Firewalls de controle

StorageGRID software

NetApp
December 03, 2025

Índice

Firewalls de controle

Controle de acesso em 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 locatários consigam se conectar ao Grid Manager pelo firewall, além de usar outros métodos para controlar o acesso ao sistema.

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

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

O logon 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 logon único.

Informações relacionadas

- "Sign in no Grid Manager"
- "Criar conta de inquilino"

- "Comunicações externas"

Gerenciar controles internos de firewall

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para sua implantação de grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Use as três guias na página de controle do Firewall para personalizar o acesso necessário para sua grade.

- **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 guia Gerenciar acesso externo.
- **Gerenciar acesso externo**: use esta guia para fechar portas que estão abertas por padrão ou reabrir portas fechadas anteriormente.
- **Rede de cliente não confiável**: use esta guia para especificar se um nó confia no tráfego de entrada da rede de cliente.

  As configurações nesta guia substituem as configurações na guia Gerenciar acesso externo.

  - Um nó com uma rede de cliente não confiável aceitará apenas conexões em portas de ponto de extremidade do balanceador de carga configuradas naquele nó (pontos de extremidade globais, de interface de nó e vinculados ao tipo de nó).
  - As portas de ponto de extremidade do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
  - Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer pontos de extremidade do balanceador de carga abertos na Rede do Cliente.

> As configurações feitas em uma guia podem afetar as alterações de acesso feitas em outra guia. Não deixe de verificar as configurações em todas as abas para garantir que sua rede se comporte da maneira esperada.

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 em firewall externo" .

Lista de endereços privilegiados e guias Gerenciar acesso externo

A guia Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso às portas de rede que estão fechadas. A guia 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 que são acessíveis por nós não pertencentes à grade por padrão). Essas duas guias geralmente podem ser usadas juntas para personalizar o acesso exato à rede que você precisa permitir para sua grade.

> Endereços IP privilegiados não têm acesso à porta de rede interna por padrão.

Exemplo 1: Use um host de salto para tarefas de manutenção

Suponha que você queira usar um host de salto (um host com segurança reforçada) para administração de rede. Você pode usar estas etapas gerais:

1. Use a guia Lista de endereços privilegiados para adicionar o endereço IP do host de salto.
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 em 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.

Depois de salvar sua configuração, todas as portas externas no nó de administração em sua grade serão bloqueadas para todos os hosts, exceto o host de salto. Você pode então usar o jump host para executar tarefas de manutenção na sua rede com mais segurança.

Exemplo 2: Bloquear portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta (por exemplo, SSH na porta 22). Você pode usar as seguintes etapas 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 para acessar o Grid Manager e o Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado em 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.

Depois de salvar sua configuração, a porta 22 e o serviço SSH estarão disponíveis para hosts na lista de endereços privilegiados. Todos os outros hosts terão o acesso ao serviço negado, independentemente da interface de onde a solicitação vier.

Exemplo 3: Desabilitar acesso a serviços não utilizados

No nível da rede, você pode desabilitar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego do cliente HTTP S3, você usaria a alternância na guia Gerenciar acesso externo para bloquear a porta 18084.

Guia Redes de clientes não confiáveis

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

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, o 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 sistema StorageGRID especificando que a Rede do Cliente em cada nó seja *não confiável*. Se a rede do cliente de um nó não for confiável, o nó só aceitará conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga. Ver"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 recuse todo o tráfego de entrada na rede do cliente, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Do"Pontos de extremidade do balanceador de carga" página, configure um ponto de extremidade do balanceador de carga para S3 sobre HTTPS na porta 443.
2. Na página de controle do Firewall, selecione Não confiável para especificar que a Rede do Cliente no Nó do Gateway não é confiável.

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

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

Suponha que você queira habilitar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas deseja impedir qualquer conexão de entrada para esse nó de armazenamento na rede do cliente. 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.

Depois de salvar sua configuração, o Nó de Armazenamento não aceita mais nenhum tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para destinos de serviços de plataforma configurados.

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

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

1. Anexe a rede do cliente dos seus nós de administração à sub-rede.
2. Use a guia Rede de cliente não confiável para configurar a Rede de cliente como não confiável.
3. Ao criar um ponto de extremidade do 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).

Depois de salvar sua configuração, somente hosts na sub-rede especificada poderão acessar o Grid Manager. Todos os outros hosts estão bloqueados.

Configurar firewall interno

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

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

- Você revisou as informações em"Gerenciar controles de firewall" e"Diretrizes de rede" .
- Se você quiser que um nó de administração ou nó de gateway aceite tráfego de entrada somente em pontos de extremidade explicitamente configurados, você terá definido os pontos de extremidade do balanceador de carga.

> Ao alterar a configuração da Rede do Cliente, as conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Sobre esta tarefa

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

Limitar o número de portas abertas para endereços IP fora da sua rede apenas para aquelas que são absolutamente necessárias aumenta a segurança da sua rede. Use 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 o uso de 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 em firewall externo" .

Controles de firewall de acesso

Passos

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

   As três guias nesta página são descritas em"Gerenciar controles de firewall" .

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

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

Lista de endereços privilegiados

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

Endereços IP e sub-redes privilegiados não têm acesso à rede interna por padrão. Além disso, os pontos de extremidade do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados podem ser acessados mesmo se bloqueados na guia Gerenciar acesso externo.

> As configurações na guia Lista de endereços privilegiados não podem substituir as configurações na guia Rede de clientes não confiáveis.

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 privilegiada.

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

   Esta opção remove algumas proteções para serviços internos. Deixe-o desabilitado, se possível.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, a porta não pode ser acessada por nenhum endereço IP que não seja da rede, 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 cliente não confiável. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede do Cliente, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de cliente não confiável substituem portas fechadas (como 443, 8443, 9443) na Rede de cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós não pertencentes à grade por padrão) para os nós na sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
   - Use o botão de alternância 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 conectados em uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seus endereços IP tenham sido adicionados à lista de endereços privilegiados.

     Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa inserindo um número de porta. Você pode inserir 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 **Salvar**

Rede de clientes não confiáveis

Se a rede do cliente de um nó não for confiável, o nó aceitará somente tráfego de entrada em portas configuradas como pontos de extremidade do balanceador de carga e, opcionalmente, portas adicionais selecionadas 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 pontos de extremidade do balanceador de carga não tiverem sido configurados.

As alterações de configuração feitas na guia **Rede de cliente não confiável** substituem as configurações na guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de cliente não confiável**.
2. Na seção Definir novo nó padrão, especifique qual deve ser a configuração padrão quando novos nós são adicionados à grade em um procedimento de expansão.
   - **Confiável** (padrão): quando um nó é adicionado em uma expansão, sua Rede de Cliente é confiável.
   - **Não confiável**: quando um nó é adicionado em uma expansão, sua Rede de Cliente não é confiável.

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

     > Esta configuração não afeta os nós existentes no seu sistema StorageGRID .
3. Use as seguintes opções para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:
   - Selecione **Desconfiar dos nós exibidos** para adicionar todos os nós exibidos na tabela à lista Rede de clientes não confiáveis.
   - Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista Rede de clientes não confiáveis.
   - Use a alternância ao lado de cada nó para definir a Rede do Cliente como Confiável ou Não Confiável para o nó selecionado.

     Por exemplo, você pode selecionar **Desconfiar nos nós exibidos** para adicionar todos os nós à lista Rede de clientes não confiáveis e, em seguida, usar a alternância ao lado de um nó individual para adicionar esse único nó à lista Rede de clientes confiáveis.

     > Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó inserindo o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a string "GW" como parte do nome serão exibidos.
4. Selecione **Salvar**.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais