Endurecimento do sistema

StorageGRID

NetApp
March 12, 2025

Índice

Endurecimento do sistema . . . 1
- Endurecimento do sistema: Visão geral . . . 1
  - Considerações gerais para o endurecimento de sistemas StorageGRID . . . 1
- Diretrizes de fortalecimento para atualizações de software . . . 1
  - Atualizações para o software StorageGRID . . . 1
  - Upgrades para serviços externos . . . 2
  - Atualizações para hypervisors . . . 2
  - * Atualizações para nós Linux* . . . 2
- Diretrizes de fortalecimento para redes StorageGRID . . . 2
  - Diretrizes para rede de Grade . . . 2
  - Diretrizes para Admin Network . . . 3
  - Diretrizes para rede de clientes . . . 3
- Diretrizes de fortalecimento para nós de StorageGRID . . . 3
  - Controle o acesso remoto IPMI ao BMC . . . 3
  - Configuração da firewall . . . 4
  - Desativar serviços não utilizados . . . 4
  - Virtualização, contêineres e hardware compartilhado . . . 4
  - Proteja os nós durante a instalação . . . 4
  - Diretrizes para nós de administração . . . 5
  - Diretrizes para nós de storage . . . 5
  - Diretrizes para nós de gateway . . . 6
  - Diretrizes para nós de dispositivos de hardware . . . 6
- Diretrizes de fortalecimento para TLS e SSH . . . 7
  - Diretrizes de endurecimento para certificados . . . 7
  - Diretrizes de fortalecimento para a política TLS e SSH . . . 8
- Outras diretrizes de endurecimento . . . 8
  - Logs e mensagens de auditoria . . . 8
  - NetApp AutoSupport . . . 8
  - Compartilhamento de recursos entre origens (CORS) . . . 8
  - Dispositivos de segurança externos . . . 9
  - Mitigação de ransomware . . . 9

Endurecimento do sistema

Endurecimento do sistema: Visão geral

O fortalecimento do sistema é o processo de eliminar o maior número possível de riscos de segurança a partir de um sistema StorageGRID.

Este documento fornece uma visão geral das diretrizes de proteção específicas do StorageGRID. Estas diretrizes são um suplemento às melhores práticas padrão do setor para o endurecimento do sistema. Por exemplo, essas diretrizes assumem que você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e ativa autenticação baseada em certificado quando disponível.

À medida que você instala e configura o StorageGRID, você pode usar essas diretrizes para ajudá-lo a cumprir quaisquer objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

StorageGRID segue o "Política de tratamento de vulnerabilidades do NetApp". Vulnerabilidades relatadas são verificadas e resolvidas de acordo com o processo de resposta a incidentes de segurança do produto.

Considerações gerais para o endurecimento de sistemas StorageGRID

Ao endurecer um sistema StorageGRID, você deve considerar o seguinte:

- Qual das três redes StorageGRID você implementou. Todos os sistemas StorageGRID devem usar a rede de grade, mas você também pode estar usando a rede de administrador, a rede de cliente ou ambos. Cada rede tem diferentes considerações de segurança.
- O tipo de plataformas que você usa para os nós individuais em seu sistema StorageGRID. Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma tem seu próprio conjunto de melhores práticas de endurecimento.
- Como as contas de inquilino são confiáveis. Se você for um provedor de serviços com contas de inquilino não confiáveis, terá preocupações de segurança diferentes do que se você usar apenas locatários internos confiáveis.
- Quais os requisitos e convenções de segurança seguidos pela sua organização. Talvez seja necessário cumprir requisitos específicos de regulamentação ou de empresas.

Diretrizes de fortalecimento para atualizações de software

Você deve manter seu sistema StorageGRID e serviços relacionados atualizados para se defender contra ataques.

Atualizações para o software StorageGRID

Sempre que possível, você deve atualizar o software StorageGRID para a versão principal mais recente ou para a versão principal anterior. Manter o StorageGRID atualizado ajuda a reduzir o tempo em que as vulnerabilidades conhecidas estão ativas e reduz a área geral da superfície de ataque. Além disso, as versões mais recentes do StorageGRID geralmente contêm recursos de proteção de segurança que não estão incluídos em versões anteriores.

Consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT) para determinar qual versão do

software StorageGRID você deve usar. Quando um hotfix é necessário, o NetApp prioriza a criação de atualizações para as versões mais recentes. Alguns patches podem não ser compatíveis com versões anteriores.

- Para baixar as versões e hotfixes mais recentes do StorageGRID, vá para "NetApp Downloads: StorageGRID".
- Para atualizar o software StorageGRID, consulte "instruções de atualização".
- Para aplicar um hotfix, consulte "Procedimento de correção do StorageGRID".

