aws

Guia do Desenvolvedor

AWS WAF, AWS Firewall Manager, e AWS Shield Advanced

AWS WAF, AWS Firewall Manager, e AWS Shield Advanced: Guia do Desenvolvedor

Table of Contents

O que são AWS WAF, AWS Shield Advanced; e AWS Firewall Manager?

Você pode usar AWS WAFAWS Shield, e AWS Firewall Manager em conjunto para criar uma solução de segurança abrangente. AWS WAF é um firewall de aplicativo da web que você pode usar para monitorar as solicitações da web que seus usuários finais enviam aos seus aplicativos e para controlar o acesso ao seu conteúdo. O Shield Advanced fornece proteção contra ataques distribuídos de negação de serviço (DDoS) para AWS recursos, nas camadas de rede e transporte (camadas 3 e 4) e na camada de aplicativos (camada 7). AWS Firewall Manager fornece gerenciamento de proteções como AWS WAF a Shield Advanced em todas as contas e recursos, mesmo quando novos recursos são adicionados.

Tópicos

O que é AWS WAF?

AWS WAF é um firewall de aplicativo web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas para os recursos protegidos do seu aplicativo web. É possível proteger os seguintes tipos de recursos:

- CloudFront Distribuição da Amazon
- API REST do Amazon API Gateway
- Application Load Balancer
- AWS AppSync API do GraphQL
- Grupo de usuários do Amazon Cognito
- AWS App Runner serviço
- AWS Instância de acesso verificado

AWS WAF permite que você controle o acesso ao seu conteúdo. Com base nas condições que você especificar, como de quais endereços IP se originam as solicitações ou os valores das strings de

consulta, seu recurso protegido responde às solicitações com o conteúdo solicitado, um código de status HTTP 403 (proibido) ou uma resposta personalizada.

No nível mais simples, AWS WAF permite escolher um dos seguintes comportamentos:

- Permitir todas as solicitações, exceto aquelas que você especificar — Isso é útil quando você deseja que a Amazon CloudFront, o Amazon API Gateway, o Application Load Balancer AWS AppSync, o Amazon Cognito AWS App Runner AWS ou o Verified Access forneçam conteúdo para um site público, mas você também deseja bloquear solicitações de invasores.
- Bloquear todas as solicitações, exceto as que você especificar: isso é útil quando você deseja fornecer conteúdo a um website restrito cujos usuários são prontamente identificáveis pelas propriedades nas solicitações da web, como os endereços IP que eles usam para navegar até o website.
- Contar as solicitações que correspondam aos seus critérios: você pode usar a ação Count para rastrear seu tráfego na web sem modificar a forma como você lida com isso. Você pode usar isso para monitoramento geral e também para testar suas novas regras de tratamento de solicitações da web. Quando quiser permitir ou bloquear solicitações com base em novas propriedades nas solicitações da Web, você pode primeiro configurar AWS WAF para contar as solicitações que correspondem a essas propriedades. Isso permite que você confirme suas novas configurações antes de mudar suas regras para permitir ou bloquear solicitações correspondentes.
- Executar verificações de CAPTCHA ou de desafio em solicitações que correspondam aos seus critérios: você pode implementar CAPTCHA e controles de desafio silenciosos em solicitações para ajudar a reduzir o tráfego de bots para seus recursos protegidos.

O uso AWS WAF tem vários benefícios:

- Proteção adicional contra ataques da web usando as condições que você especificar. Você pode definir condições usando as características das solicitações da web, como as seguintes:
  - Endereços IP dos quais as solicitações se originam.
  - País de origem das solicitações.
  - Valores nos cabeçalhos da solicitação.
  - As strings exibidas em solicitações, sejam strings específicas ou strings correspondentes a padrões de expressão regular (regex).
  - Comprimento das solicitações.
  - Presença de código SQL que pode ser mal-intencionado (conhecido como injeção de SQL).

  - Presença de um script que provavelmente é mal-intencionado (conhecido como cross-site scripting).
- Regras que podem permitir, bloquear ou contar solicitações da web que atendem aos critérios especificados. Como alternativa, as regras podem bloquear ou contar solicitações da web que não apenas atendam aos critérios especificados, mas também excedam um número específico de solicitações em um ou cinco minutos.
- Regras que você pode reutilizar para várias aplicações web.
- Grupos de regras gerenciados de AWS e AWS Marketplace vendedores.
- Métricas em tempo real e solicitações da web amostradas.
- Administração automatizada usando a AWS WAF API.

Se você deseja ter controle granular sobre a proteção que é adicionada aos seus recursos, apenas o AWS WAF é a escolha certa. Para obter mais informações sobre AWS WAF, consulteAWS WAF.

O que é AWS Shield Advanced?

Você pode usar listas de controle de acesso à AWS WAF web (ACLs da web) para ajudar a minimizar os efeitos de um ataque distribuído de negação de serviço (DDoS). Para proteção adicional contra ataques de DDoS, AWS também fornece AWS Shield Standard e. AWS Shield Advanced AWS Shield Standard é incluído automaticamente sem nenhum custo extra além do que você já paga AWS WAF e de seus outros AWS serviços.

O Shield Advanced fornece proteção expandida contra ataques de DDoS para suas instâncias do Amazon EC2, balanceadores de carga do Elastic Load Balancing, distribuições, CloudFront zonas hospedadas do Route 53 e aceleradores padrão. AWS Global Accelerator O Shield Advanced incorre em cobranças adicionais. As opções e atributos do Shield Advanced incluem mitigação automática de DDoS na camada de aplicativos, visibilidade avançada de eventos e suporte dedicado da Shield Response Team (SRT). Se você possui sites de alta visibilidade ou suscetíveis a ataques de DDoS frequentes, avalie a possibilidade de comprar os recursos adicionais que o Shield Advanced fornece. Para obter informações adicionais, consulte AWS Shield Advanced capacidades e opções e Como decidir se deseja assinar o AWS Shield Advanced e aplicar proteções adicionais.

O que é AWS Firewall Manager?

AWS Firewall Manager simplifica suas tarefas de administração e manutenção em várias contas e recursos para uma variedade de proteções AWS WAF, incluindo grupos de segurança e ACLs de

rede AWS Shield Advanced da Amazon VPC e o Amazon Route 53 Resolver AWS Network Firewall DNS Firewall. Com o Firewall Manager, você configura suas proteções apenas uma vez e o serviço aplica-as automaticamente em todas as contas e recursos, mesmo quando novos recursos e contas forem adicionados.

Para obter mais informações sobre o Firewall Manager, consulte AWS Firewall Manager.

Configurando sua conta para usar os serviços

Este tópico descreve as etapas preliminares, como criar uma conta, para prepará-lo para usar AWS WAF AWS Firewall Manager, AWS Shield Advanced e. Não há cobrança por esses itens preliminares. Você é cobrado somente pelos AWS serviços que você usa.

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Fazer download das ferramentas

AWS Management Console Inclui um console para AWS WAF, AWS Shield Advanced, e AWS Firewall Manager, mas se você quiser acessar os serviços programaticamente, consulte o seguinte:

- Os guias da API documentam as operações que os serviços suportam e fornecem links para a documentação relacionada do SDK e da CLI:
  - AWS WAF API Reference
  - AWS Shield Advanced API Reference
  - AWS Firewall Manager API Reference
- Para chamar uma API sem precisar lidar com detalhes de baixo nível, como montar solicitações HTTP brutas, você pode usar um AWS SDK. Os AWS SDKs fornecem funções e tipos de dados que encapsulam a funcionalidade dos serviços. AWS Para baixar um AWS SDK e acessar as instruções de instalação, consulte a página aplicável:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Para obter uma lista completa dos AWS SDKs, consulte Ferramentas para Amazon Web Services.

- Você pode usar o AWS Command Line Interface (AWS CLI) para controlar vários AWS serviços na linha de comando. Você também pode automatizar seus comandos usando scripts. Para ter mais informações, consulte AWS Command Line Interface.
- AWS Tools for Windows PowerShell suporta esses AWS serviços. Para obter mais informações, consulte Referência de Cmdlets do AWS Tools for PowerShell.

AWS WAF

AWS WAF é um firewall de aplicativo web que permite monitorar as solicitações HTTP (S) que são encaminhadas para seus recursos protegidos de aplicativos web. É possível proteger os seguintes tipos de recursos:

- CloudFront Distribuição da Amazon
- API REST do Amazon API Gateway
- Application Load Balancer
- AWS AppSync API do GraphQL
- Grupo de usuários do Amazon Cognito
- AWS App Runner serviço
- AWS Instância de acesso verificado

AWS WAF permite que você controle o acesso ao seu conteúdo. Com base nas condições que você especificar, como de quais endereços IP se originam as solicitações ou os valores das strings de consulta, o serviço associado ao seu recurso protegido responde às solicitações com o conteúdo solicitado, um código de status HTTP 403 (proibido) ou uma resposta personalizada.

> **Note**
>
> Você também pode usar AWS WAF para proteger seus aplicativos hospedados em contêineres do Amazon Elastic Container Service (Amazon ECS). O Amazon ECS é um serviço de gerenciamento de contêineres com alta escalabilidade e rapidez que facilita a execução, a interrupção e o gerenciamento de contêineres do Docker em um cluster. Para usar essa opção, você configura o Amazon ECS para usar um Application Load Balancer que está habilitado AWS WAF para rotear e proteger o tráfego HTTP (S) da camada 7 em todas as tarefas em seu serviço. Para obter mais informações, consulte Balanceamento de carga de serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

Tópicos

- AWS WAF listas de controle de acesso à web (ACLs da web)
- AWS WAF grupos de regras
- AWS WAF regras
- Tratamento de componentes de solicitação de tamanho grande no AWS WAF
- Correspondência de padrões de expressão regular em AWS WAF
- Conjuntos de IP e conjuntos de padrões regex em AWS WAF
- Solicitações e respostas personalizadas da web no AWS WAF
- AWS WAF rótulos em solicitações da web
- AWS WAF mitigação inteligente de ameaças
- Registrando AWS WAF tráfego de ACL da web
- Testando e ajustando suas AWS WAF proteções
- Como AWS WAF funciona com os CloudFront recursos da Amazon
- Segurança no uso do AWS WAF serviço
- AWS WAF cotas
- Migrando seus recursos AWS WAF clássicos para AWS WAF

Como AWS WAF funciona

Você usa AWS WAF para controlar como seus recursos protegidos respondem às solicitações da web HTTP (S). Você faz isso definindo uma lista de controle de acesso (ACL) à web e, em seguida, associando a um ou mais recursos de aplicativos da web que você deseja proteger. Os recursos associados encaminham as solicitações recebidas AWS WAF para inspeção pela ACL da web.

Na sua web ACL, você cria regras para definir padrões de tráfego a serem procurados nas solicitações e para especificar as ações a serem tomadas nas solicitações correspondentes. As opções de ações incluem o seguinte:

- Permitir que a solicitação seja encaminhada para o recurso protegido para processamento e resposta.
- Bloquear as solicitações.
- Contar as solicitações.
- Executar o CAPTCHA ou contestar verificações em relação às solicitações para verificar os usuários humanos e o uso do navegador padrão.

AWS WAF componentes

A seguir estão os componentes centrais de AWS WAF:

- ACLs da Web — Você usa uma lista de controle de acesso à Web (ACL) para proteger um conjunto de AWS recursos. Você cria uma web ACL e define sua estratégia de proteção adicionando regras. As regras definem critérios para inspecionar solicitações da web e especificam ação a ser tomadem relação a solicitações que correspondam aos critérios. Você também define uma ação padrão para a web ACL que indica se deve bloquear ou permitir qualquer solicitação que as regras ainda não tenham bloqueado ou permitido. Para obter mais informações web ACLs, consulte AWS WAF listas de controle de acesso à web (ACLs da web).

  Uma ACL da web é um AWS WAF recurso.

- Regras: cada regra contém uma instrução que define os critérios de inspeção e uma ação a ser tomada se uma solicitação da web atender aos critérios. Quando uma solicitação da web atende aos critérios, isso é uma correspondência. Você pode configurar regras para bloquear solicitações correspondentes, permitir que elas sejam atendidas, contá-las ou executar Controles de Bots contra elas que usam quebra-cabeças CAPTCHA ou desafios silenciosos do navegador do cliente. Para obter mais informações sobre regras, consulte AWS WAF regras.

  Uma regra não é um AWS WAF recurso. Ela só existe no contexto de uma web ACL ou de um grupo de regras.

- Grupos de regras — Você pode definir regras diretamente dentro de uma ACL da web ou em grupos de regras reutilizáveis. AWS As regras gerenciadas e AWS Marketplace os vendedores fornecem grupos de regras gerenciados para seu uso. Você também pode definir seus próprios grupos de regras. Para obter mais informações sobre grupos de regras, consulte AWS WAF grupos de regras.

  Um grupo de regras é um AWS WAF recurso.

Tópicos

- AWS WAF unidades de capacidade web ACL (WCUs)
- Recursos que você pode proteger com AWS WAF

AWS WAF unidades de capacidade web ACL (WCUs)

AWS WAF usa unidades de capacidade de ACL da web (WCU) para calcular e controlar os recursos operacionais necessários para executar suas regras, grupos de regras e ACLs da web. AWS WAF impõe limites de WCU quando você configura seus grupos de regras e ACLs da web. As WCUs não afetam a forma como AWS WAF inspeciona o tráfego da web.

AWS WAF gerencia a capacidade de regras, grupos de regras e ACLs da web.

WCUs de regra

AWS WAF calcula a capacidade da regra quando você cria ou atualiza uma regra. AWS WAF calcula a capacidade de forma diferente para cada tipo de regra, para refletir o custo relativo de cada regra. Regras simples que custam pouco para serem executadas usam menos WCUs que as regras mais complexas que utilizam mais poder de processamento. Por exemplo, uma instrução de regra de restrição de tamanho usa menos WCUs do que uma instrução que inspeciona solicitações usando um conjunto de padrões regex.

Os requisitos de capacidade da regra geralmente começam com um custo base para o tipo de regra e aumentam com a complexidade, por exemplo, quando você adiciona transformações de texto antes da inspeção ou se inspeciona o corpo do JSON. Para obter informações sobre os requisitos de capacidade das regras, consulte as listas das instruções de regras em Princípios básicos da instrução de regras.

WCUs de grupo de regras

Os requisitos de WCU para um grupo de regras são determinados pelas regras que você define dentro do grupo de regras. A capacidade máxima para um grupo de regras é de 5.000 WCUs.

Cada grupo de regras tem uma configuração de capacidade imutável, que o proprietário atribui na criação. Isso vale para grupos de regras gerenciados e grupos de regras que você cria por meio de AWS WAF. Quando você modifica um grupo de regras, suas alterações devem manter a WCU do grupo de regras dentro de sua capacidade. Isso garante que as web ACLsque estão usando o grupo de regras permaneçam dentro de sua capacidade máxima.

As WCUs que estão em uso em um grupo de regras são a soma das WCUs das regras menos quaisquer otimizações de processamento que possam ser AWS WAF obtidas combinando o comportamento das regras. Por exemplo, se você definir duas regras para examinar o mesmo componente de solicitação da web e cada uma aplicar uma transformação específica ao componente antes de inspecioná-lo, AWS WAF talvez seja possível cobrar apenas uma vez pela aplicação

da transformação. O custo da WCU para usar um grupo de regras em uma web ACL é sempre a configuração fixa da WCU que você definiu na criação do grupo de regras.

Ao criar um grupo de regras, defina uma capacidade alta o suficiente para acomodar as regras que você deseja usar durante toda a vida útil do grupo de regras.

WCUs de web ACL

Os requisitos de WCU para uma web ACL são determinados pelas regras e grupos de regras que você usa dentro da web ACL.

- O custo de usar um grupo de regras em uma web ACL é a configuração de capacidade do grupo de regras.
- O custo do uso de uma regra são as WCUs calculadas pela regra menos quaisquer otimizações de processamento que possam ser AWS WAF obtidas da combinação de regras da ACL da web. Por exemplo, se você definir duas regras para examinar o mesmo componente de solicitação da web e cada uma aplicar uma transformação específica ao componente antes de inspecioná-lo, AWS WAF talvez seja possível cobrar apenas uma vez pela aplicação da transformação.

O preço básico de uma web ACL inclui até 1.500 WCUs. O uso de mais de 1.500 WCUs gera taxas adicionais, de acordo com um modelo de preços em camadas. AWS WAF ajusta automaticamente o preço da sua ACL da web à medida que o uso da WCU da web ACL muda. Para obter detalhes sobre os preços, consulte Preços do AWS WAF.

A capacidade máxima de uma web ACL é de 5.000 WCUs.

Determinando as WCUs para um grupo de regras ou ACL da web

Conforme observado nas seções anteriores, o total de WCUs usadas em um grupo de regras ou web ACL será igual ou menor que a soma das WCUs para todas as regras definidas no grupo de regras ou na web ACL.

No AWS WAF console, você pode ver a capacidade consumida ao adicionar regras à sua ACL da web ou grupo de regras. O console exibe as unidades de capacidade atual usadas à medida que você adiciona as regras.

Por meio da API, você pode verificar os requisitos de capacidade máxima para as regras que deseja usar em uma web ACL ou grupo de regras. Para fazer isso, forneça a lista JSON das regras para a chamada de verificação de capacidade. Para obter mais informações, consulte CheckCapacitya Referência da API AWS WAF V2.

Recursos que você pode proteger com AWS WAF

Você pode usar uma AWS WAF Web ACL para proteger tipos de recursos globais ou regionais. Você faz isso associando a web ACL aos recursos que deseja proteger. A ACL da web e todos AWS WAF os recursos que ela usa devem estar localizados na região em que o recurso associado está localizado. Para CloudFront distribuições da Amazon, isso é definido como Leste dos EUA (Norte da Virgínia).

CloudFront Distribuições da Amazon

Você pode associar uma ACL AWS WAF da web a uma CloudFront distribuição usando o AWS WAF console ou as APIs. Você também pode associar uma ACL da web a uma CloudFront distribuição ao criar ou atualizar a própria distribuição. Para configurar uma associação em AWS CloudFormation, você deve usar a configuração CloudFront de distribuição. Para obter informações sobre a Amazon CloudFront, consulte Como usar AWS WAF para controlar o acesso ao seu conteúdo no Amazon CloudFront Developer Guide.

AWS WAF está disponível globalmente para CloudFront distribuições, mas você deve usar a região Leste dos EUA (Norte da Virgínia) para criar sua ACL da web e quaisquer recursos usados na ACL da web, como grupos de regras, conjuntos de IP e conjuntos de padrões regex. Algumas interfaces oferecem uma opção de região de “Global (CloudFront)”. Escolher isso é idêntico a escolher a região Leste dos EUA (N. da Virgínia) ou “us-east-1”.

recursos regionais

Você pode proteger os recursos regionais em todas as regiões onde AWS WAF estiver disponível. Você pode ver a lista em endpoints e cotas do AWS WAF no Referência geral da Amazon Web Services.

Você pode usar AWS WAF para proteger os seguintes tipos de recursos regionais:

- API REST do Amazon API Gateway
- Application Load Balancer
- AWS AppSync API do GraphQL
- Grupo de usuários do Amazon Cognito
- AWS App Runner serviço
- AWS Instância de acesso verificado

Você só pode associar uma web ACL a um Application Load Balancer que esteja dentro das Regiões da AWS. Por exemplo, você não pode associar uma web ACL a um Application Load Balancer que esteja no AWS Outposts.

A ACL da web e quaisquer outros AWS WAF recursos que ela usa devem estar localizados na mesma região que os recursos protegidos. Ao monitorar e gerenciar solicitações da web para um recurso regional protegido, AWS WAF mantém todos os dados na mesma região do recurso protegido.

Restrições às associações de múltiplos recursos

Você pode associar uma única ACL da web a um ou mais AWS recursos, com as seguintes restrições:

- Você pode associar cada AWS recurso a somente uma Web ACL. A relação entre a Web ACL e AWS os recursos é one-to-many.
- Você pode associar uma ACL da web a uma ou mais CloudFront distribuições. Você não pode associar uma Web ACL associada a uma CloudFront distribuição a nenhum outro tipo de AWS recurso.

Começando com AWS WAF

Este tutorial mostra como usar AWS WAF para realizar as seguintes tarefas:

- Configurar AWS WAF.
- Crie uma lista de controle de acesso à web (Web ACL) usando o assistente no AWS WAF console.
- Escolha os AWS recursos para os quais você deseja AWS WAF inspecionar as solicitações da Web. Este tutorial aborda as etapas da Amazon CloudFront. O processo é basicamente o mesmo para uma API REST do Amazon API Gateway, um Application Load Balancer, uma API GraphQL AWS AppSync , um grupo de usuários do Amazon Cognito, um AWS App Runner serviço ou uma instância de acesso verificado. AWS
- Adicione as regras e os grupos de regras que deseja usar para filtrar solicitações da web. Por exemplo, você pode especificar os endereços IP dos quais se originam as solicitações e os valores na solicitação que são usados apenas por invasores. Para cada regra, especifique como lidar com solicitações da web correspondentes. Você pode fazer coisas como bloqueá-las ou contá-las, além de executar desafios de bots, como CAPTCHA. Você define uma ação para cada regra que você define dentro de uma web ACL e para cada regra que você define dentro de um grupo de regras.

- Especifique uma ação padrão para a web ACL: Block ou Allow. Essa é a ação que AWS WAF ocorre em uma solicitação quando as regras na ACL da web não a permitem ou bloqueiam explicitamente.

> **Note**
>
> AWS normalmente cobra menos de USD 0,25 por dia pelos recursos que você cria durante este tutorial. Quando você tiver concluído o tutorial, recomendamos que exclua os recursos para impedir cobranças desnecessárias.

Tópicos

Etapa 1: configurar AWS WAF

Se você ainda não seguiu as etapas gerais de configuração em Configurando sua conta para usar os serviços, faça isso agora.

Etapa 2: Criar uma web ACL

O AWS WAF console orienta você no processo de configuração AWS WAF para bloquear ou permitir solicitações da Web com base nos critérios que você especifica, como os endereços IP dos quais as solicitações se originam ou os valores nas solicitações. Nesta etapa, você cria uma web ACL. Para obter mais informações sobre ACLs AWS WAF da web, consulteAWS WAF listas de controle de acesso à web (ACLs da web).

Para criar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

2. Na página AWS WAF inicial, escolha Create web ACL.
3. Em Nome, insira o nome que deseja usar para identificar esta web ACL.

> **Note**
>
> Você não pode alterar o nome depois de criar a web ACL.

4. (Opcional) Em Descrição: opcional, insira uma descrição mais longa para a web ACL, se desejar.
5. Para nome da CloudWatch métrica, altere o nome padrão, se aplicável. Siga as orientações no console para usar caracteres válidos. O nome não pode conter caracteres especiais, espaços em branco ou nomes de métrica reservados para o AWS WAF, incluindo “All” e “Default_Action”.

> **Note**
>
> Você não pode alterar o nome da CloudWatch métrica depois de criar a Web ACL.

6. Em Tipo de recurso, escolha CloudFrontdistribuições. A região é preenchida automaticamente como Global (CloudFront) para CloudFront distribuições.
7. (Opcional) Para AWS Recursos associados - opcional, escolha Adicionar AWS recursos. Na caixa de diálogo, escolha os recursos que deseja associar e, em seguida, escolha Adicionar. O AWS WAF retorna você à página Descrever web ACL e recursos da AWS associados.
8. Escolha Próximo.

Etapa 3: Adicionar uma regra de correspondência de string

Nesta etapa, você cria uma regra com uma instrução de correspondência de string e indica o que fazer com as solicitações correspondentes. Uma instrução de regra de correspondência de string identifica as strings que você deseja que AWS WAF busque em uma solicitação. Geralmente, uma string consiste em caracteres ASCII imprimíveis, mas você pode especificar qualquer caractere, do hexadecimal 0x00 a 0xFF (decimal 0 a 255). Além de especificar a string a ser pesquisada, você especifica o componente de solicitação da web que deseja pesquisar, como um cabeçalho, uma string de consulta ou o corpo da solicitação.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

  > **Warning**
  >
  > Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

  Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.

- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Para obter informações adicionais sobre AWS WAF regras, consulteAWS WAF regras.

Para criar uma instrução de regra de correspondência de string

1. Na página Adicionar regras e grupos de regras escolha Adicionar regras, Adicionar minhas próprias regras e grupos de regras, Construtor de regras e Editor visual de regras.

   > **Note**
   >
   > O console fornece o Editor visual de regras e um Editor JSON de regras. O editor JSON facilita a cópia de configurações entre web ACLse é necessário para conjuntos de regras mais complexos, como aqueles com vários níveis de aninhamento.
   > Este procedimento usa o Editor visual de regras.

2. Em Nome, insira o nome que deseja usar para identificar esta regra.
3. Em Type (Tipo), escolha Regular rule (Regra regular).
4. Para If a request (Se uma solicitação), escolha matches the statement (corresponder à instrução).

As outras opções são para os tipos de instrução de regra lógica. Você pode usá-las para combinar ou negar os resultados de outras instruções de regras.

5. Em Declaração, para Inspecionar, abra a lista suspensa e escolha o componente de solicitação da web que você deseja AWS WAF inspecionar. Para este exemplo, selecione Header.

   Ao escolher Header (Cabeçalho), você também especifica qual cabeçalho o AWS WAF deve inspecionar. Insira **`User-Agent`**. Esse valor não diferencia maiúsculas de minúsculas.

6. Em Match type (Tipo de correspondência), escolha onde a string especificada deve aparecer no cabeçalho `User-Agent`.

   Para este exemplo, escolha Exactly matches string (Correspondência exata). Isso indica que AWS WAF inspeciona o cabeçalho do agente de usuário em cada solicitação da web em busca de uma string idêntica à string especificada.

7. Em String to match (String a corresponder), especifique uma string que você deseja que o AWS WAF pesquise. O tamanho máximo de String to match (String a corresponder) é 200 caracteres. Se você quiser especificar um valor codificado em base64, poderá especificar até 200 caracteres antes da codificação.

   Para este exemplo, insira MyAgent. AWS WAF inspecionará o `User-Agent` cabeçalho nas solicitações da web em busca do valor`MyAgent`.

8. Deixe o campo Text transformation (Transformação de texto) definido como None (Nenhuma).

9. Em Ação, selecione a ação que você deseja que a regra execute quando ela corresponder a uma solicitação da web. Neste exemplo, escolha Contar e deixe as outras opções como estão. Isso cria métricas para solicitações da web que correspondem à regra, mas não determina se a regra é permitida ou bloqueada. Para obter mais informações sobre essas opções, consulte Ação da regra e Avaliação de regras da web ACL e do grupo de regras.

10. Escolha Adicionar regra.

Etapa 4: Adicionar um grupo de regras de regras AWS gerenciadas

AWS O Managed Rules oferece um conjunto de grupos de regras gerenciados para seu uso, a maioria dos quais é gratuita para AWS WAF os clientes. Para obter mais informações sobre grupos de regras, consulte AWS WAF grupos de regras. Adicionaremos um grupo de regras de regras AWS gerenciadas a essa ACL da web.

Para adicionar um grupo de regras de regras AWS gerenciadas

1. Na página Add rules and rule groups (Adicionar regras e grupos de regras), escolha Add rules (Adicionar regras) e, em seguida, escolha Add managed rule groups (Adicionar grupos de regras gerenciados).
2. Na página Add managed rule groups (Adicionar grupos de regras gerenciados), expanda a oferta dos grupos de regras gerenciados do AWS . (Você também verá anúncios oferecidos para AWS Marketplace vendedores. Você pode assinar suas ofertas e depois usá-las da mesma forma que nos grupos de regras de regras AWS gerenciadas.)
3. Para cada grupo de regras que você deseja adicionar, faça o seguinte:
   a. Na coluna Ação, ative a opção Adicionar à web ACL.
   b. Selecione Editar e, na lista de Regras do grupo de regras, abra o menu suspenso Substituir todas as ações de regra e selecione Count. Isso define a ação para todas as regras no grupo somente como contagem. Isso permite que você veja como todas as regras no grupo de regras lidam com suas solicitações da web antes de serem implementadas.
   c. Escolha Salvar regras.
4. Na página Adicionar grupos de regras gerenciadas, escolha Adicionar regras. Isso levará você de volta à página Adicionar regras e grupos de regras.

Etapa 5: concluir a configuração da web ACL

Após adicionar regras e grupos de regras à sua configuração da web ACL, a última etapa é definir a prioridade das regras na ACL e outras configurações como métricas, marcação e registro em log.

Para concluir a configuração da web ACL

1. Na página Add rules and rule groups (Adicionar regras e grupos de regras), escolha Next (Próximo).
2. Na página Definir prioridade da regra, você pode ver a ordem de processamento das regras e grupos de regras na ACL da web. AWS WAF os processa começando do topo da lista. Você pode alterar a ordem de processamento movendo as regras para cima e para baixo. Para isso, selecione uma regra na lista e escolha Move up (Mover para cima) ou Move down (Mover para baixo). Para obter mais informações sobre prioridade de regra, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.
3. Escolha Próximo.

4. Na página Configurar métricas, para CloudWatchmétricas da Amazon, você pode ver as métricas planejadas para suas regras e grupos de regras e você pode ver as opções de amostragem de solicitações na web. Para obter informações sobre como visualizar solicitações de exemplo, consulte Visualizar um exemplo de solicitações da web. Para obter informações sobre CloudWatch as métricas da Amazon, consulteMonitoramento com a Amazon CloudWatch.

   Você pode acessar resumos das métricas de tráfego da web na página da ACL da web no AWS WAF console, na guia Visão geral do tráfego. Os painéis do console fornecem resumos quase em tempo real das métricas da Amazon da ACL da web. CloudWatch Para ter mais informações, consulte Painéis de visão geral do tráfego de web ACL.
5. Escolha Próximo.
6. Na página Review and create web ACL (Revisar e criar web ACL), revise suas configurações e escolha Create web ACL (Criar web ACL).

O assistente retorna à página Web ACL onde sua nova web ACL está listada.

Etapa 6: Limpar os recursos

Você concluiu com êxito o tutorial. Para evitar que sua conta acumule AWS WAF cobranças adicionais, limpe os AWS WAF objetos que você criou. Como alternativa, você pode alterar a configuração para corresponder às solicitações da Web que você realmente deseja gerenciar usando AWS WAF.

> **Note**
>
> AWS normalmente cobra menos de USD 0,25 por dia pelos recursos que você cria durante este tutorial. Quando você tiver terminado, recomendamos excluir os recursos para impedir que cobranças desnecessárias.

Para excluir os objetos que AWS WAF cobram

1. Na página Web ACL selecione sua web ACL na lista e escolha Edit (Editar).
2. Na guia AWS Recursos associados, para cada recurso associado, selecione o botão de rádio ao lado do nome do recurso e escolha Desassociar. Isso desassocia a ACL da web de seus recursos. AWS
3. Em cada uma das telas a seguir, escolha Next (Próximo) até retornar à página Web ACL .

Na página Web ACL, selecione sua web ACL na lista e escolha Delete (Excluir).

Instruções de regras e regras não existem fora do grupo de regras e definições de web ACL. Ao excluir uma web ACL, você exclui todas as regras individuais definidas nela. Quando você remove um grupo de regras de uma web ACL, só a referência ao grupo é removida.

AWS WAF listas de controle de acesso à web (ACLs da web)

A lista de controle de acesso da web (web ACL) oferece controle detalhado sobre todas as solicitações web HTTP (S) às quais o recurso protegido responde. Você pode proteger os recursos da Amazon CloudFront, do Amazon API Gateway, do Application Load Balancer AWS AppSync, do Amazon Cognito AWS e do AWS App Runner Verified Access.

Você pode usar critérios como os seguintes para permitir ou bloquear solicitações:

- Origem do endereço IP da solicitação
- País de origem da solicitação
- Correspondência de string ou correspondência de expressão regular (regex) em uma parte da solicitação
- Tamanho de uma parte específica da solicitação
- Detecção de código SQL malicioso ou script

Você também pode testar qualquer combinação dessas condições. Você pode bloquear ou contar solicitações da web que não apenas atendam às condições especificadas, mas também excedam um número específico de solicitações em um único minuto. Você pode combinar condições usando operadores lógicos. Você também pode executar quebra-cabeças CAPTCHA e desafios silenciosos de sessões de clientes contra solicitações.

Você fornece seus critérios de correspondência e a ação a ser tomada em relação às correspondências nas declarações de AWS WAF regras. Você pode definir instruções de regras diretamente na sua web ACL e em grupos de regras reutilizáveis que você usa na sua web ACL. Para obter uma lista completa das opções, consulte Princípios básicos da instrução de regras e Ação da regra.

Para especificar seus critérios de inspeção e tratamento de solicitações da web, execute as seguintes tarefas:

1. Escolha a ação padrão, Allow ou Block, para solicitações da web que não corresponderem a nenhuma das regras que você especificar. Para ter mais informações, consulte A ação padrão da web ACL.
2. Adicione quaisquer grupos de regras que você deseja usar na sua web ACL. Os grupos de regras gerenciadas geralmente contêm regras que bloqueiam solicitações da Web. Para obter informações sobre grupos de regras, consulte AWS WAF grupos de regras.
3. Especifique critérios adicionais de correspondência e instruções de tratamento em uma ou mais regras. Para adicionar mais de uma regra, comece com instruções de regra `AND` ou `OR` e aninhe as regras que você deseja combinar nessas instruções. Se você deseja negar uma opção de regra, aninhe a regra em uma instrução NOT. Você também pode usar uma regra baseada em intervalos em vez de uma regra regular para limitar o número de solicitações de qualquer endereço IP único que atenda às condições. Para obter mais informações sobre regras, consulte AWS WAF regras.

Se você adicionar mais de uma regra a uma ACL da web, AWS WAF avalia as regras na ordem em que estão listadas para a ACL da web. Para ter mais informações, consulte Avaliação de regras da web ACL e do grupo de regras.

Ao criar uma web ACL, especifique os tipos de recursos com os quais pretende utilizá-la. Para mais informações, consulte Criação de uma web ACL. Depois de definir uma web ACL, é possível associá-la aos seus recursos para começar a fornecer proteção para eles. Para ter mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

Como AWS os recursos lidam com os atrasos de resposta de AWS WAF

Em algumas ocasiões, AWS WAF pode encontrar um erro interno que atrasa a resposta aos AWS recursos associados sobre se deve permitir ou bloquear uma solicitação. Nessas ocasiões, CloudFront normalmente permite a solicitação ou veicula o conteúdo, enquanto os serviços regionais normalmente negam a solicitação e não veiculam o conteúdo.

Tópicos

- Avaliação de regras da web ACL e do grupo de regras
- A ação padrão da web ACL
- Gerenciando os limites de tamanho da inspeção corporal
- Configurações para CAPTCHA, desafio e tokens
- Trabalho com :web ACLs

Avaliação de regras da web ACL e do grupo de regras

A forma como uma web ACL processa uma solicitação da web depende do seguinte:

- As configurações de prioridade numérica das regras na web ACL e dentro dos grupos de regras
- As configurações de ação nas regras e na web ACL
- Todas as substituições que você colocar nas regras e grupos de regras que você adicionar

Para obter uma lista das configurações de ação de regra, consulte Ação da regra.

Agora você pode personalizar a solicitação e o tratamento de resposta nas configurações de ação de regra e nas configurações de ação padrão da web ACL. Para mais informações, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Tópicos

Ordem de processamento de regras e grupos de regras em uma web ACL

Em uma web ACL e dentro de qualquer grupo de regras, você determina a ordem de avaliação das regras usando configurações de prioridade numérica. Você deve atribuir a cada regra em uma web ACL uma configuração de prioridade exclusiva dentro dessa web ACL e deve dar a cada regra em um grupo de regras uma configuração de prioridade exclusiva dentro desse grupo de regras.

> **Note**
>
> Quando você gerencia grupos de regras e ACLs da web por meio do console, AWS WAF atribui configurações de prioridade numérica exclusivas para você com base na ordem das regras na lista. AWS WAF atribui a prioridade numérica mais baixa à regra na parte superior da lista e a prioridade numérica mais alta à regra na parte inferior.

Ao AWS WAF avaliar qualquer ACL da web ou grupo de regras em relação a uma solicitação da web, ele avalia as regras da configuração de prioridade numérica mais baixa até encontrar uma correspondência que encerre a avaliação ou esgote todas as regras.

Por exemplo, digamos que você tenha as seguintes regras e grupos de regras em sua web ACL, priorizados conforme mostrado:

- Regra1: prioridade 0
- RuleGroupA — prioridade 100
  - RegraA1: prioridade 10.000
  - RegraA2: prioridade 20.000
- Regra2: prioridade 200
- RuleGroupB — prioridade 300
  - RegraB1: prioridade 0
  - RegraB2: prioridade 1

AWS WAF avaliaria as regras para essa ACL da web na seguinte ordem:

- Rule1
- RuleGroupUma regra A1
- RuleGroupUma regra A2
- Rule2
- RuleGroupPor RuleB1
- RuleGroupPor RuleB2

Como AWS WAF manipula as ações de regras e grupos de regras em uma ACL da web

Ao configurar suas regras e grupos de regras, você escolhe como deseja AWS WAF lidar com as solicitações da web correspondentes:

- Allow e Block estão encerrando ações: as ações Allow e Block interrompem todos os outros processamentos da web ACL na solicitação da web correspondente. Se uma regra em uma ACL da web encontrar uma correspondência para uma solicitação e a ação da regra for Allow ouBlock, essa correspondência determinará a disposição final da solicitação da web para a ACL da web. AWS WAF não processa nenhuma outra regra na ACL da web que venha depois da correspondente. Isso é verdadeiro para regras que você adiciona diretamente à web ACL e às regras que estão dentro de um grupo de regras adicionado. Com a ação Block, o recurso protegido não recebe nem processa a solicitação da web.

- Count não é uma ação de encerramento: quando uma regra com uma ação Count corresponde a uma solicitação, o AWS WAF conta a solicitação e, em seguida, continua processando as regras que seguem no conjunto de regras da web ACL.
- CAPTCHAe Challenge podem ser ações de encerramento ou encerramento — quando uma regra com uma dessas ações corresponde a uma solicitação, AWS WAF verifica o status do token. Se a solicitação tiver um token válido, AWS WAF tratará a correspondência de forma semelhante a uma Count correspondência e, em seguida, continuará processando as regras que seguem no conjunto de regras da Web ACL. Se a solicitação não tiver um token válido, AWS WAF encerra a avaliação e envia ao cliente um quebra-cabeça CAPTCHA ou um desafio silencioso de uma sessão de cliente em segundo plano para resolver.

Se a avaliação da regra não resultar em nenhuma ação de encerramento, AWS WAF aplicará a ação padrão da Web ACL à solicitação. Para mais informações, consulte A ação padrão da web ACL.

Na sua web ACL, você pode substituir as configurações de ação das regras dentro de um grupo de regras e substituir a ação retornada por um grupo de regras. Para mais informações, consulte Opções de substituição de ação para grupos de regras.

Interação entre ações e configurações de prioridade

As ações que AWS WAF se aplicam a uma solicitação da web são afetadas pelas configurações de prioridade numérica das regras na ACL da web. Por exemplo, digamos que sua web ACL tenha uma regra com ação Allow e uma prioridade numérica de 50 e outra regra com ação Count e uma prioridade numérica de 100. O AWS WAF avalia as regras em uma web ACL na ordem de prioridade, começando pela configuração mais baixa, para que avalie a regra de permissão antes da regra de contagem. Uma solicitação da web que corresponda às duas regras corresponderá primeiro à regra de permissão. Como Allow é uma ação de encerramento, AWS WAF interromperá a avaliação nesta partida e não avaliará a solicitação de acordo com a regra de contagem.

- Se você quiser incluir apenas solicitações que não correspondam à regra de permissão nas métricas da regra de contagem, as configurações de prioridade das regras funcionarão.
- Por outro lado, se você quiser contar métricas da regra de contagem, mesmo para solicitações que correspondam à regra de permissão, precisará atribuir à regra de contagem uma configuração de prioridade numérica menor do que a regra de permissão, para que ela seja executada primeiro.

Para obter mais informações sobre configurações de prioridade, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

Opções de substituição de ação para grupos de regras

Ao adicionar um grupo de regras à sua web ACL, você pode substituir as ações que ele executa nas solicitações da web correspondentes. Substituir as ações de um grupo de regras dentro da configuração da web ACL não altera o grupo de regras em si. Ele só altera a forma como AWS WAF usa o grupo de regras no contexto da ACL da web.

Substituições de ações de regras de grupos de regras

Você pode substituir as ações das regras dentro de um grupo de regras por qualquer ação de regra válida. Quando você faz isso, as solicitações correspondentes são tratadas exatamente como se a ação da regra configurada fosse a configuração de substituição.

> **Note**
>
> As ações de regra podem ser de encerramento ou não. Uma ação de encerramento interrompe a avaliação da web ACL da solicitação e permite que ela continue em seu aplicativo protegido ou a bloqueia.

Veja as opções da ação da regra:

- Allow— AWS WAF permite que a solicitação seja encaminhada ao AWS recurso protegido para processamento e resposta. Essa é uma ação de encerramento. Nas regras que define, você pode inserir cabeçalhos personalizados na solicitação antes de encaminhá-la para o recurso protegido.
- Block— AWS WAF bloqueia a solicitação. Essa é uma ação de encerramento. Por padrão, seu AWS recurso protegido responde com um código de `403 (Forbidden)` status HTTP. Nas regras que você define, você pode personalizar a resposta. Quando AWS WAF bloqueia uma solicitação, as configurações da Block ação determinam a resposta que o recurso protegido envia de volta ao cliente.
- Count— AWS WAF conta a solicitação, mas não determina se ela deve ser permitida ou bloqueada. Essa não é uma ação de encerramento, o AWS WAF continua processando as regras restantes na web ACL. Nas regras que você define, você pode inserir cabeçalhos personalizados na solicitação e adicionar rótulos com os quais outras regras possam corresponder.
- CAPTCHAe Challenge — AWS WAF usa quebra-cabeças de CAPTCHA e desafios silenciosos para verificar se a solicitação não vem de um bot e AWS WAF usa tokens para rastrear as respostas recentes bem-sucedidas dos clientes.

Os quebra-cabeças de CAPTCHA e os desafios silenciosos só podem ser executados quando os navegadores estão acessando endpoints HTTPS. Os clientes do navegador devem estar sendo executados em contextos seguros para adquirir tokens.

> **Note**
>
> São cobradas taxas adicionais quando você usa a ação de regra CAPTCHA ou Challenge em uma de suas regras ou como uma substituição de ação de regra em um grupo de regras. Para obter mais informações, consulte Preços do AWS WAF.

Essas ações de regra podem ser terminais ou não, dependendo do estado do token na solicitação:

- Não encerramento para token válido e não expirado — Se o token for válido e não expirado de acordo com o CAPTCHA configurado ou o tempo de imunidade de desafio, AWS WAF tratará a solicitação de forma semelhante à ação. Count AWS WAF continua inspecionando a solicitação da web com base nas regras restantes na ACL da web. Semelhante à configuração de Count, nas regras que define, você pode, opcionalmente, configurar essas ações com cabeçalhos personalizados para inserir na solicitação e adicionar rótulos aos quais outras regras possam corresponder.
- AWS WAF Encerramento com solicitação bloqueada de token inválido ou expirado — Se o token for inválido ou a data e hora indicada expirar, encerra a inspeção da solicitação da web e bloqueia a solicitação, semelhante à ação. Block AWS WAF em seguida, responde ao cliente com um código de resposta personalizado. PoisCAPTCHA, se o conteúdo da solicitação indicar que o navegador do cliente pode lidar com isso, AWS WAF envia um quebra-cabeça CAPTCHA em um JavaScript intersticial, projetado para distinguir clientes humanos de bots. Para a Challenge ação, AWS WAF envia um JavaScript intersticial com um desafio silencioso projetado para distinguir navegadores normais de sessões que estão sendo executadas por bots.

Para obter informações adicionais, consulte CAPTCHAe Challenge em AWS WAF.

Para obter informações sobre como utilizar essa opção, consulte Substituir ações de regra para um grupo de regras.

Substituição da ação da regra para Count

O caso de uso mais comum para substituições de ações de regras é substituir algumas ou todas as ações de regras para Count, para testar e monitorar o comportamento de um grupo de regras antes de colocá-lo em produção.

Você também pode usar isso para solucionar problemas de um grupo de regras que está gerando falsos positivos. Falsos positivos ocorrem quando um grupo de regras bloqueia o tráfego que você não espera que ele bloqueie. Se você identificar uma regra em um grupo de regras que bloquearia as solicitações que você deseja permitir, você pode manter a substituição da ação de contagem nessa regra, para evitar que ela atue em suas solicitações.

Para obter mais informações sobre como usar a substituição de ação de regra em testes, consulte Testando e ajustando suas AWS WAF proteções.

Lista JSON: **`RuleActionOverrides`** substitui **`ExcludedRules`**

Se você definiu ações de regras de grupo de regras Count em sua configuração de ACL da web antes de 27 de outubro de 2022, AWS WAF salvou suas substituições na web ACL JSON como. `ExcludedRules` Agora, a configuração JSON para substituir uma regra para Count está nas configurações `RuleActionOverrides`.

Quando você usa o AWS WAF console para editar as configurações existentes do grupo de regras, o console converte automaticamente qualquer `ExcludedRules` configuração no JSON em `RuleActionOverrides` configurações, com a ação de substituição definida como. Count

- Exemplo de configuração atual:

```
      "ManagedRuleGroupStatement": {
         "VendorName": "AWS",
         "Name": "AWSManagedRulesAdminProtectionRuleSet",
         "RuleActionOverrides": [
           {
             "Name": "AdminProtection_URIPATH",
             "ActionToUse": {
               "Count": {}
             }
           }
         ]
```

- Exemplo de configuração antiga:

```
OLD SETTING
```

```
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesAdminProtectionRuleSet",
           "ExcludedRules": [
             {
               "Name": "AdminProtection_URIPATH"
             }
           ]
OLD SETTING
```

Recomendamos que você atualize todas as configurações `ExcludedRules` em suas listas de JSON para configurações `RuleActionOverrides` com a ação definida como Count. A API aceita qualquer uma das configurações, mas você obterá consistência em suas listas de JSON, entre o trabalho do console e o trabalho da API, se usar apenas a nova configuração `RuleActionOverrides`.

Substituição da ação de retorno do grupo de regras para Count

Você pode substituir a ação que o grupo de regras retorna, definindo-a como Count.

> **Note**
>
> Essa não é uma boa opção para testar as regras em um grupo de regras, pois não altera a forma como AWS WAF avalia o próprio grupo de regras. Isso afeta apenas a forma como AWS WAF manipula os resultados que são retornados à ACL da web a partir da avaliação do grupo de regras. Se você quiser testar as regras em um grupo de regras, use a opção descrita na seção anterior, Substituições de ações de regras de grupos de regras.

Quando você substitui a ação do grupo de regras paraCount, AWS WAF processa a avaliação do grupo de regras normalmente.

Se nenhuma regra no grupo de regras corresponder ou se todas as regras correspondentes tiverem uma ação Count, essa substituição não terá efeito no processamento do grupo de regras ou da web ACL.

A primeira regra no grupo de regras que corresponde a uma solicitação da web e que tem uma ação de regra de encerramento faz AWS WAF com que pare de avaliar o grupo de regras e retorne o resultado da ação de encerramento ao nível de avaliação da ACL da web. Nesse ponto, na avaliação da Web ACL, essa substituição entra em vigor. AWS WAF substitui a ação de encerramento para

que o resultado da avaliação do grupo de regras seja somente uma ação. Count AWS WAF em seguida, continua processando o resto das regras na ACL da web.

Para obter informações sobre como utilizar essa opção, consulte Substituição do resultado da avaliação de um grupo de regras para Count.

A ação padrão da web ACL

Ao criar e configurar uma web ACL, você deve definir a ação padrão da web ACL. O AWS WAF aplica essa ação a qualquer solicitação da web que passe por todas as avaliações de regras da web ACL sem ter uma ação de encerramento aplicada a ela. Uma ação de encerramento interrompe a avaliação da web ACL da solicitação e permite que ela continue em seu aplicativo protegido ou a bloqueia. Para informações sobre as ações de regra, consulte Ação da regra.

A ação padrão da web ACL deve determinar a disposição final da solicitação da web, portanto, é uma ação de encerramento:

- Allow: se você deseja permitir que a maioria dos usuários acesse seu website, mas deseja bloquear o acesso a invasores cujas solicitações se originam de endereços IP especificados ou que pareçam conter código SQL mal-intencionado ou valores especificados, escolha Allow como ação padrão. Em seguida, ao adicionar regras à web ACL, adicione regras que identifiquem e bloqueiem as solicitações específicas que você deseja bloquear. Com essa ação, você pode inserir cabeçalhos personalizados na solicitação antes de encaminhá-la para o recurso protegido.
- Block: se você deseja impedir que a maioria dos aspirantes a usuários acesse seu website, mas quer permitir acesso aos usuários cujas solicitações se originem de endereços IP especificados ou cujas solicitações contenham valores especificados, escolha Block como ação padrão. Em seguida, ao adicionar regras à web ACL, adicione regras que identifiquem e permitam as solicitações específicas que você deseja permitir. Por padrão, para a Block ação, o AWS recurso responde com um código de `403 (Forbidden)` status HTTP, mas você pode personalizar a resposta.

Para obter informações sobre como personalizar solicitações e respostas, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Sua configuração de suas próprias regras e grupos de regras depende, em parte, se você deseja permitir ou bloquear a maioria das solicitações da web. Por exemplo, se desejar permitir a maioria das solicitações, defina a ação padrão da web ACL para Allow, e adicione regras que identifiquem solicitações da web que você deseja bloquear, como as seguintes:

- Solicitações originadas de endereços IP que estão fazendo um número sem cabimento de solicitações
- Solicitações originadas de países nos quais você não faz negócios ou que sejam as origens de ataques frequentes
- Solicitações que incluem valores falsos no cabeçalho do `User-agent`
- Solicitações que aparentem incluir código SQL mal-intencionado

As regras do grupo de regras gerenciadas geralmente usam a ação Block, mas nem todas usam. Por exemplo, algumas regras usadas para o Controle de Bots usam as configurações de ação CAPTCHA e Challenge. Para obter informações sobre grupos de regras gerenciadas, consulte Grupos de regras gerenciadas.

Gerenciando os limites de tamanho da inspeção corporal

O limite de tamanho da inspeção do corpo é o tamanho máximo do corpo da solicitação que AWS WAF pode ser inspecionado. Quando o corpo de uma solicitação da web é maior que o limite, o serviço de hospedagem subjacente encaminha apenas o conteúdo que está dentro do limite AWS WAF para inspeção.

- Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB (8.192 bytes).
- Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB (16.384 bytes), e você pode aumentar o limite para qualquer tipo de recurso em incrementos de 16 KB, até 64 KB. As opções de configuração são 16 KB, 32 KB, 48 KB e 64 KB.

Tratamento de corpo de tamanho grande

Se seu tráfego na web incluir corpos maiores que o limite, seu tratamento configurado de tamanho grande será aplicado. Para obter informações sobre as opções de manuseio de tamanhos grandes, consulteTratamento de componentes de solicitação de tamanho grande no AWS WAF.

Considerações sobre preços para aumentar a definição do limite

AWS WAF cobra uma taxa básica para inspecionar o tráfego que está dentro do limite padrão para o tipo de recurso.

Para CloudFront recursos do API Gateway, Amazon Cognito, App Runner e Verified Access, se você aumentar a configuração do limite, o tráfego que AWS WAF pode ser inspecionado incluirá tamanhos

corporais até seu novo limite. Você é cobrado a mais somente pela inspeção de solicitações com tamanhos de corpo maiores do que os 16 KB padrão. Para obter mais informações sobre precificação, consulte Precificação do AWS WAF.

Opções para modificar o limite de tamanho da inspeção da carroceria

Você pode configurar o limite de tamanho da inspeção corporal para CloudFront recursos do API Gateway, Amazon Cognito, App Runner ou Verified Access.

Ao criar ou editar uma ACL da web, você pode modificar os limites de tamanho da inspeção corporal na configuração da associação de recursos. Para a API, consulte a configuração de associação da ACL da web em AssociationConfig. Para o console, consulte a configuração na página em que você especifica os recursos associados à ACL da web. Para obter orientação sobre a configuração do console, consulte Trabalho com :web ACLs.

Configurações para CAPTCHA, desafio e tokens

Você pode configurar opções em sua ACL da web para as regras que usam as ações da Challenge regra CAPTCHA ou e para os SDKs de integração de aplicativos que gerenciam desafios silenciosos de clientes para proteções AWS WAF gerenciadas.

Esses recursos atenuam a atividade dos bots desafiando os usuários finais com quebra-cabeças CAPTCHA e apresentando desafios silenciosos às sessões dos clientes. Quando o cliente responde com sucesso, o AWS WAF fornece um token para ele usar em sua solicitação na web, com timestamp do último quebra-cabeça bem-sucedido e das respostas ao desafio. Para ter mais informações, consulte AWS WAF mitigação inteligente de ameaças.

Na sua configuração de ACL da web, você pode configurar como AWS WAF gerencia esses tokens:

- Tempos de imunidade de CAPTCHA e desafio: especificam por quanto tempo um CAPTCHA ou timestamp de desafio permanece válido. As configurações de web ACL são herdadas por todas as regras que não têm suas próprias configurações de tempo de imunidade definidas e também pelos SDKs de integração de aplicativos. Para ter mais informações, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.
- Domínios de token — Por padrão, AWS WAF aceita tokens somente para o domínio do recurso ao qual a ACL da web está associada. Se você configurar uma lista de domínios de tokens, AWS WAF aceitará tokens para todos os domínios na lista e para o domínio do recurso associado. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

Trabalho com :web ACLs

Esta seção fornece procedimentos para criar, gerenciar e usar ACLs da web por meio do AWS console.

Para qualquer ACL da web que você estiver usando, você pode acessar resumos das métricas de tráfego da web na página da ACL da web no AWS WAF console, na guia Visão geral do tráfego. Os painéis do console fornecem resumos quase em tempo real das CloudWatch métricas da Amazon que são AWS WAF coletadas quando avalia o tráfego web do seu aplicativo. Para obter mais informações sobre o painel, consulte Painéis de visão geral do tráfego de web ACL. Para obter informações adicionais sobre como monitorar o tráfego da sua web ACL, consulte Monitoramento e ajuste.

Risco de tráfego de produção

Antes de implantar alterações em sua web ACL para tráfego de produção, teste-as e ajuste-as em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

Note

O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Tópicos

Criação de uma web ACL

Para criar uma nova web ACL, use o assistente de criação de web ACL seguindo o procedimento encontrado nesta página.

⚠ Risco de tráfego de produção

Antes de implantar alterações em sua web ACL para tráfego de produção, teste-as e ajuste-as em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

Para criar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. Escolha Web ACLs (:web ACLs) no painel de navegação e escolha Create web ACL (Criar web ACL).
3. Em Nome, insira o nome que deseja usar para identificar esta web ACL.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar a web ACL.

4. (Opcional) Em Descrição: opcional, insira uma descrição mais longa para a web ACL, se desejar.
5. Para nome da CloudWatch métrica, altere o nome padrão, se aplicável. Siga as orientações no console para usar caracteres válidos. O nome não pode conter caracteres especiais, espaços em branco ou nomes de métricas reservados para AWS WAF, incluindo “All” e “Default_Action”.

   > **Note**
   >
   > Você não pode alterar o nome da CloudWatch métrica depois de criar a Web ACL.

6. Em Tipo de recurso, escolha a categoria de AWS recurso que você deseja associar a essa ACL da web, CloudFront distribuições da Amazon ou recursos regionais. Para ter mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.
7. Em Região, se você escolheu um tipo de recurso regional, escolha a região em que deseja armazenar AWS WAF a ACL da web.

Só é necessário escolher essa opção para tipos de recursos regionais. Para CloudFront distribuições, a região é codificada para a região Leste dos EUA (Norte da Virgínia),`us-east-1`, para aplicativos globais (). CloudFront

8. (CloudFront, API Gateway, Amazon Cognito, App Runner e Verified Access) Para o limite de tamanho de inspeção por solicitação da Web - opcional, se você quiser especificar um limite de tamanho de inspeção corporal diferente, selecione o limite. A inspeção de tamanhos de carroceria acima do padrão de 16 KB pode gerar custos adicionais. Para obter mais informações sobre esta opção, consulte Gerenciando os limites de tamanho da inspeção corporal.
9. (Opcional) Para AWS Recursos associados - opcional, se você quiser especificar seus recursos agora, escolha Adicionar AWS recursos. Na caixa de diálogo, escolha os recursos que você deseja associar e, em seguida, escolha Adicionar. AWS WAF retorna você para a página Descrever a ACL da web e AWS os recursos associados.
10. Escolha Próximo.
11. (Opcional) Se quiser adicionar grupos de regras gerenciadas, na página Add rules and rule groups (Adicionar regras e grupos de regras) escolha Add rules (Adicionar regras), e, em seguida, escolha Add managed rule groups (Adicionar grupos de regras gerenciados). Faça o seguinte para cada grupo de regras gerenciadas que você deseja adicionar:

    a. Na página Adicionar grupos de regras gerenciadas, expanda a lista para grupos de regras AWS gerenciadas ou para o AWS Marketplace vendedor de sua escolha.

    b. Para o grupo de regras que você deseja adicionar, ative a alternância Adicionar à web ACL na coluna Ação .

    Para personalizar como sua web ACL usa o grupo de regras, escolha Editar. A seguir, são mostradas as configurações de personalização comuns:

    - Substitua as ações da regra para algumas ou todas as regras. Se você não definir uma ação de substituição para uma regra, a avaliação usará a ação de regra definida dentro do grupo de regras. Para obter mais informações sobre esta opção, consulte Opções de substituição de ação para grupos de regras.
    - Reduza o escopo das solicitações da web que o grupo de regras inspeciona adicionando uma instrução de redução de escopo. Para obter mais informações sobre esta opção, consulte Instruções de redução de escopo.
    - Alguns grupos de regras gerenciadas exigem que você forneça configurações adicionais. Consulte a documentação do seu provedor de grupos de regras gerenciadas. Para

obter informações específicas sobre os grupos de regras de regras AWS gerenciadas, consulteAWS Regras gerenciadas para AWS WAF.

Ao concluir suas configurações, escolha Salvar regra.

Escolha Add rules (Adicionar regras) para concluir a adição de regras gerenciadas e retornar à página Add rules and rule groups (Adicionar regras e grupos de regras).

12. (Opcional) Se quiser adicionar seu próprio grupo de regras, na página Add rules and rule groups (Adicionar regras e grupos de regras) escolha Add rules (Adicionar regras), e, em seguida, escolha Add my own rules and rule groups (Adicionar minhas próprias regras e grupos de regras). Faça o seguinte para cada grupo de regras que você deseja adicionar:

    a. Na página Add my own rules and rule groups (Adicionar minhas próprias regras e grupos de regras) escolha Rule group (Grupo de regras).

    b. Em Nome, insira o nome que você deseja usar para a regra do grupo de regras nessa web ACL. Não use nomes que comecem com `AWS`, `Shield`, `PreFM` ou `PostFM`. Essas sequências de caracteres são reservadas ou podem causar confusão com grupos de regras gerenciadas para você por outros serviços. Consulte Grupos de regras fornecidos por outros serviços.

    c. Escolha seu grupo de regras na lista.

    > **Note**
    >
    > Se você quiser substituir as ações de regra de um grupo de regras próprio, primeiro salve-as na ACL da Web e, em seguida, edite a ACL da Web e a declaração de referência do grupo de regras na lista de regras da ACL da Web. Você pode substituir as ações da regra por qualquer configuração de ação válida, da mesma forma que pode fazer com grupos de regras gerenciados.

    d. Escolha Adicionar regra.

13. (Opcional) Se você quiser adicionar sua própria regra, na página Add rules and rule groups (Adicionar regras e grupos de regras), escolha Add rules (Adicionar regras), Add my own rules and rule groups (Adicionar minhas próprias regras e grupos de regras), Rule builder (Construtor de regras), e Editor visual de regras.

> **Note**
>
> O console Editor visual de regras oferece suporte a um nível de aninhamento. Por exemplo, você pode usar uma única instrução `AND` ou `OR` lógica e aninhar um nível de outras instruções dentro dela, mas você não pode aninhar instruções lógicas dentro de instruções lógicas. Para gerenciar instruções de regra mais complexas, use o Editor JSON de regras. Para obter informações sobre todas as opções de regras, consulte AWS WAF regras.
> Este procedimento abrange o Editor visual de regras.

a. Em Nome, insira o nome que deseja usar para identificar esta regra. Não use nomes que comecem com `AWS`, `Shield`, `PreFM` ou `PostFM`. Essas sequências de caracteres são reservadas ou podem causar confusão com grupos de regras gerenciadas para você por outros serviços.

b. Digite sua definição de regra, de acordo com suas necessidades. Você pode combinar regras dentro de instruções de regra `AND` e `OR` lógicas. O assistente orienta você pelas opções de cada regra, de acordo com o contexto. Para obter informações sobre as opções de regras, consulte AWS WAF regras.

c. Em Action (Ação), selecione a ação que você deseja que a regra execute quando ela corresponder a uma solicitação da web. Para obter informações sobre suas escolhas, consulte Ação da regra e Avaliação de regras da web ACL e do grupo de regras.

   Se você estiver usando a ação Challenge ou CAPTCHA, ajuste a configuração do Tempo de imunidade conforme necessário para a regra. Se você não especificar a configuração, a regra a herdará da web ACL. Para modificar as configurações de tempo de imunidade da web ACL, edite a web ACL depois de criá-la. Para obter mais informações sobre os tempos de imunidade, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.

   > **Note**
   >
   > São cobradas taxas adicionais quando você usa a ação de regra CAPTCHA ou Challenge em uma de suas regras ou como uma substituição de ação de regra em um grupo de regras. Para obter mais informações, consulte Preços do AWS WAF.

Se você quiser personalizar a solicitação ou a resposta, escolha as opções para isso e preencha os detalhes da sua personalização. Para ter mais informações, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Se você quiser que sua regra adicione rótulos às solicitações da web correspondentes, escolha as opções para isso e preencha os detalhes do rótulo. Para ter mais informações, consulte AWS WAF rótulos em solicitações da web.

d. Escolha Adicionar regra.

14. Selecione a ação padrão para a web ACL, Block ou Allow. Essa é a ação que AWS WAF ocorre em uma solicitação quando as regras na ACL da web não a permitem ou bloqueiam explicitamente. Para ter mais informações, consulte A ação padrão da web ACL.

    Se você quiser personalizar a ação padrão, escolha as opções para isso e preencha os detalhes da sua personalização. Para ter mais informações, consulte Solicitações e respostas personalizadas da web no AWS WAF.

15. Você pode definir uma Lista de domínios de tokens para permitir o compartilhamento de tokens entre aplicativos protegidos. Os tokens são usados pelas Challenge ações CAPTCHA e pelos SDKs de integração de aplicativos que você implementa ao usar os grupos de regras AWS gerenciadas para controle de AWS WAF fraudes, criação de contas, prevenção de fraudes (ACFP), controle de AWS WAF fraudes, prevenção de aquisição de contas (ATP) e controle de bots. AWS WAF

    Não são permitidos sufixos públicos. Por exemplo, você não pode usar `gov.au` ou `co.uk` como um domínio de token.

    Por padrão, AWS WAF aceita tokens somente para o domínio do recurso protegido. Se você adicionar domínios de token nessa lista, AWS WAF aceitará tokens para todos os domínios na lista e para o domínio do recurso associado. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

16. Escolha Próximo.

17. Na página Definir prioridade da regra, selecione e mova suas regras e grupos de regras para a ordem em que você AWS WAF deseja processá-los. AWS WAF processa as regras começando do topo da lista. Quando você salva a web ACL, o AWS WAF atribui configurações de prioridade numérica às regras, na ordem em que você as listou. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

18. Escolha Próximo.
19. Na página Configurar métricas, revise as opções e aplique as atualizações necessárias. Você pode combinar métricas de várias fontes fornecendo o mesmo nome de CloudWatch métrica para elas.
20. Escolha Próximo.
21. Na página Review and create web ACL (Revisar e criar web ACL) verifique suas definições. Se quiser alterar qualquer área, escolha Edit (Editar) para a área. Isso retorna você à página no assistente de web ACL. Faça quaisquer alterações e, em seguida, escolha Next (Próximo) nas páginas até voltar à página Create web ACL (Revisar e criar web ACL) .
22. Escolha Criar web ACL. Sua nova web ACL está listada na página Web ACLs .

Edição de uma web ACL

Para adicionar ou remover regras de uma web ACL ou alterar as definições de configuração, acesse a web ACL usando o procedimento desta página. Ao atualizar uma ACL da web, AWS WAF fornece cobertura contínua aos recursos que você associou à ACL da web.

> **Risco de tráfego de produção**
>
> Antes de implantar alterações em sua web ACL para tráfego de produção, teste-as e ajuste-as em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

Para editar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da web ACL a ser editada. O console leva você para a descrição da web ACL.

> **Note**
>
> As ACLs da Web gerenciadas por AWS Firewall Manager têm nomes que começam com`FMManagedWebACLV2-`. O administrador do Firewall Manager os gerencia nas AWS WAF políticas do Firewall Manager. Essas web ACLs podem conter conjuntos de grupos de regras designados para serem executados primeiro e por último na web ACL, nos dois lados das regras ou dos grupos de regras que você adicionar e gerenciar. Você não pode alterar nenhuma dessas especificações do primeiro e do último grupo de regras. O primeiro e o último grupos de regras têm nomes que começam com `PREFMManaged-` e `POSTFMManaged-`, respectivamente. Para obter mais informações sobre essas políticas, consulte AWS WAF políticas.

4. Edite a web ACL, conforme necessário. Escolha as guias das áreas de configuração de seu interesse e edite as configurações mutáveis. Para cada configuração que você edita, ao escolher Salvar e retornar à página de descrição da web ACL, o console salva suas alterações na web ACL.

   A seguir estão listadas as guias que contêm componentes de configuração de web ACL.

   - Guia Regras
     - Regras definidas na web ACL: você pode editar e gerenciar as regras que você definiu na web ACL da mesma forma que fez durante a criação da web ACL.

     > **Note**
     >
     > Não altere os nomes de nenhuma regra que você não tenha adicionado manualmente à sua web ACL. Se você estiver usando outros serviços para gerenciar regras para você, alterar seus nomes pode remover ou diminuir a capacidade deles de fornecer as proteções pretendidas. AWS Shield Advanced e AWS Firewall Manager ambos criam regras em sua ACL da web. Para mais informações, consulte Grupos de regras fornecidos por outros serviços.

> **Note**
>
> Se você alterar o nome de uma regra e quiser que o nome da métrica da regra reflita a alteração, você também deverá atualizar o nome da métrica. AWS WAF não atualiza automaticamente o nome da métrica de uma regra quando você altera o nome da regra. Você pode alterar o nome da métrica ao editar a regra no console, usando o editor JSON de regras. Você também pode alterar os dois nomes por meio das APIs e em qualquer lista JSON usada para definir sua web ACL ou grupo de regras.

Para obter informações sobre regras e configurações de grupos de regras, consulte AWS WAF regras e AWS WAF grupos de regras.

- Unidades de capacidade de regras de web ACL usadas: o uso atual da capacidade da sua web ACL. Isso é somente para visualização.
- Ação padrão da web ACL para solicitações que não correspondem a nenhuma regra: para obter informações sobre essa configuração, consulte A ação padrão da web ACL.
- Configurações de CAPTCHA e desafio da web ACL: esses tempos de imunidade determinam por quanto tempo um CAPTCHA ou token de desafio permanece válido após ser adquirido. Você só pode modificar essa configuração aqui, depois de criar a web ACL. Para obter informações sobre essas configurações, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.
- Lista de domínios de tokens — AWS WAF aceita tokens para todos os domínios da lista e para o domínio do recurso associado. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

- Aba de AWS recursos associados
  - Limite de tamanho de inspeção de solicitações da Web — Incluído somente para ACLs da Web que protegem CloudFront distribuições. O limite de tamanho da inspeção do corpo determina quanto do componente do corpo é encaminhado AWS WAF para inspeção. Para obter mais informações sobre essa configuração, consulte Gerenciando os limites de tamanho da inspeção corporal.
  - AWS Recursos associados — A lista de recursos aos quais a ACL da web está atualmente associada e protegendo. Você pode localizar recursos que estão na mesma região da

web ACL e associá-los à web ACL. Para ter mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

- Guia Corpos de resposta personalizados
  - Corpos de resposta personalizados que estão disponíveis para uso por suas regras de web ACL que têm a ação definida como Block. Para ter mais informações, consulte Respostas personalizadas para ações Block.
- Guia Logs e métricas
  - Logs: logs do tráfego que a web ACL avalia. Para mais informações, consulte Registrando AWS WAF tráfego de ACL da web.
  - Solicitações amostradas: informações sobre as regras que correspondem às solicitações da web. Para obter informações sobre como visualizar solicitações de exemplo, consulte Visualizar um exemplo de solicitações da web.
  - CloudWatch métricas — Métricas para as regras em sua ACL da web. Para obter informações sobre CloudWatch as métricas da Amazon, consulteMonitoramento com a Amazon CloudWatch.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Gerenciar o comportamento do grupo de regras em uma web ACL

Esta seção descreve suas opções para modificar o modo como você usa um grupo de regras na web ACL. Essas informações se aplicam a todos os tipos de grupos de regras. Depois de adicionar um grupo de regras a uma web ACL, você pode substituir as ações das regras individuais no grupo de regras para Count ou para qualquer outra configuração de ação de regra válida. Você também pode substituir a ação resultante do grupo de regras para Count, o que não tem efeito sobre como as regras são avaliadas dentro do grupo de regras.

Para obter informações sobre essas opções, consulte Opções de substituição de ação para grupos de regras.

Substituir ações de regra para um grupo de regras

Para cada grupo de regras em uma web ACL, você pode substituir as ações da regra contida, definindo a ação para todas ou algumas das regras.

O caso de uso mais comum para isso é substituir as ações da regra para Count para testar regras novas ou atualizadas. Se você tiver métricas ativadas, receberá métricas para cada regra que você substituir. Para ter mais informações sobre armazenamento, consulte Testando e ajustando suas AWS WAF proteções.

Para substituir ações de regra para um grupo de regras

Você pode fazer essas alterações ao adicionar um grupo de regras gerenciadas à ACL da web e pode fazê-las em qualquer tipo de grupo de regras ao editar a ACL da web. Essas instruções são para um grupo de regras que já foi adicionado à web ACL. Veja informações adicionais sobre essa opção emSubstituições de ações de regras de grupos de regras.

1. Edite a web ACL.
2. Na guia Regras na página da web ACL, selecione o grupo de regras e escolha Editar.
3. Na seção Regras do grupo de regras, gerencie as configurações de ação conforme necessário.

    - Todas as regras: para definir uma ação de substituição para todas as regras no grupo de regras, abra o menu suspenso Substituir todas as ações de regra e selecione a ação de substituição. Para remover as substituições de todas as regras, selecione Remover todas as substituições.
    - Regra única: para definir uma ação de substituição para uma única regra, abra a lista suspensa da regra e selecione a ação de substituição. Para remover a substituição de uma regra, abra a lista suspensa da regra e selecione Remover substituição.

4. Quando terminar de fazer as alterações, escolha Salvar regra. As configurações de ação de regra e ação de substituição estão listadas na página do grupo de regras.

O exemplo de lista JSON a seguir mostra uma instrução de grupo de regras dentro de uma web ACL que substitui as ações de regra para Count para as regras `CategoryVerifiedSearchEngine` e `CategoryVerifiedSocialMedia`. No JSON, você substitui todas as ações da regra fornecendo uma entrada `RuleActionOverrides` para cada regra individual.

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
        "ExcludedRules": []
    },
   "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

Substituição do resultado da avaliação de um grupo de regras para Count

Você pode substituir a ação resultante da avaliação de um grupo de regras sem alterar a forma como as regras do grupo de regras são configuradas ou avaliadas. Essa opção não é comumente usado.

Se alguma regra no grupo de regras resultar em uma correspondência, essa substituição definirá a ação resultante do grupo de regras como Count.

> **Note**
>
> Esse é um caso de uso incomum. A maioria das substituições de ações é feita no nível da regra, dentro do grupo de regras, conforme descrito em. Substituir ações de regra para um grupo de regras

Você pode substituir a ação resultante do grupo de regras na web ACL ao adicionar ou editar o grupo de regras. No console, abra o painel Substituir ação do grupo de regras: opcional do grupo de regras e habilite a substituição. No JSON, defina `OverrideAction` na instrução de grupo de regras, conforme mostrado no seguinte exemplo de lista:

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

Associando ou desassociando uma ACL da web com um recurso AWS

Você pode usar AWS WAF para criar as seguintes associações entre o Web ACLS e seus recursos:

- Associe uma web ACL regional a qualquer um dos recursos regionais listados abaixo. Para essa opção, a web ACL deve estar na mesma região que seu recurso.
  - API REST do Amazon API Gateway

  - Application Load Balancer
  - AWS AppSync API do GraphQL
  - Grupo de usuários do Amazon Cognito
  - AWS App Runner serviço
  - AWS Instância de acesso verificado
- Associe uma ACL global da web a uma CloudFront distribuição da Amazon. A web ACL global terá uma região de codificação rígida da região Leste dos EUA (Norte da Virgínia).

Você também pode associar uma ACL da web a uma CloudFront distribuição ao criar ou atualizar a própria distribuição. Para obter informações, consulte Como usar AWS WAF para controlar o acesso ao seu conteúdo no Amazon CloudFront Developer Guide.

Restrições às associações múltiplas

Você pode associar uma única ACL da web a um ou mais AWS recursos, de acordo com as seguintes restrições:

- Você pode associar cada AWS recurso a somente uma ACL da web. A relação entre a Web ACL e AWS os recursos é one-to-many.
- Você pode associar uma ACL da web a uma ou mais CloudFront distribuições. Você não pode associar uma Web ACL associada a uma CloudFront distribuição a nenhum outro tipo de AWS recurso.

Restrições adicionais

As seguintes restrições adicionais se aplicam a associações de web ACL:

- Você só pode associar uma web ACL a um Application Load Balancer nas Regiões da AWS. Por exemplo, você não pode associar uma web ACL a um Application Load Balancer que esteja no AWS Outposts.
- Você não pode associar um grupo de usuários do Amazon Cognito a uma ACL da web que usa o grupo de regras gerenciadas de prevenção de AWS WAF fraudes na criação de contas do Fraud Control (ACFP) `AWSManagedRulesACFPRuleSet` ou o grupo de regras gerenciadas de prevenção de aquisição de contas do AWS WAF Fraud Control (ATP). `AWSManagedRulesATPRuleSet` Para obter informações sobre prevenção de fraudes na criação de contas, consulte AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes

(ACFP). Para obter informações sobre prevenção de apropriação de contas, consulte AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP).

⚠ Risco de tráfego de produção

Antes de implantar sua web ACL para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

Para associar uma ACL da web a um recurso AWS

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da web ACL que deseja associar a um recurso. O console leva você para a descrição da web ACL, onde é possível editá-la.
4. Na guia AWS Recursos associados, escolha Adicionar AWS recursos.
5. Quando solicitado, selecione o tipo de recurso, selecione o botão de opção ao lado do recurso que você deseja associar e depois selecione Adicionar.

Para desassociar uma Web ACL de um recurso AWS

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da web ACL que deseja dissociar de seu recurso. O console leva você para a descrição da web ACL, onde é possível editá-la.
4. Na guia AWS Recursos associados, selecione o recurso do qual você deseja desassociar essa Web ACL.

> **Note**
>
> Você deve desassociar um recurso por vez. Não escolha vários recursos.

5. Escolha Desassociar. O console abre um diálogo de confirmação. Confirme sua opção de desassociar a Web ACL do AWS recurso.

Exclusão de uma web ACL

Para excluir uma ACL da Web, primeiro desassocie todos os AWS recursos da ACL da Web. Execute o procedimento a seguir.

Para excluir uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Selecione o nome da web ACL a ser excluída. O console leva você para a descrição da web ACL, onde é possível editá-la.
4. Na guia AWS Recursos associados, para cada recurso associado, selecione o botão de rádio ao lado do nome do recurso e escolha Desassociar. Isso desassocia a ACL da web de seus recursos. AWS
5. No painel de navegação, selecione Web ACLs.
6. Selecione o botão de opção ao lado da web ACL que você está excluindo e selecione Delete (Excluir).

AWS WAF grupos de regras

Um grupo de regras é um conjunto reutilizável de regras que você pode adicionar a uma web ACL. Para obter mais informações web ACLs, consulte AWS WAF listas de controle de acesso à web (ACLs da web).

Os grupos de regras se enquadram em duas categorias principais:

- Seus próprios grupos de regras, que você cria e mantém.

- Grupos de regras AWS gerenciadas que as equipes de regras gerenciadas criam e mantêm para você.
- Grupos de regras gerenciados que AWS Marketplace os vendedores criam e mantêm para você.
- Grupos de regras que pertencem e são gerenciados por outros serviços, como AWS Firewall Manager o Shield Advanced.

Diferenças entre grupos de regras e web ACLs

Grupos de regras e web ACLs contêm regras que são definidas da mesma maneira em ambos os locais. Os grupos de regras diferem das web ACLs das seguintes maneiras:

- Os grupos de regras não podem conter instruções de referência de grupos de regras.
- Você pode reutilizar um único grupo de regras em várias web ACLs adicionando uma instrução de referência de grupo de regras a cada web ACL. Não é possível reutilizar uma web ACL.
- Grupos de regras não têm ações padrão. Em uma web ACL, você define uma ação padrão para cada regra ou grupo de regras que você incluir. Cada regra individual dentro de um grupo de regras ou web ACL tem uma ação definida.
- Você não associa diretamente um grupo de regras a um AWS recurso. Para proteger recursos usando um grupo de regras, use o grupo de regras em uma web ACL.
- As web ACLs têm uma capacidade máxima definida pelo sistema de 5.000 unidades de capacidade da web ACL (WCUs). Cada grupo de regras tem uma configuração WCU que deve ser definida na criação. Você pode usar essa configuração para calcular os requisitos de capacidade adicionais que o uso de um grupo de regras adicionaria à web ACL. Para obter informações sobre WCUs, consulte AWS WAF unidades de capacidade web ACL (WCUs).

Para obter mais informações sobre regras, consulte AWS WAF regras.

Esta seção fornece orientações [ara criar e gerenciar seus próprios grupos de regras, descreve os grupos de regras gerenciados que estão disponíveis para você e fornece orientações para usar os grupos de regras gerenciadas.

Tópicos

Grupos de regras gerenciadas

Grupos de regras gerenciadas são coleções de ready-to-use regras predefinidas que AWS AWS Marketplace os vendedores escrevem e mantêm para você. AWS WAF O preço básico se aplica ao uso de qualquer grupo de regras gerenciadas. Para obter informações sobre AWS WAF preços, consulte AWS WAF Preços.

- Os grupos de regras AWS gerenciadas para controle de AWS WAF bots, controle de AWS WAF fraudes, prevenção de aquisição de contas (ATP) e controle de fraudes para prevenção de AWS WAF fraudes na criação de contas (ACFP) estão disponíveis por taxas adicionais, além das cobranças básicas. AWS WAF Para obter detalhes sobre os preços, consulte Preços do AWS WAF.
- Todos os outros grupos de regras de regras AWS gerenciadas estão disponíveis para AWS WAF os clientes sem custo adicional.
- AWS Marketplace grupos de regras gerenciadas estão disponíveis por assinatura em AWS Marketplace. Cada um desses grupos de regras pertence e é gerenciado pelo AWS Marketplace vendedor. Para obter informações sobre preços para usar um grupo de regras AWS Marketplace gerenciadas, entre em contato com o AWS Marketplace vendedor.

Alguns grupos de regras gerenciados são projetados para ajudar a proteger tipos específicos de aplicativos da WebWordPress, como Joomla ou PHP. Outros oferecem ampla proteção contra ameaças conhecidas ou vulnerabilidades de aplicativos web comuns, como as listadas no OWASP Top 10. Se estiver sujeito à compatibilidade regulatória, como PCI ou HIPAA, você poderá usar grupos de regras gerenciadas para atender aos requisitos de firewall do aplicativo web.

Atualizações automáticas

Manter se atualizado sobre o panorama de ameaças em constante alteração pode ser demorado e caro. Os grupos de regras do Marketplace podem economizar tempo ao implementar e usar o AWS WAF. Muitos AWS AWS Marketplace vendedores atualizam automaticamente os grupos de regras gerenciados e fornecem novas versões dos grupos de regras quando surgem novas vulnerabilidades e ameaças.

Em alguns casos, AWS é notificado sobre novas vulnerabilidades antes da divulgação pública, devido à sua participação em várias comunidades privadas de divulgação. Nesses casos, AWS pode atualizar os grupos de regras de regras AWS gerenciadas e implantá-los para você mesmo antes que uma nova ameaça seja amplamente conhecida.

Acesso restrito às regras em um grupo de regras gerenciadas

Cada grupo de regras gerenciadas fornece uma descrição abrangente dos tipos de ataques e vulnerabilidades contra os quais ele foi projetado para proteger. Para proteger a propriedade intelectual dos provedores do grupo de regras, você não poderá visualizar todos os detalhes para as regras individuais dentro de um grupo de regras. Essa restrição também ajuda a impedir que usuários mal-intencionados projetem ameaças que ignorem especificamente regras publicadas.

Tópicos

- Grupos de regras gerenciados com versão
- Trabalhar com grupos de regras gerenciadas
- AWS Regras gerenciadas para AWS WAF
- AWS Marketplace grupos de regras gerenciados

Grupos de regras gerenciados com versão

Muitos provedores de grupos de regras gerenciados usam o controle de versão para atualizar as opções e os recursos de um grupo de regras. Normalmente, uma versão específica de um grupo de regras gerenciadas é estática. Ocasionalmente, um provedor pode precisar atualizar algumas ou todas as versões estáticas de um grupo de regras gerenciadas, por exemplo, para responder a uma ameaça de segurança emergente.

Ao usar um grupo de regras gerenciadas com controle de versão em sua ACL da web, você pode selecionar a versão padrão e deixar que o provedor gerencie qual versão estática você usa, ou você pode selecionar uma versão estática específica.

Não consegue encontrar a versão que você quer?

Se você não vê uma versão na lista de versões de um grupo de regras, a versão provavelmente está programada para expirar ou já expirou. Depois que uma versão está programada para expirar, AWS WAF não é mais possível escolhê-la para o grupo de regras.

Notificações de SNS para grupos de regras de regras AWS gerenciadas

Todos os grupos de regras de regras AWS gerenciadas fornecem notificações de controle de versão e atualização do SNS, exceto o grupo de regras de reputação de IP. Todos os grupos de regras AWS gerenciadas que fornecem notificações usam o mesmo tópico do SNS Amazon Resource Name (ARN). Para se inscrever para receber notificações do SNS, consulteComo receber notificações sobre novas versões e atualizações.

Tópicos

Ciclo de vida de versão para grupos de regras gerenciadas

Os provedores lidam com os seguintes estágios do ciclo de vida de uma versão estática do grupo de regras gerenciadas:

- Lançamento e atualizações: um provedor de grupos de regras gerenciadas anuncia as próximas e novas versões estáticas de seus grupos de regras gerenciadas por meio de notificações para um tópico do Amazon Simple Notification Service (Amazon SNS). Os provedores também podem usar o tópico para comunicar outras informações importantes sobre seus grupos de regras, como atualizações urgentes e necessárias.

  Você pode se inscrever no tópico do grupo de regras e configurar como deseja receber notificações. Para obter mais informações, consulte Como receber notificações sobre novas versões e atualizações.
- Programação de expiração: um provedor de grupos de regras gerenciadas programa versões mais antigas de um grupo de regras para expiração. Uma versão programada para expirar não pode ser adicionada às suas regras de web ACL. Depois que a expiração é programada para uma versão, AWS WAF monitora a expiração com uma métrica de contagem regressiva na Amazon CloudWatch.
- Expiração da versão — Se você tiver uma ACL da web configurada para usar uma versão expirada de um grupo de regras gerenciadas, durante a avaliação da ACL da web, AWS WAF usará a versão padrão do grupo de regras. Além disso, AWS WAF bloqueia todas as atualizações da Web ACL que não removam o grupo de regras nem alterem sua versão para uma não expirada.

Se você usa grupos de regras AWS Marketplace gerenciados, peça ao provedor qualquer informação adicional sobre os ciclos de vida da versão.

Expiração da versão para grupos de regras gerenciados

Se você usa uma versão específica de um grupo de regras, certifique-se de não continuar usando uma versão após a data de expiração. Você pode monitorar a expiração da versão por meio das notificações do SNS do grupo de regras e por meio das CloudWatch métricas da Amazon.

Se uma versão que você está usando em uma ACL da Web expirar, AWS WAF bloqueia todas as atualizações da ACL da Web que não incluam a mudança do grupo de regras para uma versão não expirada. Você pode atualizar o grupo de regras para uma versão disponível ou removê-lo da sua ACL da web.

O tratamento da expiração de um grupo de regras gerenciadas depende do provedor do grupo de regras. Para grupos de regras de regras AWS gerenciadas, uma versão expirada é automaticamente alterada para a versão padrão do grupo de regras. Para grupos de AWS Marketplace regras, pergunte ao provedor como eles lidam com a expiração.

Quando o provedor cria uma nova versão do grupo de regras, ele define a vida útil prevista da versão. Embora a versão não esteja programada para expirar, o valor CloudWatch métrico da Amazon é definido como a configuração de vida útil prevista e, em CloudWatch, você verá um valor fixo para a métrica. Depois que o provedor programa a métrica para expirar, o valor da métrica diminui a cada dia até chegar a zero no dia da expiração. Para obter informações sobre o monitoramento da expiração, consulteAcompanhamento da expiração da versão.

Práticas recomendadas para lidar com versões gerenciadas de grupos de regras

Siga essa orientação de práticas recomendadas para lidar com o versionamento ao usar um grupo de regras gerenciadas versionado.

Ao usar um grupo de regras gerenciadas em sua web ACL, você pode optar por usar uma versão específica e estática do grupo de regras ou pode optar por usar a versão padrão:

- Versão padrão — AWS WAF sempre define a versão padrão como a versão estática atualmente recomendada pelo provedor. Quando o provedor atualiza a versão estática recomendada, o AWS WAF atualiza automaticamente a configuração da versão padrão para o grupo de regras em sua web ACL.

  Ao usar a versão padrão de um grupo de regras gerenciadas, faça o seguinte como prática recomendada:

  - Inscreva-se nas notificações: inscreva-se nas notificações de mudanças no grupo de regras e fique de olho nelas. A maioria dos provedores envia notificações avançadas sobre novas versões estáticas e alterações na versão padrão. Eles permitem que você verifique os efeitos de uma nova versão estática antes AWS de mudar a versão padrão para ela. Para obter mais informações, consulte Como receber notificações sobre novas versões e atualizações.
  - Revise os efeitos das configurações da versão estática e fazer os ajustes necessários antes que seu padrão seja definido: antes que seu padrão seja definido como uma nova versão estática,

revise os efeitos da versão estática no monitoramento e no gerenciamento de suas solicitações da web. A nova versão estática pode ter novas regras para revisar. Procure falsos positivos ou outros comportamentos inesperados, caso precise modificar a forma como você usa o grupo de regras. Você pode definir regras para contar, por exemplo, para impedir que elas bloqueiem o tráfego enquanto você descobre como deseja lidar com o novo comportamento. Para ter mais informações, consulte Testando e ajustando suas AWS WAF proteções.

- Versão estática: se você optar por usar uma versão estática, deverá atualizar manualmente a configuração da versão quando estiver pronto para adotar uma nova versão do grupo de regras.

  Ao usar a versão estática de um grupo de regras gerenciadas, faça o seguinte como prática recomendada:

  - Mantenha sua versão atualizada: mantenha seu grupo de regras gerenciadas o mais próximo possível da versão mais recente. Quando uma nova versão for lançada, teste-a, ajuste as configurações conforme necessário e implemente-a em tempo hábil. Para ter mais informações sobre testes, consulte Testando e ajustando suas AWS WAF proteções.
  - Inscreva-se para receber notificações: inscreva-se nas notificações de alterações no grupo de regras para saber quando seu provedor lançará novas versões estáticas. A maioria dos provedores notifica com antecedência as alterações de versão. Além disso, seu provedor pode precisar atualizar a versão estática que você está usando para fechar uma brecha de segurança ou por outros motivos urgentes. Você saberá o que está acontecendo se estiver inscrito nas notificações do provedor. Para ter mais informações, consulte Como receber notificações sobre novas versões e atualizações.
  - Evite a expiração da versão: não permita que uma versão estática expire enquanto você a estiver usando. O tratamento de versões expiradas pelo provedor pode variar e pode incluir forçar uma atualização para uma versão disponível ou outras alterações que possam ter consequências inesperadas. Acompanhe a métrica de AWS WAF expiração e defina um alarme que forneça um número suficiente de dias para atualizar com êxito para uma versão compatível. Para ter mais informações, consulte Acompanhamento da expiração da versão.

Trabalhar com grupos de regras gerenciadas

Esta seção fornece orientações para acessar e gerenciar seus grupos de regras gerenciadas.

Ao adicionar um grupo de regras gerenciadas à sua web ACL, você pode escolher as mesmas opções de configuração que faria com seus próprios grupos de regras, além de configurações adicionais.

Por meio do console, você acessa as informações gerenciadas do grupo de regras durante o processo de adição e edição das regras em suas :web ACLs. Por meio das APIs e da interface de linha de comandos (CLI), você pode solicitar diretamente informações gerenciadas do grupo de regras.

Ao usar um grupo de regras gerenciadas na sua web ACL, você pode editar as seguintes configurações:

- Versão: isso estará disponível somente se o grupo de regras for versionado. Para ter mais informações, consulte Grupos de regras gerenciados com versão.
- Substituir ações de regras: você pode substituir as ações das regras no grupo de regras por qualquer ação. Configurá-los como Count é útil para testar um grupo de regras antes de usá-lo para gerenciar suas solicitações da web. Para ter mais informações, consulte Substituições de ações de regras de grupos de regras.
- Instrução de redução de escopo: você pode adicionar uma instrução de redução de escopo para filtrar solicitações da web que você não deseja avaliar com o grupo de regras. Para ter mais informações, consulte Instruções de redução de escopo.
- Substituir ação do grupo de regras: você pode substituir a ação que resulta da avaliação do grupo de regras e defini-la como Count somente. Essa opção não é comumente usada. Isso não altera a forma como AWS WAF avalia as regras no grupo de regras. Para ter mais informações, consulte Substituição da ação de retorno do grupo de regras para Count.

Para editar as configurações do grupo de regras gerenciadas em sua web ACL

- Console
  - Opção) Ao adicionar o grupo de regras gerenciadas à sua web ACL, você pode escolher Editar para visualizar e editar as configurações.
  - (Opção) Depois de adicionar o grupo de regras gerenciadas à sua web ACL, na página :web ACLs, escolha a web ACL que você acabou de criar. Isso leva você para a página de edição da web ACL.
    - Escolha Regras.
    - Selecione o grupo de regras e escolha Editar para visualizar e editar as configurações.
- APIs e CLI: fora do console, você pode gerenciar as configurações do grupo de regras gerenciadas ao criar e atualizar a web ACL.

Recuperação da lista de grupos de regras gerenciadas

Você pode recuperar a lista de grupos de regras gerenciadas que estão disponíveis para uso em suas :web ACLs. A lista inclui o seguinte:

- Todos os grupos de regras de regras AWS gerenciadas.
- Os grupos de AWS Marketplace regras nos quais você se inscreveu.

> **Note**
>
> Para obter informações sobre como se inscrever em grupos de AWS Marketplace regras, consulteAWS Marketplace grupos de regras gerenciados.

Quando você recupera a lista de grupos de regras gerenciadas, a lista que você recebe depende da interface que você está usando:

- Console — Por meio do console, você pode ver todos os grupos de regras gerenciados, incluindo os grupos de AWS Marketplace regras nos quais você ainda não se inscreveu. Para aqueles em que você ainda não se inscreveu, a interface fornece links que você pode seguir para fazê-lo.
- APIs e CLI: fora do console, sua solicitação retorna somente os grupos de regras que estão disponíveis para você usar.

Para recuperar a lista de grupos de regras gerenciadas

- Console: durante o processo de criação de uma web ACL, na página Adicionar regras e grupos de regras, escolha Adicionar grupos de regras gerenciadas. No nível superior, os nomes dos provedores são listados. Expanda cada listagem de fornecedor para ver a lista de grupos de regras gerenciadas. Para grupos de regras versionados, as informações mostradas nesse nível são para a versão padrão. Quando você adiciona um grupo de regras gerenciado à web ACL, o console o lista com base no esquema de nomeação `<Vendor Name>-<Managed Rule Group Name>`.
- API:
  - `ListAvailableManagedRuleGroups`
- CLI:
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

Recuperação das regras em um grupo de regras gerenciadas

Você pode recuperar uma lista de regras em um grupo de regras gerenciadas. As chamadas de API e CLI retornam as especificações de regras que você pode referenciar no modelo JSON ou por meio dele. AWS CloudFormation

Para recuperar a lista de regras em um grupo de regras gerenciadas

- Console
  - (Opção) Ao adicionar o grupo de regras gerenciadas à sua web ACL, você pode escolher Editar para visualizar as configurações.
  - (Opção) Depois de adicionar o grupo de regras gerenciadas à sua web ACL, na página :web ACLs, escolha a web ACL que você acabou de criar. Isso leva você para a página de edição da web ACL.
    - Escolha Regras.
    - Selecione o grupo de regras para o qual você deseja ver uma lista de regras e escolha Editar. AWS WAF mostra a lista de regras no grupo de regras.
- API: `DescribeManagedRuleGroup`
- CLI: `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Recuperação das versões disponíveis para um grupo de regras gerenciadas

As versões disponíveis de um grupo de regras gerenciadas são versões que ainda não foram programadas para expirar. A lista indica qual versão é a versão padrão atual para o grupo de regras.

Para recuperar uma lista das versões disponíveis de um grupo de regras gerenciadas

- Console
  - (Opção) Ao adicionar o grupo de regras gerenciadas à sua web ACL, você pode escolher Editar para visualizar as informações do grupo de regras. Expanda o menu suspenso Versão para ver a lista de versões disponíveis.
  - (Opção) Depois de adicionar o grupo de regras gerenciadas à sua web ACL, escolha Editar na web ACL e, em seguida, selecione e edite a regra do grupo de regras. Expanda o menu suspenso Versão para ver a lista de versões disponíveis.
- API:

  - `ListAvailableManagedRuleGroupVersions`
- CLI:
  - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Como adicionar um grupo de regras gerenciadas a uma web ACL por meio do console

Essa orientação se aplica a todos os grupos de regras de regras AWS gerenciadas e aos grupos de AWS Marketplace regras nos quais você está inscrito.

> **Risco de tráfego de produção**
>
> Antes de implantar alterações em sua web ACL para tráfego de produção, teste-as e ajuste-as em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

Para adicionar um grupo de regras gerenciadas a uma web ACL por meio do console

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Na página :web ACLs, na lista de :web ACLs, selecione aquela à qual você deseja adicionar o grupo de regras. Você irá para a página da web ACL única.
4. Na página de configurações da web ACL, escolha a guia Regras.
5. No painel Regras, escolha Adicionar regras, então Adicionar grupos de regras gerenciadas.

6. Na página Adicionar grupos de regras gerenciadas, expanda a seleção do fornecedor do seu grupo de regras para ver a lista de grupos de regras disponíveis.
7. Para cada grupo de regras que você deseja adicionar, escolha Adicionar à web ACL. Se você quiser alterar a configuração da web ACL para o grupo de regras, escolha Editar, faça suas alterações e escolha Salvar regra. Para obter informações sobre as opções, consulte a orientação de versionamento em Grupos de regras gerenciados com versão e a orientação para usar um grupo de regras gerenciadas em uma web ACL em Declaração do grupo de regras gerenciadas.
8. Na página Adicionar grupos de regras gerenciadas, escolha Adicionar regras.
9. Na página Definir prioridade da regra, ajuste a ordem em que as regras são executadas conforme necessário e escolha Salvar. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

Na página da sua web ACL, os grupos de regras gerenciadas que você adicionou estão listados na guia Regras.

Teste e ajuste todas as alterações em suas AWS WAF proteções antes de usá-las para tráfego de produção. Para mais informações, consulte Testando e ajustando suas AWS WAF proteções.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Como receber notificações sobre novas versões e atualizações de um grupo de regras gerenciadas

Um provedor de grupos de regras gerenciadas usa notificações do SNS para anunciar alterações no grupo de regras, como novas versões futuras e atualizações de segurança urgentes.

Para assinar as notificações do SNS

Para se inscrever nas notificações de um grupo de regras, você cria uma assinatura do Amazon SNS para o ARN do tópico do Amazon SNS do grupo de regras na região Leste dos EUA (Norte da Virgínia) us-east-1.

Para obter informações sobre como se inscrever, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> Crie sua assinatura para o tópico do SNS somente na região us-east-1.

Todos os grupos de regras do AWS Managed Rules versionados usam o mesmo tópico do SNS Amazon Resource Name (ARN). Para obter mais informações sobre notificações de grupos de regras de regras AWS gerenciadas, consulteNotificações de implantação.

Onde encontrar o ARN do tópico do Amazon SNS para um grupo de regras gerenciadas

AWS Os grupos de regras de regras gerenciadas usam um único ARN de tópico do SNS, para que você possa recuperar o ARN do tópico de um dos grupos de regras e se inscrever nele para receber notificações de todos os grupos de regras de regras gerenciadas que fornecem notificações AWS do SNS.

- Console
  - (Opção) Ao adicionar o grupo de regras gerenciadas à sua web ACL, escolha Editar para ver as informações do grupo de regras, que inclui o ARN do tópico do Amazon SNS do grupo de regras.
  - (Opção) Depois de adicionar o grupo de regras gerenciadas à sua web ACL, escolha Editar na web ACL e, em seguida, selecione e edite a regra do grupo de regras para ver o ARN do tópico do Amazon SNS do grupo de regras.
- API: `DescribeManagedRuleGroup`

- CLI: `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Para obter informações gerais sobre os formatos de notificação do Amazon SNS e como filtrar as notificações que você recebe, consulte Análise de formatos de mensagens e Políticas de filtro de assinatura do Amazon SNS no guia do desenvolvedor do Amazon Simple Notification Service.

Acompanhamento da expiração da versão de um grupo de regras

Se você usa uma versão específica de um grupo de regras, certifique-se de não continuar usando uma versão após a data de expiração.

> **Tip**
>
> Inscreva-se para receber notificações do Amazon SNS para grupos de regras gerenciados e mantenha-se atualizado com as versões de grupos de regras gerenciadas. Você se beneficiará da maioria das up-to-date proteções do grupo de regras e permanecerá antes da expiração. Para mais informações, consulte Como receber notificações sobre novas versões e atualizações.

Para monitorar o agendamento de expiração para um grupo de regras gerenciado por meio da Amazon CloudWatch

1. Em CloudWatch, localize as métricas de expiração do seu grupo AWS WAF de regras gerenciadas. As métricas têm os seguintes nomes e dimensões:
   - Nome da métrica: DaysToExpiry
   - Dimensões de métrica: Region, ManagedRuleGroup, Vendor e Version

   Se você tiver um grupo de regras gerenciadas em sua web ACL que esteja avaliando o tráfego, você obterá uma métrica para isso. A métrica não está disponível para grupos de regras que você não usa.
2. Defina um alarme para as métricas nas quais você está interessado, para que você seja notificado a tempo de mudar para uma versão mais recente do grupo de regras.

Para obter informações sobre o uso de CloudWatch métricas da Amazon e a configuração de alarmes, consulte o Guia CloudWatch do usuário da Amazon.

Exemplo de configurações de grupos de regras gerenciadas em JSON e YAML

As chamadas de API e CLI retornam uma lista de todas as regras no grupo de regras gerenciadas que você pode referenciar no modelo JSON ou por meio dele. AWS CloudFormation

JSON

Você pode consultar e modificar grupos de regras gerenciadas dentro de uma instrução de regra usando JSON. A lista a seguir mostra o grupo de regras de regras AWS gerenciadas,`AWSManagedRulesCommonRuleSet`, no formato JSON. A especificação RuleActionOverrides lista uma regra cuja ação foi substituída por Count.

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
```

```
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

Você pode consultar e modificar grupos de regras gerenciadas em uma instrução de regra usando o modelo YAML do AWS CloudFormation . A lista a seguir mostra o grupo de regras de regras AWS gerenciadas`AWSManagedRulesCommonRuleSet`,, no AWS CloudFormation modelo. A especificação RuleActionOverrides lista uma regra cuja ação foi substituída por Count.

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS Regras gerenciadas para AWS WAF

AWS O Managed Rules for AWS WAF é um serviço gerenciado que fornece proteção contra vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados. Você tem a opção de selecionar um ou mais grupos de regras das Regras AWS Gerenciadas para cada ACL da Web, até o limite máximo da unidade de capacidade da ACL da Web (WCU).

Mitigação de falsos positivos e testes de mudanças no grupo de regras

Antes de usar qualquer grupo de regras gerenciadas na produção, teste-o em um ambiente que não seja de produção, conforme as orientações em Testando e ajustando suas AWS WAF proteções. Siga as orientações de teste e ajuste ao adicionar um grupo de regras à sua web ACL, para testar

uma nova versão de um grupo de regras e sempre que um grupo de regras não estiver gerenciando seu tráfego da web conforme necessário.

Responsabilidades de segurança compartilhadas

AWS As regras gerenciadas foram projetadas para proteger você contra ameaças comuns na web. Quando usados de acordo com a documentação, os grupos de regras de regras AWS gerenciadas adicionam outra camada de segurança aos seus aplicativos. No entanto, os grupos de regras de Regras AWS Gerenciadas não substituem suas responsabilidades de segurança, que são determinadas pelos AWS recursos que você seleciona. Consulte o Modelo de Responsabilidade Compartilhada para garantir que seus recursos AWS estejam devidamente protegidos.

AWS Lista de grupos de regras de regras gerenciadas

As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Esta seção descreve as versões mais recentes dos grupos de regras de regras AWS gerenciadas. Essas informações são visualizadas no console quando você adiciona um grupo de regras gerenciadas à sua web ACL. Por meio da API, você pode recuperar essa lista junto com os grupos de regras AWS Marketplace gerenciados nos quais está inscrito por meio de chamadas. `ListAvailableManagedRuleGroups`

> **Note**
>
> Para obter informações sobre como recuperar as versões de um grupo de regras de regras AWS gerenciadas, consulteRecuperação das versões disponíveis para um grupo de regras gerenciadas.

Todos os grupos de regras de regras AWS gerenciadas oferecem suporte à rotulagem, e as listagens de regras nesta seção incluem especificações de etiquetas. Você pode recuperar os rótulos de um grupo de regras gerenciadas por meio da API chamando `DescribeManagedRuleGroup`. Os rótulos estão listados na propriedade AvailableLabels na resposta. Para obter informações sobre rotulagem, consulte AWS WAF rótulos em solicitações da web.

Teste e ajuste todas as alterações em suas AWS WAF proteções antes de usá-las para tráfego de produção. Para mais informações, consulte Testando e ajustando suas AWS WAF proteções.

AWS Grupos de regras de regras gerenciadas

- Grupos de regras de linha de base
  - Grupo de regras gerenciadas do conjunto de regras principais (CRS)
  - Grupo de regras gerenciadas de proteção administrativa
  - Grupo de regras gerenciadas de entradas nocivas conhecidas
- Grupos de regras específicos de caso de uso
  - Grupo de regras gerenciadas do banco de dados SQL
  - Grupo de regras gerenciadas do sistema operacional Linux
  - Grupo de regras gerenciadas do sistema operacional POSIX
  - Grupo de regras gerenciadas do sistema operacional Windows
  - Grupo de regras gerenciadas do aplicativo PHP
  - WordPress grupo de regras gerenciado por aplicativos
- Grupos de regras de reputação de IP
  - Grupo de regras gerenciadas da lista de reputação de IPs da Amazon
  - Grupo de regras gerenciadas da lista de IPs anônimos
- AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes
  - Considerações sobre o uso desse grupo de regras
  - Rótulos adicionados por esse grupo de regras
    - rótulos de token
    - rótulos do ACFP
  - Lista de regras de prevenção contra fraude na criação de contas
- AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes
  - Considerações sobre o uso desse grupo de regras
  - Rótulos adicionados por esse grupo de regras
    - rótulos de token
    - rótulos do ATP
  - Lista de regras de prevenção contra apropriação de contas

- AWS WAF Grupo de regras do Bot Control
  - Níveis de proteção
  - Considerações sobre o uso desse grupo de regras
  - Rótulos adicionados por esse grupo de regras
    - rótulos de token
    - Rótulos do Controle de Bots
  - Lista de regras do Controle de Bots

Grupos de regras de linha de base

Os grupos de regras gerenciadas de linha de base fornecem proteção geral contra uma grande variedade de ameaças comuns. Escolha um ou mais desses grupos de regras para estabelecer a proteção da linha de base para seus recursos.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que agentes mal-intencionados possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Grupo de regras gerenciadas do conjunto de regras principais (CRS)

VendorName:`AWS`, Nome:`AWSManagedRulesCommonRuleSet`, WCU: 700

O grupo de regras do conjunto de regras principais (CRS) contém regras que são aplicáveis de modo geral a aplicativos web. Isso fornece proteção contra a exploração de uma ampla gama de vulnerabilidades, incluindo algumas das vulnerabilidades comuns e de alto risco descritas em publicações do OWASP, como OWASP Top 10.. Considere usar esse grupo de regras para qualquer caso de AWS WAF uso.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para regras executadas após esse grupo de regras em sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais

sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`NoUserAgent_HEADER`	Inspeciona as solicitações sem o cabeçalho HTTP `User-Agent` . Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	Inspeciona valores de cabeçalho `User-Agent` comuns que indicam que a solicitação é um bot inválido. Os padrões de exemplo incluem `nessus` e `nmap`. Para gerenciamento de bots, consulte também AWS WAF Grupo de regras do Bot Control. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	Inspeciona strings de consulta de URI com mais de 2.048 bytes. Ação de regra: Block

Nome da regra	Descrição e rótulo
	Rótulo: `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`
`SizeRestrictions_Cookie_HEADER`	Inspeciona cabeçalhos de cookies com mais de 10.240 bytes. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header`
`SizeRestrictions_BODY`	Inspeciona corpos de solicitação com mais de 8 KB (8.192 bytes). Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Body`
`SizeRestrictions_URIPATH`	Inspeciona paths de URI com mais de 1.024 bytes. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`

Nome da regra	Descrição e rótulo
`EC2MetaDataSSRF_BODY`	Inspeciona tentativas de exfiltrar metadados Amazon EC2 do corpo da solicitação. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Nome da regra	Descrição e rótulo
`EC2MetaDataSSRF_COOKIE`	Inspeciona tentativas de exfiltrar metadados Amazon EC2 do cookie de solicitação. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`
`EC2MetaDataSSRF_URIPATH`	Amazon EC2Inspeciona tentativas de exfiltrar metadados do path do URI de solicitação. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	Inspeciona tentativas de exfiltrar metadados do Amazon EC2 dos argumentos da consulta de solicitação. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`
`GenericLFI_QUERYARGUMENTS`	Inspeciona a presença de explorações de inclusão local de arquivos (LFI) nos argumentos de consulta. Exemplos incluem tentativas de path traversal usando técnicas como `../../`. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`

Nome da regra	Descrição e rótulo
`GenericLFI_URIPATH`	Inspeciona a presença de explorações de inclusão local de arquivos (LFI) no caminho do URI. Exemplos incluem tentativas de path traversal usando técnicas como `../../`. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

Nome da regra	Descrição e rótulo
`GenericLFI_BODY`	Inspeciona a presença de explorações de inclusão local de arquivos (LFI) no corpo da solicitação. Exemplos incluem tentativas de path traversal usando técnicas como `../../`. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Nome da regra	Descrição e rótulo
`RestrictedExtensions_URIPATH`	Inspeciona as solicitações cujos caminhos de URI contêm extensões de arquivos do sistema que não são seguras para leitura ou execução. Os padrões de exemplo incluem extensões como `.log` e `.ini`. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath`
`RestrictedExtensions_QUERYARGUMENTS`	Inspeciona as solicitações cujos argumentos de consulta contêm extensões de arquivos do sistema que não são seguras para leitura ou execução. Os padrões de exemplo incluem extensões como `.log` e `.ini`. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments`

Nome da regra	Descrição e rótulo
`GenericRFI_QUERYARGUMENTS`	Inspeciona os valores de todos os parâmetros de consulta em busca de tentativas de explorar a RFI (inclusão remota de arquivos) em aplicativos da web incorporando URLs que contêm endereços IPv4. Os exemplos incluem padrões como `http://`, `https://`, `ftp://`, `ftps://` e `file://`, com um cabeçalho de host IPv4 na tentativa de exploração. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments`

Nome da regra	Descrição e rótulo
`GenericRFI_BODY`	Inspeciona o corpo da solicitação em busca de tentativas de explorar a RFI (inclusão remota de arquivos) em aplicativos da web incorporando URLs que contêm endereços IPv4. Os exemplos incluem padrões como `http://`, `https://`, `ftp://`, `ftps://` e `file://`, com um cabeçalho de host IPv4 na tentativa de exploração. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericRFI_Body`

Nome da regra	Descrição e rótulo
`GenericRFI_URIPATH`	Inspeciona o caminho da URI em busca de tentativas de explorar a RFI (inclusão remota de arquivos) em aplicativos da web incorporando URLs que contêm endereços IPv4. Os exemplos incluem padrões como `http://`, `https://`, `ftp://`, `ftps://` e `file://`, com um cabeçalho de host IPv4 na tentativa de exploração. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`

Nome da regra	Descrição e rótulo
`CrossSiteScripting_COOKIE`	Inspeciona os valores dos cabeçalhos de cookies em busca de padrões comuns de cross-site scripting (XSS) usando o integrado . AWS WAF Instrução de regra de ataque de script entre sites Os padrões de exemplo incluem scripts como `<script>alert("hello")</script>` . **Note** Os detalhes da correspondência de regras nos AWS WAF registros não são preenchidos para a versão 2.0 desse grupo de regras. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

Nome da regra	Descrição e rótulo
`CrossSiteScripting_QUERYARGUMENTS`	Inspeciona os valores dos argumentos de consulta para padrões comuns de cross-site scripting (XSS) usando o integrado. AWS WAF Instrução de regra de ataque de script entre sites Os padrões de exemplo incluem scripts como `<script>alert("hello")</script>` . **Note** Os detalhes da correspondência de regras nos AWS WAF registros não são preenchidos para a versão 2.0 desse grupo de regras. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Nome da regra	Descrição e rótulo
`CrossSiteScripting_BODY`	Inspeciona o corpo da solicitação em busca de padrões comuns de cross-site scripting (XSS) usando o integrado. AWS WAF Instrução de regra de ataque de script entre sites Os padrões de exemplo incluem scripts como `<script>alert("hello")</script>` . **Note** Os detalhes da correspondência de regras nos AWS WAF registros não são preenchidos para a versão 2.0 desse grupo de regras. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFron t API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes

Nome da regra	Descrição e rótulo
	de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	Inspeciona o valor do caminho do URI para padrões comuns de cross-site scripting (XSS) usando o integrado. AWS WAF Instrução de regra de ataque de script entre sites Os padrões de exemplo incluem scripts como `<script>alert("hello")</script>` . **Note** Os detalhes da correspondência de regras nos AWS WAF registros não são preenchidos para a versão 2.0 desse grupo de regras. Ação de regra: Block Rótulo: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

Grupo de regras gerenciadas de proteção administrativa

VendorName:`AWS`, Nome:`AWSManagedRulesAdminProtectionRuleSet`, WCU: 100

O grupo de regras de proteção de administrador contém regras que permitem bloquear o acesso externo a páginas administrativas expostas. Isso poderá ser útil se você executar software de terceiros ou quiser reduzir o risco de um agente mal-intencionado obter acesso administrativo ao aplicativo.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para regras executadas após esse grupo de regras em sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`AdminProtection_URIPATH`	Inspeciona caminhos de URI que geralmente são reservados para a administração de um aplicativo ou servidor web. Os padrões de exemplo incluem `sqlmanager` . Ação de regra: Block Rótulo: `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

Grupo de regras gerenciadas de entradas nocivas conhecidas

VendorName:`AWS`, Nome:`AWSManagedRulesKnownBadInputsRuleSet`, WCU: 200

O grupo de regras de entradas nocivas conhecidas contém regras para bloquear padrões de solicitação conhecidos como inválidos e associados à exploração ou à descoberta de

vulnerabilidades. Isso pode ajudar a reduzir o risco de um agente mal-intencionado descobrir um aplicativo vulnerável.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para regras executadas após esse grupo de regras em sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`JavaDeserializationRCE_HEADER`	Inspeciona as chaves e os valores dos cabeçalhos de solicitação HTTP em busca de padrões que indiquem tentativas de execução remota de comando (RCE) de desserialização de Java, como as vulnerabilidades do Spring Core e Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Os padrões de exemplo incluem `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Essa regra inspeciona somente os primeiros 8 KB dos cabeçalhos da solicitação ou os primeiros 200 cabeçalhos, qualquer que seja o limite atingido primeiro, e usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratament

Nome da regra	Descrição e rótulo
	o de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

Nome da regra	Descrição e rótulo
`JavaDeserializationRCE_BODY`	Inspeciona o corpo da solicitação em busca de padrões que indiquem tentativas de execução remota de comando (RCE) de desserialização de Java, como as vulnerabilidades do Spring Core e Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Os padrões de exemplo incluem `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block

Nome da regra	Descrição e rótulo
	Rótulo: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`
`JavaDeserializationRCE_URIPATH`	Inspeciona o URI da solicitação em busca de padrões que indiquem tentativas de execução remota de comando (RCE) de desserialização de Java, como as vulnerabilidades do Spring Core e Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Os padrões de exemplo incluem `(java.lang.Runtime).getRuntime().exec("whoami")` . Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath`
`JavaDeserializationRCE_QUERYSTRING`	Inspeciona a string de consulta da solicitação em busca de padrões que indiquem tentativas de execução remota de comando (RCE) de desserialização de Java, como as vulnerabilidades do Spring Core e Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Os padrões de exemplo incluem `(java.lang.Runtime).getRuntime().exec("whoami")` . Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString`

Nome da regra	Descrição e rótulo
`Host_localhost_HEADER`	Inspeciona o cabeçalho do host na solicitação buscando padrões que indicam localhost. Os padrões de exemplo incluem `localhost` . Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header`
`PROPFIND_METHOD`	Inspeciona o método HTTP na solicitação buscando `PROPFIND`, que é um método semelhante ao `HEAD`, mas com a intenção adicional de exfiltrar objetos XML. Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:Propfind_Method`
`ExploitablePaths_URIPATH`	Inspeciona o caminho do URI buscando tentativas de acessar caminhos de aplicativos web exploráveis. Os padrões de exemplo incluem caminhos como `web-inf`. Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath`

Nome da regra	Descrição e rótulo
`Log4JRCE_HEADER`	Inspeciona as chaves e os valores dos cabeçalhos de solicitação quanto à presença da vulnerabilidade do Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protege contra tentativas de execução remota de código (RCE). Os padrões de exemplo incluem `${jndi:ldap://example.com/}` . **Warning** Essa regra inspeciona somente os primeiros 8 KB dos cabeçalho s da solicitação ou os primeiros 200 cabeçalhos, qualquer que seja o limite atingido primeiro, e usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratament o de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:known-ba d-inputs:Log4JRCE_Header`

Nome da regra	Descrição e rótulo
`Log4JRCE_QUERYSTRING`	Inspeciona as strings de consulta quanto à presença da vulnerabilidade do Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protege contra tentativas de execução remota de código (RCE). Os padrões de exemplo incluem `${jndi:ldap://example.com/}` . Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

Nome da regra	Descrição e rótulo
`Log4JRCE_BODY`	Inspeciona o corpo quanto à presença da vulnerabilidade do Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protege contra tentativas de execução remota de código (RCE). Os padrões de exemplo incluem `${jndi:ldap://example.com/}` . **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Nome da regra	Descrição e rótulo
`Log4JRCE_URIPATH`	Inspeciona o caminho do URI quanto à presença da vulnerabilidade do Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) e protege contra tentativas de execução remota de código (RCE). Os padrões de exemplo incluem `${jndi:ldap://example.com/}` . Ação de regra: Block Rótulo: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

Grupos de regras específicos de caso de uso

Grupos de regras específicos para casos de uso fornecem proteção incremental para diversos AWS WAF casos de uso. Escolha os grupos de regras que se aplicam ao seu aplicativo.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Grupo de regras gerenciadas do banco de dados SQL

VendorName:`AWS`, Nome:`AWSManagedRulesSQLiRuleSet`, WCU: 200

O grupo de regras do banco de dados SQL contém regras para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Isso pode ajudar a evitar a injeção remota de consultas não autorizadas. Avalie esse grupo de regras para uso se o aplicativo fizer interface com um banco de dados SQL.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`SQLi_QUERYARGUMENTS`	Usa o integrado AWS WAF Instrução de regra de ataque de injeção de SQL, com o nível de sensibilidade definido comoLow, para inspecionar os valores de todos os parâmetros de consulta em busca de padrões que correspondam ao código SQL malicioso. Ação de regra: Block Rótulo: `awswaf:managed:aws:sql-database:SQLi_QueryArguments`
`SQLiExtendedPatterns_QUERYARGUMENTS`	Inspeciona os valores de todos os parâmetros de consulta buscando padrões que correspondem ao código SQL mal-intencionado. Os padrões que essa regra inspeciona não são cobertos pelo `SQLi_QUERYARGUMENTS` da regra. Ação de regra: Block

Nome da regra	Descrição e rótulo
	Rótulo: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments`

Nome da regra	Descrição e rótulo
`SQLi_BODY`	Usa o integrado AWS WAF Instrução de regra de ataque de injeção de SQL, com o nível de sensibilidade definido comoLow, para inspecionar o corpo da solicitação em busca de padrões que correspondam ao código SQL malicioso. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:sql-database:SQLi_Body`

Nome da regra	Descrição e rótulo
`SQLiExtendedPatterns_BODY`	Inspeciona o corpo da solicitação em busca de padrões que correspondam ao código SQL malicioso. Os padrões que essa regra inspeciona não são cobertos pelo `SQLi_BODY` da regra. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body`

Nome da regra	Descrição e rótulo
`SQLi_COOKIE`	Usa o integrado AWS WAF Instrução de regra de ataque de injeção de SQL, com o nível de sensibilidade definido comoLow, para inspecionar os cabeçalhos dos cookies de solicitação em busca de padrões que correspondam ao código SQL malicioso. Ação de regra: Block Rótulo: `awswaf:managed:aws:sql-database:SQLi_Cookie`

Grupo de regras gerenciadas do sistema operacional Linux

VendorName:`AWS`, Nome:`AWSManagedRulesLinuxRuleSet`, WCU: 200

O grupo de regras do sistema operacional Linux contém regras que bloqueiam padrões de solicitação associados à exploração de vulnerabilidades específicas do Linux, incluindo ataques de inclusão local de arquivos (LFI) específicos do Linux. Isso pode ajudar a evitar ataques que expõem o conteúdo do arquivo ou executam código ao qual o invasor não deveria ter tido acesso. Você deve avaliar esse grupo de regras se qualquer parte do seu aplicativo for executado no Linux. Você deve usar esse grupo de regras com o grupo de regras Sistema operacional POSIX.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`LFI_URIPATH`	Inspeciona o caminho da solicitação buscando tentativas de explorar vulnerabilidades de inclusão local de arquivos (LFI) em aplicativos web. Os padrões de exemplo incluem arquivos como `/proc/version` , que podem fornecer informações do sistema operacional para invasores. Ação de regra: Block Rótulo: `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	Inspeciona os valores de todas as sequências de consulta buscando tentativas de explorar vulnerabilidades de inclusão local de arquivos (LFI) em aplicativos web. Os padrões de exemplo incluem arquivos como `/proc/version` , que podem fornecer informações do sistema operacional para invasores. Ação de regra: Block Rótulo: `awswaf:managed:aws:linux-os:LFI_QueryString`
`LFI_HEADER`	Inspeciona o corpo da solicitação buscando tentativas de explorar vulnerabilidades de inclusão local de arquivos (LFI) em aplicativos web. Os padrões de exemplo incluem arquivos como `/proc/version` , que podem fornecer informações do sistema operacional para invasores.

Nome da regra	Descrição e rótulo
	Warning Essa regra inspeciona somente os primeiros 8 KB dos cabeçalho s da solicitação ou os primeiros 200 cabeçalhos, qualquer que seja o limite atingido primeiro, e usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratament o de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:linux-os :LFI_Header`

Grupo de regras gerenciadas do sistema operacional POSIX

VendorName:`AWS`, Nome:`AWSManagedRulesUnixRuleSet`, WCU: 100

O grupo de regras do sistema operacional POSIX contém regras que bloqueiam padrões de solicitação associados à exploração de vulnerabilidades específicas para sistemas operacionais POSIX e semelhantes, incluindo ataques de inclusão local de arquivos (LFI). Isso pode ajudar a evitar ataques que expõem o conteúdo do arquivo ou executam código ao qual o invasor não deveria ter tido acesso. Você deverá avaliar esse grupo de regras se qualquer parte do aplicativo for executada em um sistema operacional POSIX ou semelhante, incluindo Linux, AIX, HP-UX, macOS, Solaris, FreeBSD e OpenBSD.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações

gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`UNIXShellCommandsVariables_QUERYSTRING`	Inspeciona os valores da sequência de caracteres de consulta em busca de tentativas de explorar vulnerabilidades de injeção de comandos, LFI e travessia de caminhos em aplicativos Web executados em sistemas Unix. Exemplos incluem padrões como `echo $HOME` e `echo $PATH`. Ação de regra: Block Rótulo: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	Inspeciona o corpo da solicitação buscando tentativas de explorar vulnerabilidades de injeção de comando, LFI e path traversal em aplicativos web executados em sistemas Unix. Exemplos incluem padrões como `echo $HOME` e `echo $PATH`. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo

Nome da regra	Descrição e rótulo
	de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

Nome da regra	Descrição e rótulo
`UNIXShellCommandsVariables_HEADER`	Inspeciona todos os cabeçalhos de solicitação em busca de tentativas de explorar vulnerabilidades de injeção de comandos, LFI e travessia de caminhos em aplicativos Web executados em sistemas Unix. Exemplos incluem padrões como `echo $HOME` e `echo $PATH`. **Warning** Essa regra inspeciona somente os primeiros 8 KB dos cabeçalhos da solicitação ou os primeiros 200 cabeçalhos, qualquer que seja o limite atingido primeiro, e usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header`

Grupo de regras gerenciadas do sistema operacional Windows

VendorName:`AWS`, Nome:`AWSManagedRulesWindowsRuleSet`, WCU: 200

O grupo de regras do sistema operacional Windows contém regras que bloqueiam padrões de solicitação associados à exploração de vulnerabilidades específicas do Windows, como a execução

remota de PowerShell comandos. Isso pode ajudar a impedir a exploração de vulnerabilidades que permitem que um invasor execute comandos não autorizados ou códigos mal-intencionados. Avalie esse grupo de regras se alguma parte do seu aplicativo for executada em um sistema operacional Windows.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`WindowsShellCommands_COOKIE`	Inspeciona os cabeçalhos do cookie de solicitação em busca de tentativas de injeção de WindowsShell comando em aplicativos da web. Os padrões de correspondência represent am WindowsShell comandos. Os padrões de exemplo incluem `||nslookup` e `;cmd`. Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie`
`WindowsShellCommands_QUERYARGUMENTS`	Inspeciona os valores de todos os parâmetro s de consulta para tentativas de injeção de WindowsShell comando em aplicativos web. Os padrões de correspondência represent am WindowsShell comandos. Os padrões de exemplo incluem `||nslookup` e `;cmd`.

Nome da regra	Descrição e rótulo
	Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`

Nome da regra	Descrição e rótulo
`WindowsShellCommands_BODY`	Inspeciona o corpo da solicitação em busca de tentativas de injeção de WindowsShell comando em aplicativos da web. Os padrões de correspondência representam WindowsSh ell comandos. Os padrões de exemplo incluem `||nslookup e ;cmd`. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFron t API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

Nome da regra	Descrição e rótulo
`PowerShellCommands_COOKIE`	Inspeciona os cabeçalhos do cookie de solicitação em busca de tentativas de injeção de PowerShell comando em aplicativos da web. Os padrões de correspondência represent am PowerShell comandos. Por exemplo, `Invoke-Expression` . Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`
`PowerShellCommands_QUERYARG UMENTS`	Inspeciona os valores de todos os parâmetro s de consulta para tentativas de injeção de PowerShell comando em aplicativos web. Os padrões de correspondência representam PowerShell comandos. Por exemplo, `Invoke-Expression` . Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:PowerShellCommands_Query Arguments`

Nome da regra	Descrição e rótulo
`PowerShellCommands_BODY`	Inspeciona o corpo da solicitação em busca de tentativas de injeção de PowerShell comando em aplicativos da web. Os padrões de correspondência representam PowerShel l comandos. Por exemplo, `Invoke-Ex pression` . **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFron t API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

Grupo de regras gerenciadas do aplicativo PHP

VendorName:`AWS`, Nome:`AWSManagedRulesPHPRuleSet`, WCU: 100

O grupo de regras do aplicativo PHP contém regras que bloqueiam padrões de solicitação associados à exploração de vulnerabilidades específicas para o uso da linguagem de programação PHP, incluindo injeção de funções PHP não seguras. Isso pode ajudar a impedir a exploração de vulnerabilidades que permitem que um invasor execute código ou comandos remotamente para os quais ele não está autorizado. Avalie este grupo de regras se o PHP estiver instalado em qualquer servidor com o qual seu aplicativo interage.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`PHPHighRiskMethodsVariables_HEADER`	Inspeciona todos os cabeçalhos buscando tentativas de injeção de código de script PHP. Os padrões de exemplo incluem funções como `fsockopen` e a variável superglobal `$_GET`. **Warning** Essa regra inspeciona somente os primeiros 8 KB dos cabeçalho s da solicitação ou os primeiros 200 cabeçalhos, qualquer que seja o limite atingido primeiro, e usa a opção `Continue` para tratamento de

Nome da regra	Descrição e rótulo
	conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`
`PHPHighRiskMethodsVariables_QUERYSTRING`	Inspeciona tudo depois do primeiro `?` na URL da solicitação, procurando por tentativas de injeção de código de script PHP. Os padrões de exemplo incluem funções como `fsockopen` e a variável superglobal `$_GET`. Ação de regra: Block Rótulo: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString`

Nome da regra	Descrição e rótulo
`PHPHighRiskMethodsVariables_BODY`	Inspeciona os valores do corpo da solicitação buscando tentativas de injeção de código de script PHP. Os padrões de exemplo incluem funções como `fsockopen` e a variável superglobal `$_GET`. **Warning** Essa regra só inspeciona o corpo da solicitação até o limite de tamanho do corpo para a ACL da web e o tipo de recurso. Para Application Load Balancer e AWS AppSync, o limite é fixado em 8 KB. Para CloudFront API Gateway, Amazon Cognito, App Runner e Verified Access, o limite padrão é de 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Essa regra usa a opção `Continue` para tratamento de conteúdo de tamanho grande. Para ter mais informações, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF. Ação de regra: Block Rótulo: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body`

WordPress grupo de regras gerenciado por aplicativos

VendorName:`AWS`, Nome:`AWSManagedRulesWordPressRuleSet`, WCU: 100

O grupo de regras do WordPress aplicativo contém regras que bloqueiam padrões de solicitação associados à exploração de vulnerabilidades específicas dos WordPress sites. Você deve avaliar esse grupo de regras se estiver executandoWordPress. Esse grupo de regras deve ser usado com os grupos de regras Banco de dados SQL e Aplicativo PHP.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

> **Note**
>
> Esta tabela descreve a versão estática mais recente desse grupo de regras. Para outras versões, use o comando da API DescribeManagedRuleGroup.

Nome da regra	Descrição e rótulo
`WordPressExploitableCommands_QUERYSTRING`	Inspeciona a string de consulta da solicitação em busca de WordPress comandos de alto risco que possam ser explorados em instalações ou plug-ins vulneráveis. Os padrões de exemplo incluem comandos como `do-reset-wordpress` . Ação de regra: Block Rótulo: `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	Inspeciona o caminho do URI da solicitação para WordPress arquivos como`xmlrpc.php` ,

Nome da regra	Descrição e rótulo
	que são conhecidos por terem vulnerabilidades facilmente exploráveis. Ação de regra: Block Rótulo: `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

Grupos de regras de reputação de IP

Os grupos de regras de reputação de IP bloqueiam solicitações com base em seu endereço IP de origem.

> **Note**
>
> Essas regras usam o endereço IP de origem da solicitação da web. Se você tiver tráfego que passa por um ou mais proxies ou balanceadores de carga, a origem da solicitação da web conterá o endereço do último proxy, e não o endereço de origem do cliente.

Escolha um ou mais desses grupos de regras se quiser reduzir sua exposição ao tráfego de bot e a tentativas de exploração ou se estiver aplicando restrições geográficas ao seu conteúdo. Para gerenciamento de bots, consulte também AWS WAF Grupo de regras do Bot Control.

Os grupos de regras nessa categoria não fornecem notificações de versionamento ou atualização do SNS.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Grupo de regras gerenciadas da lista de reputação de IPs da Amazon

VendorName:`AWS`, Nome:`AWSManagedRulesAmazonIpReputationList`, WCU: 25

O grupo de regras da lista de reputação de IP da Amazon contém regras baseadas na inteligência de ameaças internas da Amazon. Isso é útil se você quiser bloquear endereços IP normalmente associados a bots ou outras ameaças. Bloquear esses endereços IP pode ajudar a diminuir bots e reduzir o risco de um agente mal-intencionado descobrir um aplicativo vulnerável.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos de acordo com CloudWatch as métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

Nome da regra	Descrição e rótulo
`AWSManagedIPReputationList`	Inspeciona os endereços IP que foram identificados como ativamente envolvidos em atividades maliciosas. AWS WAF coleta a lista de endereços IP de várias fontes MadPot, incluindo uma ferramenta de inteligência contra ameaças que a Amazon usa para proteger os clientes contra crimes cibernéticos. Para obter mais informações sobre MadPot, consultehttps://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime. Ação de regra: Block Rótulo: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	Inspeciona as conexões de endereços IP que estão realizando reconhecimento em relação aos recursos da AWS .

Nome da regra	Descrição e rótulo
	Ação de regra: Block Rótulo: `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	Inspeciona os endereços IP que foram identificados como ativamente envolvidos em atividades de DDoS. Ação de regra: Count Rótulo: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

Grupo de regras gerenciadas da lista de IPs anônimos

VendorName:`AWS`, Nome:`AWSManagedRulesAnonymousIpList`, WCU: 50

Esse grupo de regras da lista de IPs anônimos contém regras para bloquear solicitações de serviços que permitem a ofuscação da identidade do visualizador. Elas incluem solicitações de VPNs, proxies, nós Tor e provedores de hospedagem. Esse grupo de regras é útil se você quiser filtrar visualizadores que podem estar tentando ocultar a identidade do seu aplicativo. Bloquear os endereços IP desses serviços pode ajudar a mitigar bots e evasão de restrições geográficas.

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos de acordo com CloudWatch as métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

Nome da regra	Descrição e rótulo
`AnonymousIPList`	Inspeciona buscando uma lista de endereços IP de fontes conhecidas por anonimizar

Nome da regra	Descrição e rótulo
	informações de clientes, como nós TOR, proxies temporários e outros serviços de mascaramento. Ação de regra: Block Rótulo: `awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`
`HostingProviderIPList`	Inspeciona buscando uma lista de endereços IP de provedores de nuvem e de hospedagem, que são menos propensos a gerar tráfego de usuário final. A lista de IPs não inclui endereços AWS IP. Ação de regra: Block Rótulo: `awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList`

AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes

VendorName:`AWS`, Nome:`AWSManagedRulesACFPRuleSet`, WCU: 50

O AWS WAF grupo de regras gerenciado para prevenção de fraudes na criação de contas (ACFP) do Fraud Control rotula e gerencia solicitações que podem fazer parte de tentativas fraudulentas de criação de contas. O grupo de regras faz isso inspecionando as solicitações de criação de conta que os clientes enviam para os endpoints de registro e criação de conta do seu aplicativo.

O grupo de regras do ACFP inspeciona as tentativas de criação de contas de várias maneiras, para oferecer visibilidade e controle sobre interações potencialmente maliciosas. O grupo de regras usa tokens de solicitação para coletar informações sobre o navegador do cliente e sobre o nível de interatividade humana na criação da solicitação de criação da conta. O grupo de regras detecta e gerencia as tentativas de criação de contas em massa agregando solicitações por endereço IP e sessão do cliente e agregando pelas informações fornecidas da conta, como endereço físico e número de telefone. Além disso, o grupo de regras detecta e bloqueia a criação de novas contas

usando credenciais que foram comprometidas, o que ajuda a proteger a postura de segurança de seu aplicativo e de seus novos usuários.

Considerações sobre o uso desse grupo de regras

Este grupo de regras requer uma configuração personalizada, que inclui a especificação dos caminhos de registro da conta e de criação da conta da aplicação. Exceto onde indicado, as regras desse grupo de regras inspecionam todas as solicitações que seus clientes enviam para esses dois endpoints. Para configurar e implementar esse grupo de regras, consulte a orientação em AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP).

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

Esse grupo de regras faz parte das proteções de mitigação de ameaças inteligentes em AWS WAF. Para obter mais informações, consulte AWS WAF mitigação inteligente de ameaças.

Para manter seus custos baixos e ter certeza de que você está gerenciando seu tráfego da web como deseja, use esse grupo de regras de acordo com as orientações em Práticas recomendadas para mitigação de ameaças inteligentes.

Esse grupo de regras não está disponível para uso com grupos de usuários do Amazon Cognito. Você não pode associar uma web ACL que usa esse grupo de regras a um grupo de usuários e não pode adicionar esse grupo de regras a uma web ACL que já esteja associada a um grupo de usuários.

Rótulos adicionados por esse grupo de regras

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para regras executadas após esse grupo de regras em sua ACL da web. AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

rótulos de token

Esse grupo de regras usa o gerenciamento de AWS WAF tokens para inspecionar e rotular solicitações da web de acordo com o status de seus AWS WAF tokens. AWS WAF usa tokens para rastreamento e verificação da sessão do cliente.

Para obter informações sobre os tokens e sobre o gerenciamento de token, consulte AWS WAF tokens de solicitação da web.

Para obter informações sobre os componentes do rótulo descritos aqui, consulte AWS WAF sintaxe de rótulos e requisitos de nomenclatura.

Rótulo de sessão do cliente

O rótulo `awswaf:managed:token:id:`*`identifier`* contém um identificador exclusivo que o gerenciamento de AWS WAF tokens usa para identificar a sessão do cliente. O identificador pode ser alterado se o cliente adquirir um novo token, por exemplo, após descartar o token que estava usando.

> **Note**
>
> AWS WAF não relata CloudWatch métricas da Amazon para esse rótulo.

Rótulos de status do token: prefixos de namespace para os rótulos

Os rótulos de status do token informam sobre o status do token e sobre as informações de desafio e de CAPTCHA que ele contém.

Cada rótulo de status do token começa com um dos seguintes prefixos de namespace:

- `awswaf:managed:token:`: usado para relatar o status geral do token e para informar o status das informações de desafio do token.
- `awswaf:managed:captcha:`: usado para relatar o status das informações de CAPTCHA do token.

Rótulos de status do token: nomes de rótulos

Na sequência do prefixo, o restante do rótulo fornece informações detalhadas sobre o status do token:

- `accepted`: o token de solicitação está presente e contém o seguinte:
  - Uma solução de desafio ou de CAPTCHA válida.
  - Um carimbo de data/hora de desafio ou de CAPTCHA não expirado.
  - Uma especificação de domínio válida para a ACL da Web.

  Exemplo: o rótulo `awswaf:managed:token:accepted` indica que o token de solicitações da Web tem uma solução de desafio válida, um carimbo de data/hora de desafio não expirado e um domínio válido.
- `rejected`: o token de solicitação está presente, mas não atende aos critérios de aceitação.

  Em conjunto com o rótulo rejeitado, o gerenciamento de token adiciona um namespace e um nome de rótulo personalizado para indicar o motivo.
  - `rejected:not_solved`: a solução de desafio ou de CAPTCHA está ausente no token.
  - `rejected:expired`: o carimbo de data/hora de desafio ou de CAPTCHA expirou no token, de acordo com os tempos de imunidade de token configurados pela sua ACL da Web.
  - `rejected:domain_mismatch`: o domínio do token não corresponde à configuração de domínio do token da sua ACL da Web.
  - `rejected:invalid`— não AWS WAF consegui ler o token indicado.

  Exemplo: os rótulos `awswaf:managed:captcha:rejected` e `awswaf:managed:captcha:rejected:expired` indicam que a solicitação foi rejeitada porque o carimbo de data/hora de CAPTCHA no token excedeu o tempo de imunidade para o token de CAPTCHA configurado na ACL da Web.
- `absent`: a solicitação não tem o token ou o gerenciador de token não conseguiu realizar a leitura dele.

  Exemplo: o rótulo `awswaf:managed:captcha:absent` indica que a solicitação não tem o token.

rótulos do ACFP

Esse grupo de regras gera rótulos com o prefixo do namespace `awswaf:managed:aws:acfp:` seguido pelo namespace personalizado e pelo nome do rótulo. O grupo de regras pode adicionar mais de um rótulo a uma solicitação.

Você pode recuperar todos os rótulos de um grupo de regras por meio da API chamando `DescribeManagedRuleGroup`. Os rótulos estão listados na propriedade `AvailableLabels` na resposta.

Lista de regras de prevenção contra fraude na criação de contas

Esta seção lista as regras de ACFP em `AWSManagedRulesACFPRuleSet` e os rótulos que as regras do grupo de regras adicionam às solicitações da Web.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Todas as regras desse grupo de regras exigem um token de solicitação da web, exceto `UnsupportedCognitoIDP` e `AllRequests` das duas primeiras. Para obter uma descrição das informações que o token fornece, consulte AWS WAF características do token.

Exceto onde indicado, as regras desse grupo de regras inspecionam todas as solicitações que seus clientes enviam para os caminhos da página de registro e criação de conta que você fornece na configuração do grupo de regras. Para obter informações sobre como configurar esse grupo de regras, consulte AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP).

Nome da regra	Descrição e rótulo
`UnsupportedCognitoIDP`	Inspeciona o tráfego da web que vai para um grupo de usuários do Amazon Cognito. O ACFP não está disponível para uso com grupos de usuários do Amazon Cognito, e essa regra ajuda a garantir que as outras regras do grupo de regras do ACFP não sejam usadas para avaliar o tráfego de grupos de usuários.

Nome da regra	Descrição e rótulo
	Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	Aplica a ação de regra às solicitações que acessam o caminho da página de registro. Você configura o caminho da página de registro ao configurar o grupo de regras. Por padrão, essa regra se aplica às solicitações Challenge. Ao aplicar essa ação, a regra garante que o cliente adquira um token de desafio antes que qualquer solicitação seja avaliada pelo restante das regras no grupo de regras. Certifique-se de que seus usuários finais carreguem o caminho da página de registro antes de enviarem uma solicitação de criação de conta. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo cliente e pelas ações de regra CAPTCHA e Challenge. Para obter a aquisição de token mais eficiente, é altamente recomendável que você use os SDKs de integração de aplicativos. Para ter mais informações, consulte AWS WAF integração de aplicativos clientes. Ação de regra: Challenge Rótulo: nenhum

Nome da regra	Descrição e rótulo
`RiskScoreHigh`	Inspeciona solicitações de criação de conta com endereços IP ou outros fatores considera dos altamente suspeitos. Essa avaliação geralmente é baseada em vários fatores contribuintes, que você pode ver nos rótulos `risk_score` que o grupo de regras adiciona à solicitação. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:ris k_score:high` A regra também pode aplicar rótulos de pontuação de risco `medium` ou `low` à solicitaç ão. Se AWS WAF não conseguir avaliar a pontuação de risco da solicitação da web, a regra adiciona o rótulo `awswaf:ma naged:aws:acfp:risk_score:e valuation_failed` Além disso, a regra adiciona rótulos com o `awswaf:managed:aws:acfp:ris k_score:contributor:` do namespace que incluem o status e os resultados da avaliação da pontuação de risco para contribui dores específicos da pontuação de risco, como avaliações de reputação de IP e credenciais roubadas.

Nome da regra	Descrição e rótulo
`SignalCredentialCompromised`	Pesquisa no banco de dados de credenciais roubadas as credenciais que foram enviadas na solicitação de criação da conta. Essa regra garante que novos clientes inicializem suas contas com uma postura de segurança positiva. **Note** Você pode adicionar uma resposta de bloqueio personalizada para descrever o problema para o usuário final e dizer a ele como proceder. Para obter mais informações, consulte Exemplo de ACFP: resposta personalizada para credenciais comprometidas. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:signal:credential_compromised` O grupo de regras aplica o rótulo relacionado a seguir, mas não executa nenhuma ação, pois nem todas as solicitações na criação da conta terão credenciais: `awswaf:managed:aws:acfp:signal:missing_credential`

Nome da regra	Descrição e rótulo
`SignalClientHumanInteractivityAbsentLow`	Inspeciona o token da solicitação de criação de conta em busca de dados que indiquem interatividade humana anormal com o aplicativo. A interatividade humana é detectada por meio de interações como movimentos do mouse e pressionamentos de teclas. Se a página tiver um formulário HTML, a interatividade humana incluirá interações com o formulário. **Note** Essa regra só inspeciona as solicitações para o caminho de criação da conta e só é avaliada se você tiver implementado os SDKs de integração de aplicativos. As implementações de SDK capturam passivamente a interatividade humana e armazenam as informações no token de solicitação. Para obter mais informações, consulte AWS WAF características do token e AWS WAF integração de aplicativos clientes. Ação da regra: CAPTCHA Rótulo: nenhum. A regra determina uma correspondência com base em vários fatores, portanto, não há um rótulo individual que se aplique a todos os cenários de correspondência possíveis.

Nome da regra	Descrição e rótulo
	O grupo de regras pode aplicar um ou mais dos rótulos a seguir às solicitações: `awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high` `awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data` `awswaf:managed:aws:acfp:signal:form_detected` .
`SignalAutomatedBrowser`	Inspeciona a solicitação em busca de indicadores de que o navegador do cliente pode ser automatizado. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	Inspeciona o token da solicitação em busca de dados inconsistentes de interrogação do navegador. Para ter mais informações, consulte AWS WAF características do token. Ação de regra: CAPTCHA Rótulo: `awswaf:managed:aws:acfp:signal:browser_inconsistency`

Nome da regra	Descrição e rótulo
`VolumetricIpHigh`	Inspeciona grandes volumes de solicitações de criação de contas enviadas de endereços IP individuais. Um volume alto é de mais de 20 solicitações em uma janela de 10 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Para o alto volume, algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: CAPTCHA Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` A regra aplica os seguintes rótulos às solicitações com volumes médios (mais de 15 solicitações por janela de 10 minutos) e volumes baixos (mais de 10 solicitações por janela de 10 minutos), mas não executa nenhuma ação: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` e.

Nome da regra	Descrição e rótulo
`VolumetricSessionHigh`	Inspeciona grandes volumes de solicitações de criação de contas enviadas de sessões individuais de clientes. Um volume alto é de mais de 10 solicitações em uma janela de 30 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` O grupo de regras aplica os seguintes rótulos às solicitações com volumes médios (mais de 5 solicitações por janela de 30 minutos) e volumes baixos (mais de 1 solicitação por janela de 30 minutos), mas não executa nenhuma ação sobre elas: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low` e.

Nome da regra	Descrição e rótulo
`AttributeUsernameTraversalHigh`	Inspeciona uma alta taxa de solicitações de criação de contas de uma única sessão de cliente que usa nomes de usuário diferentes. O limite para uma avaliação alta é de mais de 10 solicitações em 30 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` O grupo de regras aplica os seguintes rótulos às solicitações com volumes médios (mais de 5 solicitações por janela de 30 minutos) e volumes baixos (mais de 1 solicitação por janela de 30 minutos) de solicitações de passagem de nome de usuário, mas não executa nenhuma ação sobre elas: e. `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low`

Nome da regra	Descrição e rótulo
`VolumetricPhoneNumberHigh`	Inspeciona grandes volumes de solicitações de criação de contas que usam o mesmo número de telefone. O limite para uma avaliação alta é de mais de 10 solicitações em 30 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` O grupo de regras aplica os seguintes rótulos às solicitações com volumes médios (mais de 5 solicitações por janela de 30 minutos) e volumes baixos (mais de 1 solicitação por janela de 30 minutos), mas não executa nenhuma ação sobre elas: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium` `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low` e.

Nome da regra	Descrição e rótulo
`VolumetricAddressHigh`	Inspeciona grandes volumes de solicitações de criação de contas que usam o mesmo endereço físico. O limite para uma avaliação alta é de mais de 100 solicitações em 30 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

Nome da regra	Descrição e rótulo
`VolumetricAddressLow`	Inspeciona volumes de solicitações baixos e médios de criação de contas que usam o mesmo endereço físico. O limite para uma avaliação média é de mais de 50 solicitações por janela de 30 minutos, e para uma avaliação baixa é de mais de 10 solicitações por janela de 30 minutos. A regra aplica a ação para volumes médios ou baixos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: CAPTCHA Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` ou `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Nome da regra	Descrição e rótulo
`VolumetricIPSuccessfulResponse`	Inspeciona um grande volume de solicitações bem-sucedidas de criação de conta para um único endereço IP. Essa regra agrega respostas bem-sucedidas do recurso protegido às solicitações de criação de conta. O limite para uma avaliação alta é de mais de 10 solicitações em 10 minutos. Essa regra ajuda a proteger contra tentativas de criação de contas em massa. Ele tem um limite menor do que o `VolumetricIpHigh` da regra, que conta apenas as solicitações. Se você configurou o grupo de regras para inspecionar o corpo da resposta ou os componentes JSON, AWS WAF pode inspecionar os primeiros 65.536 bytes (64 KB) desses tipos de componentes em busca de indicadores de sucesso ou falha. Essa regra aplica a ação e a rotulagem da regra a novas solicitações da web de um endereço IP, com base nas respostas de sucesso e falha do recurso protegido às recentes tentativas de login do mesmo endereço IP. Você define como contar os sucessos e as falhas ao configurar o grupo de regras. **Note** AWS WAF avalia essa regra somente em ACLs da web que protegem as distribuições da Amazon CloudFront .

Nome da regra	Descrição e rótulo
	Note Os limites aplicados por essa regra podem variar um pouco devido à latência. É possível que o cliente envie mais tentativas bem-sucedidas de criação de conta do que as permitidas antes que a regra comece a correspon der às tentativas subsequentes. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:agg regate:volumetric:ip:succes sful_creation_response:high` O grupo de regras também aplica os seguintes rótulos relacionados às solicitaç ões, sem nenhuma ação associada. Todas as contagens são para uma janela de 10 minutos. `awswaf:managed:aws:acfp:agg regate:volumetric:ip:succes sful_creation_response:medi um` para mais de 5 solicitações bem-suced idas, `awswaf:managed:aws:acfp:agg regate:volumetric:ip:succes sful_creation_response:low` para mais de 1 solicitação bem-sucedida, `awswaf:managed:aws:acfp:agg regate:volumetric:ip:failed _creation_response:high` para mais de 10 solicitações malsucedidas, `awswaf:ma naged:aws:acfp:aggregate:vo`

Nome da regra	Descrição e rótulo
	`lumetric:ip:failed_creation_response:medium` para mais de 5 solicitações malsucedidas e `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` para mais de 1 solicitação malsucedida.

Nome da regra	Descrição e rótulo
`VolumetricSessionSuccessful Response`	Inspeciona um baixo volume de respostas bem-sucedidas do recurso protegido às solicitações de criação de conta que estão sendo enviadas de uma única sessão do cliente. Essa regra ajuda a proteger contra tentativas de criação de contas em massa. O limite para uma avaliação alta é de mais de 1 solicitação em 30 minutos. Isso ajuda a proteger contra tentativas de criação de contas em massa. Essa regra usa um limite inferior ao da regra `Volumetri cSessionHigh` , que acompanha somente as solicitações. Se você configurou o grupo de regras para inspecionar o corpo da resposta ou os componentes JSON, AWS WAF pode inspecionar os primeiros 65.536 bytes (64 KB) desses tipos de componentes em busca de indicadores de sucesso ou falha. Essa regra aplica a ação e a rotulagem da regra a novas solicitações da web de um endereço IP, com base nas respostas de sucesso e falha do recurso protegido às recentes tentativas de login da mesma sessão de cliente. Você define como contar os sucessos e as falhas ao configurar o grupo de regras.

Nome da regra	Descrição e rótulo
	Note AWS WAF avalia essa regra somente em ACLs da web que protegem as distribuições da Amazon CloudFront .
	Note Os limites aplicados por essa regra podem variar um pouco devido à latência. É possível que o cliente envie mais tentativas mal sucedidas de criação de conta do que as permitidas antes que a regra comece a correspon der às tentativas subsequentes.
	Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:agg regate:volumetric:session:s uccessful_creation_response:low` O grupo de regras também aplica os seguintes rótulos relacionados às solicitações. Todas as contagens são para uma janela de 30 minutos. `awswaf:managed:aws:acfp:agg regate:volumetric:session:s uccessful_creation_response :high` para mais de 10 solicitações bem-sucedidas, `awswaf:managed:aws :acfp:aggregate:volumetric: session:successful_creation`

Nome da regra	Descrição e rótulo
	`_response:medium` para mais de 5 solicitações bem-sucedidas, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` para mais de 10 solicitações malsucedidas, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` para mais de 5 solicitações malsucedidas e `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` para mais de 1 solicitação malsucedida.
`VolumetricSessionTokenReuseIp`	Inspeciona as solicitações de criação de conta para o uso de um único token entre mais de 5 endereços IP distintos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes

VendorName:`AWS`, Nome:`AWSManagedRulesATPRuleSet`, WCU: 50

O grupo de regras gerenciado de prevenção de invasão de contas (ATP) do AWS WAF Fraud Control rotula e gerencia solicitações que podem fazer parte de tentativas maliciosas de invasão de contas. O grupo de regras faz isso inspecionando as tentativas de login que os clientes enviam para o endpoint de login do seu aplicativo.

- Inspeção de solicitações: o ATP oferece visibilidade e controle sobre tentativas de login anômalas e tentativas de login que usam credenciais roubadas, para evitar apropriações de contas que possam levar a atividades fraudulentas. O ATP verifica as combinações de e-mail e senha em seu banco de dados de credenciais roubadas, que é atualizado regularmente à medida que novas credenciais vazadas são encontradas na dark web. O ATP agrega dados por endereço IP e sessão do cliente, para detectar e bloquear clientes que enviam muitas solicitações de natureza suspeita.
- Inspeção de resposta — Para CloudFront distribuições, além de inspecionar as solicitações de login recebidas, o grupo de regras ATP inspeciona as respostas do seu aplicativo às tentativas de login, para monitorar as taxas de sucesso e falha. Usando essas informações, o ATP pode bloquear temporariamente sessões de clientes ou endereços IP que tenham muitas falhas de login. O AWS WAF executa a inspeção de resposta de forma assíncrona, para que isso não aumente a latência no tráfego da web.

Considerações sobre o uso desse grupo de regras

Esse grupo de regras exige uma configuração específica. Para configurar e implementar esse grupo de regras, consulte a orientação em AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP).

Esse grupo de regras faz parte das proteções de mitigação de ameaças inteligentes em AWS WAF. Para obter mais informações, consulte AWS WAF mitigação inteligente de ameaças.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

Para manter seus custos baixos e ter certeza de que você está gerenciando seu tráfego da web como deseja, use esse grupo de regras de acordo com as orientações em Práticas recomendadas para mitigação de ameaças inteligentes.

Esse grupo de regras não está disponível para uso com grupos de usuários do Amazon Cognito. Você não pode associar uma web ACL que usa esse grupo de regras a um grupo de usuários e não pode adicionar esse grupo de regras a uma web ACL que já esteja associada a um grupo de usuários.

Rótulos adicionados por esse grupo de regras

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web. AWS WAF também registra os rótulos de acordo com CloudWatch as métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

rótulos de token

Esse grupo de regras usa o gerenciamento de AWS WAF tokens para inspecionar e rotular solicitações da web de acordo com o status de seus AWS WAF tokens. AWS WAF usa tokens para rastreamento e verificação da sessão do cliente.

Para obter informações sobre os tokens e sobre o gerenciamento de token, consulte AWS WAF tokens de solicitação da web.

Para obter informações sobre os componentes do rótulo descritos aqui, consulte AWS WAF sintaxe de rótulos e requisitos de nomenclatura.

Rótulo de sessão do cliente

O rótulo `awswaf:managed:token:id:`*`identifier`* contém um identificador exclusivo que o gerenciamento de AWS WAF tokens usa para identificar a sessão do cliente. O identificador pode ser alterado se o cliente adquirir um novo token, por exemplo, após descartar o token que estava usando.

> **Note**
>
> AWS WAF não relata CloudWatch métricas da Amazon para esse rótulo.

Rótulos de status do token: prefixos de namespace para os rótulos

Os rótulos de status do token informam sobre o status do token e sobre as informações de desafio e de CAPTCHA que ele contém.

Cada rótulo de status do token começa com um dos seguintes prefixos de namespace:

- `awswaf:managed:token:`: usado para relatar o status geral do token e para informar o status das informações de desafio do token.
- `awswaf:managed:captcha:`: usado para relatar o status das informações de CAPTCHA do token.

Rótulos de status do token: nomes de rótulos

Na sequência do prefixo, o restante do rótulo fornece informações detalhadas sobre o status do token:

- `accepted`: o token de solicitação está presente e contém o seguinte:
  - Uma solução de desafio ou de CAPTCHA válida.
  - Um carimbo de data/hora de desafio ou de CAPTCHA não expirado.
  - Uma especificação de domínio válida para a ACL da Web.

  Exemplo: o rótulo `awswaf:managed:token:accepted` indica que o token de solicitações da Web tem uma solução de desafio válida, um carimbo de data/hora de desafio não expirado e um domínio válido.
- `rejected`: o token de solicitação está presente, mas não atende aos critérios de aceitação.

  Em conjunto com o rótulo rejeitado, o gerenciamento de token adiciona um namespace e um nome de rótulo personalizado para indicar o motivo.
  - `rejected:not_solved`: a solução de desafio ou de CAPTCHA está ausente no token.
  - `rejected:expired`: o carimbo de data/hora de desafio ou de CAPTCHA expirou no token, de acordo com os tempos de imunidade de token configurados pela sua ACL da Web.
  - `rejected:domain_mismatch`: o domínio do token não corresponde à configuração de domínio do token da sua ACL da Web.
  - `rejected:invalid`— não AWS WAF consegui ler o token indicado.

Exemplo: os rótulos `awswaf:managed:captcha:rejected` e `awswaf:managed:captcha:rejected:expired` indicam que a solicitação foi rejeitada porque o carimbo de data/hora de CAPTCHA no token excedeu o tempo de imunidade para o token de CAPTCHA configurado na ACL da Web.

- `absent`: a solicitação não tem o token ou o gerenciador de token não conseguiu realizar a leitura dele.

  Exemplo: o rótulo `awswaf:managed:captcha:absent` indica que a solicitação não tem o token.

rótulos do ATP

O grupo de regras gerenciadas do ATP gera rótulos com o `awswaf:managed:aws:atp:` do prefixo do namespace seguido pelo namespace personalizado e pelo nome do rótulo.

O grupo de regras pode adicionar qualquer um dos rótulos a seguir, além dos rótulos indicados na lista de regras:

- `awswaf:managed:aws:atp:signal:credential_compromised`: indica que as credenciais enviadas na solicitação estão no banco de dados de credenciais roubadas.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Disponível somente para CloudFront distribuições protegidas da Amazon. Indica que uma sessão do cliente enviou várias solicitações que usaram uma impressão digital TLS suspeita.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`: indica o uso de um único token entre mais de 5 endereços IP distintos. Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que o rótulo seja aplicado.

Você pode recuperar todos os rótulos de um grupo de regras por meio da API chamando `DescribeManagedRuleGroup`. Os rótulos estão listados na propriedade `AvailableLabels` na resposta.

Lista de regras de prevenção contra apropriação de contas

Esta seção lista as regras de ATP em `AWSManagedRulesATPRuleSet` e os rótulos que as regras do grupo de regras adicionam às solicitações da Web.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Nome da regra	Descrição e rótulo
`UnsupportedCognitoIDP`	Inspeciona o tráfego da web que vai para um grupo de usuários do Amazon Cognito. O ATP não está disponível para uso com grupos de usuários do Amazon Cognito, e essa regra ajuda a garantir que as outras regras do grupo de regras do ATP não sejam usadas para avaliar o tráfego de grupos de usuários. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	Inspeciona grandes volumes de solicitações de criação de contas enviadas de endereços IP individuais. Um volume alto é de mais de 20 solicitações em uma janela de 10 minutos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Para o alto volume, algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada.

Nome da regra	Descrição e rótulo
	Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:volumetric:ip:high` O grupo de regras aplica os seguintes rótulos às solicitações com volumes médios (mais de 15 solicitações por janela de 10 minutos) e volumes baixos (mais de 10 solicitações por janela de 10 minutos), mas não executa nenhuma ação em relação a elas: `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` `awswaf:managed:aws:atp:aggregate:volumetric:ip:low` e.

Nome da regra	Descrição e rótulo
`VolumetricSession`	Inspeciona grandes volumes de solicitações de criação de contas enviadas de sessões de clientes individuais. O limite é de mais de 20 solicitações em 30 minutos. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:volumetric:session`

Nome da regra	Descrição e rótulo
`AttributeCompromisedCredentials`	Inspeciona várias solicitações da mesma sessão do cliente que usam credenciais roubadas. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`
`AttributeUsernameTraversal`	Inspeciona várias solicitações da mesma sessão do cliente que usam traversal de nome de usuário. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	Inspeciona várias solicitações com o mesmo nome de usuário que usam a passagem de senha. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:attribute:password_traversal`

Nome da regra	Descrição e rótulo
`AttributeLongSession`	Inspeciona várias solicitações da mesma sessão do cliente que usam solicitações de longa duração. O limite é de mais de 6 horas de tráfego com pelo menos uma solicitação de login a cada 30 minutos. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:attribute:long_session`

Nome da regra	Descrição e rótulo
`TokenRejected`	Inspeciona solicitações com tokens que foram rejeitados pelo gerenciamento de AWS WAF tokens. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. Ação de regra: Block Rótulo: nenhum. Para verificar se o token foi rejeitado, use uma regra de correspondência de rótulo para corresponder ao rótulo: `awswaf:managed:token:rejected`
`SignalMissingCredential`	Inspeciona solicitações com credenciais sem o nome de usuário ou a senha. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:signal:missing_credential`

Nome da regra	Descrição e rótulo
`VolumetricIpFailedLoginResponseHigh`	Inspeciona endereços IP que recentemente foram a fonte de uma taxa muito alta de tentativas de login malsucedidas. Um volume alto é de mais de 10 solicitações de login malsucedidas de um endereço IP em uma janela de 10 minutos. Se você configurou o grupo de regras para inspecionar o corpo da resposta ou os componentes JSON, AWS WAF pode inspecionar os primeiros 65.536 bytes (64 KB) desses tipos de componentes em busca de indicadores de sucesso ou falha. Essa regra aplica a ação e a rotulagem da regra a novas solicitações da web de um endereço IP, com base nas respostas de sucesso e falha do recurso protegido às recentes tentativas de login do mesmo endereço IP. Você define como contar os sucessos e as falhas ao configurar o grupo de regras. **Note** AWS WAF avalia essa regra somente em ACLs da web que protegem as distribuições da Amazon CloudFront. **Note** Os limites aplicados por essa regra podem variar um pouco devido à

Nome da regra	Descrição e rótulo
	latência. É possível que o cliente envie mais tentativas mal sucedidas de login do que as permitidas antes que a regra comece a corresponder às tentativas subsequentes. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` O grupo de regras também aplica os seguintes rótulos relacionados às solicitações, sem nenhuma ação associada. Todas as contagens são para uma janela de 10 minutos. `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium` para mais de 5 solicitações malsucedidas, `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low` para mais de 1 solicitação malsucedida, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high` para mais de 10 solicitações bem-sucedidas, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium` para mais de 5 solicitações bem-sucedidas e `awswaf:managed:aws:atp:aggregate:volumetric:i`

Nome da regra	Descrição e rótulo
	`p:successful_login_response:low` para mais de 1 solicitação bem-sucedida.

Nome da regra	Descrição e rótulo
`VolumetricSessionFailedLoginResponseHigh`	Inspeciona sessões de clientes que recentemente foram a fonte de uma taxa muito alta de tentativas de login malsucedidas. Um volume alto é mais de 10 solicitações de login malsucedidas de uma sessão de cliente em uma janela de 30 minutos. Se você configurou o grupo de regras para inspecionar o corpo da resposta ou os componentes JSON, AWS WAF pode inspecionar os primeiros 65.536 bytes (64 KB) desses tipos de componentes em busca de indicadores de sucesso ou falha. Essa regra aplica a ação e a rotulagem da regra a novas solicitações da web de um endereço IP, com base nas respostas de sucesso e falha do recurso protegido às recentes tentativas de login da mesma sessão de cliente. Você define como contar os sucessos e as falhas ao configurar o grupo de regras. **Note** AWS WAF avalia essa regra somente em ACLs da web que protegem as distribuições da Amazon CloudFront . **Note** Os limites aplicados por essa regra podem variar um pouco devido à

Nome da regra	Descrição e rótulo
	latência. É possível que o cliente envie mais tentativas mal sucedidas de login do que as permitidas antes que a regra comece a corresponder às tentativas subsequentes. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. Ação de regra: Block Rótulo: `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` O grupo de regras também aplica os seguintes rótulos relacionados às solicitações, sem nenhuma ação associada. Todas as contagens são para uma janela de 30 minutos. `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` para mais de 5 solicitações malsucedidas, `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low` para mais de 1 solicitação malsucedida, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_`

Nome da regra	Descrição e rótulo
	`login_response:high` para mais de 10 solicitações bem-sucedidas, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium` para mais de 5 solicitações bem-sucedidas e `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` para mais de 1 solicitação bem-sucedida.

AWS WAF Grupo de regras do Bot Control

VendorName:`AWS`, Nome:`AWSManagedRulesBotControlRuleSet`, WCU: 50

O grupo de regras gerenciadas do Controle de Bots fornece regras que gerenciam solicitações de bots. Os bots podem consumir recursos em excesso, distorcer as métricas de negócios, causar tempo de inatividade e realizar atividades maliciosas.

Níveis de proteção

O grupo de regras gerenciadas do Controle de Bots fornece dois níveis de proteção que você pode escolher:

- Comum: detecta uma variedade de bots que se identificam automaticamente, como estruturas de raspagem web, mecanismos de pesquisa e navegadores automatizados. As proteções do Controle de Bots nesse nível identificam bots comuns usando técnicas tradicionais de detecção de bots, como análise estática de dados de solicitações. As regras rotulam o tráfego desses bots e bloqueiam aqueles que eles não podem verificar.
- Direcionado: inclui proteções de nível comum e adiciona detecção direcionada para bots sofisticados que não se identificam. As proteções direcionadas mitigam a atividade dos bots usando uma combinação de limitação de intervalo e CAPTCHA e desafios de navegador em segundo plano.
  - **`TGT_`**: as regras que fornecem proteção direcionada têm nomes que começam com `TGT_`. Todas as proteções direcionadas usam técnicas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots.

- **`TGT_ML_`**: as regras de proteção direcionada que usam machine learning têm nomes que começam com `TGT_ML_`. Essas regras usam análise automatizada de aprendizado de máquina das estatísticas de tráfego do site para detectar comportamentos anômalos indicativos de atividades de bots distribuídas e coordenadas. AWS WAF analisa estatísticas sobre o tráfego do seu site, como registros de data e hora, características do navegador e URL anterior visitado, para melhorar o modelo de aprendizado de máquina do Bot Control. Os recursos de machine learning são ativados por padrão, mas você pode desativá-los na configuração do grupo de regras. Quando o aprendizado de máquina está desativado, AWS WAF não avalia essas regras.

O nível de proteção desejado e a declaração de regra AWS WAF baseada em taxas fornecem limitação de taxa. Para uma comparação das duas opções, consulte Opções para limitação de intervalo em regras baseadas em intervalos e regras direcionadas do Controle de Bots.

Considerações sobre o uso desse grupo de regras

Esse grupo de regras faz parte das proteções de mitigação de ameaças inteligentes em AWS WAF. Para mais informações, consulte AWS WAF mitigação inteligente de ameaças.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

Para manter seus custos baixos e ter certeza de que você está gerenciando seu tráfego da web como deseja, use esse grupo de regras de acordo com as orientações em Práticas recomendadas para mitigação de ameaças inteligentes.

Atualizamos periodicamente nossos modelos de aprendizado de máquina (ML) para as regras baseadas em ML do nível de proteção direcionado, a fim de melhorar as previsões de bots. As regras baseadas em ML têm nomes que começam com. `TGT_ML_` Se você notar uma mudança repentina e substancial nas previsões de bots feitas por essas regras, entre em contato conosco por meio de seu gerente de conta ou abra um caso no AWS Support Center.

Rótulos adicionados por esse grupo de regras

Esse grupo de regras gerenciadas adiciona rótulos às solicitações da web que ele avalia, que estão disponíveis para as regras que são executadas após esse grupo de regras na sua ACL da web.

AWS WAF também registra os rótulos nas CloudWatch métricas da Amazon. Para obter informações gerais sobre rótulos e métricas de rótulos, consulte Rótulos em solicitações da web e Métricas e dimensões do rótulo.

rótulos de token

Esse grupo de regras usa o gerenciamento de AWS WAF tokens para inspecionar e rotular solicitações da web de acordo com o status de seus AWS WAF tokens. AWS WAF usa tokens para rastreamento e verificação da sessão do cliente.

Para obter informações sobre os tokens e sobre o gerenciamento de token, consulte AWS WAF tokens de solicitação da web.

Para obter informações sobre os componentes do rótulo descritos aqui, consulte AWS WAF sintaxe de rótulos e requisitos de nomenclatura.

Rótulo de sessão do cliente

O rótulo `awswaf:managed:token:id:`*`identifier`* contém um identificador exclusivo que o gerenciamento de AWS WAF tokens usa para identificar a sessão do cliente. O identificador pode ser alterado se o cliente adquirir um novo token, por exemplo, após descartar o token que estava usando.

> **Note**
>
> AWS WAF não relata CloudWatch métricas da Amazon para esse rótulo.

Rótulos de status do token: prefixos de namespace para os rótulos

Os rótulos de status do token informam sobre o status do token e sobre as informações de desafio e de CAPTCHA que ele contém.

Cada rótulo de status do token começa com um dos seguintes prefixos de namespace:

- `awswaf:managed:token:`: usado para relatar o status geral do token e para informar o status das informações de desafio do token.
- `awswaf:managed:captcha:`: usado para relatar o status das informações de CAPTCHA do token.

Rótulos de status do token: nomes de rótulos

Na sequência do prefixo, o restante do rótulo fornece informações detalhadas sobre o status do token:

- `accepted`: o token de solicitação está presente e contém o seguinte:
  - Uma solução de desafio ou de CAPTCHA válida.
  - Um carimbo de data/hora de desafio ou de CAPTCHA não expirado.
  - Uma especificação de domínio válida para a ACL da Web.

  Exemplo: o rótulo `awswaf:managed:token:accepted` indica que o token de solicitações da Web tem uma solução de desafio válida, um carimbo de data/hora de desafio não expirado e um domínio válido.
- `rejected`: o token de solicitação está presente, mas não atende aos critérios de aceitação.

  Em conjunto com o rótulo rejeitado, o gerenciamento de token adiciona um namespace e um nome de rótulo personalizado para indicar o motivo.
  - `rejected:not_solved`: a solução de desafio ou de CAPTCHA está ausente no token.
  - `rejected:expired`: o carimbo de data/hora de desafio ou de CAPTCHA expirou no token, de acordo com os tempos de imunidade de token configurados pela sua ACL da Web.
  - `rejected:domain_mismatch`: o domínio do token não corresponde à configuração de domínio do token da sua ACL da Web.
  - `rejected:invalid`— não AWS WAF consegui ler o token indicado.

  Exemplo: os rótulos `awswaf:managed:captcha:rejected` e `awswaf:managed:captcha:rejected:expired` indicam que a solicitação foi rejeitada porque o carimbo de data/hora de CAPTCHA no token excedeu o tempo de imunidade para o token de CAPTCHA configurado na ACL da Web.
- `absent`: a solicitação não tem o token ou o gerenciador de token não conseguiu realizar a leitura dele.

  Exemplo: o rótulo `awswaf:managed:captcha:absent` indica que a solicitação não tem o token.

Rótulos do Controle de Bots

O grupo de regras gerenciadas do Controle de Bots gera rótulos com o `awswaf:managed:aws:bot-control:` do prefixo do namespace seguido pelo namespace

personalizado e pelo nome do rótulo. O grupo de regras pode adicionar mais de um rótulo a uma solicitação.

Cada rótulo reflete as descobertas de regras do Controle de Bots:

- `awswaf:managed:aws:bot-control:bot:`: informações sobre o bot associado à solicitação.
  - `awswaf:managed:aws:bot-control:bot:name:`*`<name>`*:O nome do bot, se houver um disponível, por exemplo, os namespaces personalizados `bot:name:slurp`, `bot:name:googlebot`, e `bot:name:pocket_parser`.
  - `awswaf:managed:aws:bot-control:bot:category:`*`<category>`*— A categoria de bot, conforme definida por AWS WAF, por exemplo, `bot:category:search_engine` `bot:category:content_fetcher` e.
  - `awswaf:managed:aws:bot-control:bot:organization:`*`<organization>`*:O publicador do bot, por exemplo, `bot:organization:google`.
  - `awswaf:managed:aws:bot-control:bot:verified`:Usado para indicar um bot que se identifica e que o Controle de Bots conseguiu verificar. Isso é usado para bots comuns desejáveis e pode ser útil quando combinado com rótulos de categoria como `bot:category:search_engine` ou rótulos de nome como `bot:name:googlebot`.

    > **Note**
    >
    > O Controle de Bots usa o endereço IP da origem da solicitação da web para ajudar a determinar se um bot foi verificado. Você não pode configurá-lo para usar a configuração de IP AWS WAF encaminhado para inspecionar uma fonte de endereço IP diferente. Se você verificou bots que fazem roteamento por meio de um proxy ou balanceador de carga, você pode adicionar uma regra que é executada antes do grupo de regras do Controle de bots para ajudar com isso. Configure sua nova regra para usar o endereço IP encaminhado e permitir explicitamente as solicitações dos bots verificados. Para obter mais informações sobre utilizar endereços IP encaminhados, consulte Endereço IP encaminhado.

  - `awswaf:managed:aws:bot-control:bot:user_triggered:verified`: Usado para indicar um bot semelhante a um bot verificado, mas que pode ser invocado diretamente pelos usuários finais. Essa categoria de bot é tratada pelas regras do Controle de Bots como um bot não verificado.
  - `awswaf:managed:aws:bot-control:bot:developer_platform:verified`: Usado para indicar um bot semelhante a um bot verificado, mas usado por plataformas de desenvolvedores

para criação de scripts, por exemplo, o Google Apps Script. Essa categoria de bot é tratada pelas regras do Controle de Bots como um bot não verificado.

  - `awswaf:managed:aws:bot-control:bot:unverified`: Usado para indicar um bot que se identifica, para que possa ser nomeado e categorizado, mas que não publica informações que possam ser usadas para verificar sua identidade de forma independente. Esses tipos de assinaturas de bots podem ser falsificados e, portanto, tratados como não verificados.

- `awswaf:managed:aws:bot-control:targeted:<additional-details>` : Usado para rótulos específicos das proteções direcionadas do Controle de Bots.
- `awswaf:managed:aws:bot-control:signal:<signal-details>` e `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` : Usados para fornecer informações adicionais sobre a solicitação em algumas situações.

  Veja a seguir exemplos de rótulos de sinal. Esta não é uma lista completa:

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`: indica a detecção de uma extensão para navegador que auxilia na automação, como o Selenium IDE.

    Este rótulo é adicionado sempre que um usuário tem esse tipo de extensão instalado, mesmo que não a esteja usando ativamente. Se você implementar uma regra de correspondência de rótulos para este caso, esteja ciente da possibilidade de obter falsos positivos na lógica da sua regra e nas configurações de ações. Por exemplo, é possível usar uma ação CAPTCHA em vez de Block, ou combinar essa correspondência de rótulos com outras correspondências de rótulos, para aumentar sua confiança de que a automação está em uso.

  - `awswaf:managed:aws:bot-control:signal:automated_browser`: Indica que a solicitação contém indicadores de que o navegador do cliente pode ser automatizado.
  - `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— Indica que o AWS WAF token da solicitação contém indicadores de que o navegador do cliente pode ser automatizado.

Você pode recuperar todos os rótulos de um grupo de regras por meio da API chamando `DescribeManagedRuleGroup`. Os rótulos estão listados na propriedade `AvailableLabels` na resposta.

O grupo de regras gerenciadas do Controle de Bots aplica rótulos a um conjunto de bots verificáveis que geralmente são permitidos. O grupo de regras não bloqueia esses bots verificados. Se quiser, você pode bloqueá-los ou um subconjunto deles escrevendo uma regra personalizada que usa

os rótulos aplicados pelo grupo de regras gerenciadas do Controle de Bots. Para obter mais informações sobre isso e exemplos, consulte AWS WAF Controle de bots.

Lista de regras do Controle de Bots

Esta seção lista as regras de Controle de Bots.

> **Note**
>
> As informações que publicamos sobre as regras nos grupos de regras de regras AWS gerenciadas têm como objetivo fornecer informações suficientes para você usar as regras, sem fornecer informações que pessoas mal-intencionadas possam usar para contorná-las. Se precisar de mais informações do que as encontradas nesta documentação, entre em contato com o AWS Support Center.

Nome da regra	Descrição
`CategoryAdvertising`	Inspeciona os bots usados para fins publicitários. Por exemplo, você pode usar serviços de publicidade de terceiros que precisam acessar seu site de forma programática. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:advertising` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryArchiver`	Inspeciona os bots usados para fins de arquivamento. Esses bots vasculham a Web

Nome da regra	Descrição
	e capturam conteúdo com o objetivo de criar arquivos. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:archiver` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryContentFetcher`	Inspeciona os bots que visitam o site do aplicativo em nome de um usuário, para buscar conteúdo, como feeds RSS, ou para verificar ou validar seu conteúdo. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:content_fetcher` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategoryEmailClient`	Inspeciona bots que verificam links em e-mails que apontam para o site do aplicativo. Isso pode incluir bots administrados por empresas e provedores de e-mail para verificar links em e-mails e sinalizar e-mails suspeitos. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:email_client` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryHttpLibrary`	Inspeciona as solicitações geradas por bots das bibliotecas HTTP de várias linguagens de programação. Isso pode incluir solicitações de API que você opta por permitir ou monitorar. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:http_library` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategoryLinkChecker`	Inspeciona os bots que verificam se há links quebrados. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:link_checker` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryMiscellaneous`	Inspeciona bots diversos que não correspondem a outras categorias. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:miscellaneous` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategoryMonitoring`	Inspeciona os bots usados para fins de monitoramento. Por exemplo, você pode usar serviços de monitoramento de bots que pingam periodicamente o site do seu aplicativo para monitorar coisas como desempenho e tempo de atividade. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:monitoring` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategoryScrapingFramework`	Inspeciona bots de estruturas de raspagem web, que são usadas para automatizar o crawling e a extração de conteúdo de sites. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:scraping_framework` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategorySearchEngine`	Inspeciona os bots dos mecanismos de pesquisa, que rastreiam sites para indexar o conteúdo e disponibilizar as informações para os resultados dos mecanismos de pesquisa. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:search_engine` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategorySecurity`	Inspeciona bots que examinam vulnerabilidades em aplicativos da web ou que realizam auditorias de segurança. Por exemplo, você pode usar um fornecedor de segurança terceirizado que escaneia, monitora ou audita a segurança do seu aplicativo da web. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:security` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategorySeo`	Inspeciona os bots usados para otimização de mecanismos de pesquisa. Por exemplo, você pode usar ferramentas de mecanismos de pesquisa que rastreiam seu site para ajudá-lo a melhorar sua classificação nos mecanismos de pesquisa. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:seo` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .
`CategorySocialMedia`	Inspeciona os bots usados pelas plataformas de mídia social para fornecer resumos de conteúdo quando os usuários compartilham seu conteúdo. Ação de regra, aplicada somente a bots não verificados: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:social_media` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`CategoryAI`	Inspeciona bots de inteligência artificial (IA). Ação de regra: Block Rótulo: `awswaf:managed:aws:bot-control:bot:category:ai`
`SignalAutomatedBrowser`	Inspeciona a solicitação em busca de indicadores de que o navegador do cliente pode ser automatizado. Navegadores automatizados podem ser usados para testes ou extração. Por exemplo, você pode usar esses tipos de navegadores para monitorar ou verificar o site do seu aplicativo. Ação de regra: Block Rótulo: `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	Inspeciona indicadores de datacenters que normalmente são usados por bots. Ação de regra: Block Rótulo: `awswaf:managed:aws:bot-control:signal:known_bot_data_center`

Nome da regra	Descrição
`SignalNonBrowserUserAgent`	Inspeciona strings do agente do usuário que não parecem ser de um navegador da web. Essa categoria pode incluir solicitações de API. Ação de regra: Block Rótulo: `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

Nome da regra	Descrição
`TGT_VolumetricIpTokenAbsent`	Inspeciona cinco ou mais solicitações de um cliente nos últimos 5 minutos que não incluem um token de desafio válido. Para mais informações sobre tokens, consulte AWS WAF tokens de solicitação da web. **Note** É possível que essa regra corresponda a uma solicitação que tenha um token se as solicitações do mesmo cliente tiverem perdido tokens recentemente. O limite aplicado por essa regra pode variar um pouco devido à latência. Essa regra trata os tokens ausentes de forma diferente da rotulagem do token: `awswaf:managed:token:absent`. A rotulagem do token rotula solicitações individuais sem um token. Essa regra mantém uma contagem de solicitações sem token para cada IP do cliente e corresponde com os clientes que ultrapassam o limite. Ação de regra, aplicada somente a clientes que não são bots verificados: Challenge Rótulo: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:ma`

Nome da regra	Descrição
	`naged:aws:bot-control:bot:verified .`

Nome da regra	Descrição
`TGT_VolumetricSession`	Inspeciona um número anormalmente alto de solicitações de uma sessão do cliente em qualquer janela de 5 minutos. A avaliação é baseada em uma comparação com as linhas de base volumétricas padrão que se AWS WAF mantêm usando padrões históricos de tráfego. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. **Note** Essa regra pode levar 5 minutos para entrar em vigor depois que você a habilitar. O Bot Control identifica um comportamento anômalo em seu tráfego na web comparando o tráfego atual com as linhas de base de tráfego computadas. AWS WAF Ação de regra, aplicada somente a clientes que não são bots verificados: CAPTCHA Rótulo: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high`

Nome da regra	Descrição
	O grupo de regras aplica os seguintes rótulos às solicitações de volume médio e menor que estão acima de um limite mínimo. Para esses níveis, a regra não executa nenhuma ação, independentemente de o cliente ser verificado: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` e `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low`. Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified`.

Nome da regra	Descrição
`TGT_SignalAutomatedBrowser`	Inspeciona o token de solicitação em busca de indicadores de que o navegador do cliente pode ser automatizado. Para ter mais informações, consulte AWS WAF caracterí sticas do token. Essa inspeção só se aplica quando a solicitaç ão da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. Ação de regra, aplicada somente a clientes que não são bots verificados: CAPTCHA Rótulo: `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`TGT_SignalBrowserInconsistency`	Inspeciona a existência de dados inconsistentes de interrogação do navegador. Para ter mais informações, consulte AWS WAF características do token. Essa inspeção só se aplica quando a solicitação da web tem um token. Os tokens são adicionados às solicitações pelos SDKs de integração do aplicativo e pelas ações de regra CAPTCHA e Challenge. Para ter mais informações, consulte AWS WAF tokens de solicitação da web. Ação de regra, aplicada somente a clientes que não são bots verificados: CAPTCHA Rótulo: `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified` .

Nome da regra	Descrição
`TGT_TokenReuseIp`	Inspeciona buscando um único token entre mais de 5 endereços IP distintos. **Note** Os limites aplicados por essa regra podem variar um pouco devido à latência. Algumas solicitações podem ultrapassar o limite antes que a ação de regra seja aplicada. Ação de regra: Count Rótulo: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Nome da regra	Descrição
`TGT_ML_CoordinatedActivityMedium` e `TGT_ML_CoordinatedActivityHigh`	Verifique se há comportamento anômalo consistente com a atividade distribuída e coordenada de bots. Os níveis das regras indicam o nível de confiança de que um grupo de solicitações participa de um ataque coordenado. **Note** Essas regras só são executadas se o grupo de regras estiver configurado para usar machine learning (ML). Para obter informações sobre como configurar essa opção, consulte Adicionar o grupo de regras gerenciadas do AWS WAF Bot Control à sua ACL da web. AWS WAF realiza essa inspeção por meio da análise de aprendizado de máquina das estatísticas de tráfego do site. AWS WAF analisa o tráfego da web a cada poucos minutos e otimiza a análise para a detecção de bots de baixa intensidade e longa duração que são distribuídos em vários endereços IP. Essas regras podem corresponder a um número muito pequeno de solicitações antes de determinar que um ataque coordenado não está em andamento. Portanto, se você ver apenas uma ou duas correspondências, os resultados podem ser falsos positivos. No entanto, se você vê muitas correspondências

Nome da regra	Descrição
	saindo dessas regras, provavelmente está enfrentando um ataque coordenado. **Note** Essas regras podem levar até 24 horas para entrarem em vigor depois que você ativar as regras direcionadas do Controle de Bots com a opção de ML. O Bot Control identifica um comportam ento anômalo em seu tráfego na web comparando o tráfego atual com as linhas de base de tráfego que foram computadas. AWS WAF AWS WAF só calcula as linhas de base enquanto você usa as regras específicas do Bot Control com a opção ML, e pode levar até 24 horas para estabelecer linhas de base significativas. Atualizamos periodicamente nossos modelos de aprendizado de máquina para essas regras, para melhorar as previsões de bots. Se você notar uma mudança repentina e substancial nas previsões de bots que essas regras fazem, entre em contato com seu gerente de conta ou abra um caso no AWS Support Center. Ações de regra, aplicadas somente a clientes que não são bots verificados: • Médio: Count • Alto: Count

Nome da regra	Descrição
	Rótulos: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` e `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` Para bots verificados, o grupo de regras não realiza nenhuma ação, mas adiciona o rótulo da regra mais o rótulo `awswaf:managed:aws:bot-control:bot:verified`. O grupo de regras também adiciona o rótulo `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` para indicar baixos níveis de confiança, mas não aplica nenhuma regra nem executa nenhuma ação para essas solicitações.

Implantações para grupos de regras de regras AWS gerenciadas com versão

AWS implanta alterações em seus grupos de regras de regras AWS gerenciadas com versões em três implantações padrão: candidato a lançamento, versão estática e versão padrão. Além disso, às vezes AWS pode ser necessário lançar uma implantação de exceção ou reverter a implantação de uma versão padrão.

> **Note**
>
> Esta seção se aplica somente aos grupos de regras de regras AWS gerenciadas com controle de versão. O único grupo de regras que não tem versão é o grupo de regras de reputação de IP.

Tópicos

Notificações para implantações de grupos de regras de regras AWS gerenciadas

Todos os grupos de regras do AWS Managed Rules versionados fornecem notificações de atualização do SNS para implantações e todos usam o mesmo tópico do SNS Amazon Resource Name (ARN). O único grupo de regras que não tem versão é o grupo de regras de reputação de IP.

Para implantações que afetam suas proteções, como alterações na versão padrão, a AWS fornece notificações do SNS para informá-lo sobre implantações planejadas e para que você saiba quando uma implantação está começando. Para implantações que não afetam suas proteções, como implantações de versão candidata e versão estática, você pode ser notificado pela AWS após o início da implantação ou mesmo após sua conclusão. Ao concluir a implantação de uma nova versão estática, AWS atualize este guia, no changelog em AWS Registro de alterações das regras gerenciadas e na página de histórico do documento em. Histórico do documento

Para receber todas as atualizações que AWS fornecem os grupos de regras de regras AWS gerenciadas, assine o feed RSS de qualquer página HTML deste guia e assine o tópico SNS para os grupos de regras de regras AWS gerenciadas. Para obter informações sobre como assinar as notificações do SNS, consulte. Como receber notificações sobre novas versões e atualizações de um grupo de regras gerenciadas

Conteúdo das notificações do SNS

Os campos nas notificações do Amazon SNS sempre incluem Assunto, Mensagem e. MessageAttributes Os campos adicionais dependem do tipo de mensagem e do grupo de regras gerenciadas para o qual a notificação se destina. Veja a seguir um exemplo de lista de notificação para `AWSManagedRulesCommonRuleSet`.

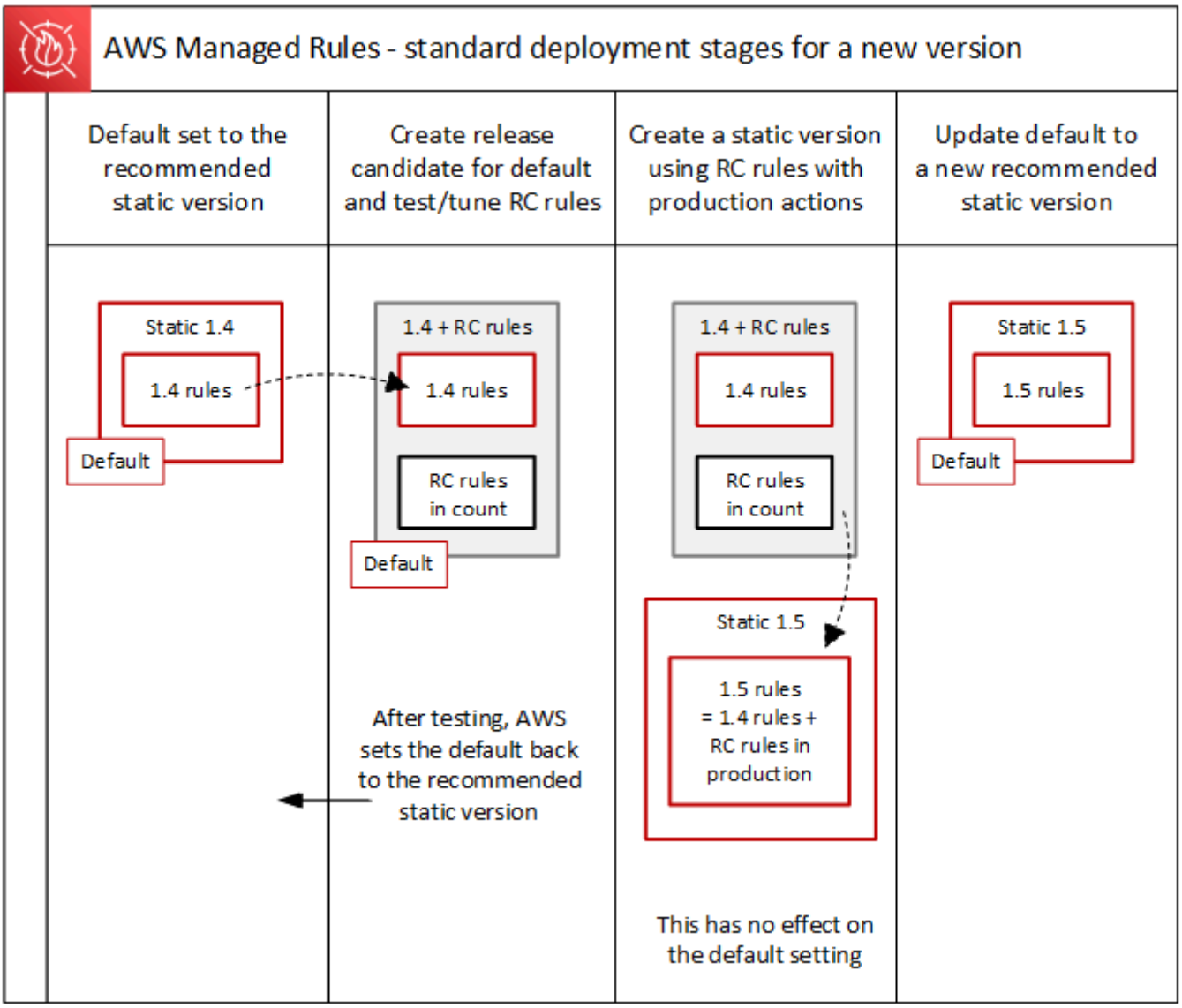
```
{
```

```
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
    }
}
```

Visão geral das implantações padrão de regras AWS gerenciadas

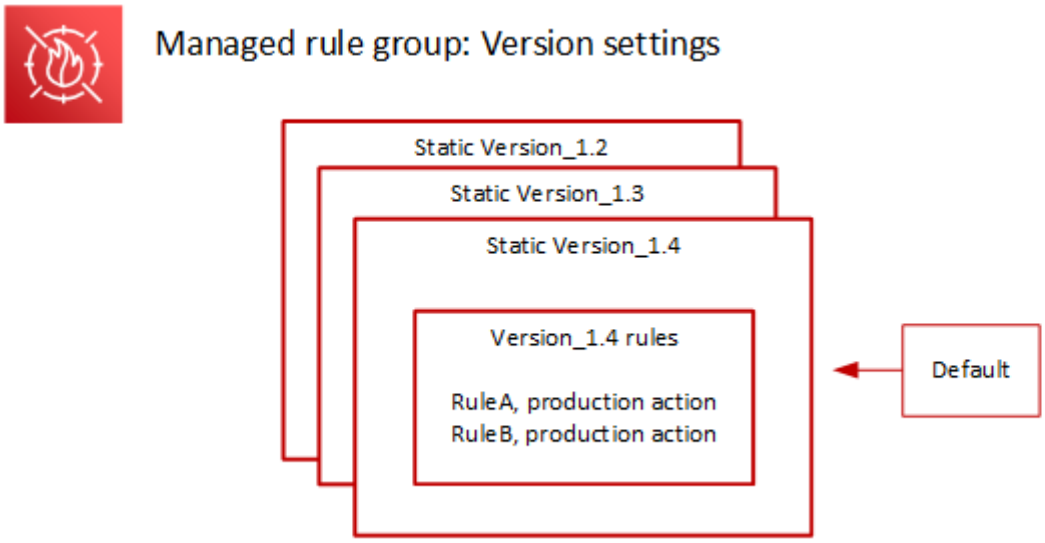
AWS implementa a nova funcionalidade de Regras AWS Gerenciadas usando três estágios padrão de implantação: candidato a lançamento, versão estática e versão padrão.

O diagrama a seguir mostra essas implantações padrão. Cada uma delas é descrita com mais detalhes nas seções seguintes.



Estados de versão típicos para regras AWS gerenciadas

Normalmente, um grupo de regras gerenciadas com versão tem várias versões estáticas não expiradas, e a versão padrão aponta para a versão estática recomendada. AWS A figura a seguir mostra um exemplo do conjunto típico de versões estáticas e da configuração de versão padrão.



A ação de produção da maioria das regras em uma versão estática é Block, mas pode ser definida como algo diferente. Para obter informações detalhadas sobre as configurações de ação de regras, consulte as listas de regras para cada grupo de regras em AWS Lista de grupos de regras de regras gerenciadas.

Implantações de Release Candidate para Regras AWS Gerenciadas

Quando AWS um conjunto candidato de regras muda para um grupo de regras gerenciado, ele as testa em uma implantação temporária do Release Candidate. AWS avalia as regras candidatas no modo de contagem em relação ao tráfego de produção e executa as atividades de ajuste final, incluindo a mitigação de falsos positivos. AWS testa as regras Release Candidate dessa forma para todos os clientes que usam a versão padrão do grupo de regras. As implantações de candidata a lançamento não se aplicam a clientes que usam uma versão estática do grupo de regras.

Se você usar a versão padrão, uma implantação de candidata a lançamento não alterará a forma como seu tráfego da web é gerenciado pelo grupo de regras. Você pode observar o seguinte enquanto as regras da candidata estão sendo testadas:

- O nome da versão padrão muda de `Default (using Version_X.Y)` para `Default (using Version_X.Y_PLUS_RC_COUNT)`.
- Métricas de contagem adicionais na Amazon CloudWatch com `RC_COUNT` seus nomes. Elas são geradas pelas regras da candidata a lançamento.

AWS testa um candidato a lançamento por cerca de uma semana, depois o remove e redefine a versão padrão para a versão estática recomendada atualmente.

AWS executa as seguintes etapas para uma implantação do Release Candidate:

1. Criar o candidato a lançamento — AWS adiciona um candidato a lançamento com base na versão estática recomendada atual, que é a versão para a qual o padrão está apontando.

   O nome do candidata a lançamento é o nome da versão estática acrescido de `_PLUS_RC_COUNT`. Por exemplo, se a versão estática recomendada atualmente for `Version_2.1`, a candidata a lançamento será nomeada `Version_2.1_PLUS_RC_COUNT`.

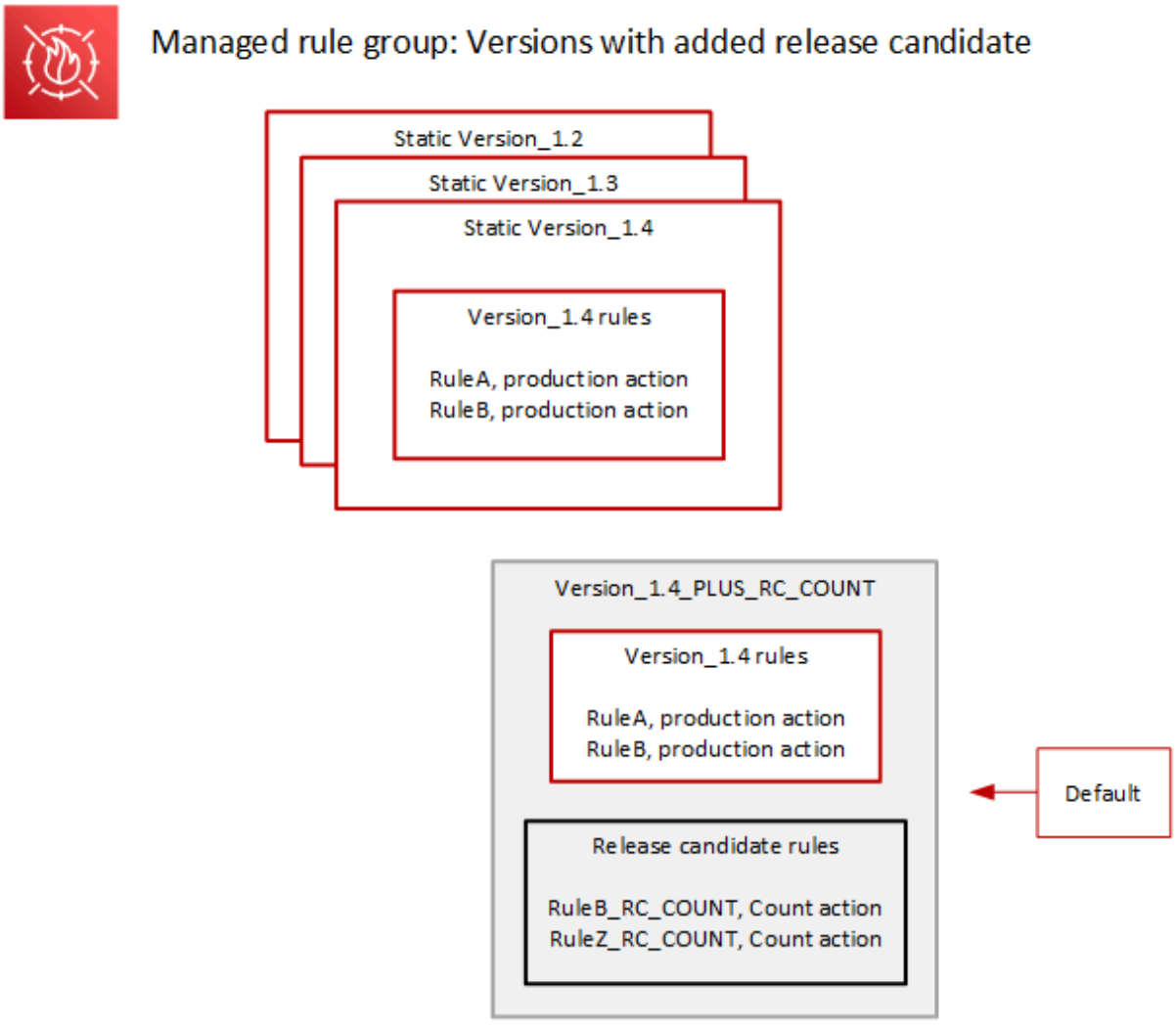
   A candidata a lançamento contém as seguintes regras:

   - Regras copiadas exatamente da versão estática recomendada atual, sem alterações nas configurações das regras.
   - Novas regras da candidata com a ação de regra definida como Count e com nomes que terminam com `_RC_COUNT`.

     A maioria das regras da candidata fornece propostas de melhorias para as regras que já existem no grupo de regras. O nome de cada uma dessas regras é o nome da regra existente acrescido de `_RC_COUNT`.
2. Defina a versão padrão para o candidato a lançamento e teste — AWS define a versão padrão para apontar para o novo candidato a lançamento, para realizar testes em relação ao seu tráfego de produção. O teste geralmente leva cerca de uma semana.

   Você verá o nome da versão padrão mudar daquele que indica somente a versão estática, como `Default (using Version_1.4)`, para um que indica a versão estática mais as regras da candidata a lançamento, como `Default (using Version_1.4_PLUS_RC_COUNT)`. Esse esquema de nomenclatura permite identificar qual versão estática você está usando para gerenciar seu tráfego da web.

   O diagrama a seguir mostra o estado das versões de exemplo de grupos de regras neste momento.



As regras da candidata a lançamento são sempre configuradas com ação Count, para que não alterem a forma como o grupo de regras gerencia o tráfego da web.

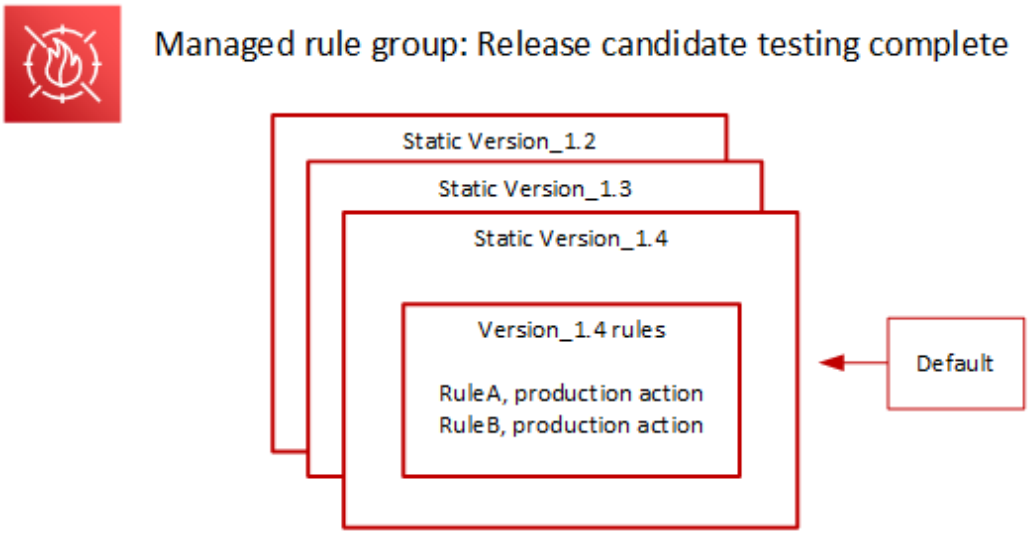
As regras do Release Candidate geram métricas de CloudWatch contagem da Amazon que são AWS usadas para verificar o comportamento e identificar falsos positivos. AWS faz ajustes conforme necessário, para ajustar o comportamento das regras de contagem de candidatos a lançamento.

A versão candidata a lançamento não é estática e não está disponível para você escolher na lista de versões estáticas de grupos de regras. Você só pode ver o nome da versão candidata a lançamento na especificação da versão padrão.

3. Retorne a versão padrão para a versão estática recomendada — Depois de testar as regras do candidato a lançamento, AWS define a versão padrão de volta para a versão estática recomendada atual. A configuração padrão do nome da versão elimina o `_PLUS_RC_COUNT` final

e o grupo de regras deixa de gerar métricas de CloudWatch contagem para as regras do Release Candidate. Essa é uma mudança silenciosa e não é o mesmo que a implantação de uma reversão de versão padrão.

O diagrama a seguir mostra o estado das versões de exemplo do grupo de regras após a conclusão do teste da candidata a lançamento.



Tempo e notificações

AWS implanta versões candidatas a lançamento conforme necessário, para testar melhorias em um grupo de regras.

- SNS — AWS envia uma notificação de SNS no início da implantação. A notificação indica o tempo estimado em que a candidata a lançamento será testada. Quando o teste for concluído, retornará AWS silenciosamente o padrão para a configuração da versão estática, sem uma segunda notificação.
- Registro de alterações — AWS não atualiza o registro de alterações ou outras partes deste guia para esse tipo de implantação.

Implantações de versões estáticas para regras AWS gerenciadas

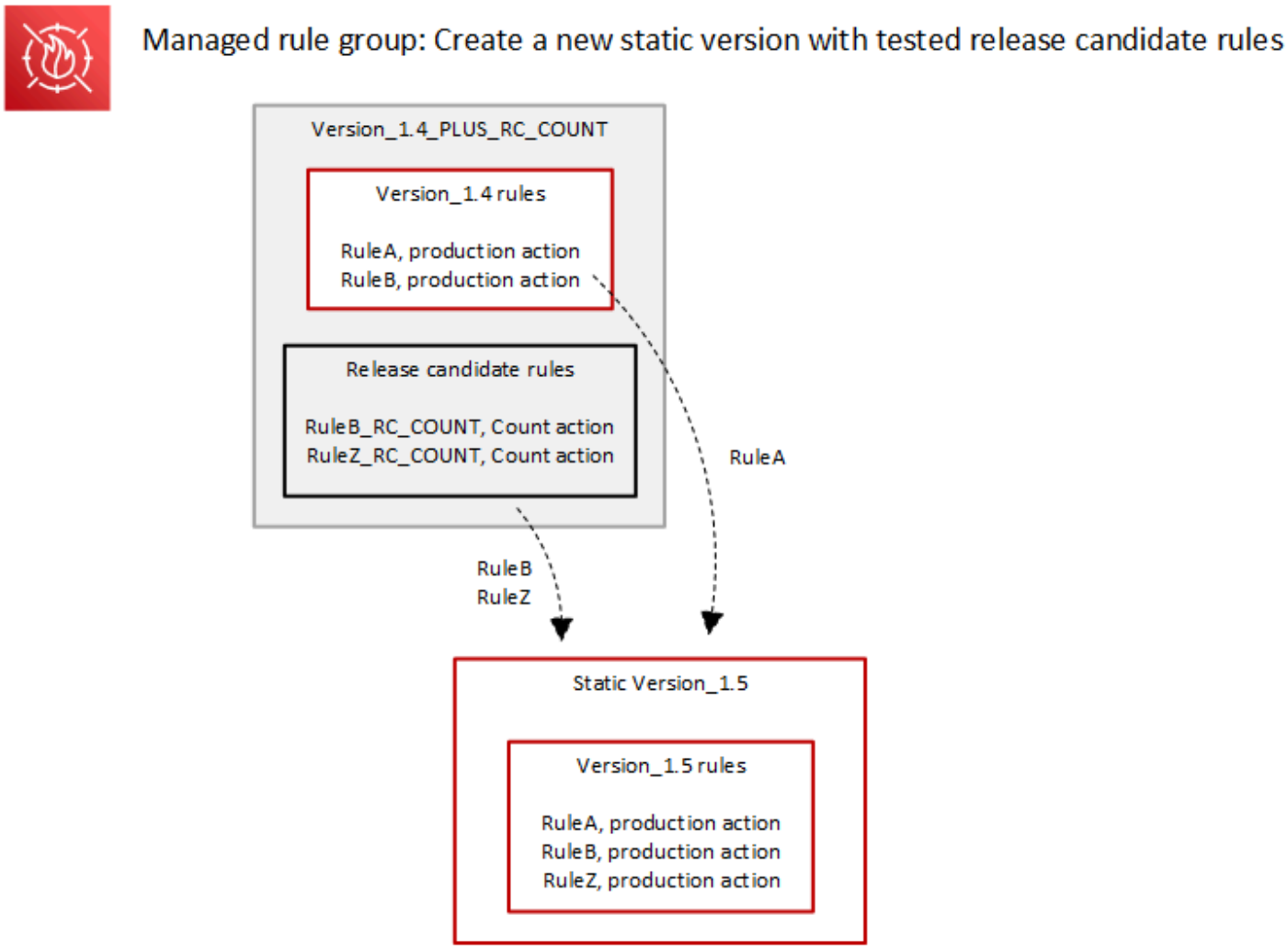
Quando AWS determina que um candidato a lançamento fornece alterações valiosas ao grupo de regras, AWS implanta uma nova versão estática para o grupo de regras com base no candidato a lançamento. Essa implantação não altera a versão padrão do grupo de regras.

A nova versão estática contém as seguintes regras da candidata a lançamento:

- Regras da versão estática anterior sem uma candidata substituta entre as regras da candidata a lançamento.
- Liberar regras da candidata, com as seguintes alterações:
  - AWS altera o nome da regra removendo o sufixo `_RC_COUNT` do candidato a lançamento.
  - AWS altera as ações da regra de Count para suas ações de regra de produção.

  Para regras de candidatas a lançamento que substituem regras anteriores existentes, isso substitui a funcionalidade das regras anteriores na nova versão estática.

O diagrama a seguir mostra a criação da nova versão estática a partir da candidata a lançamento.



Após a implantação, a nova versão estática estará disponível para você testar e usar em suas proteções, se quiser. Você pode revisar as ações e descrições de regras novas e atualizadas nas listas de regras do grupo de regras em AWS Lista de grupos de regras de regras gerenciadas.

Uma versão estática é imutável após a implantação e só muda quando AWS expira. Para obter informações sobre ciclos de vida de versão, consulte Grupos de regras gerenciados com versão.

Tempo e notificações

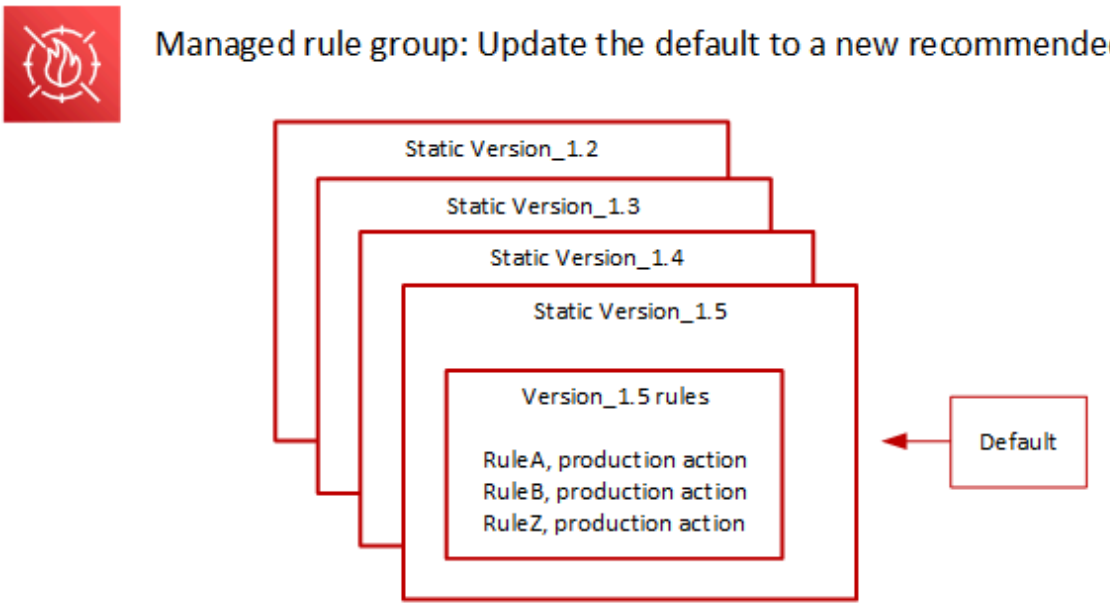
AWS implanta uma nova versão estática conforme necessário, a fim de implantar melhorias na funcionalidade do grupo de regras. A implantação de uma versão estática não afeta a configuração da versão padrão.

- SNS — AWS envia uma notificação de SNS quando a implantação é concluída.
- Registro de alterações — Depois que AWS WAF a implantação for concluída em todos os lugares disponíveis, AWS atualiza a definição do grupo de regras neste guia conforme necessário e, em seguida, anuncia o lançamento no registro de alterações do grupo de regras de regras AWS gerenciadas e na página de histórico da documentação.

Implantações de versão padrão para regras AWS gerenciadas

Quando AWS determina que uma nova versão estática fornece proteções aprimoradas para o grupo de regras em comparação com o padrão atual, AWS atualiza a versão padrão para a nova versão estática. AWS pode lançar várias versões estáticas antes de promover uma para a versão padrão do grupo de regras.

O diagrama a seguir mostra o estado das versões de exemplo do grupo de regras depois de AWS mover a configuração da versão padrão para a nova versão estática.



Antes de implantar essa alteração na versão padrão, AWS fornece notificações para que você possa testar e se preparar para as próximas alterações. Se você usar a versão padrão, não poderá realizar nenhuma ação e permanecer nela durante a atualização. Se, em vez disso, você quiser adiar a mudança para a nova versão, antes do início planejado da implantação da versão padrão, você pode configurar explicitamente seu grupo de regras para usar a versão estática para a qual o padrão está definido.

Tempo e notificações

AWS atualiza a versão padrão quando recomenda uma versão estática diferente para o grupo de regras daquela que está em uso no momento.

- SNS — AWS envia uma notificação de SNS pelo menos uma semana antes do dia de implantação pretendido e outra no dia da implantação, no início da implantação. Cada notificação inclui o nome do grupo de regras, a versão estática para a qual a versão padrão está sendo atualizada, a data de implantação e o horário programado da implantação para cada AWS região em que a atualização está sendo executada.
- Registro de alterações — AWS não atualiza o registro de alterações ou outras partes deste guia para esse tipo de implantação.

Implantações de exceções para regras gerenciadas da AWS

AWS pode ignorar os estágios padrão de implantação para implantar rapidamente atualizações que abordem riscos críticos de segurança. Uma implantação de exceção pode envolver qualquer um dos tipos de implantação padrão e pode ser implementada rapidamente em todas as AWS regiões.

AWS fornece o máximo de notificação antecipada possível para implantações de exceções.

Tempo e notificações

AWS executa implantações de exceção somente quando necessário.

- SNS — AWS envia uma notificação de SNS o mais cedo possível do dia de implantação pretendido e, em seguida, outra no início da implantação. Cada notificação inclui o nome do grupo de regras, a alteração que está sendo feita e a data de implantação.
- Registro de alterações — Se a implantação for para uma versão estática, depois que AWS WAF a implantação for concluída em todos os lugares disponíveis, AWS atualiza a definição do grupo de regras neste guia conforme necessário e, em seguida, anuncia a versão no registro de alterações do grupo de regras AWS gerenciadas e na página de histórico da documentação.

Reversões de implantação padrão para AWS regras gerenciadas

Sob certas condições, AWS pode reverter a versão padrão para a configuração anterior. Uma reversão geralmente leva menos de dez minutos para todas as AWS regiões.

AWS executa uma reversão somente para mitigar um problema significativo em uma versão estática, como um nível inaceitavelmente alto de falsos positivos.

Após a reversão da configuração da versão padrão, AWS acelera a expiração da versão estática que tem o problema e o lançamento de uma nova versão estática para resolver o problema.

Tempo e notificações

AWS executa reversões de versão padrão somente quando necessário.

- SNS — AWS envia uma única notificação de SNS no momento da reversão. A notificação inclui o nome do grupo de regras, a versão para a qual a versão padrão está sendo definida e a data de implantação. Esse tipo de implantação é muito rápido, então a notificação não fornece informações de tempo para regiões.
- Registro de alterações — AWS não atualiza o registro de alterações ou outras partes deste guia para esse tipo de implantação.

AWS Aviso de isenção de responsabilidade sobre regras gerenciadas

AWS As regras gerenciadas foram projetadas para proteger você contra ameaças comuns na web. Quando usados de acordo com a documentação, os grupos de regras de regras AWS gerenciadas adicionam outra camada de segurança aos seus aplicativos. No entanto, os grupos de regras de Regras AWS Gerenciadas não substituem suas responsabilidades de segurança, que são determinadas pelos AWS recursos que você seleciona. Consulte o Modelo de Responsabilidade Compartilhada para garantir que seus recursos AWS estejam devidamente protegidos.

AWS Registro de alterações das regras gerenciadas

Esta seção lista as alterações nas regras AWS gerenciadas AWS WAF desde seu lançamento em novembro de 2019.

> **Note**
>
> Esse changelog relata alterações nas regras e grupos de regras em Regras AWS gerenciadas para. AWS WAF

Para oGrupos de regras de reputação de IP, esse changelog relata alterações nas regras e no grupo de regras e relata mudanças significativas nas fontes das listas de endereços IP que as regras usam. Ele não relata alterações nas listas de endereços IP em si, devido à natureza dinâmica dessas listas. Se você tiver dúvidas sobre as listas de endereços IP, entre em contato com seu gerente de conta ou abra um caso no AWS Support Center.

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do sistema operacional Linux Todas as regras	Lançou a versão 2.3 estática desse grupo de regras. Isso não altera a configuração da versão padrão. Assinaturas adicionadas para melhorar a detecção.	2024-06-06
AWS WAF Grupo de regras do Bot Control AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes	Os grupos de regras de bots e fraudes agora estão versionados. Se você estiver usando qualquer um desses grupos de regras, essa atualização não altera a forma como eles lidam com seu tráfego na web. Essa atualização define a versão atual do grupo de regras para a versão estática 1.0 e define a versão padrão para apontar para ela. Para obter mais informações sobre regras gerenciadas com versão, consulte o seguinte: • Grupos de regras gerenciados com versão	2024-05-29

Grupos de regras e regras	Descrição	Data
	• Implantações para grupos de regras de regras AWS gerenciadas com versão • Como receber notificações sobre novas versões e atualizações de um grupo de regras gerenciadas	

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do sistema operacional POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS` • `UNIXShellCommandsVariables_QUERYSTRING` • `UNIXShellCommandsVariables_HEADER` • `UNIXShellCommandsVariables_BODY`	Lançou a versão 3.0 estática desse grupo de regras. Isso não altera a configuração da versão padrão. Removido `UNIXShellCommandsVariables_QUERYARGUMENTS` e substituído por`UNIXShellCommandsVariables_QUERYSTRING`. Se você tiver regras que correspondam ao rótulo de`UNIXShellCommandsVariables_QUERYARGUMENTS`, ao usar esta versão, troque-as para que correspondam ao rótulo de`UNIXShellCommandsVariables_QUERYSTRING`. O novo rótulo é`awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`. Foi adicionada a regra`UNIXShellCommandsVariables_HEADER`, que corresponde a todos os cabeçalhos. Todas as regras do grupo de regras gerenciadas foram	2024-05-28

Grupos de regras e regras	Descrição	Data
	atualizadas com uma lógica de detecção aprimorada. Foi corrigida a capitalização documentada do rótulo para. `UNIXShellCommandsVariables_BODY`	
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `CrossSiteScripting*`	Lançou a versão estática 1.12 desse grupo de regras. Adição de assinaturas para todas as regras de Cross-Site Scripting para aprimorar a detecção e reduzir os falsos positivos.	2024-05-21
Grupo de regras gerenciadas do banco de dados SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLiExtendedPatterns_QUERYARGUMENTS`	Lançou a versão 1.2 estática desse grupo de regras. A transformação de `JS_DECODE` texto foi adicionada às regras listadas.	2024-05-14

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_QUERYSTRING` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_BODY` • `Log4JRCE_HEADER`	Lançou a versão estática 1.22 desse grupo de regras. A transformação de `JS_DECODE` texto foi adicionada às regras listadas.	2024-05-08
Grupo de regras gerenciadas do sistema operacional POSIX	Lançada a versão estática 2.2 desse grupo de regras. A transformação de `JS_DECODE` texto foi adicionada às duas regras.	2024-05-08
Grupo de regras gerenciadas do sistema operacional Windows • `PowerShellCommands_BODY`	Lançada a versão estática 2.1 desse grupo de regras. Assinaturas adicionadas `PowerShellCommands_BODY` para melhorar a detecção.	2024-05-03

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas da lista de reputação de IPs da Amazon • `AWSManagedIPReputationList`	As fontes da lista de reputação de IP foram atualizadas para melhorar a identificação de endereços que estão ativamente envolvidos em atividades maliciosas e reduzir os falsos positivos. Essa atualização não envolve uma nova versão porque esse grupo de regras não tem versão.	2024-03-13
Grupo de regras gerenciadas de entradas nocivas conhecidas	Lançamento da versão estática 1.21 deste grupo de regras. Adição de assinaturas para aprimorar a detecção e reduzir os falsos positivos.	2023-12-16

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `ExploitablePaths_URIPATH`	Lançamento da versão estática 1.20 deste grupo de regras. Atualização da regra `ExploitablePaths_URIPATH` para adicionar detecção para solicitações que correspondem à vulnerabilidade de autorização inadequada (CVE-2023-22518) do Confluence da Atlassian. Esta vulnerabilidade afeta todas as versões do Confluence Data Center e do Confluence Server. Para obter mais informações, consulte NIST: National Vulnerability Database: CVE-2023-22518 Detail.	2023-12-14
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `CrossSiteScripting*`	Lançamento da versão estática 1.11 deste grupo de regras. Adição de assinaturas para todas as regras de Cross-Site Scripting para aprimorar a detecção e reduzir os falsos positivos.	2023-12-06

Grupos de regras e regras	Descrição	Data
AWS WAF Grupo de regras do Bot Control • Novo rótulo: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	Adição do rótulo de baixa atividade coordenada aos rótulos de nível de proteção direcionados do grupo de regras. Este rótulo não está associado a nenhuma regra. Esta rotulagem corresponde a um complemento às regras e aos rótulos de médio e de alto nível.	2023-12-05
Rótulos do Controle de Bots • Rótulo: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	Adição de um rótulo de sinalização ao grupo de regras que indica a detecção de uma extensão para navegador que auxilia na automação. Este rótulo não é específico para uma regra individual.	2023-11-14
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `EC2MetaDataSSRF_QUERYARGUMENTS`	Lançada a versão estática 1.10 desse grupo de regras. Uma regra foi atualizada para melhorar a detecção e reduzir os falsos positivos.	2023-11-02

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_URIPATH` • `EC2MetaDataSSRF_QUERYARGUMENTS`	Lançada a versão estática 1.9 desse grupo de regras. Regras atualizadas para melhorar a detecção e reduzir os falsos positivos.	2023-10-30
Grupo de regras gerenciadas do sistema operacional POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS`	Lançada a versão estática 2.1 desse grupo de regras. A regra de argumentos de consulta foi atualizada para melhorar a detecção.	12/10/2023

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Lançada a versão estática 1.8 desse grupo de regras. Regras atualizadas para melhorar a detecção.	11/010/2023

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `ExploitablePaths_URIPATH`	Implantação de exceção: lançada a versão estática 1.19 desse grupo de regras. A versão padrão foi atualizada para usar a versão 1.19. A regra `ExploitablePaths_URIPATH` foi atualizada para adicionar detecção para solicitações que correspondam à vulnerabilidade de escalonamento de privilégios do Atlassian Confluence CVE-2023-22515. Essa vulnerabilidade afeta algumas versões do Atlassian Confluence. Para obter mais informações, consulte NIST: National Vulnerability Database: CVE-2023-22515 Detail e Atlassian Support: FAQ for CVE-2023-22515. Para obter mais informações sobre esse tipo de implantação, consulte Implantações de exceções para regras gerenciadas da AWS.	2023-10-04

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `Host_localhost_HEADER` • `Log4J*` • `JavaDeserialization*`	Implantação de exceção: lançada a versão estática 1.18 desse grupo de regras. Esse é um lançamento rápido dessa versão estática para acomodar a criação e o lançamento da versão 1.19. A regra `Host_localhost_HEADER` e todas as regras de desserialização do Log4J e do Java foram atualizadas para melhorar a detecção. Para obter mais informações sobre esse tipo de implantação, consulte Implantações de exceções para regras gerenciadas da AWS.	2023-10-04

Grupos de regras e regras	Descrição	Data
AWS WAF Grupo de regras do Bot Control • `TGT_TokenReuseIp` • `TGT_ML_CoordinatedActivityMedium` • `TGT_ML_CoordinatedActivityHigh`	Regras adicionadas ao grupo de regras com ação Count. A regra de IP de reutilização de tokens detecta e conta o compartilhamento de tokens entre endereços IP. As regras de atividades coordenadas usam análise automatizada de machine learning (ML) do tráfego do site para detectar atividade s relacionadas a bots. Na configuração do grupo de regras, você pode cancelar o uso de ML. Com esta versão, os clientes que atualment e usam o nível de proteção direcionado optam pelo uso de ML. A desativação desativa as regras de atividades coordenadas.	2023-09-06
AWS WAF Grupo de regras do Bot Control • `CategoryAI`	A regra `CategoryAI` foi adicionada ao grupo de regras.	2023-08-30

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_QUERYARGUMENTS` • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_URIPATH`	Lançada a versão estática 1.7 desse grupo de regras. Atualizadas as extensões restritas e regras SSRF de metadados do EC2 para melhorar a detecção e reduzir os falsos positivos.	2023-07-26
AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes Todas as regras no novo grupo de regras	Foi adicionado o grupo de regras `AWSManagedRulesACFPRuleSet` .	2023-06-13

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do sistema operacional Linux • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	Lançada a versão estática 2.2 desse grupo de regras. Assinaturas adicionadas para melhorar a detecção.	2023-05-22
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	Lançada a versão estática 1.6 desse grupo de regras. O cross-site scripting (XSS) e as regras de extensão restritas foram atualizados para melhorar a detecção e reduzir os falsos positivos.	2023-04-28

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do aplicativo PHP • Atualização do `PHPHighRiskMethodsVariables_BODY` • Removido `PHPHighRiskMethodsVariables_QUERYARGUMENTS` • `PHPHighRiskMethodsVariables_QUERYSTRING` adicionado • `PHPHighRiskMethodsVariables_HEADER` adicionado	Lançada a versão estática 2.0 desse grupo de regras. Assinaturas adicionadas para melhorar a detecção em todas as regras. A regra `PHPHighRiskMethodsVariables_QUERYARGUMENTS` foi substituída por `PHPHighRiskMethodsVariables_QUERYSTRING`, que inspeciona toda a sequência de caracteres de consulta em vez de apenas os argumentos da consulta. Foi adicionada a regra `PHPHighRiskMethodsVariables_HEADER` para expandir a cobertura para incluir todos os cabeçalhos. Os rótulos a seguir foram atualizados para se alinharem com o rótulo padrão de regras AWS gerenciadas: • Nome antigo: `PHPHighRiskMethodsVariables_BODY` Novo nome: `PHPHighRiskMethodsVariables_Body` • Nome antigo: `PHPHighRiskMethodsVariables`	2023-02-27

Grupos de regras e regras	Descrição	Data
	`_QUERYARGUMENTS` Novo nome: `PHPHighRiskMethodsVariables_QueryString`	
AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes • `VolumetricIpFailedLoginResponseHigh` • `VolumetricSessionFailedLoginResponseHigh`	Foram adicionadas regras de inspeção de respostas de login para uso com CloudFront distribuições protegidas da Amazon. Essas regras podem bloquear novas tentativas de login de endereços IP e sessões de clientes que recentemente foram a fonte de muitas tentativas de login malsucedidas.	2023-02-15
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Lançada a versão estática 1.5 desse grupo de regras. Filtros de Cross Site Scripting (XSS) atualizados para melhorar a detecção.	2023-01-25

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do sistema operacional Linux • `LFI_COOKIE` : removido • `LFI_HEADER` : adicionado • `LFI_URIPATH` • `LFI_QUERYSTRING`	Lançada a versão estática 2.1 desse grupo de regras. A regra `LFI_COOKIE` e seu rótulo `awswaf:managed:aws:linux-os:LFI_Cookie` foram removidos e substituídos pela nova regra `LFI_HEADER` e seu rótulo `awswaf:managed:aws:linux-os:LFI_Header` . Essa alteração expande a inspeção para vários cabeçalhos. Foram adicionadas transformações de texto e assinaturas a todas as regras para melhorar a detecção.	2022-12-15

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Lançada a versão estática 1.4 desse grupo de regras. Foi adicionada uma transformação de texto para `NoUserAgent_HEADER` para remover todos os bytes nulos. Filtros nas regras de Cross Site Scripting (XSS) atualizados para melhorar a detecção.	2022-12-05

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER`	Lançada a versão estática 1.17 desse grupo de regras. As regras de desserialização de Java foram atualizadas para adicionar detecção de solicitações correspondentes ao CVE-2022-42889 da Apache, uma vulnerabilidade de execução remota de código (RCE) nas versões do Apache Commons Text anteriores à 1.10.0. Para obter mais informações, consulte NIST: National Vulnerability Database: CVE-2022-42889 Detail e CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults. Detecção aprimorada em `Host_localhost_HEADER` .	2022-10-20

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY`	Lançada a versão estática 1.16 desse grupo de regras. Foram removidos os falsos positivos AWS identificados na versão 1.15.	2022-10-05
Grupo de regras gerenciadas do sistema operacional POSIX Grupo de regras gerenciadas do aplicativo PHP WordPress grupo de regras gerenciado por aplicativos	Foram corrigidos os nomes dos rótulos documentados.	2022-09-19
Grupos de regras de reputação de IP • `AWSManagedIPDDoSList`	Essa alteração não altera a forma como o grupo de regras lida com o tráfego da web. Foi adicionada uma nova regra com a ação Count de inspecionar endereços IP que estão ativamente envolvidos em atividades de DDoS, de acordo com a inteligência de ameaças da Amazon.	2022-08-30

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	Lançada a versão estática 1.15 desse grupo de regras. Log4JRCE foi removido e substituído por Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI e Log4JRCE_BODY , para um monitoramento e gerenciamento mais granulares de falsos positivos. Assinaturas adicionadas para melhorar a detecção e o bloqueio de PROPFIND_METHOD e para todas as regras JavaDeserialization RCE* e Log4JRCE* . Rótulos atualizados para corrigir a capitalização em Host_localhost_HEADER e em todas as regras JavaDeserialization RCE* . Corrigida a descrição de JavaDeserialization RCE_HEADER .	2022-08-22

Grupos de regras e regras	Descrição	Data
AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes • `UnsupportedCognitoIDP`	Foi adicionada uma regra para impedir o uso do grupo de regras gerenciadas de prevenção de apropriação de contas para o tráfego da web do grupo de usuários do Amazon Cognito.	2022-08-11
Grupo de regras gerenciadas do conjunto de regras principais (CRS)	AWS tem expiração programada para as versões `Version_1.2` e `Version_2.0` do grupo de regras. As versões expirarão em 9 de setembro de 2022. Para obter informações sobre a expiração da versão, consulte Grupos de regras gerenciados com versão.	2022-06-09
Grupo de regras gerenciadas do conjunto de regras principais (CRS) • `GenericLFI_URIPATH` `GenericRFI_URIPATH`	Lançada a versão 1.3 desse grupo de regras. Essa versão atualiza as assinaturas de correspondências nas regras `GenericLFI_URIPATH` e `GenericRFI_URIPATH`, para melhorar a detecção.	2022-05-24
AWS WAF Grupo de regras do Bot Control • `CategoryEmailClient`	A regra `CategoryEmailClient` foi adicionada ao grupo de regras.	2022-04-06

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	Lançada a versão 1.14 desse grupo de regras. As quatro regras JavaDeserializtionRCE são movidas para o modo Block.	2022-03-31
Grupo de regras gerenciadas de entradas nocivas conhecidas • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	Lançada a versão 1.13 desse grupo de regras. A transformação de texto foi atualizada para as vulnerabilidades do Spring Core e do Cloud Function RCE. Essas regras estão no modo de contagem para coletar métricas e avaliar padrões correspondentes. O rótulo pode ser usado para bloquear solicitações em uma regra personalizada. Uma versão subsequente será implantada com essas regras no modo de bloqueio.	2022-03-31

Grupos de regras e regras	Descrição	Data
Grupo de regras gerenciadas de entradas nocivas conhecidas • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	Lançada a versão 1.12 desse grupo de regras. Assinaturas adicionadas para as vulnerabilidades do Spring Core e do Cloud Function RCE. Essas regras estão no modo de contagem para coletar métricas e avaliar padrões correspondentes. O rótulo pode ser usado para bloquear solicitações em uma regra personalizada. Uma versão subsequente será implantada com essas regras no modo de bloqueio. As regras Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI e Log4JRCE_BODY foram removidas e substituídas pela regra Log4JRCE.	2022-03-30
Grupos de regras de reputação de IP • AWSManagedReconnaissanceList	Atualizou a regra AWSManagedReconnaissanceList para alterar a ação de contagem para bloqueio.	2022-02-15

Grupos de regras e regras	Descrição	Data
AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes Todas as regras no novo grupo de regras	Foi adicionado o grupo de regras `AWSManagedRulesATPRuleSet` .	2022-02-11
Grupo de regras gerenciadas de entradas nocivas conhecidas • `Log4JRCE` • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URI` • `Log4JRCE_BODY`	Lançada a versão 1.9 desse grupo de regras. A regra `Log4JRCE` foi removida e substituída pelas regras `Log4JRCE_HEADER` , `Log4JRCE_QUERYSTRING` , `Log4JRCE_URI` e `Log4JRCE_BODY` , para flexibilidade no uso dessa funcionalidade. Assinaturas adicionadas para melhorar a detecção e o bloqueio.	2022-01-28

Grupos de regras e regras	Descrição	Data
Conjunto de regras principais (CRS) • `CrossSiteScripting_URIPATH` • `CrossSiteScripting_BODY` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_COOKIE`	Lançada a versão 2.0 desse grupo de regras. Para essas regras, sintonize as assinaturas de detecção para reduzir os falsos positivos. A transformação de texto `URL_DECODE` foi substituída pela transformação de texto duplo `URL_DECODE_UNI`. Foi adicionada a transformação de texto `HTML_ENTITY_DECODE`.	2022-01-10
Conjunto de regras principais (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Como parte do lançamento da versão 2.0 desse grupo de regras, foi adicionada a transformação de texto `URL_DECODE_UNI`. Removida a transformação de texto `URL_DECODE` de `RestrictedExtensions_URIPATH`.	2022-01-10

Grupos de regras e regras	Descrição	Data
Banco de dados SQL • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	Lançada a versão 2.0 desse grupo de regras. A transformação de texto URL_DECODE foi substituída pela transformação de texto duplo URL_DECODE_UNI e a transformação de texto COMPRESS_WHITE_SPACE foi adicionada. Mais assinaturas de detecção foram adicionadas a SQLiExtendedPatterns_QUERYARGUMENTS . Inspeção de JSON adicionada a SQLi_BODY . A regra SQLiExtendedPatterns_BODY foi adicionada. A regra SQLi_URIPATH foi removida.	2022-01-10
Entradas nocivas conhecidas • Log4JRCE	Lançada a versão 1.8 da regra Log4JRCE para melhorar a inspeção de cabeçalhos e os critérios de correspondência.	2021-12-17

Grupos de regras e regras	Descrição	Data
Entradas nocivas conhecidas • `Log4JRCE`	Lançada a versão 1.4 da regra `Log4JRCE` para ajustar os critérios de correspondência e inspecionar cabeçalhos adicionais. Lançada a versão 1.5 para ajustar os critérios de correspondência.	2021-12-11
Entradas nocivas conhecidas • `Log4JRCE` • `BadAuthToken_COOKIE_AUTHORIZATION`	Foi adicionada a versão 1.2 da regra `Log4JRCE` em resposta ao problema de segurança recentemente divulgado no Log4j. Para obter mais informações, consulte o CVE-2021-44228. Essa regra inspeciona caminhos de URI comuns, strings de consulta, os primeiros 8 KB do corpo da solicitação e cabeçalhos comuns. A regra usa transformações duplas de texto `URL_DECODE_UNI` . Lançada a versão 1.3 de `Log4JRCE` para ajustar os critérios de correspondência e inspecionar cabeçalhos adicionais. A regra `BadAuthToken_COOKIE_AUTHORIZATION` foi removida.	2021-12-10

A tabela a seguir lista as alterações anteriores a dezembro de 2021.

Grupos de regras e regras	Descrição	Data	
Lista de reputação de IP da Amazon	`AWSManagedReconnaissanceList`	Foi adicionada a regra `AWSManagedReconnaissanceList` no modo de monitoramento/contagem. Essa regra contém endereços IP que estão realizando reconhecimento em relação aos recursos. AWS	2021-11-23
Sistema operacional Windows	`WindowsShellCommands` `PowerShellCommands`	Foram adicionadas três novas regras para WindowsShell comandos: `WindowsShellCommands_COOKIE` `WindowsShellCommands_QUERYARGUMENTS`, `WindowsShellCommands_BODY` e. Foi adicionada uma nova PowerShell regra:`PowerShellCommands_COOKIE`.	2021-11-23

Grupos de regras e regras	Descrição	Data	
		A nomenclatura das regras `PowerShellComands` foi reestruturada com a remoção das strings _Set1 e _Set2. Adicionadas assinaturas de detecção mais abrangentes a `PowerShellRules`. Adicionada a transformação de texto `URL_DECODE_UNI` a todas as regras do sistema operacional Windows.	

Grupos de regras e regras	Descrição	Data	
Sistema operacional Linux	`LFI_URIPATH` `LFI_QUERYSTRING` `LFI_BODY` `LFI_COOKIE`	Substituída a transformação dupla de texto `URL_DECODE` por `URL_DECODE_UNI` dupla. Adicionado `NORMALIZE_PATH_WIN` como uma segunda transformação de texto. Substituída a regra `LFI_BODY` pela regra `LFI_COOKIE` . Foram adicionadas as assinaturas de detecção mais abrangentes para todas as regras `LFI`.	2021-11-23
Conjunto de regras principais (CRS)	`SizeRestrictions_BODY`	Reduzido o limite de tamanho para bloquear solicitações da web com cargas corporais maiores que 8 KB. Anteriormente, o limite era de 10 KB.	2021-10-27

Grupos de regras e regras	Descrição	Data	
Conjunto de regras principais (CRS)	`EC2MetaDataSSRF_BODY` `EC2MetaDataSSRF_COOKIE` `EC2MetaDataSSRF_URIPATH` `EC2MetaDataSSRF_QUERYARGUMENTS`	Adicionadas mais assinaturas de detecção. Adicionada a decodificação dupla de URL Unicode para melhorar o bloqueio.	2021-10-27
Conjunto de regras principais (CRS)	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` `RestrictedExtensions_URIPATH` `RestrictedExtensions_QUERYARGUMENTS`	Adicionada a decodificação dupla de URL Unicode para melhorar o bloqueio.	2021-10-27

Grupos de regras e regras	Descrição	Data	
Conjunto de regras principais (CRS)	`GenericRFI_QUERYARGUMENTS` `GenericRFI_BODY` `GenericRFI_URIPATH`	As assinaturas de regras foram atualizadas para reduzir os falsos positivos, com base no feedback dos clientes. Adicionada a decodificação dupla de URL Unicode para melhorar o bloqueio.	2021-10-27
Todos	Todas as regras	Foi adicionado suporte para AWS WAF rótulos a todas as regras que ainda não eram compatíveis com rótulos.	2021-10-25
Lista de reputação de IP da Amazon	`AWSManagedIPReputationList_xxxx`	Reestruturou a lista de reputação de IP, removeu sufixos do nome da regra e adicionou suporte para AWS WAF rótulos.	2021-05-04
Lista de IPs anônimos	`AnonymousIPList` `HostingProviderList`	Foi adicionado suporte para AWS WAF rótulos.	2021-05-04
Controle de Bots	Todos	Foi adicionado o conjunto de regras do Controle de Bots.	2021-04-01

Grupos de regras e regras	Descrição	Data	
Conjunto de regras principais (CRS)	`GenericRFI_QUERYARGUMENTS`	Adicionada a decodificação dupla de URL.	2021-03-03
Conjunto de regras principais (CRS)	`RestrictedExtensions_URIPATH`	Melhoria da configuração das regras e adição de uma decodificação de URL extra.	2021-03-03
Proteção do administrador	`AdminProtection_URIPATH`	Adicionada a decodificação dupla de URL.	2021-03-03
Entradas nocivas conhecidas	`ExploitablePaths_URIPATH`	Melhoria da configuração das regras e adição de uma decodificação de URL extra.	2021-03-03
Sistema operacional Linux	`LFI_QUERYARGUMENTS`	Melhoria da configuração das regras e adição de uma decodificação de URL extra.	2021-03-03
Sistema operacional Windows	Todos	A configuração das regras foi aprimorada.	2020-09-23

Grupos de regras e regras	Descrição	Data	
Aplicativo PHP	`PHPHighRiskMethodsVariables_QUERYARGUMENTS` `PHPHighRiskMethodsVariables_BODY`	Alteração da transformação de texto de decodificação de HTML para decodificação de URL, para melhorar o bloqueio.	2020-09-16
Sistema operacional POSIX	`UNIXShellCommandsVariables_QUERYARGUMENTS` `UNIXShellCommandsVariables_BODY`	Alteração da transformação de texto de decodificação de HTML para decodificação de URL, para melhorar o bloqueio.	2020-09-16
Conjunto de regras principais	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` GenericLFI_BODY	Alteração da transformação de texto de decodificação de HTML para decodificação de URL, para melhorar o bloqueio.	2020-08-07

Grupos de regras e regras	Descrição	Data	
Sistema operacional Linux	`LFI_URIPATH` `LFI_QUERY ARGUMENTS` `LFI_BODY`	Alteração da transformação de texto de decodific ação de entidade HTML para decodific ação de URL, para melhorar a detecção e o bloqueio.	2020-05-19
Lista de IPs anônimos	Todos	Novo grupo de regras em Grupos de regras de reputação de IP para bloquear solicitaç ões de serviços que permitem a ofuscação da identidade do visualizador, a fim de ajudar a mitigar bots e evasão de restrições geográficas.	2020-03-06
WordPress aplicação	`WordPress Exploitab leCommand s_QUERYSTRING`	Nova regra que verifica comandos exploráveis na string de consulta.	2020-03-03

Grupos de regras e regras	Descrição	Data	
Conjunto de regras principais (CRS)	`SizeRestrictions_QUERYSTRING` `SizeRestrictions_Cookie_HEADER` `SizeRestrictions_BODY` `SizeRestrictions_URIPATH`	Ajuste das restrições de valor de tamanho para maior precisão.	2020-03-03
Banco de dados SQL	`SQLi_URIPATH`	Agora, as regras verificam o URI da mensagem.	2020-01-23
Banco de dados SQL	`SQLi_BODY` `SQLi_QUERYARGUMENTS` `SQLi_COOKIE`	Atualizações de transformações de texto.	2019-12-20

Grupos de regras e regras	Descrição	Data	
Conjunto de regras principais (CRS)	`CrossSite Scripting _URIPATH` `CrossSite Scripting_BODY` `CrossSite Scripting _QUERYARG UMENTS` `CrossSite Scripting _COOKIE`	Atualizações de transformações de texto.	2019-12-20

AWS Marketplace grupos de regras gerenciados

AWS Marketplace grupos de regras gerenciadas estão disponíveis por assinatura por meio do AWS Marketplace console em AWS Marketplace. Depois de se inscrever em um grupo de regras AWS Marketplace gerenciadas, você pode usá-lo em AWS WAF. Para usar um grupo de AWS Marketplace regras em uma AWS Firewall Manager AWS WAF política, cada conta em sua organização deve se inscrever nele.

Teste e ajuste todas as alterações em suas AWS WAF proteções antes de usá-las para tráfego de produção. Para mais informações, consulte Testando e ajustando suas AWS WAF proteções.

AWS Marketplace Preços do Rule Group

AWS Marketplace grupos de regras estão disponíveis sem contratos de longo prazo e sem compromissos mínimos. Quando você se inscrever em um grupo de regras, será cobrada uma taxa mensal (pro-rata por hora) e taxas contínuas com base no volume de solicitações. Para obter mais informações, consulte AWS WAF Preços e a descrição de cada grupo de AWS Marketplace regras em AWS Marketplace.

Tem dúvidas sobre um grupo de AWS Marketplace regras?

Para perguntas sobre um grupo de regras gerenciado por um AWS Marketplace vendedor e para solicitar alterações na funcionalidade, entre em contato com a equipe de suporte ao cliente do fornecedor. Para encontrar informações de contato, consulte a lista do provedor em AWS Marketplace.

O provedor do grupo de AWS Marketplace regras determina como gerenciar o grupo de regras, por exemplo, como atualizar o grupo de regras e se o grupo de regras tem versão. O provedor também determina os detalhes do grupo de regras, incluindo as regras, as ações das regras e quaisquer rótulos que as regras adicionem às solicitações da web correspondentes.

Inscrever-se em grupos de regras AWS Marketplace gerenciados

Você pode se inscrever e cancelar a inscrição em grupos de AWS Marketplace regras no AWS WAF console.

> **Important**
>
> Para usar um grupo de AWS Marketplace regras em uma AWS Firewall Manager política, cada conta em sua organização deve primeiro se inscrever nesse grupo de regras.

Para se inscrever em um grupo de regras AWS Marketplace gerenciadas

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha AWS Marketplace.
3. Na seção Available marketplace products, escolha o nome de um grupo de regras para visualizar os detalhes e as informações da definição de preço.
4. Se você quiser se inscrever no grupo de regras, escolha Continue.

   > **Note**
   >
   > Se você não quiser se inscrever nesse grupo de regras, basta fechar esta página em seu navegador.

5. Escolha Set up your account.

6. Adicione o grupo de regras a uma web ACL de maneira semelhante à forma como você adiciona uma regra individual. Para obter mais informações, consulte Criação de uma web ACL ou Edição de uma web ACL.

> **Note**
>
> Ao adicionar um grupo de regras a uma web ACL, você pode modificar as ações das regras no grupo de regras e do resultado do grupo de regras. Para ter mais informações, consulte Opções de substituição de ação para grupos de regras.

Depois de se inscrever em um grupo de AWS Marketplace regras, você o usa em suas ACLs da web da mesma forma que faz com outros grupos de regras gerenciados. Para mais informações, consulte Criação de uma web ACL.

Cancelamento da assinatura de grupos de regras AWS Marketplace gerenciados

Você pode cancelar a assinatura de grupos de AWS Marketplace regras no AWS WAF console.

> **Important**
>
> Para interromper as cobranças de assinatura de um grupo de regras AWS Marketplace gerenciadas, você deve removê-lo de todas as ACLs da web em AWS WAF e em qualquer AWS WAF política do Firewall Manager, além de cancelar a assinatura. Se você cancelar a assinatura de um grupo de regras AWS Marketplace gerenciadas, mas não o remover de suas ACLs da web, você continuará sendo cobrado pela assinatura.

Para cancelar a assinatura de um grupo de regras AWS Marketplace gerenciadas

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. Remova o grupo de regras de todas as :web ACLs. Para ter mais informações, consulte Edição de uma web ACL.
3. No painel de navegação, escolha AWS Marketplace.
4. Escolha Manage your subscriptions.
5. Escolha Cancel subscription ao lado do nome do grupo de regras do qual você deseja cancelar a assinatura.

6. Escolha Yes, cancel subscription.

Solução de problemas de grupos de AWS Marketplace regras

Se você descobrir que um grupo de AWS Marketplace regras está bloqueando o tráfego legítimo, você pode solucionar o problema executando as etapas a seguir.

Para solucionar problemas de um grupo de regras do AWS Marketplace

1. Substitua as ações para contar com as regras que estão bloqueando o tráfego legítimo. Você pode identificar quais regras estão bloqueando solicitações específicas usando os AWS WAF exemplos de solicitações ou AWS WAF registros. Você pode identificar as regras examinando o campo `ruleGroupId` no log ou o `RuleWithinRuleGroup` na solicitação de amostra. Você pode identificar a regra no padrão `<Seller Name>#<RuleGroup Name>#<Rule Name>`.
2. Se definir regras específicas para contar apenas solicitações não resolver o problema, você poderá substituir todas as ações da regra ou alterar a ação do próprio grupo de AWS Marketplace regras de Sem substituição para Substituir para contar. Isso permite que a solicitação da web passe, independentemente das ações de regra individuais dentro do grupo de regras.
3. Depois de ignorar a ação de regra individual ou toda a ação do grupo de AWS Marketplace regras, entre em contato com a equipe de suporte ao cliente do provedor do grupo de regras para solucionar o problema. Para obter informações de contato, consulte a lista de grupos de regras nas páginas de lista de produtos no AWS Marketplace.

Contatando AWS o suporte

Para problemas com AWS WAF ou com um grupo de regras gerenciado por AWS, entre em contato com AWS Support. Para problemas com um grupo de regras gerenciado por um AWS Marketplace vendedor, entre em contato com a equipe de suporte ao cliente do fornecedor. Para encontrar informações de contato, consulte a lista do provedor em AWS Marketplace.

Gerenciar seus próprios grupos de regras

Você pode criar seu próprio grupo de regras para reutilizar coleções de regras que você não encontra nas ofertas de grupos de regras gerenciadas ou que você mesmo prefere manipular.

Grupos de regras que você cria retém as regras da mesma forma que uma web ACL faz, e você adiciona regras a um grupo de regras da mesma forma como faz a uma web ACL. Ao criar seu próprio grupo de regras, você deve definir uma capacidade máxima imutável para ele.

Tópicos

Criar um grupo de regras

Para criar um novo grupo de regras, siga o procedimento nesta página.

Para criar um grupo de regras

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Rule groups (Grupos de regras), e, em seguida, Create rule group (Criar grupo de regras).
3. Insira um nome e uma descrição para o grupo de regras. Você usará essas informações para identificar o conjunto de regras a fim de gerenciá-lo e usá-lo.

   Não use nomes que comecem com `AWS`, `Shield`, `PreFM` ou `PostFM`. Essas sequências de caracteres são reservadas ou podem causar confusão com grupos de regras gerenciadas para você por outros serviços. Consulte Grupos de regras fornecidos por outros serviços.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar o grupo de regras.

4. Para Region (Região), escolha a região onde deseja armazenar o grupo de regras. Para usar um grupo de regras em ACLs da web que protegem CloudFront as distribuições da Amazon, você deve usar a configuração global. Você também pode usar a configuração global para aplicações regionais.

5. Escolha Próximo.
6. Adicione regras ao grupo de regras usando o assistente do Rule builder (Construtor de regras) da mesma forma que você faz no gerenciamento de web ACL. A única diferença é que você não pode adicionar um grupo de regras a outro grupo de regras.
7. Para Capacity (Capacidade), defina o máximo para o uso do grupo de regras de unidades de capacidade da web ACL (WCUs). Essa é uma configuração imutável. Para obter informações sobre WCUs, consulte AWS WAF unidades de capacidade web ACL (WCUs).

   À medida que você adiciona regras ao grupo de regras, o painel Add rules and set capacity (Adicionar regras e definir capacidade) exibe a capacidade mínima necessária, que se baseia nas regras que você já adicionou. Você pode usar isso e seus planos futuros para o grupo de regras a fim de ajudar a estimar a capacidade que o grupo de regras exigirá.
8. Revise as configurações do grupo de regras e selecione Create (Criar).

Como editar um grupo de regras

Para adicionar ou remover regras de um grupo de regras ou alterar as configurações, acesse o grupo de regras usando o procedimento desta página.

> ⚠ Risco de tráfego de produção
>
> Se você alterar um grupo de regras que está usando atualmente em uma web ACL, essas alterações afetarão o comportamento da sua web ACL onde quer que ela esteja sendo usada. Certifique-se de testar e ajustar todas as alterações em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

Para editar um grupo de regras

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Grupos de regras.
3. Escolha o nome do grupo de regras que você deseja editar. O console leva você à página do grupo de regras.

4. Edite o grupo de regras, conforme necessário. Você pode editar as propriedades mutáveis do grupo de regras, da mesma forma que você fez durante a criação. O console salva suas alterações à medida que você avança.

> **Note**
>
> Se você alterar o nome de uma regra e quiser que o nome da métrica da regra reflita a alteração, você também deverá atualizar o nome da métrica. AWS WAF não atualiza automaticamente o nome da métrica de uma regra quando você altera o nome da regra. Você pode alterar o nome da métrica ao editar a regra no console, usando o editor JSON de regras. Você também pode alterar os dois nomes por meio das APIs e em qualquer lista JSON usada para definir sua web ACL ou grupo de regras.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Usar o seu grupo de regras em uma web ACL

Para usar um grupo de regras em uma web ACL, você o adiciona à web ACL em uma instrução de referência do grupo de regras.

Risco de tráfego de produção

Antes de implantar alterações em sua web ACL para tráfego de produção, teste-as e ajuste-as em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste suas regras atualizadas no modo de contagem com seu tráfego de produção antes de ativá-las. Para obter orientações, consulte Testando e ajustando suas AWS WAF proteções.

Note

O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

No console, ao adicionar ou atualizar as regras em sua web ACL, na página Adicionar regras e grupos de regras selecione Adicionar regras, e, em seguida, selecione Adicionar minhas próprias regras e grupos de regras. Em seguida, selecione Rule group (Grupo de regras) e selecione seu grupo de regras na lista.

Em sua web ACL, você pode alterar o comportamento de um grupo de regras e suas regras definindo as ações de regras individuais como Count ou qualquer outra ação. Isso pode ajudar você a fazer coisas como testar um grupo de regras, identificar falsos positivos de regras em um grupo de regras e personalizar como um grupo de regras gerenciadas lida com suas solicitações. Para ter mais informações, consulte Opções de substituição de ação para grupos de regras.

Se seu grupo de regras contiver uma instrução baseada em intervalos, cada web ACL em que você usa o grupo de regras tem seu próprio acompanhamento e gerenciamento de intervalos separados para a regra baseada em intervalos, independente de qualquer outra web ACL em que você usa o grupo de regras. Para ter mais informações, consulte Instrução de regra baseada em intervalos.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Compartilhar um grupo de regras com outra conta

Você pode compartilhar um grupo de regras com outras contas, para uso por essas contas. Você pode compartilhar com uma ou mais contas específicas e pode compartilhar com todas as contas em uma organização.

Para fazer isso, use a AWS WAF API para criar uma política para o compartilhamento de grupos de regras que você deseja. Para obter mais informações, consulte PutPermissionPolicya Referência AWS WAF da API.

Excluir um grupo de regras

Siga as orientações nesta seção para excluir um grupo de regras.

Como excluir um conjunto e grupo de regras refenciados

Quando você exclui uma entidade que pode ser usada em uma ACL da web, como um conjunto de IP, conjunto de padrões regex ou grupo de regras, AWS WAF verifica se a entidade está sendo usada atualmente em uma ACL da web. Se descobrir que está em uso, AWS WAF avisa você. AWS WAF quase sempre é capaz de determinar se uma entidade está sendo referenciada por uma ACL da web. No entanto, em casos raros, talvez não seja possível fazer isso. Se você precisar ter certeza de que nada está usando a entidade no momento, verifique em suas web ACLs antes de excluir. Se a entidade for um conjunto referenciado, verifique também se nenhum grupo de regras está utilizando-a.

Para excluir um grupo de regras

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Grupos de regras.
3. Escolha o grupo de regras que você deseja excluir e, em seguida, selecione Delete (Excluir).

Grupos de regras fornecidos por outros serviços

Se você ou um administrador da sua organização usa AWS Firewall Manager ou AWS Shield Advanced gerencia proteções de recursos usando AWS WAF, talvez você veja declarações de referência de grupos de regras adicionadas às ACLs da web em sua conta.

Os nomes desses grupos de regras começam com as seguintes sequências de caracteres:

- **`ShieldMitigationRuleGroup`**— Esses grupos de regras são gerenciados AWS Shield Advanced e usados para fornecer mitigação automática de DDoS na camada de aplicativo para recursos protegidos da camada de aplicativos (camada 7).

  Quando você ativa a mitigação automática de DDoS na camada de aplicativo para um recurso protegido, o Shield Advanced adiciona um desses grupos de regras à web ACL que você associou ao recurso. O Shield Advanced atribui à instrução de referência do grupo de regras uma configuração de prioridade de 10.000.000, para que ela seja executada após as regras que você configurou na web ACL. Para obter mais informações sobre esses grupos de regras, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

  > **Warning**
  >
  > Não tente gerenciar manualmente esse grupo de regras na sua web ACL. Em particular, não exclua manualmente a instrução de referência do grupo de regras `ShieldMitigationRuleGroup` da sua web ACL. Fazer isso pode ter consequências não intencionais para todos os recursos associados à web ACL. Em vez disso, use o Shield Advanced para desativar a mitigação automática dos recursos que estão associados à web ACL. O Shield Advanced removerá o grupo de regras para você quando ele não for necessário para a mitigação automática.

- **`PREFMManaged`**e **`POSTFMManaged`** — Esses grupos de regras são gerenciados por AWS Firewall Manager. O Firewall Manager os fornece dentro de web ACLsque o Firewall Manager cria e

gerencia. Os nomes das web ACLs começam com `FMManagedWebACLV2`. Para obter informações sobre essas web ACLs e grupos de regras, consulte AWS WAF políticas.

AWS WAF regras

Uma AWS WAF regra define como inspecionar solicitações web HTTP (S) e a ação a ser tomada em uma solicitação quando ela corresponde aos critérios de inspeção. Você define regras somente no contexto de um grupo de regras ou web ACL.

As regras não existem AWS WAF sozinhas. Eles não são AWS recursos e não têm nomes de recursos da Amazon (ARNs). Você pode acessar uma regra por nome no grupo de regras ou na web ACL em que ela está definida. Você pode gerenciar regras e copiá-las para outras web ACLsusando o formato JSON do grupo de regras ou da web ACL que contém a regra. Você também pode gerenciá-los por meio do criador de regras do AWS WAF console, que está disponível para ACLs da web e grupos de regras.

Nome da regra

Cada regra exige um nome. Evite nomes que comecem com `AWS` e nomes usados para grupos de regras ou regras gerenciadas para você por outros serviços. Consulte Grupos de regras fornecidos por outros serviços.

> **Note**
>
> Se você alterar o nome de uma regra e quiser que o nome da métrica da regra reflita a alteração, você também deverá atualizar o nome da métrica. AWS WAF não atualiza automaticamente o nome da métrica de uma regra quando você altera o nome da regra. Você pode alterar o nome da métrica ao editar a regra no console, usando o editor JSON de regras. Você também pode alterar os dois nomes por meio das APIs e em qualquer lista JSON usada para definir sua web ACL ou grupo de regras.

Instrução de regra

Cada regra também exige uma instrução de regra que defina como a regra inspeciona as solicitações da web. A instrução de regra pode conter outras instruções aninhadas em qualquer profundidade, dependendo da regra e do tipo de instrução. Algumas instruções de regras exigem conjuntos de critérios. Por exemplo, você pode especificar até 10.000 endereços IP ou intervalos de endereços IP em uma regra de endereços IP.

Você pode definir regras que inspecionam critérios como os seguintes:

- Scripts que provavelmente são mal-intencionados. Os invasores incorporam scripts que podem explorar vulnerabilidades nas aplicações web. Isso é conhecido como cross-site scripting (XSS).
- Endereços IP ou intervalos de endereços IP dos quais as solicitações se originam.
- País ou localização geográfica de origem das solicitações.
- Comprimento da parte específica da solicitação, como a string de consulta.
- Código SQL que provavelmente é mal-intencionado. Os invasores tentam extrair dados do seu banco de dados ao incorporarem código SQL mal-intencionado a uma solicitação da web. Isso é conhecido como injeção de SQL.
- Strings que aparecem na solicitação, por exemplo, valores que aparecem no cabeçalho `User-Agent` ou strings de texto que aparecem na string de consulta. Você também pode usar expressões regulares (regex) para especificar essas strings.
- Rótulos que as regras anteriores na web ACL adicionaram à solicitação.

Além de instruções com critérios de inspeção de solicitações da web, como as da lista anterior, AWS WAF oferece suporte a instruções lógicas para `AND`, `OR`, e `NOT` que você usa para combinar instruções em uma regra.

Por exemplo, com base em solicitações recentes que você viu de um invasor, você pode criar uma regra com uma instrução `AND` lógica que combina as seguintes instruções aninhadas:

- As solicitações vêm de 192.0.2.44.
- Elas contém o valor `BadBot` no cabeçalho do `User-Agent`.
- Elas parecem incluir código do tipo SQL na query string.

Nesse caso, a solicitação da web precisa corresponder a todas as instruções para resultar em uma correspondência para o `AND` de nível superior.

Tópicos

- Instruções de regra do grupo de regras

Ação da regra

A ação da regra diz AWS WAF o que fazer com uma solicitação da web quando ela corresponde aos critérios definidos na regra. Opcionalmente, você pode adicionar um comportamento personalizado a cada ação da regra.

> **Note**
>
> As ações de regra podem ser de encerramento ou não. Uma ação de encerramento interrompe a avaliação da web ACL da solicitação e permite que ela continue em seu aplicativo protegido ou a bloqueia.

Veja as opções da ação da regra:

- Allow— AWS WAF permite que a solicitação seja encaminhada ao AWS recurso protegido para processamento e resposta. Essa é uma ação de encerramento. Nas regras que define, você pode inserir cabeçalhos personalizados na solicitação antes de encaminhá-la para o recurso protegido.
- Block— AWS WAF bloqueia a solicitação. Essa é uma ação de encerramento. Por padrão, seu AWS recurso protegido responde com um código de `403 (Forbidden)` status HTTP. Nas regras que você define, você pode personalizar a resposta. Quando AWS WAF bloqueia uma solicitação, as configurações da Block ação determinam a resposta que o recurso protegido envia de volta ao cliente.
- Count— AWS WAF conta a solicitação, mas não determina se ela deve ser permitida ou bloqueada. Essa não é uma ação de encerramento, o AWS WAF continua processando as regras restantes na web ACL. Nas regras que você define, você pode inserir cabeçalhos personalizados na solicitação e adicionar rótulos com os quais outras regras possam corresponder.
- CAPTCHAe Challenge — AWS WAF usa quebra-cabeças de CAPTCHA e desafios silenciosos para verificar se a solicitação não vem de um bot e AWS WAF usa tokens para rastrear as respostas recentes bem-sucedidas dos clientes.

  Os quebra-cabeças de CAPTCHA e os desafios silenciosos só podem ser executados quando os navegadores estão acessando endpoints HTTPS. Os clientes do navegador devem estar sendo executados em contextos seguros para adquirir tokens.

> **Note**
>
> São cobradas taxas adicionais quando você usa a ação de regra CAPTCHA ou Challenge em uma de suas regras ou como uma substituição de ação de regra em um grupo de regras. Para obter mais informações, consulte Preços do AWS WAF.

Essas ações de regra podem ser terminais ou não, dependendo do estado do token na solicitação:

- Não encerramento para token válido e não expirado — Se o token for válido e não expirado de acordo com o CAPTCHA configurado ou o tempo de imunidade de desafio, AWS WAF tratará a solicitação de forma semelhante à ação. Count AWS WAF continua inspecionando a solicitação da web com base nas regras restantes na ACL da web. Semelhante à configuração de Count, nas regras que define, você pode, opcionalmente, configurar essas ações com cabeçalhos personalizados para inserir na solicitação e adicionar rótulos aos quais outras regras possam corresponder.
- AWS WAF Encerramento com solicitação bloqueada de token inválido ou expirado — Se o token for inválido ou a data e hora indicada expirar, encerra a inspeção da solicitação da web e bloqueia a solicitação, semelhante à ação. Block AWS WAF em seguida, responde ao cliente com um código de resposta personalizado. PoisCAPTCHA, se o conteúdo da solicitação indicar que o navegador do cliente pode lidar com isso, AWS WAF envia um quebra-cabeça CAPTCHA em um JavaScript intersticial, projetado para distinguir clientes humanos de bots. Para a Challenge ação, AWS WAF envia um JavaScript intersticial com um desafio silencioso projetado para distinguir navegadores normais de sessões que estão sendo executadas por bots.

Para obter informações adicionais, consulte CAPTCHAe Challenge em AWS WAF.

Para obter informações sobre como personalizar solicitações e respostas, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Para obter informações sobre como adicionar rótulos às solicitações correspondentes, consulte AWS WAF rótulos em solicitações da web.

Para obter mais informações sobre como a web ACL e as configurações de regra interagem, consulte Avaliação de regras da web ACL e do grupo de regras.

Princípios básicos da instrução de regras

As declarações de regras são parte de uma regra que informa AWS WAF como inspecionar uma solicitação da web. Quando AWS WAF encontramos os critérios de inspeção em uma solicitação da web, dizemos que a solicitação da web corresponde à declaração. Cada instrução de regra especifica o que procurar e como, de acordo com o tipo de instrução.

Cada regra em AWS WAF tem uma única declaração de regra de nível superior, que pode conter outras declarações. As instruções de regras podem ser muito simples. Por exemplo, você pode ter uma instrução que forneça um conjunto de países de origem para inspecionar suas solicitações da web ou você pode ter uma instrução de regra em uma web ACL que apenas faça referência a um grupo de regras. As instruções de regras também podem ser muito complexas. Por exemplo, você pode ter uma instrução que combina muitas outras instruções com instruções lógicas AND, OR, and NOT.

Para a maioria das regras, você pode adicionar AWS WAF rótulos personalizados às solicitações correspondentes. As regras nos grupos de regras de regras AWS gerenciadas adicionam rótulos às solicitações correspondentes. Os rótulos que uma regra adiciona fornecem informações sobre a solicitação às regras que são avaliadas posteriormente na ACL da web e também em AWS WAF registros e métricas. Para obter informações sobre rotulagem, consulte AWS WAF rótulos em solicitações da web Instrução de regra de correspondência de rótulo e.

Como aninhar instruções de regra

AWS WAF suporta aninhamento para muitas declarações de regras, mas não para todas. Por exemplo, você não pode aninhar uma instrução de grupo de regras dentro de outra instrução. Você precisa usar o aninhamento em alguns cenários, como instruções de redução de escopo e instruções lógicas. As listas de instruções de regras e os detalhes das regras a seguir descrevem os recursos e requisitos de aninhamento de cada categoria e regra.

O editor visual de regras no console oferece suporte a apenas um nível de aninhamento para instruções de regras. Por exemplo, você pode aninhar muitos tipos de instruções dentro de uma regra lógica AND ou OR, mas não pode aninhar outra regra AND ou OR, porque isso requer um segundo nível de aninhamento. Para implementar vários níveis de aninhamento, forneça a definição da regra em JSON, seja por meio do editor de regras JSON no console ou por meio das APIs.

Tópicos

- Instruções que fazem referência a um conjunto ou a um grupo de regras

Especificação e tratamento de componentes de solicitações da Web

Esta seção descreve as configurações que você pode especificar nas instruções de regra que inspecionam um componente da solicitação da web. Para obter informações sobre o uso, consulte as instruções de regras individuais em Instruções de regra de correspondência.

Um subconjunto desses componentes de solicitação da web também pode ser usado em regras baseadas em taxas, como chaves personalizadas de agregação de solicitações. Para mais informações, consulte Opções e chaves de agregação de regras com base em taxas.

Para as configurações do componente de solicitação, você especifica o próprio tipo de componente e quaisquer opções adicionais, dependendo do tipo de componente. Por exemplo, ao inspecionar um tipo de componente que contém texto, você pode aplicar transformações de texto nele antes de inspecioná-lo.

> **Note**
>
> Salvo indicação em contrário, se uma solicitação da Web não tiver o componente de solicitação especificado na declaração da regra, a solicitação será AWS WAF avaliada como não correspondendo aos critérios da regra.

Sumário

  - Corpo
  - Corpo JSON
- Endereço IP encaminhado
- Opções para inspecionar pseudo-cabeçalhos HTTP/2
- Opções de transformação de texto

Solicitar opções de componentes

Esta seção descreve os componentes da solicitação da web que você pode especificar para inspeção. Você especifica o componente de solicitação para instruções de regra de correspondência que procuram padrões dentro da solicitação da web. Esses tipos de instruções incluem correspondência de string, padrão regex, ataque de injeção de SQL e instruções de restrição de tamanho. Para obter informações sobre como usar essas configurações de componentes de solicitação, consulte as instruções de regras individuais em Instruções de regra de correspondência

Salvo indicação em contrário, se uma solicitação da Web não tiver o componente de solicitação especificado na declaração da regra, a solicitação será AWS WAF avaliada como não correspondendo aos critérios da regra.

> **Note**
>
> Especifique um único componente de solicitação para cada instrução de regra que o exija. Para inspecionar mais de um componente de uma solicitação, crie uma instrução de regra para cada componente.

A documentação do AWS WAF console e da API fornece orientação para as configurações do componente de solicitação nos seguintes locais:

- Construtor de regras no console:Nas configurações de Instrução de um tipo de regra comum, escolha o componente que você deseja inspecionar na caixa de diálogo Inspecionar em Solicitar componentes.
- Conteúdo da instrução da API: `FieldToMatch`

O restante desta seção descreve as opções da parte da solicitação da web a inspecionar.

Tópicos

- Método HTTP
- Cabeçalho único
- Todos os cabeçalhos
- Ordem de cabeçalho
- Cookies
- Caminho do URI
- Impressão digital JA3
- String de consulta
- Parâmetro de consulta única
- Todos os parâmetros da consulta
- Corpo
- Corpo JSON

Método HTTP

Inspectiona o método HTTP para a solicitação. O método HTTP indica o tipo de operação que a solicitação da Web está solicitando que seu recurso protegido realize, como `POST` ou `GET`.

Cabeçalho único

Inspeciona um único cabeçalho nomeado na solicitação.

Para essa opção, você especifica o nome do cabeçalho, por exemplo, `User-Agent` ou `Referer`. A correspondência de string para o nome não diferencia maiúsculas de minúsculas.

Todos os cabeçalhos

Inspeciona todos os cabeçalhos da solicitação, incluindo cookies. É possível aplicar um filtro para inspecionar um subconjunto de todos os cabeçalhos.

Para essa opção, você fornece as seguintes especificações:

- Padrões de correspondência — O filtro a ser usado para obter um subconjunto de cabeçalhos para inspeção. AWS WAF procura esses padrões nas teclas dos cabeçalhos.

  A configuração de padrões de correspondência pode ser uma das seguintes:

  - Tudo:Corresponder todas as teclas. Avalie os critérios de inspeção de regras para todos os cabeçalhos.

  - Cabeçalhos excluídos:Inspeciona apenas os cabeçalhos cujas chaves não correspondem a nenhuma das strings especificadas aqui. A correspondência de string para uma chave não diferencia maiúsculas de minúsculas.
  - Cabeçalhos incluídos:Inspeciona apenas os cabeçalhos que têm uma chave que corresponda a uma das strings especificadas aqui. A correspondência de string para uma chave não diferencia maiúsculas de minúsculas.
- Escopo correspondente — As partes dos cabeçalhos que AWS WAF devem ser inspecionadas de acordo com os critérios de inspeção da regra. Você pode especificar chaves, valores ou tudo para inspecionar as chaves e os valores em busca de uma correspondência.

  Tudo não exige que uma correspondência seja encontrada nas chaves e que uma correspondência seja encontrada nos valores. Isso requer que uma correspondência seja encontrada nas chaves, nos valores ou nos dois. Para exigir uma correspondência nas chaves e nos valores, use uma instrução lógica `AND` para combinar duas regras de correspondência, uma que inspeciona as chaves e outra que inspeciona os valores.
- Manipulação de tamanho grande — Como AWS WAF lidar com solicitações que têm dados de cabeçalho maiores do que os que AWS WAF podem ser inspecionados. AWS WAF pode inspecionar no máximo os primeiros 8 KB (8.192 bytes) dos cabeçalhos da solicitação e, no máximo, os primeiros 200 cabeçalhos. O conteúdo está disponível para inspeção AWS WAF até o primeiro limite atingido. Você pode optar por continuar a inspeção ou pular a inspeção e marcar a solicitação como compatível ou não com a regra. Para obter mais informações sobre como processar conteúdo de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

Ordem de cabeçalho

Inspecione uma string contendo a lista dos nomes dos cabeçalhos da solicitação, ordenados conforme aparecem na solicitação da web que AWS WAF recebe para inspeção. AWS WAF gera a string e, em seguida, a usa como campo para combinar o componente em sua inspeção. AWS WAF separa os nomes dos cabeçalhos na string com dois pontos e sem espaços adicionados, por exemplo. `host:user-agent:accept:authorization:referer`

Para essa opção, você fornece as seguintes especificações:

- Manipulação de tamanho grande — Como AWS WAF lidar com solicitações que têm dados de cabeçalho mais numerosos ou maiores do que os que AWS WAF podem ser inspecionados. AWS WAF pode inspecionar no máximo os primeiros 8 KB (8.192 bytes) dos cabeçalhos da solicitação

e, no máximo, os primeiros 200 cabeçalhos. O conteúdo está disponível para inspeção AWS WAF até o primeiro limite atingido. Você pode optar por continuar a inspeção dos cabeçalhos que estão disponíveis ou pular a inspeção e marcar a solicitação como compatível ou não com a regra. Para obter mais informações sobre como processar conteúdo de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

Cookies

Inspeciona todos os cookies de solicitação. É possível aplicar um filtro para inspecionar um subconjunto de todos os cookies.

Para essa opção, você fornece as seguintes especificações:

- Padrões de correspondência:O filtro a ser usado para obter um subconjunto de cookies para inspeção. O AWS WAF procura esses padrões nas chaves dos cookies.

  A configuração de padrões de correspondência pode ser uma das seguintes:

  - Tudo:Corresponder todas as teclas. Avalie os critérios de inspeção de regras para todos os cookies.
  - Cookies excluídos:Inspeciona apenas os cookies cujas chaves não correspondem a nenhuma das strings especificadas aqui. A correspondência de string para uma chave diferencia maiúsculas de minúsculas e deve ser exata.
  - Cookies incluídos:Inspeciona apenas os cookies que têm uma chave que corresponda a uma das strings especificadas aqui. A correspondência de string para uma chave diferencia maiúsculas de minúsculas e deve ser exata.
- Escopo da correspondência — As partes dos cookies que AWS WAF devem ser inspecionadas de acordo com os critérios de inspeção da regra. Você pode especificar chaves, valores ou tudo para chaves e valores.

  Tudo não exige que uma correspondência seja encontrada nas chaves e que uma correspondência seja encontrada nos valores. Isso requer que uma correspondência seja encontrada nas chaves, nos valores ou nos dois. Para exigir uma correspondência nas chaves e nos valores, use uma instrução lógica `AND` para combinar duas regras de correspondência, uma que inspeciona as chaves e outra que inspeciona os valores.
- Manipulação de tamanho grande — Como AWS WAF lidar com solicitações que têm dados de cookies maiores do que os que AWS WAF podem ser inspecionados. AWS WAF pode inspecionar no máximo os primeiros 8 KB (8.192 bytes) dos cookies de solicitação e no máximo os primeiros

200 cookies. O conteúdo está disponível para inspeção AWS WAF até o primeiro limite atingido. Você pode optar por continuar a inspeção ou pular a inspeção e marcar a solicitação como compatível ou não com a regra. Para obter mais informações sobre como processar conteúdo de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

Caminho do URI

Inspeciona a parte de um URL que identifica um recurso, como `/images/daily-ad.jpg`. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

Se você não usa uma transformação de texto com essa opção, AWS WAF não normaliza o URI e o inspeciona exatamente como o recebe do cliente na solicitação. Para obter mais informações sobre transformações de texto, consulte Opções de transformação de texto.

Impressão digital JA3

Inspeciona a impressão digital JA3 da solicitação.

> **Note**
>
> A inspeção de impressão digital JA3 está disponível somente para CloudFront distribuições da Amazon e Application Load Balancers.

A impressão digital JA3 é um hash de 32 caracteres derivado do Hello do cliente TLS de uma solicitação recebida. Essa impressão digital serve como um identificador exclusivo para a configuração TLS do cliente. AWS WAF calcula e registra essa impressão digital para cada solicitação que tenha informações suficientes do TLS Client Hello para o cálculo. Quase todas as solicitações da web incluem essas informações.

Como obter a impressão digital JA3 para um cliente

Você pode obter a impressão digital JA3 para as solicitações de um cliente nos logs de web ACL. Se AWS WAF for capaz de calcular a impressão digital, ela a inclui nos registros. Para obter informações sobre os campos de log, consulte Campos de log.

Requisitos de instrução de regras

Você pode inspecionar a impressão digital JA3 somente dentro de uma instrução de correspondência de string definida para corresponder exatamente à string fornecida. Forneça a string de impressão digital JA3 dos logs em sua especificação de instrução de correspondência de string, para corresponder a quaisquer solicitações futuras que tenham a mesma configuração de TLS. Para obter mais informações sobre instruções de regra de correspondência de string, consulte Instrução de regra de correspondência de string.

Você deve fornecer um comportamento de fallback para essa instrução de regra. O comportamento de fallback é o status de correspondência que você deseja atribuir AWS WAF à solicitação da web AWS WAF se não conseguir calcular a impressão digital JA3. Se você optar pela correspondência, AWS WAF trata a solicitação como correspondente à instrução da regra e aplica a ação da regra à solicitação. Se você optar por não corresponder, AWS WAF tratará a solicitação como não correspondente à declaração da regra.

Para usar essa opção de correspondência, você deve registrar seu tráfego de web ACL. Para obter mais informações, consulte Registrando AWS WAF tráfego de ACL da web.

String de consulta

Inspeciona parte de um URL exibida após um caractere `?`, se houver.

> **Note**
>
> Para condições de correspondência de cross-site scripting, recomendamos que você escolha Todos os parâmetros de consulta em vez de String de consulta. A escolha de Todos os parâmetros de consulta adiciona 10 WCUs ao custo base.

Parâmetro de consulta única

Inspeciona um único parâmetro de consulta que você definiu como parte da cadeia de caracteres de consulta. AWS WAF inspeciona o valor do parâmetro que você especifica.

Para essa opção, você também especifica um Argumento de consulta. Por exemplo, se o URL for `www.xyz.com?UserName=abc&SalesRegion=seattle`, você pode especificar `UserName` ou `SalesRegion` para o argumento da consulta. O tamanho máximo para o nome do argumento é de 30 caracteres. O nome não diferencia maiúsculas e minúsculas, portanto, se você especificar `UserName`, o AWS WAF combina a todas as variações de `UserName`, incluindo `username` e `UsERName`.

Se a string de consulta contiver mais de uma instância do argumento de consulta que você especificou, AWS WAF inspeciona todos os valores em busca de uma correspondência usando a OR lógica. Por exemplo, no URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle`, o AWS WAF avalia o nome que você especificou em `boston` e `seattle`. Se qualquer um for uma correspondência, a inspeção é uma correspondência.

Todos os parâmetros da consulta

Inspeciona todos os parâmetros de consulta na solicitação. Isso é semelhante à escolha do componente de parâmetro de consulta único, mas AWS WAF inspeciona os valores de todos os argumentos na string de consulta. Por exemplo, se o URL for `www.xyz.com?UserName=abc&SalesRegion=seattle`, o AWS WAF dispara uma correspondência se o valor `UserName` ou `SalesRegion` corresponder aos critérios de inspeção.

A escolha dessa opção adiciona 10 WCUs ao custo base.

Corpo

Inspeciona o corpo da solicitação, avaliado como texto simples. Você também pode avaliar o corpo como JSON usando o tipo de conteúdo JSON.

O corpo da solicitação é a parte da solicitação que segue imediatamente os cabeçalhos da solicitação. Contém quaisquer dados adicionais necessários para a solicitação da Web, por exemplo, dados de um formulário.

- No console, você seleciona isso na opção Corpo da Opção de solicitação, selecionando a opção Tipo de conteúdo Texto simples.
- Na API, na especificação da regra `FieldToMatch`, você especifica `Body` para inspecionar o corpo da solicitação como texto simples.

Para Application Load Balancer e AWS AppSync, AWS WAF pode inspecionar os primeiros 8 KB do corpo de uma solicitação. Pois CloudFront, o API Gateway, o Amazon Cognito, o App Runner e o Verified Access, por padrão, AWS WAF podem inspecionar os primeiros 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Para ter mais informações, consulte Gerenciando os limites de tamanho da inspeção corporal.

Você deve especificar o tratamento de tamanho grande para esse tipo de componente. O tratamento de tamanho grande define como AWS WAF lida com solicitações que têm dados corporais maiores

do que os que AWS WAF podem ser inspecionados. Você pode optar por continuar a inspeção ou pular a inspeção e marcar a solicitação como compatível ou não com a regra. Para obter mais informações sobre como processar conteúdo de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

Você também pode avaliar o corpo como JSON analisado. Para obter mais informações, consulte a seção abaixo.

Corpo JSON

Inspeciona o corpo da solicitação, avaliado como JSON. Você também pode avaliar o corpo como texto simples.

O corpo da solicitação é a parte da solicitação que segue imediatamente os cabeçalhos da solicitação. Contém quaisquer dados adicionais necessários para a solicitação da Web, por exemplo, dados de um formulário.

- No console, você seleciona isso na opção Corpo da Opção de solicitação, selecionando a opção Tipo de conteúdo JSON.
- Na API, na especificação da regra `FieldToMatch`, você especifica `JsonBody`.

Para Application Load Balancer e AWS AppSync, AWS WAF pode inspecionar os primeiros 8 KB do corpo de uma solicitação. Pois CloudFront, o API Gateway, o Amazon Cognito, o App Runner e o Verified Access, por padrão, AWS WAF podem inspecionar os primeiros 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Para ter mais informações, consulte Gerenciando os limites de tamanho da inspeção corporal.

Você deve especificar o tratamento de tamanho grande para esse tipo de componente. O tratamento de tamanho grande define como AWS WAF lida com solicitações que têm dados corporais maiores do que os que AWS WAF podem ser inspecionados. Você pode optar por continuar a inspeção ou pular a inspeção e marcar a solicitação como compatível ou não com a regra. Para obter mais informações sobre como processar conteúdo de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

A escolha dessa opção dobra as WCUs de custo base da instrução de correspondência. Por exemplo, se o custo base da instrução de correspondência for 5 WCUs sem análise JSON, usar a análise JSON dobra o custo para 10 WCUs.

Etapas e opções para inspeção corporal JSON

Ao AWS WAF inspecionar o corpo da solicitação da web como JSON, ele executa etapas para analisar o corpo e extrair os elementos JSON para inspeção. A seguir estão listadas as etapas e suas opções adicionais de configuração para esse tipo de componente de solicitação.

1. Analisar o conteúdo do corpo — AWS WAF analisa o conteúdo do corpo da solicitação da web para extrair os elementos JSON para inspeção. AWS WAF faz o possível para analisar todo o conteúdo do corpo, mas a análise pode falhar em vários estados de erro no conteúdo. Os exemplos incluem caracteres inválidos, chaves duplicadas, truncamento e conteúdo cujo nó raiz não é um objeto ou uma matriz.

   A opção Body parsing fallback behavior determina o que AWS WAF acontece se ela falhar na análise completa do corpo JSON:

   - Nenhum (comportamento padrão) - AWS WAF avalia o conteúdo somente até o ponto em que ele encontrou um erro de análise.
   - Avaliar como string - inspecione o corpo como texto simples. AWS WAF aplica as transformações de texto e os critérios de inspeção que você definiu para a inspeção JSON à string do corpo do texto.
   - Corresponder - Trate a solicitação da web como correspondente à declaração da regra. AWS WAF aplica a ação da regra à solicitação.
   - Sem correspondência: tratar a solicitação da Web como não correspondente à instrução de regra.

   > **Note**
   >
   > Esse comportamento alternativo só é acionado quando AWS WAF encontra um erro ao analisar a string JSON.

   A análise não valida totalmente o JSON

   AWS WAF a análise não valida totalmente a string JSON de entrada, portanto, a análise pode ser bem-sucedida mesmo para JSON inválido.

   Por exemplo, AWS WAF analisa o seguinte JSON inválido sem erros:

   - Vírgula ausente: `{"key1":"value1""key2":"value2"}`
   - Dois pontos ausentes: `{"key1":"value1","key2""value2"}`
   - Dois pontos extras: `{"key1"::"value1","key2""value2"}`

Para casos como esses em que a análise é bem-sucedida, mas o resultado não é um JSON totalmente válido, o resultado das etapas subsequentes da avaliação pode variar. A extração pode perder alguns elementos ou a avaliação da regra pode ter resultados inesperados. Recomendamos que você valide o JSON recebido em seu aplicativo e trate o JSON inválido conforme necessário.

2. Extraia os elementos JSON — AWS WAF identifica o subconjunto de elementos JSON a serem inspecionados de acordo com suas configurações:

   - A opção JSON match scope especifica os tipos de elementos no JSON que AWS WAF devem ser inspecionados.

     Você pode especificar chaves, valores ou tudo para chaves e valores.

     Tudo não exige que uma correspondência seja encontrada nas chaves e que uma correspondência seja encontrada nos valores. Isso requer que uma correspondência seja encontrada nas chaves, nos valores ou nos dois. Para exigir uma correspondência nas chaves e nos valores, use uma instrução lógica `AND` para combinar duas regras de correspondência, uma que inspeciona as chaves e outra que inspeciona os valores.

   - A opção Conteúdo a ser inspecionado especifica como filtrar o conjunto de elementos para o subconjunto que você deseja AWS WAF inspecionar.

     É necessário especificar um dos seguintes:

     - Conteúdo JSON completo - Avalie todos os elementos.
     - Somente elementos incluídos - Avalie somente os elementos cujos caminhos correspondam aos critérios do JSON Pointer fornecidos por você. Não use essa opção para indicar todos os caminhos no JSON. Em vez disso, use conteúdo JSON completo.

       Para obter informações sobre a sintaxe do JSON Pointer, consulte a documentação do Internet Engineering Task Force (IETF) JavaScript Object Notation (JSON) Pointer.

       Por exemplo, é possível fornecer o seguinte no console:

       ```
       /dogs/0/name
       /dogs/1/name
       ```

       Na API ou na CLI, você pode fornecer o seguinte:

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

Por exemplo, digamos que a configuração Conteúdo a ser inspecionado seja Somente elementos incluídos e a configuração de elementos incluídos seja`/a/b`.

Para o exemplo de corpo JSON a seguir:

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

Os conjuntos de elementos que AWS WAF inspecionariam cada configuração do escopo de correspondência JSON estão listados abaixo. Observe que a chaveb, que faz parte do caminho dos elementos incluídos, não é avaliada.

- Todos:`e`, `f`, `g` e.
- Chaves: `e` `f` e.
- Valores:`g`.

3. Inspecione o conjunto de elementos JSON — AWS WAF aplica todas as transformações de texto que você especificou aos elementos JSON extraídos e, em seguida, compara o conjunto de elementos resultante com os critérios de correspondência da declaração de regra. Esse é o mesmo comportamento de transformação e avaliação de outros componentes de solicitação da web. Se algum dos elementos JSON extraídos corresponder, a solicitação da web corresponderá à regra.

Endereço IP encaminhado

Esta seção se aplica às instruções de regras que usam o endereço IP de uma solicitação da web. Por padrão, AWS WAF usa o endereço IP da origem da solicitação da web. No entanto, se uma solicitação da web passar por um ou mais proxies ou balanceadores de carga, a origem da solicitação da web conterá o endereço do último proxy, e não o endereço de origem do cliente.

Nesse caso, o endereço do cliente de origem geralmente é encaminhado em outro cabeçalho HTTP. Esse cabeçalho normalmente é `X-Forwarded-For` (XFF), mas pode ser diferente.

Instruções de regra que usam endereços IP

As instruções de regra que usam endereços IP são as seguintes:

- Correspondência de conjunto de IPs: Inspeciona o endereço IP em busca de uma correspondência com os endereços definidos em um conjunto de IPs.
- Correspondência geográfica: Usa o endereço IP para determinar o país e a região de origem e corresponde o país de origem com uma lista de países.
- Instrução de regra baseada em intervalos: Pode agregar solicitações por seus endereços IP para garantir que nenhum endereço IP individual envie solicitações em intervalos muito altos. Você pode usar a agregação de endereços IP sozinha ou em combinação com outras chaves de agregação.

Você pode AWS WAF instruir o uso de um endereço IP encaminhado para qualquer uma dessas declarações de regra, seja do `X-Forwarded-For` cabeçalho ou de outro cabeçalho HTTP, em vez de usar a origem da solicitação da web. Para obter detalhes sobre como fornecer as especificações, consulte a orientação para os tipos individuais de instrução de regra.

> **Note**
>
> Se o cabeçalho que você especificar não estiver presente na solicitação, a regra AWS WAF não será aplicada à solicitação da Web.

Comportamento de fallback

Ao usar o endereço IP encaminhado, você indica o status de correspondência AWS WAF a ser atribuído à solicitação da web se a solicitação não tiver um endereço IP válido na posição especificada:

- MATCH - Trate a solicitação da web como correspondente à declaração da regra. AWS WAF aplica a ação da regra à solicitação.
- Sem correspondência: tratar a solicitação da Web como não correspondente à instrução de regra.

Endereços IP usados no AWS WAF Bot Control

O grupo de regras gerenciadas do Bot Control verifica os bots usando os endereços IP de AWS WAF. Se você usa o Controle de Bots e verificou que os bots são roteados por meio de um proxy ou balanceador de carga, é necessário permitir explicitamente que eles usem uma regra personalizada. Por exemplo, você pode configurar uma regra personalizada de correspondência de conjuntos de IP que usa endereços IP encaminhados para detectar e permitir que seus bots sejam verificados. Você pode usar a regra para personalizar seu gerenciamento de bots de várias maneiras. Para obter informações e exemplos, consulte AWS WAF Controle de bots.

Considerações gerais sobre o uso de endereços IP encaminhados

Antes de usar um endereço IP encaminhado, observe as seguintes advertências gerais:

- Um cabeçalho pode ser modificado por proxies ao longo do caminho, e os proxies podem tratar o cabeçalho de maneiras diferentes.
- Os invasores podem alterar o conteúdo do cabeçalho na tentativa de contornar as inspeções do AWS WAF .
- O endereço IP dentro do cabeçalho pode estar incorreto ou ser inválido.
- O cabeçalho que você especifica pode não estar presente em uma solicitação.

Considerações sobre o uso de endereços IP encaminhados com AWS WAF

A lista a seguir descreve os requisitos e as advertências para o uso de endereços IP encaminhados em: AWS WAF

- Para qualquer regra única, você pode especificar um cabeçalho para o endereço IP encaminhado. A especificação do cabeçalho não diferencia maiúsculas de minúsculas.
- Para instruções de regras baseadas em intervalos, nenhuma instrução de escopo aninhada herda a configuração de IP encaminhada. Especifique a configuração para cada instrução que usa um endereço IP encaminhado.
- Para regras de correspondência geográfica e baseadas em taxas, AWS WAF usa o primeiro endereço no cabeçalho. Por exemplo, se um cabeçalho contiver `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF usos `10.1.1.1`
- Para correspondência de conjunto de IP, você indica se deseja corresponder ao primeiro, ao último ou a qualquer endereço no cabeçalho. Se você especificar algum, AWS WAF inspeciona todos os endereços no cabeçalho em busca de uma correspondência, até 10 endereços. Se o cabeçalho contiver mais de 10 endereços, AWS WAF inspeciona os últimos 10.

- Os cabeçalhos que contêm vários endereços devem usar um separador de vírgula entre os endereços. Se uma solicitação usar um separador diferente de uma vírgula, o AWS WAF considerará os endereços IP no cabeçalho incorretos.
- Se os endereços IP dentro do cabeçalho estiverem incorretos ou forem inválidos, o AWS WAF designa a solicitação da web como compatível ou não com a regra, de acordo com o comportamento de fallback especificado na configuração de IP encaminhado.
- Se o cabeçalho que você especificar não estiver presente em uma solicitação, AWS WAF a regra não será aplicada à solicitação. Isso significa que AWS WAF não aplica a ação da regra e não aplica o comportamento alternativo.
- Uma instrução de regra que usa um cabeçalho IP encaminhado para o endereço IP não usará o endereço IP informado pela origem da solicitação da web.

Práticas recomendadas para usar endereços IP encaminhados com AWS WAF

Ao usar endereços IP encaminhados, siga as seguintes práticas recomendadas:

- Considere cuidadosamente todos os estados possíveis dos cabeçalhos de sua solicitação antes de ativar a configuração de IP encaminhado. Talvez seja necessário usar mais de uma regra para obter o comportamento desejado.
- Para inspecionar vários cabeçalhos de IP encaminhados ou inspecionar a origem da solicitação da web e um cabeçalho de IP encaminhado, use uma regra para cada fonte de endereço IP.
- Para bloquear solicitações da web que tenham um cabeçalho inválido, defina a ação de regra para bloquear e defina o comportamento de fallback para que a configuração de IP encaminhado corresponda.

Exemplo de JSON para endereços IP encaminhados

A seguinte instrução de correspondência geográfica corresponde somente se o cabeçalho `X-Forwarded-For` contiver um IP cujo país de origem seja `US`:

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

A seguinte regra baseada em intervalos agrega solicitações com base no primeiro IP no cabeçalho `X-Forwarded-For`. A regra conta somente as solicitações que correspondem à instrução de correspondência geográfica aninhada e bloqueia somente as solicitações que correspondem à instrução de correspondência geográfica. A instrução de correspondência geográfica aninhada também usa o cabeçalho `X-Forwarded-For` para determinar se o endereço IP indica um país de origem de US. Em caso afirmativo, ou se o cabeçalho estiver presente, mas malformado, a instrução de correspondência geográfica retornará uma correspondência.

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
```

```
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

Opções para inspecionar pseudo-cabeçalhos HTTP/2

AWS Os recursos protegidos que oferecem suporte ao tráfego HTTP/2 não encaminham pseudoceçalhos HTTP/2 AWS WAF para inspeção, mas fornecem conteúdo de pseudo-cabeçalhos em componentes de solicitação da web que inspecionam. AWS WAF

Você pode usar AWS WAF para inspecionar somente os pseudo-cabeçalhos listados na tabela a seguir.

Conteúdo do pseudocabeçalho HTTP/2 mapeado para componentes de solicitação da web

Pseudocabeçalho HTTP/2	Componente de solicitação da web para inspecionar	Documentação
`:method`	Método HTTP	Método HTTP
`:authority`	`Host`Cabeçalho	Cabeçalho único Todos os cabeçalhos
Caminho do URI `:path`	Caminho do URI	Caminho do URI
	String de consulta	String de consulta

Pseudocabeçalho HTTP/2	Componente de solicitação da web para inspecionar	Documentação
`:path` query		Parâmetro de consulta única Todos os parâmetros da consulta

Opções de transformação de texto

Nas instruções que buscam padrões ou definem restrições, você pode fornecer transformações para serem aplicadas antes de inspecionar AWS WAF a solicitação. A transformação reformata uma solicitação da Web para eliminar algumas das formatações incomuns que os invasores usam em uma tentativa de contornar o AWS WAF.

Quando você usa isso com a seleção do componente de solicitação de corpo JSON, o AWS WAF aplica suas transformações após analisar e extrair os elementos a serem inspecionados do JSON. Para ter mais informações, consulte Corpo JSON.

Se você fornecer mais de uma transformação, também definirá a ordem em que o AWS WAF deve aplicá-las.

WCUs:Cada transformação de texto é de 10 WCUs.

A documentação do AWS WAF console e da API também fornece orientação para essas configurações nos seguintes locais:

- Criador de regras no console:Transformação de texto. Essa opção está disponível quando você usa componentes de solicitação.
- Conteúdo da instrução da API: `TextTransformations`

Opções para transformações de texto

Cada lista de transformação mostra as especificações do console e da API seguidas pela descrição.

Base64 decode – `BASE64_DECODE`

AWS WAF decodifica uma string codificada em Base64.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF decodifica uma string codificada em Base64, mas usa uma implementação indulgente que ignora caracteres que não são válidos.

Command line – `CMD_LINE`

Essa opção atenua situações em que os invasores podem estar injetando um comando de linha de comando do sistema operacional e usando uma formatação incomum para disfarçar parte ou a totalidade do comando.

Use essa opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: `\ " ' ^`
- Excluir espaços antes os seguintes caracteres: `/ (`
- Substituir os seguintes caracteres por um espaço: `, ;`
- Substituir vários espaços por um espaço
- Converter as letras maiúsculas, `A-Z`, em minúsculas, `a-z`

Compress whitespace – `COMPRESS_WHITE_SPACE`

AWS WAF comprime o espaço em branco substituindo vários espaços por um espaço e substituindo os seguintes caracteres por um caractere de espaço (ASCII 32):

- Quebra de página (ASCII 12)
- Tabulação (ASCII 9)
- Nova linha (ASCII 10)
- Retorno de carro (ASCII 13)
- Tabulação vertical (ASCII 11)
- Espaço rígido (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF decodifica caracteres que foram codificados usando regras de escape CSS 2.x. `syndata.html#characters` Essa função utiliza até dois bytes no processo de decodificação e, portanto, pode ajudar a descobrir caracteres ASCII codificados com CSS que normalmente não seriam codificados. Ela também é útil para combater a evasão, que é uma combinação de barra invertida e caracteres não hexadecimais. Por exemplo, `ja\vascript` para `javascript`.

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF decodifica as seguintes sequências de escape ANSI C:`\a`,,`\b`,`\f`,,`\n`,`\r`,`\t`, `\v` `\\?`, `\xHH` (hexadecimal) `\'\"`, (octal). `\0000` As codificações que não são válidas permanecem na saída.

Hex decode – `HEX_DECODE`

AWS WAF decodifica uma sequência de caracteres hexadecimais em um binário.

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF substitui os caracteres representados em formato hexadecimal `&#xhhhh;` ou decimal pelos caracteres correspondentes. `&#nnnn;`

AWS WAF substitui os seguintes caracteres codificados em HTML por caracteres não codificados. Essa lista usa codificação HTML em minúsculas, mas o tratamento não diferencia maiúsculas de minúsculas, por exemplo, `&QuOt;` e `"` é tratado da mesma forma.

Caractere codificado em HTML	substituído por…
`"`	`"`
`&`	`&`
`<`	`<`
`>`	`>`
` ` ou ` `	espaço incondicional, decimal 160
`
`	`\n`, decimal 10
` `	`\t`, decimal 9
`{` ou `{`	`{`
`|`, `|` ou `|`	`|`
`}` ou `}`	`}`
`!`	`!`

Caractere codificado em HTML	substituído por…
#	#
$	$
&percent; ou %	%
'	\
(	(
)	)
* ou *	*
+	+
,	,
.	.
/	/
:	:
;	;
=	=
?	?
˜ ou ˜	~
−	-
[ou [	[
\	\\
] ou]	]

Caractere codificado em HTML	substituído por…
`&hat;`	^
`_` ou `&underbar;`	_
`` ou ```	`

JS decode – `JS_DECODE`

AWS WAF decodifica sequências de JavaScript escape. Se um código `\uHHHH` estiver no intervalo de código ASCII de largura total de `FF01-FF5E`, o byte maior será utilizado para detectar e ajustar o byte menor. Caso contrário, somente o byte menor será utilizado, e o byte maior será zerado, causando uma possível perda de informações.

Lowercase – `LOWERCASE`

AWS WAF converte letras maiúsculas (A-Z) em minúsculas (a-z).

MD5 – `MD5`

AWS WAF calcula um hash MD5 a partir dos dados na entrada. O hash calculado está em um formato binário bruto.

None – `NONE`

AWS WAF inspeciona a solicitação da web conforme recebida, sem nenhuma transformação de texto.

Normalize path – `NORMALIZE_PATH`

AWS WAF normaliza a string de entrada removendo várias barras, autorreferências de diretório e referências anteriores de diretório que não estão no início da entrada.

Normalize path Windows – `NORMALIZE_PATH_WIN`

AWS WAF converte caracteres de barra invertida em barras progressivas e, em seguida, processa a string resultante usando a transformação. `NORMALIZE_PATH`

Remove nulls – `REMOVE_NULLS`

AWS WAF remove todos os `NULL` bytes da entrada.

Replace comments – `REPLACE_COMMENTS`

AWS WAF substitui cada ocorrência de um comentário no estilo C (/*... */) por um único espaço. Ele não comprime várias ocorrências consecutivas. Substitui comentários sem término por um espaço (ASCII 0x20). Isso não altera o encerramento independente de um comentário (*/).

Replace nulls – `REPLACE_NULLS`

AWS WAF substitui cada `NULL` byte na entrada pelo caractere de espaço (ASCII 0x20).

SQL hex decode – `SQL_HEX_DECODE`

AWS WAF decodifica dados hexadecimais SQL. Por exemplo, AWS WAF decodifica (`0x414243`) para (`ABC`).

URL decode – `URL_DECODE`

AWS WAF decodifica um valor codificado em URL.

URL decode Unicode – `URL_DECODE_UNI`

Como `URL_DECODE`, mas com suporte para codificação `%u` específica da Microsoft. Se o código estiver no intervalo de código ASCII de largura total de `FF01-FF5E`, o byte maior será utilizado para detectar e ajustar o byte menor. Caso contrário, somente o byte menor será utilizado, e o byte maior será zerado.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF converte todas as sequências de caracteres UTF-8 em Unicode. Isso ajuda a normalizar a entrada e minimiza falsos positivos e falsos negativos em idiomas que não sejam o inglês.

Instruções de redução de escopo

Uma instrução de redução de escopo é uma instrução de regra aninhável que você adiciona dentro de uma instrução de grupo de regras gerenciadas ou em uma instrução baseada em intervalo para restringir o conjunto de solicitações que a regra que a contém avalia. A regra de contenção avalia apenas as solicitações que correspondem primeiro à instrução de redução de escopo.

- Declaração de grupo de regras gerenciadas — Se você adicionar uma instrução de escopo reduzido a uma instrução de grupo de regras gerenciadas, AWS WAF avaliará qualquer solicitação que não corresponda à instrução de escopo inferior como não correspondente ao grupo de regras. As solicitações apenas serão avaliadas pelo grupo de regras se corresponderem à instrução de

redução de escopo. Para grupos de regras gerenciadas com preços baseados no número de solicitações avaliadas, as instruções de redução de escopo podem ajudar a conter os custos.

Para obter mais informações sobre instruções de grupos de regras gerenciadas, consulte Declaração do grupo de regras gerenciadas.

- Instrução de regra baseada em intervalos:Uma instrução de regra baseada em intervalos sem uma instrução de redução de escopo limita todas as solicitações que a regra avalia. Se você quiser controlar somente o intervalo de uma categoria específica de solicitações, adicione uma instrução de redução de escopo à regra baseada em intervalos. Por exemplo, para acompanhar e controlar somente a taxa de solicitações de uma área geográfica específica, você pode especificar essa área geográfica em uma instrução de correspondência geográfica e adicioná-la à sua regra baseada em intervalos como a instrução de redução de escopo.

  Para obter mais informações sobre regras baseadas em intervalos, consulte Instrução de regra baseada em intervalos.

É possível usar qualquer regra aninhável em uma instrução de redução de escopo. Para ver as instruções disponíveis, consulte Instruções de regra de correspondência e Instruções de regras lógicas. As WCUs para uma instrução de redução de escopo são as WCUs necessárias para a instrução de regra que você define nela. Não há custos adicionais pelo uso de uma instrução de redução de escopo.

Você pode configurar uma instrução de redução de escopo da mesma forma que você faz quando usa a instrução em uma regra regular. Por exemplo, você pode aplicar transformações de texto a um componente de solicitação da web que está inspecionando e especificar um endereço IP encaminhado para usar como endereço IP. Essas configurações se aplicam somente à instrução de redução de escopo não são herdadas pelo grupo de regras gerenciadas que o contém ou pela instrução de regra baseada em intervalos.

Por exemplo, se você aplicar transformações de texto a uma string de consulta em sua instrução de redução de escopo, a instrução de redução de escopo inspeciona a string de consulta depois de aplicar as transformações. Se a solicitação corresponder aos critérios da instrução de redução de escopo, o AWS WAF passará a solicitação da web para a regra que a contém em seu estado original, sem as transformações da instrução de redução de escopo. A regra que contém a instrução de redução de escopo pode aplicar suas próprias transformações de texto, mas não herda nenhuma da instrução de redução de escopo.

Você não pode usar uma instrução de redução de escopo para especificar qualquer configuração de inspeção de solicitação para a instrução de regra que a contém. Você não pode usar uma instrução de redução de escopo como pré-processador de solicitações da web para a instrução de regra que a contém. A única função de uma instrução de redução de escopo é determinar quais solicitações são passadas para a instrução de regra que a contém para inspeção.

Instruções que fazem referência a um conjunto ou a um grupo de regras

Algumas regras usam entidades que são reutilizáveis e gerenciadas fora de suas ACLs da web, seja por você ou por um AWS vendedor. AWS Marketplace Quando a entidade reutilizável é atualizada, o AWS WAF propaga a atualização para sua regra. Por exemplo, se você usar um grupo de regras AWS gerenciadas em uma ACL da web, ao AWS atualizar o grupo de regras, AWS propagará a alteração para sua ACL da web para atualizar seu comportamento. Se você usar uma instrução de conjunto de IP em uma regra, ao atualizar o conjunto, a alteração será AWS WAF propagada para todas as regras que fazem referência a ela, portanto, todas as ACLs da web que usam essas regras são mantidas up-to-date com suas alterações.

A seguir estão as entidades reutilizáveis que você pode usar em uma instrução de regra.

