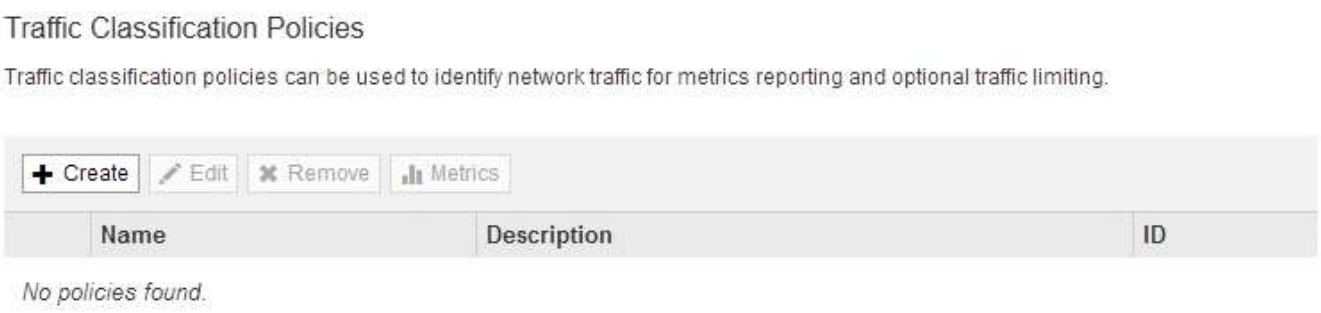
O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Você precisa ter criado os pontos de extremidade do balanceador de carga que você deseja corresponder.
- Você deve ter criado os inquilinos que você deseja corresponder.

Passos

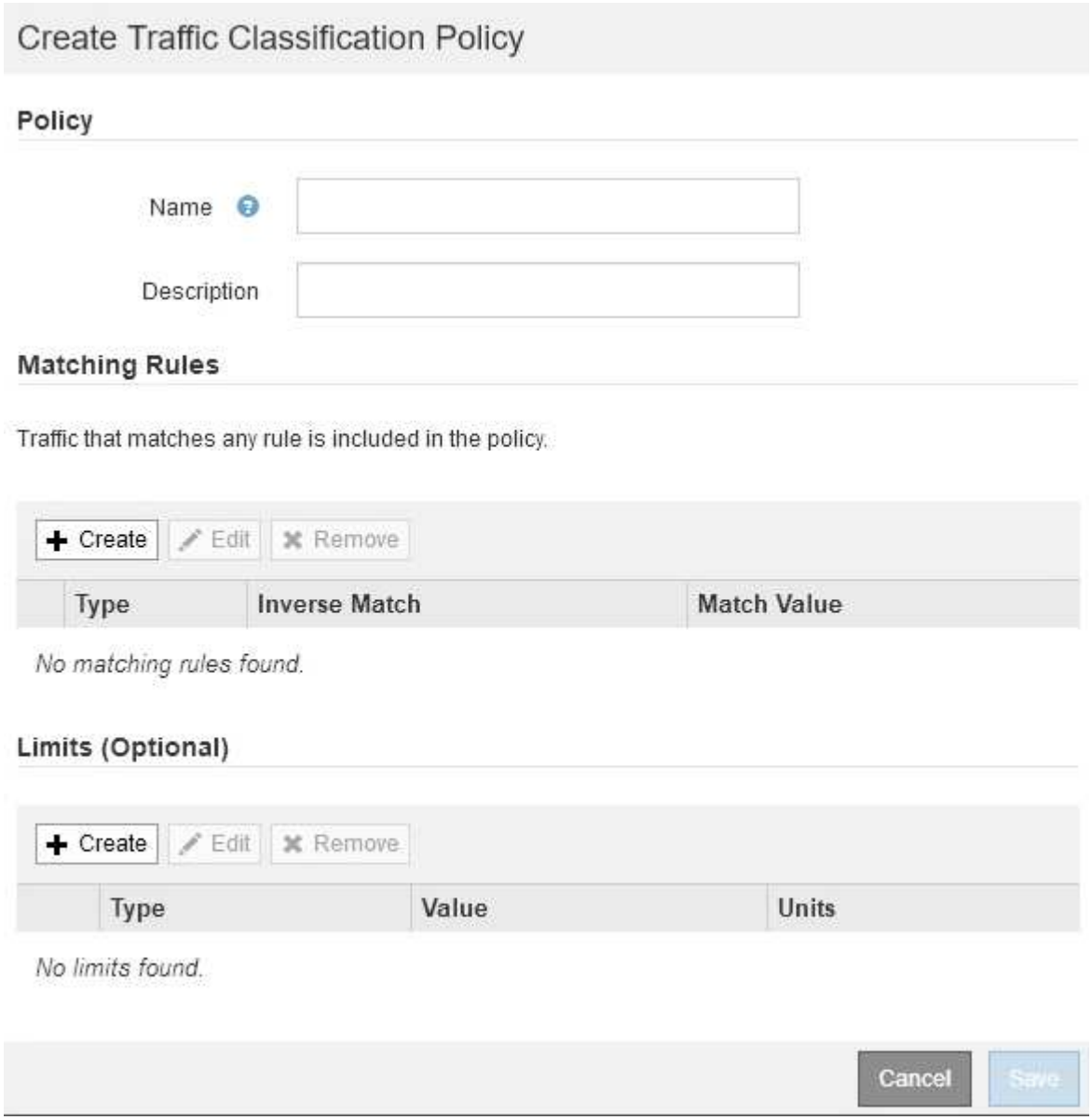
1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   É apresentada a página políticas de classificação de tráfego.



2. Clique em **criar**.

   É apresentada a caixa de diálogo criar política de classificação de tráfego.



3. No campo **Nome**, insira um nome para a política.

   Introduza um nome descritivo para que possa reconhecer a política.

4. Opcionalmente, adicione uma descrição para a política no campo **Description**.

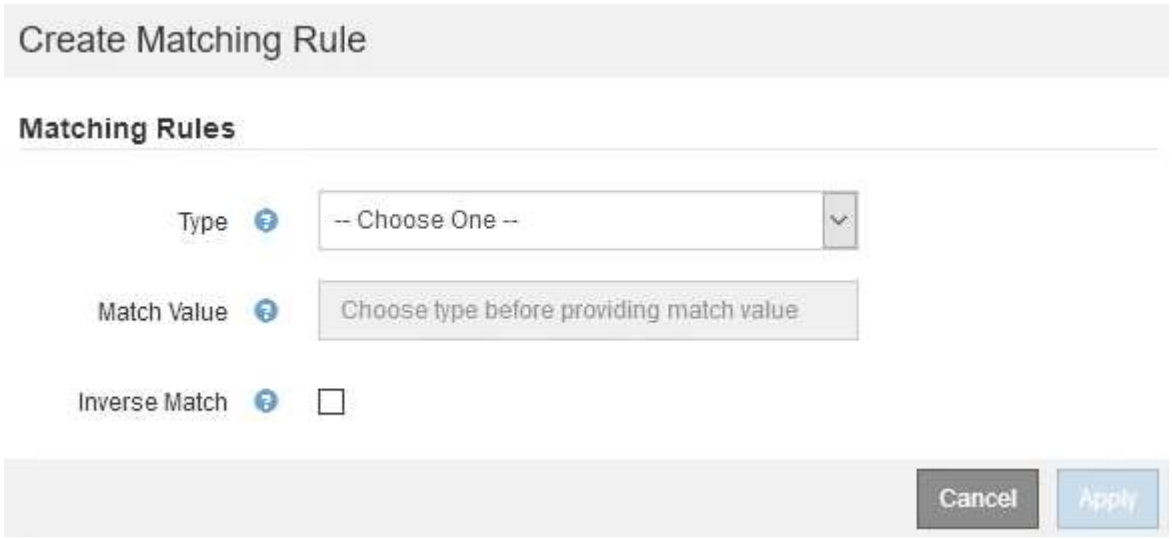
   Por exemplo, descreva ao que esta política de classificação de tráfego se aplica e ao que ela limitará.

5. Crie uma ou mais regras correspondentes para a política.

   Regras de correspondência controlam quais entidades serão afetadas por esta política de classificação de tráfego. Por exemplo, selecione Locatário se desejar que essa diretiva se aplique ao tráfego de rede de um locatário específico. Ou selecione ponto final se pretender que esta política se aplique ao tráfego de rede num ponto de extremidade do balanceador de carga específico.

   a. Clique em **criar** na seção **regras correspondentes**.

      A caixa de diálogo criar regra de correspondência é exibida.



   b. Na lista suspensa **Type**, selecione o tipo de entidade a ser incluída na regra correspondente.

   c. No campo **valor de correspondência**, insira um valor de correspondência com base no tipo de entidade que você escolheu.

      - Balde: Introduza um nome de intervalo.
      - Bucket Regex: Insira uma expressão regular que será usada para corresponder a um conjunto de nomes de bucket.

        A expressão regular não está ancorada. Use a âncora "caret" para corresponder ao início do nome do intervalo e use a âncora "doll" para corresponder ao final do nome.

      - CIDR: Insira uma sub-rede IPv4, na notação CIDR, que corresponda à sub-rede desejada.
      - Endpoint: Selecione um endpoint na lista de endpoints existentes. Esses são os pontos finais do balanceador de carga definidos na página pontos finais do balanceador de carga.
      - Locatário: Selecione um locatário na lista de inquilinos existentes. A correspondência de inquilinos baseia-se na propriedade do bucket que está sendo acessado. O acesso anônimo a um bucket corresponde ao locatário que possui o bucket.

   d. Se você quiser corresponder todo tráfego de rede *exceto* tráfego consistente com o valor tipo e correspondência definido, marque a caixa de seleção **Inverse**. Caso contrário, deixe a caixa de seleção desmarcada.

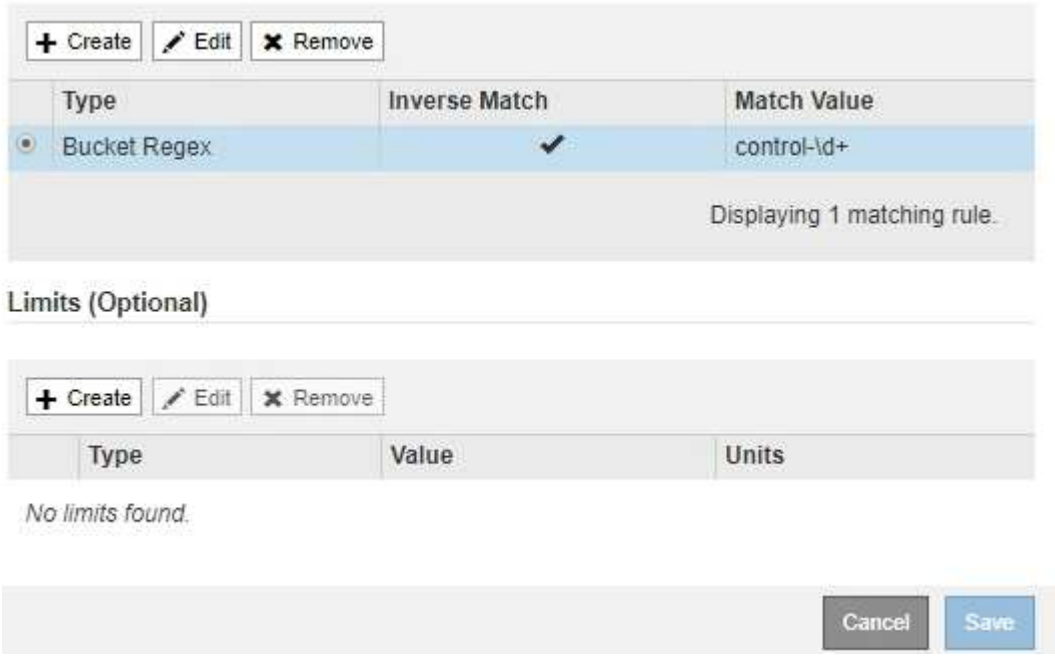
      Por exemplo, se você quiser que essa política se aplique a todos os pontos finais do balanceador de

