Gerenciar a segurança

StorageGRID

NetApp
March 12, 2025

Índice

Gerenciar a segurança

Gerenciar a segurança: Visão geral

Você pode configurar várias configurações de segurança do Gerenciador de Grade para ajudar a proteger seu sistema StorageGRID.

Gerenciar a criptografia

O StorageGRID oferece várias opções para criptografar dados. Você deve "reveja os métodos de encriptação disponíveis"determinar quais atendem aos requisitos de proteção de dados.

Gerenciar certificados

Você pode "configure e gerencie os certificados do servidor" usar para conexões HTTP ou os certificados de cliente usados para autenticar uma identidade de cliente ou usuário no servidor.

Configurar servidores de gerenciamento de chaves

O uso de um "servidor de gerenciamento de chaves" permite proteger os dados do StorageGRID mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

> Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **criptografia de nó** para cada dispositivo durante a instalação, antes que o dispositivo seja adicionado à grade.

Gerenciar configurações de proxy

Se você estiver usando serviços de plataforma S3 ou pools de storage em nuvem, poderá configurar um "servidor proxy de storage" entre nós de storage e os pontos de extremidade externos do S3. Se você enviar pacotes do AutoSupport usando HTTPS ou HTTP, poderá configurar um "servidor proxy admin" entre nós de administração e suporte técnico.

Controle firewalls

Para melhorar a segurança do sistema, você pode controlar o acesso aos nós de administração do StorageGRID abrindo ou fechando portas específicas no "firewall externo". Você também pode controlar o acesso à rede a cada nó configurando o respetivo "firewall interno". Você pode impedir o acesso em todas as portas, exceto as necessárias para sua implantação.

Reveja os métodos de encriptação StorageGRID

O StorageGRID oferece várias opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais métodos atendem aos requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

Opção de criptografia	Como funciona	Aplica-se a
Servidor de gerenciamento de chaves (KMS) no Grid Manager	"configurar um servidor de gerenciamento de chaves"Você para o site StorageGRID e "habilite a criptografia de nó para o dispositivo". Em seguida, um nó de dispositivo se coneta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivo que têm **Node Encryption** ativado durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. **Nota**: O gerenciamento de chaves de criptografia com um KMS só é suportado para nós de armazenamento e dispositivos de serviços.
Página de criptografia de unidade no instalador de dispositivos StorageGRID	Se o dispositivo contiver unidades que suportem criptografia de hardware, você poderá definir uma senha de unidade durante a instalação. Quando você define uma senha de unidade, é impossível para qualquer pessoa recuperar dados válidos de unidades que foram removidas do sistema, a menos que eles saibam a senha. Antes de iniciar a instalação, aceda a **Configurar hardware** > **encriptação da unidade** para definir uma frase-passe de unidade que se aplica a todas as unidades de encriptação automática geridas pela StorageGRID num nó.	Dispositivos que contêm unidades com autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas pelo SANtricity. Se você tiver um dispositivo de storage com unidades com autocriptografia e controladoras SANtricity, poderá habilitar a segurança da unidade no SANtricity.
Conduza a segurança no Gerenciador de sistemas do SANtricity	Se o recurso Segurança da unidade estiver ativado para o seu dispositivo StorageGRID, você poderá usar "Gerente do sistema da SANtricity" o para criar e gerenciar a chave de segurança. A chave é necessária para aceder aos dados nas unidades seguras.	Dispositivos de storage com unidades Full Disk Encryption (FDE) ou unidades com autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com quaisquer dispositivos de serviços.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de objeto armazenado	Você ativa a "Criptografia de objeto armazenado" opção no Gerenciador de Grade. Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objeto S3 e Swift recém-ingeridos. Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.
Criptografia de bucket do S3	Você emite uma solicitação PutBucketEncryption para ativar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados. "Operações em baldes"
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o `x-amz-server-side-encryption` cabeçalho da solicitação.	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. StorageGRID gerencia as chaves. "Use a criptografia do lado do servidor"
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Somente dados de objeto S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use a criptografia do lado do servidor"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de volume externo ou datastore	Você usa um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação o suportar.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado. Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.
Criptografia de objetos fora do StorageGRID	Você usa um método de criptografia fora do StorageGRID para criptografar dados e metadados de objetos antes que eles sejam ingeridos no StorageGRID.	Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados). Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente"

Use vários métodos de criptografia

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistemas do SANtricity para "criptografar duas vezes" os dados nas unidades com autocriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de criptografia de objeto armazenado para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

Gerenciar certificados

Gerenciar certificados de segurança: Visão geral

Certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre componentes do StorageGRID e entre componentes do

StorageGRID e sistemas externos.

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para os dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam uma identidade de cliente ou usuário no servidor, fornecendo autenticação mais segura do que senhas sozinhas. Os certificados de cliente não encriptam dados.

Quando um cliente se coneta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

O StorageGRID funciona como o servidor para algumas conexões (como o endpoint do balanceador de carga) ou como o cliente para outras conexões (como o serviço de replicação do CloudMirror).

- Certificado padrão de CA de grade*

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado interno da CA de grade durante a instalação do sistema. O certificado de CA de grade é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora seja possível usar o certificado da CA de Grade para um ambiente que não seja de produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não protegidas sem certificado também são suportadas, mas não são recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser os especificados para verificar conexões de servidor.
- Todos os certificados personalizados devem atender ao "diretrizes de fortalecimento do sistema para certificados de servidor".
- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados da CA).

> ⓘ O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa em vez do certificado CA do sistema operacional.

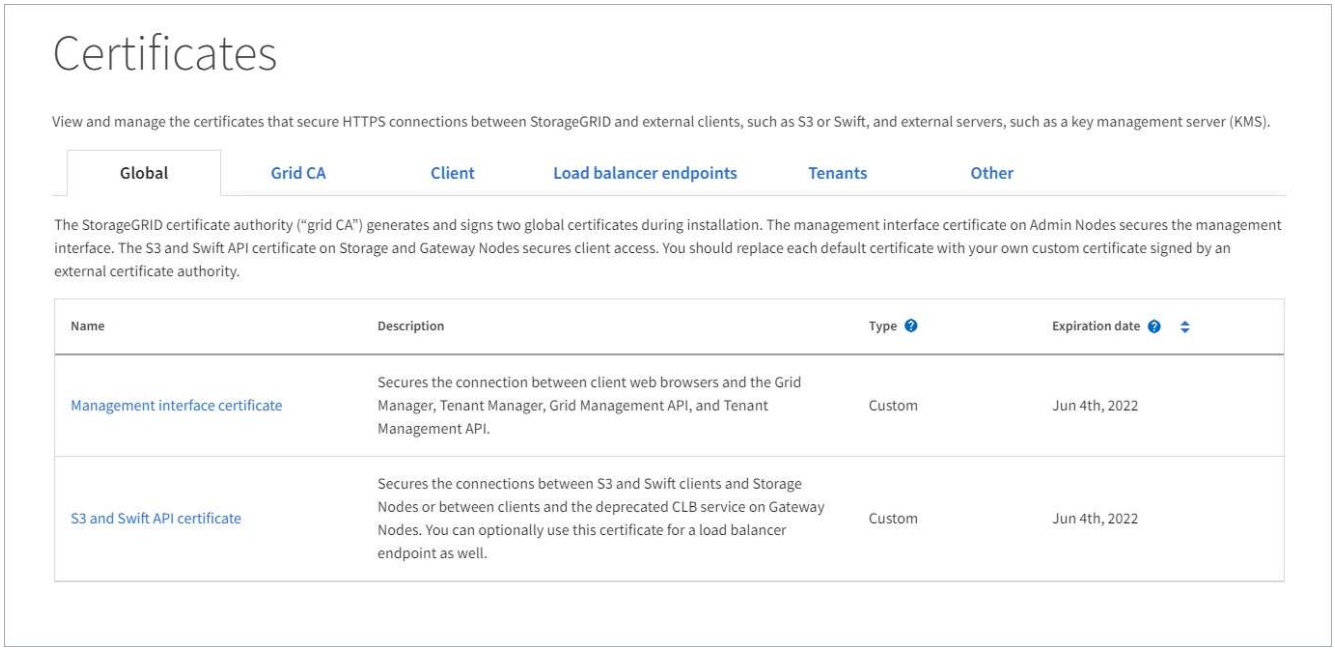
Variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Acesse certificados de segurança

Você pode acessar informações sobre todos os certificados do StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates**.