- Conjuntos de IPs: Você cria e gerencia seus próprios conjuntos de IPs. No console, você pode acessá-los a partir do painel de navegação. Para obter informações sobre como gerenciar conjuntos de IPs, consulte Conjuntos de IP e conjuntos de padrões regex em AWS WAF.
- Conjuntos de correspondências regex:Você cria e gerencia seus próprios conjuntos de correspondências regex. No console, você pode acessá-los a partir do painel de navegação. Para obter informações sobre como gerenciar conjuntos de padrões de regex, consulte Conjuntos de IP e conjuntos de padrões regex em AWS WAF.
- AWS Grupos de regras gerenciadas — AWS gerencia esses grupos de regras. No console, eles estão disponíveis para seu uso quando você adiciona um grupo de regras gerenciadas à web ACL. Para obter mais informações sobre essas ferramentas, consulte AWS Lista de grupos de regras de regras gerenciadas.
- AWS Marketplace grupos de regras gerenciados — AWS Marketplace os vendedores gerenciam esses grupos de regras e você pode se inscrever neles para usá-los. Para gerenciar suas assinaturas, no painel de navegação do console, escolha AWS Marketplace. Os grupos de regras AWS Marketplace gerenciadas são listados quando você adiciona um grupo de regras gerenciadas à sua ACL da web. Para grupos de regras nos quais você ainda não se inscreveu, você também pode encontrar um link AWS Marketplace nessa página. Para obter mais

informações sobre grupos de regras gerenciados pelo AWS Marketplace vendedor, consulteAWS Marketplace grupos de regras gerenciados.

- Seus próprios grupos de regras:Você gerencia seus próprios grupos de regras, geralmente quando você precisa de algum comportamento que não esteja disponível por meio dos grupos de regras gerenciados. No console, você pode acessá-los a partir do painel de navegação. Para ter mais informações, consulte Gerenciar seus próprios grupos de regras.

Como excluir um conjunto referenciado ou grupo de regras

Quando você exclui uma entidade referenciada, AWS WAF verifica se ela está sendo usada atualmente em uma ACL da web. Se AWS WAF descobrir que está em uso, ele avisa você. AWS WAF quase sempre é capaz de determinar se uma entidade está sendo referenciada por uma ACL da web. No entanto, em casos raros, pode não ser possível fazer isso. Se você precisa r certeza de que a entidade que você deseja excluir não está em uso, verifique se ela está em suas web ACLsantes de excluí-la.

Instruções de regra de correspondência

As instruções de regra de correspondência comparam a solicitação da Web ou sua origem com as condições fornecidas por você. Para muitas declarações desse tipo, AWS WAF compara um componente específico da solicitação de conteúdo correspondente.

As instruções de correspondência são aninháveis. Você pode aninhar qualquer uma dessas instruções em instruções de regras lógicas e usá-las em instruções de redução de escopo. Para obter mais informações sobre instruções de regras lógicas, consulte Instruções de regras lógicas. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo.

Esta tabela descreve as instruções de correspondência regular que você pode adicionar a uma regra e fornece algumas diretrizes para calcular o uso de unidades de capacidade de web ACL (WCU) para cada uma delas. Para obter informações sobre WCUs, consulte AWS WAF unidades de capacidade web ACL (WCUs).

Instrução de correspondência	Descrição	WCUs
Correspondência geográfica	Inspeciona o país de origem da solicitação e aplica rótulos	1

Instrução de correspondência	Descrição	WCUs
	para o país e a região de origem.	
Correspondência de conjunto de IPs	Inspeciona a solicitação em comparação com um conjunto de endereços IP e intervalos de endereços.	1 para a maioria dos casos. Se você configurar a instrução para usar um cabeçalho com endereços IP encaminhados e especificar uma posição no cabeçalho de Any, aumente as WCUs em 4.
Instrução de regra de correspondência de rótulo	Inspeciona a solicitação de rótulos que foram adicionados por outras regras na mesma web ACL.	1
Instrução de regra de correspondência de regex	Compara um padrão regex com um componente de solicitação especificado.	3, como custo base. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.

Instrução de correspondência	Descrição	WCUs
Conjunto padrão Regex	Compara padrões regex com um componente de solicitação especificado.	25 por conjunto de padrões, como custo base. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.
Restrição de tamanho	Verifica restrições de tamanho em relação a um componente de solicitação especificado.	1, como custo base. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.

Instrução de correspondência	Descrição	WCUs
Ataque SQLi	Inspeciona o código SQL mal-intencionado em um componente de solicitação especificado.	20, como custo base. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.
Correspondência de strings	Compara uma string com um componente de solicitação especificado.	O custo base depende do tipo de correspondência de string e está entre 1 e 10. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.

Instrução de correspondência	Descrição	WCUs
Ataque de script XSS	Inspeciona ataques de script entre sites em um component e de solicitação especificado.	40, como custo base. Se você usar o component e de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transform ação de texto aplicada, adicione 10 WCUs.

Instrução de regra de correspondência geográfica

Use instruções de correspondência geográfica para gerenciar solicitações da web com base no país e na região de origem. Uma instrução de correspondência geográfica adiciona rótulos às solicitações da web que indicam o país de origem e a região de origem. Ela adiciona esses rótulos independentemente de os critérios da instrução corresponderem à solicitação. Uma instrução de correspondência geográfica também realiza a correspondência com o país de origem da solicitação.

Como usar a instrução de correspondência geográfica

Você pode usar a instrução de correspondência geográfica para correspondência de país ou região, da seguinte forma:

- País — Você pode usar uma regra de correspondência geográfica sozinha para gerenciar solicitações com base apenas no país de origem. A instrução de regra faz correspondência em relação aos códigos de país. Você também pode seguir uma regra de correspondência geográfica com uma regra de correspondência de rótulo que corresponda ao rótulo do país de origem.
- Região — Use uma regra de correspondência geográfica seguida por uma regra de correspondência de rótulo para gerenciar solicitações com base na região de origem. Você não pode usar uma regra de correspondência geográfica sozinha para fazer correspondência em relação aos códigos de região.

Para obter informações sobre o uso de regras de correspondência de rótulos, consulte Instrução de regra de correspondência de rótulo e AWS WAF rótulos em solicitações da web.

Como funciona a instrução de correspondência geográfica

Com a declaração de correspondência geográfica, AWS WAF gerencia cada solicitação da web da seguinte forma:

1. Determina os códigos de país e região da solicitação — AWS WAF determina o país e a região de uma solicitação com base em seu endereço IP. Por padrão, AWS WAF usa o endereço IP da origem da solicitação da web. Você pode AWS WAF instruir o uso de um endereço IP de um cabeçalho de solicitação alternativo, por exemplo`X-Forwarded-For`, habilitando a configuração de IP encaminhado nas configurações da declaração de regra.

   AWS WAF determina a localização das solicitações usando bancos de dados MaxMind GeoIP. MaxMind relata uma precisão muito alta de seus dados em nível de país, embora a precisão varie de acordo com fatores como país e tipo de IP. Para obter mais informações sobre MaxMind, consulte Geolocalização MaxMind IP. Se achar que algum dado do GeoIP está incorreto, você pode enviar uma solicitação de correção para a Maxmind em MaxMind Correct GeoIP2 Data.

   AWS WAF usa os códigos alfa-2 de país e região do padrão 3166 da Organização Internacional de Padronização (ISO). Você pode encontrar os códigos nos seguintes locais:

   - No site da ISO, você pode pesquisar os códigos dos países na Plataforma de navegação online da ISO (OBP).
   - Na Wikipedia, os códigos de país estão listados na ISO 3166-2.

     Os códigos de região de um país estão listados na URL `https://en.wikipedia.org/wiki/ISO_3166-2:`*`<ISO country code>`*. Por exemplo, as regiões dos Estados Unidos estão em ISO 3166-2:US e as da Ucrânia estão em ISO 3166-2:UA.
2. Determina o rótulo do país e o rótulo da região a serem adicionados à solicitação — Os rótulos indicam se a instrução de correspondência geográfica usa o IP de origem ou uma configuração de IP encaminhado.

   - IP de origem

     O rótulo do país é `awswaf:clientip:geo:country:`*`<ISO country code>`*. Por exemplo, `awswaf:clientip:geo:country:US` para os Estados Unidos.

O rótulo da região é `awswaf:clientip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*. Exemplo para Oregon nos Estados Unidos: `awswaf:clientip:geo:region:US-OR`.

- IP encaminhado

  O rótulo do país é `awswaf:forwardedip:geo:country:`*`<ISO country code>`*. Por exemplo, `awswaf:forwardedip:geo:country:US` para os Estados Unidos.

  O rótulo da região é `awswaf:forwardedip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*. Exemplo para Oregon nos Estados Unidos: `awswaf:forwardedip:geo:region:US-OR`.

Se o código do país ou região não estiver disponível para o endereço IP especificado de uma solicitação, o AWS WAF usa XX nos rótulos, no lugar do valor. Por exemplo, o rótulo a seguir é para um IP de cliente cujo código de país não está disponível: `awswaf:clientip:geo:country:XX`, e o seguinte é para um IP encaminhado cujo país são os Estados Unidos, mas cujo código de região não está disponível: `awswaf:forwardedip:geo:region:US-XX`.

3. Avalia o código do país da solicitação em relação aos critérios da regra

A instrução de correspondência geográfica adiciona rótulos de país e região a todas as solicitações que ela inspeciona, independentemente de encontrar uma correspondência.

> **Note**
>
> AWS WAF adiciona qualquer rótulo ao final da avaliação da solicitação web de uma regra. Por esse motivo, qualquer correspondência de rótulo usada com os rótulos de uma instrução de correspondência geográfica deve ser definida em uma regra separada da regra que contém a instrução de correspondência geográfica.

Se quiser inspecionar somente valores de região, você pode escrever uma regra de correspondência geográfica com ação Count e com uma única correspondência de código de país, seguida por uma regra de correspondência de rótulos para os rótulos de região. Você deve fornecer um código de país para que a regra de correspondência geográfica seja avaliada, mesmo para essa abordagem. Você pode reduzir o registro em log e as métricas especificando um país que provavelmente não será uma origem de tráfego para seu site.

CloudFront distribuições e o recurso de CloudFront restrição geográfica

Para CloudFront distribuições, se você usar CloudFront o recurso de restrição geográfica, saiba que o recurso não encaminha solicitações bloqueadas para o. AWS WAF Ele encaminha as solicitações permitidas para AWS WAF. Se você quiser bloquear solicitações com base na geografia e em outros critérios que você pode especificar AWS WAF, use a declaração de correspondência AWS WAF geográfica e não use o recurso de restrição CloudFront geográfica.

Características da instrução de correspondência geográfica

Aninhável: você pode aninhar esse tipo de instrução.

WCUs : 1 WCU.

Configurações: essa instrução usa as seguintes configurações:

- Códigos de país: uma matriz de códigos de país para comparar em uma correspondência geográfica. Estes devem ser códigos de país de dois caracteres, por exemplo, `["US","CN"]`, dos códigos ISO de países alfa-2 da norma internacional ISO 3166.
- (Opcional) Configuração de IP encaminhada — Por padrão, AWS WAF usa o endereço IP na origem da solicitação da web para determinar o país de origem. Como alternativa, você pode configurar a regra para usar um IP encaminhado em um cabeçalho HTTP, como `X-Forwarded-For` alternativa. AWS WAF usa o primeiro endereço IP no cabeçalho. Com essa configuração, você também especifica um comportamento de fallback a ser aplicado a uma solicitação da web com um endereço IP incorreto no cabeçalho. O comportamento de fallback define o resultado correspondente da solicitação como correspondente ou não correspondente. Para ter mais informações, consulte Endereço IP encaminhado.

Onde encontrar essa instrução de regra

- Criador de regras no console: para a opção Solicitação, escolha Origina de um país em.
- API — GeoMatchStatement

Exemplos

Você pode usar a instrução de correspondência geográfica para gerenciar solicitações de países ou regiões específicos. Por exemplo, se deseja bloquear determinados países, mas ainda permitir solicitações de um conjunto específico de endereços IP nesses países, você pode criar uma regra com a ação definida como Block e as seguintes instruções aninhadas, mostradas no pseudocódigo:

- Instrução AND
  - Instrução de correspondência geográfica que relaciona os países que você quer bloquear
  - Instrução NOT
    - Instrução de conjunto de IPs que especifica os endereços IP que você deseja permitir

Ou, se você quiser bloquear algumas regiões em determinados países, mas ainda permitir solicitações de outras regiões nesses países, você pode primeiro definir uma regra de correspondência geográfica com a ação definida como Count. Em seguida, defina uma regra de correspondência de rótulos que corresponda aos rótulos de correspondência geográfica adicionados e gerencie as solicitações conforme necessário.

O pseudocódigo a seguir descreve um exemplo dessa abordagem:

1. Instrução de correspondência geográfica listando os países com regiões que você deseja bloquear, mas com a ação definida como Contagem. Isso rotula todas as solicitações da web, independentemente do status da correspondência, e também fornece métricas de contagem para os países de interesse.
2. Instrução `AND` com ação de bloqueio
   - Instrução de correspondência de rótulos que especifica os rótulos dos países que você deseja bloquear
   - Instrução `NOT`
     - Instrução de correspondência de rótulos que especifica os rótulos das regiões nos países que você deseja permitir a passagem

A lista JSON a seguir mostra uma implementação das duas regras descritas no pseudocódigo anterior. Essas regras bloqueiam todo o tráfego dos Estados Unidos, exceto o tráfego de Oregon e Washington. A instrução de correspondência geográfica adiciona rótulos de país e região a todas as solicitações que ela inspeciona. A regra de correspondência de rótulos é executada após a regra de correspondência geográfica, para que possa corresponder aos rótulos de país e região que a regra de correspondência geográfica acabou de adicionar. A instrução de correspondência geográfica usa um endereço IP encaminhado, portanto, a correspondência de rótulos também especifica rótulos de IPs encaminhados.

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
```

```
    "Statement": {
      "GeoMatchStatement": {
        "CountryCodes": [
          "US"
        ],
        "ForwardedIPConfig": {
            "HeaderName": "X-Forwarded-For",
            "FallbackBehavior": "MATCH"
        }
      }
    },
    "Action": {
      "Count": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "geoMatchForLabels"
    }
},
{
    "Name": "blockUSButNotOROrWA",
    "Priority": 11,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:forwardedip:geo:country:US"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                 "OrStatement": {
                   "Statements": [
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-OR"
                        }
                     },
                     {
```

```
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-WA"
                        }
                      }
                    ]
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "blockUSButNotOROrWA"
      }
}
```

Como outro exemplo, você pode combinar a correspondência geográfica com regras baseadas em intervalos para priorizar recursos para usuários em um determinado país ou região. Você cria uma instrução com base em intervalos diferente para cada instrução de correspondência geográfica ou de correspondência de rótulo que você usa para diferenciar seus usuários. Defina um limite de intervalo mais alto para usuários no país ou região preferido e um limite de intervalo mais baixo para os outros usuários.

A lista JSON a seguir mostra uma regra de correspondência geográfica seguida por regras baseadas em intervalos que limitam o intervalo de tráfego dos Estados Unidos. As regras permitem que o tráfego do Oregon chegue a um intervalo mais alto do que o tráfego de qualquer outro lugar do país.

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
```

```
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
```

```
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

Instrução de regra de correspondência de conjunto de IPs

A instrução de correspondência de conjunto de IPs inspeciona o endereço IP de uma solicitação da Web em relação a um conjunto de endereços IP e intervalos de endereços. Use para permitir ou bloquear solicitações da Web com base nos endereços IP dos quais as solicitações são originadas. Por padrão, o AWS WAF usa o endereço IP da origem da solicitação da web, mas você pode configurar a regra para usar um cabeçalho HTTP, como `X-Forwarded-For`.

AWS WAF suporta todos os intervalos CIDR IPv4 e IPv6, exceto o. `/0` Para obter mais informações sobre a notação CIDR, consulte o artigo na Wikipédia sobre CIDR. Um conjunto de IPs pode conter até 10.000 endereços IP ou intervalos de endereços IP para verificar.

> **Note**
>
> Cada regra de correspondência de conjunto de IP faz referência a um conjunto de IP, que você cria e mantém independente de suas regras. Você pode usar um único conjunto de IP em várias regras e, ao atualizar o conjunto referenciado, atualiza AWS WAF automaticamente todas as regras que fazem referência a ele.
> Para obter informações sobre como criar e gerenciar um conjunto de IP, consulte Criar e gerenciar um conjunto de IP.

Ao adicionar ou atualizar as regras em seu grupo de regras ou web ACL, escolha a opção conjunto de IPs e selecione o nome do conjunto de IPs que deseja usar.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 1 WCU para a maioria. Se você configurar a instrução para usar endereços IP encaminhados e especificar uma posição de ANY, aumente o uso da WCU em 4.

Essa instrução usa as seguintes configurações:

- Especificação do conjunto de IP: Escolha o conjunto de IPs que você deseja usar na lista ou crie um novo.
- (Opcional) Configuração de IP encaminhado:Um nome de cabeçalho de IP encaminhado alternativo para usar no lugar da origem da solicitação. Você especifica se deseja corresponder ao primeiro, ao último ou a qualquer endereço no cabeçalho. Você também especifica um comportamento de fallback a ser aplicado a uma solicitação da web com um endereço IP incorreto no cabeçalho. O comportamento de fallback define o resultado correspondente da solicitação como correspondente ou não correspondente. Para ter mais informações, consulte Endereço IP encaminhado.

Onde encontrar essa instrução de regra

- Criador de regras no console: para a opção Solicitação, escolha Origina de um endereço IP em.

- Página Adicionar minhas próprias regras e grupos de regras no console: Escolha a opção de conjunto de IP.
- API — IP SetReferenceStatement

Instrução de regra de correspondência de rótulo

A instrução de correspondência de rótulos inspeciona os rótulos que estão na solicitação da web em relação a uma especificação de string. Os rótulos que estão disponíveis para uma regra para inspeção são aqueles que já foram adicionados à solicitação da web por outras regras na mesma avaliação da web ACL.

Os rótulos não persistem fora da avaliação da Web ACL, mas você pode acessar as métricas dos rótulos CloudWatch e ver resumos das informações dos rótulos de qualquer ACL da Web no console. AWS WAF Para ter mais informações, consulte Métricas e dimensões do rótulo e Monitoramento e ajuste. Você também pode ver rótulos nos logs. Para mais informações, consulte Campos de log.

> **Note**
>
> Uma instrução de correspondência de rótulo só pode ver rótulos de regras que foram avaliadas anteriormente na web ACL. Para obter informações sobre como AWS WAF avalia as regras e os grupos de regras em uma ACL da web, consulte. Ordem de processamento de regras e grupos de regras em uma web ACL

Para obter mais informações sobre como adicionar e corresponder rótulos, consulte AWS WAF rótulos em solicitações da web.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 1 WCU.

Essa instrução usa as seguintes configurações:

- Escopo da correspondência:Defina como Rótulo para corresponder ao nome do rótulo e, opcionalmente, aos namespaces e prefixo anteriores. Defina isso como Namespace para corresponder a algumas ou todas as especificações do namespace e, opcionalmente, ao prefixo anterior.
- Chave:A string com a qual você deseja corresponder. Se você especificar um escopo de correspondência de namespace, isso deve especificar somente os namespaces e, opcionalmente,

o prefixo, com dois pontos finais. Se você especificar um escopo de correspondência de rótulo, isso deverá incluir o nome do rótulo e, opcionalmente, poderá incluir namespaces e prefixos anteriores.

Para obter mais informações sobre essas configurações, consulte AWS WAF regras que correspondem aos rótulos e AWS WAF exemplos de correspondência de rótulos.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Opção de solicitação, escolha Tem rótulo.
- API — LabelMatchStatement

Instrução de regra de correspondência de regex

Uma instrução de correspondência regex instrui AWS WAF a correspondência de um componente de solicitação com uma única expressão regular (regex). Uma solicitação da web corresponderá à instrução se o componente de solicitação corresponder à regex especificada.

Esse tipo de instrução é uma boa alternativa a Instrução de regra de correspondência do conjunto de padrões de regex para situações em que você deseja combinar seus critérios de correspondência usando lógica matemática. Por exemplo, se você quiser que um componente de solicitação corresponda a alguns padrões de regex e não corresponda a outros, você pode combinar as instruções de correspondência de regex usando o Instrução de regra do AND e o Instrução de regra do NOT.

AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 3 WCUs, como custo base. Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

  > **Warning**
  >
  > Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

  Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.

- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Onde encontrar essa instrução de regra

- Criador de regras no console:Para Tipo de correspondência, escolha Corresponde à expressão regular.
- API — RegexMatchStatement

Instrução de regra de correspondência do conjunto de padrões de regex

A correspondência de conjunto de padrões regex inspeciona a parte da solicitação da web especificada para os padrões de expressão regular especificados dentro de um conjunto de padrões regex.

AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.

> **Note**
>
> Cada regra de correspondência de conjunto de padrões de regex faz referência a um conjunto de padrões de regex, que você cria e mantém independente de suas regras. Você pode usar um único padrão de regex definido em várias regras e, ao atualizar o conjunto referenciado, atualiza AWS WAF automaticamente todas as regras que fazem referência a ele.
> Para obter informações sobre como criar e gerenciar um conjunto de padrões de regex, consulte Criar e gerenciar um conjunto de padrões Regex.

Uma instrução regex pattern set match instrui AWS WAF a pesquisar qualquer um dos padrões no conjunto dentro do componente de solicitação que você escolher. Uma solicitação da Web corresponderá à instrução de regra de conjunto de padrões se o componente de solicitação corresponder a qualquer um dos padrões no conjunto.

Se você quiser combinar suas correspondências de padrões de regex usando lógica, por exemplo, para comparar com algumas expressões regulares e não com outras, considere usar Instrução de regra de correspondência de regex.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 25 WCUs, como custo base. Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

> **Warning**
>
> Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.

- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Esta instrução requer as seguintes configurações:

- Especificação do conjunto de padrões de regex: Escolha o conjunto de padrões de regex que deseja usar na lista ou crie um novo.

Onde encontrar essa instrução de regra

- Criador de regras no console: Para Tipo de correspondência, escolha Condição de correspondência de string > Corresponde ao padrão do conjunto de expressões regulares.
- API — RegexPatternSetReferenceStatement

Instrução de regra de restrição de tamanho

Uma instrução de restrição de tamanho compara o número de bytes em um componente de solicitação da web com um número fornecido por você e corresponde de acordo com seus critérios de comparação. O critério de comparação é um operador, como maior que (>) ou menor que (<). Por exemplo, você pode fazer a correspondência em solicitações que tenham uma string de consulta com um tamanho maior que 100 bytes.

> **Note**
>
> Essa instrução inspeciona somente o tamanho do componente de solicitação da web. Ela não inspeciona o conteúdo do componente.

Se você inspecionar o caminho do URI, qualquer `/` no caminho conta como um caractere. Por exemplo, o caminho do URI `/logo.jpg` tem nove caracteres de comprimento.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 1 WCU, como custo base. Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo. Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.

  Uma instrução de restrição de tamanho inspeciona somente o tamanho do componente após a aplicação de qualquer transformação. Ela não inspeciona o conteúdo do componente.
- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecionar seu tamanho. Por exemplo, você pode compactar espaços em branco ou decodificar entidades HTML. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Além disso, essa instrução requer as seguintes configurações:

- Condição de correspondência de tamanho: indica o operador de comparação numérica a ser usado para comparar o tamanho fornecido com o componente de solicitação escolhido. Escolha o operador na lista.
- Tamanho: A configuração de tamanho, em bytes, a ser usada na comparação.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Tipo de correspondência, em Condição de correspondência de tamanho, escolha a condição que você deseja usar.
- API — SizeConstraintStatement

Instrução de regra de ataque de injeção de SQL

Uma instrução de regra de injeção de SQL que inspeciona códigos SQL mal-intencionados. Invasores às vezes inserem código SQL mal-intencionado em solicitações da Web na tentativa de realizar ações como modificar seu banco de dados ou extrair dados dele.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs:O custo base depende da configuração do nível de sensibilidade da instrução de regra: Low custa 20 e High custa 30.

Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

  > **Warning**
  >
  > Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

  Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.
- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Além disso, essa instrução requer as seguintes configurações:

- Nível de sensibilidade:Essa configuração ajusta a sensibilidade dos critérios de correspondência de injeção de SQL. As opções são LOW e HIGH. A configuração padrão é LOW.

  A configuração HIGH detecta mais ataques de injeção de SQL e é a configuração recomendada. Devido à maior sensibilidade, essa configuração gera mais falsos positivos, especialmente se as solicitações da web contiverem normalmente strings pouco comuns. Durante os testes e ajustes da web ACL, talvez você precise trabalhar mais para mitigar os falsos positivos. Para mais informações, consulte Testando e ajustando suas AWS WAF proteções.

  A configuração mais baixa fornece uma detecção de injeção de SQL menos rigorosa, o que também resulta em menos falsos positivos. LOW pode ser uma opção melhor para recursos com outras proteções contra ataques de injeção de SQL ou com baixa tolerância a falsos positivos.

Onde encontrar essa instrução de regra

- Construtor de regras no console: Para Tipo de correspondência, escolha Condições de correspondência de ataque > Contém ataques de injeção de SQL.
- API — SqliMatchStatement

Instrução de regra de correspondência de string

Uma declaração de correspondência de string indica AWS WAF a string que você deseja pesquisar em uma solicitação, onde e como pesquisar na solicitação. Por exemplo, você pode procurar uma string específica no início de qualquer string de consulta na solicitação ou como uma correspondência exata para o cabeçalho `User-agent` da solicitação. Geralmente, a string consiste em caracteres ASCII imprimíveis, mas você pode usar qualquer caractere, do hexadecimal 0x00 a 0xFF (decimal 0 a 255).

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: o custo base depende do tipo de correspondência que você usa.

- Corresponde exatamente à string: 2
- Começa com a string: 2
- Termina com a string: 2
- Contém a string: 10
- Contém a palavra: 10

Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

  > **Warning**
  >
  > Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

  Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.
- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Além disso, essa instrução requer as seguintes configurações:

- String to match — Essa é a string que você AWS WAF deseja comparar com o componente de solicitação especificado. Geralmente, a string consiste em caracteres ASCII imprimíveis, mas você pode usar qualquer caractere, do hexadecimal 0x00 a 0xFF (decimal 0 a 255).
- Condição de correspondência de string — Isso indica o tipo de pesquisa que você AWS WAF deseja realizar.
  - Corresponde exatamente à string: a string única e o valor do componente de solicitação são idênticos.
  - Começa com a strin: a string aparece no início do componente de solicitação.
  - Termina com a string: a string aparece no final do componente de solicitação.

- Contém string: a string aparece em qualquer lugar no componente de solicitação.
- Contém a palavra: a string especificada deve aparecer no componente de solicitação.

  Para esta opção, a string especificada deve conter apenas caracteres alfanuméricos ou sublinhado (A-Z, a-z, 0-9 ou _).

  Uma das seguintes opções deve ser verdadeira para que a solicitação corresponda:

  - A string corresponde exatamente ao valor do componente de solicitação, como o valor de um cabeçalho.
  - A string está no início do componente de solicitação e é seguida por um caractere diferente de um caractere alfanumérico ou sublinhado (_), por exemplo, `BadBot;`.
  - A string está no fim do componente de solicitação e é precedida por um caractere diferente de um caractere alfanumérico ou sublinhado (_), por exemplo, `;BadBot`.
  - A string está no meio do componente de solicitação e é precedida e seguida por caracteres diferentes de caracteres alfanuméricos ou sublinhados (_), por exemplo, `-BadBot;`.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Tipo de correspondência, escolha Condição de correspondência de string e preencha as strings com as quais você deseja corresponder.
- API — ByteMatchStatement

Instrução de regra de ataque de script entre sites

Uma instrução de ataque XSS (cross-site scripting) inspeciona scripts maliciosos em um componente de solicitação da web. Em ataques XSS, o invasor usa vulnerabilidades em um site benigno como veículo para injetar scripts mal-intencionados no lado do cliente em outros navegadores legítimos.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: 40 WCUs, como custo base. Se você usar o componente de solicitação Todos os parâmetros de consulta, adicione 10 WCUs. Se você usar o Corpo JSON do componente de solicitação, dobre as WCUs de custo base. Para cada Transformação de texto aplicada, adicione 10 WCUs.

Esse tipo de instrução opera em um componente de solicitação da web e requer as seguintes configurações do componente de solicitação:

- Componente de solicitação: a parte da solicitação da web para inspecionar, por exemplo, uma string de consulta ou o corpo.

  > **Warning**
  >
  > Se você inspecionar os componentes da solicitação Body, JSON body, Headers ou Cookies, leia sobre as limitações de quanto conteúdo AWS WAF pode ser inspecionado. Tratamento de componentes de solicitação de tamanho grande no AWS WAF

  Para informações sobre componentes de solicitação da web, consulte Especificação e tratamento de componentes de solicitações da Web.

- Transformações de texto opcionais — Transformações que você deseja AWS WAF realizar no componente de solicitação antes de inspecioná-lo. Por exemplo, você pode transformar para minúsculas ou normalizar o espaço em branco. Se você especificar mais de uma transformação, as AWS WAF processará na ordem listada. Para mais informações, consulte Opções de transformação de texto.

Onde encontrar essa instrução de regra

- Construtor de regras no console: para Tipo de correspondência, escolha Condições de correspondência de ataque > Contém ataques de injeção de XSS.
- API — XssMatchStatement

Instruções de regras lógicas

Usa instruções de regras lógicas para combinar outras instruções ou negar os resultados delas. Cada instrução de regra lógica leva pelo menos uma instrução aninhada.

Para combinar ou negar logicamente os resultados de instruções de regra, aninhe-as em instruções de regra lógicas.

As instruções de regras lógicas são aninháveis. Você pode aninhá-las em outras instruções de regras lógicas e usá-las em instruções de redução de escopo. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo.

> **Note**
>
> O editor visual no console suporta um nível de aninhamento de instrução de regra, que funciona para muitas necessidades. Para aninhar mais níveis, você pode editar a representação JSON da regra no console ou usar as APIs.

Esta tabela descreve as instruções de correspondência regular que você pode adicionar a uma regra e fornece algumas diretrizes para calcular o uso de unidades de capacidade de web ACL (WCU) para cada uma delas. Para obter informações sobre WCUs, consulte AWS WAF unidades de capacidade web ACL (WCUs).

Instrução lógica	Descrição	WCUs
Lógica do AND	Combina instruções aninhadas com a lógica AND.	Com base em instruções aninhadas
Lógica do NOT	Nega os resultados de uma instrução aninhada.	Com base na instrução aninhada
Lógica do OR	Combina instruções aninhadas com a lógica OR.	Com base em instruções aninhadas

Instrução de regra do AND

A instrução de regra AND combina instruções aninhadas com uma operação AND lógica, portanto, todas as instruções aninhadas devem corresponder à instrução AND para corresponder. Isso requer pelo menos duas declarações aninhadas.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: depende das instruções aninhadas.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Se uma solicitação, escolha corresponder a todas as instruções (AND) e preencha as instruções aninhadas.
- API — AndStatement

Exemplos

A lista a seguir mostra o uso de AND e instruções de regras lógicas NOT para eliminar falsos positivos das correspondências de uma instrução de ataque de injeção de SQL. Neste exemplo, suponha que possamos escrever uma instrução de correspondência de byte único para corresponder às solicitações que estão resultando em falsos positivos.

A instrução AND corresponde às solicitações que não correspondem à instrução de correspondência de byte e que correspondem à instrução de ataque de injeção de SQL.

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
```

```
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "SQLiExcludeFalsePositives"
      }
    }
```

Usando o editor visual de regras do console, você pode aninhar uma instrução não lógica ou uma instrução NOT sob uma instrução OR ou AND. O aninhamento da instrução NOT é mostrado no exemplo anterior.

Usando o editor visual de regras do console, você pode agrupar a maioria das instruções aninháveis em uma instrução de regra lógica, como a mostrada no exemplo anterior. Você não pode usar o editor visual para aninhar instruções OR ou AND. Para configurar esse tipo de aninhamento, você precisa fornecer sua instrução de regra em JSON. Por exemplo, a lista de regras JSON a seguir inclui uma instrução OR aninhada dentro de uma instrução AND.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
```

```
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
```

```
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Instrução de regra do NOT

A instrução de regra NOT nega logicamente os resultados de uma única instrução aninhada, portanto, as instruções aninhadas não devem corresponder em relação à instrução NOT a corresponder e vice-versa. Isso requer uma instrução aninhada.

Por exemplo, se você deseja bloquear solicitações que não são originadas em um país específico, crie uma instrução NOT com ação definida para bloquear e aninhe uma instrução de correspondência geográfica que especifique o país.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: depende da instrução aninhada.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Se uma solicitação, escolha não corresponde à instrução (NOT) e, em seguida, preencha a instrução aninhada.
- API — NotStatement

Instrução de regra do OR

A instrução de regra OR combina instruções aninhadas com a lógica OR, portanto, uma das instruções aninhadas deve corresponder para que a instrução OR corresponda. Isso requer pelo menos duas declarações aninhadas.

Por exemplo, se você deseja bloquear solicitações que vêm de um país específico ou que contêm uma string de consulta específica, você pode criar uma instrução OR e aninhar nela uma instrução de correspondência geográfica para o país e uma instrução de correspondência de string para a string de consulta.

Se, em vez disso, você deseja bloquear solicitações que não vêm de um país específico ou que contêm uma string de consulta específica, você modificaria a instrução OR anterior para aninhar a instrução de correspondência geográfica um nível inferior, dentro de uma instrução NOT. Esse nível de aninhamento requer que você use a formatação JSON, pois o console suporta apenas um nível de aninhamento.

Aninhável: você pode aninhar esse tipo de instrução.

WCUs: depende das instruções aninhadas.

Onde encontrar essa instrução de regra

- Criador de regras no console: para Se uma solicitação, escolha corresponder a pelo menos uma das instruções (OR), e preencha as instruções aninhadas.
- API — OrStatement

Exemplos

A lista a seguir mostra o uso de OR para combinar duas outras instruções. A instrução OR é compatível se alguma das instruções aninhadas corresponder.

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
```

```
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

Usando o editor visual de regras do console, você pode agrupar a maioria das instruções aninháveis em uma instrução de regra lógica, mas não pode usar o editor visual para aninhar instruções OR ou AND. Para configurar esse tipo de aninhamento, você precisa fornecer sua instrução de regra em JSON. Por exemplo, a lista de regras JSON a seguir inclui uma instrução OR aninhada dentro de uma instrução AND.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
```

```
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Instrução de regra baseada em intervalos

Uma regra baseada em intervalos conta as solicitações recebidas e limita as solicitações quando elas chegam a um intervalo muito rápido. A regra agrega solicitações de acordo com seus critérios

e conta e limita os agrupamentos agregados, com base na janela de avaliação, no limite de solicitações e nas configurações de ação da regra.

> **Note**
>
> Você também pode limitar a taxa de solicitações da web usando o nível de proteção direcionado do grupo de regras de regras AWS gerenciadas do Bot Control. O uso desse grupo de regras gerenciadas gera taxas adicionais. Para ter mais informações, consulte Opções para limitação de intervalo em regras baseadas em intervalos e regras direcionadas do Controle de Bots.

AWS WAF rastreia e gerencia solicitações da web separadamente para cada instância de uma regra baseada em taxas que você usa. Por exemplo, se você fornecer as mesmas configurações de regra com base em taxa em duas ACLs da web, cada uma das duas instruções de regra representará uma instância separada da regra baseada em taxa e cada uma receberá seu próprio controle e gerenciamento por. AWS WAF Se você definir uma regra baseada em taxas dentro de um grupo de regras e depois usar esse grupo de regras em vários lugares, cada uso cria uma instância separada da regra baseada em taxas que recebe seu próprio controle e gerenciamento. AWS WAF

Não aninháve: você não pode aninhar esse tipo de instrução dentro de outras instruções. Você pode incluí-la diretamente em uma web ACL ou em um grupo de regras.

Instrução de escopo reduzido — Esse tipo de regra pode usar uma instrução de escopo reduzido para restringir o escopo das solicitações que a regra rastreia e os limites de taxa. A instrução scope-down pode ser opcional ou obrigatória, dependendo das outras configurações da regra. Os detalhes são abordados nesta seção. Para obter informações gerais sobre declarações de escopo, consulte. Instruções de redução de escopo

WCUs: 2, como custo base. Para cada chave de agregação personalizada que você especificar, adicione 30 WCUs. Se você usar uma instrução de redução de escopo na regra, calcule e adicione as WCUs para isso.

Onde encontrar essa instrução de regra

- Criador de regras em sua web ACL, no console:Em Regra, para Tipo, escolha regra baseada em intervalos.
- API — RateBasedStatement

Tópicos

Configurações de alto nível de regra baseada em intervalos

Uma declaração de regra baseada em taxa usa as seguintes configurações de alto nível:

- Janela de avaliação — A quantidade de tempo, em segundos, que AWS WAF deve ser incluída em suas contagens de solicitações, considerando a hora atual. Por exemplo, para uma configuração de 120, quando AWS WAF verifica a taxa, ela conta as solicitações dos 2 minutos imediatamente anteriores à hora atual. As configurações válidas são 60 (1 minuto), 120 (2 minutos), 300 (5 minutos) e 600 (10 minutos), e 300 (5 minutos) é o padrão.

  Essa configuração não determina a frequência com que a taxa é AWS WAF verificada, mas o quão antiga ela olha cada vez que verifica. AWS WAF verifica a taxa com frequência, com um tempo independente da configuração da janela de avaliação.
- Limite de taxa — O número máximo de solicitações que correspondem aos seus critérios e que AWS WAF devem ser monitoradas apenas para a janela de avaliação especificada. A configuração de limite mais baixa permitida é 100. Quando esse limite é violado, AWS WAF aplica a configuração de ação de regra a solicitações adicionais que correspondam aos seus critérios.

  AWS WAF aplica uma limitação de taxa próxima ao limite que você definiu, mas não garante uma correspondência exata do limite. Para ter mais informações, consulte Advertências de regras baseadas em taxas.
- Agregação de solicitações:Os critérios de agregação a serem usados nas solicitações da web que a regra baseada em intervalos conta e limita o intervalo. O limite de taxa definido se aplica a cada instância de agregação. Para obter mais detalhes, consulte Opções e chaves de agregação e Instâncias e contagens de agregação.

- Ação:A ação a ser tomada em relação às solicitações que o intervalo da regra limita. Você pode usar qualquer ação de regra, exceto Allow. Isso é definido no nível da regra, como de costume, mas tem algumas restrições e comportamentos específicos das regras baseadas em taxas. Para obter informações gerais sobre as ações de regra, consulte Ação da regra. Para obter informações específicas sobre limitação de taxa, consulte Comportamento de limitação da taxa de solicitação de regras com base em taxas nesta seção.
- Escopo de inspeção e limitação de intervalo:Você pode restringir o escopo das solicitações que a instrução baseada em intervalos acompanha e os limites de intervalo adicionando uma instrução de redução de escopo. Se você especificar uma instrução de redução de escopo, a regra somente agregará, contará e limitará o intervalo das solicitações que correspondam à instrução de redução de escopo. Se você escolher a opção de agregação de solicitações Contar tudo, a instrução de redução de escopo será necessária. Para obter mais informações sobre instruções de redução do escopo, consulte Instruções de redução de escopo.
- (Opcional) Configuração de IP encaminhado:Isso só é usado se você especificar o Endereço IP no cabeçalho da sua agregação de solicitações, isoladamente ou como parte das configurações de chaves personalizadas. O AWS WAF recupera o primeiro endereço IP no cabeçalho especificado e o usa como valor de agregação. Um cabeçalho comum para essa finalidade é `X-Forwarded-For`, mas você pode especificar qualquer cabeçalho. Para ter mais informações, consulte Endereço IP encaminhado.

Advertências de regras baseadas em taxas

AWS WAF a limitação de taxa foi projetada para controlar as altas taxas de solicitação e proteger a disponibilidade do seu aplicativo da maneira mais eficiente e eficaz possível. Não se destina a limitar com precisão o intervalo de solicitações.

- AWS WAF estima a taxa de solicitações atual usando um algoritmo que dá mais importância às solicitações mais recentes. Por esse motivo, AWS WAF aplicará uma limitação de taxa próxima ao limite que você definiu, mas não garante uma correspondência exata do limite.
- Cada vez que AWS WAF estima a taxa de solicitações, AWS WAF analisa o número de solicitações recebidas durante a janela de avaliação configurada. Devido a esse e a outros fatores, como atrasos na propagação, é possível que as solicitações cheguem com uma taxa muito alta por vários minutos antes de serem AWS WAF detectadas e limitadas pela taxa. Da mesma forma, a taxa de solicitação pode ficar abaixo do limite por um período de tempo antes de AWS WAF detectar a diminuição e interromper a ação de limitação da taxa. Normalmente, esse atraso é inferior a 30 segundos.

- Se você alterar qualquer uma das configurações de limite de taxa em uma regra que está em uso, a alteração redefinirá as contagens de limite de taxa da regra. Isso pode pausar as atividades de limitação de taxa da regra por até um minuto. As configurações de limite de taxa são a janela de avaliação, o limite de taxa, as configurações de agregação de solicitações, a configuração de IP encaminhado e o escopo da inspeção.

Opções e chaves de agregação de regras com base em taxas

Por padrão, uma regra baseada em intervalo agrega e limita o intervalo das solicitações com base no endereço IP da solicitação. Você pode configurar a regra para usar várias outras chaves de agregação e combinações de teclas. Por exemplo, você pode agregar com base em um endereço IP encaminhado, no método HTTP ou em um argumento de consulta. Você também pode especificar combinações de chaves de agregação, como endereço IP e método HTTP, ou os valores de dois cookies diferentes.

> **Note**
>
> Todos os componentes da solicitação que você especifica na chave de agregação devem estar presentes em uma solicitação da web para que a solicitação seja avaliada ou o intervalo seja limitado pela regra.

Você pode configurar sua regra baseada em intervalos com as seguintes opções de agregação.

- Endereço IP de origem:Agregar usando apenas o endereço IP da origem da solicitação da web.

  O endereço IP de origem pode não conter o endereço do cliente de origem. Se uma solicitação da web passar por um ou mais proxies ou balanceadores de carga, ela conterá o endereço do último proxy.
- Endereço IP no cabeçalho:Agregar usando apenas um endereço de cliente em um cabeçalho HTTP. Isso também é conhecido como endereço IP encaminhado.

  Com essa configuração, você também especifica um comportamento de fallback a ser aplicado a uma solicitação da web com um endereço IP incorreto no cabeçalho. O comportamento de fallback define o resultado correspondente da solicitação como correspondente ou não correspondente. Sem correspondência, a regra baseada em intervalos não conta nem limita o intervalo da solicitação. Para corresponder, a regra baseada em intervalos agrupa a solicitação junto com outras solicitações que têm um endereço IP incorreto no cabeçalho especificado.

Tenha cuidado com essa opção, pois os cabeçalhos podem ser manipulados de forma inconsistente por proxies e também podem ser modificados para ignorar a inspeção. Para obter informações adicionais e práticas recomendadas, consulte Endereço IP encaminhado.

- Contar tudo:Contar e limitar o intervalo de todas as solicitações que correspondam à instrução de redução de escopo da regra. Essa opção requer uma instrução de redução de escopo. Isso geralmente é usado para limitar o intervalo de um conjunto específico de solicitações, como todas as solicitações com um rótulo específico ou todas as solicitações de uma área geográfica específica.
- Chaves personalizadas:Agregar usando uma ou mais chaves de agregação personalizadas. Para combinar qualquer uma das opções de endereço IP com outras chaves de agregação, defina-as aqui em chaves personalizadas.

  As chaves de agregação personalizadas são um subconjunto das opções do componente de solicitação da web descritas em Solicitar opções de componentes.

  As principais opções são as seguintes. Exceto onde indicado, você pode usar uma opção várias vezes, por exemplo, dois cabeçalhos ou três namespaces de rótulo.

  - Namespace de rótulo:Usar um namespace de rótulo como chave de agregação. Cada nome de rótulo distinto totalmente qualificado que tem o namespace de rótulo especificado contribui para a instância de agregação. Se você usar apenas um namespace de rótulo como chave personalizada, cada nome de rótulo definirá totalmente uma instância de agregação.

    A regra baseada em intervalos usa somente rótulos que foram adicionados à solicitação por regras que são avaliadas previamente na web ACL.

    Para obter mais informações sobre namespaces, consulte AWS WAF sintaxe de rótulos e requisitos de nomenclatura.
  - Cabeçalho:Usar um cabeçalho nomeado como chave de agregação. Cada valor distinto no cabeçalho contribui para a instância de agregação.

    O cabeçalho usa uma transformação de texto opcional. Consulte Opções de transformação de texto.
  - Cookie:Usar um cookie nomeado como chave de agregação. Cada valor distinto no cookie contribui para a instância de agregação.

    O cookie faz uma transformação de texto opcional. Consulte Opções de transformação de texto.

- Argumento de consulta:Usar um único argumento de consulta na solicitação como uma chave agregada. Cada valor distinto para o argumento de consulta nomeado contribui para a instância de agregação.

  O argumento de consulta usa uma transformação de texto opcional. Consulte Opções de transformação de texto.

- String de consulta:Use toda a string de consulta na solicitação como uma chave agregada. Cada string de consulta distinta contribui para a instância de agregação. Você pode usar esse tipo de chave uma vez.

  A string de consulta usa uma transformação de texto opcional. Consulte Opções de transformação de texto.

- Caminho do URI:Usar o caminho do URI na solicitação como uma chave agregada. Cada caminho de URI distinto contribui para a instância de agregação. Você pode usar esse tipo de chave uma vez.

  O caminho do URI usa uma transformação de texto opcional. Consulte Opções de transformação de texto.

- Método HTTP:Usar o método HTTP da solicitação como uma chave agregada. Cada método HTTP distinto contribui para a instância de agregação. Você pode usar esse tipo de chave uma vez.

- Endereço IP:Agregar usando o endereço IP da origem da solicitação da web em combinação com outras chaves.

  Pode não conter o endereço do cliente de origem. Se uma solicitação da web passar por um ou mais proxies ou balanceadores de carga, ela conterá o endereço do último proxy.

- Endereço IP no cabeçalho:Agregar usando o endereço do cliente em um cabeçalho HTTP em combinação com outras chaves. Isso também é conhecido como endereço IP encaminhado.

  Tenha cuidado com essa opção, pois os cabeçalhos podem ser tratados de forma inconsistente por proxies e podem ser modificados para ignorar a inspeção. Para obter informações adicionais e práticas recomendadas, consulte Endereço IP encaminhado.

Instâncias e contagens de agregação de regras com base em taxas

Quando uma regra baseada em intervalos avalia solicitações da web usando seus critérios de agregação, cada conjunto exclusivo de valores que a regra encontra para as chaves de agregação especificadas define uma instância de agregação exclusiva.

- Várias chaves:Se você definiu várias chaves personalizadas, o valor de cada chave contribuirá para a definição da instância de agregação. Cada combinação exclusiva de valores define uma instância de agregação.
- Chave única:Se você escolheu uma chave única, seja nas chaves personalizadas ou selecionando uma das opções de endereço IP único, cada valor exclusivo da chave define uma instância de agregação.
- Contar tudo: sem chaves:Se você selecionou a opção de agregação Contar tudo, todas as solicitações avaliadas pela regra pertencerão a uma única instância de agregação da regra. Essa escolha requer uma instrução de redução de escopo.

Uma regra baseada em intervalos conta solicitações da web separadamente para cada instância de agregação que identifica.

Por exemplo, suponha que uma regra baseada em intervalos avalie solicitações da web com os seguintes valores de endereço IP e método HTTP:

- Endereço IP 10.1.1.1, método HTTP POST
- Endereço IP 10.1.1.1, método HTTP GET
- Endereço IP 127.0.0.0, método HTTP POST
- Endereço IP 10.1.1.1, método HTTP GET

A regra cria diferentes instâncias de agregação de acordo com seus critérios de agregação.

- Se o critério de agregação for apenas o endereço IP, cada endereço IP individual será uma instância de agregação e AWS WAF contará as solicitações separadamente para cada um. As instâncias de agregação e as contagens de solicitações do nosso exemplo seriam as seguintes:
  - Endereço IP 10.1.1.1: contagem 3
  - Endereço IP 127.0.0.0: contagem 1

- Se o critério de agregação for o método HTTP, cada método HTTP individual será uma instância de agregação. As instâncias de agregação e as contagens de solicitações do nosso exemplo seriam as seguintes:
  - Método HTTP POST: contagem 2
  - Método HTTP GET: contagem 2
- Se os critérios de agregação forem endereço IP e método HTTP, cada endereço IP e cada método HTTP contribuirão para a instância de agregação combinada. As instâncias de agregação e as contagens de solicitações do nosso exemplo seriam as seguintes:
  - Endereço IP 10.1.1.1, método HTTP POST: contagem 1
  - Endereço IP 10.1.1.1, método HTTP GET: contagem 2
  - Endereço IP 127.0.0.0, método HTTP POST: contagem 1

Comportamento de limitação da taxa de solicitação de regras com base em taxas

Os critérios AWS WAF usados para limitar a taxa de solicitações de uma regra baseada em taxas são os mesmos AWS WAF usados para agregar solicitações para a regra. Se você definir uma instrução de escopo para a regra, AWS WAF somente agregará, contará e limitará as solicitações que correspondam à instrução de escopo reduzido.

Os critérios de correspondência que fazem com que uma regra baseada em intervalos aplique suas configurações de ação de regra a uma solicitação da web específica são os seguintes:

- A solicitação da web corresponde à instrução de redução de escopo da regra, se uma estiver definida.
- A solicitação da web pertence a uma instância de agregação cuja contagem de solicitações está atualmente acima do limite da regra.

Como AWS WAF se aplica a ação da regra

Quando uma regra baseada em taxa aplica limitação de taxa a uma solicitação, ela aplica a ação da regra e, se você tiver definido algum tratamento ou rótulo personalizado em sua especificação de ação, a regra os aplica. Esse tratamento de solicitações é o mesmo que a forma como uma regra de correspondência aplica suas configurações de ação às solicitações da web correspondentes. Uma regra baseada em intervalos só aplica rótulos ou executa outras ações em solicitações que estejam ativamente limitando o intervalo.

Você pode usar qualquer ação de regra, exceto Allow. Para obter informações gerais sobre as ações de regra, consulte Ação da regra.

A lista a seguir descreve como a limitação de taxa funciona para cada uma das ações.

- Block— AWS WAF bloqueia a solicitação e aplica qualquer comportamento de bloqueio personalizado que você tenha definido.
- Count— AWS WAF conta a solicitação, aplica todos os cabeçalhos ou rótulos personalizados que você definiu e continua a avaliação da web ACL da solicitação.

  Essa ação não limita a taxa de solicitações. Ele apenas conta as solicitações que estão acima do limite.
- CAPTCHA ou Challenge:O AWS WAF trata a solicitação como Block ou como Count, dependendo do estado do token da solicitação.

  Essa ação não limita a taxa de solicitações que têm tokens válidos. Isso limita a taxa de solicitações que estão acima do limite e também não têm tokens válidos.

  - Se a solicitação não tiver um token válido e não expirado, a ação bloqueia a solicitação e envia o quebra-cabeça CAPTCHA ou o desafio do navegador de volta ao cliente.

    Se o usuário final ou o navegador do cliente responder com êxito, o cliente receberá um token válido e reenviará automaticamente a solicitação original. Se a limitação de intervalo para a instância de agregação ainda estiver em vigor, essa nova solicitação com o token válido e não expirado terá a ação aplicada a ela conforme descrito no próximo marcador.
  - Se a solicitação tiver um token válido e não expirado, a ação CAPTCHA ou Challenge verificará o token e não executará nenhuma ação sobre a solicitação, semelhante à ação Count. A regra baseada em taxa retorna a avaliação da solicitação de volta à ACL da web sem realizar nenhuma ação de encerramento, e a ACL da web continua avaliando a solicitação.

  Para obter informações adicionais, consulte CAPTCHAe Challenge em AWS WAF.

Se você limitar o intervalo apenas do endereço IP ou do endereço IP encaminhado

Quando você configura a regra para limitar a intervalo somente do endereço IP para o endereço IP encaminhado, a instância da regra pode limitar o intervalo de até 10.000 endereços IP. Se uma instância de regra identificar mais de 10.000 endereços IP até o limite de intervalo, ela limitará apenas os 10.000 remetentes mais altos.

Com essa configuração, você pode recuperar a lista de endereços IP que uma regra baseada em taxa limita atualmente. Se você estiver usando uma instrução scope-down, as solicitações com taxa limitada são somente aquelas na lista de IPs que correspondem à instrução scope-down. Para obter informações sobre como recuperar a lista de endereços IP, consulte Como listar endereços IP que estão sendo limitados por regras baseadas em intervalos.

Exemplos de regras baseadas em intervalos

Esta seção descreve exemplos de configurações para uma variedade de casos de uso comuns de regras baseadas em intervalos.

Cada exemplo fornece uma descrição do caso de uso e, em seguida, mostra a solução nas listas JSON para as regras personalizadas configuradas.

> **Note**
>
> As listas JSON mostradas nesses exemplos foram criadas no console configurando a regra e depois editando-a usando o Editor JSON de regras.

Tópicos

- Limite de intervalo das solicitações a uma página de login
- Limite de intervalo das solicitações a uma página de login a partir de qualquer endereço IP, par de agente de usuário
- Limite de intervalo de solicitações sem um cabeçalho específico
- Limite de intervalo de solicitações com rótulos específicos
- Limite de intervalo das solicitações de rótulos com um namespace de rótulo especificado

Limite de intervalo das solicitações a uma página de login

Para limitar o número de solicitações à página de login do seu site sem afetar o tráfego para o resto do site, você pode criar uma regra baseada em intervalos com uma instrução de redução de escopo que corresponda às solicitações à sua página de login e com a agregação de solicitações definida como Contar tudo.

A regra baseada em intervalos contará todas as solicitações à página de login em uma única instância de agregação e aplicará a ação da regra quando as solicitações excederem o limite.

A lista JSON a seguir mostra um exemplo dessa configuração de regra. A opção de agregação Contar tudo está listada no JSON como a `CONSTANT` da configuração. Este exemplo corresponde às páginas de login que começam com `/login`.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Limite de intervalo das solicitações a uma página de login a partir de qualquer endereço IP, par de agente de usuário

Para limitar o número de solicitações de endereço IP na página de login do seu site, use pares de agentes de usuário que excedam seu limite, defina a agregação de solicitações como Chaves personalizadas e forneça os critérios de agregação.

A lista JSON a seguir mostra um exemplo dessa configuração de regra. Neste exemplo, definimos o limite para 100 solicitações em qualquer período de cinco minutos por endereço IP, par de agentes de usuário.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
      ],
```

```
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Limite de intervalo de solicitações sem um cabeçalho específico

Para limitar o número de solicitações sem um cabeçalho específico, você pode usar a opção de agregação Contar tudo com uma instrução de redução de escopo. Configure a instrução de redução de escopo com uma instrução NOT lógica contendo uma instrução que retornará verdadeira somente se o cabeçalho existir e tiver um valor.

A lista JSON a seguir mostra um exemplo dessa configuração de regra.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
```

```
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

Limite de intervalo de solicitações com rótulos específicos

Você pode combinar a limitação de intervalo com qualquer regra ou grupo de regras que adicione rótulos às solicitações para limitar o número de solicitações de várias categorias. Para fazer isso, você configura sua web ACL da seguinte forma:

- Adicione as regras ou grupos de regras que adicionam rótulos e configure-os para que não bloqueiem ou permitam as solicitações que você deseja limitar. Se você usa grupos de regras gerenciadas, talvez seja necessário substituir algumas ações de regras de grupos de regras para Count alcançar esse comportamento.
- Adicione uma regra baseada em taxa à sua ACL da web com uma configuração de número de prioridade maior do que as regras de rotulagem e os grupos de regras. AWS WAF avalia as regras em ordem numérica, começando pela mais baixa, para que sua regra baseada em taxas seja executada após as regras de rotulagem. Configure seu limite de intervalo nos rótulos usando uma

combinação de correspondência de rótulos na instrução de redução de escopo e agregação de rótulos da regra.

O exemplo a seguir usa o grupo de regras AWS Managed Rules da lista de reputação de IP da Amazon. A regra do grupo de regras `AWSManagedIPDDoSList` detecta e rotula solicitações cujos IPs são conhecidos por estarem ativamente envolvidos em atividades de DDoS. A ação de regra é configurada para Count na definição do grupo de regras. Para obter mais informações sobre o grupo de regras, consulte the section called “Lista de reputação de IP da Amazon”.

A lista JSON da web ACL a seguir usa o grupo de regras de reputação de IPs seguido por uma regra baseada em intervalos de correspondência de rótulos. A regra baseada em intervalos usa uma instrução de redução de escopo para filtrar as solicitações que foram marcadas pela regra do grupo de regras. A instrução de regra baseada em intervalos agrega e limita as solicitações filtradas por seus endereços IP.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
```

```
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Limite de intervalo das solicitações de rótulos com um namespace de rótulo especificado

As regras de nível comum no grupo de regras gerenciadas do Controle de Bots adicionam rótulos para bots de várias categorias, mas só bloqueiam solicitações de bots não verificados. Para obter informações sobre essas regras, consulte Lista de regras do Controle de Bots.

Se você usa o grupo de regras gerenciadas do Controle de Bots, pode adicionar limitação de intervalo para solicitações de bots verificados individuais. Para fazer isso, você adiciona uma regra baseada em intervalos que é executada após o grupo de regras do Controle de Bots e agrega as solicitações por seus rótulos de nome de bot. Você especifica a chave de agregação do Namespace do rótulo e define a chave do namespace como `awswaf:managed:aws:bot-control:bot:name:`. Cada rótulo exclusivo com o namespace especificado definirá uma instância de agregação. Por exemplo, os rótulos `awswaf:managed:aws:bot-control:bot:name:axios` e `awswaf:managed:aws:bot-control:bot:name:curl` cada um definem uma instância de agregação.

A lista JSON de web ACL a seguir mostra essa configuração. A regra neste exemplo limita as solicitações de qualquer instância única de agregação de bots a 1.000 em um período de dois minutos.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
```

```
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Como listar endereços IP que estão sendo limitados por regras baseadas em intervalos

Se sua regra baseada em taxa agregar apenas o endereço IP ou o endereço IP encaminhado, você poderá recuperar a lista de endereços IP que a regra limita atualmente. AWS WAF armazena esses endereços IP na lista de chaves gerenciadas da regra.

> **Note**
>
> Essa opção só estará disponível se você agregar somente o endereço IP ou somente um endereço IP em um cabeçalho. Se você usar a agregação de solicitações de chaves personalizadas, não poderá recuperar uma lista de endereços IP com intervalos limitados, mesmo se usar uma das especificações de endereço IP em suas chaves personalizadas.

Uma regra baseada em intervalos aplica sua ação de regra às solicitações da lista de chaves gerenciadas da regra que correspondem à instrução de escopo da regra. Quando uma regra não tem uma instrução de redução de escopo, ela aplica a ação a todas as solicitações dos endereços IP que estão na lista. A ação de regra é Block por padrão, mas pode ser qualquer ação de regra válida, exceto Allow. O número máximo de endereços IP que AWS WAF podem limitar a taxa usando uma única instância de regra baseada em taxa é 10.000. Se mais de 10.000 endereços excederem o limite de taxa, AWS WAF limite aqueles com as taxas mais altas.

Você pode acessar a lista de chaves gerenciadas de uma regra com base em intervalos usando a CLI, a API ou qualquer um dos SDKs. Este tópico aborda o acesso usando a CLI e as APIs. O console não fornece acesso à lista no momento.

Para a AWS WAF API, o comando é GetRateBasedStatementManagedKeys.

Para a AWS WAF CLI, o comando é get-rate-based-statement -managed-keys.

Veja a seguir a sintaxe para recuperar a lista de endereços IP com taxa limitada para uma regra baseada em taxa que está sendo usada em uma ACL da web em uma distribuição da Amazon. CloudFront

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

Veja a seguir a sintaxe de um aplicativo regional, uma API REST do Amazon API Gateway, um Application Load Balancer, uma API AWS AppSync GraphQL, um grupo de usuários do Amazon Cognito, um serviço ou AWS App Runner uma instância de acesso verificado. AWS

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF monitora solicitações da Web e gerencia as chaves de forma independente para cada combinação exclusiva de ACL da Web, grupo de regras opcional e regra baseada em taxas. Por exemplo, se você definir uma regra baseada em intervalos dentro de um grupo de regras e, em seguida, usar o grupo em uma web ACL, o AWS WAF monitora solicitações da web e gerencia as chaves dessa web ACL, instrução de referência do grupo de regras e instância de regra baseada em intervalos. Se você usar o mesmo grupo de regras em uma segunda ACL da web, AWS WAF monitora as solicitações da web e gerencia as chaves para esse segundo uso de forma totalmente independente da primeira.

Para uma regra baseada em intervalos que você definiu dentro de um grupo de regras, você precisa fornecer o nome da instrução de referência do grupo de regras em sua solicitação, além do nome da web ACL e do nome da regra baseada em intervalos dentro do grupo de regras. Veja a seguir a sintaxe de um aplicativo regional em que a regra baseada em intervalos é definida dentro de um grupo de regras e o grupo de regras é usado em uma web ACL.

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --rule-name=RuleName
```

Instruções de regra do grupo de regras

As instruções de regras de grupo de regras não são aninháveis.

Esta seção descreve as instruções de regras de grupo de regras que você pode usar em sua web ACL. As unidades de capacidade de web ACL (WCUs) do grupo de regras são definidas pelo proprietário do grupo de regras no momento da criação. Para obter informações sobre WCUs, consulte AWS WAF unidades de capacidade web ACL (WCUs).

Instrução do grupo de regras	Descrição	WCUs
Grupo de regras gerenciadas		

Instrução do grupo de regras	Descrição	WCUs
	Executa as regras definidas no grupo de regras gerenciadas especificado. Você pode restringir o escopo das solicitações que o grupo de regras avalia adicionando uma instrução de redução de escopo. Você não pode aninhar uma instrução de grupo de regras dentro de qualquer outro tipo de instrução.	Definido pelo grupo de regras, além de quaisquer WCUs adicionais para uma instrução de redução de escopo.
Grupo de regras	Executa as regras definidas em um grupo de regras que você gerencia. Não é possível adicionar uma instrução de redução de escopo a uma instrução de referência de grupo de regras para seu próprio grupo de regras. Você não pode aninhar uma instrução de grupo de regras dentro de qualquer outro tipo de instrução	Você define o limite de WCU para o grupo de regras ao criá-lo.

Declaração do grupo de regras gerenciadas

A instrução de regra de grupo de regras gerenciadas adiciona uma referência na lista de regras de web ACL a um grupo de regras gerenciadas. Você não vê essa opção em suas instruções de regra

no console, mas quando você trabalha com o formato JSON da web ACL, todos os grupos de regras gerenciados que você adicionou aparecem sob as regras da web ACL como esse tipo.

Um grupo de regras gerenciadas é um grupo de regras AWS gerenciadas, a maioria dos quais é gratuita para AWS WAF clientes, ou um grupo de regras AWS Marketplace gerenciadas. Você se inscreve automaticamente nos grupos de regras de regras AWS gerenciadas pagos ao adicioná-los à sua ACL da web. Você pode se inscrever em grupos de regras AWS Marketplace gerenciados por meio de AWS Marketplace. Para ter mais informações, consulte Grupos de regras gerenciadas.

Ao adicionar um grupo de regras a uma web ACL, você pode modificar as ações de regras no grupo para Count ou para outra ação de regra. Para ter mais informações, consulte Opções de substituição de ação para grupos de regras.

Você pode restringir o escopo das solicitações que são AWS WAF avaliadas com o grupo de regras. Para fazer isso, você adiciona uma instrução de redução de escopo dentro da instrução do grupo de regras. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo. Isso pode ajudá-lo a gerenciar como o grupo de regras afeta seu tráfego e pode ajudá-lo a conter os custos associados ao volume de tráfego quando você usa o grupo de regras. Para obter informações e exemplos de uso de instruções de escopo reduzido com o grupo de regras gerenciadas do AWS WAF Bot Control, consulte. AWS WAF Controle de bots

Não aninhável:Você não pode aninhar esse tipo de instrução dentro de outras instruções e não pode incluí-la em um grupo de regras. Você pode incluí-la diretamente em uma web ACL.

(Opcional) Instrução de redução de escopo:Esse tipo de regra usa uma instrução opcional de redução de escopo para restringir o escopo das solicitações que o grupo de regras avalia. Para ter mais informações, consulte Instruções de redução de escopo.

WCUs: definido para o grupo de regras na criação.

Onde encontrar essa instrução de regra

- Console:durante o processo de criação de uma web ACL, na página Adicionar regras e grupos de regras, escolha Adicionar grupos de regras gerenciados e, em seguida, localize e selecione o grupo de regras que você deseja usar.
- API — ManagedRuleGroupStatement

Instrução do grupo de regras

A instrução de regra de grupo de regras adiciona uma referência à lista de regras de web ACL a um grupo de regras que você gerencia. Você não vê essa opção em suas instruções de regra no console, mas quando você trabalha com o formato JSON da web ACL, qualquer um dos seus próprios grupos de regras que você adicionou aparece sob as regras da web ACL como esse tipo. Para obter informações sobre como usar seus próprios grupos de regras, consulte Gerenciar seus próprios grupos de regras.

Ao adicionar um grupo de regras a uma web ACL, você pode modificar as ações de regras no grupo para Count ou para outra ação de regra. Para ter mais informações, consulte Opções de substituição de ação para grupos de regras.

Não aninhável:Você não pode aninhar esse tipo de instrução dentro de outras instruções e não pode incluí-la em um grupo de regras. Você pode incluí-la diretamente em uma web ACL.

WCUs: definido para o grupo de regras na criação.

Onde encontrar essa instrução de regra

- Console: durante o processo de criação de uma web ACL, na página Adicionar regras e grupos de regras, escolha Adicionar minhas próprias regras e grupos de regras, Grupo de regras, e, em seguida, adicione o grupo de regras que você deseja usar.
- API — RuleGroupReferenceStatement

Tratamento de componentes de solicitação de tamanho grande no AWS WAF

AWS WAF não suporta a inspeção de conteúdos muito grandes para o corpo, cabeçalhos ou cookies dos componentes da solicitação da web. O serviço host subjacente tem limites de contagem e tamanho para o que ele encaminha AWS WAF para inspeção. Por exemplo, o serviço de hospedagem não envia mais de 200 cabeçalhos para AWS WAF, portanto, para uma solicitação da web com 205 cabeçalhos, não é AWS WAF possível inspecionar os últimos 5 cabeçalhos.

Quando AWS WAF permite que uma solicitação da Web prossiga para seu recurso protegido, toda a solicitação da Web é enviada, incluindo qualquer conteúdo que esteja fora dos limites de contagem e tamanho que AWS WAF pudemos inspecionar.

Limites de tamanho de inspeção de componentes

Os limites de tamanho de inspeção de componentes são os seguintes:

- **`Body`**e **`JSON Body`** — Para Application Load Balancer and AWS AppSync, AWS WAF pode inspecionar os primeiros 8 KB do corpo de uma solicitação. Pois CloudFront, o API Gateway, o Amazon Cognito, o App Runner e o Verified Access, por padrão, AWS WAF podem inspecionar os primeiros 16 KB e você pode aumentar o limite até 64 KB na sua configuração de ACL da web. Para ter mais informações, consulte Gerenciando os limites de tamanho da inspeção corporal.
- **`Headers`**— AWS WAF pode inspecionar no máximo os primeiros 8 KB (8.192 bytes) dos cabeçalhos da solicitação e no máximo os primeiros 200 cabeçalhos. O conteúdo está disponível para inspeção AWS WAF até o primeiro limite atingido.
- **`Cookies`**— AWS WAF pode inspecionar no máximo os primeiros 8 KB (8.192 bytes) dos cookies de solicitação e no máximo os primeiros 200 cookies. O conteúdo está disponível para inspeção AWS WAF até o primeiro limite atingido.

Opções de tratamento de tamanho grande para suas instruções de regras

Ao escrever uma instrução de regra que inspeciona um desses tipos de componentes de solicitação, você especifica como lidar com componentes de tamanho grande. O tratamento de tamanho excessivo diz AWS WAF o que fazer com uma solicitação da Web quando o componente da solicitação que a regra inspeciona está acima dos limites de tamanho.

As opções para o tratamento de tamanhos acima do limitesão as seguintes:

- Continue— Inspecione o componente da solicitação normalmente de acordo com os critérios de inspeção da regra. AWS WAF inspecionará o conteúdo do componente da solicitação que está dentro dos limites de tamanho.
- Match— Trate a solicitação da web como se correspondesse à declaração da regra. AWS WAF aplica a ação da regra à solicitação sem avaliá-la de acordo com os critérios de inspeção da regra.
- No match— Trate a solicitação da web como se não correspondesse à declaração da regra sem avaliá-la de acordo com os critérios de inspeção da regra. AWS WAF continua sua inspeção da solicitação da web usando o resto das regras na ACL da web, como faria com qualquer regra não correspondente.

No AWS WAF console, você precisa escolher uma dessas opções de manuseio. Fora do console, a opção padrão é Continue.

Se você usar a opção Match em uma regra que tenha sua ação definida como Block, a regra bloqueará uma solicitação cujo componente inspecionado seja muito grande. Com qualquer outra configuração, a disposição final da solicitação depende de vários fatores, como a configuração das outras regras em sua web ACL e a configuração de ação padrão da web ACL.

Tratamento de tamanho grande em grupos de regras que você não possui

As limitações de tamanho e contagem de componentes se aplicam a todas as regras que você usa na sua web ACL. Isso inclui todas as regras que você usa, mas não gerencia, em grupos de regras gerenciadas e em grupos de regras que são compartilhados com você por outra conta.

Quando você usa um grupo de regras que você não gerencia, o grupo de regras pode ter uma regra que inspeciona um componente de solicitação limitado, mas que não processa conteúdos de tamanho grande da maneira que você precisa que eles sejam tratados. Para obter informações sobre como as regras AWS gerenciadas gerenciam componentes de grande porte, consulteAWS Lista de grupos de regras de regras gerenciadas. Para obter informações sobre outros grupos de regras, pergunte ao seu provedor de grupos de regras.

Diretrizes para gerenciar componentes de tamanho grande em sua web ACL

A maneira como você lida com componentes de tamanho grande na sua web ACL pode depender de vários fatores, como o tamanho esperado do conteúdo do componente da solicitação, o tratamento padrão da solicitação da sua web ACL e como outras regras na sua web ACL correspondem e tratam as solicitações.

As diretrizes gerais para gerenciar componentes de tamanho grande de solicitações da web são as seguintes:

- Se você precisar permitir algumas solicitações com conteúdo de componente de tamanho grande, se possível, adicione regras para permitir explicitamente somente essas solicitações. Priorize essas regras para que elas sejam executadas antes de qualquer outra regra na web ACL que inspecione os mesmos tipos de componentes. Com essa abordagem, você não poderá usá-la AWS WAF para inspecionar todo o conteúdo dos componentes grandes que você permite passar para seu recurso protegido.
- Para todas as outras solicitações, você pode impedir a passagem de bytes adicionais bloqueando as solicitações que ultrapassam o limite:
  - Suas regras e grupos de regras:Nas regras que inspecionam componentes com limites de tamanho, configure o tratamento de tamanho grande para bloquear solicitações que ultrapassem o limite. Por exemplo, se sua regra bloquear solicitações com conteúdo de cabeçalho específico,

defina o tratamento de tamanho grande para corresponder às solicitações com conteúdo de cabeçalho grande. Como alternativa, se sua web ACL bloquear solicitações por padrão e sua regra permitir conteúdos de cabeçalho específicos, configure o tratamento de tamanho grande da regra para não corresponder a nenhuma solicitação com conteúdo de cabeçalho de tamanho grande.

- Grupos de regras que você não gerencia:Para evitar que grupos de regras que você não gerencia permitam componentes de solicitação de tamanho grande, você pode adicionar uma regra separada que inspecione o tipo de componente da solicitação e bloqueie as solicitações que ultrapassam os limites. Priorize a regra em sua web ACL para que ela seja executada antes dos grupos de regras. Por exemplo, você pode bloquear solicitações com conteúdo do corpo grande antes que qualquer uma das regras de inspeção do corpo seja executada na web ACL. O procedimento a seguir descreve como adicionar esse tipo de regra.

Bloqueio de componentes de solicitação da web de grandes dimensões

Você pode adicionar uma regra na sua ACL da web que bloqueia solicitações com componentes superdimensionados.

Para adicionar uma regra que bloqueie conteúdos grandes

1. Ao criar ou editar sua web ACL, nas configurações de regras, escolha Adicionar regras, Adicionar minhas próprias regras e grupos de regras, Criador de regras e Editor visual de regras. Para obter orientação sobre como criar ou editar uma web ACL, consulte Trabalho com :web ACLs.
2. Insira um nome para sua regra e deixe a configuração Tipo em Regra normal.
3. Altere as seguintes configurações de correspondência de seus padrões:

    a. Em Instrução, para Inspecionar, abra a lista suspensa e escolha o componente de solicitação da web de que você precisa, seja Corpo, Cabeçalhos ou Cookies.

    b. Para Tipo de correspondência, escolha Tamanho maior que.

    c. Em Tamanho, digite um número que seja pelo menos o tamanho mínimo para o tipo de componente. Para cabeçalhos e cookies, digite8192. Em Application Load Balancer ou AWS AppSync web ACLs, para corpos, digite. 8192 Para corpos em CloudFront API Gateway, Amazon Cognito, App Runner ou Verified Access web ACLs, se você estiver usando o limite padrão de tamanho corporal, digite. 16384 Caso contrário, digite o limite de tamanho do corpo que você definiu para sua ACL da web.

   d. Para Tratamento de tamanhos grandes, selecione Corresponder.
4. Em Ação, selecione Bloquear.
5. Escolha Adicionar regra.
6. Depois de adicionar a regra, na página Definir prioridade da regra, mova-a acima de qualquer regra ou grupo de regras em sua web ACL que inspecione o mesmo tipo de componente. Isso dá à nova regra uma configuração de prioridade numérica mais baixa, o que faz com que AWS WAF seja avaliada primeiro. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

Correspondência de padrões de expressão regular em AWS WAF

AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE. `libpcre` A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl.

AWS WAF não suporta todas as construções da biblioteca. Por exemplo, ele suporta algumas afirmações de largura zero, mas não todas. Não temos uma lista abrangente das estruturas suportadas. No entanto, se você fornecer um padrão regex que não seja válido ou usar construções sem suporte, a AWS WAF API relatará uma falha.

AWS WAF não suporta os seguintes padrões de PCRE:

- Referências reversas e subexpressões de captura
- Referências de sub-rotina e padrões recursivos
- Padrões condicionais
- Verbos de controle de referência reversa
- A diretiva de byte único \C
- A diretiva de correspondência de nova linha \R
- O início \K da diretiva de redefinição da correspondência
- Callouts e códigos integrados
- Agrupamento atômico e quantificadores possessivos

Conjuntos de IP e conjuntos de padrões regex em AWS WAF

AWS WAF armazena algumas informações mais complexas em conjuntos que você usa referenciando-os em suas regras. Cada um desses conjuntos tem um nome e recebe um Nome

de recurso da Amazon (ARN) na criação. Você pode gerenciar esses conjuntos de dentro de suas instruções de regra e pode acessá-los e gerenciá-los por conta própria, através do painel de navegação do console.

Você pode usar um conjunto gerenciado em um grupo de regras ou ACL da web.

- Para usar um conjunto de IPs, consulteInstrução de regra de correspondência de conjunto de IPs.
- Para usar um conjunto de padrões regex, consulteInstrução de regra de correspondência do conjunto de padrões de regex.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Tópicos

- Criar e gerenciar um conjunto de IP
- Criar e gerenciar um conjunto de padrões Regex

Criar e gerenciar um conjunto de IP

Um conjunto de IP fornece uma coleção de endereços IP e intervalos de endereços IP que você deseja usar juntos em uma instrução de regra. Os conjuntos de IP são AWS recursos.

Para usar um IP definido em uma ACL da web ou grupo de regras, primeiro você cria um AWS recurso, `IPSet` com suas especificações de endereço. Em seguida, você faz referência ao conjunto ao adicionar uma instrução de regra de conjunto de IP a uma web ACL ou grupo de regras.

Tópicos

Criar um conjunto de IP

Siga o procedimento nesta seção para criar um novo conjunto de IP.

> **Note**
>
> Além do procedimento nesta seção, você tem a opção de adicionar um novo conjunto de IP ao adicionar uma regra de correspondência de IP à web ACL ou grupo de regras. Escolher essa opção requer que você forneça as mesmas configurações que as exigidas por este procedimento.

Para criar um conjunto de IP

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha IP sets (Conjuntos de IP) e, em seguida, Create IP set (Criar conjunto de IP).
3. Digite um nome e uma descrição para o conjunto de IP. Você usará essas informações para identificar o conjunto quando quiser usá-lo.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar o conjunto de IP.

4. Em Região, escolha Global (CloudFront) ou escolha a região em que você deseja armazenar o conjunto de IP. Você pode usar conjuntos de IPs regionais somente em web ACLsque protejam recursos regionais. Para usar um IP definido em ACLs da web que protegem CloudFront as distribuições da Amazon, você deve usar Global ()CloudFront.
5. Para a versão IP, selecione a versão que deseja usar.
6. Na caixa de texto Endereços IP, insira um endereço IP ou intervalo de endereços IP por linha, na notação CIDR. AWS WAF suporta todos os intervalos CIDR IPv4 e IPv6, exceto o. `/0` Para obter mais informações sobre a notação CIDR, consulte o artigo na Wikipédia sobre CIDR.

   Veja alguns exemplos:

   - Para especificar o endereço IPv4 192.0.2.44, digite 192.0.2.44/32.
   - Para especificar o endereço IPv6 2620:0:2d0:200:0:0:0:0, digite 2620:0:2d0:200:0:0:0:0/128.
   - Para especificar o intervalo de endereços IPv4 de 192.0.2.0 a 192.0.2.255, digite 192.0.2.0/24.
   - Para especificar o intervalo de endereços IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, insira 2620:0:2d0:200::/64.
7. Revise as configurações do conjunto de IP e escolha Criar conjunto de IP.

Excluir um conjunto de IP

Siga as orientações nesta seção para excluir um conjunto referenciado.

Como excluir um conjunto e grupo de regras refenciados

Quando você exclui uma entidade que pode ser usada em uma ACL da web, como um conjunto de IP, conjunto de padrões regex ou grupo de regras, AWS WAF verifica se a entidade está sendo usada atualmente em uma ACL da web. Se descobrir que está em uso, AWS WAF avisa você. AWS WAF quase sempre é capaz de determinar se uma entidade está sendo referenciada por uma ACL da web. No entanto, em casos raros, talvez não seja possível fazer isso. Se você precisar ter certeza de que nada está usando a entidade no momento, verifique em suas web ACLs antes de excluir. Se a entidade for um conjunto referenciado, verifique também se nenhum grupo de regras está utilizando-a.

Para excluir um conjunto de IP

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

2. No painel de navegação, escolha Conjuntos de IP.
3. Selecione o conjunto de IP que deseja excluir e escolha Delete (Excluir).

Criar e gerenciar um conjunto de padrões Regex

Um conjunto de padrões regex fornece uma coleção de expressões regulares que você deseja usar em conjunto em uma instrução de regra. Os conjuntos de padrões Regex são AWS recursos.

Para usar um padrão regex definido em uma ACL da web ou grupo de regras, primeiro você cria um AWS recurso, `RegexPatternSet` com suas especificações de padrão regex. Em seguida, você faz referência ao conjunto ao adicionar uma instrução de regra de conjunto de padrões regex a uma web ACL ou grupo de regras. Um conjunto de padrões regex deve conter pelo menos um padrão regex.

Se o seu conjunto de padrões regex contiver mais de um padrão regex, quando ele for usado em uma regra, a correspondência de padrões é combinada com uma lógica `OR`. Ou seja, uma solicitação web corresponderá à instrução de regra de conjunto de padrões se o componente de solicitação corresponder a qualquer um dos padrões no conjunto.

AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.

Tópicos

- Criar um conjunto de padrões regex
- Excluir um conjunto de padrões regex

Criar um conjunto de padrões regex

Siga o procedimento nesta seção para criar um novo conjunto de padrões regex.

Para criar um conjunto de padrões regex

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Regex pattern sets (Conjuntos de padrões Regex) e Create regex pattern set (Criar conjunto de padrões regex).

3. Informe um nome e uma descrição para o conjunto de padrões regex. Você usará esses dados para identificá-lo quando quiser usar o conjunto.

   > **Note**
   >
   > Não é possível alterar o nome depois de criar o conjunto de padrões regex.

4. Em Região, escolha Global (CloudFront) ou escolha a Região em que você deseja armazenar o conjunto de padrões regex. Você pode usar conjuntos de padrões regex regionais somente em web ACLsque protejam recursos regionais. Para usar um padrão de regex definido em ACLs da web que protegem CloudFront as distribuições da Amazon, você deve usar Global (). CloudFront
5. Na caixa de texto Regular expressions (Expressões regulares) insira um padrão de regex por linha.

   Por exemplo, a expressão regular `I[a@]mAB[a@]dRequest` corresponde às seguintes strings: `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` e `I@mAB@dRequest`.

   AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.
6. Revise as configurações do conjunto de padrões regex e escolha Create regex pattern set (Criar conjunto de padrões regex).

Excluir um conjunto de padrões regex

Siga as orientações nesta seção para excluir um conjunto referenciado.

Como excluir um conjunto e grupo de regras refenciados

Quando você exclui uma entidade que pode ser usada em uma ACL da web, como um conjunto de IP, conjunto de padrões regex ou grupo de regras, AWS WAF verifica se a entidade está sendo usada atualmente em uma ACL da web. Se descobrir que está em uso, AWS WAF avisa você. AWS WAF quase sempre é capaz de determinar se uma entidade está sendo referenciada por uma ACL da web. No entanto, em casos raros, talvez não seja possível fazer isso. Se você precisar ter certeza de que nada está usando a entidade no momento, verifique em suas web ACLs antes de excluir. Se a entidade for um conjunto referenciado, verifique também se nenhum grupo de regras está utilizando-a.

Como excluir um conjunto de padrões regex

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Regex pattern sets (Conjuntos de padrões Regex).
3. Selecione o conjunto de padrões regex que deseja deletar e escolha Delete (Excluir).

Solicitações e respostas personalizadas da web no AWS WAF

Você pode adicionar um comportamento personalizado de solicitação e tratamento de respostas da web às suas ações de AWS WAF regra e ações padrão da ACL da web. Suas configurações personalizadas se aplicam sempre que a ação à qual elas estão anexadas se aplica.

É possível personalizar solicitações e respostas da web das seguintes maneiras:

- Com as ações Allow, Count, CAPTCHA e Challenge, você pode inserir cabeçalhos personalizados na solicitação da web. Quando o AWS WAF encaminha a solicitação da web para o recurso protegido, a solicitação contém toda a solicitação original mais os cabeçalhos personalizados que você inseriu. Para as ações CAPTCHA, Challenge e AWS WAF , só se aplica a personalização se a solicitação for aprovada na inspeção do CAPTCHA ou do token de desafio.

- Com ações Block, você pode definir uma resposta personalizada completa, com código de resposta, cabeçalhos e corpo. O recurso protegido responde à solicitação usando a resposta personalizada fornecida pelo AWS WAF. Sua resposta personalizada substitui a resposta de ação Block padrão de `403 (Forbidden)`.

Configurações de ação que você pode personalizar

Você pode especificar uma solicitação ou resposta personalizada ao definir as seguintes configurações de ação:

- A ação da regra. Para mais informações, consulte Ação da regra.
- Ação padrão para uma web ACL. Para mais informações, consulte A ação padrão da web ACL.

Configurações de ação que você não pode personalizar

Você não pode especificar o tratamento personalizado da solicitação na ação de substituição de um grupo de regras que você usa em uma web ACL. Consulte Avaliação de regras da web ACL e do grupo de regras. Consulte também Declaração do grupo de regras gerenciadas e Instrução do grupo de regras.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Limites no uso de solicitações e respostas personalizadas

AWS WAF define configurações máximas para o uso de solicitações e respostas personalizadas. Por exemplo, um número máximo de cabeçalhos de solicitação por web ACL ou grupo de regras e um número máximo de cabeçalhos personalizados para uma única definição de resposta personalizada. Para mais informações, consulte AWS WAF cotas.

Tópicos

- Inserções de cabeçalho de solicitação personalizadas para ações sem bloqueio
- Respostas personalizadas para ações Block
- Códigos de status compatíveis para resposta personalizada

Inserções de cabeçalho de solicitação personalizadas para ações sem bloqueio

Você pode AWS WAF instruir a inserir cabeçalhos personalizados na solicitação HTTP original quando uma ação de regra não bloqueia a solicitação. Com essa opção, você só adiciona itens à solicitação. Não é possível modificar nem substituir nenhuma parte da solicitação original. Os casos de uso para inserção de cabeçalhos personalizados incluem sinalizar um aplicativo de downstream para processar a solicitação de forma diferente com base nos cabeçalhos inseridos e sinalizar a solicitação para análise.

Essa opção se aplica às ações de regra Allow, Count, CAPTCHA e Challenge e às ações padrão da web ACL definidas como Allow. Para obter mais informações sobre as ações de regra, consulte Ação da regra. Para obter mais informações sobre ações padrão de web ACL, consulte A ação padrão da web ACL.

Nomes de cabeçalho de solicitação personalizados

AWS WAF prefixa todos os cabeçalhos de solicitação com os quais ele é inserido`x-amzn-waf-`, para evitar confusão com os cabeçalhos que já estão na solicitação. Por exemplo, se você especificar o nome do cabeçalho`sample`, AWS WAF insere o cabeçalho`x-amzn-waf-sample`.

Cabeçalhos com o mesmo nome

Se a solicitação já tiver um cabeçalho com o mesmo nome que AWS WAF está sendo inserido, AWS WAF substituirá o cabeçalho. Portanto, se você definir cabeçalhos em várias regras com nomes idênticos, a última regra a inspecionar a solicitação e encontrar uma correspondência teria seu cabeçalho adicionado, e as regras anteriores não.

Cabeçalhos personalizados com ações de regra que não são de encerramento

Ao contrário da Allow ação, a Count ação não AWS WAF impede o processamento da solicitação da web usando o resto das regras na ACL da web. Da mesma forma, quando CAPTCHA e Challenge determinam que o token da solicitação é válido, essas ações não param AWS WAF de processar a solicitação da web. Portanto, se você inserir cabeçalhos personalizados usando uma regra com uma dessas ações, as regras subsequentes também poderão inserir cabeçalhos personalizados. Para obter mais informações sobre comportamento de ações de regra, consulte Ação da regra.

Por exemplo, suponha que você tenha as seguintes regras, priorizadas na ordem mostrada:

1. RegraA com uma ação Count e um cabeçalho personalizado chamado `RuleAHeader`.

2. RegraB com uma ação Allow e um cabeçalho personalizado chamado `RuleBHeader`.

Se uma solicitação corresponder à regra A e à regra B, AWS WAF insere os cabeçalhos `x-amzn-waf-RuleAHeader` ex`-amzn-waf-RuleBHeader`, em seguida, encaminha a solicitação para o recurso protegido.

AWS WAF insere cabeçalhos personalizados em uma solicitação da Web quando termina de inspecionar a solicitação. Portanto, se você usar o tratamento personalizado de solicitações com uma regra que tenha a ação definida como Count, os cabeçalhos personalizados adicionados não serão inspecionados pelas regras subsequentes.

Exemplo de tratamento personalizado de solicitações

Você define o tratamento personalizado de solicitações para a ação de uma regra ou para a ação padrão de uma web ACL. A lista a seguir mostra o JSON para tratamento personalizado adicionado à ação padrão de uma web ACL.

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
```

```
  "MetricName": "SampleWebACL"
 }
}
```

Respostas personalizadas para ações Block

Você pode AWS WAF instruir a enviar uma resposta HTTP personalizada de volta ao cliente para ações de regra ou ações padrão de ACL da web definidas como. Block Para obter mais informações sobre as ações de regra, consulte Ação da regra. Para obter mais informações sobre ações padrão de web ACL, consulte A ação padrão da web ACL.

Ao definir o tratamento personalizado de resposta para uma ação Block, você define o código de status, os cabeçalhos e o corpo da resposta. Para obter uma lista de códigos de status que você pode usar com AWS WAF, consulte a seção a seguir,Códigos de status compatíveis para resposta personalizada.

Casos de uso

Os casos de uso de respostas personalizadas incluem o seguinte:

- Enviar um código de status não padrão de volta ao cliente.
- Enviar cabeçalhos de resposta personalizada de volta ao cliente. É possível especificar qualquer nome de cabeçalho, exceto `content-type`.
- Enviar uma página de erro estática de volta ao cliente.
- Redirecionar o cliente para um URL diferente. Para fazer isso, você especifica um dos códigos de status de redirecionamento `3xx`, como `301 (Moved Permanently)` ou `302 (Found)`, e depois especifica um novo cabeçalho `Location` com o novo URL.

Interação com respostas que você define em seu recurso protegido

As respostas personalizadas que você especifica para a AWS WAF Block ação têm precedência sobre qualquer especificação de resposta definida no seu recurso protegido.

O serviço de hospedagem do AWS recurso com o qual você protege AWS WAF pode permitir o tratamento personalizado de respostas para solicitações da web. Os exemplos incluem:

- Com a Amazon CloudFront, você pode personalizar a página de erro com base no código de status. Para obter informações, consulte Geração de respostas de erro personalizadas no Amazon CloudFront Developer Guide.

- Com o Amazon API Gateway, você pode definir a resposta e o código de status do seu gateway. Para obter mais informações, consulte Respostas do API Gateway no Guia do desenvolvedor do Amazon API Gateway.

Você não pode combinar configurações de resposta AWS WAF personalizadas com configurações de resposta personalizadas no AWS recurso protegido. A especificação de resposta para qualquer solicitação individual da web vem totalmente do AWS WAF ou totalmente do recurso protegido.

Para solicitações da web que AWS WAF bloqueiam, o seguinte mostra a ordem de precedência.

1. AWS WAF resposta personalizada — Se a AWS WAF Block ação tiver uma resposta personalizada ativada, o recurso protegido enviará a resposta personalizada configurada de volta ao cliente. Qualquer configuração de resposta que você possa ter definido no próprio recurso protegido não tem efeito.
2. Resposta personalizada definida no recurso protegido:Caso contrário, se o recurso protegido tiver configurações de resposta personalizada especificadas, o recurso protegido usará essas configurações para responder ao cliente.
3. AWS WAF Blockresposta padrão — Caso contrário, o recurso protegido responderá ao cliente com a Block resposta AWS WAF `403 (Forbidden)` padrão.

Para solicitações da Web que AWS WAF permitem, sua configuração do recurso protegido determina a resposta que ele envia de volta ao cliente. Você não pode definir as configurações de resposta AWS WAF para solicitações permitidas. A única personalização que você pode configurar AWS WAF para solicitações permitidas é a inserção de cabeçalhos personalizados na solicitação original, antes de encaminhar a solicitação para o recurso protegido. Isso é descrito na seção anterior, Inserções de cabeçalho de solicitação personalizadas para ações sem bloqueio.

Cabeçalhos de resposta personalizada

É possível especificar qualquer nome de cabeçalho, exceto `content-type`.

Corpos de resposta personalizada

Você define o corpo de uma resposta personalizada dentro do contexto da web ACL ou do grupo de regras em que deseja usá-la. Depois de definir um corpo de resposta personalizada, você pode usá-lo como referência em qualquer outro lugar na web ACL ou no grupo de regras em que você o criou. Nas configurações de ação individual Block, você faz referência ao corpo personalizado que deseja usar e define o código de status e o cabeçalho da resposta personalizada.

Ao criar uma resposta personalizada no console, você pode escolher entre os corpos de resposta que já foram definidos ou criar um novo corpo. Fora do console, você define seus corpos de resposta personalizada no nível da web ACL ou do grupo de regras e, em seguida, faz referência a eles nas configurações de ação dentro da web ACL ou do grupo de regras. Isso é mostrado no exemplo JSON na seção a seguir.

Exemplo de resposta personalizada

O exemplo a seguir lista o JSON de um grupo de regras com configurações de resposta personalizada. O corpo da resposta personalizada é definido para todo o grupo de regras e, em seguida, referenciado por chave na ação da regra.

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
    }
   },
```

```
    "Name": "GeoMatchRule",
    "Priority": 1,
    "Statement": {
     "GeoMatchStatement": {
      "CountryCodes": [
       "US"
      ]
     }
    },
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestRuleGroupReferenceMetric",
     "SampledRequestsEnabled": true
    }
   }
  ],
  "VisibilityConfig": {
   "CloudWatchMetricsEnabled": true,
   "MetricName": "TestRuleGroupMetric",
   "SampledRequestsEnabled": true
  }
}
```

Códigos de status compatíveis para resposta personalizada

Para obter informações detalhadas sobre códigos de status HTTP, consulte Códigos de status da Internet Engineering Task Force (IETF) e Lista de códigos de status HTTP na Wikipedia.

A seguir estão os códigos de status HTTP que AWS WAF oferecem suporte para respostas personalizadas.

- `2xx Successful`
  - `200 – OK`
  - `201 – Created`
  - `202 – Accepted`
  - `204 – No Content`
  - `206 – Partial Content`
- `3xx Redirection`
  - `300 – Multiple Choices`

  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable
  - 504 – Gateway Timeout
  - 505 – HTTP Version Not Supported

AWS WAF rótulos em solicitações da web

Um rótulo são metadados adicionados a uma solicitação da Web por uma regra quando a regra corresponde à solicitação. Depois de adicionada, uma etiqueta permanece disponível na solicitação até que a avaliação da Web ACL termine. Você pode acessar rótulos em regras que serão executadas posteriormente na avaliação da web ACL usando uma instrução de correspondência de rótulos. Para obter detalhes, consulte Instrução de regra de correspondência de rótulo.

Os rótulos nas solicitações da web geram métricas de CloudWatch rótulos da Amazon. Para obter uma lista das métricas e dimensões, consulte Métricas e dimensões do rótulo. Para obter informações sobre como acessar métricas e resumos de métricas por CloudWatch meio do AWS WAF console, consulteMonitoramento e ajuste.

Casos de uso de rótulos

Os casos de uso comuns de AWS WAF rótulos incluem o seguinte:

- Avaliação de uma solicitação da Web em relação a várias declarações de regra antes de agir sobre a solicitação — Depois que uma correspondência for encontrada com uma regra em uma ACL da Web, AWS WAF continue avaliando a solicitação em relação à ACL da Web se a ação da regra não encerrar a avaliação da ACL da Web. Você pode usar rótulos para avaliar e coletar informações de várias regras antes de decidir permitir ou bloquear a solicitação. Para fazer isso, altere as ações de suas regras existentes para Count e configure-as para adicionar rótulos às solicitações correspondentes. Em seguida, adicione uma ou mais novas regras para serem executadas após as outras regras e configure-as para avaliar os rótulos e gerenciar as solicitações de acordo com as combinações de correspondência de rótulo.
- Gerenciamento de solicitações da web por região geográfica:Você pode usar somente a regra de correspondência geográfica para gerenciar solicitações da web por país de origem. Para ajustar a localização até o nível da região, você usa a regra de correspondência geográfica com uma ação Count seguida por uma regra de correspondência de rótulo. Para obter informações sobre regras de geo correspondência, consulte Instrução de regra de correspondência geográfica.
- Reutilização da lógica em várias regras:Se você precisar reutilizar a mesma lógica em várias regras, poderá usar rótulos para criar uma única fonte da lógica e apenas testar os resultados. Quando você tem várias regras complexas que usam um subconjunto comum de instruções de regras aninhadas, duplicar o conjunto de regras comuns em suas regras complexas pode ser demorado e propenso a erros. Com rótulos, você pode criar uma nova regra com o subconjunto de regras comuns que conta as solicitações correspondentes e adiciona um rótulo a elas. Você

adiciona a nova regra à sua web ACL para que ela seja executada antes das regras complexas originais. Em seguida, nas regras originais, você substitui o subconjunto de regras compartilhadas por uma única regra que verifica o rótulo.

Por exemplo, digamos que você tenha várias regras que deseja aplicar somente aos seus caminhos de login. Em vez de fazer com que cada regra especifique a mesma lógica para corresponder a possíveis caminhos de login, você pode implementar uma única nova regra que contenha essa lógica. Faça com que a nova regra adicione um rótulo às solicitações correspondentes para indicar que a solicitação está em um caminho de login. Em sua web ACL, atribua a essa nova regra uma configuração de prioridade numérica menor do que as regras originais para que ela seja executada primeiro. Em seguida, nas regras originais, substitua a lógica compartilhada por uma verificação da presença do rótulo. Para obter mais informações sobre as configurações de prioridade, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

- Criação de exceções às regras em grupos de regras:Essa opção é particularmente útil para grupos de regras gerenciadas, que você não pode visualizar nem alterar. Muitas regras de grupos de regras gerenciadas adicionam rótulos às solicitações da web correspondentes, para indicar as regras que corresponderam e, possivelmente, para fornecer informações adicionais sobre a correspondência. Ao usar um grupo de regras que adiciona rótulos às solicitações, você pode substituir as regras do grupo de regras para contar as correspondências e, em seguida, executar uma regra após o grupo de regras que trata a solicitação da web com base nos rótulos do grupo de regras. Todas as regras gerenciadas da AWS adicionam rótulos às solicitações da web correspondentes. Para obter detalhes, consulte as descrições da regra em AWS Lista de grupos de regras de regras gerenciadas.
- Usando métricas de rótulos para monitorar padrões de tráfego:Você pode acessar métricas para rótulos que você adiciona por meio de suas regras e para métricas adicionadas por qualquer grupo de regras gerenciadas que você usa em sua web ACL. Todos os grupos de regras das regras gerenciadas da AWS adicionam rótulos às solicitações da web que eles avaliam. Para obter uma lista das métricas e dimensões, consulte Métricas e dimensões do rótulo. Você pode acessar métricas e resumos de métricas por CloudWatch meio da página Web ACL no AWS WAF console. Para mais informações, consulte Monitoramento e ajuste.

Como funciona a AWS WAF rotulagem

Quando uma regra corresponde a uma solicitação da web, se a regra tiver rótulos definidos, AWS WAF adicionará os rótulos à solicitação no final da avaliação da regra. As regras que são

avaliadas após a regra de correspondência na web ACL podem corresponder aos rótulos que a regra adicionou.

Quem adiciona rótulos às solicitações

Os componentes da web ACL que avaliam as solicitações podem adicionar rótulos às solicitações.

- Qualquer regra que não seja uma instrução de referência de grupo de regras pode adicionar rótulos às solicitações da web correspondentes. Os critérios de rotulagem fazem parte da definição da regra e, quando uma solicitação da Web corresponde à regra, AWS WAF os rótulos da regra são adicionados à solicitação. Para mais informações, consulte the section called “Regras que adicionam rótulos”.
- A instrução da regra de correspondência geográfica adiciona rótulos de país e região a qualquer solicitação que ela inspeciona, independentemente de a instrução resultar em uma correspondência. Para mais informações, consulte the section called “Correspondência geográfica”.
- As regras AWS gerenciadas para AWS WAF todos adicionam rótulos às solicitações que eles inspecionam. Elas adicionam alguns rótulos com base nas correspondências de regras no grupo de regras e alguns com base nos processos da AWS que os grupos de regras gerenciadas usam, como o rótulo de token adicionado quando você usa um grupo de regras de mitigação de ameaças inteligentes. Para obter informações sobre os rótulos que cada grupo de regras gerenciadas adiciona, consulte the section called “AWS Lista de grupos de regras de regras gerenciadas”.

Como AWS WAF gerencia rótulos

AWS WAF adiciona os rótulos da regra à solicitação ao final da inspeção da solicitação pela regra. A rotulagem faz parte das atividades de correspondência de uma regra, semelhante à ação.

Os rótulos não persistem com a solicitação da web após o término da avaliação da web ACL. Para que outras regras correspondam a um rótulo que sua regra adiciona, sua ação de regra não deve encerrar a avaliação da solicitação da web pela web ACL. A ação da regra deve ser definida como Count, CAPTCHA ou Challenge. Quando a avaliação da web ACL não termina, as regras subsequentes na web ACL podem executar seus critérios de correspondência de rótulos em relação à solicitação. Para obter mais informações sobre as ações de regra, consulte Ação da regra.

Acesso aos rótulos durante a avaliação da ACL na web

Depois de adicionados, os rótulos permanecem disponíveis na solicitação, desde que a solicitação AWS WAF seja avaliada em relação à ACL da web. Qualquer regra em uma web ACL pode acessar

rótulos que foram adicionados pelas regras que já foram executadas na mesma web ACL. Isso inclui regras que são definidas diretamente dentro da web ACL e regras definidas dentro dos grupos de regras que são usados na web ACL.

- Você pode fazer uma correspondência com um rótulo nos critérios de inspeção de solicitação da sua regra usando a instrução de correspondência de rótulos. Você pode corresponder com qualquer rótulo anexado à solicitação. Para obter detalhes da instrução, consulte Instrução de regra de correspondência de rótulo.
- A instrução de correspondência geográfica adiciona rótulos com ou sem correspondência, mas eles só estão disponíveis depois que a regra da web ACL que contém a instrução tiver concluído a avaliação da solicitação.
  - Você não pode usar uma única regra, por exemplo, uma instrução lógica AND, para executar uma instrução de correspondência geográfica seguida por uma instrução de correspondência de rótulo com os rótulos geográficos. Você deve colocar a instrução de correspondência de rótulos em uma regra separada que é executada após a regra que contém a instrução de correspondência geográfica.
  - Se você usar uma instrução de correspondência geográfica como uma instrução de redução de escopo dentro de uma instrução de regra baseada em intervalos ou instrução de referência de grupo de regras gerenciadas, os rótulos adicionados pela instrução de correspondência geográfica não estarão disponíveis para inspeção pela instrução da regra que a contém. Se você precisar inspecionar a rotulagem geográfica em uma instrução de regra baseada em intervalos ou em um grupo de regras, deverá executar a instrução de correspondência geográfica em uma regra separada que seja executada previamente.

Acesso às informações do rótulo fora da avaliação da ACL na web

Os rótulos não persistem com a solicitação da web após o término da avaliação da web ACL, mas o AWS WAF registra as informações dos rótulos nos logs e nas métricas.

- AWS WAF armazena CloudWatch métricas da Amazon para as primeiras 100 etiquetas em qualquer solicitação única. Para obter informações sobre como acessar métricas de rótulo, consulte Monitoramento com a Amazon CloudWatch e Métricas e dimensões do rótulo.
- AWS WAF resume as métricas do CloudWatch rótulo nos painéis de visão geral do tráfego da ACL da web no console. AWS WAF Você pode acessar os painéis em qualquer página de web ACL. Para ter mais informações, consulte Painéis de visão geral do tráfego de web ACL.

- AWS WAF registra as etiquetas nos registros das primeiras 100 etiquetas de uma solicitação. Você pode usar rótulos, junto com a ação de regra, para filtrar os logs que o AWS WAF registra. Para mais informações, consulte Registrando AWS WAF tráfego de ACL da web.

Sua avaliação de ACL da web pode aplicar mais de 100 rótulos a uma solicitação da web e comparar com mais de 100 rótulos, mas registra AWS WAF somente os 100 primeiros nos registros e métricas.

AWS WAF sintaxe de rótulos e requisitos de nomenclatura

Um rótulo é uma string composta por um prefixo, namespaces opcionais e um nome. Os componentes de um rótulo são delimitados com dois pontos. As rótulos têm os seguintes requisitos e características:

- Os rótulos diferenciam maiúsculas de minúsculas.
- Cada namespace de rótulo ou nome de rótulo pode ter até 128 caracteres.
- Você pode especificar até 5 namespaces em um rótulo.
- Os componentes de um rótulo são separados por dois pontos (`:`).
- Você não pode usar as seguintes sequências de caracteres reservadas nos namespaces ou no nome que você especifica para um rótulo: `awswaf`, `aws`, `waf`, `rulegroup`, `webacl`, `regexpatternset`, `ipset` e `managed`.

Sintaxe de rótulos

Um rótulo totalmente qualificado têm um prefixo, namespaces opcionais e nome de rótulo. O prefixo identifica o grupo de regras ou o contexto de web ACL da regra que adicionou o rótulo. Os namespaces podem ser usados para adicionar mais contexto ao rótulo. O nome do rótulo fornece o nível mais baixo de detalhes para um rótulo. Geralmente indica a regra específica que adicionou o rótulo à solicitação.

O prefixo do rótulo varia de acordo com sua origem.

- Seus rótulos:Veja a seguir a sintaxe completa dos rótulos que você cria em sua web ACL e nas regras do grupo de regras. Os tipos de entidade são `rulegroup` e `webacl`.

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

  - Prefixo do namespace do rótulo: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - Adições personalizadas de namespace: `<custom namespace>:…:`

  Ao definir um rótulo para uma regra em um grupo de regras ou web ACL, você controla as strings de namespace personalizadas e o nome do rótulo. O resto é gerado para você por AWS WAF. AWS WAF prefixa automaticamente todos os rótulos com as `awswaf` configurações da conta e da web ACL ou da entidade do grupo de regras.

- Rótulos de grupos de regras gerenciadas:Veja a seguir a sintaxe completa dos rótulos criados por regras em grupos de regras gerenciadas.

  ```
  awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
  ```

  - Prefixo do namespace do rótulo: `awswaf:managed:<vendor>:<rule group name>:`
  - Adições personalizadas de namespace: `<custom namespace>:…:`

  Todos os grupos de regras de regras AWS gerenciadas adicionam rótulos. Para obter informações sobre grupos de regras gerenciadas, consulte Grupos de regras gerenciadas.

- Rótulos de outros AWS processos — Esses processos são usados por grupos de regras de regras AWS gerenciadas, então você os vê adicionados às solicitações da web que você avalia usando grupos de regras gerenciadas. Veja a seguir a sintaxe completa dos rótulos criados por processos chamados por grupos de regras gerenciadas.

  ```
  awswaf:managed:<process>:<custom namespace>:...:<label name>
  ```

  - Prefixo do namespace do rótulo: `awswaf:managed:<process>:`
  - Adições personalizadas de namespace: `<custom namespace>:…:`

  Rótulos desse tipo são listados para os grupos de regras gerenciadas que chamam o processo da AWS . Para obter informações sobre grupos de regras gerenciadas, consulte Grupos de regras gerenciadas.

Exemplos de rótulos para suas regras

Os rótulos de exemplo a seguir são definidos por regras em um grupo de regras chamado `testRules` que pertence à conta, 111122223333.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

A lista a seguir mostra um exemplo de especificação de rótulo em JSON. Esses nomes de rótulos incluem strings de namespace personalizadas antes do nome final do rótulo.

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> Você pode acessar esse tipo de lista no console por meio do editor JSON de regras.

Se você executar a regra anterior no mesmo grupo de regras e conta dos exemplos de rótulos anteriores, os rótulos totalmente qualificados resultantes seriam os seguintes:

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Exemplos de rótulos para grupos de regras gerenciadas

Veja a seguir exemplos de rótulos de grupos de regras AWS gerenciadas e processos que eles invocam.

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF regras que adicionam rótulos

Em quase todas as regras, você pode definir rótulos e AWS WAF aplicá-los a qualquer solicitação correspondente.

Os seguintes tipos de regras são as únicas exceções:

- As regras baseadas em taxas rotulam somente enquanto limitam a taxa — As regras baseadas em taxas adicionam rótulos apenas às solicitações da web para uma instância de agregação específica, enquanto essa instância está sendo limitada por. AWS WAF Para obter mais informações sobre regras baseadas em intervalos, consulte Instrução de regra baseada em intervalos.
- A rotulagem não é permitida em declarações de referência de grupos de regras — o console não aceita rótulos para esses tipos de regras. Por meio da API, especificar um rótulo para qualquer tipo de instrução resulta em uma exceção de validação. Para obter informações sobre esses tipos de instrução, consulte Declaração do grupo de regras gerenciadas e Instrução do grupo de regras.

WCUs:1 WCU para cada cinco rótulos que você define em sua web ACL ou regras de grupo de regras.

Onde encontrar isso

- Criador de regras no console:Nas configurações da Ação da regra, em Rótulo.
- Tipo de dados de API: `Rule` `RuleLabels`

Você define um rótulo em uma regra especificando as cadeias de caracteres e o nome do namespace personalizados a serem anexados ao prefixo do namespace do rótulo. AWS WAF deriva o prefixo do contexto no qual você define a regra. Para obter informações sobre isso, consulte as informações de sintaxe do rótulo em AWS WAF sintaxe de rótulos e requisitos de nomenclatura.

AWS WAF regras que correspondem aos rótulos

Você pode usar uma instrução de correspondência de rótulos para avaliar rótulos de solicitações da web. Você pode corresponder com Rótulo, que exige o nome do rótulo, ou com Namespace, que exige uma especificação de namespace. Para rótulo ou namespace, você pode opcionalmente incluir namespaces anteriores e o prefixo em sua especificação. Para obter informações gerais sobre esse tipo de instrução, consulte Instrução de regra de correspondência de rótulo.

O prefixo de um rótulo define o contexto do grupo de regras ou web ACL em que a regra do rótulo é definida. Na declaração de correspondência de rótulo de uma regra, se sua string de correspondência de rótulo ou namespace não especificar o prefixo, AWS WAF use o prefixo para a regra de correspondência de rótulo.

- Os rótulos das regras definidas diretamente em uma web ACL têm um prefixo que especifica o contexto da web ACL.
- Os rótulos das regras que estão dentro de um grupo de regras têm um prefixo que especifica o contexto do grupo de regras. Esse pode ser seu próprio grupo de regras ou um grupo de regras gerenciadas para você.

Para obter informações sobre isso, consulte a sintaxe do rótulo em AWS WAF sintaxe de rótulos e requisitos de nomenclatura.

> **Note**
>
> Alguns grupos de regras gerenciadas adicionam rótulos. Você pode recuperá-los por meio da API chamando `DescribeManagedRuleGroup`. Os rótulos estão listados na propriedade `AvailableLabels` na resposta.

Se você quiser fazer a correspondência com uma regra que esteja em um contexto diferente do contexto da sua regra, forneça o prefixo na sequência de caracteres de correspondência. Por exemplo, se você quiser fazer a correspondência com rótulos adicionados por regras em um grupo de regras gerenciadas, você pode adicionar uma regra em sua web ACL com uma instrução de correspondência de rótulo cuja string de correspondência especifica o prefixo do grupo de regras seguido por seus critérios de correspondência adicionais.

Na string de correspondência da instrução de correspondência de rótulo, você especifica um rótulo ou um namespace:

- Rótulo:A especificação da rótulo para uma partida consiste na parte final da rótulo. Você pode incluir qualquer número de namespaces contíguos que precedem imediatamente o nome do rótulo seguido pelo nome. Você também pode fornecer a rótulo totalmente qualificado iniciando a especificação com o prefixo.

  Especificações de exemplo:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- Namespace:A especificação do namespace para uma correspondência consiste em qualquer subconjunto contíguo da especificação do rótulo, excluindo o nome. Você pode incluir o prefixo e incluir uma ou mais strings de namespace.

  Especificações de exemplo:

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF exemplos de correspondência de rótulos

Esta seção fornece exemplos de especificações de correspondência para a instrução da regra de correspondência de rótulos.

> **Note**
>
> Essas listas JSON foram criadas no console adicionando uma regra a uma web ACL com as especificações de correspondência de rótulos e, em seguida, editando a regra e mudando para o Editor JSON de regras. Você também pode obter o JSON para um grupo de regras ou web ACL por meio das APIs ou da interface da linha de comando.

Tópicos

Corresponda com um rótulo local

A lista JSON a seguir mostra uma instrução de correspondência de rótulo para um rótulo que foi adicionado à solicitação da web localmente, no mesmo contexto dessa regra.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Se você usar essa instrução de correspondência na conta 111122223333, em uma regra que você define para `testWebACL` da web ACL, ela corresponderá aos rótulos a seguir.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

Não corresponderia ao rótulo a seguir, porque a string do rótulo não é uma correspondência exata.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

Não corresponderia ao rótulo a seguir, porque o contexto não é o mesmo e, portanto, o prefixo não corresponde. Isso é verdade mesmo se você adicionou o `productionRules` do grupo de regras ao `testWebACL` da web ACL, onde a regra é definida.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Correspondência com um rótulo de outro contexto

A lista JSON a seguir mostra uma regra de correspondência de rótulos que corresponde a um rótulo de uma regra dentro de um grupo de regras criado pelo usuário. O prefixo é obrigatório na

especificação para todas as regras em execução na web ACL que não fazem parte do grupo de regras nomeado. Este exemplo de especificação de rótulo corresponde somente ao rótulo exato.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Correspondência com um rótulo de grupo de regras gerenciadas

Este é um caso especial de correspondência com um rótulo que é de outro contexto que não o da regra de correspondência. A lista JSON a seguir mostra uma instrução de correspondência de rótulo para um rótulo de grupo de regras gerenciadas. Isso corresponde somente ao rótulo exato especificado na configuração de chave da instrução de correspondência do rótulo.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Correspondência com um namespace local

A lista JSON a seguir mostra uma instrução de correspondência de rótulo para um namespace local.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Semelhante à correspondência `Label` local, se você usar essa instrução na conta 111122223333, em uma regra que você define para `testWebACL` da web ACL, ela corresponderá ao rótulo a seguir.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

Não corresponderia ao rótulo a seguir, porque a conta não é a mesma e, portanto, o prefixo não corresponde.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

O prefixo também não corresponde a nenhum rótulo aplicado por grupos de regras gerenciadas, como o seguinte.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Correspondência com um namespace de grupo de regras gerenciadas

A lista JSON a seguir mostra uma instrução de correspondência de rótulo para um namespace de grupo de regras gerenciadas. Para um grupo de regras que você possui, você também precisaria fornecer o prefixo para corresponder a um namespace que esteja fora do contexto da regra.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
```

```
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Essa especificação corresponde aos rótulos de exemplo a seguir.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

Não corresponde ao rótulo a seguir.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF mitigação inteligente de ameaças

Esta seção aborda os recursos gerenciados de mitigação inteligente de ameaças fornecidos pela. AWS WAF Essas são proteções avançadas e especializadas que você pode implementar para se proteger contra ameaças, como bots maliciosos e tentativas de apropriação de contas.

> **Note**
>
> Os recursos descritos aqui têm custos adicionais, além das taxas básicas de uso AWS WAF. Para obter mais informações, consulte Preços do AWS WAF.

A orientação fornecida nesta seção é destinada a usuários que geralmente sabem como criar e gerenciar ACLs AWS WAF da Web, regras e grupos de regras. Esses tópicos são abordados nas seções anteriores deste guia.

Tópicos

- Opções para mitigação de ameaças inteligentes

- Práticas recomendadas para mitigação de ameaças inteligentes
- AWS WAF tokens de solicitação da web
- AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP)
- AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP)
- AWS WAF Controle de bots
- AWS WAF integração de aplicativos clientes
- CAPTCHAe Challenge em AWS WAF

Opções para mitigação de ameaças inteligentes

Esta seção fornece uma comparação detalhada das opções para implementar a mitigação de ameaças inteligentes.

AWS WAF oferece os seguintes tipos de proteções para mitigação inteligente de ameaças.

- AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP) — Detecta e gerencia tentativas maliciosas de criação de contas na página de inscrição do seu aplicativo. A funcionalidade principal é fornecida pelo grupo de regras gerenciadas do ACFP. Para ter mais informações, consulte AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP) e AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.
- AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP) — Detecta e gerencia tentativas maliciosas de invasão na página de login do seu aplicativo. A funcionalidade principal é fornecida pelo grupo de regras gerenciadas do ATP. Para ter mais informações, consulte AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP) e AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.
- AWS WAF Controle de bots — identifica, rotula e gerencia bots amigáveis e maliciosos. Esse recurso fornece gerenciamento para bots comuns com assinaturas exclusivas em todos os aplicativos e também para bots direcionados que têm assinaturas específicas para um aplicativo. A funcionalidade principal é fornecida pelo grupo de regras gerenciadas do Controle de Bots. Para ter mais informações, consulte AWS WAF Controle de bots e AWS WAF Grupo de regras do Bot Control.
- SDKs de integração de aplicativos clientes — valide sessões de clientes e usuários finais em suas páginas da web e adquira AWS WAF tokens para os clientes usarem em suas solicitações na web. Se você usa ACFP, ATP ou Controle de Bots, implemente os SDKs de integração de

aplicativos em seu aplicativo cliente, se possível, para aproveitar ao máximo todos os recursos do grupo de regras. Só recomendamos usar esses grupos de regras sem uma integração do SDK como medida temporária, quando um recurso essencial precisa ser protegido rapidamente e não há tempo suficiente para a integração do SDK. Para obter informações sobre como implementar SDKs, consulte AWS WAF integração de aplicativos clientes.

- Challengee ações de CAPTCHA regras — valide sessões de clientes e usuários finais e adquira AWS WAF tokens para os clientes usarem em suas solicitações na web. Você pode implementá-las em qualquer lugar em que especifique uma ação de regra, em suas regras e como substituições nos grupos de regras que você usa. Essas ações usam AWS WAF JavaScript intersticiais para interrogar o cliente ou o usuário final e exigem aplicativos cliente que ofereçam suporte. JavaScript Para ter mais informações, consulte CAPTCHAe Challenge em AWS WAF.

Os grupos de regras AWS gerenciadas de mitigação inteligente de ameaças ACFP, ATP e Bot Control usam tokens para detecção avançada. Para obter informações sobre os recursos que os tokens habilitam nos grupos de regras, consulte Por que você deve usar os SDKs de integração de aplicativos com o ACFP, Por que você deve usar os SDKs de integração de aplicativos com o ATP e Por que você deve usar os SDKs de integração de aplicativos com o Controle de Bots.

Suas opções para implementar a mitigação inteligente de ameaças vão desde o uso básico de ações de regras para enfrentar desafios e impor a aquisição de tokens até os recursos avançados oferecidos pelos grupos de regras gerenciadas de mitigação AWS inteligente de ameaças.

As tabelas a seguir fornecem comparações detalhadas das opções dos recursos básicos e avançados.

Tópicos

- Opções para desafios e aquisição de tokens
- Opções para grupos de regras gerenciados de mitigação inteligente de ameaças
- Opções para limitação de intervalo em regras baseadas em intervalos e regras direcionadas do Controle de Bots

Opções para desafios e aquisição de tokens

Você pode oferecer desafios e adquirir tokens usando os SDKs de integração de AWS WAF aplicativos ou as ações de regras Challenge e. CAPTCHA Em termos gerais, as ações de regras são mais fáceis de implementar, mas geram custos adicionais, interferem mais na experiência do cliente

e exigem. JavaScript Os SDKs exigem programação em seus aplicativos cliente, mas eles podem fornecer uma melhor experiência ao cliente, são gratuitos e podem ser usados com JavaScript ou em aplicativos Android ou iOS. Você só pode usar os SDKs de integração de aplicativos com web ACLsque usam um dos grupos de regras gerenciadas pagos de mitigação de ameaças inteligentes, descritos na seção a seguir.

Comparação de opções para desafios e aquisição de tokens

	Ação da regra do Challenge	Ação da regra do CAPTCHA	JavaScript Desafio do SDK	Desafio do SDK móvel
O que é	Ação de regra que impõe a aquisição do AWS WAF token, apresentando ao cliente do navegador um desafio intersticial silencioso	Ação de regra que impõe a aquisição do AWS WAF token, apresentando ao usuário final do cliente um desafio visual ou de áudio (intersticial)	Camada de integração de aplicativos, para navegadores de clientes e outros dispositivos que são executados JavaScript. Renderiza o desafio silencioso e adquire um token	Camada de integração de aplicativos, para aplicativos Android e iOS. Renderiza nativamente o desafio silencioso e adquire um token
Boa escolha para...	Validação silenciosa contra sessões de bot e aplicação da aquisição de tokens para clientes que oferecem suporte JavaScript	Validação silenciosa e de usuário final em relação a sessões de bots e aplicação da aquisição de tokens, para clientes que oferecem suporte JavaScript	Validação silenciosa contra sessões de bot e aplicação da aquisição de tokens para clientes que oferecem suporte JavaScript. Os SDKs fornecem a menor latência	Validação silenciosa contra sessões de bots e aplicação da aquisição de tokens para aplicativos móveis nativos no Android e iOS. Os SDKs fornecem a menor latência

	Ação da regra do Challenge	Ação da regra do CAPTCHA	JavaScript Desafio do SDK	Desafio do SDK móvel
			e o melhor controle sobre onde o script de desafio é executado no aplicativo.	e o melhor controle sobre onde o script de desafio é executado no aplicativo.
Considerações de implement ação	Implement ado como uma configuração de ação de regra	Implement ado como uma configuração de ação de regra	Requer um dos grupos de regras pagas de ACFP, ATP ou Controle de Bots na web ACL. Requer codificaç ão no aplicativo cliente.	Requer um dos grupos de regras pagas de ACFP, ATP ou Controle de Bots na web ACL. Requer codificaç ão no aplicativo cliente.
Considerações sobre runtime	Fluxo intrusivo para solicitaç ões sem tokens válidos. O cliente é redirecionado para um AWS WAF desafio intersticial. Adiciona viagens de ida e volta à rede e exige uma segunda avaliação da solicitação da web.	Fluxo intrusivo para solicitaç ões sem tokens válidos. O cliente é redirecio nado para uma intersticial de CAPTCHA do AWS WAF . Adiciona viagens de ida e volta à rede e exige uma segunda avaliação da solicitação da web.	Pode ser executado nos bastidores. Oferece mais controle sobre a experiência do desafio.	Pode ser executado nos bastidores. Oferece mais controle sobre a experiência do desafio.

	Ação da regra do Challenge	Ação da regra do CAPTCHA	JavaScript Desafio do SDK	Desafio do SDK móvel
Requer JavaScript	Sim	Sim	Sim	Não
Clientes compatíveis	Navegador e dispositivos que executam Javascript	Navegador e dispositivos que executam Javascript	Navegador e dispositivos que executam Javascript	Dispositivos Android e iOS
Oferece suporte a aplicativos de página única (SPA)	Somente aplicação. Você pode usar a ação Challenge em conjunto com os SDKs para garantir que as solicitações tenham um token de desafio válido. Você não pode usar a ação de regra para entregar o script de desafio à página.	Somente aplicação. Você pode usar a ação CAPTCHA em conjunto com os SDKs para garantir que as solicitações tenham um token CAPTCHA válido. Você não pode usar a ação de regra para entregar o script CAPTCHA à página.	Sim	N/D

	Ação da regra do Challenge	Ação da regra do CAPTCHA	JavaScript Desafio do SDK	Desafio do SDK móvel
Custos adicionais	Sim, para configurações de ação que você especifica explicitamente, nas regras que você define ou como substituições de ação de regra nos grupos de regras que você usa. Não em todos os outros casos.	Sim, para configurações de ação que você especifica explicitamente, nas regras que você define ou como substituições de ação de regra nos grupos de regras que você usa. Não em todos os outros casos.	Não, mas requer um dos grupos de regras pagas de ACFP, ATP ou Controle de Bots.	Não, mas requer um dos grupos de regras pagas de ACFP, ATP ou Controle de Bots.

Para obter detalhes sobre os custos associados a essas opções, consulte as informações sobre mitigação de ameaças inteligentes em Preços do AWS WAF.

Pode ser mais simples executar desafios e fornecer a aplicação básica de tokens simplesmente adicionando uma regra com uma ação Challenge ou CAPTCHA. Talvez seja necessário usar as ações da regra, por exemplo, se você não tiver acesso ao código do aplicativo.

No entanto, se você puder implementar os SDKs, poderá economizar custos e reduzir a latência na avaliação da web ACL das solicitações da web do cliente, em comparação com o uso da ação Challenge:

- Você pode escrever sua implementação de SDK para executar o desafio em qualquer ponto do seu aplicativo. Você pode adquirir o token em segundo plano, antes de qualquer ação do cliente que envie uma solicitação da web ao seu recurso protegido. Dessa forma, o token fica disponível para envio com a primeira solicitação do seu cliente.
- Se, em vez disso, você adquirir tokens implementando uma regra com a ação Challenge, a regra e a ação exigirão avaliação e processamento adicionais da solicitação da web quando o cliente enviar uma solicitação pela primeira vez e sempre que o token expirar. A ação Challenge bloqueia a solicitação que não tem um token válido e não expirado e envia o intersticial do desafio de

volta ao cliente. Depois que o cliente responde com sucesso ao desafio, a intersticial reenvia a solicitação original da web com o token válido, que é então avaliado pela segunda vez pela web ACL.

Opções para grupos de regras gerenciados de mitigação inteligente de ameaças

Os grupos de regras AWS gerenciadas de mitigação inteligente de ameaças fornecem gerenciamento de bots básicos, detecção e mitigação de bots sofisticados e maliciosos, detecção e mitigação de tentativas de invasão de contas e detecção e mitigação de tentativas fraudulentas de criação de contas. Esses grupos de regras, combinados com os SDKs de integração de aplicativos descritos na seção anterior, fornecem as proteções mais avançadas e o acoplamento seguro com seus aplicativos clientes.

Comparação das opções de grupo de regras gerenciadas

	ACFP	ATP	Nível comum do Controle de Bots	Nível direciona do do Controle de Bots
O que é	Gerencia solicitações que podem fazer parte de tentativas fraudulentas de criação de conta nas páginas de registro e inscrição de um aplicativo. Não gerencia bots. Consulte AWS WAF Grupo de regras de prevenção de	Gerencia solicitações que podem fazer parte de tentativas maliciosas de apropriação na página de login de um aplicativo. Não gerencia bots. Consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP)	Gerencia bots comuns que se identific am automatic amente, com assinaturas exclusivas em todos os aplicativ os. Consulte AWS WAF Grupo de regras do Bot Control.	Gerencia bots direcionados que não se identificam, com assinaturas específicas para um aplicativo. Consulte AWS WAF Grupo de regras do Bot Control.

	ACFP	ATP	Nível comum do Controle de Bots	Nível direcionado do Controle de Bots
	fraudes (ACFP) para criação de contas de controle de fraudes.	de controle de fraudes.		
Boa escolha para...	Inspeção do tráfego de criação de conta em busca de ataques fraudulentos de criação de contas, como tentativas de criação com traversal de nome de usuário e muitas novas contas criadas a partir de um único endereço IP.	Inspeção do tráfego de login para ataques de apropriação de conta, como tentativas de login com traversal de senha e muitas tentativas de login do mesmo endereço IP. Quando usado com tokens, também fornece proteções agregadas, como limitação de intervalo de IPs e sessões de clientes para grandes volumes de tentativas de login malsucedidas.	Proteção básica de bots e rotulagem de tráfego de bots comum e automatizado.	Proteção direcionada contra bots sofisticados, incluindo limitação de intervalo no nível da sessão do cliente e detecção e mitigação de ferramentas de automação do navegador, como Selenium e Puppeteer.

	ACFP	ATP	Nível comum do Controle de Bots	Nível direciona do do Controle de Bots
Adiciona rótulos que indicam os resultados da avaliação	Sim	Sim	Sim	Sim
Adiciona rótulos de token	Sim	Sim	Sim	Sim
Bloqueio para solicitações sem um token válido	Não incluído. Consulte Bloqueio de solicitações que não têm um AWS WAF token válido.	Não incluído. Consulte Bloqueio de solicitações que não têm um AWS WAF token válido.	Não incluído. Consulte Bloqueio de solicitações que não têm um AWS WAF token válido.	Bloqueia sessões de clientes que enviam cinco solicitações sem um token.
Requer o AWS WAF token `aws-waf-token`	Necessário para todas as regras. Consulte Por que você deve usar os SDKs de integração de aplicativos com o ACFP.	Necessário para muitas regras. Consulte Por que você deve usar os SDKs de integração de aplicativos com o ATP.	Não	Sim
Adquire o token AWS WAF `aws-waf-token`	Sim, imposto pelo `AllRequests` da regra	Não	Não	Algumas regras usam ações de regra Challenge ou CAPTCHA, que adquirem tokens.

Para obter detalhes sobre os custos associados a essas opções, consulte as informações sobre mitigação de ameaças inteligentes em Preços do AWS WAF.

Opções para limitação de intervalo em regras baseadas em intervalos e regras direcionadas do Controle de Bots

O nível-alvo do grupo de regras do AWS WAF Bot Control e a declaração de regra AWS WAF baseada em taxas fornecem limitação da taxa de solicitações na web. A tabela a seguir compara as duas opções.

Comparação de opções para detecção e mitigação com base em intervalo

	AWS WAF regra baseada em taxas	AWS WAF Regras específicas do Bot Control	
Como a limitação de intervalo é aplicada	Atua em grupos de solicitações que estão chegando com uma taxa muito alta. Você pode aplicar qualquer ação, exceto Allow a.	Impõe padrões de acesso semelhantes aos humanos e aplica limitação dinâmica de intervalo, por meio do uso de tokens de solicitação.	
Com base nas linhas de base históricas de tráfego?	Não	Sim	
Tempo necessário para acumular linhas de base históricas de tráfego	N/D	Cinco minutos para limites dinâmicos. N/A para token ausente.	
Atraso de mitigação	Normalmente 30 a 50 segundos. Pode levar alguns minutos.	Geralmente menos que 10 segundos. Pode levar alguns minutos.	

	AWS WAF regra baseada em taxas	AWS WAF Regras específicas do Bot Control	
Alvos de mitigação	Configurável. Você pode agrupar solicitações usando uma instrução de escopo reduzido e por uma ou mais chaves de agregação, como endereço IP, método HTTP e sequência de caracteres de consulta.	Endereços IP e sessões de clientes	
Nível de volume de tráfego necessário para acionar mitigações	Médio - pode ser tão baixo quanto 100 solicitações na janela de tempo especificada	Baixo: destinado a detectar padrões de clientes, como extratores lentos	
Limites personalizáveis	Sim	Não	

	AWS WAF regra baseada em taxas	AWS WAF Regras específicas do Bot Control	
Ação de mitigação padrão	O padrão do console é Block. Nenhuma configuração padrão na API; a configuração é obrigatória. Você pode definir isso para qualquer ação de regra, exceto Allow.	As configurações de ação da regra do grupo de regras são Challenge para ausência de token e CAPTCHA para tráfego de alto volume de uma única sessão de cliente. Você pode definir qualquer uma dessas regras para qualquer ação de regra válida.	
Resiliência contra ataques altamente distribuídos	Médio - máximo de 10.000 endereços IP para limitação de endereço IP por si só	Média: limitado a um total de 50.000 entre endereços IP e tokens	
AWS WAF Definição de preço	Incluído nas taxas padrão para AWS WAF.	Incluído nas taxas do nível-alvo de mitigação inteligente de ameaças do Bot Control.	
Para obter mais informações	Instrução de regra baseada em intervalos	AWS WAF Grupo de regras do Bot Control	

Práticas recomendadas para mitigação de ameaças inteligentes

Siga as práticas recomendadas desta seção para obter a implementação mais eficiente e econômica dos recursos de mitigação de ameaças inteligentes.

- Implemente JavaScript os SDKs de integração de aplicativos móveis — Implemente a integração de aplicativos para habilitar o conjunto completo de funcionalidades de ACFP, ATP ou Bot Control da maneira mais eficaz possível. Os grupos de regras gerenciadas usam os tokens fornecidos pelos SDKs para separar o tráfego legítimo do cliente do tráfego indesejado no nível da sessão. Os SDKs de integração de aplicativos garantem que esses tokens estejam sempre disponíveis. Para obter detalhes, consulte:
  - Por que você deve usar os SDKs de integração de aplicativos com o ACFP
  - Por que você deve usar os SDKs de integração de aplicativos com o ATP
  - Por que você deve usar os SDKs de integração de aplicativos com o Controle de Bots

  Use as integrações para implementar desafios em seu cliente e, para JavaScript, personalizar a forma como os quebra-cabeças CAPTCHA são apresentados aos seus usuários finais. Para obter detalhes, consulte AWS WAF integração de aplicativos clientes.

  Se você personalizar os quebra-cabeças de CAPTCHA usando a JavaScript API e usar a ação de CAPTCHA regra em qualquer lugar da sua ACL da web, siga as orientações para lidar com a resposta do AWS WAF CAPTCHA em seu cliente em. Manipulando uma resposta CAPTCHA de AWS WAF Essa orientação se aplica a todas as regras que usam a ação CAPTCHA, incluindo aquelas do grupo de regras gerenciadas do ACFP e o nível de proteção direcionada do grupo de regras gerenciadas do Controle de Bots.
- Limite as solicitações que você envia aos grupos de regras ACFP, ATP e Bot Control — Você incorre em taxas adicionais pelo uso dos grupos de regras gerenciadas de mitigação AWS inteligente de ameaças. O grupo de regras do ACFP inspeciona as solicitações para os endpoints de registro e criação da conta que você especificar. O grupo de regras do ATP inspeciona as solicitações para o endpoint de login que você especificar. O grupo de regras do Controle de Bots inspeciona cada solicitação que chega até ele na avaliação da web ACL.

  Considere as seguintes abordagens para reduzir o uso desses grupos de regras:
  - Exclua solicitações da inspeção com uma instrução de redução de escopo na instrução do grupo de regras gerenciadas. Você pode fazer isso com qualquer instrução aninhável. Para mais informações, consulte Instruções de redução de escopo.

  - Exclua solicitações da inspeção adicionando regras antes do grupo de regras. Para regras que você não pode usar em uma instrução de redução de escopo e para situações mais complexas, como rotulagem seguida pela correspondência de rótulos, convém adicionar regras que sejam executadas antes dos grupos de regras. Para obter informações, consulte Instruções de redução de escopo e Princípios básicos da instrução de regras.
  - Execute os grupos de regras depois de regras mais baratas. Se você tiver outras AWS WAF regras padrão que bloqueiam solicitações por qualquer motivo, execute-as antes desses grupos de regras pagas. Para obter mais informações sobre regras e gerenciamento de regras, consulte Princípios básicos da instrução de regras.
  - Se você estiver usando mais de um dos grupos de regras gerenciadas de mitigação de ameaças inteligentes, execute-os na seguinte ordem para manter os custos baixos: Controle de Bots, ATP, ACFP.

  Para obter informações detalhadas sobre definição de preço, consulte Definição de preço do AWS WAF.
- Ativar o nível de proteção direcionada do grupo de regras do Controle de Bots durante o tráfego normal da web:Algumas regras do nível de proteção direcionada precisam de tempo para estabelecer linhas de base para os padrões normais de tráfego antes que possam reconhecer e responder a padrões de tráfego irregulares ou maliciosos. Por exemplo, as regras `TGT_ML_*` precisam de até 24 horas para se aquecerem.

  Adicione essas proteções quando você não estiver enfrentando um ataque e dê a elas tempo para estabelecer suas linhas de base antes de esperar que respondam adequadamente aos ataques. Se você adicionar essas regras durante um ataque, após o término do ataque, o tempo para estabelecer uma linha de base geralmente é do dobro ao triplo do tempo normal necessário, devido à distorção adicionada pelo tráfego do ataque. Para obter informações adicionais sobre as regras e os tempos de aquecimento exigidos, consulte Lista de regras.
- Para proteção distribuída de negação de serviço (DDoS), usar a mitigação automática de DDoS da camada de aplicativo do Shield Advanced:Os grupos de regras de mitigação de ameaças inteligentes não oferecem proteção contra DDoS. O ACFP protege contra tentativas fraudulentas de criação de conta na página de inscrição do seu aplicativo. O ATP protege contra tentativas de apropriação de conta em sua página de login. O Controle de Bots se concentra em aplicar padrões de acesso semelhantes aos humanos usando tokens e limitação dinâmica de intervalos nas sessões do cliente.

Quando você usa o Shield Advanced com a mitigação automática de DDoS na camada de aplicação ativada, o Shield Advanced responde automaticamente aos ataques de DDoS detectados criando, avaliando e implantando mitigações personalizadas em seu nome. AWS WAF Para obter mais informações sobre Shield Advanced, consulte AWS Shield Advanced visão geral e AWS Shield Advanced proteções da camada de aplicação (camada 7).

- Ajustar e configurar o tratamento de tokens:Ajuste o tratamento de tokens da web ACL para obter a melhor experiência do usuário.
  - Para reduzir os custos operacionais e melhorar a experiência do usuário final, ajuste seus tempos de imunidade de gerenciamento de tokens para o máximo que seus requisitos de segurança permitirem. Isso reduz ao mínimo o uso de quebra-cabeças CAPTCHA e desafios silenciosos. Para mais informações, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.
  - Para ativar o compartilhamento de tokens entre aplicativos protegidos, configure uma lista de domínios de tokens para sua web ACL. Para mais informações, consulte AWS WAF domínios de token e listas de domínios.
- Rejeitar solicitações com especificações arbitrárias de host:Configure seus recursos protegidos para exigir que os cabeçalhos `Host` nas solicitações da web correspondam ao recurso-alvo. Você pode aceitar um valor ou um conjunto específico de valores, como `myExampleHost.com` e `www.myExampleHost.com`, mas não aceitar valores arbitrários para o host.
- Para Application Load Balancers que são origens de CloudFront distribuições, configure CloudFront e manipule AWS WAF corretamente os tokens — Se você associar sua Web ACL a um Application Load Balancer e implantar o Application Load Balancer como origem de uma distribuição, consulte. CloudFront Configuração necessária para balanceadores de carga de aplicativos que são origens CloudFront
- Testar e ajustar antes da implantação:Antes de implementar qualquer alteração em sua web ACL, siga os procedimentos de testes e ajustes neste guia para ter certeza de que você está obtendo o comportamento esperado. Isso é especialmente importante para esses recursos pagos. Para obter orientação geral, consulte Testando e ajustando suas AWS WAF proteções. Para obter informações específicas sobre os grupos de regras gerenciadas pagos, consulte Testando e implantando o ACFP, Testando e implantando o ATP e Testando e implantando o AWS WAF Bot Control.

AWS WAF tokens de solicitação da web

AWS WAF os tokens são parte integrante das proteções aprimoradas oferecidas pela mitigação AWS WAF inteligente de ameaças. Um token, às vezes chamado de impressão digital, é uma coleção de informações sobre uma única sessão de cliente que o cliente armazena e fornece com cada solicitação da web enviada. AWS WAF usa tokens para identificar e separar sessões maliciosas de clientes de sessões legítimas, mesmo quando ambas se originam de um único endereço IP. O uso de tokens impõe custos insignificantes para usuários legítimos, mas caros em grande escala para botnets.

AWS WAF usa tokens para oferecer suporte à funcionalidade de desafio do navegador e do usuário final, que é fornecida pelos SDKs de integração de aplicativos e pelas ações de regras Challenge e. CAPTCHA Além disso, os tokens habilitam recursos dos grupos de regras gerenciados de controle de AWS WAF bots e prevenção de invasão de contas.

AWS WAF cria, atualiza e criptografa tokens para clientes que respondem com sucesso a desafios silenciosos e quebra-cabeças de CAPTCHA. Quando um cliente com um token envia uma solicitação da web, ele inclui o token criptografado, AWS WAF decodifica o token e verifica seu conteúdo.

Tópicos

Como AWS WAF usa tokens

AWS WAF usa tokens para registrar e verificar os seguintes tipos de validação da sessão do cliente:

- CAPTCHA:Os quebra-cabeças CAPTCHA ajudam a distinguir bots de usuários humanos. Um CAPTCHA é executado somente pela ação de regra CAPTCHA. Após a conclusão bem-sucedida do quebra-cabeça, o script do CAPTCHA atualiza o timestamp do CAPTCHA do token. Para ter mais informações, consulte CAPTCHAe Challenge em AWS WAF.

- Desafio:Os desafios são executados silenciosamente para ajudar a distinguir as sessões regulares dos clientes das sessões de bots e para tornar a operação dos bots mais dispendiosa. Quando o desafio é concluído com sucesso, o script do desafio adquire automaticamente um novo token, AWS WAF se necessário, e então atualiza a data e hora do desafio do token.

  AWS WAF executa desafios nas seguintes situações:

  - SDKs de integração de aplicativos:Os SDKs de integração de aplicativos são executados dentro das sessões do aplicativo cliente e ajudam a garantir que as tentativas de login só sejam permitidas após o cliente ter respondido com sucesso a um desafio. Para ter mais informações, consulte AWS WAF integração de aplicativos clientes.
  - Ação de regra Challenge:Para mais informações, consulte CAPTCHAe Challenge em AWS WAF.
  - CAPTCHA:Quando um intersticial CAPTCHA é executada, se o cliente ainda não tiver um token, o script executa automaticamente um desafio primeiro, para verificar a sessão do cliente e inicializar o token.

Os tokens são exigidos por muitas das regras dos grupos de regras de regras AWS gerenciadas de ameaças inteligentes. As regras usam tokens para fazer coisas como distinguir entre clientes no nível da sessão, determinar as características do navegador e entender o nível de interatividade humana na página da web do aplicativo. Esses grupos de regras invocam o gerenciamento de AWS WAF tokens, que aplica a rotulagem de tokens que os grupos de regras então inspecionam.

- AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP) — As regras da ACFP exigem solicitações na web com tokens válidos. Para obter mais informações sobre as regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.
- AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP) — As regras da ATP que evitam sessões de alto volume e longa duração com clientes exigem solicitações da web que tenham um token válido com um timestamp de desafio não expirado. Para ter mais informações, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.
- AWS WAF Controle de bots — As regras específicas desse grupo de regras limitam o número de solicitações da web que um cliente pode enviar sem um token válido e usam o rastreamento de sessão de token para monitoramento e gerenciamento em nível de sessão. Conforme necessário, as regras aplicam as ações de regra Challenge e CAPTCHApara impor a aquisição de tokens e o

comportamento válido do cliente. Para ter mais informações, consulte AWS WAF Grupo de regras do Bot Control.

AWS WAF características do token

Cada token tem as seguintes características:

- O token é armazenado em um cookie chamado `aws-waf-token`.
- O token é criptografado.
- O token imprime a sessão do cliente com um identificador granular fixo que contém as seguintes informações:
  - O timestamp da última resposta bem-sucedida do cliente a um desafio silencioso.
  - O timestamp da última resposta bem-sucedida do usuário final a um CAPTCHA. Isso só está presente se você usar CAPTCHA em suas proteções.
  - Informações adicionais sobre o cliente e o comportamento do cliente que podem ajudar a separar seus clientes legítimos do tráfego indesejado. As informações incluem vários identificadores de clientes e sinais do lado do cliente que podem ser usados para detectar atividades automatizadas. As informações coletadas não são exclusivas e não podem ser mapeadas para um ser humano individual.
    - Todos os tokens incluem dados da interrogação do navegador do cliente, como indicações de automação e inconsistências nas configurações do navegador. Essas informações são recuperadas pelos scripts que são executados pela ação Challenge e pelos SDKs do aplicativo cliente. Os scripts interrogam ativamente o navegador e colocam os resultados no token.
    - Além disso, quando você implementa um SDK de integração de aplicativos clientes, o token inclui informações coletadas passivamente sobre a interatividade do usuário final com a página do aplicativo. A interatividade inclui movimentos do mouse, pressionamentos de teclas e interações com qualquer formulário HTML presente na página. Essas informações ajudam o AWS WAF a detectar o nível de interatividade humana no cliente, para desafiar usuários que não parecem ser humanos. Para obter informações sobre integrações do lado do cliente, consulte AWS WAF integração de aplicativos clientes.

Por motivos de segurança, AWS não fornece uma descrição completa do conteúdo dos AWS WAF tokens nem informações detalhadas sobre o processo de criptografia do token.

Expiração do timestamp: tempos de imunidade AWS WAF do token

AWS WAF usa tempos de imunidade de desafio e CAPTCHA para controlar a frequência com que uma única sessão de cliente pode receber um desafio ou CAPTCHA. Depois que um usuário final responde com sucesso a um CAPTCHA, o tempo de imunidade do CAPTCHA determina por quanto tempo o usuário final permanece imune à apresentação de outro CAPTCHA. Da mesma forma, o tempo de imunidade ao desafio determina por quanto tempo uma sessão de cliente permanece imune a ser desafiada novamente após responder com sucesso a um desafio.

AWS WAF registra uma resposta bem-sucedida a um desafio ou CAPTCHA atualizando o timestamp correspondente dentro do token. Ao AWS WAF inspecionar o token em busca de desafio ou CAPTCHA, ele subtrai o timestamp da hora atual. Se o resultado for maior que o tempo de imunidade configurado, o timestamp expirará.

Você pode configurar os tempos de imunidade de desafio e CAPTCHA na web ACL e também em qualquer regra que use a ação da regra CAPTCHA ou Challenge.

- A configuração padrão de web ACL para ambos os tempos de imunidade é de 300 segundos.
- Você pode especificar o tempo de imunidade para qualquer regra que use a ação CAPTCHA ou Challenge. Se você não especificar o tempo de imunidade para a regra, ela herdará a configuração da web ACL.
- Para uma regra dentro de um grupo de regras que usa a ação CAPTCHA ou Challenge, se você não especificar o tempo de imunidade para a regra, ela herdará a configuração de cada web ACL em que você usa o grupo de regras.
- Os SDKs de integração de aplicativos usam o tempo de imunidade ao desafio da web ACL.

O valor mínimo do tempo limite do desafio de imunidade é 300 segundos. O valor mínimo do tempo limite do CAPTCHA de imunidade é 60 segundos. O valor máximo para ambos os tempos de imunidade é de 259.200 segundos ou três dias.

Você pode usar a web ACL e as configurações de tempo de imunidade de nível de regra para ajustar a ação CAPTCHA, Challenge ou o comportamento de gerenciamento de desafios do SDK. Por exemplo, você pode configurar regras que controlam o acesso a dados altamente confidenciais com baixos tempos de imunidade e, em seguida, definir tempos de imunidade mais altos em sua web ACL para que suas outras regras e os SDKs herdem.

Em particular para o CAPTCHA, resolver um quebra-cabeça pode degradar a experiência do seu cliente no site, portanto, ajustar o tempo de imunidade do CAPTCHA pode ajudá-lo a mitigar o impacto na experiência do cliente e, ao mesmo tempo, fornecer as proteções desejadas.

Para obter informações adicionais sobre como ajustar os tempos de imunidade para o uso das ações de regra Challenge e CAPTCHA, consulte Práticas recomendadas para usar as ações CAPTCHA e Challenge.

Onde definir os tempos de imunidade do AWS WAF token

Você pode definir os tempos de imunidade em sua web ACL e em suas regras que usam as ações de regra Challenge e CAPTCHA.

Para obter informações gerais sobre como gerenciar uma web ACL e suas regras, consulte Trabalho com :web ACLs.

Onde definir o tempo de imunidade para uma web ACL

- Console:Ao editar a web ACL, na guia Regras, edite e altere as configurações nos painéis Configuração de CAPTCHA de web ACL e Configuração de desafio de web ACL. No console, você pode configurar o CAPTCHA da web ACL e desafiar os tempos de imunidade somente depois de criar a web ACL.
- Fora do console:O tipo de dados da web ACL tem parâmetros de configuração de CAPTCHA e desafio, que você pode configurar e fornecer às suas operações de criação e atualização na web ACL.

Onde definir o tempo de imunidade para uma regra

- Console:Ao criar ou editar uma regra e especificar a ação CAPTCHA ou Challenge, você pode modificar a configuração do tempo de imunidade da regra.
- Fora do console:O tipo de dados da regra tem parâmetros de configuração de CAPTCHA e desafio, que você pode configurar ao definir a regra.

AWS WAF domínios de token e listas de domínios

Ao AWS WAF criar um token para um cliente, ele o configura com um domínio de token. Quando o AWS WAF inspeciona um token em uma solicitação da web, ele rejeita o token como inválido se o domínio não corresponder a nenhum dos domínios considerados válidos para a web ACL.

Por padrão, AWS WAF só aceita tokens cuja configuração de domínio corresponda exatamente ao domínio host do recurso associado à ACL da web. Esse é o valor do cabeçalho `Host` na solicitação da web. Em um navegador, você pode encontrar esse domínio na JavaScript `window.location.hostname` propriedade e no endereço que o usuário vê na barra de endereço.

Você também pode especificar domínios de token aceitáveis na configuração da web ACL, conforme descrito na seção a seguir. Nesse caso, AWS WAF aceita correspondências exatas com o cabeçalho do host e correspondências com domínios na lista de domínios do token.

Você pode especificar domínios de token para AWS WAF serem usados ao definir o domínio e ao avaliar um token em uma ACL da web. Os domínios que você especifica não podem ser sufixos públicos, como `gov.au`. Para os domínios que você não pode usar, consulte a lista https://publicsuffix.org/list/public_suffix_list.dat em Lista pública de sufixos.

AWS WAF configuração da lista de domínios do token Web ACL

Você pode configurar uma ACL da web para compartilhar tokens em vários recursos protegidos fornecendo uma lista de domínios de tokens com os domínios adicionais que você AWS WAF deseja aceitar. Com uma lista de domínios de token, AWS WAF ainda aceita o domínio host do recurso. Além disso, ele aceita todos os domínios da lista de domínios de tokens, incluindo seus subdomínios prefixados.

Por exemplo, uma especificação de domínio `example.com` na sua lista de domínios de tokens corresponde a `example.com` (de `http://example.com/`), `api.example.com`, (de `http://api.example.com/`) e `www.example.com` (de `http://www.example.com/`). Não corresponde a `example.api.com`, (de `http://example.api.com/`) ou `apiexample.com` (de `http://apiexample.com/`).

Você pode configurar a lista de domínios de tokens na sua web ACL ao criá-la ou editá-la. Para obter informações gerais sobre como gerenciar uma web ACL, consulte Trabalho com :web ACLs.

AWS WAF configurações de domínio de token

AWS WAF cria tokens a pedido dos scripts de desafio, que são executados pelos SDKs de integração de aplicativos Challenge e pelas ações de CAPTCHA regras.

O domínio AWS WAF definido em um token é determinado pelo tipo de script de desafio que o está solicitando e por qualquer configuração adicional de domínio de token fornecida por você. AWS WAF define o domínio no token para a configuração mais curta e geral que ele pode encontrar na configuração.

- JavaScript SDK — Você pode configurar o JavaScript SDK com uma especificação de domínio de token, que pode incluir um ou mais domínios. Os domínios que você configura devem ser domínios que AWS WAF serão aceitos, com base no domínio do host protegido e na lista de domínios de token da ACL da web.

  Quando AWS WAF emite um token para o cliente, ele define o domínio do token como um que corresponda ao domínio do host e seja o mais curto, entre o domínio do host e os domínios na sua lista configurada. Por exemplo, se o domínio do host for `api.example.com` e a lista de domínios do token tiver`example.com`, AWS WAF use `example.com` o token, porque ele corresponde ao domínio do host e é mais curto. Se você não fornecer uma lista de domínios de token na configuração da JavaScript API, AWS WAF defina o domínio como o domínio host do recurso protegido.

  Para ter mais informações, consulte Fornecimento de domínios para uso nos tokens.

- SDK móvel:No código do seu aplicativo, você deve configurar o SDK móvel com uma propriedade de domínio de token. Essa propriedade deve ser um domínio que o AWS WAF aceite, com base no domínio do host protegido e na lista de domínios de tokens da web ACL.

  Ao AWS WAF emitir um token para o cliente, ele usa essa propriedade como domínio do token. AWS WAF não usa o domínio host nos tokens que ele emite para o cliente SDK móvel.

  Para obter mais informações, consulte a configuração `WAFConfiguration` de `domainName` em A AWS WAF especificação do SDK móvel.

- Challengeação — Se você especificar uma lista de domínios de token na ACL da web, AWS WAF defina o domínio de token como um que corresponda ao domínio do host e seja o mais curto, entre o domínio do host e os domínios na lista. Por exemplo, se o domínio do host for `api.example.com` e a lista de domínios do token tiver`example.com`, AWS WAF use `example.com` o token, porque ele corresponde ao domínio do host e é mais curto. Se você não fornecer uma lista de domínios de token na Web ACL, AWS WAF defina o domínio como o domínio host do recurso protegido.

AWS WAF rotulagem de tokens pelo bot e grupos de regras gerenciados por fraudes

Esta seção descreve os rótulos que o gerenciamento de AWS WAF tokens adiciona às solicitações da web. Para obter informações gerais sobre rótulos, consulteAWS WAF rótulos em solicitações da web.

Quando você usa qualquer um dos grupos de regras gerenciados por AWS WAF bots ou controle de fraudes, os grupos de regras usam o gerenciamento de AWS WAF tokens para inspecionar os tokens de solicitação da web e aplicar a rotulagem de tokens às solicitações. Para obter informações sobre os grupos de regras gerenciadas, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes, AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes e AWS WAF Grupo de regras do Bot Control.

> **Note**
>
> AWS WAF aplica rótulos de token somente quando você usa um desses grupos de regras gerenciadas de mitigação inteligente de ameaças.

O gerenciamento de token pode adicionar os rótulos apresentados a seguir às solicitações da Web.

Rótulo de sessão do cliente

O rótulo `awswaf:managed:token:id:`*`identifier`* contém um identificador exclusivo que o gerenciamento de AWS WAF tokens usa para identificar a sessão do cliente. O identificador pode ser alterado se o cliente adquirir um novo token, por exemplo, após descartar o token que estava usando.

> **Note**
>
> AWS WAF não relata CloudWatch métricas da Amazon para esse rótulo.

Rótulos de status do token: prefixos de namespace para os rótulos

Os rótulos de status do token informam sobre o status do token e sobre as informações de desafio e de CAPTCHA que ele contém.

Cada rótulo de status do token começa com um dos seguintes prefixos de namespace:

- `awswaf:managed:token:`: usado para relatar o status geral do token e para informar o status das informações de desafio do token.
- `awswaf:managed:captcha:`: usado para relatar o status das informações de CAPTCHA do token.

Rótulos de status do token: nomes de rótulos

Na sequência do prefixo, o restante do rótulo fornece informações detalhadas sobre o status do token:

- `accepted`: o token de solicitação está presente e contém o seguinte:
  - Uma solução de desafio ou de CAPTCHA válida.
  - Um carimbo de data/hora de desafio ou de CAPTCHA não expirado.
  - Uma especificação de domínio válida para a ACL da Web.

  Exemplo: o rótulo `awswaf:managed:token:accepted` indica que o token de solicitações da Web tem uma solução de desafio válida, um carimbo de data/hora de desafio não expirado e um domínio válido.
- `rejected`: o token de solicitação está presente, mas não atende aos critérios de aceitação.

  Em conjunto com o rótulo rejeitado, o gerenciamento de token adiciona um namespace e um nome de rótulo personalizado para indicar o motivo.
  - `rejected:not_solved`: a solução de desafio ou de CAPTCHA está ausente no token.
  - `rejected:expired`: o carimbo de data/hora de desafio ou de CAPTCHA expirou no token, de acordo com os tempos de imunidade de token configurados pela sua ACL da Web.
  - `rejected:domain_mismatch`: o domínio do token não corresponde à configuração de domínio do token da sua ACL da Web.
  - `rejected:invalid`— não AWS WAF consegui ler o token indicado.

  Exemplo: os rótulos `awswaf:managed:captcha:rejected` e `awswaf:managed:captcha:rejected:expired` indicam que a solicitação foi rejeitada porque o carimbo de data/hora de CAPTCHA no token excedeu o tempo de imunidade para o token de CAPTCHA configurado na ACL da Web.
- `absent`: a solicitação não tem o token ou o gerenciador de token não conseguiu realizar a leitura dele.

  Exemplo: o rótulo `awswaf:managed:captcha:absent` indica que a solicitação não tem o token.

Bloqueio de solicitações que não têm um AWS WAF token válido

Quando você usa os grupos de regras AWS gerenciadas de ameaças inteligentes`AWSManagedRulesACFPRuleSet`, e

`AWSManagedRulesATPRuleSetAWSManagedRulesBotControlRuleSet`, os grupos de regras invocam o gerenciamento de AWS WAF tokens para avaliar o status do token de solicitação da web e rotular as solicitações adequadamente.

> **Note**
>
> A rotulagem de token é aplicada somente às solicitações da web que você avalia usando um desses grupos de regras gerenciadas.

Para obter informações sobre a rotulagem que o gerenciamento de token aplica, consulte a seção anterior, AWS WAF rotulagem de tokens pelo bot e grupos de regras gerenciados por fraudes.

Os grupos de regras gerenciadas de mitigação de ameaças inteligentes, então, lidam com os requisitos de token da seguinte forma:

- A regra `AllRequests` de `AWSManagedRulesACFPRuleSet` está configurada para executar a ação Challenge em todas as solicitações, bloqueando efetivamente qualquer uma que não tenha o rótulo de token `accepted`.
- O `AWSManagedRulesATPRuleSet` bloqueia as solicitações que têm o rótulo de token `rejected`, mas não bloqueia as solicitações com o rótulo de token `absent`.
- O nível de proteção direcionada do `AWSManagedRulesBotControlRuleSet` desafia os clientes depois que eles enviam cinco solicitações sem um rótulo de token `accepted`. Ele não bloqueia uma solicitação individual que não tenha um token válido. O nível de proteção comum do grupo de regras não gerencia os requisitos de token.

Para obter detalhes adicionais sobre os grupos de regras de ameaças inteligentes, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes, AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes e AWS WAF Grupo de regras do Bot Control.

Para bloquear solicitações sem tokens ao usar o grupo de regras gerenciadas do Controle de Bots ou do ATP

Com os grupos de regras do Controle de Bots e do ATP, é possível que uma solicitação sem um token válido saia da avaliação do grupo de regras e continue sendo avaliada pela web ACL.

Para bloquear todas as solicitações sem token ou cujo token foi rejeitado, adicione uma regra a ser executada imediatamente após o grupo de regras gerenciadas para capturar e bloquear solicitações que o grupo de regras não processa para você.

Veja a seguir um exemplo de lista JSON para uma web ACL que usa o grupo de regras gerenciadas do ATP. A web ACL tem uma regra adicional para capturar o rótulo `awswaf:managed:token:absent` e tratá-lo. A regra restringe sua avaliação às solicitações da web que vão para o endpoint de login, de acordo com o escopo do grupo de regras do ATP. A regra adicionada está listada em negrito.

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
```

```
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "/web/login",
              "FieldToMatch": {
                "UriPath": {}
              },
              "TextTransformations": [
```

```
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "STARTS_WITH"
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "POST",
              "FieldToMatch": {
                "Method": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "EXACTLY"
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "RequireTokenForLogins"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "exampleWebACL"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
```

```
}
```

Configuração necessária para balanceadores de carga de aplicativos que são origens CloudFront

Leia esta seção se você associar sua ACL da web a um Application Load Balancer e implantar o Application Load Balancer como origem de uma distribuição. CloudFront

Com essa arquitetura, você precisa fornecer a seguinte configuração adicional para que as informações do token sejam tratadas corretamente.

- Configure CloudFront para encaminhar o `aws-waf-token` cookie para o Application Load Balancer. Por padrão, CloudFront remove os cookies da solicitação da web antes de encaminhá-la para a origem. Para manter o cookie de token com a solicitação da web, configure o comportamento CloudFront do cache para incluir apenas o cookie de token ou todos os cookies. Para obter informações sobre como fazer isso, consulte Armazenamento em cache de conteúdo com base em cookies no Amazon CloudFront Developer Guide.
- Configure AWS WAF para que ele reconheça o domínio da CloudFront distribuição como um domínio de token válido. Por padrão, CloudFront define o `Host` cabeçalho como a origem do Application Load Balancer e a AWS WAF usa como o domínio do recurso protegido. O navegador do cliente, no entanto, vê a CloudFront distribuição como o domínio do host, e os tokens gerados para o cliente usam o CloudFront domínio como o domínio do token. Sem nenhuma configuração adicional, ao AWS WAF verificar o domínio do recurso protegido em relação ao domínio do token, haverá uma incompatibilidade. Para corrigir isso, adicione o nome do domínio de CloudFront distribuição à lista de domínios do token na sua configuração de ACL da web. Para obter informações sobre como fazer isso, consulte AWS WAF configuração da lista de domínios do token Web ACL.

AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP)

A fraude na criação de conta é uma atividade ilegal online na qual um invasor tenta criar uma ou mais contas falsas. Os invasores usam contas falsas para executar atividades fraudulentas, como abusar de bônus promocionais e de inscrição, se passar por alguém e realizar ataques cibernéticos, como phishing. A presença de contas falsas pode impactar negativamente seus negócios, prejudicando sua reputação com os clientes e sua exposição a fraudes financeiras.

Você pode monitorar e controlar as tentativas de fraude na criação de contas implementando o recurso AWS WAF de prevenção de fraudes na criação de contas (ACFP). AWS WAF oferece esse recurso no grupo de regras de regras AWS gerenciadas `AWSManagedRulesACFPRuleSet` com SDKs complementares de integração de aplicativos.

O grupo de regras gerenciadas do ACFP rotula e gerencia solicitações que podem fazer parte de tentativas maliciosas de criação de contas. O grupo de regras faz isso inspecionando as tentativas de criação de conta que os clientes enviam para o endpoint de inscrição de conta do seu aplicativo.

O ACFP protege as páginas de inscrição da sua conta monitorando as solicitações de inscrição de conta em busca de atividades anômalas e bloqueando automaticamente as solicitações suspeitas. O grupo de regras usa identificadores de solicitação, análise comportamental e machine learning para detectar solicitações fraudulentas.

- Inspeção de solicitações:O ACFP oferece visibilidade e controle sobre tentativas anômalas de criação de conta e tentativas que usam credenciais roubadas, para evitar a criação de contas fraudulentas. O ACFP verifica as combinações de e-mail e senha em seu banco de dados de credenciais roubadas, que é atualizado regularmente à medida que novas credenciais vazadas são encontradas na dark web. O ACFP avalia os domínios usados em endereços de e-mail e monitora o uso de números de telefone e campos de endereço para verificar as entradas e detectar comportamentos fraudulentos. O ACFP agrega dados por endereço IP e sessão do cliente, para detectar e bloquear clientes que enviam muitas solicitações de natureza suspeita.
- Inspeção de respostas — Para CloudFront distribuições, além de inspecionar as solicitações de criação de contas recebidas, o grupo de regras do ACFP inspeciona as respostas do seu aplicativo às tentativas de criação de contas, para monitorar as taxas de sucesso e falha. Usando essas informações, o ACFP pode bloquear temporariamente sessões de clientes ou endereços IP que tenham muitas tentativas com falha. O AWS WAF executa a inspeção de resposta de forma assíncrona, para que isso não aumente a latência no tráfego da web.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

> **Note**
>
> O recurso do ACFP não está disponível para grupos de usuários do Amazon Cognito.

Tópicos

AWS WAF Componentes do ACFP

Os principais componentes da prevenção de AWS WAF fraudes na criação de contas (ACFP) do Fraud Control são os seguintes:

- **`AWSManagedRulesACFPRuleSet`**— As regras desse grupo de regras de regras AWS gerenciadas detectam, rotulam e tratam vários tipos de atividades fraudulentas de criação de contas. O grupo de regras inspeciona as solicitações `GET` de HTTP de texto/html que os clientes enviam para o endpoint de registro de conta especificado e as solicitações da web `POST` que os clientes enviam para o endpoint de inscrição de conta especificado. Para CloudFront distribuições protegidas, o grupo de regras também inspeciona as respostas que a distribuição envia de volta às solicitações de criação de conta. Para obter uma lista das regras desse grupo de regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes. Você inclui esse grupo de regras em sua web ACL usando uma instrução de referência de grupo de regras gerenciadas. Para obter informações sobre como usar dxxd grupo de regras, consulte Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL.

  > **Note**
  >
  > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

- Detalhes sobre as páginas de registro e criação de conta do seu aplicativo:Você deve fornecer informações sobre as páginas de registro e criação de sua conta ao adicionar o grupo de regras `AWSManagedRulesACFPRuleSet` à sua web ACL. Isso permite que o grupo de regras restrinja o escopo das solicitações inspecionadas e valide adequadamente as solicitações web de criação de conta. A página de registro deve aceitar solicitações `GET` de texto/html. O caminho de criação da conta deve aceitar solicitações `POST`. O grupo de regras do ACFP funciona com nomes de usuário em formato de e-mail. Para ter mais informações, consulte Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL.
- Para CloudFront distribuições protegidas, detalhes sobre como seu aplicativo responde às tentativas de criação de conta — Você fornece detalhes sobre as respostas do seu aplicativo às tentativas de criação de conta, e o grupo de regras do ACFP rastreia e gerencia as tentativas de criação de contas em massa a partir de um único endereço IP ou de uma única sessão de cliente. Para obter informações sobre como configurar essa opção, consulte Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL.
- JavaScript e SDKs de integração de aplicativos móveis — implemente os SDKs móveis AWS WAF JavaScript e os SDKs com sua implementação de ACFP para habilitar o conjunto completo de recursos que o grupo de regras oferece. Muitas das regras do ACFP usam as informações fornecidas pelos SDKs para verificação de clientes em nível de sessão e agregação de comportamento, necessárias para separar o tráfego legítimo de clientes do tráfego de bots. Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes.

Você pode combinar sua implementação de ACFP com o seguinte para ajudar a monitorar, ajustar e personalizar suas proteções.

- Registro e métricas — Você pode monitorar seu tráfego e entender como o grupo de regras gerenciadas do ACFP o afeta, configurando e habilitando registros, a coleta de dados do Amazon Security Lake e as CloudWatch métricas da Amazon para sua ACL web. Os rótulos `AWSManagedRulesACFPRuleSet` adicionados às suas solicitações da web são incluídos nos dados. Para obter informações sobre as opções, consulte Registrando AWS WAF tráfego de ACL da webMonitoramento com a Amazon CloudWatch, e O que é o Amazon Security Lake? .

  Dependendo das suas necessidades e do tráfego que você vê, talvez você queira personalizar sua implementação de `AWSManagedRulesACFPRuleSet`. Por exemplo, talvez você queira excluir algum tráfego da avaliação do ACFP ou alterar a forma como ele lida com algumas das tentativas de fraude na criação de contas que ele identifica, usando AWS WAF recursos como declarações de escopo ou regras de correspondência de rótulos.

- Rótulos e regras de correspondência de rótulos:Para qualquer uma das regras em `AWSManagedRulesACFPRuleSet`, você pode alternar o comportamento de bloqueio para contagem e, em seguida, corresponder com os rótulos adicionados pelas regras. Use essa abordagem para personalizar a forma como você lida com solicitações da web identificadas pelo grupo de regras gerenciadas do ACFP. Para obter mais informações sobre rotulagem e uso de instruções de correspondência de rótulos, consulte Instrução de regra de correspondência de rótulo e AWS WAF rótulos em solicitações da web.
- Solicitações e respostas personalizadas:Você pode adicionar cabeçalhos personalizados às solicitações permitidas e enviar respostas personalizadas para solicitações bloqueadas. Para fazer isso, você combina sua correspondência de rótulos com os recursos personalizados de solicitação e resposta do AWS WAF . Para obter informações sobre como personalizar solicitações e respostas, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Por que você deve usar os SDKs de integração de aplicativos com o ACFP

É altamente recomendável implementar os SDKs de integração de aplicativos para o uso mais eficiente do grupo de regras do ACFP.

- Funcionalidade completa do grupo de regras:A regra `SignalClientHumanInteractivityAbsentLow` do ACFP só funciona com tokens que são preenchidos pelas integrações de aplicativos. Essa regra detecta e gerencia a interatividade humana anormal com a página do aplicativo. Os SDKs de integração de aplicativos podem detectar a interatividade humana normal por meio de movimentos do mouse, pressionamentos de teclas e outras medições. As intersticiais que são enviadas pelas ações da regra CAPTCHA e Challenge não podem fornecer esse tipo de dados.
- Latência reduzida:A regra `AllRequests` do grupo de regras aplica a ação de regra Challenge a qualquer solicitação que ainda não tenha um token de desafio. Quando isso acontece, a solicitação é avaliada pelo grupo de regras duas vezes: uma vez sem o token e uma segunda vez após o token ser adquirido por meio da intersticial da ação Challenge. Não é cobrada nenhuma taxa adicional apenas pelo uso da regra `AllRequests`, mas essa abordagem aumenta o tráfego da web e aumenta a latência da experiência do usuário final. Se você adquirir o token do lado do cliente usando as integrações de aplicativos, antes de enviar a solicitação de criação da conta, o grupo de regras do ACFP avaliará a solicitação uma vez.

Para obter mais informações sobre as capacidades do grupo de regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes. Para obter informações sobre AWS WAF tokens, consulteAWS WAF tokens de solicitação da web. Para mais informações sobre as ações de regra, consulte CAPTCHAe Challenge em AWS WAF.

Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL

Para configurar o grupo de regras gerenciadas do ACFP para reconhecer atividades fraudulentas de criação de conta em seu tráfego da web, você fornece informações sobre como os clientes acessam sua página de registro e enviam solicitações de criação de conta para seu aplicativo. Para CloudFront distribuições protegidas da Amazon, você também fornece informações sobre como seu aplicativo responde às solicitações de criação de contas. Essa configuração é adicional à configuração normal de um grupo de regras gerenciadas.

Para obter a descrição do grupo de regras e a lista de regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

> **Note**
>
> O banco de dados de credenciais roubadas do ACFP contém apenas nomes de usuário em formato de e-mail.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia. Para obter informações básicas sobre como adicionar um grupo de regras gerenciadas à sua web ACL, consulte Como adicionar um grupo de regras gerenciadas a uma web ACL por meio do console.

Siga as práticas recomendadas

Use o grupo de regras do ACFP de acordo com as práticas recomendadas em Práticas recomendadas para mitigação de ameaças inteligentes.

Para usar o grupo de regras **`AWSManagedRulesACFPRuleSet`** em sua web ACL

1. Adicione o grupo de regras AWS gerenciadas `AWSManagedRulesACFPRuleSet` à sua ACL da web e edite as configurações do grupo de regras antes de salvar.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

2. No painel Configuração de grupo de regras, forneça as informações que o grupo de regras do ACFP usa para inspecionar as solicitações de criação de conta.

   a. Em Usar expressão regular em caminhos, ative essa opção se quiser realizar AWS WAF a correspondência de expressões regulares para suas especificações de caminho de página de registro e criação de conta.

      AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.

   b. Em Caminho da página de registro, forneça o caminho do endpoint da página de registro para seu aplicativo. Esta página deve aceitar solicitações `GET` de texto/html. O grupo de regras inspeciona somente solicitações `GET` de HTTP de texto/html para o endpoint da página de registro especificada.

      > **Note**
      >
      > A correspondência para endpoints não diferencia maiúsculas de minúsculas. As especificações para Regex não devem conter o sinalizador `(?-i)`, que desativa a correspondência que não diferencia maiúsculas de minúsculas. As especificações para string devem começar com uma barra `/`.

      Por exemplo, para o URL `https://example.com/web/registration`, é possível fornecer a especificação de caminho da string `/web/registration`. Os caminhos da página de registro que começam com o caminho fornecido por você são considerados uma correspondência. Por exemplo, `/web/registration` corresponde aos caminhos de registro `/web/registration`, `/web/registration/`, `/web/registrationPage` e `/web/registration/thisPage`, mas não corresponde ao caminho `/home/web/registration` ou `/website/registration`.

> **Note**
>
> Certifique-se de que seus usuários finais carreguem a página de registro antes de enviarem uma solicitação de criação de conta. Isso ajuda a garantir que as solicitações de criação de conta enviadas pelo cliente incluam tokens válidos.

c. Para Caminho de criação da conta, forneça o URI em seu site que aceita o preenchimento de novos detalhes de usuário. Este URI deve aceitar solicitações `POST`.

> **Note**
>
> A correspondência para endpoints não diferencia maiúsculas de minúsculas. As especificações para Regex não devem conter o sinalizador `(?-i)`, que desativa a correspondência que não diferencia maiúsculas de minúsculas. As especificações para string devem começar com uma barra `/`.

Por exemplo, para o URL `https://example.com/web/newaccount`, é possível fornecer a especificação de caminho da string `/web/newaccount`. Os caminhos de criação da conta que começam com o caminho fornecido são considerados correspondentes. Por exemplo, `/web/newaccount` corresponde aos caminhos de criação de conta `/web/newaccount`, `/web/newaccount/`, `/web/newaccountPage` e `/web/newaccount/thisPage`, mas não corresponde ao caminho `/home/web/newaccount` ou `/website/newaccount`.

d. Em Inspeção de solicitações, especifique como seu aplicativo aceita tentativas de criação de conta fornecendo o tipo de carga da solicitação e os nomes dos campos no corpo da solicitação em que o nome de usuário, a senha e outros detalhes de criação de conta são fornecidos.

> **Note**
>
> Para os campos de endereço principal e número de telefone, forneça os campos na ordem em que aparecem na carga da solicitação.

Sua especificação dos nomes dos campos depende do tipo de carga.

- Tipo de carga JSON:Especifique os nomes dos campos na sintaxe JSON do ponteiro. Para obter informações sobre a sintaxe do JSON Pointer, consulte a documentação do Internet Engineering Task Force (IETF) JavaScriptObject Notation (JSON) Pointer.

  Por exemplo, para o exemplo de carga JSON a seguir, a especificação do campo de nome de usuário é `/signupform/username` e as especificações do campo de endereço principal são `/signupform/addrp1`, `/signupform/addrp2` e `/signupform/addrp3`.

  ```
  {
      "signupform": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD",
          "addrp1": "PRIMARY_ADDRESS_LINE_1",
          "addrp2": "PRIMARY_ADDRESS_LINE_2",
          "addrp3": "PRIMARY_ADDRESS_LINE_3",
          "phonepcode": "PRIMARY_PHONE_CODE",
          "phonepnumber": "PRIMARY_PHONE_NUMBER"
      }
  }
  ```

- Tipo de carga FORM_ENCODED:Use os nomes dos formulários em HTML.

  Por exemplo, para um formulário HTML com elementos de entrada de usuário e senha chamados `username1` e `password1`, a especificação do campo do nome de usuário é `username1` e a especificação do campo da senha é `password1`.

e. Se você estiver protegendo CloudFront as distribuições da Amazon, em Inspeção de respostas, especifique como seu aplicativo indica sucesso ou falha em suas respostas às tentativas de criação de conta.

> **Note**
>
> A inspeção de resposta do ACFP está disponível somente em ACLs da web que protegem distribuições. CloudFront

Especifique um único componente na resposta de criação da conta que você deseja que o ACFP inspecione. Para os tipos de componentes Body e JSON, é AWS WAF possível inspecionar os primeiros 65.536 bytes (64 KB) do componente.

Forneça seus critérios de inspeção para o tipo de componente, conforme indicado pela interface. Você deve fornecer critérios de sucesso e falha para inspecionar no componente.

Por exemplo, digamos que seu aplicativo indique o status de uma tentativa de criação de conta no código de status da resposta e use `200 OK` para sucesso e `403 Forbidden` ou `401 Unauthorized` para falha. Você definiria o Tipo de componente de inspeção de resposta como Código de status e, na caixa de texto Sucesso, inseriria `200` e, na caixa de texto Falha, inseriria `401` na primeira linha e `403` na segunda.

O grupo de regras do ACFP conta somente as respostas que correspondem aos seus critérios de inspeção de sucesso ou falha. As regras do grupo de regras atuam nos clientes quando eles têm uma taxa de sucesso muito alta entre as respostas contadas, a fim de mitigar as tentativas de criação de contas em massa. Para um comportamento preciso de acordo com as regras do grupo de regras, forneça informações completas sobre tentativas bem-sucedidas e malsucedidas de criação de conta.

Para ver as regras que inspecionam as respostas de criação de contas, procure `VolumetricIPSuccessfulResponse` e `VolumetricSessionSuccessfulResponse` na lista de regras em AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

3. Forneça qualquer configuração adicional desejada para o grupo de regras.

   Você pode limitar ainda mais o escopo das solicitações que o grupo de regras inspeciona adicionando uma instrução de redução de escopo à instrução do grupo de regras gerenciadas. Por exemplo, você pode inspecionar somente solicitações com um argumento de consulta ou cookie específico. O grupo de regras inspecionará somente as solicitações que corresponderem aos critérios em sua instrução de redução de escopo e que foram enviadas para os caminhos de registro e de criação de conta que você especificou na configuração do grupo de regras. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo.

4. Salve suas alterações na web ACL.

Antes de implantar sua implementação de ACFP para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las. Consulte a seção a seguir para obter orientação.

Testando e implantando o ACFP

Esta seção fornece orientação geral para configurar e testar uma implementação de prevenção de AWS WAF fraudes na criação de contas de controle de fraudes (ACFP) para seu site. As etapas específicas que você escolher seguir dependerão de suas necessidades, recursos e solicitações da web que você receber.

Essas informações são adicionais às informações gerais sobre testes e ajustes fornecidas em Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> AWS As regras gerenciadas foram projetadas para proteger você contra ameaças comuns na web. Quando usados de acordo com a documentação, os grupos de regras de regras AWS gerenciadas adicionam outra camada de segurança aos seus aplicativos. No entanto, os grupos de regras de regras AWS gerenciadas não substituem suas responsabilidades de segurança, que são determinadas pelos AWS recursos que você seleciona. Consulte o Modelo de Responsabilidade Compartilhada para garantir que seus recursos AWS estejam devidamente protegidos.

> **Risco de tráfego de produção**
>
> Antes de implantar sua implementação de ACFP para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las.

AWS WAF fornece credenciais de teste que você pode usar para verificar sua configuração de ACFP. No procedimento a seguir, você configurará uma web ACL de teste para usar o grupo de regras gerenciadas do ACFP, configurará uma regra para capturar o rótulo adicionado pelo grupo de regras e, em seguida, executará uma tentativa de criação de conta usando essas credenciais de teste. Você verificará se sua ACL da web gerenciou adequadamente a tentativa verificando as CloudWatch métricas da Amazon para a tentativa de criação da conta.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia.

Para configurar e testar uma implementação de prevenção de AWS WAF fraudes (ACFP) de criação de conta de controle de fraudes

Execute estas etapas primeiro em um ambiente de teste e depois na produção.

1. Adicione o AWS WAF grupo de regras gerenciadas de prevenção de fraudes (ACFP) de criação de contas do Fraud Control no modo de contagem

   > **Note**
   >
   > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

   Adicione o grupo de regras AWS gerenciadas `AWSManagedRulesACFPRuleSet` a uma ACL da web nova ou existente e configure-a para que não altere o comportamento atual da ACL da web. Para obter detalhes sobre as regras e rótulos desse grupo de regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

   - Ao adicionar o grupo de regras gerenciadas, edite-o e faça o seguinte:
     - No painel Configuração de grupo de regras, forneça os detalhes das páginas de registro e criação da conta do seu aplicativo. O grupo de regras do ACFP usa essas informações para monitorar as atividades de login. Para ter mais informações, consulte Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL.
     - No painel Regras, abra o menu suspenso Substituir todas as ações da regra e escolha Count. Com essa configuração, o AWS WAF avalia as solicitações em relação a todas as regras do grupo de regras e conta apenas as correspondências resultantes, sem deixar de adicionar rótulos às solicitações. Para ter mais informações, consulte Substituir ações de regra para um grupo de regras.

       Com essa substituição, você pode monitorar o impacto potencial das regras gerenciadas do ACFP para determinar se deseja adicionar exceções, como exceções para casos de uso internos.

- Posicione o grupo de regras para que ele seja avaliado de acordo com as regras existentes na web ACL, com uma configuração de prioridade que seja numericamente maior do que qualquer regra ou grupo de regras que você já esteja usando. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

  Dessa forma, seu tratamento atual de tráfego não é interrompido. Por exemplo, se você tiver regras que detectem tráfego mal-intencionado, como injeção de SQL ou scripts entre sites, elas continuarão detectando e registrando isso. Como alternativa, se você tiver regras que permitem tráfego não malicioso conhecido, elas podem continuar permitindo esse tráfego, sem que ele seja bloqueado pelo grupo de regras gerenciadas do ACFP. Você pode decidir ajustar a ordem de processamento durante suas atividades de teste e ajuste.

2. Implemente os SDKs de integração de aplicativos

   Integre o AWS WAF JavaScript SDK aos caminhos de registro e criação de conta do seu navegador. AWS WAF também fornece SDKs móveis para integrar dispositivos iOS e Android. Para obter mais informações sobre SDKs de integração, consulte AWS WAF integração de aplicativos clientes. Para obter mais informações sobre essa recomendação, consulte Por que você deve usar os SDKs de integração de aplicativos com o ACFP.

   > **Note**
   >
   > Se você não conseguir usar os SDKs de integração de aplicativos, é possível testar o grupo de regras do ACFP editando-o na sua web ACL e removendo a substituição que você colocou na regra `AllRequests`. Isso ativa a configuração da ação de regra Challenge, para garantir que as solicitações incluam um token de desafio válido. Faça isso primeiro em um ambiente de teste e depois com muito cuidado em seu ambiente de produção. Essa abordagem tem o potencial de bloquear usuários. Por exemplo, se o caminho da página de registro não aceitar solicitações `GET` de texto/html, essa configuração de regra poderá bloquear efetivamente todas as solicitações na página de registro.

3. Ative o registro e as métricas para a ACL da web

   Conforme necessário, configure o registro em log, a coleta de dados do Amazon Security Lake, a amostragem de solicitações e CloudWatch as métricas da Amazon para a ACL da web. Você pode usar essas ferramentas de visibilidade para monitorar a interação do grupo de regras gerenciadas do ACFP com seu tráfego.

- Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.
- Para obter informações sobre o Amazon Security Lake, consulte O que é o Amazon Security Lake? e Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.
- Para obter informações sobre CloudWatch as métricas da Amazon, consulteMonitoramento com a Amazon CloudWatch.
- Para obter informações sobre amostragem de solicitações da web, consulte Visualizar um exemplo de solicitações da web.

4. Associar a web ACL a um recurso

   Se a web ACL ainda não estiver associada a um recurso de teste, associe-a. Para mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

5. Monitore o tráfego e as correspondências de regras do ACFP

   Verifique se o tráfego normal está fluindo e se as regras do grupo de regras gerenciadas do ACFP estão adicionando rótulos às solicitações da web correspondentes. Você pode ver os rótulos nos registros e ver o ACFP e as métricas do rótulo nas métricas da Amazon CloudWatch . Nos logs, as regras que você substituiu para contar no grupo de regras aparecem em `ruleGroupList` com `action` definido para contar e com `overriddenAction` indicando a ação de regra configurada que você substituiu.

6. Teste os recursos de verificação de credenciais do grupo de regras

   Execute uma tentativa de criação de conta com credenciais comprometidas de teste e verifique se o grupo de regras corresponde a elas conforme o esperado.

   a. Acesse a página de registro da conta do seu recurso protegido e tente adicionar uma nova conta. Use o seguinte par AWS WAF de credenciais de teste e insira qualquer teste

      - Usuário: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Senha: `WAF_TEST_CREDENTIAL_PASSWORD`

      Essas credenciais de teste são categorizadas como credenciais comprometidas, e o grupo de regras gerenciadas do ACFP adicionará o rótulo `awswaf:managed:aws:acfp:signal:credential_compromised` à solicitação de criação da conta, que você pode ver nos logs.

b. Nos seus logs de web ACL, procure o rótulo `awswaf:managed:aws:acfp:signal:credential_compromised` no campo `labels` nas entradas de log da solicitação de criação da sua conta de teste. Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.

Depois de verificar se o grupo de regras captura as credenciais comprometidas conforme o esperado, você pode tomar medidas para configurar sua implementação conforme necessário para seu recurso protegido.

7. Para CloudFront distribuições, teste o gerenciamento de tentativas de criação de contas em massa pelo grupo de regras

   Execute esse teste para cada critério de resposta bem-sucedida que você configurou para o grupo de regras do ACFP. Espere pelo menos 30 minutos entre os testes.

   a. Para cada um dos seus critérios de sucesso, identifique uma tentativa de criação de conta que será bem-sucedida com esses critérios de sucesso na resposta. Em seguida, a partir de uma única sessão de cliente, realize pelo menos cinco tentativas bem-sucedidas de criação de conta em menos de 30 minutos. Normalmente, um usuário criaria apenas uma única conta em seu site.

      Após a primeira criação bem-sucedida da conta, a regra `VolumetricSessionSuccessfulResponse` deve começar a se comparar com o resto das respostas de criação da conta, rotulando-as e contando-as, com base na substituição da ação de regra. A regra pode perder a primeira ou duas primeiras devido à latência.

   b. Nos seus logs de web ACL, procure o rótulo `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` no campo `labels` nas entradas de log das solicitações da web de criação da sua conta de teste. Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.

   Esses testes verificam se seus critérios de sucesso correspondem às suas respostas, verificando se as contagens bem-sucedidas agregadas pela regra ultrapassam o limite da regra. Depois de atingir o limite, se você continuar enviando solicitações de criação de conta da mesma sessão, a regra continuará a ser compatível até que a taxa de sucesso caia abaixo do limite. Embora o limite seja excedido, a regra corresponde às tentativas bem-sucedidas ou malsucedidas de criação de conta a partir do endereço da sessão.

8. Personalize o tratamento de solicitações da web do ACFP

   Conforme necessário, adicione suas próprias regras que permitam ou bloqueiem solicitações explicitamente, para alterar a forma como as regras do ACFP lidariam com elas.

   Por exemplo, você pode usar rótulos do ACFP para permitir ou bloquear solicitações ou para personalizar o tratamento de solicitações. Você pode adicionar uma regra de correspondência de rótulos após o grupo de regras gerenciadas do ACFP para filtrar solicitações rotuladas para o tratamento que você deseja aplicar. Após o teste, mantenha as regras do ACFP relacionadas no modo de contagem e mantenha as decisões de tratamento da solicitação em sua regra personalizada. Para ver um exemplo, consulte Exemplo de ACFP: resposta personalizada para credenciais comprometidas.
9. Remova suas regras de teste e ative as configurações do grupo de regras gerenciadas do ACFP

   Dependendo da sua situação, você pode ter decidido deixar algumas regras do ACFP no modo de contagem. Para as regras que você deseja executar conforme configuradas dentro do grupo de regras, desative o modo de contagem na configuração do grupo de regras da web ACL. Ao terminar o teste, você também pode remover as regras de correspondência do rótulo de teste.
10. Monitore e ajuste

    Para ter certeza de que as solicitações da web estão sendo tratadas como você deseja, monitore de perto seu tráfego depois de ativar a funcionalidade do ACFP que você pretende usar. Ajuste o comportamento conforme necessário com a substituição da contagem de regras no grupo de regras e com suas próprias regras.

Depois de terminar de testar a implementação do grupo de regras do ACFP, se você ainda não tiver integrado o AWS WAF JavaScript SDK às páginas de registro e criação de conta do seu navegador, é altamente recomendável que você faça isso. AWS WAF também fornece SDKs móveis para integrar dispositivos iOS e Android. Para obter mais informações sobre SDKs de integração, consulte AWS WAF integração de aplicativos clientes. Para obter mais informações sobre essa recomendação, consulte Por que você deve usar os SDKs de integração de aplicativos com o ACFP.

AWS WAF Exemplos de prevenção de fraudes (ACFP) na criação de contas de controle de fraudes

Esta seção mostra exemplos de configurações que atendem aos casos de uso comuns das implementações de prevenção contra fraude na criação de contas (ACFP) do AWS WAF Fraud Control.

Cada exemplo fornece uma descrição do caso de uso e, em seguida, mostra a solução nas listas JSON para as regras personalizadas configuradas.

> **Note**
>
> Você pode recuperar listas JSON como as mostradas nesses exemplos por meio do console, web ACL, download de JSON ou editor JSON de regras, ou por meio da operação `getWebACL` nas APIs e na interface da linha de comando.

Tópicos

Exemplo de ACFP: configuração simples

A lista JSON a seguir mostra um exemplo de ACL da web com um grupo de regras gerenciadas para prevenção de AWS WAF fraudes na criação de contas (ACFP) do Fraud Control. Observe as configurações adicionais de `CreationPath` e `RegistrationPagePath`, juntamente com o tipo de carga e as informações necessárias para localizar novas informações da conta na carga, a fim de verificá-las. O grupo de regras usa essas informações para monitorar e gerenciar suas solicitações de criação de conta. Esse JSON inclui as configurações geradas automaticamente pela web ACL, como o namespace do rótulo e o URL de integração de aplicativo da web ACL.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
```

```
            "VendorName": "AWS",
            "Name": "AWSManagedRulesACFPRuleSet",
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesACFPRuleSet": {
                  "CreationPath": "/web/signup/submit-registration",
                  "RegistrationPagePath": "/web/signup/registration",
                  "RequestInspection": {
                    "PayloadType": "JSON",
                    "UsernameField": {
                      "Identifier": "/form/username"
                    },
                    "PasswordField": {
                      "Identifier": "/form/password"
                    },
                    "EmailField": {
                      "Identifier": "/form/email"
                    },
                    "PhoneNumberFields": [
                      {
                        "Identifier": "/form/country-code"
                      },
                      {
                        "Identifier": "/form/region-code"
                      },
                      {
                        "Identifier": "/form/phonenumber"
                      }
                    ],
                    "AddressFields": [
                      {
                        "Identifier": "/form/name"
                      },
                      {
                        "Identifier": "/form/street-address"
                      },
                      {
                        "Identifier": "/form/city"
                      },
                      {
                        "Identifier": "/form/state"
                      },
                      {
                        "Identifier": "/form/zipcode"
```

```
                    }
                  ]
                },
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

Exemplo de ACFP: resposta personalizada para credenciais comprometidas

Por padrão, a verificação de credenciais realizada pelo `AWSManagedRulesACFPRuleSet` do grupo de regras trata as credenciais comprometidas rotulando e bloqueando a solicitação. Para obter detalhes sobre o grupo de regras e o comportamento das regras, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

Para informar ao usuário que as credenciais da conta que ele forneceu foram comprometidas, você pode fazer o seguinte:

- Substituir a regra **`SignalCredentialCompromised`** por Count:Isso faz com que a regra conte e rotule somente as solicitações correspondentes.

- Adicione uma regra de correspondência de rótulo com tratamento personalizado:Configure essa regra para corresponder ao rótulo do ACFP e para realizar seu tratamento personalizado.

As listagens de web ACL a seguir mostram o grupo de regras gerenciadas do ACFP do exemplo anterior, com a ação de regra `SignalCredentialCompromised` substituída para contar. Com essa configuração, quando esse grupo de regras avalia qualquer solicitação da web que usa credenciais comprometidas, ele rotula a solicitação, mas não a bloqueia.

Além disso, a web ACL agora tem uma resposta personalizada chamada `aws-waf-credential-compromised` e uma nova regra chamada `AccountSignupCompromisedCredentialsHandling`. A prioridade da regra é uma configuração numérica maior que a do grupo de regras, portanto, ela é executada após o grupo de regras na avaliação da web ACL. A nova regra corresponde a qualquer solicitação com o rótulo de credenciais comprometidas do grupo de regras. Quando a regra encontra uma correspondência, ela aplica a ação Block à solicitação com o corpo de resposta personalizado. O corpo de resposta personalizado fornece informações ao usuário final de que suas credenciais foram comprometidas e propõe uma ação a ser tomada.

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
```

```
            "UsernameField": {
              "Identifier": "/form/username"
            },
            "PasswordField": {
              "Identifier": "/form/password"
            },
            "EmailField": {
              "Identifier": "/form/email"
            },
            "PhoneNumberFields": [
              {
                "Identifier": "/form/country-code"
              },
              {
                "Identifier": "/form/region-code"
              },
              {
                "Identifier": "/form/phonenumber"
              }
            ],
            "AddressFields": [
              {
                "Identifier": "/form/name"
              },
              {
                "Identifier": "/form/street-address"
              },
              {
                "Identifier": "/form/city"
              },
              {
                "Identifier": "/form/state"
              },
              {
                "Identifier": "/form/zipcode"
              }
            ]
          },
          "EnableRegexInPath": false
        }
      }
    ],
    "RuleActionOverrides": [
      {
```

```
            "Name": "SignalCredentialCompromised",
            "ActionToUse": {
              "Count": {}
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  },
  {
    "Name": "AccountSignupCompromisedCredentialsHandling",
    "Priority": 1,
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
      }
    },
    "Action": {
      "Block": {
        "CustomResponse": {
          "ResponseCode": 406,
          "CustomResponseBodyKey": "aws-waf-credential-compromised",
          "ResponseHeaders": [
            {
              "Name": "aws-waf-credential-compromised",
              "Value": "true"
            }
          ]
        }
      }
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AccountSignupCompromisedCredentialsHandling"
```

```
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

Exemplo de ACFP: configuração de inspeção de resposta

A lista JSON a seguir mostra um exemplo de ACL da web com um grupo de regras gerenciado de prevenção de AWS WAF fraudes na criação de contas (ACFP) do Fraud Control configurado para inspecionar as respostas de origem. Observe a configuração da inspeção de resposta, que especifica os códigos de sucesso e status da resposta. Você também pode definir as configurações de sucesso e resposta com base nas correspondências JSON de cabeçalho, corpo e corpo. Esse JSON inclui as configurações geradas automaticamente pela web ACL, como o namespace do rótulo e o URL de integração de aplicativo da web ACL.

> **Note**
>
> A inspeção de resposta ATP está disponível somente em ACLs da web que protegem CloudFront distribuições.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
```

```
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
```

```
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401
                  ]
                }
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
```

```
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
  }
```

AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP)

A apropriação de conta é uma atividade ilegal online na qual um invasor obtém acesso não autorizado à conta de uma pessoa. O invasor pode fazer isso de várias maneiras, como usar credenciais roubadas ou adivinhar a senha da vítima por meio de uma série de tentativas. Quando o invasor obtém acesso, ele pode roubar dinheiro, informações ou serviços da vítima. O invasor pode se passar por vítima para obter acesso a outras contas que a vítima possui ou para obter acesso às contas de outras pessoas ou organizações. Além disso, eles podem tentar alterar a senha do usuário para bloquear a vítima de suas próprias contas.

Você pode monitorar e controlar as tentativas de invasão de contas implementando o recurso de prevenção de controle de AWS WAF fraudes (ATP). AWS WAF oferece esse recurso no grupo de regras AWS gerenciadas `AWSManagedRulesATPRuleSet` e nos SDKs de integração de aplicativos complementares.

O grupo de regras gerenciadas do ATP rotula e gerencia solicitações que podem fazer parte de tentativas maliciosas de apropriação de contas. O grupo de regras faz isso inspecionando as tentativas de login que os clientes enviam para o endpoint de login do seu aplicativo.

- Inspeção de solicitações: o ATP oferece visibilidade e controle sobre tentativas de login anômalas e tentativas de login que usam credenciais roubadas, para evitar apropriações de contas que possam levar a atividades fraudulentas. O ATP verifica as combinações de e-mail e senha em seu banco de dados de credenciais roubadas, que é atualizado regularmente à medida que novas credenciais vazadas são encontradas na dark web. O ATP agrega dados por endereço IP e sessão do cliente, para detectar e bloquear clientes que enviam muitas solicitações de natureza suspeita.
- Inspeção de resposta — Para CloudFront distribuições, além de inspecionar as solicitações de login recebidas, o grupo de regras ATP inspeciona as respostas do seu aplicativo às tentativas de login, para monitorar as taxas de sucesso e falha. Usando essas informações, o ATP pode bloquear temporariamente sessões de clientes ou endereços IP que tenham muitas falhas de login. O AWS WAF executa a inspeção de resposta de forma assíncrona, para que isso não aumente a latência no tráfego da web.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

> **Note**
>
> O recurso do ATP não está disponível para grupos de usuários do Amazon Cognito.

Tópicos

AWS WAF Componentes ATP

Os principais componentes da prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control são os seguintes:

- **`AWSManagedRulesATPRuleSet`**— As regras desse grupo de regras de regras AWS gerenciadas detectam, rotulam e gerenciam vários tipos de atividades de aquisição de contas. O grupo de regras inspeciona as solicitações `POST` HTTP da web que os clientes enviam para o endpoint de login especificado. Para CloudFront distribuições protegidas, o grupo de regras também inspeciona as respostas que a distribuição envia de volta a essas solicitações. Para obter uma lista das regras do grupo de regras, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes. Você inclui esse grupo de regras em sua web ACL usando uma instrução de referência de grupo de regras gerenciadas. Para obter informações sobre como usar dxxd grupo de regras, consulte Adicionando grupos de regras gerenciadas à sua web ACL..

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

- Detalhes sobre a página de login do seu aplicativo:Você deve fornecer informações sobre sua página de login ao adicionar o grupo de regras `AWSManagedRulesATPRuleSet` à sua web ACL. Isso permite que o grupo de regras restrinja o escopo das solicitações inspecionadas e valide adequadamente o uso de credenciais nas solicitações da web. O grupo de regras do ATP funciona com nomes de usuário em formato de e-mail. Para ter mais informações, consulte Adicionando grupos de regras gerenciadas à sua web ACL..
- Para CloudFront distribuições protegidas, detalhes sobre como seu aplicativo responde às tentativas de login — você fornece detalhes sobre as respostas do seu aplicativo às tentativas de login, e o grupo de regras rastreia e gerencia clientes que estão enviando muitas tentativas de login malsucedidas. Para obter informações sobre como configurar essa opção, consulte Adicionando grupos de regras gerenciadas à sua web ACL..
- JavaScript e SDKs de integração de aplicativos móveis — implemente os SDKs móveis AWS WAF JavaScript e os SDKs com sua implementação de ATP para habilitar o conjunto completo de recursos que o grupo de regras oferece. Muitas das regras do ATP usam as informações fornecidas pelos SDKs para verificação de clientes em nível de sessão e agregação de comportamento, necessárias para separar o tráfego legítimo de clientes do tráfego de bots. Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes.

Você pode combinar sua implementação de ATP com o seguinte para ajudar a monitorar, ajustar e personalizar suas proteções.

- Registro e métricas — Você pode monitorar seu tráfego e entender como o grupo de regras gerenciadas do ACFP o afeta, configurando e habilitando registros, a coleta de dados do Amazon Security Lake e as CloudWatch métricas da Amazon para sua ACL web. Os rótulos `AWSManagedRulesATPRuleSet` adicionados às suas solicitações da web são incluídos nos dados. Para obter informações sobre as opções, consulte Registrando AWS WAF tráfego de ACL da webMonitoramento com a Amazon CloudWatch, e O que é o Amazon Security Lake? .

  Dependendo das suas necessidades e do tráfego que você vê, talvez você queira personalizar sua implementação de `AWSManagedRulesATPRuleSet`. Por exemplo, talvez você queira excluir algum tráfego da avaliação do ATP ou alterar a forma como ele lida com algumas das tentativas de

aquisição de conta que ele identifica, usando AWS WAF recursos como instruções de escopo ou regras de correspondência de rótulos.

- Rótulos e regras de correspondência de rótulos:Para qualquer uma das regras em `AWSManagedRulesATPRuleSet`, você pode alternar o comportamento de bloqueio para contagem e, em seguida, corresponder com os rótulos adicionados pelas regras. Use essa abordagem para personalizar a forma como você lida com solicitações da web identificadas pelo grupo de regras gerenciadas do ATP. Para obter mais informações sobre rotulagem e uso de instruções de correspondência de rótulos, consulte Instrução de regra de correspondência de rótulo e AWS WAF rótulos em solicitações da web.
- Solicitações e respostas personalizadas:Você pode adicionar cabeçalhos personalizados às solicitações permitidas e enviar respostas personalizadas para solicitações bloqueadas. Para fazer isso, você combina sua correspondência de rótulos com os recursos personalizados de solicitação e resposta do AWS WAF . Para obter informações sobre como personalizar solicitações e respostas, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Por que você deve usar os SDKs de integração de aplicativos com o ATP

O grupo de regras gerenciadas do ATP exige os tokens de desafio que os SDKs de integração de aplicativos geram. Os tokens permitem o conjunto completo de proteções que o grupo de regras oferece.

É altamente recomendável implementar os SDKs de integração de aplicativos para o uso mais eficiente do grupo de regras do ATP. O script de desafio deve ser executado antes do grupo de regras do ATP para que o grupo de regras se beneficie dos tokens que o script adquire. Isso acontece automaticamente com os SDKs de integração de aplicativos. Se você não conseguir usar os SDKs, poderá configurar alternativamente sua web ACL para que ela execute a ação de regra Challenge ou CAPTCHA em todas as solicitações que serão inspecionadas pelo grupo de regras do ATP. O uso da ação de regra Challenge ou CAPTCHA pode incorrer em taxas adicionais. Para obter detalhes sobre os preços, consulte Preços do AWS WAF.

Capacidades do grupo de regras do ATP que não exigem um token

Quando as solicitações da web não têm um token, o grupo de regras gerenciadas do ATP é capaz de bloquear os seguintes tipos de tráfego:

- Endereços IP únicos que fazem muitas solicitações de login.
- Endereços IP únicos que fazem muitas solicitações de login malsucedidas em um curto espaço de tempo.

- Tentativas de login com traversal de senha, usando o mesmo nome de usuário, mas alterando as senhas.

Capacidades do grupo de regras do ATP que exigem um token

As informações fornecidas no token de desafio expandem os recursos do grupo de regras e da segurança geral do aplicativo cliente.

O token fornece informações do cliente com cada solicitação da web, o que permite que o grupo de regras do ATP separe sessões legítimas de clientes de sessões de clientes mal-comportados, mesmo quando ambas se originam de um único endereço IP. O grupo de regras usa as informações nos tokens para agregar o comportamento da solicitação de sessão do cliente para a detecção e mitigação ajustadas.

Quando o token está disponível em solicitações da web, o grupo de regras do ATP pode detectar e bloquear as seguintes categorias adicionais de clientes no nível da sessão:

- Sessões de clientes que falham no desafio silencioso que os SDKs gerenciam.
- Sessões de clientes que abrangem nomes de usuário ou senhas. Isso também é conhecido como preenchimento de credenciais.
- Sessões de clientes que usam repetidamente credenciais roubadas para fazer login.
- Sessões de clientes que passam muito tempo tentando fazer login.
- Sessões de clientes que fazem muitas solicitações de login. O grupo de regras ATP fornece melhor isolamento do cliente do que a regra AWS WAF baseada em taxa, que pode bloquear clientes por endereço IP. O grupo de regras do ATP também usa um limite inferior.
- Sessões de clientes que fazem muitas solicitações de login malsucedidas em um curto espaço de tempo. Essa funcionalidade está disponível para CloudFront distribuições protegidas da Amazon.

Para obter mais informações sobre as capacidades do grupo de regras, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.

Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes. Para obter informações sobre AWS WAF tokens, consulteAWS WAF tokens de solicitação da web. Para mais informações sobre as ações de regra, consulte CAPTCHAe Challenge em AWS WAF.

Adicionando grupos de regras gerenciadas à sua web ACL.

Para configurar o grupo de regras gerenciadas do ATP para reconhecer atividades de apropriação de conta em seu tráfego da web, você fornece informações sobre como os clientes enviam solicitações de login para seu aplicativo. Para CloudFront distribuições protegidas da Amazon, você também fornece informações sobre como seu aplicativo responde às solicitações de login. Essa configuração é adicional à configuração normal de um grupo de regras gerenciadas.

Para obter a descrição do grupo de regras e a lista de regras, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.

> **Note**
>
> O banco de dados de credenciais roubadas do ATP contém apenas nomes de usuário em formato de e-mail.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia. Para obter informações básicas sobre como adicionar um grupo de regras gerenciadas à sua web ACL, consulte Como adicionar um grupo de regras gerenciadas a uma web ACL por meio do console.

Siga as práticas recomendadas

Use o grupo de regras do ATP de acordo com as práticas recomendadas em Práticas recomendadas para mitigação de ameaças inteligentes.

Para usar o grupo de regras **`AWSManagedRulesATPRuleSet`** em sua web ACL

1. Adicione o grupo de regras AWS gerenciadas `AWSManagedRulesATPRuleSet` à sua ACL da web e edite as configurações do grupo de regras antes de salvar.

   > **Note**
   >
   > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

2. No painel Configuração de grupo de regras, forneça as informações que o grupo de regras do ATP usa para inspecionar as solicitações de login.

a. Em Usar expressão regular em caminhos, ative essa opção se quiser realizar AWS WAF a correspondência de expressões regulares com as especificações do caminho da sua página de login.

   AWS WAF suporta a sintaxe padrão usada pela biblioteca PCRE, `libpcre` com algumas exceções. A biblioteca está documentada em PCRE: Expressões regulares compatíveis com Perl. Para obter informações sobre AWS WAF suporte, consulteCorrespondência de padrões de expressão regular em AWS WAF.

b. Para Caminho de login, forneça o caminho do endpoint de login do seu aplicativo. O grupo de regras inspeciona somente solicitações `POST` de HTTP para seu endpoint de login especificado.

   > **Note**
   >
   > A correspondência para endpoints não diferencia maiúsculas de minúsculas. As especificações para Regex não devem conter o sinalizador `(?-i)`, que desativa a correspondência que não diferencia maiúsculas de minúsculas. As especificações para string devem começar com uma barra `/`.

   Por exemplo, para o URL `https://example.com/web/login`, é possível fornecer a especificação de caminho da string `/web/login`. Os caminhos de login que começam com o caminho fornecido por você são considerados uma correspondência. Por exemplo, `/web/login` corresponde aos caminhos de login `/web/login`, `/web/login/`, `/web/loginPage` e `/web/login/thisPage`, mas não corresponde ao caminho de login `/home/web/login` ou `/website/login`.

c. Para Inspeção de solicitações, especifique como seu aplicativo aceita tentativas de login fornecendo o tipo de carga da solicitação e os nomes dos campos no corpo da solicitação em que o nome de usuário e a senha são fornecidos. Sua especificação dos nomes dos campos depende do tipo de carga.

   - Tipo de carga JSON:Especifique os nomes dos campos na sintaxe JSON do ponteiro. Para obter informações sobre a sintaxe do JSON Pointer, consulte a documentação do Internet Engineering Task Force (IETF) JavaScriptObject Notation (JSON) Pointer.

Por exemplo, para o exemplo de carga JSON a seguir, a especificação do campo de nome de usuário é `/login/username` e a especificação do campo de senha é `/login/password`.

```
{
    "login": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD"
    }
}
```

- Tipo de carga FORM_ENCODED:Use os nomes dos formulários em HTML.

  Por exemplo, para um formulário HTML com elementos de entrada chamados `username1` e `password1`, a especificação do campo do nome de usuário é `username1` e a especificação do campo da senha é `password1`.

d. Se você estiver protegendo CloudFront as distribuições da Amazon, em Inspeção de resposta, especifique como seu aplicativo indica sucesso ou falha em suas respostas às tentativas de login.

> **Note**
>
> A inspeção de resposta ATP está disponível somente em ACLs da web que protegem CloudFront distribuições.

Especifique um único componente na resposta de login que você deseja que o ATP inspecione. Para os tipos de componentes Corpo e JSON, o AWS WAF pode inspecionar os primeiros 65.536 bytes (64 KB) do componente.

Forneça seus critérios de inspeção para o tipo de componente, conforme indicado pela interface. Você deve fornecer critérios de sucesso e falha para inspecionar no componente.

Por exemplo, digamos que seu aplicativo indique o status de uma tentativa de login no código de status da resposta e use `200 OK` para sucesso e `403 Forbidden` ou `401 Unauthorized` para falha. Você definiria o Tipo de componente de inspeção de resposta como Código de status e, na caixa de texto Sucesso, inseriria `200` e, na caixa de texto Falha, inseriria `401` na primeira linha e `403` na segunda.

O grupo de regras do ATP conta somente as respostas que correspondem aos seus critérios de inspeção de sucesso ou falha. As regras do grupo de regras agem sobre os clientes quando eles têm uma taxa de falha muito alta entre as respostas que são contadas. Para um comportamento preciso de acordo com as regras do grupo de regras, forneça informações completas sobre tentativas bem-sucedidas e malsucedidas de login.

Para ver as regras que inspecionam as respostas de login, procure `VolumetricIpFailedLoginResponseHigh` e `VolumetricSessionFailedLoginResponseHigh` na lista de regras em AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.

3. Forneça qualquer configuração adicional desejada para o grupo de regras.

   Você pode limitar ainda mais o escopo das solicitações que o grupo de regras inspeciona adicionando uma instrução de redução de escopo à instrução do grupo de regras gerenciadas. Por exemplo, você pode inspecionar somente solicitações com um argumento de consulta ou cookie específico. O grupo de regras inspecionará somente as solicitações `POST` de HTTP para seu endpoint de login especificado que correspondam aos critérios em sua instrução de escopo. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo.

4. Salve suas alterações na web ACL.

Antes de implantar sua implementação de ATP para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las. Consulte a seção a seguir para obter orientação.

Testando e implantando o ATP

Esta seção fornece orientação geral para configurar e testar uma implementação de prevenção de aquisição de contas (ATP) do Controle de AWS WAF Fraudes em seu site. As etapas específicas que você escolher seguir dependerão de suas necessidades, recursos e solicitações da web que você receber.

Essas informações são adicionais às informações gerais sobre testes e ajustes fornecidas em Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> AWS As regras gerenciadas foram projetadas para proteger você contra ameaças comuns na web. Quando usados de acordo com a documentação, os grupos de regras de regras AWS gerenciadas adicionam outra camada de segurança aos seus aplicativos. No entanto, os grupos de regras de regras AWS gerenciadas não substituem suas responsabilidades de segurança, que são determinadas pelos AWS recursos que você seleciona. Consulte o Modelo de Responsabilidade Compartilhada para garantir que seus recursos AWS estejam devidamente protegidos.

> **Risco de tráfego de produção**
>
> Antes de implantar sua implementação de ATP para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las.

AWS WAF fornece credenciais de teste que você pode usar para verificar sua configuração de ATP. No procedimento a seguir, você configurará uma web ACL de teste para usar o grupo de regras gerenciadas do ATP, configurará uma regra para capturar o rótulo adicionado pelo grupo de regras e, em seguida, executará uma tentativa de login usando essas credenciais de teste. Você verificará se sua ACL da web gerenciou adequadamente a tentativa verificando as CloudWatch métricas da Amazon para a tentativa de login.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia.

Para configurar e testar uma implementação de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control

Execute estas etapas primeiro em um ambiente de teste e depois na produção.

1. Adicione o grupo de regras gerenciadas de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control no modo de contagem

   > **Note**
   >
   > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

   Adicione o grupo de regras AWS gerenciadas `AWSManagedRulesATPRuleSet` a uma ACL da web nova ou existente e configure-a para que não altere o comportamento atual da ACL da web. Para obter detalhes sobre as regras e rótulos desse grupo de regras, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.

   - Ao adicionar o grupo de regras gerenciadas, edite-o e faça o seguinte:
     - No painel Configuração de grupo de regras, forneça os detalhes da página de login do seu aplicativo. O grupo de regras do ATP usa essas informações para monitorar as atividades de login. Para ter mais informações, consulte Adicionando grupos de regras gerenciadas à sua web ACL..
     - No painel Regras, abra o menu suspenso Substituir todas as ações da regra e escolha Count. Com essa configuração, o AWS WAF avalia as solicitações em relação a todas as regras do grupo de regras e conta apenas as correspondências resultantes, sem deixar de adicionar rótulos às solicitações. Para ter mais informações, consulte Substituir ações de regra para um grupo de regras.

       Com essa substituição, você pode monitorar o impacto potencial das regras gerenciadas do ATP para determinar se deseja adicionar exceções, como exceções para casos de uso internos.
   - Posicione o grupo de regras para que ele seja avaliado de acordo com as regras existentes na web ACL, com uma configuração de prioridade que seja numericamente maior do que qualquer regra ou grupo de regras que você já esteja usando. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

     Dessa forma, seu tratamento atual de tráfego não é interrompido. Por exemplo, se você tiver regras que detectem tráfego mal-intencionado, como injeção de SQL ou scripts entre sites, elas continuarão detectando e registrando isso. Como alternativa, se você tiver regras que permitem tráfego não malicioso conhecido, elas podem continuar permitindo esse tráfego,

sem que ele seja bloqueado pelo grupo de regras gerenciadas do ATP. Você pode decidir ajustar a ordem de processamento durante suas atividades de teste e ajuste.

2. Ative o registro e as métricas para a ACL da web

   Conforme necessário, configure o registro, a coleta de dados do Amazon Security Lake, a amostragem de solicitações e CloudWatch as métricas da Amazon para a ACL da web. Você pode usar essas ferramentas de visibilidade para monitorar a interação do grupo de regras gerenciadas do ATP com seu tráfego.

   - Para obter informações sobre como configurar e usar logs, consulte Registrando AWS WAF tráfego de ACL da web.
   - Para obter informações sobre o Amazon Security Lake, consulte O que é o Amazon Security Lake? e Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.
   - Para obter informações sobre CloudWatch as métricas da Amazon, consulteMonitoramento com a Amazon CloudWatch.
   - Para obter informações sobre amostragem de solicitações da web, consulte Visualizar um exemplo de solicitações da web.

3. Associar a web ACL a um recurso

   Se a web ACL ainda não estiver associada a um recurso de teste, associe-a. Para mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

4. Monitore o tráfego e as correspondências de regras do ATP

   Verifique se o tráfego normal está fluindo e se as regras do grupo de regras gerenciadas do ATP estão adicionando rótulos às solicitações da web correspondentes. Você pode ver os rótulos nos registros e ver o ATP e as métricas do rótulo nas métricas da Amazon CloudWatch . Nos logs, as regras que você substituiu para contar no grupo de regras aparecem em `ruleGroupList` com `action` definido para contar e com `overriddenAction` indicando a ação de regra configurada que você substituiu.

5. Teste os recursos de verificação de credenciais do grupo de regras

   Execute uma tentativa de login com credenciais comprometidas de teste e verifique se o grupo de regras corresponde a elas conforme o esperado.

   a. Faça login na página de login do seu recurso protegido usando o seguinte par de credenciais de AWS WAF teste:

- Usuário: `WAF_TEST_CREDENTIAL@wafexample.com`
- Senha: `WAF_TEST_CREDENTIAL_PASSWORD`

Essas credenciais de teste são categorizadas como credenciais comprometidas, e o grupo de regras gerenciadas do ATP adicionará o rótulo `awswaf:managed:aws:atp:signal:credential_compromised` à solicitação de login, que você pode ver nos logs.

b. Nos seus logs de web ACL, procure o rótulo `awswaf:managed:aws:atp:signal:credential_compromised` no campo `labels` nas entradas de log das solicitações da web de login de teste. Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.

Depois de verificar se o grupo de regras captura as credenciais comprometidas conforme o esperado, você pode tomar medidas para configurar sua implementação conforme necessário para seu recurso protegido.

6. Para CloudFront distribuições, teste o gerenciamento de falhas de login do grupo de regras

a. Execute um teste para cada critério de resposta a falhas que você configurou para o grupo de regras do ATP. Espere pelo menos 10 minutos entre os testes.

Para testar um único critério de falha, identifique uma tentativa de login que falhará com esse critério na resposta. Em seguida, a partir de um único endereço IP de cliente, realize pelo menos 10 tentativas de login malsucedidas em menos de 10 minutos.

Após as primeiras seis falhas, a regra de login com falha volumétrica deve começar a corresponder às demais tentativas, rotulando-as e contando-as. A regra pode perder a primeira ou duas primeiras devido à latência.

b. Nos seus logs de web ACL, procure o rótulo `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` no campo `labels` nas entradas de log das solicitações da web de login de teste. Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.

Esses testes verificam se seus critérios de falha correspondem às suas respostas, verificando se as contagens de login com falha ultrapassam os limites da regra

`VolumetricIpFailedLoginResponseHigh`. Depois de atingir os limites, se você continuar enviando solicitações de login do mesmo endereço IP, a regra continuará a corresponder até que a taxa de falhas caia abaixo do limite. Embora os limites sejam excedidos, a regra corresponde aos logins bem-sucedidos ou malsucedidos do endereço IP.

7. Personalize o tratamento de solicitações da web do ATP

   Conforme necessário, adicione suas próprias regras que permitam ou bloqueiem solicitações explicitamente, para alterar a forma como as regras do ATP lidariam com elas.

   Por exemplo, você pode usar rótulos do ATP para permitir ou bloquear solicitações ou para personalizar o tratamento de solicitações. Você pode adicionar uma regra de correspondência de rótulos após o grupo de regras gerenciadas do ATP para filtrar solicitações rotuladas para o tratamento que você deseja aplicar. Após o teste, mantenha as regras do ATP relacionadas no modo de contagem e mantenha as decisões de tratamento da solicitação em sua regra personalizada. Para ver um exemplo, consulte Exemplo de ATP: tratamento personalizado para credenciais ausentes e comprometidas.

8. Remova suas regras de teste e ative as configurações do grupo de regras gerenciadas do ATP

   Dependendo da sua situação, você pode ter decidido deixar algumas regras do ATP no modo de contagem. Para as regras que você deseja executar conforme configuradas dentro do grupo de regras, desative o modo de contagem na configuração do grupo de regras da web ACL. Ao terminar o teste, você também pode remover as regras de correspondência do rótulo de teste.

9. Monitore e ajuste

   Para ter certeza de que as solicitações da web estão sendo tratadas como você deseja, monitore de perto seu tráfego depois de ativar a funcionalidade do ATP que você pretende usar. Ajuste o comportamento conforme necessário com a substituição da contagem de regras no grupo de regras e com suas próprias regras.

Depois de terminar de testar a implementação do grupo de regras do ATP, se você ainda não tiver feito isso, recomendamos que você integre o AWS WAF JavaScript SDK à página de login do seu navegador para aprimorar os recursos de detecção. AWS WAF também fornece SDKs móveis para integrar dispositivos iOS e Android. Para obter mais informações sobre SDKs de integração, consulte AWS WAF integração de aplicativos clientes. Para obter mais informações sobre essa recomendação, consulte Por que você deve usar os SDKs de integração de aplicativos com o ATP.

AWS WAF Exemplos de prevenção de aquisição de contas (ATP) de controle de fraudes

Esta seção mostra exemplos de configurações que atendem aos casos de uso comuns das implementações de prevenção contra apropriação de contas (ATP) do AWS WAF Fraud Control.

Cada exemplo fornece uma descrição do caso de uso e, em seguida, mostra a solução nas listas JSON para as regras personalizadas configuradas.

> **Note**
>
> Você pode recuperar listas JSON como as mostradas nesses exemplos por meio do console, web ACL, download de JSON ou editor JSON de regras, ou por meio da operação `getWebACL` nas APIs e na interface da linha de comando.

Tópicos

- Exemplo de ATP: configuração simples
- Exemplo de ATP: tratamento personalizado para credenciais ausentes e comprometidas
- Exemplo de ATP: configuração de inspeção de resposta

Exemplo de ATP: configuração simples

A lista JSON a seguir mostra um exemplo de ACL da web com um grupo de regras gerenciadas para prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control. Observe a configuração adicional da página de login, que fornece ao grupo de regras as informações necessárias para monitorar e gerenciar suas solicitações de login. Esse JSON inclui as configurações geradas automaticamente pela web ACL, como o namespace do rótulo e o URL de integração de aplicativo da web ACL.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
```

```
            "OverrideAction": {
                "None": {}
            },
            "VisibilityConfig": {
                "SampledRequestsEnabled": true,
                "CloudWatchMetricsEnabled": true,
                "MetricName": "AccountTakeOverValidationRule"
            },
            "Name": "DetectCompromisedUserCredentials",
            "Statement": {
                "ManagedRuleGroupStatement": {
                    "VendorName": "AWS",
                    "Name": "AWSManagedRulesATPRuleSet",
                    "ManagedRuleGroupConfigs": [
                      {
                        "AWSManagedRulesATPRuleSet": {
                          "LoginPath": "/web/login",
                          "RequestInspection": {
                            "PayloadType": "JSON",
                            "UsernameField": {
                              "Identifier": "/form/username"
                            },
                            "PasswordField": {
                              "Identifier": "/form/password"
                            }
                          },
                          "EnableRegexInPath": false
                        }
                      }
                    ]
                }
            }
        }
    ],
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
        "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
```

```
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

Exemplo de ATP: tratamento personalizado para credenciais ausentes e comprometidas

Por padrão, as verificações de credenciais realizadas pelo `AWSManagedRulesATPRuleSet` do grupo de regras tratam as solicitações da web da seguinte forma:

- Credenciais ausentes: identifica e bloqueia a solicitação.
- Credenciais comprometidas:Rotula a solicitação, mas não a bloqueia nem conta.

Para obter detalhes sobre o grupo de regras e o comportamento das regras, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.

Você pode adicionar um tratamento personalizado para solicitações da web que tenham credenciais ausentes ou comprometidas fazendo o seguinte:

- Substituir a regra **`MissingCredential`** por Count:Essa substituição da ação de regra faz com que a regra conte e rotule somente as solicitações correspondentes.
- Adicione uma regra de correspondência de rótulo com tratamento personalizado:Configure essa regra para corresponder aos dois rótulos do ATP e para realizar seu tratamento personalizado. Por exemplo, você pode redirecionar o cliente para sua página de inscrição.

As regra a seguir mostra o grupo de regras gerenciadas do ATP do exemplo anterior, com a ação de regra `MissingCredential` substituída para contar. Isso faz com que a regra aplique seu rótulo às solicitações correspondentes e, em seguida, conte apenas as solicitações, em vez de bloqueá-las.

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
```

```
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

Com essa configuração, quando esse grupo de regras avalia qualquer solicitação da web com credenciais ausentes ou comprometidas, ele rotula a solicitação, mas não a bloqueia.

A regra a seguir tem uma configuração de prioridade que é maior numericamente do que o grupo de regras anterior. O AWS WAF avalia as regras em ordem numérica, começando pela mais baixa, então essa regra será avaliada após a avaliação do grupo de regras. A regra está configurada para corresponder a qualquer um dos rótulos de credenciais e para enviar uma resposta personalizada para solicitações correspondentes.

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

Exemplo de ATP: configuração de inspeção de resposta

A lista JSON a seguir mostra um exemplo de ACL da web com um grupo de regras gerenciado de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control que está configurado para inspecionar as respostas de origem. Observe a configuração da inspeção de resposta, que especifica os códigos de sucesso e status da resposta. Você também pode definir as configurações de sucesso e resposta com base nas correspondências JSON de cabeçalho, corpo e corpo. Esse JSON inclui as configurações geradas automaticamente pela web ACL, como o namespace do rótulo e o URL de integração de aplicativo da web ACL.

> **Note**
>
> A inspeção de resposta ATP está disponível somente em ACLs da web que protegem CloudFront distribuições.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
```

```
                            "LoginPath": "/web/login",
                            "RequestInspection": {
                              "PayloadType": "JSON",
                              "UsernameField": {
                                "Identifier": "/form/username"
                              },
                              "PasswordField": {
                                "Identifier": "/form/password"
                              }
                            },
                            "ResponseInspection": {
                              "StatusCode": {
                                "SuccessCodes": [
                                  200
                                ],
                                "FailureCodes": [
                                  401
                                ]
                              }
                            },
                            "EnableRegexInPath": false
                          }
                        }
                      ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
```

```
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF Controle de bots

Com o Controle de Bots, você pode facilmente monitorar, bloquear ou limitar o intervalo de bots, como extratores, scanners, crawlers, monitores de status e mecanismos de pesquisa. Se você usar o nível de inspeção direcionado do grupo de regras, também poderá desafiar bots que não se identificam, tornando mais difícil e mais caro que bots mal-intencionados operem em seu site. Você pode proteger seus aplicativos usando o grupo de regras gerenciadas do Bot Control sozinho ou em combinação com outros grupos de regras de regras AWS gerenciadas e suas próprias AWS WAF regras personalizadas.

O Controle de Bots inclui um painel de console que mostra quanto do seu tráfego atual vem de bots, com base na amostragem de solicitações. Com o grupo de regras gerenciadas do Controle de Bots adicionado à sua web ACL, você pode agir contra o tráfego de bots e receber informações detalhadas e em tempo real sobre o tráfego comum de bots que chega aos seus aplicativos.

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

O grupo de regras gerenciadas do Controle de Bots fornece um nível de proteção básico e comum que adiciona rótulos aos bots que se identificam automaticamente, verifica os bots geralmente desejáveis e detecta assinaturas de bots de alta confiança. Isso permite monitorar e controlar categorias comuns de tráfego de bots.

O grupo de regras do Controle de Bots também fornece um nível de proteção direcionada que adiciona detecção para bots sofisticados que não se identificam. As proteções direcionadas usam técnicas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots. Além disso, as proteções direcionadas fornecem uma análise opcional automatizada de machine learning das estatísticas de tráfego do site para detectar atividades relacionadas a bots. Quando você ativa o machine learning, o AWS WAF usa estatísticas sobre o tráfego do site, como timestamps, características do navegador e URL anterior visitado, para melhorar o modelo de machine learning do Controle de Bots.

Para obter mais informações sobre grupos de regras gerenciadas pelo Controle de Bots, consulte AWS WAF Grupo de regras do Bot Control.

Quando AWS WAF avalia uma solicitação da web em relação ao grupo de regras gerenciadas do Bot Control, o grupo de regras adiciona rótulos às solicitações que ele detecta como relacionadas ao bot, por exemplo, a categoria do bot e o nome do bot. Você pode comparar esses rótulos em suas próprias AWS WAF regras para personalizar o manuseio. Os rótulos gerados pelo grupo de regras gerenciadas do Bot Control são incluídos nas CloudWatch métricas da Amazon e nos seus registros de ACL na web.

Você também pode usar AWS Firewall Manager AWS WAF políticas para implantar o grupo de regras gerenciadas do Bot Control em seus aplicativos em várias contas que fazem parte da sua organização em AWS Organizations.

AWS WAF Componentes do Bot Control

Os principais componentes de uma implementação do Controle de Bots são os seguintes:

- **`AWSManagedRulesBotControlRuleSet`**:O grupo de regras gerenciadas do Controle de Bots cujas regras detectam e lidam com várias categorias de bots. Esse grupo de regras adiciona rótulos às solicitações da web que ele detecta como tráfego de bots.

  > **Note**
  >
  > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

  O grupo de regras gerenciadas do Controle de Bots fornece dois níveis de proteção que você pode escolher:

  - Comum: detecta uma variedade de bots que se identificam automaticamente, como estruturas de raspagem web, mecanismos de pesquisa e navegadores automatizados. As proteções do Controle de Bots nesse nível identificam bots comuns usando técnicas tradicionais de detecção de bots, como análise estática de dados de solicitações. As regras rotulam o tráfego desses bots e bloqueiam aqueles que eles não podem verificar.
  - Direcionado: inclui proteções de nível comum e adiciona detecção direcionada para bots sofisticados que não se identificam. As proteções direcionadas mitigam a atividade dos bots

usando uma combinação de limitação de intervalo e CAPTCHA e desafios de navegador em segundo plano.

- **`TGT_`**: as regras que fornecem proteção direcionada têm nomes que começam com `TGT_`. Todas as proteções direcionadas usam técnicas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots.
- **`TGT_ML_`**: as regras de proteção direcionada que usam machine learning têm nomes que começam com `TGT_ML_`. Essas regras usam análise automatizada de aprendizado de máquina das estatísticas de tráfego do site para detectar comportamentos anômalos indicativos de atividades de bots distribuídas e coordenadas. AWS WAF analisa estatísticas sobre o tráfego do seu site, como registros de data e hora, características do navegador e URL anterior visitado, para melhorar o modelo de aprendizado de máquina do Bot Control. Os recursos de machine learning são ativados por padrão, mas você pode desativá-los na configuração do grupo de regras. Quando o aprendizado de máquina está desativado, AWS WAF não avalia essas regras.

Para obter detalhes, incluindo informações sobre as regras do grupo de regras, consulte AWS WAF Grupo de regras do Bot Control.

Você inclui esse grupo de regras em sua web ACL usando uma instrução de referência do grupo de regras gerenciadas e indicando o nível de inspeção que você deseja usar. Para o nível direcionado, você também indica se deseja ativar o machine learning. Para obter mais informações sobre como adicionar esse grupo de regras gerenciadas à sua web ACL, consulte Adicionar o grupo de regras gerenciadas do AWS WAF Bot Control à sua ACL da web.

- Painel de controle de bots: o painel de monitoramento de bots para sua web ACL, disponível na guia Controle de bots da web ACL. Use esse painel para monitorar seu tráfego e entender quanto dele vem de vários tipos de bots. Esse pode ser um ponto de partida para personalizar seu gerenciamento de bots, conforme descrito neste tópico. Você também pode usá-lo para verificar suas alterações e monitorar a atividade de vários bots e categorias de bots.
- JavaScript e SDKs de integração de aplicativos móveis — Você deve implementar os SDKs móveis AWS WAF JavaScript e os SDKs se usar o nível de proteção direcionado do grupo de regras do Bot Control. As regras direcionadas usam informações fornecidas pelos SDKs nos tokens do cliente para aprimorar a detecção contra bots maliciosos. Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes.
- Registro e métricas — Você pode monitorar seu tráfego de bots e entender como o grupo de regras gerenciadas do Bot Control avalia e gerencia seu tráfego estudando os dados coletados

para sua ACL da web por AWS WAF logs, Amazon Security Lake e Amazon. CloudWatch Os rótulos que o Bot Control adiciona às suas solicitações da web são incluídos nos dados. Para obter informações sobre essas opções, consulte Registrando AWS WAF tráfego de ACL da webMonitoramento com a Amazon CloudWatch, e O que é o Amazon Security Lake? .

Dependendo das suas necessidades e do tráfego que você vê, talvez você queira personalizar sua implementação do Controle de Bots. A seguir estão algumas das opções mais usadas.

- Instruções de redução de escopo: você pode excluir parte do tráfego das solicitações da web que o grupo de regras gerenciadas do Controle de Bots avalia adicionando uma instrução de redução de escopo dentro da instrução de referência do grupo de regras gerenciadas do Controle de Bots. Uma instrução de redução de escopo pode ser qualquer instrução de regra aninhável. Quando uma solicitação não corresponde à instrução de escopo, AWS WAF avalia-a como não correspondente à declaração de referência do grupo de regras sem avaliá-la em relação ao grupo de regras. Para obter mais informações sobre instruções de redução do escopo, consulte Instruções de redução de escopo.

  Os preços do grupo de regras gerenciadas do Controle de Bots aumentam com o número de solicitações da web que são avaliadas pelo AWS WAF com ele. Você pode ajudar a reduzir esses custos usando uma instrução de escopo para limitar as solicitações que o grupo de regras avalia. Por exemplo, talvez você queira permitir que sua página inicial seja carregada para todos, incluindo bots, e depois aplicar as regras do grupo de regras às solicitações que vão para as APIs do seu aplicativo ou que contêm um tipo específico de conteúdo.
- Regras de correspondência de rótulos e rótulos — Você pode personalizar como o grupo de regras de controle de bots lida com parte do tráfego de bots que ele identifica usando a declaração de regra de correspondência de AWS WAF rótulos. O grupo de regras do Controle de Bots adiciona rótulos às suas solicitações da web. Você pode adicionar regras de correspondência de rótulos após o grupo de regras do Controle de Bots que correspondem aos rótulos do Controle de Bots e aplicar o tratamento de que você precisa. Para obter mais informações sobre rotulagem e uso de instruções de correspondência de rótulos, consulte Instrução de regra de correspondência de rótulo e AWS WAF rótulos em solicitações da web.
- Solicitações e respostas personalizadas — Você pode adicionar cabeçalhos personalizados às solicitações permitidas e enviar respostas personalizadas para solicitações bloqueadas combinando a etiqueta com os recursos AWS WAF personalizados de solicitação e resposta. Para obter informações sobre como personalizar solicitações e respostas, consulte Solicitações e respostas personalizadas da web no AWS WAF.

Por que você deve usar os SDKs de integração de aplicativos com o Controle de Bots

A maioria das proteções direcionadas do grupo de regras gerenciadas do Controle de Bots exige os tokens de desafio que os SDKs de integração de aplicativos geram. As regras que não exigem um token de desafio na solicitação são as proteções de nível comum do Controle de Bots e as regras de machine learning de nível direcionado. Para obter descrições dos níveis de proteção e das regras no grupo de regras, consulte AWS WAF Grupo de regras do Bot Control.

É altamente recomendável implementar os SDKs de integração de aplicativos para o uso mais eficiente do grupo de regras do Controle de Bots. O script de desafio deve ser executado antes do grupo de regras do Controle de Bots para que o grupo de regras se beneficie dos tokens que o script adquire.

- Com os SDKs de integração de aplicativos, o script é executado automaticamente.
- Se você não conseguir usar os SDKs, poderá configurar sua web ACL para que ela execute a ação de regra Challenge ou CAPTCHA em todas as solicitações que serão inspecionadas pelo grupo de regras do Controle de Bots. O uso da ação de regra Challenge ou CAPTCHA pode incorrer em taxas adicionais. Para obter detalhes sobre os preços, consulte Preços do AWS WAF.

Ao implementar os SDKs de integração de aplicativos em seus clientes ou usar uma das ações de regra que executa o script de desafio, você expande os recursos do grupo de regras e da segurança geral do aplicativo cliente.

Os tokens fornecem informações do cliente com cada solicitação da web. Essas informações adicionais permitem que o grupo de regras do Controle de Bots separe sessões legítimas de clientes de sessões de clientes mal-comportados, mesmo quando ambas se originam de um único endereço IP. O grupo de regras usa as informações nos tokens para agregar o comportamento da solicitação de sessão do cliente para a detecção e mitigação ajustadas que o nível de proteção direcionada fornece.

Para obter mais informações sobre os SDKs, consulte AWS WAF integração de aplicativos clientes. Para obter informações sobre AWS WAF tokens, consulteAWS WAF tokens de solicitação da web. Para mais informações sobre as ações de regra, consulte CAPTCHAe Challenge em AWS WAF.

Adicionar o grupo de regras gerenciadas do AWS WAF Bot Control à sua ACL da web

O `AWSManagedRulesBotControlRuleSet` do grupo de regras gerenciadas do Controle de Bots exige configuração adicional para identificar o nível de proteção que você deseja implementar.

Para obter a descrição do grupo de regras e a lista de regras, consulte AWS WAF Grupo de regras do Bot Control.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia. Para obter informações básicas sobre como adicionar um grupo de regras gerenciadas à sua web ACL, consulte Como adicionar um grupo de regras gerenciadas a uma web ACL por meio do console.

Siga as práticas recomendadas

Use o grupo de regras do Controle de Bots de acordo com as práticas recomendadas em Práticas recomendadas para mitigação de ameaças inteligentes.

Para usar o grupo de regras **`AWSManagedRulesBotControlRuleSet`** em sua web ACL

1. Adicione o grupo de regras AWS gerenciadas `AWSManagedRulesBotControlRuleSet` à sua ACL da web. Para obter a descrição completa do grupo de regras, consulte the section called “Grupo de regras do Controle de Bots”.

   > **Note**
   >
   > Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

   Ao adicionar o grupo de regras, edite-o para abrir a página de configuração do grupo de regras.
2. Na página de configuração do grupo de regras, no painel Nível de inspeção, selecione o nível de inspeção que você deseja usar.

   - Comum: detecta uma variedade de bots que se identificam automaticamente, como estruturas de raspagem web, mecanismos de pesquisa e navegadores automatizados. As proteções do Controle de Bots nesse nível identificam bots comuns usando técnicas tradicionais de detecção de bots, como análise estática de dados de solicitações. As regras rotulam o tráfego desses bots e bloqueiam aqueles que eles não podem verificar.
   - Direcionado: inclui proteções de nível comum e adiciona detecção direcionada para bots sofisticados que não se identificam. As proteções direcionadas mitigam a atividade dos bots usando uma combinação de limitação de intervalo e CAPTCHA e desafios de navegador em segundo plano.

- **`TGT_`**: as regras que fornecem proteção direcionada têm nomes que começam com `TGT_`. Todas as proteções direcionadas usam técnicas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots.
- **`TGT_ML_`**: as regras de proteção direcionada que usam machine learning têm nomes que começam com `TGT_ML_`. Essas regras usam análise automatizada de aprendizado de máquina das estatísticas de tráfego do site para detectar comportamentos anômalos indicativos de atividades de bots distribuídas e coordenadas. AWS WAF analisa estatísticas sobre o tráfego do seu site, como registros de data e hora, características do navegador e URL anterior visitado, para melhorar o modelo de aprendizado de máquina do Bot Control. Os recursos de machine learning são ativados por padrão, mas você pode desativá-los na configuração do grupo de regras. Quando o aprendizado de máquina está desativado, AWS WAF não avalia essas regras.

3. Se você estiver usando o nível de proteção direcionado e não quiser usar o aprendizado de máquina (ML) AWS WAF para analisar o tráfego da web em busca de atividades de bots distribuídas e coordenadas, desative a opção de aprendizado de máquina. O machine learning é necessário para as regras do Controle de Bots cujos nomes começam com `TGT_ML_`. Para obter detalhes sobre essas regras, consulte Lista de regras do Controle de Bots.
4. Adicione uma instrução de redução de escopo para o grupo de regras, para conter os custos de seu uso. Uma instrução de redução de escopo restringe o conjunto de solicitações que o grupo de regras inspeciona. Por exemplos de casos de uso, comece com Exemplo de controle de bots: use o controle de bots somente para a página de login e Exemplo de controle de bots: use o controle de bots somente para conteúdo dinâmico.
5. Forneça qualquer configuração adicional necessária para o grupo de regras.
6. Salve suas alterações na web ACL.

Antes de implantar sua implementação de Controle de Bots para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las. Consulte as seções a seguir para obter orientação.

Falsos positivos com o AWS WAF Bot Control

Selecionamos cuidadosamente as regras no grupo de regras gerenciadas do AWS WAF Bot Control para minimizar os falsos positivos. Testamos as regras em relação ao tráfego global e monitoramos seu impacto nas web ACLsde teste. No entanto, ainda é possível obter falsos positivos devido às

mudanças nos padrões de tráfego. Além disso, sabe-se que alguns casos de uso causam falsos positivos e exigirão personalização específica para seu tráfego da web.

As situações em que você pode encontrar falsos positivos incluem o seguinte:

- Os aplicativos móveis geralmente têm agentes de usuário que não são do navegador, que a regra `SignalNonBrowserUserAgent` bloqueia por padrão. Se você espera tráfego de aplicativos móveis ou de qualquer outro tráfego legítimo com agentes de usuário que não sejam do navegador, precisará adicionar uma exceção para permitir isso.
- Você pode confiar em algum tráfego específico de bots para coisas como monitoramento de tempo de atividade, testes de integração ou ferramentas de marketing. Se o Controle de Bots identificar e bloquear o tráfego de bots que você deseja permitir, você precisará alterar o tratamento adicionando suas próprias regras. Embora esse não seja um cenário de falso positivo para todos os clientes, se for para você, você precisará lidar com isso da mesma forma que com um falso positivo.
- O grupo de regras gerenciadas do Bot Control verifica os bots usando os endereços IP de AWS WAF. Se você usa o Controle de Bots e verificou que os bots são roteados por meio de um proxy ou balanceador de carga, pode ser necessário permitir explicitamente que eles usem uma regra personalizada. Para obter mais informações sobre a criação de uma regra personalizada deste tipo, consulte Endereço IP encaminhado.
- Uma regra do Controle de Bots com uma baixa taxa global de falsos positivos pode impactar fortemente dispositivos ou aplicativos específicos. Por exemplo, em testes e validação, talvez não tenhamos observado solicitações de aplicativos com baixos volumes de tráfego ou de navegadores ou dispositivos menos comuns.
- Uma regra do Controle de Bots que tem uma taxa historicamente baixa de falsos positivos pode ter aumentado os falsos positivos para tráfego válido. Isso pode ser devido a novos padrões de tráfego ou recursos de solicitação que surgem com tráfego válido, fazendo com que ele corresponda à regra onde não correspondia antes. Essas mudanças podem ocorrer devido a situações como as seguintes:
  - Detalhes do tráfego que são alterados à medida que o tráfego flui por meio de dispositivos de rede, como balanceadores de carga ou redes de distribuição de conteúdo (CDN).
  - Mudanças emergentes nos dados de tráfego, por exemplo, novos navegadores ou novas versões para navegadores existentes.

Para obter informações sobre como lidar com falsos positivos que você pode obter do grupo de regras gerenciadas do Controle de Bots do AWS WAF , consulte as orientações na seção a seguir, Testando e implantando o AWS WAF Bot Control.

Testando e implantando o AWS WAF Bot Control

Esta seção fornece orientação geral para configurar e testar uma implementação do AWS WAF Bot Control para seu site. As etapas específicas que você escolher seguir dependerão de suas necessidades, recursos e das solicitações da web que você receber.

Essas informações são adicionais às informações gerais sobre testes e ajustes fornecidas em Testando e ajustando suas AWS WAF proteções.

> **Note**
>
> AWS As regras gerenciadas foram projetadas para proteger você contra ameaças comuns na web. Quando usados de acordo com a documentação, os grupos de regras de regras AWS gerenciadas adicionam outra camada de segurança aos seus aplicativos. No entanto, os grupos de regras de regras AWS gerenciadas não substituem suas responsabilidades de segurança, que são determinadas pelos AWS recursos que você seleciona. Consulte o Modelo de Responsabilidade Compartilhada para garantir que seus recursos AWS estejam devidamente protegidos.

> **Risco de tráfego de produção**
>
> Antes de implantar sua implementação de Controle de Bots para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las.

Essa orientação é destinada a usuários que geralmente sabem como criar e gerenciar :web ACLs, regras e grupos de regras do AWS WAF . Esses tópicos são abordados nas seções anteriores deste guia.

Para configurar e testar uma implementação do Controle de Bots

Execute estas etapas primeiro em um ambiente de teste e depois na produção.

1. Adicione o grupo de regras gerenciadas do Controle de Bots

> **Note**
>
> Você paga taxas adicionais ao usar esse grupo de regras gerenciadas. Para obter mais informações, consulte Preços do AWS WAF.

Adicione o grupo de AWS regras gerenciadas `AWSManagedRulesBotControlRuleSet` a uma ACL da Web nova ou existente e configure-a para que ele não altere o comportamento atual da ACL da Web.

- Ao adicionar o grupo de regras gerenciadas, edite-o e faça o seguinte:
  - No painel Nível de inspeção, selecione o nível de inspeção que você deseja usar.
    - Comum: detecta uma variedade de bots que se identificam automaticamente, como estruturas de raspagem web, mecanismos de pesquisa e navegadores automatizados. As proteções do Controle de Bots nesse nível identificam bots comuns usando técnicas tradicionais de detecção de bots, como análise estática de dados de solicitações. As regras rotulam o tráfego desses bots e bloqueiam aqueles que eles não podem verificar.
    - Direcionado: inclui proteções de nível comum e adiciona detecção direcionada para bots sofisticados que não se identificam. As proteções direcionadas mitigam a atividade dos bots usando uma combinação de limitação de intervalo e CAPTCHA e desafios de navegador em segundo plano.
      - **`TGT_`**: as regras que fornecem proteção direcionada têm nomes que começam com `TGT_`. Todas as proteções direcionadas usam técnicas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots.
      - **`TGT_ML_`**: as regras de proteção direcionada que usam machine learning têm nomes que começam com `TGT_ML_`. Essas regras usam análise automatizada de aprendizado de máquina das estatísticas de tráfego do site para detectar comportamentos anômalos indicativos de atividades de bots distribuídas e coordenadas. AWS WAF analisa estatísticas sobre o tráfego do seu site, como registros de data e hora, características do navegador e URL anterior visitado, para melhorar o modelo de aprendizado de máquina do Bot Control. Os recursos de machine learning são ativados por padrão, mas você pode desativá-los na configuração do grupo de regras. Quando o aprendizado de máquina está desativado, AWS WAF não avalia essas regras.

Para obter mais informações sobre essa opção, consulte AWS WAF Grupo de regras do Bot Control.

- No painel Regras, abra o menu suspenso Substituir todas as ações da regra e escolha Count. Com essa configuração, AWS WAF avalia as solicitações em relação a todas as regras do grupo de regras e conta apenas as correspondências resultantes, sem deixar de adicionar rótulos às solicitações. Para ter mais informações, consulte Substituir ações de regra para um grupo de regras.

  Com essa substituição, você pode monitorar o impacto potencial das regras do Controle de Bots no seu tráfego para determinar se deseja adicionar exceções para coisas como casos de uso internos ou bots desejados.

- Posicione o grupo de regras para que ele seja avaliado por último na web ACL, com uma configuração de prioridade numericamente maior do que qualquer outra regra ou grupo de regras que você já esteja usando. Para ter mais informações, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

  Dessa forma, seu tratamento atual de tráfego não é interrompido. Por exemplo, se você tiver regras que detectem tráfego mal-intencionado, como injeção de SQL ou scripts entre sites, elas continuarão detectando e registrando essas solicitações. Como alternativa, se você tiver regras que permitem tráfego não malicioso conhecido, elas podem continuar permitindo esse tráfego, sem que ele seja bloqueado pelo grupo de regras gerenciadas do Controle de Bots. Você pode decidir ajustar a ordem de processamento durante suas atividades de teste e ajuste, mas essa é uma boa maneira de começar.

2. Ative o registro e as métricas para a ACL da web

   Conforme necessário, configure o registro em log, a coleta de dados do Amazon Security Lake, a amostragem de solicitações e CloudWatch as métricas da Amazon para a ACL da web. Você pode usar essas ferramentas de visibilidade para monitorar a interação do grupo de regras gerenciadas do Bot Control com seu tráfego.

   - Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.
   - Para obter informações sobre o Amazon Security Lake, consulte O que é o Amazon Security Lake? e Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.
   - Para obter informações sobre CloudWatch as métricas da Amazon, consulteMonitoramento com a Amazon CloudWatch.

- Para obter informações sobre amostragem de solicitações da web, consulte Visualizar um exemplo de solicitações da web.

3. Associar a web ACL a um recurso

   Se a web ACL ainda não estiver associada a um recurso, associe-a. Para mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

4. Monitore as correspondências de tráfego e regras do Controle de Bots

   Verifique se o tráfego está fluindo e se as regras do grupo de regras gerenciadas do Controle de Bots estão adicionando rótulos às solicitações da web correspondentes. Você pode ver os rótulos nos registros e ver as métricas de bots e rótulos nas CloudWatch métricas da Amazon. Nos logs, as regras que você substituiu para contar no grupo de regras aparecem em `ruleGroupList` com `action` definido para contar e com `overriddenAction` indicando a ação de regra configurada que você substituiu.

   > **Note**
   >
   > O grupo de regras gerenciadas do Controle de Bots verifica os bots usando os endereços IP do AWS WAF. Se você usa o Controle de Bots e verificou que os bots são roteados por meio de um proxy ou balanceador de carga, pode ser necessário permitir explicitamente que eles usem uma regra personalizada. Para obter informações sobre como criar uma regra personalizada, consulte Endereço IP encaminhado. Para obter informações sobre como você pode usar a regra para personalizar o tratamento de solicitações web do Controle de Bots, consulte a próxima etapa.

   Analise cuidadosamente o tratamento de solicitações da web em busca de falsos positivos que você possa precisar mitigar com o tratamento personalizado. Para exemplos de falsos positivos, consulte Falsos positivos com o AWS WAF Bot Control.

5. Personalize o tratamento de solicitações da web do Controle de Bots

   Conforme necessário, adicione suas próprias regras que permitam ou bloqueiem solicitações explicitamente, para alterar a forma como as regras do Controle de Bots lidariam com elas.

   A forma como você faz isso depende do seu caso de uso, mas as soluções a seguir são comuns:

- Permita explicitamente solicitações com uma regra que você adiciona antes do grupo de regras gerenciadas do Controle de Bots. Com isso, as solicitações permitidas nunca chegam ao grupo de regras para avaliação. Isso pode ajudar a conter o custo de usar o grupo de regras gerenciadas do Controle de Bots.
- Exclua solicitações da avaliação do Controle de Bots adicionando uma instrução de escopo abaixo da instrução do grupo de regras gerenciadas do Controle de Bots. Isso funciona da mesma forma que a opção anterior. Isso pode ajudar a conter o custo do uso do grupo de regras gerenciadas do Controle de Bots porque as solicitações que não correspondem à instrução de redução de escopo nunca chegam à avaliação do grupo de regras. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo.

  Para obter exemplos, consulte os seguintes:

  - Excluir o intervalo de IP do gerenciamento de bots
  - Permitir o tráfego de um bot que você controla
- Use rótulos do Controle de Bots no tratamento de solicitações para permitir ou bloquear solicitações. Adicione uma regra de correspondência de rótulo após o grupo de regras gerenciadas do Controle de Bots para filtrar as solicitações rotuladas que você deseja permitir daquelas que deseja bloquear.

  Após o teste, mantenha as regras do Controle de Bots relacionadas no modo de contagem e mantenha as decisões de tratamento da solicitação em sua regra personalizada. Para obter mais informações sobre instruções de correspondência de rótulo, consulte Instrução de regra de correspondência de rótulo.

  Para obter exemplos desse tipo de personalização, consulte o seguinte:

  - Criar uma exceção para um agente de usuário bloqueado
  - Permitir um bot bloqueado específico
  - Bloquear bots verificados

Para obter exemplos adicionais, consulte AWS WAF Exemplos de controle de bots.

6. Conforme necessário, habilite as configurações do grupo de regras gerenciadas do Controle de Bots

   Dependendo da sua situação, você pode ter decidido deixar algumas regras do Controle de Bots no modo de contagem ou com uma substituição de ação diferente. Para as regras que você deseja que sejam executadas conforme configuradas dentro do grupo de regras, habilite a configuração de regra normal. Para fazer isso, edite a instrução do grupo de regras em sua web ACL e faça suas alterações no painel Regras.

AWS WAF Exemplos de controle de bots

Esta seção mostra exemplos de configurações que atendem a uma variedade de casos de uso comuns para implementações do AWS WAF Bot Control.

Cada exemplo fornece uma descrição do caso de uso e, em seguida, mostra a solução nas listas JSON para as regras personalizadas configuradas.

> **Note**
>
> As listas JSON mostradas nesses exemplos foram criadas no console configurando a regra e depois editando-a usando o Editor JSON de regras.

Tópicos

Exemplo de controle de bots: configuração simples

A lista JSON a seguir mostra um exemplo de ACL da web com um grupo de regras gerenciadas pelo AWS WAF Bot Control. Observe a configuração de visibilidade, que faz com que AWS WAF as amostras e métricas de solicitações sejam armazenadas para fins de monitoramento.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
```

```
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

Exemplo de controle de bots: permitir explicitamente bots verificados

AWS WAF O Bot Control não bloqueia bots conhecidos por AWS serem comuns e verificáveis. Quando o Controle de Bots identifica uma solicitação da web como proveniente de um bot verificado, ele adiciona um rótulo que nomeia o bot e um rótulo que indica que é um bot verificado. O Controle de Bots não adiciona nenhum outro rótulo, como rótulos de sinais, para evitar que bots conhecidos como bons sejam bloqueados.

Você pode ter outras AWS WAF regras que bloqueiam bots verificados. Se você quiser garantir que bots verificados sejam permitidos, adicione uma regra personalizada para permiti-los com base nos rótulos do Controle de Bots. Sua nova regra deve ser executada após o grupo de regras gerenciadas do Controle de Bots, para que os rótulos estejam disponíveis para correspondência.

A regra a seguir permite explicitamente bots verificados.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

Exemplo de controle de bots: bloqueie bots verificados

Para bloquear bots verificados, você deve adicionar uma regra para bloqueá-los que seja executada após o grupo de regras gerenciadas do Controle de Bots do AWS WAF . Para fazer isso, identifique os nomes dos bots que você deseja bloquear e use uma instrução de correspondência de rótulo para

identificá-los e bloqueá-los. Se você quiser apenas bloquear todos os bots verificados, você pode omitir a correspondência com o rótulo `bot:name:`.

A regra a seguir bloqueia somente o bot verificado `bingbot`. Essa regra deve ser executada após o grupo de regras gerenciadas do Controle de Bots.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

A regra a seguir bloqueia todos os bots verificados.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
```

```
    "Action": {
      "Block": {}
    }
}
```

Exemplo de controle de bots: permitir que um bot específico seja bloqueado

É possível que um bot seja bloqueado por mais de uma das regras do Controle de Bots. Execute o procedimento a seguir para cada regra de bloqueio.

Se uma AWS WAF regra de controle de bots estiver bloqueando um bot que você não deseja bloquear, faça o seguinte:

1. Identifique a regra do Controle de Bots que está bloqueando o bot verificando os logs. A regra de bloqueio será especificada nos logs nos campos cujos nomes começam com `terminatingRule`. Para obter mais informações sobre os logs de ACL, consulte Registrando AWS WAF tráfego de ACL da web. Observe o rótulo que a regra adiciona às solicitações.
2. Na sua web ACL, substitua a ação da regra de bloqueio para contar. Para fazer isso no console, edite a regra do grupo de regras na web ACL e escolha uma substituição de ação de regra de Count para a regra. Isso garante que o bot não seja bloqueado pela regra, mas a regra ainda aplicará seu rótulo às solicitações correspondentes.
3. Adicione uma regra de correspondência de rótulos à sua web ACL depois do grupo de regras gerenciadas do Controle de Bots. Configure a regra para corresponder ao rótulo da regra substituída e bloquear todas as solicitações correspondentes, exceto o bot que você não deseja bloquear.

   Sua web ACL agora está configurada para que o bot que você deseja permitir não seja mais bloqueado pela regra de bloqueio que você identificou por meio dos logs.

Verifique o tráfego e seus logs novamente, para ter certeza de que o bot está sendo autorizado a passar. Caso contrário, execute o procedimento acima novamente.

Por exemplo, suponha que você queira bloquear todos os bots de monitoramento, exceto o `pingdom`. Nesse caso, você substitui a regra `CategoryMonitoring` para contar e, em seguida, escreve uma regra para bloquear todos os bots de monitoramento, exceto aqueles com o rótulo do nome do bot `pingdom`.

A regra a seguir usa o grupo de regras gerenciadas do Controle de Bots, mas substitui a ação da regra para `CategoryMonitoring` para contar. A regra de monitoramento de categorias aplica seus

rótulos normalmente às solicitações correspondentes, mas só os conta em vez de realizar sua ação usual de bloqueio.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

A regra a seguir corresponde ao rótulo de monitoramento de categoria que a regra `CategoryMonitoring` anterior adiciona às solicitações da web correspondentes. Entre as solicitações de monitoramento de categorias, essa regra bloqueia todas, exceto aquelas que têm um rótulo para o nome do bot `pingdom`.

A regra a seguir deve ser executada após o grupo de regras gerenciadas anterior do Controle de Bots na ordem de processamento da web ACL.

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Exemplo de controle de bots: criar uma exceção para um agente de usuário bloqueado

Se o tráfego de alguns agentes de usuário que não são do navegador estiver sendo bloqueado erroneamente, você pode criar uma exceção definindo a regra de controle de AWS WAF bots ofensiva como Count e, em seguida, combinando `SignalNonBrowserUserAgent` a rotulagem da regra com seus critérios de exceção.

> **Note**
>
> Os aplicativos móveis geralmente têm agentes de usuário que não são do navegador, que a regra `SignalNonBrowserUserAgent` bloqueia por padrão.

A regra a seguir usa o grupo de regras gerenciadas do Controle de Bots, mas substitui a ação da regra para `SignalNonBrowserUserAgent` para contar. A regra de sinal aplica seus rótulos normalmente às solicitações correspondentes, mas só os conta em vez de realizar sua ação usual de bloqueio.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
```

```
}
```

A regra a seguir corresponde ao rótulo de sinal que o `SignalNonBrowserUserAgent` da regra do Controle de Bots adiciona a suas solicitações da web correspondentes. Entre as solicitações de sinal, essa regra bloqueia todas, exceto aquelas que têm o agente de usuário que queremos permitir.

A regra a seguir deve ser executada após o grupo de regras gerenciadas anterior do Controle de Bots na ordem de processamento da web ACL.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ]
                }
              }
            }
          }
        ]
      }
```

```
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
}
```

Exemplo de controle de bots: use o controle de bots somente para a página de login

O exemplo a seguir usa uma declaração de escopo reduzido para aplicar o AWS WAF Bot Control somente ao tráfego que chega à página de login de um site, que é identificado pelo caminho do URI. `login` O caminho do URI para sua página de login pode ser diferente do exemplo, dependendo do aplicativo e do ambiente.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
```

```
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

Exemplo de controle de bots: use o controle de bots somente para conteúdo dinâmico

Este exemplo usa uma declaração de escopo reduzido para aplicar o AWS WAF Bot Control somente ao conteúdo dinâmico.

A instrução de redução de escopo exclui o conteúdo estático negando os resultados da correspondência para um conjunto de padrões regex:

- O conjunto de padrões regex é configurado para corresponder às extensões do conteúdo estático. Por exemplo, a especificação do conjunto de padrões regex pode ser `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`. Para obter informações sobre como gerenciar conjuntos e instruções de padrões de regex, consulte Instrução de regra de correspondência do conjunto de padrões de regex.
- Na instrução de redução de escopo, excluímos o conteúdo estático correspondente aninhando a instrução regex de definição de padrão dentro de uma instrução `NOT`. Para obter mais informações sobre a instrução `NOT`, consulte Instrução de regra do NOT.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
```

```
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

Exemplo de controle de bots: exclua o intervalo de IP do gerenciamento de bots

Se você quiser excluir um subconjunto do tráfego da web do gerenciamento do AWS WAF Bot Control e puder identificar esse subconjunto usando uma declaração de regra, exclua-o adicionando uma declaração de escopo reduzido à sua declaração de grupo de regras gerenciadas pelo Bot Control.

A regra a seguir executa o gerenciamento normal de bots do Controle de Bots em todo o tráfego da web, exceto para solicitações da web provenientes de um intervalo específico de endereços IP.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

Exemplo de controle de bots: permita o tráfego de um bot que você controla

Você pode configurar alguns bots de monitoramento de sites e bots personalizados para enviar cabeçalhos personalizados. Se você quiser permitir o tráfego desses tipos de bots, você pode configurá-los para adicionar um segredo compartilhado em um cabeçalho. Em seguida, você pode

excluir as mensagens que têm o cabeçalho adicionando uma declaração de escopo reduzido à declaração do grupo de regras gerenciadas pelo AWS WAF Bot Control.

O exemplo de regra a seguir exclui o tráfego com um cabeçalho secreto da inspeção do Controle de Bots.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
```

```
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

Exemplo de controle de bots: nível de inspeção direcionado

Para um nível aprimorado de proteção, você pode ativar o nível de inspeção direcionado em seu grupo de regras gerenciadas pelo AWS WAF Bot Control.

No exemplo a seguir, os recursos de aprendizado de máquina estão habilitados. Você pode optar por não participar desse comportamento configurando `EnableMachineLearning` como`false`.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

Exemplo de controle de bots: use duas declarações para limitar o uso do nível de inspeção desejado

Como uma otimização de custos, você pode usar duas declarações de grupo de regras gerenciadas pelo AWS WAF Bot Control em sua ACL da web, com níveis de inspeção e escopo separados. Por exemplo, você pode definir o escopo da declaração de nível de inspeção direcionado somente para endpoints de aplicativos mais sensíveis.

As duas declarações no exemplo a seguir têm escopo mutuamente exclusivo. Sem essa configuração, uma solicitação poderia resultar em duas avaliações cobradas.

> **Note**
>
> Não `AWSManagedRulesBotControlRuleSet` há suporte para referências a várias declarações no editor visual do console. Em vez disso, use o editor JSON.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
             "ManagedRuleGroupConfigs": [
               {
                 "AWSManagedRulesBotControlRuleSet": {
                   "InspectionLevel": "COMMON"
                 }
               }
             ],
```

```
            "RuleActionOverrides": [],
            "ExcludedRules": []
         },
         "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Common"
          },
          "ScopeDownStatement": {
             "NotStatement": {
               "Statement": {
                 "ByteMatchStatement": {
                   "FieldToMatch": {
                     "UriPath": {}
                   },
                   "PositionalConstraint": "STARTS_WITH",
                   "SearchString": "/sensitive-endpoint",
                   "TextTransformations": [
                     {
                       "Type": "NONE",
                       "Priority": 0
                     }
                   ]
                 }
               }
             }
           }
       },
       {
        "Name": "AWS-AWSBotControl-Targeted",
        "Priority": 6,
        "Statement": {
           "ManagedRuleGroupStatement": {
              "VendorName": "AWS",
              "Name": "AWSManagedRulesBotControlRuleSet",
              "ManagedRuleGroupConfigs": [
                {
                  "AWSManagedRulesBotControlRuleSet": {
                    "InspectionLevel": "TARGETED",
                    "EnableMachineLearning": true
                  }
                }
              ],
```

```
            "RuleActionOverrides": [],
            "ExcludedRules": []
          },
          "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Targeted"
           },
           "ScopeDownStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "UriPath": {}
                  },
                  "PositionalConstraint": "STARTS_WITH",
                  "SearchString": "/sensitive-endpoint",
                  "TextTransformations": [
                    {
                      "Type": "NONE",
                      "Priority": 0
                    }
                  ]
                }
              }
            }
        }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF integração de aplicativos clientes

Use APIs de integração de aplicativos AWS WAF clientes para unir as proteções do lado do cliente às proteções AWS de ACL da Web do lado do servidor, para ajudar a verificar se os aplicativos cliente que enviam solicitações da Web aos recursos protegidos são os clientes pretendidos e se os usuários finais são seres humanos.

Use as integrações do cliente para gerenciar desafios silenciosos do navegador e quebra-cabeças CAPTCHA, obter tokens com provas de respostas bem-sucedidas do navegador e do usuário final e incluir esses tokens nas solicitações aos seus endpoints protegidos. Para obter informações gerais sobre AWS WAF tokens, consulteAWS WAF tokens de solicitação da web.

Combine suas integrações de clientes com proteções de web ACL que exigem tokens válidos para acessar seus recursos. Você pode usar grupos de regras que verificam e monitoram os tokens de desafio, como os listados na próxima seção, em Integração de ameaças inteligentes e regras gerenciadas da AWS, e você pode usar as ações de regras CAPTCHA e Challenge para verificar, conforme descrito em CAPTCHAe Challenge em AWS WAF.

AWS WAF fornece dois níveis de integração para JavaScript aplicativos e um para aplicativos móveis:

- Integração inteligente de ameaças — verifique o aplicativo do cliente e forneça aquisição e gerenciamento de AWS tokens. Isso é semelhante à funcionalidade fornecida pela ação da AWS WAF Challenge regra. Essa funcionalidade integra totalmente seu aplicativo cliente ao grupo de regras gerenciadas `AWSManagedRulesACFPRuleSet`, ao grupo de regras gerenciadas `AWSManagedRulesATPRuleSet` e ao nível de proteção direcionada do grupo de regras gerenciadas `AWSManagedRulesBotControlRuleSet`.

  As APIs inteligentes de integração de ameaças usam o desafio do navegador AWS WAF silencioso para ajudar a garantir que as tentativas de login e outras chamadas para seu recurso protegido sejam permitidas somente após o cliente adquirir um token válido. As APIs gerenciam a autorização de token para as sessões do aplicativo cliente e coletam informações sobre o cliente para ajudar a determinar se ele está sendo operado por um bot ou por um ser humano.

  > **Note**
  >
  > Isso está disponível para JavaScript e para aplicativos móveis Android e iOS.

- Integração com CAPTCHA: verifique os usuários finais com o quebra-cabeça CAPTCHA personalizado que você gerencia em seu aplicativo. Isso é semelhante à funcionalidade fornecida pela ação da AWS WAF CAPTCHA regra, mas com controle adicional sobre o posicionamento e o comportamento do quebra-cabeça.

  Essa integração aproveita a integração JavaScript inteligente de ameaças para executar desafios silenciosos e fornecer AWS WAF tokens para a página do cliente.

> **Note**
>
> Isso está disponível para JavaScript aplicativos.

Tópicos

Integração de ameaças inteligentes e regras gerenciadas da AWS

As APIs de integração inteligente de ameaças funcionam com web ACLsque usam os grupos de regras de ameaças inteligentes para permitir a funcionalidade completa desses grupos de regras gerenciadas avançadas.

- AWS WAF Grupo de regras gerenciadas para prevenção de fraudes (ACFP) para criação de contas de controle de fraudes. `AWSManagedRulesACFPRuleSet`

  A fraude na criação de conta é uma atividade online ilegal na qual um invasor cria contas inválidas em seu aplicativo para fins como receber bônus de inscrição ou se passar por alguém. O grupo de regras gerenciadas do ACFP fornece regras para bloquear, rotular e gerenciar solicitações que podem fazer parte de tentativas fraudulentas de criação de conta. As APIs permitem a verificação refinada do navegador do cliente e as informações de interatividade humana que as regras do ACFP usam para separar o tráfego válido do cliente do tráfego malicioso.

  Para ter mais informações, consulte AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes e AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP).
- AWS WAF Grupo de regras gerenciadas para prevenção de aquisição de contas (ATP) para controle de fraudes. `AWSManagedRulesATPRuleSet`

  A apropriação de conta é uma atividade ilegal online na qual um invasor obtém acesso não autorizado à conta de uma pessoa. O grupo de regras gerenciadas do ATP fornece regras para bloquear, rotular e gerenciar solicitações que podem fazer parte de tentativas maliciosas de

apropriação de contas. As APIs permitem a verificação refinada do cliente e a agregação de comportamento que as regras do ATP usam para separar o tráfego válido do cliente do tráfego malicioso.

Para ter mais informações, consulte AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes e AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP).

- Nível de proteção direcionado do grupo de regras gerenciadas do AWS WAF Bot Control`AWSManagedRulesBotControlRuleSet`.

  Os bots vão desde os que se identificam automaticamente e são úteis, como a maioria dos mecanismos de pesquisa e crawlers, até bots maliciosos que operam contra seu site e não se identificam. O grupo de regras gerenciadas do Controle de Bots fornece regras para monitorar, rotular e gerenciar a atividade de bots em seu tráfego da web. Quando você usa o nível de proteção direcionada desse grupo de regras, as regras direcionadas usam as informações da sessão do cliente que as APIs fornecem para detectar melhor os bots mal-intencionados.

  Para ter mais informações, consulte AWS WAF Grupo de regras do Bot Control e AWS WAF Controle de bots.

Para adicionar um desses grupos de regras gerenciadas à sua web ACL, consulte os procedimentos Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL, Adicionando grupos de regras gerenciadas à sua web ACL. e Adicionar o grupo de regras gerenciadas do AWS WAF Bot Control à sua ACL da web.

> **Note**
>
> Atualmente, os grupos de regras gerenciadas não bloqueiam solicitações sem tokens. Para bloquear solicitações sem tokens, depois de implementar suas APIs de integração de aplicativos, siga as orientações em Bloqueio de solicitações que não têm um AWS WAF token válido.

Acessando as APIs de integração de aplicativos AWS WAF clientes

As APIs de JavaScript integração estão geralmente disponíveis e você pode usá-las em seus navegadores e outros dispositivos que são JavaScript executados.

AWS WAF oferece SDKs personalizados de integração inteligente de ameaças para aplicativos móveis Android e iOS.

- Para aplicativos móveis Android, os AWS WAF SDKs funcionam com a API Android versão 23 (Android versão 6) e versões posteriores. Para obter informações sobre as versões do Android, consulte as Notas de lançamento da plataforma de SDK.
- Para aplicativos móveis iOS, AWS WAF os SDKs funcionam para iOS versão 13 e posterior. Para obter informações sobre as versões do iOS, consulte as Notas de versão do iOS e iPadOS.

Para acessar as APIs de integração por meio do console

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. Escolha Integração de aplicativos no painel de navegação e, em seguida, escolha a guia na qual você está interessado.

   - A integração inteligente de ameaças está disponível para JavaScript aplicativos móveis.

     A guia contém o seguinte:

     - Uma lista das web ACLshabilitadas para a integração de aplicativos de ameaças inteligentes. A lista inclui cada web ACL que usa o grupo de regras gerenciadas `AWSManagedRulesACFPRuleSet`, o grupo de regras gerenciadas `AWSManagedRulesATPRuleSet` ou o nível de proteção direcionada do grupo de regras gerenciadas `AWSManagedRulesBotControlRuleSet`. Ao implementar as APIs de ameaças inteligentes, você usa o URL de integração da web ACL com a qual deseja se integrar.
     - As APIs às quais você tem acesso. As JavaScript APIs estão sempre disponíveis. Para acessar os SDKs móveis, entre em contato com o suporte em Entrar em contato com a AWS.
   - A integração CAPTCHA está disponível para JavaScript aplicativos.

     A guia contém o seguinte:

     - O URL de integração para uso em sua integração.
     - As chaves de API que você criou para os domínios do seu aplicativo cliente. Seu uso da API CAPTCHA requer uma chave de API criptografada que dê aos clientes o direito de acessar o AWS WAF CAPTCHA de seus domínios. Para cada cliente com o qual você se integra,

use uma chave de API que contenha o domínio do cliente. Para obter mais informações sobre esses requisitos e sobre o gerenciamento dessas chaves, consulte Gerenciamento de chaves de API para a API JS CAPTCHA.

AWS WAF JavaScript integrações

Você pode usar as APIs de JavaScript integração para implementar integrações de AWS WAF aplicativos em seus navegadores e outros dispositivos que são executados. JavaScript

Os quebra-cabeças de CAPTCHA e os desafios silenciosos só podem ser executados quando os navegadores estão acessando endpoints HTTPS. Os clientes do navegador devem estar sendo executados em contextos seguros para adquirir tokens.

- As APIs de ameaças inteligentes permitem que você gerencie a autorização de tokens por meio de um desafio silencioso do navegador do lado do cliente e inclua os tokens nas solicitações que você envia aos seus recursos protegidos.
- A API de integração CAPTCHA se soma às APIs de ameaças inteligentes e permite que você personalize o posicionamento e as características do quebra-cabeça CAPTCHA em seus aplicativos clientes. Essa API aproveita as APIs de ameaças inteligentes para adquirir tokens do AWS WAF para uso na página após o usuário final concluir com êxito o quebra-cabeça CAPTCHA.

Ao usar essas integrações, você garante que as chamadas de procedimento remoto feitas pelo seu cliente contenham um token válido. Quando essas APIs de integração estão implementadas nas páginas do seu aplicativo, você pode implementar regras de mitigação na sua web ACL, como bloquear solicitações que não contêm um token válido. Você também pode implementar regras que imponham o uso dos tokens que seus aplicativos clientes obtêm, usando as ações Challenge ou CAPTCHA em suas regras.

A lista a seguir mostra os componentes básicos de uma implementação típica das APIs de ameaças inteligentes em uma página de aplicativo da web.

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
```

```
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

A API de integração CAPTCHA permite que você personalize a experiência de quebra-cabeça CAPTCHA de seus usuários finais. A integração CAPTCHA aproveita a integração JavaScript inteligente de ameaças, para verificação do navegador e gerenciamento de tokens, além de adicionar uma função para configurar e renderizar o quebra-cabeça do CAPTCHA.

A lista a seguir mostra os componentes básicos de uma implementação típica da JavaScript API CAPTCHA em uma página de aplicativo web.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>
```

```
<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Tópicos

- Fornecimento de domínios para uso nos tokens
- Usando a JavaScript API com políticas de segurança de conteúdo
- Usando a JavaScript API de ameaças inteligentes
- Usando a API CAPTCHA JavaScript

Fornecimento de domínios para uso nos tokens

Por padrão, ao AWS WAF criar um token, ele usa o domínio host do recurso associado à Web ACL. Você pode fornecer domínios adicionais para os tokens AWS WAF criados para as JavaScript APIs. Para fazer isso, configure a variável global `window.awsWafCookieDomainList`, com um ou mais domínios de token.

Ao AWS WAF criar um token, ele usa o domínio mais adequado e mais curto dentre a combinação dos domínios `window.awsWafCookieDomainList` e do domínio do host do recurso associado à ACL da web.

Exemplo de configurações:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

Você não pode usar sufixos públicos nessa lista. Por exemplo, você não pode usar `gov.au` ou `co.uk` como domínios de token na lista.

Os domínios que você especifica nessa lista devem ser compatíveis com seus outros domínios e configurações de domínio:

- Os domínios devem ser aqueles que AWS WAF aceitarão, com base no domínio do host protegido e na lista de domínios do token configurada para a Web ACL. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

- Se você usa a API JavaScript CAPTCHA, pelo menos um domínio em sua chave de API CAPTCHA deve corresponder exatamente a um dos domínios de token `window.awsWafCookieDomainList` ou deve ser o domínio ápice de um desses domínios de token.

  Por exemplo, para o domínio do token `mySubdomain.myApex.com`, a chave de API `mySubdomain.myApex.com` é uma correspondência exata e a chave de API `myApex.com` é o domínio apex. Qualquer chave corresponde ao domínio do token.

  Para obter mais informações sobre as chaves de API, consulte Gerenciamento de chaves de API para a API JS CAPTCHA.

Se você usar o grupo de regras gerenciadas `AWSManagedRulesACFPRuleSet`, poderá configurar um domínio que corresponda ao do caminho de criação da conta que você forneceu para a configuração do grupo de regras. Para obter mais informações sobre essa configuração, consulte Adicionando o grupo de regras gerenciadas do ACFP à sua web ACL.

Se você usar o grupo de regras gerenciadas `AWSManagedRulesATPRuleSet`, poderá configurar um domínio que corresponda ao do caminho de login que você forneceu para a configuração do grupo de regras. Para obter mais informações sobre essa configuração, consulte Adicionando grupos de regras gerenciadas à sua web ACL..

Usando a JavaScript API com políticas de segurança de conteúdo

Se você aplicar políticas de segurança de conteúdo (CSP) aos seus recursos, para que sua JavaScript implementação funcione, você precisa colocar o domínio AWS WAF apex na lista de permissões. `awswaf.com` Os JavaScript SDKs fazem chamadas para AWS WAF endpoints diferentes, portanto, a lista de permissões desse domínio fornece as permissões de que os SDKs precisam para operar.

Veja a seguir um exemplo de configuração para permitir o domínio AWS WAF apex na lista de permissões:

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

Se você tentar usar os JavaScript SDKs com recursos que usam CSP e não tiver permitido o AWS WAF domínio, você receberá erros como os seguintes:

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

Usando a JavaScript API de ameaças inteligentes

As APIs de ameaças inteligentes fornecem operações para executar desafios silenciosos no navegador do usuário e para lidar com os AWS WAF tokens que comprovam o sucesso do desafio e das respostas CAPTCHA.

Implemente a JavaScript integração primeiro em um ambiente de teste e depois na produção. Para obter orientações adicionais sobre codificação, consulte as seções a seguir.

Para usar as APIs de ameaças inteligentes

1. Instale as APIs

   Se você usar a API CAPTCHA, você poderá ignorar esta etapa. Quando você instala a API CAPTCHA, o script instala automaticamente as APIs de ameaças inteligentes.

   a. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   b. No painel de navegação, escolha Integração de aplicativos. Na página Integração de aplicativos, você pode ver as opções com guias.

   c. Selecione Integração de ameaças inteligentes

   d. Na guia, selecione a web ACL com a qual você deseja se integrar. A lista de web ACLsinclui apenas web ACLsque usam o grupo de regras gerenciadas `AWSManagedRulesACFPRuleSet`, o grupo de regras gerenciadas `AWSManagedRulesATPRuleSet` ou o nível de proteção direcionada do grupo de regras gerenciadas `AWSManagedRulesBotControlRuleSet`.

   e. Abra o painel JavaScript SDK e copie a tag do script para usar em sua integração.

   f. No código da página do aplicativo, na seção `<head>`, insira a tag de script que você copiou para a web ACL. Essa inclusão faz com que seu aplicativo cliente recupere automaticamente um token em segundo plano no carregamento da página.

   ```
   <head>
       <script type="text/javascript" src="Web ACL integration URL/challenge.js”
    defer></script>
   ```

```
<head>
```

Essa lista `<script>` é configurada com o recurso `defer`, mas você pode alterar a configuração para `async` se quiser um comportamento diferente para sua página.

2. (Opcional) Adicionar configuração de domínio para os tokens do cliente — Por padrão, ao AWS WAF criar um token, ele usa o domínio host do recurso associado à ACL da web. Para fornecer domínios adicionais para as JavaScript APIs, siga as orientações em. Fornecimento de domínios para uso nos tokens
3. Codificar sua integração de ameaças inteligentes: escreva seu código para garantir que a recuperação do token seja concluída antes que o cliente envie suas solicitações para os endpoints protegidos. Se você já estiver usando a API `fetch` para fazer sua chamada, poderá substituir o wrapper de integração `fetch` do AWS WAF . Se você não usa a `fetch` API, pode usar a `getToken` operação de AWS WAF integração em vez disso. Para ver orientações de codificação, consulte as seções a seguir.
4. Adicionar verificação de token em sua web ACL: adicione pelo menos uma regra à sua web ACL que verifique se há um token de desafio válido nas solicitações da web enviadas pelo seu cliente. Você pode usar grupos de regras que verificam e monitoram tokens de desafio, como o nível direcionado do grupo de regras gerenciadas do Controle de Bots, e você pode usar a ação de regra Challenge para verificar, conforme descrito em CAPTCHAe Challenge em AWS WAF.

   As adições da web ACL verificam se as solicitações para seus endpoints protegidos incluem o token que você adquiriu na integração com o cliente. Solicitações que incluem um token válido e não expirado passam pela inspeção Challenge e não enviam outro desafio silencioso ao seu cliente.
5. (Opcional) Bloquear solicitações sem tokens: se você usar as APIs com o grupo de regras gerenciadas do ACFP, o grupo de regras gerenciadas do ATP ou as regras direcionadas do grupo de regras do Controle de Bots, essas regras não bloquearão solicitações sem tokens. Para bloquear solicitações sem tokens, siga as orientações em Bloqueio de solicitações que não têm um AWS WAF token válido.

Tópicos

- Especificação da API de ameaças inteligentes
- Como usar o wrapper de integração fetch
- Como usar a integração getToken

Especificação da API de ameaças inteligentes

Esta seção lista a especificação dos métodos e propriedades das APIs inteligentes de mitigação JavaScript de ameaças. Use essas APIs para integrações de ameaças inteligentes e CAPTCHA.

`AwsWafIntegration.fetch()`

Envia a `fetch` solicitação HTTP para o servidor usando a implementação da AWS WAF integração.

`AwsWafIntegration.getToken()`

Recupera o AWS WAF token armazenado e o armazena em um cookie na página atual com o nome `aws-waf-token` e o valor definido como o valor do token.

`AwsWafIntegration.hasToken()`

Retorna um booleano indicando se o cookie `aws-waf-token` atualmente contém um token não expirado.

Se você também estiver usando a integração CAPTCHA, consulte a especificação para isso em Especificação da API CAPTCHA JavaScript .

Como usar o wrapper de integração **`fetch`**

Você pode usar o AWS WAF `fetch` wrapper alterando suas `fetch` chamadas normais para a `fetch` API no `AwsWafIntegration` namespace. O AWS WAF wrapper suporta todas as mesmas opções da chamada de JavaScript `fetch` API padrão e adiciona o tratamento de tokens para a integração. Essa abordagem geralmente é a maneira mais simples de integrar seu aplicativo.

Antes da implementação do wrapper

A lista de exemplo a seguir mostra o código padrão antes de implementar o wrapper `fetch` de `AwsWafIntegration`.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Após a implementação do wrapper

A lista a seguir mostra o mesmo código com a implementação do wrapper `fetch` de `AwsWafIntegration`.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Como usar a integração **`getToken`**

AWS WAF exige que suas solicitações para endpoints protegidos incluam o cookie nomeado `aws-waf-token` com o valor do seu token atual.

A operação `getToken` é uma chamada de API assíncrona que recupera o token do AWS WAF e o armazena em um cookie na página atual com o nome `aws-waf-token` e o valor definido como o valor do token. Você pode usar esse cookie de token conforme necessário em sua página.

Quando você chama `getToken`, ele faz o seguinte:

- Se um token não expirado já estiver disponível, a chamada o retornará imediatamente.
- Caso contrário, a chamada recuperará um novo token do provedor do token, aguardando até 2 segundos para que o fluxo de trabalho de aquisição do token seja concluído antes do tempo limite. Se a operação atingir o tempo limite, ela gerará um erro, que seu código de chamada deve processar.

A operação `getToken` tem uma operação `hasToken` complementar, que indica se o cookie `aws-waf-token` atualmente contém um token não expirado.

`AwsWafIntegration.getToken()`recupera um token válido e o armazena como um cookie. A maioria das chamadas de clientes anexa automaticamente esse cookie, mas algumas não. Por exemplo, chamadas feitas em domínios de host não anexam o cookie. Nos detalhes de implementação a seguir, mostramos como trabalhar com os dois tipos de chamadas de clientes.

`getToken`Implementação básica, para chamadas que anexam o **`aws-waf-token`** cookie

A lista de exemplo a seguir mostra o código padrão para implementar a operação `getToken` com uma solicitação de login.

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

Envie o formulário somente após o token estar disponível em **`getToken`**

A lista a seguir mostra como registrar um receptor de eventos para interceptar envios de formulários até que um token válido esteja disponível para uso.