carga, especifique o ponto final do balanceador de carga a ser excluído e selecione **inverso**.

> Para uma política que contenha vários matchers em que pelo menos um é um matcher inverso, tenha cuidado para não criar uma política que corresponda a todas as solicitações.

e. Clique em **aplicar**.

A regra é criada e está listada na tabela regras correspondentes.



a. Repita estas etapas para cada regra que você deseja criar para a política.

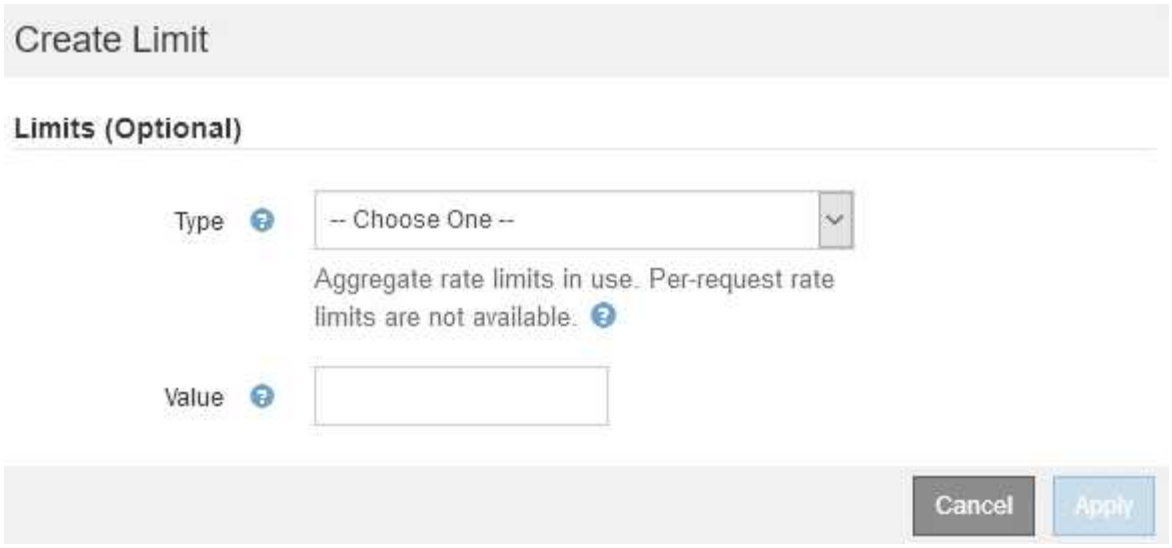
> O tráfego que corresponde a qualquer regra é Tratado pela política.

6. Opcionalmente, crie limites para a política.

> Mesmo que você não crie limites, o StorageGRID coleta métricas para que você possa monitorar o tráfego de rede que corresponde à política.

a. Clique em **criar** na seção **limites**.

A caixa de diálogo criar limite é exibida.



b. Na lista suspensa **Type**, selecione o tipo de limite que deseja aplicar à política.

Na lista a seguir, **in** refere-se ao tráfego de clientes S3 ou Swift para o balanceador de carga StorageGRID, e **OUT** refere-se ao tráfego do balanceador de carga para clientes S3 ou Swift.

- Agregar largura de banda em
- Agregar largura de banda para fora
- Solicitações de leitura simultânea
- Solicitações de gravação simultânea
- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

Para limites de largura de banda, o StorageGRID aplica a política que melhor corresponde ao tipo de limite definido. Por exemplo, se você tem uma política que limita o tráfego em apenas uma direção, então o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais que tenham limites de largura de banda. A StorageGRID implementa as correspondências "melhores" para limites de largura de banda na seguinte ordem:

- Endereço IP exato (/máscara 32)
- Nome exato do balde
- Regex do balde
- Locatário
- Endpoint
- Correspondências CIDR não exatas (não /32)