2. Selecione uma guia na página certificados para obter informações sobre cada categoria de certificado e para acessar as configurações de certificado. Pode aceder a um separador se tiver o "permissão apropriada".

   - * Global*: Protege o acesso à StorageGRID de navegadores da web e clientes de API externos.
   - * Grade CA*: Protege o tráfego interno do StorageGRID.
   - **Cliente**: Protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
   - * Terminais de balanceador de carga*: Protege conexões entre clientes S3 e Swift e o balanceador de carga StorageGRID.
   - * Inquilinos*: Protege conexões com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de armazenamento S3.
   - **Outros**: Protege conexões StorageGRID que exigem certificados específicos.

   Cada guia é descrito abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso à StorageGRID a partir de navegadores da Web e clientes externos da API S3 e Swift. Dois certificados globais são inicialmente gerados pela autoridade de certificação StorageGRID durante a instalação. A prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- Certificado de interface de gerenciamento: Protege as conexões do navegador da Web do cliente às interfaces de gerenciamento do StorageGRID.
- Certificado API S3 e Swift: Protege as conexões da API do cliente aos nós de storage, nós de administração e nós de gateway, que os aplicativos clientes S3 e Swift usam para carregar e baixar dados de objetos.

As informações sobre os certificados globais instalados incluem:

- **Nome**: Nome do certificado com link para gerenciar o certificado.
- **Descrição**
- **Tipo**: Personalizado ou padrão. Você deve sempre usar um certificado personalizado para melhorar a segurança da grade.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
  - "Substitua o certificado padrão da interface de gerenciamento gerado pelo StorageGRID" Usado para conexões do Grid Manager e do Tenant Manager.
  - "Substitua o certificado API S3 e Swift" Usado para conexões do nó de armazenamento e do ponto de extremidade do balanceador de carga (opcional).
- "Restaure o certificado padrão da interface de gerenciamento."
- "Restaure o certificado padrão da API S3 e Swift."
- "Use um script para gerar um novo certificado de interface de gerenciamento autoassinado."
- Copie ou transfira a "certificado de interface de gerenciamento" ou "Certificado API S3 e Swift".

CA da grelha

O Certificado CA de grade, gerado pela autoridade de certificação StorageGRID durante a instalação do StorageGRID, protege todo o tráfego interno do StorageGRID.

As informações do certificado incluem a data de validade do certificado e o conteúdo do certificado.

Você pode "Copie ou baixe o certificado da CA de Grade", mas não pode alterá-lo.

Cliente

Certificados de cliente, Gerado por uma autoridade de certificação externa, proteja as conexões entre ferramentas de monitoramento externas e o banco de dados do StorageGRID Prometheus.

A tabela de certificados tem uma linha para cada certificado de cliente configurado e indica se o certificado pode ser usado para acesso ao banco de dados Prometheus, juntamente com a data de validade do certificado.

Você pode:

- "Carregue ou gere um novo certificado de cliente."
- Selecione um nome de certificado para exibir os detalhes do certificado onde você pode:
  - "Altere o nome do certificado do cliente."
  - "Defina a permissão de acesso Prometheus."
  - "Carregue e substitua o certificado do cliente."
  - "Copie ou baixe o certificado do cliente."
  - "Remova o certificado do cliente."
- Selecione **ações** para rapidamente "editar", "fixe", ou "retire" um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los ao mesmo tempo usando **ações** > **Remover**.

Pontos de extremidade do balanceador de carga

Certificados de terminais do balanceador de carga Proteja as conexões entre clientes S3 e Swift e o serviço de balanceamento de carga StorageGRID em nós de gateway e nós de administração.

A tabela de endpoint do balanceador de carga tem uma linha para cada endpoint do balanceador de carga configurado e indica se o certificado global S3 e Swift API ou um certificado de endpoint do balanceador de carga personalizado está sendo usado para o endpoint. A data de validade de cada certificado também é exibida.

> As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- "Exibir um ponto final do balanceador de carga", incluindo os respetivos detalhes do certificado.
- "Especifique um certificado de endpoint do balanceador de carga para o FabricPool."
- "Use o certificado global S3 e Swift API" em vez de gerar um novo certificado de endpoint do balanceador de carga.

Inquilinos

Os locatários podem usar certificados de servidor de federação de identidade ou certificados de endpoint de serviço de plataformaproteger suas conexões com o StorageGRID.

A tabela de locatário tem uma linha para cada locatário e indica se cada locatário tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- "Selecione um nome de locatário para iniciar sessão no Gestor de inquilinos"
- "Selecione um nome de locatário para exibir os detalhes da federação de identidade do locatário"
- "Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma do locatário"
- "Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint"

Outros

O StorageGRID usa outros certificados de segurança para fins específicos. Estes certificados são listados pelo seu nome funcional. Outros certificados de segurança incluem:

- Certificados do Cloud Storage Pool
- Certificados de notificação de alerta por e-mail
- Certificados de servidor syslog externos
- Certificados de conexão de federação de grade
- Certificados de federação de identidade
- Certificados de servidor de gerenciamento de chaves (KMS)
- Certificados de logon único

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração do certificado do servidor e do cliente, conforme aplicável. A seleção de um nome de função abre uma guia do navegador onde você pode exibir e editar os detalhes do certificado.

> Só pode ver e aceder a informações de outros certificados se tiver o "permissão apropriada".

Você pode:

- "Especifique um certificado do Cloud Storage Pool para S3, C2S S3 ou Azure"
- "Especifique um certificado para notificações por e-mail de alerta"
- "Use um certificado para um servidor syslog externo"
- "Girar certificados de conexão de federação de grade"
- "Exibir e editar um certificado de federação de identidade"
- "Carregar certificados de servidor de gerenciamento de chaves (KMS) e cliente"
- "Especifique manualmente um certificado SSO para uma confiança de parte dependente"

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre navegadores da Web cliente e a interface de gerenciamento do StorageGRID, permitindo que os usuários acessem o Gerenciador de Grade e o Gerenciador de locatário sem avisos de segurança. Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário. Pode utilizar o certificado predefinido criado durante a instalação ou carregar um certificado personalizado.	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **Management interface certificate**	"Configurar certificados de interface de gerenciamento"

Certificado API S3 e Swift

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 ou Swift a um nó de storage e a terminais de balanceador de carga (opcional).	**CONFIGURATION** > **Security** > **Certificates**, selecione a guia **Global** e, em seguida, selecione **S3 e Swift API certificate**	"Configure os certificados API S3 e Swift"

Certificado CA de grade

Consulte Descrição do certificado da CA de Grade padrão.

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de cliente externo. • Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**CONFIGURATION** > **Security** > **Certificates** e selecione a guia **Client**	"Configurar certificados de cliente"

Certificado de ponto final do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode fazer upload ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos clientes usam o certificado do balanceador de carga ao se conetar ao StorageGRID para salvar e recuperar dados de objeto. Você também pode usar uma versão personalizada do certificado global Certificado API S3 e Swiftpara autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga. **Nota:** o certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID.	**CONFIGURATION** > **Network** > **Load balancer endpoints**	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade do balanceador de carga para o FabricPool"

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de storage de nuvem do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **conjuntos de armazenamento**	"Crie um pool de storage em nuvem"

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**ALERTAS** > **Configuração do e-mail**	"Configurar notificações por e-mail para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que Registra eventos no StorageGRID. **Nota:** não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP a um servidor syslog externo.	**CONFIGURATION** > **Monitoring** > **servidor de auditoria e syslog**	"Use um servidor syslog externo"

certificado de conexão de federação de grade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentique e criptografe as informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grade.	**CONFIGURATION** > **System** > **Grid Federation**	• "Crie conexões de federação de grade" • "Rode os certificados de ligação"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como ative Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, que permite que grupos de administração e usuários sejam gerenciados por um sistema externo.	**CONFIGURATION** > **Access Control** > **Identity Federation**	"Use a federação de identidade"

Certificado de servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	**CONFIGURATION** > **Security** > **Key Management Server**	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID a um recurso de storage S3.	**Gerenciador do Locatário** > **ARMAZENAMENTO (S3)** > **terminais de serviços da plataforma**	"Criar endpoint de serviços de plataforma" "Editar endpoint de serviços de plataforma"

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como AD FS (Serviços de Federação do ative Directory) e StorageGRID usados para solicitações de logon único (SSO).	**CONFIGURATION** > **access control** > **Single sign-on**	"Configurar o logon único"

Exemplos de certificados

Exemplo 1: Serviço do Load Balancer

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 ou Swift para o endpoint do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se coneta ao endpoint do balanceador de carga usando HTTPS.