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
```

```
                e.target.submit();
            }, (reason) => { console.log("Error:"+reason) });
        }
    });
</script>
</body>
```

Anexar o token quando seu cliente não anexa o **`aws-waf-token`** cookie por padrão

`AwsWafIntegration.getToken()`recupera um token válido e o armazena como um cookie, mas nem todas as chamadas de clientes anexam esse cookie por padrão. Por exemplo, chamadas feitas em domínios de host não anexam o cookie.

O `fetch` wrapper trata esses casos automaticamente, mas se você não conseguir usar o `fetch` wrapper, poderá lidar com isso usando um cabeçalho personalizado`x-aws-waf-token`. AWS WAF lê os tokens desse cabeçalho, além de lê-los do `aws-waf-token` cookie. O código a seguir mostra um exemplo de configuração do cabeçalho.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

Por padrão, AWS WAF só aceita tokens que contenham o mesmo domínio do domínio host solicitado. Todos os tokens entre domínios exigem entradas correspondentes na lista de domínios de tokens da ACL da web. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

Para obter informações adicionais sobre o uso de tokens entre domínios, consulte aws-waf-bot-controlaws-samples/ -. api-protection-with-captcha

Usando a API CAPTCHA JavaScript

A JavaScript API CAPTCHA permite que você configure o quebra-cabeça CAPTCHA e o coloque onde quiser em seu aplicativo cliente. Essa API aproveita os recursos das JavaScript APIs de ameaças inteligentes para adquirir e usar AWS WAF tokens depois que um usuário final conclui com êxito um quebra-cabeça de CAPTCHA.

Implemente a JavaScript integração primeiro em um ambiente de teste e depois na produção. Para obter orientações adicionais sobre codificação, consulte as seções a seguir.

Para usar a API de integração CAPTCHA

1. Instale a API

   a. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   b. No painel de navegação, escolha Integração de aplicativos. Na página Integração de aplicativos, você pode ver as opções com guias.

   c. Selecione Integração CAPTCHA.

   d. Copie a tag do script de JavaScript integração listada para uso em sua integração.

   e. No código da página do aplicativo, na seção `<head>`, insira a tag de script que você copiou. Essa inclusão torna o quebra-cabeça CAPTCHA disponível para configuração e uso.

   ```
   <head>
       <script type="text/javascript" src="integrationURL/jsapi.js" defer></
   script>
   </head>
   ```

   Essa lista `<script>` é configurada com o recurso `defer`, mas você pode alterar a configuração para `async` se quiser um comportamento diferente para sua página.

   O script do CAPTCHA também carrega automaticamente o script de integração de ameaças inteligentes, caso ele ainda não esteja presente. O script de integração de ameaças inteligentes faz com que seu aplicativo cliente recupere automaticamente um token em segundo plano no carregamento da página e fornece outras funcionalidades de gerenciamento de tokens necessárias para o uso da API CAPTCHA.

2. (Opcional) Adicionar configuração de domínio para os tokens do cliente — Por padrão, ao AWS WAF criar um token, ele usa o domínio host do recurso associado à ACL da web. Para fornecer domínios adicionais para as JavaScript APIs, siga as orientações em. Fornecimento de domínios para uso nos tokens

3. Obtenha a chave de API criptografada para o cliente — A API CAPTCHA requer uma chave de API criptografada que contenha uma lista de domínios de clientes válidos. AWS WAF usa essa chave para verificar se o domínio do cliente que você está usando com a integração foi

aprovado para usar AWS WAF CAPTCHA. Para gerar sua chave de API, siga as orientações em Gerenciamento de chaves de API para a API JS CAPTCHA.

4. Codificar a implementação do widget CAPTCHA: implemente a chamada de API `renderCaptcha()` em sua página, no local em que você deseja usá-la. Para obter informações sobre como configurar e usar essa função, consulte as seguintes seções, Especificação da API CAPTCHA JavaScript e Como renderizar o quebra-cabeça CAPTCHA.

   A implementação do CAPTCHA se integra às APIs inteligentes de integração de ameaças para gerenciamento de tokens e execução de chamadas de busca que usam os tokens. AWS WAF Para obter orientação sobre o uso dessas APIs, consulte Usando a JavaScript API de ameaças inteligentes.

5. Adicionar verificação de token em sua web ACL: adicione pelo menos uma regra à sua web ACL que verifique se há um token de CAPTCHA válido nas solicitações da web enviadas pelo seu cliente. Você pode usar a ação de regra CAPTCHA para verificar, conforme descrito em CAPTCHAe Challenge em AWS WAF.

   As adições da web ACL verificam se as solicitações que vão para seus endpoints protegidos incluem o token que você adquiriu na integração com o cliente. Solicitações que incluem um token de CAPTCHA válido e não expirado passam pela inspeção de ação de regra CAPTCHA e não apresentam ao usuário final outro quebra-cabeça CAPTCHA.

Tópicos

- Especificação da API CAPTCHA JavaScript
- Como renderizar o quebra-cabeça CAPTCHA
- Manipulando uma resposta CAPTCHA de AWS WAF
- Gerenciamento de chaves de API para a API JS CAPTCHA

Especificação da API CAPTCHA JavaScript

Esta seção lista a especificação dos métodos e propriedades das APIs CAPTCHA JavaScript . Use as JavaScript APIs CAPTCHA para executar quebra-cabeças CAPTCHA personalizados em seus aplicativos cliente.

Essa API se baseia nas APIs de ameaças inteligentes, que você usa para configurar e gerenciar a aquisição e o uso de AWS WAF tokens. Consulte Especificação da API de ameaças inteligentes.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

Apresenta um quebra-cabeça de AWS WAF CAPTCHA para o usuário final e, em caso de sucesso, atualiza o token do cliente com a validação do CAPTCHA. Ele está disponível apenas com a integração CAPTCHA. Use essa chamada junto com as APIs de ameaças inteligentes para gerenciar a recuperação de tokens e fornecer o token em suas chamadas `fetch`. Veja as APIs de ameaças inteligentes em Especificação da API de ameaças inteligentes.

Ao contrário do intersticial CAPTCHA que AWS WAF envia, o quebra-cabeça CAPTCHA renderizado por esse método exibe o quebra-cabeça imediatamente, sem uma tela de título inicial.

`container`

O objeto `Element` do elemento do contêiner de destino na página. Isso geralmente é recuperado chamando `document.getElementById()` ou `document.querySelector()`.

Obrigatório: Sim

Tipo: `Element`

configuração

Um objeto contendo as configurações do CAPTCHA, da seguinte forma:

`apiKey`

A chave de API criptografada que habilita permissões para o domínio do cliente. Use o console do AWS WAF para gerar suas chaves de API para seus domínios de clientes. Você pode usar uma chave para até cinco domínios. Para mais informações, consulte Gerenciamento de chaves de API para a API JS CAPTCHA.

Obrigatório: Sim

Tipo: `string`

`onSuccess: (wafToken: string) => void;`

Chamado com um AWS WAF token válido quando o usuário final conclui com sucesso um quebra-cabeça de CAPTCHA. Use o token nas solicitações que você envia aos endpoints que você protege com uma AWS WAF Web ACL. O token fornece a prova e o timestamp da conclusão bem-sucedida do último quebra-cabeça.

Obrigatório: Sim

`onError?: (error: CaptchaError) => void;`

Chamado com um objeto de erro quando ocorre um erro durante a operação CAPTCHA.

Obrigatório: não

Definição de classe **`CaptchaError`**: o manipulador `onError` fornece um tipo de erro com a seguinte definição de classe.

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- `kind`: o tipo de erro retornado.
- `statusCode`: o código de status do HTTP, se disponível. Isso é usado por `network_error` se o erro for devido a um erro no HTTP.

`onLoad?: () => void;`

Chamado quando um novo quebra-cabeça CAPTCHA é carregado.

Obrigatório: não

`onPuzzleTimeout?: () => void;`

Chamado quando um quebra-cabeça CAPTCHA não é concluído antes de expirar.

Obrigatório: não

`onPuzzleCorrect?: () => void;`

Chamado quando uma resposta correta é fornecida a um quebra-cabeça CAPTCHA.

Obrigatório: não

`onPuzzleIncorrect?: () => void;`

Chamado quando uma resposta incorreta é fornecida a um quebra-cabeça CAPTCHA.

Obrigatório: não

`defaultLocale`

A localidade padrão a ser usada para o quebra-cabeça CAPTCHA. As instruções escritas para quebra-cabeças CAPTCHA estão disponíveis em árabe (ar-SA), chinês simplificado (zh-CN), holandês (nl-NL), inglês (en-US), francês (fr-FR), alemão (de-DE), italiano (it-IT), japonês (ja-JP), português do Brasil (pt-BR), espanhol (es-ES) e turco (tr-TR). As instruções de áudio estão disponíveis para todos os idiomas escritos, exceto chinês e japonês, cujos padrões são o inglês. Para alterar o idioma padrão, forneça o idioma internacional e o código de localidade, por exemplo,`ar-SA`.

Padrão: o idioma atualmente em uso no navegador do usuário final

Obrigatório: não

Tipo: `string`

`disableLanguageSelector`

Se definido como `true`, o quebra-cabeça CAPTCHA oculta o seletor de idioma.

Padrão: `false`

Exigido: Não

Tipo: `boolean`

`dynamicWidth`

Se definido como `true`, o quebra-cabeça CAPTCHA muda de largura para compatibilidade com a largura da janela do navegador.

Padrão: `false`

Exigido: Não

Tipo: `boolean`

`skipTitle`

Se definido como `true`, o quebra-cabeça CAPTCHA não exibirá o título do quebra-cabeça Resolva o quebra-cabeça.

Padrão: `false`

Exigido: Não

Tipo: `boolean`

Como renderizar o quebra-cabeça CAPTCHA

Você pode usar a AWS WAF `renderCaptcha` chamada onde quiser na interface do cliente. A chamada recupera um quebra-cabeça de CAPTCHA AWS WAF, o renderiza e envia os resultados para verificação. AWS WAF Ao fazer a chamada, você fornece a configuração de renderização do quebra-cabeça e os retornos de chamada que deseja executar quando os usuários finais concluírem o quebra-cabeça. Consulte a seção anterior, Especificação da API CAPTCHA JavaScript , para detalhes sobre as opções.

Use essa chamada em conjunto com a funcionalidade de gerenciamento de tokens das APIs de integração de ameaças inteligentes. Essa chamada fornece ao seu cliente um token que verifica a conclusão bem-sucedida do quebra-cabeça CAPTCHA. Use as APIs inteligentes de integração de ameaças para gerenciar o token e fornecer o token nas chamadas do seu cliente para os endpoints protegidos com ACLs AWS WAF da web. Para obter informações sobre as APIs de ameaças inteligentes, consulte Usando a JavaScript API de ameaças inteligentes.

Exemplos de implementação

A lista de exemplos a seguir mostra uma implementação padrão de CAPTCHA, incluindo o posicionamento da URL de AWS WAF integração na <head> seção.

Essa listagem configura a função `renderCaptcha` com um retorno de chamada bem-sucedido que usa o wrapper `AwsWafIntegration.fetch` das APIs de integração de ameaças inteligentes. Para ter mais informações sobre essa função, consulte Como usar o wrapper de integração `fetch`.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
```

```
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Exemplo de definições de configuração

A lista de exemplo a seguir mostra o `renderCaptcha` com configurações não padrão para as opções de largura e o título.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

Para obter informações completas sobre as opções de configuração, consulte Especificação da API CAPTCHA JavaScript .

Manipulando uma resposta CAPTCHA de AWS WAF

Uma AWS WAF regra com uma CAPTCHA ação encerra a avaliação de uma solicitação da web correspondente se a solicitação não tiver um token com um carimbo de data/hora CAPTCHA válido. Se a solicitação for uma chamada `GET` de texto/html, a ação CAPTCHA então serve ao cliente uma intersticial com um quebra-cabeça CAPTCHA. Quando você não integra a JavaScript API CAPTCHA, o intersticial executa o quebra-cabeça e, se o usuário final o resolver com sucesso, reenvia automaticamente a solicitação.

Ao integrar a JavaScript API CAPTCHA e personalizar o tratamento do CAPTCHA, você precisa detectar a resposta final do CAPTCHA, fornecer seu CAPTCHA personalizado e, se o usuário final resolver o quebra-cabeça com sucesso, reenviar a solicitação web do cliente.

O exemplo de código a seguir mostra como fazer isso.

> **Note**
>
> A resposta da AWS WAF CAPTCHA ação tem um código de status HTTP 405, que usamos para reconhecer a CAPTCHA resposta nesse código. Se seu endpoint protegido usa um código de status HTTP 405 para comunicar qualquer outro tipo de resposta para a mesma chamada, esse código de exemplo também renderizará um quebra-cabeça CAPTCHA para essas respostas.

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
```

```
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

Gerenciamento de chaves de API para a API JS CAPTCHA

Para integrar o AWS WAF CAPTCHA em um aplicativo cliente com a JavaScript API, você precisa da tag de integração da JavaScript API e da chave de API criptografada para o domínio do cliente em que deseja executar o quebra-cabeça do CAPTCHA.

A integração do aplicativo CAPTCHA JavaScript usa as chaves de API criptografadas para verificar se o domínio do aplicativo cliente tem permissão para usar a API AWS WAF CAPTCHA. Ao chamar a API CAPTCHA do seu JavaScript cliente, você fornece uma chave de API com uma lista de

domínios que inclui um domínio para o cliente atual. Você pode listar até 5 domínios em uma única chave criptografada.

Requisitos de chaves de API

A chave de API que você usa na integração do CAPTCHA deve conter um domínio que se aplique ao cliente em que você usa a chave.

- Se você especificar um `window.awsWafCookieDomainList` na integração de ameaças inteligentes do seu cliente, pelo menos um domínio em sua chave de API deverá corresponder exatamente a um dos domínios de token em `window.awsWafCookieDomainList` ou deverá ser o domínio apex de um desses domínios de token.

  Por exemplo, para o domínio do token `mySubdomain.myApex.com`, a chave de API `mySubdomain.myApex.com` é uma correspondência exata e a chave de API `myApex.com` é o domínio apex. Qualquer chave corresponde ao domínio do token.

  Para obter informações sobre a configuração da lista de domínios de tokens, consulte Fornecimento de domínios para uso nos tokens.
- Caso contrário, o domínio atual deverá estar contido na chave da API. O domínio atual é o domínio que você pode ver na barra de endereço do navegador.

Os domínios que você usa devem ser aqueles que AWS WAF serão aceitos, com base no domínio de host protegido e na lista de domínios de token configurada para a Web ACL. Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

Como escolher a região para sua chave de API

AWS WAF pode gerar chaves de API CAPTCHA em qualquer região onde AWS WAF esteja disponível.

Como regra geral, você deve usar a mesma região para sua chave de API CAPTCHA que usa para sua ACL da web. No entanto, se você espera um público global para uma ACL da web regional, pode obter uma tag de JavaScript integração CAPTCHA com escopo CloudFront e uma chave de API com escopo definido e usá-las com uma ACL da web regional. CloudFront Essa abordagem permite que os clientes carreguem um quebra-cabeça CAPTCHA da região mais próxima a eles, o que reduz a latência.

As chaves da API CAPTCHA com escopo definido para regiões diferentes das não CloudFront são suportadas para uso em várias regiões. Eles só podem ser usados na região para a qual se destinam.

Para gerar uma chave de API para seus domínios de clientes

Para obter o URL de integração e gerar e recuperar as chaves de API por meio do console.

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Integração de aplicativos.
3. No painel Web ACLs habilitadas para integração de aplicativos, selecione a região que você deseja usar para sua chave de API. Você também pode selecionar a região no painel de chaves de API da guia de integração CAPTCHA.
4. Escolha a guia Integração de CAPTCHA. Essa guia fornece a tag de JavaScript integração CAPTCHA, que você pode usar em sua integração, e a lista de chaves de API. Ambos têm como escopo a região selecionada.
5. No painel Chaves de API, escolha Gerar chave. A caixa de diálogo de geração de chaves é exibida.
6. Insira os domínios de cliente que você deseja incluir na chave. Você pode inserir até 5. Quando terminar, escolha Gerar chave. A interface retorna à guia de integração do CAPTCHA, onde sua nova chave está listada.

   Depois de criada, uma chave de API é imutável. Se você precisar fazer alterações em uma chave, gere uma nova chave e use-a em vez disso.
7. (Opcional) Copie a chave recém-gerada para uso em sua integração.

Você também pode usar as APIs REST ou um dos AWS SDKs específicos da linguagem para esse trabalho. As chamadas da API REST são CreateApiKey e ListApiKeys.

Para excluir uma chave de API

Para excluir uma chave de API, você deve usar a API REST ou um dos AWS SDKs específicos da linguagem. A chamada da API REST é DeleteApiKey. Você não pode usar o console para excluir uma chave.

Depois de excluir uma chave, pode levar até 24 horas para AWS WAF proibir o uso da chave em todas as regiões.

AWS WAF integração de aplicativos móveis

Você pode usar os SDKs AWS WAF móveis para implementar SDKs AWS WAF inteligentes de integração de ameaças para aplicativos móveis Android e iOS.

- Para aplicativos móveis Android, os AWS WAF SDKs funcionam com a API Android versão 23 (Android versão 6) e versões posteriores. Para obter informações sobre as versões do Android, consulte as Notas de lançamento da plataforma de SDK.
- Para aplicativos móveis iOS, AWS WAF os SDKs funcionam para iOS versão 13 e posterior. Para obter informações sobre as versões do iOS, consulte as Notas de versão do iOS e iPadOS.

Com o SDK móvel, você pode gerenciar a autorização de tokens e incluir os tokens nas solicitações que você envia aos seus recursos protegidos. Ao usar os SDKs, você garante que essas chamadas de procedimento remoto feitas pelo seu cliente contenham um token válido. Além disso, quando essa integração está implementada nas páginas do seu aplicativo, você pode implementar regras de mitigação na sua web ACL, como bloquear solicitações que não contenham um token válido.

Para acessar os SDKs móveis, entre em contato com o suporte em Entrar em contato com a AWS.

> **Note**
>
> Os SDKs AWS WAF móveis não estão disponíveis para personalização de CAPTCHA.

A abordagem básica para usar o SDK é criar um provedor de token usando um objeto de configuração e, em seguida, usar o provedor de token para recuperar tokens. AWS WAF Por padrão, o provedor de token inclui os tokens recuperados em suas solicitações da web para seu recurso protegido.

Veja a seguir uma lista parcial de uma implementação de SDK, que mostra os principais componentes. Para obter mais exemplos detalhados, consulte Escrevendo seu código para o SDK AWS WAF móvel.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
```

```
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

Instalando o SDK AWS WAF móvel

Para acessar os SDKs móveis, entre em contato com o suporte em Entrar em contato com a AWS.

Implemente a integração com SDK móvel primeiro em um ambiente de teste e depois na produção.

Para instalar o SDK AWS WAF móvel

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha Integração de aplicativos.
3. Na guia Integrações de ameaças inteligentes, faça o seguinte:
   a. No painel web ACLshabilitadas para integração de aplicativos, localize a web ACL com a qual você está se integrando. Copie e salve o URL de integração da web ACL para uso em sua implementação. Você também pode obter esse URL por meio da chamada da API `GetWebACL`.
   b. Escolha o tipo e a versão do dispositivo móvel e, em seguida, escolha Baixar. Você pode escolher qualquer versão que desejar, mas recomendamos usar a versão mais recente. AWS WAF baixa o `zip` arquivo do seu dispositivo em seu local de download padrão.
4. Em seu ambiente de desenvolvimento de aplicativos, descompacte o arquivo em um local de trabalho de sua escolha. No diretório de nível superior do arquivo zip, localize e abra o `README`. Siga as instruções no `README` arquivo para instalar o SDK AWS WAF móvel para uso no código do seu aplicativo móvel.

5. Programe seu aplicativo de acordo com as orientações nas seções a seguir.

A AWS WAF especificação do SDK móvel

Esta seção lista os objetos, as operações e as configurações de SDK para a versão mais recente disponível do SDK móvel do AWS WAF . Para obter informações detalhadas sobre como o provedor de token e as operações funcionam para as várias combinações de configurações, consulte Como o SDK AWS WAF móvel funciona.

`WAFToken`

Guarda uma AWS WAF ficha.

`getValue()`

Recupera a representação `String` de `WAFToken`.

`WAFTokenProvider`

Gerencia tokens em seu aplicativo móvel. Implemente isso usando um objeto `WAFConfiguration`.

`getToken()`

Se a atualização em segundo plano estiver ativada, isso retornará o token em cache. Se a atualização em segundo plano estiver desativada, isso fará uma chamada síncrona e bloqueadora AWS WAF para recuperar um novo token.

`onTokenReady(WAFTokenResultCallback)`

Instrui o provedor de token a atualizar o token e invocar o retorno de chamada fornecido quando um token ativo estiver pronto. O provedor do token invocará seu retorno de chamada em um thread em segundo plano quando o token estiver armazenado em cache e pronto. Chame isso quando seu aplicativo for carregado pela primeira vez e também quando ele voltar ao estado ativo. Para obter mais informações sobre como retornar a um estado ativo, consulte the section called “Recuperação de um token após a inatividade do aplicativo”.

Para aplicativos Android ou iOS, você pode definir `WAFTokenResultCallback` para a operação que deseja que o provedor de token invoque quando um token solicitado estiver pronto. Sua implementação do `WAFTokenResultCallback` deve seguir os parâmetros `WAFToken`, `SdkError`. Para aplicativos iOS, você pode criar alternadamente uma função embutida.

`storeTokenInCookieStorage(WAFToken)`

Instrui o `WAFTokenProvider` a armazenar o AWS WAF token especificado no gerenciador de cookies do SDK. Por padrão, o token só é adicionado ao armazenamento de cookies quando é adquirido pela primeira vez e quando é atualizado. Se o aplicativo limpar o armazenamento de cookies compartilhado por qualquer motivo, o SDK não adicionará automaticamente o AWS WAF token de volta até a próxima atualização.

`WAFConfiguration`

Mantém a configuração para a implementação do `WAFTokenProvider`. Ao implementar isso, você fornece o URL de integração da sua web ACL, o nome de domínio a ser usado no token e todas as configurações não padrão que você deseja que o provedor de token use.

A lista a seguir especifica as configurações que você pode gerenciar no objeto `WAFConfiguration`.

`applicationIntegrationUrl`

O URL de integração do aplicativo. Obtenha isso no AWS WAF console ou por meio da chamada de `getWebACL` API.

Obrigatório: Sim

Tipo: URL específico do aplicativo. Para iOS, consulte o URL do iOS. Para Android, consulte o URL do java.net.

`backgroundRefreshEnabled`

Indica se você deseja que o provedor de token atualize o token em segundo plano. Se você definir isso, o provedor de token atualizará seus tokens em segundo plano de acordo com as configurações que regem as atividades de atualização automática de tokens.

Obrigatório: não

Tipo: `Boolean`

Valor padrão: `TRUE`

`domainName`

O domínio a ser usado no token, que é usado na aquisição e armazenamento de cookies. Por exemplo, o `example.com` ou o `aws.amazon.com`. Geralmente, esse é o domínio do host

do seu recurso associado à web ACL, para onde você enviará solicitações da web. Para o grupo de regras gerenciadas do ACFP, `AWSManagedRulesACFPRuleSet`, geralmente será um único domínio que corresponde ao domínio no caminho de criação da conta que você forneceu na configuração do grupo de regras. Para o grupo de regras gerenciadas do ATP, `AWSManagedRulesATPRuleSet`, geralmente será um único domínio que corresponde ao domínio no caminho de login fornecido na configuração do grupo de regras.

Não são permitidos sufixos públicos. Por exemplo, você não pode usar `gov.au` ou `co.uk` como domínio do token.

O domínio deve ser aceito, com base no domínio do host protegido e na lista de domínios de tokens da ACL da web. AWS WAF Para ter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL.

Obrigatório: Sim

Tipo: `String`

`maxErrorTokenRefreshDelayMsec`

O tempo máximo em milissegundos a se esperar antes de repetir uma atualização de token após uma tentativa malsucedida. Esse valor é usado depois que a recuperação do token falhou e foi repetida `maxRetryCount` vezes.

Obrigatório: não

Tipo: `Integer`

Valor padrão: `5000` (5 segundos)

Valor mínimo permitido: `1` (1 milissegundo)

Valor máximo permitido: `30000` (30 segundos)

`maxRetryCount`

O número máximo de novas tentativas a serem executadas com recuo exponencial quando um token é solicitado.

Obrigatório: não

Tipo: `Integer`

Valor padrão: se a atualização em segundo plano estiver ativada, `5`. Caso contrário, `3`.

Valor mínimo permitido: `0`

Valor máximo permitido: `10`

`setTokenCookie`

Indica se você deseja que o gerenciador de cookies do SDK adicione um cookie de token às suas solicitações. Por padrão, isso adiciona um cookie de token a todas as solicitações. O gerenciador de cookies adiciona um cookie de token a qualquer solicitação cujo caminho esteja abaixo do caminho especificado em `tokenCookiePath`.

Obrigatório: não

Tipo: `Boolean`

Valor padrão: `TRUE`

`tokenCookiePath`

Usado quando `setTokenCookie` é `TRUE`. Indica o caminho de nível superior em que você deseja que o gerenciador de cookies do SDK adicione um cookie de token. O gerente adiciona um cookie de token a todas as solicitações que você envia para esse caminho e para todos os caminhos secundários.

Por exemplo, se você definir isso como `/web/login`, o gerenciador incluirá o cookie de token para tudo o que é enviado para `/web/login` e para qualquer um de seus caminhos secundários, como `/web/login/help`. Ele não inclui o token para solicitações enviadas para outros caminhos, como `/`, `/web` ou `/web/order`.

Obrigatório: não

Tipo: `String`

Valor padrão: `/`

`tokenRefreshDelaySec`

Usado para atualização em segundo plano. O tempo máximo em segundos entre as atualizações do token em segundo plano.

Obrigatório: não

Tipo: `Integer`

Valor padrão: 88

Valor mínimo permitido: 88

Valor máximo permitido: `300` (5 minutos)

Como o SDK AWS WAF móvel funciona

Os SDKs móveis fornecem um provedor de token configurável que você pode usar para recuperação e uso de tokens. O provedor do token verifica se as solicitações que você permite são de clientes legítimos. Ao enviar solicitações para os AWS recursos com os quais você protege AWS WAF, você inclui o token em um cookie para validar a solicitação. Você pode manipular o cookie do token manualmente ou fazer com que o provedor do token faça isso por você.

Esta seção aborda as interações entre as classes, propriedades e métodos incluídos no SDK móvel. Para obter a especificação do SDK, consulte A AWS WAF especificação do SDK móvel.

Recuperação e armazenamento em cache de tokens

Ao criar a instância do provedor de token em seu aplicativo móvel, você configura como deseja que ela gerencie os tokens e a recuperação de tokens. Sua principal opção é como manter tokens válidos e não expirados para uso nas solicitações da web do seu aplicativo:

- Atualização em segundo plano ativada: esse é o padrão. O provedor de token atualiza automaticamente o token em segundo plano e o armazena em cache. Com a atualização em segundo plano ativada, quando você chama `getToken()`, a operação recupera o token em cache.

  O provedor de token executa a atualização do token em intervalos configuráveis, para que um token não expirado esteja sempre disponível no cache enquanto o aplicativo estiver ativo. A atualização em segundo plano é pausada enquanto seu aplicativo está em um estado inativo. Para obter mais informações sobre isso, consulte Recuperação de um token após a inatividade do aplicativo.
- Atualização em segundo plano desativada: você pode desativar a atualização de tokens em segundo plano e, em seguida, recuperar tokens somente sob demanda. Os tokens recuperados sob demanda não são armazenados em cache e você pode recuperar mais de um, se quiser. Cada token é independente de qualquer outro que você recupere e cada um tem seu próprio timestamp que é usado para calcular a expiração.

Você tem as seguintes opções para recuperação de token quando a atualização em segundo plano está desativada:

- **`getToken()`**— Quando você liga `getToken()` com a atualização em segundo plano desativada, a chamada recupera de forma síncrona um novo token de. AWS WAF Essa é uma chamada potencialmente bloqueadora que pode afetar a capacidade de resposta do aplicativo se você a invocar no thread principal.
- **`onTokenReady(WAFTokenResultCallback)`**: essa chamada recupera de forma assíncrona um novo token e, em seguida, invoca o retorno de chamada do resultado fornecido em um thread em segundo plano quando um token está pronto.

Como o provedor de token tenta novamente recuperações de tokens com falha

O provedor de token repete automaticamente a recuperação do token quando a recuperação falha. As novas tentativas são executadas inicialmente usando o recuo exponencial com um tempo de espera inicial de 100 ms. Para obter mais repetições de tentaivas exponenciais, consulte Novas tentativas e recuo exponencial na AWS.

Quando o número de novas tentativas atinge o `maxRetryCount` configurado, o provedor do token para de tentar ou passa a tentar a cada `maxErrorTokenRefreshDelayMsec` milissegundos, dependendo do tipo de recuperação do token:

- **`onTokenReady()`**: o provedor do token passa a esperar `maxErrorTokenRefreshDelayMsec` milissegundos entre as tentativas e continua tentando recuperar o token.
- Atualização em segundo plano: o provedor de token passa a esperar `maxErrorTokenRefreshDelayMsec` milissegundos entre as tentativas e continua tentando recuperar o token.
- Chamadas **`getToken()`** sob demanda, quando a atualização em segundo plano está desativada: o provedor de token para de tentar recuperar um token e retorna o valor do token anterior ou um valor nulo se não houver nenhum token anterior.

Recuperação de um token após a inatividade do aplicativo

A atualização em segundo plano só é realizada enquanto seu aplicativo é considerado ativo para seu tipo de aplicativo:

- iOS: a atualização em segundo plano é realizada quando o aplicativo está em primeiro plano.

- Android: a atualização em segundo plano é realizada quando o aplicativo não está fechado, seja em primeiro plano ou em segundo plano.

Se seu aplicativo permanecer em qualquer estado que não ofereça suporte à atualização em segundo plano por mais tempo do que os `tokenRefreshDelaySec` segundos configurados, o provedor de token pausará a atualização em segundo plano. Por exemplo, para um aplicativo iOS, se `tokenRefreshDelaySec` for 300 e o aplicativo fechar ou ficar em segundo plano por mais de 300 segundos, o provedor do token interromperá a atualização do token. Quando o aplicativo retorna ao estado ativo, o provedor de token reinicia automaticamente a atualização em segundo plano.

Quando seu aplicativo voltar ao estado ativo, chame `onTokenReady()` para que você possa ser notificado quando o provedor do token tiver recuperado e armazenado em cache um novo token. Não chame simplesmente `getToken()`, porque o cache pode ainda não conter um token válido e atual.

Escrevendo seu código para o SDK AWS WAF móvel

Esta seção fornece exemplos de código para uso do SDK móvel.

Inicialização do provedor de tokens e obtenção de tokens

Você inicia sua instância do provedor de token usando um objeto de configuração. Em seguida, você pode recuperar tokens usando as operações disponíveis. Veja a seguir os componentes básicos do código necessário.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
```

```
 //error occurred after exhausting all retries
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

Exemplo de Java:

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Exemplo de Kotlin:

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
    .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

Permitindo que o SDK forneça o cookie de token em suas solicitações HTTP

Se `setTokenCookie` é `TRUE`, o provedor de token inclui o cookie de token para você em suas solicitações da web para todos os locais no caminho especificado em `tokenCookiePath`. Por padrão, `setTokenCookie` é `TRUE` e `tokenCookiePath` é `/`.

Você pode restringir o escopo das solicitações que incluem um cookie de token especificando o caminho do cookie de token, por exemplo, `/web/login`. Se você fizer isso, verifique se suas AWS WAF regras não inspecionam os tokens nas solicitações que você envia para outros caminhos. Ao usar o grupo de regras `AWSManagedRulesACFPRuleSet`, você configura os caminhos de registro e criação da conta, e o grupo de regras verifica os tokens nas solicitações enviadas para esses caminhos. Para ter mais informações, consulte Adicionando o grupo de regras gerenciadas do ACFP

à sua web ACL. Da mesma forma, ao usar o grupo de regras `AWSManagedRulesATPRuleSet`, você configura o caminho de login e o grupo de regras verifica os tokens nas solicitações enviadas para esse caminho. Para ter mais informações, consulte Adicionando grupos de regras gerenciadas à sua web ACL..

iOS

Quando `setTokenCookie` é`TRUE`, o provedor de token armazena o AWS WAF token em um `HTTPCookieStorage.shared` e inclui automaticamente o cookie nas solicitações para o domínio que você especificou`WAFConfiguration`.

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

Quando `setTokenCookie` estiver`TRUE`, o provedor de token armazena o AWS WAF token em uma `CookieHandler` instância que é compartilhada em todo o aplicativo. O provedor de token inclui automaticamente o cookie nas solicitações para o domínio que você especificou em `WAFConfiguration`.

Exemplo de Java:

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Exemplo de Kotlin:

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

Se você já tiver a instância padrão `CookieHandler` inicializada, o provedor de token a usará para gerenciar cookies. Caso contrário, o provedor de token inicializará uma nova `CookieManager` instância com o AWS WAF token

`CookiePolicy.ACCEPT_ORIGINAL_SERVER` e, em seguida, definirá essa nova instância como a instância padrão em`CookieHandler`.

O código a seguir mostra como o SDK inicializa o gerenciador e o manipulador de cookies quando eles não estão disponíveis no seu aplicativo.

Exemplo de Java:

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Exemplo de Kotlin:

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

Fornecimento manual do cookie de token em suas solicitações HTTP

Se você definir `setTokenCookie` como `FALSE`, precisará fornecer o cookie de token manualmente, como um cabeçalho de solicitação HTTP de cookie, em suas solicitações para seu endpoint protegido. O código a seguir mostra como fazer isso.

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Exemplo de Java:

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Exemplo de Kotlin:

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHAe Challenge em AWS WAF

Você pode configurar suas AWS WAF regras para executar uma Challenge ação CAPTCHA OR contra solicitações da web que correspondam aos critérios de inspeção da sua regra. Você também pode programar seus aplicativos JavaScript cliente para executar quebra-cabeças de CAPTCHA e desafios de navegador localmente.

Os quebra-cabeças de CAPTCHA e os desafios silenciosos só podem ser executados quando os navegadores estão acessando endpoints HTTPS. Os clientes do navegador devem estar sendo executados em contextos seguros para adquirir tokens.

- CAPTCHA— Exige que o usuário final resolva um quebra-cabeça de CAPTCHA para provar que um ser humano está enviando a solicitação. Os quebra-cabeças CAPTCHA devem ser bastante fáceis e rápidos para os humanos concluírem com sucesso e difíceis para os computadores concluírem com sucesso ou aleatoriamente com qualquer taxa significativa de sucesso.

  Nas regras de ACL da web, o CAPTCHA é comumente usado quando uma Block ação interrompe muitas solicitações legítimas, mas deixar todo o tráfego passar resultaria em níveis inaceitavelmente altos de solicitações indesejadas, como de bots. Para obter informações sobre o comportamento da ação da regra, consulteComo as ações de regra AWS WAFCAPTCHA e Challenge funcionam.

  Você também pode programar uma implementação de quebra-cabeça de CAPTCHA nas APIs de integração de aplicativos do cliente. Ao fazer isso, você pode personalizar o comportamento e o

posicionamento do quebra-cabeça em seu aplicativo cliente. Para ter mais informações, consulte AWS WAF integração de aplicativos clientes.

- Challenge— Executa um desafio silencioso que exige que a sessão do cliente verifique se é um navegador e não um bot. A verificação é executada em segundo plano sem envolver o usuário final. Essa é uma boa opção para verificar clientes que você suspeita serem inválidos sem afetar negativamente a experiência do usuário final com um quebra-cabeça CAPTCHA. Para obter informações sobre o comportamento da ação da regra, consulteComo as ações de regra AWS WAFCAPTCHA e Challenge funcionam.

  A ação de regra Challenge é semelhante ao desafio executado pelas APIs de integração de ameaças inteligentes do cliente, descrito em AWS WAF integração de aplicativos clientes.

> **Note**
>
> São cobradas taxas adicionais quando você usa a ação de regra CAPTCHA ou Challenge em uma de suas regras ou como uma substituição de ação de regra em um grupo de regras. Para obter mais informações, consulte Preços do AWS WAF.

Para obter descrições de todas as opções de ação da regra, consulteAção da regra.

Tópicos

- AWS WAF Quebra-cabeças CAPTCHA
- Como as ações de regra AWS WAFCAPTCHA e Challenge funcionam
- Práticas recomendadas para usar as ações CAPTCHA e Challenge

AWS WAF Quebra-cabeças CAPTCHA

AWS WAF fornece a funcionalidade CAPTCHA padrão que desafia os usuários a confirmar que são seres humanos. CAPTCHA significa teste de Turing público completamente automatizado para diferenciar computadores de humanos. Os quebra-cabeças CAPTCHA são projetados para verificar se um humano está enviando solicitações e para evitar atividades como captura de dados na web, preenchimento de credenciais e spam. Os quebra-cabeças CAPTCHA não eliminam todas as solicitações indesejadas. Muitos quebra-cabeças foram resolvidos usando aprendizado de máquina e inteligência artificial. Em um esforço para contornar o CAPTCHA, algumas organizações complementam as técnicas automatizadas com a intervenção humana. Apesar disso, o CAPTCHA

continua sendo uma ferramenta útil para evitar tráfego de bots menos sofisticado e aumentar os recursos necessários para operações em grande escala.

AWS WAF gera aleatoriamente seus quebra-cabeças de CAPTCHA e os percorre para garantir que os usuários enfrentem desafios únicos. AWS WAF adiciona regularmente novos tipos e estilos de quebra-cabeças para permanecer eficaz contra as técnicas de automação. Além dos quebra-cabeças, o script AWS WAF CAPTCHA reúne dados sobre o cliente para garantir que a tarefa seja concluída por um humano e para evitar ataques repetidos.

Cada quebra-cabeça CAPTCHA inclui um conjunto padrão de controles para o usuário final solicitar um novo quebra-cabeça, alternar entre quebra-cabeças de áudio e visuais, acessar instruções adicionais e enviar uma solução de quebra-cabeça. Todos os quebra-cabeças incluem suporte para leitores de tela, controles de teclado e cores contrastantes.

Os quebra-cabeças AWS WAF CAPTCHA atendem aos requisitos das Diretrizes de Acessibilidade de Conteúdo da Web (WCAG). Para obter informações, consulte Visão geral das Diretrizes de Acessibilidade de Conteúdo da Web (WCAG) no site do World Wide Web Consortium (W3C).

Tópicos

Suporte ao idioma do quebra-cabeça CAPTCHA

O quebra-cabeça do CAPTCHA começa com instruções escritas no idioma do navegador do cliente ou, se o idioma do navegador não for suportado, em inglês. O quebra-cabeça fornece opções de idioma alternativo por meio de um menu suspenso.

O usuário pode alternar para as instruções de áudio selecionando o ícone do fone de ouvido na parte inferior da página. A versão em áudio do quebra-cabeça fornece instruções faladas sobre o texto que o usuário deve digitar em uma caixa de texto, sobrepostas por ruídos de fundo.

A tabela a seguir lista os idiomas que você pode selecionar para as instruções escritas em um quebra-cabeça CAPTCHA e o suporte de áudio para cada seleção.

AWS WAF Idiomas suportados pelo quebra-cabeça CAPTCHA

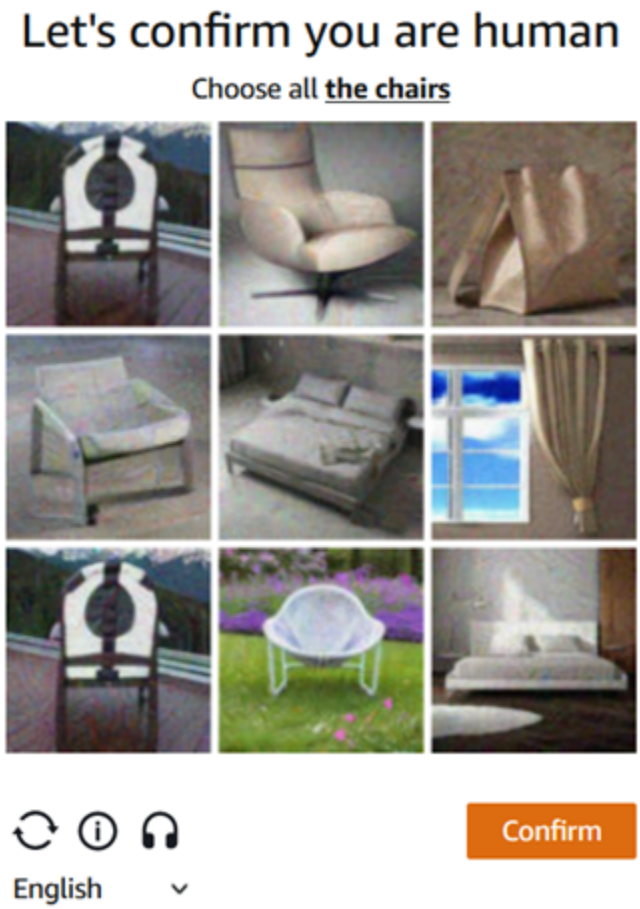
Suporte de instruções escritas	Código local	Suporte de instruções de áudio

Suporte de instruções escritas	Código local	Suporte de instruções de áudio
Árabe	Ar-sa	Árabe
Chinês simplificado	zh-CN	Áudio em inglês
Holandês	nl-NL	Holandês
Inglês	en-US	Inglês
Francês	fr-FR	Francês
Alemão	de-DE	Alemão
Italiano	it-IT	Italiano
Japonês	ja-JP	Áudio em inglês
Português do Brasil	pt-BR	Português do Brasil
Espanhol	es-ES	Espanhol
Turco	tr-TR	Turco

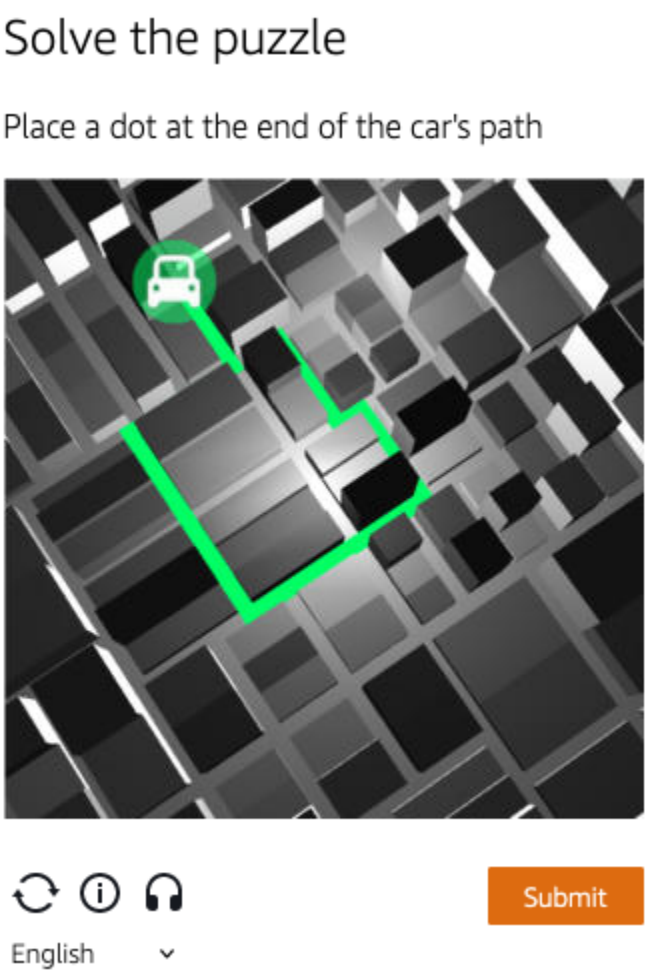
Exemplos de quebra-cabeças CAPTCHA

Um quebra-cabeça CAPTCHA visual típico requer interação para mostrar que o usuário pode compreender e interagir com uma ou mais imagens.

A captura de tela a seguir mostra um exemplo de um quebra-cabeça de grade de imagens. Esse quebra-cabeça exige que você selecione todas as imagens na grade que incluem um tipo específico de objeto.

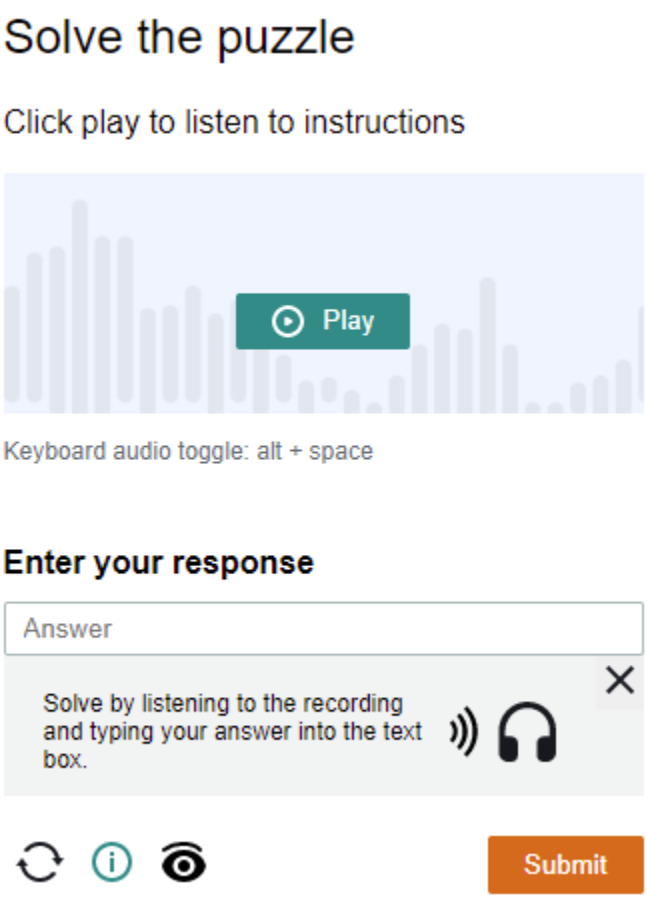


A captura de tela a seguir mostra um exemplo de quebra-cabeça que exige que você identifique o ponto final do caminho de um carro em um desenho.



Um quebra-cabeça de áudio fornece ruído de fundo sobreposto a instruções faladas sobre o texto que o usuário deve digitar em uma caixa de texto.

A captura de tela a seguir mostra a tela da escolha do quebra-cabeça de áudio.



Como as ações de regra AWS WAFCAPTCHA e Challenge funcionam

AWS WAF CAPTCHAe Challenge são ações de regras padrão, portanto, são relativamente fáceis de implementar. Para usar qualquer um deles, você cria os critérios de inspeção para sua regra que identificam as solicitações que você deseja inspecionar e, em seguida, especifica uma das duas ações da regra. Para obter informações gerais sobre as opções de ação de regra, consulte Ação da regra.

Além de implementar desafios silenciosos e quebra-cabeças de CAPTCHA do lado do servidor, você pode integrar desafios silenciosos em seus aplicativos clientes JavaScript iOS e Android e renderizar quebra-cabeças de CAPTCHA em seus clientes. JavaScript Essas integrações permitem que você forneça aos usuários finais um melhor desempenho e experiências de quebra-cabeça CAPTCHA, além de reduzir os custos associados ao uso das ações de regras e dos grupos de regras de mitigação de ameaças inteligentes. Para obter mais informações sobre essas opções, consulte AWS WAF integração de aplicativos clientes. Para obter informações sobre a definição de preço, consulte Definição de preço do AWS WAF.

Tópicos

Comportamento de ações CAPTCHA e Challenge

Quando uma solicitação da web corresponde aos critérios de inspeção de uma regra CAPTCHA ou Challenge ação, AWS WAF determina como lidar com a solicitação de acordo com o estado do token e a configuração do tempo de imunidade. AWS WAF também considera se a solicitação pode lidar com o quebra-cabeça CAPTCHA ou com os intersticiais do script de desafio. Os scripts foram projetados para serem tratados como conteúdo HTML e só podem ser tratados adequadamente por um cliente que espera conteúdo HTML.

> **Note**
>
> São cobradas taxas adicionais quando você usa a ação de regra CAPTCHA ou Challenge em uma de suas regras ou como uma substituição de ação de regra em um grupo de regras. Para obter mais informações, consulte Preços do AWS WAF.

Como a ação lida com a solicitação da web

AWS WAF aplica a Challenge ação CAPTCHA ou a uma solicitação da web da seguinte forma:

- Token válido — AWS WAF trata isso de forma semelhante a uma Count ação. AWS WAF aplica todos os rótulos e personalizações de solicitação que você configurou para a ação da regra e, em seguida, continua avaliando a solicitação usando as regras restantes na Web ACL.
- Token ausente, inválido ou expirado — AWS WAF interrompe a avaliação da web ACL da solicitação e impede que ela vá para o destino pretendido.

  AWS WAF gera uma resposta que é enviada de volta ao cliente, de acordo com o tipo de ação da regra:

  - Challenge: AWS WAF inclui o seguinte na resposta:
    - O cabeçalho `x-amzn-waf-action` com um valor de `challenge`.

> **Note**
>
> Esse cabeçalho não está disponível para JavaScript aplicativos executados no navegador do cliente. Para obter detalhes, consulte a seção a seguir.

  - Código de status do HTTP `202 Request Accepted`.
  - Se a solicitação contiver um `Accept` cabeçalho com um valor `detext/html`, a resposta incluirá um intersticial de JavaScript página com um script de desafio.
- CAPTCHA— AWS WAF inclui o seguinte na resposta:
  - O cabeçalho `x-amzn-waf-action` com um valor de `captcha`.

> **Note**
>
> Esse cabeçalho não está disponível para JavaScript aplicativos executados no navegador do cliente. Para obter detalhes, consulte a seção a seguir.

  - Código de status do HTTP `405 Method Not Allowed`.
  - Se a solicitação contiver um `Accept` cabeçalho com um valor `detext/html`, a resposta incluirá um intersticial de JavaScript página com um script CAPTCHA.

Para configurar o tempo de expiração do token no nível da web ACL ou da regra, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.

Os cabeçalhos não estão disponíveis para JavaScript aplicativos executados no navegador do cliente

Quando AWS WAF responde a uma solicitação do cliente com um CAPTCHA ou uma resposta de desafio, ela não inclui cabeçalhos de compartilhamento de recursos de origem cruzada (CORS). Os cabeçalhos CORS são um conjunto de cabeçalhos de controle de acesso que informam ao navegador da Web do cliente quais domínios, métodos HTTP e cabeçalhos HTTP podem ser usados pelos aplicativos. JavaScript Sem os cabeçalhos CORS, os JavaScript aplicativos executados em um navegador cliente não têm acesso aos cabeçalhos HTTP e, portanto, não conseguem ler o `x-amzn-waf-action` cabeçalho fornecido nas respostas e. CAPTCHA Challenge

O que o desafio e as intersticiais CAPTCHA fazem

Quando uma intersticial de desafio é executada, depois que o cliente responde com sucesso, se ele ainda não tiver um token, a intersticial inicializa um para ele. Em seguida, ela atualiza o token com o timestamp de resolução do desafio.

Quando uma intersticial CAPTCHA é executada, se o cliente ainda não tiver um token, a intersticial CAPTCHA invoca primeiro o script de desafio para desafiar o navegador e inicializar o token. Em seguida, a intersticial executa seu quebra-cabeça CAPTCHA. Quando o usuário final conclui o quebra-cabeça com sucesso, a intersticial atualiza o token com o timestamp de resolução do CAPTCHA.

Em ambos os casos, depois que o cliente responde com sucesso e o script atualiza o token, o script reenvia a solicitação web original usando o token atualizado.

Você pode configurar como AWS WAF manipula os tokens. Para mais informações, consulte AWS WAF tokens de solicitação da web.

Ações CAPTCHA e Challenge nos logs e métricas

As ações CAPTCHA e Challenge podem ser de não encerramento, como Count, ou de encerramento, como Block. O resultado depende se a solicitação tem um token válido com um timestamp não expirado para o tipo de ação.

- Token válido — Quando a ação encontra um token válido e não bloqueia a solicitação, AWS WAF captura métricas e registros da seguinte forma:
  - Incrementa as métricas de `CaptchaRequests` e `RequestsWithValidCaptchaToken` ou `ChallengeRequests` e `RequestsWithValidChallengeToken`.
  - Registra a correspondência como uma entrada `nonTerminatingMatchingRules` com ação de CAPTCHA ou Challenge. A lista a seguir mostra a seção de um log desse tipo de correspondência com a ação CAPTCHA.

```
"nonTerminatingMatchingRules": [
{
  "ruleId": "captcha-rule",
  "action": "CAPTCHA",
  "ruleMatchDetails": [],
  "captchaResponse": {
    "responseCode": 0,
    "solveTimestamp": 1632420429
  }
}
```

```
  ]
```

- Token ausente, inválido ou expirado — Quando a ação bloqueia a solicitação devido a um token ausente ou inválido, AWS WAF captura métricas e registros da seguinte forma:
  - Incrementa a métrica para `CaptchaRequests` ou `ChallengeRequests`.
  - Registra a correspondência como uma entrada `CaptchaResponse` com código de status HTTP `405` ou como uma entrada `ChallengeResponse` com código de status HTTP `202`. O log indica se a solicitação não tinha o token ou tinha um timestamp expirado. O registro também indica se AWS WAF enviou uma página intersticial CAPTCHA para o cliente ou um desafio silencioso para o navegador do cliente. A lista a seguir mostra as seções de um log desse tipo de correspondência com a ação CAPTCHA.

```
"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
```

Para obter informações sobre os AWS WAF registros, consulteRegistrando AWS WAF tráfego de ACL da web.

Para obter informações sobre AWS WAF métricas, consulteAWS WAF métricas e dimensões.

Para obter informações sobre as opções de ação de regra, consulte Ação da regra.

Práticas recomendadas para usar as ações CAPTCHA e Challenge

Siga as orientações nesta seção para planejar e implementar o AWS WAF CAPTCHA ou o desafio.

Planeje sua implementação de CAPTCHA e desafio

Determine onde colocar os quebra-cabeças CAPTCHA ou os desafios silenciosos com base no uso do seu site, na sensibilidade dos dados que você deseja proteger e no tipo de solicitação. Selecione

as solicitações nas quais você aplicará o CAPTCHA para apresentar os quebra-cabeças conforme necessário, mas evite apresentá-los onde eles não seriam úteis e poderiam prejudicar a experiência do usuário. Use a Challenge ação para executar desafios silenciosos que tenham menos impacto no usuário final, mas ainda ajudem a verificar se a solicitação vem de um navegador JavaScript habilitado.

Os quebra-cabeças de CAPTCHA e os desafios silenciosos só podem ser executados quando os navegadores estão acessando endpoints HTTPS. Os clientes do navegador devem estar sendo executados em contextos seguros para adquirir tokens.

Decida onde executar quebra-cabeças CAPTCHA e desafios silenciosos em seus clientes

Identifique solicitações que você não quer que sejam afetadas pelo CAPTCHA, por exemplo, solicitações de CSS ou imagens. Use CAPTCHA somente quando necessário. Por exemplo, se você planeja fazer uma verificação de CAPTCHA no login e o usuário sempre é levado diretamente do login para outra tela, a exigência de uma verificação de CAPTCHA na segunda tela provavelmente não seria necessária e poderia prejudicar sua experiência de usuário final.

Configure seu Challenge e CAPTCHA use para que AWS WAF só envie quebra-cabeças CAPTCHA e desafios silenciosos em resposta às solicitações. `GET` `text/html` Você não pode resolver o quebra-cabeça nem o desafio em resposta a solicitações `POST`, solicitações `OPTIONS` de comprovação do compartilhamento de recursos de origem cruzada (CORS) ou qualquer outro tipo de solicitação não `GET`. O comportamento do navegador para outros tipos de solicitação pode variar e talvez não consiga lidar com as intersticiais adequadamente.

É possível que um cliente aceite HTML, mas ainda não consiga lidar com a intersticial do CAPTCHA ou desafio. Por exemplo, um widget em uma página da web com um iFrame pequeno pode aceitar HTML, mas não conseguir exibir um CAPTCHA ou processá-lo. Evite colocar as ações de regra para esses tipos de solicitações, da mesma forma que para solicitações que não aceitam HTML.

Use CAPTCHA ou Challenge para verificar a aquisição prévia do token

Você pode usar as ações da regra somente para verificar a existência de um token válido, em locais onde usuários legítimos sempre devem ter um. Nessas situações, não importa se a solicitação pode lidar com os intersticiais.

Por exemplo, se você implementar a API CAPTCHA do aplicativo JavaScript cliente e executar o quebra-cabeça CAPTCHA no cliente imediatamente antes de enviar a primeira solicitação ao seu endpoint protegido, sua primeira solicitação sempre deverá incluir um token válido tanto para o

desafio quanto para o CAPTCHA. Para obter informações sobre a integração JavaScript do aplicativo cliente, consulteAWS WAF JavaScript integrações.

Para essa situação, em sua web ACL, você pode adicionar uma regra que corresponda a essa primeira chamada e configurá-la com a ação de regra Challenge ou CAPTCHA. Quando a regra coincide com um usuário final e um navegador legítimos, a ação encontrará um token válido e, portanto, não bloqueará a solicitação nem enviará um desafio ou um quebra-cabeça CAPTCHA em resposta. Para obter mais informações sobre como as ações de regra funcionam, consulte Comportamento de ações CAPTCHA e Challenge.

Proteja seus dados confidenciais não HTML com CAPTCHA e Challenge

Você pode usar CAPTCHA e proteções Challenge para dados confidenciais não HTML, como APIs, com a abordagem a seguir.

1. Identifique as solicitações que recebem respostas em HTML e que são executadas próximas às solicitações de seus dados confidenciais que não sejam HTML.
2. Escreva regras CAPTCHA ou Challenge que correspondam às solicitações de HTML e às solicitações de seus dados confidenciais.
3. Ajuste suas configurações de tempo de imunidade de CAPTCHA e Challenge para que, nas interações normais do usuário, os tokens que os clientes obtêm das solicitações de HTML estejam disponíveis e não expirem em suas solicitações de dados confidenciais. Para obter informações sobre ajustes, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.

Quando uma solicitação de seus dados confidenciais corresponder a uma regra CAPTCHA ou Challenge, ela não será bloqueada se o cliente ainda tiver um token válido do quebra-cabeça ou desafio anterior. Se o token não estiver disponível ou o timestamp expirar, a solicitação para acessar seus dados confidenciais falhará. Para obter mais informações sobre como as ações de regra funcionam, consulte Comportamento de ações CAPTCHA e Challenge.

Use CAPTCHA e Challenge para ajustar suas regras existentes

Revise suas regras existentes para ver se você deseja alterá-las ou adicioná-las. Veja a seguir alguns cenários comuns a serem considerados.

- Se você tem uma regra baseada em intervalos que bloqueia o tráfego, mas mantém o limite de intervalo relativamente alto para evitar o bloqueio de usuários legítimos, considere adicionar uma segunda regra baseada em intervalos após a regra de bloqueio. Dê à segunda regra um limite

inferior ao da regra de bloqueio e defina a ação da regra como CAPTCHA ou Challenge. A regra de bloqueio ainda bloqueará solicitações que estão chegando com um intervalo muito alto, e a nova regra bloqueará a maior parte do tráfego automatizado a um intervalo ainda menor. Para obter mais informações sobre regras baseadas em intervalos, consulte Instrução de regra baseada em intervalos.

- Se você tiver um grupo de regras gerenciadas que bloqueia solicitações, poderá mudar o comportamento de algumas ou de todas as regras de Block para CAPTCHA ou Challenge. Para fazer isso, na configuração do grupo de regras gerenciadas, substitua a configuração da ação da regra. Para obter mais informações sobre modificar ações de regra, consulte Substituições de ações de regras de grupos de regras.

Teste seu CAPTCHA e desafie as implementações antes de implantá-las

Quanto a todas as novas funcionalidades, siga as orientações em the section called “Testar e ajustar suas proteções”.

Durante o teste, revise os requisitos de expiração do timestamp do token e defina as configurações de tempo de imunidade em nível de regra e web ACL para obter um bom equilíbrio entre controlar o acesso ao seu site e fornecer uma boa experiência aos seus clientes. Para mais informações, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token.

Registrando AWS WAF tráfego de ACL da web

Você pode habilitar o registro em log para obter informações detalhadas sobre o tráfego que é analisado pela web ACL. As informações registradas incluem a hora em que AWS WAF recebeu uma solicitação da web do seu AWS recurso, informações detalhadas sobre a solicitação e detalhes sobre as regras às quais a solicitação correspondeu. Você pode enviar registros de ACL da web para um grupo de CloudWatch logs do Amazon Logs, um bucket do Amazon Simple Storage Service (Amazon S3) ou um stream de entrega do Amazon Data Firehose.

Outras opções de coleta e análise de dados

Além do registro, você pode ativar as seguintes opções para coleta e análise de dados:

- Amazon Security Lake — Você pode configurar o Security Lake para coletar dados de ACL da web. O Security Lake coleta dados de registros e eventos de várias fontes para normalização, análise e gerenciamento. Para obter informações sobre essa opção, consulte O que é o Amazon Security Lake? e Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.

AWS WAF não cobra pelo uso dessa opção. Para obter informações sobre preços, consulte Preços do Security Lake e Como os preços do Security Lake são determinados no guia do usuário do Amazon Security Lake.

- Amostragem de solicitações — Você pode configurar sua ACL da web para obter amostras das solicitações da web que ela avalia, para ter uma ideia do tipo de tráfego que seu aplicativo está recebendo. Para obter mais informações sobre esta opção, consulte Visualizar um exemplo de solicitações da web.

> **Note**
>
> A configuração de registro do Web ACL afeta somente os AWS WAF registros. Em particular, a configuração de campos editados para registro não tem impacto na amostragem de solicitações ou na coleta de dados do Security Lake. A coleta de dados do Security Lake é configurada inteiramente por meio do serviço Security Lake. A única maneira de excluir campos das solicitações de amostra é desabilitando a amostragem para a ACL da web.

Tópicos

Preços para registrar informações de tráfego de web ACL

Você é cobrado pelo registro das informações de tráfego da web ACL de acordo com os custos associados a cada tipo de destino de log. Essas cobranças são adicionais às cobranças de uso do AWS WAF. Seus custos podem variar dependendo de fatores como o tipo de destino escolhido e a quantidade de dados que você registra.

Veja a seguir links para as informações de preços de cada tipo de destino de logs:

- CloudWatch Registros — As cobranças são pela entrega de toras vendidas. Consulte os preços do Amazon CloudWatch Logs. Em Nível pago, escolha a guia Registros e, em Vended Logs, veja as informações de Entrega para CloudWatch registros.
- Buckets Amazon S3 — As cobranças do Amazon S3 são as cobranças combinadas pela entrega de CloudWatch logs vendidos pelos Logs para os buckets do Amazon S3 e pelo uso do Amazon S3.
  - Para o Amazon S3, consulte Preços do Amazon S3.
  - Para entrega de CloudWatch registros vendidos pela Logs para o Amazon S3, consulte CloudWatch Amazon Logs Pricing. Em Nível pago, escolha a guia Logs e, em Logs fornecidos, veja as informações de Entrega para o S3.
- Firehose — Veja os preços do Amazon Data Firehose.

Para obter informações sobre AWS WAF preços, consulte AWS WAF Preços.

AWS WAF destinos de registro

Esta seção descreve as opções de registro que você pode escolher para seus logs do AWS WAF . Cada seção fornece orientações para configurar os logs, incluindo informações sobre qualquer comportamento específico para o tipo de destino. Depois de configurar seu destino de logs, você pode fornecer suas especificações para a configuração de logs da sua web ACL para iniciar o registro nele.

Tópicos

- Grupo de CloudWatch registros do Amazon Logs
- Bucket do Amazon Simple Storage Service
- Stream de entrega do Amazon Data Firehose

Grupo de CloudWatch registros do Amazon Logs

Este tópico fornece informações para enviar seus registros de tráfego da Web ACL para um grupo de CloudWatch registros de registros.

> **Note**
>
> Você é cobrado pelo login, além das cobranças pelo uso do AWS WAF. Para mais informações, consulte Preços para registrar informações de tráfego de web ACL.

Para enviar registros para o Amazon CloudWatch Logs, você cria um grupo de CloudWatch registros de registros. Ao ativar o login AWS WAF, você fornece o ARN do grupo de registros. Depois de ativar o registro para sua ACL da web, AWS WAF entrega os registros para o grupo de CloudWatch registros de registros em fluxos de registros.

Ao usar o CloudWatch Logs, você pode explorar os registros da sua ACL da web no AWS WAF console. Na sua página de web ACL, selecione a guia Log Insights. Essa opção é um acréscimo aos insights de registro fornecidos para o CloudWatch Logs por meio do CloudWatch console.

Configure o grupo de registros para registros de ACL AWS WAF da web na mesma região da ACL da web e usando a mesma conta que você usa para gerenciar a ACL da web. Para obter informações sobre como configurar um grupo de CloudWatch registros, consulte Como trabalhar com grupos de registros e fluxos de registros.

Cotas para grupos de CloudWatch registros de registros

CloudWatch O Logs tem uma cota máxima padrão de taxa de transferência, compartilhada entre todos os grupos de registros em uma região, que você pode solicitar para aumentar. Se seus requisitos de registro forem muito altos para a configuração atual de taxa de transferência, você verá métricas de limitação `PutLogEvents` para sua conta. Para ver o limite no console Service Quotas e solicitar um aumento, consulte a cota de CloudWatch registros PutLogEvents .

Nomenclatura de grupos de logs

Os nomes dos grupos de logs devem começar com `aws-waf-logs-` e terminar com qualquer sufixo que você quiser, por exemplo, `aws-waf-logs-testLogGroup2`.

O formato resultante do ARN é o seguinte:

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

Os fluxos de log têm o seguinte formato de nomenclatura:

```
Region_web-acl-name_log-stream-number
```

O exemplo a seguir mostra um exemplo de fluxo de log para web ACL `TestWebACL` na região `us-east-1`.

```
us-east-1_TestWebACL_0
```

Permissões necessárias para publicar registros no CloudWatch Logs

A configuração do registro de tráfego da Web ACL para um grupo de CloudWatch registros de registros requer as configurações de permissões descritas nesta seção. As permissões são definidas para você quando você usa uma das políticas gerenciadas de acesso AWS WAF total, `AWSWAFConsoleFullAccess` ou`AWSWAFFullAccess`. Se você quiser gerenciar um acesso mais refinado ao seu registro e aos seus AWS WAF recursos, você mesmo pode definir as permissões. Para obter informações sobre o gerenciamento de permissões, consulte Gerenciamento de acesso para AWS recursos no Guia do usuário do IAM. Para obter informações sobre as políticas gerenciadas do AWS WAF , consulte AWS políticas gerenciadas para AWS WAF.

Essas permissões permitem que você altere a configuração de registro da Web ACL, configure a entrega de CloudWatch registros para registros e recupere informações sobre seu grupo de registros. Essas permissões devem ser anexadas ao usuário que você usa para gerenciar o AWS WAF.

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

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
```

```
         "Action":[
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Quando as ações são permitidas em todos os AWS recursos, isso é indicado na política com uma `"Resource"` configuração de`"*"`. Isso significa que as ações são permitidas em todos os AWS recursos que cada ação suporta. Por exemplo, a ação `wafv2:PutLoggingConfiguration` é suportada somente para `wafv2` registrar recursos de configuração.

Bucket do Amazon Simple Storage Service

Este tópico fornece informações para enviar seus logs de tráfego da web ACL para um bucket do Amazon S3.

> **Note**
>
> Você é cobrado pelo login, além das cobranças pelo uso do AWS WAF. Para obter mais informações, consulte Preços para registrar informações de tráfego de web ACL.

Para enviar seus logs de tráfego da web ACL para o Amazon S3, você configura um bucket do Amazon S3 a partir da mesma conta que usa para gerenciar a web ACL e nomeia o bucket começando com `aws-waf-logs-`. Ao ativar o login AWS WAF, você fornece o nome do bucket. Para obter informações sobre como criar um bucket de log, consulte Criar um bucket, no Guia do usuário do Amazon Simple Storage Service.

Você pode acessar e analisar seus logs do Amazon S3 usando o serviço de consulta interativa do Amazon Athena. O Athena facilita analisar dados diretamente no Amazon S3 com o SQL padrão. Com algumas ações no AWS Management Console, você pode direcionar o Athena para seus dados armazenados no Amazon S3 e começar rapidamente a usar o SQL padrão para executar

consultas ad-hoc e obter resultados. Para obter mais informações, consulte Como consultar AWS WAF registros no guia do usuário do Amazon Athena. Para exemplos adicionais de consultas do Amazon Athena, consulte waf-log-sample-athenaaws-samples/ -queries no site. GitHub

> **Note**
>
> AWS WAF suporta criptografia com buckets Amazon S3 para o tipo de chave Amazon S3 (SSE-S3) e para (SSE-KMS). AWS Key Management Service AWS KMS keys AWS WAF não oferece suporte à criptografia para AWS Key Management Service chaves gerenciadas pelo AWS.

Suas web ACLspublicam seus arquivos de log no bucket do Amazon S3 em intervalos de cinco minutos. Cada arquivo de log contém os registros de log de fluxo para o tráfego de IP registrado nos últimos cinco minutos.

O tamanho máximo de um arquivo de log é de 75 MB. Se o arquivo de log atingir o limite de tamanho no período de 5 minutos, o log para de adicionar registros de log de fluxo, publica o arquivo no bucket do Amazon S3 e cria um novo arquivo de log.

Os arquivos de log são compactados. Se você abrir os arquivos usando o console do Amazon S3, o Amazon S3 descompacta os registros de log e os exibe. Se você baixar os arquivos de log, será necessário descompactá-los para visualizar os registros de log de fluxo.

Um único arquivo de log contém entradas intercaladas com vários registros. Para ver todos os arquivos de log de uma web ACL, procure entradas agregadas pelo nome da web ACL, região e ID da sua conta.

Requisitos de nomenclatura e sintaxe

Os nomes dos seus buckets para AWS WAF registro devem começar com `aws-waf-logs-` e terminar com qualquer sufixo que você quiser. Por exemplo, `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Localização do bucket

Os locais do bucket usam a seguinte sintaxe:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

ARN do bucket

O formato do bucket do nome do recurso da Amazon (ARN) é o seguinte:

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Localizações de buckets com prefixos

Se você usar prefixos no nome das chaves de objeto para organizar os dados que você armazena nos seus buckets, você pode fornecer seus prefixos nos nomes dos buckets de logs.

> **Note**
>
> Essa opção não está disponível no console. Use as AWS WAF APIs, a CLI ou. AWS CloudFormation

Para obter informações sobre o uso de prefixos no Amazon S3, consulte Organização de objetos usando prefixos no Guia do usuário do Amazon Simple Storage Service.

Os locais do bucket com prefixos usam a seguinte sintaxe:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Pastas e nomes de arquivos do bucket

Dentro de seus buckets, e seguindo os prefixos fornecidos por você, seus AWS WAF registros são gravados em uma estrutura de pastas determinada pelo ID da conta, pela região, pelo nome da ACL da web e pela data e hora.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

Dentro das pastas, os nomes dos arquivos de log seguem um formato semelhante:

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

As especificações de hora usadas na estrutura de pastas e no nome do arquivo de log seguem a especificação de formato de timestamp `YYYYMMddTHHmmZ`.

Veja abaixo um exemplo de arquivo de log em um bucket do Amazon S3 para um bucket chamado `DOC-EXAMPLE-BUCKET`. O Conta da AWS é`11111111111`. A web ACL é `TEST-WEBACL` e a região é `us-east-1`.

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> Os nomes dos seus buckets para AWS WAF registro devem começar com `aws-waf-logs-` e terminar com qualquer sufixo que você quiser.

Permissões necessárias para publicar logs no Amazon S3

Configurar os logs de tráfego da web ACL para um bucket do Amazon S3 requer as seguintes configurações de permissão. Essas permissões são definidas para você quando você usa uma das políticas gerenciadas de acesso total do AWS WAF , `AWSWAFConsoleFullAccess` ou `AWSWAFFullAccess`. Se você quiser gerenciar um acesso mais refinado ao seu registro e aos seus AWS WAF recursos, você mesmo pode definir essas permissões. Para obter informações sobre como gerenciar permissões, consulte Gerenciamento de acesso a recursos da AWS no Guia do usuário do IAM. Para obter informações sobre as políticas AWS WAF gerenciadas, consulteAWS políticas gerenciadas para AWS WAF.

As permissões a seguir permitem que você altere a configuração de logs de web ACL e configure a entrega de logs para seu bucket do Amazon S3. Essas permissões devem ser anexadas ao usuário que você usa para gerenciar o AWS WAF.

> **Note**
>
> Ao definir as permissões listadas abaixo, você pode ver erros em seus AWS CloudTrail registros que indicam acesso negado, mas as permissões estão corretas para o AWS WAF registro.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
```

```
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Quando as ações são permitidas em todos os AWS recursos, isso é indicado na política com uma `"Resource"` configuração de`"*"`. Isso significa que as ações são permitidas em todos os AWS recursos que cada ação suporta. Por exemplo, a ação `wafv2:PutLoggingConfiguration` é suportada somente para `wafv2` registrar recursos de configuração.

Por padrão, os buckets do Amazon S3 e os objetos que eles contêm são privados. Somente o proprietário do bucket pode acessá-los. No entanto, o proprietário do bucket pode conceder acesso a outros recursos e usuários por meio da criação de uma política de acesso.

Se o usuário que cria um log de fluxo possui o bucket, o serviço anexa automaticamente as políticas de bucket a seguir para conceder permissão ao log de fluxo para publicar logs nele:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
```

```
      }
    }
  ]
}
```

> **Note**
>
> Os nomes dos seus buckets para AWS WAF registro devem começar com `aws-waf-logs-` e terminar com qualquer sufixo que você quiser.

Se o usuário que cria o log não possui o bucket nem tem as permissões `GetBucketPolicy` e `PutBucketPolicy` para o bucket, ocorre uma falha na criação do log de fluxo. Nesse caso, o proprietário do bucket deve adicionar manualmente as políticas acima ao bucket e especificar o ID do Conta da AWS do criador do log. Para obter mais informações, consulte Como adiciono uma política de bucket do S3? no Guia do usuário do Amazon Simple Storage Service. Se o bucket recebe logs de fluxo de várias contas, adicione uma entrada de elemento `Resource` à instrução de política `AWSLogDeliveryWrite` para cada conta.

Por exemplo, a política de bucket a seguir Conta da AWS `111122223333` permite publicar registros em um bucket chamado`aws-waf-logs-`*`DOC-EXAMPLE-BUCKET`*:

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
```

```
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

Permissões para uso de AWS Key Management Service com uma chave KMS

Se seu destino de registro usa criptografia do lado do servidor com chaves armazenadas em AWS Key Management Service (SSE-KMS) e você usa uma chave gerenciada pelo cliente (chave KMS), você deve dar AWS WAF permissão para usar sua chave KMS. Para fazer isso, você adiciona uma política de chave à chave KMS do destino escolhido. Isso permite que os logs do AWS WAF gravem seus arquivos de log no seu destino.

Adicione a seguinte política de chaves à sua chave KMS AWS WAF para permitir o login no seu bucket do Amazon S3.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
```

```
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Permissões necessárias para acessar arquivos de log do Amazon S3

O Amazon S3 usa listas de controle de acesso (ACLs) para gerenciar o acesso aos arquivos de log criados por um log AWS WAF . Por padrão, o proprietário do bucket tem permissões `FULL_CONTROL` em cada arquivo de log. O proprietário da entrega de logs, se é diferente do proprietário do bucket, não tem nenhuma permissão. A conta de entrega de logs tem permissões `READ` e `WRITE`. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon Simple Storage Service.

Stream de entrega do Amazon Data Firehose

Esta seção fornece informações para enviar seus registros de tráfego de ACL da web para um stream de entrega do Amazon Data Firehose.

> **Note**
>
> Você é cobrado pelo login, além das cobranças pelo uso do AWS WAF. Para mais informações, consulte Preços para registrar informações de tráfego de web ACL.

Para enviar registros para o Amazon Data Firehose, você envia registros da sua ACL da web para um stream de entrega do Amazon Data Firehose que você configura no Firehose. Depois de ativar o registro, AWS WAF entrega os registros ao seu destino de armazenamento por meio do endpoint HTTPS do Firehose.

Um AWS WAF registro é equivalente a um registro do Firehose. Se você normalmente recebe 10.000 solicitações por segundo e ativa registros completos, deve ter uma configuração de 10.000 registros por segundo no Firehose. Se você não configurar o Firehose corretamente, não AWS WAF gravará todos os registros. Para obter mais informações, consulte as cotas do Amazon Kinesis Data Firehose.

Para obter informações sobre como criar um stream de entrega do Amazon Data Firehose e revisar seus registros armazenados, consulte O que é o Amazon Data Firehose?

Para obter informações sobre como criar seu stream de entrega, consulte Criação de um stream de entrega do Amazon Data Firehose.

Configurando um stream de entrega do Amazon Data Firehose para sua ACL web

Configure um stream de entrega do Amazon Data Firehose para sua ACL web da seguinte forma.

- Crie-o usando a mesma conta que você usa para gerenciar a web ACL.
- Crie-o na mesma região da web ACL. Se você estiver capturando registros para a Amazon CloudFront, crie a mangueira de incêndio na região Leste dos EUA (Norte da Virgínia),. `us-east-1`
- Dê ao data firehose um nome que comece com o prefixo `aws-waf-logs-`. Por exemplo, `aws-waf-logs-us-east-2-analytics`.
- Configure-o para colocação direta, o que permite que os aplicativos acessem diretamente o fluxo de entrega. No console do Amazon Data Firehose, para a configuração Fonte do stream de entrega, escolha Direct PUT ou outras fontes. Por meio da API, defina a propriedade do fluxo de entrega `DeliveryStreamType` como `DirectPut`.

> **Note**
>
> Não use um `Kinesis stream` como fonte.

Permissões necessárias para publicar registros em um stream de entrega do Amazon Data Firehose

Para entender as permissões necessárias para a configuração do Kinesis Data Firehose, consulte Controlar o acesso com o Amazon Kinesis Data Firehose.

Você deve ter as seguintes permissões para habilitar com sucesso o registro de ACL na web com um stream de entrega do Amazon Data Firehose.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Para obter mais informações sobre funções vinculadas ao serviço e a permissão do `iam:CreateServiceLinkedRole`, consulte Usando funções vinculadas a serviços para AWS WAF.

Configuração de registro do Web ACL

É possível habilitar e desabilitar o registro em log para uma web ACL a qualquer momento.

> **Note**
>
> Você é cobrado pelo login, além das cobranças pelo uso do AWS WAF. Para obter mais informações, consulte Preços para registrar informações de tráfego de web ACL.

Se não for possível encontrar um registro em log em seus logs

Em raras ocasiões, é possível que a entrega de AWS WAF registros fique abaixo de 100%, com registros entregues com base no melhor esforço. A AWS WAF arquitetura prioriza a segurança de seus aplicativos acima de todas as outras considerações. Em algumas situações, como quando os fluxos de registro em log sofrem controle de utilização de tráfego, isso pode resultar no descarte de registros. Isso não deve afetar mais do que alguns registros. Se você notar a ausência de diversas entradas de log, entre em contato com o AWS Support Center.

Na configuração de registro da sua ACL da web, você pode personalizar o que é AWS WAF enviado para os registros.

- Redação de campo: você pode editar os seguintes campos dos registros de log para as regras que usam as configurações de correspondência correspondentes: Caminho do URI, String de consulta, Cabeçalho único e Método HTTP. Os campos editados são exibidos como `REDACTED` nos logs. Por exemplo, se você editar o campo String de consulta, nos logs, ele será listado como `REDACTED` para todas as regras que usam a configuração de componente de correspondência String de consulta. A edição se aplica somente ao componente de solicitação que você especifica para correspondência na regra, portanto, a edição do componente Cabeçalho único não se aplica às regras que correspondem em Cabeçalhos. Para obter uma lista de campos de log, consulte Campos de log.

  > **Note**
  >
  > Essa configuração não tem impacto na amostragem da solicitação. Com a amostragem de solicitações, a única maneira de excluir campos é desabilitando a amostragem para a ACL da web.

- Filtragem de log: você pode adicionar filtros para especificar quais solicitações da web são mantidas nos logs e quais são removidas. Você filtra as configurações que AWS WAF se aplicam durante a avaliação da solicitação da web. Você pode filtrar nas seguintes configurações:
  - Rótulos totalmente qualificados: rótulos totalmente qualificados têm um prefixo, namespaces opcionais e nome de rótulo. O prefixo identifica o grupo de regras ou o contexto de web ACL da regra que adicionou o rótulo. Para obter informações sobre rótulos, consulte AWS WAF rótulos em solicitações da web.
  - Ação de regra: você pode filtrar por qualquer configuração de ação de regra normal e também pela opção de substituição antiga `EXCLUDED_AS_COUNT` para regras de grupos de regras. Para informações sobre as configurações de ações de regra, consulte Ação da regra. Para obter informações sobre substituições de ações de regras atuais e antigas para regras de grupos de regras, consulte Opções de substituição de ação para grupos de regras.
    - Os filtros normais de ação de regra se aplicam às ações configuradas nas regras e também às ações configuradas usando a opção atual para substituir uma ação de regra do grupo de regras.
    - O filtro de log `EXCLUDED_AS_COUNT` se sobrepõe ao filtro de log de ação `Count`. `EXCLUDED_AS_COUNT` filtra as opções atuais e antigas para substituir uma ação de regra de grupo de regras para Count.

Habilitando o registro para uma ACL da web

Para habilitar o registro em um Web ACL, você já deve ter configurado um destino de registro. Para obter informações sobre suas opções de destino e os requisitos de cada uma, consulte AWS WAF destinos de registro.

Para habilitar o registro de uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Selecione o nome da web ACL para a qual você deseja habilitar o registro em log. O console leva você para a descrição da web ACL, onde é possível editá-la.
4. Na guia Registro em log, selecione Habilitar registro em log.
5. Escolha o tipo de destino de logs e, em seguida, escolha o destino de logs que você configurou. Você deve escolher um destino de registro em log cujo nome comece com `aws-waf-logs-`.

6. (Opcional) Se você não quiser que alguns campos sejam incluídos nos logs, edite-os. Selecione o campo para editar e, em seguida, selecione Adicionar. Repita conforme necessário para editar campos adicionais.

> **Note**
>
> Essa configuração não tem impacto na amostragem da solicitação. Com a amostragem de solicitações, a única maneira de excluir campos é desabilitando a amostragem para a ACL da web.

7. (Opcional) Se você não quiser enviar todas as solicitações para os logs, adicione seus critérios e comportamento de filtragem. Em Filtrar logs, para cada filtro que você deseja aplicar, escolha Adicionar filtro, escolha seus critérios de filtragem e especifique se deseja manter ou eliminar solicitações que correspondam aos critérios. Ao terminar de adicionar filtros, se necessário, modifique o Comportamento de registro de logs padrão.
8. Selecione Habilitar registro em log.

> **Note**
>
> Quando você habilitar o registro com êxito, AWS WAF criará uma função vinculada ao serviço com as permissões necessárias para gravar registros no destino do registro. Para ter mais informações, consulte Usando funções vinculadas a serviços para AWS WAF.

Campos de log

A lista a seguir descreve os possíveis campos dos registros em log.

ação

A ação de encerramento AWS WAF aplicada à solicitação. Isso indica permissão, bloqueio, CAPTCHA ou desafio. As ações CAPTCHA e Challenge são encerradas quando a solicitação da web não contém um token válido.

args

A string de consulta.

captchaResponse

O status da ação CAPTCHA da solicitação, preenchido quando uma CAPTCHA ação é aplicada à solicitação. Esse campo é preenchido para qualquer CAPTCHA ação, seja ela de encerramento ou não. Se uma solicitação tiver a CAPTCHA ação aplicada várias vezes, esse campo será preenchido a partir da última vez em que a ação foi aplicada.

A ação CAPTCHA encerra a inspeção da solicitação da web quando a solicitação não inclui um token ou o token é inválido ou expirou. Se a CAPTCHA ação estiver sendo encerrada, esse campo incluirá um código de resposta e o motivo da falha. Se a ação não for finalizada, esse campo incluirá um carimbo de data/hora de resolução. Para diferenciar entre uma ação de encerramento e uma ação não encerradora, você pode filtrar por um atributo não vazio nesse campo`failureReason`.

challengeResponse

O status da ação de desafio da solicitação, preenchido quando uma Challenge ação é aplicada à solicitação. Esse campo é preenchido para qualquer Challenge ação, seja ela de encerramento ou não. Se uma solicitação tiver a Challenge ação aplicada várias vezes, esse campo será preenchido a partir da última vez em que a ação foi aplicada.

A ação Challenge encerra a inspeção da solicitação da web quando a solicitação não inclui um token ou o token é inválido ou expirou. Se a Challenge ação estiver sendo encerrada, esse campo incluirá um código de resposta e o motivo da falha. Se a ação não for finalizada, esse campo incluirá um carimbo de data/hora de resolução. Para diferenciar entre uma ação de encerramento e uma ação não encerradora, você pode filtrar por um atributo não vazio nesse campo`failureReason`.

clientIp

O endereço IP do cliente que está enviando a solicitação.

country

O país de origem da solicitação. Se não AWS WAF for possível determinar o país de origem, ele definirá esse campo como`-`.

excludedRules

Usado somente para regras de grupo de regras. A lista de regras no grupo de regras que você excluiu. A ação para essas regras é definida como Count.

Se você substituir uma regra para contar usando a opção de ação de substituição da regra, as correspondências não serão listadas aqui. Elas estão listadas como pares de ação `action` e `overriddenAction`.

exclusionType

Um tipo que indica que a regra excluída tem a ação Count.

ruleId

O ID da regra no grupo de regras que foi excluída.

formatVersion

A versão do formato do log.

headers

A lista de cabeçalhos.

httpMethod

O método HTTP na solicitação.

httpRequest

Os metadados sobre a solicitação.

httpSourceId

O identificador do recurso associado:

- Para uma CloudFront distribuição da Amazon, o ID está *`distribution-id`* na sintaxe do ARN:

  `arn:`*`partition`*`cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*

- Para um Application Load Balancer, o ID é o *`load-balancer-id`* na sintaxe do ARN:

  `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account-id`*`:loadbalancer/app/`*`load-balancer-name/load-balancer-id`*

- Para uma API REST do Amazon API Gateway, o ID é o *`api-id`* na sintaxe do ARN:

  `arn:`*`partition`*`:apigateway:`*`region`*`::/restapis/`*`api-id`*`/stages/`*`stage-name`*

- Para uma API do AWS AppSync GraphQL, o ID está *`GraphQLApiId`* na sintaxe do ARN:

  `arn:`*`partition`*`:appsync:`*`region`*`:`*`account-id`*`:apis/`*`GraphQLApiId`*

- Para um grupo de usuários do Amazon Cognito, o ID é o *user-pool-id* na sintaxe do ARN:

  `arn:`*partition*`:cognito-idp:`*region*`:`*account-id*`:userpool/`*user-pool-id*

- Para um AWS App Runner serviço, o ID está *apprunner-service-id* na sintaxe do ARN:

  `arn:`*partition*`:apprunner:`*region*`:`*account-id*`:service/`*apprunner-service-name*`/`*apprunner-service-id*

httpSourceName

A origem da solicitação. Valores possíveis: `CF` para Amazon CloudFront, `APIGW` Amazon API Gateway, `ALB` Application Load Balancer, `APPSYNC` Amazon Cognito AWS AppSync`APPRUNNER`, `COGNITOIDP` App Runner e Verified Access. `VERIFIED_ACCESS`

httpVersion

A versão HTTP.

ja3Fingerprint

A impressão digital JA3 da solicitação.

> **Note**
>
> A inspeção de impressão digital JA3 está disponível somente para CloudFront distribuições da Amazon e Application Load Balancers.

A impressão digital JA3 é um hash de 32 caracteres derivado do Hello do cliente TLS de uma solicitação recebida. Essa impressão digital serve como um identificador exclusivo para a configuração TLS do cliente. AWS WAF calcula e registra essa impressão digital para cada solicitação que tenha informações suficientes do TLS Client Hello para o cálculo.

Você fornece esse valor ao configurar uma correspondência de impressão digital JA3 em suas regras de web ACL. Para obter informações sobre como criar uma correspondência com a impressão digital JA3, consulte Impressão digital JA3 no Solicitar opções de componentes para obter uma instrução de regra.

rótulos

Os rótulos na solicitação da web. Esses rótulos foram aplicados por regras usadas para avaliar a solicitação. AWS WAF registra os primeiros 100 rótulos.

nonTerminatingMatchingRegras

A lista de regras não encerradas que corresponderam à solicitação. Cada item na lista contém as seguintes informações.

ação

A ação AWS WAF aplicada à solicitação. Isso indica contagem, CAPTCHA ou desafio. O CAPTCHA e o Challenge são de não encerramento quando a solicitação da web contém um token válido.

ruleId

O ID da regra que correspondeu à solicitação e que não era de encerramento.

ruleMatchDetails

Informações detalhadas sobre a regra que correspondeu à solicitação. Isso é preenchido somente para instruções de regra de correspondência de injeção de SQL e cross-site scripting (XSS). Uma regra de correspondência pode exigir uma correspondência para mais de um critério de inspeção, portanto, esses detalhes da correspondência são fornecidos como uma matriz de critérios de correspondência.

Qualquer informação adicional fornecida para cada regra varia de acordo com fatores como a configuração da regra, o tipo de correspondência da regra e os detalhes da correspondência. Por exemplo, para regras com uma Challenge ação CAPTCHA ou, o `captchaResponse` ou `challengeResponse` será listado. Se a regra correspondente estiver em um grupo de regras e você tiver substituído a ação de regra configurada, a ação configurada será fornecida em. `overriddenAction`

oversizeFields

A lista de campos na solicitação da web que foram inspecionados pela ACL da web e que estão acima do limite de AWS WAF inspeção. Se um campo for muito grande, mas a web ACL não o inspecionar, ele não será listado aqui.

Essa lista pode conter zero ou mais dos seguintes valores: `REQUEST_BODY`, `REQUEST_JSON_BODY`, `REQUEST_HEADERS` e `REQUEST_COOKIES`. Para obter mais informações sobre os campos de tamanho acima do limite, consulte Tratamento de componentes de solicitação de tamanho grande no AWS WAF.

rateBasedRuleLista

A lista de regras baseadas em taxas que agiram na solicitação. Para obter mais informações sobre regras baseadas em intervalos, consulte Instrução de regra baseada em intervalos.

rateBasedRuleIdentificação

O ID da regra baseada em taxa que agiu na solicitação. Se isso encerrou a solicitação, o ID para `rateBasedRuleId` será o mesmo que o ID para `terminatingRuleId`.

rateBasedRuleNome

O ID da regra baseada em intervalos que agiu na solicitação.

limitKey

O tipo de agregação que a regra está usando. Os valores possíveis são `IP` para a origem da solicitação da web, `FORWARDED_IP` para um IP encaminhado em um cabeçalho na solicitação, `CUSTOMKEYS` para configurações personalizadas de chave agregada e `CONSTANT` para contar todas as solicitações juntas, sem agregação.

limitValue

Usado somente quando o intervalo é limitado por um único tipo de endereço IP. Se uma solicitação contiver um endereço IP que não seja válido, o `limitvalue` é `INVALID`.

maxRateAllowed

O número máximo de solicitações permitidas na janela de tempo especificada para uma instância de agregação específica. A instância de agregação é definida pelo `limitKey` acréscimo de quaisquer especificações de chave adicionais que você tenha fornecido na configuração da regra baseada em taxas.

evaluationWindowSec

A quantidade de tempo AWS WAF incluída na solicitação é contabilizada, em segundos.

customValues

Valores exclusivos identificados pela regra baseada em intervalos na solicitação. Para valores de string, os registros imprimem os primeiros 32 caracteres do valor da string. Dependendo do tipo de chave, esses valores podem ser apenas para uma chave, como para o método HTTP ou string de consulta, ou podem ser para uma chave e um nome, como para o cabeçalho e o nome do cabeçalho.

requestHeadersInserted

A lista de cabeçalhos inseridos para tratamento personalizado de solicitações.

requestId

O ID da solicitação, que é gerado pelo serviço de host subjacente. Para o Application Load Balancer, esse é o ID de rastreamento. Para todos os outros, esse é o ID da solicitação.

responseCodeSent

O código de resposta enviado com uma resposta personalizada.

ruleGroupId

O ID do grupo de regras. Se a regra bloqueou a solicitação, o ID para `ruleGroupID` será o mesmo que o ID para `terminatingRuleId`.

ruleGroupList

A lista de grupos de regras que agiram nessa solicitação, com informações de correspondência.

terminatingRule

O tipo de regra que encerrou a solicitação. Se isso estiver presente, ele conterá as seguintes informações.

ação

A ação de encerramento AWS WAF aplicada à solicitação. Isso indica permissão, bloqueio, CAPTCHA ou desafio. As ações CAPTCHA e Challenge são encerradas quando a solicitação da web não contém um token válido.

ruleId

A ID da regra que corresponde à solicitação.

ruleMatchDetails

Informações detalhadas sobre a regra que correspondeu à solicitação. Isso é preenchido somente para instruções de regra de correspondência de injeção de SQL e cross-site scripting (XSS). Uma regra de correspondência pode exigir uma correspondência para mais de um critério de inspeção, portanto, esses detalhes da correspondência são fornecidos como uma matriz de critérios de correspondência.

Qualquer informação adicional fornecida para cada regra varia de acordo com fatores como a configuração da regra, o tipo de correspondência da regra e os detalhes da correspondência.

Por exemplo, para regras com uma Challenge ação CAPTCHA ou, o `captchaResponse` ou `challengeResponse` será listado. Se a regra correspondente estiver em um grupo de regras e você tiver substituído a ação de regra configurada, a ação configurada será fornecida em. `overriddenAction`

terminatingRuleId

O ID da regra que encerrou a solicitação. Se nada encerrar a solicitação, o valor será `Default_Action`.

terminatingRuleMatchDetalhes

Informações detalhadas sobre a regra de encerramento que correspondeu à solicitação. Uma regra de encerramento tem uma ação que encerra o processo de inspeção em relação a uma solicitação da Web. As ações possíveis para uma regra de rescisão incluem Allow, Block, CAPTCHA e Challenge. Durante a inspeção de uma solicitação da web, na primeira regra que corresponda à solicitação e que tenha uma ação de encerramento, AWS WAF interrompe a inspeção e aplica a ação. A solicitação da web pode conter outras ameaças, além da que é relatada no log da regra de encerramento correspondente.

Isso é preenchido somente para instruções de regra de correspondência de injeção de SQL e cross-site scripting (XSS). A regra de correspondência pode exigir uma correspondência para mais de um critério de inspeção, portanto, esses detalhes da correspondência são fornecidos como uma matriz de critérios de correspondência.

terminatingRuleType

O tipo de regra que encerrou a solicitação. Valores possíveis: RATE_BASED, REGULAR, GROUP e MANAGED_RULE_GROUP.

timestamp

O timestamp em milissegundos.

uri

O URI da solicitação.

webaclId

O GUID da web ACL.

Exemplos de log

Example Regra baseada em intervalos 1: configuração da regra com uma chave, definida como **`Header:dogname`**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example Regra baseada em intervalos 1: entrada de log para solicitação bloqueada pela regra baseada em intervalos

```
{
   "timestamp":1683355579981,
```

```
    "formatVersion":1,
    "webaclId": ...,
    "terminatingRuleId":"RateBasedRule",
    "terminatingRuleType":"RATE_BASED",
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId": ...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.45",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.45"
          },
          {
             "name":"X-Forwarded-Proto",
```

```
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example Regra baseada em intervalos 2: configuração de regras com duas chaves, definidas como **`Header:dogname`** e **`Header:catname`**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
```

```
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example Regra baseada em intervalos 2: entrada de log para solicitação bloqueada pela regra baseada em intervalos

```
{
   "timestamp":1633322211194,
```

```
    "formatVersion":1,
    "webaclId":...,
    "terminatingRuleId":"RateBasedRule",
    "terminatingRuleType":"RATE_BASED",
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId":...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             },
             {
                "key":"HEADER",
                "name":"catname",
                "value":"goofie"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.35",
       "country":"FR",
       "headers":[
          {
```

```
            "name":"X-Forwarded-For",
            "value":"52.46.82.35"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
         },
         {
            "name":"catname",
            "value":"goofie"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example Saída de log para uma regra que foi acionada na detecção de SQLi (encerramento)


```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
```

```
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Saída de log para uma regra que foi acionada na detecção de SQLi (não encerramento)

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
```

```
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Saída de log para várias regras acionadas dentro de um grupo de regras (RuleA-XSS é de encerramento e Rule-B é de não encerramento)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
```

```
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
```

```
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Saída de log para uma regra que foi acionada para a inspeção de corpo da solicitação com o tipo de conteúdo JSON

AWS WAF atualmente relata a localização da inspeção corporal JSON comoUNKNOWN.

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
```

```
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Saída de log para uma regra CAPTCHA em relação a uma solicitação da web com um token CAPTCHA válido e não expirado

A lista de logs a seguir é para uma solicitação da web que correspondeu a uma regra com uma ação CAPTCHA. A solicitação da web tem um token CAPTCHA válido e não expirado e só é anotada como uma correspondência de CAPTCHA por AWS WAF, semelhante ao comportamento da ação. Count Essa correspondência de CAPTCHA está indicada em `nonTerminatingMatchingRules`.

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
```

```
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
```

```
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
```

```
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example Saída de log para uma regra CAPTCHA em relação a uma solicitação da web que não tem um token CAPTCHA

A lista de logs a seguir é para uma solicitação da web que correspondeu a uma regra com uma ação CAPTCHA. A solicitação da web não tinha um token CAPTCHA e foi bloqueada por. AWS WAF

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
```

```
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
```

```
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
```

```
}
```

Testando e ajustando suas AWS WAF proteções

Recomendamos que você teste e ajuste todas as alterações AWS WAF na sua ACL da web antes de aplicá-las ao tráfego do seu site ou aplicativo da web.

> ⚠ Risco de tráfego de produção
>
> Antes de implantar sua implementação de web ACL para tráfego de produção, teste-a e ajuste-a em um ambiente de preparação ou teste até se sentir confortável com o impacto potencial em seu tráfego. Em seguida, teste e ajuste as regras no modo de contagem com seu tráfego de produção antes de ativá-las.

Esta seção fornece orientação para testar e ajustar suas ACLs AWS WAF da web, regras, grupos de regras, conjuntos de IP e conjuntos de padrões regex.

Esta seção também fornece orientação geral para testar seu uso de grupos de regras gerenciadas por outra pessoa. Isso inclui AWS grupos de regras de regras AWS Marketplace gerenciadas, grupos de regras gerenciadas e grupos de regras que são compartilhados com você por outra conta. Para esses grupos de regras, siga também qualquer orientação recebida do provedor do grupo de regras.

- Para o grupo de regras de regras AWS gerenciadas do Bot Control, consulte tambémTestando e implantando o AWS WAF Bot Control.
- Para o grupo de regras de regras AWS gerenciadas de prevenção de aquisição de contas, consulte Testando e implantando o ATP também.
- Para o grupo de regras de regras AWS gerenciadas para prevenção de fraudes na criação de contas, consulte tambémTestando e implantando o ACFP.

Inconsistências temporárias durante as atualizações

Quando você cria ou altera uma ACL da web ou outros AWS WAF recursos, as alterações demoram um pouco para se propagar em todas as áreas em que os recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a alguns minutos.

Os seguintes são exemplos de inconsistências temporárias com as quais você pode se deparar durante a propagação da alteração:

- Depois de criar uma web ACL, se você tentar associá-la a um recurso, poderá obter uma exceção indicando que a web ACL não está disponível.
- Depois de adicionar um grupo de regras a uma web ACL, as novas regras do grupo de regras podem estar em vigor em uma área em que a web ACL é usada e não em outra.
- Depois de alterar uma configuração de ação de regra, você pode se deparar com a ação antiga em alguns lugares e a nova ação em outros.
- Ou, se você adicionar um endereço IP a um conjunto de IP que esteja em uso em uma regra de bloqueio, o novo endereço poderá ser brevemente bloqueado em uma área, enquanto ainda é permitido em outra.

Testes e ajustes de etapas de alto nível

Esta seção fornece uma lista de verificação das etapas para testar alterações em sua web ACL, incluindo quaisquer regras ou grupos de regras que ela usa.

> **Note**
>
> Para seguir as orientações desta seção, você precisa entender como criar e gerenciar proteções do AWS WAF como :web ACLs, regras e grupos de regras. Essas informações são abordadas nas seções anteriores deste guia.

Para testar e ajustar sua web ACL

Execute estas etapas primeiro em um ambiente de teste e depois na produção.

1. Preparar para testes

   Prepare seu ambiente de monitoramento, alterne suas novas AWS WAF proteções para o modo de contagem para testes e crie todas as associações de recursos necessárias.

   Consulte Preparando-se para testes.
2. Monitore e ajuste ambientes de teste e produção

   Monitore e ajuste suas AWS WAF proteções primeiro em um ambiente de teste ou teste e depois na produção, até que você tenha certeza de que elas podem lidar com o tráfego conforme necessário.

Consulte Monitoramento e ajuste.

3. Ative suas proteções na produção

   Quando estiver satisfeito com suas proteções de teste, coloque-as no modo de produção, limpe todos os artefatos de teste desnecessários e continue monitorando.

   Consulte Ativando suas proteções na produção.

Depois de concluir a implementação das alterações, continue monitorando o tráfego da web e as proteções na produção para garantir que estejam funcionando como você deseja. Os padrões de tráfego da web podem mudar com o tempo, então talvez seja necessário ajustar as proteções ocasionalmente.

Preparando-se para testes

Esta seção descreve como se preparar para testar e ajustar suas AWS WAF proteções.

> **Note**
>
> Para seguir as orientações desta seção, você precisa entender geralmente como criar e gerenciar AWS WAF proteções, como ACLs da web, regras e grupos de regras. Essas informações são abordadas nas seções anteriores deste guia.

Para se preparar para testes

1. Ative o registro de ACL da web, CloudWatch métricas da Amazon e amostragem de solicitações da web para a ACL da web

   Use logs, métricas e amostragem para monitorar a interação das regras de web ACL com seu tráfego da web.

   - Registro — Você pode configurar AWS WAF para registrar as solicitações da web que uma ACL da web avalia. Você pode enviar registros para CloudWatch logs, um bucket do Amazon S3 ou um stream de entrega do Amazon Data Firehose. Você pode editar campos e aplicar filtragem. Para ter mais informações, consulte Registrando AWS WAF tráfego de ACL da web.
   - Amazon Security Lake — Você pode configurar o Security Lake para coletar dados de ACL da web. O Security Lake coleta dados de registros e eventos de várias fontes para normalização,

análise e gerenciamento. Para obter informações sobre essa opção, consulte O que é o Amazon Security Lake? e Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.

- CloudWatch Métricas da Amazon — Na sua configuração de ACL na web, forneça especificações métricas para tudo o que você deseja monitorar. Você pode ver as métricas por meio dos AWS WAF CloudWatch consoles e. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.
- Amostragem de solicitações da web: você pode ver uma amostra de todas as solicitações da web que sua web ACL avalia. Para obter informações sobre amostragem de solicitações da web, consulte Visualizar um exemplo de solicitações da web.

2. Defina suas proteções para o modo Count

   Na configuração da web ACL, alterne tudo o que você deseja testar para o modo de contagem. Isso faz com que as proteções de teste registrem correspondências com solicitações da web sem alterar a forma como as solicitações são tratadas. Você poderá ver as correspondências em suas métricas, logs e amostras de solicitações, para verificar os critérios de correspondência e entender quais podem ser os efeitos no seu tráfego da web. As regras que adicionam rótulos às solicitações correspondentes adicionarão rótulos independentemente da ação da regra.

   - Regra definida na web ACL: edite as regras na web ACL e defina suas ações como Count.
   - Grupo de regras:Na configuração da web ACL, edite a instrução da regra para o grupo de regras e, no painel Regras, abra o menu suspenso Substituir todas as ações de regra e escolha Count. Se você gerencia a web ACL em JSON, adicione as regras às configurações `RuleActionOverrides` na instrução de referência do grupo de regras, com `ActionToUse` definido como Count. A lista de exemplos a seguir mostra as substituições de duas regras no grupo de regras de regras `AWSManagedRulesAnonymousIpList` AWS gerenciadas.

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
      },
      {
```

```
          "ActionToUse": {
            "Count": {}
          },
          "Name": "HostingProviderIPList"
        }
      ],
      "ExcludedRules": []
    }
  },
```

Para obter mais informações sobre alterações de ações, consulte Substituir ações de regra para um grupo de regras.

Para seu próprio grupo de regras, não modifique as ações da regra no próprio grupo de regras. As regras de grupo de regras com ação Count não geram as métricas ou outros artefatos necessários para seus testes. Além disso, a alteração de um grupo de regras afeta todas as web ACLsque o usam, enquanto as alterações na configuração da web ACL afetam somente a web ACL única.

- web ACL: se você estiver testando uma nova web ACL, defina a ação padrão para que a web ACL permita solicitações. Isso permite que você experimente a web ACL sem afetar o tráfego de forma alguma.

Em geral, o modo de contagem gera mais correspondências do que a produção. Isso ocorre porque uma regra que conta as solicitações não interrompe a avaliação da solicitação pela web ACL, portanto, as regras que são executadas posteriormente na web ACL também podem corresponder à solicitação. Quando você altera suas ações de regra para suas configurações de produção, as regras que permitem ou bloqueiam solicitações encerrarão a avaliação das solicitações correspondentes. Como resultado, as solicitações correspondentes geralmente serão inspecionadas por menos regras na web ACL. Para obter mais informações sobre os efeitos das ações de regra na avaliação geral de uma solicitação da web, consulte Ação da regra.

Com essas configurações, suas novas proteções não alterarão o tráfego da web, mas gerarão informações de correspondência em métricas, logs de web ACL e amostras de solicitações.

3. Associar a web ACL a um recurso

   Se a web ACL ainda não estiver associada ao recurso, associe-a.

Consulte Associando ou desassociando uma ACL da web com um recurso AWS.

Agora você está pronto para monitorar e ajustar sua web ACL.

Monitoramento e ajuste

Esta seção descreve como monitorar e ajustar suas AWS WAF proteções.

> **Note**
>
> Para seguir as orientações desta seção, você precisa entender geralmente como criar e gerenciar AWS WAF proteções, como ACLs da web, regras e grupos de regras. Essas informações são abordadas nas seções anteriores deste guia.

Monitore o tráfego da web e as correspondências de regras para verificar o comportamento da web ACL. Se você encontrar problemas, ajuste suas regras para corrigir e depois monitore para verificar os ajustes.

Repita o procedimento a seguir até que a web ACL esteja gerenciando seu tráfego da web conforme necessário.

Para monitorar e ajustar

1. Monitore o tráfego e as correspondências de regras

   Verifique se o tráfego está fluindo e se suas regras de teste estão descobrindo solicitações correspondentes.

   Procure as seguintes informações sobre as proteções que você está testando:

   - Logs: acesse informações sobre as regras que correspondem a uma solicitação da web:
     - Suas regras: as regras na web ACL com ação Count estão listadas em `nonTerminatingMatchingRules`. As regras com Allow ou Block estão listadas como o `terminatingRule`. Regras com CAPTCHA ou Challenge podem ser de encerramento ou de não encerramento, portanto, são listadas em uma das duas categorias, de acordo com o resultado da correspondência de regras.

  - Grupos de regras: os grupos de regras são identificados no campo `ruleGroupId`, com suas correspondências de regras categorizadas da mesma forma que as regras autônomas.
  - Rótulos: os rótulos que as regras aplicaram à solicitação são listados no campo `Labels`.

  Para ter mais informações, consulte Campos de log.

- CloudWatch Métricas da Amazon — Você pode acessar as seguintes métricas para avaliar sua solicitação de ACL na web.
  - Suas regras — As métricas são agrupadas pela ação da regra. Por exemplo, quando você testa uma regra no Count modo, suas correspondências são listadas como `Count` métricas para a Web ACL.
  - Seus grupos de regras — As métricas dos seus grupos de regras estão listadas nas métricas do grupo de regras.
  - Grupos de regras pertencentes a outra conta — As métricas do grupo de regras geralmente são visíveis somente para o proprietário do grupo de regras. No entanto, se você substituir a ação da regra por uma regra, as métricas dessa regra serão listadas em suas métricas de ACL da web. Além disso, os rótulos adicionados por qualquer grupo de regras são listados em suas métricas de ACL da web.

    Os grupos de regras nessa categoria sãoAWS Regras gerenciadas para AWS WAF,AWS Marketplace grupos de regras gerenciados,Grupos de regras fornecidos por outros serviços, e grupos de regras que são compartilhados com você por outra conta.
  - Rótulos - Os rótulos que foram adicionados a uma solicitação da web durante a avaliação são listados nas métricas dos rótulos da ACL da web. Você pode acessar as métricas de todos os rótulos, independentemente de terem sido adicionados por suas regras e grupos de regras ou por regras em um grupo de regras de propriedade de outra conta.

  Para ter mais informações, consulte Visualização de métricas para sua web ACL.

- Painéis de visão geral do tráfego da Web ACL — Acesse resumos do tráfego da Web que uma ACL da Web avaliou acessando a página da ACL da Web no AWS WAF console e abrindo a guia Visão geral do tráfego.

  Os painéis de visão geral do tráfego fornecem resumos quase em tempo real das CloudWatch métricas da Amazon que são AWS WAF coletadas quando avalia o tráfego do seu aplicativo na web.

  Para ter mais informações, consulte Painéis de visão geral do tráfego de web ACL.

- Solicitações da web amostradas:Acesse as informações das regras que correspondem a uma amostra das solicitações da web. As informações de amostra identificam as regras correspondentes pelo nome da métrica da regra na web ACL. Para grupos de regras, a métrica identifica a instrução de referência do grupo de regras. Para regras dentro de grupos de regras, o exemplo lista o nome da regra correspondente em `RuleWithinRuleGroup`.

  Para ter mais informações, consulte Visualizar um exemplo de solicitações da web.

2. Configure mitigações para lidar com falsos positivos

   Se você determinar que uma regra está gerando falsos positivos, correspondendo solicitações da web quando não deveria, as opções a seguir podem ajudá-lo a ajustar suas proteções de web ACL para mitigar.

   Correção de critérios de inspeção de regras

   Para suas próprias regras, muitas vezes você só precisa ajustar as configurações que está usando para inspecionar solicitações da web. Os exemplos incluem alterar as especificações em um conjunto de padrões regex, ajustar as transformações de texto que você aplica a um componente de solicitação antes da inspeção ou mudar para o uso de um endereço IP encaminhado. Consulte a orientação sobre o tipo de regra que está causando problemas, em Princípios básicos da instrução de regras.

   Correção de problemas mais complexos

   Para critérios de inspeção que você não controla e para algumas regras complexas, talvez seja necessário fazer outras alterações, como adicionar regras que permitam ou bloqueiem solicitações explicitamente ou que eliminem as solicitações da avaliação pela regra problemática. Os grupos de regras gerenciadas geralmente precisam desse tipo de mitigação, mas outras regras também precisam. Os exemplos incluem a instrução de regra baseada em intervalos e a instrução de regra de ataque de injeção de SQL.

   O que você faz para mitigar falsos positivos depende do seu caso de uso. A seguir, são mostradas as abordagens comuns:

   - Adicionar uma regra atenuante:Adicione uma regra que seja executada antes da nova regra e que permita explicitamente solicitações que estejam causando falsos positivos. Para obter informações sobre a ordem de avaliação de regras em uma web ACL, consulte Ordem de processamento de regras e grupos de regras em uma web ACL.

Com essa abordagem, as solicitações permitidas são enviadas ao recurso protegido, para que nunca cheguem à nova regra para avaliação. Se a nova regra for um grupo de regras gerenciadas pago, essa abordagem também poderá ajudar a conter o custo do uso do grupo de regras.

- Adicionar uma regra lógica com uma regra de mitigação:Use instruções de regras lógicas para combinar a nova regra com uma regra que exclua os falsos positivos. Para mais informações, consulte Instruções de regras lógicas.

  Por exemplo, digamos que você esteja adicionando uma instrução de correspondência de ataque de injeção de SQL que está gerando falsos positivos para uma categoria de solicitações. Crie uma regra que corresponda a essas solicitações e, em seguida, combine as regras usando instruções de regras lógicas para que você corresponda somente às solicitações que em que ambas não correspondam aos critérios de falsos positivos e correspondam aos critérios de ataque de injeção de SQL.

- Adicionar uma instrução de redução de escopo:Para instruções baseadas em taxas e instruções de referência de grupos de regras gerenciadas, exclua as solicitações que resultam em falsos positivos da avaliação adicionando uma instrução de redução de escopo dentro da instrução principal.

  Uma solicitação que não corresponda à instrução de escopo inferior nunca chega ao grupo de regras ou à avaliação baseada em intervalos. Para informações sobre instruções de redução de escopo, consulte Instruções de redução de escopo. Para ver um exemplo, consulte Excluir o intervalo de IP do gerenciamento de bots.

- Adicionar uma regra de correspondência de rótulos:Para grupos de regras que usam rótulos, identifique o rótulo que a regra problemática está aplicando às solicitações. Talvez seja necessário definir primeiro as regras do grupo de regras no modo de contagem, caso ainda não tenha feito isso. Adicione uma regra de correspondência de rótulo, posicionada para ser executada após o grupo de regras, que corresponda ao rótulo que está sendo adicionado pela regra problemática. Na regra de correspondência de rótulos, você pode filtrar as solicitações que deseja permitir daquelas que deseja bloquear.

  Se você usar essa abordagem, ao terminar o teste, mantenha a regra problemática no modo de contagem no grupo de regras e mantenha sua regra de correspondência de rótulos personalizada em vigor. Para obter mais informações sobre instruções de correspondência de rótulo, consulte Instrução de regra de correspondência de rótulo. Veja exemplos em Permitir

um bot bloqueado específico e Exemplo de ATP: tratamento personalizado para credenciais ausentes e comprometidas.

- Alterar a versão de um grupo de regras gerenciadas:Para grupos versionados de regras gerenciadas, altere a versão que você está usando. Por exemplo, você pode voltar para a última versão estática que estava usando com sucesso.

  Geralmente, essa é uma solução temporária. Você pode alterar a versão do seu tráfego de produção enquanto continua testando a versão mais recente em seu ambiente de teste ou preparação, ou enquanto espera por uma versão mais compatível do provedor. Para obter informações sobre as versões de grupos de regras gerenciadas, consulte Grupos de regras gerenciadas.

Quando estiver convencido de que as novas regras estão correspondendo às solicitações conforme necessário, passe para a próxima etapa dos testes e repita esse procedimento. Execute a etapa final de testes e ajustes em seu ambiente de produção.

Visualização de métricas para sua web ACL

Depois de associar uma ACL da web a um ou mais AWS recursos, você pode visualizar as métricas resultantes da associação em um CloudWatch gráfico da Amazon.

Para obter informações sobre AWS WAF métricas, consulteAWS WAF métricas e dimensões. Para obter informações sobre CloudWatch métricas, consulte o Guia CloudWatch do usuário da Amazon.

Para cada uma de suas regras em uma ACL da web e para todas as solicitações que um recurso associado encaminha AWS WAF para uma ACL da web, você pode fazer CloudWatch o seguinte:

- Visualize dados da hora anterior ou das três horas anteriores.
- Altere o intervalo entre os pontos de dados.
- Altere o cálculo que é CloudWatch executado nos dados, como máximo, mínimo, média ou soma.

> **Note**
>
> AWS WAF with CloudFront é um serviço global e as métricas estão disponíveis somente quando você escolhe a região Leste dos EUA (Norte da Virgínia) no AWS Management Console. Se você escolher outra região, nenhuma AWS WAF métrica aparecerá no CloudWatch console.

Para visualizar os dados das regras em uma web ACL

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região para aquela em que seus AWS recursos estão localizados. Para CloudFront, escolha a região Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, em Métricas, escolha Todas as métricas e pesquise na guia Procurar por `AWS::WAFV2`.
4. Marque a caixa de seleção da web ACL da qual você deseja visualizar os dados.
5. Altere as configurações aplicáveis:

   Estatística

   Escolha o cálculo que é CloudWatch executado nos dados.

   Intervalo de tempo

   Escolha se você deseja visualizar dados da hora anterior ou das três horas anteriores.

   Período

   Escolha o intervalo entre pontos de dados no gráfico.

   Regras

   Escolha as regras das quais você deseja visualizar os dados.

   > **Note**
   >
   > Se você alterar o nome de uma regra e quiser que o nome da métrica da regra reflita a alteração, você também deverá atualizar o nome da métrica. AWS WAF não atualiza automaticamente o nome da métrica de uma regra quando você altera o nome da regra. Você pode alterar o nome da métrica ao editar a regra no console, usando o editor JSON de regras. Você também pode alterar os dois nomes por meio das APIs e em qualquer lista JSON usada para definir sua web ACL ou grupo de regras.

   Observe o seguinte:

- Se você associou recentemente uma ACL da web a um AWS recurso, talvez seja necessário aguardar alguns minutos para que os dados apareçam no gráfico e para que a métrica da ACL da web apareça na lista de métricas disponíveis.
- Se você associar mais de um recurso a uma Web ACL, os CloudWatch dados incluirão solicitações para todos eles.
- Você pode passar o cursor do mouse sobre o ponto de dados para obter mais informações.
- O gráfico não é automaticamente atualizado. Para atualizar a exibição, escolha o ícone de atualização
  ().

Para obter mais informações sobre CloudWatch métricas, consulte[Monitoramento com a Amazon CloudWatch](#).

Painéis de visão geral do tráfego de web ACL

Esta seção descreve os painéis de visão geral do tráfego da Web ACL no AWS WAF console. Depois de associar uma ACL da web a um ou mais AWS recursos e habilitar métricas para a ACL da web, você pode acessar resumos do tráfego da web que a ACL da web avalia acessando a guia Visão geral do tráfego da ACL da web no console. AWS WAF Os painéis incluem resumos quase em tempo real das CloudWatch métricas da Amazon que são AWS WAF coletadas quando avalia o tráfego web do seu aplicativo.

> **Note**
>
> Se você não vê nada nos painéis, verifique se você tem métricas habilitadas para a Web ACL.

A guia Visão geral do tráfego para a ACL da Web contém painéis com guias que têm as seguintes categorias de informações:

- Todo o tráfego:Todas as solicitações da web que a web ACL avalia.

  O foco do painel está no encerramento de ações, mas é possível visualizar as correspondências para as regras de contagem nos seguintes locais:

  - Painel Dez principais regras deste painel. Alterne Alternar para a contagem de ações para mostrar as correspondências das regras de contagem.
  - Guia Solicitações de amostra da página da ACL da Web. Esta nova guia inclui um gráfico de todas as correspondências de regras. Para mais informações, consulte Visualizar um exemplo de solicitações da web.
- Controle de Bots:Solicitações da web que a web ACL avalia usando o grupo de regras gerenciadas do Controle de Bots.

  Se você não estiver usando esse grupo de regras na sua web ACL, essa guia mostra os resultados da avaliação de uma amostra do seu tráfego da web em relação às regras do Controle de Bots. Isso lhe dá uma ideia do tráfego de bots que a aplicação recebe, e está disponível gratuitamente.

  Esse grupo de regras faz parte das opções inteligentes de mitigação de ameaças que AWS WAF oferece. Para ter mais informações, consulte AWS WAF Controle de bots e AWS WAF Grupo de regras do Bot Control.
- Prevenção de aquisição de contas — a Web solicita que a ACL da web avalie usando o grupo de regras gerenciadas de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control. Essa guia só estará disponível se você estiver usando esse grupo de regras na sua web ACL.

  O grupo de regras do ATP faz parte das ofertas de mitigação de ameaças inteligentes do AWS WAF . Para ter mais informações, consulte AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP) e AWS WAF Grupo de regras de prevenção de aquisição de contas (ATP) de controle de fraudes.
- Prevenção de fraudes na criação de contas — a Web solicita que a ACL da web avalie usando o grupo de regras gerenciadas de prevenção de AWS WAF fraudes na criação de contas (ACFP) do Fraud Control. Essa guia só estará disponível se você estiver usando esse grupo de regras na sua web ACL.

  O grupo de regras do ACFP faz parte das ofertas de mitigação de ameaças inteligentes do AWS WAF . Para ter mais informações, consulte AWS WAF Controle de fraudes na criação de contas e prevenção de fraudes (ACFP) e AWS WAF Grupo de regras de prevenção de fraudes (ACFP) para criação de contas de controle de fraudes.

Os painéis são baseados nas CloudWatch métricas da ACL da web, e os gráficos fornecem acesso às métricas correspondentes em. CloudWatch Para os painéis de mitigação inteligente de ameaças, como o Controle de Bots, as métricas usadas são principalmente as métricas de rótulos.

- Para obter uma lista das métricas que AWS WAF fornece, consulteAWS WAF métricas e dimensões.
- Para obter informações sobre CloudWatch métricas, consulte o Guia CloudWatch do usuário da Amazon.

Os painéis fornecem resumos de seus padrões de tráfego para as ações de encerramento e o intervalo de datas que você seleciona. Os painéis de mitigação inteligente de ameaças incluem solicitações que o grupo de regras gerenciadas correspondente avaliou, independentemente de o próprio grupo de regras gerenciadas ter aplicado a ação de encerramento. Por exemplo, se Block for selecionado, o painel de Prevenção contra apropriação de contas inclui informações para todas as solicitações da web que foram avaliadas pelo grupo de regras gerenciadas do ATP e bloqueadas em algum momento durante a avaliação da web ACL. As solicitações podem ser bloqueadas pelo grupo de regras gerenciadas do ATP, por uma regra executada após o grupo de regras na web ACL ou pela ação padrão da web ACL.

Visualizando os painéis de uma web ACL

Siga o procedimento nesta seção para acessar os painéis da web ACL e definir os critérios de filtragem de dados. Se você associou recentemente uma ACL da web a um AWS recurso, talvez seja necessário aguardar alguns minutos para que os dados sejam disponibilizados nos painéis.

Os painéis incluem as solicitações de todos os recursos que você associou à web ACL.

Para visualizar os painéis de Visão geral do tráfego para uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, escolha ACLd da web e, em seguida, pesquise a web ACL na qual você está interessado.
3. Selecione a web ACL. O console leva você para a página da web ACL. A guia Visão geral de tráfego é selecionada por padrão.
4. Altere as configurações dos Filtros de dados conforme necessário.

- Ações de regra de encerramento:Selecione as ações de encerramento a serem incluídas nos painéis. Os painéis resumem as métricas das solicitações da Web que tiveram uma das ações selecionadas aplicadas pela avaliação da ACL da Web. Se você selecionar todas as ações disponíveis, os painéis incluirão todas as solicitações web avaliadas. Para obter informações sobre as ações, consulte Como AWS WAF manipula as ações de regras e grupos de regras em uma ACL da web.
- Intervalo de tempo: selecione o intervalo de tempo a ser visualizado nos painéis. Você pode optar por visualizar um período de tempo relativo a agora, por exemplo, as últimas três horas ou a última semana, e você pode selecionar um intervalo de tempo absoluto em um calendário.
- Fuso horário: essa configuração se aplica quando você especifica um intervalo de tempo absoluto. Você pode usar o fuso horário local do seu navegador ou UTC (Tempo Universal Coordenado).

Examine as informações nas guias nas quais você tem interesse. As seleções do filtro de dados se aplicam a todos os painéis. Nos painéis gráficos, você pode passar o cursor sobre um ponto de dados ou uma área para ver detalhes adicionais.

Regras de ação Count

É possível visualizar informações sobre as correspondências de ações de contagem em um dos dois locais.

- Na guia Visão geral do tráfego, no painel Todo o tráfego, encontre o painel Dez principais regras e alterne Alternar para a contagem de ações. Com esta opção ativada, o painel mostrará as correspondências de regras de contagem em vez de encerrar as correspondências de regras.
- Na guia Solicitações de amostra da ACL da Web, visualize um gráfico de todas as correspondências de regras e ações para o intervalo de tempo definido na guia Visão geral do tráfego. Para obter informações sobre a guia Solicitações de amostra, consulte Visualizar um exemplo de solicitações da web.

CloudWatch Métricas da Amazon

Nos painéis gráficos do painel, você pode acessar as CloudWatch métricas dos dados representados graficamente. Escolha a opção na parte superior do painel gráfico ou no menu suspenso ⋮ (reticências verticais) dentro do painel.

Atualização dos painéis

Os painéis não são atualizados automaticamente. Para atualizar a exibição, escolha o ícone de atualização

.

Exemplos dos painéis de visão geral do tráfego para :web ACLs

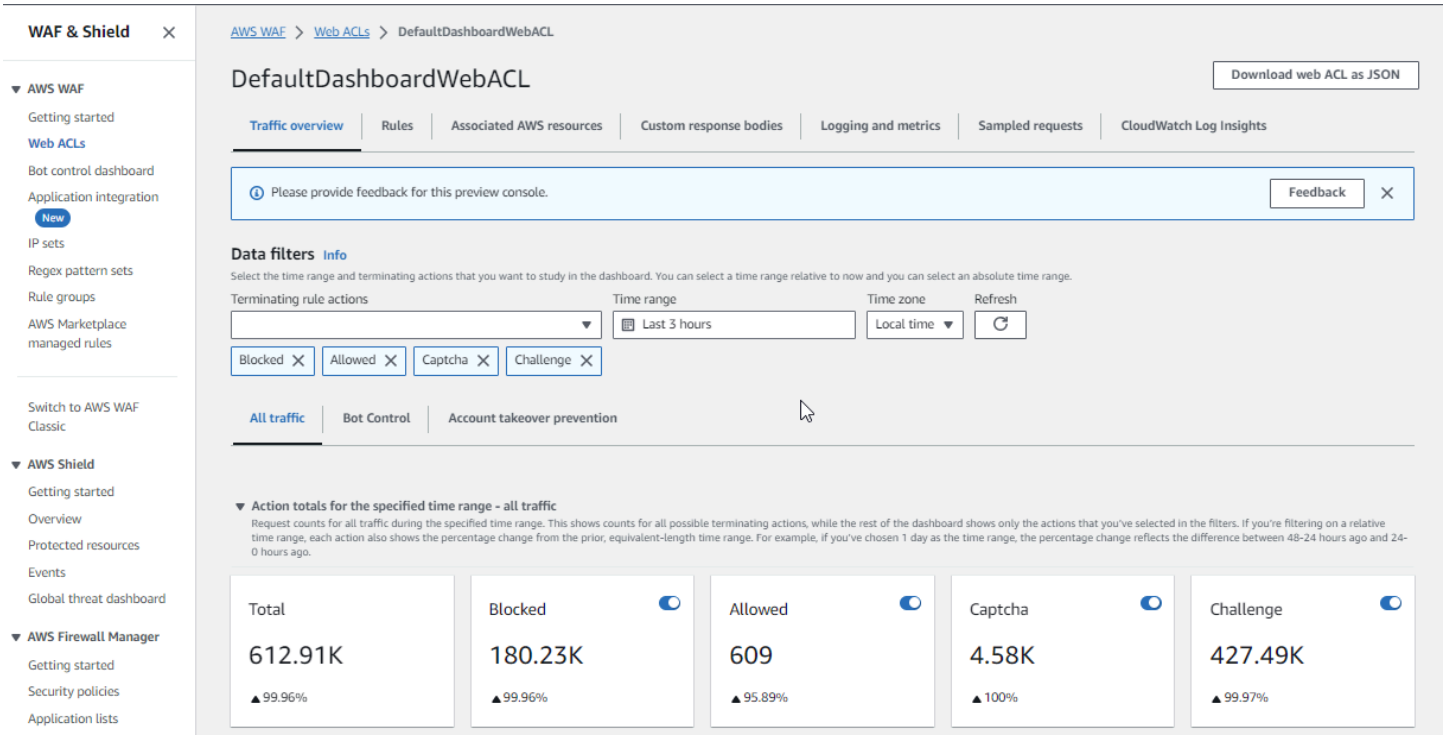
Esta seção mostra exemplos de telas dos painéis de visão geral do tráfego para :web ACLs.

> **Note**
>
> Se você já estiver usando AWS WAF para proteger os recursos do seu aplicativo, poderá ver os painéis de qualquer uma das suas ACLs da web em sua página no AWS WAF console. Para mais informações, consulte Visualizando os painéis de uma web ACL.

Exemplo de tela: filtros de dados e contagem de ações do painel Todo o tráfego

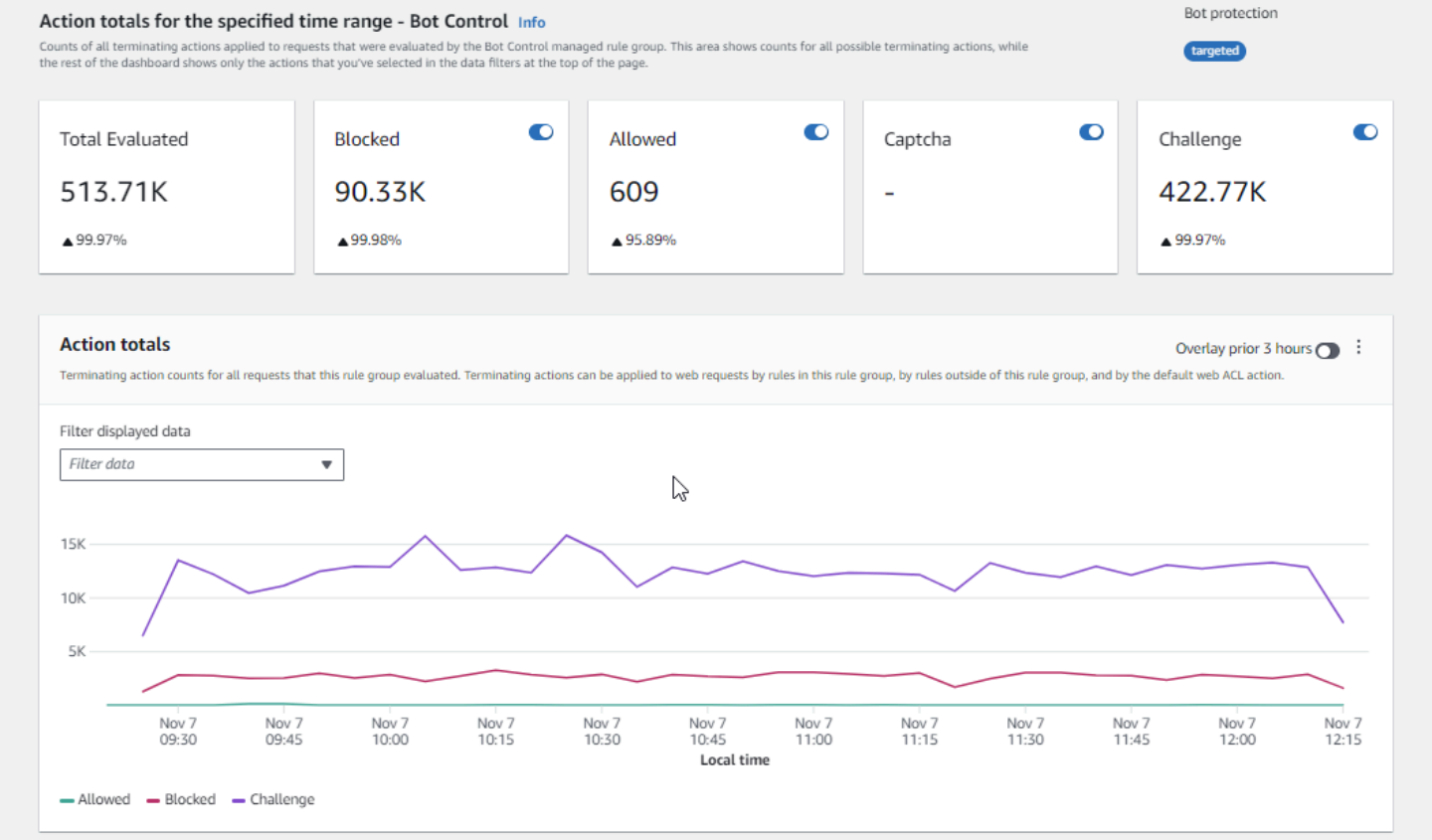
A captura de tela a seguir mostra a visão geral do tráfego de uma web ACL com a guia Todo o tráfego selecionada. Os filtros de dados são definidos de acordo com os padrões: todas as ações de encerramento nas últimas três horas.

Dentro do painel de todo o tráfego estão os totais de ações das várias ações de encerramento. Cada painel lista a contagem de solicitações e mostra uma seta para cima/para baixo indicando a alteração desde o período anterior de três horas.



Exemplo de tela: contagem de ações do painel do Controle de Bots

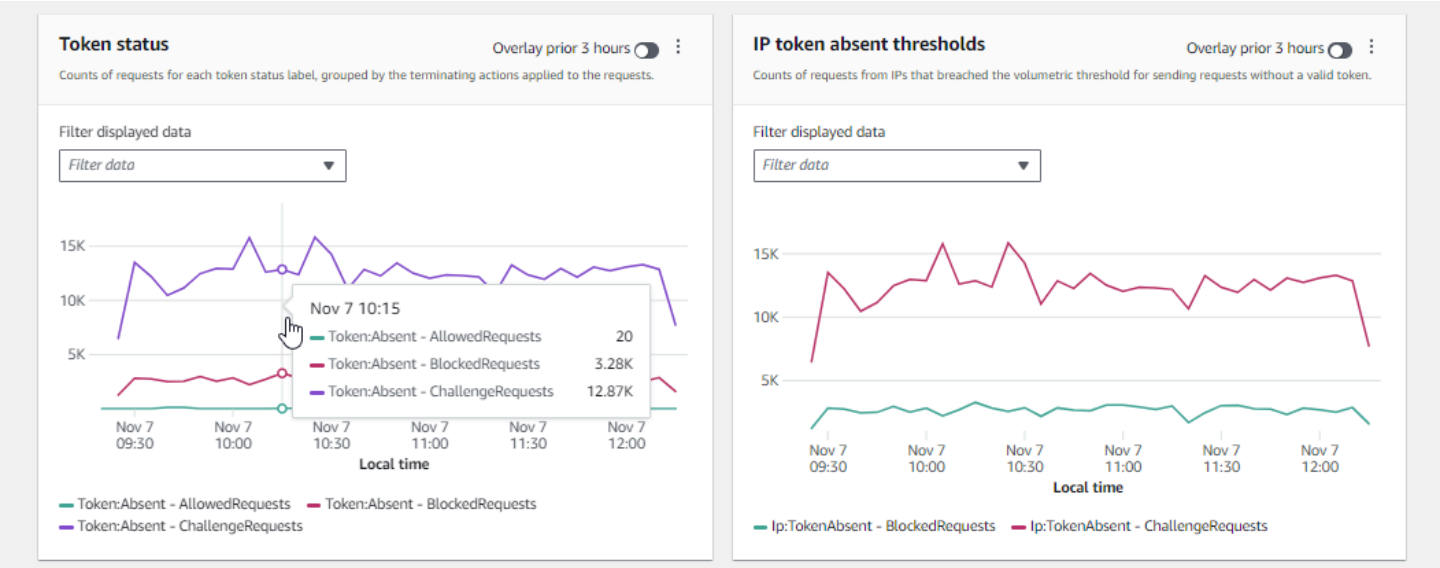
A captura de tela a seguir mostra as contagens de ações do painel do Controle de Bots. Isso mostra os mesmos painéis de totais para o intervalo de tempo, mas as contagens são apenas para solicitações que o grupo de regras do Controle de Bots avaliou. Mais abaixo, no painel Totais de ações, você pode ver as contagens de ações em todo o intervalo de tempo especificado de três horas. Nesse intervalo de tempo, a ação CAPTCHA não foi aplicada a nenhuma das solicitações avaliadas pelo grupo de regras.



Exemplo de tela: gráficos de resumo de status de token do painel do Controle de Bots

A captura de tela a seguir mostra dois dos gráficos resumidos disponíveis no painel do Controle de Bots. O painel Status do token mostra as contagens dos vários rótulos de status do token, emparelhados com a ação da regra que foi aplicada à solicitação. O painel de Limites ausentes de token de IP mostra dados de solicitações de IPs que estavam enviando muitas solicitações sem um token.

Passar o mouse sobre qualquer área no gráfico exibe os detalhes das informações disponíveis. No painel de Status do token nesta captura de tela, o mouse está passando sobre um ponto no tempo, sem estar em nenhuma linha do gráfico, então o console exibe os dados de todas as linhas naquele momento.



Esta seção mostra apenas alguns dos resumos de tráfego fornecidos nos painéis de visão geral do tráfego da web ACL. Para ver os painéis de qualquer uma das suas :web ACLs, abra a página da web ACL no console. Para obter informações sobre como fazer isso, consulte as orientações em Visualizando os painéis de uma web ACL.

Visualizar um exemplo de solicitações da web

Esta seção descreve a guia Solicitações de amostra de ACL da web no AWS WAF console. Nessa guia, você pode ver um gráfico de todas as correspondências de regras para solicitações da web que AWS WAF foram inspecionadas. Além disso, se você tiver a amostragem de solicitações ativada para a ACL da Web, poderá ver uma exibição em tabela de uma amostra das solicitações da Web que AWS WAF foram inspecionadas. Você também pode recuperar amostras de informações de solicitação por meio da chamada de API. `GetSampledRequests`

Os exemplos contém até 100 solicitações que correspondem aos critérios para uma regra na web ACL e outras 100 solicitações para solicitações que não correspondem a qualquer regra e tiveram a ação padrão da web ACL aplicada. As solicitações na amostra vêm de todos os recursos protegidos que receberam solicitações para seu conteúdo nas últimas três horas.

Quando uma solicitação da web corresponde aos critérios de uma regra e a ação dessa regra não encerra a avaliação da solicitação, AWS WAF continua inspecionando a solicitação da web usando as regras subsequentes na ACL da web. Por esse motivo, uma solicitação da Web pode aparecer diversas vezes. Para obter informações sobre os comportamentos de ações de regras, consulte Ação da regra.

Como visualizar o gráfico de todas as regras e as solicitações de amostra

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da web ACL para a qual deseja exibir solicitações. O console leva você para a descrição da web ACL, onde é possível editá-la.
4. Na guia Solicitações de amostra, é possível visualizar o seguinte:

   - Gráfico de todas as regras: este gráfico mostra as regras e as ações de regras correspondentes para todas as avaliações de solicitações da Web que foram executadas durante o intervalo de tempo indicado.

     > **Note**
     >
     > O intervalo de tempo para este gráfico é definido na guia Visão geral do tráfego para a ACL da Web, na seção Filtros de dados. Para mais informações, consulte Visualizando os painéis de uma web ACL.

   - Tabela de solicitações de amostra: esta tabela exibe dados de solicitações de amostra das últimas três horas. Para cada entrada, a tabela exibe os seguintes dados:

     Nome da métrica

     O nome da CloudWatch métrica da regra na ACL da web que correspondeu à solicitação. Se uma solicitação da web não corresponder a nenhuma regra na web ACL, esse valor será Padrão.

     > **Note**
     >
     > Se você alterar o nome de uma regra e quiser que o nome da métrica da regra reflita a alteração, você também deverá atualizar o nome da métrica. AWS WAF não atualiza automaticamente o nome da métrica de uma regra quando você altera o nome da regra. Você pode alterar o nome da métrica ao editar a regra no console, usando o editor JSON de regras. Você também pode alterar os dois nomes por meio das APIs e em qualquer lista JSON usada para definir sua web ACL ou grupo de regras.

IP de origem

O endereço IP da qual a solicitação se originou ou, se o visualizador tiver usado um proxy HTTP ou um Application Load Balancer para enviar a solicitação, o endereço IP do proxy ou do Application Load Balancer.

URI

A parte de um URL que identifica um recurso, como `/images/daily-ad.jpg`.

Regra dentro de grupo de regras

Se o nome da métrica identificar uma instrução de referência do grupo de regras, isso identificará a regra dentro do grupo de regras que correspondeu à solicitação.

Ação

Indica a ação para a regra correspondente. Para obter informações sobre as possíveis ações de regras, consulte Ação da regra.

Tempo

A hora em que AWS WAF recebeu a solicitação do recurso protegido.

Para exibir informações adicionais sobre os componentes de uma solicitação da Web, escolha o nome do URI na linha da solicitação.

Ativando suas proteções na produção

Quando você terminar a etapa final de testes e ajustes em seu ambiente de produção, ative suas proteções no modo de produção.

> **Risco de tráfego de produção**
>
> Antes de implantar sua implementação de web ACL para tráfego de produção, teste-a e ajuste-a em um ambiente de teste até se sentir confortável com o impacto potencial em seu tráfego. Além disso, teste e ajuste-o no modo de contagem com seu tráfego de produção antes de ativar suas proteções para o tráfego de produção.

> **Note**
>
> Para seguir as orientações desta seção, você precisa entender geralmente como criar e gerenciar AWS WAF proteções, como ACLs da web, regras e grupos de regras. Essas informações são abordadas nas seções anteriores deste guia.

Execute estas etapas primeiro em seu ambiente de teste e depois na produção.

Ative suas AWS WAF proteções na produção

1. Mude para suas proteções de produção

   Atualize sua web ACL e alterne suas configurações para produção.

   a. Remova todas as regras de teste que você não precisa

      Se você adicionou regras de teste que não são necessárias na produção, remova-as. Se você estiver usando alguma regra de correspondência de rótulos para filtrar os resultados das regras do grupo de regras gerenciadas, deixe-as em vigor.

   b. Mude para ações de produção

      Altere as configurações de ação das novas regras para as configurações de produção pretendidas.

      - Regra definida na web ACL: edite as regras na web ACL e altere suas ações de Count para suas ações de produção.
      - Grupo de regras: na configuração de web ACL do grupo de regras, alterne as regras para usar suas próprias ações ou deixe-as com a substituição da ação Count, de acordo com os resultados de suas atividades de teste e ajuste. Se você estiver usando uma regra de correspondência de rótulos para filtrar os resultados de uma regra de grupo de regras, certifique-se de deixar a substituição dessa regra em vigor.

        Para passar a usar a ação de uma regra, na configuração da web ACL, edite a instrução da regra para o grupo de regras e remova a substituição Count da regra. Se você gerencia a web ACL em JSON, na instrução de referência do grupo de regras, remova a entrada da regra da lista `RuleActionOverrides`.
      - web ACL: se você alterou a ação padrão da web ACL para seus testes, mude-a para sua configuração de produção.

Com essas configurações, suas novas proteções gerenciarão o tráfego da web conforme você pretende.

Quando você salva sua web ACL, os recursos aos quais ela está associada usarão suas configurações de produção.

2. Monitore e ajuste

   Para ter certeza de que as solicitações da web estão sendo tratadas como você deseja, monitore de perto seu tráfego depois de ativar a nova funcionalidade. Você monitorará métricas e logs de suas ações de regras de produção, em vez das ações de contagem que estava monitorando em seu trabalho de ajuste. Continue monitorando e ajuste o comportamento conforme necessário para se adaptar às mudanças no seu tráfego da web.

Como AWS WAF funciona com os CloudFront recursos da Amazon

Ao criar uma ACL da web, você pode especificar uma ou mais CloudFront distribuições que deseja AWS WAF inspecionar. AWS WAF começa a inspecionar e gerenciar solicitações da web para essas distribuições com base nos critérios que você identifica na ACL da web. CloudFront fornece alguns recursos que aprimoram a AWS WAF funcionalidade. Este capítulo descreve algumas maneiras que você pode configurar CloudFront para criar CloudFront e AWS WAF trabalhar melhor em conjunto.

Tópicos

- Usando AWS WAF com páginas de erro CloudFront personalizadas
- Usando AWS WAF with CloudFront para aplicativos executados em seu próprio servidor HTTP
- Escolhendo os métodos HTTP que CloudFront respondem a

Usando AWS WAF com páginas de erro CloudFront personalizadas

Por padrão, quando AWS WAF bloqueia uma solicitação da Web com base nos critérios que você especifica, ela retorna o código de status HTTP `403 (Forbidden)` para CloudFront e CloudFront retorna esse código de status para o visualizador. O visualizador, em seguida, exibirá uma breve mensagem padrão esparsamente formatada, semelhante à seguinte:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Você pode substituir esse comportamento em suas regras de ACL AWS WAF da web definindo respostas personalizadas. Para obter mais informações sobre como personalizar o comportamento de resposta usando AWS WAF regras, consulteRespostas personalizadas para ações Block.

> **Note**
>
> As respostas que você personaliza usando AWS WAF regras têm precedência sobre qualquer especificação de resposta que você define nas páginas de erro CloudFront personalizadas.

Se você preferir exibir uma mensagem de erro personalizada CloudFront, possivelmente usando a mesma formatação do resto do seu site, você pode configurar CloudFront para retornar ao visualizador um objeto (por exemplo, um arquivo HTML) que contém sua mensagem de erro personalizada.

> **Note**
>
> CloudFront não consigo distinguir entre um código de status HTTP 403 que é retornado pela sua origem e um que é retornado AWS WAF quando uma solicitação é bloqueada. Isso significa que você não pode retornar diferentes páginas de erro personalizadas com base em diferentes causas de um código de status HTTP 403.

Para obter mais informações sobre páginas de erro CloudFront personalizadas, consulte Geração de respostas de erro personalizadas no Amazon CloudFront Developer Guide.

Usando AWS WAF with CloudFront para aplicativos executados em seu próprio servidor HTTP

Ao usar AWS WAF com CloudFront, você pode proteger seus aplicativos em execução em qualquer servidor web HTTP, seja um servidor web executado no Amazon Elastic Compute Cloud (Amazon EC2) ou um servidor web que você gerencia de forma privada. Você também pode configurar CloudFront para exigir HTTPS CloudFront entre seu próprio servidor web, bem como entre visualizadores e. CloudFront

Exigindo HTTPS entre CloudFront e seu próprio servidor web

Para exigir HTTPS entre CloudFront e seu próprio servidor web, você pode usar o recurso de origem CloudFront personalizada e definir a Política de Protocolo de Origem e as configurações do Nome de Domínio de Origem para origens específicas. Na sua CloudFront configuração, você pode especificar o nome DNS do servidor junto com a porta e o protocolo que você deseja usar CloudFront ao buscar objetos da sua origem. Você também deve garantir que o certificado SSL/TLS no servidor da origem personalizada corresponda ao nome de domínio de origem configurado. Ao usar seu próprio servidor web HTTP fora do AWS, você deve usar um certificado assinado por uma autoridade de certificação (CA) terceirizada confiável, por exemplo, Comodo ou DigiCert Symantec. Para obter mais informações sobre a exigência de HTTPS para comunicação entre CloudFront e seu próprio servidor web, consulte o tópico Exigindo HTTPS para comunicação entre CloudFront e sua origem personalizada no Amazon CloudFront Developer Guide.

Exigindo HTTPS entre um visualizador e CloudFront

Para exigir HTTPS entre visualizadores e CloudFront, você pode alterar a Política de Protocolo do Visualizador para um ou mais comportamentos de cache em sua CloudFront distribuição. Para obter mais informações sobre o uso de HTTPS entre espectadores e CloudFront, consulte o tópico Exigindo HTTPS para comunicação entre espectadores e CloudFront no Amazon CloudFront Developer Guide. Você também pode trazer seu próprio certificado SSL para que os espectadores possam se conectar à sua CloudFront distribuição via HTTPS usando seu próprio nome de domínio, por exemplo, https://www.mysite.com. Para obter mais informações, consulte o tópico Configurando nomes de domínio alternativos e HTTPS no Amazon CloudFront Developer Guide.

Escolhendo os métodos HTTP que CloudFront respondem a

Ao criar uma distribuição CloudFront web da Amazon, você escolhe os métodos HTTP que deseja CloudFront processar e encaminhar para sua origem. Você pode escolher entre as seguintes opções:

- **`GET`**, **`HEAD`** — Você pode usar CloudFront somente para obter objetos de sua origem ou para obter cabeçalhos de objetos.
- **`GET`**,**`HEAD`**, **`OPTIONS`** — Você pode usar CloudFront somente para obter objetos da sua origem, obter cabeçalhos de objetos ou recuperar uma lista das opções suportadas pelo seu servidor de origem.
- **`GET`**,**`HEAD`**,**`OPTIONS`**,**`PUT`**,**`POST`**,**`PATCH`**, **`DELETE`** — Você pode usar CloudFront para obter, adicionar, atualizar e excluir objetos e para obter cabeçalhos de objetos. Além disso, você pode executar outras operações de `POST`, como enviar dados de um formulário da web.

Você também pode usar instruções de regra de correspondência de AWS WAF bytes para permitir ou bloquear solicitações com base no método HTTP, conforme descrito emInstrução de regra de correspondência de string. Se você quiser usar uma combinação de métodos que CloudFront ofereça suporte`HEAD`, como `GET` e, não precisará configurar AWS WAF para bloquear solicitações que usem os outros métodos. Se você quiser permitir uma combinação de métodos que CloudFront não oferece suporte, como,, e `GET` `HEAD``POST`, você pode configurar CloudFront para responder a todos os métodos e, em seguida, usar AWS WAF para bloquear solicitações que usam outros métodos.

Para obter mais informações sobre como escolher os métodos que CloudFront respondem, consulte Métodos HTTP permitidos no tópico Valores que você especifica ao criar ou atualizar uma distribuição na Web no Amazon CloudFront Developer Guide.

Segurança no uso do AWS WAF serviço

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

> **Note**
>
> Esta seção fornece diretrizes AWS de segurança padrão para o uso do AWS WAF serviço e de seus AWS recursos, como ACLs AWS WAF da web e grupos de regras.
> Para obter informações sobre como proteger seus AWS recursos usando AWS WAF, consulte o restante do AWS WAF guia.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto 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. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS WAF, consulte AWS Serviços no escopo por programa de conformidade.

- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, como a confidencialidade de seus dados, os requisitos da sua organização, leis e regulamentos aplicáveis.

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

Tópicos

Proteção de dados em AWS WAF

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS WAF. 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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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 os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- 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 sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS WAF ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

AWS WAF entidades — como ACLs da web, grupos de regras e conjuntos de IP — são criptografadas em repouso, exceto em determinadas regiões onde a criptografia não está disponível, incluindo China (Pequim) e China (Ningxia). Chaves de criptografia exclusivas são usadas para cada região.

Excluir recursos do AWS WAF

Você pode excluir os recursos que você criou no AWS WAF. Consulte as orientações para cada tipo de recurso nas seções abaixo.

- Exclusão de uma web ACL
- Excluir um grupo de regras
- Excluir um conjunto de IP
- Excluir um conjunto de padrões regex

Gerenciamento de identidade e acesso para AWS WAF

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) a usar AWS WAF os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS WAF.

Usuário do serviço — Se você usar o AWS WAF serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS WAF recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS WAF, consulte Solução de problemas AWS WAF de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS WAF recursos da sua empresa, provavelmente tem acesso total AWS WAF a. É seu trabalho determinar quais AWS WAF recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS WAF, consulteComo AWS WAF funciona com o IAM.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS WAF. Para ver exemplos de políticas AWS WAF baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS

raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). 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.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso

usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
- Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas

permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

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.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os

administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada

uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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 WAF funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS WAF, saiba com quais recursos do IAM estão disponíveis para uso AWS WAF.

Recursos do IAM que você pode usar com AWS WAF

Atributo do IAM	AWS WAF apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não

Atributo do IAM	AWS WAF apoio
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como AWS WAF 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.

Políticas baseadas em identidade para AWS WAF

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para ver exemplos de políticas AWS WAF baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF

Políticas baseadas em recursos dentro AWS WAF

É compatível com políticas baseadas em atributos	Sim

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

AWS WAF usa políticas baseadas em recursos para apoiar o compartilhamento de grupos de regras entre contas. Você compartilha um grupo de regras que você possui com outra AWS conta fornecendo as configurações de política com base em recursos para a chamada de AWS WAF API `PutPermissionPolicy` ou para uma chamada de CLI ou SDK equivalente. Para obter informações adicionais, incluindo exemplos e links para a documentação dos outros idiomas disponíveis, consulte PutPermissionPolicya Referência da AWS WAF API. Essa funcionalidade não está disponível por outros meios, como o console ou o AWS CloudFormation.

Ações políticas para AWS WAF

Oferece compatibilidade 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS WAF ações e permissões para cada uma, consulte Ações definidas pela AWS WAF V2 na Referência de Autorização de Serviço.

As ações de política AWS WAF usam o seguinte prefixo antes da ação:

```
wafv2
```

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

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações AWS WAF que começam com`List`, inclua a seguinte ação:

```
"Action": "wafv2:List*"
```

Para ver exemplos de políticas AWS WAF baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF

Ações que exigem configurações de permissões adicionais

Algumas ações exigem permissões que não podem ser completamente descritas em Ações definidas pela AWS WAF V2 na Referência de Autorização de Serviço. Esta seção fornece informações adicionais sobre permissões.

Tópicos

- Permissões para AssociateWebACL
- Permissões para DisassociateWebACL
- Permissões para GetWebACLForResource
- Permissões para ListResourcesForWebACL

Permissões para **`AssociateWebACL`**

Esta seção lista as permissões necessárias para associar uma web ACL a um recurso usando a ação `AssociateWebACL` do AWS WAF .

Para CloudFront distribuições da Amazon, em vez dessa ação, use a CloudFront ação`UpdateDistribution`. Para obter mais informações, consulte UpdateDistributiona Amazon CloudFront API Reference.

API REST do Amazon API Gateway

Requer permissão para chamar o API Gateway `SetWebACL` no tipo de recurso da API REST e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Requer permissão para chamar `elasticloadbalancing:SetWebACL` uma ação no tipo de recurso do Application Load Balancer e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API do GraphQL

Requer permissão para chamar AWS AppSync `SetWebACL` o tipo de recurso da API GraphQL e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
```

```
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Grupo de usuários do Amazon Cognito

Requer permissão para chamar a `AssociateWebACL` ação do Amazon Cognito no tipo de recurso do grupo de usuários e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner serviço

Requer permissão para chamar a `AssociateWebACL` ação do App Runner no tipo de recurso do serviço App Runner e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
```

```
            "wafv2:AssociateWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "AssociateWebACL2",
        "Effect": "Allow",
        "Action": [
            "apprunner:AssociateWebAcl"
        ],
        "Resource": [
            "arn:aws:apprunner:*:account-id:service/*/*"
        ]
    }
```

AWS Instância de acesso verificado

Requer permissão para chamar a `ec2:AssociateVerifiedAccessInstanceWebAcl` ação no tipo de recurso da instância de acesso verificado e para chamar AWS WAF `AssociateWebACL` uma ACL da web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Permissões para **`DisassociateWebACL`**

Esta seção lista as permissões necessárias para desassociar uma web ACL de um recurso usando a ação `DisassociateWebACL` do AWS WAF .

Para CloudFront distribuições da Amazon, em vez dessa ação, use a CloudFront ação `UpdateDistribution` com um ID de ACL da web vazio. Para obter mais informações, consulte UpdateDistributiona Amazon CloudFront API Reference.

API REST do Amazon API Gateway

Requer permissão para chamar `SetWebACL` do API Gateway no tipo de recurso da API REST. Não requer permissão para ligar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Requer permissão para chamar a ação `elasticloadbalancing:SetWebACL` no tipo de recurso do Application Load Balancer. Não requer permissão para ligar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API do GraphQL

Requer permissão para chamar o AWS AppSync `SetWebACL` tipo de recurso da API GraphQL. Não requer permissão para ligar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Grupo de usuários do Amazon Cognito

Requer permissão para chamar a `DisassociateWebACL` ação do Amazon Cognito no tipo de recurso do grupo de usuários e para chamar. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner serviço

Requer permissão para chamar a `DisassociateWebACL` ação App Runner no tipo de recurso de serviço App Runner e para chamar. AWS WAF `DisassociateWebACL`

```
{
```

```
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instância de acesso verificado

Requer permissão para chamar a `ec2:DisassociateVerifiedAccessInstanceWebAcl` ação no tipo de recurso da instância de Acesso Verificado e para chamar AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Permissões para **`GetWebACLForResource`**

Esta seção lista as permissões necessárias para obter a web ACL para um recurso protegido usando a ação `GetWebACLForResource` do AWS WAF .

Para CloudFront distribuições da Amazon, em vez dessa ação, use a CloudFront ação`GetDistributionConfig`. Para obter mais informações, consulte GetDistributionConfiga Amazon CloudFront API Reference.

> **Note**
>
> `GetWebACLForResource` requer permissão para chamar `GetWebACL`. Nesse contexto, AWS WAF usa `GetWebACL` apenas para verificar se sua conta tem a permissão necessária para acessar a Web ACL que `GetWebACLForResource` retorna. Ao ligar`GetWebACLForResource`, você pode receber um erro indicando que sua conta não está autorizada a atuar `wafv2:GetWebACL` no recurso. AWS WAF não adiciona esse tipo de erro ao histórico de AWS CloudTrail eventos.

API REST do Amazon API Gateway, Application Load Balancer e API GraphQL AWS AppSync

Exigir permissão para ligar AWS WAF `GetWebACLForResource` e `GetWebACL` solicitar uma ACL da web.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Grupo de usuários do Amazon Cognito

Requer permissão para chamar a `GetWebACLForResource` ação do Amazon Cognito no tipo de recurso do grupo de usuários e para chamar e. AWS WAF `GetWebACLForResource` `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
```

```
            "wafv2:GetWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "GetWebACLForResource2",
        "Effect": "Allow",
        "Action": [
            "cognito-idp:GetWebACLForResource"
        ],
        "Resource": [
            "arn:aws:cognito-idp:*:account-id:userpool/*"
        ]
    }
```

AWS App Runner serviço

Requer permissão para chamar a `DescribeWebAclForService` ação App Runner no tipo de recurso do serviço App Runner e para chamar e. AWS WAF `GetWebACLForResource` `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instância de acesso verificado

Requer permissão para chamar a `ec2:GetVerifiedAccessInstanceWebAcl` ação no tipo de recurso da instância de Acesso Verificado e para chamar AWS WAF `GetWebACLForResource` `GetWebACL` e.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Permissões para **`ListResourcesForWebACL`**

Esta seção lista as permissões necessárias para recuperar a lista de recursos protegidos para uma web ACL usando a ação `ListResourcesForWebACL` do AWS WAF .

Para CloudFront distribuições da Amazon, em vez dessa ação, use a CloudFront ação`ListDistributionsByWebACLId`. Para obter mais informações, consulte ListDistributionsByWebAcLID na Amazon CloudFront API Reference.

API REST do Amazon API Gateway, Application Load Balancer e API GraphQL AWS AppSync

Exigir permissão AWS WAF `ListResourcesForWebACL` para solicitar uma Web ACL.

```
{
```

```
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Grupo de usuários do Amazon Cognito

Requer permissão para chamar a ação `ListResourcesForWebACL` do Amazon Cognito no tipo de recurso do grupo de usuários e para chamar `ListResourcesForWebACL` do AWS WAF .

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner serviço

Requer permissão para chamar a `ListAssociatedServicesForWebAcl` ação App Runner no tipo de recurso de serviço App Runner e para chamar. AWS WAF `ListResourcesForWebACL`

```
{
```

```
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instância de acesso verificado

Requer permissão para chamar a ação `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` no tipo de recurso da instância do acesso verificado e para chamar `ListResourcesForWebACL` do AWS WAF .

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
```

```
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Recursos políticos para AWS WAF

Oferece compatibilidade 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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver a lista de tipos de AWS WAF recursos e seus ARNs, consulte Recursos definidos pela AWS WAF V2 na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pela AWS WAF V2. Para permitir ou negar acesso a um subconjunto de AWS WAF recursos, inclua o ARN do recurso no elemento `resource` da sua política.

Os ARNs dos AWS WAF `wafv2` recursos têm o seguinte formato:

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Para obter informações sobre os ARNs, consulte Nomes de recurso da Amazon (ARN) na Referência geral da Amazon Web Services.

A seguir, são listados os requisitos específicos dos ARNs dos recursos `wafv2`:

- *região*: para AWS WAF recursos que você usa para proteger as CloudFront distribuições da Amazon, defina `us-east-1` isso como. Caso contrário, defina isso para a região que você está usando com seus recursos regionais protegidos.
- *escopo*: defina o escopo `global` para uso com uma CloudFront distribuição da Amazon ou `regional` para uso com qualquer um dos recursos regionais que oferecem AWS WAF suporte. Os recursos regionais são uma API REST do Amazon API Gateway, um Application Load Balancer, uma API GraphQL AWS AppSync , um grupo de usuários do Amazon Cognito, um AWS App Runner serviço e uma instância de acesso verificado. AWS
- *resource-type*: especifique um dos seguintes valores: `webacl`, `rulegroup`, `ipset`, `regexpatternset` ou `managedruleset`.
- *resource-name*: especifique o nome que você deu ao recurso AWS WAF ou especifique um curinga (`*`) para indicar todos os recursos que atendem às outras especificações no ARN. Você deve especificar o nome do recurso e a ID do recurso ou especificar um caractere curinga para ambos.
- *resource-id*: especifique o ID do recurso AWS WAF ou especifique um curinga (`*`) para indicar todos os recursos que atendem às outras especificações no ARN. Você deve especificar o nome do recurso e a ID do recurso ou especificar um caractere curinga para ambos.

Por exemplo, o ARN a seguir especifica todas as web ACLscom escopo regional da conta `111122223333` na região `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

O ARN a seguir especifica o grupo de regras nomeado `MyIPManagementRuleGroup` com escopo global para a conta `111122223333` na Região `us-east-1`:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Para ver exemplos de políticas AWS WAF baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF

Chaves de condição de política para AWS WAF

Suporta 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Além disso, AWS WAF oferece suporte às seguintes chaves de condição que você pode usar para fornecer uma filtragem refinada para suas políticas do IAM:

- onda 2: LogDestinationResource

  Essa chave de condição usa uma especificação do Amazon Resource Name (ARN) para o destino do registro. Esse é o ARN que você fornece para o destino de registro ao usar a chamada da API REST. `PutLoggingConfiguration`

  Você pode especificar explicitamente um ARN e especificar a filtragem para o ARN. O exemplo a seguir especifica a filtragem para ARNs de bucket do Amazon S3 que têm uma localização e um prefixo específicos.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- onda 2: LogScope

Essa chave de condição define a origem da configuração de registro em uma string. Atualmente, isso é sempre definido como o padrão de`Customer`, o que indica que o destino do registro pertence e é gerenciado por você.

Para ver uma lista de chaves de AWS WAF condição, consulte Chaves de condição para AWS WAF V2 na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela AWS WAF V2.

Para ver exemplos de políticas AWS WAF baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF

ACLs em AWS WAF

Oferece compatibilidade 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS WAF

Oferece compatibilidade com ABAC (tags em políticas)	Parcial

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS WAF

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Encaminhar sessões de acesso para serviço AWS WAF

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS WAF

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, 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 AWS WAF a funcionalidade. Edite as funções de serviço somente quando AWS WAF fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS WAF

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções AWS WAF vinculadas a serviços, consulte. Usando funções vinculadas a serviços para AWS WAF

Exemplos de políticas baseadas em identidade para o AWS WAF

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS WAF . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS WAF, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para AWS WAF V2 na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de políticas
- Usar o console do AWS WAF
- Permitir que os usuários visualizem suas próprias permissões
- Conceda acesso somente de leitura a AWS WAF,, e CloudFront CloudWatch
- Conceda acesso total a AWS WAF, CloudFront, e CloudWatch
- Conceda acesso a um único Conta da AWS
- Conceda acesso a uma única web ACL
- Conceda acesso a CLI a uma web ACL e a um grupo de regras

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS WAF recursos em sua conta. Essas ações podem incorrer em custos para a 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 mais informações, 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 mais informações 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: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode 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 AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition 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 acionáveis para ajudar você a criar políticas seguras e funcionais. Para mais informações, 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 a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

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

Usar o console do AWS WAF

Para acessar o AWS WAF console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS WAF recursos em seu

Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do 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 a operação de API que estiverem tentando executar.

Para garantir que usuários e funções possam usar o AWS WAF console, anexe também pelo menos a política AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS gerenciada às entidades. Para obter mais informações sobre esta política gerenciada, consulte AWS política gerenciada: AWSWAFConsoleReadOnlyAccess. Para obter mais informações sobre como adicionar uma política a um usuário, consulte Adição de permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

Conceda acesso somente de leitura a AWS WAF,, e CloudFront CloudWatch

A política a seguir concede aos usuários acesso somente de leitura aos AWS WAF recursos, às distribuições CloudFront web da Amazon e às métricas da Amazon. CloudWatch É útil para usuários que precisam de permissão para visualizar as configurações em AWS WAF condições, regras e ACLs da web para ver qual distribuição está associada a uma ACL da web e para monitorar métricas e uma amostra de solicitações recebidas. CloudWatch Esses usuários não podem criar, atualizar nem excluir recursos do AWS WAF :

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Conceda acesso total a AWS WAF, CloudFront, e CloudWatch

A política a seguir permite que os usuários realizem qualquer AWS WAF operação, executem qualquer operação em distribuições CloudFront da web e monitorem métricas e uma amostra de solicitações recebidas. CloudWatch É útil para usuários que são AWS WAF administradores.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Recomendamos que você configure autenticação multifator (MFA) para os usuários que tiverem permissões administrativas. Para obter mais informações, consulte Como usar dispositivos com autenticação multifator (MFA) com o AWS no Guia do usuário do IAM.

Conceda acesso a um único Conta da AWS

Esta política concede as seguintes permissões para a conta 444455556666:

- Acesso total a todas as AWS WAF operações e recursos.
- Leia e atualize o acesso a todas as CloudFront distribuições, o que permite associar ACLs e CloudFront distribuições da web.
- Acesso de leitura a todas as CloudWatch métricas e estatísticas métricas, para que você possa visualizar CloudWatch dados e uma amostra de solicitações no AWS WAF console.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

Conceda acesso a uma única web ACL

A política a seguir permite que os usuários realizem qualquer AWS WAF operação por meio do console em uma Web ACL específica na conta444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
```

```
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Conceda acesso a CLI a uma web ACL e a um grupo de regras

A política a seguir permite que os usuários realizem qualquer AWS WAF operação por meio da CLI em uma ACL da web específica e em um grupo de regras específico na conta. 444455556666

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

A política a seguir permite que os usuários realizem qualquer AWS WAF operação por meio do console em uma Web ACL específica na conta444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS políticas gerenciadas para AWS WAF

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: AWSWAFReadOnlyAccess

Essa política concede permissões somente de leitura que permitem aos usuários acessar AWS WAF recursos e recursos para serviços integrados, como Amazon, Amazon API Gateway CloudFront, Application Load Balancer, AWS AppSync Amazon Cognito e Verified Access. AWS App Runner AWS Você pode anexar essa política às suas identidades do IAM. AWS WAF também anexa essa política a uma função de serviço que permite AWS WAF realizar ações em seu nome.

Para obter detalhes sobre essa política, consulte AWSWAFReadOnlyAccessno console do IAM.

AWS política gerenciada: AWSWAFFullAccess

Essa política concede acesso total a AWS WAF recursos e recursos para serviços integrados, como Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner e Verified Access. AWS Você pode anexar essa política às suas identidades do IAM. AWS WAF também anexa essa política a uma função de serviço que permite AWS WAF realizar ações em seu nome.

Para obter detalhes sobre essa política, consulte AWSWAFFullAccessno console do IAM.

AWS política gerenciada: AWSWAFConsoleReadOnlyAccess

Essa política concede permissões somente de leitura ao AWS WAF console, o que inclui recursos para AWS WAF e para serviços integrados, como Amazon, Amazon API Gateway CloudFront, Application Load Balancer, AWS AppSync Amazon Cognito e Verified Access AWS App Runner. AWS Você pode anexar essa política às suas identidades do IAM. AWS WAF também anexa essa política à função de serviço aiam/home#/policies/arn:aws:iam: :aws:policy/ $ que permite realizar ações em seu nome. AWSWAFConsoleFullAccess serviceLevelSummary AWS WAF

Para obter detalhes sobre essa política, consulte AWSWAFConsoleReadOnlyAccessno console do IAM.

AWS política gerenciada: AWSWAFConsoleFullAccess

Essa política concede acesso total ao AWS WAF console, que inclui recursos para AWS WAF e para serviços integrados, como Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner e Verified Access. AWS Você pode anexar essa política às suas identidades do IAM. AWS WAF também anexa essa política a uma função de serviço que permite AWS WAF realizar ações em seu nome.

Para obter detalhes sobre essa política, consulte AWSWAFConsoleFullAccessno console do IAM.

AWS política gerenciada: WAFV2 LoggingServiceRolePolicy

Essa política permite AWS WAF gravar registros no Amazon Data Firehose. Essa política é usada somente se você habilitar o login AWS WAF. Esta política é anexada à função vinculada ao serviço `AWSServiceRoleForWAFV2Logging`. Para obter mais informações sobre a função vinculada ao serviço, consulte Usando funções vinculadas a serviços para AWS WAF.

Para obter detalhes sobre essa política, consulte WAFV2 LoggingServiceRolePolicy no console do IAM.

AWS WAF atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS WAF desde que esse serviço começou a rastrear essas alterações. Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico do AWS WAF documento emHistórico do documento.

Política	Descrição de alteração	Data
`WAFV2LoggingServiceRolePolicy` Essa política permite AWS WAF gravar registros no Amazon Data Firehose. Ele é usado somente se você ativar o registro.	IDs de declaração (Sids) adicionados às configurações de permissões na função vinculada ao serviço à qual essa política está anexada.	2024-06-03

Política	Descrição de alteração	Data
Detalhes no console do IAM: WAFV2 LoggingServiceRolePolicy.		
`AWSServiceRoleForWAFV2Logging` Essa função vinculada ao serviço fornece políticas de permissões que permitem AWS WAF gravar registros no Amazon Data Firehose. Detalhes no console do IAM: AWSServiceRoleForWAFV2Logging.	IDs de declaração (Sids) adicionados às configurações de permissões.	2024-06-03
AWS WAF adições ao rastreamento de alterações	AWS WAF começou a rastrear as alterações na política gerenciada `WAFV2LoggingServiceRolePolicy` e na função vinculada ao serviço. `AWSServiceRoleForWAFV2Logging`	2024-06-03
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Permissões expandidas para adicionar instâncias de acesso AWS verificado aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-06-17

Política	Descrição de alteração	Data
`AWSWAFReadOnlyAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFReadOnlyAccess.	Permissões expandidas para adicionar instâncias de acesso AWS verificado aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-06-17
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Permissões expandidas para adicionar instâncias de acesso AWS verificado aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-06-17
`AWSWAFConsoleReadOnlyAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleReadOnlyAccess.	Permissões expandidas para adicionar instâncias de acesso AWS verificado aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-06-17

Política	Descrição de alteração	Data
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Permissões expandidas para corrigir as configurações de acesso AWS App Runner dos serviços.	2023-06-06
`AWSWAFReadOnlyAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFReadOnlyAccess.	Permissões expandidas para corrigir as configurações de acesso AWS App Runner dos serviços.	2023-06-06
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Permissões expandidas para corrigir as configurações de acesso AWS App Runner dos serviços.	2023-06-06

Política	Descrição de alteração	Data
`AWSWAFConsoleReadOnlyAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleReadOnlyAccess.	Permissões expandidas para corrigir as configurações de acesso AWS App Runner dos serviços.	2023-06-06
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Permissões expandidas para adicionar AWS App Runner serviços aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-03-30
`AWSWAFReadOnlyAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFReadOnlyAccess.	Permissões expandidas para adicionar AWS App Runner serviços aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-03-30

Política	Descrição de alteração	Data
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Permissões expandidas para adicionar AWS App Runner serviços aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-03-30
`AWSWAFConsoleReadOnlyAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleReadOnlyAccess.	Permissões expandidas para adicionar AWS App Runner serviços aos tipos de recursos com os quais você pode se proteger AWS WAF.	2023-03-30
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Permissões expandidas para adicionar grupos de usuários do Amazon Cognito aos tipos de recursos com os quais você pode se proteger. AWS WAF	2022-08-25

Política	Descrição de alteração	Data
`AWSWAFReadOnlyAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFReadOnlyAccess.	Permissões expandidas para adicionar grupos de usuários do Amazon Cognito aos tipos de recursos com os quais você pode se proteger. AWS WAF	2022-08-25
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Permissões expandidas para adicionar grupos de usuários do Amazon Cognito aos tipos de recursos com os quais você pode se proteger. AWS WAF	2022-08-25
`AWSWAFConsoleReadOnlyAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleReadOnlyAccess.	Permissões expandidas para adicionar grupos de usuários do Amazon Cognito aos tipos de recursos com os quais você pode se proteger. AWS WAF	2022-08-25

Política	Descrição de alteração	Data
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Foram corrigidas as configurações de permissões para entrega de registros para o Amazon Simple Storage Service (Amazon S3) e o Amazon Logs. CloudWatch Essa alteração soluciona os erros de acesso negado que estavam ocorrendo durante a configuração dos logs. Para obter informações sobre como registrar seu tráfego de web ACL, consulte Registrando AWS WAF tráfego de ACL da web.	2022-01-11
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Foram corrigidas as configurações de permissões para entrega de registros para o Amazon Simple Storage Service (Amazon S3) e o Amazon Logs. CloudWatch Essa alteração soluciona os erros de acesso que estavam ocorrendo durante a configuração dos logs. Para obter informações sobre como registrar seu tráfego de web ACL, consulte Registrando AWS WAF tráfego de ACL da web.	2022-01-11

Política	Descrição de alteração	Data
`AWSWAFFullAccess` Essa política permite AWS WAF gerenciar AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFFullAccess.	Foram adicionadas novas permissões para opções de logs expandidas. Essa alteração dá AWS WAF acesso aos destinos de registro adicionais Amazon Simple Storage Service (Amazon S3) e CloudWatch Amazon Logs. Para obter informações sobre como registrar seu tráfego de web ACL, consulte Registrando AWS WAF tráfego de ACL da web.	2021-11-15
`AWSWAFConsoleFullAccess` Essa política permite AWS WAF gerenciar recursos AWS do console e outros AWS recursos em seu nome em AWS WAF e em serviços integrados. Detalhes no console do IAM: AWSWAFConsoleFullAccess.	Foram adicionadas novas permissões para opções de logs expandidas. Essa alteração dá AWS WAF acesso aos destinos de registro adicionais Amazon Simple Storage Service (Amazon S3) e CloudWatch Amazon Logs. Para obter informações sobre como registrar seu tráfego de web ACL, consulte Registrando AWS WAF tráfego de ACL da web.	2021-11-15
AWS WAF começou a rastrear alterações	AWS WAF começou a rastrear as mudanças em suas políticas AWS gerenciadas.	2021-3-01

Solução de problemas AWS WAF de identidade e acesso

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

Tópicos

Não estou autorizado a realizar uma ação em AWS WAF

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 `wafv2:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2: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 `wafv2:`*`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 uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS WAF.