Upgrades para serviços externos

Os serviços externos podem ter vulnerabilidades que afetam o StorageGRID indiretamente. Você deve garantir que os serviços dos quais o StorageGRID depende são atualizados. Esses serviços incluem LDAP, KMS (ou servidor KMIP), DNS e NTP.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Atualizações para hypervisors

Se seus nós do StorageGRID estiverem em execução no VMware ou em outro hypervisor, você deverá garantir que o software e o firmware do hypervisor estejam atualizados.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

* Atualizações para nós Linux*

Se seus nós do StorageGRID estiverem usando plataformas host Linux, você deve garantir que as atualizações de segurança e as atualizações do kernel sejam aplicadas ao sistema operacional do host. Além disso, você deve aplicar atualizações de firmware a hardware vulnerável quando essas atualizações estiverem disponíveis.

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Diretrizes de fortalecimento para redes StorageGRID

O sistema StorageGRID suporta até três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual de acordo com seus requisitos de segurança e acesso.

Para obter informações detalhadas sobre redes StorageGRID, consulte "Tipos de rede StorageGRID".

Diretrizes para rede de Grade

Você deve configurar uma rede de grade para todo o tráfego interno do StorageGRID. Todos os nós de grade estão na rede de grade e eles devem ser capazes de falar com todos os outros nós.

Ao configurar a rede de Grade, siga estas diretrizes:

- Certifique-se de que a rede está protegida de clientes não fidedignos, como os que se encontram na

Internet aberta.

- Quando possível, use a rede de Grade exclusivamente para tráfego interno. Tanto a rede Admin quanto a rede Client têm restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da rede de Grade para tráfego de cliente externo é suportado, mas esse uso oferece menos camadas de proteção.
- Se a implantação do StorageGRID abranger vários data centers, use uma rede privada virtual (VPN) ou equivalente na rede de grade para fornecer proteção adicional para o tráfego interno.
- Alguns procedimentos de manutenção exigem acesso de shell seguro (SSH) na porta 22 entre o nó de administração principal e todos os outros nós de grade. Use um firewall externo para restringir o acesso SSH a clientes confiáveis.

Diretrizes para Admin Network

A rede de administração é normalmente usada para tarefas administrativas (funcionários confiáveis usando o Gerenciador de Grade ou SSH) e para se comunicar com outros serviços confiáveis, como LDAP, DNS, NTP ou KMS (ou servidor KMIP). No entanto, o StorageGRID não aplica esse uso internamente.

Se você estiver usando a rede Admin, siga estas diretrizes:

- Bloqueie todas as portas de tráfego internas na rede Admin. Consulte "lista de portas internas".
- Se os clientes não confiáveis puderem acessar a rede de administração, bloqueie o acesso ao StorageGRID na rede de administração com um firewall externo.

Diretrizes para rede de clientes

A rede do cliente é normalmente usada para locatários e para se comunicar com serviços externos, como o serviço de replicação do CloudMirror ou outro serviço de plataforma. No entanto, o StorageGRID não aplica esse uso internamente.

Se você estiver usando a rede de clientes, siga estas diretrizes:

- Bloqueie todas as portas de tráfego internas na rede do cliente. Consulte "lista de portas internas".
- Aceite o tráfego de clientes de entrada apenas em endpoints explicitamente configurados. Consulte as informações sobre "gerenciamento de controles de firewall"o .

Diretrizes de fortalecimento para nós de StorageGRID

Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma e cada tipo de nó tem seu próprio conjunto de práticas recomendadas de endurecimento.

Controle o acesso remoto IPMI ao BMC

Você pode ativar ou desativar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite o acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisar de acesso remoto IPMI ao BMC, desative esta opção.

- Para controlar o acesso remoto IPMI ao BMC no Gerenciador de Grade, vá para **CONFIGURATION** >

Security > **Security settings** > **Appliances**:

- Desmarque a caixa de seleção **Enable Remote IPMI Access** (Ativar acesso remoto IPMI) para desativar o acesso IPMI ao BMC.
- Marque a caixa de seleção **Enable Remote IPMI Access** (Ativar acesso remoto IPMI) para habilitar o acesso IPMI ao BMC.

Configuração da firewall

Como parte do processo de fortalecimento do sistema, você deve revisar as configurações de firewall externo e modificá-las para que o tráfego seja aceito apenas a partir dos endereços IP e nas portas a partir das quais é estritamente necessário.

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. Você deve "gerenciar controles internos de firewall"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.

Especificamente, você pode gerenciar essas áreas:

- **Endereços privilegiados**: Você pode permitir que endereços IP ou sub-redes selecionadas acessem portas fechadas por configurações na guia Gerenciar acesso externo.
- **Gerenciar acesso externo**: Você pode fechar portas abertas por padrão ou reabrir portas previamente fechadas.
- **Rede cliente não confiável**: Você pode especificar se um nó confia no tráfego de entrada da rede cliente, bem como as portas adicionais que deseja abrir quando a rede cliente não confiável está configurada.

Embora esse firewall interno forneça uma camada adicional de proteção contra algumas ameaças comuns, ele não remove a necessidade de um firewall externo.

Para obter uma lista de todas as portas internas e externas usadas pelo StorageGRID, "Referência da porta de rede"consulte .

Desativar serviços não utilizados

Para todos os nós do StorageGRID, você deve desativar ou bloquear o acesso a serviços não utilizados. Por exemplo, se você não estiver planejando configurar o acesso do cliente aos compartilhamentos de auditoria para NFS, bloqueie ou desative o acesso a esses serviços.

Virtualização, contêineres e hardware compartilhado

Para todos os nós do StorageGRID, evite executar o StorageGRID no mesmo hardware físico que o software não confiável. Não assuma que as proteções do hipervisor irão impedir que o malware acesse dados protegidos pela StorageGRID se o StorageGRID e o malware existirem no mesmo hardware físico. Por exemplo, os ataques Meltdown e Spectre exploram vulnerabilidades críticas em processadores modernos e permitem que programas roubem dados na memória no mesmo computador.

Proteja os nós durante a instalação

Não permita que usuários não confiáveis acessem nós do StorageGRID pela rede quando os nós estiverem sendo instalados. Os nós não são totalmente seguros até que eles se juntem à grade.

Diretrizes para nós de administração

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Quando você entra no Gerenciador de Grade ou no Gerenciador de Tenant, você está se conetando a um nó Admin.

Siga estas diretrizes para proteger os nós de administração no seu sistema StorageGRID:

- Proteja todos os nós de administração de clientes não confiáveis, como aqueles na Internet aberta. Certifique-se de que nenhum cliente não confiável possa acessar qualquer nó Admin na rede de Grade, na rede Admin ou na rede Cliente.
- Os grupos StorageGRID controlam o acesso aos recursos do Gerenciador de Grade e do Gerenciador de Locatário. Conceda a cada grupo de usuários as permissões mínimas necessárias para sua função e use o modo de acesso somente leitura para impedir que os usuários alterem a configuração.
- Ao usar pontos de extremidade do balanceador de carga do StorageGRID, use nós de gateway em vez de nós de administrador para obter tráfego de cliente não confiável.
- Se você tiver locatários não confiáveis, não permita que eles tenham acesso direto ao Gerenciador do Locatário ou à API de Gerenciamento do Locatário. Em vez disso, peça a qualquer inquilino não confiável que use um portal de locatário ou um sistema de gerenciamento de inquilino externo, que interage com a API de gerenciamento do locatário.
- Opcionalmente, use um proxy de administrador para obter mais controle sobre a comunicação do AutoSupport de nós de administração para o suporte do NetApp. Consulte os passos para "criando um proxy de administrador".
- Opcionalmente, use as portas 8443 e 9443 restritas para separar as comunicações do Grid Manager e do Tenant Manager. Bloqueie a porta compartilhada 443 e limite as solicitações do locatário à porta 9443 para proteção adicional.
- Opcionalmente, use nós de administração separados para administradores de grade e usuários de locatário.

Para obter mais informações, consulte as instruções para "Administrando o StorageGRID".

Diretrizes para nós de storage

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Siga estas diretrizes para proteger os nós de storage em seu sistema StorageGRID.

- Não permita que clientes não confiáveis se conetem diretamente aos nós de storage. Use um ponto de extremidade do balanceador de carga servido por um nó de gateway ou um balanceador de carga de terceiros.
- Não ative serviços de saída para locatários não confiáveis. Por exemplo, ao criar a conta para um locatário não confiável, não permita que o locatário use sua própria fonte de identidade e não permita o uso de serviços de plataforma. Consulte os passos para "criando uma conta de locatário".
- Use um balanceador de carga de terceiros para tráfego de clientes não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.
- Como opção, use um proxy de storage para obter mais controle sobre a comunicação de pools de storage em nuvem e serviços de plataforma dos nós de storage para serviços externos. Consulte os passos para "criando um proxy de armazenamento".
- Opcionalmente, conete-se a serviços externos usando a rede do cliente. Em seguida, selecione **CONFIGURATION** > **Security** > **Firewall control** > **UnTrusted Client Networks** e indique que a rede do cliente no nó de armazenamento não é confiável. O nó de armazenamento não aceita mais nenhum

tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para Serviços de plataforma.

Diretrizes para nós de gateway

Os nós de gateway fornecem uma interface de balanceamento de carga opcional que os aplicativos clientes podem usar para se conetar ao StorageGRID. Siga estas diretrizes para proteger quaisquer nós de gateway no seu sistema StorageGRID:

- Configure e use pontos de extremidade do balanceador de carga. "Considerações para balanceamento de carga"Consulte .
- Use um balanceador de carga de terceiros entre o cliente e o nó de gateway ou nós de storage para obter tráfego de cliente não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques. Se você usar um balanceador de carga de terceiros, o tráfego de rede ainda poderá ser configurado opcionalmente para passar por um ponto de extremidade do balanceador de carga interno ou ser enviado diretamente para nós de storage.
- Se você estiver usando pontos de extremidade do balanceador de carga, opcionalmente, faça com que os clientes se conetem pela rede do cliente. Em seguida, selecione **CONFIGURATION** > **Security** > **Firewall control** > **UnTrusted Client Networks** e indique que a rede Client no Gateway Node não é confiável. O Gateway Node aceita apenas tráfego de entrada nas portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

Diretrizes para nós de dispositivos de hardware

Os aparelhos de hardware StorageGRID são especialmente projetados para uso em um sistema StorageGRID. Alguns dispositivos podem ser usados como nós de storage. Outros dispositivos podem ser usados como nós de administrador ou nós de gateway. Você pode combinar nós de dispositivo com nós baseados em software ou implantar grades totalmente projetadas para todos os dispositivos.

Siga estas diretrizes para proteger todos os nós de dispositivos de hardware no seu sistema StorageGRID:

- Se o dispositivo usar o Gerenciador de sistema do SANtricity para o gerenciamento do controlador de storage, evite que clientes não confiáveis acessem o Gerenciador de sistema do SANtricity pela rede.
- Se o dispositivo tiver um controlador de gerenciamento de placa base (BMC), esteja ciente de que a porta de gerenciamento BMC permite acesso a hardware de baixo nível. Conete a porta de gerenciamento BMC somente a uma rede de gerenciamento interna segura, confiável. Se nenhuma rede estiver disponível, deixe a porta de gerenciamento do BMC desconetada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.
- Se o dispositivo suportar o gerenciamento remoto do hardware do controlador via Ethernet usando o padrão IPMI (Intelligent Platform Management Interface), bloqueie o tráfego não confiável na porta 623.

> Você pode ativar ou desativar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite o acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisar de acesso remoto IPMI ao BMC, desative esta opção usando um dos seguintes métodos: No Gerenciador de Grade, vá para **CONFIGURATION** > **Security** > **Security** > **Security settings** > **Appliances** e desmarque a caixa de seleção **Enable Remote IPMI Access**. Na API de gerenciamento de grade, use o endpoint privado: `PUT /private/bmc`.

- Para modelos de dispositivo que contêm unidades SED, FDE ou FIPS NL-SAS que você gerencia com o SANtricity System Manager, "Ative e configure a Segurança da Unidade SANtricity".

- Para modelos de dispositivo que contêm SSDs NVMe FIPS ou SED que você gerencia usando o instalador de dispositivos StorageGRID e o Gerenciador de Grade, "Ativar e configurar a encriptação da unidade StorageGRID".
- Para dispositivos sem unidades SED, FDE ou FIPS, habilite e configure a criptografia de nó de software do StorageGRID "Usando um servidor de gerenciamento de chaves (KMS)" .

Diretrizes de fortalecimento para TLS e SSH

Você deve substituir os certificados padrão criados durante a instalação e selecionar a diretiva de segurança apropriada para conexões TLS e SSH.

Diretrizes de endurecimento para certificados

Você deve substituir os certificados padrão criados durante a instalação por seus próprios certificados personalizados.

Para muitas organizações, o certificado digital autoassinado para o acesso à Web StorageGRID não é compatível com suas políticas de segurança de informações. Em sistemas de produção, você deve instalar um certificado digital assinado pela CA para uso na autenticação do StorageGRID.

Especificamente, você deve usar certificados de servidor personalizados em vez desses certificados padrão:

- **Certificado de interface de gerenciamento**: Usado para proteger o acesso ao Gerenciador de Grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento do locatário.
- **Certificado API S3 e Swift**: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos clientes S3 e Swift usam para carregar e baixar dados de objetos.