4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública e com uma assinatura baseada na chave privada.
5. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objeto para o StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externas (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software servidor de gerenciamento de chaves externo, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Gerenciador de Grade, você configura um servidor KMS e carrega os certificados de servidor e cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura com base na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

Configurar certificados de servidor

Tipos de certificado de servidor suportados

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

> O tipo de codificação da diretiva de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, as cifras RSA exigem certificados RSA e as cifras ECDSA exigem certificados ECDSA. "Gerenciar certificados de segurança"Consulte . Se configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, pode "reverter temporariamente para a política de segurança padrão".

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, "Segurança para clientes S3 e Swift"consulte .

Configurar certificados de interface de gerenciamento

Você pode substituir o certificado de interface de gerenciamento padrão por um único certificado personalizado que permite que os usuários acessem o Gerenciador de Grade e o Gerenciador do locatário sem encontrar avisos de segurança. Você também pode reverter para o certificado de interface de gerenciamento padrão ou gerar um novo.

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 interface de gerenciamento personalizado comum e uma chave privada correspondente.

Como um único certificado de interface de gerenciamento personalizado é usado para todos os nós de administração, 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 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 de grade 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** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado da interface de gerenciamento na guia Global.

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 de interface de gerenciamento personalizado expira.
- reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrãoVocê .

Adicione um certificado de interface de gerenciamento personalizado

Para adicionar um certificado de interface de gerenciamento personalizado, você pode fornecer seu próprio certificado ou gerar um usando o Gerenciador de Grade.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

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

- **Pacote CA**: Um único arquivo opcional 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.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

Gerar certificado

Gere os ficheiros de certificado do servidor.

> A prática recomendada para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a incluir no certificado.
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

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

> Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página de certificado de interface de gerenciamento exibe informações detalhadas de certificado para os certificados que estão em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da interface de gerenciamento

Você pode reverter para o uso do certificado de interface de gerenciamento padrão para conexões do Gerenciador de Grade e do Gerenciador de Tenant.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura o certificado de interface de gerenciamento padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de cliente subsequentes.

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

Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação estrita do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

Antes de começar

- Você "permissões de acesso específicas"tem .
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade de certificação externa.

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 da interface de gerenciamento, que é usado pelo Gerenciador de Grade e pelo Gerenciador de Locatário.
   - 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 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 720
```

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 **CONFIGURATION** > **Security** > **Certificates**
   c. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

Transfira ou copie o certificado da interface de gestão

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configure os certificados API S3 e Swift

Você pode substituir ou restaurar o certificado de servidor usado para conexões de cliente S3 ou Swift para nós de armazenamento ou para terminais de balanceador de carga. 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, você também pode precisar instalar o certificado de CA de Grade no cliente API S3 ou Swift que você usará 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 global Server certificate for S3 and Swift API** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de expiração do certificado API S3 e Swift na guia Global.

Você pode fazer upload ou gerar um certificado personalizado de API S3 e Swift.

Adicione um certificado personalizado de API S3 e Swift

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor**: O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado**: O arquivo de chave privada de certificado de servidor personalizado (`.key`).

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

- **Pacote CA**: Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado personalizado da API S3 e Swift que foi carregado. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**.

  O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

Gerar certificado

Gere os ficheiros de certificado do servidor.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a incluir no certificado.

Campo	Descrição
Assunto (opcional)	X,509 Assunto ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicione extensões de uso de chave	Se selecionado (padrão e recomendado), o uso de chave e extensões estendidas de uso de chave são adicionados ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. **Nota**: Deixe esta caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM para o certificado personalizado da API S3 e Swift que foi gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**.

O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

5. Selecione uma guia para exibir metadados para o certificado padrão do servidor StorageGRID, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.

> Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da Web seja atualizado.
7. Depois de adicionar um certificado personalizado de API S3 e Swift, a página de certificado de API S3 e Swift exibe informações detalhadas de certificado para o certificado personalizado de API S3 e Swift que está em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da API S3 e Swift

Você pode reverter para o uso do certificado padrão S3 e Swift API para conexões de clientes S3 e Swift para nós de storage. No entanto, você não pode usar o certificado padrão S3 e Swift API para um endpoint de balanceador de carga.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **Use default certificate** (usar certificado padrão).

   Quando você restaura a versão padrão do certificado global S3 e Swift API, os arquivos de certificado de servidor personalizado que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão S3 e Swift API será usado para novas conexões de clientes S3 e Swift subsequentes aos nós de armazenamento.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3 e Swift.

   Se você tiver permissão de acesso root e o certificado personalizado S3 e Swift API foi usado para conexões de endpoint do balanceador de carga, uma lista será exibida de endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão S3 e Swift API. Aceda a "Configurar pontos de extremidade do balanceador de carga" para editar ou remover os endpoints afetados.

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

Faça o download ou copie o certificado API S3 e Swift

Você pode salvar ou copiar o conteúdo do certificado S3 e Swift API para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA `.pem`. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

   Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

   Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

b. Cole o certificado copiado em um editor de texto.

c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Informações relacionadas

- "USE A API REST DO S3"
- "Use a API Swift REST"
- "Configurar nomes de domínio de endpoint S3"

Copie o certificado da CA de Grade

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

Antes de começar

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

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 **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificate PEM**, baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.
b. Cole o certificado copiado em um editor de texto.
c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Configurar 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.

Antes de começar

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

Sobre esta tarefa

Ao criar um endpoint de 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, "Configurar o StorageGRID para FabricPool"consulte .

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 opcional da 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.

Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus, fornecendo uma maneira segura para que ferramentas externas monitorem o StorageGRID.

Se você precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deve carregar ou gerar um certificado de cliente usando o Gerenciador de Grade e copiar as informações do certificado para a ferramenta externa.

"Gerenciar certificados de segurança"Consulte e "Configurar certificados de servidor personalizados".

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION** > **Security** > **Certificates** e observando a data de validade do certificado do cliente na guia Client.

> Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivo especialmente configurados, consulte as informações específicas sobre "Carregar um certificado de cliente KMS"o .

Antes de começar

- Você tem permissão de acesso root.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Para configurar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.
  - Se tiver configurado o certificado da interface de gerenciamento do StorageGRID, você terá a CA, o certificado do cliente e a chave privada usadas para configurar o certificado da interface de gerenciamento.