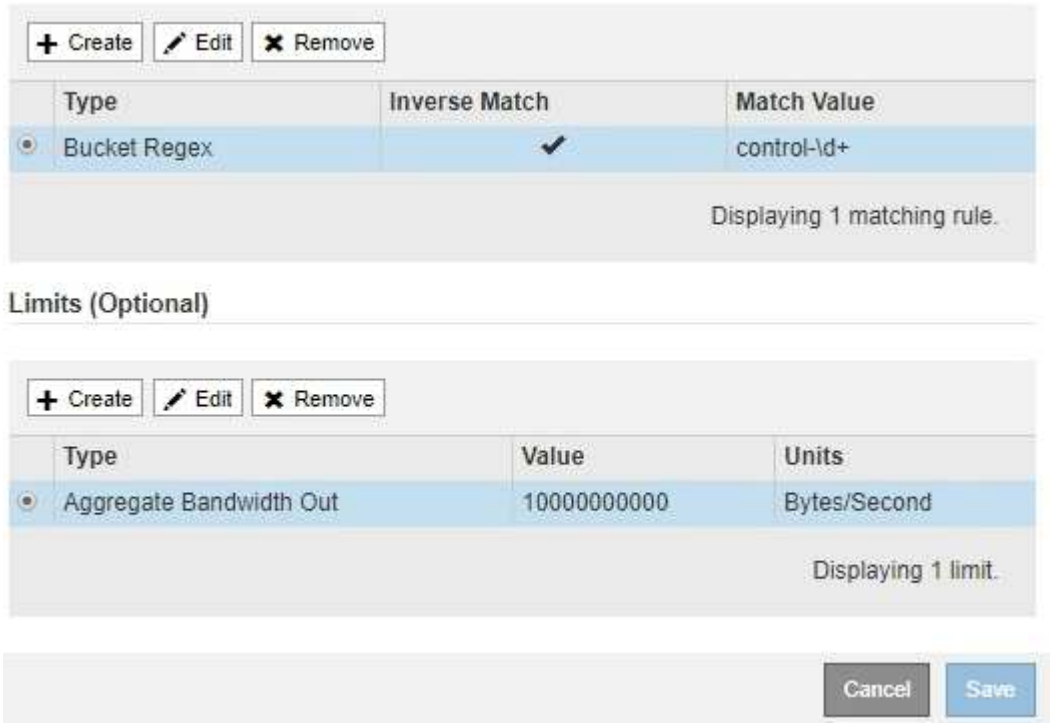
- Correspondências inversas

c. No campo **value**, insira um valor numérico para o tipo de limite escolhido.

   As unidades esperadas são mostradas quando você seleciona um limite.

d. Clique em **aplicar**.

   O limite é criado e é listado na tabela limites.



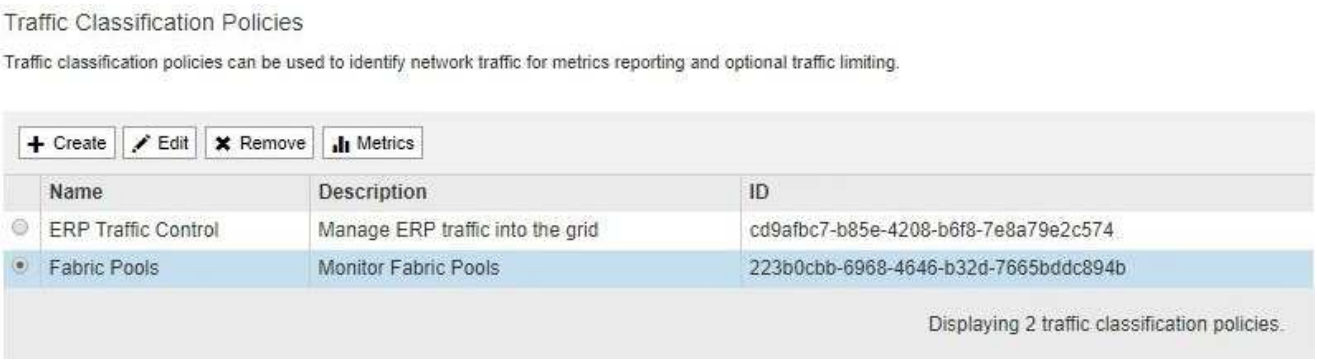
e. Repita estas etapas para cada limite que você deseja adicionar à política.

   Por exemplo, se você quiser criar um limite de largura de banda de 40 Gbps para um nível SLA, crie uma largura de banda agregada no limite e um limite de largura de banda agregada para fora e defina cada um para 40 Gbps.

> Para converter megabytes por segundo em gigabits por segundo, multiplique por oito. Por exemplo, 125 MB/s é equivalente a 1.000 Mbps ou 1 Gbps.

7. Quando terminar de criar regras e limites, clique em **Salvar**.

   A política é guardada e está listada na tabela políticas de classificação de tráfego.



O tráfego de clientes S3 e Swift agora é Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Informações relacionadas

"Gerenciamento do balanceamento de carga"

"Visualização de métricas de tráfego de rede"

