Controlar firewalls

StorageGRID software

NetApp
July 23, 2026

Índice

Controlar firewalls

Controlar o acesso ao StorageGRID em um firewall externo

Você pode abrir ou fechar portas específicas no firewall externo.

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode querer impedir que os tenants se conectem ao Grid Manager no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se você deseja configurar o firewall interno do StorageGRID, consulte "Configurar firewall interno".

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para Admin Nodes	Navegadores web e clientes de API de gerenciamento podem acessar o Grid Manager, a Grid Management API, o Tenant Manager e a Tenant Management API. **Nota:** A porta 443 também é usada para algum tráfego interno.
8443	Porta do Grid Manager restrita em nós de administração	• Navegadores web e clientes da API de gerenciamento podem acessar o Grid Manager e a Grid Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Tenant Manager nem a Tenant Management API. • Solicitações de conteúdo interno serão rejeitadas.
9443	Porta do Tenant Manager restrita em Admin Nodes	• Navegadores web e clientes da API de gerenciamento podem acessar o Tenant Manager e a Tenant Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Grid Manager nem a Grid Management API. • Solicitações de conteúdo interno serão rejeitadas.

O login único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com login único.

Informações relacionadas

- "Faça login no Grid Manager"
- "Criar conta de locatário"
- "Comunicação externa"

Gerencie os controles internos do firewall no StorageGRID

StorageGRID inclui um firewall interno em cada nó que aumenta a segurança do seu grid, permitindo que você controle o acesso à rede do nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para a sua implementação específica do grid. As alterações de configuração que você faz na página de controle do firewall são aplicadas a cada nó.

Utilize as três abas na página de controle do Firewall para personalizar o acesso necessário para seu grid.

- **Lista de endereços privilegiados**: Use esta aba para permitir acesso selecionado a portas fechadas. Você pode adicionar endereços IP ou sub-redes na notação CIDR que podem acessar portas fechadas usando a aba Gerenciar acesso externo.
- **Gerenciar acesso externo**: Use esta aba para fechar portas que estão abertas por padrão ou reabrir portas previamente fechadas.
- **Rede de cliente não confiável**: Use esta aba para especificar se um nó confia no tráfego de entrada da rede de cliente.

  As configurações desta guia substituem as configurações da guia Gerenciar acesso externo.

  - Um nó com uma Client Network não confiável aceitará apenas conexões nas portas de endpoint do balanceador de carga configuradas nesse nó (globais, de interface de nó e vinculadas ao tipo de nó).
  - As portas dos endpoints do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Manage external networks.
  - Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer endpoints de balanceamento de carga abertos na Client Network.

> As configurações que você define em uma guia podem afetar as alterações de acesso que você faz em outra guia. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporte da maneira que você espera.

Para configurar os controles internos do firewall, consulte "Configurar controles de firewall".

Para obter mais informações sobre firewalls externos e segurança de rede, consulte "Controle de acesso no firewall externo".

Guias Lista de endereços privilegiados e Gerenciar acesso externo

A aba Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso a portas do grid que estão fechadas. A aba Gerenciar acesso externo permite que você feche o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (portas externas são portas acessíveis por nós que não fazem parte do grid por padrão). Essas duas abas geralmente podem ser usadas juntas para personalizar exatamente o acesso à rede que você precisa permitir para seu grid.

> Endereços IP privilegiados não possuem acesso à porta interna da grid por padrão.

Exemplo 1: use um servidor de salto para tarefas de manutenção

Suponha que você queira usar um jump host (um host com segurança reforçada) para administração de rede. Você pode seguir estes passos gerais:

1. Utilize a aba Lista de endereços privilegiados para adicionar o endereço IP do jump host.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

> Adicione o endereço IP privilegiado antes de bloquear as portas 443 e 8443. Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, todas as portas externas no Admin Node do seu grid serão bloqueadas para todos os hosts, exceto o jump host. Você poderá então usar o jump host para realizar tarefas de manutenção no seu grid com mais segurança.

Exemplo 2: bloqueio de portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta. Você pode seguir os seguintes passos gerais:

1. Use a guia Lista de endereços privilegiados para conceder acesso somente aos hosts que precisam acessar o serviço.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.

> Adicione o endereço IP privilegiado antes de bloquear o acesso a quaisquer portas atribuídas ao Grid Manager e ao Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, a porta sensível e o serviço nessa porta ficam disponíveis para os hosts na lista de endereços privilegiados. Todos os outros hosts são impedidos de acessar o serviço, independentemente da interface de origem da solicitação.