  - Para carregar o seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
  - A chave privada deve ter sido salva ou gravada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.
- Para editar um certificado de cliente:
  - Você tem o endereço IP ou o nome de domínio do nó Admin.

- Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no computador local.

Adicionar certificados de cliente

Para adicionar o certificado de cliente, use um destes procedimentos:

- Certificado de interface de gerenciamento já configurado
- Certificado de cliente emitido pela CA
- Certificado gerado pelo Grid Manager

Certificado de interface de gerenciamento já configurado

Use este procedimento para adicionar um certificado de cliente se um certificado de interface de gerenciamento já estiver configurado usando uma CA fornecida pelo cliente, um certificado de cliente e uma chave privada.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
5. Selecione **continuar**.
6. Para a etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
   a. Selecione **carregar certificado**.
   b. Selecione **Procurar** e selecione o ficheiro de certificado da interface de gestão (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      O novo certificado é exibido na guia Cliente.
7. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use um certificado de cliente emitido pela CA e uma chave privada.

Passos

1. Execute as etapas para "configurar um certificado de interface de gerenciamento".
2. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

3. Selecione **Adicionar**.
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
6. Selecione **continuar**.
7. Para a etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote CA:
   a. Selecione **carregar certificado**.
   b. Selecione **Procurar** e selecione o certificado do cliente, a chave privada e os ficheiros do pacote CA (`.pem`).
      - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
      - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

      Os novos certificados aparecem na guia Cliente.
8. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use a função gerar certificado no Gerenciador de Grade.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
5. Selecione **continuar**.
6. Para a etapa **Anexar certificados**, selecione **gerar certificado**.
7. Especifique as informações do certificado:
   - **Assunto** (opcional): X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

8. Selecione **Generate**.
9. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

     Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
   - Selecione **Download private key** para salvar a chave privada como um arquivo.

     Especifique o nome do arquivo de chave privada e o local de download.

10. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

    O novo certificado é exibido na guia Cliente.

11. No Gerenciador de Grade, selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Global**.
12. Selecione **certificado de interface de gestão**.
13. Selecione **usar certificado personalizado**.
14. Carregue os arquivos certificate.pem e private_key.pem da detalhes do certificado do cliente etapa. Não há necessidade de carregar o pacote CA.
    a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
    b. Carregar cada ficheiro de certificado (`.pem`).
    c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.

       O novo certificado é exibido na página de certificado da Interface de Gerenciamento.

15. Configurar uma ferramenta de monitoramento externo, Como Grafana.

Configure uma ferramenta de monitoramento externa

Passos

1. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.
   a. **Nome**: Insira um nome para a conexão.

      O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

   b. **URL**: Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

Por exemplo: `https://admin-node.example.com:9091`

c. Ative **TLS Client Auth** e **com CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole
   - A interface de gerenciamento certificado CA para **CA Cert**
   - O certificado de cliente para **Cert de cliente**
   - A chave privada para **chave do cliente**

e. **ServerName**: Insira o nome de domínio do nó Admin.

   Servername deve corresponder ao nome de domínio como aparece no certificado da interface de gerenciamento.

2. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

   Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

   Para obter informações sobre as métricas, consulte o "Instruções para monitorar o StorageGRID".

Editar certificados de cliente

Você pode editar um certificado de cliente administrador para alterar seu nome, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione **Editar nome e permissão**
4. Introduza um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir prometheus**.
6. Selecione **continuar** para salvar o certificado no Gerenciador de Grade.

   O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.

   As datas de expiração do certificado e as permissões de acesso Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta

será acionado.

2. Selecione o certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.

b. Carregue o nome do certificado do cliente (`.pem`).

   Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   - Selecione **Transferir certificado** para guardar o ficheiro de certificado.

     Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

   O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

   - **Assunto** (opcional): X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
   - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que é gerado.
   - * Adicionar extensões de uso de chave*: Se selecionado (padrão e recomendado), o uso de chave e extensões de uso de chave estendidas são adicionados ao certificado gerado.

     Essas extensões definem a finalidade da chave contida no certificado.

     Deixe essa caixa de seleção selecionada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

   Não será possível visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou transfira a chave para um local seguro.

   - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

  Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

  Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

  Especifique o nome do arquivo de chave privada e o local de download.

e. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

Baixe ou copie certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende copiar ou transferir.
3. Baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado `.pem`.

a. Selecione **Baixar certificado**.
b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie o texto do certificado para colar em outro lugar.

a. Selecione **Copiar certificado PEM**.
b. Cole o certificado copiado em um editor de texto.
c. Salve o arquivo de texto com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

Remover certificados de cliente

Se você não precisar mais de um certificado de cliente administrador, poderá removê-lo.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende remover.
3. Selecione **Delete** e confirme.

> Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **ações** > **Excluir**.

Depois que um certificado é removido, os clientes que usaram o certificado devem especificar um novo certificado de cliente para acessar o banco de dados do StorageGRID Prometheus.

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.
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**.

Configurar servidores de gerenciamento de chaves

Configurar servidores de gerenciamento de chaves: Visão geral

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para proteger os dados em nós de dispositivo especialmente configurados.

O StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista de produtos e versões compatíveis, use o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

O que é um servidor de gerenciamento de chaves (KMS)?

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiros que fornece chaves de criptografia para nós de dispositivos StorageGRID no site associado do StorageGRID usando o Protocolo de interoperabilidade de Gerenciamento de chaves (KMIP).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó de dispositivo StorageGRID que tenha a configuração **criptografia de nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do dispositivo. Se você pretende usar um servidor de gerenciamento de chaves externo para proteger dados do StorageGRID, você deve entender como configurar esse servidor e entender como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo dessas instruções. Se precisar de ajuda, consulte a documentação do servidor de gerenciamento de chaves ou entre em Contato com o suporte técnico.

Visão geral do KMS e da configuração do appliance

Antes de usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID nos nós do dispositivo, você deve concluir duas tarefas de configuração: Configurar um ou mais servidores KMS e habilitar a criptografia de nós para os nós do dispositivo. Quando essas duas tarefas de configuração são concluídas, o processo de gerenciamento de chaves ocorre automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger os dados do StorageGRID em nós do dispositivo.

O fluxograma mostra a configuração do KMS e a configuração do appliance ocorrendo em paralelo; no entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nó para novos nós de dispositivo, com base em seus requisitos.

Configurar o servidor de gerenciamento de chaves (KMS)

A configuração de um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

Passo	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada cluster KMS ou KMS.	"Configure o StorageGRID como um cliente no KMS"

Passo	Consulte
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configure o StorageGRID como um cliente no KMS"
Adicione o KMS ao Gerenciador de Grade, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS.	"Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui os seguintes passos de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo.

   > ⓘ Não é possível ativar a configuração **criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm criptografia de nó ativada.

2. Execute o Instalador de dispositivos StorageGRID. Durante a instalação, uma chave de criptografia de dados aleatórios (DEK) é atribuída a cada volume de dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco LUKS (Unified Key Setup) do Linux no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). O KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conetar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

