Configure as definições de segurança

StorageGRID

NetApp
March 12, 2025

Índice

Configure as definições de segurança

Gerencie 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 StorageGRID internos.

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 critérios comuns ou que você precise usar outras cifras.

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Selecione uma política de segurança

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.

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

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

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

Política	Descrição
FIPS rigoroso	Use esta política se você precisar de certificação Common Criteria e precisar usar o módulo de segurança criptográfica NetApp 3.0.8 para conexões de clientes externos para terminais de balanceador de carga, Gerenciador de locatário e Gerenciador de Grade. O uso desta política pode reduzir o desempenho. **Nota**: Depois de selecionar esta política, todos os nós devem "reinicializado de uma forma rolling"ativar o módulo de segurança criptográfica do NetApp. Utilize **Maintenance** > **Rolling Reboot** para iniciar e monitorizar reinicializações.
Personalizado	Crie uma política personalizada se você precisar aplicar seus próprios cifras.

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

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

Crie uma política de segurança personalizada

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

Passos

1. No bloco da política que é o mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e, em seguida, 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 **Use policy**.

Uma marca de seleção verde aparece ao lado de **Current policy** no mosaico Custom policy (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 tiver configurado uma política de segurança personalizada, talvez não consiga entrar no Gerenciador de Grade se a diretiva TLS configurada for incompatível com o "certificado de servidor configurado".

Você pode reverter temporariamente para a política de segurança padrão.

Passos

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@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 `#`.

2. Execute o seguinte comando:

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

3. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.
4. Siga as etapas em Selecione uma política de segurança para configurar a política novamente.

Configurar a segurança de rede e de objetos

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

Criptografia de objeto armazenado

A criptografia de objeto armazenado permite a criptografia de todos os dados de objeto à medida que são ingeridos através do 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 aos objetos armazenados existentes. Se desativar a encriptação, os objetos atualmente encriptados permanecem encriptados, mas os objetos recentemente ingeridos não são encriptados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos S3 que não tenham sido criptografados por criptografia no nível do bucket ou no nível do objeto.

Para obter mais detalhes sobre os métodos de criptografia StorageGRID, "Reveja os métodos de encriptação StorageGRID"consulte .

Impedir a modificação do cliente

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

S3 API REST

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

Swift REST API

- Eliminar pedidos de contentor
- Solicitações para modificar qualquer objeto existente. Por exemplo, as seguintes operações são negadas: Put Overwrite, Delete, Metadata Update e assim por diante.

Ative HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para quaisquer conexões diretas aos nós de storage. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nó de armazenamento somente se os clientes S3 e Swift precisarem fazer conexões HTTP diretamente aos nós de armazenamento. Não é necessário usar essa opção para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode "configure cada ponto de extremidade do balanceador de carga"usar HTTP ou HTTPS).

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas S3 e clientes Swift usam ao se conetar a nós de armazenamento usando HTTP ou HTTPS.

Selecione as opções

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem permissão de acesso root.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **nenhum** (padrão) se você não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **Prevent client modification** se você quiser impedir que clientes S3 e Swift façam solicitações específicas.

   Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

5. Opcionalmente, selecione **Ativar HTTP para conexões de nó de armazenamento** se os clientes se

conetarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.

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

6. Selecione **Guardar**.

Alterar as definições de segurança da interface

As configurações de segurança da interface permitem que você controle se os usuários estão desconetados se estiverem inativos por mais do que o tempo especificado e se um rastreamento de pilha está incluído nas respostas de erro da API.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "Permissão de acesso à raiz"tem .

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações **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 estar inativo antes de o usuário ser desconetado. O padrão é 15 minutos.

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

- Um temporizador StorageGRID separado, não configurável, incluído para a segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o login do usuário. Quando a autenticação de um usuário expira, esse usuário é desconetado 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 entrar novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja ativado para o StorageGRID.

  Se o SSO estiver ativado e o navegador de um usuário expirar, o usuário deverá inserir novamente suas credenciais SSO para acessar o StorageGRID novamente. "Configurar o logon único"Consulte .

Rastreamento de pilha de API de gerenciamento

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

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

Passos

1. Selecione **CONFIGURATION** > **Security** > **Security settings**.
2. Selecione a guia **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 de 15 minutos.
   c. Para desativar este recurso, desmarque a caixa de seleção.
   d. Selecione **Guardar**.

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

4. Para alterar a configuração de 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 do Grid Manager e do Tenant Manager API.

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

   c. Selecione **Guardar**.

Informações sobre direitos autorais

Informações sobre marcas comerciais