"Gerenciar certificados de segurança"Consulte para obter detalhes e instruções.

> O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, "Configurar pontos de extremidade do balanceador de carga"consulte .

Ao usar certificados de servidor personalizados, siga estas diretrizes:

- Os certificados devem ter um `subjectAltName` que corresponda às entradas de DNS para StorageGRID. Para obter detalhes, consulte a seção 4,2.1,6, "Nome alternativo do assunto", em "RFC 5280: Certificado PKIX e perfil CRL".
- Quando possível, evite o uso de certificados curinga. Uma exceção a essa diretriz é o certificado para um endpoint de estilo hospedado virtual S3, que requer o uso de um curinga se os nomes de bucket não forem conhecidos antecipadamente.
- Quando você deve usar curingas em certificados, você deve tomar medidas adicionais para reduzir os riscos. Use um padrão curinga como `*.s3.example.com` , e não use o `s3.example.com` sufixo para outros aplicativos. Esse padrão também funciona com acesso S3D de estilo caminho, como `dc1-s1.s3.example.com/mybucket` .
- Defina os tempos de expiração do certificado como curtos (por exemplo, 2 meses) e use a API Grid Management para automatizar a rotação do certificado. Isso é especialmente importante para certificados curinga.

Além disso, os clientes devem usar uma verificação rigorosa do nome de host ao se comunicar com o

StorageGRID.

Diretrizes de fortalecimento para a política TLS e SSH

Você pode selecionar uma política de segurança para determinar 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. Como prática recomendada, você deve desativar as opções de criptografia que não são necessárias para a compatibilidade de aplicativos. Use a política moderna padrão, a menos que seu sistema precise ser compatível com critérios comuns ou que você precise usar outras cifras.

"Gerencie a política TLS e SSH"Consulte para obter detalhes e instruções.

Outras diretrizes de endurecimento

Além de seguir as diretrizes de proteção para redes e nós StorageGRID, você deve seguir as diretrizes de proteção para outras áreas do sistema StorageGRID.

Logs e mensagens de auditoria

Proteja sempre os logs do StorageGRID e a saída de mensagens de auditoria de forma segura. Os logs do StorageGRID e as mensagens de auditoria fornecem informações inestimáveis do ponto de vista de suporte e disponibilidade do sistema. Além disso, as informações e detalhes contidos nos logs do StorageGRID e na saída de mensagens de auditoria são geralmente de natureza sensível.

Configure o StorageGRID para enviar eventos de segurança para um servidor syslog externo. Se estiver usando a exportação syslog, selecione TLS e RELP/TLS para os protocolos de transporte.

Consulte o "Referência de ficheiros de registo" para obter mais informações sobre os registos do StorageGRID. Consulte "Auditar mensagens" para obter mais informações sobre mensagens de auditoria do StorageGRID.

NetApp AutoSupport

O recurso AutoSupport do StorageGRID permite que você monitore proativamente a integridade do seu sistema e envie automaticamente pacotes para o site de suporte da NetApp, a equipe de suporte interna da sua organização ou um parceiro de suporte. Por padrão, o envio de pacotes AutoSupport para o NetApp é ativado quando o StorageGRID é configurado pela primeira vez.

O recurso AutoSupport pode ser desativado. No entanto, o NetApp recomenda habilitá-lo, pois o AutoSupport ajuda a acelerar a identificação e resolução de problemas caso surja algum problema no seu sistema StorageGRID.

O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível dos pacotes AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar pacotes AutoSupport para o NetApp.

Compartilhamento de recursos entre origens (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e objetos nesse bucket estejam acessíveis a aplicativos da Web em outros domínios. Em

geral, não ative o CORS a menos que seja necessário. Se CORS for necessário, restrinja-o a origens confiáveis.

Consulte os passos para "Configurando o compartilhamento de recursos entre origens (CORS)".

Dispositivos de segurança externos

Uma solução completa de endurecimento deve abordar mecanismos de segurança fora do StorageGRID. O uso de dispositivos de infraestrutura adicionais para filtrar e limitar o acesso ao StorageGRID é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esses dispositivos de segurança externos incluem firewalls, sistemas de prevenção de intrusão (IPSs) e outros dispositivos de segurança.

Um balanceador de carga de terceiros é recomendado para tráfego de clientes não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.

Mitigação de ransomware

Ajude a proteger os dados de objetos de ataques de ransomware seguindo as recomendações da "Defesa contra ransomware com o StorageGRID".

Informações sobre direitos autorais

Informações sobre marcas comerciais