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 fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS WAF. 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 acessem meus AWS WAF recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode 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), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS WAF compatível com esses recursos, consulteComo AWS WAF 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 usar funções e políticas baseadas em recursos 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 WAF

AWS WAF usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS WAF As funções vinculadas ao serviço são predefinidas AWS WAF 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 AWS WAF porque você não precisa adicionar manualmente as permissões necessárias. AWS WAF define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS WAF pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

É possível excluir uma função vinculada ao serviço somente depois de excluir os recursos relacionados da função. Isso protege seus AWS WAF recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS WAF

AWS WAF usa a função vinculada ao serviço `AWSServiceRoleForWAFV2Logging` para gravar registros no Amazon Data Firehose. Essa função é usada somente se você habilitar o login AWS WAF. Para obter informações sobre registro em log, consulte Registrando AWS WAF tráfego de ACL da web.

Essa função vinculada ao serviço é anexada à política AWS gerenciada. `WAFV2LoggingServiceRolePolicy` Para obter mais informações sobre a política gerenciada, consulte AWS política gerenciada: WAFV2 LoggingServiceRolePolicy.

A função vinculada ao serviço `AWSServiceRoleForWAFV2Logging` confia no serviço `wafv2.amazonaws.com` para presumir a função.

As políticas de permissões da função AWS WAF permitem concluir as seguintes ações nos recursos especificados:

- Ações do Amazon Data Firehose: `PutRecord` e no `PutRecordBatch` Firehose, recursos de streaming de dados com um nome que começa com. `aws-waf-logs-` Por exemplo, `aws-waf-logs-us-east-2-analytics`.
- AWS Organizations ação: `DescribeOrganization` sobre os recursos das organizações da Organizations.

Veja a função completa vinculada ao serviço no console do IAM:. AWSServiceRoleForWAFV2Logging

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Crie uma função vinculada ao serviço para o AWS WAF

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você ativa o AWS WAF registro no AWS Management Console, ou faz uma `PutLoggingConfiguration` solicitação na AWS WAF CLI ou na AWS WAF API, AWS WAF cria a função vinculada ao serviço para você.

Você deve ter a permissão `iam:CreateServiceLinkedRole` para habilitar o registro em log.

Se excluir essa função vinculada a serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você ativa o AWS WAF registro em log, AWS WAF cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o AWS WAF

AWS WAF não permite que você edite a função `AWSServiceRoleForWAFV2Logging` 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 obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS WAF

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o AWS WAF serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir AWS WAF recursos usados pelo **`AWSServiceRoleForWAFV2Logging`**

1. No AWS WAF console, remova o registro em log de cada Web ACL. Para ter mais informações, consulte Registrando AWS WAF tráfego de ACL da web.
2. Usando a API ou a CLI, envie uma solicitação `DeleteLoggingConfiguration` para cada web ACL que tem o registro em log habilitado. Para obter mais informações, consulte Referência de API do AWS WAF.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir a função vinculada ao serviço `AWSServiceRoleForWAFV2Logging`. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS WAF

AWS WAF suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte AWS WAF Endpoints e cotas.

Registro e monitoramento em AWS WAF

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS WAF suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus AWS WAF recursos e responder a possíveis eventos:

CloudWatch Alarmes da Amazon

Usando CloudWatch alarmes, você observa uma única métrica durante um período de tempo especificado. Se a métrica exceder um determinado limite, CloudWatch envia uma notificação para um tópico AWS Auto Scaling ou política do Amazon SNS. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.

AWS CloudTrail troncos

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS WAF. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS WAF, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Registro de chamadas de API do AWS CloudTrail com.

AWS WAF registro de tráfego de ACL da web

AWS WAF oferece registro do tráfego que suas ACLs da web analisam. Os registros incluem informações como a hora em que AWS WAF recebeu a solicitação do seu AWS recurso protegido, informações detalhadas sobre a solicitação e a configuração de ação da regra à qual a solicitação correspondeu. Para ter mais informações, consulte Registrando AWS WAF tráfego de ACL da web.

Validação de conformidade para AWS WAF

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. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os

atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS WAF

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 executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

Segurança da infraestrutura no AWS WAF

Como serviço gerenciado, AWS WAF é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS WAF pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

AWS WAF cotas

> **Note**
>
> Esta é a versão mais recente do AWS WAF. Para AWS WAF Classic, consulteAWS WAF clássico.

AWS WAF está sujeito às seguintes cotas (anteriormente chamadas de limites). Essas cotas são as mesmas para todas as regiões em que AWS WAF está disponível. Cada região está sujeita a essas cotas individualmente. As cotas não são cumulativas entre regiões.

AWS WAF tem cotas padrão no número máximo de entidades que você pode ter por conta. Você pode solicitar um aumento dessas cotas.

Recurso	Cota padrão por conta por região
Número máximo de :web ACLs	100
Número máximo de grupos de regras	100
Número máximo de conjuntos de IP	100
Número máximo de solicitações por segundo por web ACL	25.000
Número máximo de cabeçalhos de solicitação personalizados por web ACL ou grupo de regras	100
Número máximo de cabeçalhos de resposta personalizados por web ACL ou grupo de regras	100
Número máximo de corpos de resposta personalizados por web ACL ou grupo de regras	50
Número máximo de domínios de token em uma lista de domínios de tokens da web ACL	10

O máximo de solicitações por segundo (RPS) permitido AWS WAF em CloudFront é definido CloudFront e descrito no Guia do CloudFront Desenvolvedor.

AWS WAF tem cotas fixas nas seguintes configurações de entidade por conta por região. Essas cotas não podem ser alteradas.

Recurso	Cotas por conta por região
Unidades de capacidade web ACL (WCUs) máximas por web ACL*	5.000
Máximo de WCUs por grupo de regras	5.000
Número máximo de instruções de referência por grupo de regras. Em um grupo de regras, uma instrução de referência pode fazer referência a um conjunto de IPs ou a um conjunto de padrões regex.	50
Número máximo de instruções de referência por web ACL. Em uma Web ACL, uma instrução de referência pode referenciar um grupo de regras, um conjunto de IPs ou um conjunto de padrões regex.	50
Número máximo de endereços IP na notação CIDR por conjunto de IP	10.000
Número máximo de regras baseadas em intervalos por web ACL	10
Número máximo de regras com base em intervalos por grupo de regras	4
Taxa mínima de solicitação que pode ser definida para uma regra baseada em taxa	100
Número máximo de endereços IP exclusivos que podem ter um intervalo limitado por regra baseada em intervalos	10.000
Número máximo de caracteres permitidos para uma instrução de correspon dência de string	200
Número máximo de caracteres em cada padrão regex	200
Número máximo de padrões de regex exclusivos por conjunto de regex	10

Recurso	Cotas por conta por região
Número máximo de conjuntos de regex	10
Tamanho máximo do corpo de uma solicitação da Web que pode ser inspecionado quanto ao Application Load AWS AppSync Balancer e às proteções	8 KB
Tamanho máximo de um corpo de solicitação da web que pode ser inspecionado CloudFront, API Gateway, Amazon Cognito, App Runner e proteções de acesso verificado**	64 KB
Número máximo de transformações de texto por instrução de regra	10
Tamanho máximo do conteúdo do corpo de resposta personalizada para uma única definição de resposta personalizada	4 KB
Número máximo de cabeçalhos personalizados para uma única definição de resposta personalizada	10
Número máximo de cabeçalhos personalizados para uma única definição de solicitação personalizada	10
Tamanho máximo combinado de todo o conteúdo do corpo de resposta para um único grupo de regras ou uma única web ACL	50 KB

*O uso de mais de 1.500 WCUs em uma web ACL gera custos além do preço básico da web ACL. Para obter mais informações, consulte AWS WAF unidades de capacidade web ACL (WCUs) e Definição de preço do AWS WAF.

**Por padrão, o limite de inspeção corporal é definido em 16 KB para CloudFront os recursos do API Gateway, Amazon Cognito, App Runner e Verified Access, mas você pode aumentá-lo para qualquer um desses recursos na sua configuração de ACL da web, até o máximo listado. Para ter mais informações, consulte Gerenciando os limites de tamanho da inspeção corporal.

AWS WAF tem as seguintes cotas fixas de chamadas por conta por região. Essas cotas se aplicam ao total de chamadas para o serviço por qualquer meio disponível, incluindo o console, a CLI, o AWS CloudFormation, a API REST e os SDKs. Essas cotas não podem ser alteradas.

Tipo de chamada	Cotas por conta por região
Número máximo de chamadas para `AssociateWebACL`	Um pedido a cada 2 segundos
Número máximo de chamadas para `DisassociateWebACL`	Um pedido a cada 2 segundos
Número máximo de chamadas para `GetWebACLForResource`	Um pedido por segundo
Número máximo de chamadas para `ListResourcesForWebACL`	Um pedido por segundo
Número máximo de chamadas para qualquer ação `Get` ou `List` individual, se nenhuma outra cota for definida para ela	Cinco solicitaç ões por segundo
Número máximo de chamadas para qualquer ação `Create`, `Put` ou `Update` individual, se nenhuma outra cota for definida para ela	Um pedido por segundo

Migrando seus recursos AWS WAF clássicos para AWS WAF

Esta seção fornece orientação para migrar suas regras e ACLs da web do AWS WAF Classic para o. AWS WAF AWS WAF foi lançado em novembro de 2019. Se você criou recursos como regras e ACLs da web usando o AWS WAF Classic, precisará trabalhar com eles usando o AWS WAF Classic ou migrá-los para a versão mais recente.

Antes de começar seu trabalho de migração, familiarize-se AWS WAF lendoAWS WAF.

Tópicos

- Por que migrar para AWS WAF?
- Como funciona a migração
- Limitações e advertências de migração
- Migrando uma ACL da web do AWS WAF Classic para o AWS WAF

Por que migrar para AWS WAF?

A versão mais recente do AWS WAF fornece muitas melhorias em relação à versão anterior, mantendo a maioria dos conceitos e terminologia com os quais você está acostumado.

A lista a seguir descreve as principais alterações na versão mais atual do AWS WAF. Antes de continuar com a migração, reserve um tempo para revisar essa lista e se familiarizar com o restante do AWS WAF guia.

- AWS Regras gerenciadas para AWS WAF — Os grupos de regras agora disponíveis por meio de regras AWS gerenciadas oferecem proteção contra ameaças comuns na web. A maioria desses grupos de regras está incluída gratuitamente no AWS WAF. Para obter mais informações, consulte AWS Lista de grupos de regras de regras gerenciadas e a postagem do blog Anunciando regras AWS gerenciadas para AWS WAF.
- Nova AWS WAF API — A nova API permite que você configure todos os seus AWS WAF recursos usando um único conjunto de APIs. Para distinguir entre aplicativos regionais e globais, a nova API inclui uma configuração `scope`. Para obter mais informações sobre a API, consulte Ações do WAFV2 AWS e AWS Tipos de dados do WAFV2 .

  Nas APIs, SDKs, CLIs e AWS CloudFormation, o AWS WAF Classic mantém seus esquemas de nomenclatura e essa versão mais recente do AWS WAF é referida com um `V2` ou adicionado`v2`, dependendo do contexto.
- Cotas de serviço simplificadas (limites) — AWS WAF agora permite mais regras por ACL da web e permite que você expresse padrões de regex mais longos. Para ter mais informações, consulte AWS WAF cotas.
- Os limites do Web ACL agora são baseados nas necessidades de computação — os limites do Web ACL agora são baseados nas unidades de capacidade do Web ACL (WCU). AWS WAF calcula a WCU para uma regra de acordo com a capacidade operacional necessária para executar a regra. O WCU de uma web ACL é a soma do WCU de todas as regras e dos grupos de regras da web ACL.

  Para obter informações gerais sobre WCU, consulte Como AWS WAF funciona. Para obter informações sobre o uso de cada regra no WCU, consulte Princípios básicos da instrução de regras.
- Escrita de regras baseada em documentos: Agora você pode escrever e expressar regras, grupos de regras e web ACLsno formato JSON. Não é mais necessário usar chamadas de API individuais para criar condições diferentes e associar as condições a uma regra. Isso simplifica muito a forma

como você escreve e mantém seu código. Você pode acessar um formato JSON de suas web ACLspor meio do console quando estiver visualizando a web ACL, escolhendo Download web ACL as JSON (Baixar web ACL como JSON). Ao criar sua própria regra, você pode acessar sua representação JSON escolhendo o Rule JSON editor (editor de regra JSON).

- Aninhamento de regras e suporte completo de operação lógica: você pode escrever regras combinadas complexas usando instruções de regra lógica e aninhamento. É possível criar instruções como `[A AND NOT(B OR C)]`. Para ter mais informações, consulte Instruções de regras lógicas.
- Regras aprimoradas com base em taxas — Na versão mais recente do AWS WAF, você pode personalizar a janela de tempo que a regra avalia e como a regra agrega as solicitações. Você pode personalizar a agregação usando combinações de várias características de solicitações da web. Além disso, as regras mais recentes baseadas em tarifas reagem mais rapidamente às mudanças no tráfego. Para ter mais informações, consulte Instrução de regra baseada em intervalos.
- Suporte de gama CIDR variável para especificações de conjunto: As especificações do conjunto de IP agora têm mais flexibilidade nos intervalos IP. Para IPv4, AWS WAF suporta a. `/1 /32` Para IPv6, AWS WAF suporta a. `/1 /128` Para obter mais informações sobre os conjuntos de IP, consulte Instrução de regra de correspondência de conjunto de IPs
- Transformações de texto encadeáveis — AWS WAF pode realizar várias transformações de texto no conteúdo da solicitação da Web antes de inspecioná-lo. Para ter mais informações, consulte Opções de transformação de texto.
- Experiência de console aprimorada — O novo AWS WAF console apresenta um criador de regras visual e um design de console mais intuitivo para o usuário.
- Opções expandidas para AWS WAF políticas do Firewall Manager — No gerenciamento de ACLs da AWS WAF web pelo Firewall Manager, agora você pode criar um conjunto de grupos de regras que são AWS WAF processados primeiro e um conjunto de grupos de regras que são AWS WAF processados por último. Depois de aplicar a AWS WAF política, os proprietários de contas locais podem adicionar seus próprios grupos de regras que AWS WAF são processados entre esses dois conjuntos. Para obter informações sobre as políticas do AWS WAF Firewall Manager, consulte AWS WAF políticas.
- AWS CloudFormation suporte para todos os tipos de declaração de regra — o AWS WAF in AWS CloudFormation oferece suporte a todos os tipos de declaração de regra compatíveis com o AWS WAF console e a API. Além disso, você pode facilmente converter as regras que você escreve no formato JSON para o formato YAML.

Como funciona a migração

A migração automatizada transfere a maior parte da configuração do AWS WAF Classic web ACL, deixando algumas coisas que você precisa manipular manualmente.

As etapas abaixo mostram como migrar uma web ACL.

1. A migração automatizada lê tudo relacionado à sua ACL da web existente, sem modificar ou excluir nada no Classic. AWS WAF Ele cria uma representação da ACL da web e de seus recursos relacionados, compatível com o. AWS WAF Ele gera um modelo de AWS CloudFormation para a nova web ACL e o armazena em um bucket do Amazon S3.
2. Você implanta o modelo em AWS CloudFormation, a fim de recriar a ACL da web e os recursos relacionados em. AWS WAF
3. Revise a web ACL e conclua manualmente a migração, certificando-se de que a nova web ACL aproveite ao máximo os recursos mais recentes do AWS WAF.
4. Alterne manualmente os recursos protegidos para a nova web ACL.

Limitações e advertências de migração

A migração não transporta todas as suas configurações, exatamente como você as tem no AWS WAF Classic. Algumas coisas, como regras gerenciadas, não são mapeadas identicamente entre as duas versões. Outras configurações, como as associações da web ACL com recursos protegidos da AWS , são desativadas inicialmente na nova versão para que você possa adicioná-las quando estiver pronto.

A lista a seguir descreve as advertências da migração e todas as etapas que você pode executar em resposta. Use esta visão geral para planejar a migração. As etapas detalhadas de migração, posteriormente, compartilham as etapas de mitigação recomendadas.

- Conta única — Você só pode migrar recursos do AWS WAF Classic de qualquer conta para AWS WAF recursos da mesma conta.
- Regras gerenciadas — A migração não traz nenhuma regra gerenciada dos AWS Marketplace vendedores. Alguns AWS Marketplace vendedores têm regras gerenciadas equivalentes para as AWS WAF quais você pode se inscrever novamente. Antes de fazer isso, revise as regras AWS gerenciadas fornecidas com a versão mais recente do AWS WAF. A maioria deles é gratuita para AWS WAF os usuários. Para obter informações sobre regras gerenciadas, consulte Grupos de regras gerenciadas.

- Associações da web ACL: a migração não traz nenhuma associação entre a web ACL e os recursos protegidos. Isso é feito por projeto, para evitar afetar sua workload de produção. Depois de verificar se tudo foi migrado corretamente, associe a nova web ACL aos recursos.
- Registro em log: O registro em log da web ACL migrada está desabilitado por padrão. Isso faz parte do design. Ative o registro quando estiver pronto para mudar do AWS WAF Classic para AWS WAF o.
- AWS Firewall Manager grupos de regras — A migração não lida com grupos de regras gerenciados pelo Firewall Manager. Você pode migrar uma web ACL gerenciada pelo Firewall Manager, mas a migração não trará o grupo de regras. Em vez de usar a ferramenta de migração para essas :web ACLs, recrie a política para o novo AWS WAF no Firewall Manager.

  > **Note**
  >
  > Os grupos de regras que o Firewall Manager gerenciou para o AWS WAF Classic foram grupos de regras do Firewall Manager. Com a nova versão do AWS WAF, os grupos de regras são grupos de AWS WAF regras. Funcionalmente, eles são iguais.

- AWS WAF Automações de segurança — Não tente migrar nenhuma automação de AWS WAF segurança. A migração não converte funções do Lambda, que podem estar em uso pelas automações. Quando uma nova solução AWS WAF de automação de segurança estiver disponível e compatível com a mais recente AWS WAF, reimplante essa solução.

Migrando uma ACL da web do AWS WAF Classic para o AWS WAF

Para migrar uma web ACL e alternar para ela, execute a migração automatizada e, então, conclua algumas etapas manuais.

Tópicos

- Migração de uma web ACL: migração automatizada
- Migração de uma web ACL: acompanhamento manual
- Migração de uma web ACL: considerações adicionais
- Migração de uma web ACL: transição

Migração de uma web ACL: migração automatizada

Para migrar automaticamente uma configuração de Web ACL do Classic para AWS WAFAWS WAF

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. Escolha Alternar para o AWS WAF clássico e revise suas configurações para a Web ACL. Anote as configurações, considerando as advertências e limitações descritas na seção anterior, Limitações e advertências de migração.
3. Na caixa de diálogo informativa na parte superior, localize a frase que começa com Migrar web ACLse escolha o link para o assistente de migração. Essa ação iniciará o assistente de migração.

   Se você não vê a caixa de diálogo informativa, talvez a tenha fechado desde que iniciou o console AWS WAF clássico. Na barra de navegação, escolha Alternar para novo e AWS WAF escolha Alternar para AWS WAF clássico, e o diálogo informativo deve reaparecer.
4. Selecione a web ACL que você deseja migrar.
5. Em Configuração de migração, forneça um bucket do Amazon S3 a ser usado para o modelo. Você precisa de um bucket do Amazon S3 que esteja configurado corretamente para a API de migração, para armazenar o AWS CloudFormation modelo que ele gera.

   - Se o bucket for criptografado, a criptografia deverá usar chaves do Amazon S3 (SSE-S3). A migração não oferece suporte à criptografia com chaves AWS Key Management Service (SSE-KMS).
   - O nome do bucket deve começar com `aws-waf-migration-`. Por exemplo, `aws-waf-migration-my-web-acl`.
   - O bucket precisa estar na região em que você está implantando o modelo. Por exemplo, para uma web ACL na região `us-west-2`, você deve usar um bucket do Amazon S3 em `us-west-2` e implantar a pilha de modelos em `us-west-2`.
6. Em Política de buckets do S3, recomendamos escolher Aplicar automaticamente a política de bucket necessária para a migração. Como opção, se quiser gerenciar o bucket por conta própria, você deverá aplicar manualmente a seguinte política de bucket:

   - Para CloudFront aplicativos globais da Amazon (`waf`):

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

- Para aplicativos regionais do Amazon API Gateway ou do Application Load Balancer (`waf-regional`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. Em Choose how to handle rules that cannot be migrated (Escolher como lidar com regras que não podem ser migradas), escolha excluir as regras que não podem ser migradas ou interromper a migração. Para obter informações sobre as regras que não podem ser migradas, consulte Limitações e advertências de migração.
8. Escolha Próximo.
9. Em Criar AWS CloudFormation modelo, verifique suas configurações e escolha Começar a criar AWS CloudFormation modelo para iniciar o processo de migração. Isso pode levar alguns minutos, dependendo da complexidade da web ACL.

10. Em Criar e executar AWS CloudFormation pilha para concluir a migração, você pode optar por acessar o AWS CloudFormation console para criar uma pilha a partir do modelo e criar a nova Web ACL e seus recursos. Para fazer isso, escolha Criar AWS CloudFormation pilha.

Após a conclusão do processo de migração automática, você estará pronto para seguir as etapas manuais de acompanhamento. Consulte Migração de uma web ACL: acompanhamento manual.

Migração de uma web ACL: acompanhamento manual

Após a conclusão da migração automatizada, revise a web ACL recém-criada e preencha os componentes que a migração não trouxe para você. O procedimento a seguir aborda os aspectos do gerenciamento de web ACL que a migração não processa. Para ver a lista, consulte Limitações e advertências de migração.

Para concluir a migração básica: etapas manuais

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.
2. O console deve usar automaticamente a versão mais recente do AWS WAF. Para verificar isso, no painel de navegação, verifique se você pode ver a opção Alternar para o AWS WAF clássico. Se você ver Alternar para novo AWS WAF, escolha essa opção para mudar para a versão mais recente.
3. No painel de navegação, selecione Web ACLs.
4. Na página Web ACLs (:web ACLs) localize a nova web ACL na lista da região em que você a criou. Escolha o nome da web ACL para exibir as configurações dela.
5. Revise todas as configurações da nova ACL da web em relação à sua ACL da web AWS WAF clássica anterior. Por padrão, o log e as associações de recursos protegidos são desabilitados. Ative-os quando estiver pronto para mudar.
6. Se sua ACL web AWS WAF clássica tinha uma regra baseada em taxas com uma condição, a condição não foi trazida na migração. Você poderá adicionar condições à regra na nova web ACL.

    a. Na página de configurações da web ACL, escolha a guia Regras.

    b. Localize a regra com base em taxas na lista, selecione-a e escolha Edit (Editar).

    c. Em Criteria to count request towards rate limit (Critérios para contar as solicitações com relação ao limite de taxas), selecione Only consider requests that match the criteria in a

rule statement (Considerar somente as solicitações que correspondem aos critérios em uma instrução de regra) e, então, forneça seus critérios adicionais. Você pode adicionar os critérios usando qualquer instrução de regra que pode ser aninhada, incluindo instruções lógicas. Para obter informações sobre suas opções, consulte Instrução de regra baseada em intervalos.

7. Se sua ACL web AWS WAF clássica tinha um grupo de regras gerenciado, a inclusão do grupo de regras não foi incluída na migração. Você poderá adicionar grupos de regras gerenciadas à nova web ACL. Analise as informações sobre grupos de regras gerenciadas, incluindo a lista de regras AWS gerenciadas que estão disponíveis com a nova versão do AWS WAF, emGrupos de regras gerenciadas. Para adicionar um grupo de regras gerenciadas, faça o seguinte:

   a. Na página de configurações de web ACL, escolha a guia Regras da web ACL.

   b. Escolha Add rules (Adicionar regras) e Add managed rule groups (Adicionar grupos de regras gerenciadas).

   c. Expanda a listagem do fornecedor da sua escolha e selecione os grupos de regras que você quer adicionar. Para AWS Marketplace vendedores, talvez seja necessário se inscrever nos grupos de regras. Para obter mais informações sobre como usar grupos de regras gerenciadas na web ACL, consulte Grupos de regras gerenciadas e Avaliação de regras da web ACL e do grupo de regras.

Depois de concluir o processo básico de migração, recomendamos que você analise suas necessidades e considere opções adicionais, para ter certeza de que a nova configuração é a mais eficiente possível e que você está usando as opções de segurança mais recentes disponíveis. Consulte Migração de uma web ACL: considerações adicionais.

Migração de uma web ACL: considerações adicionais

Analise sua nova ACL da web e considere as opções disponíveis na nova AWS WAF para garantir que a configuração seja a mais eficiente possível e que esteja usando as opções de segurança mais recentes disponíveis.

Regras AWS gerenciadas adicionais

Considere implementar regras AWS gerenciadas adicionais em sua ACL da web para aumentar a postura de segurança do seu aplicativo. Estes estão incluídos sem AWS WAF custo adicional. AWS As regras gerenciadas apresentam os seguintes tipos de grupos de regras:

- Os grupos de regras de linha de base fornecem proteção geral contra várias ameaças comuns, como o impedimento de entradas nocivas conhecidas no seu aplicativo e o acesso à página de administração.
- Os grupos de regras específicos de caso de uso fornecem proteção incremental para muitos casos de uso e ambientes.
- As listas de reputação de IP fornecem informações sobre ameaças com base no IP de origem do cliente.

Para ter mais informações, consulte AWS Regras gerenciadas para AWS WAF.

Otimização e limpeza das regras

Revise suas regras antigas e considere otimizá-las reescrevendo-as ou removendo aquelas que estiverem desatualizadas. Por exemplo, se no passado você implantou um AWS CloudFormation modelo do artigo técnico sobre as 10 principais vulnerabilidades de aplicativos Web do OWASP, Prepare-se para o uso das 10 principais vulnerabilidades de aplicativos da Web do OWASP AWS WAF e nosso novo white paper, considere substituí-lo por regras gerenciadas. AWS Embora o conceito encontrado no documento ainda seja aplicável e possa ajudá-lo a escrever suas próprias regras, as regras criadas pelo modelo foram amplamente substituídas pelas Regras AWS gerenciadas.

CloudWatch Métricas e alarmes da Amazon

Revise suas CloudWatch métricas da Amazon e configure alarmes conforme necessário. A migração não transmite CloudWatch alarmes e é possível que os nomes das métricas não sejam o que você deseja.

Reveja com sua equipe de aplicativos

Trabalhe com sua equipe de aplicativos e verifique sua segurança. Descubra quais campos são analisados com frequência pelo aplicativo e adicione regras para depurar a entrada de forma adequada. Verifique se há casos com lacunas e adicione regras para detectar esses casos se a lógica de negócios do aplicativo não conseguir processá-los.

Planeje a transição

Planeje o cronograma da transição com sua equipe de aplicativos. A mudança da antiga associação de web ACL para a nova pode levar um pouco de tempo para se propagar para todas as áreas em que seus recursos estão armazenados. O tempo de propagação pode ser de alguns segundos a

alguns minutos. Durante esse período, algumas solicitações serão processadas pela antiga web ACL e outras serão processadas pela nova web ACL. Seus recursos estarão protegidos durante toda a mudança, mas você poderá notar inconsistências no tratamento da solicitação enquanto a mudança estiver em andamento.

Quando estiver pronto para mudar, siga o procedimento em Migração de uma web ACL: transição.

Migração de uma web ACL: transição

Depois de verificar as novas configurações da web ACL, você pode começar a usá-la no lugar da web ACL do AWS WAF Classic.

Para começar a usar sua nova AWS WAF Web ACL

1. Associe a AWS WAF Web ACL aos recursos que você deseja proteger, seguindo as orientações emAssociando ou desassociando uma ACL da web com um recurso AWS. Isso automaticamente desassocia os recursos da web ACL antiga.

   A mudança pode levar de alguns segundos a alguns minutos para se propagar. Durante esse período, algumas solicitações podem ser processadas pela antiga web ACL e outras pela nova web ACL. Seus recursos estarão protegidos durante toda a mudança, mas você poderá notar inconsistências no tratamento da solicitação até que ela seja concluída.
2. Configure o log para a nova web ACL, seguindo as orientações em Registrando AWS WAF tráfego de ACL da web.
3. (Opcional) Se sua ACL web AWS WAF clássica não estiver mais associada a nenhum recurso, considere removê-la totalmente do AWS WAF Classic. Para mais informações, consulte Exclusão de uma ACL da web.

AWS WAF clássico

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

AWS WAF O Classic é um firewall de aplicativo web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas para uma API do Amazon API Gateway, Amazon CloudFront ou Application Load Balancer. AWS WAF O Classic também permite que você controle o acesso ao seu conteúdo. Com base nas condições que você especifica, como os endereços IP dos quais as solicitações se originam ou os valores das cadeias de caracteres de consulta, o API Gateway CloudFront ou um Application Load Balancer responde às solicitações com o conteúdo solicitado ou com um código de status HTTP 403 (Proibido). Você também pode configurar CloudFront para retornar uma página de erro personalizada quando uma solicitação for bloqueada.

Tópicos

Configurando o AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Este tópico descreve as etapas preliminares, como a criação de uma conta de usuário, para prepará-lo para usar o AWS WAF Classic. Você não é cobrado por isso. Você é cobrado somente pelos AWS serviços que você usa.

> **Note**
>
> Se você for um novo usuário do AWS WAF, não siga estas etapas de configuração do AWS WAF Classic. Em vez disso, siga as etapas da versão mais recente do AWS WAF, emConfigurando sua conta para usar os serviços.

Depois de concluir essas etapas, consulte Começando com o AWS WAF Classic para continuar começando a usar o AWS WAF Classic.

> **Note**
>
> AWS Shield Standard está incluído no AWS WAF Classic e não requer configuração adicional. Para ter mais informações, consulte Como o AWS Shield Shield Advanced funcionam.

Antes de usar o AWS WAF Classic ou AWS Shield Advanced pela primeira vez, conclua as etapas nesta seção.

Tópicos

- Inscreva-se para um Conta da AWS

- Criar um usuário com acesso administrativo
- Fazer download das ferramentas

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Fazer download das ferramentas

AWS Management Console Inclui um console para o AWS WAF Classic, mas se você quiser acessar o AWS WAF Classic programaticamente, consulte o seguinte:

- Se você quiser chamar a API AWS WAF clássica sem precisar lidar com detalhes de baixo nível, como montar solicitações HTTP brutas, use um AWS SDK. Os AWS SDKs fornecem funções e tipos de dados que encapsulam a funcionalidade do AWS WAF Classic e de outros serviços. AWS Para baixar um AWS SDK, consulte a página aplicável, que também inclui pré-requisitos e instruções de instalação:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Para obter uma lista completa dos AWS SDKs, consulte Ferramentas para Amazon Web Services.
- Se você estiver usando uma linguagem de programação para a qual AWS não fornece um SDK, a Referência da AWS WAF API documenta as operações suportadas pelo AWS WAF Classic.
- O AWS Command Line Interface (AWS CLI) oferece suporte ao AWS WAF Classic. Isso AWS CLI permite que você controle vários AWS serviços a partir da linha de comando e os automatize por meio de scripts. Para ter mais informações, consulte AWS Command Line Interface.
- AWS Tools for Windows PowerShell suporta AWS WAF Classic. Para obter mais informações, consulte Referência de Cmdlets do AWS Tools for PowerShell.

Como funciona o AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.

Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Você usa o AWS WAF Classic para controlar como o API Gateway, a Amazon CloudFront ou um Application Load Balancer respondem às solicitações da web. Comece criando condições, regras e listas de controle de acesso à web (web ACLs). Você define as condições, combina as condições em regras e combinar as regras em uma web ACL.

> **Note**
>
> Você também pode usar o AWS WAF Classic para proteger seus aplicativos hospedados em contêineres do Amazon Elastic Container Service (Amazon ECS). O Amazon ECS é um serviço de gerenciamento de contêineres com alta escalabilidade e rapidez que facilita a execução, a interrupção e o gerenciamento de contêineres do Docker em um cluster. Para usar essa opção, você configura o Amazon ECS para usar um Application Load Balancer habilitado para AWS WAF Classic para rotear e proteger o tráfego HTTP/HTTPS (camada 7) nas tarefas do seu serviço. Para obter mais informações, consulte o tópico Balanceador de carga de serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

Condições

As condições definem as características básicas que você deseja que o AWS WAF Classic observe nas solicitações da web:

- Scripts que provavelmente são mal-intencionados. Os invasores incorporam scripts que podem explorar vulnerabilidades nas aplicações web. Isso é conhecido como cross-site scripting.
- Endereços IP ou intervalos de endereços IP dos quais as solicitações se originam.
- País ou localização geográfica de origem das solicitações.
- Comprimento das partes específicas da solicitação, como a string de consulta.
- Código SQL que provavelmente é mal-intencionado. Os invasores tentam extrair dados do seu banco de dados ao incorporarem código SQL mal-intencionado a uma solicitação da web. Isso é conhecido como injeção de SQL.
- Strings que aparecem na solicitação, por exemplo, valores que aparecem no cabeçalho `User-Agent` ou strings de texto que aparecem na string de consulta. Você também pode usar expressões regulares (regex) para especificar essas strings.

Algumas condições têm vários valores. Por exemplo, você pode especificar até 10,000 endereços IP ou intervalos de endereços IP em uma condição de IP.

Regras

Você combina condições em regras para direcionar com precisão as solicitações que você deseja permitir, bloquear ou contar. AWS WAF O Classic fornece dois tipos de regras:

Regra regular

As regras regulares usam apenas condições para apontar solicitações específicas. Por exemplo, com base nas solicitações recentes que está vendo de um invasor, você pode criar uma regra que inclui as seguintes condições:

- As solicitações vêm de 192.0.2.44.
- Elas contém o valor `BadBot` no cabeçalho do `User-Agent`.
- Elas parecem incluir código do tipo SQL na query string.

Quando uma regra inclui várias condições, como neste exemplo, o AWS WAF Classic procura solicitações que correspondam a todas as condições, ou seja, ele usa o `AND` para unir as condições.

Adicione pelo menos uma condição a uma regra regular. Uma regra regular sem condições não pode corresponder a nenhuma solicitação, portanto, a ação da regra (permitir, contar ou bloquear) nunca é acionada.

Regra baseada em intervalos

As regras baseada em intervalos são como regras regulares com um limite de taxa adicional. Uma regra baseada em intervalos conta as solicitações que chegam de endereços IP que atendem às condições da regra. Se as solicitações de um endereço IP excederem o limite de taxa em um período de cinco minutos, a regra poderá acionar uma ação. Pode levar um ou dois minutos para que a ação seja acionada.

As condições são opcionais nas regras com base em taxa. Se você não adicionar nenhuma condição em uma regra com base em taxa, o limite de taxa será aplicado a todos os endereços IP. Se você combinar condições com o limite de taxa, o limite de taxa será aplicado aos endereços IP que corresponderem às condições.

Por exemplo, com base nas solicitações recentes que você viu de um invasor, é possível criar uma regra baseada em intervalos que inclui as seguintes condições:

- As solicitações vêm de 192.0.2.44.
- Elas contém o valor `BadBot` no cabeçalho do `User-Agent`.

Nesta regra baseada em intervalos, você também define um limite de taxa. Neste exemplo, vamos supor que você crie um limite de taxa de 1.000. As solicitações que atenderem às duas condições anteriores e excederem 1.000 solicitações por cinco minutos acionarão a ação da regra (bloquear ou contar), que foi definida na web ACL.

As solicitações que não atenderem a ambas as condições não serão contabilizadas para o limite de taxa e não serão afetadas por essa regra.

Como um segundo exemplo, suponha que você queira limitar as solicitações a uma determinada página em seu site. Para fazer isso, você pode adicionar a seguinte condição de correspondência de string a uma regra baseada em intervalos:

- A Parte da solicitação a ser usada como filtro é `URI`.
- O Match Type é `Starts with`.
- O Value to match é `login`.

Além disso, você especifica um `RateLimit` de 1.000.

Ao adicionar essa regra baseada em intervalos a uma web ACL, você pode limitar as solicitações à sua página de login sem afetar o restante do site.

Web ACLs

Depois de combinar suas condições em regras, você combina as regras em uma web ACL. É neste ponto que você define uma ação para cada regra: permitir, bloquear ou contar, além de uma ação padrão:

Uma ação para cada regra

Quando uma solicitação da web corresponde a todas as condições de uma regra, o AWS WAF Classic pode bloquear a solicitação ou permitir que a solicitação seja encaminhada para a API do API Gateway, CloudFront distribuição ou um Application Load Balancer. Você especifica a ação que deseja que o AWS WAF Classic execute para cada regra.

AWS WAF O Classic compara uma solicitação com as regras em uma ACL da web na ordem em que você listou as regras. AWS WAF Em seguida, o Classic executa a ação associada à primeira regra à qual a solicitação corresponde. Por exemplo, se uma solicitação da Web

corresponder a uma regra que permite solicitações e outra regra que bloqueia solicitações, o AWS WAF Classic permitirá ou bloqueará a solicitação, dependendo da regra listada primeiro.

Se quiser testar uma nova regra antes de começar a usá-la, você também pode configurar o AWS WAF Classic para contar as solicitações que atendem a todas as condições da regra. Assim como ocorre com regras que permitem ou bloqueiam solicitações, uma regra que conta solicitações é afetada pela posição que ocupa na lista de regras da web ACL. Por exemplo, se uma solicitação da web corresponder a uma regra que permite solicitações e a outra regra que conta solicitações, e se a regra que permite solicitações estiver listada primeiro, a solicitação não será contada.

Uma ação padrão

A ação padrão determina se o AWS WAF Classic permite ou bloqueia uma solicitação que não corresponde a todas as condições em nenhuma das regras na ACL da web. Por exemplo, vamos supor que você cria uma web ACL e adiciona apenas a regra que definiu antes:

- As solicitações vêm de 192.0.2.44.
- Elas contém o valor `BadBot` no cabeçalho do `User-Agent`.
- Elas parecem incluir código SQL mal-intencionado na string de consulta.

Se uma solicitação não atender às três condições da regra e se a ação padrão for`ALLOW`, o AWS WAF Classic encaminha a solicitação para o API Gateway CloudFront ou para um Application Load Balancer, e o serviço responderá com o objeto solicitado.

Se você adicionar duas ou mais regras a uma ACL da web, o AWS WAF Classic executará a ação padrão somente se uma solicitação não atender a todas as condições em nenhuma das regras. Por exemplo, vamos supor que você adicione uma segunda regra que contém uma condição:

- As solicitações que contêm o valor `BIGBadBot` no cabeçalho `User-Agent`.

AWS WAF O Classic executa a ação padrão somente quando uma solicitação não atende às três condições na primeira regra e não atende a uma condição na segunda regra.

Em algumas ocasiões, AWS WAF pode encontrar um erro interno que atrasa a resposta ao Amazon API Gateway, à Amazon CloudFront ou a um Application Load Balancer sobre a possibilidade de permitir ou bloquear uma solicitação. Nessas ocasiões, CloudFront normalmente permite a solicitação ou veicula o conteúdo. O API Gateway e um Application Load Balancer normalmente negarão a solicitação e não fornecerão o conteúdo.

AWS WAF Preços clássicos

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Com o AWS WAF Classic, você paga somente pelas ACLs e regras da web que você cria e pelo número de solicitações HTTP que o AWS WAF Classic inspeciona. Para obter mais informações, consulte Preços do AWS WAF Classic.

Começando com o AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Este tutorial mostra como usar o AWS WAF Classic para realizar as seguintes tarefas:

- Configure o AWS WAF Classic.
- Crie uma lista de controle de acesso à web (Web ACL) usando o console AWS WAF Classic e especifique as condições que você deseja usar para filtrar solicitações da web. Por exemplo, você pode especificar os endereços IP dos quais se originam as solicitações e os valores na solicitação que são usados apenas por invasores.
- Adicione as condições a uma regra. As regras permitem que você direcione as solicitações da web que você deseja bloquear ou permitir. Uma solicitação da web deve corresponder a todas

as condições em uma regra antes que o AWS WAF Classic bloqueie ou permita solicitações com base nas condições que você especificar.

- Adicione as regras à web ACL. É aqui onde você especifica se deseja bloquear solicitações da web ou permiti-las, de acordo com as condições que você adiciona a cada regra.
- Especifique uma ação padrão, seja bloquear ou permitir. Essa é a ação que o AWS WAF Classic executa quando uma solicitação da web não corresponde a nenhuma de suas regras.
- Escolha a CloudFront distribuição da Amazon para a qual você deseja que o AWS WAF Classic inspecione as solicitações da web. Este tutorial aborda as etapas somente para CloudFront, mas o processo das APIs do Application Load Balancer e do Amazon API Gateway é basicamente o mesmo. AWS WAF O formato clássico CloudFront está disponível para todos Regiões da AWS. AWS WAF O Classic para uso com o API Gateway ou um Application Load Balancer está disponível nas regiões listadas nos endpoints de AWS serviço.

> **Note**
>
> AWS normalmente cobra menos de USD 0,25 por dia pelos recursos que você cria durante este tutorial. Quando você tiver concluído o tutorial, recomendamos que exclua os recursos para impedir cobranças desnecessárias.

Tópicos

Etapa 1: configurar o AWS WAF Classic

Se você ainda não seguiu as etapas gerais de configuração em Configurando o AWS WAF Classic, faça isso agora.

Etapa 2: Criar uma web ACL

O console AWS WAF Classic orienta você pelo processo de configuração do AWS WAF Classic para bloquear ou permitir solicitações da Web com base nas condições que você especificar, como os endereços IP dos quais as solicitações se originam ou os valores nas solicitações. Nesta etapa, você cria uma web ACL.

Para criar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Se for a primeira vez que você usa o AWS WAF Classic, escolha Go to AWS WAF Classic e, em seguida, escolha Configure web ACL.

   Se você já usou o AWS WAF Classic antes, escolha Web ACLs no painel de navegação e, em seguida, escolha Criar Web ACL.
3. Na página Name web ACL (Nomear web ACL), insira um nome em Web ACL name (Nome da web ACL).

   > **Note**
   >
   > Você não pode alterar o nome depois de criar a web ACL.
4. Para nome da CloudWatch métrica, insira um nome. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9). Ele não pode conter espaços em branco.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar a web ACL.
5. Em Region (Região da), escolha uma região. Se você associar essa ACL da web a uma CloudFront distribuição, escolha Global (CloudFront).

6. Em AWS resource to associate, escolha o recurso que você deseja associar à web ACL e, em seguida, escolha Next (Próximo).

Etapa 3: Criar uma condição de correspondência de IP

Uma condição de correspondência de IP especifica os endereços IP ou intervalos de endereços IP dos quais se originam as solicitações. Nesta etapa, você cria uma condição de correspondência de IP. Em uma etapa posterior, você especifica se deseja permitir ou bloquear solicitações originadas de endereços IP especificados.

> **Note**
>
> Para obter mais informações sobre as condições de correspondência de IP, consulte Trabalhar com condições de correspondência de IP.

Para criar uma condição de correspondência de IP

1. Na página Create conditions, em IP match conditions, escolha Create condition.
2. Na caixa de diálogo Create IP match condition (Criar condição de correspondência de IP), digite um nome em Name (Nome). O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./.
3. Em Address (Endereço), insira 192.0.2.0/24. Este intervalo de endereços IP, especificado na notação CIDR, inclui os endereços IP de 192.0.2.0 a 192.0.2.255. (O intervalo de endereços IP 192.0.2.0/24 é reservado para exemplos; portanto, não se originam de solicitações da web desses endereços IP.)

   AWS WAF O Classic suporta intervalos de endereços IPv4: /8 e qualquer intervalo entre /16 a /32. AWS WAF O Classic oferece suporte a intervalos de endereços IPv6: /24, /32, /48, /56, /64 e /128. (Para especificar um único endereço IP, como 192.0.2.44, digite 192.0.2.44/32.) Não há suporte para outros intervalos.

   Para obter mais informações sobre a notação CIDR, consulte o artigo na Wikipédia sobre CIDR.
4. Escolha Criar.

Etapa 4: Criar uma condição de correspondência geográfica

Uma condição de correspondência geográfica especifica o país ou os países de origem das solicitações. Nesta etapa, você cria uma condição de correspondência geográfica. Em uma etapa posterior, você especificará se deseja permitir ou bloquear solicitações originadas dos países especificados.

> **Note**
>
> Para obter mais informações sobre condições de correspondência geográfica, consulte Trabalhar com condições de correspondência geográfica.

Para criar uma condição de correspondência geográfica

1. Na página Create conditions, em Geo match conditions, escolha Create condition.
2. Na caixa de diálogo Create geo match condition (Criar condição de correspondência geográfica), digite um nome em Name (Nome). O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./.
3. Escolha um Location type e um país. Atualmente, o Location type (Tipo de local) só pode ser Country (País).
4. Escolha Add location.
5. Escolha Criar.

Etapa 5: Criar uma condição de correspondência de string

Uma condição de correspondência de string identifica as cadeias de caracteres que você deseja que o AWS WAF Classic pesquise em uma solicitação, como um valor especificado em um cabeçalho ou em uma string de consulta. Geralmente, uma string consiste em caracteres ASCII imprimíveis, mas você pode especificar qualquer caractere, do hexadecimal 0x00 a 0xFF (decimal 0 a 255). Nesta etapa, você cria uma condição de correspondência de string. Em uma etapa posterior, você especifica se deseja permitir ou bloquear as solicitações que contêm as strings especificadas.

> **Note**
>
> Para obter mais informações sobre as condições de correspondência de string, consulte Trabalhar com condições de correspondência de string.

Para criar uma condição de correspondência de string

1. Na página Create conditions (Criar condições), em String and regex match conditions (Condições de correspondência de string e regex), selecione Create condition (Criar condição).
2. Na caixa de diálogo Criar condição de correspondência de string, digite os seguintes valores:

   Nome

   Insira um nome. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./.

   Tipo

   Escolha String match.

   Parte da solicitação a ser usada como filtro

   Escolha a parte da solicitação da web que você deseja que o AWS WAF Classic inspecione em busca de uma string especificada.

   Para este exemplo, selecione Header.

   > **Note**
   >
   > Se você escolher Corpo para o valor de Parte da solicitação a ser filtrada, o AWS WAF Classic inspeciona somente os primeiros 8192 bytes (8 KB), pois CloudFront encaminha somente os primeiros 8192 bytes para inspeção. Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Header (Obrigatório se “Parte da solicitação a ser usada como filtro” for “Cabeçalho”)

Como você escolheu Cabeçalho para filtrar parte da solicitação, você deve especificar qual cabeçalho deseja que o AWS WAF Classic inspecione. Insira User-Agent. (Esse valor não diferencia maiúsculas de minúsculas.)

Tipo de correspondência

Escolha onde a string especificada deve aparecer no cabeçalho User-Agent. Por exemplo, no início, no fim ou em qualquer lugar da string.

Neste exemplo, escolha Exactly matches, o que indica que o AWS WAF Classic inspeciona solicitações da Web em busca de um valor de cabeçalho idêntico ao valor que você especificou.

Transformação

Em um esforço para contornar o AWS WAF Classic, os invasores usam formatação incomum em solicitações da web, por exemplo, adicionando espaço em branco ou codificando a URL de parte ou de toda a solicitação. As transformações convertem a solicitação da web em um formato mais padrão, removendo o espaço em branco, decodificando por URL a solicitação ou executando outras operações que eliminam grande parte da formatação incomum que os invasores normalmente usam.

Você só pode especificar um único tipo de transformação de texto.

Para este exemplo, selecione Nenhum.

O valor é codificado por Base64

Quando o valor que você digita em Value to match (Valor para corresponder) já é codificado por Base64, marque esta caixa de seleção.

Para este exemplo, não marque a caixa de seleção.

Valor para corresponder

Especifique o valor que você deseja que o AWS WAF Classic pesquise na parte das solicitações da web que você indicou em Parte da solicitação a ser filtrada.

Para este exemplo, insira BadBot. AWS WAF O Classic inspecionará o `User-Agent` cabeçalho nas solicitações da web em busca do valor BadBot.

O tamanho máximo de Value to match é 50 caracteres. Se você quiser especificar um valor codificado em base64, poderá fornecer até 50 caracteres antes da codificação.

3. Se você quiser que o AWS WAF Classic inspecione solicitações da Web em busca de vários valores, como um `User-Agent` cabeçalho que contém `BadBot` e uma string de consulta que contém`BadParameter`, você tem duas opções:

   - Se você deseja permitir ou bloquear solicitações da web somente quando elas contiverem os dois valores (`AND`), crie uma condição de correspondência de string para cada valor.
   - Se você deseja permitir ou bloquear solicitações da web quando elas contiverem um só dos valores ou ambos (`OR`), adicione os dois valores à mesma condição de correspondência de string.

   Para este exemplo, selecione Criar.

Etapa 5A: Criar uma condição regex (opcional)

Uma condição de expressão regular é um tipo de condição de correspondência de cadeia de caracteres e similar, pois identifica as cadeias de caracteres que você deseja que o AWS WAF Classic pesquise em uma solicitação, como um valor especificado em um cabeçalho ou em uma cadeia de caracteres de consulta. A principal diferença é que você usa uma expressão regular (regex) para especificar o padrão de string que você deseja que o AWS WAF Classic pesquise. Nesta etapa, você cria uma condição de correspondência regex. Em uma etapa posterior, você especifica se deseja permitir ou bloquear as solicitações que contêm as strings especificadas.

> **Note**
>
> Para obter mais informações sobre as condições de correspondência regex, consulte Trabalhar com condições de correspondência regex.

Para criar uma condição de correspondência regex

1. Na página Create conditions (Criar condições), em String match and regex conditions (Correspondência de string e condições de regex), selecione Create condition (Criar condição).
2. Na caixa de diálogo Criar condição de correspondência de string, digite os seguintes valores:

Nome

Insira um nome. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./.

Tipo

Escolha Regex match.

Parte da solicitação a ser usada como filtro

Escolha a parte da solicitação da web que você deseja que o AWS WAF Classic inspecione em busca de uma string especificada.

Para este exemplo, selecione Body.

> **Note**
>
> Se você escolher Corpo para o valor de Parte da solicitação a ser filtrada, o AWS WAF Classic inspeciona somente os primeiros 8192 bytes (8 KB), pois CloudFront encaminha somente os primeiros 8192 bytes para inspeção. Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Transformação

Em um esforço para contornar o AWS WAF Classic, os invasores usam formatação incomum em solicitações da web, por exemplo, adicionando espaço em branco ou codificando a URL de parte ou de toda a solicitação. As transformações convertem a solicitação da web em um formato mais padrão, removendo o espaço em branco, decodificando por URL a solicitação ou executando outras operações que eliminam grande parte da formatação incomum que os invasores normalmente usam.

Você só pode especificar um único tipo de transformação de texto.

Para este exemplo, selecione Nenhum.

Padrões regex para corresponder à solicitação

Escolha Create regex pattern set.

Nome do novo conjunto padrão

Insira um nome e, em seguida, especifique o padrão regex que você deseja que o AWS WAF Classic pesquise.

Em seguida, insira a expressão regular I [a@] mAb [a@] dRequest. AWS WAF O Classic inspecionará o `User-Agent` cabeçalho nas solicitações da web em busca dos valores:

- Eu sou BadRequest
- IamAB@dRequest
- Eu @mA BadRequest
- I@mAB@dRequest

3. Escolha Create pattern set and add filter.
4. Escolha Criar.

Etapa 6: Criar uma condição de correspondência de injeção de SQL

Uma condição de correspondência de injeção de SQL identifica a parte das solicitações da web, como um cabeçalho ou uma string de consulta, que você deseja que o AWS WAF Classic inspecione em busca de código SQL malicioso. Os invasores usam consultas SQL para extrair dados do seu banco de dados. Nesta etapa, você cria uma condição de correspondência de injeção de SQL. Em uma etapa posterior, você especifica se deseja permitir solicitações ou bloquear solicitações que aparentem conter código SQL mal-intencionado.

> **Note**
>
> Para obter mais informações sobre as condições de correspondência de string, consulte Trabalhar com condições de correspondência de injeção de SQL.

Para criar uma condição de correspondência de injeção de SQL

1. Na página Create conditions, em SQL injection match conditions, escolha Create condition.

2. Na caixa de diálogo Criar condição de correspondência de injeção de SQL, digite os seguintes valores:

   Nome

   Insira um nome.

   Parte da solicitação a ser usada como filtro

   Escolha a parte das solicitações da web que você deseja que o AWS WAF Classic inspecione em busca de código SQL malicioso.

   Para este exemplo, escolha Query string.

   > **Note**
   >
   > Se você escolher Corpo para o valor de Parte da solicitação a ser filtrada, o AWS WAF Classic inspeciona somente os primeiros 8192 bytes (8 KB), pois CloudFront encaminha somente os primeiros 8192 bytes para inspeção. Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

   Transformação

   Para este exemplo, selecione URL decode.

   Os atacantes usam formatação incomum, como codificação de URL, em um esforço para contornar o Classic. AWS WAF A opção URL decode elimina parte dessa formatação da solicitação da web antes que o AWS WAF Classic a inspecione.

   Você só pode especificar um único tipo de transformação de texto.

3. Escolha Criar.
4. Escolha Próximo.

Etapa 7: (Opcional) Criar condições adicionais

AWS WAF O clássico inclui outras condições, incluindo as seguintes:

- Condições de restrição de tamanho — identifica a parte das solicitações da web, como um cabeçalho ou uma string de consulta, que você deseja que o AWS WAF Classic verifique quanto ao comprimento. Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.
- Condições de correspondência de scripts entre sites — identifica a parte das solicitações da web, como um cabeçalho ou uma sequência de caracteres de consulta, que você deseja AWS WAF inspecionar em busca de scripts maliciosos. Para ter mais informações, consulte Trabalhar com condições de correspondência de cross-site scripting.

Você também pode criar essas condições agora ou você pular para Etapa 8: Criar uma regra e adicionar condições.

Etapa 8: Criar uma regra e adicionar condições

Você cria uma regra para especificar as condições que deseja que o AWS WAF Classic pesquise nas solicitações da web. Se você adicionar mais de uma condição a uma regra, uma solicitação da web deverá corresponder a todas as condições da regra para que o AWS WAF Classic permita ou bloqueie solicitações com base nessa regra.

> **Note**
>
> Para obter mais informações sobre regras, consulte Trabalhar com regras.

Para criar uma regra e adicionar condições

1. Na página Create rules, selecione Criar regra.
2. Na caixa de diálogo Create rule (Criar regra), digite os seguintes valores:

   Nome

   Insira um nome.

CloudWatch nome da métrica

Insira um nome para a CloudWatch métrica que o AWS WAF Classic criará e associará à regra. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9). Ele não pode conter espaços em branco.

Tipo de regra

Selecione Regular rule (Regra regular) ou Rate-based rule (Regra com base em taxa). As regras com base em taxa são idênticas às regras regulares, mas também levam em conta o número de solicitações que chegam do endereço IP identificado em qualquer período de cinco minutos. Para obter mais informações sobre os tipos de regra, consulte Como funciona o AWS WAF Classic. Para este exemplo, selecione `Regular rule`.

Limite de taxa

Para uma regra com base em taxa, insira o número máximo de solicitações a serem permitidas, em qualquer período de cinco minutos, de um endereço IP que corresponda às condições da regra.

3. Para a primeira condição que você deseja adicionar à regra, especifique as seguintes configurações:

   - Escolha se você deseja que o AWS WAF Classic permita ou bloqueie solicitações com base no fato de uma solicitação da Web corresponder ou não às configurações da condição.

     Para este exemplo, selecione does.
   - Escolha o tipo de condição que você deseja adicionar à regra: uma condição de conjunto de correspondência de IP, uma condição de conjunto de correspondência de string ou uma condição do conjunto de correspondência de injeção de SQL.

     Para este exemplo, selecione originate from IP addresses in.
   - Escolha a condição que você deseja adicionar à regra.

     Para este exemplo, escolha a condição de correspondência de IP criada em tarefas anteriores.
4. Escolha Adicionar condição.
5. Adicione a condição de correspondência geográfica criada por você anteriormente. Especifique os seguintes valores:

   - When a request does

- originate from a geographic location in
- Escolha a condição de correspondência geográfica.

6. Escolha Add another condition.
7. Adicione a condição de correspondência de string criada anteriormente. Especifique os seguintes valores:
   - When a request does
   - match at least one of the filters in the string match condition
   - Escolha a condição de correspondência de string.
8. Escolha Adicionar condição.
9. Adicione a condição de correspondência de injeção de SQL criada anteriormente. Especifique os seguintes valores:
   - When a request does
   - match at least one of the filters in the SQL injection match condition
   - Escolha sua condição de correspondência de injeção de SQL.
10. Escolha Adicionar condição.
11. Adicione a condição de restrição de tamanho criada anteriormente. Especifique os seguintes valores:
    - When a request does
    - match at least one of the filters in the size constraint condition
    - Escolha sua condição de restrição de tamanho.
12. Se você tiver criado outras condições, como uma condição regex, adicione-as de maneira semelhante.
13. Escolha Criar.
14. Para Default action, escolha Allow all requests that don't match any rules.
15. Selecione Review and create.

Etapa 9: Adicionar a regra a uma web ACL

Quando você adiciona a regra a uma web ACL, especifique as seguintes configurações:

- A ação que você deseja que o AWS WAF Classic execute em solicitações da web que correspondam a todas as condições da regra: permitir, bloquear ou contar as solicitações.
- A ação padrão para a web ACL. Essa é a ação que você deseja que o AWS WAF Classic execute em solicitações da web que não correspondem a todas as condições da regra: permitir ou bloquear as solicitações.

AWS WAF O Classic começa a bloquear solicitações CloudFront da web que correspondam a todas as condições a seguir (e a quaisquer outras que você possa ter adicionado):

- O valor do cabeçalho do `User-Agent` é `BadBot`
- (Se você tiver criado e adicionado a condição regex) O valor do `Body` é uma das quatro strings correspondente ao padrão `I[a@]mAB[a@]dRequest`
- As solicitações se originam de endereços IP no intervalo 192.0.2.0-192.0.2.255
- As solicitações se originam do país selecionado por você em sua condição de correspondência geográfica
- As solicitações parecem incluir código SQL mal-intencionado na string de consulta

AWS WAF O Classic permite CloudFront responder a qualquer solicitação que não atenda a todas essas três condições.

Etapa 10: Limpar os recursos

Você concluiu com êxito o tutorial. Para evitar que sua conta acumule cobranças adicionais do AWS WAF Classic, você deve limpar os objetos AWS WAF Classic que você criou. Como alternativa, você pode alterar a configuração de acordo com as solicitações da web que deseja realmente permitir, bloquear e contar.

> **Note**
>
> AWS normalmente cobra menos de USD 0,25 por dia pelos recursos que você cria durante este tutorial. Quando você tiver terminado, recomendamos excluir os recursos para impedir que cobranças desnecessárias.

Para excluir os objetos pelos quais o AWS WAF Classic cobra

1. Desassocie sua ACL da web da sua CloudFront distribuição:

a. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.

b. Selecione o nome da web ACL que deseja Delete. Isso abre uma página com os detalhes da ACL da web no painel direito.

c. No painel direito, na guia Regras, vá para a seção Recursos da AWS utilizando esta web ACL. Para a CloudFront distribuição à qual você associou a Web ACL, escolha o x na coluna Tipo.

2. Remova as condições de sua regra:

   a. No painel de navegação, escolha Regras.

   b. Escolha a regra criada durante o tutorial.

   c. Selecione Edit rule.

   d. Escolha x à direita do cabeçalho de cada condição.

   e. Escolha Atualizar.

3. Remova a regra de sua web ACL e exclua a web ACL:

   a. No painel de navegação, selecione Web ACLs.

   b. Escolha o nome da web ACL criada durante o tutorial. Isso abre uma página com os detalhes da ACL da web no painel direito.

   c. Na guia Rules, escolha Edit web ACL.

   d. Escolha x à direita do cabeçalho da regra.

   e. Escolha Ações e, em seguida, selecione Delete web ACL.

4. Exclua a regra:

   a. No painel de navegação, escolha Regras.

   b. Escolha a regra criada durante o tutorial.

   c. Escolha Delete.

   d. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.

AWS WAF O Classic não cobra pelas condições, mas se você quiser concluir a limpeza, execute o procedimento a seguir para remover os filtros das condições e excluí-las.

Para Delete filtros e condições

1. Exclua o intervalo de endereços IP na sua condição de correspondência de IP e exclua a condição de correspondência de IP:
   a. No painel de navegação do console AWS WAF clássico, escolha endereços IP.
   b. Escolha a condição de correspondência de IP criada durante o tutorial.
   c. Marque a caixa de seleção do intervalo de endereços IP que você adicionou.
   d. Selecione Delete IP address or range.
   e. No painel IP match conditions, escolha Delete.
   f. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.
2. Exclua o filtro na sua condição de correspondência de injeção de SQL e exclua a condição de correspondência de injeção SQL:
   a. No painel de navegação, selecione SQL injection.
   b. Escolha a condição de correspondência de injeção de SQL criada durante o tutorial.
   c. Marque a caixa de seleção para o filtro que você adicionou.
   d. Escolha Delete filter.
   e. No painel SQL injection match conditions, escolha Delete.
   f. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.
3. Exclua o filtro na sua condição de correspondência de string e exclua a condição de correspondência de string:
   a. No painel de navegação, escolha String and regex matching.
   b. Escolha a condição de correspondência de string criada durante o tutorial.
   c. Marque a caixa de seleção para o filtro que você adicionou.
   d. Escolha Delete filter.
   e. No painel String match conditions, escolha Delete.
   f. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.
4. Se você tiver criado um, exclua o filtro na condição de correspondência regex e exclua a condição de correspondência regex:
   a. No painel de navegação, escolha String and regex matching.
   b. Escolha a condição de correspondência regex criada por você durante o tutorial.

c. Marque a caixa de seleção para o filtro que você adicionou.

d. Escolha Delete filter.

e. No painel Regex match conditions, escolha Delete.

f. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.

5. Exclua o filtro na sua condição de restrição de tamanho e exclua a condição de restrição de tamanho:

a. No painel de navegação, selecione Size constraints.

b. Escolha a condição de restrição de tamanho criada durante o tutorial.

c. Marque a caixa de seleção para o filtro que você adicionou.

d. Escolha Delete filter.

e. No painel Size constraint conditions, escolha Delete.

f. Na caixa de diálogo Delete, escolha Delete novamente para confirmar.

Criar e configurar uma lista de controle de acesso à web (web ACL)

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Uma lista de controle de acesso à web (web ACL) oferece um controle refinado sobre as solicitações da web às quais sua API do Amazon API Gateway, CloudFront distribuição da Amazon ou Application Load Balancer responde. Você pode permitir ou bloquear os seguintes tipos de solicitações:

- Tenham se originado a partir de um endereço IP ou de um intervalo de endereços IP
- Origem de um país ou países específicos
- Contêm uma string especificada ou correspondem a um padrão de expressão regular (regex) em uma determinada parte das solicitações

- Excedam o comprimento especificado
- Pareçam conter código SQL mal-intencionado (conhecido como SQL injection)
- Pareçam conter scripts mal-intencionados (conhecidos como cross-site scripting)

Você também pode testar qualquer combinação dessas condições, bloquear ou contar solicitações da web que não apenas atendem às condições especificadas, mas também excedem um determinado número de solicitações em qualquer período de cinco minutos.

Para escolher as solicitações às quais você deseja dar acesso ao seu conteúdo ou que deseja bloquear, execute as seguintes tarefas:

1. Escolha a ação padrão, permitir ou bloquear, para solicitações da web que não corresponderem a nenhuma das condições que você especificar. Para ter mais informações, consulte Decidir quanto à ação padrão da web ACL.
2. Especifique as condições sob as quais você deseja permitir ou bloquear solicitações:
   - Para permitir ou bloquear solicitações com base no fato de as solicitações aparentarem conter ou não scripts mal-intencionados, crie condições de correspondência de cross-site scripting. Para ter mais informações, consulte Trabalhar com condições de correspondência de cross-site scripting.
   - Para permitir ou bloquear solicitações com base nos endereços IP dos quais elas se originam, crie condições de correspondência de IP. Para ter mais informações, consulte Trabalhar com condições de correspondência de IP.
   - Para permitir ou bloquear solicitações com base no país do qual elas se originam, crie condições de correspondência geográfica. Para ter mais informações, consulte Trabalhar com condições de correspondência geográfica.
   - Para permitir ou bloquear solicitações com base no fato de as solicitações excederem ou não um comprimento especificado, crie condições de restrição de tamanho. Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.
   - Para permitir ou bloquear solicitações com base no fato de as solicitações aparentarem conter código SQL mal-intencionado, crie condições de correspondência de injeção de SQL. Para ter mais informações, consulte Trabalhar com condições de correspondência de injeção de SQL.
   - Para permitir ou bloquear solicitações com base nas strings que aparecem nas solicitações, crie condições de correspondência de strings. Para ter mais informações, consulte Trabalhar com condições de correspondência de string.

- Para permitir ou bloquear solicitações com base em um padrão regex exibido nas solicitações, crie condições de correspondência regex. Para ter mais informações, consulte Trabalhar com condições de correspondência regex.

3. Adicione as condições para uma ou mais regras. Se você adicionar mais de uma condição à mesma regra, as solicitações da web deverão corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base na regra. Para ter mais informações, consulte Trabalhar com regras. Você também pode usar uma regra com base em taxa em vez de uma regra regular para limitar o número de solicitações de qualquer endereço IP que atenda às condições.
4. Adicione as regras para uma web ACL. Para cada regra, especifique se você deseja que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições que você adicionou à regra. Se você adicionar mais de uma regra a uma ACL da web, o AWS WAF Classic avaliará as regras na ordem em que elas estão listadas na ACL da web. Para ter mais informações, consulte Trabalho com :web ACLs.

   Quando você adiciona uma nova regra ou atualiza regras existentes, pode levar até um minuto para que as alterações apareçam e fiquem ativas nas ACLs e recursos da web.

Tópicos

Trabalhar com condições

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

As condições especificam quando você deseja permitir ou bloquear solicitações.

- Para permitir ou bloquear solicitações com base no fato de as solicitações aparentarem conter ou não scripts mal-intencionados, crie condições de correspondência de cross-site scripting. Para ter mais informações, consulte Trabalhar com condições de correspondência de cross-site scripting.
- Para permitir ou bloquear solicitações com base nos endereços IP dos quais elas se originam, crie condições de correspondência de IP. Para ter mais informações, consulte Trabalhar com condições de correspondência de IP.
- Para permitir ou bloquear solicitações com base no país do qual elas se originam, crie condições de correspondência geográfica. Para ter mais informações, consulte Trabalhar com condições de correspondência geográfica.
- Para permitir ou bloquear solicitações com base no fato de as solicitações excederem ou não um comprimento especificado, crie condições de restrição de tamanho. Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.
- Para permitir ou bloquear solicitações com base no fato de as solicitações aparentarem conter código SQL mal-intencionado, crie condições de correspondência de injeção de SQL. Para ter mais informações, consulte Trabalhar com condições de correspondência de injeção de SQL.
- Para permitir ou bloquear solicitações com base nas strings que aparecem nas solicitações, crie condições de correspondência de strings. Para ter mais informações, consulte Trabalhar com condições de correspondência de string.
- Para permitir ou bloquear solicitações com base em um padrão regex exibido nas solicitações, crie condições de correspondência regex. Para ter mais informações, consulte Trabalhar com condições de correspondência regex.

Tópicos

Trabalhar com condições de correspondência de cross-site scripting

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Invasores, às vezes, inserem scripts nas solicitações da web na tentativa de explorar as vulnerabilidades das aplicações web. Você pode criar uma ou mais condições de correspondência de scripts entre sites para identificar as partes das solicitações da web, como o URI ou a string de consulta, que você deseja que o AWS WAF Classic inspecione em busca de possíveis scripts maliciosos. Mais adiante no processo, ao criar uma web ACL, você especificará se deseja permitir ou bloquear solicitações que aparentem conter scripts mal-intencionados.

Tópicos

Criar condições de correspondência de cross-site scripting

Ao criar condições de correspondência de cross-site scripting, você pode especificar filtros. Os filtros indicam a parte das solicitações da Web que você deseja que o AWS WAF Classic inspecione em busca de scripts maliciosos, como o URI ou a string de consulta. Você pode adicionar mais de um filtro a uma condição de correspondência de cross-site scripting ou então criar uma condição separada para cada filtro. Veja como cada configuração afeta o comportamento do AWS WAF Classic:

- Mais de um filtro por condição de correspondência de script entre sites (recomendado) — Quando você adiciona uma condição de correspondência de script entre sites que contém vários filtros a uma regra e adiciona a regra a uma ACL da web, uma solicitação da web deve corresponder a

apenas um dos filtros na condição de correspondência de script entre sites para que o AWS WAF Classic permita ou bloqueie a solicitação com base nessa condição.

Por exemplo, vamos supor que você crie uma condição de correspondência de cross-site scripting e essa condição contenha dois filtros. Um filtro instrui o AWS WAF Classic a inspecionar o URI em busca de scripts maliciosos e o outro instrui o AWS WAF Classic a inspecionar a string de consulta. AWS WAF O Classic permite ou bloqueia solicitações se elas parecerem conter scripts maliciosos no URI ou na sequência de caracteres de consulta.

- Um filtro por condição de correspondência de script entre sites — Quando você adiciona as condições separadas de correspondência de script entre sites a uma regra e adiciona a regra a uma ACL da web, as solicitações da web devem corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições.

  Vamos supor que você crie duas condições e que cada condição contenha um dos dois filtros do exemplo anterior. Quando você adiciona as duas condições à mesma regra e adiciona a regra a uma ACL da web, o AWS WAF Classic permite ou bloqueia solicitações somente quando o URI e a string de consulta parecem conter scripts maliciosos.

> **Note**
>
> Ao adicionar uma condição de correspondência de script entre sites a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não pareçam conter scripts maliciosos.

Para criar uma condição de correspondência de cross-site scripting

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Cross-site scripting.
3. Escolha Create condition.
4. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de cross-site scripting.
5. Escolha Add another filter.

6. Se você quiser adicionar outro filtro, repita as etapas 4 e 5.
7. Ao terminar de adicionar os filtros, escolha Criar.

Valores especificados ao criar ou editar condições de correspondência de cross-site scripting

Ao criar ou atualizar uma condição de correspondência de cross-site scripting, você especifica os seguintes valores:

Nome

O nome da condição de correspondência de cross-site scripting.

O nome pode conter somente os caracteres A-Z, a-z, 0-9 e os caracteres especiais _-!"#`+*},./ . Você não poderá alterar o nome de uma condição depois de criá-la.

Parte da solicitação a ser usada como filtro

Escolha a parte de cada solicitação da web que você deseja que o AWS WAF Classic inspecione em busca de scripts maliciosos:

Cabeçalho

Um cabeçalho da solicitação especificada, como o cabeçalho `User-Agent` ou `Referer`. Se você selecionar Header, especifique o nome do cabeçalho no campo Header.

Método HTTP

O método HTTP, que indica o tipo de operação que a solicitação pede à origem para executar. CloudFront suporta os seguintes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`,, `PUT` e.

String de consulta

A parte de um URL exibida após um caractere `?`, se houver.

> **Note**
>
> Para condições de correspondência de scripts entre sites, recomendamos que você selecione Todos os parâmetros de consulta (somente valores) em vez de String de consulta para Parte da solicitação a ser usada como filtro.

URI

O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

A menos que uma transformação seja especificada, um URI não é normalizado e é inspecionado da mesma forma que o AWS recebe do cliente como parte da solicitação. Uma Transformação reformata o URI conforme especificado.

Corpo

A parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário.

> **Note**
>
> Se você selecionar Corpo para o valor de Parte da solicitação a ser usada como filtro, o AWS WAF Classic inspecionará somente os primeiros 8.192 bytes (8 KB). Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Parâmetro de consulta única (somente valor)

Qualquer parâmetro que você tenha definido como parte da string de consulta. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle”, você pode adicionar um filtro ao parâmetro ou. UserNameSalesRegion

Se você escolher Single query parameter (value only) [Parâmetro de consulta única (somente valor)], também especificará um Query parameter name (Nome de parâmetro de consulta). Esse é o parâmetro na sequência de caracteres de consulta que você inspecionará, como UserNameou SalesRegion. O tamanho máximo do Query parameter name (Nome de parâmetro de consulta) é 30 caracteres. O Query parameter name (Nome de parâmetro de consulta) não diferencia maiúsculas de minúsculas. Por exemplo, se você especificar UserNamecomo o nome do parâmetro Query, isso corresponderá a todas as variações de UserName, como username e userName.

Todos os parâmetros de consulta (somente valores)

Semelhante ao parâmetro de consulta única (somente valor), mas em vez de inspecionar os valores de um único parâmetro, o AWS WAF Classic inspeciona todos os valores de parâmetros na string de consulta em busca de possíveis scripts maliciosos. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle” e você escolher Todos os parâmetros de consulta (somente valores), o AWS WAF Classic acionará uma correspondência se o valor ou contiver possíveis scripts maliciosos. UserNameSalesRegion

Cabeçalho

Se você escolher Cabeçalho para filtrar parte da solicitação, escolha um cabeçalho na lista de cabeçalhos comuns ou insira o nome de um cabeçalho que você deseja que o AWS WAF Classic inspecione em busca de scripts mal-intencionados.

Transformação

Uma transformação reformata uma solicitação da web antes que o AWS WAF Classic inspecione a solicitação. Isso elimina algumas das formatações incomuns que os invasores usam nas solicitações da web em um esforço para contornar o Classic. AWS WAF

Você só pode especificar um único tipo de transformação de texto.

As transformações podem executar as seguintes operações:

Nenhum

AWS WAF O Classic não realiza nenhuma transformação de texto na solicitação da web antes de inspecioná-la para verificar se a string em Value corresponde.

Converter para minúsculas

AWS WAF O Classic converte letras maiúsculas (A-Z) em minúsculas (a-z).

Decodificação de HTML

AWS WAF O Classic substitui caracteres codificados em HTML por caracteres não codificados:

- Substitui `"` por &
- Substitui ` ` por espaço incondicional
- Substitui `<` por <
- Substitui `>` por >

- Substitui caracteres representados em formato hexadecimal, &#xhhhh;, pelos caracteres correspondentes
- Substitui caracteres representados em formato decimal, &#nnnn;, pelos caracteres correspondentes

Normalizar espaços em branco

AWS WAF O clássico substitui os seguintes caracteres por um caractere de espaço (decimal 32):

- \f, quebra de página, decimal 12
- \t, tabulação, decimal 9
- \n, quebra de linha, decimal 10
- \r, retorno de carro, decimal 13
- \v, tabulação vertical, decimal 11
- espaço incondicional, decimal 160

Além disso, essa opção substitui vários espaços por um único.

Simplificar a linha de comando

Para solicitações que contenham comandos de linha de comando do sistema operacional, use esta opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: \" '^
- Excluir espaços antes os seguintes caracteres: / (
- Substituir os seguintes caracteres por um espaço: , ;
- Substituir vários espaços por um espaço
- Converter maiúsculas (A-Z) em minúsculas (a-z)

Decodificar URL

Decodifica uma solicitação codificada por URL.

Adicionar excluir filtros em uma condição de correspondência de cross-site scripting

Você pode adicionar ou excluir filtros em uma condição de correspondência de cross-site scripting. Para alterar um filtro, adicione um novo e exclua o antigo.

Para adicionar ou excluir filtros em uma condição de correspondência de cross-site scripting

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Cross-site scripting.
3. Escolha a condição na qual você deseja adicionar ou excluir filtros.
4. Para adicionar filtros, execute as etapas a seguir:

   a. Escolha Adicionar filtro.

   b. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de cross-site scripting.

   c. Escolha Add.
5. Para excluir filtros, execute as etapas a seguir:

   a. Selecione o filtro que você deseja excluir.

   b. Escolha Delete filter.

Excluir condições de correspondência de cross-site scripting

Se você deseja excluir uma condição de correspondência de cross-site scripting, é preciso primeiro excluir todos os filtros na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de correspondência de cross-site scripting

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Cross-site scripting.
3. No painel Cross-site scripting match conditions, selecione a condição de correspondência de cross-site scripting que você deseja excluir.
4. No painel direito, selecione a guia Associated rules.

Se a lista de regras que usam essa condição de correspondência de cross-site scripting estiver vazia, vá para a etapa 6. Se a lista contiver regras, anote-as e continue para a etapa 5.

5. Para remover a condição de correspondência de cross-site scripting das regras que a estão usando, execute as seguintes etapas:

   a. No painel de navegação, escolha Rules (Regras).

   b. Escolha o nome de uma regra que esteja usando a condição de correspondência de cross-site scripting que você deseja excluir.

   c. No painel direito, selecione a condição de correspondência de cross-site scripting que você deseja remover da regra e escolha Remove selected condition.

   d. Repita as etapas b e c para todas as demais regras que estão usando a condição de correspondência de cross-site scripting que você deseja excluir.

   e. No painel de navegação, escolha Cross-site scripting.

   f. No painel Cross-site scripting match conditions, selecione a condição de correspondência de cross-site scripting que você deseja excluir.

6. Selecione Delete (Excluir) para excluir a condição selecionada.

Trabalhar com condições de correspondência de IP

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você deseja permitir ou bloquear solicitações da web com base nos endereços IP dos quais as solicitações se originam, crie uma ou mais condições de correspondência de IP. Uma condição de correspondência de IP lista até 10,000 endereços IP ou intervalos de endereços IP dos quais se originam suas solicitações. Mais adiante no processo, ao criar uma web ACL, você especifica se deseja permitir ou bloquear solicitações desses endereços IP.

Tópicos

Criação de uma condição de correspondência de IP

Se você deseja permitir algumas solicitações da web e bloquear outras com base nos endereços IP dos quais as solicitações se originam, crie uma condição de correspondência para os endereços IP que você deseja permitir e outra condição de correspondência de IP para os endereços IP que você deseja bloquear.

> **Note**
>
> Ao adicionar uma condição de correspondência de IP a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não se originam dos endereços IP especificados na condição.

Para criar uma condição de correspondência de IP

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione IP addresses.
3. Escolha Create condition.
4. Insira um nome no campo Name (Nome).

   O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.
5. Selecione a versão de IP correta e especifique um endereço IP ou um intervalo de endereços IP usando notação CIDR. Veja alguns exemplos:

   - Para especificar o endereço IPv4 192.0.2.44, digite 192.0.2.44/32.
   - Para especificar o endereço IPv6 0:0:0:0:0:ffff:c000:22c, digite 0:0:0:0:0:ffff:c000:22c/128.
   - Para especificar o intervalo de endereços IPv4 de 192.0.2.0 a 192.0.2.255, digite 192.0.2.0/24.

- Para especificar o intervalo de endereços IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, insira 2620:0:2d0:200::/64.

AWS WAF O Classic suporta intervalos de endereços IPv4: /8 e qualquer intervalo entre /16 a /32. AWS WAF O Classic suporta intervalos de endereços IPv6: /24, /32, /48, /56, /64 e /128. Para obter mais informações sobre a notação CIDR, consulte o artigo na Wikipédia sobre CIDR.

6. Selecione Add another IP address or range.
7. Se você deseja adicionar outro endereço IP ou intervalo, repita as etapas 5 e 6.
8. Ao terminar de adicionar os valores, escolha Create IP match condition.

Editar condições de correspondência de IP

Você pode adicionar um intervalo de endereços IP a uma condição de correspondência de IP ou excluir um intervalo. Para alterar um intervalo, adicione um novo e exclua o antigo.

Para editar uma condição de correspondência de IP

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione IP addresses.
3. No painel IP match conditions, selecione a condição de correspondência de IP que você deseja editar.
4. Para adicionar um intervalo de endereços IP:

   a. No painel direito, selecione Add IP address or range.
   b. Selecione a versão correta do IP e digite um intervalo de endereços IP usando a notação CIDR. Veja alguns exemplos:

      - Para especificar o endereço IPv4 192.0.2.44, insira 192.0.2.44/32.
      - Para especificar o endereço IPv6 0:0:0:0:0:ffff:c000:22c, insira 0:0:0:0:0:ffff:c000:22c/128.
      - Para especificar o intervalo de endereços IPv4 de 192.0.2.0 a 192.0.2.255, insira 192.0.2.0/24.
      - Para especificar o intervalo de endereços IPv6 de 2620:0:2d0:200:0:0:0:0 a 2620:0:2d0:200:ffff:ffff:ffff:ffff, insira 2620:0:2d0:200::/64.

AWS WAF O Classic suporta intervalos de endereços IPv4: /8 e qualquer intervalo entre /16 a /32. AWS WAF O Classic suporta intervalos de endereços IPv6: /24, /32, /48, /56, /64 e /128. Para obter mais informações sobre a notação CIDR, consulte o artigo na Wikipédia sobre CIDR.

c. Para adicionar mais endereços IP, escolha Add another IP address (Adicionar outro endereço IP) e digite o valor.

d. Escolha Add.

5. Para excluir um endereço ou faixa de endereços IP:

a. No painel direito, selecione os valores que você deseja excluir.

b. Selecione Delete IP address or range.

Excluir condições de correspondência de IP

Se você deseja excluir uma condição de correspondência de IP, é preciso primeiro excluir todos endereços e intervalos de endereços IP na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de correspondência de IP

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.

2. No painel de navegação, selecione IP addresses.
3. No painel IP match conditions, selecione a condição de correspondência de IP que você deseja excluir.
4. No painel direito, selecione a guia Rules.

   Se a lista de regras que usa essa condição de correspondência de IP estiver vazia, vá para a etapa 6. Se a lista contiver regras, anote-as e continue para a etapa 5.

5. Para remover a condição de correspondência de IP das regras que a estão usando, execute as seguintes etapas:

a. No painel de navegação, escolha Rules.

b. Escolha o nome de uma regra que esteja usando a condição de correspondência de IP que você deseja excluir.
c. No painel direito, selecione a condição de correspondência de IP que você deseja remover da regra e escolha Remove selected condition.
d. Repita as etapas b e c para todas as demais regras que estão usando a condição de correspondência de IP que você deseja excluir.
e. No painel de navegação, selecione IP match conditions.
f. No painel IP match conditions, selecione a condição de correspondência de IP que você deseja excluir.

6. Selecione Delete para excluir a condição selecionada.

Trabalhar com condições de correspondência geográfica

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você quiser permitir ou bloquear solicitações da web com base no país dos quais as solicitações se originam, crie uma ou mais condições de correspondência geográfica. A solicitação de correspondência geográfica lista países de origem das solicitações. Mais adiante no processo, ao criar uma web ACL, você especifica se deseja permitir ou bloquear solicitações desses países.

Você pode usar condições de correspondência geográfica com outras condições ou regras AWS WAF clássicas para criar uma filtragem sofisticada. Por exemplo, se quiser bloquear determinados países, mas ainda permitir endereços IP específicos do país, você poderá criar uma regra contendo uma condição de correspondência geográfica e uma condição de correspondência de IP. Configure a regra para bloquear solicitações originadas desse país e não correspondentes aos endereços IP aprovados. Assim como acontece em outro exemplo, se quiser priorizar recursos para usuários em um determinado país, você poderá incluir uma condição de correspondência geográfica em duas regras baseadas em taxas diferentes. Defina um limite de taxa mais alto para usuários no país preferido e um limite de taxa mais baixo para todos os outros usuários.

> **Note**
>
> Se você estiver usando CloudFront o recurso de restrição geográfica para impedir que um país acesse seu conteúdo, qualquer solicitação desse país será bloqueada e não será encaminhada para o Classic. AWS WAF Portanto, se você quiser permitir ou bloquear solicitações com base na geografia e em outras condições AWS WAF clássicas, não use CloudFront o recurso de restrição geográfica. Em vez disso, você deve usar uma condição de correspondência geográfica AWS WAF clássica.

Tópicos

Criar uma condição de correspondência geográfica

Se você quiser permitir algumas solicitações da web e bloquear outras com base nos países de origem das solicitações, crie uma condição de correspondência geográfica para os países que deseja permitir e outra condição de correspondência geográfica para os países que deseja bloquear.

> **Note**
>
> Ao adicionar uma condição de correspondência geográfica a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não sejam originárias do país especificado na condição.

Para criar uma condição de correspondência geográfica

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Geo match.
3. Escolha Create condition.

4. Insira um nome no campo Name (Nome).

   O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.
5. Escolha uma Region.
6. Escolha um Location type e um país. Atualmente, o Location type (Tipo de local) só pode ser Country (País).
7. Escolha Add location.
8. Escolha Criar.

Editar condições de correspondência geográfica

Você pode adicionar ou excluir países da condição de correspondência geográfica.

Para editar uma condição de correspondência geográfica

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Geo match.
3. No painel Geo match conditions, escolha a condição de correspondência geográfica que você deseja editar.
4. Para adicionar um país:
   a. No painel à direita, escolha Add filter.
   b. Escolha um Location type e um país. Atualmente, o Location type (Tipo de local) só pode ser Country (País).
   c. Escolha Add.
5. Para excluir um país:
   a. No painel direito, selecione os valores que você deseja excluir.
   b. Escolha Delete filter.

Excluir condições de correspondência geográfica

Se quiser excluir uma condição de correspondência geográfica, você deverá primeiro remover todos os países na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de correspondência geográfica

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Remova a condição de correspondência geográfica das regras que a estejam usando:
   a. No painel de navegação, escolha Rules.
   b. Escolha o nome de uma regra que esteja usando a condição de correspondência geográfica que você deseja excluir.
   c. No painel à direita, escolha Edit rule.
   d. Escolha o X ao lado da condição que você deseja excluir.
   e. Escolha Atualizar.
   f. Repita para todas as demais regras que estejam usando a condição de correspondência geográfica que você deseja excluir.
3. Remova os filtros da condição que você deseja excluir:
   a. No painel de navegação, escolha Geo match.
   b. Escolha o nome da condição de correspondência geográfica que você deseja excluir.
   c. No painel à direita, marque a caixa de seleção ao lado de Filter para selecionar todos os filtros.
   d. Escolha Delete filter.
4. No painel de navegação, escolha Geo match.
5. No painel Geo match conditions, escolha a condição de correspondência geográfica que você deseja excluir.
6. Selecione Delete para excluir a condição selecionada.

Trabalhar com condições de restrição de tamanho

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você deseja permitir ou bloquear as solicitações da web com base no comprimento de partes específicas das solicitações, crie uma ou mais condições de restrição de tamanho. Uma condição de restrição de tamanho identifica a parte das solicitações da web que você deseja que o AWS WAF Classic examine, o número de bytes que você deseja que o AWS WAF Classic procure e um operador, como maior que (>) ou menor que (<). Por exemplo, você pode usar uma condição de restrição de tamanho para procurar strings de consulta com mais de 100 bytes. Mais adiante no processo, ao criar uma web ACL, você especifica se deseja permitir ou bloquear solicitações com base nessas configurações.

Observe que, se você configurar o AWS WAF Classic para inspecionar o corpo da solicitação, por exemplo, pesquisando no corpo uma string especificada, o AWS WAF Classic inspecionará somente os primeiros 8192 bytes (8 KB). Se o corpo das suas solicitações da web nunca exceder 8192 bytes, você pode criar uma condição de restrição de tamanho e bloquear solicitações que tenham um corpo de solicitação maior que 8192 bytes.

Tópicos

Criar condições de restrição de tamanho

Ao criar condições de restrição de tamanho, você especifica filtros que identificam a parte das solicitações da Web para a qual você deseja que o AWS WAF Classic avalie o tamanho. Você pode

adicionar mais de um filtro a uma condição de restrição de tamanho ou criar uma condição separada para cada filtro. Veja como cada configuração afeta o comportamento do AWS WAF Classic:

- Um filtro por condição de restrição de tamanho — Quando você adiciona as condições de restrição de tamanho separadas a uma regra e adiciona a regra a uma ACL da web, as solicitações da web devem corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições.

  Por exemplo, vamos supor que você cria duas condições. Uma corresponde às solicitações da web para as quais as strings de consulta são maiores que 100 bytes. A outra corresponde a solicitações da web para as quais o corpo da solicitação é maior que 1024 bytes. Quando você adiciona as duas condições à mesma regra e adiciona a regra a uma ACL da web, o AWS WAF Classic permite ou bloqueia solicitações somente quando ambas as condições são verdadeiras.
- Mais de um filtro por condição de restrição de tamanho — Quando você adiciona uma condição de restrição de tamanho que contém vários filtros a uma regra e adiciona a regra a uma ACL da web, uma solicitação da web precisa corresponder apenas a um dos filtros na condição de restrição de tamanho para que o AWS WAF Classic permita ou bloqueie a solicitação com base nessa condição.

  Suponha que você crie uma condição em vez de duas, e a única condição contenha os mesmos dois filtros do exemplo anterior. AWS WAF O Classic permite ou bloqueia solicitações se a string de consulta for maior que 100 bytes ou o corpo da solicitação for maior que 1024 bytes.

> **Note**
>
> Ao adicionar uma condição de restrição de tamanho a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não correspondam aos valores da condição.

Para criar uma condição de restrição de tamanho

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Size constraints.

3. Escolha Create condition.
4. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de restrição de tamanho.
5. Escolha Add another filter.
6. Se você quiser adicionar outro filtro, repita as etapas 4 e 5.
7. Ao terminar de adicionar os filtros, escolha Create size constraint condition.

Valores especificados ao criar ou editar condições de restrição de tamanho

Ao criar ou atualizar uma condição de restrição de tamanho, você especifica os seguintes valores:

Nome

Digite um nome para a condição de restrição de tamanho.

O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.

Parte da solicitação a ser usada como filtro

Escolha a parte de cada solicitação da web para a qual você deseja que o AWS WAF Classic avalie a duração:

Cabeçalho

Um cabeçalho da solicitação especificada, como o cabeçalho `User-Agent` ou `Referer`. Se você selecionar Header, especifique o nome do cabeçalho no campo Header.

Método HTTP

O método HTTP, que indica o tipo de operação que a solicitação pede à origem para executar. CloudFront suporta os seguintes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`,, `PUT` e.

String de consulta

A parte de um URL exibida após um caractere `?`, se houver.

URI

O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

A menos que uma transformação seja especificada, um URI não é normalizado e é inspecionado da mesma forma que o AWS recebe do cliente como parte da solicitação. Uma Transformação reformata o URI conforme especificado.

Corpo

A parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário.

Parâmetro de consulta única (somente valor)

Qualquer parâmetro que você tenha definido como parte da string de consulta. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle”, você pode adicionar um filtro ao parâmetro ou. UserNameSalesRegion

Se você escolher Single query parameter (value only) [Parâmetro de consulta única (somente valor)], também especificará um Query parameter name (Nome de parâmetro de consulta). Esse é o parâmetro na sequência de caracteres de consulta que você inspecionará, como UserName. O tamanho máximo do Query parameter name (Nome de parâmetro de consulta) é 30 caracteres. O Query parameter name (Nome de parâmetro de consulta) não diferencia maiúsculas de minúsculas. Por exemplo, se você especificar UserNamecomo o nome do parâmetro Query, isso corresponderá a todas as variações de UserName, como username e userName.

Todos os parâmetros de consulta (somente valores)

Semelhante ao parâmetro de consulta única (somente valor), mas em vez de inspecionar o valor de um único parâmetro, o AWS WAF Classic inspeciona os valores de todos os parâmetros na sequência de caracteres de consulta quanto à restrição de tamanho. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle” e você escolher Todos os parâmetros de consulta (somente valores), o AWS WAF Classic acionará uma correspondência com o valor de se um ou exceder o tamanho especificado. UserNameSalesRegion

Cabeçalho (somente quando “Parte da solicitação a ser usada como filtro” for “Cabeçalho”)

Se você escolher Cabeçalho para filtrar parte da solicitação, escolha um cabeçalho na lista de cabeçalhos comuns ou digite o nome de um cabeçalho cujo tamanho você deseja que o AWS WAF Classic avalie.

Operador de comparação

Escolha como você deseja que o AWS WAF Classic avalie o tamanho da sequência de caracteres de consulta nas solicitações da Web em relação ao valor que você especifica para Tamanho.

Por exemplo, se você escolher É maior que para o operador Comparação e digitar 100 para Tamanho, o AWS WAF Classic avaliará as solicitações da web para uma sequência de caracteres de consulta com mais de 100 bytes.

Tamanho

Insira o tamanho, em bytes, que você deseja que o AWS WAF Classic observe nas cadeias de caracteres de consulta.

> **Note**
>
> Se você escolher URI para o valor de Parte da solicitação a ser usada como filtro, a / no URI contará como um caractere. Por exemplo, o caminho do URI `/logo.jpg` tem nove caracteres de comprimento.

Transformação

Uma transformação reformata uma solicitação da web antes que o AWS WAF Classic avalie o tamanho da parte especificada da solicitação. Isso elimina algumas das formatações incomuns que os invasores usam nas solicitações da web em um esforço para contornar o Classic. AWS WAF

> **Note**
>
> Se você escolher Corpo como Parte da solicitação a ser filtrada, não poderá configurar o AWS WAF Classic para realizar uma transformação porque somente os primeiros 8192 bytes são encaminhados para inspeção. No entanto, você ainda pode filtrar o tráfego com base no tamanho do corpo da solicitação HTTP e especificar uma transformação de Nenhum. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.)

Você só pode especificar um único tipo de transformação de texto.

As transformações podem executar as seguintes operações:

Nenhum

AWS WAF O Classic não realiza nenhuma transformação de texto na solicitação da web antes de verificar o tamanho.

Converter para minúsculas

AWS WAF O Classic converte letras maiúsculas (A-Z) em minúsculas (a-z).

Decodificação de HTML

AWS WAF O Classic substitui caracteres codificados em HTML por caracteres não codificados:

- Substitui `"` por &
- Substitui ` ` por espaço incondicional
- Substitui `<` por <
- Substitui `>` por >
- Substitui caracteres representados em formato hexadecimal, `&#xhhhh;`, pelos caracteres correspondentes
- Substitui caracteres representados em formato decimal, `&#nnnn;`, pelos caracteres correspondentes

Normalizar espaços em branco

AWS WAF O clássico substitui os seguintes caracteres por um caractere de espaço (decimal 32):

- \f, quebra de página, decimal 12
- \t, tabulação, decimal 9
- \n, quebra de linha, decimal 10
- \r, retorno de carro, decimal 13
- \v, tabulação vertical, decimal 11
- espaço incondicional, decimal 160

Além disso, essa opção substitui vários espaços por um único.

Simplificar a linha de comando

Para solicitações que contenham comandos de linha de comando do sistema operacional, use esta opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: \" '^
- Excluir espaços antes os seguintes caracteres: / (
- Substituir os seguintes caracteres por um espaço: , ;
- Substituir vários espaços por um espaço
- Converter maiúsculas (A-Z) em minúsculas (a-z)

Decodificar URL

Decodifica uma solicitação codificada por URL.

Adicionar excluir filtros em uma condição de restrição de tamanho

Você pode adicionar ou excluir filtros em uma condição de restrição de tamanho. Para alterar um filtro, adicione um novo e exclua o antigo.

Para adicionar ou excluir filtros em uma condição de restrição de tamanho

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Size constraint.
3. Escolha a condição na qual você deseja adicionar ou excluir filtros.
4. Para adicionar filtros, execute as etapas a seguir:

   a. Escolha Adicionar filtro.

   b. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de restrição de tamanho.

   c. Escolha Add.
5. Para excluir filtros, execute as etapas a seguir:

   a. Selecione o filtro que você deseja excluir.

   b. Escolha Delete filter.

Excluir condições de restrição de tamanho

Se você deseja excluir uma condição de restrição de tamanho, é preciso primeiro excluir todos os filtros na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de restrição de tamanho

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Size constraints.
3. No painel Size constraint conditions, selecione a condição de restrição de tamanho que você deseja excluir.
4. No painel direito, selecione a guia Associated rules.

   Se a lista de regras usando essa condição de restrição de tamanho estiver vazia, vá para a etapa 6. Se a lista contiver regras, anote-as e continue para a etapa 5.
5. Para remover a condição de restrição de tamanho das regras que a estão usando, execute as seguintes etapas:

   a. No painel de navegação, escolha Rules.

   b. Escolha o nome de uma regra que esteja usando a condição de restrição de tamanho que você deseja excluir.

   c. No painel direito, selecione a condição de restrição de tamanho que você deseja remover da regra e escolha Remove selected condition.

   d. Repita as etapas b e c para todas as demais regras que estão usando a condição de restrição de tamanho que você deseja excluir.

   e. No painel de navegação, selecione Size constraint.

   f. No painel Size constraint conditions, selecione a condição de restrição de tamanho que você deseja excluir.
6. Selecione Delete para excluir a condição selecionada.

Trabalhar com condições de correspondência de injeção de SQL

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Invasores às vezes inserem código SQL mal-intencionado em solicitações da web ma tentativa de extrair dados do seu banco de dados. Para permitir ou bloquear solicitações da web que aparentem conter código SQL mal-intencionado, crie uma ou mais condições de correspondência de injeção de SQL. Uma condição de correspondência de injeção de SQL identifica a parte das solicitações da web, como o caminho do URI ou a string de consulta, que você deseja que o AWS WAF Classic inspecione. Mais adiante no processo, ao criar uma web ACL, você especificará se deseja permitir ou bloquear solicitações que aparentem conter código SQL mal-intencionado.

Tópicos

- Criar condições de correspondência de injeção de SQL
- Valores especificados ao criar ou editar condições de correspondência de injeção de SQL
- Adicionar e excluir filtros em uma condição de correspondência de injeção de SQL
- Excluir condições de correspondência de injeção de SQL

Criar condições de correspondência de injeção de SQL

Ao criar condições de correspondência de injeção de SQL, você especifica filtros, que indicam a parte das solicitações da Web que você deseja que o AWS WAF Classic inspecione em busca de código SQL mal-intencionado, como o URI ou a string de consulta. Você pode adicionar mais de um filtro a uma condição de correspondência de injeção de SQL ou criar uma condição separada para cada filtro. Veja como cada configuração afeta o comportamento do AWS WAF Classic:

- Mais de um filtro por condição de correspondência de injeção de SQL (recomendado) — Quando você adiciona uma condição de correspondência de injeção de SQL contendo vários filtros a uma regra e adiciona a regra a uma ACL da web, uma solicitação da web precisa corresponder apenas

a um dos filtros na condição de correspondência de injeção de SQL para que o AWS WAF Classic permita ou bloqueie a solicitação com base nessa condição.

Por exemplo, vamos supor que você crie uma condição de correspondência de injeção de SQL e a condição contém dois filtros. Um filtro instrui o AWS WAF Classic a inspecionar o URI em busca de código SQL malicioso e o outro instrui o AWS WAF Classic a inspecionar a string de consulta. AWS WAF O Classic permite ou bloqueia solicitações se elas parecerem conter código SQL malicioso no URI ou na string de consulta.

- Um filtro por condição de correspondência de injeção de SQL — Quando você adiciona as condições de correspondência de injeção de SQL separadas a uma regra e adiciona a regra a uma ACL da web, as solicitações da web devem corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições.

  Vamos supor que você crie duas condições e que cada condição contenha um dos dois filtros do exemplo anterior. Quando você adiciona as duas condições à mesma regra e adiciona a regra a uma ACL da web, o AWS WAF Classic permite ou bloqueia solicitações somente quando o URI e a string de consulta parecem conter código SQL malicioso.

> **Note**
>
> Ao adicionar uma condição de correspondência de injeção de SQL a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não pareçam conter código SQL malicioso.

Para criar uma condição de correspondência de injeção de SQL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione SQL injection.
3. Escolha Create condition.
4. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de injeção de SQL.
5. Escolha Add another filter.

6. Se você quiser adicionar outro filtro, repita as etapas 4 e 5.
7. Ao terminar de adicionar os filtros, escolha Criar.

Valores especificados ao criar ou editar condições de correspondência de injeção de SQL

Ao criar ou atualizar uma condição de correspondência de injeção de SQL, você especifica os seguintes valores:

Nome

O nome da condição de correspondência de injeção de SQL.

O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.

Parte da solicitação a ser usada como filtro

Escolha a parte de cada solicitação da web que você deseja que o AWS WAF Classic inspecione em busca de código SQL malicioso:

Cabeçalho

Um cabeçalho da solicitação especificada, como o cabeçalho `User-Agent` ou `Referer`. Se você selecionar Header, especifique o nome do cabeçalho no campo Header.

Método HTTP

O método HTTP, que indica o tipo de operação que a solicitação pede à origem para executar. CloudFront suporta os seguintes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`,, `PUT` e.

String de consulta

A parte de um URL exibida após um caractere ?, se houver.

> **Note**
>
> Para condições de correspondência de injeção de SQL, recomendamos que você selecione Todos os parâmetros de consulta (somente valores) em vez de String de consulta para Parte da solicitação a ser usada como filtro.

URI

O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

A menos que uma transformação seja especificada, um URI não é normalizado e é inspecionado da mesma forma que o AWS recebe do cliente como parte da solicitação. Uma Transformação reformata o URI conforme especificado.

Corpo

A parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário.

> **Note**
>
> Se você selecionar Corpo para o valor de Parte da solicitação a ser usada como filtro, o AWS WAF Classic inspecionará somente os primeiros 8.192 bytes (8 KB). Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Parâmetro de consulta única (somente valor)

Qualquer parâmetro que você tenha definido como parte da string de consulta. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle”, você pode adicionar um filtro ao parâmetro ou. UserNameSalesRegion

Se você escolher Single query parameter (value only) [Parâmetro de consulta única (somente valor)], também especificará um Query parameter name (Nome de parâmetro de consulta). Esse é o parâmetro na sequência de caracteres de consulta que você inspecionará, como UserNameou SalesRegion. O tamanho máximo do Query parameter name (Nome de parâmetro de consulta) é 30 caracteres. O Query parameter name (Nome de parâmetro de consulta) não diferencia maiúsculas de minúsculas. Por exemplo, se você especificar UserNamecomo o nome do parâmetro Query, isso corresponderá a todas as variações de UserName, como username e userName.

Todos os parâmetros de consulta (somente valores)

Semelhante ao parâmetro de consulta única (somente valor), mas em vez de inspecionar o valor de um único parâmetro, o AWS WAF Classic inspeciona o valor de todos os parâmetros na string de consulta em busca de possíveis códigos SQL maliciosos. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle” e você escolher Todos os parâmetros de consulta (somente valores), o AWS WAF Classic acionará uma correspondência se o valor de um ou contiver um possível código SQL malicioso. UserNameSalesRegion

Cabeçalho

Se você escolher Cabeçalho para filtrar parte da solicitação, escolha um cabeçalho na lista de cabeçalhos comuns ou insira o nome de um cabeçalho que você deseja que o AWS WAF Classic inspecione em busca de código SQL mal-intencionado.

Transformação

Uma transformação reformata uma solicitação da web antes que o AWS WAF Classic inspecione a solicitação. Isso elimina algumas das formatações incomuns que os invasores usam nas solicitações da web em um esforço para contornar o Classic. AWS WAF

Você só pode especificar um único tipo de transformação de texto.

As transformações podem executar as seguintes operações:

Nenhum

AWS WAF O Classic não realiza nenhuma transformação de texto na solicitação da web antes de inspecioná-la para verificar se a string em Value corresponde.

Converter para minúsculas

AWS WAF O Classic converte letras maiúsculas (A-Z) em minúsculas (a-z).

Decodificação de HTML

AWS WAF O Classic substitui caracteres codificados em HTML por caracteres não codificados:

- Substitui `"` por &
- Substitui ` ` por espaço incondicional
- Substitui `<` por <

- Substitui `>` por >
- Substitui caracteres representados em formato hexadecimal, `&#xhhhh;`, pelos caracteres correspondentes
- Substitui caracteres representados em formato decimal, `&#nnnn;`, pelos caracteres correspondentes

Normalizar espaços em branco

AWS WAF O clássico substitui os seguintes caracteres por um caractere de espaço (decimal 32):

- \f, quebra de página, decimal 12
- \t, tabulação, decimal 9
- \n, quebra de linha, decimal 10
- \r, retorno de carro, decimal 13
- \v, tabulação vertical, decimal 11
- espaço incondicional, decimal 160

Além disso, essa opção substitui vários espaços por um único.

Simplificar a linha de comando

Para solicitações que contenham comandos de linha de comando do sistema operacional, use esta opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: \" '^
- Excluir espaços antes os seguintes caracteres: / (
- Substituir os seguintes caracteres por um espaço: , ;
- Substituir vários espaços por um espaço
- Converter maiúsculas (A-Z) em minúsculas (a-z)

Decodificar URL

Decodifica uma solicitação codificada por URL.

Adicionar e excluir filtros em uma condição de correspondência de injeção de SQL

Você pode adicionar ou excluir filtros em uma condição de correspondência de injeção de SQL. Para alterar um filtro, adicione um novo e exclua o antigo.

Para adicionar ou excluir filtros de uma condição de correspondência de injeção de SQL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione SQL injection.
3. Escolha a condição na qual você deseja adicionar ou excluir filtros.
4. Para adicionar filtros, execute as etapas a seguir:

   a. Escolha Adicionar filtro.

   b. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de injeção de SQL.

   c. Escolha Add.
5. Para excluir filtros, execute as etapas a seguir:

   a. Selecione o filtro que você deseja excluir.

   b. Escolha Delete filter.

Excluir condições de correspondência de injeção de SQL

Se você deseja excluir uma condição de correspondência de injeção de SQL, é preciso primeiro excluir todos os filtros na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de correspondência de injeção de SQL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione SQL injection.
3. No painel SQL injection match conditions, selecione a condição de correspondência de SQL injection que você deseja excluir.
4. No painel direito, selecione a guia Associated rules.

Se a lista de regras usando essa condição de correspondência de injeção de SQL estiver vazia, vá para a etapa 6. Se a lista contiver regras, anote-as e continue para a etapa 5.

5. Para remover a condição de correspondência de injeção de SQL das regras que a estão usando, execute as seguintes etapas:

   a. No painel de navegação, escolha Rules.

   b. Escolha o nome de uma regra que esteja usando a condição de correspondência de injeção de SQL que você deseja excluir.

   c. No painel direito, selecione a condição de correspondência de SQL injection que você deseja remover da regra e escolha Remove selected condition.

   d. Repita as etapas b e c para todas as demais regras que estão usando a condição de correspondência de injeção de SQL que você deseja excluir.

   e. No painel de navegação, selecione SQL injection.

   f. No painel SQL injection match conditions, selecione a condição de correspondência de SQL injection que você deseja excluir.

6. Selecione Delete para excluir a condição selecionada.

Trabalhar com condições de correspondência de string

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você deseja permitir ou bloquear solicitações da web com base nas strings que aparecem nas solicitações, crie uma ou mais condições de correspondência de string. Uma condição de correspondência de string identifica a string que você deseja pesquisar e a parte das solicitações da web, como um cabeçalho especificado ou a string de consulta, que você deseja que o AWS WAF Classic inspecione em busca da string. Mais adiante no processo, ao criar uma web ACL, você especifica se deseja permitir ou bloquear solicitações que contêm a string.

Tópicos

Criar uma condição de correspondência de string

Ao criar condições de correspondência de string, você especifica filtros que identificam a string que você deseja pesquisar e a parte das solicitações da web que você deseja que o AWS WAF Classic inspecione para essa string, como o URI ou a string de consulta. Você pode adicionar mais de um filtro a uma condição de correspondência de string, ou então criar uma condição de correspondência de string separada para cada filtro. Veja como cada configuração afeta o comportamento do AWS WAF Classic:

- Um filtro por condição de correspondência de string — Quando você adiciona as condições de correspondência de string separadas a uma regra e adiciona a regra a uma ACL da web, as solicitações da web devem corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições.

  Por exemplo, vamos supor que você cria duas condições. Uma corresponde às solicitações da web que contêm o valor `BadBot` no cabeçalho `User-Agent`. A outra corresponde a solicitações da web que contêm o valor `BadParameter` nas strings de consulta. Quando você adiciona as duas condições à mesma regra e adiciona a regra a uma ACL da web, o AWS WAF Classic permite ou bloqueia solicitações somente quando elas contêm os dois valores.
- Mais de um filtro por condição de correspondência de string — Quando você adiciona uma condição de correspondência de string que contém vários filtros a uma regra e adiciona a regra a uma ACL da web, uma solicitação da web precisa corresponder apenas a um dos filtros na condição de correspondência de string para que o AWS WAF Classic permita ou bloqueie a solicitação com base em uma condição.

  Suponha que você crie uma condição em vez de duas, e a única condição contenha os mesmos dois filtros do exemplo anterior. AWS WAF O Classic permite ou bloqueia solicitações se elas contiverem *`BadBot`* no *`User-Agent`* cabeçalho ou *`BadParameter`* na string de consulta.

> **Note**
>
> Ao adicionar uma condição de correspondência de string a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não correspondam aos valores da condição.

Para criar uma condição de correspondência de string

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha Create condition.
4. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de string.
5. Escolha Adicionar filtro.
6. Se você quiser adicionar outro filtro, repita as etapas 4 e 5.
7. Ao terminar de adicionar os filtros, escolha Criar.

Valores especificados ao criar ou editar condições de correspondência de string

Ao criar ou atualizar uma condição de correspondência de string, você especifica os seguintes valores:

Nome

Digite um nome para a condição de correspondência de string. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.

Tipo

Escolha String match.

Parte da solicitação a ser usada como filtro

Escolha a parte de cada solicitação da web que você deseja que o AWS WAF Classic inspecione em busca da string especificada em Valor para corresponder:

Cabeçalho

Um cabeçalho da solicitação especificada, como o cabeçalho `User-Agent` ou `Referer`. Se você selecionar Header, especifique o nome do cabeçalho no campo Header.

Método HTTP

O método HTTP, que indica o tipo de operação que a solicitação pede à origem para executar. CloudFront suporta os seguintes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`,, `PUT` e.

String de consulta

A parte de um URL exibida após um caractere `?`, se houver.

URI

O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

A menos que uma transformação seja especificada, um URI não é normalizado e é inspecionado da mesma forma que o AWS recebe do cliente como parte da solicitação. Uma Transformação reformata o URI conforme especificado.

Corpo

A parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário.

> **Note**
>
> Se você selecionar Corpo para o valor de Parte da solicitação a ser usada como filtro, o AWS WAF Classic inspecionará somente os primeiros 8.192 bytes (8 KB). Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Parâmetro de consulta única (somente valor)

Qualquer parâmetro que você tenha definido como parte da string de consulta. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle”, você pode adicionar um filtro ao parâmetro ou. UserNameSalesRegion

Se os parâmetros duplicados aparecem na string de consulta, os valores serão avaliadas como um “OR”. Ou seja, nenhum dos valores acionará uma correspondência. Por exemplo, na URL “www.xyz.com? SalesRegion =boston& SalesRegion =seattle”, “boston” ou “seattle” em Value to match acionarão uma correspondência.

Se você escolher Single query parameter (value only) [Parâmetro de consulta única (somente valor)], também especificará um Query parameter name (Nome de parâmetro de consulta). Esse é o parâmetro na sequência de caracteres de consulta que você inspecionará, como UserNameou SalesRegion. O tamanho máximo do Query parameter name (Nome de parâmetro de consulta) é 30 caracteres. O Query parameter name (Nome de parâmetro de consulta) não diferencia maiúsculas de minúsculas. Por exemplo, se você especificar UserNamecomo o nome do parâmetro Query, isso corresponderá a todas as variações de UserName, como username e userName.

Todos os parâmetros de consulta (somente valores)

Semelhante ao parâmetro de consulta única (somente valor), mas em vez de inspecionar o valor de um único parâmetro, o AWS WAF Classic inspeciona o valor de todos os parâmetros na string de consulta para verificar se o valor corresponde. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle” e você escolher Todos os parâmetros de consulta (somente valores), o AWS WAF Classic acionará uma correspondência se o valor de um UserNameou SalesRegionfor especificado como o Valor a ser correspondido.

Cabeçalho (somente quando “Parte da solicitação a ser usada como filtro” for “Cabeçalho”)

Se você escolher Cabeçalho na parte da solicitação para filtrar na lista, escolha um cabeçalho na lista de cabeçalhos comuns ou insira o nome de um cabeçalho que você deseja que o AWS WAF Classic inspecione.

Tipo de correspondência

Na parte da solicitação que você deseja que o AWS WAF Classic inspecione, escolha onde a string em Value to match deve aparecer para corresponder a esse filtro:

Contém

A string aparece em qualquer lugar da parte especificada da solicitação.

Contém palavra

A parte especificada da solicitação da web deve incluir Value to match, e Value to match deve conter apenas caracteres alfanuméricos ou sublinhado (A-Z, a-z, 0-9 ou _). Além disso, Value to match deve ser uma palavra que tem um dos seguintes significados:

- Value to match corresponde exatamente ao valor da parte especificada da solicitação da web, como o valor de um cabeçalho.
- Value to match está no início da parte especificada da solicitação da web e é seguido por um caractere diferente de um caractere alfanumérico ou sublinhado (_), por exemplo, `BadBot;`.
- Value to match está no fim da parte especificada da solicitação da web e é precedido por um caractere diferente de um caractere alfanumérico ou sublinhado (_), por exemplo, `;BadBot`.
- Value to match está no meio da parte especificada da solicitação da web e é precedido e seguido por caracteres diferentes de caracteres alfanuméricos ou sublinhados (_), por exemplo, `-BadBot;`.

Correspondência exata com

A string e o valor da parte especificada da solicitação são idênticos.

Inicia com

A string aparece no início da parte especificada da solicitação.

Termina com

A string aparece no fim da parte especificada da solicitação.

Transformação

Uma transformação reformata uma solicitação da web antes que o AWS WAF Classic inspecione a solicitação. Isso elimina algumas das formatações incomuns que os invasores usam nas solicitações da web em um esforço para contornar o Classic. AWS WAF

Você só pode especificar um único tipo de transformação de texto.

As transformações podem executar as seguintes operações:

Nenhum

AWS WAF O Classic não realiza nenhuma transformação de texto na solicitação da web antes de inspecioná-la para verificar se a string em Value corresponde.

Converter para minúsculas

AWS WAF O Classic converte letras maiúsculas (A-Z) em minúsculas (a-z).

Decodificação de HTML

AWS WAF O Classic substitui caracteres codificados em HTML por caracteres não codificados:

- Substitui `"` por &
- Substitui ` ` por espaço incondicional
- Substitui `<` por <
- Substitui `>` por >
- Substitui caracteres representados em formato hexadecimal, `&#xhhhh;`, pelos caracteres correspondentes
- Substitui caracteres representados em formato decimal, `&#nnnn;`, pelos caracteres correspondentes

Normalizar espaços em branco

AWS WAF O clássico substitui os seguintes caracteres por um caractere de espaço (decimal 32):

- \f, quebra de página, decimal 12
- \t, tabulação, decimal 9
- \n, quebra de linha, decimal 10
- \r, retorno de carro, decimal 13
- \v, tabulação vertical, decimal 11
- espaço incondicional, decimal 160

Além disso, essa opção substitui vários espaços por um único.

Simplificar a linha de comando

Quando você estiver preocupado que os invasores estão injetando um comando de linha de comando no sistema operacional e usando formatações incomuns para mascarar alguns ou todos os comandos, use esta opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: \" '^
- Excluir espaços antes os seguintes caracteres: / (
- Substituir os seguintes caracteres por um espaço: , ;
- Substituir vários espaços por um espaço
- Converter maiúsculas (A-Z) em minúsculas (a-z)

Decodificar URL

Decodifica uma solicitação codificada por URL.

O valor é codificado por Base64

Se o valor em Value to match for codificado por Base64, marque esta caixa de seleção. Use a codificação Base64 para especificar caracteres não imprimíveis, como guias e linefeeds, que os invasores incluem em suas solicitações.

Valor para corresponder

Especifique o valor que você deseja que o AWS WAF Classic pesquise nas solicitações da web. O comprimento máximo é de 50 bytes. Se você for codificar o valor por base64, o comprimento máximo de 50 bytes será aplicado ao valor antes de ser codificado.

Adicionar e excluir filtros em uma condição de correspondência de string

Você pode adicionar filtros a uma condição de correspondência de string ou excluir filtros. Para alterar um filtro, adicione um novo e exclua o antigo.

Para adicionar ou excluir filtros em uma condição de correspondência de string

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha a condição na qual você deseja adicionar ou excluir filtros.
4. Para adicionar filtros, execute as etapas a seguir:

   a. Escolha Adicionar filtro.

   b. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar condições de correspondência de string.

c. Escolha Add.

5. Para excluir filtros, execute as etapas a seguir:

   a. Selecione o filtro que você deseja excluir.

   b. Escolha Delete Filter.

Excluir condições de correspondência de string

Se você deseja excluir uma condição de correspondência de string, é preciso primeiro excluir todos os filtros na condição e remover a condição de todas as regras que a estiverem usando, conforme descrito no procedimento a seguir.

Para excluir uma condição de correspondência de string

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.

2. Remova a condição de correspondência da string das regras que a estejam usando:

   a. No painel de navegação, escolha Rules.

   b. Escolha o nome de uma regra que esteja usando a condição de correspondência de string que você deseja excluir.

   c. No painel à direita, escolha Edit rule.

   d. Escolha o X ao lado da condição que você deseja excluir.

   e. Escolha Atualizar.

   f. Repita para todas as demais regras que estejam usando a condição de correspondência de string que você deseja excluir.

3. Remova os filtros da condição que você deseja excluir:

   a. No painel de navegação, escolha String and regex matching.

   b. Escolha o nome da condição de correspondência da string que você deseja excluir.

   c. No painel à direita, marque a caixa de seleção ao lado de Filter para selecionar todos os filtros.

   d. Escolha Delete filter.

4. No painel de navegação, escolha String and regex matching.

5. No painel String and regex match conditions, selecione a condição de correspondência da string que você deseja excluir.
6. Selecione Delete para excluir a condição selecionada.

Trabalhar com condições de correspondência regex

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você quiser permitir ou bloquear solicitações da web com base em strings que correspondam a um padrão de expressão regular (regex) exibido nas solicitações, crie uma ou mais condições de correspondência regex. Uma condição de correspondência de regex é um tipo de condição de correspondência de string que identifica o padrão que você deseja pesquisar e a parte das solicitações da web, como um cabeçalho especificado ou a string de consulta, que você deseja que o AWS WAF Classic inspecione para ver o padrão. Posteriormente no processo, ao criar uma ACL da web, você especifica se deseja permitir ou bloquear solicitações que contenham o padrão.

Tópicos

- Criar uma condição de correspondência regex
- Valores que você especifica ao criar ou editar condições de RegEx correspondência
- Editar uma condição de correspondência regex

Criar uma condição de correspondência regex

Ao criar condições de correspondência regex, você especifica conjuntos de padrões que identificam a string (usando uma expressão regular) que deseja procurar. Em seguida, você adiciona esses conjuntos de padrões aos filtros que especificam a parte das solicitações da Web que você deseja que o AWS WAF Classic inspecione para esse conjunto de padrões, como o URI ou a string de consulta.

Você pode adicionar várias expressões regulares a um único conjunto de padrões. Se você fizer isso, essas expressões serão combinadas com um OR. Ou seja, uma solicitação da web corresponderá ao conjunto de padrões se a parte apropriada da solicitação corresponder a qualquer uma das expressões listadas.

Ao adicionar uma condição de correspondência de regex a uma regra, você também pode configurar o AWS WAF Classic para permitir ou bloquear solicitações da web que não correspondam aos valores da condição.

AWS WAF O Classic suporta a maioria das expressões regulares compatíveis com Perl (PCRE) padrão. No entanto, não há suporte para o seguinte:

- Referências reversas e subexpressões de captura
- Asserções de largura zero arbitrárias
- Referências de sub-rotina e padrões recursivos
- Padrões condicionais
- Verbos de controle de referência reversa
- A diretiva de byte único \C
- A diretiva de correspondência de nova linha \R
- O início \K da diretiva de redefinição da correspondência
- Callouts e códigos integrados
- Agrupamento atômico e quantificadores possessivos

Para criar uma condição de correspondência regex

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha Create condition.
4. Especifique as configurações de filtro aplicáveis. Para ter mais informações, consulte Valores que você especifica ao criar ou editar condições de RegEx correspondência.
5. Escolha Create pattern set and add filter se você tiver criado um novo conjunto de padrões, ou Add filter se você tiver usado um conjunto de padrões existente.

6. Escolha Criar.

Valores que você especifica ao criar ou editar condições de RegEx correspondência

Ao criar ou atualizar uma condição de correspondência regex, você especifica os seguintes valores:

Nome

Digite um nome para a condição de correspondência regex. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Você não poderá alterar o nome de uma condição depois de criá-la.

Tipo

Escolha Regex match.

Parte da solicitação a ser usada como filtro

Escolha a parte de cada solicitação da web que você deseja que o AWS WAF Classic inspecione em busca do padrão especificado em Value to match:

Cabeçalho

Um cabeçalho da solicitação especificada, como o cabeçalho `User-Agent` ou `Referer`. Se você selecionar Header, especifique o nome do cabeçalho no campo Header.

Método HTTP

O método HTTP, que indica o tipo de operação que a solicitação pede à origem para executar. CloudFront suporta os seguintes métodos: `DELETEGET`,`HEAD`, `OPTIONSPATCH`,`POST`,, `PUT` e.

String de consulta

A parte de um URL exibida após um caractere `?`, se houver.

URI

O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

A menos que uma transformação seja especificada, um URI não é normalizado e é inspecionado da mesma forma que o AWS recebe do cliente como parte da solicitação. Uma Transformação reformata o URI conforme especificado.

Corpo

A parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário.

> **Note**
>
> Se você selecionar Corpo para o valor de Parte da solicitação a ser usada como filtro, o AWS WAF Classic inspecionará somente os primeiros 8.192 bytes (8 KB). Para permitir ou bloquear solicitações para as quais o corpo seja maior que 8.192 bytes, você pode criar uma condição de restrição de tamanho. (AWS WAF Classic obtém o comprimento do corpo dos cabeçalhos da solicitação.) Para ter mais informações, consulte Trabalhar com condições de restrição de tamanho.

Parâmetro de consulta única (somente valor)

Qualquer parâmetro que você tenha definido como parte da string de consulta. Por exemplo, se o URL for “www.xyz.com? UserName =abc& SalesRegion =seattle”, você pode adicionar um filtro ao parâmetro ou. UserNameSalesRegion

Se os parâmetros duplicados aparecem na string de consulta, os valores serão avaliadas como um “OR”. Ou seja, nenhum dos valores acionará uma correspondência. Por exemplo, na URL “www.xyz.com? SalesRegion =boston& SalesRegion =seattle”, um padrão que corresponda a “boston” ou “seattle” em Value to match acionará uma correspondência.

Se você escolher Single query parameter (value only) [Parâmetro de consulta única (somente valor)], também especificará um Query parameter name (Nome de parâmetro de consulta). Esse é o parâmetro na sequência de caracteres de consulta que você inspecionará, como UserNameou SalesRegion. O tamanho máximo do Query parameter name (Nome de parâmetro de consulta) é 30 caracteres. O Query parameter name (Nome de parâmetro de consulta) não diferencia maiúsculas de minúsculas. Por exemplo, se você especificar UserNamecomo o nome do parâmetro Query, isso corresponderá a todas as variações de UserName, como username e userName.

Todos os parâmetros de consulta (somente valores)

Semelhante ao parâmetro de consulta única (somente valor), mas em vez de inspecionar o valor de um único parâmetro, o AWS WAF Classic inspeciona o valor de todos os parâmetros na string de consulta em busca do padrão especificado no Valor a ser correspondente. Por

exemplo, na URL “www.xyz.com? UserName =abc& SalesRegion =seattle”, um padrão em Value to match que corresponde ao valor em ou acionará uma correspondência. UserNameSalesRegion

Cabeçalho (somente quando “Parte da solicitação a ser usada como filtro” for “Cabeçalho”)

Se você escolher Cabeçalho na parte da solicitação para filtrar na lista, escolha um cabeçalho na lista de cabeçalhos comuns ou insira o nome de um cabeçalho que você deseja que o AWS WAF Classic inspecione.

Transformação

Uma transformação reformata uma solicitação da web antes que o AWS WAF Classic inspecione a solicitação. Isso elimina algumas das formatações incomuns que os invasores usam nas solicitações da web em um esforço para contornar o Classic. AWS WAF

Você só pode especificar um único tipo de transformação de texto.

As transformações podem executar as seguintes operações:

Nenhum

AWS WAF O Classic não realiza nenhuma transformação de texto na solicitação da web antes de inspecioná-la para verificar se a string em Value corresponde.

Converter para minúsculas

AWS WAF O Classic converte letras maiúsculas (A-Z) em minúsculas (a-z).

Decodificação de HTML

AWS WAF O Classic substitui caracteres codificados em HTML por caracteres não codificados:

- Substitui `"` por &
- Substitui ` ` por espaço incondicional
- Substitui `<` por <
- Substitui `>` por >
- Substitui caracteres representados em formato hexadecimal, `&#xhhhh;`, pelos caracteres correspondentes
- Substitui caracteres representados em formato decimal, `&#nnnn;`, pelos caracteres correspondentes

Normalizar espaços em branco

AWS WAF O clássico substitui os seguintes caracteres por um caractere de espaço (decimal 32):

- \f, quebra de página, decimal 12
- \t, tabulação, decimal 9
- \n, quebra de linha, decimal 10
- \r, retorno de carro, decimal 13
- \v, tabulação vertical, decimal 11
- espaço incondicional, decimal 160

Além disso, essa opção substitui vários espaços por um único.

Simplificar a linha de comando

Quando você estiver preocupado que os invasores estão injetando um comando de linha de comando no sistema operacional e usando formatações incomuns para mascarar alguns ou todos os comandos, use esta opção para executar as seguintes transformações:

- Excluir os seguintes caracteres: \" '^
- Excluir espaços antes os seguintes caracteres: / (
- Substituir os seguintes caracteres por um espaço: , ;
- Substituir vários espaços por um espaço
- Converter maiúsculas (A-Z) em minúsculas (a-z)

Decodificar URL

Decodifica uma solicitação codificada por URL.

Padrão Regex de acordo com a solicitação

Você pode escolher um conjunto de padrões existente ou criar um novo. Se você criar um novo, especifique o seguinte:

Nome do novo conjunto padrão

Insira um nome e, em seguida, especifique o padrão regex que você deseja que o AWS WAF Classic pesquise.

Se você adicionar várias expressões regulares a um conjunto de padrões, essas expressões serão combinadas com um OR. Ou seja, uma solicitação da web corresponderá ao conjunto

de padrões se a parte apropriada da solicitação corresponder a qualquer uma das expressões listadas.

O tamanho máximo de Value to match é 70 caracteres.

Editar uma condição de correspondência regex

Você pode fazer as seguintes alterações em uma condição de correspondência regex existente:

- Excluir um padrão de um conjunto de padrões existente
- Adicionar um padrão a um conjunto de padrões existente
- Excluir um filtro de uma condição de correspondência regex existente
- Adicione um filtro a uma condição de correspondência de expressão regular existente (você pode ter somente um filtro em uma condição de correspondência de expressão regular. Portanto, para adicionar um filtro, você deve excluir o filtro existente primeiro.)
- Excluir uma condição de correspondência regex existente

> **Note**
>
> Você não pode adicionar nem excluir um conjunto de padrões de um filtro existente. Você deve editar o conjunto de padrões ou excluir o filtro e criar um novo filtro com um novo conjunto de padrões.

Para excluir um padrão de um conjunto de padrões existente

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha View regex pattern sets.
4. Escolha o nome do conjunto de padrões que você deseja editar.
5. Selecione a opção Editar.
6. Escolha o X ao lado do padrão que você deseja excluir.
7. Selecione Salvar.

Para adicionar um padrão a um conjunto de padrões existente

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha View regex pattern sets.
4. Escolha o nome do conjunto de padrões a ser editado.
5. Selecione a opção Editar.
6. Digite um novo padrão regex.
7. Escolha o + ao lado do novo padrão.
8. Selecione Salvar.

Para excluir um filtro de uma condição de correspondência regex existente

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha String and regex matching.
3. Escolha o nome da condição com o filtro que você deseja excluir.
4. Escolha a caixa ao lado do filtro que você deseja excluir.
5. Escolha Delete filter.

Para excluir uma condição de correspondência regex

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Exclua o filtro da condição regex. Consulte Para excluir um filtro de uma condição de correspondência regex existente para obter instruções sobre como fazer isso.
3. Remova a condição de correspondência regex das regras que a estejam usando:

   a. No painel de navegação, escolha Rules.

b. Escolha o nome de uma regra que esteja usando a condição de correspondência regex que você deseja excluir.
c. No painel à direita, escolha Edit rule.
d. Escolha o X ao lado da condição que você deseja excluir.
e. Escolha Atualizar.
f. Repita para todas as demais regras que estejam usando a condição de correspondência regex que você deseja excluir.

4. No painel de navegação, escolha String and regex matching.
5. Selecione o botão ao lado da condição que você deseja excluir.
6. Escolha Delete.

Para adicionar ou alterar um filtro para uma condição de correspondência regex existente

Você pode ter somente um filtro em uma condição de correspondência regex. Se quiser adicionar ou alterar o filtro, você deve primeiro excluir o filtro existente.

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Exclua o filtro da condição regex que você deseja alterar. Consulte Para excluir um filtro de uma condição de correspondência regex existente para obter instruções sobre como fazer isso.
3. No painel de navegação, escolha String and regex matching.
4. Escolha o nome da condição que você deseja alterar.
5. Escolha Adicionar filtro.
6. Insira os valores apropriados para o novo filtro e escolha Add.

Trabalhar com regras

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.

Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

As regras permitem que você direcione com precisão as solicitações da web que você deseja que o AWS WAF Classic permita ou bloqueie, especificando as condições exatas que você deseja que o AWS WAF Classic observe. Por exemplo, o AWS WAF Classic pode observar os endereços IP dos quais as solicitações se originam, as cadeias de caracteres que as solicitações contêm e onde as cadeias de caracteres aparecem e se as solicitações parecem conter código SQL malicioso.

Tópicos

Criar uma regra e editar condições

Note

Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você adicionar mais de uma condição a uma regra, uma solicitação da web deverá corresponder a todas as condições para que o AWS WAF Classic permita ou bloqueie solicitações com base nessa regra.

Para criar uma regra e adicionar condições

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Regras.

3. Selecione Criar regra.
4. Insira os seguintes valores:

   Nome

   Insira um nome.

   CloudWatch nome da métrica

   Insira um nome para a CloudWatch métrica que o AWS WAF Classic criará e associará à regra. O nome pode conter somente caracteres alfanuméricos (A-Z, a-z, 0-9), com tamanho máximo de 128 e tamanho mínimo de um. Ele não pode conter espaços em branco ou nomes de métricas reservados para AWS WAF Classic, incluindo “All” e “Default_Action”.

   Tipo de regra

   Escolha `Regular rule` ou `Rate-based rule`. As regras baseadas em intervalos são idênticas às regras regulares, mas também levam em conta o número de solicitações que chegam do endereço IP identificado em qualquer período de cinco minutos. Para obter mais informações sobre esses tipos de regra, consulte Como funciona o AWS WAF Classic.

   Limite de taxa

   Para uma regra com base em taxa, insira o número máximo de solicitações a serem permitidas, em qualquer período de cinco minutos, de um endereço IP que corresponda às condições da regra. O limite de taxa deve ser de pelo menos 100.

   Você pode especificar apenas um limite de taxa, ou um limite de taxa e condições. Se você especificar somente um limite de taxa, AWS WAF colocará o limite em todos os endereços IP. Se você especificar um limite de taxa e condições, AWS WAF colocará o limite nos endereços IP que correspondam às condições.

   Quando um endereço IP atinge o limite de taxa, AWS WAF aplica a ação atribuída (bloquear ou contar) o mais rápido possível, geralmente em 30 segundos. Depois que a ação estiver em vigor, se passarem cinco minutos sem nenhuma solicitação do endereço IP, AWS WAF o contador será zerado.
5. Para adicionar uma condição à regra, especifique os seguintes valores:

Quando uma solicitação atende/não atende

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base nos filtros de uma condição, escolha sim. Por exemplo, se uma condição de correspondência de IP incluir o intervalo de endereços IP 192.0.2.0/24 e você quiser que o AWS WAF Classic permita ou bloqueie solicitações provenientes desses endereços IP, escolha does.

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base no inverso dos filtros em uma condição, escolha não. Por exemplo, se uma condição de correspondência de IP incluir o intervalo de endereços IP 192.0.2.0/24 e você quiser que o AWS WAF Classic permita ou bloqueie solicitações que não venham desses endereços IP, escolha não.

corresponder/originar de

Escolha o tipo de condição que você deseja adicionar à regra:

- Condições de correspondência de cross-site scripting: selecione corresponder a pelo menos um dos filtros na condição de correspondência de cross-site scripting
- Condições de correspondência de IP: selecione se originam de um endereço IP em
- Condições de correspondência geográfica: selecione se originam de uma localização geográfica em
- Condições de restrição de tamanho: selecione corresponder a pelo menos um dos filtros na condição de restrição de tamanho
- Condições de correspondência de injeção de SQL: selecione corresponder a pelo menos um dos filtros na condição de correspondência de injeção de SQL
- Condições de correspondência de string: selecione corresponder a pelo menos um dos filtros na condição de correspondência de string
- Condições de correspondência de expressão regular: selecione corresponder a pelo menos um dos filtros de correspondência de expressão regular

nome da condição

Escolha a condição que você deseja adicionar à regra. A lista exibe somente condições do tipo que você escolheu na etapa anterior.

6. Para adicionar outra condição à regra, escolha Add another condition e repita as etapas 4 e 5. Observe o seguinte:

- Se você adicionar mais de uma condição, uma solicitação da web deverá corresponder a pelo menos um filtro em cada condição para que o AWS WAF Classic permita ou bloqueie solicitações com base nessa regra.
- Se você adicionar duas condições de correspondência de IP à mesma regra, o AWS WAF Classic só permitirá ou bloqueará solicitações originadas de endereços IP que aparecem nas duas condições de correspondência de IP.

7. Ao terminar de adicionar as condições, escolha Criar.

Adicionar e remover condições de uma regra

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Você pode alterar uma regra ao adicionar ou remover condições.

Para adicionar ou remover condições de uma regra

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Rules.
3. Escolha o nome da regra na qual você deseja adicionar ou remover condições.
4. Escolha Adicionar regra.
5. Para adicionar uma condição, escolha Add condition e especifique os seguintes valores:

Quando uma solicitação atende/não atende

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base nos filtros em uma condição, por exemplo, solicitações da web originadas do intervalo de endereços IP 192.0.2.0/24, escolha does.

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base no inverso dos filtros em uma condição, escolha não. Por exemplo, se uma condição de correspondência de IP incluir o intervalo de endereços IP 192.0.2.0/24 e você quiser que o AWS WAF Classic permita ou bloqueie solicitações que não venham desses endereços IP, escolha não.

corresponder/originar de

Escolha o tipo de condição que você deseja adicionar à regra:

- Condições de correspondência de cross-site scripting: selecione corresponder a pelo menos um dos filtros na condição de correspondência de cross-site scripting
- Condições de correspondência de IP: selecione se originam de um endereço IP em
- Condições de correspondência geográfica: selecione se originam de uma localização geográfica em
- Condições de restrição de tamanho: selecione corresponder a pelo menos um dos filtros na condição de restrição de tamanho
- Condições de correspondência de injeção de SQL: selecione corresponder a pelo menos um dos filtros na condição de correspondência de injeção de SQL
- Condições de correspondência de string: selecione corresponder a pelo menos um dos filtros na condição de correspondência de string
- Condições de correspondência de expressão regular: selecione corresponder a pelo menos um dos filtros de correspondência de expressão regular

nome da condição

Escolha a condição que você deseja adicionar à regra. A lista exibe somente condições do tipo que você escolheu na etapa anterior.

6. Para remover uma condição, selecione o X à direita do nome da condição
7. Selecione Atualizar.

Como excluir uma regra

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Se você quiser excluir uma regra, é preciso primeiro removê-la das web ACLs que a estiverem usando e remover as condições incluídas nela.

Para excluir uma regra

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Para remover a regra das web ACLs que as usam, execute as seguintes etapas para cada uma das web ACLs:

   a. No painel de navegação, selecione Web ACLs.

   b. Escolha o nome de uma web ACL que está usando a regra que você deseja excluir.

   c. Escolha a guia Rules.

   d. Escolha Edit web ACL.

   e. Escolha o X à direita da regra que você deseja remover e escolha Update.
3. No painel de navegação, escolha Rules.
4. Selecione o nome da regra que você deseja excluir.
5. Escolha Excluir.

AWS Marketplace grupos de regras

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

AWS WAF O Classic fornece grupos de AWS Marketplace regras para ajudar você a proteger seus recursos. AWS Marketplace grupos de regras são coleções de ready-to-use regras predefinidas que são escritas e atualizadas por empresas AWS parceiras AWS e empresas parceiras.

Alguns grupos de AWS Marketplace regras são projetados para ajudar a proteger tipos específicos de aplicativos da Web WordPress, como Joomla ou PHP. Outros grupos de AWS Marketplace regras oferecem ampla proteção contra ameaças conhecidas ou vulnerabilidades comuns de aplicativos da Web, como as listadas no OWASP Top 10.

Você pode instalar um único grupo de AWS Marketplace regras do seu AWS parceiro preferido e também pode adicionar suas próprias regras AWS WAF clássicas personalizadas para maior proteção. Se estiver sujeito à compatibilidade regulatória, como PCI ou HIPAA, você poderá usar grupos de regras do AWS Marketplace para atender aos requisitos de firewall do aplicativo web.

AWS Marketplace grupos de regras estão disponíveis sem contratos de longo prazo e sem compromissos mínimos. Quando você se inscrever em um grupo de regras, será cobrada uma taxa mensal (pro-rata por hora) e taxas contínuas com base no volume de solicitações. Para obter mais informações, consulte Preços AWS WAF clássicos e a descrição de cada grupo de AWS Marketplace regras em AWS Marketplace.

Atualizações automáticas

Manter-se atualizado sobre o cenário de ameaças em constante mudança pode ser demorado e caro. AWS Marketplace grupos de regras podem economizar seu tempo ao implementar e usar o AWS WAF Classic. Outro benefício é que AWS nossos AWS parceiros atualizam automaticamente os grupos de AWS Marketplace regras quando surgem novas vulnerabilidades e ameaças.

Muitos dos parceiros serão notificados sobre novas vulnerabilidades antes da divulgação pública. Eles podem atualizar os grupos de regras e implantá-los para você, mesmo antes de uma nova

ameaça ser amplamente conhecida. Muitos também têm equipes de pesquisa de ameaças para investigar e analisar as ameaças mais recentes e gravar as regras mais relevantes.

Acesso às regras em um grupo de AWS Marketplace regras

Cada grupo de AWS Marketplace regras fornece uma descrição abrangente dos tipos de ataques e vulnerabilidades contra os quais ele foi projetado para se proteger. Para proteger a propriedade intelectual dos provedores do grupo de regras, você não poderá visualizar as regras individuais dentro de um grupo de regras. Essa restrição também ajuda a impedir que usuários mal-intencionados projetem ameaças que ignorem especificamente regras publicadas.

Como você não pode visualizar regras individuais em um AWS Marketplace grupo de regras, você também não pode editar nenhuma AWS Marketplace regra em um grupo de regras. No entanto, você pode excluir regras específicas de um grupo de regras. Isso é chamado de “exceção do grupo de regras”. A exclusão de regras não remove essas regras. Em vez disso, ela muda a ação das regras para `COUNT`. Portanto, as solicitações que correspondem a uma regra excluída serão contadas, mas não bloqueadas. Você receberá métricas de COUNT para cada regra excluída.

A exclusão de regras pode ser útil ao solucionar problemas de grupos de regras que estão bloqueando o tráfego inesperadamente (falsos positivos). Uma técnica de solução de problemas é identificar a regra específica dentro do grupo de regras que está bloqueando o tráfego desejado e, em seguida, desativar (excluir) essa determinada regra.

Além de excluir regras específicas, você poderá refinar sua proteção habilitando ou desabilitando grupos de regras inteiros, bem como escolhendo a ação do grupo de regras a ser realizada. Para ter mais informações, consulte Usando grupos de AWS Marketplace regras.

Cotas

Você pode habilitar somente um grupo de AWS Marketplace regras. Você também pode ativar um grupo de regras personalizado que você cria usando AWS Firewall Manager. Esses grupos de regras contam para a cota máxima de 10 regras por web ACL. Portanto, você pode ter um grupo de AWS Marketplace regras, um grupo de regras personalizadas e até oito regras personalizadas em uma única ACL da web.

Definição de preço

Para preços de grupos de AWS Marketplace regras, consulte Preços AWS WAF clássicos e a descrição de cada grupo de AWS Marketplace regras em AWS Marketplace.

Usando grupos de AWS Marketplace regras

Você pode se inscrever e cancelar a inscrição em grupos de AWS Marketplace regras no console AWS WAF Classic. Você pode excluir regras específicas de um grupo de regras.

Para assinar e usar um grupo de regras do AWS Marketplace

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Marketplace.
3. Na seção Available marketplace products, escolha o nome de um grupo de regras para visualizar os detalhes e as informações da definição de preço.
4. Se você quiser se inscrever no grupo de regras, escolha Continue.

   > **Note**
   >
   > Se você não quiser se inscrever nesse grupo de regras, basta fechar esta página em seu navegador.

5. Escolha Set up your account.
6. Adicione o grupo de regras a uma ACL da web, como você adicionaria uma regra individual. Para obter mais informações, consulte Criação de uma web ACL ou Edição de uma web ACL.

   > **Note**
   >
   > Ao adicionar um grupo de regras a uma ACL da web, a ação que você definir para o grupo de regras (No override (Sem substituição) ou Override to count (Substituição para contagem)) é chamada de ação de substituição do grupo de regras. Para ter mais informações, consulte Substituição do grupo de regras.

Para cancelar uma assinatura de um grupo de regras do AWS Marketplace

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.

2. Remova o grupo de regras de todas as :web ACLs. Para ter mais informações, consulte Edição de uma web ACL.
3. No painel de navegação, selecione Marketplace.
4. Escolha Manage your subscriptions.
5. Escolha Cancel subscription ao lado do nome do grupo de regras do qual você deseja cancelar a assinatura.
6. Escolha Yes, cancel subscription.

Como excluir uma regra de um grupo de regras (exceção do grupo de regras)

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Se ainda não estiver habilitado, ative o registro AWS WAF clássico. Para ter mais informações, consulte Registrar em log as informações de tráfego da web ACL. Use os registros AWS WAF clássicos para identificar os IDs das regras que você deseja excluir. Essas são normalmente as regras que estão bloqueando solicitações legítimas.
3. No painel de navegação, selecione Web ACLs.
4. Escolha o nome da web ACL a ser editada. Isso abre uma página com os detalhes da web ACL no painel direito.

   > **Note**
   >
   > O grupo de regras que você deseja editar deverá estar associado a uma web ACL antes que você possa excluir uma regra desse grupo de regras.
5. Na guia Rules no painel direito, escolha Edit web ACL.
6. Na seção Exceções do grupo de regras, expanda o grupo de regras que você deseja editar.
7. Selecione o X ao lado da regra que você deseja excluir. Você pode identificar o ID correto da regra usando os registros AWS WAF clássicos.
8. Escolha Atualizar.

   A exclusão de regras não remove essas regras do grupo de regras. Em vez disso, ela muda a ação das regras para `COUNT`. Portanto, as solicitações que correspondem a uma regra excluída

serão contadas, mas não bloqueadas. Você receberá métricas de `COUNT` para cada regra excluída.

> **Note**
>
> Você pode usar esse mesmo procedimento para excluir regras de grupos de regras personalizadas que você criou no AWS Firewall Manager. No entanto, em vez de excluir uma regra de um grupo de regras personalizadas usando essas etapas, também é possível simplesmente editar um grupo de regras personalizadas usando as etapas descritas em Adicionar e excluir regras de um grupo de regras AWS WAF clássico.

Substituição do grupo de regras

AWS Marketplace grupos de regras têm duas ações possíveis: Sem substituição e Substituir para contar. Se você quiser testar o grupo de regras, defina a ação como Override to count. Essa ação do grupo de regras substitui qualquer ação de bloqueio especificada por regras individuais contidas no grupo. Ou seja, se a ação do grupo de regras for definida como Override to count, em vez de possivelmente bloquear solicitações correspondentes de acordo com a ação de regras individuais do grupo, essas solicitações serão contabilizadas. Por outro lado, se você definir a ação do grupo de regras como No override, as ações das regras individuais do grupo serão usadas.

Solucionar problemas de grupos de regras do AWS Marketplace

Se você descobrir que um grupo de AWS Marketplace regras está bloqueando o tráfego legítimo, execute as etapas a seguir.

Para solucionar problemas de um grupo de regras do AWS Marketplace

1. Exclua as regras específicas que estão bloqueando o tráfego legítimo. Você pode identificar quais regras estão bloqueando quais solicitações usando os registros AWS WAF clássicos. Para obter mais informações sobre a exclusão de regras, consulte Como excluir uma regra de um grupo de regras (exceção do grupo de regras).
2. Se a exclusão de regras específicas não resolver o problema, você poderá alterar a ação do grupo de AWS Marketplace regras de Sem substituição para Substituir para contar. Isso permite que a solicitação da web passe, independentemente das ações de regra individuais dentro do grupo de regras. Isso também fornece CloudWatch métricas da Amazon para o grupo de regras.

3. Depois de definir a ação do grupo de AWS Marketplace regras como Substituir para contar, entre em contato com a equipe de suporte ao cliente do provedor do grupo de regras para solucionar o problema. Para obter informações de contato, consulte a lista de grupos de regras nas páginas de lista de produtos no AWS Marketplace.

Entrar em contato com suporte ao cliente

Em caso de problemas com o AWS WAF Classic ou com um grupo de regras gerenciado por AWS, entre em contato com AWS Support. Para problemas com um grupo de regras gerenciado por um AWS parceiro, entre em contato com a equipe de suporte ao cliente desse parceiro. Para encontrar as informações de contato do parceiro, consulte a listagem do parceiro em AWS Marketplace.

Criar e vender grupos de regras do AWS Marketplace

Se você quiser vender grupos de AWS Marketplace regras AWS Marketplace, consulte Como vender seu software em AWS Marketplace.

Trabalho com :web ACLs

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Ao adicionar regras a uma ACL da web, você especifica se deseja que o AWS WAF Classic permita ou bloqueie solicitações com base nas condições das regras. Se você adicionar mais de uma regra a uma ACL da web, o AWS WAF Classic avalia cada solicitação em relação às regras na ordem em que você as lista na ACL da web. Quando uma solicitação da web corresponde a todas as condições em uma regra, o AWS WAF Classic imediatamente executa a ação correspondente — permitir ou bloquear — e não avalia a solicitação em relação às regras restantes na ACL da web, se houver.

Se uma solicitação da Web não corresponder a nenhuma das regras em uma ACL da Web, o AWS WAF Classic executará a ação padrão que você especificou para a ACL da Web. Para ter mais informações, consulte Decidir quanto à ação padrão da web ACL.

Se quiser testar uma regra antes de começar a usá-la para permitir ou bloquear solicitações, você pode configurar o AWS WAF Classic para contar as solicitações da web que correspondem às condições da regra. Para ter mais informações, consulte Testar web ACLs.

Tópicos

Decidir quanto à ação padrão da web ACL

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Ao criar e configurar uma ACL da web, a primeira e mais importante decisão que você deve tomar é se a ação padrão deve ser permitir solicitações da web ou bloquear solicitações da web para o AWS WAF Classic. A ação padrão indica o que você deseja que o AWS WAF Classic faça depois de inspecionar uma solicitação da Web em busca de todas as condições especificadas, e a solicitação da Web não corresponde a nenhuma dessas condições:

- Permitir: se você deseja permitir que a maioria dos usuários acesse seu website, mas deseja bloquear o acesso a invasores cujas solicitações se originam de endereços IP especificados ou que pareçam conter código SQL mal-intencionado ou valores especificados, escolha Permitir como a ação padrão.

- Bloquear: se você deseja impedir que a maioria dos aspirantes a usuários acesse seu website, mas deseja permitir o acesso aos usuários cujas solicitações se originam de endereços IP especificados ou contêm valores especificados, escolha Bloquear como a ação padrão.

Muitas decisões que você tomar depois decidir uma ação padrão dependerão de você querer permitir ou bloquear a maioria das solicitações da web. Por exemplo, se você deseja permitir a maioria das solicitações, as condições de correspondência criadas deverão especificar, no geral, as solicitações da web que você deseja bloquear, como as seguintes:

- Solicitações originadas de endereços IP que estão fazendo um número sem cabimento de solicitações
- Solicitações originadas de países nos quais você não faz negócios ou que sejam as origens de ataques frequentes
- Solicitações que incluem valores falsos no cabeçalho User-Agent
- Solicitações que aparentem incluir código SQL mal-intencionado

Criação de uma web ACL

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Para criar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. Se for a primeira vez que você usa o AWS WAF Classic, escolha Go to AWS WAF Classic e depois Configure Web ACL. Se você já usou o AWS WAF Classic antes, escolha Web ACLs no painel de navegação e, em seguida, escolha Criar Web ACL.

3. Em Nome da web ACL, insira um nome.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar a web ACL.

4. Para nome da CloudWatch métrica, altere o nome padrão, se aplicável. O nome pode conter somente caracteres alfanuméricos (A-Z, a-z, 0-9), com tamanho máximo de 128 e tamanho mínimo de um. Ele não pode conter espaços em branco ou nomes de métricas reservados para AWS WAF Classic, incluindo “All” e “Default_Action”.

   > **Note**
   >
   > Você não pode alterar o nome depois de criar a web ACL.