Exemplo 3: desativar o acesso a serviços não utilizados

Em nível de rede, você pode desativar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego de cliente HTTP S3, você usaria a opção na guia Gerenciar acesso externo para bloquear a porta 18084.

Aba Redes de Clientes Não Confiáveis

Se você estiver usando uma Client Network, poderá ajudar a proteger o StorageGRID contra ataques hostis, aceitando o tráfego de entrada de clientes somente em endpoints explicitamente configurados.

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, StorageGRID confia nas conexões de entrada para cada nó da grade em todos os "portas externas disponíveis".

Você pode reduzir a ameaça de ataques hostis ao seu StorageGRID especificando que a Client Network em cada nó seja *não confiável*. Se a Client Network de um nó for não confiável, o nó aceita apenas conexões de entrada em portas explicitamente configuradas como endpoints do balanceador de carga. Consulte "Configurar pontos de extremidade do balanceador de carga" e "Configurar controles de firewall".

Exemplo 1: o nó de gateway aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway rejeite todo o tráfego de entrada na Client Network, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Na página "Pontos de extremidade do balanceador de carga", configure um endpoint de balanceador de carga para S3 sobre HTTPS na porta 443.
2. Na página de controle do Firewall, selecione Não confiável para especificar que a Client Network no Gateway Node não é confiável.

Após salvar sua configuração, todo o tráfego de entrada na rede cliente do nó de gateway é bloqueado, exceto as solicitações HTTPS S3 na porta 443 e as solicitações de eco ICMP (ping).

Exemplo 2: nó de armazenamento envia solicitações de serviços da plataforma S3

Suponha que você queira habilitar o tráfego de saída dos serviços da plataforma S3 a partir de um Storage Node, mas queira impedir quaisquer conexões de entrada para esse Storage Node na Client Network. Você executaria esta etapa geral:

- Na guia "Redes de Clientes Não Confiáveis" da página de controle do Firewall, indique que a Rede de Clientes no Nó de Armazenamento não é confiável.

Após salvar sua configuração, o Nó de Armazenamento deixa de aceitar qualquer tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para os destinos de serviços de plataforma configurados.

Exemplo 3: limitar o acesso ao Grid Manager a uma sub-rede

Suponha que você queira permitir o acesso do Grid Manager apenas em uma sub-rede específica. Você executaria os seguintes passos:

1. Conecte a rede do cliente dos seus nós de administração à subnet.
2. Utilize a guia Rede de Cliente Não Confiável para configurar a Rede de Cliente como não confiável.
3. Ao criar um endpoint de balanceador de carga da interface de gerenciamento, insira a porta e selecione a interface de gerenciamento que a porta acessará.
4. Selecione **Sim** para Rede de Cliente Não Confiável.
5. Use a guia Gerenciar acesso externo para bloquear todas as portas externas (com ou sem endereços IP privilegiados definidos para hosts fora dessa sub-rede).

Após salvar sua configuração, somente os hosts na sub-rede que você especificou poderão acessar o Grid Manager. Todos os outros hosts são bloqueados.

Configurar o firewall interno do StorageGRID

Você pode configurar o firewall do StorageGRID para controlar o acesso à rede a portas específicas nos seus nós do StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "navegador web compatível".
- Você tem "permissões de acesso específicas".
- Você analisou as informações em "Gerenciar controles de firewall" e "Diretrizes de networking".
- Se você deseja que um Nó de Administração ou um Nó de Gateway aceite tráfego de entrada somente em endpoints explicitamente configurados, você definiu os endpoints do balanceador de carga.

Ao alterar a configuração da Rede do Cliente, as conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

Sobre esta tarefa

StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas portas nos nós da sua grade. Você pode usar as abas de controle do Firewall para abrir ou fechar portas que estão abertas por padrão na Grid Network, Admin Network e Client Network. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas da grade que estão fechadas. Se você estiver usando uma Client Network, pode especificar se um nó confia no tráfego de entrada da Client Network e configurar o acesso a portas específicas na Client Network.

Limitar o número de portas abertas para endereços IP externos à sua grid apenas àquelas absolutamente necessárias aumenta a segurança da sua grid. Você usa as configurações em cada uma das três guias de controle do Firewall para garantir que somente as portas necessárias estejam abertas.

Para obter mais informações sobre como usar os controles de firewall, incluindo exemplos, consulte "Gerenciar controles de firewall".

Para obter mais informações sobre firewalls externos e segurança de rede, consulte "Controle de acesso no firewall externo".