```
https://docs.netapp.com/us-en/storagegrid-
appliances/installconfig/optional-enabling-node-
encryption.html["Habilite a criptografia do nó"^]Consulte para obter
detalhes.
```

Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível que são executadas automaticamente.

1. Quando você instala um dispositivo que tem criptografia de nó ativada na grade, o StorageGRID determina se existe uma configuração de KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o appliance receberá a configuração do KMS.
   - Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão a ser criptografados pelo KEK temporário até que você configure um KMS para o site e o appliance receba a configuração do KMS.
2. O dispositivo usa a configuração KMS para se conetar ao KMS e solicitar uma chave de criptografia.

3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui o KEK temporário e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

> Todos os dados existentes antes do nó de dispositivo criptografado se conetarem ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra a remoção do data center até que a chave temporária seja substituída pela chave de criptografia KMS.

4. Se o aparelho estiver ligado ou reinicializado, ele se reconeta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não pode sobreviver a uma perda de energia ou a uma reinicialização.

Considerações e requisitos para usar um servidor de gerenciamento de chaves

Antes de configurar um servidor de gerenciamento de chaves externo (KMS), você deve entender as considerações e os requisitos.

Qual versão do KMIP é suportada?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

Quais são as considerações de rede?

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique através da porta usada para comunicações KMIP (Key Management Interoperability Protocol). A porta KMIP padrão é 5696.

Você deve garantir que cada nó de dispositivo que usa criptografia de nó tenha acesso de rede ao cluster KMS ou KMS configurado para o site.

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode dar suporte ao protocolo TLS 1,2 ou TLS 1,3 quando faz conexões KMIP a um cluster KMS ou KMS, com base no suporte do KMS e no qual "Política TLS e SSH" você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1,2) ou conjunto de cifra (TLS 1,3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e conjuntos de cifras/cifras estão disponíveis, consulte `tlsOutbound` a seção da política TLS e SSH ativa da grade (**CONFIGURATION** > **Security Security Security Security settings**).

Quais aparelhos são suportados?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar chaves de criptografia para qualquer dispositivo StorageGRID em sua grade que tenha a configuração **criptografia de nó** ativada. Esta definição só pode ser ativada durante a fase de configuração de hardware da instalação do dispositivo utilizando o Instalador de dispositivos StorageGRID.

> Não é possível ativar a criptografia de nó depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para dispositivos StorageGRID e nós de dispositivo.

Não é possível usar o KMS configurado para nós baseados em software (não-appliance), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados nos mecanismos de contêiner em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no armazenamento de dados ou no nível de disco.

Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, você normalmente deve configurar um ou mais servidores de gerenciamento de chaves no Gerenciador de Grade antes de criar locatários. Essa ordem garante que os nós sejam protegidos antes que quaisquer dados de objeto sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Gerenciador de Grade antes ou depois de instalar os nós do dispositivo.

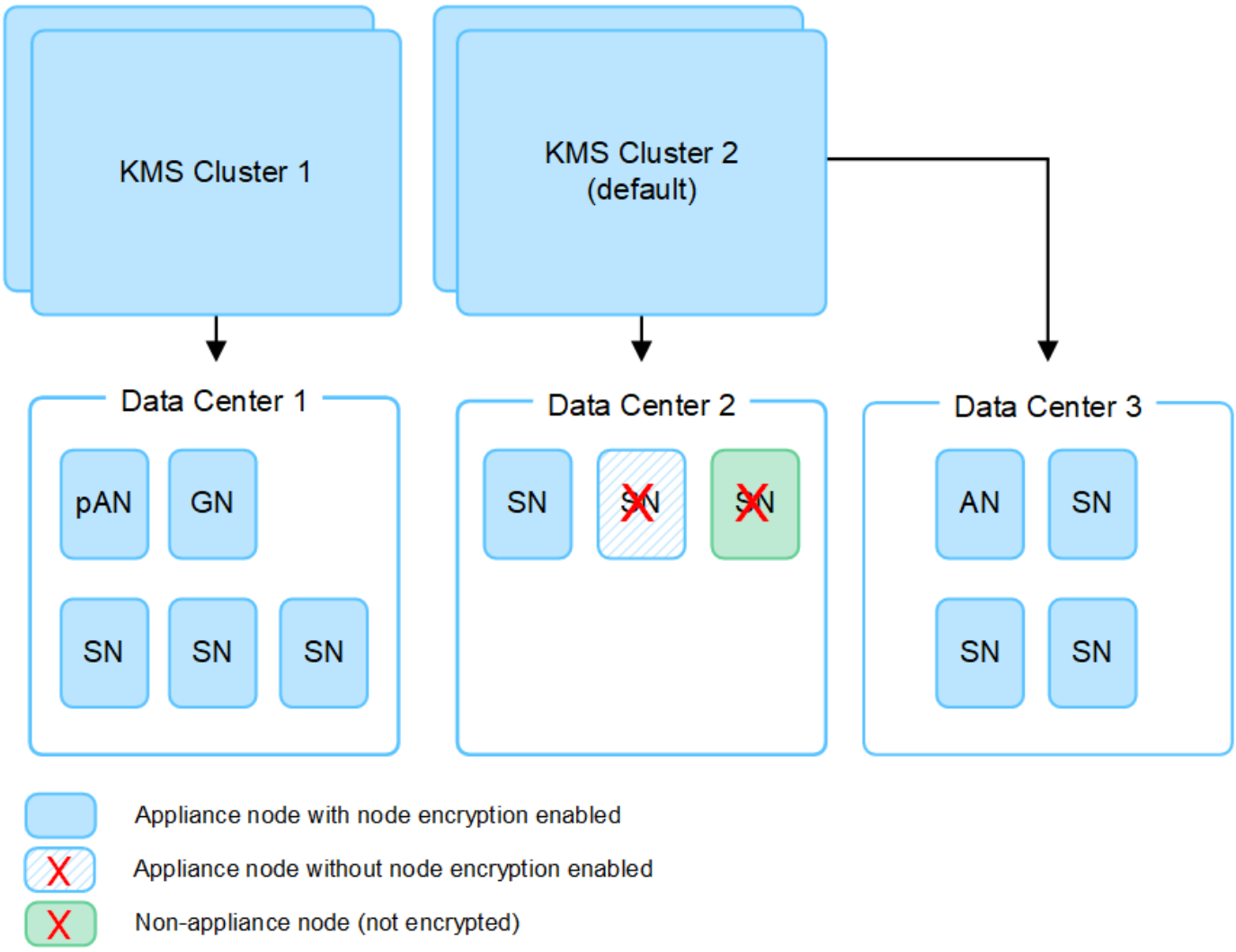
Quantos servidores de gerenciamento de chaves eu preciso?

Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

O StorageGRID é compatível com o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham configurações e chaves de criptografia. O uso de clusters KMS para gerenciamento de chaves é recomendado porque melhora os recursos de failover de uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros locais. Ao adicionar o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que não é possível usar um KMS para nós que não sejam do dispositivo ou para nenhum nó de dispositivo que não tenha a configuração **criptografia do nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como uma prática recomendada de segurança, você deve ser usado periodicamente "rode a chave de encriptação"por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós de dispositivos criptografados no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora de quando a chave é girada.
- Se o nó do dispositivo criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reinicializada.
- Se a nova versão de chave não puder ser usada para criptografar volumes de appliance por qualquer motivo, o alerta **rotação da chave de criptografia KMS falhou** é acionado para o nó do appliance. Talvez seja necessário entrar em Contato com o suporte técnico para obter ajuda na resolução desse alerta.

Posso reutilizar um nó de appliance depois que ele foi criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID, primeiro será necessário desativar o nó da grade para mover dados de objeto para outro nó. Em seguida, você pode usar o Instalador de dispositivos StorageGRID para "Limpe a configuração do KMS". A limpeza da configuração KMS desativa a configuração **criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração

KMS para o site StorageGRID.

> Sem acesso à chave de criptografia KMS, todos os dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

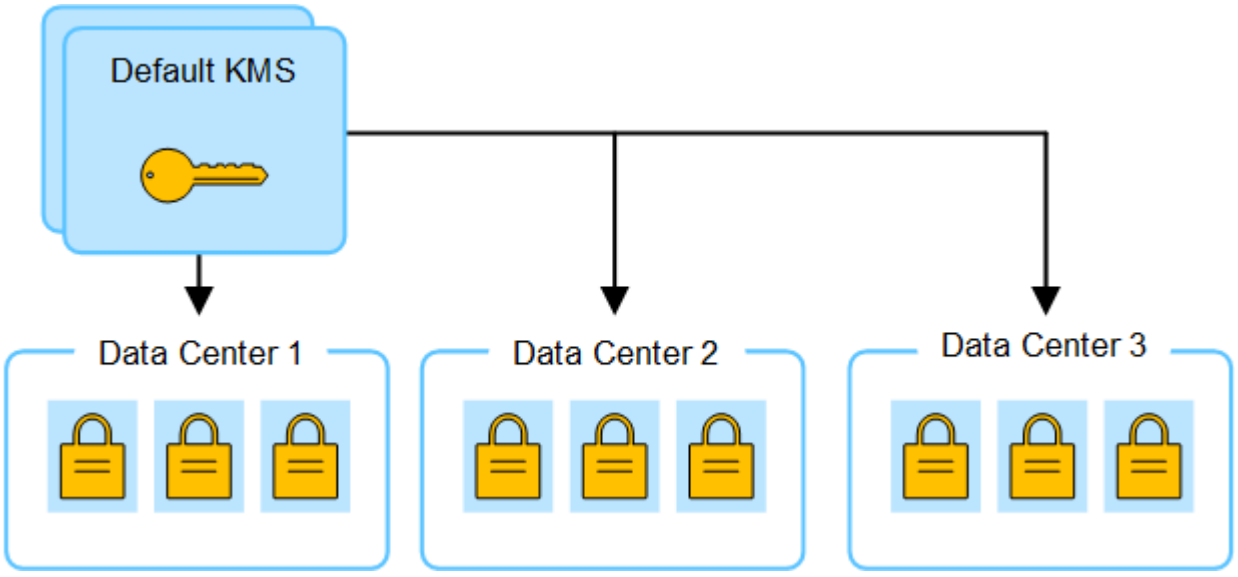
Considerações para alterar o KMS para um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único local ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

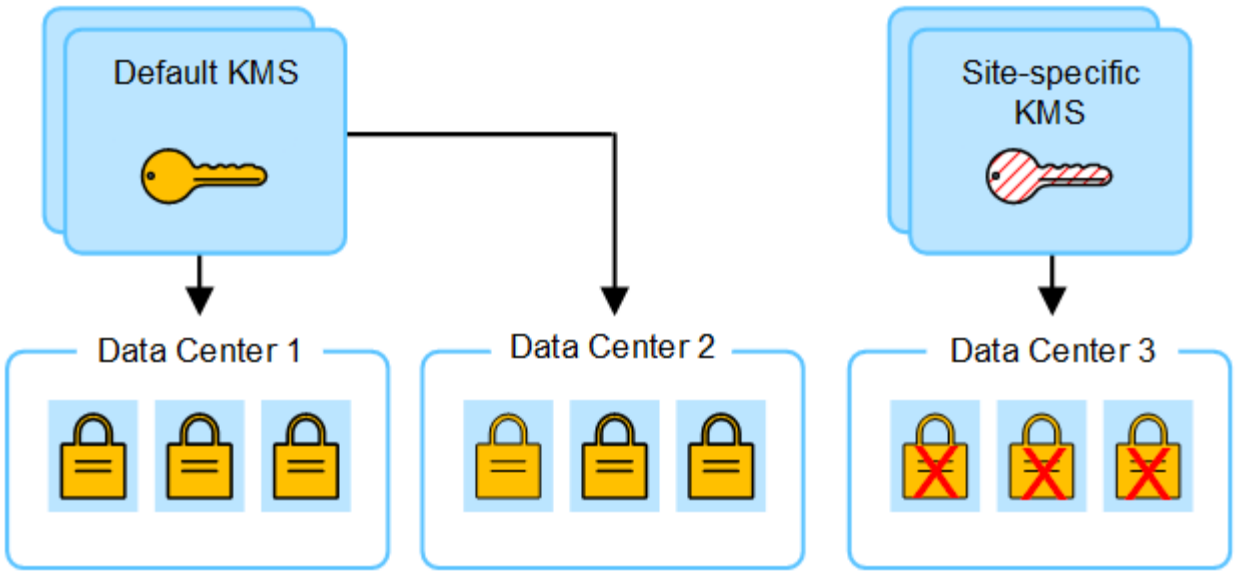
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

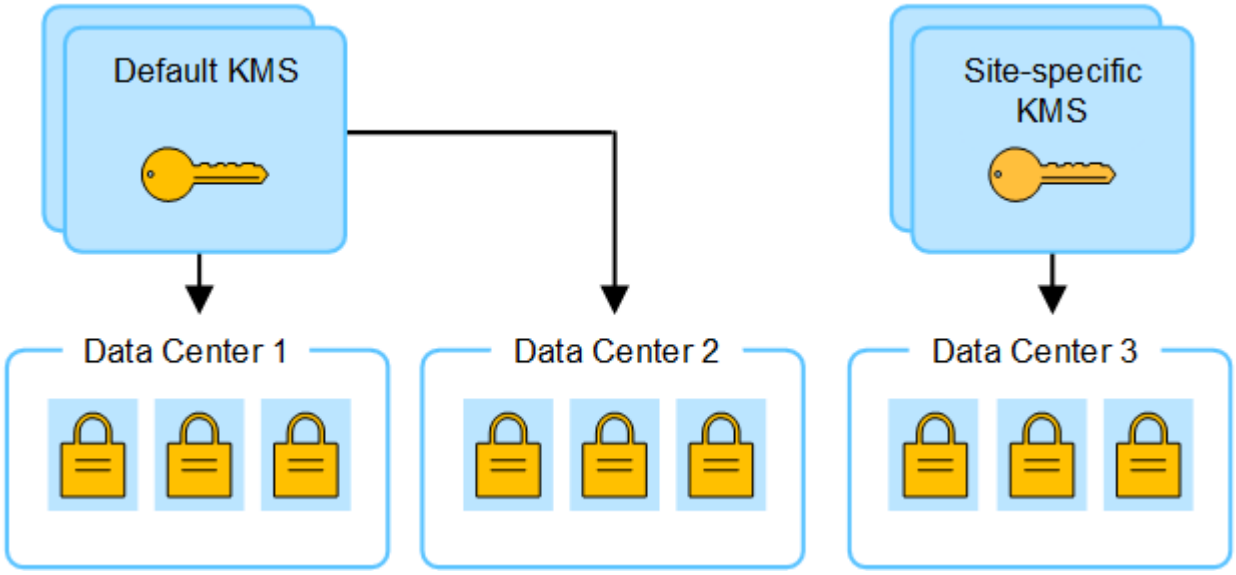
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós do dispositivo em todos os locais. Esta mesma chave também deve ser usada para descriptografar esses aparelhos.



3. Você decide adicionar um KMS específico para um site (Data Center 3 na figura). No entanto, como os nós do appliance já estão criptografados, um erro de validação ocorre quando você tenta salvar a configuração para o KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós nesse site.



4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original torna-se uma versão anterior da nova chave.) O KMS específico do local agora tem a chave correta para descriptografar os nós do appliance no Data Center 3, para que ele possa ser salvo no StorageGRID.



Casos de uso para alterar qual KMS é usado para um site

A tabela resume as etapas necessárias para os casos mais comuns para alterar o KMS de um site.

Caso de uso para alterar o KMS de um site	Passos necessários
Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como KMS padrão.	Edite o KMS específico do site. No campo **gerencia chaves para**, selecione **Sites não gerenciados por outro KMS (KMS padrão)**. O KMS específico do site agora será usado como o KMS padrão. Ele se aplicará a quaisquer sites que não tenham um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"

Caso de uso para alterar o KMS de um site	Passos necessários
Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não quer usar o KMS padrão para o novo site.	1. Se os nós de appliance no novo site já tiverem sido criptografados pelo KMS padrão, use o software KMS para copiar a versão atual da chave de criptografia do KMS padrão para um novo KMS. 2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS para um site use um servidor diferente.	1. Se os nós do dispositivo no local já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS. 2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configure o StorageGRID como um cliente no KMS

Você deve configurar o StorageGRID como um cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de poder adicionar o KMS ao StorageGRID.

Estas instruções se aplicam ao Thales CipherTrust Manager e Hashicorp Vault. Para obter uma lista de produtos e versões compatíveis, use o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Passos

1. A partir do software KMS, crie um cliente StorageGRID para cada cluster KMS ou KMS que você pretende usar.

   Cada KMS gerencia uma única chave de criptografia para os nós do StorageGRID Appliances em um único local ou em um grupo de sites.

2. Crie uma chave usando um dos seguintes dois métodos:
   - Use a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada cluster KMS ou KMS.

     A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

   - Peça ao StorageGRID que crie a chave. Você será solicitado quando testar e salvar após "carregar certificados de cliente".
3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando adicionar o KMS ao StorageGRID:

   - Nome do host ou endereço IP para cada servidor.

- Porta KMIP usada pelo KMS.