5. Em Region (Região da), escolha uma região.
6. Em Recurso do AWS , escolha o recurso que você deseja associar a essa web ACL e, em seguida, escolha Next (Próximo).
7. Se você já criou as condições que deseja que o AWS WAF Classic use para inspecionar suas solicitações da web, escolha Avançar e continue na próxima etapa.

   Se você ainda não tiver criado condições, faça isso agora. Para obter mais informações, consulte os tópicos a seguir.

   - Trabalhar com condições de correspondência de cross-site scripting
   - Trabalhar com condições de correspondência de IP
   - Trabalhar com condições de correspondência geográfica
   - Trabalhar com condições de restrição de tamanho
   - Trabalhar com condições de correspondência de injeção de SQL
   - Trabalhar com condições de correspondência de string
   - Trabalhar com condições de correspondência regex
8. Se você já criou as regras ou grupos de regras (ou se inscreveu em um grupo de AWS Marketplace regras) que deseja adicionar a essa ACL da web, adicione as regras à ACL da web:

   a. Na lista Rules, escolha uma regra.

   b. Selecione Add rule to web ACL.

c. Repita as etapas a e b até adicionar todas as regras que você deseja a essa web ACL.

d. Vá para a etapa 10.

9. Se você ainda não tiver criado regras, pode adicioná-las agora:

a. Escolha a opção Criar regra.

b. Insira os seguintes valores:

Nome

Insira um nome.

CloudWatch nome da métrica

Insira um nome para a CloudWatch métrica que o AWS WAF Classic criará e associará à regra. O nome pode conter somente caracteres alfanuméricos (A-Z, a-z, 0-9), com tamanho máximo de 128 e tamanho mínimo de um. Ele não pode conter espaços em branco ou nomes de métrica reservados para o AWS WAF Classic, incluindo “All” e “Default_Action”.

> **Note**
>
> Você não pode alterar o nome da métrica depois de criar a regra.

c. Para adicionar uma condição à regra, especifique os seguintes valores:

Quando uma solicitação atende/não atende

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base nos filtros em uma condição, por exemplo, solicitações da web originadas do intervalo de endereços IP 192.0.2.0/24, escolha does.

Se você quiser que o AWS WAF Classic permita ou bloqueie solicitações com base no inverso dos filtros em uma condição, escolha não. Por exemplo, se uma condição de correspondência de IP incluir o intervalo de endereços IP 192.0.2.0/24 e você quiser que o AWS WAF Classic permita ou bloqueie solicitações que não venham desses endereços IP, escolha não.

corresponder/originar de

Escolha o tipo de condição que você deseja adicionar à regra:

- Condições de correspondência de cross-site scripting: selecione corresponder a pelo menos um dos filtros na condição de correspondência de cross-site scripting
- Condições de correspondência de IP: selecione se originam de um endereço IP em
- Condições de correspondência geográfica: selecione se originam de uma localização geográfica em
- Condições de restrição de tamanho: selecione corresponder a pelo menos um dos filtros na condição de restrição de tamanho
- Condições de correspondência de injeção de SQL: selecione corresponder a pelo menos um dos filtros na condição de correspondência de injeção de SQL
- Condições de correspondência de string: selecione corresponder a pelo menos um dos filtros na condição de correspondência de string
- Condições de correspondência de expressões regulares: escolha corresponder a pelo menos um dos filtros na condição de correspondência de expressão regular

nome da condição

Escolha a condição que você deseja adicionar à regra. A lista exibe somente as condições do tipo que você escolheu na lista anterior.

d. Para adicionar outra condição à regra, escolha Add another condition (Adicionar outra condição) e, em seguida, repita as etapas b e c. Observe o seguinte:

- Se você adicionar mais de uma condição, uma solicitação da web deverá corresponder a pelo menos um filtro em cada condição para que o AWS WAF Classic permita ou bloqueie solicitações com base nessa regra.
- Se você adicionar duas condições de correspondência de IP à mesma regra, o AWS WAF Classic só permitirá ou bloqueará solicitações originadas de endereços IP que aparecem nas duas condições de correspondência de IP.

e. Repita a etapa 9 até criar todas as regras que você deseja adicionar a esta web ACL.

f. Escolha Criar.

g. Continue para a etapa 10.

10. Para cada regra ou grupo de regras na ACL da web, escolha o tipo de gerenciamento que você deseja que o AWS WAF Classic forneça, da seguinte forma:

- Para cada regra, escolha se você deseja que o AWS WAF Classic permita, bloqueie ou conte solicitações da web com base nas condições da regra:

- Permitir — o API Gateway CloudFront ou um Application Load Balancer responde com o objeto solicitado. No caso de CloudFront, se o objeto não estiver no cache de borda, CloudFront encaminhe a solicitação para a origem.
- Bloquear — O API Gateway CloudFront ou um Application Load Balancer responde à solicitação com um código de status HTTP 403 (Proibido). CloudFront também pode responder com uma página de erro personalizada. Para ter mais informações, consulte Usando o AWS WAF Classic com páginas de erro CloudFront personalizadas.
- Contagem — O AWS WAF Classic incrementa um contador de solicitações que correspondem às condições da regra e, em seguida, continua inspecionando a solicitação da web com base nas regras restantes na ACL da web.

  Para obter informações sobre como usar o Count para testar uma web ACL antes de começar a usá-lo para permitir ou bloquear solicitações da web, consulte Contar as solicitações da web correspondentes às regras de uma web ACL.

- Para cada grupo de regras, defina a ação de substituição para o grupo de regras:
  - Não substituir: faz com que as ações das regras individuais no grupo de regras sejam usadas.
  - Substituir para contagem: substitui todas as ações de bloqueio especificadas por regras individuais no grupo, para que todas as solicitações correspondentes sejam apenas contadas.

  Para ter mais informações, consulte Substituição do grupo de regras.

11. Se você quiser alterar a ordem das regras na ACL da web, use as setas na coluna Ordem. AWS WAF O Classic inspeciona as solicitações da web com base na ordem em que as regras aparecem na ACL da web.
12. Para remover uma regra que você adicionou à web ACL, selecione x na linha da regra.
13. Selecione a ação padrão para a web ACL. Essa é a ação que o AWS WAF Classic executa quando uma solicitação da web não corresponde às condições em nenhuma das regras dessa ACL da web. Para ter mais informações, consulte Decidir quanto à ação padrão da web ACL.
14. Selecione Review and create.
15. Analise as configurações da web ACL e selecione Confirm and create.

Associar ou desassociar uma Web ACL com uma API do Amazon API Gateway, uma CloudFront distribuição ou um Application Load Balancer

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Para associar ou desassociar uma web ACL, execute o procedimento aplicável. Observe que você também pode associar uma ACL da web a uma CloudFront distribuição ao criar ou atualizar a distribuição. Para obter mais informações, consulte Usando o AWS WAF Classic para controlar o acesso ao seu conteúdo no Amazon CloudFront Developer Guide.

As seguintes restrições se aplicam ao associar uma web ACL:

- Cada API do API Gateway, Application Load Balancer e CloudFront distribuição podem ser associados a apenas uma ACL da web.
- As Web ACLs associadas a uma CloudFront distribuição não podem ser associadas a uma API do Application Load Balancer ou do API Gateway. No entanto, a ACL da web pode ser associada a outras CloudFront distribuições.

Para associar uma ACL da web a uma API Gateway, API, CloudFront distribuição ou Application Load Balancer

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da ACL da web que você deseja associar a uma API do API Gateway, CloudFront distribuição ou Application Load Balancer. Isso abre uma página com os detalhes da web ACL no painel direito.

4. Na guia Regras, em Recursos da AWS utilizando esta web ACL, selecione Adicionar associação.
5. Quando solicitado, use a lista de recursos para escolher a API do API Gateway, a CloudFront distribuição ou o Application Load Balancer à qual você deseja associar essa ACL da web. Se você escolher um Application Load Balancer, deverá também especificar uma região.
6. Escolha Add.
7. Para associar essa ACL da web a uma API adicional do API Gateway, CloudFront distribuição ou outro Application Load Balancer, repita as etapas 4 a 6.

Para desassociar uma ACL da web de uma API Gateway, API, CloudFront distribuição ou Application Load Balancer

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da ACL da web que você deseja desassociar de uma API do API Gateway, CloudFront distribuição ou Application Load Balancer. Isso abre uma página com os detalhes da web ACL no painel direito.
4. Na guia Regras, em AWS recursos usando essa ACL da web, escolha o x para cada API do API Gateway, CloudFront distribuição ou Application Load Balancer da qual você deseja desassociar essa ACL da web.

Edição de uma web ACL

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Para adicionar ou remover as regras de uma web ACL ou alterar a ação padrão, execute o procedimento a seguir.

Para editar uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Web ACLs.
3. Escolha o nome da web ACL a ser editada. Isso abre uma página com os detalhes da ACL da web no painel direito.
4. Na guia Rules no painel direito, escolha Edit web ACL.
5. Para adicionar regras à web ACL, execute as seguintes etapas:

   a. Na lista Rules, selecione a regra que você deseja adicionar.

   b. Selecione Add rule to web ACL.

   c. Repita as etapas a e b até que você tenha adicionado todas as regras que quiser.
6. Se você quiser alterar a ordem das regras na ACL da web, use as setas na coluna Ordem. AWS WAF O Classic inspeciona as solicitações da web com base na ordem em que as regras aparecem na ACL da web.
7. Para remover uma regra da web ACL, selecione x à direita da linha dessa regra. Isso não exclui a regra do AWS WAF Classic, apenas remove a regra dessa ACL da web.
8. Para alterar a ação para uma regra ou ação padrão para a web ACL, escolha a opção preferida.

   > **Note**
   >
   > Ao definir a ação para um grupo de regras ou um grupo de AWS Marketplace regras (em oposição a uma única regra), a ação que você define para o grupo de regras (Sem substituição ou Substituir para contar) é chamada de ação de substituição. Para mais informações, consulte Substituição do grupo de regras.
9. Escolha Salvar alterações.

Exclusão de uma ACL da web

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Para excluir uma ACL da web, você deve remover as regras incluídas na ACL da web e desassociar todas as CloudFront distribuições e os Application Load Balancers da ACL da web. Execute o procedimento a seguir.

Para excluir uma web ACL

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, selecione Web ACLs.
3. Selecione o nome da web ACL que deseja excluir. Isso abre uma página com os detalhes da ACL da web no painel direito.
4. Na guia Rules no painel direito, escolha Edit web ACL.
5. Para remover todas as regras da web ACL, selecione x à direita da linha de cada regra. Isso não exclui as regras do AWS WAF Classic, apenas remove as regras dessa ACL da web.
6. Escolha Atualizar.
7. Desassocie a Web ACL de todas as CloudFront distribuições e Application Load Balancers. Na guia Regras, em AWS Recursos usando essa ACL da web, escolha o x para cada API do API Gateway, CloudFront distribuição ou Application Load Balancer.
8. Na página Web ACLs , confirme se a ACL da web que você deseja excluir está selecionada e, em seguida, escolha Delete (Excluir).

Testar web ACLs

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Para garantir que você não configure acidentalmente o AWS WAF Classic para bloquear solicitações da web que você deseja permitir ou permitir solicitações que deseja bloquear, recomendamos que você teste minuciosamente sua ACL da web antes de começar a usá-la em seu site ou aplicativo da web.

Tópicos

Contar as solicitações da web correspondentes às regras de uma web ACL

Ao adicionar regras a uma ACL da web, você especifica se deseja que o AWS WAF Classic permita, bloqueie ou conte as solicitações da web que correspondem a todas as condições dessa regra. Recomendamos que você comece com a seguinte configuração:

- Configure todas as regras de uma web ACL para contar solicitações da web
- Defina a ação padrão para a web ACL permitir solicitações

Nessa configuração, o AWS WAF Classic inspeciona cada solicitação da web com base nas condições da primeira regra. Se a solicitação da web corresponder a todas as condições dessa regra, o AWS WAF Classic incrementa um contador para essa regra. Em seguida, o AWS WAF Classic inspeciona a solicitação da web com base nas condições da próxima regra. Se a solicitação corresponder a todas as condições dessa regra, o AWS WAF Classic incrementa um contador para a regra. Isso continua até que o AWS WAF Classic tenha inspecionado a solicitação com base nas condições de todas as suas regras.

Depois de configurar todas as regras em uma ACL da web para contar solicitações e associar a ACL da web a uma API do Amazon API Gateway, CloudFront distribuição ou Application Load Balancer, você pode visualizar as contagens resultantes em um gráfico da Amazon. CloudWatch Para cada regra em uma ACL da web e para todas as solicitações que o API Gateway CloudFront ou um Application Load Balancer encaminha para o Classic AWS WAF para uma CloudWatch ACL da web, você pode:

- Visualize dados da hora anterior ou das três horas anteriores
- Altere o intervalo entre os pontos de dados
- Altere o cálculo que é CloudWatch executado nos dados, como máximo, mínimo, média ou soma

> **Note**
>
> AWS WAF O Classic with CloudFront é um serviço global e as métricas estão disponíveis somente quando você escolhe a região Leste dos EUA (Norte da Virgínia) no AWS Management Console. Se você escolher outra região, nenhuma métrica AWS WAF clássica aparecerá no CloudWatch console.

Para visualizar os dados das regras em uma web ACL

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, em Métricas, escolha WAF.
3. Marque a caixa de seleção da web ACL da qual você deseja visualizar os dados.
4. Altere as configurações aplicáveis:

   Estatística

   Escolha o cálculo que é CloudWatch executado nos dados.

   Intervalo de tempo

   Escolha se você deseja visualizar dados da hora anterior ou das três horas anteriores.

   Período

   Escolha o intervalo entre pontos de dados no gráfico.

Regras

Escolha as regras das quais você deseja visualizar os dados.

Observe o seguinte:

- Se você acabou de associar uma ACL da web a uma API do API Gateway, CloudFront distribuição ou Application Load Balancer, talvez seja necessário aguardar alguns minutos para que os dados apareçam no gráfico e para que a métrica da ACL da web apareça na lista de métricas disponíveis.
- Se você associar mais de uma API do API Gateway, CloudFront distribuição ou Application Load Balancer a uma ACL da web, os CloudWatch dados incluirão todas as solicitações de todas as distribuições associadas à ACL da web.
- Você pode passar o cursor do mouse sobre o ponto de dados para obter mais informações.
- O gráfico não é automaticamente atualizado. Para atualizar a exibição, escolha o ícone de atualização ().

5. (Opcional) Visualize informações detalhadas sobre solicitações individuais que o API Gateway CloudFront ou um Application Load Balancer encaminharam para o Classic. AWS WAF Para ter mais informações, consulte Visualizando uma amostra das solicitações da web que o API Gateway CloudFront ou um Application Load Balancer encaminharam para o Classic AWS WAF.
6. Se você determinar que a regra é interceptar as solicitações que você não quer que sejam interceptadas, altere as configurações aplicáveis. Para ter mais informações, consulte Criar e configurar uma lista de controle de acesso à web (web ACL).

   Quando você estiver satisfeito com todas as suas regras interceptando apenas as solicitações corretas, altere a ação de cada uma delas regras para Allow ou Block. Para ter mais informações, consulte Edição de uma web ACL.

Visualizando uma amostra das solicitações da web que o API Gateway CloudFront ou um Application Load Balancer encaminharam para o Classic AWS WAF

No console AWS WAF Classic, você pode ver uma amostra das solicitações que o API Gateway CloudFront ou um Application Load Balancer encaminharam ao AWS WAF Classic para inspeção. Para cada solicitação amostrada, você pode exibir dados detalhados sobre a solicitação, como o

endereço IP de origem e os cabeçalhos incluídos na solicitação. Você também pode visualizar a solicitação correspondente e se a regra é configurada para permitir ou bloquear solicitações.

Os exemplos contém até 100 solicitações que correspondem a todas as condições em cada regra e outras 100 solicitações para a ação padrão, que se aplica a solicitações que não correspondem a todas as condições em qualquer regra. As solicitações na amostra vêm de todas as APIs do API Gateway, CloudFront pontos de presença ou balanceadores de carga de aplicativos que receberam solicitações para seu conteúdo nos últimos 15 minutos.

Para ver uma amostra das solicitações da web que o API Gateway; CloudFront ou um Application Load Balancer encaminhou para o Classic AWS WAF

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha a web ACL da qual você deseja visualizar as solicitações.
3. No painel direito, selecione a guia Requests.

   A tabela Sampled requests exibe os seguintes valores para cada solicitação:

   IP de origem

   O endereço IP da qual a solicitação se originou ou, se o visualizador tiver usado um proxy HTTP ou um Application Load Balancer para enviar a solicitação, o endereço IP do proxy ou do Application Load Balancer.

   URI

   O caminho do URI da solicitação, que identifica o recurso, por exemplo, `/images/daily-ad.jpg`. Isso não inclui a string de consulta ou os componentes de fragmento do URI. Para obter mais informações, consulte Identificador de recurso uniforme (URI): sintaxe genérica.

   Corresponde à regra

   Identifica a primeira regra na web ACL para a qual a solicitação da web correspondeu a todas as condições. Se uma solicitação da web não corresponder a todas as condições em qualquer regra na web ACL, o valor de Matches rule será Default.

   Observe que quando uma solicitação da web corresponde a todas as condições em uma regra e a ação dessa regra é Count, o AWS WAF Classic continua inspecionando a

solicitação da web com base nas regras subsequentes na ACL da web. Neste caso, uma solicitação da web pode aparecer duas vezes na lista de solicitações de amostra: uma vez para a regra que tem uma ação Count e mais uma vez para a regra subsequente ou para a ação padrão.

Ação

Indica se a ação para a regra correspondente é Allow, Block ou Count.

Time

A hora em que o AWS WAF Classic recebeu a solicitação do API Gateway CloudFront ou do seu Application Load Balancer.

4. Para exibir informações adicionais sobre a solicitação, escolha a seta no lado esquerdo do endereço IP dessa solicitação. AWS WAF O Classic exibe as seguintes informações:

IP de origem

O mesmo endereço IP como o valor na coluna Source IP da tabela.

País

O código de país com duas letras do país do qual a solicitação se originou. Se o visualizador tiver usado um proxy HTTP ou um Application Load Balancer para enviar a solicitação, este será o código de duas letras do país em que o proxy HTTP ou um Application Load Balancer está.

Para obter uma lista de códigos de país de duas letras e nomes de países correspondentes, consulte a entrada da Wikipédia ISO 3166-1 alfa-2.

Método

O método de solicitação HTTP para a solicitação: `GET`, `HEAD`, `OPTIONS`, `PUT`, `POST`, `PATCH` ou `DELETE`.

URI

O mesmo URI como o valor na coluna URI da tabela.

Cabeçalhos de solicitação

Os valores do cabeçalho e dos cabeçalhos de solicitação na solicitação.

5. Para atualizar a lista de solicitações de amostra, escolha Get new samples.

Trabalhando com grupos de regras AWS WAF clássicos para uso com AWS Firewall Manager

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Um grupo de regras AWS WAF clássico é um conjunto de regras que você adiciona a uma AWS Firewall Manager política AWS WAF clássica. Você pode criar seu próprio grupo de regras ou comprar um grupo de regras gerenciadas AWS Marketplace.

> **Important**
>
> Se você quiser adicionar um grupo de AWS Marketplace regras à sua política do Firewall Manager, cada conta em sua organização deve primeiro se inscrever nesse grupo de regras. Depois que todas as contas estiverem inscritas, você poderá adicionar o grupo de regras a uma política. Para ter mais informações, consulte AWS Marketplace grupos de regras.

Tópicos

Criação de um grupo de regras AWS WAF clássico

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.

Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Ao criar um grupo de regras AWS WAF clássico para usar com AWS Firewall Manager, você especifica quais regras adicionar ao grupo.

Para criar um grupo de regras (console)

1. Faça login AWS Management Console usando a conta de AWS Firewall Manager administrador que você configurou nos pré-requisitos e abra o console do Firewall Manager em. https://console.aws.amazon.com/wafv2/fms

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte Etapa 2: criar uma conta de administrador AWS Firewall Manager padrão.

2. No painel de navegação, escolha Alternar para AWS WAF clássico.
3. No painel de navegação AWS WAF Clássico, escolha Grupos de regras.
4. Escolha Criar grupo de regras.

   > **Note**
   >
   > Não é possível adicionar regras baseadas em tarifas a um grupo de regras.

5. Se você já tiver criado as regras que deseja adicionar ao grupo de regras, escolha Usar regras existentes para este grupo de regras. Se você deseja criar novas regras para adicionar ao grupo de regras, escolha Criar regras e condições para este grupo de regras.
6. Escolha Próximo.
7. Se você optar por criar regras, siga as etapas para criá-las em Criar uma regra e editar condições.

   > **Note**
   >
   > Use o console AWS WAF Clássico para criar suas regras.

Depois de criar todas as regras necessárias, avance para a próxima etapa.

8. Digite um nome para o grupo de regras.
9. Para adicionar uma regra ao grupo de regras, selecione uma regra e escolha Adicionar regra. Escolha se deseja permitir, bloquear ou contar solicitações que correspondam às condições da regra. Para obter mais informações sobre as opções, consulte Como funciona o AWS WAF Classic.
10. Quando terminar de adicionar regras, escolha Criar.

Você pode testar seu grupo de regras adicionando-o a uma AWS WAF WebACL e definindo a ação WebACL como Substituir para Contagem. Essa ação substitui qualquer ação que você escolher para as regras contidas no grupo e só conta as solicitações correspondentes. Para ter mais informações, consulte Criação de uma web ACL.

Adicionar e excluir regras de um grupo de regras AWS WAF clássico

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Você pode adicionar ou excluir regras em um grupo de regras AWS WAF clássico.

A exclusão de uma regra do grupo de regras não exclui a regra em si. Ela só remove a regra do grupo.

Para adicionar ou excluir regras de um grupo de regras (console)

1. Faça login AWS Management Console usando a conta de AWS Firewall Manager administrador que você configurou nos pré-requisitos e abra o console do Firewall Manager em. https://console.aws.amazon.com/wafv2/fms

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte Etapa 2: criar uma conta de administrador AWS Firewall Manager padrão.

2. No painel de navegação, escolha Alternar para AWS WAF clássico.
3. No painel de navegação AWS WAF Clássico, escolha Grupos de regras.
4. Escolha o grupo de regras que você deseja editar.
5. Escolha Editar grupo de regras.
6. Para adicionar regras, execute as etapas a seguir:

   a. Selecione uma regra e escolha Adicionar regra ao grupo de regras. Escolha se deseja permitir, bloquear ou contar solicitações que correspondam às condições da regra. Para obter mais informações sobre as opções, consulte Como funciona o AWS WAF Classic. Repita essa etapa para adicionar mais regras ao grupo de regras.

   > **Note**
   >
   > Você não pode adicionar regras baseadas em intervalos ao grupo de regras.

   b. Escolha Atualizar.
7. Para excluir regras, execute as etapas a seguir:

   a. Escolha o X ao lado da regra que você deseja excluir. Repita essa etapa para excluir mais regras do grupo de regras.

   b. Selecione Atualizar.

Introdução AWS Firewall Manager para ativar as regras AWS WAF clássicas

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro

de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Você pode usar AWS Firewall Manager para habilitar AWS WAF regras, regras AWS WAF clássicas, AWS Shield Advanced proteções e grupos de segurança da Amazon VPC. As etapas de configuração são um pouco diferentes para cada um:

- Para usar o Firewall Manager para habilitar regras usando a versão mais recente do AWS WAF, não use este tópico. Em vez disso, siga as etapas em Introdução às AWS Firewall ManagerAWS WAF políticas.
- Para usar o Firewall Manager para ativar AWS Shield Advanced as proteções, siga as etapas emIntrodução às AWS Firewall ManagerAWS Shield Advanced políticas.
- Para usar o Firewall Manager para habilitar grupos de segurança do Amazon VPC, siga as etapas em Introdução às políticas de grupos de segurança AWS Firewall Manager da Amazon VPC.

Para usar o Firewall Manager para ativar as regras AWS WAF clássicas, execute as etapas a seguir em sequência.

Tópicos

Etapa 1: Concluir os pré-requisitos

Note

Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para Etapa 2: Criar regras.

Etapa 2: Criar regras

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Nesta etapa, você cria regras usando o AWS WAF Classic. Se você já tem regras AWS WAF clássicas com as quais deseja usar AWS Firewall Manager, pule esta etapa e vá paraEtapa 3: Criar um grupo de regras.

> **Note**
>
> Use o console AWS WAF Clássico para criar suas regras.

Para criar regras AWS WAF clássicas (console)

- Crie as regras e, em seguida, adicione as condições nas regras. Para ter mais informações, consulte Criar uma regra e editar condições.

Você está pronto para ir para Etapa 3: Criar um grupo de regras.

Etapa 3: Criar um grupo de regras

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro

de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Um grupo de regras é um conjunto de regras que define as ações que serão executadas quando um determinado conjunto de condições for satisfeito. Você pode usar grupos de regras AWS Marketplace gerenciados e criar seus próprios grupos de regras. Para obter informações sobre grupos de regras gerenciadas, consulte AWS Marketplace grupos de regras.

Para criar seu próprio grupo de regras, execute o procedimento a seguir.

Para criar um grupo de regras (console)

1. Faça login AWS Management Console usando a conta de AWS Firewall Manager administrador que você configurou nos pré-requisitos e abra o console do Firewall Manager em. https://console.aws.amazon.com/wafv2/fms
2. No painel de navegação, escolha Políticas de segurança.
3. Se você não atender aos pré-requisitos, o console exibirá instruções sobre como corrigir os problemas. Siga as instruções e, em seguida, inicie esta etapa (criar um grupo de regras) novamente. Se você já cumpriu os pré-requisitos, escolha Close (Fechar).
4. Escolha Criar política.

   Em Tipo de política, escolha AWS WAF Classic.
5. Escolha Criar uma AWS Firewall Manager política e adicionar um novo grupo de regras.
6. Escolha um e Região da AWS, em seguida, escolha Avançar.
7. Como você já criou as regras, não precisa criar as condições. Escolha Próximo.
8. Como você já criou as regras, não precisa criar regras. Escolha Próximo.
9. Escolha Criar grupo de regras.
10. Em Nome, insira um nome fácil de lembrar.
11. Insira um nome para a CloudWatch métrica que o AWS WAF Classic criará e associará ao grupo de regras. O nome pode conter somente os caracteres alfanuméricos (A-Z, a-z, 0-9) ou os seguintes caracteres especiais _-!"#`+*},./. Ele não pode conter espaços em branco.
12. Selecione uma regra e escolha Add rule (Adicionar regra). Uma regra tem uma configuração de ação que permite que você escolha se deseja permitir, bloquear ou contar solicitações que

correspondam às condições da regra. Para este tutorial, escolha Contar. Repita a etapa de adição de regras até adicionar todas as regras que você deseja ter no grupo de regras.

13. Escolha Criar.

Você está pronto para ir para Etapa 4: criar e aplicar uma política AWS Firewall ManagerAWS WAF clássica.

Etapa 4: criar e aplicar uma política AWS Firewall ManagerAWS WAF clássica

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Depois de criar o grupo de regras, você cria uma AWS Firewall Manager AWS WAF política. Uma AWS WAF política do Firewall Manager contém o grupo de regras que você deseja aplicar aos seus recursos.

Para criar uma AWS WAF política do Firewall Manager (console)

1. Depois de criar o grupo de regras (a última etapa no procedimento anterior, Etapa 3: Criar um grupo de regras), o console exibe a página Rule group summary (Resumo do grupo de regras). Escolha Próximo.
2. Em Nome, insira um nome fácil de lembrar.
3. Em Tipo de política, escolha WAF.
4. Para Região, escolha um Região da AWS. Para proteger os CloudFront recursos da Amazon, escolha Global.

   Para proteger recursos em várias regiões (exceto CloudFront recursos), você deve criar políticas separadas do Firewall Manager para cada região.
5. Selecione um grupo de regras para adicionar e, em seguida, escolha Add rule group (Adicionar grupo de regras).

6. Uma política executa duas ações possíveis: Action set by rule group (Ação definida pelo grupo de regras) e Count (Contar). Se você quiser testar a política e o grupo de regras, defina a ação como Count (Contar). Essa ação substitui qualquer ação de bloqueio especificada pelo grupo de regras contido na política. Em outras palavras, se a ação da política for definida como Count (Contar), as solicitações serão apenas contadas, e não bloqueadas. Por outro lado, se você definir a ação da política como Action set by rule group (Ação definida pelo grupo de regras), as ações do grupo de regras da política serão usadas. Para este tutorial, escolha Contar.
7. Escolha Próximo.
8. Se você deseja incluir apenas contas específicas na política ou, como alternativa, excluir contas específicas da política, selecione Select accounts to include/exclude from this policy (optional) (Selecionar contas para incluir/excluir desta política (opcional)). Selecione Include only these accounts in this policy (Incluir apenas essas contas nessa política) ou Exclude these accounts from this policy (Excluir essas contas dessa política). Você só pode escolher uma opção. Escolha Add. Selecione os números de contas para incluir ou excluir e selecione OK.

   > **Note**
   >
   > Se você não selecionar essa opção, o Firewall Manager aplicará uma política a todas as contas na sua organização no AWS Organizations. Se você adicionar uma nova conta à organização, o Firewall Manager aplicará automaticamente a política a essa conta.

9. Escolha os tipos de recurso que você deseja proteger.
10. Se você quiser proteger ou excluir somente os recursos com tags específicas, selecione Use tags to include/exclude resources (Usar tags para incluir/excluir recursos), digite as tags e, depois, selecione Include (Incluir) ou Exclude (Excluir). Você só pode escolher uma opção.

    Se você inserir mais de uma tag (separada por vírgula) e se um recurso tiver qualquer uma dessas tags, a correspondência será estabelecida.

    Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
11. Escolha Create and apply this policy to existing and new resources (Criar e aplicar esta política aos recursos novos e existentes).

    Essa opção cria uma ACL da web em cada conta aplicável em AWS Organizations uma organização e associa a ACL da web aos recursos especificados nas contas. Essa opção também aplica a política a todos os recursos novos que correspondam aos critérios mencionados anteriormente (tipo de recurso e tags). Como alternativa, se você selecionar Criar

política mas não aplicá-la a recursos novos ou existentes, o Firewall Manager criará a ACL da web em cada conta aplicável da organização, mas não aplicará a ACL da web a nenhum dos recursos. Você deverá aplicar a política aos recursos mais tarde.

12. Deixe a opção Replace existing associated web ACLs (Substituir as ACLs da web associadas existentes) na configuração padrão.

    Quando essa opção está selecionada, o Firewall Manager removeu todas as associações de ACL da web existentes dos recursos no escopo antes de associar as ACLs da web da nova política a elas.

13. Escolha Próximo.
14. Analise a nova política. Para fazer quaisquer alterações, escolha Edit (Editar). Quando estiver satisfeito com a política, escolha Criar política.

Tutorial: Criar uma política do AWS Firewall Manager com regras hierárquicas

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Com AWS Firewall Manager, você pode criar e aplicar políticas de proteção AWS WAF clássicas que contêm regras hierárquicas. Ou seja, você pode criar e impor regras de forma centralizada, mas delegar a criação e a manutenção de regras específicas de contas para outras pessoas. Você pode monitorar as regras (comuns) aplicadas de forma centralizada para qualquer remoção acidental ou inépcia, garantindo, assim, que elas sejam aplicadas de forma consistente. As regras especificas de contas adicionam mais proteção personalizada para as necessidades de equipes individuais.

> **Note**
>
> Na versão mais recente do AWS WAF, esse recurso é incorporado e não requer nenhum tratamento especial. Se você ainda não estiver usando o AWS WAF Classic, use a versão mais recente. Consulte Criação de uma AWS Firewall Manager política para AWS WAF.

O tutorial a seguir descreve como criar um conjunto hierárquico de regras de proteção.

Tópicos

Etapa 1: designar uma conta de administrador do Firewall Manager

Para usar AWS Firewall Manager, você deve designar uma conta em sua organização como a conta de administrador do Firewall Manager. Essa conta pode ser a conta de gerenciamento ou uma conta-membro na organização.

Você pode usar a conta de administrador do Firewall Manager para criar um conjunto de regras comuns que se aplicam a outras contas na organização. Outras contas na organização não podem alterar essas regras aplicadas de forma centralizada.

Para designar uma conta como uma conta de administrador do Firewall Manager e concluir outros pré-requisitos para usar o Firewall Manager, consulte as instruções em AWS Firewall Manager pré-requisitos. Se você já tiver concluído os pré-requisitos, vá para a etapa 2 deste tutorial.

Neste tutorial, chamamos a conta de administrador de **`Firewall-Administrator-Account`**.

Etapa 2: criar um grupo de regras usando a conta de administrador do Firewall Manager

Depois, crie um grupo de regras usando **`Firewall-Administrator-Account`**. Esse grupo de regras contém as regras comuns que você aplicará a todas as contas-membro sujeitas à política

que você criar na próxima etapa. Só **Firewall-Administrator-Account** pode fazer alterações nessas regras e no grupo de regras de contêiner.

Neste tutorial, chamamos esse grupo de regras de contêiner de **Common-Rule-Group**.

Para criar um grupo de regras, consulte as instruções em Criação de um grupo de regras AWS WAF clássico. Lembre-se de fazer login no console usando sua conta de administrador do Firewall Manager (**Firewall-Administrator-Account**) ao seguir estas instruções.

Etapa 3: criar uma política do Firewall Manager e associar o grupo de regras comuns

Usando **Firewall-Administrator-Account**, crie uma política do Firewall Manager. Ao criar essa política, faça o seguinte:

- Adicione **Common-Rule-Group** à nova política.
- Inclua todas as contas na organização às quais você deseja aplicar **Common-Rule-Group**.
- Adicione todos os recursos aos quais você deseja aplicar **Common-Rule-Group**.

Para obter instruções sobre como criar uma política, consulte Criação de uma AWS Firewall Manager política.

Isso cria uma web ACL em cada conta especificada e adiciona **Common-Rule-Group** a cada uma dessas web ACLs. Depois de criar a política, essa web ACL e regras comuns são implantadas em todas as contas especificadas.

Neste tutorial, chamamos essa web ACL de **Administrator-Created-ACL**. Uma **Administrator-Created-ACL** exclusiva agora existe em cada conta-membro especificada da organização.

Etapa 4: Adicionar regras específicas de contas

Cada conta-membro na organização agora pode adicionar suas próprias regras específicas de contas à **Administrator-Created-ACL** existente na conta. As regras comuns já existentes **Administrator-Created-ACL** continuam a ser aplicadas, juntamente com as novas regras específicas da conta. AWS WAF inspeciona solicitações da web com base na ordem em que as regras aparecem na ACL da web. Isso se aplica à **Administrator-Created-ACL** e às regras específicas de contas.

Para adicionar regras ao **`Administrator-Created-ACL`**, consulte Edição de uma web ACL.

Conclusão

Você agora tem uma web ACL que contém regras comuns administradas pela conta de administrador do Firewall Manager, bem como as regras específicas mantidas por cada conta-membro.

A **`Administrator-Created-ACL`** em cada conta faz referência ao **`Common-Rule-Group`** único. Portanto, futuras alterações feitas pela conta de administrador do Firewall Manager em **`Common-Rule-Group`** serão aplicadas imediatamente a cada conta-membro.

As contas-membro não podem alterar nem remover as regras comuns em **`Common-Rule-Group`**.

As regras específicas de contas não afetam outras contas.

Registrar em log as informações de tráfego da web ACL

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

> **Note**
>
> Você não pode usar o Amazon Security Lake para coletar dados do AWS WAF Classic.

Você pode habilitar o registro em log para obter informações detalhadas sobre o tráfego que é analisado pela web ACL. As informações contidas nos registros incluem a hora em que o AWS WAF Classic recebeu a solicitação do seu AWS recurso, informações detalhadas sobre a solicitação e a ação da regra à qual cada solicitação correspondeu.

Para começar, configure um Amazon Kinesis Data Firehose. Como parte desse processo, selecione um destino para armazenar seus logs. Em seguida, selecione a web ACL para a qual você

deseja habilitar o registro em log. Depois de ativar o registro, AWS WAF entrega os registros pela mangueira de incêndio até seu destino de armazenamento.

Para obter informações sobre como criar um Amazon Kinesis Data Firehose e revisar seus registros armazenados, consulte O que é o Amazon Data Firehose? Para entender as permissões necessárias para a configuração do Kinesis Data Firehose, consulte Controlar acesso com o Amazon Kinesis Data Firehose.

Você deve ter as seguintes permissões para habilitar o registro em log com êxito:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Para obter mais informações sobre funções vinculadas ao serviço e as permissões do `iam:CreateServiceLinkedRole`, consulte Usando funções vinculadas a serviços para Classic AWS WAF.

Para habilitar o registro de uma web ACL

1. Crie um Amazon Kinesis Data Firehose usando um nome começando com o aws-waf-logs prefixo "-" Por exemplo,. `aws-waf-logs-us-east-2-analytics` Crie o Data Firehose com uma origem PUT e na região em que você está operando. Se você estiver capturando registros para a Amazon CloudFront, crie a mangueira de incêndio no Leste dos EUA (Norte da Virgínia). Para obter mais informações, consulte Creating an Amazon Data Firehose Delivery Stream.

   > **Important**
   >
   > Não escolha `Kinesis stream` como sua origem.
   > Um registro AWS WAF Classic é equivalente a um registro do Firehose. Se você normalmente recebe 10.000 solicitações por segundo e ativa registros completos, deve ter uma configuração de 10.000 registros por segundo no Firehose. Se você não configurar o Firehose corretamente, o AWS WAF Classic não gravará todos os registros. Para obter mais informações, consulte Cotas do Amazon Kinesis Data Firehose.

2. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.

3. No painel de navegação, selecione Web ACLs.
4. Selecione o nome da web ACL para a qual você deseja habilitar o registro em log. Isso abre uma página com os detalhes da web ACL no painel direito.
5. Na guia Registro em log, selecione Habilitar registro em log.
6. Habilite o Kinesis Data Firehose criado na primeira etapa. Você deve escolher uma mangueira de incêndio que comece com "aws-waf-logs-".
7. (Opcional) Se você não deseja que determinados campos e seus valores sejam incluídos nos logs, edite esses campos. Selecione o campo para editar e, em seguida, selecione Adicionar. Repita conforme necessário para editar campos adicionais. Os campos editados são exibidos como `REDACTED` nos logs. Por exemplo, se você editar o campo cookie, cookie ele será `REDACTED` nos logs.
8. Selecione Habilitar registro em log.

> **Note**
>
> Quando você habilita o registro com sucesso, o AWS WAF Classic cria uma função vinculada ao serviço com as permissões necessárias para gravar registros no Amazon Kinesis Data Firehose. Para ter mais informações, consulte Usando funções vinculadas a serviços para Classic AWS WAF.

Para desabilitar o registro em log de uma web ACL

1. No painel de navegação, selecione Web ACLs.
2. Selecione o nome da web ACL para a qual você deseja desabilitar o registro em log. Isso abre uma página com os detalhes da web ACL no painel direito.
3. Na guia Registro em log, selecione Desabilitar registro em log.
4. Na caixa de diálogo, selecione Desabilitar registro em log.

Example Log de exemplo

```
{
```

```
"timestamp":1533689070589,
"formatVersion":1,
"webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
"terminatingRuleId":"Default_Action",
"terminatingRuleType":"REGULAR",
"action":"ALLOW",
"httpSourceName":"CF",
"httpSourceId":"i-123",
"ruleGroupList":[
                        {
                         "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                         "terminatingRule":null,
                         "nonTerminatingMatchingRules":[
                                                         {"action" : "COUNT",
                                                         "ruleId" :
"4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                        ],
                         "excludedRules":               [
                                                         {"exclusionType" :
"EXCLUDED_AS_COUNT",
                                                          "ruleId" :
"5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                        ]
                        }
                       ],

"rateBasedRuleList":[
                            {
                             "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                             "limitKey":"IP",
                             "maxRateAllowed":100

                            },
                            {
                             "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                             "limitKey":"IP",
                             "maxRateAllowed":100
                             }
                             ],

"nonTerminatingMatchingRules":[
                                       {"action" : "COUNT",
```

```
                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                      ],

 "httpRequest":{
                       "clientIp":"192.10.23.23",

                       "country":"US",

                       "headers":[

                                  {
                                   "name":"Host",
                                   "value":"127.0.0.1:1989"
                                  },
                                  {
                                   "name":"User-Agent",
                                   "value":"curl/7.51.2"
                                  },
                                  {
                                   "name":"Accept",
                                   "value":"*/*"
                                  }
                                ],
                     "uri":"REDACTED",
                     "args":"usernam=abc",
                     "httpVersion":"HTTP/1.1",
                     "httpMethod":"GET",
                     "requestId":"cloud front Request id"
                     }
}
```


Veja a seguir uma explicação de cada item listado nesses logs:

timestamp

O timestamp em milissegundos.

formatVersion

A versão do formato do log.

webaclId

O GUID da web ACL.

terminatingRuleId

O ID da regra que encerrou a solicitação. Se nada encerrar a solicitação, o valor será `Default_Action`.

terminatingRuleType

O tipo de regra que encerrou a solicitação. Valores possíveis: RATE_BASED, REGULAR e GROUP.

ação

A ação. Os valores possíveis para uma regra de encerramento: ALLOW e BLOCK. COUNT não é um valor válido para o encerramento de uma regra.

terminatingRuleMatchDetalhes

Informações detalhadas sobre a regra de encerramento que correspondeu à solicitação. Uma regra de encerramento tem uma ação que encerra o processo de inspeção em relação a uma solicitação da Web. As ações possíveis para uma regra de encerramento são ALLOW e BLOCK. Isso é preenchido somente para instruções de regra de correspondência de injeção de SQL e cross-site scripting (XSS). Tal como acontece com todas as instruções de regra que inspecionam mais de uma coisa, o AWS WAF aplica a ação na primeira correspondência e para de inspecionar a solicitação da Web. Uma solicitação da Web com uma ação de encerramento pode conter outras ameaças, além da relatada no log.

httpSourceName

A origem da solicitação. Valores possíveis: CF (se a origem for Amazon CloudFront), APIGW (se a origem for Amazon API Gateway) e ALB (se a origem for um Application Load Balancer).

httpSourceId

O ID de origem. Esse campo mostra o ID da CloudFront distribuição associada da Amazon, a API REST para o API Gateway ou o nome de um Application Load Balancer.

ruleGroupList

A lista de grupos de regras que agiram nessa solicitação. No exemplo de código anterior, há apenas um.

ruleGroupId

O ID do grupo de regras. Se a regra bloqueou a solicitação, o ID para `ruleGroupID` será o mesmo que o ID para `terminatingRuleId`.

terminatingRule

A regra do grupo de regras que encerrou a solicitação. Se esse for um valor não nulo, ele também conterá um ruleid e uma action (ação). Nesse caso, a ação será sempre BLOCK.

nonTerminatingMatchingRegras

A lista de regras do grupo de regras que corresponde à solicitação. Elas sempre serão regras COUNT (regras correspondentes que não são de encerramento).

ação (grupo de nonTerminatingMatching regras)

Isso sempre será COUNT (regras correspondentes que não são de encerramento).

ruleID (grupo de regrasnonTerminatingMatching)

O ID da regra do grupo de regras que corresponde à solicitação e que não era de encerramento. Ou seja, regras COUNT.

excludedRules

A lista de regras no grupo de regras que você excluiu. A ação para essas regras é definida como COUNT.

exclusionType (grupo de excludedRules)

Um tipo que indica que a regra excluída tem a ação COUNT.

ruleId (grupo de excludedRules)

O ID da regra no grupo de regras que foi excluída.

rateBasedRuleLista

A lista de regras baseadas em taxas que agiram na solicitação.

rateBasedRuleIdentificação

O ID da regra baseada em taxa que agiu na solicitação. Se isso encerrou a solicitação, o ID para `rateBasedRuleId` será o mesmo que o ID para `terminatingRuleId`.

limitKey

O campo AWS WAF usado para determinar se as solicitações provavelmente estão chegando de uma única fonte e, portanto, estão sujeitas ao monitoramento de taxas. Valor possível: IP.

maxRateAllowed

O número máximo de solicitações, que têm o valor idêntico no campo que é especificado por `limitKey`, permitidas em um período de cinco minutos. Se o número de solicitações exceder o `maxRateAllowed` e os outros predicados especificados na regra também forem atendidos, AWS WAF acionará a ação especificada para essa regra.

httpRequest

Os metadados sobre a solicitação.

clientIp

O endereço IP do cliente que está enviando a solicitação.

country

O país de origem da solicitação. Se não AWS WAF for possível determinar o país de origem, ele definirá esse campo como`-`.

headers

A lista de cabeçalhos.

uri

O URI da solicitação. Este exemplo de código anterior demonstra qual seria o valor se esse campo tivesse sido editado.

args

A string de consulta.

httpVersion

A versão HTTP.

httpMethod

O método HTTP na solicitação.

requestId

O ID da solicitação.

Listagem de endereços IP bloqueados pelas regras baseadas em intervalo

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

AWS WAF O Classic fornece uma lista de endereços IP que são bloqueados por regras baseadas em taxas.

Para exibir os endereços bloqueados pelas regras baseadas em intervalos

1. Faça login no AWS Management Console e abra o AWS WAF console em https://console.aws.amazon.com/wafv2/.

   Se você ver Alternar para o AWS WAF clássico no painel de navegação, selecione-o.
2. No painel de navegação, escolha Regras.
3. Na coluna Nome, selecione uma regra baseada em intervalos.

   A lista mostra os endereços IP que a regra bloqueia no momento.

Como o AWS WAF Classic funciona com os CloudFront recursos da Amazon

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.

Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Ao criar uma ACL da web, você pode especificar uma ou mais CloudFront distribuições que você deseja que o AWS WAF Classic inspecione. AWS WAF O Classic começa a permitir, bloquear ou contar solicitações da web para essas distribuições com base nas condições que você identifica na ACL da web. CloudFront fornece alguns recursos que aprimoram a funcionalidade AWS WAF clássica. Este capítulo descreve algumas maneiras que você pode configurar CloudFront para fazer CloudFront com que o AWS WAF Classic funcione melhor em conjunto.

Tópicos

Usando o AWS WAF Classic com páginas de erro CloudFront personalizadas

Quando o AWS WAF Classic bloqueia uma solicitação da web com base nas condições que você especifica, ele retorna o código de status HTTP 403 (Proibido) para CloudFront. Em seguida, CloudFront retorna esse código de status para o visualizador. O visualizador em seguida exibirá uma breve mensagem padrão esparsamente formatada, semelhante à seguinte:

```
Forbidden: You don't have permission to access /myfilename.html on this
server.
```

Se você preferir exibir uma mensagem de erro personalizada, possivelmente usando a mesma formatação do resto do seu site, você pode configurar CloudFront para retornar ao visualizador um objeto (por exemplo, um arquivo HTML) que contém sua mensagem de erro personalizada.

> **Note**
>
> CloudFront não consigo distinguir entre um código de status HTTP 403 que é retornado por sua origem e um que é retornado pelo AWS WAF Classic quando uma solicitação

é bloqueada. Isso significa que você não pode retornar diferentes páginas de erro personalizadas com base em diferentes causas de um código de status HTTP 403.

Para obter mais informações sobre páginas de erro CloudFront personalizadas, consulte Personalização de respostas de erro no Amazon CloudFront Developer Guide.

Usando o AWS WAF Classic com CloudFront para aplicativos executados em seu próprio servidor HTTP

Ao usar o AWS WAF Classic with CloudFront, você pode proteger seus aplicativos em execução em qualquer servidor web HTTP, seja um servidor web executado no Amazon Elastic Compute Cloud (Amazon EC2) ou um servidor web que você gerencia de forma privada. Você também pode configurar CloudFront para exigir HTTPS CloudFront entre seu próprio servidor web, bem como entre visualizadores e. CloudFront

Exigindo HTTPS entre CloudFront e seu próprio servidor web

Para exigir HTTPS entre CloudFront e seu próprio servidor web, você pode usar o recurso de origem CloudFront personalizada e definir a Política de Protocolo de Origem e as configurações do Nome de Domínio de Origem para origens específicas. Na sua CloudFront configuração, você pode especificar o nome DNS do servidor junto com a porta e o protocolo que você deseja usar CloudFront ao buscar objetos da sua origem. Você também deve garantir que o certificado SSL/TLS no servidor da origem personalizada corresponda ao nome de domínio de origem configurado. Ao usar seu próprio servidor web HTTP fora do AWS, você deve usar um certificado assinado por uma autoridade de certificação (CA) terceirizada confiável, por exemplo, Comodo ou DigiCert Symantec. Para obter mais informações sobre a exigência de HTTPS para comunicação entre CloudFront e seu próprio servidor web, consulte o tópico Exigindo HTTPS para comunicação entre CloudFront e sua origem personalizada no Amazon CloudFront Developer Guide.

Exigindo HTTPS entre um visualizador e CloudFront

Para exigir HTTPS entre visualizadores e CloudFront, você pode alterar a Política de Protocolo do Visualizador para um ou mais comportamentos de cache em sua CloudFront distribuição. Para obter mais informações sobre o uso de HTTPS entre espectadores e CloudFront, consulte o tópico Exigindo HTTPS para comunicação entre espectadores e CloudFront no Amazon CloudFront Developer Guide. Você também pode trazer seu próprio certificado SSL para que os espectadores possam se conectar à sua CloudFront distribuição via HTTPS usando seu próprio nome de domínio,

por exemplo, https://www.mysite.com. Para obter mais informações, consulte o tópico Configurando nomes de domínio alternativos e HTTPS no Amazon CloudFront Developer Guide.

Escolhendo os métodos HTTP que CloudFront respondem a

Ao criar uma distribuição CloudFront web da Amazon, você escolhe os métodos HTTP que deseja CloudFront processar e encaminhar para sua origem. Você pode escolher entre as seguintes opções:

- GET, HEAD — Você pode usar CloudFront somente para obter objetos de sua origem ou para obter cabeçalhos de objetos.
- GET, HEAD, OPTIONS — Você pode usar CloudFront somente para obter objetos de sua origem, obter cabeçalhos de objetos ou recuperar uma lista das opções suportadas pelo seu servidor de origem.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE — Você pode usar CloudFront para obter, adicionar, atualizar e excluir objetos e obter cabeçalhos de objetos. Além disso, você pode executar outras operações de POST, como enviar dados de um formulário da web.

Você também pode usar as condições AWS WAF clássicas de correspondência de strings para permitir ou bloquear solicitações com base no método HTTP, conforme descrito emTrabalhar com condições de correspondência de string. Se você quiser usar uma combinação de métodos que CloudFront ofereça suporte, como `GET` e`HEAD`, não precisará configurar o AWS WAF Classic para bloquear solicitações que usam os outros métodos. Se você quiser permitir uma combinação de métodos que CloudFront não oferece suporte, como,, e `GET` `HEAD``POST`, você pode configurar CloudFront para responder a todos os métodos e, em seguida, usar o AWS WAF Classic para bloquear solicitações que usam outros métodos.

Para obter mais informações sobre como escolher os métodos que CloudFront respondem, consulte Métodos HTTP permitidos no tópico Valores que você especifica ao criar ou atualizar uma distribuição na Web no Amazon CloudFront Developer Guide.

Segurança no AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro

de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada 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 isto 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. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS WAF Classic, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, como a confidencialidade de seus dados, os requisitos da sua organização, leis e regulamentos aplicáveis.

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

Tópicos

Proteção de dados no AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no AWS WAF Classic. 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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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 os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- 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 sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais

informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AWS WAF Classic ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

AWS WAF Entidades clássicas, como ACLs, regras e condições da web, são criptografadas em repouso, exceto em determinadas regiões onde a criptografia não está disponível, incluindo China (Pequim) e China (Ningxia). Chaves de criptografia exclusivas são usadas para cada região.

Excluindo recursos do AWS WAF Classic

Você pode excluir os recursos que você cria no AWS WAF Classic. Consulte as orientações para cada tipo de recurso nas seções abaixo.

- Exclusão de uma ACL da web
- Adicionar e excluir regras de um grupo de regras AWS WAF clássico
- Como excluir uma regra

Gerenciamento de identidade e acesso para AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

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 WAF Classic. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AWS WAF Classic.

Usuário do serviço — Se você usa o serviço AWS WAF Classic para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos AWS WAF clássicos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS WAF Classic, consulte Solução de problemas de identidade e acesso AWS WAF clássicos.

Administrador de serviços — Se você é responsável pelos recursos do AWS WAF Classic em sua empresa, provavelmente tem acesso total ao AWS WAF Classic. É seu trabalho determinar quais recursos e recursos AWS WAF clássicos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o AWS WAF Classic, consulteComo o AWS WAF Classic funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AWS WAF Classic. Para ver exemplos de políticas AWS WAF clássicas baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF Classic

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). 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.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service

(Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

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.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do

usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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 o AWS WAF Classic funciona com o IAM

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

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

Recursos do IAM que você pode usar com o AWS WAF Classic

Atributo do IAM	AWS WAF Suporte clássico
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim

Atributo do IAM	AWS WAF Suporte clássico
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como o AWS WAF Classic 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.

Políticas baseadas em identidade para Classic AWS WAF

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para ver exemplos de políticas AWS WAF clássicas baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF Classic

Políticas baseadas em recursos no Classic AWS WAF

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AWS WAF Classic

Oferece compatibilidade 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações AWS WAF clássicas, consulte Ações definidas por AWS WAF e Ações definidas por AWS WAF Regional na Referência de Autorização de Serviço.

As ações de política no AWS WAF Classic usam o seguinte prefixo antes da ação:

```
waf
```

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

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações no AWS WAF Classic que começam com`List`, inclua a seguinte ação:

```
"Action": "waf:List*"
```

Para ver exemplos de políticas AWS WAF clássicas baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF Classic

Recursos de política para AWS WAF Classic

Oferece compatibilidade 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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver a lista de tipos de recursos AWS WAF clássicos e seus ARNs, consulte Recursos definidos por AWS WAF e Recursos definidos por AWS WAF regional na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas por AWS WAF e Ações definidas por AWS WAF Regional. Para permitir ou negar acesso a um subconjunto de recursos AWS WAF clássicos, inclua o ARN do recurso no elemento `resource` da sua política.

No AWS WAF Classic, os recursos são ACLs e regras da web. AWS WAF O Classic também oferece suporte a condições como correspondência de bytes, correspondência de IP e restrição de tamanho.

Esses recursos e condições têm nomes de recurso da Amazon (ARNs) exclusivos associados a eles, conforme mostrado na tabela a seguir.

Nome no AWS WAF console	Nome no AWS WAF SDK/CLI	Formato do ARN
Web ACL	`WebACL`	`arn:aws:waf::` *`account`*`:`*`webacl`*`/`*`ID`*
Regra	`Rule`	`arn:aws:waf::` *`account`*`:`*`rule`*`/`*`ID`*
Condição de correspondência de string	`ByteMatchSet`	`arn:aws:waf::` *`account`*`:`*`bytematchset`* `/`*`ID`*
SQL injection match condition	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:`*`sqlinjectionset`* `/`*`ID`*

Nome no AWS WAF console	Nome no AWS WAF SDK/CLI	Formato do ARN	
(condição de correspondência de injeção de SQL)			
Condição de restrição de tamanho	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:sizeconstraintset /`*`ID`*	
IP match condition (condição de correspondência de IP)	`IPSet`	`arn:aws:waf::` *`account`*`:ipset/`*`ID`	
Condição de correspondência de cross-site scripting	`XssMatchSet`	`arn:aws:waf::` *`account`*`:xssmatchset /`*`ID`	

Para permitir ou negar acesso a um subconjunto de recursos AWS WAF clássicos, inclua o ARN do recurso no elemento `resource` da sua política. Os ARNs do AWS WAF Classic têm o seguinte formato:

```
arn:aws:waf::account:resource/ID
```

Substitua as variáveis *`account`*, *`resource`* e *`ID`* por valores válidos. Os valores válidos podem ser os seguintes:

- *`conta`*: O ID do seu Conta da AWS. Você deve especificar um valor.
- *`recurso`*: o tipo de recurso AWS WAF clássico.

- *ID*: O ID do recurso AWS WAF clássico ou um curinga (*) para indicar todos os recursos do tipo especificado que estão associados ao especificado Conta da AWS.

Por exemplo, o ARN a seguir especifica todas as web ACLs para a conta 111122223333:

```
arn:aws:waf::111122223333:webacl/*
```

Chaves de condição de política para AWS WAF Classic

Suporta 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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 de chaves de condição AWS WAF clássicas, consulte Chaves de condição AWS WAF e recursos definidos por AWS WAF regional na Referência de autorização de serviço. Para

saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS WAF e Ações definidas por AWS WAF Regional.

Para ver exemplos de políticas AWS WAF clássicas baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS WAF Classic

ACLs no Classic AWS WAF

Oferece compatibilidade 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS WAF Classic

Oferece compatibilidade com ABAC (tags em políticas)	Parcial

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS WAF o Classic

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS WAF Classic

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída.

Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço para o AWS WAF Classic

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, 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 WAF Classic. Edite as funções de serviço somente quando o AWS WAF Classic fornecer orientação para fazer isso.

Funções vinculadas a serviços para Classic AWS WAF

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço AWS WAF Classic, consulte. Usando funções vinculadas a serviços para Classic AWS WAF

Exemplos de políticas baseadas em identidade para o AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos AWS WAF clássicos. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

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

Tópicos

- Práticas recomendadas de políticas
- Usando o console AWS WAF clássico
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos AWS WAF clássicos em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe 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 mais informações, 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 mais informações 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: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode 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 AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition 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 acionáveis para ajudar você a criar políticas seguras e funcionais. Para mais informações, 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 a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

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

Usando o console AWS WAF clássico

Para acessar o console AWS WAF clássico, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos AWS WAF clássicos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do 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 a operação de API que estiverem tentando executar.

Os usuários que podem acessar e usar o AWS console também podem acessar o console AWS WAF Clássico. Nenhuma permissão adicional é necessária.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

Solução de problemas de identidade e acesso AWS WAF clássicos

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

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

Tópicos

- Não estou autorizado a realizar uma ação no AWS WAF Classic
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS WAF Classic

Não estou autorizado a realizar uma ação no AWS WAF Classic

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 `waf:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `waf:`*`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 WAF Classic.

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 uma usuária do IAM chamada `marymajor` tenta usar o console para realizar uma ação no AWS WAF Classic. 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 acessem meus Conta da AWS recursos do AWS WAF Classic

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS WAF Classic oferece suporte a esses recursos, consulteComo o AWS WAF Classic 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Usando funções vinculadas a serviços para Classic AWS WAF

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

AWS WAF Funções vinculadas ao serviço Classic Usa AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao

AWS WAF Classic. As funções vinculadas ao serviço são predefinidas pelo AWS WAF Classic e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS WAF Classic porque você não precisa adicionar manualmente as permissões necessárias. AWS WAF O Classic define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o AWS WAF Classic pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

É possível excluir uma função vinculada ao serviço somente depois de excluir os recursos relacionados da função. Isso protege seus recursos AWS WAF clássicos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculada a serviço para o AWS WAF Classic

AWS WAF O Classic usa as seguintes funções vinculadas ao serviço:

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF O Classic usa essas funções vinculadas ao serviço para gravar registros no Amazon Data Firehose. Essas funções são usadas somente se você ativar o login AWS WAF. Para ter mais informações, consulte Registrar em log as informações de tráfego da web ACL.

As funções vinculadas a serviços `AWSServiceRoleForWAFLogging` e `AWSServiceRoleForWAFRegionalLogging` confiam nos seguintes serviços (respectivamente) para assumir a função:

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

As políticas de permissões das funções permitem que o AWS WAF Classic conclua as seguintes ações nos recursos especificados:

- Ação: `firehose:PutRecord` e `firehose:PutRecordBatch` no Amazon Data Firehose, recursos de fluxo de dados com um nome que começa com "aws-waf-logs-". Por exemplo, `aws-waf-logs-us-east-2-analytics`.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de função vinculada a serviço no Guia do usuário do IAM.

Criação de função vinculada a serviço para o AWS WAF Classic

Não é necessário criar manualmente uma função vinculada a serviço. Quando você ativa o registro AWS WAF clássico no AWS Management Console, ou faz uma `PutLoggingConfiguration` solicitação na CLI clássica ou na API AWS WAF clássica, AWS WAF o AWS WAF Classic cria a função vinculada ao serviço para você.

Você deve ter a permissão `iam:CreateServiceLinkedRole` para habilitar o registro em log.

Se excluir essa função vinculada a serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você ativa o registro AWS WAF clássico, o AWS WAF Classic cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada a serviço para o AWS WAF Classic

AWS WAF O Classic não permite que você edite as funções `AWSServiceRoleForWAFLogging` `AWSServiceRoleForWAFRegionalLogging` vinculadas 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 obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Exclusão de uma função vinculada a serviço para o AWS WAF Classic

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço AWS WAF Classic estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos AWS WAF clássicos usados pelo **`AWSServiceRoleForWAFLogging`** e **`AWSServiceRoleForWAFRegionalLogging`**

1. No console AWS WAF clássico, remova o registro de cada ACL da web. Para ter mais informações, consulte Registrar em log as informações de tráfego da web ACL.
2. Usando a API ou a CLI, envie uma solicitação `DeleteLoggingConfiguration` para cada web ACL que tem o registro em log habilitado. Para obter mais informações, consulte Referência da API do AWS WAF Classic.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir funções vinculadas a serviços `AWSServiceRoleForWAFLogging` e `AWSServiceRoleForWAFRegionalLogging`. Para obter mais informações, consulte Excluir uma função vinculada a serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas a serviços do AWS WAF Classic

AWS WAF O Classic oferece suporte ao uso de funções vinculadas a serviços a seguir. Regiões da AWS

Nome da região	Identidade da região	Support no AWS WAF Classic
Leste dos EUA (Norte da Virgínia)	`us-east-1`	Sim
Leste dos EUA (Ohio)	`us-east-2`	Sim
Oeste dos EUA (N. da Califórnia)	`us-west-1`	Sim
Oeste dos EUA (Oregon)	`us-west-2`	Sim
Ásia-Pacífico (Mumbai)	`ap-south-1`	Sim

Nome da região	Identidade da região	Support no AWS WAF Classic
Asia Pacific (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim
Europa (Paris)	eu-west-3	Sim
América do Sul (São Paulo)	sa-east-1	Sim

Registro e monitoramento no AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS WAF Classic e de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus recursos do AWS WAF Classic e responder a possíveis eventos:

CloudWatch Alarmes da Amazon

Usando CloudWatch alarmes, você observa uma única métrica durante um período de tempo especificado por você. Se a métrica exceder um determinado limite, CloudWatch envia uma notificação para um tópico AWS Auto Scaling ou política do Amazon SNS. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no AWS WAF Classic. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao AWS WAF Classic, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Registro de chamadas de API do AWS CloudTrail com.

Validação de conformidade para AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

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. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no clássico AWS WAF

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

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 executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

Segurança de infraestrutura no AWS WAF Classic

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

Como um serviço gerenciado, o AWS WAF Classic é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o AWS WAF Classic pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

AWS WAF Cotas clássicas

> **Note**
>
> Essa é a documentação do AWS WAF Classic. Você só deve usar essa versão se tiver criado AWS WAF recursos, como regras e ACLs da web, AWS WAF antes de novembro de 2019 e ainda não os tiver migrado para a versão mais recente. Para migrar os recursos, consulte Migrando seus recursos AWS WAF clássicos para AWS WAF.
> Para obter a versão mais recente do AWS WAF, consulteAWS WAF.

AWS WAF O Classic está sujeito às seguintes cotas (anteriormente chamadas de limites).

AWS WAF O Classic tem cotas padrão sobre o número de entidades por conta por região. Você pode solicitar um aumento para elas.

Recurso	Cota padrão por conta por região
Web ACLs	50
Regras	100

Recurso	Cota padrão por conta por região
R ate-based-rules	5
Condições por conta da por região	Para todas as condições , exceto para correspondência de regex e correspondência geográfica, 100 de cada tipo de condição. Por exemplo: 100 condições de restrição de tamanho e 100 condições de correspon dência de IP. Para condições de correspon dência geográfic a e de regex, consulte a tabela abaixo.
Solicitações por segundo	25.000 por web ACL*

*Essa cota se aplica somente ao AWS WAF Classic em um Application Load Balancer. As cotas de solicitações por segundo (RPS) para AWS WAF Classic on CloudFront são iguais às cotas de RPS suportadas, conforme descrito no CloudFront Guia do desenvolvedor. CloudFront

As cotas a seguir em entidades AWS WAF clássicas não podem ser alteradas.

Recurso	Cotas por conta por região
Grupos de regras por web ACL	2:1 grupo de regras criado pelo cliente e 1 AWS Marketplace grupo de regras
Regras por web ACL	10
Condições por regra	10
intervalos de endereços IP (em notação CIDR) por condição de correspondência de IP	10.000 Você pode atualizar até 1.000 endereços por vez. A chamada de API `UpdateIPSet` aceita no máximo 1.000 endereços em uma única solicitação.
Endereços de IP bloqueadas por regra baseada em intervalos	10.000
Limite de taxa mínimo da regra baseada em intervalos por período de cinco minutos	100
Filtros por condição de correspondência de script entre sites	10
Filtros por condição de restrição de tamanho	10
Filtros por condição de correspondência de injeção de SQL	10

Recurso	Cotas por conta por região
Filtros por condição de correspondência de sequência	10
Em condições de correspondência de strings, o número de caracteres nos nomes dos cabeçalhos HTTP, quando você configura o AWS WAF Classic para inspecionar os cabeçalhos nas solicitações da Web em busca de um valor especificado	40
Em condições de correspondência de strings, o número de caracteres no valor que você deseja que o AWS WAF Classic pesquise	50
Condições de correspondência regex	10
Em condições de correspondência de regex, o número de caracteres no padrão que você deseja que o AWS WAF Classic pesquise	70
Em condições de correspondência regex, o número de padrões por conjunto padrão	10
Em condições de correspondência regex, o número de conjuntos de padrões por condição regex	1
Conjuntos de padrões	5
Condições de correspondência geográfica	50
Localizações por condição de correspondência geográfica	50

AWS WAF O Classic tem as seguintes cotas fixas de chamadas por conta por região. Essas cotas se aplicam ao total de chamadas para o serviço por qualquer meio disponível, incluindo o console, a CLI AWS CloudFormation, a API REST e os SDKs. Essas cotas não podem ser alteradas.

Tipo de chamada	Cotas por conta por região
Número máximo de chamadas para `AssociateWebACL`	1 pedido a cada 2 segundos
Número máximo de chamadas para `DisassociateWebACL`	1 pedido a cada 2 segundos
Número máximo de chamadas para `GetWebACLForResource`	1 pedido por segundo
Número máximo de chamadas para `ListResourcesForWebACL`	1 pedido por segundo
Número máximo de chamadas para `CreateWebACLMigrationStack`	1 pedido por segundo
Número máximo de chamadas para `GetChangeToken`	10 solicitações por segundo
Número máximo de chamadas para `GetChangeTokenStatus`	1 pedido por segundo
Número máximo de chamadas para qualquer ação `List` individual, se nenhuma outra cota for definida para ela	5 solicitações por segundo
Número máximo de chamadas para qualquer ação `Create`, `Put`, `Get`, ou `Update` individual, se nenhuma outra cota for definida para ela	1 pedido por segundo

AWS Shield

A proteção contra ataques do tipo negação de serviço distribuída (Distributed Denial of Service, DDoS) é de fundamental importância para seus aplicativos voltados para a Internet. Ao criar seu aplicativo AWS, você pode usar proteções AWS sem custo adicional. Além disso, você pode usar o serviço AWS Shield Advanced gerenciado de proteção contra ameaças para melhorar sua postura de segurança com recursos adicionais de detecção, mitigação e resposta de DDoS.

AWS tem o compromisso de fornecer a você as ferramentas, as melhores práticas e os serviços para ajudar a garantir alta disponibilidade, segurança e resiliência em sua defesa contra agentes mal-intencionados na Internet. Este guia é fornecido para ajudar os tomadores de decisão de TI e engenheiros de segurança a entender como usar o Shield e o Shield Advanced para proteger melhor seus aplicativos contra ataques de DDoS e outras ameaças externas.

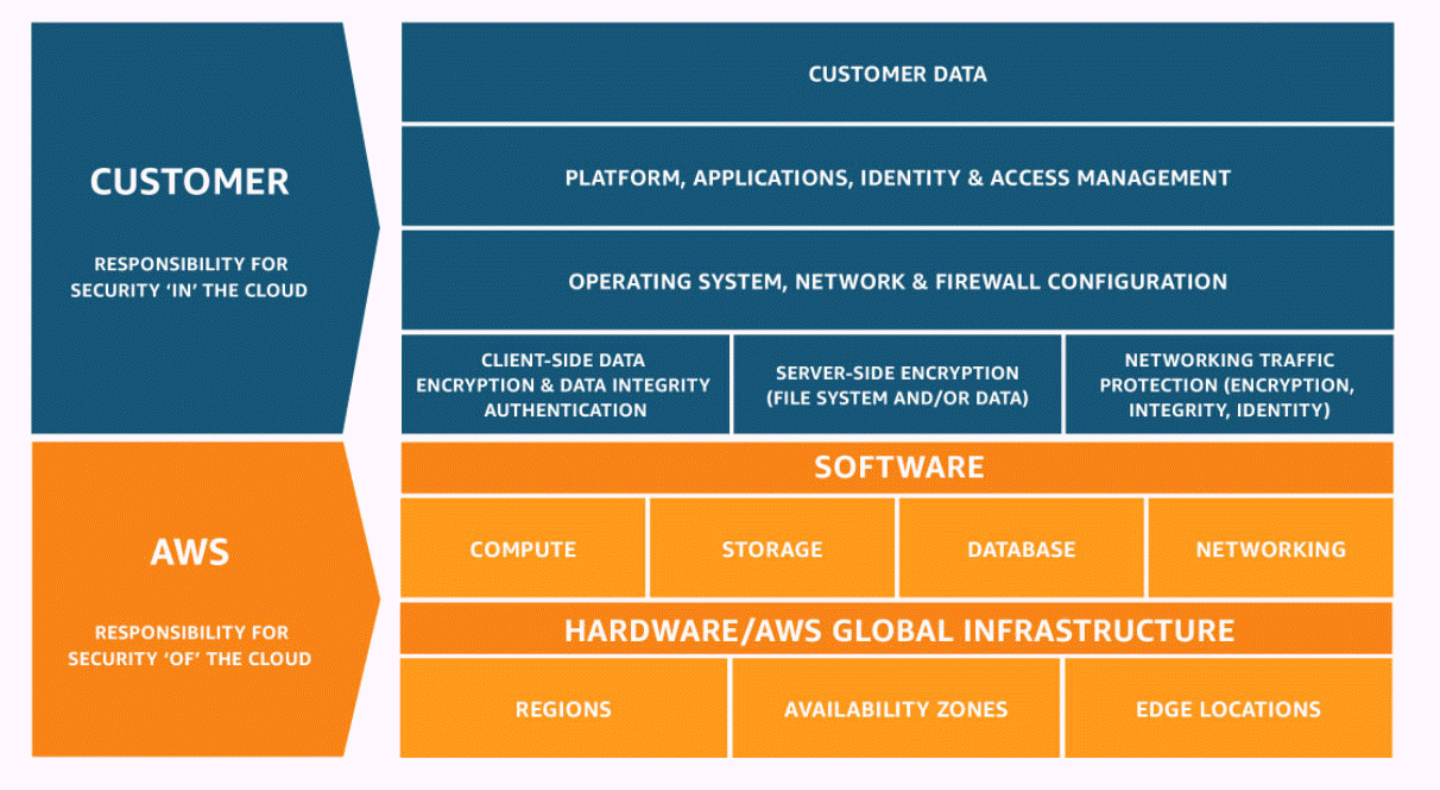
Ao criar seu aplicativo AWS, você recebe proteção automática AWS contra vetores de ataque DDoS volumétricos comuns, como ataques de reflexão UDP e inundações de TCP SYN. Você pode aproveitar essas proteções para garantir a disponibilidade dos aplicativos em AWS que você executa projetando e configurando sua arquitetura para resiliência de DDoS.

Este guia fornece recomendações que podem ajudá-lo a projetar, criar e configurar suas arquiteturas de aplicativos para resiliência de DDoS. Os aplicativos que seguem as práticas recomendadas fornecidas neste guia podem se beneficiar de uma maior continuidade de disponibilidade quando são alvo de ataques maiores de DDoS e de uma variedade maior de vetores de ataque de DDoS. Além disso, este guia mostra como usar o Shield Advanced para implementar uma postura otimizada de proteção contra DDoS para seus aplicativos críticos. Isso inclui aplicativos para os quais você garantiu um certo nível de disponibilidade para seus clientes e aqueles que exigem suporte operacional AWS durante eventos de DDoS.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto 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. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Shield Advanced, consulte Serviços da AWS no escopo pelo programa de conformidade.

- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, como a confidencialidade de seus dados, os requisitos da sua organização, leis e regulamentos aplicáveis.



Como o AWS Shield Shield Advanced funcionam

AWS Shield Standard e AWS Shield Advanced forneça proteções contra ataques de negação de serviço distribuído (DDoS) para AWS recursos nas camadas de rede e transporte (camadas 3 e 4) e na camada de aplicação (camada 7). Um ataque de DDoS é um ataque no qual vários sistemas comprometidos tentam inundar um alvo com tráfego. Um ataque DDoS pode evitar que usuários legítimos acessem um serviço e pode fazer com que o sistema falhe por conta do grande volume de tráfego.

AWS Shield fornece proteção contra uma ampla variedade de vetores de ataque DDoS e vetores de ataque de dia zero conhecidos. A detecção e mitigação do Shield foram projetadas para fornecer cobertura contra ameaças, mesmo que elas não sejam explicitamente conhecidas pelo serviço no momento da detecção. O Shield Básico é fornecido automaticamente e sem custos adicionais quando você usa a AWS.

As classes de ataques que o Shield detecta incluem as seguintes:

- Ataques volumétricos de rede (camada 3): essa é uma subcategoria de vetores de ataque da camada de infraestrutura. Esses vetores tentam saturar a capacidade da rede ou do recurso-alvo, para negar o serviço a usuários legítimos.
- Ataques de protocolo de rede (camada 4): essa é uma subcategoria de vetores de ataque da camada de infraestrutura. Esses vetores abusam de um protocolo para negar serviço ao recurso-alvo. Um exemplo comum de ataque de protocolo de rede é um flood TCP SYN, que pode esgotar o estado da conexão em recursos como servidores, balanceadores de carga ou firewalls. Um ataque de protocolo de rede também pode ser volumétrico. Por exemplo, um flood TCP SYN maior pode ter a intenção de saturar a capacidade de uma rede e, ao mesmo tempo, esgotar o estado do recurso-alvo ou dos recursos intermediários.
- Ataques na camada de aplicação (camada 7): essa categoria de vetor de ataque tenta negar serviço a usuários legítimos inundando um aplicativo com consultas válidas para o alvo, como inundações de solicitações da web.

Sumário

- AWS Shield Advanced lógica de mitigação para aplicativos web

AWS Shield Standard visão geral

AWS Shield é um serviço gerenciado de proteção contra ameaças que protege o perímetro do seu aplicativo. O perímetro é o primeiro ponto de entrada para o tráfego de aplicativos vindo de fora da AWS rede.

Para determinar qual é o perímetro do seu aplicativo, considere como os usuários acessam seu aplicativo pela internet. Se o primeiro ponto de entrada estiver em uma AWS região, o perímetro do aplicativo será sua Amazon Virtual Private Cloud (VPC). Se os usuários forem direcionados ao seu aplicativo pelo Amazon Route 53 e acessarem primeiro o aplicativo usando o Amazon CloudFront ou AWS Global Accelerator, o perímetro do aplicativo começará na borda da AWS rede.

O Shield fornece benefícios de detecção e mitigação de DDoS para todos os aplicativos em execução AWS, mas as decisões que você toma ao projetar sua arquitetura de aplicativos influenciarão seu nível de resiliência de DDoS. A resiliência de DDoS é a capacidade do seu aplicativo de continuar operando dentro dos parâmetros esperados durante um ataque.

Todos os AWS clientes se beneficiam da proteção automática do Shield Standard, sem custo adicional. O Shield Standard oferece defesa contra a maioria dos frequentes ataques de DDoS à camada de transporte e de rede que alvejam seus sites ou aplicativos. Embora o Shield Standard ajude a proteger todos os AWS clientes, você obtém benefícios especiais com as zonas hospedadas do Amazon Route 53, CloudFront as distribuições da Amazon e os aceleradores AWS Global Accelerator padrão. Esses recursos recebem proteção abrangente de disponibilidade contra todos os ataques conhecidos das camadas de rede e transporte.

AWS Shield Advanced visão geral

AWS Shield Advanced é um serviço gerenciado que ajuda você a proteger seu aplicativo contra ameaças externas, como ataques de DDoS, bots volumétricos e tentativas de exploração de vulnerabilidades. Para níveis mais altos de proteção contra ataques, você pode se inscrever no AWS Shield Advanced.

Quando você assina o Shield Advanced e adiciona proteção aos seus recursos, o Shield Advanced fornece proteção expandida contra ataques de DDoS para esses recursos. As proteções que você recebe do Shield Advanced podem variar dependendo de suas opções de arquitetura e configuração. Use as informações deste guia para criar e proteger aplicativos resilientes usando o Shield Advanced e para encaminhar quando precisar de ajuda especializada.

Assinaturas e custos do Shield Advanced AWS WAF

Sua assinatura do Shield Advanced cobre os custos de uso dos AWS WAF recursos padrão dos recursos que você protege com o Shield Advanced. As AWS WAF taxas padrão cobertas pelas proteções Shield Advanced são o custo por ACL da web, o custo por regra e o preço base por milhão de solicitações para inspeção de solicitações da web, até 1.500 WCUs e até o tamanho padrão do corpo.

A ativação da mitigação automática de DDoS na camada de aplicação do Shield Advanced adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced, O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).

Sua assinatura do Shield Advanced não cobre o uso AWS WAF de recursos que você não protege usando o Shield Advanced. Também não cobre nenhum custo adicional não padronizado AWS WAF para recursos protegidos. Exemplos de AWS WAF custos não padrão são aqueles para o Bot Control, para a ação da CAPTCHA regra, para ACLs da web que usam mais de 1.500 WCUs e para inspecionar o corpo da solicitação além do tamanho padrão. A lista completa é fornecida na página AWS WAF de preços.

Para obter informações completas e exemplos de preços, consulte Preços do Shield e Preços do AWS WAF.

Cobrança da assinatura do Shield Advanced

Se você for um revendedor de AWS canais, fale com a equipe da sua conta para obter informações e orientações. Essas informações de cobrança são para clientes que não são revendedores de AWS canais.

Para todos os outros, as seguintes diretrizes de assinatura e cobrança se aplicam:

- Para contas que são membros de uma AWS Organizations organização, AWS as assinaturas do Shield Advanced são cobradas da conta pagante da organização, independentemente de a própria conta do pagador estar assinada.
- Quando você assina várias contas que estão na mesma família AWS Organizations de contas de faturamento consolidado, um preço de assinatura cobre todas as contas inscritas na família. A organização deve possuir todas as Contas da AWS e todos os seus recursos.
- Ao assinar várias contas para várias organizações, você ainda pode pagar uma taxa de assinatura em todas as organizações, contas e recursos, desde que seja proprietário de todas elas. Entre

em contato com seu gerente de conta ou AWS suporte e solicite uma isenção de taxa sobre as cobranças de AWS Shield Advanced assinatura para todas as organizações, exceto uma.

Para obter informações detalhadas sobre preços e exemplos, consulte Preços do AWS Shield.

Tópicos

- AWS Shield Advanced recursos protegidos
- AWS Shield Advanced capacidades e opções
- Como decidir se deseja assinar o AWS Shield Advanced e aplicar proteções adicionais

AWS Shield Advanced recursos protegidos

> **Note**
>
> As proteções Shield Advanced só estão habilitadas para recursos que você especificou explicitamente no Shield Advanced ou que você protege por meio de uma política AWS Firewall Manager Shield Advanced. O Shield Advanced não protege automaticamente seus recursos.

Você pode usar o Shield Advanced para monitoramento e proteção avançados com os seguintes tipos de recursos:

- CloudFront Distribuições da Amazon. Para implantação CloudFront contínua, o Shield Advanced protege qualquer distribuição temporária associada a uma distribuição primária protegida.
- Zonas hospedadas do Amazon Route 53.
- AWS Global Accelerator aceleradores padrão.
- Endereços de IP elástico do Amazon EC2. O Shield Advanced protege os recursos associados aos endereços IP elásticos protegidos.
- Instâncias do Amazon EC2, por meio de associação com endereços IP elásticos do Amazon EC2.
- Os seguintes balanceadores de carga do Elastic Load Balancing (ELB):
  - Application Load Balancers.
  - Classic Load Balancers.
  - Network Load Balancers, por meio de associações com endereços IP elásticos do Amazon EC2.

Para obter informações adicionais sobre proteções para esses tipos de recursos, consulte AWS Shield Advanced proteções por tipo de recurso.

AWS Shield Advanced capacidades e opções

AWS Shield Advanced a assinatura inclui os seguintes recursos e opções. Eles complementam os recursos de detecção e mitigação de DDoS que você já recebe. AWS

- AWS WAF integração — o Shield Advanced usa ACLs, regras e grupos de regras da AWS WAF web como parte das proteções da camada de aplicação. Para obter mais informações sobre AWS WAF, consulteComo AWS WAF funciona.

  > **Note**
  >
  > Sua assinatura do Shield Advanced cobre os custos de uso dos AWS WAF recursos padrão dos recursos que você protege com o Shield Advanced. As AWS WAF taxas padrão cobertas pelas proteções Shield Advanced são o custo por ACL da web, o custo por regra e o preço base por milhão de solicitações para inspeção de solicitações da web, até 1.500 WCUs e até o tamanho padrão do corpo.
  >
  > A ativação da mitigação automática de DDoS na camada de aplicação do Shield Advanced adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced, O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).
  >
  > Sua assinatura do Shield Advanced não cobre o uso AWS WAF de recursos que você não protege usando o Shield Advanced. Também não cobre nenhum custo adicional não padronizado AWS WAF para recursos protegidos. Exemplos de AWS WAF custos não padrão são aqueles para o Bot Control, para a ação da CAPTCHA regra, para ACLs da web que usam mais de 1.500 WCUs e para inspecionar o corpo da solicitação além do tamanho padrão. A lista completa é fornecida na página AWS WAF de preços.
  >
  > Para obter informações completas e exemplos de preços, consulte Preços do Shield e Preços do AWS WAF.

- Mitigação automática de DDoS na camada de aplicação: você pode configurar o Shield Advanced para responder automaticamente para mitigar os ataques da camada de aplicação (camada 7) contra seus recursos protegidos. Com a mitigação automática, o Shield Advanced impõe a limitação AWS WAF de taxa nas solicitações de fontes conhecidas de DDoS e adiciona e gerencia

automaticamente AWS WAF proteções personalizadas em resposta aos ataques de DDoS detectados. Você pode configurar a mitigação automática para contar ou bloquear as solicitações da web que fazem parte de um ataque.

Para ter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

- Detecção baseada em integridade: você pode usar as verificações de integridade do Amazon Route 53 com o Shield Advanced para informar a detecção e mitigação de eventos. As verificações de integridade monitoram seu aplicativo de acordo com suas especificações, relatando integridade quando suas especificações são atendidas e não integridade quando não são. O uso de verificações de integridade com o Shield Advanced ajuda a evitar falsos positivos e fornece detecção e mitigação mais rápidas quando um recurso protegido não está íntegro. Você pode usar a detecção baseada em integridade para qualquer tipo de recurso, exceto as zonas hospedadas do Route 53. O engajamento proativo do Shield Advanced está disponível somente para recursos que tenham a detecção baseada em saúde habilitada.

  Para ter mais informações, consulte Detecção baseada em saúde usando verificações de saúde.
- Grupos de proteção: você pode usar grupos de proteção para criar agrupamentos lógicos de seus recursos protegidos, para melhorar a detecção e a mitigação do grupo como um todo. Você pode definir os critérios de participação em um grupo de proteção para que os recursos recém-protegidos sejam incluídos automaticamente. Um recurso protegido pode pertencer a vários grupos de proteção.

  Para ter mais informações, consulte AWS Shield Advanced grupos de proteção.
- Visibilidade aprimorada de eventos e ataques de DDoS: o Shield Advanced fornece acesso a métricas e relatórios avançados em tempo real para ampla visibilidade de eventos e ataques aos seus recursos da AWS protegidos. Você pode acessar essas informações por meio da API e do console Shield Advanced e por meio das CloudWatch métricas da Amazon.

  Para ter mais informações, consulte Visibilidade de eventos de DDoS.
- Gerenciamento centralizado das proteções do Shield Advanced por AWS Firewall Manager: você pode usar o Firewall Manager para aplicar automaticamente as proteções do Shield Advanced às suas novas contas e recursos e para implantar regras do AWS WAF em suas web ACLs. As políticas de proteção do Shield Advanced para o Firewall Manager estão incluídas sem custo adicional para os clientes do Shield Advanced. Você também pode centralizar as atividades de monitoramento do Shield Advanced para suas contas usando o Firewall Manager com um tópico do Amazon Simple Notification Service (SNS) ou do AWS Security Hub.

Para obter mais informações sobre o uso do Firewall Manager para gerenciar as proteções do Shield Advanced, consulte AWS Firewall Manager e AWS Shield Advanced políticas. Para obter informações sobre a definição de preço de solicitações, consulte Preços do AWS Firewall Manager.

- AWS Shield Response Team (SRT) — A SRT tem profunda experiência em proteger AWS a Amazon.com e suas subsidiárias. Como cliente do AWS Shield Advanced , você pode entrar em contato com a SRT a qualquer momento para obter assistência durante um ataque de DDoS que afete a disponibilidade do seu aplicativo. Você também pode trabalhar com a SRT para criar e gerenciar mitigações personalizadas para seus recursos. Para usar os serviços da DRT, você deve ser assinante do plano Business Support ou Enterprise Support.

  Para ter mais informações, consulte Suporte do Shield Response Team (SRT).
- Envolvimento proativo: com envolvimento proativo, o Shield Response Team (SRT) entrará em contato diretamente com você se a verificação de integridade do Amazon Route 53 associada ao seu recurso protegido tornar-se não íntegra durante um evento detectado pelo Shield Advanced. Isso permite que você interaja com especialistas mais rapidamente quando a disponibilidade do seu aplicativo puder ser afetada por um ataque suspeito.

  Para ter mais informações, consulte Como configurar o engajamento proativo.
- Oportunidades de proteção de custos — O Shield Advanced oferece alguma proteção de custo contra picos em sua AWS fatura que podem resultar de um ataque de DDoS contra seus recursos protegidos. Isso pode incluir cobertura para picos nas taxas de uso de transferência de dados (DTO) do Shield Advanced. O Shield Advanced fornece qualquer proteção de custo na forma de créditos de serviço do Shield Advanced.

  Para ter mais informações, consulte Solicitando um crédito em AWS Shield Advanced.

Como decidir se deseja assinar o AWS Shield Advanced e aplicar proteções adicionais

Analise os cenários desta seção para obter ajuda para decidir quais contas inscrever no AWS Shield Advanced e onde aplicar proteções adicionais. Com o Shield Advanced, você paga uma taxa de assinatura mensal para todas as contas criadas em uma conta de cobrança consolidada, além de taxas de uso com base em GB de dados transferidos. Para obter informações sobre os preços do Shield Advanced, consulte Preços do AWS Shield Advanced.

Para proteger um aplicativo e seus recursos com o Shield Advanced, você inscreve as contas que gerenciam o aplicativo no Shield Advanced e, em seguida, adiciona proteções aos recursos

do aplicativo. Para obter informações sobre como inscrever contas e proteger recursos, consulte Começando com AWS Shield Advanced.

Assinaturas e custos do Shield Advanced AWS WAF

Sua assinatura do Shield Advanced cobre os custos de uso dos AWS WAF recursos padrão dos recursos que você protege com o Shield Advanced. As AWS WAF taxas padrão cobertas pelas proteções Shield Advanced são o custo por ACL da web, o custo por regra e o preço base por milhão de solicitações para inspeção de solicitações da web, até 1.500 WCUs e até o tamanho padrão do corpo.

A ativação da mitigação automática de DDoS na camada de aplicação do Shield Advanced adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced, O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).

Sua assinatura do Shield Advanced não cobre o uso AWS WAF de recursos que você não protege usando o Shield Advanced. Também não cobre nenhum custo adicional não padronizado AWS WAF para recursos protegidos. Exemplos de AWS WAF custos não padrão são aqueles para o Bot Control, para a ação da CAPTCHA regra, para ACLs da web que usam mais de 1.500 WCUs e para inspecionar o corpo da solicitação além do tamanho padrão. A lista completa é fornecida na página AWS WAF de preços.

Para obter informações completas e exemplos de preços, consulte Preços do Shield e Preços do AWS WAF.

Cobrança da assinatura do Shield Advanced

Se você for um revendedor de AWS canais, fale com a equipe da sua conta para obter informações e orientações. Essas informações de cobrança são para clientes que não são revendedores de AWS canais.

Para todos os outros, as seguintes diretrizes de assinatura e cobrança se aplicam:

- Para contas que são membros de uma AWS Organizations organização, AWS as assinaturas do Shield Advanced são cobradas da conta pagante da organização, independentemente de a própria conta do pagador estar assinada.

- Quando você assina várias contas que estão na mesma família AWS Organizations de contas de faturamento consolidado, um preço de assinatura cobre todas as contas inscritas na família. A organização deve possuir todas as Contas da AWS e todos os seus recursos.
- Ao assinar várias contas para várias organizações, você ainda pode pagar uma taxa de assinatura em todas as organizações, contas e recursos, desde que seja proprietário de todas elas. Entre em contato com seu gerente de conta ou AWS suporte e solicite uma isenção de taxa sobre as cobranças de AWS Shield Advanced assinatura para todas as organizações, exceto uma.

Para obter informações detalhadas sobre preços e exemplos, consulte Preços do AWS Shield.

Identificação dos aplicativos a serem protegidos

Considere a implementação das proteções do Shield Advanced para aplicativos em que você precisa de qualquer um dos seguintes:

- Disponibilidade garantida para os usuários do aplicativo.
- Acesso rápido a especialistas em mitigação de DDoS se o aplicativo for afetado por um ataque de DDoS.
- Conscientização de AWS que o aplicativo pode ser afetado por um ataque de DDoS e notificação de ataques AWS e escalonamento para suas equipes de segurança ou operações.
- Previsibilidade nos custos da nuvem, inclusive quando um ataque de DDoS afeta o uso dos serviços da AWS .

Se um aplicativo ou seus recursos exigirem alguma das opções acima, considere criar assinaturas para as contas relacionadas.

Identificando os recursos a serem protegidos

Para cada conta inscrita, considere adicionar uma proteção do Shield Advanced a cada recurso que tenha qualquer uma das seguintes características:

- O recurso atende usuários externos na internet.
- O recurso está exposto à internet e também faz parte de um aplicativo crítico. Considere cada recurso exposto, independentemente de você pretender que seja acessado por usuários na internet.
- O recurso é protegido por uma AWS WAF Web ACL.

Para saber mais sobre como criar e gerenciar proteções para seus recursos, consulte Proteções de recursos em AWS Shield Advanced.

Além disso, siga as recomendações deste guia para ajudar a garantir que você arquitete seu aplicativo para resiliência de DDoS e tenha configurado adequadamente os atributos do Shield Advanced para obter proteções ideais.

Tipos de ataques DDoS

AWS Shield Advanced fornece proteção expandida contra vários tipos de ataques.

A lista a seguir descreve alguns tipos de ataques comuns:

Ataques de reflexão de UDP

Em ataques de reflexão UDP, um invasor pode fazer o spoofing da origem de uma solicitação e usar UDP para obter uma grande resposta do servidor. O tráfego de rede extra direcionado para o endereço IP atacado mascarado pode deixar o servidor de destino mais lento e evitar que usuários legítimos acessem os recursos necessários.

flood TCP SYN

O objetivo de um ataque SYN é esgotar os recursos disponíveis de um sistema, deixando conexões em estado meio aberto. Quando um usuário se conecta a um serviço de TCP, como um servidor web, o cliente envia um pacote SYN. O servidor retorna a confirmação e o cliente retorna sua própria confirmação, concluindo um handshake de três vias. Em um flood TCP SYN, a terceira confirmação nunca é retornada e o servidor fica aguardando uma resposta. Isso pode impedir que outros usuários se conectem ao servidor.

DNS query flood

Em uma inundação de consultas de DNS, um invasor usa várias consultas de DNS para esgotar os recursos de um servidor DNS. AWS Shield Advanced pode ajudar a fornecer proteção contra ataques de inundação de consultas de DNS nos servidores DNS do Route 53.

Ataques de HTTP flood/cache busting (camada 7)

Com um HTTP flood, incluindo floods `GET` e `POST`, um invasor envia várias solicitações HTTP que parecem ser de um usuário real do aplicativo web. Ataques cache busting são um tipo de HTTP flood que usa variações na string de consulta HTTP que impede o uso de conteúdo em cache localizado no edge e força o conteúdo a ser servido pelo servidor da web de origem, causando esforço adicional e potencialmente prejudicial no servidor web de origem.

Como AWS Shield detecta eventos

AWS opera sistemas de detecção de nível de serviço para a AWS rede e AWS serviços individuais, para garantir que eles permaneçam disponíveis durante um ataque de DDoS. Além disso, os sistemas de detecção em nível de recurso monitoram cada AWS recurso individual para garantir que o tráfego em direção ao recurso permaneça dentro dos parâmetros esperados. Essa combinação protege o AWS recurso e os AWS serviços direcionados, aplicando mitigações que eliminam pacotes inválidos conhecidos, destacam o tráfego potencialmente malicioso e priorizam o tráfego dos usuários finais.

Os eventos detectados aparecem nos resumos de eventos, nos detalhes do ataque e nas CloudWatch métricas da Amazon do Shield Advanced como o nome do vetor de ataque de DDoS ou como `Volumetric` se a avaliação fosse baseada no volume de tráfego em vez da assinatura. Para obter mais informações sobre as dimensões do vetor de ataque que estão disponíveis na `DDoSDetected` CloudWatch métrica, consulte AWS Shield Advanced métricas

Tópicos

- Lógica de detecção para ameaças na camada de infraestrutura
- Lógica de detecção para ameaças na camada de aplicativo
- Lógica de detecção para vários recursos em um aplicativo

Lógica de detecção para ameaças na camada de infraestrutura

A lógica de detecção usada para proteger AWS os recursos direcionados contra ataques de DDoS nas camadas de infraestrutura (camada 3 e camada 4) depende do tipo de recurso e se o recurso está protegido com AWS Shield Advanced.

Detecção para Amazon CloudFront e Amazon Route 53

Quando você serve seu aplicativo web com CloudFront o Route 53, todos os pacotes para o aplicativo são inspecionados por um sistema de mitigação de DDoS totalmente embutido, que não introduz nenhuma latência observável. Os ataques de DDoS contra CloudFront distribuições e zonas hospedadas do Route 53 são mitigados em tempo real. Essas proteções se aplicam independentemente de você usar o AWS Shield Advanced.

Siga as melhores práticas de usar CloudFront o Route 53 como ponto de entrada de seu aplicativo web sempre que possível para a detecção e mitigação mais rápidas de eventos de DDoS.

AWS Global Accelerator Detecção para serviços regionais

A detecção em nível de recurso protege aceleradores e recursos AWS Global Accelerator padrão que são lançados em AWS regiões, como Classic Load Balancers, Application Load Balancers e endereços IP elásticos (EIPs). Esses tipos de recursos são monitorados em busca de elevações de tráfego que podem indicar a presença de um ataque de DDoS que exija mitigação. A cada minuto, o tráfego de cada recurso da AWS é avaliado. Se o tráfego para um recurso for elevado, verificações adicionais serão realizadas para medir a capacidade do recurso.

O Shield executa as seguintes verificações padrão:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2), EIPs anexados às instâncias do Amazon EC2: o Shield recupera a capacidade do recurso protegido. A capacidade depende do tipo de instância do alvo, do tamanho da instância e de outros fatores, como se a instância está usando redes avançadas.
- Classic Load Balancers e Application Load Balancers: o Shield recupera a capacidade do nó do balanceador de carga alvo.
- EIPs conectados a Network Load Balancers: o Shield recupera a capacidade do balanceador de carga alvo. A capacidade é independente da configuração do grupo do balanceador de carga alvo.
- AWS Global Accelerator aceleradores padrão — o Shield recupera a capacidade, que é baseada na configuração do endpoint.

Essas avaliações ocorrem em várias dimensões do tráfego de rede, como porta e protocolo. Se a capacidade do recurso-alvo for excedida, a Shield coloca uma mitigação de DDoS. As mitigações impostas pelo Shield reduzirão o tráfego de DDoS, mas talvez não o eliminem. O Shield também pode oferecer uma mitigação se uma fração da capacidade do recurso for excedida em uma dimensão de tráfego consistente com os vetores de ataque de DDoS conhecidos. A Shield coloca essa mitigação em um tempo de vida limitado (TTL), que se estende enquanto o ataque estiver em andamento.

> **Note**
>
> As mitigações impostas pelo Shield reduzirão o tráfego de DDoS, mas talvez não o eliminem. Você pode aumentar o Shield com soluções como AWS Network Firewall ou um firewall no host, como iptables para impedir que seu aplicativo processe tráfego que não é válido para seu aplicativo ou que não foi gerado por usuários finais legítimos.

As proteções do Shield Advanced adicionam o seguinte às atividades existentes de detecção do Shield:

- Limites de detecção mais baixos: o Shield Advanced coloca as mitigações em metade da capacidade calculada. Isso pode fornecer mitigações mais rápidas para ataques que aumentam lentamente e mitigação de ataques que têm uma assinatura volumétrica mais ambígua.
- Proteção contra ataques intermitentes: o Shield Advanced coloca mitigações com um aumento exponencial do tempo de vida (TTL), com base na frequência e duração dos ataques. Isso mantém as mitigações em vigor por mais tempo quando um recurso é atacado com frequência e quando um ataque ocorre em intervalos curtos.
- Detecção baseada em integridade: quando você associa uma verificação de integridade do Route 53 a um recurso protegido do Shield Advanced, o status da verificação de saúde é usado na lógica de detecção. Durante um evento detectado, se a verificação de integridade estiver íntegra, o Shield Advanced exige mais confiança de que o evento é um ataque antes de fazer uma mitigação. Se, em vez disso, a verificação de integridade não estiver íntegra, o Shield Advanced poderá fazer uma mitigação antes mesmo que a confiança seja estabelecida. Esse atributo ajuda a evitar falsos positivos e fornece reações mais rápidas aos ataques que afetam seu aplicativo. Para obter informações sobre verificações de integridade com o Shield Advanced, consulte Detecção baseada em saúde usando verificações de saúde.

Lógica de detecção para ameaças na camada de aplicativo

AWS Shield Advanced fornece detecção de camadas de aplicativos web para CloudFront distribuições protegidas da Amazon e Application Load Balancers. Ao proteger esses tipos de recursos com o Shield Advanced, você pode associar uma ACL da web do AWS WAF à sua proteção para permitir a detecção da camada do aplicativo da web. O Shield Advanced consome dados de solicitação para a ACL da web associada e cria uma linha de base de tráfego para seu aplicativo. A detecção da camada de aplicativos da web depende da integração nativa entre o Shield Advanced e o AWS WAF. Para saber mais sobre as proteções da camada de aplicação, incluindo a associação de uma ACL AWS WAF da web a um recurso protegido do Shield Advanced, consulte. AWS Shield Advanced proteções da camada de aplicação (camada 7)

Para a detecção da camada de aplicativos web, o Shield Advanced monitora o tráfego do aplicativo e o compara às linhas de base históricas em busca de anomalias. Esse monitoramento abrange o volume total e a composição do tráfego. Durante um ataque de DDoS, esperamos que o volume e a composição do tráfego mudem, e o Shield Advanced exige um desvio estatisticamente significativo em ambos para declarar um evento.

O Shield Advanced realiza suas medições em relação a janelas de tempo históricas. Essa abordagem reduz as notificações de falsos positivos provenientes de mudanças legítimas no volume de tráfego ou de alterações no tráfego que correspondam a um padrão esperado, como uma venda oferecida no mesmo horário todos os dias.

> **Note**
>
> Evite falsos positivos em suas proteções do Shield Advanced dando tempo ao Shield Advanced para estabelecer linhas de base que representem padrões de tráfego normais e legítimos. O Shield Advanced começa a coletar informações para sua linha de base quando você associa uma ACL da web ao seu recurso protegido. Associe uma ACL da web ao seu recurso protegido pelo menos 24 horas antes de qualquer evento planejado que possa causar padrões incomuns em seu tráfego na web. A detecção da camada de aplicativo da web do Shield Advanced é mais precisa quando se observa 30 dias de tráfego normal.

O tempo que o Shield Advanced leva para detectar um evento é afetado pela quantidade de mudanças que ele observa no volume de tráfego. Para mudanças de volume menores, o Shield Advanced observa o tráfego por um período mais longo, a fim de aumentar a confiança de que um evento está ocorrendo. Para mudanças de volume maiores, o Shield Advanced detecta e relata um evento mais rapidamente.

Uma regra baseada em taxas em sua ACL da web, seja adicionada por você ou pelo recurso de mitigação automática da camada de aplicação do Shield Advanced, pode mitigar um ataque antes que ele atinja um nível detectável. Para obter mais informações sobre a mitigação automática de DDoS na camada de aplicativo, consulte. Mitigação automática de DDoS da camada de aplicação do Shield Advanced

> **Note**
>
> Você pode arquitetar seu aplicativo para reduzir a escala horizontalmente em resposta ao tráfego ou à carga elevados para garantir que ele não seja afetado por pequenas inundações de solicitações. Com o Shield Advanced, seus recursos protegidos são cobertos pela proteção de custos. Isso ajuda a protegê-lo contra aumentos inesperados em sua conta de nuvem que podem ocorrer como resultado de um ataque de DDoS. Para saber mais sobre a proteção de custos do Shield Advanced, consulte Solicitando um crédito em AWS Shield Advanced.

Lógica de detecção para vários recursos em um aplicativo

Você pode usar grupos de AWS Shield Advanced proteção para criar coleções de recursos protegidos que fazem parte do mesmo aplicativo. Você pode escolher quais recursos protegidos colocar em um grupo ou indicar que todos os recursos do mesmo tipo devem ser tratados como um grupo. Por exemplo, você pode criar um grupo de todos os Application Load Balancers. Quando você cria um grupo de proteção, a detecção do Shield Advanced agrega todo o tráfego dos recursos protegidos dentro do grupo. Isso é útil se você tiver muitos recursos, cada um com uma pequena quantidade de tráfego, mas com um grande volume agregado. Você também pode usar grupos de proteção para preservar as linhas de base do aplicativo, no caso de implantações azuis/verdes em que o tráfego é transferido entre recursos protegidos.

É possível optar por agregar o tráfego do seu grupo de proteção de uma das seguintes maneiras:

- Soma: essa agregação combina todo o tráfego entre os recursos no grupo de proteção. Você pode usar essa agregação para garantir que os recursos recém-criados tenham uma linha de base existente e para reduzir a sensibilidade de detecção, o que pode ajudar a evitar falsos positivos.
- Média: essa agregação usa a média de todo o tráfego no grupo de proteção. Você pode usar essa agregação para aplicativos em que o tráfego entre recursos é uniforme, como balanceadores de carga.
- Máximo: essa agregação usa o maior tráfego de qualquer recurso no grupo de proteção. Você pode usar essa agregação quando há vários níveis de um aplicativo em um grupo de proteção. Por exemplo, você pode ter um grupo de proteção que inclua uma CloudFront distribuição, sua origem do Application Load Balancer e os alvos da instância Amazon EC2 do Application Load Balancer.

Você também pode usar grupos de proteção para melhorar a velocidade com que a Shield Advanced aplica mitigações para ataques que visam vários IPs elásticos voltados para a internet ou aceleradores padrão do AWS Global Accelerator . Quando um recurso em um grupo de proteção é o alvo, o Shield Advanced estabelece confiança nos outros recursos do grupo. Isso coloca a detecção do Shield Advanced em alerta e pode reduzir o tempo necessário para criar mitigações adicionais.

Para saber mais sobre os grupos, consulte AWS Shield Advanced grupos de proteção.

Como AWS Shield atenua os eventos

A lógica de mitigação que protege seu aplicativo pode variar dependendo da arquitetura do aplicativo. Ao proteger uma aplicação web com a Amazon CloudFront e o Amazon Route 53, você

se beneficia de mitigações específicas para casos de uso da web e do DNS e que protegem todo o tráfego dos serviços. Quando o ponto de entrada do seu aplicativo é um recurso executado em uma AWS região, a lógica de mitigação varia de acordo com o serviço, o tipo de recurso e o uso do. AWS Shield Advanced

AWS Os sistemas de mitigação de DDoS são desenvolvidos pelos engenheiros da Shield e estão intimamente integrados aos serviços. AWS Os engenheiros levam em consideração aspectos de sua arquitetura, como a capacidade e a integridade dos recursos alvo. Os engenheiros do Shield monitoram continuamente a eficácia e o desempenho dos sistemas de mitigação de DDoS e são capazes de responder rapidamente quando novas ameaças são descobertas ou antecipadas.

Você pode arquitetar seu aplicativo para escalar em resposta ao tráfego elevado ou à carga elevada, para ajudar a garantir que ele não seja afetado por pequenos fluxos de solicitações. Se você usa o Shield Advanced para proteger seus recursos, receberá cobertura contra aumentos inesperados em sua conta de nuvem que possam ocorrer como resultado de um ataque de DDoS.

Mitigações da infraestrutura

Para ataques na camada de infraestrutura, os sistemas de mitigação de AWS Shield DDoS estão presentes na fronteira da AWS rede e nos locais periféricos. AWS A colocação de vários níveis de controles de segurança em toda a AWS infraestrutura fornece defense-in-depth aos seus aplicativos em nuvem.

O Shield mantém sistemas de mitigação de DDoS em todos os pontos de entrada da Internet. Quando o Shield detecta um ataque de DDoS, para cada ponto de entrada ele redireciona o tráfego pelos sistemas de mitigação de DDoS no mesmo local. Isso não introduz nenhuma latência adicional observável e fornece uma capacidade de mitigação de mais de 100 TeraBits por segundo (Tbps) em todas as AWS regiões e todos os pontos de presença. O Shield protege a disponibilidade dos seus recursos sem redirecionar o tráfego para centros de depuração externos ou remotos, o que pode aumentar a latência.

- Na fronteira da AWS rede, para qualquer AWS serviço ou recurso, os sistemas de mitigação de DDoS mitigam os ataques da camada de infraestrutura provenientes da Internet. Os sistemas realizam suas mitigações quando sinalizados pela detecção do Shield ou por um engenheiro no Shield Response Team (SRT).
- Nos pontos AWS de presença, os sistemas de mitigação de DDoS inspecionam continuamente cada pacote que é encaminhado para as distribuições da Amazon CloudFront e para as zonas hospedadas do Amazon Route 53, independentemente de sua origem. Quando necessário, os sistemas aplicam mitigações que são projetadas especificamente para o tráfego da web e do DNS.

Um benefício adicional de usar a Amazon CloudFront e o Amazon Route 53 para proteger seus aplicativos web é que os ataques de DDoS são imediatamente mitigados, sem exigir um sinal da detecção do Shield.

Mitigações da camada de aplicação

O Shield Advanced fornece mitigações na camada de aplicativos web para as CloudFront distribuições e os balanceadores de carga de aplicativos da Amazon nos quais você habilitou as proteções do Shield Advanced. Ao habilitar a proteção, você associa uma AWS WAF Web ACL ao recurso para habilitar a detecção da camada de aplicação Web. Além disso, você tem a opção de habilitar a mitigação automática para a camada da aplicação, que instrui o Shield Avançado a gerenciar as proteções para você durante um ataque de DDoS.

O Shield fornece apenas mitigações personalizadas para ataques na camada de aplicação em recursos para os quais você ativou o Shield Advanced e a mitigação automática da camada de aplicação. Com a mitigação automática, o Shield Advanced impõe a limitação AWS WAF de taxa nas solicitações de fontes conhecidas de DDoS e adiciona e gerencia automaticamente AWS WAF proteções personalizadas em resposta aos ataques de DDoS detectados. Para obter informações detalhadas sobre mitigações desse tipo, consulte Como o Shield Advanced gerencia a mitigação automática.

Uma regra baseada em taxas em sua ACL da web, seja adicionada por você ou adicionada pelo recurso de mitigação automática da camada de aplicação do Shield Advanced, pode mitigar um ataque antes que ele atinja um nível detectável. Para obter mais informações sobre detecção, consulteLógica de detecção para ameaças na camada de aplicativo.

Atributos de mitigação

As principais características da mitigação de AWS Shield DDoS são as seguintes:

- Validação de pacotes: isso garante que cada pacote inspecionado esteja em conformidade com uma estrutura esperada e seja válido para seu protocolo. As validações de protocolo suportadas incluem IP, TCP (incluindo cabeçalho e opções), UDP, ICMP, DNS e NTP.
- Listas de controle de acesso (ACLs) e shapers: uma ACL avalia o tráfego em relação a atributos específicos e descarta o tráfego correspondente ou o mapeia para um shaper. O shaper limita a taxa de pacotes para o tráfego correspondente, descartando pacotes em excesso para conter o volume que chega ao destino. AWS Shield Os engenheiros de detecção e do Shield Response Team (SRT) podem fornecer alocações de taxas dedicadas para o tráfego esperado e alocações

de taxas mais restritivas para o tráfego com atributos que correspondem aos vetores de ataque de DDoS conhecidos. Os atributos que uma ACL pode combinar incluem porta, protocolo, sinalizadores TCP, endereço de destino, país de origem e padrões arbitrários na carga útil do pacote.

- Pontuação de suspeita: usa o conhecimento que o Shield tem do tráfego esperado para aplicar uma pontuação a cada pacote. Pacotes que seguem mais de perto os padrões de tráfego em boas condições recebem uma pontuação de suspeita mais baixa. A observação de atributos conhecidos de tráfego incorreto pode aumentar a pontuação de suspeita de um pacote. Quando é necessário limitar a taxa de pacotes, o Shield descarta primeiro os pacotes com maior pontuação de suspeita. Isso ajuda o Shield a mitigar ataques de DDoS conhecidos e de dia zero, evitando falsos positivos.
- Proxy TCP SYN: isso fornece proteção contra floods TCP SYN enviando cookies TCP SYN para desafiar novas conexões antes de permitir que elas passem para o serviço protegido. O proxy TCP SYN fornecido pela mitigação de DDoS do Shield não tem estado, o que permite mitigar os maiores ataques de flood TCP SYN conhecidos sem atingir a exaustão do estado. Isso é obtido por meio da integração com AWS os serviços para transferir o estado da conexão, em vez de manter um proxy contínuo entre o cliente e o serviço protegido. Atualmente, o proxy TCP SYN está disponível na Amazon e no CloudFront Amazon Route 53.
- Distribuição de intervalos: isso ajusta continuamente os valores do shaper por local com base no padrão de entrada de tráfego em direção a um recurso protegido. Isso evita a limitação da taxa de tráfego de clientes que podem não entrar na AWS rede uniformemente.

AWS Shield lógica de mitigação para CloudFront e Route 53

A mitigação de DDoS do Shield inspeciona continuamente o tráfego e o Route 53. CloudFront Esses serviços operam a partir de uma rede distribuída globalmente AWS de pontos de presença que fornecem amplo acesso à capacidade de mitigação de DDoS da Shield e entregam seu aplicativo a partir de uma infraestrutura mais próxima de seus usuários finais.

- CloudFront— As mitigações de DDoS do Shield permitem apenas que o tráfego válido para aplicativos da web passe para o serviço. Isso fornece proteção automática contra muitos vetores comuns de DDoS, como ataques de reflexão UDP.

  CloudFront mantém conexões persistentes com a origem do aplicativo, as inundações de TCP SYN são automaticamente mitigadas por meio da integração com o recurso de proxy Shield TCP SYN e o Transport Layer Security (TLS) é encerrado na borda. Esses atributos combinados garantem que a origem do seu aplicativo receba apenas solicitações da web bem formadas e que esteja protegida contra ataques de DDoS de camada inferior, floods de conexão e abuso de TLS.

CloudFront usa uma combinação de direção de tráfego DNS e roteamento anycast. Essas técnicas melhoram a resiliência do seu aplicativo mitigando ataques próximos à origem, fornecendo isolamento de falhas e garantindo acesso à capacidade de mitigar os maiores ataques conhecidos.

- Route 53: as mitigações do Shield só permitem que solicitações de DNS válidas cheguem ao serviço. O Shield mitiga floods de consultas ao DNS usando a pontuação de suspeita que prioriza consultas reconhecidamente válidas e retira a prioridade das consultas que contenham atributos de ataque de DDoS suspeitos ou conhecidos.

  O Route 53 usa fragmentação aleatória para fornecer um conjunto exclusivo de quatro endereços IP do resolvedor para cada zona hospedada, tanto para IPv4 quanto para IPv6. Cada endereço IP corresponde a um subconjunto diferente de localizações do Route 53. Cada subconjunto de localização consiste em servidores DNS autoritativos que se sobrepõem apenas parcialmente à infraestrutura em qualquer outro subconjunto. Isso garante que, se uma consulta do usuário falhar por qualquer motivo, ela será atendida com sucesso em uma nova tentativa.

  O Route 53 usa o roteamento anycast para direcionar consultas ao DNS ao ponto de presença mais próximo, com base no local da borda. O Anycast também distribui o tráfego de DDoS para vários locais da borda, o que impede que os ataques se concentrem em um único local.

Além da velocidade de mitigação, CloudFront o Route 53 fornece amplo acesso à capacidade distribuída globalmente do Shield. Para aproveitar esses recursos, use esses serviços como ponto de entrada de seus aplicativos web dinâmicos ou estáticos.

Para saber mais sobre como usar o CloudFront Route 53 para proteger aplicativos web, consulte Como ajudar a proteger aplicativos web dinâmicos contra ataques de DDoS usando o Amazon CloudFront e o Amazon Route 53. Para saber mais sobre isolamento de falhas no Route 53, consulte Um estudo de caso sobre isolamento global de falhas.

AWS Shield lógica de mitigação para regiões AWS

Os recursos lançados nas AWS regiões são protegidos por sistemas de mitigação de AWS Shield DDoS colocados pela detecção em nível de recurso do Shield. Os recursos regionais incluem IPs elásticos (EIPs), Classic Load Balancers e Application Load Balancers.

Antes de fazer uma mitigação, o Shield identifica o recurso alvo e sua capacidade. O Shield usa a capacidade de determinar o tráfego total máximo que suas mitigações devem permitir que seja encaminhado para o recurso. As listas de controle de acesso (ACLs) e outros shapers dentro da

mitigação podem diminuir os volumes permitidos para algum tráfego, por exemplo, tráfego que corresponda a vetores de ataque de DDoS conhecidos ou que não se espera que venha em grande volume. Isso limita ainda mais a quantidade de tráfego que as mitigações permitem para ataques de reflexão UDP ou para tráfego TCP que possuem sinalizadores TCP SYN ou FIN.

O Shield determina a capacidade e coloca as mitigações de forma diferente para cada tipo de recurso.

- Para uma instância do Amazon EC2 ou um EIP anexado a uma instância do Amazon EC2, o Shield calcula a capacidade com base no tipo de instância e em outros atributos da instância, como se a instância tivesse uma rede aprimorada habilitada.
- Para um Application Load Balancer ou Classic Load Balancer, o Shield calcula a capacidade individualmente para cada nó de destino do balanceador de carga. As mitigações de ataques de DDoS para esses recursos são fornecidas por uma combinação de mitigações de DDoS Shield e escalonamento automático pelo balanceador de carga. Quando o Shield Response Team (SRT) está envolvido em um ataque contra um recurso do Application Load Balancer ou do Classic Load Balancer, ele pode acelerar o escalonamento como uma medida adicional de proteção.
- O Shield calcula a capacidade de alguns AWS recursos com base na capacidade disponível da AWS infraestrutura subjacente. Esses tipos de recursos incluem balanceadores de carga de rede (NLBs) e recursos que roteiam o tráfego por meio de balanceadores de carga de gateway ou. AWS Network Firewall

> **Note**
>
> Proteja seus Network Load Balancers anexando EIPs protegidos pelo Shield Advanced. Você pode trabalhar com o SRT para criar mitigações personalizadas com base no tráfego e na capacidade esperados do aplicativo subjacente.

Quando o Shield coloca uma mitigação, os limites de taxa iniciais que o Shield define na lógica de mitigação são aplicados igualmente a cada sistema de mitigação de DDoS do Shield. Por exemplo, se o Shield colocar uma mitigação com um limite de 100.000 pacotes por segundo (pps), ele inicialmente permitirá 100.000 pps em cada local. Em seguida, o Shield agrega continuamente métricas de mitigação para determinar a proporção real de tráfego e usa a proporção para adaptar o limite de taxa para cada local. Isso evita falsos positivos e garante que as mitigações não sejam excessivamente permissivas.

AWS Shield lógica de mitigação para aceleradores padrão AWS Global Accelerator

As mitigações do Shield permitem apenas que o tráfego válido alcance os endpoints de receptor de um acelerador padrão do Global Accelerator. Os aceleradores padrão são implantados globalmente e fornecem endereços IP que você pode usar para rotear o tráfego para AWS recursos em qualquer AWS região. Os limites de taxa que o Shield impõe para a mitigação do Global Accelerator são baseados nas capacidades dos recursos para os quais o acelerador padrão direciona o tráfego. O Shield coloca mitigações quando o tráfego total excede a taxa determinada e também quando uma fração dessa taxa é excedida para vetores de DDoS conhecidos.

Ao configurar um acelerador padrão, você define grupos de endpoints para cada região AWS para a qual direcionará o tráfego para seu aplicativo. Quando o Shield faz uma mitigação, ela calcula a capacidade de cada grupo de endpoints e atualiza adequadamente os limites de taxa em cada sistema de mitigação de DDoS do Shield. A taxa varia para cada local, com base nas suposições feitas pela Shield sobre como o tráfego será roteado da Internet para seus AWS recursos. A capacidade de um grupo de endpoints é calculada como o número de recursos no grupo multiplicado pela menor capacidade de qualquer recurso no grupo. Em intervalos regulares, o Shield recalcula a capacidade do seu aplicativo e atualiza os limites de taxa conforme necessário.

> **Note**
>
> Usar discagens de tráfego para alterar a porcentagem de tráfego direcionado a um grupo de endpoints não altera a forma como o Shield calcula ou distribui os limites de taxa para seus sistemas de mitigação de DDoS. Se você usa discagens de tráfego, configure seus grupos de endpoints para se espelharem em termos de tipo e quantidade de recursos. Isso ajuda a garantir que a capacidade calculada pelo Shield seja representativa dos recursos que estão fornecendo tráfego para seu aplicativo.

Para obter mais informações sobre grupos de endpoints e discagens de tráfego no Global Accelerator, consulte Grupos de endpoints em aceleradores padrão AWS Global Accelerator.

AWS Shield Advanced lógica de mitigação para Elastic IPs

Quando você protege um IP elástico (EIP) com AWS Shield Advanced, o Shield Advanced aprimora as mitigações que a Shield coloca durante um evento de DDoS. Os sistemas de mitigação de DDoS Shield Advanced replicam a configuração Network ACL (NACL) para a sub-rede pública à qual o EIP está associado. Por exemplo, se sua NACL estiver configurada para bloquear todo o tráfego UDP, o Shield Advanced mescla essa regra com as mitigações que o Shield coloca.

Essa funcionalidade adicional pode ajudá-lo a evitar riscos de disponibilidade devido ao tráfego que não é válido para seu aplicativo. Você também pode usar NACLs para bloquear endereços IP de origem individuais ou intervalos CIDR de endereços IP de origem. Isso pode ser uma ferramenta de mitigação útil para ataques de DDoS que não são distribuídos. Ele também permite que você gerencie facilmente suas próprias listas de permissões ou bloqueie endereços IP que não deveriam se comunicar com seu aplicativo, sem depender da intervenção de AWS engenheiros.

AWS Shield Advanced lógica de mitigação para aplicativos web

AWS Shield Advanced usa AWS WAF para mitigar ataques na camada de aplicativos da web. AWS WAF está incluído no Shield Advanced sem custo adicional.

Proteção padrão da camada da aplicação

Ao proteger uma CloudFront distribuição da Amazon ou um Application Load Balancer com o Shield Advanced, você pode usar o Shield Advanced para associar uma ACL AWS WAF da web ao seu recurso protegido, caso ainda não tenha uma associada. Se você ainda não configurou uma web ACL, pode usar o assistente de console Shield Advanced para criar uma e adicionar uma regra baseada em intervalos a ela. Uma regra baseada em intervalos limita o número de solicitações por janela de tempo de cinco minutos para cada endereço IP, fornecendo proteções básicas contra floods de solicitações na camada de aplicativos web. Você pode configurar o intervalo, começando em 100. Para ter mais informações, consulte ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas.

Você também pode usar o AWS WAF serviço para gerenciar a Web ACL. Por meio AWS WAF disso, você pode expandir a configuração da ACL da web para fazer coisas como inspecionar componentes específicos da solicitação da web em busca de correspondências ou padrões de seqüências de caracteres, adicionar tratamento personalizado de solicitações e respostas e comparar com a geolocalização da origem da solicitação. Para obter mais informações sobre AWS WAF regras, consulteAWS WAF regras.

Mitigação automática da camada de aplicativos

Para maior proteção, ative a mitigação automática da camada de aplicação do Shield Advanced. Com essa opção, o Shield Advanced mantém uma regra AWS WAF de limitação de taxa para solicitações de fontes conhecidas de DDoS e fornece mitigações personalizadas para ataques de DDoS detectados.

Quando o Shield Avançado detecta um ataque a um recurso protegido, ele tenta identificar uma assinatura de ataque que isole o tráfego de ataque do tráfego normal para a aplicação. O Shield

Advanced avalia a assinatura de ataque identificada em relação aos padrões históricos de tráfego do recurso que está sob ataque, bem como de qualquer outro recurso associado à mesma ACL da web.

Se o Shield Advanced determinar que a assinatura do ataque isola somente o tráfego envolvido no ataque de DDoS, ele implementará a assinatura em AWS WAF regras dentro da ACL da web associada. Você pode instruir o Shield Advanced para implementar mitigações que contabilizem apenas o tráfego com o qual elas coincidem ou que o bloqueiem, e você pode alterar a configuração a qualquer momento. Quando o Shield Advanced determina que suas regras de mitigação não são mais necessárias, ele as remove da ACL da web. Para obter mais informações sobre a mitigação de eventos para a camada da aplicação, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

Para obter mais informações sobre as mitigações para a camada da aplicação do Shield Avançado, consulte AWS Shield Advanced proteções da camada de aplicação (camada 7).

Exemplos de arquiteturas básicas resilientes a DDoS

A resiliência a DDoS é a capacidade da arquitetura de seu aplicativo de resistir a ataques de negação de serviço distribuído (DDoS) e, ao mesmo tempo, continuar atendendo aos usuários finais legítimos. Um aplicativo altamente resiliente pode permanecer disponível durante um ataque com impacto mínimo nas métricas de desempenho, como erros ou latência. Esta seção mostra alguns exemplos comuns de arquiteturas e descreve como usar os recursos de detecção e mitigação de DDoS fornecidos pela AWS e pelo Shield Advanced para aumentar sua resiliência de DDoS.

Os exemplos de arquiteturas nesta seção destacam os serviços da AWS que oferecem os maiores benefícios de resiliência de DDoS para seus aplicativos implantados. Os benefícios dos serviços destacados incluem os seguintes:

- Acesso à capacidade de rede distribuída globalmente — Os serviços Amazon CloudFront e Amazon Route 53 fornecem acesso à Internet e capacidade de mitigação de DDoS em toda a rede de borda AWS global. AWS Global Accelerator Isso é útil para mitigar ataques volumétricos maiores, que podem atingir terabits em escala. Você pode executar seu aplicativo em qualquer AWS região e usar esses serviços para proteger a disponibilidade e otimizar o desempenho para seus usuários legítimos.
- Proteção contra vetores de ataque de DDoS na camada de aplicativos da Web — Os ataques de DDoS na camada de aplicativos da web são mais bem mitigados usando uma combinação de escala de aplicativos e um firewall de aplicativos da web (WAF). O Shield Advanced usa registros de inspeção de solicitações da web AWS WAF para detectar anomalias que podem ser mitigadas

automaticamente ou por meio da interação com a AWS Shield Response Team (SRT). A mitigação automática está disponível por meio de regras baseadas em intervalos do AWS WAF que foram implantadas e também por meio da mitigação automática de DDoS da camada de aplicação do Shield Advanced.

Além de analisar esses exemplos, analise e siga as práticas recomendadas aplicáveis em Práticas recomendadas da AWS para resiliência de DDoS.

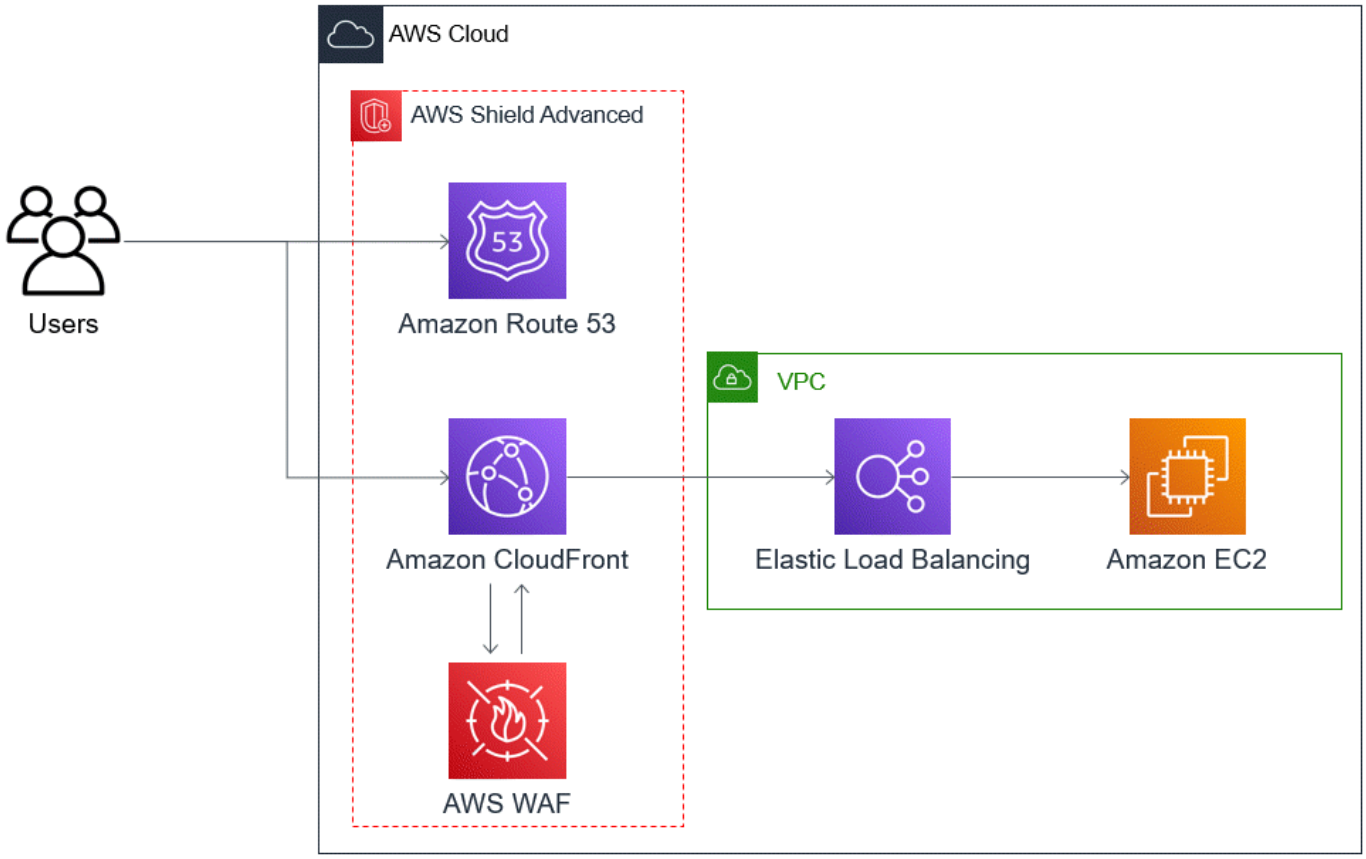
Exemplo de resiliência a DDoS para aplicativos web comuns

Você pode criar um aplicativo web em qualquer AWS região e receber proteção automática contra DDoS a partir dos recursos de detecção e mitigação AWS fornecidos na região.

Este exemplo é para arquiteturas que direcionam usuários para um aplicativo web usando recursos como Classic Load Balancers, Application Load Balancers, Network Load Balancers, soluções do Marketplace da AWS ou sua própria camada de proxy. Você pode melhorar a resiliência de DDoS inserindo zonas hospedadas do Amazon Route 53, distribuições da CloudFront Amazon AWS WAF e ACLs da web entre esses recursos do aplicativo web e seus usuários. Essas inserções podem ofuscar a origem do aplicativo, atender às solicitações mais perto dos usuários finais e detectar e mitigar as inundações de solicitações na camada de aplicação. Os aplicativos que fornecem conteúdo estático ou dinâmico para seus usuários com o Route 53 são protegidos por um sistema de mitigação de DDoS integrado CloudFront e totalmente embutido que atenua os ataques na camada de infraestrutura em tempo real.

Com essas melhorias arquitetônicas implementadas, você pode proteger suas zonas hospedadas do Route 53 e suas CloudFront distribuições com o Shield Advanced. Quando você protege CloudFront distribuições, o Shield Advanced solicita que você associe ACLs AWS WAF da web e crie regras baseadas em taxas para elas, além de oferecer a opção de ativar a mitigação automática de DDoS na camada de aplicação ou o engajamento proativo. O engajamento proativo e a mitigação automática de DDoS na camada de aplicação usam as verificações de integridade do Route 53 que você associa ao recurso. Para saber mais sobre essas opções, consulte Proteções de recursos em AWS Shield Advanced.

O diagrama de referência a seguir mostra essa arquitetura resiliente a DDoS para um aplicativo web.



Os benefícios que essa abordagem oferece ao seu aplicativo web incluem os seguintes:

- Proteção contra ataques de DDoS na camada de infraestrutura (camada 3 e camada 4) usada com frequência, sem atraso na detecção. Além disso, se um recurso for um alvo frequente, o Shield Advanced coloca mitigações por longos períodos de tempo. O Shield Advanced também usa o contexto do aplicativo inferido de Network ACLs (NACLs) para bloquear o tráfego indesejado ainda mais acima. Isso isola as falhas mais perto de sua origem, minimizando o efeito sobre usuários legítimos.
- Proteção contra inundações TCP SYN. Os sistemas de mitigação de DDoS integrados ao Route 53 AWS Global Accelerator fornecem um recurso de proxy TCP SYN que desafia novas tentativas de conexão e atende apenas a usuários legítimos. CloudFront
- Proteção contra ataques à camada de aplicação de DNS, porque o Route 53 é responsável por fornecer respostas autorizadas de DNS.
- Proteção contra inundações de solicitações na camada de aplicação da web. A regra baseada em taxa que você configura na sua ACL AWS WAF da web bloqueia os IPs de origem quando eles estão enviando mais solicitações do que o permitido pela regra.

- Mitigação automática de DDoS na camada de aplicação para suas CloudFront distribuições, se você optar por ativar essa opção. Com a mitigação automática de DDoS, o Shield Advanced mantém uma regra baseada em taxas na ACL da AWS WAF web associada à distribuição que limita o volume de solicitações de fontes conhecidas de DDoS. Além disso, quando o Shield Avançado detecta um evento que afeta a integridade da aplicação, ele cria, testa e gerencia automaticamente as regras de mitigação na ACL da Web.
- Engajamento proativo com a Shield Response Team (SRT), se você optar por ativar essa opção. Quando o Shield Advanced detecta um evento que afeta a integridade do seu aplicativo, o SRT responde e interage proativamente com suas equipes de segurança ou operações usando as informações de contato fornecidas por você. O SRT analisa padrões em seu tráfego e pode atualizar suas AWS WAF regras para bloquear o ataque.

Exemplo de resiliência a DDoS para aplicativos TCP e UDP

Este exemplo mostra uma arquitetura resiliente a DDoS para aplicativos TCP e UDP em uma região AWS que usa instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou endereços IP elásticos (EIP).

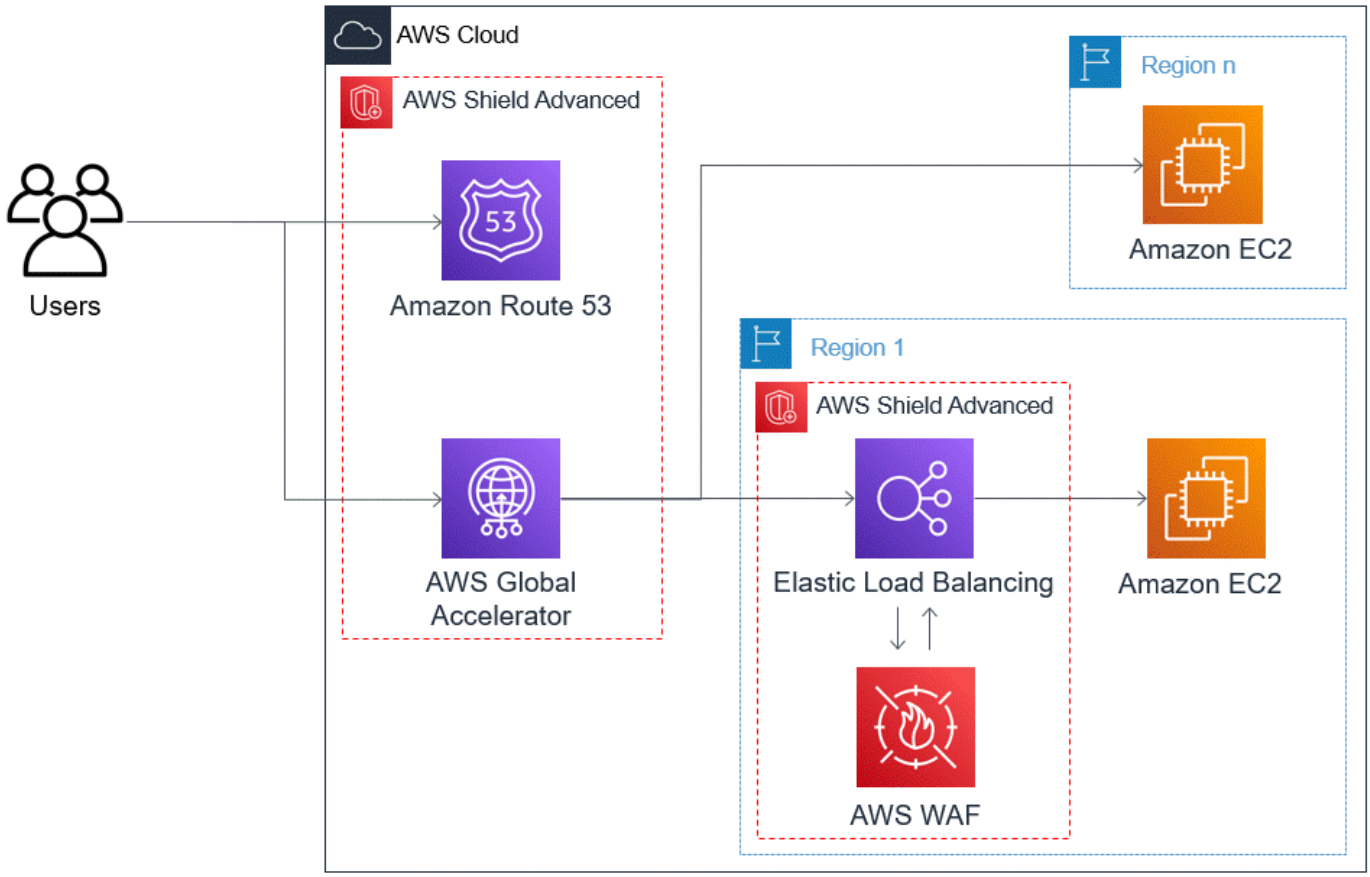
Você pode seguir esse exemplo geral para melhorar a resiliência de DDoS para os seguintes tipos de aplicativos:

- Aplicativos TCP ou UDP. Por exemplo, aplicativos usados para jogos, IoT e voz sobre IP.
- Aplicativos da web que exigem endereços IP estáticos ou que usam protocolos que a Amazon CloudFront não suporta. Por exemplo, seu aplicativo pode exigir endereços IP que seus usuários possam adicionar às listas de permissões de firewall e que não sejam usados por nenhum outro AWS cliente.

Você pode melhorar a resiliência a DDoS para esses tipos de aplicativos introduzindo o Amazon Route 53 e o AWS Global Accelerator. Esses serviços podem direcionar os usuários para o seu aplicativo e fornecer ao seu aplicativo endereços IP estáticos que são anycast de qualquer forma pela rede de borda global da AWS . Os aceleradores padrão do Global Accelerator podem melhorar a latência do usuário em até 60%. Se você tiver uma aplicação Web, poderá detectar e mitigar as inundações de solicitações da camada da aplicação Web executando a aplicação em um Application Load Balancer e, em seguida, protegendo o Application Load Balancer com uma ACL da web. AWS WAF

Depois de criar seu aplicativo, proteja suas zonas hospedadas do Route 53, os aceleradores padrão do Global Accelerator e quaisquer Application Load Balancers de carga de aplicativos com o Shield Advanced. Ao proteger seus Application Load Balancers, você pode associar ACLs AWS WAF da web e criar regras baseadas em taxas para elas. Você pode configurar o engajamento proativo com o SRT tanto para seus aceleradores padrão do Global Accelerator quanto para seus Application Load Balancers associando verificações de integridade novas ou existentes do Route 53. Para saber mais sobre as opções, consulte Proteções de recursos em AWS Shield Advanced.

O diagrama de referência a seguir mostra essa arquitetura resiliente a DDoS para aplicativos TCP e UDP.



Os benefícios que essa abordagem oferece ao seu aplicativo incluem o seguinte:

- Proteção contra os maiores ataques de DDoS conhecidos na camada de infraestrutura (camada 3 e camada 4). Se o volume de um ataque causar congestionamento a montante AWS, a falha será isolada mais perto de sua origem e terá um efeito minimizado em seus usuários legítimos.
- Proteção contra ataques à camada de aplicação de DNS, porque o Route 53 é responsável por fornecer respostas autorizadas de DNS.

- Se você tiver um aplicativo web, essa abordagem fornece proteção contra inundações de solicitações na camada de aplicação web. A regra baseada em taxa que você configura na sua ACL AWS WAF da web bloqueia os IPs de origem enquanto eles estão enviando mais solicitações do que o permitido pela regra.
- Engajamento proativo com a Shield Response Team (SRT), se você optar por ativar essa opção para os recursos elegíveis. Quando o Shield Advanced detecta um evento que afeta a integridade do seu aplicativo, o SRT responde e interage proativamente com suas equipes operaiconais ou de segurança usando as informações de contato fornecidas por você.

Exemplos de casos de uso do Shield Advanced

Você pode usar o Shield Advanced para proteger seus recursos em muitos tipos de cenários. No entanto, em alguns casos, você deve usar outros serviços ou combinar outros serviços com o Shield Advanced para oferecer a melhor proteção. Veja a seguir exemplos de como usar o Shield Advanced ou outros AWS serviços para ajudar a proteger seus recursos.

Objetivo	Serviços sugeridos	Documentação do serviço relacionado
Proteger um aplicativo web e APIs RESTful contra ataques DDoS	Shield Advanced protegendo uma CloudFront distribuição da Amazon e um Application Load Balancer	Documentação do Elastic Load Balancing, documentação da Amazon CloudFront
Proteger um aplicativo com base em TCP contra ataques DDoS	Shield Advanced protegendo um acelerador AWS Global Accelerator padrão; conectado a um endereço IP elástico	AWS Global Accelerator Documentação, documentação do Elastic Load Balancing
Proteger um servidor de jogo com base em UDP contra ataques DDoS	Shield Advanced protegendo uma instância do Amazon EC2 anexada a um endereço IP elástico	Documentação do Amazon Elastic Compute Cloud

Por exemplo, se você usa o Shield Advanced para proteger um endereço IP elástico, o Shield Advanced protege qualquer recurso associado a ele. Durante um ataque, o Shield Advanced

implanta automaticamente suas ACLs de rede na borda da AWS rede. Quando suas ACLs de rede estão na borda da rede, o Shield Advanced pode fornecer proteção contra eventos DDoS maiores. Normalmente, ACLs de rede são aplicadas perto de suas instâncias do Amazon EC2 na sua Amazon VPC. A rede ACL pode atenuar ataques somente até a capacidade máxima de processamento da Amazon VPC e da instância. Se a interface de rede anexada à sua instância do Amazon EC2 puder processar até 10 Gbps, volumes com mais de 10 Gbps ficarão lentos e possivelmente bloquearão o tráfego para essa instância. Durante um ataque, o Shield Advanced promove sua network ACL para a borda da AWS , que pode processar vários terabytes de tráfego. Sua network ACL é capaz de oferecer proteção para seu recurso muito além da capacidade típica da sua rede. Para obter mais informações sobre network ACLs, consulte network ACLs.

Começando com AWS Shield Advanced

Este tutorial explica como começar a AWS Shield Advanced usar o console Shield Advanced.

> **Note**
>
> O Shield Advanced exige uma assinatura, mas AWS Shield Standard não. As proteções fornecidas pelo Shield Básico estão disponíveis gratuitamente para todos os clientes da AWS .

O Shield Advanced fornece detecção e proteção de mitigação de DDoS avançadas para ataques às camadas de rede (camada 3), de transporte (camada 4) e aplicativos (camada 7). Para obter mais informações sobre o Shield Advanced, consulte AWS Shield Advanced visão geral.

A comunidade AWS técnica publicou um exemplo de um processo automatizado para configurar o Shield Advanced usando as ferramentas de infraestrutura como código (IaC) AWS CloudFormation e o Terraform. Você pode usar AWS Firewall Manager essa solução se suas contas fizerem parte de uma organização AWS Organizations e se você estiver protegendo qualquer tipo de recurso, exceto o Amazon Route 53 ou AWS Global Accelerator. Para explorar essa opção, consulte o repositório de código em aws-samples/ aws-shield-advanced-one-click-deployment e o tutorial em Implantação com um clique do Shield Advanced.

> **Note**
>
> É importante configurar totalmente o Shield Advanced antes de um evento do tipo negação distribuída de serviço (DDoS). Conclua a configuração para ajudar a garantir que seu

aplicativo esteja protegido e que você esteja pronto para responder se o aplicativo for afetado por um ataque de DDoS.

Execute as etapas a seguir em sequência para começar a usar o Shield Advanced.

Sumário

Inscrever-se em AWS Shield Advanced

Você deve assinar o Shield Advanced para cada um Conta da AWS que você deseja proteger. Não é necessário assinar o Shield Básico.

Cobrança da assinatura do Shield Advanced

Se você for um revendedor de AWS canais, fale com a equipe da sua conta para obter informações e orientações. Essas informações de cobrança são para clientes que não são revendedores de AWS canais.

Para todos os outros, as seguintes diretrizes de assinatura e cobrança se aplicam:

- Para contas que são membros de uma AWS Organizations organização, AWS as assinaturas do Shield Advanced são cobradas da conta pagante da organização, independentemente de a própria conta do pagador estar assinada.
- Quando você assina várias contas que estão na mesma família AWS Organizations de contas de faturamento consolidado, um preço de assinatura cobre todas as contas inscritas na família. A organização deve possuir todas as Contas da AWS e todos os seus recursos.

- Ao assinar várias contas para várias organizações, você ainda pode pagar uma taxa de assinatura em todas as organizações, contas e recursos, desde que seja proprietário de todas elas. Entre em contato com seu gerente de conta ou AWS suporte e solicite uma isenção de taxa sobre as cobranças de AWS Shield Advanced assinatura para todas as organizações, exceto uma.

Para obter informações detalhadas sobre preços e exemplos, consulte Preços do AWS Shield.

Simplifique as assinaturas com AWS Firewall Manager

Se suas contas fizerem parte de uma organização, recomendamos que você use o AWS Firewall Manager , se possível, para automatizar suas assinaturas e proteções para a organização. O Firewall Manager oferece suporte a todos os tipos de recursos protegidos, exceto o Amazon Route 53 e AWS Global Accelerator. Para usar o Firewall Manager, consulte AWS Firewall Manager e Introdução às AWS Firewall ManagerAWS Shield Advanced políticas.

Se você não usa o Firewall Manager, para cada conta com recursos para proteger, assine e adicione proteções usando os procedimentos a seguir.

Para assinar uma conta em AWS Shield Advanced

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. Na barra de navegação AWS Shield, escolha Conceitos básicos. Escolha Inscrever-se no Shield Advanced.
3. Na página Assine o Shield Advanced, leia cada termo do contrato e marque todas as caixas de seleção para indicar que você aceita os termos. Para contas em uma família de faturamento consolidado, você deve concordar com os termos de cada conta.

   > **Important**
   >
   > Quando você está inscrito, para cancelar a inscrição, você deve entrar em contato com AWS Support.
   > Para desativar a renovação automática de sua assinatura, você deve usar a operação da API Shield ou o comando CLI UpdateSubscriptionupdate-subscription.

   Escolha Inscrever-se no Shield Advanced. Isso inscreve sua conta no Shield Advanced e ativa o serviço.

Sua conta está inscrita. Continue com as etapas a seguir para proteger os recursos da sua conta com o Shield Advanced.

> **Note**
>
> O Shield Advanced não protege automaticamente seus recursos após você assinar. Você deve especificar os recursos que deseja que o Shield Advanced proteja e configurar as proteções.

Adicione recursos para proteger e configurar proteções

O Shield Advanced protege somente os recursos que você especifica, seja por meio do Shield Advanced ou em uma política Shield Advanced do Firewall Manager. Ele não protege automaticamente os recursos de uma conta assinada.

Se você usa uma política AWS Firewall Manager Shield Advanced para suas proteções, não precisa executar essa etapa. Você configura a política com os tipos de recursos a serem protegidos, e o Firewall Manager adiciona automaticamente proteções aos recursos que estão dentro do escopo da política.

Se você não usa o Firewall Manager, siga os procedimentos a seguir para cada conta que tenha recursos para proteger.

Para escolher os recursos a serem protegidos usando o Shield Advanced

1. Escolha Adicionar recursos para proteger na página de confirmação da assinatura do procedimento anterior ou na página Recursos protegidos ou Visão geral.
2. Na página Escolher recursos para proteger com o Shield Advanced, em Especificar a região e os tipos de recursos, forneça as especificações de região e tipo de recurso para os recursos que você deseja proteger. Você pode proteger recursos em várias regiões selecionando Todas as regiões, e pode restringir a seleção a recursos globais selecionando Global. Você pode desmarcar qualquer tipo de recurso que não queira proteger. Para obter informações sobre proteções para seus tipos de recursos, consulte AWS Shield Advanced proteções por tipo de recurso.
3. Escolha Carregar recursos. O Shield Advanced preenche a seção Selecionar recursos com os recursos AWS que correspondem aos seus critérios.

4. Na seção Selecionar recursos, você pode filtrar a lista de recursos inserindo uma string para pesquisar nas listas de recursos.

   Escolha os recursos que você deseja proteger.

5. Na seção Tags, se você quiser adicionar tags às proteções Shield Advanced que estiver criando, especifique-as. Para obter mais informações sobre como marcar recursos AWS , consulte Trabalhar com o Tag Editor.
6. Escolha Proteger com o Shield Advanced. Isso adiciona as proteções do Shield Advanced aos recursos.

Continue nas telas do assistente do console para concluir a configuração de suas proteções de recursos.

Tópicos

- Configure as proteções contra DDoS da camada de aplicativo (camada 7) com AWS WAF
- Configurar a detecção baseada em integridade às suas proteções
- Configurar alarmes e notificações
- Revise e conclua sua configuração de proteção

Configure as proteções contra DDoS da camada de aplicativo (camada 7) com AWS WAF

Para proteger um recurso da camada de aplicação, o Shield Advanced usa uma AWS WAF Web ACL com uma regra baseada em taxas como ponto de partida. AWS WAF é um firewall de aplicativo web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas para os recursos da camada de aplicativos e permite controlar o acesso ao seu conteúdo com base nas características das solicitações. Uma regra baseada em intervalos limita o volume de tráfego com base nos critérios de agregação de solicitações, fornecendo proteção básica contra DDoS ao seu aplicativo. Para ter mais informações, consulte Como AWS WAF funciona e Instrução de regra baseada em intervalos.

Como opção, é possível habilitar a mitigação automática de DDoS para a camada da aplicação do Shield Avançado com a finalidade de limitar o volume de solicitações de fontes de DDoS conhecidas para o Shield Avançado e fornecer automaticamente proteções específicas de incidentes.

> **Important**
>
> Se você gerencia suas proteções Shield Advanced AWS Firewall Manager usando uma política Shield Advanced, você não pode gerenciar as proteções da camada de aplicativos aqui. Você deve gerenciá-las na política do Shield Advanced do Firewall Manager.

Assinaturas e custos do Shield Advanced AWS WAF

Sua assinatura do Shield Advanced cobre os custos de uso dos AWS WAF recursos padrão dos recursos que você protege com o Shield Advanced. As AWS WAF taxas padrão cobertas pelas proteções Shield Advanced são o custo por ACL da web, o custo por regra e o preço base por milhão de solicitações para inspeção de solicitações da web, até 1.500 WCUs e até o tamanho padrão do corpo.

A ativação da mitigação automática de DDoS na camada de aplicação do Shield Advanced adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced, O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).

Sua assinatura do Shield Advanced não cobre o uso AWS WAF de recursos que você não protege usando o Shield Advanced. Também não cobre nenhum custo adicional não padronizado AWS WAF para recursos protegidos. Exemplos de AWS WAF custos não padrão são aqueles para o Bot Control, para a ação da CAPTCHA regra, para ACLs da web que usam mais de 1.500 WCUs e para inspecionar o corpo da solicitação além do tamanho padrão. A lista completa é fornecida na página AWS WAF de preços.

Para obter informações completas e exemplos de preços, consulte Preços do Shield e Preços do AWS WAF.

Para configurar proteções contra DDoS de camada 7 para uma região

O Shield Advanced oferece a opção de configurar a mitigação de DDoS de camada 7 para cada região nas quais os recursos escolhidos estão localizados. Se você estiver adicionando proteções em várias regiões, o assistente o guiará pelo procedimento a seguir para cada região.