Editar uma política de classificação de tráfego

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

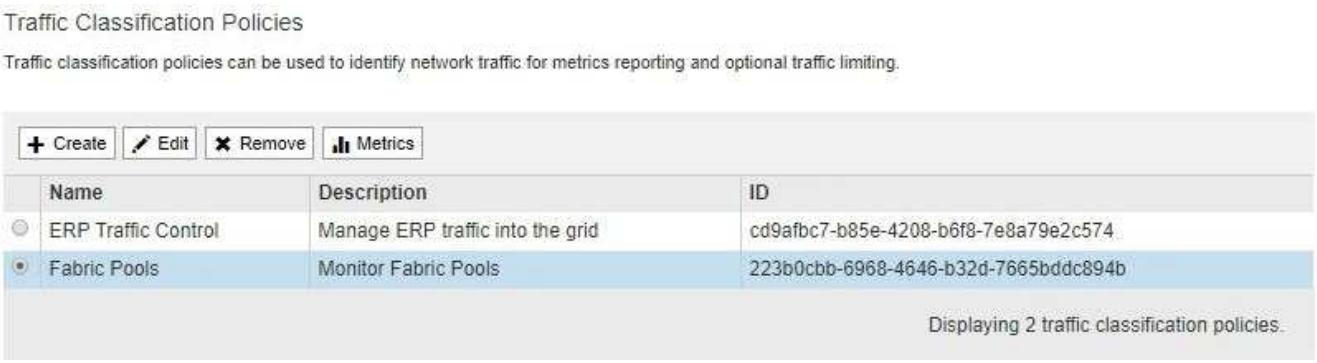
O que você vai precisar

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

Passos

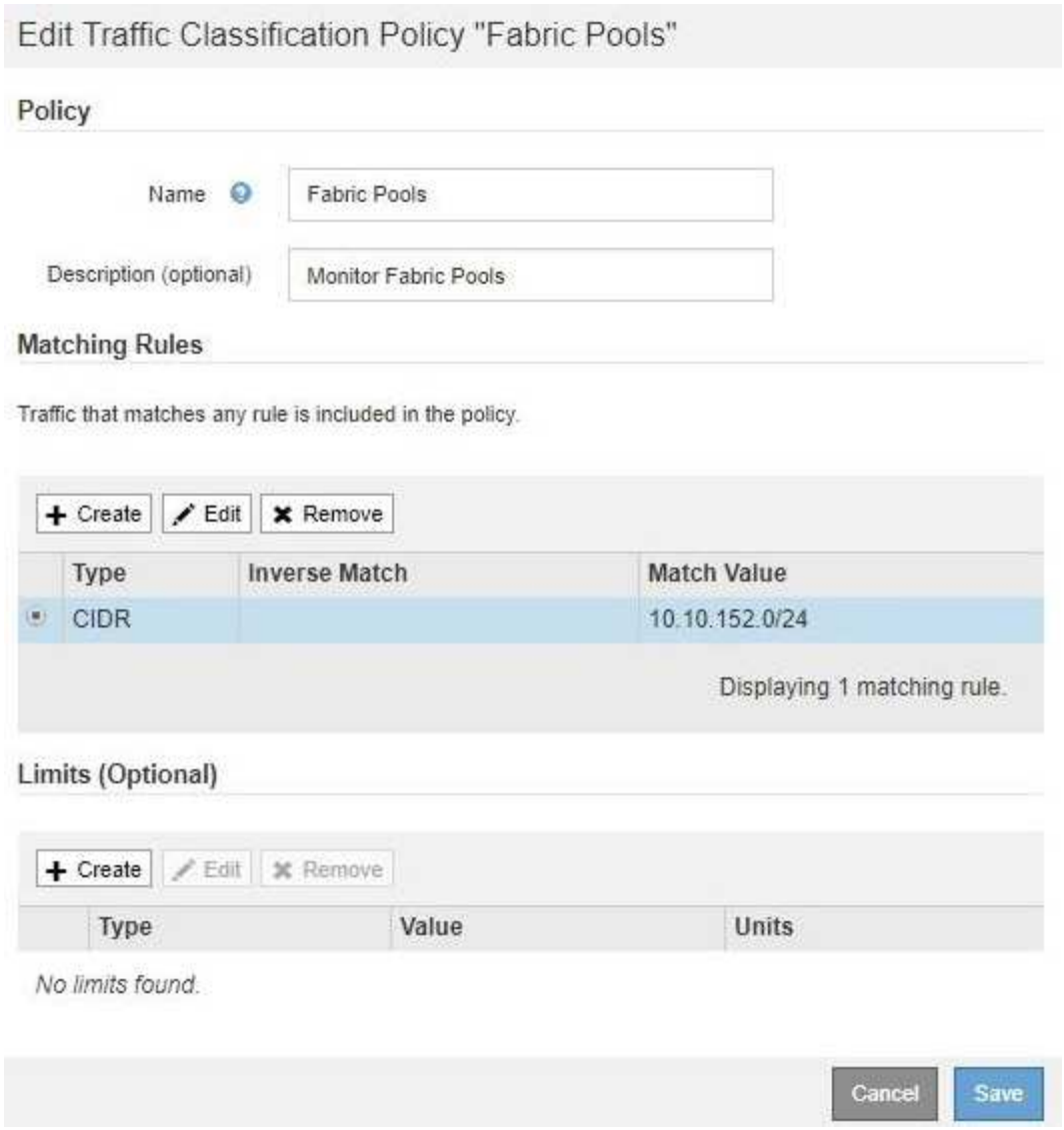
1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.



2. Selecione o botão de opção à esquerda da política que pretende editar.
3. Clique em **Editar**.

   A caixa de diálogo Editar diretiva de classificação de tráfego é exibida.



4. Crie, edite ou remova regras e limites correspondentes conforme necessário.
   a. Para criar uma regra ou limite correspondente, clique em **criar** e siga as instruções para criar uma regra ou criar um limite.
   b. Para editar uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite, clique em **Editar** na seção **regras correspondentes** ou na seção **limites** e siga as instruções para criar uma regra ou criar um limite.
   c. Para remover uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover a regra ou limite.
5. Quando terminar de criar ou editar uma regra ou um limite, clique em **aplicar**.
6. Quando terminar de editar a política, clique em **Salvar**.

   As alterações feitas na política são salvas e o tráfego de rede é agora Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

Eliminar uma política de classificação de tráfego

Se você não precisar mais de uma política de classificação de tráfego, você pode excluí-la.

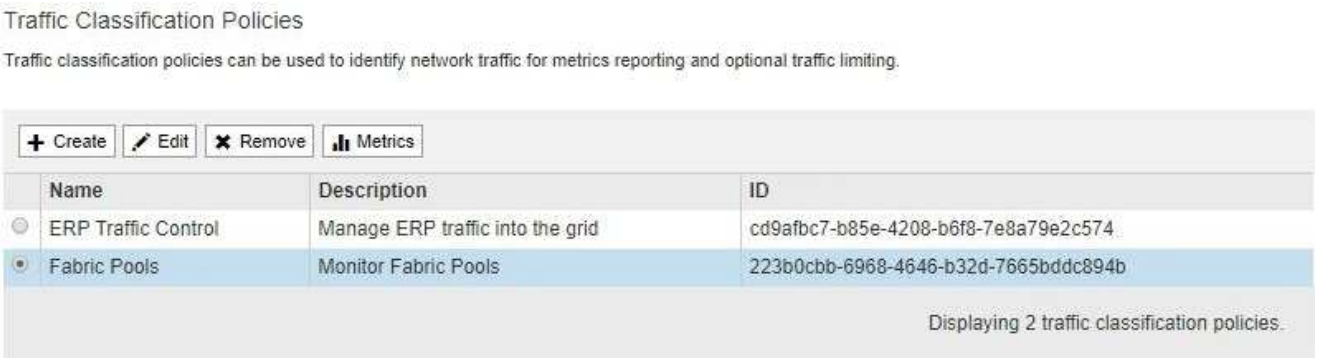
O que você vai precisar

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

Passos

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.



2. Selecione o botão de opção à esquerda da política que pretende eliminar.
3. Clique em **Remover**.

   É apresentada uma caixa de diálogo Aviso.

4. Clique em **OK** para confirmar que deseja excluir a política.

   A política é eliminada.

Visualização de métricas de tráfego de rede

Pode monitorizar o tráfego de rede visualizando os gráficos disponíveis na página políticas de classificação de tráfego.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter a permissão de acesso root.

Sobre esta tarefa

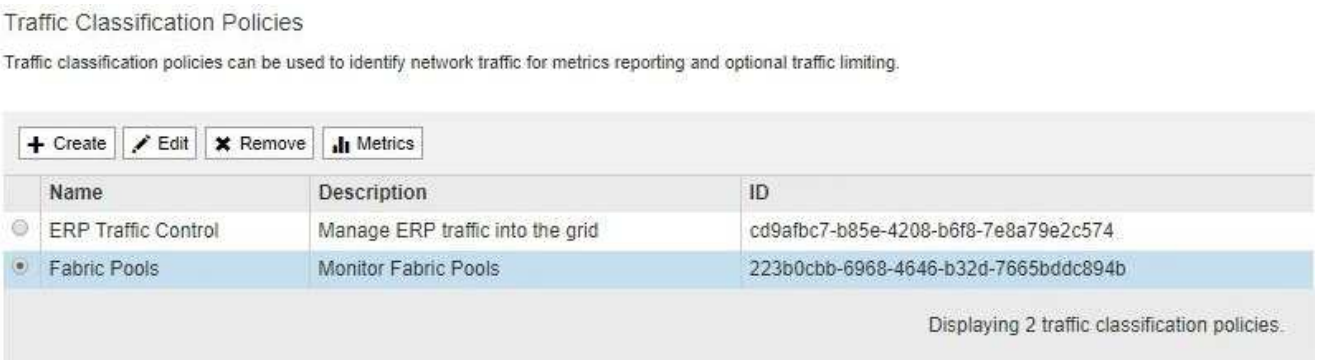
Para qualquer política de classificação de tráfego existente, você pode exibir métricas para o serviço Load Balancer para determinar se a diretiva está limitando com êxito o tráfego na rede. Os dados nos gráficos podem ajudá-lo a determinar se você precisa ajustar a política.

Mesmo que nenhum limite seja definido para uma política de classificação de tráfego, as métricas são coletadas e os gráficos fornecem informações úteis para entender as tendências de tráfego.

Passos

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.



2. Selecione o botão de opção à esquerda da política para a qual deseja exibir as métricas.
3. Clique em **Metrics**.

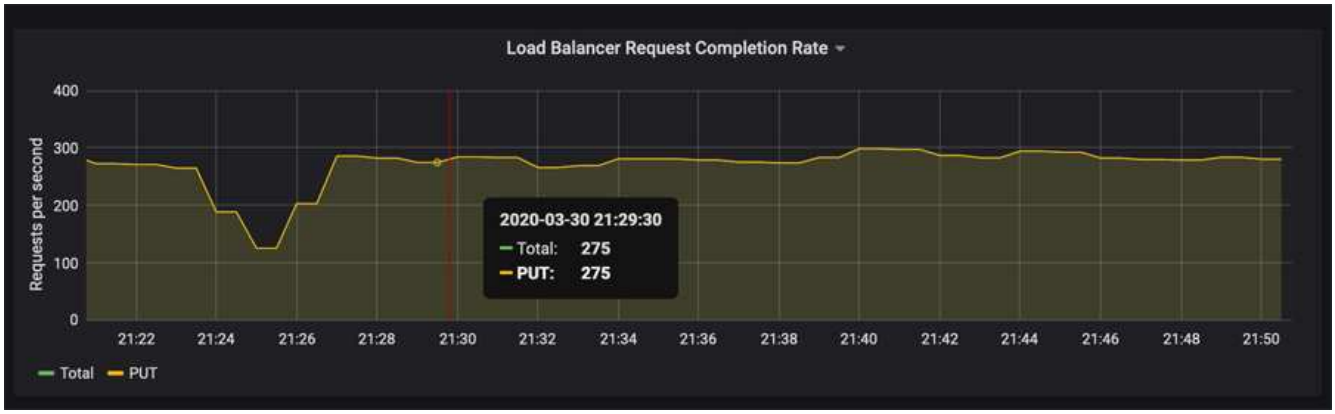
   Uma nova janela do navegador é aberta e os gráficos da Política de classificação de tráfego são exibidos. Os gráficos exibem métricas apenas para o tráfego que corresponde à política selecionada.

   Você pode selecionar outras políticas para exibir usando a lista suspensa **policy**.

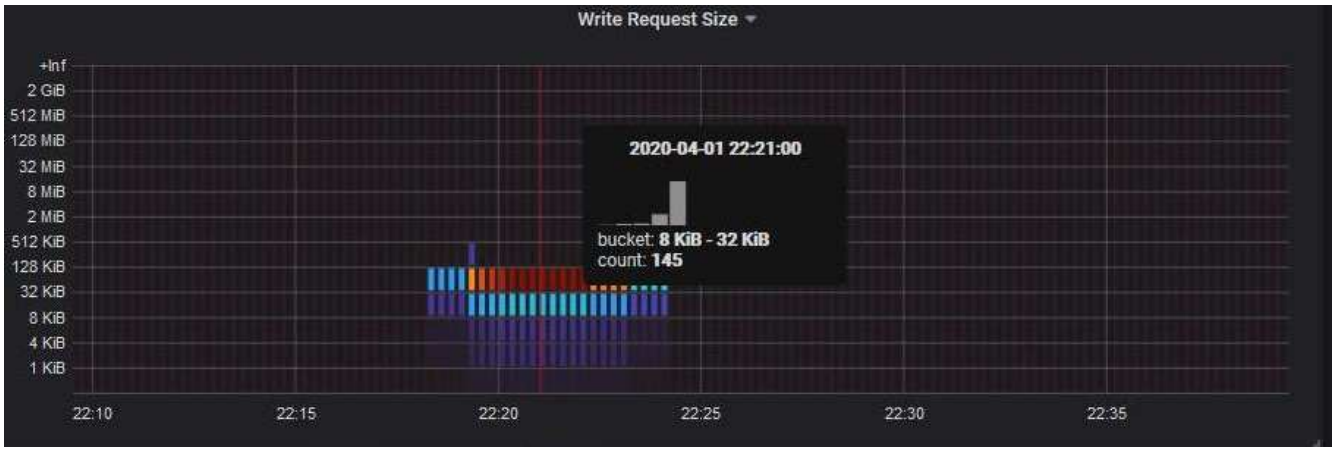
Os gráficos a seguir estão incluídos na página da Web.

- Tráfego de solicitação do Load Balancer: Este gráfico fornece uma média móvel de 3 minutos da taxa de transferência de dados transmitidos entre os pontos de extremidade do balanceador de carga e os clientes que fazem as solicitações, em bits por segundo.
- Taxa de conclusão da solicitação do Load Balancer: Este gráfico fornece uma média móvel de 3 minutos do número de solicitações concluídas por segundo, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Este valor é atualizado quando os cabeçalhos de uma nova solicitação tiverem sido validados.
- Taxa de resposta de erro: Este gráfico fornece uma média móvel de 3 minutos do número de respostas de erro retornadas aos clientes por segundo, discriminada pelo código de resposta de erro.
- Duração média da solicitação (não-erro): Este gráfico fornece uma média móvel de 3 minutos de duração da solicitação, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Cada duração da solicitação começa quando um cabeçalho de solicitação é analisado pelo serviço Load Balancer e termina quando o corpo de resposta completo é retornado ao cliente.
- Taxa de solicitação de gravação por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de gravação são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de escrita referem-se apenas a SOLICITAÇÕES PUT.
- Taxa de solicitação de leitura por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de leitura são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de leitura referem-se apenas a SOLICITAÇÕES GET. As cores no mapa de calor indicam a frequência relativa de um tamanho de objeto dentro de um gráfico individual. As cores mais frias (por exemplo, roxo e azul) indicam taxas relativas mais baixas, e as cores mais quentes (por exemplo, laranja e vermelho) indicam taxas relativas mais altas.

4. Passe o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.



5. Passe o cursor sobre um mapa de calor para ver um pop-up que mostra a data e a hora da amostra, os tamanhos de objetos que são agregados na contagem e o número de solicitações por segundo durante esse período de tempo.



6. Use a lista suspensa **Policy** (Política*) no canto superior esquerdo para selecionar uma política diferente.

   São apresentados os gráficos da política selecionada.

7. Em alternativa, aceda aos gráficos a partir do menu **Support**.
   a. Selecione **Support** > **Tools** > **Metrics**.
   b. Na seção **Grafana** da página, selecione **Política de classificação de tráfego**.
   c. Selecione a política na lista suspensa no canto superior esquerdo da página.

      As políticas de classificação de tráfego são identificadas pelo seu ID. Os IDs de política são listados na página políticas de classificação de tráfego.

8. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

Informações relacionadas

"Monitorizar Resolução de problemas"

Quais são os custos da ligação

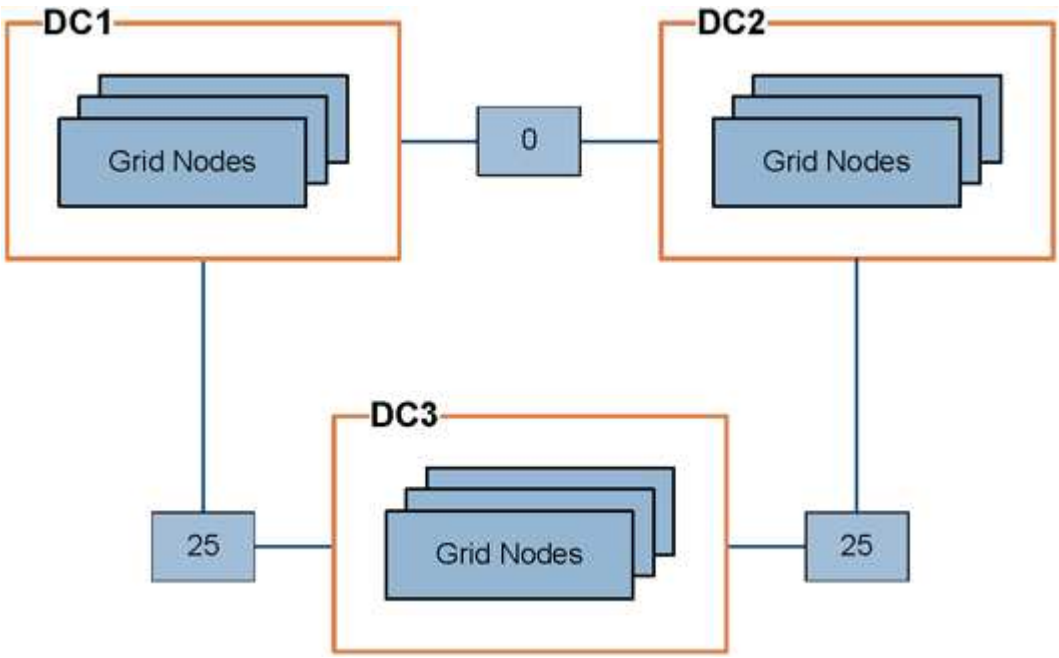
Os custos de link permitem que você priorize qual local do data center fornece um serviço solicitado quando existem dois ou mais locais de data center. Você pode ajustar

os custos de link para refletir a latência entre sites.

- Os custos de link são usados para priorizar qual cópia de objeto é usada para cumprir recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatário para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço CLB nos nós do Gateway para direcionar as conexões do cliente.

> O serviço CLB está obsoleto.

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço CLB nos nós de Gateway distribui igualmente as conexões de cliente para todos os nós de armazenamento no mesmo local do data center e para qualquer local do data center com um custo de link de 0.

  No exemplo, um nó de gateway no local do data center 1 (DC1) distribui igualmente as conexões de cliente para nós de storage em DC1 e para nós de storage em DC2. Um nó de gateway em DC3 envia conexões de cliente somente para nós de storage em DC3.

- Ao recuperar um objeto que existe como várias cópias replicadas, o StorageGRID recupera a cópia no data center que tem o menor custo de link.

  No exemplo, se um aplicativo cliente em DC2 recupera um objeto que é armazenado em DC1 e DC3, o objeto é recuperado de DC1, porque o custo do link de DC1 para D2 é 0, o que é menor do que o custo do link de DC3 para DC2 (25).

Os custos de ligação são números relativos arbitrários sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado menos preferencialmente do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

Link	Custo da ligação	Notas
Entre locais de data center físico	25 (predefinição)	Data centers conectados por um link WAN.
Entre locais lógicos de data center no mesmo local físico	0	Data centers lógicos no mesmo prédio físico ou campus conetados por uma LAN.

Informações relacionadas

"Como funciona o balanceamento de carga - serviço CLB"

Atualizar custos de link

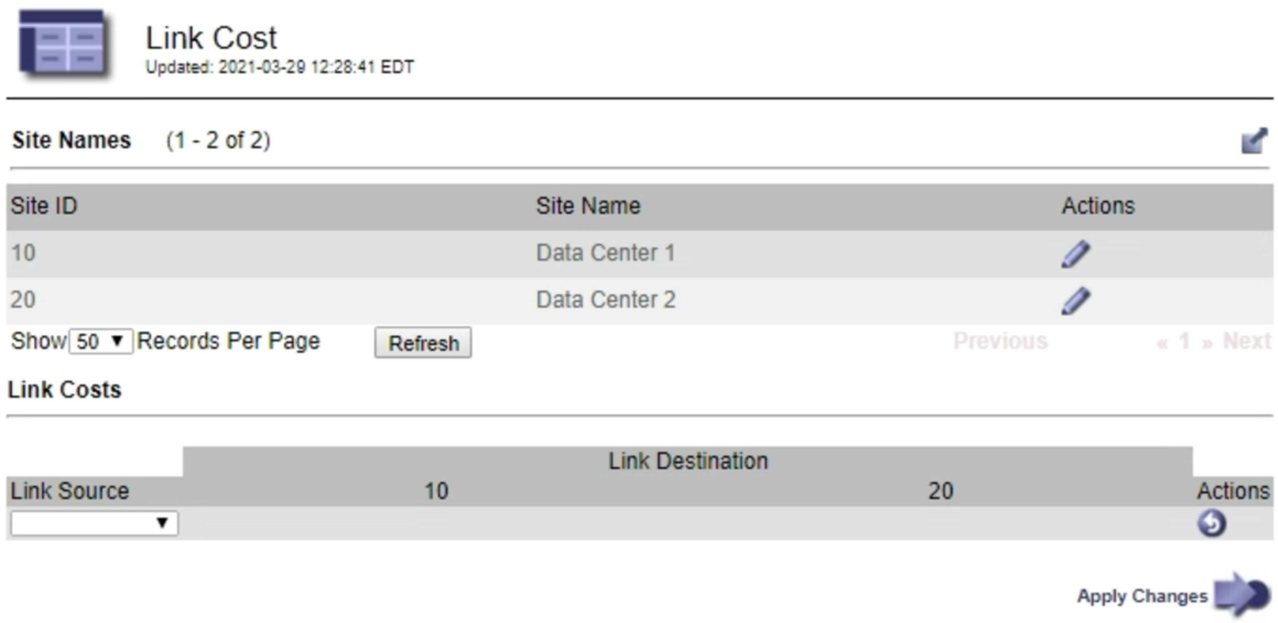
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Configuração da Página de topologia de Grade.

Passos

1. Selecione **Configuração** > **Definições de rede** > **custo de ligação**.



2. Selecione um site em **Link Source** e insira um valor de custo entre 0 e 100 em **Link Destination**.

   Não é possível alterar o custo do link se a origem for igual ao destino.

   Para cancelar as alterações, clique em **Revert**.

3. Clique em **aplicar alterações**.

Informações sobre direitos autorais

Informações sobre marcas comerciais