- Alias de chave para a chave de criptografia no KMS.

4. Para cada cluster KMS ou KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contém cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.

   O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

   - O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).
   - O campo Nome alternativo do assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP ao qual o StorageGRID se conetará.

     > Ao configurar o KMS no StorageGRID, você deve inserir os mesmos FQDNs ou endereços IP no campo **Nome do host**.

   - O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.

5. Obtenha o certificado de cliente público emitido para o StorageGRID pelo KMS externo e a chave privada para o certificado de cliente.

   O certificado de cliente permite que o StorageGRID se autentique no KMS.

Adicionar um servidor de gerenciamento de chaves (KMS)

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para adicionar cada cluster KMS ou KMS.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você tem "Configurado o StorageGRID como um cliente no KMS", e você tem as informações necessárias para cada cluster KMS ou KMS.
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Se possível, configure qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. "Considerações para alterar o KMS para um site"Consulte para obter detalhes.

Passo 1: KMS detalhes

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

A página servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **criar**.

   A etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. **Nota**: Se você não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.
Gere as chaves para	O site StorageGRID que será associado a este KMS. Se possível, você deve configurar qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplica a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico. • Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que se aplicará a quaisquer sites que não tenham um KMS dedicado e a quaisquer sites que você adicionar em expansões subsequentes. **Nota:** Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas você não forneceu a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.

5. Selecione **continuar**.

Passo 2: Faça upload do certificado do servidor

Na Etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado do servidor (ou pacote de certificados) para o KMS. O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

Passos

1. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.
2. Carregue o ficheiro de certificado.

   Os metadados do certificado do servidor são exibidos.

   > Se você carregou um pacote de certificados, os metadados de cada certificado serão exibidos em sua própria guia.

3. Selecione **continuar**.

Passo 3: Faça upload de certificados de cliente

Na Etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado de cliente e a chave privada do certificado de cliente. O certificado de cliente permite que o StorageGRID se autentique no KMS.

Passos

1. A partir de **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.
2. Carregue o ficheiro de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Carregue o ficheiro de chave privada.
5. Selecione **testar e salvar**.

   Se uma chave não existir, você será solicitado a que o StorageGRID crie uma.

   As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

   > Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status atual.

6. Se uma mensagem de erro for exibida quando você selecionar **Test and save**, revise os detalhes da mensagem e selecione **OK**.

   Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão

falhar.

7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **Force save**.

> Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

   A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Gerenciar um KMS

O gerenciamento de um servidor de gerenciamento de chaves (KMS) envolve a visualização ou edição de detalhes, o gerenciamento de certificados, a visualização de nós criptografados e a remoção de um KMS quando não for mais necessário.

Antes de começar

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

Ver detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo detalhes das chaves e o status atual dos certificados de servidor e cliente.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

   - A guia Detalhes da configuração lista todos os servidores de gerenciamento de chaves configurados.
   - A guia nós criptografados lista todos os nós que têm criptografia de nó ativada.

2. Para exibir os detalhes de um KMS específico e executar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gere as chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou **sites não gerenciados por outro KMS (KMS padrão).**

Campo	Descrição
Nome do anfitrião	O nome de domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS são listados juntamente com o número de servidores de gerenciamento de chaves adicionais no cluster. Por exemplo: `10.10.10.10 and 10.10.10.11` Ou `10.10.10.10 and 2 others`. Para visualizar todos os nomes de host em um cluster, selecione um KMS e selecione **Editar** ou **ações** > **Editar**.

3. Selecione uma guia na página de detalhes do KMS para exibir as seguintes informações:

Separador	Campo	Descrição
Principais detalhes	Nome da chave	O alias de chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Modificado pela última vez
A data e a hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (Privacy Enhanced mail) para o certificado.
Certificado de cliente	Metadados	Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.

4. sempre que exigido pelas práticas de segurança da sua organização, selecione **Rotate key** ou use o software KMS para criar uma nova versão da chave.

   Quando a rotação da chave é bem-sucedida, os campos UID da chave e Last modified são atualizados.

Se você girar a chave de criptografia usando o software KMS, gire-a da última versão usada da chave para uma nova versão da mesma chave. Não rode para uma chave totalmente diferente.

Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. O StorageGRID requer que todas as versões de chave usadas anteriormente (bem como quaisquer versões futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

Gerenciar certificados

Resolver imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes de expirarem.

Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.
2. Na tabela, observe o valor de expiração do certificado para cada KMS.
3. Se a expiração do certificado para qualquer KMS for desconhecida, aguarde até 30 minutos e, em seguida, atualize seu navegador da Web.
4. Se a coluna expiração do certificado indicar que um certificado expirou ou está prestes a expirar, selecione o KMS para ir para a página de detalhes do KMS.
   a. Selecione **certificado do servidor** e verifique o valor do campo "expira em".
   b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
   c. Repita essas subetapas e selecione **certificado do cliente** em vez de certificado do servidor.
5. Quando os alertas **expiração do certificado KMS CA**, **expiração do certificado do cliente KMS** e **expiração do certificado do servidor KMS** forem acionados, anote a descrição de cada alerta e execute as ações recomendadas.

Pode demorar StorageGRID até 30 minutos para obter atualizações para a expiração do certificado. Atualize seu navegador da Web para ver os valores atuais.

Exibir nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Na parte superior da página, selecione a guia **nós criptografados**.

A guia nós criptografados lista os nós do dispositivo no sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

3. Revise as informações na tabela para cada nó de dispositivo.

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Local	O nome do site do StorageGRID onde o nó está instalado.
KMS nome	O nome descritivo do KMS usado para o nó. Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS. "Adicionar um servidor de gerenciamento de chaves (KMS)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para ver um UID de chave inteiro, selecione o texto. Um traço (--) indica que a chave UID é desconhecida, possivelmente por causa de um problema de conexão entre o nó do aparelho e o KMS.
Estado	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conetado, o carimbo de data/hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações de configuração do KMS. **Observação:** Atualize seu navegador para ver os novos valores.

4. Se a coluna Status indicar um problema KMS, solucione o problema imediatamente.

   Durante as operações normais de KMS, o status será **conectado ao KMS**. Se um nó for desconetado da grade, o estado de conexão do nó é mostrado (administrativamente para baixo ou desconhecido).

   Outras mensagens de status correspondem a alertas StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração DE KMS
   - Erro de conetividade DE KMS
   - Nome da chave de encriptação KMS não encontrado
   - Falha na rotação da chave de CRIPTOGRAFIA KMS
   - A chave KMS falhou ao desencriptar um volume de aparelho
