Configurar definições de segurança

StorageGRID software

NetApp
December 03, 2025

Índice

Configurar definições de segurança

Gerenciar a política TLS e SSH

A política TLS e SSH determina quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços internos do StorageGRID .

A política de segurança controla como TLS e SSH criptografam dados em movimento. Em geral, use a política de compatibilidade Moderna (padrão), a menos que seu sistema precise ser compatível com os Critérios Comuns ou você precise usar outras cifras.

Alguns serviços do StorageGRID não foram atualizados para usar as cifras nessas políticas.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Selecione uma política de segurança

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.

   A aba **Políticas TLS e SSH** mostra as políticas disponíveis. A política atualmente ativa é indicada por uma marca de seleção verde no bloco de políticas.

2. Revise os blocos para saber mais sobre as políticas disponíveis.

Política	Descrição
Compatibilidade moderna (padrão)	Use a política padrão se precisar de criptografia forte e a menos que tenha requisitos especiais. Esta política é compatível com a maioria dos clientes TLS e SSH.
Compatibilidade com legados	Use esta política se precisar de opções adicionais de compatibilidade para clientes mais antigos. As opções adicionais nesta política podem torná-la menos segura do que a política de compatibilidade moderna.
Critérios comuns	Use esta política se precisar da certificação Common Criteria.

Política	Descrição
FIPS estrito	Use esta política se você precisar de certificação Common Criteria e usar o NetApp Cryptographic Security Module 3.0.8 para conexões de clientes externos com endpoints do balanceador de carga, Tenant Manager e Grid Manager. Usar esta política pode reduzir o desempenho. **Observação**: Depois de selecionar esta política, todos os nós devem ser"reiniciado de forma contínua" para ativar o Módulo de Segurança Criptográfica NetApp . Use **Manutenção** > **Reinicialização contínua** para iniciar e monitorar reinicializações.
Personalizado	Crie uma política personalizada se precisar aplicar suas próprias cifras.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Exibir detalhes**.
4. Para alterar a política atual, selecione **Usar política**.

   Uma marca de seleção verde aparece ao lado de **Política atual** no bloco de políticas.

Crie uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar suas próprias cifras.

Passos

1. No bloco da política mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e depois selecione **Cancelar**.

3. No bloco **Política personalizada**, selecione **Configurar e usar**.
4. Cole o JSON que você copiou e faça as alterações necessárias.
5. Selecione **Usar política**.

Uma marca de seleção verde aparece ao lado de **Política atual** no bloco Política personalizada.

6. Opcionalmente, selecione **Editar configuração** para fazer mais alterações na nova política personalizada.

Reverter temporariamente para a política de segurança padrão

Se você configurou uma política de segurança personalizada, talvez não consiga fazer login no Grid Manager se a política TLS configurada for incompatível com a"certificado de servidor configurado" .

Você pode reverter temporariamente para a política de segurança padrão.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .

2. Execute o seguinte comando:

   ```
   restore-default-cipher-configurations
   ```

3. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.
4. Siga os passos emSelecione uma política de segurança para configurar a política novamente.

Configurar a segurança da rede e do objeto

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, impedir determinadas solicitações do S3 ou permitir que conexões de clientes com nós de armazenamento usem HTTP em vez de HTTPS.

Criptografia de objetos armazenados

A criptografia de objetos armazenados permite a criptografia de todos os dados de objetos à medida que são ingeridos pelo S3. Por padrão, os objetos armazenados não são criptografados, mas você pode optar por criptografar objetos usando o algoritmo de criptografia AES-128 ou AES-256. Quando você ativa a configuração, todos os objetos recém-ingeridos são criptografados, mas nenhuma alteração é feita nos objetos armazenados existentes. Se você desabilitar a criptografia, os objetos criptografados atualmente permanecerão criptografados, mas os objetos recém-ingeridos não serão criptografados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos do S3 que não foram criptografados pela criptografia em nível de bucket ou de objeto.

Para obter mais detalhes sobre os métodos de criptografia StorageGRID , consulte"Revise os métodos de criptografia do StorageGRID" .

Impedir modificação do cliente

Impedir modificação do cliente é uma configuração de todo o sistema. Quando a opção **Impedir modificação do cliente** é selecionada, as seguintes solicitações são negadas.

API REST S3

- Solicitações DeleteBucket
- Quaisquer solicitações para modificar dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

Habilitar HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos cliente usam o protocolo de rede HTTPS para qualquer conexão direta com os nós de armazenamento. Opcionalmente, você pode habilitar HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nós de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente com os nós de armazenamento. Você não precisa usar esta opção para clientes que usam apenas conexões HTTPS ou para clientes que se conectam ao serviço Load Balancer (porque você pode"configurar cada ponto de extremidade do balanceador de carga" para usar HTTP ou HTTPS).

Ver"Resumo: Endereços IP e portas para conexões de clientes" para saber quais portas os clientes S3 usam ao se conectar aos nós de armazenamento usando HTTP ou HTTPS.

Selecionar opções

Antes de começar

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

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.
2. Selecione a aba **Rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **Nenhum** (padrão) se não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **Impedir modificação do cliente** se quiser impedir que clientes S3 façam solicitações específicas.

   Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

5. Opcionalmente, selecione **Habilitar HTTP para conexões de nós de armazenamento** se os clientes se conectarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

   Tenha cuidado ao habilitar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

6. Selecione **Salvar**.

Alterar as configurações de segurança da interface

As configurações de segurança da interface permitem que você controle se os usuários serão desconectados caso fiquem inativos por mais tempo do que o especificado e se um rastreamento de pilha será incluído nas respostas de erro da API.

Antes de começar

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

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações de **Tempo limite de inatividade do navegador** e **Rastreamento de pilha da API de gerenciamento**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode ficar inativo antes que ele seja desconectado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelo seguinte:

- Um temporizador StorageGRID separado e não configurável, incluído para segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o usuário efetuar login. Quando a autenticação de um usuário expira, esse usuário é desconectado automaticamente, mesmo que o tempo limite de inatividade do navegador esteja desativado ou o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve efetuar login novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja habilitado para StorageGRID.

  Se o SSO estiver habilitado e o navegador do usuário expirar, o usuário deverá inserir novamente suas credenciais de SSO para acessar o StorageGRID novamente. Ver "Configurar logon único" .

Rastreamento de pilha da API de gerenciamento

Controla se um rastreamento de pilha é retornado nas respostas de erro da API do Grid Manager e do Tenant Manager.

Esta opção está desabilitada por padrão, mas talvez você queira habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve deixar o rastreamento de pilha desabilitado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

Passos

1. Selecione **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança**.
2. Selecione a aba **Interface**.
3. Para alterar a configuração de tempo limite de inatividade do navegador:
   a. Expanda o acordeão.
   b. Para alterar o período de tempo limite, especifique um valor entre 60 segundos e 7 dias. O tempo limite padrão é 15 minutos.

c. Para desativar esse recurso, desmarque a caixa de seleção.

d. Selecione **Salvar**.

   A nova configuração não afeta os usuários que estão conectados no momento. Os usuários devem fazer login novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.

4. Para alterar a configuração do rastreamento de pilha da API de gerenciamento:

   a. Expanda o acordeão.

   b. Marque a caixa de seleção para retornar um rastreamento de pilha nas respostas de erro da API do Grid Manager e do Tenant Manager.

      Deixe o rastreamento de pilha desabilitado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

   c. Selecione **Salvar**.

Informações sobre direitos autorais

Informações sobre marcas comerciais