Acessar controles de firewall

Passos

1. Selecione **Configuração** > **Segurança** > **Controle de firewall**.

   As três abas desta página são descritas em "Gerenciar controles de firewall".

2. Selecione qualquer aba para configurar os controles do firewall.

   Você pode usar essas abas em qualquer ordem. As configurações definidas em uma aba não limitam o que você pode fazer nas outras abas; no entanto, as alterações de configuração feitas em uma aba podem alterar o comportamento das portas configuradas em outras abas.

Lista de endereços privilegiados

Você usa a guia Lista de endereços privilegiados para conceder acesso a hosts a portas que estão fechadas por padrão ou fechadas pelas configurações na guia Gerenciar acesso externo.

Endereços IP e sub-redes privilegiados não têm acesso interno à grid por padrão. Além disso, os endpoints do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados são acessíveis mesmo que estejam bloqueados na guia Gerenciar acesso externo.

As configurações na guia Lista de endereços privilegiados não podem substituir as configurações na guia Rede de cliente não confiável.

Passos

1. Na guia Lista de endereços privilegiados, insira o endereço ou a sub-rede IP à qual você deseja conceder acesso às portas fechadas.
2. Opcionalmente, selecione **Adicionar outro endereço IP ou sub-rede na notação CIDR** para adicionar clientes privilegiados adicionais.

Adicione o mínimo possível de endereços à lista de privilegiados.

3. Opcionalmente, selecione **Permitir que endereços IP privilegiados acessem as portas internas do StorageGRID**. Consulte "Portas internas do StorageGRID".

Esta opção remove algumas proteções para serviços internos. Se possível, deixe-a desativada.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, ela não pode ser acessada por nenhum endereço IP fora da grid, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas que estejam abertas por padrão e só pode abrir portas que você tenha fechado.

As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia Rede de clientes não confiáveis. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede de clientes, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de clientes não confiáveis substituem as portas fechadas (como 443, 8443, 9443) na Rede de clientes.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não fazem parte da grade por padrão) para os nós em sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
   - Utilize o botão ao lado de cada porta para abrir ou fechar a porta selecionada.
   - Selecione **Abrir todas as portas exibidas** para abrir todas as portas listadas na tabela.
   - Selecione **Fechar todas as portas exibidas** para fechar todas as portas listadas na tabela.

Se você fechar as portas 443 ou 8443 do Grid Manager, todos os usuários atualmente conectados a uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Use a barra de rolagem à direita da tabela para garantir que você visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa digitando um número de porta. Você pode digitar um número de porta parcial. Por exemplo, se você digitar **2**, todas as portas que têm a sequência "2" como parte do nome serão exibidas.

3. Selecione **Save**

Rede de cliente não confiável

Se a Rede Cliente de um nó não for confiável, o nó aceitará tráfego de entrada apenas nas portas configuradas como endpoints do balanceador de carga e, opcionalmente, em portas adicionais que você selecionar nesta guia. Você também pode usar esta guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

As conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

As alterações de configuração que você faz na guia **Rede de Clientes Não Confiáveis** substituem as configurações da guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de Cliente Não Confiável**.
2. Na seção Definir padrão para novos nós, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grid em um procedimento de expansão.
   - **Confiável** (padrão): Quando um nó é adicionado em uma expansão, sua Client Network é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede de clientes é não confiável.

     Se necessário, você pode retornar a esta aba para alterar a configuração de um novo nó específico.

     Essa configuração não afeta os nós existentes no seu sistema StorageGRID.
3. Utilize as seguintes opções para selecionar os nós que devem permitir conexões de clientes somente em endpoints de balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:
   - Selecione **Não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista de Rede de Cliente Não Confiável.
   - Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista de Rede de Cliente Não Confiável.
   - Use o botão ao lado de cada nó para definir a Client Network como confiável ou não confiável para o nó selecionado.

     Por exemplo, você pode selecionar **Não confiar nos nós exibidos** para adicionar todos os nós à lista de Rede de Clientes Não Confiáveis e, em seguida, usar a opção ao lado de um nó individual para adicionar esse nó específico à lista de Rede de Clientes Confiáveis.

     Use a barra de rolagem à direita da tabela para garantir que você visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó digitando o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a sequência "GW" como parte do nome serão exibidos.
4. Selecione **Salvar**.

   As novas configurações do firewall são aplicadas e entram em vigor imediatamente. As conexões de cliente existentes podem falhar se os endpoints do balanceador de carga não tiverem sido configurados.

Informações sobre direitos autorais

Informações sobre marcas comerciais