aws

Guia do desenvolvedor

AWS Gerente de segurança de rede



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Gerente de segurança de rede: Guia do desenvolvedor

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o AWS Network Security Manager? 1
Como AWS O Network Security Manager funciona em um piscar de olhos 1
Características do AWS Gerente de segurança de rede 1
Casos de uso 2
Serviços relacionados 3
Acesso AWS Gerente de segurança de rede 4
Preços 4
Você é um usuário iniciante do ? 5
Como funciona o AWS Network Security Manager 6
AWS Modelo de recursos do Network Security Manager 6
AWS Ciclo de vida, fusão e sincronização de recursos do Network Security Manager 7
Ciclo de vida preliminar e ativo 7
Versionamento 8
Priority-based fusão de políticas 9
Descoberta de recursos com AWS Config 10
Sincronização e remediação 11
Contas de administrador e membro 12
Service-linked papel 13
Configurando o AWS Network Security Manager 14
Escolha seu modelo organizacional 14
Configuração para uso de conta única 14
Configurando para uso em várias contas com AWS Organizações 15
Criando um AWS Conta de administrador do Network Security Manager 16
Crie uma identidade do IAM com AWS Permissões do Network Security Manager 18
Inscreva-se para um Conta da AWS 19
Utilizar AWS Network Security Manager em regiões que estão desativadas por padrão 19
Tutorial: implante sua primeira proteção de segurança de rede 20
Pré-requisitos 20
Etapa 1: criar uma regra 21
Etapa 2: criar um modelo 22
Etapa 3: criar uma política 23
Etapa 4: criar um escopo 24
Etapa 5: criar e publicar uma implantação 24
Etapa 6: Monitorar o status da sincronização 25

Etapa 7: limpar ... 26
Próximas etapas ... 27
Gerenciando firewalls e serviços de segurança ... 28
Gerenciando ACLs da web para AWS WAF ... 28
AWS Conceitos do WAF ... 28
Criação rápida para AWS WAF ... 32
Processo de criação padrão para AWS WAF ... 36
Gerenciando proteções contra DDoS para Shield AWS Advanced ... 42
Criação rápida para AWS Shield Advanced ... 43
Processo de criação padrão para AWS Shield Advanced ... 47
AWS Gerenciador de Segurança de Rede e Gerenciador de Firewall ... 51
Coexistência com AWS Firewall Manager ... 51
Precedência durante a remediação ... 51
Migração planejada de AWS Firewall Manager ... 51
Segurança ... 53
Proteção de dados ... 54
Criptografia em repouso ... 55
Criptografia em trânsito ... 55
Gerenciamento de chaves ... 55
Gerenciamento de identidade e acesso ... 55
Público ... 56
Autenticação com identidades ... 56
Gerenciar o acesso usando políticas ... 57
Como AWS O Network Security Manager funciona com o IAM ... 59
Identity-based exemplos de políticas ... 65
Solução de problemas ... 70
Service-linked funções ... 72
Service-linked permissões de função ... 72
Criar um perfil vinculado ao serviço ... 83
Editar um perfil vinculado ao serviço ... 83
Excluir um perfil vinculado ao serviço ... 83
Regiões aceitas ... 84
Validação de conformidade ... 84
Resiliência ... 85
Segurança da infraestrutura ... 85
Práticas recomendadas de segurança ... 86

Controles preventivos 86
Controles de detecção 86
Monitoramento AWS Gerente de segurança de rede 87
Monitorando o status de sincronização 87
Operações de status de sincronização 87
Entendendo os valores do status de sincronização 88
Entendendo os timestamps de avaliação 88
Cross-account visibilidade 88
Diagnosticando recursos fora de sincronia 89
CloudTrail troncos 89
AWS Informações sobre o Network Security Manager em CloudTrail 90
Exemplo: CreatePolicy evento 91
Cotas 94
Cotas de recurso 94
Cotas de composição de recursos 94
Cotas de configuração do escopo 95
Cotas da conta do administrador 95
Cotas de paginação da API 95
Ajustabilidade da cota 96
Histórico do documento 97
..... xcviii

O que é AWS Gerente de segurança de rede?

Com o AWS Network Security Manager, você pode definir e implantar centralmente proteções de segurança de rede, como as regras WAF AWS e AWS Shield Advanced, em uma ou mais contas e recursos em sua organização. Em vez de trabalhar com cada recurso individualmente, você define objetos de política reutilizáveis (regras, modelos e políticas) uma vez e os implanta em grande escala, com monitoramento contínuo para detectar e corrigir desvios de políticas.

Como AWS O Network Security Manager funciona em um piscar de olhos

Você define um conjunto de objetos de política hierárquica e os aplica aos escopos de destino. O nível mais baixo dos objetos de política são as regras. Você pode agrupar regras em modelos, que podem ser combinados em políticas com resolução de conflitos baseada em prioridades. Em seguida, você seleciona contas e recursos para proteger com um escopo e aplica suas políticas publicando uma implantação.

Após a implantação, o AWS Network Security Manager monitora continuamente o ambiente com escopo e as políticas implantadas para verificar se elas correspondem às definições pretendidas. Caso contrário, o AWS Network Security Manager pode, opcionalmente, corrigir recursos que se desviam da configuração pretendida. Para obter detalhes completos sobre o modelo de recursos, o ciclo de vida e a arquitetura, consulte. Como funciona o AWS Network Security Manager

Características do AWS Gerente de segurança de rede

- Support para vários tipos de firewall — O AWS Network Security Manager oferece suporte a AWS WAF para configurações de ACL da web e grupos de regras. Os tipos de recursos protegidos incluem CloudFront distribuições da Amazon, Application Load Balancers e estágios do Amazon API Gateway. AWS O Network Security Manager também oferece suporte ao AWS Shield Advanced para proteção contra DDoS de CloudFront distribuições da Amazon, Application Load Balancers, Classic Load Balancers e endereços IP elásticos.
- Configurações de segurança reutilizáveis — defina objetos de política uma vez como regras, agrupe-os em modelos e crie escopos para direcionar recursos. Reutilize regras, modelos e escopos em várias políticas e implantações.

- Priority-based mesclagem de políticas — Quando várias políticas protegem o mesmo recurso, o AWS Network Security Manager mescla suas configurações com base na prioridade da política, fornecendo uma resolução previsível de conflitos.
- Single-account e suporte a vários administradores — Use o AWS Network Security Manager em uma única conta ou designe várias contas de administrador, cada uma com um nível de prioridade. Quando as políticas dos administradores se sobrepõem, o AWS Network Security Manager resolve os conflitos primeiro pela prioridade do administrador e depois pela prioridade da política em cada conta.
- Estados preliminares e ativos — Cada recurso do AWS Network Security Manager, incluindo regras, modelos, políticas, escopos e implantações, oferece suporte aos estados Rascunho e Ativo. Salve recursos como rascunho sem afetar as proteções ativas e publique quando estiver pronto para aplicá-las.
- Instantâneos com versão — Cada recurso do AWS Network Security Manager, incluindo regras, modelos, políticas, escopos e implantações, oferece suporte a instantâneos imutáveis e numerados por versão. Use o controle de versão para preservar as configurações de recursos do AWS Network Security Manager em boas condições.
- Protected-resource diagnóstico de sincronização — Para cada recurso dentro do escopo, veja exatamente quais configurações estão fora de sincronia e por quê, com as configurações esperadas em comparação com os valores reais de cada campo de configuração.
- Correção automática — opcionalmente, habilite o AWS Network Security Manager para corrigir automaticamente os recursos fora de sincronia e alinhá-los com a configuração pretendida sem intervenção manual.
- Natural-language geração de regras — Use a `GenerateRuleConfiguration` operação para descrever uma regra em linguagem simples e receber a configuração correspondente JSON, desenvolvida pelo Amazon Bedrock.

Casos de uso

A seguir estão os casos de uso comuns do AWS Network Security Manager:

- Aplique as regras básicas do AWS WAF em todas as contas — defina um conjunto de grupos de regras do AWS WAF que todo aplicativo voltado para a Internet deve usar e, em seguida, implante-os em toda a organização. AWS O Network Security Manager aplica automaticamente as regras aos novos recursos dentro do escopo à medida que eles entram no escopo.

- Crie regras específicas de AWS WAF personalizadas ou de exceção em recursos específicos — Defina um conjunto de regras de AWS WAF que se apliquem somente a um conjunto específico de recursos. Esse conjunto pode ser uma unidade de negócios ou aplicativo específico que você identifica por ID AWS da conta, OU, tag ou Amazon Resource Names (ARNs).
- Verifique a proteção contra DDoS em recursos voltados para a Internet — Crie uma política AWS Shield Advanced com escopo para tipos de recursos públicos e implante-a em toda a organização para que recursos críticos tenham a proteção contra DDoS ativada.
- Detecte e corrija desvios de configuração — Use o monitoramento do status de sincronização para identificar recursos cujas configurações de firewall saíram do estado pretendido e, opcionalmente, habilite a correção automática para trazê-los de volta à conformidade.
- Delegue o gerenciamento de segurança a várias equipes — designe várias contas de administrador com diferentes níveis de prioridade e acesso limitado a contas, unidades organizacionais ou tipos de firewall específicos, permitindo que as equipes gerenciem suas próprias políticas de segurança dentro de limites definidos.

Serviços relacionados

- AWS WAF — Use o AWS WAF para proteger seus aplicativos e APIs da Web contra explorações e bots comuns da Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. AWS O Network Security Manager usa o AWS WAF para criar e gerenciar ACLs da web e grupos de regras para recursos em uma única conta ou em várias contas em sua organização.
- AWS Shield Advanced — Um serviço gerenciado de proteção contra DDoS que fornece proteções expandidas para seus aplicativos em execução. AWS AWS O Network Security Manager usa o Shield Advanced para fornecer proteções contra DDoS para recursos em uma única conta ou em várias contas em sua organização.
- AWS Organizations — Ajuda você a gerenciar e governar centralmente seu ambiente à medida que você cresce e escala seus AWS recursos. AWS O Network Security Manager exige que AWS as Organizations gerenciem as proteções nas contas dos membros.
- AWS Config — Um serviço que permite avaliar, auditar e avaliar as configurações de seus recursos. AWS AWS O Network Security Manager usa um gravador AWS Config vinculado ao serviço para descobrir recursos em suas contas de membros.

Acesso AWS Gerente de segurança de rede

Você pode acessar o AWS Network Security Manager por meio das seguintes interfaces:

AWS Console de gerenciamento

Uma interface baseada na web para gerenciar os recursos do AWS Network Security Manager.

Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.

AWS Interface de linha de comando (AWS CLI)

Fornece comandos para as operações do AWS Network Security Manager. Para obter mais informações, consulte a opção AWS Referência de comandos da CLI.

AWS SDKs

AWS fornece SDKs que consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação. Os SDKs fornecem uma maneira conveniente de criar acesso programático ao AWS Network Security Manager. Para obter mais informações, consulte Ferramentas para a Amazon Web Services.

AWS API do Gerenciador de Segurança de Rede

Uma API REST que usa JSON sobre HTTPS. O formato do endpoint da API é `network-security-manager.{region}.api.aws`. Para obter mais informações, consulte a Referência da API do AWS Network Security Manager.

Para começar a usar o AWS Network Security Manager, consulte Configurando o AWS Network Security Manager Tutorial: implante sua primeira proteção de segurança de rede e.

Preços

Você paga por cada recurso dentro do escopo que o AWS Network Security Manager monitora e protege. Cobranças adicionais se aplicam aos serviços de segurança subjacentes que você implanta, como AWS WAF e AWS Shield Advanced. Para obter informações detalhadas sobre preços, consulte os preços do AWS Network Security Manager no AWS site.

Você é um usuário iniciante do ?

Se você for um usuário iniciante do AWS Network Security Manager, recomendamos que você leia os tópicos a seguir na ordem:

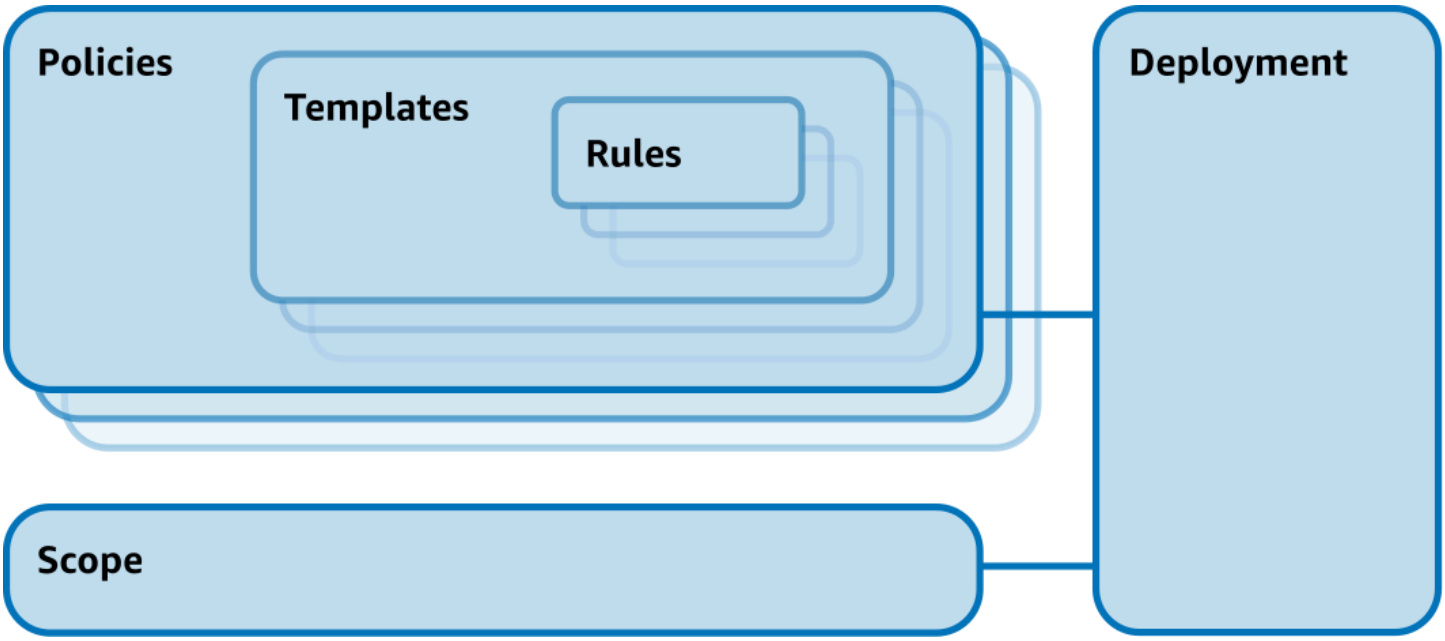
1. Como funciona o AWS Network Security Manager— Saiba mais sobre o modelo de recursos, os estados do ciclo de vida, a fusão de políticas e a sincronização.
2. Configurando o AWS Network Security Manager— Preencha os pré-requisitos para usar o AWS Network Security Manager.
3. Tutorial: implante sua primeira proteção de segurança de rede— Veja um tutorial completo que cria sua primeira implantação.