   - KMS não está configurado

   Execute as ações recomendadas para esses alertas.

Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

Edite um KMS

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

Antes de começar

- Se pretende atualizar o site selecionado para um KMS, analisou o "Considerações para alterar o KMS para um site".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja editar e selecione **ações** > **Editar**.

   Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes em **Etapa 1 (detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

Campo	Descrição
KMS nome	Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres.
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.
Gere as chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione **Sites não gerenciados por outro KMS (KMS padrão)**. Esta seleção converte um KMS específico do site para o KMS padrão, que se aplicará a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão. **Observação:** se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não será possível selecionar um site específico.

Campo	Descrição
Porta	A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP.
Nome do anfitrião	O nome de domínio ou endereço IP totalmente qualificado para o KMS. **Nota:** o campo Nome alternativo (SAN) do assunto do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **continuar**.

   A etapa 2 (carregar certificado do servidor) do assistente Editar um servidor de gerenciamento de chaves é exibida.

6. Se precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.
7. Selecione **continuar**.

   A etapa 3 (carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se precisar substituir o certificado de cliente e a chave privada do certificado de cliente, selecione **Procurar** e carregue os novos arquivos.
9. Selecione **testar e salvar**.

   As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados por nós nos locais afetados são testadas. Se todas as conexões de nó forem válidas e a chave correta for encontrada no KMS, o servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

10. Se for apresentada uma mensagem de erro, reveja os detalhes da mensagem e selecione **OK**.

    Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Force save**.

    > Selecionar **Force save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

    A configuração do KMS é salva.

12. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.

A configuração do KMS é salva, mas a conexão com o KMS não é testada.

Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se você tiver desativado o site.

Antes de começar

- Você revisou o "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de dispositivo com criptografia de nó ativada.
- Você pode remover o KMS padrão se um KMS específico do site já existir para cada site que tenha nós de dispositivo com criptografia de nó ativada.

Passos

1. Selecione **CONFIGURATION** > **Security** > **Key Management Server**.

   A página servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja remover e selecione **ações** > **Remover**.

   Você também pode remover um KMS selecionando o nome do KMS na tabela e selecionando **Remover** na página de detalhes do KMS.

3. Confirme se o seguinte é verdadeiro:
   - Você está removendo um KMS específico do site para um site que não tem nó de dispositivo com criptografia de nó ativada.
   - Você está removendo o KMS padrão, mas um KMS específico do site já existe para cada site com criptografia de nó.
4. Selecione **Sim**.

   A configuração do KMS é removida.

Gerenciar configurações de proxy

Configurar 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.

> As configurações de proxy de armazenamento configuradas não se aplicam aos endpoints de serviços da plataforma Kafka.

Antes de começar

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

Sobre esta tarefa

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

Passos

1. Selecione **CONFIGURATION** > **Security** > **Proxy settings**.
2. Na guia **armazenamento**, marque a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
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.

   Deixe este campo em branco para usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Guardar**.

   Depois que o proxy de armazenamento é 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.
8. Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configure as configurações de proxy de administrador

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

Para obter mais informações sobre o AutoSupport, "Configurar o AutoSupport"consulte .

Antes de começar

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

Sobre esta tarefa

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

Passos

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

   A página Configurações de proxy é exibida. Por padrão, o armazenamento é selecionado no menu de guias.

2. Selecione a guia **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 um nome de usuário e senha para o servidor proxy.

   Deixe esses campos em branco se o servidor proxy não exigir um nome de usuário ou uma senha.

7. Selecione uma das seguintes opções:

   - Se você quiser proteger a conexão com o proxy de administrador, selecione **Verify proxy certificate**. Carregue um pacote CA para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy admin.

     O AutoSupport On Demand, o e-Series AutoSupport através do StorageGRID e a determinação do caminho de atualização na página de atualização do StorageGRID não funcionarão se um certificado proxy for verificado.

   Depois de carregar o pacote CA, os metadados são exibidos.

   - Se você não quiser validar certificados ao se comunicar com o servidor proxy de administrador, selecione **não verificar o certificado de proxy**.

8. Selecione **Guardar**.

   Depois que o proxy de administração é salvo, o servidor proxy entre nós de administração 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 de administrador, desmarque a caixa de seleção **Ativar proxy de administrador** e selecione **Salvar**.

Controle firewalls

Controle o acesso no 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 evitar que os locatários sejam capazes de se conetar ao Gerenciador de Grade no firewall, além de usar outros métodos para controlar o acesso ao sistema.

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

Porta	Descrição	Se a porta estiver aberta…
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade, a API de gerenciamento de grade, o Gerenciador de locatário e a API de gerenciamento do locatário. **Nota:** a porta 443 também é usada para algum tráfego interno.
8443	Porta restrita do Gerenciador de Grade em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS. • Os navegadores da Web e os clientes de API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário. • As solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Gerenciador de inquilinos em nós de administração	• Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS. • Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade. • As solicitações de conteúdo interno serão rejeitadas.

O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

- "Faça login no Gerenciador de Grade"
- "Crie uma conta de locatário"
- "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 as necessárias para a implantação da 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 de que você precisa para sua grade.

- **Lista de endereços privilegiados**: Use esta guia para permitir o 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 abertas por padrão ou reabrir portas previamente fechadas.
- **Rede cliente não confiável**: Use esta guia para especificar se um nó confia no tráfego de entrada da rede cliente.

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

  - Um nó com uma rede cliente não confiável aceitará somente conexões em portas de endpoint do balanceador de carga configuradas nesse nó (pontos de extremidade globais, de interface de nó e de tipo de nó).
  - As portas de endpoint do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
  - Quando confiável, todas as portas abertas na guia Gerenciar acesso externo são acessíveis, bem 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. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporta da maneira que você espera.

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

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

Lista de endereços privilegiados e Gerenciar guias de acesso externo

A guia lista de endereços privilegiados permite que você Registre um ou mais endereços IP que recebem acesso a portas de grade fechadas. A guia Gerenciar acesso externo permite fechar o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (as portas externas são portas que são acessíveis por nós que não são de grade por padrão). Essas duas guias geralmente podem ser usadas em conjunto para personalizar o acesso exato à rede que você precisa para permitir a sua grade.

> Os endereços IP privilegiados não têm acesso interno à porta de grade por padrão.

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

Suponha que você queira usar um host de salto (um host de segurança endurecido) 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. Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão 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 Admin Node em sua grade serão bloqueadas para todos os hosts, exceto o host jump. Em seguida, você pode usar o host jump para executar tarefas de manutenção em sua grade de forma mais segura.

Exemplo 2: Limite o acesso ao Gerenciador de Grade e ao Gerenciador do Locatário

Suponha que você queira limitar o acesso ao Gerenciador de Grade e ao gerenciador de locatário (portas predefinidas) por motivos de segurança. Você pode usar estas etapas gerais:

1. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 443.
2. Use a opção na guia Gerenciar acesso externo para permitir o acesso à porta 8443.
3. Use a opção na guia Gerenciar acesso externo para permitir o acesso à porta 9443.

Depois de salvar sua configuração, os hosts não poderão acessar a porta 443, mas ainda poderão acessar o Gerenciador de Grade pela porta 8443 e o Gerenciador de Tenant pela porta 9443.

As portas 443, 8443 e 9443 são as portas predefinidas para o Grid Manager e o Tenant Manager. Você pode alternar qualquer porta para limitar o acesso a um Gerenciador de Grade específico ou gerente de locatário.

Exemplo 3: 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 ao Access Grid Manager e ao Gerenciador de inquilinos (as portas predefinidas são 443 e 8443). Todos os usuários conetados atualmente em uma porta bloqueada, incluindo você, perderão 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 os hosts na lista de endereços privilegiados. Todos os outros hosts terão acesso negado ao serviço, independentemente da interface da solicitação.

Exemplo 4: Desativar o acesso a serviços não utilizados

Em um nível de rede, você pode desativar alguns serviços que você não pretende usar. Por exemplo, se você não fornecer acesso Swift, você executaria as seguintes etapas gerais:

1. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 18083.
2. Use a alternância na guia Gerenciar acesso externo para bloquear a porta 18085.

Depois de salvar sua configuração, o nó de armazenamento não permite mais a conetividade Swift, mas continua a permitir o acesso a outros serviços em portas desbloqueadas.

Separador redes Cliente não fidedignas

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

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todos "portas externas disponíveis".

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

Exemplo 1: O Gateway Node 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 para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na "Pontos de extremidade do balanceador de carga" página, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página de controle do Firewall, selecione não confiável para especificar que a rede do cliente no nó de gateway não é confiável.

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

Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma

Suponha que você queira ativar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede do cliente. Você executaria este passo geral:

- Na guia redes de clientes não confiáveis da página de controle do Firewall, indique que a rede de cliente 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 a permitir solicitações de saída para destinos de serviços de plataforma configurados.

Exemplo 3: Limitando o acesso ao Gerenciador de Grade a uma sub-rede

Suponha que você queira permitir o acesso do Gerenciador de Grade somente em uma sub-rede específica. Você executaria os seguintes passos:

1. Anexe a rede cliente dos seus nós de administrador à sub-rede.
2. Use a guia rede de cliente não confiável para configurar a rede de cliente como não confiável.
3. Quando você cria 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 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 os hosts na sub-rede especificada podem acessar o Gerenciador de Grade. Todos os outros hosts estão bloqueados.

Configurar firewall interno

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

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você "permissões de acesso específicas"tem .
- Você revisou as informações em "Gerenciar controles de firewall" e "Diretrizes de rede".
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.

> Ao alterar a configuração da rede do cliente, as conexões de cliente existentes podem falhar se os endpoints 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 das portas nos nós da grade. Você pode usar as guias de controle do Firewall para abrir ou fechar portas abertas por padrão na rede de Grade, na rede Admin e na rede do Cliente. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas de grade fechadas. Se você estiver usando uma rede de cliente, poderá especificar se um nó confia no tráfego de entrada da rede de cliente e configurar o acesso de portas específicas na rede de cliente.

Limitar o número de portas abertas para endereços IP fora da sua grade a apenas aquelas que são absolutamente necessárias aumenta a segurança da sua grade. 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 controles de firewall, incluindo exemplos, "Gerenciar controles de firewall"consulte .

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

Aceder aos controlos da firewall

Passos

1. Selecione **CONFIGURATION** > **Security** > **Firewall control**.

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

2. Selecione qualquer separador para configurar os controlos da 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 fechadas por padrão ou fechadas por configurações na guia Gerenciar acesso externo.

Endereços IP privilegiados e sub-redes não têm acesso interno à grade por padrão. Além disso, os pontos de extremidade 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 cliente não confiável.

Passos

1. Na guia lista de endereços privilegiados, insira o endereço ou a sub-rede IP que deseja conceder acesso a 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 endereços IP privilegiados para acessar portas internas do StorageGRID**. "Portas internas do StorageGRID"Consulte .

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

4. Selecione **Guardar**.

Gerenciar o 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 grade, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas abertas por padrão e só pode abrir portas fechadas.

> As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia rede 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 do cliente não confiável substituem as portas fechadas (como 443, 8443, 9443) na rede do cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não são da grade por padrão) para os nós da grade.
2. Configure as portas que deseja abrir e fechar usando as seguintes opções:
   - Utilize a 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 Gerenciador de Grade, qualquer usuário conetado atualmente em uma porta bloqueada, incluindo você, perderá o acesso ao Gerenciador de Grade, a menos que seu endereço IP tenha sido adicionado 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. Utilize o campo de pesquisa para encontrar as definições de qualquer porta externa introduzindo um número de porta. Pode introduzir um número de porta parcial. Por exemplo, se você inserir um **2**, todas as portas que têm a string "2" como parte de seu nome serão exibidas.

3. Selecione **Guardar**

Rede cliente não confiável

Se a rede do cliente para um nó não for confiável, o nó só aceita o tráfego de entrada em portas configuradas como endpoints do balanceador de carga e, opcionalmente, portas adicionais selecionadas nesta guia. Você também pode usar essa guia para especificar a configuração padrão para novos nós adicionados em uma expansão.

As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

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

Passos

1. Selecione **rede Cliente não fidedigna**.
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.
   - **Trusted** (padrão): Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável.

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

     Esta configuração não afeta os nós existentes no seu sistema StorageGRID.
3. Use as opções a seguir para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente ou em portas selecionadas adicionais:
   - Selecione **não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista rede cliente não confiável.
   - Selecione **confiar em nós exibidos** para remover todos os nós exibidos na tabela da lista rede de clientes não confiável.
   - 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 **não confiar nos nós exibidos** para adicionar todos os nós à lista

rede de clientes não confiável e, em seguida, usar a alternância além de um nó individual para adicionar esse nó único à lista rede de clientes confiáveis.

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

4. Selecione **Guardar**.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais