Endurecimento do sistema

StorageGRID software

NetApp
December 03, 2025

Índice

Endurecimento do sistema

Considerações gerais para o reforço do sistema

O reforço do sistema é o processo de eliminar o máximo possível de riscos de segurança de um sistema StorageGRID .

Ao instalar e configurar o StorageGRID, use estas diretrizes para ajudar a atender a quaisquer objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade.

Você já deve estar usando as melhores práticas padrão do setor para reforço do sistema. Por exemplo, você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e habilita a autenticação baseada em certificado quando disponível.

O StorageGRID segue o "Política de tratamento de vulnerabilidades da NetApp" . As vulnerabilidades relatadas são verificadas e tratadas de acordo com o processo de resposta a incidentes de segurança do produto.

Ao fortalecer um sistema StorageGRID , considere o seguinte:

- *Qual das três redes StorageGRID * você implementou? Todos os sistemas StorageGRID devem usar a Rede Grid, mas você também pode usar a Rede de administração, a Rede de cliente ou ambas. Cada rede tem diferentes considerações de segurança.
- **O tipo de plataforma** que você usa para os nós individuais no 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 práticas recomendadas de proteção.
- **Quão confiáveis são as contas dos inquilinos**. Se você for um provedor de serviços com contas de locatários não confiáveis, terá preocupações de segurança diferentes do que se usasse apenas locatários internos confiáveis.
- **Quais requisitos e convenções de segurança** sua organização segue. Talvez seja necessário cumprir requisitos regulatórios ou corporativos específicos.

Diretrizes de reforço 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 vulnerabilidades conhecidas ficam ativas e reduz a área geral da superfície de ataque. Além disso, as versões mais recentes do StorageGRID geralmente contêm recursos de reforço de segurança que não estão incluídos nas versões anteriores.

Consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" (IMT) para determinar qual versão do software StorageGRID você deve usar. Quando um hotfix é necessário, a NetApp prioriza a criação de atualizações para as versões mais recentes. Alguns patches podem não ser compatíveis com versões anteriores.

- Para baixar os lançamentos e hotfixes mais recentes do StorageGRID , acesse "Downloads da NetApp : StorageGRID" .
- Para atualizar o software StorageGRID , consulte o"instruções de atualização" .
- Para aplicar um hotfix, consulte o"Procedimento de correção do StorageGRID" .

Atualizações para serviços externos

Serviços externos podem ter vulnerabilidades que afetam o StorageGRID indiretamente. Você deve garantir que os serviços dos quais o StorageGRID depende sejam mantidos 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 da NetApp" .

Atualizações para hipervisores

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

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Atualizações para nós Linux

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

Para obter uma lista de versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Diretrizes de proteção 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 para atender aos seus requisitos de segurança e acesso.

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

Diretrizes para Rede de Grade

Você deve configurar uma Grid Network para todo o tráfego interno do StorageGRID . Todos os nós da grade estão na Rede da Grade e devem ser capazes de se comunicar com todos os outros nós.

Ao configurar a rede Grid, siga estas diretrizes:

- Certifique-se de que a rede esteja protegida de clientes não confiáveis, como aqueles na internet aberta.
- Sempre que possível, use a Grid Network exclusivamente para tráfego interno. Tanto a Rede de Administração quanto a Rede de Cliente têm restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da Grid Network para tráfego de clientes externos 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 Grid Network para fornecer proteção adicional para o tráfego interno.
- Alguns procedimentos de manutenção exigem acesso SSH (Secure Shell) na porta 22 entre o nó de administração primário e todos os outros nós da grade. Use um firewall externo para restringir o acesso SSH a clientes confiáveis.

Diretrizes para a rede de administração

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

Se você estiver usando a Rede de Administração, siga estas diretrizes:

- Bloqueie todas as portas de tráfego interno na rede de administração. Veja o"lista de portas internas" .
- Se 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 normalmente é usada para locatários e para comunicação com serviços externos, como o serviço de replicação do CloudMirror ou outro serviço de plataforma. No entanto, o StorageGRID não impõe esse uso internamente.

Se você estiver usando a Rede de Clientes, siga estas diretrizes:

- Bloqueie todas as portas de tráfego interno na rede do cliente. Veja o"lista de portas internas" .
- Aceite tráfego de entrada de clientes somente em endpoints configurados explicitamente. Veja as informações sobre"gerenciando controles de firewall" .

Diretrizes de proteção para nós do 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 proteção.

Controle o acesso remoto do IPMI ao BMC

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

- Para controlar o acesso remoto do IPMI ao BMC no Grid Manager, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** > **Dispositivos**:
  - Desmarque a caixa de seleção **Habilitar acesso IPMI remoto** para desabilitar o acesso IPMI ao BMC.
  - Marque a caixa de seleção **Habilitar acesso IPMI remoto** para habilitar o acesso IPMI ao BMC.