Como AWS O Network Security Manager funciona

Use o modelo de recursos do AWS Network Security Manager para projetar e gerenciar proteções de segurança de rede para recursos em uma única conta ou em várias contas em sua organização. Este capítulo explica os cinco tipos de recursos, como eles formam uma hierarquia e os principais conceitos que governam seu comportamento.

AWS Modelo de recursos do Network Security Manager

AWS O Network Security Manager usa cinco tipos de recursos organizados em uma hierarquia de composição:



Os recursos fazem referência uns aos outros de forma ascendente na hierarquia. As regras são usadas em modelos e políticas. Modelos, regras ou ambos são usados nas políticas. Um escopo faz referência aos recursos que as políticas protegem em uma implantação.

As seções a seguir descrevem cada tipo de recurso na hierarquia.

Regra — A unidade atômica da configuração de segurança da rede. Há dois tipos de regras: regras de inspeção de tráfego e regras de configuração de firewall. A inspeção de tráfego se concentra em como o serviço de segurança aborda o tráfego. Uma regra de configuração especifica as operações do sistema fora da inspeção de tráfego. A estrutura de uma regra varia de acordo com o tipo de firewall.

Modelo — Um grupo de regras ordenado e reutilizável para um único tipo de firewall. Use modelos para agrupar regras relacionadas e compartilhá-las em várias políticas. Os modelos são opcionais.

Política — combina um conjunto ordenado de modelos e regras com configurações de fiscalização para um tipo de firewall. Cada política tem uma prioridade (um número menor indica uma prioridade maior). Quando várias políticas protegem o mesmo recurso, a prioridade determina como os conflitos são resolvidos. Para regras de inspeção de tráfego, a prioridade determina a ordem na qual as regras são agregadas. Para regras de configuração de firewall, a prioridade determina qual configuração se aplica a cada recurso e suas políticas dentro do escopo.

Escopo — Uma seleção declarativa de onde as proteções se aplicam. Um escopo especifica quais tipos de recursos proteger e, opcionalmente, você pode filtrar recursos por tag ou atributo de configuração. No modo de várias contas, um escopo também especifica quais contas ou OUs devem ser incluídas ou excluídas. No modo de conta única, o escopo se aplica à própria conta. O modo de um escopo é fixo quando você o cria. Você não pode alternar um escopo entre os modos de várias contas e de conta única em nenhuma direção, portanto, um escopo de várias contas nunca pode se tornar um escopo de conta única ou vice-versa.

Implantação — vincula uma ou mais políticas a um escopo. A publicação de uma implantação ativa a fiscalização. AWS O Network Security Manager descobre recursos no escopo, calcula a configuração pretendida e, opcionalmente, corrige recursos fora de sincronia.

Para ver os limites de composição de recursos, consulteCotas.

AWS Ciclo de vida, fusão e sincronização de recursos do Network Security Manager

As seções a seguir explicam os comportamentos e os mecanismos que controlam como os recursos do AWS Network Security Manager operam depois que você os cria.

Ciclo de vida preliminar e ativo

Cada recurso do AWS Network Security Manager — incluindo regras, modelos, políticas, escopos e implantações — tem um status de Rascunho ou Ativo:

- Ativo — O status padrão. O recurso está publicado e está disponível para uso. Outros recursos podem referenciá-lo, e implantações que o incluam reforçam sua configuração.

- Rascunho — O recurso foi salvo, mas ainda não está ativo. Os recursos preliminares não são aplicados e não podem ser referenciados por outros recursos. Ao criar ou atualizar um recurso, escolha Salvar rascunho para mantê-lo no status de rascunho.

Por padrão, o AWS Network Security Manager cria recursos como Ativos. Para criar um recurso como Draft usando a API, defina o `isPublished` parâmetro como `false` na operação de criação ou atualização.

Quando você atualiza um recurso, os seguintes cenários se aplicam:

Estado atual	Ação	Resultado
Rascunho	Escolha Salvar rascunho	Atualizar o rascunho (permanece como rascunho)
Rascunho	Escolha Publicar	Publica o rascunho (fica ativo)
Ativo	Escolha Publicar	Atualize e permaneça ativo (ativo)
Ativo	Escolha Salvar rascunho	Crie uma sobreposição de rascunho (se torna Rascunho com um recurso ativo abaixo)

O `hasPublishedVersion` campo aparece na lista e recebe respostas. Esse campo informa se um recurso ativo publicado existe abaixo de um rascunho. Quando um recurso tem o status de Rascunho e `hasPublishedVersion: true` um rascunho pendente fica em cima de um recurso ativo ativo publicado e ativo.

Você não pode excluir um recurso ativo referenciado por outro recurso ativo.

Versionamento

Todos os recursos do AWS Network Security Manager, incluindo regras, modelos, políticas, escopos e implantações, podem ser versionados. Para criar uma versão de um recurso ativo, selecione o recurso, escolha Ação e, em seguida, escolha Criar instantâneo versionado. As versões não são criadas automaticamente em cada atualização.

> **AWS Alternativa de CLI**
>
> Você também pode criar uma versão usando a operação de `Create{Resource}Snapshot` API em um recurso ativo.

Propriedades da versão principal:

- Cada versão tem um número exclusivo (um número inteiro sequencial) e um ARN qualificado para a versão (por exemplo,). `arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- As versões são imutáveis. Eles não podem ser atualizados.
- Você pode criar até 10 versões por recurso.
- As versões podem ser marcadas.

Use versões para preservar as variantes de configuração desejadas. Para reverter um recurso, leia uma versão e atualize o recurso ativo com a configuração desejada da versão.

Priority-based fusão de políticas

Quando várias políticas protegem o mesmo recurso, o AWS Network Security Manager mescla suas configurações em um único resultado. Um número de prioridade mais baixo indica uma prioridade mais alta (a prioridade 1 tem precedência sobre a prioridade 2). Quando o AWS Network Security Manager mescla políticas que contêm regras de inspeção de tráfego, a prioridade determina a ordem na qual as regras são agregadas. Para regras de configuração de firewall, a política de maior prioridade determina qual configuração se aplica.

AWS O Network Security Manager avalia a prioridade em dois níveis, nesta ordem:

1. Prioridade do administrador — O AWS Network Security Manager avalia primeiro a prioridade do administrador. Cada administrador da organização recebe uma prioridade, conforme descrito emthe section called “Contas de administrador e membro”. Quando o AWS Network Security Manager mescla políticas, ele classifica uma política de administrador acima da política de conta única da própria conta membro. Se uma política do administrador e a política de conta única da conta do membro se aplicarem a um recurso e entrarem em conflito, a configuração da política do administrador será a vencedora. Uma conta de membro não pode optar por não participar, substituir ou se isentar de uma política de administrador.

2. Prioridade da política — Em cada conta, o AWS Network Security Manager usa a prioridade da política para resolver os conflitos restantes. Os valores de prioridade da política são números inteiros a partir de 1 e devem ser exclusivos por conta.

Você define a prioridade do administrador com o `priority` campo obrigatório na `PutAdminAccount` operação, um número inteiro de 1 a 10. Os valores de prioridade são exclusivos, portanto, dois administradores nunca compartilham uma prioridade e não é necessário desempate. Para obter mais informações, consulte a Referência da API do AWS Network Security Manager.

O resultado combinado de todas as políticas aplicáveis a um recurso é a configuração efetiva do firewall. AWS O Network Security Manager calcula essa configuração, a compara com a configuração real do recurso e relata quaisquer diferenças como status de sincronização.

Quando as políticas entram em conflito, o AWS Network Security Manager compara cada atributo e aplica o valor da política de maior prioridade. Se a política de prioridade mais alta não definir um atributo, o valor da política de prioridade mais baixa será aplicado. Um recurso que corresponde à configuração efetiva é IN_SYNC. Um recurso protegido por uma política de menor prioridade cujas configurações foram substituídas por uma política de maior prioridade é reportado como OUT_OF_SYNC para a implantação de menor prioridade. Esse é um comportamento esperado, não uma falha.

Descoberta de recursos com AWS Config

AWS O Network Security Manager descobre recursos protegidos em suas contas usando um gravador de AWS configuração Config vinculado ao serviço. Esse gravador é criado automaticamente em cada conta quando essa conta entra no escopo de uma implantação. Ao contrário do AWS Firewall Manager, você não precisa realizar nenhuma configuração adicional. AWS O uso do Config pelo AWS Network Security Manager não é cobrado do cliente do AWS Network Security Manager.

Principais características do gravador vinculado ao serviço:

- Ela se chama `AWSConfigurationRecorderForNetworkSecurityManager`.
- Ele é separado de qualquer gravador de configuração gerenciado pelo cliente na conta.
- Ele registra somente os tipos de recursos relevantes para seus escopos e implantações ativos.
- Você não precisa configurar o AWS Config nem criar um gravador de configuração. AWS O Network Security Manager gerencia isso automaticamente. AWS O uso do Config pelo AWS Network Security Manager não é cobrado do cliente.

- Você não pode modificar ou excluir o gravador enquanto ele estiver em uso. AWS O Network Security Manager gerencia seu ciclo de vida automaticamente.

Você não precisa habilitar ou configurar o AWS Config manualmente para que o AWS Network Security Manager funcione. O serviço processa a descoberta de recursos automaticamente após a publicação de uma implantação.

Sincronização e remediação

A fiscalização no AWS Network Security Manager é assíncrona e, eventualmente, consistente. Depois de publicar uma implantação ou quando um recurso é alterado, os seguintes estágios ocorrem:

1. Descoberta de recursos — O AWS Network Security Manager descobre recursos no escopo usando um gravador AWS Config vinculado ao serviço.
2. Cálculo da configuração — Para cada recurso descoberto, o AWS Network Security Manager calcula a configuração efetiva do firewall mesclando todas as políticas aplicáveis por prioridade.
3. Avaliação da sincronização — O AWS Network Security Manager compara a configuração efetiva com a configuração real do recurso e registra o status da sincronização.
4. Remediação (opcional) — Se você definir `remediationEnabled` a política, o AWS Network Security Manager corrige os recursos fora de sincronia para corresponder à configuração efetiva.

Cada estágio é assíncrono. Consequências para seu fluxo de trabalho:

- Há um atraso entre a publicação de uma implantação e a proteção dos recursos.
- Há um atraso entre a criação de um novo recurso no escopo e sua proteção.
- O `Last Checked` carimbo de data/hora nas entradas de status de sincronização informa quando o AWS Network Security Manager avaliou um recurso pela última vez.

A remediação e a limpeza de recursos são configurações em nível de política. Você configura cada uma por política no `policyConfiguration` objeto.

`remediationEnabled`

Especifica se o AWS Network Security Manager corrige automaticamente os recursos não compatíveis. Quando você habilita essa configuração, o AWS Network Security Manager corrige os recursos fora de sincronia para que correspondam à configuração efetiva.

`resourcesCleanUp`

Especifica se o AWS Network Security Manager remove automaticamente os recursos criados quando eles não são mais necessários. AWS O Network Security Manager exclui um firewall criado quando você remove a implantação ou quando a conta ou o recurso sai do escopo.

Ambas `resourcesCleanUp` as configurações `remediationEnabled` e são padronizadas para`false`. AWS O Network Security Manager não corrige nem limpa recursos até que você habilite essas configurações. O `policyConfiguration` objeto também é válido`wafConfig`, o que se aplica às políticas do AWS WAF. Para obter mais informações, consulte a Referência da API do AWS Network Security Manager.

Quando um recurso está fora de sincronia, o status da sincronização inclui motivos fora de sincronia com detalhes por configuração que mostram os valores esperados em comparação com os valores reais. Os motivos estão organizados nas seguintes categorias:

- `missingFirewall`— Nenhuma proteção de firewall está associada ao recurso.
- `invalidFirewall`— Existe um firewall, mas sua configuração é diferente da configuração efetiva. Isso inclui seis compartimentos de detalhes: `incorrectSingleValueConfigurations`,`missingAppendableConfigurationValues`,`unexpected`e. `unexpectedMergeableConfigurationValues`

Se a remediação estiver habilitada, mas o AWS Network Security Manager não conseguir corrigir um recurso`issueType`, o `remediationIssues` campo fornecerá uma `message` descrição do problema e uma `correctiveAction` sugestão de como resolvê-lo.

AWS O Network Security Manager não avalia configurações que ele não gerencia. Se um campo não aparecer em nenhuma regra de contribuição, o AWS Network Security Manager o ignorará durante a avaliação da sincronização.

Contas de administrador e membro

AWS O Network Security Manager usa um modelo de gerenciamento entre contas baseado em AWS Organizations:

- Conta de administrador — A conta na qual você cria e gerencia os recursos do AWS Network Security Manager (regras, modelos, políticas, escopos e implantações). Você designa uma ou mais contas de administrador, cada uma com uma prioridade de 1 a 10.

- Contas de membros — As contas em que o AWS Network Security Manager descobre recursos, avalia o status da sincronização e, opcionalmente, corrige configurações fora de sincronia. AWS O Network Security Manager atua nas contas dos membros por meio de uma função vinculada ao serviço. Para obter mais informações, consulte the section called “Service-linked papel”.

Opcionalmente, você pode definir o escopo de cada administrador para um subconjunto de contas, OUs e tipos de firewall. Use esse recurso para delegar o gerenciamento de áreas específicas a equipes diferentes.

AWS O Network Security Manager é um serviço regional. Você cria recursos e implantações por região sem dependências entre regiões.

Service-linked papel

AWS O Network Security Manager usa uma função vinculada ao serviço IAM nomeada `AWSServiceRoleForNetworkSecurityManager` para atuar nas contas dos membros da sua organização em seu nome. Essa função confia no diretor `network-security-manager.amazonaws.com` de serviço. Ele usa a política `NetworkSecurityManagerServiceRolePolicy` AWS gerenciada.

AWS O Network Security Manager cria essa função automaticamente quando você ativa o serviço, portanto, não há configuração manual. A função permite que o AWS Network Security Manager gerencie as proteções AWS WAF e AWS Shield Advanced, descubra recursos protegidos por meio do AWS Config e realize operações entre contas. Para obter mais informações, consulte the section called “Service-linked funções”.

Configurar AWS Gerente de segurança de rede

Com o AWS Network Security Manager, você pode trabalhar em dois modelos organizacionais. Use-o diretamente em uma única conta ou use-o com AWS Organizations para gerenciar proteções em várias contas. As etapas de configuração dependem do modelo escolhido.

Tópicos

- Escolha seu modelo organizacional
- Configuração para uso de conta única
- Configurando para uso em várias contas com AWS Organizações
- Criando um AWS Conta de administrador do Network Security Manager
- Crie uma identidade do IAM com AWS Permissões do Network Security Manager
- Utilizar AWS Network Security Manager em regiões que estão desativadas por padrão

Escolha seu modelo organizacional

Escolha entre os seguintes modelos organizacionais:

- Single-account— Use o AWS Network Security Manager para proteger os recursos em uma conta. Você não precisa de AWS Organizations nem de uma conta de administrador. Crie uma identidade do IAM com as permissões do AWS Network Security Manager e comece a usar o serviço diretamente. AWS O Network Security Manager cria automaticamente uma função vinculada ao serviço em sua conta.
- Multi-account— Use o AWS Network Security Manager with AWS Organizations para proteger recursos em várias contas. Esse modo requer a configuração de AWS Organizations, a ativação do acesso confiável e a criação de uma conta de administrador.

Configuração para uso de conta única

Para usar o AWS Network Security Manager em uma única conta, crie uma identidade do IAM com as permissões apropriadas e comece a usar o serviço diretamente. Você não precisa criar uma conta de administrador. AWS O Network Security Manager cria automaticamente uma função vinculada ao serviço em sua conta em segundo plano. Vá para the section called “Crie uma identidade do IAM com AWS Permissões do Network Security Manager”.

Configurando para uso em várias contas com AWS Organizações

Para gerenciar as proteções em várias contas, estabeleça a associação e a configuração necessárias do AWS Organizations.

1. Escolha uma conta para usar como administrador do AWS Network Security Manager para a organização — Essa é a conta a partir da qual você cria e gerencia os recursos do AWS Network Security Manager.
2. Verifique a associação à organização — Se a conta escolhida ainda não for membro da organização, faça com que ela participe. Siga as orientações em Como convidar uma AWS conta para se juntar à sua organização no Guia do Usuário do AWS Organizations.
3. Ative todos os recursos em sua organização — O AWS Organizations tem dois conjuntos de recursos disponíveis: recursos de faturamento consolidado e todos os recursos. Para usar o AWS Network Security Manager, sua organização deve estar habilitada para todos os recursos. Se sua organização estiver configurada somente para faturamento consolidado, siga as orientações em Habilitando todos os recursos em sua organização no Guia do Usuário do AWS Organizations.
4. Habilitar acesso confiável para o AWS Network Security Manager — Habilite o acesso confiável para o AWS Network Security Manager in AWS Organizations. Com o acesso confiável ativado, o AWS Network Security Manager pode criar uma função vinculada ao serviço nas contas dos membros e gerenciar recursos em seu nome.
5. Registre uma conta de administrador delegado — Registre a conta escolhida como administrador delegado do AWS Network Security Manager in Organizations AWS . Use a conta de gerenciamento da Organizations para concluir essa etapa.

⚠ Multi-account proteções desativadas ao desativar o acesso confiável

Se você desativar o acesso confiável ao AWS Network Security Manager in AWS Organizations ou cancelar o registro de uma conta de administrador delegado, o AWS Network Security Manager definirá o escopo e a implantação de várias contas em um `DISABLED` estado e limpará as proteções que ele gerencia.

Criando um AWS Conta de administrador do Network Security Manager

Essa etapa se aplica somente ao modo de várias contas. Somente a conta de gerenciamento da organização pode criar contas de administrador do AWS Network Security Manager.

Depois de concluir a configuração do Organizations, registre sua conta como administrador do AWS Network Security Manager. Você pode fazer isso no console ou na Interface de Linha de AWS Comando (AWS CLI).

Quando você cria uma conta de administrador, o AWS Network Security Manager cria automaticamente uma função vinculada ao serviço em todas as contas da sua organização. Com essa função, o AWS Network Security Manager descobre recursos e gerencia as proteções nas contas dos membros.

Com o AWS Network Security Manager, você pode ter vários administradores que gerenciam os recursos de firewall da sua organização. Se quiser usar vários administradores em sua organização, você pode aplicar condições de escopo administrativo a cada administrador para definir os recursos que eles podem gerenciar. Isso lhe dá a flexibilidade de ter diferentes funções de administrador em sua organização e ajuda a manter o princípio do acesso menos privilegiado. Por exemplo, um administrador pode gerenciar um conjunto de unidades organizacionais (OUs). Outro administrador pode gerenciar somente tipos específicos de políticas.

Para saber o número máximo de administradores que você pode ter por organização, consulte Cotas.

> **Registro de região**
>
> Você registra uma conta de administrador do AWS Network Security Manager em uma única AWS região. Para usar o AWS Network Security Manager em regiões adicionais, repita essa etapa em cada região.

Para criar uma conta de administrador usando o console

1. Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.

2. No painel de navegação, selecione Configurações.
3. Escolha Adicionar administrador.
4. Selecione a conta e insira um valor de prioridade (1 a 10).
5. Escolha Adicionar administrador para confirmar.

Para criar uma conta de administrador usando o AWS CLI

Chame a operação `PutAdminAccount`. Você deve fornecer um valor de prioridade (1 a 10).

O exemplo de AWS CLI a seguir registra uma conta como administrador do AWS Network Security Manager com prioridade 1:

```
aws network-security-manager put-admin-account \
    --account-id 123456789012 \
    --priority 1
```

Você pode designar várias contas de administrador, cada uma com uma prioridade diferente. Opcionalmente, você pode limitar cada administrador a contas específicas, OUs ou tipos de firewall fornecendo um `adminScope` parâmetro.

Para remover uma conta de administrador usando o console

> ⚠ Multi-account proteções desativadas ao remover um administrador
>
> Quando você remove uma conta de administrador, o AWS Network Security Manager define o escopo e a implantação de várias contas em um `DISABLED` estado e limpa as proteções que ele gerencia.

1. Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.
2. No painel de navegação, selecione Configurações.
3. Selecione a conta de administrador que você deseja remover.
4. Escolha Remove administrator (Remover administrador).
5. Para confirmar, escolha Confirmar exclusão do administrador.

Crie uma identidade do IAM com AWS Permissões do Network Security Manager

Para usar o AWS Network Security Manager, você precisa de uma identidade do IAM (usuário ou função) com permissões para chamar as operações do AWS Network Security Manager. As ações do IAM usam o prefixo`network-security-manager`.

O exemplo de política do IAM a seguir contém três declarações. A primeira declaração concede acesso total a todas as operações do AWS Network Security Manager. A segunda declaração concede as permissões adicionais de AWS Organizations e AWS WAF de que o AWS Network Security Manager precisa. AWS O Network Security Manager usa essas permissões para identificar as contas e unidades organizacionais (OUs) em sua organização e para listar os grupos de regras do WAF e os produtos gerenciados disponíveis. Essas permissões também permitem que o AWS Network Security Manager habilite o acesso confiável e registre um administrador delegado no AWS Organizations. A terceira declaração concede a `iam:CreateServiceLinkedRole` permissão que o AWS Network Security Manager precisa para criar sua função vinculada ao serviço, necessária tanto para o uso de uma conta única quanto de várias contas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "network-security-manager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "wafv2:ListRuleGroups",
                "wafv2:ListAvailableManagedRuleGroups",
                "wafv2:DescribeAllManagedProducts"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*"
        }
    ]
}
```

Para uso em produção, recomendamos que você conceda somente as permissões mínimas necessárias. Para obter mais informações, consulte the section called “Gerenciamento de identidade e acesso”.

Inscreva-se para um Conta da AWS

Para começar AWS, você precisa de um Conta da AWS. Para obter informações sobre como criar um Conta da AWS, consulte Introdução a um Conta da AWS no Guia de AWS Gerenciamento de contas referência.

Utilizar AWS Network Security Manager em regiões que estão desativadas por padrão

Para usar o AWS Network Security Manager em uma região que está desabilitada por padrão, você deve habilitar a Região tanto para a conta de gerenciamento da sua organização quanto para a conta de administrador do AWS Network Security Manager. Para obter informações sobre regiões que estão desativadas por padrão e como habilitá-las, consulte Gerenciando AWS regiões na Referência AWS geral.

Para habilitar uma região desabilitada

Tanto para a conta de gerenciamento do Organizations quanto para a conta de administrador do AWS Network Security Manager, siga as orientações em Habilitando uma Região na Referência AWS Geral.

Implemente sua primeira proteção de segurança de rede

Este tutorial explica como implantar uma Web ACL do AWS WAF usando o console do AWS Network Security Manager. Você conclui as seguintes etapas:

1. Criar uma regra
2. Criar um modelo
3. Criar uma política
4. Criar um escopo
5. Crie e publique uma implantação
6. Monitore o status da sincronização

Neste tutorial, você cria uma AWS WAF web ACL que protege os Application Load Balancers nas contas selecionadas. Esse processo é praticamente idêntico para todos os serviços de segurança e firewalls suportados pelo AWS Network Security Manager.

Tempo para concluir: aproximadamente 10 minutos

Custo: este tutorial usa AWS serviços que podem incorrer em cobranças. Para obter os preços atuais, consulte os preços do AWS Network Security Manager no AWS site.

Pré-requisitos

Antes de começar, verifique se você atende aos seguintes requisitos:

- Etapas de configuração concluídas conforme descrito emConfigurando o AWS Network Security Manager.
- Uma AWS identidade do Identity and Access Management (IAM) AWS com permissões do Network Security Manager.
- Uma organização da AWS Organizations com todos os recursos habilitados e uma conta de administrador designada do AWS Network Security Manager (necessária para implantações com várias contas).
- Acesso ao console do AWS Network Security Manager.

Etapa 1: criar uma regra

Uma regra é o alicerce da sua configuração de segurança. Nesta etapa, você cria duas regras do AWS WAF: uma que define a ação padrão e outra que define a configuração de visibilidade. Ação padrão e VisibilityConfig são campos obrigatórios para uma Web ACL AWS do WAF.

Para criar a regra de ação padrão, siga estas etapas:

1. Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.
2. No painel de navegação, selecione Visão geral.
3. Na página Visão geral, escolha Criar regra.
4. Em Nome da regra, insira um nome descritivo, como `my-default-action-rule`.
5. Na seção Definição de regra, em Tipo de firewall, escolha AWS WAF.
6. Em Selecionar tipo de regra, escolha Configuração.
7. Escolha Inserir tipos de configuração e, em seguida, selecione Ação padrão. Um editor JSON aparece com uma configuração padrão.
8. No editor JSON, remova a `Block` seção e mantenha somente a `Allow` seção.
9. Escolha Criar regra.

Para criar a VisibilityConfig regra, siga estas etapas:

1. No painel de navegação, selecione Visão geral.
2. Na página Visão geral, escolha Criar regra.
3. Em Nome da regra, insira um nome descritivo, como `my-visibility-config-rule`.
4. Na seção Definição de regra, em Tipo de firewall, escolha AWS WAF.
5. Em Selecionar tipo de regra, escolha Configuração.
6. Escolha Inserir tipos de configuração e, em seguida, selecione VisibilityConfig. Um editor JSON aparece com uma configuração padrão.
7. Escolha Criar regra.

> **AWS Alternativa de CLI**
>
> Você também pode criar regras com a AWS CLI:

```
aws network-security-manager create-rule \
    --rule-name "my-default-action-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"DefaultAction": {"Allow": {}}}' \
    --is-published true

aws network-security-manager create-rule \
    --rule-name "my-visibility-config-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true,
 "CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \
    --is-published true
```

Etapa 2: criar um modelo

Um modelo agrupa uma ou mais regras para reutilização em todas as políticas. Nesta etapa, você cria um modelo que inclui a regra da Etapa 1:

1. No painel de navegação, selecione Visão geral.
2. Na página Visão geral, escolha Criar modelo.
3. Em Nome do modelo, insira um nome descritivo, como`my-waf-template`.
4. Para Tipo de firewall, escolha AWS WAF.
5. Na seção Regras, escolha Adicionar regra e selecione as regras que você criou na Etapa 1.
6. Selecione Criar modelo.

AWS Alternativa de CLI

Você também pode criar um modelo com a AWS CLI:

```
aws network-security-manager create-template \
    --template-name "my-waf-template" \
    --firewall-type WAF \
    --associated-rule-list '[{"ruleIdentifier": "rule-arn-from-step-1"}]' \
```

```
    --is-published true
```

Etapa 3: criar uma política

Uma política combina modelos com configurações de fiscalização. Nesta etapa, você cria uma política que faz referência ao seu modelo e permite a correção automática:

1. No painel de navegação, selecione Visão geral.
2. Na página Visão geral, escolha Criar política.
3. Em Nome da política, insira um nome descritivo, como `my-waf-policy`.
4. Para Tipo de firewall, escolha AWS WAF.
5. Na seção Prioridade da política, as políticas existentes e suas prioridades são exibidas. Analise a prioridade da nova política. Se precisar ajustá-lo, escolha o campo de prioridade e altere o valor para 1 ou qualquer número de prioridade não utilizado.
6. Na seção Modelos e regras, escolha Adicionar modelo e selecione o modelo que você criou na Etapa 2.
7. Para Remediação, selecione Ativado.
8. Para Resolução de ACL na web do cliente existente, escolha Sem remediação.
9. Selecione Criar política.

AWS Alternativa de CLI

Você também pode criar uma política com a AWS CLI:

```
aws network-security-manager create-policy \
    --policy-name "my-waf-policy" \
    --firewall-type WAF \
    --priority 1 \
    --associated-template-and-rule-list '[{"templateIdentifier": "template-arn-
from-step-2"}]' \
    --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":
 false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \
    --is-published true
```

Etapa 4: criar um escopo

Um escopo define onde suas proteções se aplicam. Nesta etapa, você cria um escopo que tem como alvo os Application Load Balancers em suas contas:

1. No painel de navegação, selecione Visão geral.
2. Na página Visão geral, escolha Criar escopo.
3. Em Nome do escopo, insira um nome descritivo, como`my-alb-scope`.
4. (Opcional) Na seção Seleção de conta e unidade organizacional, em Selecionar método de controle do escopo administrativo, selecione Escopo para toda a AWS organização (todas as OUs e contas). Ignore esta etapa para implantações com uma única conta.
5. Na seção Recursos, em Tipos de recursos, selecione Application Load Balancer.
6. Escolha Create scope (Criar escopo).

AWS Alternativa de CLI

Você também pode criar um escopo com a AWS CLI:

```
aws network-security-manager create-scope \
    --scope-name "my-alb-scope" \
    --scope-configuration '{
        "accountFilter": {"includeAll": {}},
        "resourceScopes": {
            "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {
                "includeAll": true
            }
        }
    }' \
    --is-published true
```

Etapa 5: criar e publicar uma implantação

Uma implantação vincula políticas a um escopo e ativa a fiscalização. Para criar e publicar uma implantação:

1. No painel de navegação, selecione Visão geral.

2. Na página Visão geral, escolha Criar implantação.
3. Em Nome da implantação, insira um nome descritivo, como`my-first-deployment`.
4. Na seção Políticas, escolha Adicionar política e selecione a política que você criou na Etapa 3.
5. Na seção Escopos, escolha Adicionar escopo e selecione o escopo que você criou na Etapa 4.
6. Escolha Criar implantação.

AWS O Network Security Manager começa a descobrir recursos e a aplicar proteções. Esse processo é assíncrono e pode levar alguns minutos para ser concluído.

> **AWS Alternativa de CLI**
>
> Você também pode criar e publicar uma implantação com a AWS CLI:

```
aws network-security-manager create-deployment \
    --deployment-name "my-first-deployment" \
    --associated-policy-list '[{"policyIdentifier": "policy-arn-from-step-3"}]'
 \
    --associated-scope-list '[{"scopeIdentifier": "scope-arn-from-step-4"}]' \
    --deployment-configuration '{"enableCrossAccountVisibility": true}' \
    --is-published true
```

Etapa 6: Monitorar o status da sincronização

Depois de publicar uma implantação, o AWS Network Security Manager descobre recursos e sincroniza suas configurações. Para monitorar o status de cada recurso:

1. No painel de navegação, selecione Visão geral.
2. Escolha a guia Grupos de implantação.
3. Escolha a implantação que você criou na Etapa 5.
4. Escolha a guia Sincronização.
5. Revise o status da sincronização de cada recurso:
   - IN_SYNC — A configuração do recurso corresponde às configurações de proteção pretendidas.
   - OUT_OF_SYNC — A configuração do recurso não corresponde. AWS O Network Security Manager corrige isso automaticamente quando a correção está ativada.

- NOT_APPLICABLE — O recurso está no escopo, mas não pode ser avaliado por essa implantação.

> **AWS Alternativa de CLI**
>
> Você também pode verificar o status da sincronização com a AWS CLI:
>
> ```
> aws network-security-manager list-resource-synchronization-statuses \
>     --deployment-identifier "deployment-arn-from-step-5"
> ```

Etapa 7: limpar

Se você não precisar mais dos recursos criados, exclua-os na ordem inversa para interromper a aplicação e remover as proteções dos recursos dentro do escopo:

A ordem inversa é importante porque esses recursos fazem referência uns aos outros. Para ver o que está associado a um recurso antes de excluí-lo, chame `ListResourceAssociations` com o ARN desse recurso. Ele retorna o ARN e o tipo de recurso de cada recurso associado. Para obter mais informações, consulte a Referência da API do AWS Network Security Manager.

1. No painel de navegação, selecione Visão geral. Escolha a guia Grupos de implantação. Selecione sua implantação, escolha Ação e, em seguida, escolha Excluir.
2. Escolha a guia Escopos. Selecione seu escopo, escolha Ação e, em seguida, escolha Excluir.
3. Escolha a guia Políticas. Selecione sua política, escolha Ação e, em seguida, escolha Excluir.
4. Escolha a guia Modelos. Selecione seu modelo, escolha Ação e, em seguida, escolha Excluir.
5. Escolha a guia Rules. Selecione sua regra, escolha Ação e, em seguida, escolha Excluir.

> **AWS Alternativa de CLI**
>
> Antes de excluir um recurso, verifique suas associações para planejar a ordem de exclusão:
>
> ```
> aws network-security-manager list-resource-associations \
>     --resource-arn "resource-arn"
> ```
>
> Se um recurso ainda tiver associações, primeiro remova ou exclua os recursos associados.

Você pode excluir recursos com a AWS CLI na ordem inversa:

```
aws network-security-manager delete-deployment \
    --deployment-identifier "deployment-arn"

aws network-security-manager delete-scope \
    --scope-identifier "scope-arn"

aws network-security-manager delete-policy \
    --policy-identifier "policy-arn"

aws network-security-manager delete-template \
    --template-identifier "template-arn"

aws network-security-manager delete-rule \
    --rule-identifier "rule-arn"
```

Próximas etapas

Agora que você tem uma implantação em funcionamento, explore as seguintes formas de expandir sua proteção de segurança de rede:

- Saiba mais sobre o modelo de recursos e o ciclo de vida em. Como funciona o AWS Network Security Manager
- Use o draft/publish fluxo de trabalho para preparar as alterações antes que elas entrem em vigor. Para obter mais informações, consulte the section called “Ciclo de vida preliminar e ativo”.
- Crie instantâneos para preservar configurações em boas condições. Para obter mais informações, consulte the section called “Versionamento”.
- Use `GenerateRuleConfiguration` para criar regras a partir de descrições em linguagem natural. Para obter mais informações, consulte a Referência da API do AWS Network Security Manager.
- Explore o gerenciamento das proteções AWS WAF e AWS Shield Advanced em toda a sua organização. Para obter mais informações, consulte Gerenciando firewalls e serviços de segurança.

Gerenciando firewalls e serviços de segurança

Com o AWS Network Security Manager, você define e implanta políticas de segurança para vários firewalls e serviços de segurança. Embora elementos comuns abranjam o portfólio de segurança de AWS rede, existem variações importantes que você precisa abordar no AWS Network Security Manager.

Para cada serviço de segurança de rede compatível, as subseções a seguir descrevem os elementos e etapas exclusivos de uma Criação Rápida e de um processo de criação padrão detalhado.

Gerenciando ACLs da web para AWS WAF

Com o AWS Network Security Manager, você configura e implanta centralmente as listas de controle de acesso à web (ACLs da web) do AWS WAF em todas as contas e recursos da sua organização. Você pode definir as regras do AWS Network Security Manager para o AWS WAF, agrupá-las em modelos de proteção e aplicá-las em grande escala por meio de políticas e implantações do AWS Network Security Manager.

AWS Conceitos do WAF

Os conceitos a seguir são específicos para usar o AWS Network Security Manager com o AWS WAF. Para obter mais informações sobre como o AWS Network Security Manager funciona, consulteComo funciona o AWS Network Security Manager.

AWS Tipos de regras do WAF

Para o AWS WAF, uma regra é de dois tipos:

- INSPEÇÃO — Contém uma definição de grupo de regras usando `PreProcessFirewallManagerRuleGroups` (regras que são executadas antes das regras definidas pelo cliente) ou `PostProcessFirewallManagerRuleGroups` (regras que são executadas depois).
- CONFIGURAÇÃO — Contém uma única configuração de ACL da web. O JSON de configuração deve conter exatamente uma chave de nível superior correspondente a uma configuração compatível (por

exemploDescription,DefaultAction,VisibilityConfig,LoggingConfiguration,CaptchaCon
AssociationConfig OnSourceDDoSProtectionConfigTokenDomains,
ouMonetizationConfig).

A maioria das configurações da Web ACL corresponde aos parâmetros da operação do AWS WAF. CreateWebACL Para obter mais informações sobre essas configurações e suas definições, consulte CreateWebACL na Referência da API AWS WAF.

A exceção éLoggingConfiguration, que você configura separadamente. Para obter mais informações, consulte the section called “Registro em log”.

AWS Fusão de políticas do WAF

Para o AWS WAF, cada configuração usa uma das seguintes estratégias de mesclagem:

SingleValue

Configurações que podem ter somente um valor. A política de maior prioridade vence. Os valores de prioridade são exclusivos, portanto, duas políticas não podem definir valores diferentes na mesma prioridade. Para obter mais informações sobre como o AWS Network Security Manager resolve a prioridade, consultethe section called “Priority-based fusão de políticas”. As configurações a seguir usam SingleValue: DefaultAction VisibilityConfigCaptchaConfig,ChallengeConfig,OnSourceDDoSProtectionConfig,Logg Description e.

Anexar (e) AppendAndSort

As entradas de todas as políticas são anexadas à lista em ordem de prioridade. TokenDomainse DataProtectionConfig.DataProtections use Append. PreProcessFirewallManagerRuleGroupse PostProcessFirewallManagerRuleGroups use AppendAndSort, que acrescenta grupos de regras de todas as políticas e os classifica por prioridade. A ordem é importante porque o AWS WAF avalia grupos de regras sequencialmente.

Mesclar

As entradas de todas as políticas se mesclam em um único conjunto, independentemente da prioridade. CustomResponseBodiese AssociationConfig.RequestBody use Merge.

As estratégias Anexar AppendAndSort, e Mesclar removem entradas duplicadas. Quando duas políticas contribuem com uma configuração idêntica, o AWS Network Security Manager mantém a

entrada da política de maior prioridade. Portanto, a configuração efetiva contém uma cópia dessa entrada, não uma cópia por política de contribuição.

Resolução de ACL da web existente

Use a `existingCustomerWebACLResolution` configuração em uma política de AWS WAF para especificar como o AWS Network Security Manager lida com recursos que já têm uma Web ACL gerenciada pelo cliente:

- `RETROFIT`— Atualize sua ACL da web existente para se alinhar à configuração efetiva.
- `OVERRIDE_ASSOCIATION`— Em vez disso, associe uma ACL da web gerenciada pelo AWS Network Security Manager ao recurso.
- `NO_REMEDIATION`— Não corrija se sua ACL da web existir.

Log de tráfego da web ACL

Você controla o registro de ACL da web com a `LoggingConfiguration` configuração de uma política. AWS O Network Security Manager aplica essa configuração usando a `PutLoggingConfiguration` operação AWS WAF. É possível definir um destino de registro em log por ACL da Web. Para obter mais informações, consulte PutLoggingConfigurationa Referência da API AWS WAF.

Cada ACL da web dentro do escopo que a política gerencia envia seus registros para o destino especificado pela política. Isso proporciona um registro centralizado em todas as contas da sua organização. Use-o para obter informações detalhadas sobre o tráfego que suas ACLs da web analisam em toda a organização.

Para o registro centralizado em várias contas, você pode enviar registros para um bucket do Amazon S3 ou para um stream de entrega do Amazon Data Firehose. Cada tipo de destino requer configuração adicional, que você deve concluir antes que o AWS Network Security Manager possa gerenciar o registro do AWS WAF em seus recursos e contas dentro do escopo. O nome do destino deve começar com`aws-waf-logs-`.

Amazon Data Firehose

Crie o fluxo de entrega com as seguintes características:

- Criado usando sua conta de administrador do AWS Network Security Manager

- Um nome que começa com `aws-waf-logs-`, por exemplo `aws-waf-logs-network-security-manager-central`
- Uma PUT fonte
- Criado na região em que você opera ou na região Leste dos EUA (Norte da Virgínia) se você capturar registros para a Amazon CloudFront

Antes de usar o stream de entrega, teste-o para confirmar se ele tem taxa de transferência suficiente para os registros da sua organização. Para obter mais informações, consulte Criação de um stream de entrega do Amazon Data Firehose no Guia do desenvolvedor do Amazon Data Firehose.

Amazon S3

Crie o bucket seguindo as orientações do Amazon S3 no Guia do desenvolvedor do AWS WAF. Você também deve configurar o bucket com as permissões que permitem que a entrega do log grave nele. A política de bucket a seguir concede essas permissões.

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryForNetworkSecurityManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
        },
        {
            "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
```

```
                }
            }
        }
    ]
}
```

*bucket-suffix*Substitua pelo seu próprio sufixo de nome de bucket e *policy-id* substitua pelo ID da sua política.

> **CloudWatch O Logs suporta somente o uso de uma única conta**
>
> Se você usa o AWS Network Security Manager em várias contas, não pode usar um grupo de CloudWatch logs do Amazon Logs como destino de registro. O grupo de registros deve estar na mesma AWS conta e na mesma região da ACL da web. Para implantações com várias contas, use um bucket Amazon S3 ou um stream de entrega do Amazon Data Firehose em vez disso.

Criação rápida para AWS WAF

Com o Quick Create, você define e implanta proteções AWS WAF em um único fluxo de trabalho guiado. Use a Criação Rápida quando quiser configurar uma proteção completa da Web ACL contra regras até a implantação em uma sessão.

Para definir e implantar uma proteção AWS WAF com o Quick Create, conclua os procedimentos a seguir na ordem.

Para criar a política e adicionar proteções

1. Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.
2. No painel de navegação, selecione Visão geral.
3. No canto superior direito da página Visão geral, escolha Criação e implantação rápidas. A página de criação e implantação rápidas aparece com vários painéis.
4. No painel Detalhes da política, em Nome, insira um nome de política. (Opcional) Em Description (Descrição), insira uma descrição.

5. No painel Definir proteções, escolha o tipo de firewall com o qual você deseja trabalhar. Selecione AWS WAF. Um subpainel Modelos e regras é exibido, onde você pode adicionar regras ou modelos.
6. Para adicionar regras, escolha Adicionar ou gerenciar regras. Na janela exibida, em Selecionar tipo de regra, escolha uma das seguintes opções:
   - AWS Regras gerenciadas — A tabela mostra todas as regras AWS gerenciadas que o AWS WAF suporta.
   - Regras — A tabela mostra os grupos de regras do AWS WAF que você possui, além das Regras AWS Gerenciadas.

   Marque as caixas de seleção das regras que você deseja adicionar à sua política. Em seguida, escolha Adicionar regras.
7. Para adicionar modelos, escolha Adicionar modelos. Na janela Adicionar modelos exibida, a tabela exibe todos os modelos disponíveis. Selecione os modelos que você deseja, junto com a versão a ser incluída na política. Em seguida, escolha Adicionar modelos.

Para configurar a política

1. Revise suas seleções na tabela Modelos e regras. O número inteiro na coluna Posição determina a ordem de avaliação das regras e modelos. Para alterar a ordem de avaliação, escolha o valor da posição na coluna Posição. Use as setas para alterar o valor. Para aceitar a alteração, escolha Confirmar. Para reverter a alteração, escolha Cancelar.
2. Em Configuração de política no painel Definir proteções, decida as ações automatizadas que o AWS Network Security Manager executará no escopo de destino:
   - A remediação aplica a política definida a todos os recursos cujo estado de segurança não esteja sincronizado com o estado desejado descrito no AWS Network Security Manager.
   - A limpeza de recursos exclui o firewall que o AWS Network Security Manager criou para um recurso quando a implantação é removida ou quando a conta ou o recurso está fora do escopo.
   - A resolução existente do WebACL do cliente determina como resolver conflitos entre a política que você está definindo e o que já pode estar implantado. No menu, escolha uma das seguintes opções:
     - Nenhuma remediação ignora a remediação em qualquer recurso que já tenha uma ACL da web.

- A associação de substituição substitui a ACL da web existente pela ACL da web criada pelo AWS Network Security Manager.
- O Retrofit adapta suas regras a cada ACL da web existente e mantém a ACL da web associada ao recurso.

3. No painel Prioridade da política, defina a prioridade. AWS O Network Security Manager avalia as políticas de acordo com sua prioridade para resolver conflitos. Posições mais baixas (números inteiros mais baixos) têm maior prioridade. Para editar a prioridade, escolha o valor da Posição. Em seguida, incremente-o com as setas ou insira um valor diretamente. Para confirmar a seleção, escolha Confirmar. Para descartar a alteração, escolha Cancelar.

Para definir o escopo

1. No painel Definir o escopo, defina o conjunto de ativos aos quais as políticas se aplicam. Em Nome do escopo, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição.
2. Multi-account somente modo

   Essa etapa se aplica somente ao modo de várias contas. No modo de várias contas, use o subpainel Seleção de conta e unidade organizacional para escolher quais contas ou OUs incluir ou excluir. No modo de conta única, esse subpainel não aparece no console, então pule esta etapa.

   No subpainel de seleção de conta e unidade organizacional, selecione uma das seguintes opções:

   - Escopo para toda a AWS organização. Nenhuma definição adicional é necessária.
   - Abrange toda a AWS organização, mas exclui contas e OUs específicas. Um subpainel Unidades organizacionais e um subpainel Contas são exibidos. Para excluir unidades organizacionais, escolha Adicionar OUs. Selecione as unidades organizacionais na árvore organizacional e escolha Adicionar OUs. Para excluir contas individuais, escolha Adicionar contas. Selecione as contas na árvore da organização e escolha Adicionar contas.
   - Não abranja toda a AWS organização e inclua apenas OUs e contas específicas. Use o mesmo mecanismo Adicionar OUs e Adicionar contas para incluir as unidades organizacionais e as contas que você deseja.

3. No subpainel Recursos, em Tipos de recursos, selecione todos os tipos de recursos do AWS WAF ou tipos específicos. As opções são uma ou mais das seguintes:

- Application Load Balancer
- API REST do Amazon API Gateway
- CloudFront Distribuição

> **CloudFront Requisito de região**
>
> Para proteger os recursos CloudFront de distribuição, use a Região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

> **Tipos de recursos globais e regionais**
>
> Você pode selecionar o tipo de recurso global (CloudFront Distribuição) ou os tipos de recursos regionais (Application Load Balancer e API REST do Amazon API Gateway), mas não ambos. Depois de selecionar um tipo de recurso, você não poderá alternar entre os tipos de recursos regionais e de CloudFront distribuição ao atualizar a configuração.

> **Recursos não gerenciados CloudFront**
>
> AWS O Network Security Manager não gerencia CloudFront distribuições que usam o CloudFront plano de preços fixos ou distribuições CloudFront intermediárias. Esses recursos aparecem fora de sincronização.

4. Para cada tipo de recurso selecionado, escolha uma das seguintes opções mutuamente exclusivas:
   - Incluir todos os recursos
   - Inclua recursos específicos
   - Excluir recursos específicos
5. Se você escolher Incluir recursos específicos, escolha um dos seguintes tipos de expressão e, em seguida, crie as combinações apropriadas de tags ou ARNs:
   - Critério único
   - Atenda a todos os critérios (AND)
   - Atenda a qualquer critério (OR)
   - NÃO

Todos os tipos de recursos têm os critérios de inclusão de Tag e ARN. Se você escolher Tag, insira uma chave e um valor opcional. Você pode identificar várias tags. Se seu tipo de recurso for um Application Load Balancer, um critério de configuração adicional será exibido. Em Configuração, escolha um Esquema, que tenha as opções Internet-facingou Interno.

Para revisar e implantar a política

1. No painel Revisar e implantar, em Nome da implantação, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição. Para determinar se o conteúdo da sua implantação está visível para outras contas em sua organização, selecione Habilitar visibilidade entre contas para esta implantação.
2. (Opcional) Para adicionar tags ao seu recurso, escolha Adicionar nova tag e insira combinações de chave e valor opcionais.
3. Para executar o que você definiu, escolha Criar e implantar. Quando o processo estiver concluído, a página Implantações será exibida, onde você poderá ver os detalhes do que foi criado.

⚠ As implantações podem incorrer em cobranças

Uma implantação cria serviços de segurança de rede e os conecta a um recurso protegido. AWS O Network Security Manager cobra pelos recursos protegidos. Os próprios serviços de segurança protegem o recurso, o que acarreta custos adicionais. Antes da implantação, consulte a página de preços do AWS Network Security Manager e a página de preços do AWS WAF.

Processo de criação padrão para AWS WAF

Com o processo de criação padrão, você cria cada componente do AWS WAF — regras, modelos, políticas, escopos e implantações — individualmente para controle total. Use essa abordagem quando quiser criar componentes reutilizáveis e combiná-los conforme necessário.

Uma política AWS WAF do AWS Network Security Manager pode conter regras e modelos. Quando você aplica a política, o AWS Network Security Manager cria uma Web ACL em cada conta dentro do escopo.

Para criar uma regra (console)

1. Entre no Console AWS de Gerenciamento usando sua conta de administrador do AWS Network Security Manager e, em seguida, abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.

   > **Configuração da conta de administrador**
   >
   > Para obter informações sobre como configurar uma conta de administrador do AWS Network Security Manager, consulteConfigurando o AWS Network Security Manager.

2. No painel de navegação, escolha AWS Network Security Manager e, em seguida, Visão geral.
3. No painel Visão geral, escolha Criar regra. Insira um nome descritivo e, em seguida, insira uma Descrição opcional.
4. No painel Definição de regra, em Tipo de firewall, escolha AWS WAF.
5. Em Tipo de regra, escolha Inspeção ou Configuração.

   Se você escolher Inspeção, um painel do editor JSON chamado Definir referência do grupo de regras aparecerá com as seguintes opções:

   - Inserir modelo — Selecione um modelo JSON para as regras First (pré-processamento) ou Last (pós-processamento). Quando você faz uma seleção, o AWS Network Security Manager insere o JSON correspondente no editor, junto com ícones de aviso, caso sejam necessárias entradas para preencher o modelo.
   - Inserir grupo de regras — Apresenta uma lista de seleção orientada por três opções:
     - Um grupo de regras de regras AWS gerenciadas (AMR)
     - Um grupo de regras personalizadas existente
     - Um grupo de regras AWS do Marketplace

     AWS O Network Security Manager apresenta os grupos de regras associados à sua escolha, e você pode selecionar uma única instância para inclusão. Depois de fazer a seleção, escolha Selecionar grupo de regras. AWS O Network Security Manager insere referências à regra de inspeção com a sintaxe correta no editor JSON.
   - Inserir com IA — Abre uma janela de sobreposição chamada gerador de configuração de IA. Use essa ferramenta para descrever sua regra em linguagem simples, e o AWS Network Security Manager gera o JSON associado no editor. Em seguida, você pode revisar o código gerado e optar por aceitar, modificar ou excluir a saída.

6. (Opcional) Depois que a definição da regra JSON for concluída, você poderá associar uma tag à sua regra. Escolha Add new tag (Adicionar nova etiqueta) e insira Key (Chave) e uma opção de Value (Valor) opcional.
7. Ao concluir suas definições, escolha Salvar rascunho para salvar um objeto inativo e potencialmente incompleto ou Criar regra.

> ⚠ Os nomes da Web ACL são permanentes
>
> Você não pode alterar o nome de uma Web ACL depois de criá-la. Se você atualizar o nome da sua política, o AWS Network Security Manager não atualizará o nome da Web ACL associada. Para que o AWS Network Security Manager crie uma Web ACL com um nome diferente, você deve criar uma nova política.

Para criar um modelo (console)

Um modelo reúne regras em ordem de prioridade para avaliação dentro de uma política. Você pode organizar seus tipos de regras em grupos alinhados às suas metas de segurança. Você também pode permitir que equipes diferentes criem declarações de controle de segurança que se alinhem às suas responsabilidades e habilidades.

1. Na página Visão geral, no painel Visão geral, escolha Criar modelo. Na página Criar modelo, insira um nome de modelo, insira uma Descrição opcional e escolha um tipo de firewall (nesse caso, AWS WAF).
2. Quando você escolhe um tipo de firewall, o painel Regras é exibido. Escolha um dos dois botões Adicionar regras para abrir uma lista das regras disponíveis. Marque a caixa de seleção à esquerda do Nome de uma regra para adicioná-la ao modelo. Para escolher uma versão específica de uma regra, selecione o campo Versão da regra. Se várias versões estiverem disponíveis, selecione a versão desejada e escolha Confirmar.
3. (Opcional) Crie uma tag para o modelo. Ao terminar, escolha Salvar rascunho ou Criar modelo. Para continuar criando uma política, escolha Criar modelo.

Para criar uma política do (console)

Essa é a etapa final da definição da política e da preparação para a implantação.

1. Na página Visão geral, no painel Visão geral, escolha Criar política. Na página Criar política, insira um Nome e uma Descrição opcional e escolha um tipo de Firewall (nesse caso, AWS WAF).
2. No painel Prioridade da política, defina a prioridade. AWS O Network Security Manager avalia as políticas de acordo com sua prioridade para resolver conflitos. Posições mais baixas (números inteiros mais baixos) têm maior prioridade. Para editar a prioridade, escolha o valor da Posição. Em seguida, incremente-o com as setas ou insira um valor diretamente. Para confirmar a seleção, escolha Confirmar. Para descartar a alteração, escolha Cancelar.
3. No painel Configuração da política, decida as ações automatizadas que o AWS Network Security Manager executa no escopo de destino:
   - A remediação aplica a política definida a todos os recursos cujo estado de segurança não esteja sincronizado com o estado desejado descrito no AWS Network Security Manager.
   - A limpeza de recursos exclui o firewall que o AWS Network Security Manager criou para um recurso quando a implantação é removida ou quando a conta ou o recurso está fora do escopo.
   - A resolução existente do WebACL do cliente determina como resolver conflitos entre a política que você está definindo e o que já pode estar implantado. No menu, escolha uma das seguintes opções:
     - Nenhuma remediação ignora a remediação em qualquer recurso que já tenha uma ACL da web.
     - A associação de substituição substitui a ACL da web existente pela ACL da web criada pelo AWS Network Security Manager.
     - O Retrofit adapta suas regras a cada ACL da web existente e mantém a ACL da web associada ao recurso.
4. Depois que essas configurações forem concluídas, selecione as regras e os modelos que você deseja adicionar à política. No painel Modelos e regras, escolha Adicionar regras ou Adicionar modelos para preencher a política. Ambos os processos abrem uma janela que opera da mesma forma que o processo de seleção de regras descrito anteriormente nesta seção.

Para criar um escopo (console)

1. Você pode iniciar essa etapa na página Visão geral ou em outras áreas da ferramenta. No painel Detalhes do escopo, insira um nome do escopo e uma descrição opcional.

2. **Multi-account somente modo**

   Essa etapa se aplica somente ao modo de várias contas. No modo de várias contas, use o subpainel Seleção de conta e unidade organizacional para escolher quais contas ou OUs incluir ou excluir. No modo de conta única, esse subpainel não aparece no console, então pule esta etapa.

   No painel Seleção de conta e unidade organizacional, escolha um dos três métodos para controlar o escopo administrativo:

   - Escopo para toda a AWS organização (todas as OUs e contas) — Nenhuma definição adicional é necessária.
   - Abrange toda a AWS organização, mas exclui contas e OUs específicas — Dois subpainéis aparecem, um para unidades organizacionais e outro para contas. Escolha Adicionar OUs para abrir a janela Adicionar OUs, selecione as unidades organizacionais necessárias na árvore organizacional e escolha Adicionar OUs. Para adicionar contas individuais, no subpainel Contas, escolha Adicionar contas, selecione as contas na árvore organizacional e escolha Adicionar contas.
   - Não abranja toda a AWS organização, inclua apenas OUs e contas específicas — use os mesmos subpainéis para adicionar OUs ou contas com o mesmo mecanismo descrito na opção anterior.

3. Em seguida, selecione recursos no subpainel Recursos. Na caixa de seleção Tipos de recursos, selecione todos os tipos de recursos do AWS WAF ou tipos específicos. Para o AWS WAF, as opções são uma ou todas as seguintes:

   - Application Load Balancer
   - API REST do Amazon API Gateway
   - CloudFront Distribuição

   CloudFront Requisito de região

   Para proteger os recursos CloudFront de distribuição, use a Região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

> **Tipos de recursos globais e regionais**
>
> Você pode selecionar o tipo de recurso global (CloudFront Distribuição) ou os tipos de recursos regionais (Application Load Balancer e API REST do Amazon API Gateway), mas não ambos. Depois de selecionar um tipo de recurso, você não poderá alternar entre os tipos de recursos regionais e de CloudFront distribuição ao atualizar a configuração.

> **Recursos não gerenciados CloudFront**
>
> AWS O Network Security Manager não gerencia CloudFront distribuições que usam o CloudFront plano de preços fixos ou distribuições CloudFront intermediárias. Esses recursos aparecem fora de sincronização.

4. Para cada tipo de recurso selecionado, escolha uma das seguintes opções mutuamente exclusivas:
   - Incluir todos os recursos
   - Inclua recursos específicos
   - Excluir recursos específicos
5. Se você escolher Incluir recursos específicos, selecione um dos seguintes tipos de expressão:
   - Critério único
   - Atenda a todos os critérios (AND)
   - Atenda a qualquer critério (OR)
   - NÃO
6. Cada tipo de expressão oferece suporte a um ou vários critérios de inclusão e ARNs, para que você possa criar combinações de tags ou ARNs. Todos os tipos de recursos são compatíveis com os critérios de inclusão de tags e ARN. Se você escolher Tag, identifique uma chave e um valor opcional. Você pode identificar várias tags.
7. Para um Application Load Balancer, aparece um critério de configuração adicional. Em Configuração, você pode definir um esquema com as opções Internet-facingou Interno.

Para criar uma implantação (console)

Uma implantação vincula suas políticas a um escopo e ativa a fiscalização, o que faz com que o AWS Network Security Manager aplique suas regras de AWS WAF aos recursos dentro do escopo.

1. Na página Visão geral, no painel Visão geral, escolha Criar implantação. Você também pode iniciar essa etapa em outras áreas da ferramenta.
2. Escolha a política que você deseja implantar.
3. Escolha o escopo que define as contas e os recursos nos quais o AWS Network Security Manager aplica a política.
4. Em Nome da implantação, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição.
5. (Opcional) Para tornar a implantação visível para outras contas em sua organização, selecione Habilitar visibilidade entre contas para essa implantação.
6. (Opcional) Para adicionar tags, escolha Adicionar nova tag e, em seguida, insira as combinações de chave e valor opcionais.
7. Selecione Create and deploy (Criar e implantar). A página Implantações é exibida, onde você pode ver os detalhes do que o AWS Network Security Manager criou.

⚠ As implantações podem incorrer em cobranças

Uma implantação cria serviços de segurança de rede e os anexa a um recurso protegido. AWS O Network Security Manager cobra pelos recursos protegidos. Os próprios serviços de segurança protegem o recurso, o que acarreta custos adicionais. Antes da implantação, consulte a página de preços do AWS Network Security Manager e a página de preços do AWS WAF.

Gerenciando proteções contra DDoS para AWS Shield Advanced

Com o AWS Network Security Manager, você configura e implanta centralmente as proteções AWS Shield Advanced em contas e recursos em sua organização. Você pode definir políticas de proteção contra DDoS e aplicá-las em grande escala por meio das políticas e implantações do AWS Network Security Manager.

> **AWS O Network Security Manager é cobrado separadamente**
>
> AWS O Network Security Manager não faz parte da oferta do AWS Shield Advanced. Para obter mais informações sobre preços, consulte os preços do AWS Network Security Manager e os preços AWS do Shield Advanced.

> **AWS Assinatura Shield Advanced**
>
> Quando uma implantação ativa inclui uma conta em seu escopo, o AWS Network Security Manager inscreve essa conta no AWS Shield Advanced. AWS O Network Security Manager não cancela a assinatura quando a conta sai do escopo ou quando você remove a implantação. Para cancelar uma assinatura AWS do Shield Advanced, consulte Assinatura AWS do Shield Advanced no Guia do desenvolvedor do AWS WAF.

Criação rápida para AWS Shield Advanced

Com o Quick Create, você define e implanta as proteções AWS Shield Advanced em um único fluxo de trabalho guiado. Use a Criação Rápida quando quiser configurar a proteção contra DDoS desde as políticas até a implantação em uma sessão.

Para definir e implantar uma proteção AWS Shield Advanced com o Quick Create, conclua os procedimentos a seguir na ordem.

Para criar a política e configurar as proteções

Execute as etapas a seguir:

1. Abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.
2. No painel de navegação, selecione Visão geral.
3. Na página Visão geral, escolha Criação e implantação rápidas. A página de criação e implantação rápidas é exibida com vários painéis.
4. No painel Detalhes da política, em Nome, insira um nome de política. (Opcional) Em Description (Descrição), insira uma descrição.

5. No painel Definir proteções, escolha o tipo de firewall com o qual você deseja trabalhar. Selecione AWS Shield Advanced.
6. Em Configuração de política no painel Definir proteções, decida as ações automatizadas que o AWS Network Security Manager executa no escopo de destino:
   - A remediação aplica a política definida a todos os recursos cujo estado de segurança não corresponda ao estado desejado descrito pelo AWS Network Security Manager.
   - A limpeza de recursos exclui a proteção contra DDoS que o AWS Network Security Manager criou para um recurso quando a implantação é removida ou quando a conta ou o recurso está fora do escopo.
   - A resolução de DDoS existente do cliente determina como resolver conflitos entre a política que você está definindo e o que já pode ter sido implantado. No menu, escolha uma das seguintes opções:
     - Nenhuma remediação ignora a remediação em qualquer recurso que já tenha uma proteção contra DDoS.
     - A associação Override substitui a proteção DDoS existente pela proteção DDoS criada pelo AWS Network Security Manager.
     - Adapte suas regras a cada proteção DDoS existente e mantém a proteção contra DDoS associada ao recurso.
7. No painel Prioridade da política, defina a prioridade. AWS O Network Security Manager avalia as políticas de acordo com sua prioridade para resolver conflitos. Posições mais baixas (números inteiros mais baixos) têm maior prioridade.

   Para editar a prioridade, escolha o valor da Posição. Em seguida, incremente-o com as setas ou insira um valor diretamente. Para confirmar a seleção, escolha Confirmar. Para descartar a alteração, escolha Cancelar.

Para definir o escopo

Execute as etapas a seguir:

1. No painel Definir o escopo, defina o conjunto de ativos aos quais as políticas se aplicam. Em Nome do escopo, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição.

2. **Multi-account somente modo**

   Essa etapa se aplica somente ao modo de várias contas. No modo de várias contas, use o subpainel Seleção de conta e unidade organizacional para escolher quais contas ou OUs incluir ou excluir. No modo de conta única, esse subpainel não aparece no console, então pule esta etapa.

   No subpainel de seleção de conta e unidade organizacional, selecione uma das seguintes opções:

   - Escopo para toda a AWS organização. Nenhuma definição adicional é necessária.
   - Abrange toda a AWS organização, mas exclui contas e OUs específicas. Um subpainel Unidades organizacionais e um subpainel Contas são exibidos. Para excluir unidades organizacionais, escolha Adicionar OUs. Selecione as unidades organizacionais na árvore organizacional e escolha Adicionar OUs. Para excluir contas individuais, escolha Adicionar contas. Selecione as contas na árvore da organização e escolha Adicionar contas.
   - Não abranja toda a AWS organização e inclua apenas OUs e contas específicas. Use o mesmo mecanismo Adicionar OUs e Adicionar contas para incluir as unidades organizacionais e as contas que você deseja.

3. No subpainel Recursos, em Tipos de recursos, selecione todos os tipos de recursos do AWS Shield Advanced ou específicos. As opções são uma ou mais das seguintes:
   - Application Load Balancer
   - CloudFront Distribuição
   - Classic Load Balancer
   - Endereços elastic IP (EIPs)
4. Para cada tipo de recurso selecionado, escolha uma das seguintes opções mutuamente exclusivas:
   - Incluir todos os recursos
   - Inclua recursos específicos
   - Excluir recursos específicos
5. Se você escolher Incluir recursos específicos, escolha um dos seguintes tipos de expressão e, em seguida, crie as combinações apropriadas de tags ou ARNs:
   - Critério único
   - Atenda a todos os critérios (AND)

- Atenda a qualquer critério (OR)
- NÃO

Todos os tipos de recursos têm os critérios de inclusão de Tag e ARN. Se você escolher Tag, insira uma chave e um valor opcional. Você pode identificar várias tags.

> **CloudFront Requisito de região**
>
> Para proteger os recursos CloudFront de distribuição, use a Região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

Para revisar e implantar a política

Execute as etapas a seguir:

1. No painel Revisar e implantar, em Nome da implantação, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição. Para determinar se o conteúdo da sua implantação está visível para outras contas em sua organização, selecione Habilitar visibilidade entre contas para esta implantação.
2. (Opcional) Para adicionar tags ao seu recurso, escolha Adicionar nova tag e insira combinações de chave e valor opcionais.
3. Para criar e implantar a política e o escopo, escolha Criar e implantar. Quando o processo estiver concluído, a página Implantações será exibida, onde você poderá ver os detalhes do que o AWS Network Security Manager criou.

> **As implantações podem incorrer em cobranças**
>
> Uma implantação cria serviços de segurança de rede e os anexa a um recurso protegido. AWS O Network Security Manager cobra pelos recursos protegidos. Os próprios serviços de segurança protegem o recurso, o que acarreta custos adicionais. Antes da implantação, consulte a página de preços do AWS Network Security Manager e a página de preços do AWS Shield Advanced.

Processo de criação padrão para AWS Shield Advanced

Com o processo de criação padrão, você configura cada componente AWS do Shield Advanced — políticas, escopos e implantações — individualmente para controle total. Use essa abordagem quando quiser criar componentes reutilizáveis e combiná-los conforme necessário.

Uma política AWS do Shield Advanced é simples e não contém regras, grupos de regras ou modelos. Quando você aplica a política, o AWS Network Security Manager cria uma proteção AWS Shield Advanced DDoS em cada conta dentro do escopo. Para obter informações sobre como o AWS Network Security Manager funciona, consulteComo funciona o AWS Network Security Manager.

Para criar uma política do (console)

Execute as etapas a seguir:

1. Entre no Console AWS de Gerenciamento usando sua conta de administrador do AWS Network Security Manager e abra o console do AWS Network Security Manager em https://console.aws.amazon.com/network-security-manager/.

   > Configuração da conta de administrador
   >
   > Para obter informações sobre como configurar uma conta de administrador do AWS Network Security Manager, consulteConfigurando o AWS Network Security Manager.

2. No painel de navegação, escolha AWS Network Security Manager e, em seguida, Visão geral.
3. No painel Visão geral, escolha Criar política. Insira um Nome e uma Descrição opcional e escolha um tipo de Firewall (nesse caso, AWS Shield Advanced).
4. No painel Prioridade da política, defina a prioridade. AWS O Network Security Manager avalia as políticas de acordo com sua prioridade para resolver conflitos. Posições mais baixas (números inteiros mais baixos) têm maior prioridade.

   Para editar a prioridade, escolha o valor da Posição. Em seguida, incremente-o com as setas ou insira um valor diretamente. Para confirmar a seleção, escolha Confirmar. Para descartar a alteração, escolha Cancelar.
5. No painel Configuração da política, decida as ações automatizadas que o AWS Network Security Manager executa no escopo de destino:

- A remediação aplica a política definida a todos os recursos cujo estado de segurança não corresponda ao estado desejado descrito pelo AWS Network Security Manager.
- A limpeza de recursos exclui a proteção contra DDoS que o AWS Network Security Manager criou para um recurso quando a implantação é removida ou quando a conta ou o recurso está fora do escopo.
- A resolução de DDoS existente do cliente determina como resolver conflitos entre a política que você está definindo e o que já pode estar implantado. No menu, escolha uma das seguintes opções:
  - Nenhuma remediação ignora a remediação em qualquer recurso que já tenha uma proteção contra DDoS.
  - A associação Override substitui a proteção DDoS existente pela proteção DDoS criada pelo AWS Network Security Manager.
  - Adapte suas regras a cada proteção DDoS existente e mantém a proteção contra DDoS associada ao recurso.

Para criar um escopo (console)

Execute as etapas a seguir:

1. No painel Detalhes do escopo, insira um nome do escopo e uma descrição opcional.
2.
   > **Multi-account somente modo**
   >
   > Essa etapa se aplica somente ao modo de várias contas. No modo de várias contas, use o subpainel Seleção de conta e unidade organizacional para escolher quais contas ou OUs incluir ou excluir. No modo de conta única, esse subpainel não aparece no console, então pule esta etapa.

   No painel Seleção de conta e unidade organizacional, escolha um dos três métodos para controlar o escopo administrativo:
   - Escopo para toda a AWS organização (todas as OUs e contas) — Nenhuma definição adicional é necessária.
   - Abrange toda a AWS organização, mas exclui contas e OUs específicas — Dois subpainéis aparecem, um para unidades organizacionais e outro para contas. Escolha Adicionar OUs para abrir a janela Adicionar OUs, selecione as unidades organizacionais necessárias e escolha

Adicionar OUs. Para adicionar contas individuais, no subpainel Contas, escolha Adicionar contas, selecione as contas e escolha Adicionar contas.

- Não abranja toda a AWS organização, inclua apenas OUs e contas específicas — use os mesmos subpainéis para adicionar OUs ou contas.

3. Em seguida, selecione recursos no subpainel Recursos. Na caixa de seleção Tipos de recursos, selecione todos os tipos de recursos AWS do Shield Advanced ou específicos. Para o AWS Shield Advanced, as opções são uma ou todas as seguintes:
   - Application Load Balancer
   - CloudFront Distribuição
   - Classic Load Balancer
   - Endereços elastic IP (EIPs)
4. Para cada tipo de recurso selecionado, escolha uma das seguintes opções mutuamente exclusivas:
   - Incluir todos os recursos
   - Inclua recursos específicos
   - Excluir recursos específicos
5. Se você escolher Incluir recursos específicos, selecione um dos seguintes tipos de expressão:
   - Critério único
   - Atenda a todos os critérios (AND)
   - Atenda a qualquer critério (OR)
   - NÃO
6. Cada tipo de expressão oferece suporte a um ou vários critérios de inclusão e ARNs, para que você possa criar combinações de tags ou ARNs. Todos os tipos de recursos são compatíveis com os critérios de inclusão de tags e ARN. Se você escolher Tag, identifique uma chave e um valor opcional. Você pode identificar várias tags.

> **CloudFront Requisito de região**
>
> Para proteger os recursos CloudFront de distribuição, use a Região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

Para criar uma implantação (console)

Uma implantação vincula suas políticas a um escopo e ativa a fiscalização. AWS Em seguida, o Network Security Manager aplica suas proteções AWS Shield Advanced DDoS aos recursos dentro do escopo.

Execute as etapas a seguir:

1. Na página Visão geral, no painel Visão geral, escolha Criar implantação.
2. Escolha a política que você deseja implantar.
3. Escolha o escopo que define as contas e os recursos nos quais o AWS Network Security Manager aplica a política.
4. Em Nome da implantação, insira um nome. (Opcional) Em Description (Descrição), insira uma descrição.
5. (Opcional) Para tornar a implantação visível para outras contas em sua organização, selecione Habilitar visibilidade entre contas para essa implantação.
6. (Opcional) Para adicionar tags, escolha Adicionar nova tag e, em seguida, insira as combinações de chave e valor opcionais.
7. Selecione Create and deploy (Criar e implantar). A página Implantações é exibida, onde você pode ver os detalhes do que o AWS Network Security Manager criou.

⚠ As implantações podem incorrer em cobranças

Uma implantação cria serviços de segurança de rede e os anexa a um recurso protegido. AWS O Network Security Manager cobra pelos recursos protegidos. Os próprios serviços de segurança protegem o recurso, o que acarreta custos adicionais. Antes da implantação, consulte a página de preços do AWS Network Security Manager e a página de preços do AWS Shield Advanced.

AWS Gerente de segurança de rede e AWS Firewall Manager

AWS O Network Security Manager é o serviço que está substituindo o AWS Firewall Manager. Os dois são serviços totalmente separados, cada um com recursos exclusivos e um modelo de preços diferente. Se você usa o AWS Firewall Manager atualmente, não precisa realizar nenhuma ação — seus firewalls e políticas existentes continuam funcionando. Este capítulo descreve como os dois serviços coexistem, como a precedência funciona quando você usa os dois e como a migração funcionará quando estiver disponível.

AWS O Network Security Manager e o AWS Firewall Manager operam lado a lado e independentemente um do outro. Em algum momento, o AWS Firewall Manager deixará de ser vendido e depois deixará de operar.

Coexistência com AWS Firewall Manager

AWS O Network Security Manager não afeta os firewalls que você criou com o AWS Firewall Manager, a menos que você inicie uma ação para alterá-los. Os firewalls e as políticas que você criou com o AWS Firewall Manager continuam operando, a menos que você os encerre. Isso é verdade mesmo após a AWS desativação do Firewall Manager.

Precedência durante a remediação

Enquanto os dois serviços operam, você pode realizar ações que afetem os firewalls criados com o AWS Firewall Manager. Ao criar políticas do AWS Network Security Manager, você as aplica a um escopo, que é um conjunto de recursos de destino. Se esse escopo incluir recursos que uma política do AWS Firewall Manager já aborda, o AWS Network Security Manager terá precedência durante a remediação. Nesse caso, a política e o escopo do AWS Network Security Manager substituem o AWS firewall e a política existentes do Firewall Manager. O comportamento específico depende das opções de resolução selecionadas.

Migração planejada de AWS Firewall Manager

A migração do AWS Firewall Manager para o AWS Network Security Manager consolida o gerenciamento do firewall em um único serviço e permite que você use seus recursos. A migração

está planejada, mas ainda não está disponível. Quando a migração estiver disponível, você poderá mover suas políticas do AWS Firewall Manager para o AWS Network Security Manager. A migração exigirá novas ações em ambos os serviços que ainda não estão em vigor.

O processo planejado copiará uma política selecionada do AWS Firewall Manager, a transferirá para o AWS Network Security Manager e a traduzirá na nova estrutura de políticas. Esse processo não afeta sua política original ou os firewalls associados no AWS Firewall Manager.

Segurança em AWS Gerente de segurança de rede

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Third-party auditores testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Network Security Manager, consulte AWS Serviços no escopo por programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e normas aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Network Security Manager. Os tópicos a seguir mostram como configurar o AWS Network Security Manager para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do AWS Network Security Manager.

Tópicos

- Proteção de dados em AWS Gerente de segurança de rede
- Gerenciamento de identidade e acesso para AWS Gerente de segurança de rede
- Usando funções vinculadas a serviços para AWS Gerente de segurança de rede
- Validação de conformidade AWS Gerente de segurança de rede
- Resiliência em AWS Gerente de segurança de rede
- Segurança de infraestrutura em AWS Gerente de segurança de rede
- Melhores práticas de segurança para AWS Gerente de segurança de rede

Proteção de dados em AWS Gerente de segurança de rede

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no AWS Network Security Manager. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Perguntas frequentes sobre privacidade de dados . Para obter informações sobre proteção de dados na Europa, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (RGPD).

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AWS Network Security Manager ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou em

campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso

AWS O Network Security Manager criptografa todos os dados em repouso usando as AWS chaves do Serviço de Gerenciamento de Chaves (AWS KMS). Service-managed As chaves KMS protegem suas configurações de recursos, estado de implantação e dados de sincronização. Você não precisa configurar ou gerenciar essas chaves.

Criptografia em trânsito

AWS O Network Security Manager criptografa todos os dados em trânsito usando o Transport Layer Security (TLS). Todas as solicitações de API exigem o TLS 1.2 ou posterior. As conexões com os endpoints da API do AWS Network Security Manager usam exclusivamente HTTPS.

Gerenciamento de chaves

AWS O Network Security Manager usa chaves AWS KMS gerenciadas pelo serviço para criptografia em repouso. Você não pode fornecer suas próprias chaves KMS no momento.

Gerenciamento de identidade e acesso para AWS Gerente de segurança de rede

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AWS Network Security Manager. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como AWS O Network Security Manager funciona com o IAM

- Identity-based exemplos de políticas para AWS Gerente de segurança de rede
- Solução de problemas AWS Identidade e acesso ao Network Security Manager

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas AWS Identidade e acesso ao Network Security Manager).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como AWS O Network Security Manager funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Identity-based exemplos de políticas para AWS Gerente de segurança de rede)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário-raiz

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas

políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Resource-based políticas são políticas embutidas que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations .
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS O Network Security Manager funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS Network Security Manager, saiba quais recursos do IAM estão disponíveis para uso com o AWS Network Security Manager.

Recurso do IAM	AWS Suporte ao Network Security Manager
Identity-based políticas	Sim
Resource-based políticas	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não

Recurso do IAM	AWS Suporte ao Network Security Manager
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Service-linked funções	Sim

Para ter uma visão de alto nível de como o AWS Network Security Manager e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Identity-based políticas para AWS Gerente de segurança de rede

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Resource-based políticas dentro AWS Gerente de segurança de rede

Compatibilidade com políticas baseadas em recursos: não

Resource-based políticas são documentos de política JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para

o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

AWS O Network Security Manager não oferece suporte a políticas baseadas em recursos.

Ações políticas para AWS Gerente de segurança de rede

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AWS Network Security Manager, consulte Ações definidas pelo AWS Network Security Manager na Referência de Autorização de Serviço.

As ações de política no AWS Network Security Manager usam o seguinte prefixo antes da ação:

```
network-security-manager
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "network-security-manager:action1",
      "network-security-manager:action2"
         ]
```

AWS O Network Security Manager define as ações do IAM em seus tipos de recursos. Isso inclui operações de criação, leitura, atualização e exclusão (CRUD) para regras, modelos, políticas, escopos e implantações, além de operações de captura instantânea, marcação, administração, status de sincronização e associação de recursos.

Recursos políticos para AWS Gerente de segurança de rede

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do AWS Network Security Manager e seus ARNs, consulte Recursos definidos pelo AWS Network Security Manager na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Network Security Manager.

AWS O Network Security Manager define um tipo de recurso do IAM para cada um de seus recursos (regra, modelo, política, escopo e implantação), além de um tipo de instantâneo para cada um (por exemplo,`rule-snapshot`). O formato do ARN é:

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

Os ARNs de rascunho são acrescentados `:DRAFT` e os ARNs de instantâneo acrescentam o número da versão (por exemplo,). `:3`

Os rascunhos não são tipos de recursos do IAM separados. Para autorização, um rascunho é tratado como filho de seu recurso ativo, que é o pai. Um ARN `:DRAFT` qualificado autoriza o recurso ativo, portanto, a permissão para agir em um rascunho vem da permissão para agir nesse recurso ativo.

Os instantâneos diferem dos rascunhos. Cada snapshot é seu próprio tipo de recurso do IAM, portanto, um ARN qualificado para versão autoriza diretamente esse tipo de recurso de snapshot, não contra o recurso ativo principal.

Chaves de condição de política para AWS Gerente de segurança de rede

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AWS Network Security Manager, consulte Chaves de condição do AWS Network Security Manager na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo AWS Network Security Manager.

AWS O Network Security Manager oferece suporte às seguintes chaves de condição de tag AWS globais para controle de acesso baseado em atributos (ABAC):

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

Tag-based as chaves de condição se aplicam aos recursos ativos e aos instantâneos. Os recursos preliminares não podem ser marcados e não oferecem suporte às `aws:ResourceTag` condições.

ACLs em AWS Gerente de segurança de rede

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

AWS O Network Security Manager não oferece suporte a listas de controle de acesso (ACLs).

ABAC com AWS Gerente de segurança de rede

Compatível com ABAC (tags em políticas): sim

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos

do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

AWS O Network Security Manager oferece suporte ao controle de acesso baseado em atributos usando todas as três chaves de condição de tag AWS globais. Você pode restringir o acesso aos recursos do AWS Network Security Manager com base nas tags anexadas a esses recursos.

Usando credenciais temporárias com AWS Gerente de segurança de rede

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Cross-service permissões principais para AWS Gerente de segurança de rede

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para AWS Gerente de segurança de rede

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AWS Network Security Manager. Edite as funções de serviço somente quando o AWS Network Security Manager fornecer orientação para fazer isso.

Service-linked funções para AWS Gerente de segurança de rede

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de realizar uma ação em seu nome. Service-linked as funções aparecem no seu Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

AWS O Network Security Manager usa uma função vinculada ao serviço para operar nas contas dos membros da sua organização. AWS O Network Security Manager cria a função vinculada ao serviço automaticamente quando você ativa o serviço. A função concede ao AWS Network Security Manager permissão para gerenciar os recursos do AWS WAF e AWS do Shield Advanced. A função também concede acesso ao AWS Config para descoberta de recursos e permissão para realizar operações entre contas.

Para obter detalhes sobre como criar e gerenciar funções vinculadas ao serviço do AWS Network Security Manager, consulte. the section called “Service-linked funções”

Identity-based exemplos de políticas para AWS Gerente de segurança de rede

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Network Security Manager. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS Network Security Manager, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do AWS Network Security Manager na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usar o AWS Console do Network Security Manager
- Permitir que os usuários visualizem suas próprias permissões
- Read-only acesso a AWS Gerente de segurança de rede
- Gerencie somente regras e modelos

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir recursos do AWS Network Security Manager em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem

usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o AWS Console do Network Security Manager

Para acessar o console do AWS Network Security Manager, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS Network Security Manager em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para acessar o console do AWS Network Security Manager, o diretor precisa de permissões mínimas para `network-security-manager:Get*` as ações `network-security-manager:List*` e.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Read-only acesso a AWS Gerente de segurança de rede

A política a seguir concede um acesso principal somente de leitura a todos os recursos do AWS Network Security Manager. Isso é útil para auditores ou funções de monitoramento que precisam visualizar as configurações e o status da sincronização sem fazer alterações.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Gerencie somente regras e modelos

A política a seguir permite que um diretor crie, atualize e exclua regras e modelos sem conceder acesso a políticas, escopos ou implantações. Isso é útil para equipes que criam configurações de segurança, mas não controlam a fiscalização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:CreateRule",
                "network-security-manager:GetRule",
                "network-security-manager:UpdateRule",
                "network-security-manager:DeleteRule",
                "network-security-manager:ListRules",
                "network-security-manager:CreateRuleSnapshot",
                "network-security-manager:ListRuleSnapshots",
                "network-security-manager:CreateTemplate",
                "network-security-manager:GetTemplate",
                "network-security-manager:UpdateTemplate",
                "network-security-manager:DeleteTemplate",
                "network-security-manager:ListTemplates",
                "network-security-manager:CreateTemplateSnapshot",
                "network-security-manager:ListTemplateSnapshots",
                "network-security-manager:TagResource",
                "network-security-manager:UntagResource",
                "network-security-manager:ListTagsForResource"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Solução de problemas AWS Identidade e acesso ao Network Security Manager

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS Network Security Manager e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Gerente de segurança de rede
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS para acessar meu AWS Recursos do Network Security Manager

Não estou autorizado a realizar uma ação em AWS Gerente de segurança de rede

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `network-security-manager:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 network-security-manager:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `network-security-manager:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Network Security Manager.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AWS Network Security Manager. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS para acessar meu AWS Recursos do Network Security Manager

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS Network Security Manager oferece suporte a esses recursos, consulteComo AWS O Network Security Manager funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.

- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usando funções vinculadas a serviços para AWS Gerente de segurança de rede

AWS O Network Security Manager usa funções vinculadas ao serviço IAM. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao AWS Network Security Manager. Service-linked as funções são predefinidas pelo AWS Network Security Manager e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS Network Security Manager porque você não precisa adicionar manualmente as permissões necessárias. AWS O Network Security Manager define as permissões de suas funções vinculadas ao serviço. A menos que definido de outra forma, somente o AWS Network Security Manager pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Você não pode anexar essa política de permissões a nenhuma outra entidade do IAM.

Você pode excluir uma função vinculada ao serviço somente depois de excluir pela primeira vez os recursos relacionados. Isso protege seus recursos do AWS Network Security Manager porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com o IAM e procure os serviços que incluem Sim na coluna de Service-linked funções. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Service-linked permissões de função para AWS Gerente de segurança de rede

AWS O Network Security Manager usa a função vinculada ao serviço chamada. `AWSServiceRoleForNetworkSecurityManager` Essa função vinculada ao serviço confia no diretor do `network-security-manager.amazonaws.com` serviço para assumir a função.

A política de permissões de função denominada `NetworkSecurityManagerServiceRolePolicy` é uma política AWS gerenciada que permite que o AWS Network Security Manager conclua ações nos recursos especificados.

A política de confiança a seguir permite que o diretor do `network-security-manager.amazonaws.com` serviço assuma a função.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "network-security-manager.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

> **Note**
>
> É necessário configurar as permissões para permitir que uma entidade do IAM (como um usuário, grupo ou perfil) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte as permissões de Service-linked função no Guia do usuário do IAM.

Detalhes das permissões

AWS O Network Security Manager exige que cada grupo de permissões proteja e descubra recursos em sua conta e organização. A política `NetworkSecurityManagerServiceRolePolicy` gerenciada concede as seguintes permissões, agrupadas por serviço:

- `wafv2`— Crie, leia, atualize e exclua ACLs da web e grupos de regras do Firewall Manager. Associe e desassocie ACLs da web com recursos protegidos. Gerencie configurações de registro de ACL da web e políticas de permissão de grupos de regras. Marcar e desmarcar recursos do . Valide a ACL da web e as configurações de regras do AWS Network Security Manager.
- `shield`— Crie, descreva, liste e exclua as proteções AWS Shield Advanced. Crie e descreva a assinatura do AWS Shield Advanced.
- `elasticloadbalancing`— Descreva os balanceadores de carga e as tags do aplicativo. Crie, exclua e defina associações de ACL da web em Application Load Balancers.

- `cloudfront`— Obtenha e liste CloudFront distribuições, configurações e tags da Amazon. Associe e desassocie ACLs da web de distribuição. Leia as origens da VPC.
- `apigateway`— Leia as APIs, estágios e tags REST do Amazon API Gateway. Defina a ACL da web em um estágio de API.
- `ec2`— Leia as ACLs e associações da web da instância de acesso verificado do Amazon EC2. Descreva os endereços IP elásticos para a proteção AWS Shield Advanced.
- `cognito-idp`,,`apprunner`, `appsyncamplify`, e `bedrock-agentcore` — Leia associações de ACL da web para grupos de usuários, serviços, APIs do AWS AppSync GraphQL AWS App Runner , AWS Amplify aplicativos e gateways Amazon AgentCore Bedrock do Amazon Cognito para que o Network Security Manager AWS possa descobrir recursos protegidos.
- `config`— Selecione configurações de recursos e gerencie o gravador de AWS Config configuração vinculado ao serviço que o AWS Network Security Manager usa para descobrir recursos dentro do escopo.
- `organizations`— Leia sua organização, contas, raízes, unidades organizacionais e administradores delegados para que o AWS Network Security Manager possa operar em toda a sua organização.
- `logs`— Crie, leia, atualize, exclua e liste entregas de registros para registro de ACL na web.
- `s3`— Obtenha e coloque políticas de bucket em buckets do Amazon S3 cujos nomes começam com `aws-waf-logs-` para que os logs de ACL da web possam ser entregues.
- `iam`— Crie as funções vinculadas ao serviço que o AWS Shield Advanced e o AWS WAF exigem, com base na chave de condição. AWS Config`iam:AWSServiceName`

O JSON a seguir mostra a política de `NetworkSecurityManagerServiceRolePolicy` permissões completa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid": "CloudfrontVpcOriginAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource": "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid": "ConfigUnscoped",
      "Effect": "Allow",
      "Action": [
        "config:SelectResourceConfig"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeOrganizationUnScoped",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeAccountScoped",
```

```
      "Effect": "Allow",
      "Action": "organizations:DescribeAccount",
      "Resource": "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid": "DescribeOrganizationUnitScoped",
      "Effect": "Allow",
      "Action": "organizations:DescribeOrganizationalUnit",
      "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid": "ListDelegatedAdministratorsScoped",
      "Effect": "Allow",
      "Action": "organizations:ListDelegatedAdministrators",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "network-security-manager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "LoadBalancerNonMutationApiAccess",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "LoadBalancerGetWebACLScoped",
      "Effect": "Allow",
      "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid": "CloudFrontDistributionNonMutationApiAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetDistribution",
```

```
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListTagsForResource"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ApiGatewayStageNonMutationApiAccess",
      "Effect": "Allow",
      "Action": "apigateway:GET",
      "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
      ]
    },
    {
      "Sid": "Wafv2General",
      "Effect": "Allow",
      "Action": [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2WebAclAndRuleGroupMutation",
      "Effect": "Allow",
      "Action": [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource": [
```

```
        "arn:aws:wafv2:*:*:*/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid": "Wafv2Logging",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2ListLogging",
      "Effect": "Allow",
      "Action": "wafv2:ListLoggingConfigurations",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2ListWebACLs",
      "Effect": "Allow",
      "Action": "wafv2:ListWebACLs",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2PermissionPolicy",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource": [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
```

```
      ]
    },
    {
      "Sid": "Wafv2WebaclDescribe",
      "Effect": "Allow",
      "Action": "wafv2:GetWebACLForResource",
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "CloudFrontListDistributions",
      "Effect": "Allow",
      "Action": [
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFrontDistributionMutation",
      "Effect": "Allow",
      "Action": [
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ElbWebAclRemediationScoped",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid": "ElbSetWebAcl",
      "Effect": "Allow",
      "Action": "elasticloadbalancing:SetWebACL",
      "Resource": "*"
    },
    {
      "Sid": "ApiGatewayWebAclRemediation",
      "Effect": "Allow",
```

```
      "Action": "apigateway:SetWebACL",
      "Resource": "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid": "CognitoWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppRunnerWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VerifiedAccessWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppSyncWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AmplifyWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "amplify:GetWebACLForResource",
```

```
        "amplify:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldGeneral",
      "Effect": "Allow",
      "Action": [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldSlrCreation",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "shield.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowConfigRecorderList",
      "Effect": "Allow",
      "Action": "config:ListConfigurationRecorders",
      "Resource": "*"
    },
    {
      "Sid": "AllowPutServiceLinkedConfigRecorder",
      "Effect": "Allow",
      "Action": "config:PutServiceLinkedConfigurationRecorder",
      "Resource": "*"
    },
```

```
    {
      "Sid": "AllowConfigRecorderScopedAccess",
      "Effect": "Allow",
      "Action": [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource": "arn:aws:config:*:*:configuration-recorder/*"
    },
    {
      "Sid": "AllowCreateConfigServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "config.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowListActionsForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowGetActionForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid": "WafV2LoggingSlrCreation",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
```

```
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "wafv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Criar uma função vinculada ao serviço para AWS Gerente de segurança de rede

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você ativa o AWS Network Security Manager, o AWS Network Security Manager cria a função vinculada ao serviço para você. Não há nenhuma etapa manual a ser executada.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, o AWS Network Security Manager recriará a função na próxima vez que você usar o serviço. Você não precisa realizar nenhuma ação.

Para saber mais, consulte Criar um perfil vinculado a serviço no Guia do usuário do IAM.

Editar uma função vinculada ao serviço para AWS Gerente de segurança de rede

Você não pode alterar as permissões da função `AWSServiceRoleForNetworkSecurityManager` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM.

Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Gerente de segurança de rede

Se você não precisar mais usar o AWS Network Security Manager, recomendamos que você exclua a função `AWSServiceRoleForNetworkSecurityManager` vinculada ao serviço.

Antes de excluir a função vinculada ao serviço, limpe os recursos gerenciados pelo AWS Network Security Manager. Desative o AWS Network Security Manager e remova as políticas e os escopos

para que nenhum recurso gerenciado pelo AWS Network Security Manager permaneça em sua conta. Em seguida, você pode excluir a função manualmente.

> **Note**
>
> Se o AWS Network Security Manager estiver usando a função ao tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Na caixa de pesquisa`AWSServiceRoleForNetworkSecurityManager`, insira e selecione a função.
4. Escolha Excluir.
5. Para confirmar a exclusão, insira o nome da função e escolha Excluir.

Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para AWS Funções vinculadas ao serviço do Network Security Manager

AWS O Network Security Manager oferece suporte ao uso de funções vinculadas a serviços em todas as AWS regiões em que o AWS Network Security Manager está disponível.

Validação de conformidade AWS Gerente de segurança de rede

Nossa nova experiência AWS de inscrição não foi projetada para cargas de trabalho regulamentadas. Se você estiver usando nossa nova experiência de AWS inscrição, mas quiser usá-la AWS para cargas de trabalho regulamentadas, você pode se inscrever AWS (avançado) ou ativar recursos avançados para seu AWS ambiente.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade

Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a documentação AWS de segurança.

Resiliência em AWS Gerente de segurança de rede

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o AWS Network Security Manager oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Segurança de infraestrutura em AWS Gerente de segurança de rede

Como um serviço gerenciado, o AWS Network Security Manager é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa chamadas de API AWS publicadas para acessar o AWS Network Security Manager pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos usar o TLS 1.2 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo direto perfeito (PFS), como DHE (Ephemeral) ou ECDHE (Elliptic Curve

Ephemeral Diffie-Hellman). Diffie-Hellman A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Melhores práticas de segurança para AWS Gerente de segurança de rede

As práticas recomendadas a seguir ajudam você a manter uma configuração segura do AWS Network Security Manager.

Controles preventivos

- Use o privilégio mínimo do IAM — conceda somente as permissões necessárias para que cada usuário ou função execute suas tarefas do AWS Network Security Manager. Use as chaves de condição do IAM para restringir o acesso a recursos específicos quando possível.
- Use funções vinculadas a serviços -- O AWS Network Security Manager usa funções vinculadas a serviços para realizar ações em seu nome. Essas funções têm permissões predefinidas com o escopo mínimo de acesso necessário.
- Configure os escopos com cuidado -- Defina configurações de escopo que tenham como alvo somente as contas e os tipos de recursos que exigem proteção. Escopos excessivamente amplos podem levar à fiscalização não intencional.

Controles de detecção

- Ativar AWS CloudTrail registro -- CloudTrail registra todas as chamadas da API do AWS Network Security Manager. Analise esses registros para auditar quem fez alterações em suas configurações de segurança e quando.
- Monitore o status da sincronização -- Verifique regularmente o status de sincronização de suas implantações para identificar recursos que estão fora de sincronia com a postura de segurança pretendida.

Monitoramento AWS Gerente de segurança de rede

O monitoramento do AWS Network Security Manager ajuda você a entender se seus recursos estão protegidos conforme o esperado. AWS O Network Security Manager fornece os seguintes recursos de monitoramento:

- APIs de status de sincronização -- Consulte o estado de proteção de recursos individuais em suas implantações.
- AWS CloudTrail-- Registre todas as chamadas da API do AWS Network Security Manager para auditoria, conformidade e solução de problemas operacionais.

Monitorando o status de sincronização

A principal forma de monitorar se seus recursos estão protegidos é por meio das APIs de status de sincronização. AWS O Network Security Manager avalia cada recurso dentro do escopo e registra se a configuração real do firewall corresponde à configuração pretendida.

Operações de status de sincronização

AWS O Network Security Manager fornece duas operações para consultar o status de sincronização:

ListResourceSynchronizationStatuses

Retorna o status por recurso para uma implantação específica. Necessário um parâmetro `deploymentIdentifier`. Opcionalmente, filtre por `synchronizationStatus` (IN_SYNC, OUT_OF_SYNC ou NOT_APPLICABLE).

ListAggregateResourceSynchronizationStatuses

Retorna o status agregado por recurso em todas as suas implantações. Opcionalmente, filtre por`synchronizationStatus`. Essa operação mostra o resultado combinado de todas as políticas que se aplicam a cada recurso.

Ambas as operações suportam paginação com `maxResults` (1 a 100) e. `nextToken`

Entendendo os valores do status de sincronização

EM_SYNC

A configuração real do firewall do recurso corresponde à configuração efetiva calculada a partir de todas as políticas aplicáveis.

FORA DE SINCRONIA

A configuração real do recurso é diferente da configuração efetiva. O `outOfSyncReasons` campo fornece detalhes por configuração mostrando valores esperados versus valores reais.

NOT_APPLICABLE

A conta e o tipo de recurso estão no escopo, mas o recurso em si não corresponde aos filtros do escopo (por exemplo, um filtro de tag o exclui). Nenhuma ação é necessária.

Se um recurso não aparecer nos resultados, a conta ou o tipo de recurso não está no escopo da implantação. Verifique a configuração do seu escopo.

Entendendo os timestamps de avaliação

Cada entrada de status de sincronização inclui dois carimbos de data e hora:

- `evaluatedAt`-- Quando o AWS Network Security Manager avaliou pela última vez a configuração do recurso. Um `evaluatedAt` valor obsoleto indica que a avaliação das mudanças recentes ainda não foi executada.
- `updatedAt`-- Quando o próprio registro de status de sincronização foi alterado pela última vez. Se `updatedAt` for mais antigo que`evaluatedAt`, o status permaneceu estável desde a última avaliação.

Cross-account visibilidade

Quando vários administradores protegem o mesmo recurso, a visibilidade do status de sincronização agregada depende da `enableCrossAccountVisibility` configuração de cada implantação.

- Se todas as implantações que abrangem um recurso tiverem a visibilidade entre contas ativada, qualquer administrador poderá ver o status agregado completo e os motivos da falta de sincronia.

- Se alguma implantação tiver a visibilidade entre contas desativada, outros administradores verão um `NOT_VISIBLE` marcador em vez de motivos detalhados. Isso indica que outro administrador também protege o recurso, mas não tem visibilidade compartilhada.

Diagnosticando recursos fora de sincronia

Quando um recurso relata OUT_OF_SYNC, o `outOfSyncReasons` campo identifica as diferenças de configuração específicas. O motivo principal é um dos seguintes:

- `missingFirewall`-- Nenhuma proteção de firewall está associada ao recurso.
- `invalidFirewall`-- Existe um firewall, mas sua configuração não corresponde às expectativas. As diferenças específicas estão listadas em compartimentos categorizados.

Se a correção estiver habilitada, mas não puder corrigir o recurso, o `remediationIssues` campo fornecerá uma `correctiveAction` orientação sobre como resolver o problema manualmente. A remediação é uma configuração em nível de política que está desativada por padrão. Para obter mais informações, consulte the section called “Sincronização e remediação”.

Várias implantações com configurações diferentes podem ter como alvo o mesmo recurso. Nesse caso, o status de sincronização por implantação pode ser OUT_OF_SYNC, enquanto o status de sincronização agregada é IN_SYNC. Esse é um comportamento esperado, não uma falha. As configurações de uma política de maior prioridade tiveram precedência durante a fusão. Como resultado, o recurso corresponde à configuração efetiva, mesmo que não corresponda à configuração da implantação de menor prioridade.

Registro em log AWS Chamadas de API do Network Security Manager com AWS CloudTrail

AWS O Network Security Manager é integrado AWS CloudTrail a um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço. CloudTrail captura todas as chamadas de API para o AWS Network Security Manager como eventos de gerenciamento. As chamadas capturadas incluem chamadas do console do AWS Network Security Manager e chamadas programáticas para as operações da API do AWS Network Security Manager.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o AWS Network Security Manager. Se você não configurar

uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

AWS Informações sobre o Network Security Manager em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no AWS Network Security Manager, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do AWS Network Security Manager, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição. Ele entrega os arquivos de log para o bucket do Amazon S3 que você especificar. Você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail

Todas as operações do AWS Network Security Manager são registradas por CloudTrail. As operações públicas incluem o seguinte:

- Operações de criação, leitura, atualização e exclusão (CRUD) para regras, modelos, políticas, escopos e implantações
- Operações de captura instantânea
- Operações de marcação
- Operações da conta de administrador
- Operações de status de sincronização
- Operações de associação de recursos
- Operações de geração de regras

Cada entrada de evento inclui as seguintes informações:

- A fonte do evento: `network-security-manager.amazonaws.com`
- O nome do evento, que é o nome da operação da API (por exemplo, `CreatePolicy` ou`ListDeployments`)
- Os recursos afetados, identificados por ARN e tipo de recurso

Read-only operações (como `GetPolicyListRules`, `eListResourceSynchronizationStatuses`) são registradas com `readOnly: true` e não incluem elementos de resposta. As operações de mutação incluem parâmetros de solicitação e elementos de resposta.

> **Note**
>
> CloudTrail redige campos confidenciais dos registros de eventos. Por exemplo, CloudTrail redige o `prompt` parâmetro na `GenerateRuleConfiguration` operação.

Exemplo: CreatePolicy evento

O exemplo a seguir mostra uma entrada de CloudTrail registro para a `CreatePolicy` operação.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLEID:my-session",
      "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAEXAMPLEID",
              "arn": "arn:aws:iam::123456789012:role/AdminRole",
              "accountId": "123456789012",
              "userName": "AdminRole"
          },
          "attributes": {
              "creationDate": "2026-08-10T18:22:41Z",
              "mfaAuthenticated": "false"
          }
```

```
      }
  },
  "eventTime": "2026-08-10T18:24:03Z",
  "eventSource": "network-security-manager.amazonaws.com",
  "eventName": "CreatePolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.44",
  "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
  "requestParameters": {
      "clientToken": "550e8400-e29b-41d4-a716-446655440001",
      "policyName": "production-web-acl-policy",
      "firewallType": "WAF",
      "priority": 1,
      "associatedTemplateAndRuleList": [
          {
              "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
          }
      ],
      "policyConfiguration": {
          "remediationEnabled": true,
          "resourcesCleanUp": false,
          "wafConfig": {
              "existingCustomerWebACLResolution": "RETROFIT",
              "conflictResolution": "MERGE_WHERE_APPLICABLE"
          }
      },
      "isPublished": true
  },
  "responseElements": {
      "policyId": "p9z8y7x6w5v4u3t2",
      "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
      "policyName": "production-web-acl-policy",
      "status": "ACTIVE",
      "version": "1"
  },
  "requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
  "eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
  "readOnly": false,
  "resources": [
      {
          "accountId": "123456789012",
          "type": "AWS::NetworkSecurityManager::Policy",
```

```
          "ARN": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"
      }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}
```

AWS Cotas do Network Security Manager

Você Conta da AWS tem as seguintes cotas padrão para o AWS Network Security Manager. Salvo indicação em contrário, cada cota é por conta, por região.

Cotas de recurso

A tabela a seguir lista o número máximo de recursos do AWS Network Security Manager que você pode criar por conta em cada região.

Recurso	Cota padrão	Ajustável
Regras por conta	200	Não
Modelos por conta	100	Não
Políticas por conta	100	Não
Escopos por conta	100	Não
Implantações por conta	100	Não
Instantâneos por recurso	10	Não

Cotas de composição de recursos

A tabela a seguir lista as cotas de como os recursos do AWS Network Security Manager fazem referência uns aos outros na hierarquia de recursos.

Quota	Valor
Regras por modelo	1 a 50
Modelos por política do AWS WAF	1 – 2
Regras e modelos combinados de acordo com a política do AWS WAF	1 a 100

Quota	Valor
Modelos ou regras de acordo com a política AWS do Shield Advanced	0 (deve estar vazio)
Políticas por implantação	1 – 2
Escopos por implantação	1 (exatamente um)

Cotas de configuração do escopo

A tabela a seguir lista as cotas para expressões de configuração de escopo.

Quota	Valor
Escopos de tipo de recurso por escopo	20
Profundidade da expressão do escopo (níveis aninhados)	2
Amplitude da expressão do escopo (critérios por nível)	20

Cotas da conta do administrador

A tabela a seguir lista as cotas para os níveis de prioridade da conta de administrador do AWS Network Security Manager.

Quota	Valor
Níveis de prioridade do administrador	1 a 10

Cotas de paginação da API

A tabela a seguir lista os limites de paginação para operações de lista.

Quota	Valor
Máximo de resultados por página (`maxResults`)	100
Resultados mínimos por página (`maxResults`)	1

Ajustabilidade da cota

As cotas listadas nas seções anteriores são fixas e não podem ser aumentadas no momento.

Histórico do documento para o AWS Guia do desenvolvedor do Network Security Manager

A tabela a seguir descreve as versões da documentação do AWS Network Security Manager.

Alteração	Descrição	Data
Lançamento inicial	Versão inicial do Guia do Desenvolvedor do AWS Network Security Manager.	1 de agosto de 2026

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.