Configuração de firewall

Como parte do processo de proteção do sistema, você deve revisar as configurações do firewall externo e modificá-las para que o tráfego seja aceito apenas dos endereços IP e nas portas dos quais ele 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" para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para sua implantação de grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Especificamente, você pode gerenciar estas áreas:

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

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

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

Desabilitar serviços não utilizados

Para todos os nós do StorageGRID , você deve desabilitar ou bloquear o acesso a serviços não utilizados. Por exemplo, se você não planeja usar DHCP, use o Grid Manager para fechar a porta 68. Selecione **CONFIGURAÇÃO** > **Controle de firewall** > **Gerenciar acesso externo**. Em seguida, altere a alternância de status da porta 68 de **Aberta** para **Fechada**.

Virtualização, contêineres e hardware compartilhado

Para todos os nós do StorageGRID , evite executar o StorageGRID no mesmo hardware físico que software não confiável. Não presuma que as proteções do hipervisor impedirão que malware acesse dados protegidos 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 do 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 estão totalmente seguros até que se juntem à grade.

Diretrizes para nós de administração

Os nós de administração fornecem serviços de gerenciamento, como configuração do sistema, monitoramento e registro. Ao fazer login no Grid Manager ou no Tenant Manager, você está se conectando a um nó de administração.

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 de administração na rede Grid, na rede de administração ou na rede de clientes.
- Os grupos StorageGRID controlam o acesso aos recursos do Grid Manager e do Tenant Manager. 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 endpoints do balanceador de carga StorageGRID , use nós de gateway em vez de nós de administração para tráfego de cliente não confiável.
- Se você tiver locatários não confiáveis, não permita que eles tenham acesso direto ao Gerenciador de Locatários ou à API de Gerenciamento de Locatários. Em vez disso, faça com que os locatários não confiáveis usem um portal de locatários ou um sistema externo de gerenciamento de locatários, que interage com a API de gerenciamento de locatários.
- Opcionalmente, use um proxy de administrador para obter mais controle sobre a comunicação do AutoSupport dos nós de administração para o suporte da NetApp . Veja os passos para"criando um proxy de administrador" .
- Opcionalmente, use as portas restritas 8443 e 9443 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 locatários.

Para mais informações, consulte as instruções para"administrando StorageGRID" .

Diretrizes para nós de armazenamento

Os nós de armazenamento gerenciam e armazenam dados de objetos e metadados. Siga estas diretrizes para proteger os nós de armazenamento no seu sistema StorageGRID .

- Não permita que clientes não confiáveis se conectem diretamente aos nós de armazenamento. Use um ponto de extremidade do balanceador de carga atendido por um nó de gateway ou um balanceador de carga de terceiros.
- Não habilite serviços de saída para locatários não confiáveis. Por exemplo, ao criar uma conta para um locatário não confiável, não permita que o locatário use sua própria fonte de identidade e não permita o uso de serviços da plataforma. Veja os passos para"criando uma conta de inquilino" .
- Use um balanceador de carga de terceiros para tráfego de clientes não confiáveis. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.
- Opcionalmente, use um proxy de armazenamento para obter mais controle sobre os pools de armazenamento em nuvem e a comunicação dos serviços de plataforma dos nós de armazenamento para serviços externos. Veja os passos para"criando um proxy de armazenamento" .
- Opcionalmente, conecte-se a serviços externos usando a Rede do Cliente. Em seguida, selecione **CONFIGURAÇÃO** > **Segurança** > **Controle de firewall** > **Redes de clientes não confiáveis** e indique que a Rede de clientes no nó de armazenamento não é confiável. O nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua permitindo 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 conectar ao StorageGRID. Siga estas diretrizes para proteger quaisquer nós de gateway

no seu sistema StorageGRID :

- Configurar e usar endpoints do balanceador de carga. Ver "Considerações para balanceamento de carga" .
- Use um balanceador de carga de terceiros entre o cliente e o nó de gateway ou nós de armazenamento para 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 para passar por um ponto de extremidade do balanceador de carga interno ou ser enviado diretamente para os nós de armazenamento.
- Se você estiver usando endpoints do balanceador de carga, opcionalmente, faça com que os clientes se conectem pela Rede do Cliente. Em seguida, selecione **CONFIGURAÇÃO** > **Segurança** > **Controle de firewall** > **Redes de clientes não confiáveis** e indique que a Rede de clientes no nó de gateway não é confiável. O nó de gateway 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 dispositivos de hardware StorageGRID são especialmente projetados para uso em um sistema StorageGRID . Alguns aparelhos podem ser usados como nós de armazenamento. Outros dispositivos podem ser usados como nós de administração ou nós de gateway. Você pode combinar nós de dispositivos com nós baseados em software ou implantar grades totalmente projetadas para todos os dispositivos.

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

- Se o dispositivo usar o SANtricity System Manager para gerenciamento do controlador de armazenamento, impeça que clientes não confiáveis acessem o SANtricity System Manager pela rede.
- Se o dispositivo tiver um controlador de gerenciamento de placa base (BMC), esteja ciente de que a porta de gerenciamento do BMC permite acesso de hardware de baixo nível. Conecte a porta de gerenciamento do BMC somente a uma rede de gerenciamento interna segura e confiável. Se nenhuma rede desse tipo estiver disponível, deixe a porta de gerenciamento do BMC desconectada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.
- Se o dispositivo oferecer suporte ao gerenciamento remoto do hardware do controlador via Ethernet usando o padrão Intelligent Platform Management Interface (IPMI), bloqueie o tráfego não confiável na porta 623.

> Você pode habilitar ou desabilitar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha BMC . Se você não precisar de acesso IPMI remoto ao BMC, desative esta opção usando um dos seguintes métodos: + No Grid Manager, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** > **Dispositivos** e desmarque a caixa de seleção **Habilitar acesso IPMI remoto**. + Na API de gerenciamento de grade, use o ponto de extremidade privado: `PUT /private/bmc` .

- Para modelos de dispositivos que contêm unidades SED, FDE ou FIPS NL-SAS que você gerencia com o SANtricity System Manager, "habilitar e configurar o SANtricity Drive Security" .
- Para modelos de dispositivos que contêm SSDs SED ou FIPS NVMe que você gerencia usando o StorageGRID Appliance Installer e o Grid Manager, "habilitar e configurar a criptografia de unidade StorageGRID" .
- Para dispositivos sem unidades SED, FDE ou FIPS, habilite e configure a criptografia do nó de software StorageGRID "usando um Servidor de Gerenciamento de Chaves (KMS)" .

Diretrizes de proteção para TLS e SSH

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

Diretrizes de reforço para certificados

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

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

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

- **Certificado de interface de gerenciamento**: usado para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API.
- **Certificado de API S3**: usado para proteger o acesso aos nós de armazenamento e nós de gateway, que os aplicativos cliente S3 usam para carregar e baixar dados de objetos.

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

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

Ao usar certificados de servidor personalizados, siga estas diretrizes:

- Os certificados devem ter uma `subjectAltName` que corresponde às entradas 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" .
- Sempre que possível, evite o uso de certificados curinga. Uma exceção a essa diretriz é o certificado para um ponto de extremidade de estilo hospedado virtual S3, que requer o uso de um curinga se os nomes dos buckets não forem conhecidos com antecedência.
- Quando você precisar usar curingas em certificados, tome medidas adicionais para reduzir os riscos. Use um padrão curinga como `*.s3.example.com` , e não use o `s3.example.com` sufixo para outras aplicações. Este padrão também funciona com acesso S3 no estilo de caminho, como `dc1-s1.s3.example.com/mybucket` .
- Defina os tempos de expiração dos certificados como curtos (por exemplo, 2 meses) e use a API de gerenciamento de grade para automatizar a rotação de certificados. Isso é especialmente importante para certificados curinga.

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

Diretrizes de reforço para 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 internos do StorageGRID .

A política de segurança controla como TLS e SSH criptografam dados em movimento. Como prática recomendada, você deve desabilitar opções de criptografia que não são necessárias para compatibilidade do aplicativo. Use a política Moderna padrão, a menos que seu sistema precise ser compatível com os Critérios Comuns ou você precise usar outras cifras.

Ver"Gerenciar a política TLS e SSH" para obter detalhes e instruções.

Outras diretrizes de endurecimento

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

Senha de instalação temporária

Para proteger o sistema StorageGRID durante a instalação, defina uma senha na página de senha temporária do instalador na interface de instalação do StorageGRID ou na API de instalação. Quando definida, essa senha se aplica a todos os métodos de instalação do StorageGRID, incluindo a interface do usuário, a API de instalação e `configure-storagegrid.py` roteiro.

Para mais informações, consulte:

- "Instalar o StorageGRID no Red Hat Enterprise Linux"
- "Instalar o StorageGRID no Ubuntu ou Debian"
- "Instalar o StorageGRID no VMware"
- "Instalar o dispositivo StorageGRID"

Logs e mensagens de auditoria

Sempre proteja os logs do StorageGRID e a saída das mensagens de auditoria de maneira segura. Os logs e mensagens de auditoria do StorageGRID fornecem informações valiosas do ponto de vista de suporte e disponibilidade do sistema. Além disso, as informações e os detalhes contidos nos logs do StorageGRID e na saída das mensagens de auditoria são geralmente de natureza confidencial.

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.

Veja o"Referência de arquivos de log" para obter mais informações sobre logs do StorageGRID .
Ver"Mensagens de auditoria" para obter mais informações sobre mensagens de auditoria do StorageGRID .

AutoSupport da NetApp

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

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

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

padrão para enviar pacotes do AutoSupport para a NetApp.

Compartilhamento de recursos de origem cruzada (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e os objetos nele sejam acessíveis a aplicativos da Web em outros domínios. Em geral, não habilite o CORS, a menos que seja necessário. Se o CORS for necessário, restrinja-o a origens confiáveis.

Veja os passos para"configurando compartilhamento de recursos de origem cruzada (CORS)" .

Dispositivos de segurança externos

Uma solução de proteção completa deve abordar mecanismos de segurança fora do StorageGRID. Usar 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 confiáveis. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.

Mitigação de ransomware

Ajude a proteger os dados do seu objeto contra ataques de ransomware seguindo as recomendações em "Defesa contra ransomware com StorageGRID" .

Informações sobre direitos autorais

Informações sobre marcas comerciais