1. A página Configurar proteções contra DDoS da camada 7 lista cada recurso que ainda não está associado a uma web ACL. Para cada uma delas, escolha uma web ACL existente ou crie uma

nova web ACL. Para qualquer recurso que já tenha uma ACL da Web associada, você pode alterar as ACLs da Web desassociando primeiro a atual. AWS WAF Para ter mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

Para web ACLs que ainda não têm uma regra baseada em intervalos, o assistente de configuração solicita que você adicione uma. Uma regra baseada em intervalos limita o tráfego de endereços IP quando eles estão enviando um grande volume de solicitações. As regras baseadas em intervalos ajudam a proteger seu aplicativo contra floods de solicitações da web, e podem fornecer alertas sobre picos repentinos no tráfego que podem indicar um possível ataque de DDoS. Adicione uma regra baseada em intervalos a uma web ACL escolhendo Adicionar regra de limite de intervalo e, em seguida, fornecendo um limite de intervalo e uma ação de regra. Você pode configurar proteções adicionais na Web ACL por meio de. AWS WAF

Para obter informações sobre o uso de web ACLs e regras baseadas em intervalos em suas proteções do Shield Advanced, incluindo opções adicionais de configuração para regras baseadas em intervalos, consulte ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas.

2. Para a mitigação automática de DDoS na camada de aplicativo, se você quiser que o Shield Advanced mitigue automaticamente os ataques de DDoS contra seus recursos da camada de aplicativo, escolha Habilitar e, em seguida, selecione a ação de AWS WAF regra que você deseja que o Shield Advanced use em suas regras personalizadas. Essa configuração se aplica a todas as web ACLs para os recursos que você gerencia nessa sessão do assistente.

   Com a mitigação automática de DDoS na camada de aplicação, o Shield Advanced mantém uma regra baseada em taxas na ACL da AWS WAF web do recurso que limita o volume de solicitações de fontes conhecidas de DDoS. Além disso, o Shield Avançado compara os padrões de tráfego atuais com as linhas de base de tráfego históricas para detectar desvios que possam indicar um ataque de DDoS. Quando o Shield Advanced detecta um ataque de DDoS, ele responde criando, avaliando e implantando regras personalizadas para responder. AWS WAF Você especifica se as regras personalizadas contam ou bloqueiam ataques em seu nome.

   > **Note**
   >
   > A mitigação automática de DDoS na camada de aplicativo funciona somente com ACLs da web que foram criadas usando a versão mais recente do (v2). AWS WAF

Para obter mais informações sobre a mitigação automática de DDoS na camada de aplicação Shield Advanced, incluindo advertências e melhores práticas para o uso desse recurso, consulte. Mitigação automática de DDoS da camada de aplicação do Shield Advanced

3. Escolha Próximo. O assistente do console avança para a página de detecção baseada em integridade.

Configurar a detecção baseada em integridade às suas proteções

Configure o Shield Advanced para usar a detecção baseada em integridade para melhorar a capacidade de resposta e a precisão na detecção e mitigação de ataques. Verificações de saúde bem configuradas são essenciais para a detecção precisa de eventos. Você pode configurar a detecção baseada em integridade para qualquer tipo de recurso, exceto para zonas hospedadas do Route 53.

Para usar a detecção baseada em integridade, defina uma verificação de saúde para seu recurso no Route 53 e, em seguida, associe a verificação de saúde à sua proteção Shield Advanced. É importante que a verificação de integridade que você configura reflita com precisão a integridade do recurso. Para obter informações e exemplos de configuração de verificações de integridade para uso com o Shield Advanced, consulte Detecção baseada em saúde usando verificações de saúde.

As verificações de integridade são necessárias para o suporte de engajamento proativo da Shield Response Team (SRT). Para obter informações sobre engajamento proativo, consulte Como configurar o engajamento proativo.

> **Note**
>
> As verificações de integridade devem ser relatadas como íntegras quando você as associa às proteções do Shield Advanced.

Para configurar a detecção baseada em integridade

1. Em Verificação de integridade associada, escolha o ID da verificação de integridade que deseja associar à proteção.

> **Note**
>
> Se você não vir a verificação de integridade necessária, vá até o console do Route 53 e verifique a verificação de integridade e seu ID. Para obter informações, consulte Criar e atualizar verificações de integridade.

2. Escolha Próximo. O assistente do console avança para a página de alarmes e notificações.

Configurar alarmes e notificações

Opcionalmente, você pode configurar notificações do Amazon Simple Notification Service para CloudWatch alarmes detectados da Amazon e atividades de regras baseadas em taxas. Você pode usá-los para receber notificações quando o Shield detectar um evento em um recurso protegido, ou ainda quando um limite de taxa configurado em uma regra baseada em intervalos for excedido.

Para obter informações sobre as CloudWatch métricas do Shield Advanced, consulteAWS Shield Advanced métricas. Para obter mais informações sobre tópicos do Amazon SNS, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Para configurar alarmes e notificações

1. Selecione os tópicos do Amazon SNS para os quais deseja receber notificações. Você pode usar um único tópico do Amazon SNS para todos os recursos protegidos e regras baseadas em intervalos, ou você pode escolher tópicos diferentes, personalizados para sua organização. Por exemplo, você pode criar um tópico de SNS para cada equipe responsável pela resposta a incidentes para um conjunto específico de recursos.
2. Escolha Próximo. O assistente do console avança para a página de revisão da proteção de recursos.

Revise e conclua sua configuração de proteção

Para revisar e definir suas configurações

1. Na página Revisar e configurar mitigação e visibilidade de DDoS, revise suas configurações. Para fazer modificações, escolha Editar na área que você deseja modificar. Isso o levará de volta à página associada no assistente do console. Faça suas alterações e escolha Avançar nas

páginas subsequentes até retornar à página Revisar e configurar a mitigação e visibilidade de DDoS.

2. Escolha Concluir configuração. A página Recursos protegidos lista seus recursos recém-protegidos.

Configurar o AWS suporte ao SRT

O Shield Response Team (SRT) é formada por engenheiros de segurança especializados em resposta a eventos de DDoS. Opcionalmente, você pode adicionar permissões que permitam ao SRT gerenciar recursos em seu nome durante um evento de DDoS. Além disso, você pode configurar o SRT para interagir proativamente com você se as verificações de integridade do Route 53 associadas aos seus recursos protegidos não estiverem íntegras durante um evento detectado. Essas duas adições às suas proteções permitem respostas mais rápidas aos eventos de DDoS.

> **Note**
>
> Para usar os serviços do Shield Response Team (SRT), você deve ser assinante do plano Business Support ou Enterprise Support.

O SRT pode monitorar dados e registros de AWS WAF solicitações durante eventos da camada de aplicação para identificar tráfego anômalo. Eles podem ajudar a criar AWS WAF regras personalizadas para mitigar fontes de tráfego ofensivas. Conforme necessário, o SRT pode fazer recomendações arquitetônicas para ajudá-lo a alinhar melhor seus recursos às AWS recomendações.

Para obter mais informações sobre o SRT, consulte Suporte do Shield Response Team (SRT).

Para conceder permissões ao SRT

1. Na página Visão geral do AWS Shield console, em Configurar suporte ao AWS SRT, escolha Editar acesso ao SRT. A página de acesso AWS do Edit Shield Response Team (SRT) é aberta.
2. Para Configuração de acesso SRT, selecione uma das opções:

   - Não conceder ao SRT acesso à minha conta: o Shield remove todas as permissões que você concedeu anteriormente ao SRT para acessar sua conta e recursos.
   - Criar uma nova função para o SRT acessar minha conta: o Shield cria uma função que confia na entidade principal do serviço `drt.shield.amazonaws.com`, que representa o SRT,

e anexa a política `AWSShieldDRTAccessPolicy` gerenciada a ele. A política gerenciada permite que o SRT faça AWS Shield Advanced chamadas de AWS WAF API em seu nome e acesse seus AWS WAF registros. Para obter mais informações sobre a política gerenciada, consulte AWS política gerenciada: AWSShieldDRTAccessPolicy.

- Escolha uma função existente para o SRT acessar minhas contas — Para essa opção, você deve modificar a configuração da função no AWS Identity and Access Management (IAM) da seguinte forma:
  - Anexe a política gerenciada `AWSShieldDRTAccessPolicy` à função. Essa política gerenciada permite que o SRT faça AWS Shield Advanced chamadas de AWS WAF API em seu nome e acesse seus AWS WAF registros. Para obter mais informações sobre a política gerenciada, consulte AWS política gerenciada: AWSShieldDRTAccessPolicy. Para obter informações sobre como anexar a política gerenciada à sua função, consulte Anexar e desanexar políticas do IAM.
  - Modifique a função para confiar no serviço principal `drt.shield.amazonaws.com`. Esta é a entidade principal do serviço que representa o SRT. Para mais informações, consulte Elementos de política JSON do IAM: principal.

3. Escolha Salvar para salvar as alterações.

Para obter mais informações sobre como dar ao SRT acesso às suas proteções e dados, consulte Como configurar o acesso para o Shield Response Team (SRT).

Como habilitar o envolvimento proativo do SRT

1. Na página Visão geral do AWS Shield console, em Engajamento proativo e contatos, na área de contatos, escolha Editar.

   Na página Editar contatos, forneça as informações de contato das pessoas com as quais você deseja que o SRT entre em contato para um engajamento proativo.

   Se você fornecer mais de um ponto de contato, em Notas, indique as circunstâncias em que cada contato deve ser usado. Inclua designações de contato primário e secundário e forneça os horários de disponibilidade e os fusos horários de cada contato.

   Exemplos de notas de contato:

   - Esta é uma linha direta que funciona 24 horas por dia, 7 dias por semana, 365 dias por ano. Trabalhe com o analista atendente, que colocará a pessoa apropriada na chamada.

- Entre em contato comigo se a linha direta não responder em 5 minutos.

2. Escolha Salvar.

   A página Visão geral reflete as informações de contato atualizadas.

3. Escolha Editar atributo de engajamento proativo, escolha Habilitar e, em seguida, escolha Salvar para ativar o engajamento proativo.

Para obter mais informações sobre engajamento proativo, consulte Como configurar o engajamento proativo.

Crie um painel de DDoS CloudWatch e CloudWatch defina alarmes

Você pode monitorar possíveis atividades de DDoS usando a Amazon CloudWatch, que coleta dados brutos do Shield Advanced e os processa em métricas legíveis, quase em tempo real. Você pode usar estatísticas CloudWatch para obter uma perspectiva sobre o desempenho de seu aplicativo ou serviço da Web. Para obter mais informações sobre o uso CloudWatch, consulte O que está CloudWatch no Guia CloudWatch do usuário da Amazon.

- Para obter instruções sobre como criar um CloudWatch painel, consulteMonitoramento com a Amazon CloudWatch.
- Para obter descrições das métricas do Shield Advanced que você pode adicionar ao painel, consulte AWS Shield Advanced métricas.

O Shield Advanced reporta métricas de recursos com CloudWatch mais frequência durante eventos de DDoS do que quando nenhum evento está em andamento. O Shield Advanced relata métricas uma vez por minuto durante um evento e, em seguida, uma vez logo após o término do evento. Enquanto não há nenhum ataque em andamento, o Shield Advanced relata métricas uma vez ao dia, no horário atribuído ao recurso. Esse relatório periódico mantém as métricas ativas e disponíveis para uso em seus alarmes personalizados CloudWatch .

Isso conclui o tutorial para começar a usar o Shield Advanced. Para aproveitar ao máximo as proteções que você escolheu, continue explorando os atributos e opções do Shield Advanced. Para começar, familiarize-se com suas opções para visualizar e responder aos eventos em Visibilidade de eventos de DDoS e Resposta a eventos de DDoS.

Suporte do Shield Response Team (SRT)

O Shield Response Team (SRT) fornece suporte adicional aos clientes do Shield Advanced. Os SRT são engenheiros de segurança especializados em resposta a eventos de DDoS. Como uma camada adicional de suporte ao seu plano AWS Support , você pode trabalhar diretamente com o SRT, aproveitando sua experiência como parte do seu fluxo de trabalho de resposta a eventos. Para obter informações sobre as opções e orientações de configuração, consulte os tópicos a seguir.

> **Note**
>
> Para usar os serviços do Shield Response Team (SRT), você deve ser assinante do plano Business Support ou do Enterprise Support.

Atividades de suporte do SRT

O objetivo principal em um contrato com o SRT é proteger a disponibilidade e o desempenho do seu aplicativo. Conforme o tipo de evento de DDoS e a arquitetura do seu aplicativo, o SRT pode realizar uma ou mais das seguintes ações:

- AWS WAF análise de registros e regras — Para recursos que usam uma ACL AWS WAF da web, o SRT pode analisar seus AWS WAF registros para identificar características de ataque nas solicitações da web do seu aplicativo. Com sua aprovação durante o engajamento, o SRT pode aplicar alterações em sua web ACL para bloquear os ataques que eles identificaram.
- Crie mitigações de rede personalizadas: o SRT pode criar mitigações personalizadas para você para ataques na camada de infraestrutura. O SRT pode trabalhar com você para entender o tráfego esperado para seu aplicativo, bloquear tráfego inesperado e otimizar os limites de taxa de pacotes por segundo. Para ter mais informações, consulte Configurando mitigações personalizadas com o Shield Response Team (SRT).
- Engenharia de tráfego de rede — O SRT trabalha em estreita colaboração com as equipes AWS de rede para proteger os clientes do Shield Advanced. Quando necessário, AWS pode alterar a forma como o tráfego da Internet chega à AWS rede para alocar mais capacidade de mitigação ao seu aplicativo.
- Recomendações arquitetônicas — O SRT pode determinar que a melhor mitigação para um ataque requer mudanças na arquitetura para melhor se alinhar às AWS melhores práticas, e elas ajudarão a apoiar a implementação dessas práticas. Para obter informações, consulte Melhores práticas AWS para resiliência de DDoS.

Tópicos

Como configurar o acesso para o Shield Response Team (SRT)

Você pode conceder permissão à Shield Response Team (SRT) para agir em seu nome, acessando seus AWS WAF registros e fazendo chamadas para as AWS WAF APIs AWS Shield Advanced e para gerenciar as proteções. Durante eventos de DDoS na camada de aplicação, o SRT pode monitorar AWS WAF solicitações para identificar tráfego anômalo e ajudar a criar AWS WAF regras personalizadas para mitigar fontes de tráfego ofensivas.

Além disso, você pode conceder ao SRT acesso a outros dados armazenados nos buckets do Amazon S3, como capturas de pacotes ou registros de um Application Load Balancer, da CloudFront Amazon ou de fontes de terceiros.

> **Note**
>
> Para usar os serviços do Shield Response Team (SRT), você deve ser assinante do plano Business Support ou Enterprise Support.

Para gerenciar permissões para o SRT

1. Na página Visão geral do AWS Shield console, em Configurar suporte ao AWS SRT, escolha Editar acesso ao SRT. A página de acesso AWS do Edit Shield Response Team (SRT) é aberta.
2. Para Configuração de acesso SRT, selecione uma das opções:

   - Não conceder ao SRT acesso à minha conta: o Shield remove todas as permissões que você concedeu anteriormente ao SRT para acessar sua conta e recursos.
   - Criar uma nova função para o SRT acessar minha conta: o Shield cria uma função que confia na entidade principal do serviço `drt.shield.amazonaws.com`, que representa o SRT, e anexa a política `AWSShieldDRTAccessPolicy` gerenciada a ele. A política gerenciada permite que o SRT faça AWS Shield Advanced chamadas de AWS WAF API em seu nome e

acesse seus AWS WAF registros. Para obter mais informações sobre a política gerenciada, consulte AWS política gerenciada: AWSShieldDRTAccessPolicy.

- Escolha uma função existente para o SRT acessar minhas contas — Para essa opção, você deve modificar a configuração da função no AWS Identity and Access Management (IAM) da seguinte forma:
  - Anexe a política gerenciada `AWSShieldDRTAccessPolicy` à função. Essa política gerenciada permite que o SRT faça AWS Shield Advanced chamadas de AWS WAF API em seu nome e acesse seus AWS WAF registros. Para obter mais informações sobre a política gerenciada, consulte AWS política gerenciada: AWSShieldDRTAccessPolicy. Para obter informações sobre como anexar a política gerenciada à sua função, consulte Anexar e desanexar políticas do IAM.
  - Modifique a função para confiar no serviço principal `drt.shield.amazonaws.com`. Esta é a entidade principal do serviço que representa o SRT. Para mais informações, consulte Elementos de política JSON do IAM: principal.

3. Para (opcional): conceda acesso SRT a um bucket do Amazon S3. Se você precisar compartilhar dados que não estejam nos AWS WAF seus registros de ACL da web, configure isso. Por exemplo, registros de acesso do Application Load Balancer, CloudFront registros da Amazon ou registros de fontes de terceiros.

   > **Note**
   >
   > Você não precisa fazer isso para seus registros de ACL AWS WAF da web. O SRT obtém acesso a eles quando você concede acesso à sua conta.

   a. Configure os buckets do Amazon S3 de acordo com as seguintes diretrizes:

      - Os locais dos buckets devem ser os Conta da AWS mesmos aos quais você concedeu acesso geral ao SRT, na etapa anterior, acesso ao AWS Shield Response Team (SRT).
      - Os buckets podem ser texto simples ou criptografados por SSE-S3. Para obter mais informações sobre a criptografia por SSE-S3 do Amazon S3, consulte Proteger dados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) no Guia do usuário do Amazon S3.

O SRT não pode visualizar ou processar registros armazenados em buckets criptografados com chaves armazenadas em AWS Key Management Service ()AWS KMS.

b. No Shield Advanced (Opcional): Conceder ao SRT acesso a uma seção de bucket do Amazon S3, para cada bucket do Amazon S3 em que seus dados ou logs estão armazenados, insira o nome do bucket e escolha Adicionar Bucket. Você pode adicionar até 10 buckets.

   Isso concede ao SRT as seguintes permissões no bucket: `s3:GetBucketLocation`, `s3:GetObject` e `s3:ListBucket`.

   Se quiser dar permissão ao SRT para acessar mais de 10 buckets, você pode fazer isso editando as políticas adicionais do bucket e concedendo manualmente as permissões listadas aqui para o SRT.

   A política a seguir mostra um exemplo de listagem de políticas.

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
    ]
}
```

4. Escolha Salvar para salvar as alterações.

Você também pode autorizar o SRT por meio da API criando uma função do IAM, anexando a política a ela e, em seguida, passando a função AWSShieldDRTAccessPolicy para a operação AssociatedRtRole.

Como configurar o engajamento proativo

Com o engajamento proativo, o Shield Response Team (SRT) entra em contato com você diretamente quando a disponibilidade ou o desempenho do seu aplicativo são afetados por causa de um possível ataque. Recomendamos esse modelo de engajamento porque ele fornece a resposta SRT mais rápida e permite que o SRT comece a solucionar problemas mesmo antes de estabelecer contato com você.

O engajamento proativo está disponível para eventos de camada de rede e camada de transporte em endereços IP elásticos e aceleradores AWS Global Accelerator padrão, e para inundações de solicitações da web em distribuições da Amazon e Application Load Balancers. CloudFront O engajamento proativo está disponível somente para proteções de recursos do Shield Advanced que tenham uma verificação de integridade associada ao Amazon Route 53. Para mais informações sobre como gerenciar e usar as verificações de integridade, consulte Detecção baseada em saúde usando verificações de saúde.

Durante um evento detectado pelo Shield Advanced, o SRT usa o estado de suas verificações de integridade para determinar se o evento se qualifica para um engajamento proativo. Em caso positivo, o SRT entrará em contato com você de acordo com as orientações de contato fornecidas em sua configuração de engajamento proativo.

Você pode configurar até dez contatos para engajamento proativo e fornecer notas para orientar o SRT a entrar em contato com você. Seus contatos proativos de engajamento devem estar disponíveis para interagir com o SRT durante os eventos. Se você não tiver um centro de operações 24 horas por dia, 7 dias por semana, você pode fornecer um contato por pager e indicar essa preferência de contato em suas notas de contato.

O envolvimento proativo exige que você faça o seguinte:

- Você deve ser assinante do plano Business Support ou Enterprise Support.
- Você deve associar uma verificação de integridade do Amazon Route 53 a qualquer recurso que você queira proteger com um engajamento proativo. O SRT usa o status de suas verificações de integridade para ajudar a determinar se um evento exige engajamento proativo, por isso é importante que suas verificações de integridade reflitam com precisão o estado de seus recursos protegidos. Para obter mais informações e orientações, consulte Detecção baseada em saúde usando verificações de saúde.
- Para um recurso que tenha uma ACL AWS WAF da Web associada, você deve criar a ACL da Web usando AWS WAF (v2), que é a versão mais recente do. AWS WAF

- Você deve fornecer pelo menos um contato para o SRT usar para engajamento proativo durante um evento. Mantenha suas informações de contato completas e atualizadas.

Como habilitar o envolvimento proativo do SRT

1. Na página Visão geral do AWS Shield console, em Engajamento proativo e contatos, na área de contatos, escolha Editar.

   Na página Editar contatos, forneça as informações de contato das pessoas com as quais você deseja que o SRT entre em contato para um engajamento proativo.

   Se você fornecer mais de um ponto de contato, em Notas, indique as circunstâncias em que cada contato deve ser usado. Inclua designações de contato primário e secundário e forneça os horários de disponibilidade e os fusos horários de cada contato.

   Exemplos de notas de contato:

   - Esta é uma linha direta que funciona 24 horas por dia, 7 dias por semana, 365 dias por ano. Trabalhe com o analista atendente, que colocará a pessoa apropriada na chamada.
   - Entre em contato comigo se a linha direta não responder em 5 minutos.
2. Escolha Salvar.

   A página Visão geral reflete as informações de contato atualizadas.
3. Escolha Editar atributo de engajamento proativo, escolha Habilitar e, em seguida, escolha Salvar para ativar o engajamento proativo.

Entrando em contato com o Shield Response Team (SRT)

Você pode entrar em contato com o Shield Response Team (SRT) de uma das seguintes maneiras:

Caso de suporte

É possível abrir um caso no AWS Shield no console do AWS Support Center.

Para obter orientação sobre como criar um caso de suporte, consulte AWS Support Center.

Selecione a gravidade adequada à sua situação e forneça seus dados de contato. Na descrição, forneça o máximo de detalhes possível. Forneça informações sobre os recursos protegidos que você acredita que podem ser afetados e o estado atual da experiência do usuário final. Por exemplo, se a

experiência do usuário for degradada ou partes do aplicativo estiverem indisponíveis no momento, forneça estas informações.

- Para suspeitas de ataques de DDoS: se a disponibilidade ou a performance da aplicação estiver afetada, no momento, por um possível ataque de DDoS, escolha as seguintes opções de gravidade e de contato:
  - Para gravidade, escolha a maior gravidade disponível para seu plano de suporte:
    - Para suporte comercial, Sistema de produção inativo: < 1 hora.
    - Para suporte corporativo, Sistema essencial para os negócios inativo: < 15 minutos.
  - Para a opção de contato, selecione Telefone ou Chat e forneça seus detalhes. Usar um método de contato ao vivo fornece a resposta mais rápida.

Envolvimento proativo

Com o engajamento AWS Shield Advanced proativo, o SRT entra em contato com você diretamente se a verificação de saúde do Amazon Route 53 associada ao seu recurso protegido ficar insalubre durante um evento detectado. Para obter mais informações sobre essa opção, consulte Como configurar o engajamento proativo.

Configurando mitigações personalizadas com o Shield Response Team (SRT)

Para seus Elastic IPs (EIPs) e seus aceleradores AWS Global Accelerator padrão, você pode trabalhar com a Shield Response Team (SRT) para configurar mitigações personalizadas. Isso é útil caso você conheça uma lógica específica que deve ser aplicada quando uma mitigação é feita. Por exemplo, talvez você queira permitir somente o tráfego de determinados países, impor limites de taxa específicos, configurar validações opcionais, proibir fragmentos ou permitir somente o tráfego que corresponda a um padrão específico na carga útil do pacote.

Exemplos de soluções de mitigação personalizadas comuns incluem:

- Correspondência de padrões: se você opera um serviço que interage com aplicativos do lado do cliente, você pode optar por combinar padrões conhecidos que são exclusivos desses aplicativos. Por exemplo, você pode operar um serviço de jogos ou comunicações que exija que o usuário final instale um software específico que você distribui. Você pode incluir um número mágico em cada pacote enviado pelo aplicativo ao seu serviço. Você pode combinar até 128 bytes (separados ou contíguos) de uma carga útil e cabeçalhos de pacotes TCP ou UDP não fragmentados. A

correspondência pode ser expressa em notação hexadecimal como um deslocamento específico do início da carga útil do pacote ou um deslocamento dinâmico após um valor conhecido. Por exemplo, a mitigação pode procurar o byte `0x01` e esperar `0x12345678` como os próximos quatro bytes.

- Específico de DNS: se você opera seu próprio serviço de DNS autoritativo usando serviços como o Global Accelerator ou o Amazon Elastic Compute Cloud (Amazon EC2), você pode solicitar uma mitigação personalizada que valide pacotes para garantir que sejam consultas ao DNS válidas e aplicar uma pontuação suspeita que avalie atributos específicos do tráfego de DNS.

Para saber mais sobre como trabalhar com o SRT para criar mitigações personalizadas, crie um caso de suporte em AWS Shield. Para saber mais sobre a criação de AWS Support casos, consulte Introdução ao AWS Support.

Proteções de recursos em AWS Shield Advanced

Você pode adicionar e configurar AWS Shield Advanced proteções para seus recursos. Você pode gerenciar as proteções de um único recurso e agrupar seus recursos protegidos em coleções lógicas para melhorar o gerenciamento de eventos. Você também pode monitorar as alterações nas proteções do Shield Advanced usando AWS Config.

Tópicos

AWS Shield Advanced proteções por tipo de recurso

O Shield Advanced protege AWS recursos nas camadas de rede e transporte (camadas 3 e 4) e na camada de aplicação (camada 7). Você pode proteger alguns recursos diretamente e outros por meio da associação com recursos protegidos. O Shield Avançado oferece suporte para IPv4, mas não oferece suporte para IPv6.

Esta seção fornece informações sobre as proteções do Shield Advanced para cada tipo de recurso.

> **Note**
>
> O Shield Advanced protege somente os recursos que você especificou no Shield Advanced ou por meio de uma política AWS Firewall Manager do Shield Advanced. Ele não protege automaticamente seus recursos.

Você pode usar o Shield Advanced para monitoramento e proteção avançados com os seguintes tipos de recursos:

- CloudFront Distribuições da Amazon. Para implantação CloudFront contínua, o Shield Advanced protege qualquer distribuição temporária associada a uma distribuição primária protegida.
- Zonas hospedadas do Amazon Route 53.
- AWS Global Accelerator aceleradores padrão.
- Endereços de IP elástico do Amazon EC2. O Shield Advanced protege os recursos associados aos endereços IP elásticos protegidos.
- Instâncias do Amazon EC2, por meio de associação com endereços IP elásticos do Amazon EC2.
- Os seguintes balanceadores de carga do Elastic Load Balancing (ELB):
  - Application Load Balancers.
  - Classic Load Balancers.
  - Network Load Balancers, por meio de associações com endereços IP elásticos do Amazon EC2.

Você não pode usar o Shield Advanced para proteger nenhum outro tipo de recurso. Por exemplo, você não pode proteger aceleradores de roteamento personalizados AWS Global Accelerator ou balanceadores de carga de gateway.

Você pode monitorar e proteger até 1.000 recursos de cada um desses tipos de recurso por Conta da AWS. Por exemplo, em uma única conta, você pode proteger 1.000 endereços IP elásticos do Amazon EC2, 1.000 CloudFront distribuições e 1.000 Application Load Balancers. Você pode solicitar um aumento no número de recursos que você pode proteger com o Shield Advanced por meio do console Service Quotas em https://console.aws.amazon.com/servicequotas/.

Protegendo instâncias do Amazon EC2 e Network Load Balancers com o Shield Advanced

Você pode proteger as instâncias do Amazon EC2 e os Network Load Balancers anexando primeiro esses recursos aos endereços IP elásticos e, em seguida, protegendo os endereços IP elásticos no Shield Advanced.

Quando você protege endereços IP elásticos, o Shield Advanced identifica e protege os recursos aos quais eles estão conectados. O Shield Advanced identifica automaticamente o tipo de recurso anexado a um endereço IP elástico e aplica as detecções e mitigações apropriadas para esse recurso. Isso inclui a configuração de network ACLs específicas para esse endereço IP elástico. Para obter mais informações sobre como usar endereços IP elásticos com seus recursos da AWS , consulte o guia apropriado: Documentação do Amazon Elastic Compute Cloud ou Documentação do Elastic Load Balancing.

Durante um ataque, o Shield Advanced implanta automaticamente suas ACLs de rede na borda da AWS rede. Quando suas ACLs de rede estão na borda da rede, o Shield Advanced pode fornecer proteção contra eventos DDoS maiores. Normalmente, ACLs de rede são aplicadas perto de suas instâncias do Amazon EC2 na sua Amazon VPC. A rede ACL pode atenuar ataques somente até a capacidade máxima de processamento da Amazon VPC e da instância. Por exemplo, se a interface de rede anexada à sua instância do Amazon EC2 puder processar até 10 Gbps, volumes com mais de 10 Gbps ficarão lentos e possivelmente bloquearão o tráfego para essa instância. Durante um ataque, o Shield Advanced promove sua network ACL para a borda da AWS , que pode processar vários terabytes de tráfego. Sua network ACL é capaz de oferecer proteção para seu recurso muito além da capacidade típica da sua rede. Para obter mais informações sobre network ACLs, consulte network ACLs.

Algumas ferramentas de escalabilidade, por exemplo AWS Elastic Beanstalk, não permitem que você anexe automaticamente um endereço IP elástico a um Network Load Balancer. Nesses casos, você precisa anexar manualmente o endereço IP elástico.

AWS Shield Advanced proteções da camada de aplicação (camada 7)

Para proteger os recursos da camada de aplicação com o Shield Advanced, você começa associando uma web ACL do AWS WAF ao recurso e adicionando uma ou mais regras baseadas em intervalos a ela. Além disso, você pode ativar a mitigação automática de DDoS na camada de aplicação, o que faz com que o Shield Advanced crie e gerencie automaticamente regras de web ACL em seu nome em resposta aos ataques de DDoS.

Quando você protege um recurso da camada de aplicação com o Shield Advanced, o Shield Advanced analisa o tráfego ao longo do tempo para estabelecer e manter as referências. O Shield

Advanced usa essas referências para detectar anomalias nos padrões de tráfego que podem indicar um ataque de DDoS. O ponto em que o Shield Advanced detecta um ataque depende do tráfego que o Shield Advanced conseguiu observar antes do ataque e da arquitetura que você usa para seus aplicativos web. As variações arquitetônicas que podem afetar o comportamento do Shield Advanced incluem o tipo de instância que você usa, o tamanho da instância e se o tipo de instância oferece suporte a redes aprimoradas. Você também pode configurar o Shield Advanced para colocar automaticamente mitigações para ataques na camada de aplicação.

Assinaturas e custos do Shield Advanced AWS WAF

Sua assinatura do Shield Advanced cobre os custos de uso dos AWS WAF recursos padrão dos recursos que você protege com o Shield Advanced. As AWS WAF taxas padrão cobertas pelas proteções Shield Advanced são o custo por ACL da web, o custo por regra e o preço base por milhão de solicitações para inspeção de solicitações da web, até 1.500 WCUs e até o tamanho padrão do corpo.

A ativação da mitigação automática de DDoS na camada de aplicação do Shield Advanced adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced, O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).

Sua assinatura do Shield Advanced não cobre o uso AWS WAF de recursos que você não protege usando o Shield Advanced. Também não cobre nenhum custo adicional não padronizado AWS WAF para recursos protegidos. Exemplos de AWS WAF custos não padrão são aqueles para o Bot Control, para a ação da CAPTCHA regra, para ACLs da web que usam mais de 1.500 WCUs e para inspecionar o corpo da solicitação além do tamanho padrão. A lista completa é fornecida na página AWS WAF de preços.

Para obter informações completas e exemplos de preços, consulte Preços do Shield e Preços do AWS WAF.

Tópicos

- Detecção e mitigação
- ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas
- Mitigação automática de DDoS da camada de aplicação do Shield Advanced

Detecção e mitigação

Esta seção descreve os fatores que afetam a detecção e a mitigação dos eventos da camada de aplicação pelo Shield Advanced.

Verificações de integridade

As verificações de saúde que relatam com precisão a integridade geral do seu aplicativo fornecem ao Shield Advanced informações sobre as condições de tráfego que seu aplicativo está enfrentando. O Shield Advanced exige menos informações que apontem para um possível ataque quando seu aplicativo está relatando problemas de integridade e exige mais evidências de um ataque se seu aplicativo estiver relatando integridade.

É importante configurar suas verificações de saúde para que elas relatem com precisão a integridade do aplicativo. Para obter mais informações e orientações, consulte Detecção baseada em saúde usando verificações de saúde.

Linhas de base de tráfego

As linhas de base de tráfego fornecem ao Shield Advanced informações sobre as características do tráfego normal do seu aplicativo. O Shield Advanced usa essas linhas de base para reconhecer quando seu aplicativo não está recebendo tráfego normal, para que ele possa notificá-lo e, conforme configurado, começar a criar e testar opções de mitigação para combater um possível ataque. Para obter informações adicionais sobre como o Shield Advanced usa linhas de base de tráfego para detectar possíveis eventos, consulte a seção de visão geral. Lógica de detecção para ameaças na camada de aplicativo

O Shield Advanced cria suas linhas de base a partir das informações fornecidas pela ACL da web que estão associadas ao recurso protegido. A ACL da web deve estar associada ao recurso por pelo menos 24 horas e até 30 dias antes que o Shield Advanced possa determinar com segurança as linhas de base do aplicativo. O tempo necessário começa quando você associa a Web ACL, por meio do Shield Advanced ou por meio AWS WAF de.

Para obter mais informações sobre o uso de uma Web ACL com as proteções da camada de aplicação Shield Advanced, consulte. ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas

Regras com base em taxa

Regras baseadas em taxas podem ajudar a mitigar ataques. Eles também podem obscurecer os ataques, mitigando-os antes que se tornem um problema grande o suficiente para aparecer nas linhas de base do tráfego normal ou nos relatórios de status da verificação de saúde.

Recomendamos o uso de regras baseadas em taxas em sua ACL da web ao proteger um recurso de aplicativo com o Shield Advanced. Embora suas mitigações possam ocultar um possível ataque, elas são uma valiosa primeira linha de defesa, ajudando a garantir que seu aplicativo permaneça disponível para seus clientes legítimos. O tráfego que suas regras baseadas em tarifas detectam e limitam a taxa é visível em suas AWS WAF métricas.

Além de suas próprias regras baseadas em taxas, se você ativar a mitigação automática de DDoS na camada de aplicação, o Shield Advanced adicionará um grupo de regras à sua ACL da web que ele usa para mitigar ataques. Nesse grupo de regras, o Shield Advanced sempre tem uma regra baseada em taxas que limita o volume de solicitações de endereços IP que são conhecidos por serem fontes de ataques de DDoS. As métricas do tráfego que as regras do Shield Advanced mitigam não estão disponíveis para você visualizar.

Para obter mais informações sobre regras baseadas em taxas, consulte. Instrução de regra baseada em intervalos Para obter informações sobre a regra baseada em taxas que o Shield Advanced usa para mitigação automática de DDoS na camada de aplicação, consulte. O grupo de regras do Shield Advanced

Para obter mais informações sobre Shield Advanced e AWS WAF métricas, consulteMonitoramento com a Amazon CloudWatch.

ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas

Para proteger um recurso da camada de aplicativo com o Shield Advanced, você começa associando uma ACL AWS WAF da web ao recurso. AWS WAF é um firewall de aplicativo web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas para os recursos da camada de aplicativos e permite controlar o acesso ao seu conteúdo com base nas características das solicitações. Você pode configurar uma web ACL para monitorar e gerenciar solicitações com base em fatores como a origem da solicitação, o conteúdo das sequências de caracteres de consulta e dos cookies e a taxa de solicitações provenientes de um único endereço IP. No mínimo, sua proteção Shield Advanced exige que você associe uma web ACL a uma regra baseada em intervalos, que limita a taxa de solicitações para cada endereço IP.

Se a web ACL associada não tiver uma regra baseada em intervalos definida, o Shield Advanced solicitará que você defina pelo menos uma. As regras baseadas em intervalos bloqueiam automaticamente o tráfego dos IPs de origem quando excedem os limites definidos por você. Elas ajudam a proteger seu aplicativo contra inundações de solicitações da web e podem fornecer alertas sobre picos repentinos no tráfego que podem indicar um possível ataque de DDoS.

> **Note**
>
> Uma regra baseada em taxas responde muito rapidamente aos picos no tráfego que a regra está monitorando. Por esse motivo, uma regra baseada em taxas pode impedir não apenas um ataque, mas também a detecção de um possível ataque pela detecção do Shield Advanced. Essa compensação favorece a prevenção em vez da visibilidade completa dos padrões de ataque. Recomendamos usar uma regra baseada em taxas como sua primeira linha de defesa contra ataques.

Com sua web ACL em vigor, se ocorrer um ataque de DDoS, você aplica mitigações adicionando e gerenciando regras na web ACL. Você pode fazer isso diretamente, com a ajuda da Shield Response Team (SRT), ou automaticamente por meio da mitigação automática de DDoS na camada de aplicação.

> **Important**
>
> Se você também usa a mitigação automática de DDoS na camada de aplicação, consulte as melhores práticas para gerenciar sua ACL da web em. Práticas recomendadas para usar a mitigação automática

Comportamento padrão de regras com base em taxas

Quando você usa uma regra baseada em taxa com sua configuração padrão, avalia AWS WAF periodicamente o tráfego na janela de tempo anterior de 5 minutos. AWS WAF bloqueia solicitações de qualquer endereço IP que exceda o limite da regra até que a taxa de solicitação caia para um nível aceitável. Ao configurar uma regra baseada em taxa por meio do Shield Advanced, configure seu limite de taxa para um valor maior do que a taxa de tráfego normal que você espera de qualquer IP de origem em qualquer janela de cinco minutos.

Talvez você queira usar mais de uma regra baseada em intervalos em uma web ACL. Por exemplo, você pode ter uma regra baseada em intervalos para todo o tráfego que tenha um limite alto,

além de uma ou mais regras adicionais configuradas para corresponder a partes selecionadas do seu aplicativo web e que tenham limites mais baixos. Por exemplo, você pode combinar o URI `/login.html` com um limite mais baixo para mitigar o abuso em uma página de login.

Você pode configurar uma regra baseada em taxa para usar uma janela de tempo de avaliação diferente e agregar solicitações por vários componentes da solicitação, como valores de cabeçalho, rótulos e argumentos de consulta. Para ter mais informações, consulte Instrução de regra baseada em intervalos.

Para obter informações e orientações adicionais, consulte a postagem do blog de segurança As três regras AWS WAF baseadas em taxas mais importantes.

Opções de configuração expandidas por meio de AWS WAF

O console Shield Advanced permite que você adicione uma regra baseada em taxas e a configure com as configurações básicas padrão. Você pode definir opções de configuração adicionais gerenciando suas regras baseadas em taxas por meio de. AWS WAF Por exemplo, você pode configurar a regra para agregar solicitações com base em chaves como um endereço IP encaminhado, uma sequência de caracteres de consulta e um rótulo. Você também pode adicionar uma declaração de redução de escopo à regra para filtrar algumas solicitações de avaliação e limitação de intervalo. Para ter mais informações, consulte Instrução de regra baseada em intervalos. Para obter informações sobre como usar AWS WAF para gerenciar suas regras de monitoramento e gerenciamento de solicitações da web, consulteCriação de uma web ACL.

Mitigação automática de DDoS da camada de aplicação do Shield Advanced

Você pode configurar o Shield Advanced para responder automaticamente para mitigar os ataques na camada de aplicação (camada 7) contra seus recursos protegidos da camada de aplicação, contando ou bloqueando as solicitações da web que fazem parte do ataque. Essa opção é uma adição à proteção da camada de aplicação que você adiciona por meio do Shield Advanced com uma ACL AWS WAF da web e sua própria regra baseada em taxas.

Quando a mitigação automática está habilitada para um recurso, o Shield Avançado mantém um grupo de regras na ACL da Web que está associada ao recurso, em que gerencia as regras de mitigação em nome do recurso. O grupo de regras contém uma regra baseada em intervalos que rastreia o volume de solicitações de endereços IP conhecidos por serem fontes de ataques de DDoS.

Além disso, o Shield Avançado compara os padrões de tráfego atuais com as linhas de base de tráfego históricas para detectar desvios que possam indicar um ataque de DDoS. O Shield Advanced

responde aos ataques de DDoS detectados criando, avaliando e implantando AWS WAF regras personalizadas adicionais no grupo de regras.

Sumário

Advertências para o uso da mitigação automática

A lista a seguir descreve as advertências da mitigação automática de DDoS na camada de aplicação Shield Advanced e descreve as etapas que você deve seguir em resposta.

- A mitigação automática de DDoS na camada de aplicativo funciona somente com ACLs da web que foram criadas usando a versão mais recente do (v2). AWS WAF
- O Shield Advanced requer tempo para estabelecer uma linha de base do tráfego normal e histórico do seu aplicativo, que ele utiliza para detectar e isolar o tráfego de ataque do tráfego normal, a fim de mitigar o tráfego de ataque. O tempo para estabelecer uma linha de base é entre 24 horas e 30 dias a partir do momento em que você associa uma ACL da web ao recurso de aplicativo protegido. Para obter informações adicionais sobre linhas de base de tráfego, consulte. Detecção e mitigação

- A ativação automática da mitigação de DDoS na camada de aplicação adiciona um grupo de regras à sua ACL da web que usa 150 unidades de capacidade da ACL da web (WCUs). Essas WCUs contam contra o uso de WCU em sua web ACL. Para obter mais informações, consulte O grupo de regras do Shield Advanced e AWS WAF unidades de capacidade web ACL (WCUs).
- O grupo de regras Shield Advanced gera AWS WAF métricas, mas elas não estão disponíveis para visualização. Isso é o mesmo que para qualquer outro grupo de regras que você usa em sua ACL da web, mas não possui, como grupos de regras de regras AWS gerenciadas. Para obter mais informações sobre AWS WAF métricas, consulteAWS WAF métricas e dimensões. Para obter informações sobre essa opção de proteção Shield Advanced, consulteMitigação automática de DDoS da camada de aplicação do Shield Advanced.
- Para ACLs da web que protegem vários recursos, a mitigação automática implementa apenas atenuações personalizadas que não afetam negativamente nenhum dos recursos protegidos.
- O tempo entre o início de um ataque de DDoS e o momento em que o Shield Avançado estabelece as regras de mitigação automáticas personalizadas varia de acordo com cada evento. Alguns ataques de DDoS podem terminar antes da implantação das regras personalizadas. Outros ataques podem ocorrer quando já existe uma mitigação e, portanto, podem ser mitigados por essas regras desde o início do evento. Além disso, as regras baseadas em taxas no grupo de regras Web ACL e Shield Advanced podem mitigar o tráfego de ataque antes que ele seja detectado como um possível evento.
- Para Application Load Balancers que recebem qualquer tráfego por meio de uma rede de distribuição de conteúdo (CDN), como a Amazon CloudFront, os recursos de mitigação automática da camada de aplicação do Shield Advanced para esses recursos do Application Load Balancer serão reduzidos. O Shield Advanced usa atributos de tráfego do cliente para identificar e isolar o tráfego de ataque do tráfego normal para seu aplicativo, e as CDNs podem não preservar ou encaminhar os atributos originais do tráfego do cliente. Se você usa CloudFront, recomendamos ativar a mitigação automática na CloudFront distribuição.
- A mitigação automática de DDoS na camada de aplicaçãos não interage com grupos de proteção. Você pode ativar a mitigação automática para recursos que estão em grupos de proteção, mas o Shield Advanced não aplica automaticamente mitigações de ataques com base nas descobertas do grupo de proteção. O Shield Advanced aplica mitigações automáticas de ataques para recursos individuais.

Práticas recomendadas para usar a mitigação automática

Siga as orientações fornecidas nesta seção ao usar a mitigação automática.

Gerenciamento geral de proteções

Siga estas diretrizes para planejar e implementar suas proteções de mitigação automática.

- Gerencie todas as suas proteções de mitigação automática por meio do Shield Advanced ou, se você estiver usando AWS Firewall Manager para gerenciar suas configurações de mitigação automática do Shield Advanced, por meio do Firewall Manager. Não misture o uso do Shield Advanced com o Firewall Manager para gerenciar essas proteções.
- Gerencie recursos semelhantes usando as mesmas web ACLs e configurações de proteção e gerencie recursos diferentes usando web ACLs diferentes. Quando o Shield Advanced mitiga um ataque de DDoS em um recurso protegido, ele define regras para a web ACL associada ao recurso e, em seguida, testa as regras em relação ao tráfego de todos os recursos associados à web ACL. O Shield Advanced só aplicará as regras se elas não afetarem negativamente nenhum dos recursos associados. Para ter mais informações, consulte Como o Shield Advanced gerencia a mitigação automática.
- Para balanceadores de carga de aplicativos que têm todo o tráfego da Internet enviado por proxy por meio de uma CloudFront distribuição da Amazon, ative apenas a mitigação automática na distribuição. CloudFront A CloudFront distribuição sempre terá o maior número de atributos de tráfego originais, que o Shield Advanced aproveita para mitigar os ataques.

Otimização de detecção e mitigação

Siga essas diretrizes para otimizar as proteções que a mitigação automática fornece aos recursos protegidos. Para obter uma visão geral da detecção e mitigação da camada de aplicação, consulte. Detecção e mitigação

- Configure verificações de saúde para seus recursos protegidos e use-as para habilitar a detecção baseada na saúde em suas proteções Shield Advanced. Para obter orientações, consulte Detecção baseada em saúde usando verificações de saúde.
- Ative a mitigação automática no Count modo até que o Shield Advanced estabeleça uma linha de base para o tráfego normal e histórico. O Shield Advanced precisa de 24 horas a 30 dias para estabelecer uma linha de base.

  Estabelecer uma linha de base dos padrões normais de tráfego requer o seguinte:

  - A associação de uma ACL da web com o recurso protegido. Você pode usar AWS WAF diretamente para associar sua ACL da web ou pode fazer com que o Shield Advanced a associe

ao habilitar a proteção da camada de aplicação Shield Advanced e especificar uma ACL da web a ser usada.

- Fluxo de tráfego normal para seu aplicativo protegido. Se seu aplicativo não estiver recebendo tráfego normal, como antes do lançamento do aplicativo, ou se ele não tiver tráfego de produção por longos períodos de tempo, os dados históricos não poderão ser coletados.

Gerenciamento da web ACL

Siga estas diretrizes para gerenciar as ACLs da web que você usa com mitigação automática.

- Se você precisar substituir a Web ACL associada ao recurso protegido, faça as seguintes alterações na ordem:
  1. No Shield Advanced, desative a mitigação automática.
  2. Em AWS WAF, desassocie a ACL da web antiga e associe a nova ACL da web.
  3. No Shield Advanced, ative a mitigação automática.

  O Shield Advanced não transfere automaticamente a mitigação automática da ACL da web antiga para a nova.
- Não exclua nenhuma regra de grupo de regras de suas web ACLs cujo nome comece com `ShieldMitigationRuleGroup`. Se você excluir esse grupo de regras, desabilitará as proteções fornecidas pela mitigação automática do Shield Advanced para cada recurso associado à Web ACL. Além disso, o Shield Advanced pode levar algum tempo para receber a notificação da alteração e atualizar suas configurações. Durante esse período, as páginas do console Shield Advanced fornecerão informações incorretas.

  Para obter mais informações sobre o grupo de regras, consulte O grupo de regras do Shield Advanced.
- Não modifique o nome de uma regra do grupo de regras cujo nome comece por `ShieldMitigationRuleGroup`. Isso também pode interferir nas proteções fornecidas pela mitigação automática do Shield Advanced por meio da web ACL.
- Ao criar regras e grupos de regras, não use nomes que comecem com `ShieldMitigationRuleGroup`. Essa sequência de caracteres é usada pelo Shield Advanced para gerenciar suas mitigações automáticas.
- No gerenciamento de suas regras de web ACL, não atribua uma configuração de prioridade de 10.000.000. O Shield Advanced atribui essa configuração de prioridade à sua regra de grupo de regras de mitigação automática quando a adiciona.

- Mantenha a regra `ShieldMitigationRuleGroup` priorizada para que ela seja executada quando você quiser em relação às outras regras em sua web ACL. O Shield Advanced adiciona a regra do grupo de regras à web ACL com prioridade 10.000.000, para ser executada após suas outras regras. Se você usar o assistente do AWS WAF console para gerenciar sua ACL da web, ajuste as configurações de prioridade conforme necessário depois de adicionar regras à ACL da web.
- Se você usa AWS CloudFormation para gerenciar suas ACLs da web, não precisa gerenciar a `ShieldMitigationRuleGroup` regra do grupo de regras. Siga as orientações em Usando AWS CloudFormation com a mitigação automática de DDoS na camada de aplicativos.

Configuração necessária para permitir a mitigação automática

Você ativa a mitigação automática do Shield Advanced como parte das proteções contra DDoS da camada de aplicação para seu recurso. Para obter informações sobre fazer isso no console, consulte Configurar as proteções contra DDoS na camada de aplicação.

A funcionalidade de mitigação automática exige que você faça o seguinte:

- Associe uma web ACL ao recurso — Isso é necessário para qualquer proteção da camada de aplicação Shield Advanced. É possível usar a mesma web ACL para vários recursos. Recomendamos fazer isso somente para recursos com tráfego semelhante. Para obter informações sobre web ACLs, incluindo os requisitos para usá-las com vários recursos, consulte Como AWS WAF funciona.
- Ative e configure a mitigação automática de DDoS da camada de aplicação do Shield Advanced — Ao ativá-la, você especifica se deseja que o Shield Advanced bloqueie ou conte automaticamente as solicitações da web que ele determina como parte de um ataque de DDoS. O Shield Advanced adiciona um grupo de regras à web ACL associada e o usa para gerenciar dinamicamente sua resposta aos ataques de DDoS ao recurso. Para obter informações sobre as opções de ações de regras, consulte Ação da regra.
- (Opcional, mas recomendado) Adicione uma regra baseada em intervalos à web ACL — Por padrão, a regra baseada em intervalos fornece ao seu recurso proteção básica contra ataques de DDoS, impedindo que qualquer endereço IP individual envie muitas solicitações em pouco tempo. Para obter informações sobre regras baseadas em intervalos, incluindo opções e exemplos personalizados de agregação de solicitações, consulte Instrução de regra baseada em intervalos.

Como o Shield Advanced gerencia a mitigação automática

Os tópicos da seção descrevem como o Shield Advanced lida com suas alterações de configuração para mitigação automática de DDoS na camada de aplicação e como ele lida com ataques de DDoS quando a mitigação automática está ativada.

Tópicos

O que acontece quando você ativa a mitigação automática

O Shield Advanced faz o seguinte quando você ativa a mitigação automática:

- Conforme necessário, adiciona um grupo de regras para uso do Shield Advanced — Se a ACL AWS WAF da web que você associou ao recurso ainda não tiver uma AWS WAF regra de grupo de regras dedicada à mitigação automática de DDoS na camada de aplicação, o Shield Advanced adicionará uma.

  O nome da regra do grupo de regras começa com `ShieldMitigationRuleGroup`. O grupo de regras sempre contém uma regra baseada em intervalos chamada `ShieldKnownOffenderIPRateBasedRule`, que limita o volume de solicitações de endereços IP conhecidos por serem fontes de ataques de DDoS. Para obter detalhes adicionais sobre o grupo de regras do Shield Avançado e a regra de ACL da Web que faz referência a ele, consulte O grupo de regras do Shield Advanced.
- Começa a responder aos ataques de DDoS contra o recurso — o Shield Advanced responde automaticamente aos ataques de DDoS do recurso protegido. Além da regra baseada em taxas, que está sempre presente, o Shield Advanced usa seu grupo de regras para implantar AWS WAF regras personalizadas para mitigação de ataques de DDoS. O Shield Advanced adapta essas regras ao seu aplicativo e aos ataques que seu aplicativo enfrenta e as testa em relação ao tráfego histórico do recurso antes de implantá-las.

O Shield Advanced usa uma única regra de grupo de regras em qualquer web ACL que você usa para mitigação automática. Se o Shield Avançado já tiver adicionado o grupo de regras para outro recurso protegido, ele não adicionará outro grupo de regras à ACL da Web.

A mitigação automática de DDoS na camada de aplicação depende da presença do grupo de regras para mitigar os ataques. Se o grupo de regras for removido da ACL da AWS WAF web por qualquer motivo, a remoção desativará a mitigação automática de todos os recursos associados à ACL da web.

Como o Shield Advanced responde aos ataques de DDoS com mitigação automática

Quando você tem a mitigação automática habilitada em um recurso protegido, a regra baseada em intervalos `ShieldKnownOffenderIPRateBasedRule` no grupo de regras do Shield Avançado responde automaticamente a volumes elevados de tráfego provenientes de fontes de DDoS conhecidas. Essa limitação de volume é aplicada rapidamente e atua como uma defesa de linha de frente contra os ataques.

Quando o Shield Avançado detecta um ataque, ele faz o seguinte:

1. Tenta identificar uma assinatura de ataque que isole o tráfego de ataque do tráfego normal para seu aplicativo. O objetivo é produzir regras de mitigação de DDoS de alta qualidade que, quando implementadas, afetem somente o tráfego de ataque e não afetem o tráfego normal do seu aplicativo.
2. Avalia a assinatura de ataque identificada em relação aos padrões históricos de tráfego do recurso que está sob ataque, bem como de qualquer outro recurso associado à mesma web ACL. O Shield Advanced faz isso antes de implantar qualquer regra em resposta ao evento.

   Dependendo dos resultados da avaliação, o Shield Advanced executará um dos seguintes procedimentos:

   - Se o Shield Avançado determinar que a assinatura do ataque isola somente o tráfego envolvido no ataque de DDoS, ele implementará a assinatura nas regras do AWS WAF no grupo de regras de mitigação do Shield Avançado na ACL da Web. O Shield Advanced fornece a essas regras a configuração de ação que você configurou para a mitigação automática do recurso - Count ou Block.
   - Caso contrário, o Shield Advanced não coloca uma mitigação.

Durante um ataque, o Shield Advanced envia as mesmas notificações e fornece as mesmas informações de eventos das proteções básicas da camada de aplicação do Shield Advanced. Você

pode ver as informações sobre eventos e ataques de DDoS e sobre qualquer mitigação de ataques do Shield Advanced no console de eventos do Shield Advanced. Para mais informações, consulte Visibilidade de eventos de DDoS.

Se você configurou a mitigação automática para usar a ação da regra Block e detectou falsos positivos nas regras de mitigação implantadas pelo Shield Advanced, você pode alterar a ação da regra para Count. Para obter informações sobre como fazer isso, consulte Como alterar a ação usada para mitigação automática de DDoS na camada de aplicação.

Como o Shield Avançado gerencia a configuração de ação de regra

É possível definir a ação de regra para suas mitigações automáticas como Block ou Count.

Quando você altera a configuração de ação da regra de mitigação automática para um recurso protegido, o Shield Advanced atualiza todas as configurações de regra do recurso. Ele atualiza todas as regras atualmente em vigor para o recurso no grupo de regras do Shield Avançado e usa a nova configuração de ação ao criar novas regras.

Para os recursos que usam a mesma ACL da Web, se você especificar ações diferentes, o Shield Avançado usará a configuração de ação Block para a regra baseada em intervalos `ShieldKnownOffenderIPRateBasedRule` do grupo de regras. O Shield Avançado cria e gerencia outras regras no grupo de regras em nome de um recurso protegido específico e usa a configuração de ação que você especificou para o recurso. Todas as regras do grupo de regras do Shield Avançado em uma ACL da Web são aplicadas ao tráfego da Web de todos os recursos associados.

A alteração da configuração de ação pode levar alguns segundos para ser propagada. Durante esse período, você pode ver a configuração antiga em alguns lugares onde o grupo de regras está em uso, e a nova configuração em outros lugares.

Você pode alterar a configuração da ação da regra para sua configuração de mitigação automática na página de eventos do console e por meio da página de configuração da camada de aplicação. Para obter mais informações sobre eventos, consulte o Resposta a eventos de DDoS. Para obter mais informações sobre a página de configuração, consulte Configurar as proteções contra DDoS na camada de aplicação.

Como o Shield Advanced gerencia as mitigações quando um ataque diminui

Quando o Shield Advanced determina que as regras de mitigação que foram implantadas para um ataque específico não são mais necessárias, ele as remove do grupo de regras de mitigação do Shield Advanced.

A remoção das regras de mitigação não coincidirá necessariamente com o fim de um ataque. O Shield Advanced monitora os padrões de ataque que ele detecta em seus recursos protegidos. Ele pode se defender proativamente contra a recorrência de um ataque com uma assinatura específica, mantendo em vigor as regras que implantou contra a ocorrência inicial desse ataque. Conforme necessário, o Shield Advanced aumenta a janela de tempo em que mantém as regras em vigor. Dessa forma, o Shield Advanced pode mitigar ataques repetidos com uma assinatura específica antes que eles afetem seus recursos protegidos.

O Shield Avançado nunca remove a regra baseada em intervalos `ShieldKnown0ffenderIPRateBasedRule`, que limita o volume de solicitações de endereços IP conhecidos por serem fontes de ataques de DDoS.

O que acontece quando você desativa a mitigação automática

O Shield Advanced faz o seguinte quando você desativa a mitigação automática para um recurso:

- Para de responder automaticamente aos ataques de DDoS — o Shield Advanced interrompe suas atividades de resposta automática para o recurso.
- Remove regras desnecessárias do grupo de regras do Shield Advanced — Se o Shield Advanced estiver mantendo alguma regra em seu grupo de regras gerenciadas em nome do recurso protegido, ele as removerá.
- Remove o grupo de regras Shield Advanced, se ele não estiver mais em uso — Se a web ACL que você associou ao recurso não estiver associada a nenhum outro recurso com a mitigação automática ativada, o Shield Advanced removerá sua regra de grupo de regras da web ACL.

O grupo de regras do Shield Advanced

O Shield Avançado gerencia atividades de mitigação automática usando regras em um grupo de regras de que ele é proprietário e gerencia para você. O Shield Avançado faz referência ao grupo de regras com uma regra na ACL da Web que você associou ao seu recurso protegido.

A regra do grupo de regras em sua ACL da Web

A regra do grupo de regras do Shield Avançado em sua ACL da Web tem as seguintes propriedades:

- Nome: `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- Unidades de capacidade de web ACL (WCU): 150. Essas WCUs contam contra o uso de WCU em sua web ACL.

O Shield Advanced cria essa regra em sua ACL da web com uma configuração de prioridade de 10.000.000, para que ela seja executada após suas outras regras e grupos de regras na ACL da web. AWS WAF executa as regras em uma ACL da web a partir da configuração de prioridade numérica mais baixa. Durante o gerenciamento da web ACL, essa configuração de prioridade pode mudar.

A funcionalidade de mitigação automática não consome recursos adicionais do AWS WAF em sua conta, exceto as WCUs usadas pelo grupo de regras na ACL da Web. Por exemplo, o grupo de regras do Shield Advanced não é contado como um dos grupos de regras da sua conta. Para obter informações sobre limites de conta em AWS WAF, consulteAWS WAF cotas.

Regras no grupo de regras

No grupo de regras referenciado do Shield Avançado, o Shield Avançado mantém uma regra baseada em intervalos `ShieldKnownOffenderIPRateBasedRule`, que limita o volume de solicitações de endereços IP conhecidos por serem fontes de ataques de DDoS. Essa regra atua como a primeira linha de defesa contra qualquer ataque, pois está sempre presente no grupo de regras e não depende da análise de padrões de tráfego para conter os ataques. A ação desta regra é definida como a ação que você escolhe para suas mitigações automáticas, assim como ocorre com as outras regras no grupo de regras. Para obter mais informações sobre regras baseadas em intervalos, consulte Instrução de regra baseada em intervalos.

> **Note**
>
> A regra baseada em taxas `ShieldKnownOffenderIPRateBasedRule` opera independentemente da detecção de eventos do Shield Advanced. Embora a mitigação automática esteja ativada, essa taxa de regra limita os endereços IP que são conhecidos por serem fontes de ataques de DDoS. Para esses endereços IP, a limitação de taxa da regra pode evitar ataques e também impedir que os ataques apareçam nas informações de detecção do Shield Advanced. Essa compensação favorece a prevenção em vez da visibilidade completa dos padrões de ataque.

Além da regra permanente baseada em taxas descrita acima, o grupo de regras contém todas as regras que a Shield Advanced está usando atualmente para mitigar ataques de DDoS. O Shield Avançado adiciona, modifica e remove essas regras, conforme necessário. Para mais informações, consulte Como o Shield Advanced gerencia a mitigação automática.

Indicadores

O grupo de regras gera AWS WAF métricas, mas como esse grupo de regras é de propriedade da Shield Advanced, essas métricas não estão disponíveis para visualização. Para ter mais informações, consulte AWS WAF métricas e dimensões.

Como gerenciar a mitigação automática de DDoS na camada de aplicação

Use as orientações desta seção para gerenciar suas configurações de mitigação automáticas de DDoS na camada de aplicação. Para obter informações sobre como funciona a mitigação automática, consulte os tópicos anteriores.

> **Note**
>
> Siga as melhores práticas descritas emPráticas recomendadas para usar a mitigação automática.

Tópicos

- Como visualizar a configuração de mitigação automática de DDoS da camada de aplicação de um recurso
- Como ativar e desativar a mitigação automática de DDoS na camada de aplicação
- Como alterar a ação usada para mitigação automática de DDoS na camada de aplicação
- Usando AWS CloudFormation com a mitigação automática de DDoS na camada de aplicativos

Como visualizar a configuração de mitigação automática de DDoS da camada de aplicação de um recurso

Você pode visualizar a configuração de mitigação automática de DDoS da camada de aplicação de um recurso na página Recursos protegidos e nas páginas de proteções individuais.

Para visualizar a configuração de mitigação automática de DDoS da camada de aplicação

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos. Na lista de recursos protegidos, a coluna Mitigação automática de DDoS na camada de aplicação indica se a mitigação automática está ativada e, quando ativada, a ação que o Shield Advanced deve usar em suas mitigações.

Você também pode selecionar qualquer recurso da camada de aplicação para ver as mesmas informações listadas na página de proteções do recurso.

Como ativar e desativar a mitigação automática de DDoS na camada de aplicação

O procedimento a seguir mostra como ativar ou desativar a resposta automática para um recurso protegido.

Para ativar ou desativar a mitigação automática de DDoS na camada de aplicação para um único recurso

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na guia Proteções, selecione o recurso da camada de aplicação para o qual você deseja ativar a mitigação automática. A página de proteções do recurso é aberta.
4. Na página de proteções do recurso, escolha Editar.
5. Na página Configurar a mitigação de DDoS da camada 7 para recursos globais: opcional para a Mitigação automática de DDoS na camada de aplicação, escolha a opção que você deseja usar para mitigações automáticas. As opções para o console são as seguintes:

   - Manter as configurações atuais: — Não fazer alterações nas configurações de mitigação automática do recurso protegido.
   - Ativar: — Ativar a mitigação automática para o recurso protegido. Ao escolher isso, selecione também a ação de regra que você deseja que as mitigações automáticas usem nas regras de web ACL. Para informações sobre as configurações de ações de regra, consulte Ação da regra.

     Se seu recurso protegido ainda não tiver um histórico de tráfego normal de aplicativos, ative a mitigação automática no Count modo até que o Shield Advanced possa estabelecer uma linha de base. O Shield Advanced começa a coletar informações para sua linha de base quando você associa uma ACL da web ao seu recurso protegido, e pode levar de 24 horas a 30 dias para estabelecer uma boa linha de base do tráfego normal.
   - Desativar: — Desativar a mitigação automática para o recurso protegido.
6. Percorra o restante das páginas até terminar e salve a configuração.

Na página Proteções, as configurações de mitigação automática são atualizadas para o recurso.

Como alterar a ação usada para mitigação automática de DDoS na camada de aplicação

Você pode alterar a ação que o Shield Advanced usa para a resposta automática da camada de aplicação em vários locais no console:

- Configuração de mitigação automática: — Altere a ação ao configurar a mitigação automática para seu recurso. Para ver o procedimento, consulte a seção Como ativar e desativar a mitigação automática de DDoS na camada de aplicação anterior.
- Página de detalhes do evento: — Altere a ação na página de detalhes do evento ao visualizar as informações do evento no console. Para mais informações, consulte AWS Shield Advanced detalhes do evento.

Se você tem dois recursos protegidos que compartilham uma ACL da Web e define a ação como Count para um dos recursos e Block para o outro, o Shield Avançado definirá a ação da regra baseada em intervalos `ShieldKnownOffenderIPRateBasedRule` do grupo de regras como Block.

Usando AWS CloudFormation com a mitigação automática de DDoS na camada de aplicativos

Entenda como usar AWS CloudFormation para gerenciar suas proteções e ACLs AWS WAF da web.

Como ativar ou desativar a mitigação automática de DDoS na camada de aplicação

Você pode ativar e desativar a mitigação automática de DDoS na camada de aplicação usando AWS CloudFormation o recurso. `AWS::Shield::Protection` O efeito é o mesmo de quando você ativa ou desativa o atributo por meio do console ou de qualquer outra interface. Para obter informações sobre o AWS CloudFormation recurso, consulte AWS::Shield::Protectiono guia AWS CloudFormation do usuário.

Como gerenciar web ACLs usadas com mitigação automática

O Shield Advanced gerencia a mitigação automática para seu recurso protegido usando uma regra de grupo de regras na ACL da AWS WAF web do recurso protegido. Por meio do AWS WAF console e das APIs, você verá a regra listada em suas regras de ACL da web, com um nome que começa com. `ShieldMitigationRuleGroup` Essa regra é dedicada à mitigação automática de DDoS na camada de aplicação, e é gerenciada para você pelo Shield Advanced e AWS WAF. Para ter mais informações, consulte O grupo de regras do Shield Advanced e Como o Shield Advanced gerencia a mitigação automática.

Se você usa AWS CloudFormation para gerenciar suas ACLs da web, não adicione a regra de grupo de regras Shield Advanced ao seu modelo de ACL da web. Quando você atualiza uma ACL da web que está sendo usada com suas proteções de mitigação automática, gerencia AWS WAF automaticamente a regra do grupo de regras na ACL da web.

Você verá as seguintes diferenças em comparação com outras ACLs da web que você gerencia por meio AWS CloudFormation de:

- AWS CloudFormation não relatará nenhum desvio no status de desvio da pilha entre a configuração real da ACL da web, com a regra de grupo de regras Shield Advanced, e seu modelo de ACL da web, sem a regra. A regra Shield Advanced não aparecerá na listagem real do recurso nos detalhes de oscilação.

  Você poderá ver a regra de grupo de regras do Shield Advanced nas listagens de ACL da web das quais você recupera AWS WAF, como por meio do AWS WAF console ou AWS WAF das APIs.
- Se você modificar o modelo de ACL da web em uma pilha, o AWS WAF Shield Advanced mantiver automaticamente a regra de mitigação automática do Shield Advanced na ACL da web atualizada. As proteções de mitigação automática fornecidas pelo Shield Advanced não são interrompidas por sua atualização na web ACL.

Não gerencie a regra Shield Advanced em seu modelo de ACL AWS CloudFormation da web. O modelo de web ACL não deve listar a regra do Shield Advanced. Siga as práticas recomendadas para gerenciamento de web ACL em Práticas recomendadas para usar a mitigação automática.

Detecção baseada em saúde usando verificações de saúde

Você pode configurar o Shield Advanced para usar a detecção baseada em integridade, o que pode melhorar a capacidade de resposta e a precisão na detecção e mitigação de ataques. Você pode usar essa opção com qualquer tipo de recurso, exceto para zonas hospedadas do Route 53.

Para configurar a detecção baseada em integridade, você define uma verificação de integridade para seu recurso no Route 53, verifica se o relatório indica integridade e, em seguida, associa-o à sua proteção Shield Advanced. Para obter informações sobre as verificações de integridade do Route 53, consulte Como o Amazon Route 53 verifica a integridade de seus recursos e Comocriar, atualizar e excluir verificações de integridade no Guia do desenvolvedor do Amazon Route 53.

> **Note**
>
> As verificações de integridade são necessárias para o suporte de engajamento proativo da Shield Response Team (SRT). Para obter informações sobre engajamento proativo, consulte Como configurar o engajamento proativo.

As verificações de integridade medem a integridade dos recursos com base nos requisitos definidos por você. O status da verificação de integridade fornece informações vitais para os mecanismos de detecção do Shield Advanced, proporcionando maior sensibilidade ao estado atual de seus aplicativos específicos.

Você pode usar a detecção baseada em integridade para qualquer tipo de recurso, exceto as zonas hospedadas do Route 53.

- Recursos da camada de rede e transporte (camada 3/camada 4) — A detecção baseada em integridade melhora a precisão da detecção e mitigação de eventos na camada de rede e na camada de transporte para Network Load Balancers, endereços IP elásticos e aceleradores padrão do Global Accelerator. Quando você protege esses tipos de recursos com o Shield Advanced, o Shield Advanced pode fornecer mitigações para ataques menores e mitigação mais rápida para ataques, mesmo quando o tráfego está dentro da capacidade do aplicativo.

  Ao adicionar detecção baseada em integridade, durante períodos em que a verificação de integridade associada não está íntegra, o Shield Advanced pode colocar mitigações ainda mais rapidamente e em limites ainda mais baixos.
- Recursos da camada de aplicativo (camada 7) — A detecção baseada em integridade melhora a precisão da detecção de inundação de solicitações da web para CloudFront distribuições e balanceadores de carga de aplicativos. Ao proteger esses tipos de recursos com o Shield Advanced, você recebe alertas de detecção de inundação de solicitações da web quando há um desvio estatisticamente significativo no volume de tráfego combinado com mudanças significativas nos padrões de tráfego, com base nas características da solicitação.

  Com a detecção baseada na integridade, quando a verificação de integridade do Route 53 associada revela que não há integridade, o Shield Advanced requer desvios menores para alertas e relata eventos mais rapidamente. Quando a verificação de integridade do Route 53 associada revela integridade, o Shield Advanced requer desvios maiores para alertas.

Sumário

Práticas recomendadas para usar verificações de integridade com o Shield Advanced

Siga as práticas recomendadas desta seção ao criar e usar verificações de integridade com o Shield Advanced.

- Planeje suas verificações de integridade identificando os componentes da sua infraestrutura que você deseja monitorar. Considere os seguintes tipos de recursos para verificações de integridade:
  - Recursos críticos.
  - Qualquer recurso para o qual você queira maior sensibilidade na detecção e mitigação do Shield Advanced.
  - Recursos para os quais você deseja que o Shield Advanced entre em contato com você de forma proativa. O engajamento proativo é informado pelo status das suas verificações de integridade.

  Exemplos de recursos que talvez você queira monitorar incluem CloudFront distribuições da Amazon, balanceadores de carga voltados para a Internet e instâncias do Amazon EC2.
- Defina verificações de integridade que reflitam com precisão a integridade da origem do seu aplicativo com o mínimo de notificações possível.
  - Faça verificações de integridade para que elas só revelem falta de integridade quando seu aplicativo não estiver disponível ou não estiver funcionando dentro dos parâmetros aceitáveis.

Você é responsável por definir e manter as verificações de integridade com base nos requisitos específicos do seu aplicativo.

- Use o mínimo possível de verificações de integridade e, ao mesmo tempo, informe com precisão a integridade do seu aplicativo. Por exemplo, vários alarmes de várias áreas do seu aplicativo, todos relatando o mesmo problema, podem sobrecarregar suas atividades de resposta sem agregar valor informativo.
- Use verificações de saúde calculadas para monitorar a integridade do aplicativo usando uma combinação de CloudWatch métricas da Amazon. Por exemplo, você pode calcular a integridade combinada com base na latência dos seus servidores de aplicativos e nas taxas de erro 5xx, que indicam que o servidor de origem não atendeu à solicitação.
- Crie e publique seus próprios indicadores de integridade do aplicativo em métricas CloudWatch personalizadas conforme necessário e use-os em uma verificação de integridade calculada.

- Implemente e gerencie suas verificações de integridade para melhorar a detecção e reduzir atividades de manutenção desnecessárias.
  - Antes de associar uma verificação de integridade a uma proteção do Shield Advanced, verifique se ela está em bom estado. Associar uma verificação de integridade que está relatando problemas de integridade pode distorcer os mecanismos de detecção do Shield Advanced para seus recursos protegidos.
  - Mantenha suas verificações de integridade disponíveis para uso pelo Shield Advanced. Não exclua uma verificação de integridade no Route 53 que você está usando para obter uma proteção Shield Advanced.
  - Use ambientes de teste e preparação somente para testar suas verificações de integridade. Mantenha associações de verificação de integridade somente para ambientes que exijam desempenho em nível de produção e disponibilidade. Não mantenha a associação de verificação de integridade no Shield Advanced para ambientes de teste e preparação.

Métricas comumente usadas para verificações de integridade

Esta seção lista as CloudWatch métricas da Amazon que são comumente usadas em verificações de saúde para medir a integridade do aplicativo durante eventos distribuídos de negação de serviço (DDoS). Para obter informações completas sobre as CloudWatch métricas de cada tipo de recurso, consulte a lista que segue a tabela.

Tópicos

- CloudWatch Métricas da Amazon para cada tipo de recurso

Para monitorar a integridade do aplicativo

Recurso	Métrica	Descrição
route 53	`HealthCheckStatus`	O status do endpoint da verificação de integridade.
CloudFront	`5xxErrorRate`	A porcentagem de todas as solicitações para as quais o código de status HTTP é 5xx. Isso indica um ataque que está afetando o aplicativo.
Application Load Balancer	`HTTPCode_ELB_5XX_Count`	O número de códigos de erro do cliente HTTP 5xx gerados pelo balanceador de carga.
Application Load Balancer	`RejectedConnectionCount`	O número de conexões que foram rejeitadas porque o balanceador de carga atingiu o número máximo de conexões.
Application Load Balancer	`TargetConnectionErrorCount`	O número de conexões que não foram estabelecidas com êxito entre o balanceador de carga e o destino.
Application Load Balancer	`TargetResponseTime`	O tempo decorrido, em segundos, depois que a solicitação deixa o balanceador de carga até o momento em que uma resposta do destino é recebida.

Recurso	Métrica	Descrição
Application Load Balancer	`UnHealthyHostCount`	O número de destinos considerados sem integridade.
Amazon EC2	`CPUUtilization`	O percentual de unidades de computação EC2 alocadas que estão atualmente em uso.

CloudWatch Métricas da Amazon para cada tipo de recurso

Para obter informações adicionais sobre as métricas disponíveis para seus recursos protegidos, consulte as seções a seguir nos guias de recursos:

- Amazon Route 53 — Monitorando seus recursos com as verificações de saúde do Amazon Route 53 e a Amazon CloudWatch no Amazon Route 53 Developer Guide.
- Amazon CloudFront — Monitoramento CloudFront com a Amazon CloudWatch no Amazon CloudFront Developer Guide.
- Application Load Balancer — CloudWatch métricas para seu Application Load Balancer no Guia do usuário para Application Load Balancers.
- Network Load Balancer — CloudWatch métricas para seu Network Load Balancer no Guia do usuário para Network Load Balancers.
- AWS Global Accelerator — Usando a Amazon CloudWatch com AWS Global Accelerator o Guia do AWS Global Accelerator Desenvolvedor.
- Amazon Elastic Compute Cloud — Liste as CloudWatch métricas disponíveis para suas instâncias em https://docs.aws.amazon.com/ AWSEC UserGuide 2/latest/ /.
- Amazon EC2 Auto Scaling — Métricas de CloudWatch monitoramento para seus grupos e instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Gerenciar associações de verificação de integridade

Você se beneficiará ao máximo com o uso de uma verificação de integridade com o Shield Advanced se a verificação de integridade só reportar integridade quando seu aplicativo estiver sendo executado dentro de parâmetros aceitáveis e só reportar falta de integridade quando ele não estiver. Use as orientações desta seção para gerenciar suas associações de verificação de integridade no Shield Advanced.

> **Note**
>
> O Shield Advanced não gerencia automaticamente suas verificações de integridade.

É necessário o seguinte para usar uma verificação de integridade com o Shield Advanced:

- A verificação de integridade deve reportar integridade quando você a associa à proteção Shield Advanced.
- A verificação de integridade deve ser relevante para a integridade do seu recurso protegido. Você é responsável por definir e manter as verificações de integridade que reportam adequadamente a integridade do seu aplicativo com base nos requisitos específicos do seu aplicativo.
- A verificação de integridade deve permanecer disponível para ser usada pela proteção do Shield Advanced. Não exclua uma verificação de integridade no Route 53 que você está usando para obter uma proteção Shield Advanced.

Tópicos

Como associar uma verificação de integridade ao seu recurso

O procedimento a seguir mostra como associar uma verificação de integridade do Amazon Route 53 a um recurso protegido.

> **Note**
>
> Antes de associar uma verificação de integridade a uma proteção do Shield Advanced, verifique se ela está em bom estado. Para informações, consulte Como monitorar o status da verificação de integridade e receber notificações no Guia do desenvolvedor do Amazon Route 53.

Para associar uma verificação de integridade

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na guia Proteções, selecione o recurso que você deseja associar a uma verificação de integridade.
4. Escolha Configurar proteções.
5. Escolha Próximo até chegar à página Configurar detecção de DDoS baseada em verificação de integridade - opcional.
6. Em Verificação de integridade associada, escolha o ID da verificação de integridade que deseja associar à proteção.

   > **Note**
   >
   > Se você não vir a verificação de integridade necessária, vá até o console do Route 53 e verifique a verificação de integridade e seu ID. Para obter informações, consulte Criar e atualizar verificações de integridade.

7. Percorra o restante das páginas até terminar a configuração. Na página Proteções, sua associação de verificação de integridade atualizada está listada para o recurso.
8. Na página Proteções, verifique se sua verificação de integridade recém-associada está reportando integridade.

   Você não pode começar a usar uma verificação de integridade no Shield Advanced enquanto a verificação de integridade estiver reportando problemas de integridade. Isso faz com que o Shield Advanced detecte falsos positivos em limites muito baixos e também pode afetar negativamente a capacidade da Shield Response Team (SRT) para fornecer engajamento proativo ao recurso.

   Se a verificação de integridade recém-associada estiver reportando problemas de integridade, faça o seguinte:

   a. Desassocie a verificação de integridade da sua proteção no Shield Advanced.
   b. Revisite suas especificações de verificação de integridade no Amazon Route 53 e verifique o desempenho geral e a disponibilidade do aplicativo.

c. Quando seu aplicativo estiver funcionando dentro de seus parâmetros de boa integridade e sua verificação de integridade estiver reportando integridade, tente associar novamente a verificação de integridade no Shield Advanced.

O procedimento de associação de verificação de integridade é concluído quando você estabelece sua nova associação de verificação de integridade e ela é reportada como íntegra no Shield Advanced.

Como desassociar uma verificação de integridade do seu recurso

O procedimento a seguir mostra como desassociar uma verificação de integridade do Amazon Route 53 de um recurso protegido.

Para desassociar uma verificação de integridade

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na guia Proteções, selecione o recurso que você deseja desassociar a uma verificação de integridade.
4. Escolha Configurar proteções.
5. Escolha Próximo até chegar à página Configurar detecção de DDoS baseada em verificação de integridade - opcional.
6. Em Verificação de integridade associada, escolha a opção vazia, listada como -.
7. Percorra o restante das páginas até terminar a configuração.

Na página Proteções, o campo de verificação de integridade do seu recurso está definido como -, indicando que não há associação de verificação de integridade.

O status da associação de verificação de integridade

Você pode ver o status da verificação de integridade associada a uma proteção na página Recursos protegidos do AWS WAF e do console do Shield e na página de detalhes de cada recurso.

- Íntegro - a verificação de integridade está disponível e reportando integridade.
- Sem integridade - a verificação de integridade está disponível e está reportando falta de integridade.

- Indisponível - a verificação de integridade não está disponível para uso pelo Shield Advanced.

Para resolver uma verificação de integridade Indisponível

Crie e use uma nova verificação de integridade. Não tente associar uma verificação de integridade novamente depois que ela tiver o status de indisponível no Shield Advanced.

Para obter orientação detalhada sobre como seguir essas etapas, consulte os tópicos anteriores.

1. No Shield Advanced, desassocie a verificação de integridade do recurso.
2. No Route 53, crie uma verificação de integridade para a proteção e anote seu ID. Para informações, consulte Criar e atualizar verificações de integridade no Guia do desenvolvedor do Amazon Route 53.
3. No Shield Advanced, associe a nova verificação de integridade ao recurso.

Exemplos de verificação de integridade

Esta seção mostra exemplos de verificação de integridade que você pode usar em uma verificação de integridade calculada. Uma verificação de integridade calculada usa várias verificações de integridade individuais para determinar um status combinado. O status de cada verificação de saúde individual é baseado na integridade de um endpoint ou no estado de uma CloudWatch métrica da Amazon. Você combina as verificações de integridade em uma verificação de integridade calculada e, em seguida, configura sua verificação de integridade calculada para relatar a integridade com base no status de integridade combinado das verificações de integridade individuais. Ajuste a sensibilidade de suas verificações de integridade calculadas de acordo com seus requisitos de desempenho e disponibilidade de aplicativos.

Para obter informações sobre verificações de integridade calculadas, consulte Monitoramento de outras verificações de integridade (verificações de integridade calculadas) no Guia do desenvolvedor do Amazon Route 53. Para obter informações adicionais, consulte o post Melhorias do Route 53 - Verificações de integridade calculadas e verificações de latência.

Tópicos

- CloudFront Distribuições da Amazon
- Balanceadores de cargas
- Endereço IP elástico (EIP) do Amazon EC2

CloudFront Distribuições da Amazon

Os exemplos a seguir descrevem as verificações de saúde que podem ser combinadas em uma verificação de saúde calculada para uma CloudFront distribuição:

- Monitore um endpoint especificando um nome de domínio para um caminho na distribuição que está veiculando conteúdo dinâmico. Uma resposta de integridade incluiria os códigos de resposta HTTP 2xx e 3xx.
- Monitore o estado de um CloudWatch alarme que está medindo a integridade da CloudFront origem. Por exemplo, você pode manter um CloudWatch alarme na métrica `TargetResponseTime` do Application Load Balancer e criar uma verificação de integridade que reflita o status do alarme. A verificação de integridade pode não reportar integridade quando o tempo de resposta, entre a solicitação que sai do balanceador de carga e o momento em que o balanceador de carga recebe uma resposta do destino, excede o limite configurado no alarme.
- Monitore o estado de um CloudWatch alarme que mede a porcentagem de solicitações para as quais o código de status HTTP da resposta é 5xx. Se a taxa de erro 5xx da CloudFront distribuição for maior que o limite definido no CloudWatch alarme, o status dessa verificação de saúde mudará para não íntegro.

Balanceadores de cargas

Os exemplos a seguir descrevem verificações de integridade que podem ser usadas em verificações de integridade calculadas para um Application Load Balancer, Network Load Balancer ou acelerador padrão Global Accelerator.

- Monitore o estado de um CloudWatch alarme que mede o número de novas conexões estabelecidas pelos clientes com o balanceador de carga. Você pode definir o limite de alarme para o número médio de novas conexões em algum grau acima da média diária. As métricas para cada tipo de recurso são as seguintes:
  - Application Load Balancer: `NewConnectionCount`
  - Network Load Balancer: `ActiveFlowCount`
  - Global Accelerator: `NewFlowCount`
- Para o Application Load Balancer e o Network Load Balancer, monitore o estado de CloudWatch um alarme que mede o número de balanceadores de carga considerados íntegros. Você pode definir o limite de alarme na Zona de Disponibilidade ou no número mínimo de hosts íntegros que seu balanceador de carga exige. As métricas disponíveis para os recursos do balanceador de carga são as seguintes:

  - Application Load Balancer: `HealthyHostCount`
  - Network Load Balancer: `HealthyHostCount`
- Para o Application Load Balancer, monitore o estado de um CloudWatch alarme que mede o número de códigos de resposta HTTP 5xx gerados pelos destinos do balanceador de carga. Para um Application Load Balancer, você pode usar a métrica `HTTPCode_Target_5XX_Count` e basear o limite de alarme na soma de todos os 5xx erros do balanceador de carga.

Endereço IP elástico (EIP) do Amazon EC2

Os exemplos de verificações de integridade a seguir podem ser combinados em uma verificação de integridade calculada para um endereço IP elástico do Amazon EC2:

- Monitore um endpoint especificando um endereço IP para o endereço IP elástico. A verificação de integridade permanecerá íntegra enquanto uma conexão TCP puder ser estabelecida com o recurso por trás do endereço IP.
- Monitore o estado de um CloudWatch alarme que mede a porcentagem de unidades computacionais alocadas do Amazon EC2 que estão atualmente em uso na instância. Você pode usar a métrica `CPUUtilization` do Amazon EC2 e basear o limite de alarme no que você considera ser uma taxa de utilização da CPU alta para seu aplicativo, por exemplo, 90%.

Gerenciando proteções de recursos em AWS Shield Advanced

Use as orientações desta seção para gerenciar as proteções do Shield Advanced para seus recursos.

> **Note**
>
> O Shield Advanced protege somente os recursos que você especificou no Shield Advanced ou por meio de uma política AWS Firewall Manager do Shield Advanced. Ele não protege automaticamente seus recursos.

Se você estiver usando uma política AWS Firewall Manager Shield Advanced, não precisará gerenciar as proteções dos recursos que estão no escopo da política. O Firewall Manager gerencia automaticamente as proteções de contas e recursos que estão no escopo de uma política, de acordo com a configuração da política. Para ter mais informações, consulte AWS Shield Advanced políticas.

Tópicos

Adicionando AWS Shield Advanced proteção aos AWS recursos

Siga as orientações nesta seção para adicionar a proteção Shield Advanced a um ou mais recursos.

Para adicionar proteção a um AWS recurso

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel de navegação, em AWS Shield escolha Recursos protegidos.
3. Escolha Adicionar recursos para proteger.
4. Na página Escolher recursos para proteger com o Shield Advanced, em Especificar a região e os tipos de recursos, forneça as especificações de região e tipo de recurso para os recursos que você quer proteger. Você pode proteger recursos em várias regiões selecionando Todas as regiões, e pode restringir a seleção a recursos globais selecionando Global. Você pode desmarcar qualquer tipo de recurso que não queira proteger. Para obter informações sobre proteções para seus tipos de recursos, consulte AWS Shield Advanced proteções por tipo de recurso.
5. Escolha Carregar recursos. O Shield Advanced preenche a seção Selecionar recursos com os recursos AWS que correspondem aos seus critérios.
6. Na seção Selecionar recursos, você pode filtrar a lista de recursos inserindo uma string para pesquisar nas listas de recursos.

   Escolha os recursos que você deseja proteger.
7. Na seção Tags, se você quiser adicionar tags às proteções Shield Advanced que estiver criando, especifique-as. Para obter mais informações sobre como marcar recursos AWS , consulte Trabalhar com o Tag Editor.
8. Escolha Proteger com o Shield Advanced. Isso adiciona as proteções do Shield Advanced aos recursos.

Configurando proteções AWS Shield Advanced

Você pode alterar as configurações de suas AWS Shield Advanced proteções a qualquer momento. Para fazer isso, você percorre as opções para as suas proteções selecionadas e modifica as configurações que precisar alterar.

Para gerenciar recursos protegidos

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na aba Proteções, escolha os recursos que você deseja proteger.
4. Escolha Configurar proteções e a opção de especificação de recursos que você deseja.
5. Percorra cada uma das opções de proteção de recursos, fazendo as alterações necessárias.

Configurar as proteções contra DDoS na camada de aplicação

Para se proteger contra ataques aos recursos da Amazon CloudFront e do Application Load Balancer, você pode adicionar ACLs AWS WAF da web e adicionar regras baseadas em taxas. Para obter mais informações sobre isso, consulte ACLs AWS WAF da web da camada de aplicação Shield Advanced e regras baseadas em taxas.

Você também pode ativar a mitigação automática de DDoS da camada de aplicação do Shield Advanced. Para obter informações sobre como AWS WAF funciona, consulteAWS WAF. Para obter informações sobre o atributo de mitigação automática, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

> **Important**
>
> Se você gerencia suas proteções Shield Advanced AWS Firewall Manager usando uma política Shield Advanced, não poderá gerenciar as proteções da camada de aplicação aqui. Para todos os outros recursos, recomendamos anexar pelo menos uma web ACL a cada recurso, mesmo que essa web ACL não contenha nenhuma regra.

> **Note**
>
> Quando você ativa a mitigação automática de DDoS na camada de aplicação para um recurso, se necessário, a operação adiciona automaticamente uma função vinculada ao serviço à sua conta para dar ao Shield Advanced as permissões necessárias para gerenciar suas proteções de web ACL. Para mais informações, consulte Usar funções vinculadas ao serviço para o Shield Advanced.

Para configurar as proteções contra DDoS na camada de aplicação

1. Na página Configurar proteções contra DDoS da camada 7, se o recurso ainda não estiver associado a uma web ACL, você poderá escolher uma web ACL existente ou criar a sua própria.

   Para criar uma web ACL, siga estas etapas:

   a. Escolha Criar web ACL.

   b. Insira um nome. Você não pode alterar o nome depois de criar a web ACL.

   c. Escolha Criar.

   > **Note**
   >
   > Se um recurso já estiver associado a uma web ACL, você não poderá mudar para uma web ACL diferente. Se você deseja alterar a web ACL, é necessário primeiro remover as web ACLs associadas do recurso. Para ter mais informações, consulte Associando ou desassociando uma ACL da web com um recurso AWS.

2. Se a web ACL não tiver uma regra baseada em intervalos definida, você poderá adicionar uma escolhendo Adicionar regra de limite de intervalo e, em seguida, executar as seguintes etapas:

   a. Insira um nome.

   b. Insira um limite de intervalo. Este é o número máximo de solicitações permitidas em um período de cinco minutos de um único endereço IP antes da ação da regra baseada em intervalos ser aplicada ao endereço IP. Quando as solicitações do endereço IP ficam abaixo do limite, a ação é interrompida.

   c. Defina a ação da regra para contar ou bloquear solicitações de endereços IP enquanto suas contagens de solicitações estiverem acima do limite. A aplicação e a remoção da

ação da regra podem entrar em vigor um ou dois minutos após a alteração do intervalo de solicitação do endereço IP.

d. Escolha Adicionar regra.

3. Para Mitigação automática de DDoS na camada de aplicação, escolha se você deseja que o Shield Advanced mitigue automaticamente os ataques de DDoS em seu nome, da seguinte forma:

   - Para ativar a mitigação automática, escolha Ativar e selecione a ação de AWS WAF regra que você deseja que o Shield Advanced use em suas regras personalizadas. Suas escolhas são Count e Block. Para obter informações sobre essas ações de AWS WAF regras, consulteAção da regra. Para obter informações sobre como o Shield Avançado gerencia essa configuração de ação, consulte Como o Shield Avançado gerencia a configuração de ação de regra.
   - Para desativar a mitigação automática, escolha Desativar.
   - Para deixar as configurações de mitigação automática inalteradas para os recursos que você está gerenciando, deixe marcada a opção padrão Manter as configurações atuais.

   Para obter informações sobre a mitigação automática de DDoS da camada de aplicação do Shield Advanced, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

4. Escolha Próximo.

Criar alarmes e notificações

O procedimento a seguir mostra como gerenciar CloudWatch alarmes para recursos protegidos.

> **Note**
>
> CloudWatch incorre em custos adicionais. Para obter CloudWatch os preços, consulte Amazon CloudWatch Pricing.

Para criar alarmes e notificações

1. Na página de proteções Criar alarmes e notificações - opcional, configure os tópicos do SNS para os alarmes e notificações que você deseja receber. Para recursos para os quais você não deseja notificações, escolha Sem tópico. Você pode adicionar um tópico do Amazon SNS ou criar um novo tópico.

2. Para criar um tópico do Amazon SNS, siga estas etapas:

    a. Na lista suspensa, escolha Criar novo tópico SNS.

    b. Insira o nome do tópico.

    c. Opcionalmente, insira um endereço de e-mail de destino para as mensagens do Amazon SNS e, em seguida, escolha Adicionar e-mail. Você pode inserir mais de um.

    d. Escolha Criar.

3. Escolha Próximo.

Removendo a AWS Shield Advanced proteção de um AWS recurso

Você pode remover a AWS Shield Advanced proteção de qualquer um dos seus AWS recursos a qualquer momento.

> **Important**
>
> A exclusão de um AWS recurso não remove o recurso de AWS Shield Advanced. Você também deve remover a proteção do recurso de AWS Shield Advanced, conforme descrito neste procedimento.

Remover a AWS Shield Advanced proteção de um AWS recurso

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na aba Proteções, escolha os recursos cujas proteções você deseja remover.
4. Escolha Excluir proteções.

    - Se você tiver um CloudWatch alarme da Amazon configurado para uma proteção, você terá a opção de excluir o alarme junto com a proteção. Se você optar por não excluir o alarme neste momento, poderá excluí-lo posteriormente usando o CloudWatch console.

> **Note**
>
> Para proteções que tenham uma verificação de integridade do Amazon Route 53 configurada, se você adicionar a proteção outra vez posteriormente, a proteção ainda incluirá a verificação de integridade.

As etapas anteriores removem a AWS Shield Advanced proteção de AWS recursos específicos. Eles não cancelam sua AWS Shield Advanced assinatura. Você continuará a ser cobrado pelo serviço. Para obter informações sobre sua AWS Shield Advanced assinatura, entre em contato com o AWS Support Centro.

Removendo um CloudWatch alarme das proteções Shield Advanced

Para remover um CloudWatch alarme das proteções do Shield Advanced, faça o seguinte:

- Exclua a proteção, como descrito em Removendo a AWS Shield Advanced proteção de um AWS recurso. Marque a caixa de seleção ao lado de Também excluir o alarme DDoSDetection relacionado.
- Exclua o alarme usando o CloudWatch console. O nome do alarme a ser excluído começa com DDoS DetectedAlarmForProtection.

AWS Shield Advanced grupos de proteção

Use grupos de proteção para criar coleções lógicas de seus recursos protegidos e gerenciar suas proteções como um grupo. Para obter mais informações sobre o gerenciamento de proteções de recurso, consulte Configurando proteções AWS Shield Advanced.

> **Note**
>
> A mitigação automática de DDoS na camada de aplicativos não interage com grupos de proteção. Você pode ativar a mitigação automática para recursos que estão em grupos de proteção, mas o Shield Advanced não aplica automaticamente mitigações de ataques com base nas descobertas do grupo de proteção. O Shield Advanced aplica mitigações automáticas de ataques para recursos individuais.

AWS Shield Advanced os grupos de proteção oferecem uma forma de autoatendimento de personalizar o escopo de detecção e mitigação tratando vários recursos protegidos como uma única unidade. O agrupamento de recursos pode oferecer vários benefícios.

- Melhorar a precisão da detecção.
- Reduzir as notificações de eventos não acionáveis.
- Aumentar a cobertura das ações de mitigação para incluir recursos protegidos que também possam ser afetados durante um evento.
- Acelerar o tempo de mitigação de ataques com vários alvos semelhantes.
- Facilitar a proteção automática de recursos protegidos recém-criados.

Os grupos de proteção podem ajudar a reduzir os falsos positivos em situações como a troca entre azul e verde, nos quais os recursos alternam entre estar quase sem carga e totalmente carregados. Outro exemplo é quando você cria e exclui recursos com frequência, mantendo um nível de carga compartilhado entre os membros do grupo. Para situações como essas, monitorar recursos individuais pode levar a falsos positivos, enquanto monitorar a saúde do grupo de recursos, não.

Você pode configurar grupos de proteção para incluir todos os recursos protegidos, todos os recursos de tipos de recursos específicos, ou recursos especificados individualmente. Os recursos recém-protegidos que atendem aos critérios do seu grupo de proteção são incluídos automaticamente no seu grupo de proteção. Um recurso protegido pode pertencer a vários grupos de proteção.

Gerenciando grupos AWS Shield Advanced de proteção

Use as orientações desta seção para gerenciar as configurações do seu grupo de proteção.

Criação de um grupo de proteção Shield Advanced

Para criar um grupo de proteção

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Escolha a guia Grupos de proteção e, em seguida, escolha Criar grupo de proteção.

4. Na página Criar grupo de proteção, forneça um nome para o seu grupo. Você usará esse nome para identificar o grupo na sua lista de recursos protegidos. Você não pode alterar o nome de um grupo de proteção após criá-lo.
5. Em Critérios de agrupamento de proteção, selecione os critérios que você deseja que o Shield Advanced use para identificar os recursos protegidos que serão incluídos no grupo. Faça suas seleções adicionais com base nos critérios que você escolheu.
6. Em Agregação, selecione como você deseja que o Shield Advanced combine os dados de recursos do grupo para detectar, mitigar e relatar eventos.
   - Soma: use o tráfego total em todo o grupo. Essa é uma boa opção para a maioria dos casos. Os exemplos incluem endereços IP elásticos para instâncias do Amazon EC2 que escalam manual ou automaticamente.
   - Média: use a média do tráfego em todo o grupo. Essa é uma boa opção para recursos que compartilham tráfego de maneira uniforme. Os exemplos incluem aceleradores e balanceadores de carga.
   - Máximo: use o maior tráfego de cada recurso. Isso é útil para recursos que não compartilham tráfego e recursos que compartilham tráfego de forma não uniforme. Os exemplos incluem CloudFront distribuições da Amazon e recursos de origem para CloudFront distribuições.
7. Escolha Salvar para salvar seu grupo de proteção e retornar à página Recursos protegidos.

Na página Eventos do Shield, você pode visualizar os eventos do seu grupo de proteção e detalhar para ver informações adicionais sobre os recursos protegidos que estão no grupo.

Atualização de um grupo de proteção Shield Advanced

Como atualizar um grupo de proteção

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na guia Grupos de proteção, marque a caixa de seleção ao lado do grupo de proteção que você deseja modificar.
4. Na página do grupo de proteção, escolha Editar. Faça suas alterações nas configurações do grupo de proteção.
5. Escolha Salvar para salvar as alterações.

Exclusão de um grupo de proteção Shield Advanced

Para excluir um grupo de proteção

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Recursos protegidos.
3. Na guia Grupos de proteção, marque a caixa de seleção ao lado do grupo de proteção que você deseja remover.
4. Na página do grupo de proteção, escolha Excluir e confirme a ação.

Rastreando mudanças na proteção de recursos em AWS Config

Você pode registrar as alterações na AWS Shield Advanced proteção de seus recursos usando AWS Config. Em seguida, você pode usar essas informações para manter um histórico de alterações de configuração para fins de solução de problemas e auditoria.

Para registrar as alterações de proteção, habilite AWS Config para cada recurso que você deseja rastrear. Para obter mais informações, consulte Conceitos básicos do AWS Config no Guia do desenvolvedor do AWS Config .

Você deve habilitar AWS Config para cada um Região da AWS que contenha os recursos rastreados. Você pode ativar AWS Config manualmente ou usar o AWS CloudFormation modelo “Ativar AWS Config” em Modelos de AWS CloudFormation StackSets amostra no Guia do AWS CloudFormation usuário.

Se você ativar AWS Config, você será cobrado conforme detalhado na página AWS Config de preços.

> **Note**
>
> Se você já AWS Config habilitou as regiões e os recursos necessários, não precisa fazer nada. AWS Config os registros sobre alterações de proteção em seus recursos começam a ser preenchidos automaticamente.

Depois de habilitar AWS Config, use a região Leste dos EUA (Norte da Virgínia) no AWS Config console para ver o histórico de alterações de configuração dos recursos AWS Shield Advanced globais.

Veja o histórico de alterações dos recursos AWS Shield Advanced regionais por meio do AWS Config console nas regiões Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Europa (Irlanda), Europa (Frankfurt), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Sydney).

Visibilidade de eventos de DDoS

AWS Shield fornece visibilidade das seguintes categorias de eventos e atividades de eventos:

- Global: todos os clientes podem acessar uma visão agregada da atividade global de ameaças nas últimas duas semanas. Você pode ver essas informações nas páginas Getting Started e Global Threat Dashboard do AWS Shield console. Para ter mais informações, consulte AWS Shield atividade global e da conta.
- Conta: todos os clientes podem acessar um resumo dos eventos de sua conta no ano anterior. Você pode ver essas informações na página Introdução do AWS Shield console. Para ter mais informações, consulte AWS Shield atividade global e da conta.

Ao assinar o Shield Advanced e adicionar proteções aos seus recursos, você obtém acesso a informações adicionais sobre os eventos e ataques de DDoS aos recursos protegidos:

- Eventos em recursos protegidos — O Shield Advanced fornece informações detalhadas para cada evento por meio da página Eventos do AWS Shield console. Para ter mais informações, consulte AWS Shield Advanced eventos.
- Métricas de eventos para recursos protegidos — O Shield Advanced publica CloudWatch métricas de detecção, mitigação e principais colaboradores da Amazon para todos os recursos que protege. Você pode usar essas métricas para configurar CloudWatch painéis e alarmes. Para ter mais informações, consulte AWS Shield Advanced métricas.
- Visibilidade de eventos entre contas para recursos protegidos — Se você usa AWS Firewall Manager para gerenciar suas proteções Shield Advanced, você pode habilitar a visibilidade das proteções em várias contas usando o Firewall Manager combinado com. AWS Security Hub Para ter mais informações, consulte Visibilidade do evento entre contas.

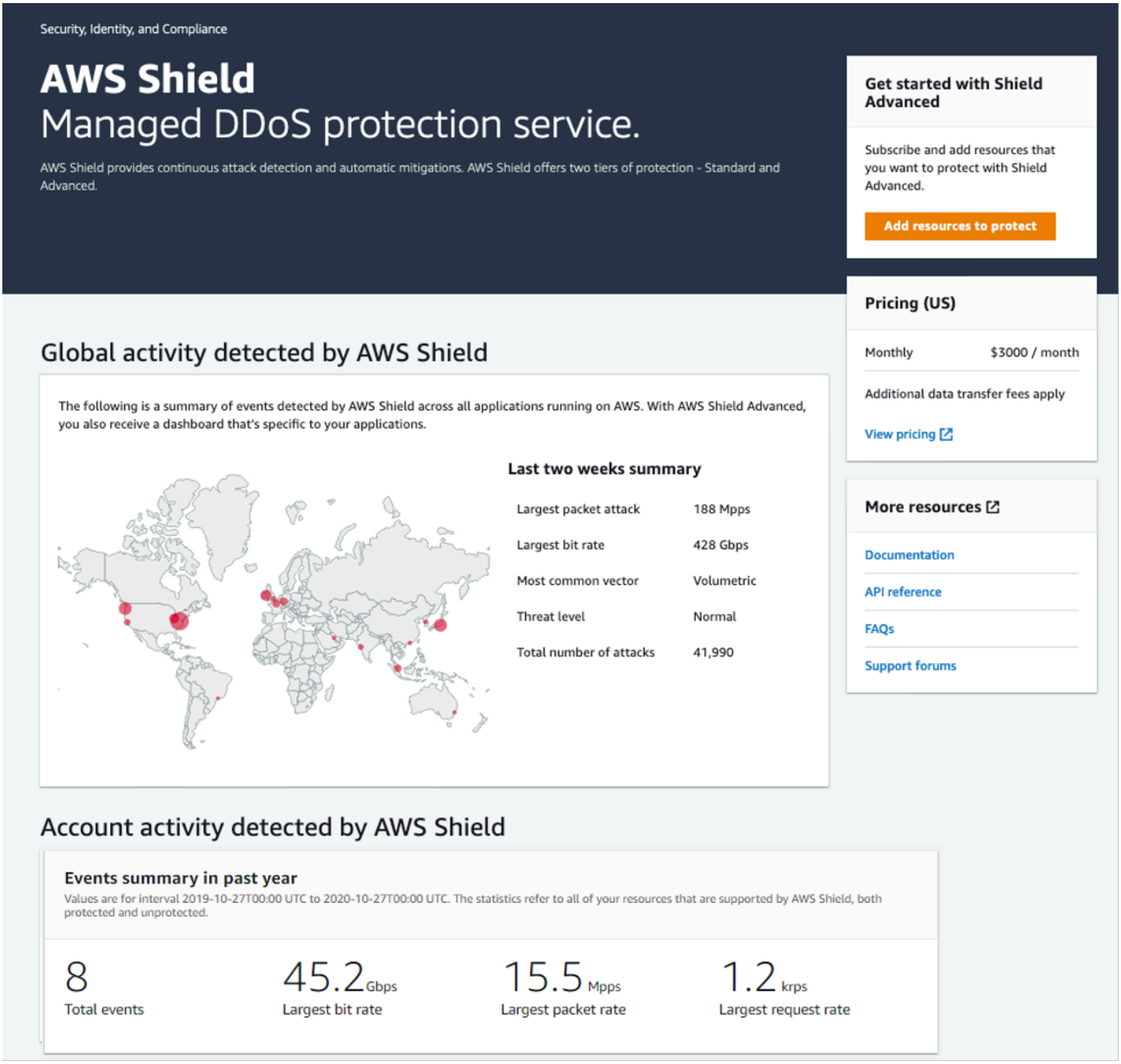
Se você habilitar a mitigação automática de DDoS na camada de aplicativo para uma proteção na camada de aplicativo,

Tópicos

AWS Shield atividade global e da conta

Você pode acessar uma visão agregada da atividade global de ameaças e um resumo de eventos por conta nas páginas de introdução e painel de controle de ameaças globais do AWS Shield console.

A captura de tela a seguir mostra uma página de exemplo de Conceitos básicos.



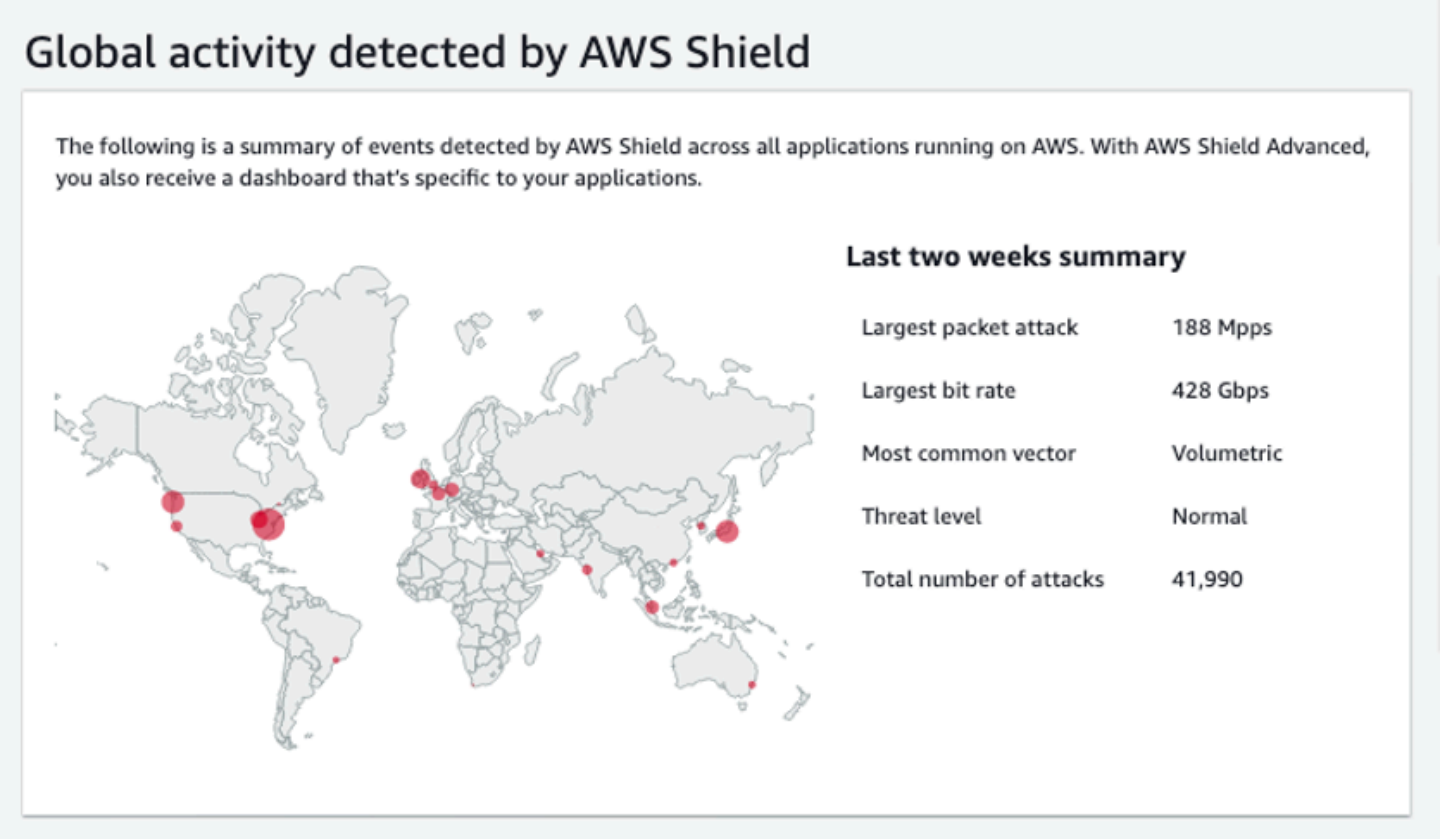
Para acessar o AWS Shield console

- Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.

Você não precisa de uma assinatura do Shield Advanced para acessar as informações resumidas de atividades globais e eventos da conta.

Atividade global

Essas informações estão disponíveis no AWS Shield console, no painel global de ameaças e nas páginas de introdução. A captura de tela a seguir mostra um exemplo do painel de atividades globais.



A atividade global descreve os eventos de DDoS observados em todos os AWS clientes. Uma vez por hora, AWS atualiza as informações das duas semanas anteriores. No painel do console, você pode ver os resultados, particionados por AWS região e exibidos em um mapa de aquecimento mundial. Ao lado do mapa, o Shield exibe informações resumidas, como o maior ataque de pacotes, a maior taxa de bits, o vetor mais comum, o número total de ataques e o nível de ameaça. O nível de ameaça é uma avaliação da atividade global atual em comparação com o que o AWS normalmente observa. O valor padrão do nível de ameaça é Normal. O AWS atualiza automaticamente o valor para Alto em atividades elevadas de DDoS.

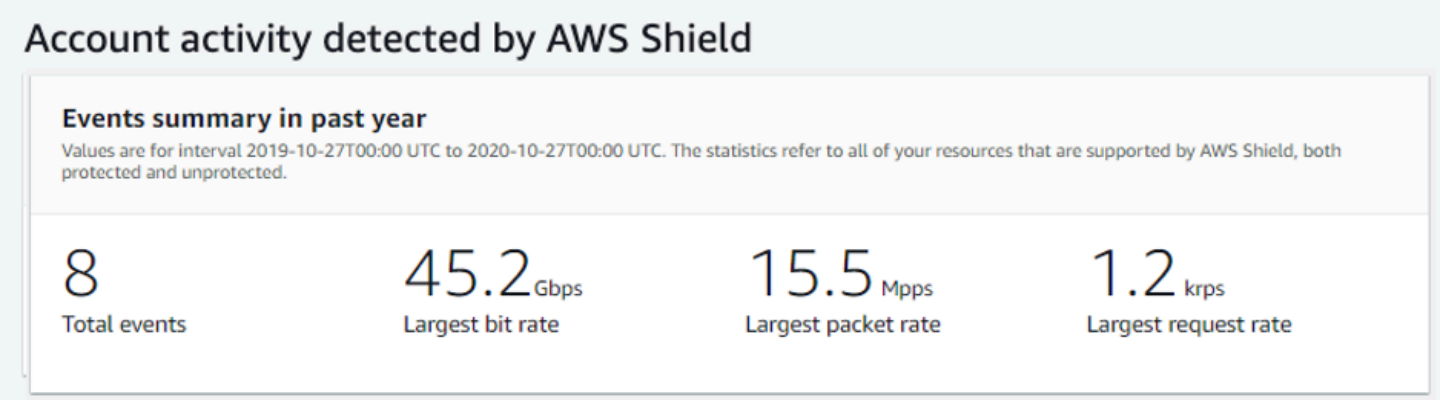
O Painel global de ameaças também fornece métricas de séries temporais e permite que você alterne entre durações de tempo. Para ver o histórico de ataques DDoS significativos, você pode personalizar o painel para visualizações do último dia até às duas últimas semanas. As métricas de séries temporais fornecem uma visão da maior taxa de bits, taxa de pacotes ou taxa de solicitação

de todos os eventos detectados AWS Shield pelos aplicativos em execução AWS durante a janela de tempo selecionada.

Atividade da conta

Essas informações estão disponíveis na página de introdução do AWS Shield console.

A captura de tela a seguir mostra um exemplo do painel de atividades da conta.



A atividade da conta descreve eventos de DDoS que o Shield detectou em seus recursos e que são elegíveis para proteção do Shield Advanced. Todos os dias, o Shield cria métricas resumidas para o ano encerrado às 00:00 UTC do dia anterior e, em seguida, exibe o total de eventos, a maior taxa de bits, a maior taxa de pacotes e a maior taxa de solicitações.

- A métrica total de eventos reflete cada vez que o Shield observou atributos suspeitos no tráfego destinado ao seu aplicativo. Os atributos suspeitos podem incluir tráfego em volume maior do que o normal, tráfego que não corresponde ao perfil histórico do seu aplicativo, ou tráfego que não corresponde à heurística definida pelo Shield para tráfego válido do aplicativo.
- As estatísticas da maior taxa de bits e da maior taxa de pacotes estão disponíveis para cada recurso.
- A maior estatística de taxa de solicitação está disponível somente para CloudFront distribuições da Amazon e Application Load Balancers que têm uma Web ACL associada AWS WAF .

> **Note**
>
> Você também pode acessar o resumo do evento no nível da conta por meio da operação AWS Shield da API DescribeAttackStatistics.

AWS Shield Advanced eventos

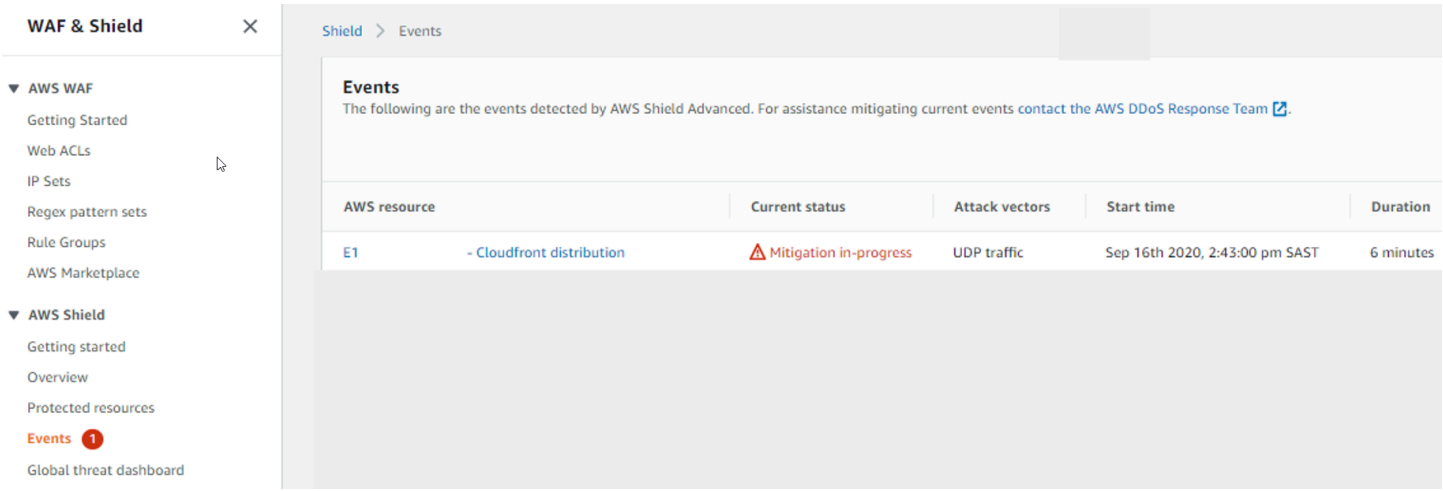
Ao assinar o Shield Advanced e proteger seus atributos, você obtém acesso a atributos adicionais de visibilidade dos atributos. Isso inclui notificação quase em tempo real de eventos detectados pelo Shield Advanced, além de informações adicionais sobre eventos e mitigações detectados.

> **Note**
>
> As informações do seu evento no console do Shield Advanced são baseadas nas métricas do Shield Advanced. Para obter informações sobre as métricas do Shield Advanced, consulte AWS Shield Advanced métricas

AWS Shield avalia o tráfego para seu recurso protegido em várias dimensões. Quando uma anomalia é detectada, o Shield Advanced cria um evento separado para cada recurso afetado.

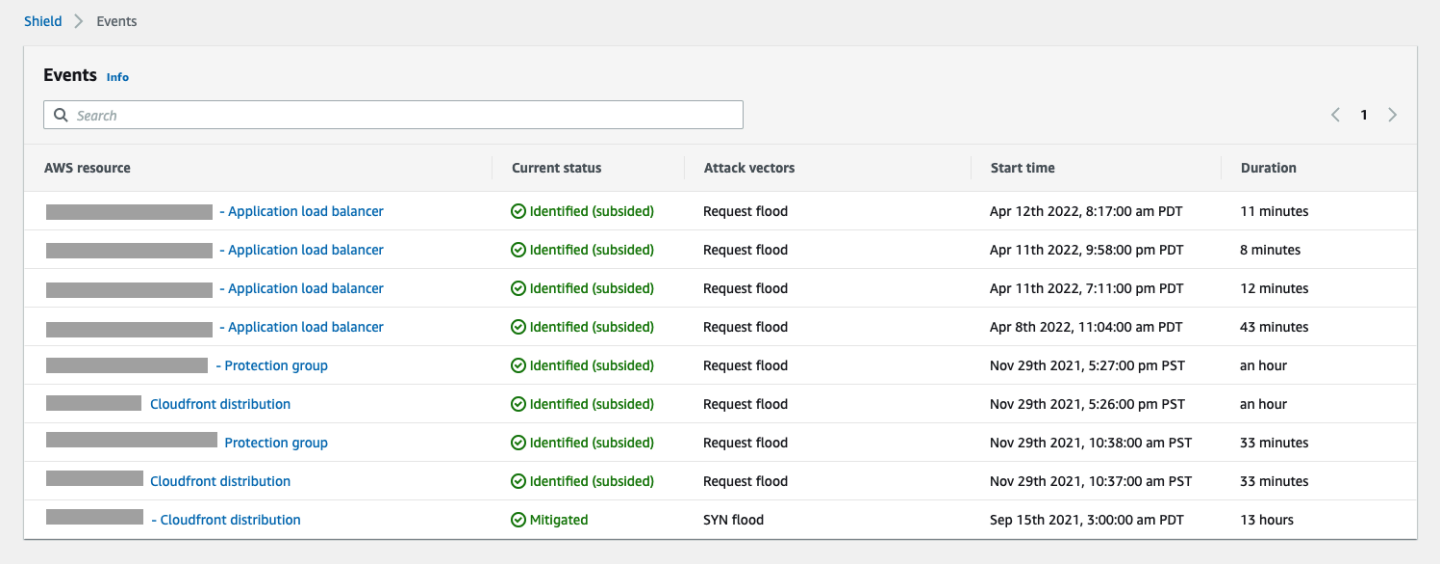
Você pode acessar os resumos e detalhes dos eventos na página Eventos do console Shield. A página Eventos do nível superior fornece uma visão geral dos eventos atuais e passados.

A captura de tela a seguir mostra uma página de Eventos de exemplo com um único evento em andamento. Esse evento ativo também é sinalizado no painel de navegação à esquerda.



O Shield Advanced também pode mitigar automaticamente os ataques, dependendo do tipo de tráfego e das proteções configuradas. Essas mitigações podem proteger seu recurso de receber tráfego excessivo ou tráfego que corresponda a uma assinatura de ataque DDoS conhecida.

A captura de tela a seguir mostra um exemplo de lista de Eventos na qual todos os eventos foram mitigados pelo Shield Advanced ou diminuíram sozinhos.



Proteja seus recursos antes de um evento

Melhore a precisão da detecção de eventos protegendo os recursos com o Shield Advanced enquanto eles recebem o tráfego normal esperado, antes de serem sujeitos a um ataque de DDoS.

Para relatar com precisão os eventos de um recurso protegido, o Shield Advanced deve primeiro estabelecer uma linha de base dos padrões de tráfego esperados para ele.

- O Shield Advanced relata os eventos da camada de infraestrutura dos recursos quando eles tiverem sido protegidos por pelo menos 15 minutos.
- O Shield Advanced relata os eventos da camada de aplicativos da web para os recursos quando eles tiverem sido protegidos por pelo menos 24 horas. A precisão da detecção de eventos da camada de aplicação é melhor após o Shield Advanced observar o tráfego esperado por 30 dias.

Para acessar informações de eventos no AWS Shield console

1. Faça login AWS Management Console e abra o console AWS WAF & Shield em https://console.aws.amazon.com/wafv2/.
2. No painel AWS Shield de navegação, escolha Eventos. O console exibe a página Eventos.
3. Na página Eventos, você pode selecionar qualquer evento na lista para ver informações adicionais resumidas e detalhes do evento.

Tópicos

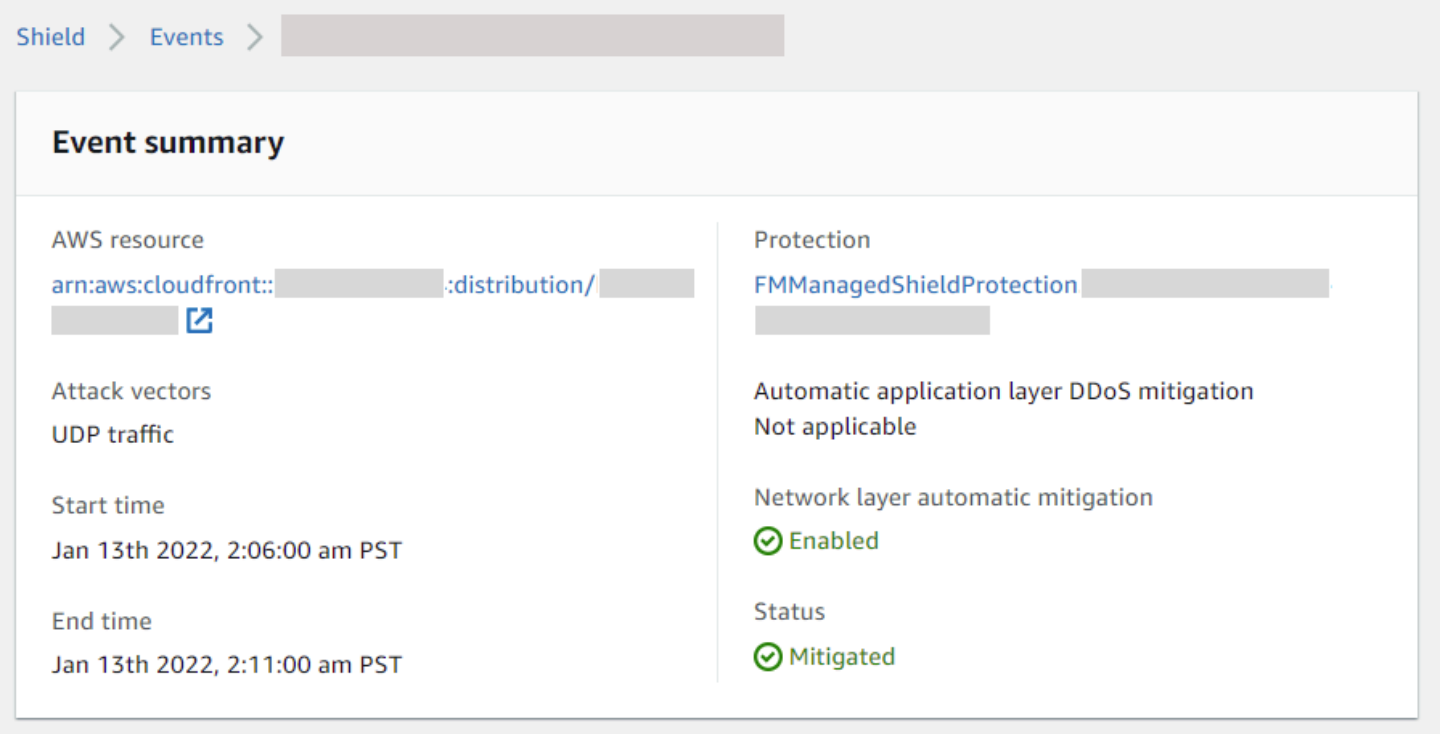
- AWS Shield Advanced resumos de eventos

- AWS Shield Advanced detalhes do evento

AWS Shield Advanced resumos de eventos

Você pode ver informações resumidas e detalhadas de um evento na página do console do evento. Para abrir a página de um evento, selecione o nome do AWS recurso na lista da página Eventos.

A captura de tela a seguir mostra um exemplo de resumo para um evento de camada de rede.



As informações de resumo da página de eventos incluem o seguinte.

- Status atual: valores que indicam o estado do evento e as ações que o Shield Advanced realizou no evento. Os valores de status se aplicam aos eventos da camada de infraestrutura (camada 3 ou 4) e da camada de aplicativo (camada 7).
  - Identificado (em andamento) e Identificado (diminuído): indica que o Shield Advanced detectou um evento, mas não tomou nenhuma medida até o momento. Identificado (diminuído) indica que o tráfego suspeito detectado pelo Shield foi interrompido sem intervenção.
  - Mitigação em andamento e Mitigado: indica que o Shield Advanced detectou um evento e tomou medidas adequadas. Mitigated também é usado quando o recurso alvo é uma CloudFront distribuição da Amazon ou uma zona hospedada do Amazon Route 53, que têm suas próprias mitigações automáticas em linha.

- Vetores de ataque: vetores de ataque de DDoS, como floods de TCP SYN, e heurísticas de detecção do Shield Advanced, como flood de solicitações. Esses podem ser indicadores de um ataque DDoS.
- Hora de início: a data e a hora em que o primeiro ponto de dados de tráfego anômalo foi detectado.
- Duração ou hora de término: o tempo decorrido entre a hora de início do evento e o último ponto de dados anômalo observado pelo Shield Advanced. Enquanto um evento estiver em andamento, esses valores continuarão aumentando.
- Proteção: nomeia a proteção do Shield Advanced associada ao recurso e fornece um link para sua página de proteção. Isso está disponível na página do evento individual.
- Mitigação automática de DDoS na camada de aplicativo: usada para proteções na camada de aplicativo, para indicar se a mitigação automática de DDoS da camada de aplicação do Shield Advanced está habilitada para o recurso. Caso esteja habilitada, isso fornecerá um link para acessar e gerenciar a configuração. Isso está disponível na página do evento individual.
- Mitigação automática da camada de rede: indica se o recurso tem mitigação automática na camada de rede. Se um recurso tiver um componente de camada de rede, ele o terá ativado. Essas informações estão disponíveis na página individual do evento.

Para recursos que são frequentemente direcionados, o Shield pode manter as mitigações em vigor após a diminuição do excesso de tráfego, evitando assim novos eventos recorrentes.

> **Note**
>
> Você também pode acessar resumos de eventos para recursos protegidos por meio da operação ListAttacksda AWS Shield API.

AWS Shield Advanced detalhes do evento

Você pode ver detalhes sobre a detecção, a mitigação e os principais responsáveis por um evento na seção inferior da página do console do evento. Essa seção pode incluir uma combinação de tráfego legítimo e potencialmente indesejado e pode representar tanto o tráfego passado para seu recurso protegido, quanto o tráfego bloqueado pelas mitigações do Shield.

- Detecção e mitigação: isso fornece informações sobre o evento observado e quaisquer mitigações aplicadas contra ele. Para obter informações sobre mitigação de eventos, consulte Resposta a eventos de DDoS.
- Principais responsáveis: isso categoriza o tráfego envolvido no evento e lista as principais fontes de tráfego que o Shield identificou para cada categoria. Para eventos da camada de aplicação, use as informações dos principais contribuidores para ter uma ideia geral da natureza de um evento, mas use os AWS WAF registros para suas decisões de segurança. Para obter mais informações, consulte as seções abaixo.

As informações do seu evento no console do Shield Advanced são baseadas nas métricas do Shield Advanced. Para obter informações sobre as métricas do Shield Advanced, consulte AWS Shield Advanced métricas

As métricas de mitigação não estão incluídas nos recursos da CloudFront Amazon ou do Amazon Route 53, porque esses serviços são protegidos por um sistema de mitigação que está sempre ativado e não exige mitigações para recursos individuais.

As seções de detalhes variam de acordo com o fato de as informações serem de uma camada de infraestrutura ou de um evento de camada de aplicativo.

Detalhes do evento da camada de aplicação

Você pode visualizar detalhes sobre a detecção, a mitigação e os principais responsáveis por um evento na camada de aplicação, na seção inferior da página do console do evento. Essa seção pode incluir uma combinação de tráfego legítimo e potencialmente indesejado e pode representar tanto o tráfego que foi passado para seu recurso protegido quanto o tráfego que foi bloqueado pelas mitigações do Shield Advanced.

Os detalhes da mitigação são para todas as regras na ACL da web associadas ao recurso, incluindo regras implantadas especificamente em resposta a um ataque e regras baseadas em taxas definidas na ACL da web. Se você habilitar a mitigação automática de DDoS na camada de aplicação para um aplicativo, as métricas de mitigação incluirão métricas para essas regras adicionais. Para obter informações sobre essas proteções da camada de aplicação, consulteAWS Shield Advanced proteções da camada de aplicação (camada 7).

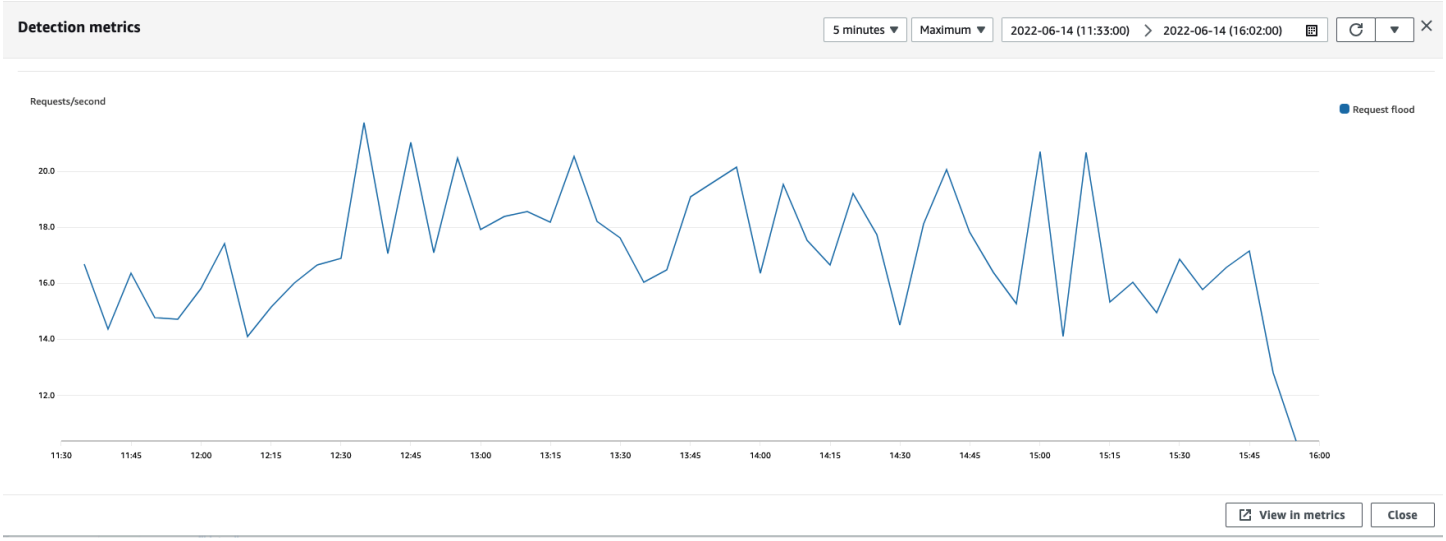
Detecção e mitigação

Para um evento da camada de aplicação (camada 7), a guia Detecção e mitigação mostra métricas de detecção baseadas nas informações obtidas dos AWS WAF registros. As métricas de mitigação

são baseadas em regras AWS WAF na web ACL associada que são configuradas para bloquear o tráfego indesejado.

Para CloudFront distribuições da Amazon, você pode configurar o Shield Advanced para aplicar mitigações automáticas para você. Com qualquer recurso da camada de aplicativo, você pode escolher definir suas próprias regras de mitigação em sua web ACL e solicitar ajuda do Shield Response Team (SRT). Para obter informações sobre essas opções, consulte Resposta a eventos de DDoS.

A captura de tela a seguir mostra um exemplo das métricas de detecção de um evento da camada de aplicação que diminuiu após algumas horas.



O tráfego de eventos que diminui antes que uma regra de mitigação entre em vigor não é representado nas métricas de mitigação. Isso pode resultar em uma diferença entre o tráfego de solicitações da web mostrado nos gráficos de detecção e as métricas de permissão e bloqueio mostradas nos gráficos de mitigação.

Principais responsáveis

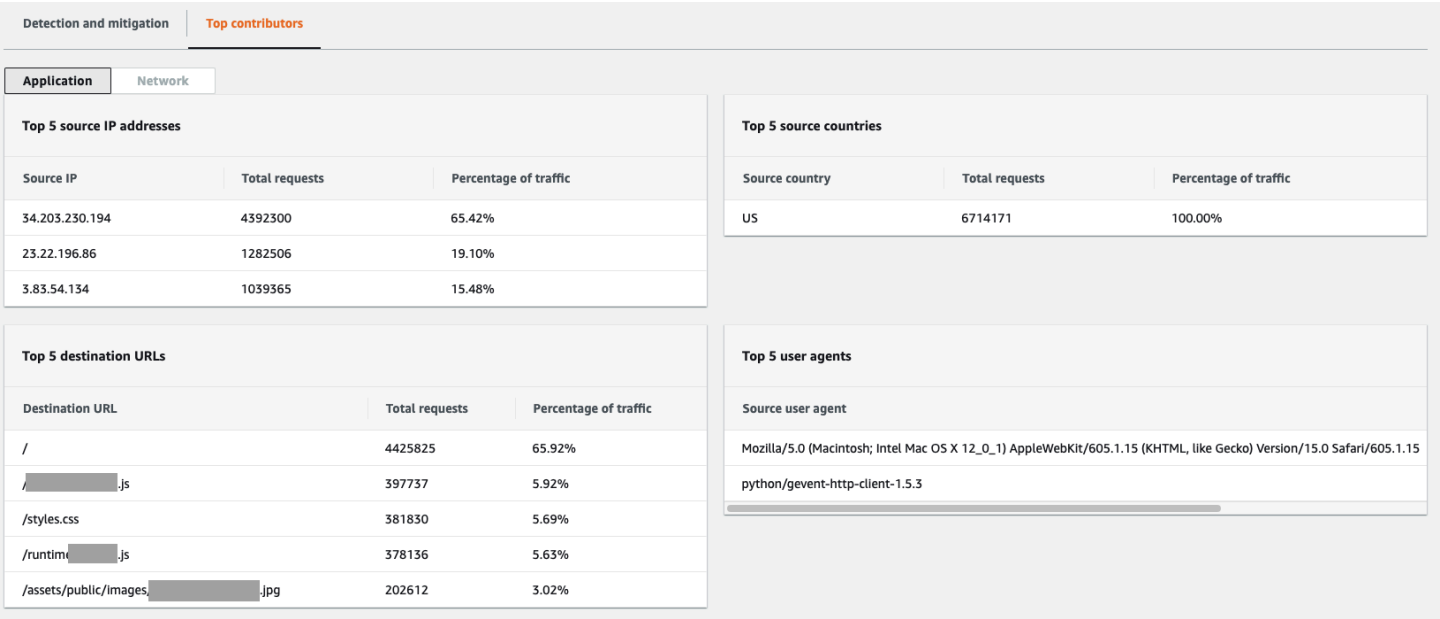
A guia Principais colaboradores dos eventos da camada de aplicação exibe os 5 principais colaboradores que a Shield identificou para o evento, com base nos AWS WAF registros recuperados. O Shield categoriza as informações dos principais responsáveis por dimensões, como IP de origem, país de origem e URL de destino.

> **Note**
>
> Para obter as informações mais precisas sobre o tráfego que está contribuindo para um evento da camada de aplicação, use os AWS WAF registros.

Use as informações dos principais responsáveis da camada de aplicação Shield somente para ter uma ideia geral da natureza de um ataque, e não baseie suas decisões de segurança nessas informações. Para eventos da camada de aplicação, os AWS WAF registros são a melhor fonte de informações para entender os contribuintes de um ataque e para elaborar suas estratégias de mitigação.

As informações dos principais colaboradores do Shield nem sempre refletem completamente os dados nos AWS WAF registros. Ao processar os logs, o Shield prioriza a redução do impacto no desempenho do sistema em vez de recuperar o conjunto completo de dados dos logs. Isso pode resultar em uma perda de granularidade nos dados que estão disponíveis para o Shield analisar. Em grande parte dos casos, a maioria das informações está disponível, mas é possível que os dados do principal responsável sejam distorcidos em algum grau devido a algum ataque.

A captura de tela a seguir mostra um exemplo da guia Principais responsáveis para um evento na camada de aplicação.



As informações do responsável são baseadas em solicitações de tráfego legítimo e potencialmente indesejado. Eventos de maior volume e eventos em que as fontes de solicitação não são altamente distribuídas têm maior probabilidade de ter os principais responsáveis identificáveis. Um ataque

significativamente distribuído pode ter qualquer número de fontes, dificultando a identificação dos principais responsáveis pelo ataque. Se o Shield Advanced não identificar responsáveis significativos para uma categoria específica, ele exibirá os dados como indisponíveis.

Detalhes do evento da camada de infraestrutura

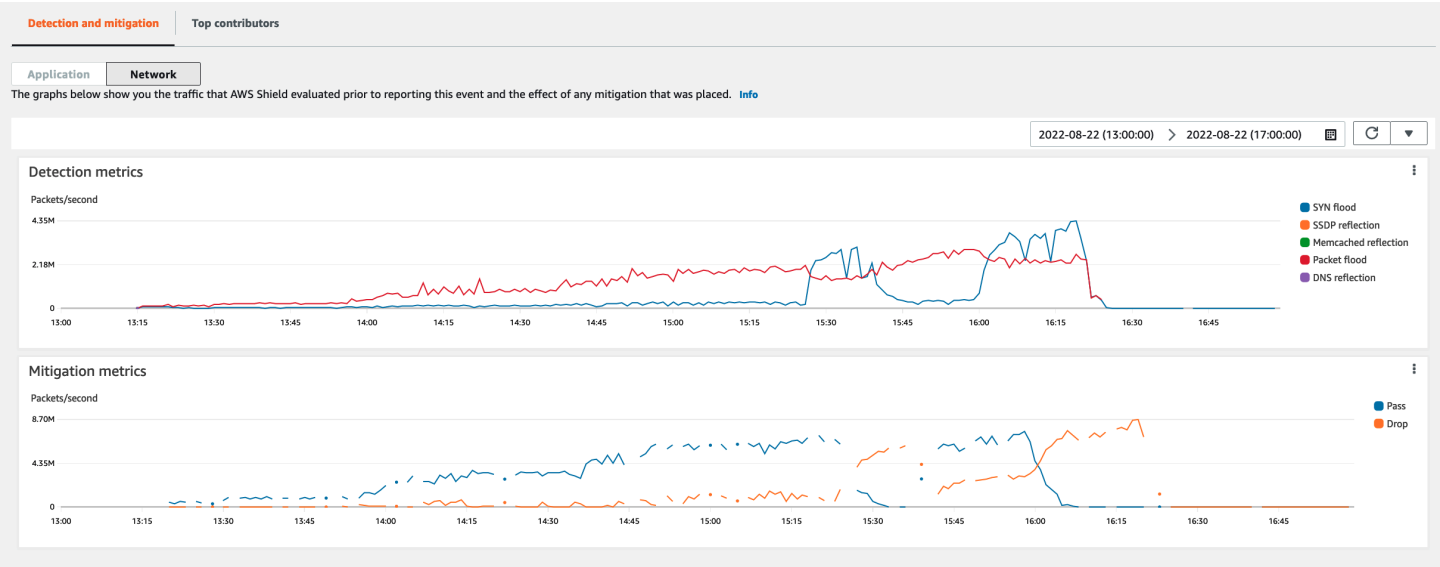
Na seção inferior da página do console do evento, você pode ver detalhes sobre a detecção, a mitigação e os principais responsáveis de um evento na camada de infraestrutura. Essa seção pode incluir uma combinação de tráfego legítimo e potencialmente indesejado e pode representar tanto o tráfego passado para seu recurso protegido, quanto o tráfego bloqueado pelas mitigações do Shield.

Detecção e mitigação

Para um evento na camada de infraestrutura (camada 3 ou 4), a guia Detecção e mitigação mostra as métricas de detecção baseadas em amostras de fluxos de rede, além das métricas de mitigação baseadas no tráfego observado pelos sistemas de mitigação. As métricas de mitigação são uma medida mais precisa do tráfego em seu recurso.

O Shield cria automaticamente uma mitigação para os tipos de recursos protegidos Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB) e acelerador padrão. AWS Global Accelerator As métricas de mitigação para endereços EIP e aceleradores AWS Global Accelerator padrão indicam o número de pacotes aprovados e descartados.

A captura de tela a seguir mostra um exemplo da guia Detecção e mitigação para um evento na camada de infraestrutura.

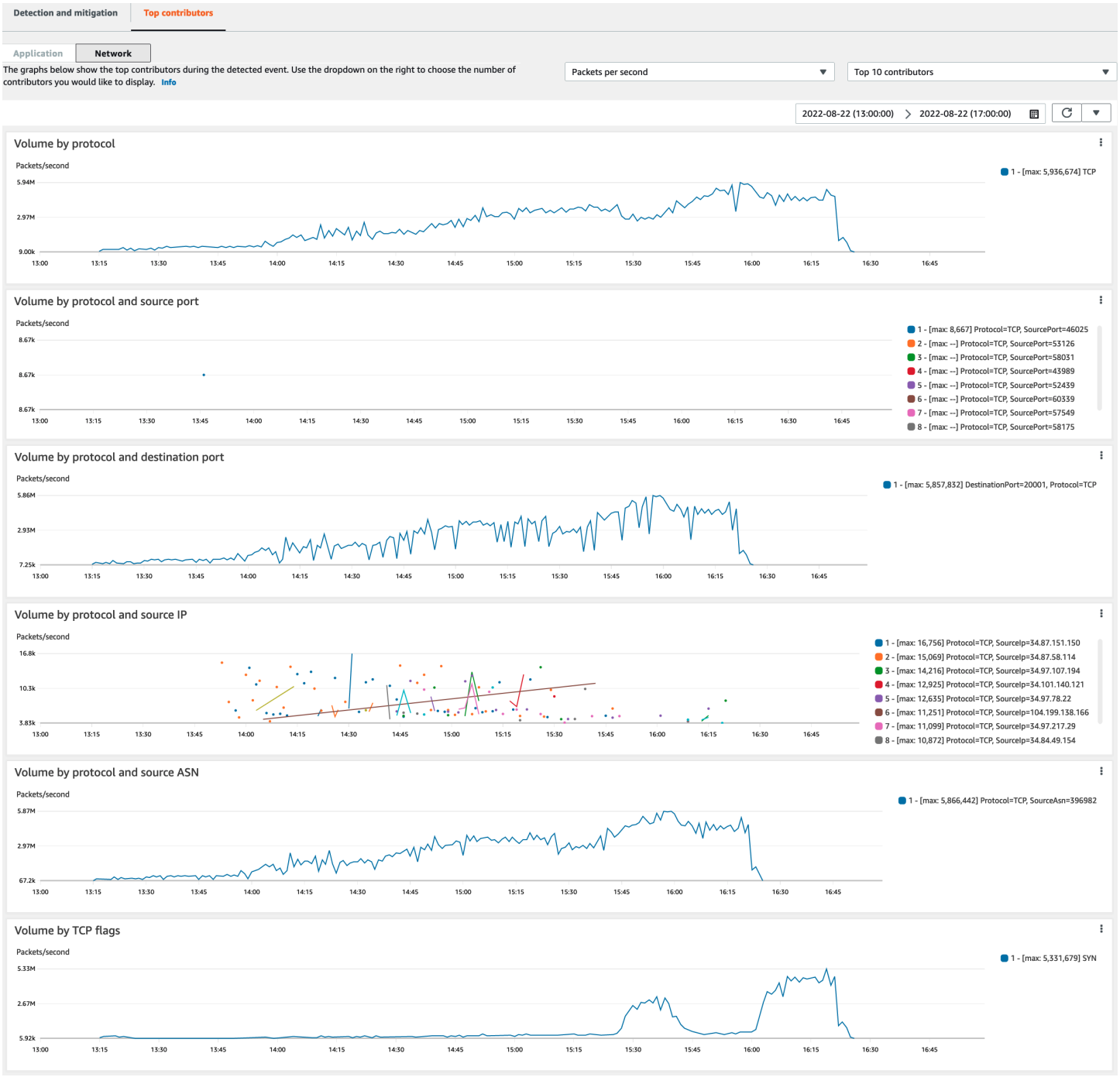


O tráfego de eventos diminui antes que o Shield faça uma mitigação não está representado nas métricas de mitigação. Isso pode resultar em uma diferença entre o tráfego mostrado nos gráficos de detecção, as métricas de aprovação e descarte mostradas nos gráficos de mitigação.

Principais responsáveis

A guia Principais responsáveis para eventos da camada de infraestrutura lista métricas para até 100 principais responsáveis em várias dimensões de tráfego. Os detalhes incluem propriedades da camada de rede para qualquer dimensão em que pelo menos cinco fontes significativas de tráfego possam ser identificadas. Exemplos de fontes de tráfego são IP de origem e ASN de origem.

A captura de tela a seguir mostra um exemplo da guia Principais responsáveis para um evento na camada de infraestrutura.



As métricas do responsável são baseadas em amostras de fluxos de rede para tráfego legítimo e potencialmente indesejado. Eventos de maior volume e eventos em que as fontes de tráfego não são altamente distribuídas têm maior probabilidade de ter os principais responsáveis identificáveis. Um ataque significativamente distribuído pode ter qualquer número de fontes, dificultando a identificação dos principais responsáveis pelo ataque. Se o Shield não identificar nenhum responsável significativo para uma métrica ou categoria específica, ele exibirá os dados como indisponíveis.

Em um ataque de DDoS na camada de infraestrutura, as fontes de tráfego podem ser falsificadas ou refletidas. Uma fonte falsificada é intencionalmente forjada pelo atacante. Uma fonte refletida é a fonte real do tráfego detectado, mas não se trata de um participante voluntário do ataque. Por exemplo, um invasor pode gerar um grande e amplificado flood de tráfego para um alvo ao refletir o ataque a serviços na Internet que normalmente são legítimos. Nesse caso, as informações da fonte podem ser válidas, embora não sejam a fonte real do ataque. Esses fatores podem limitar a viabilidade das técnicas de mitigação que bloqueiam as fontes com base nos cabeçalhos dos pacotes.

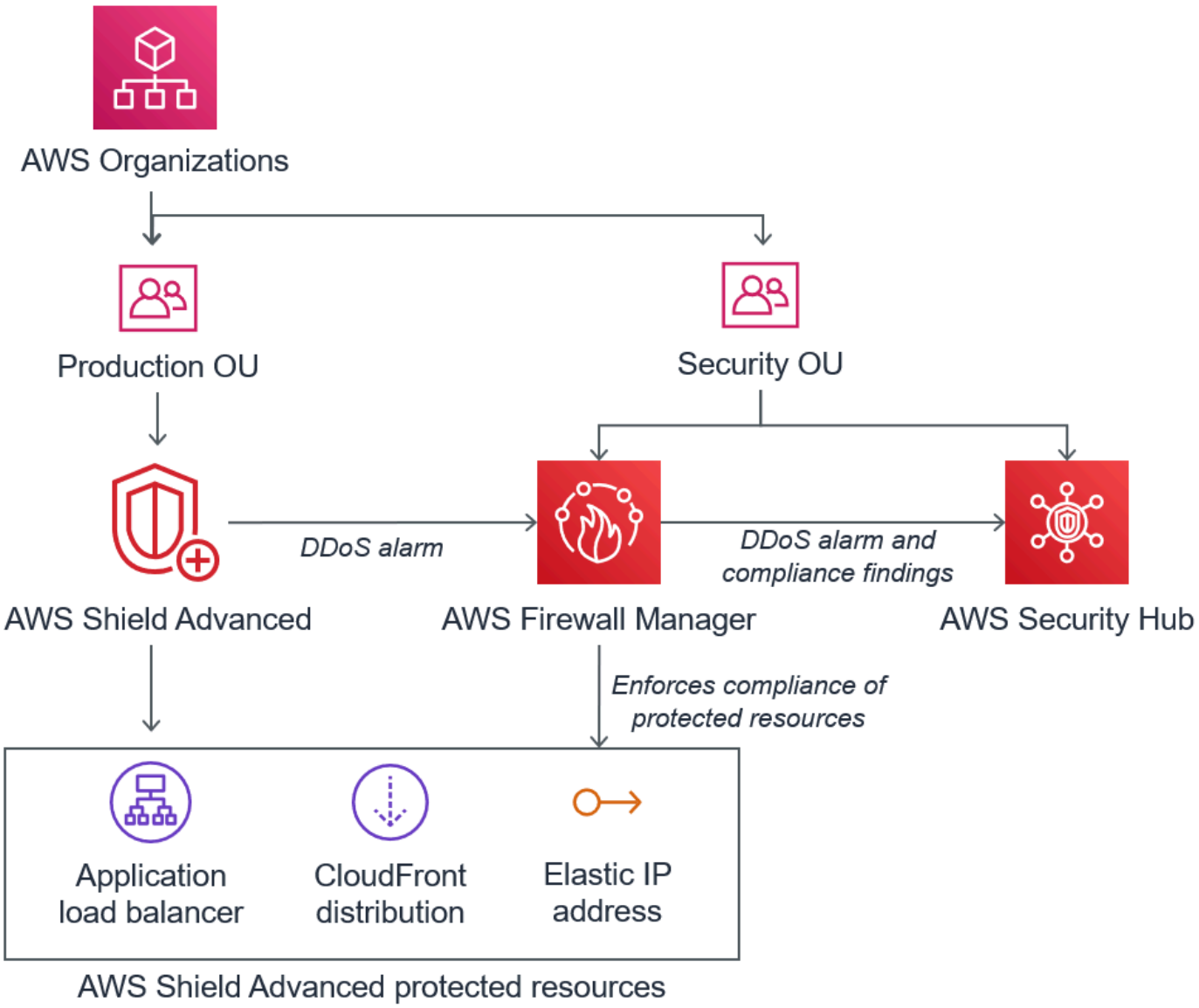
Visibilidade do evento entre contas

Você pode usar AWS Firewall Manager e AWS Security Hub gerenciar e monitorar recursos AWS Shield Advanced protegidos em várias contas.

Com o Firewall Manager, você pode criar uma política de segurança do Shield Advanced que reporta e impõe a conformidade da proteção contra DDoS em todas as suas contas. O Firewall Manager monitora seus recursos protegidos, incluindo a adição de proteções a novos recursos que entram no escopo da política do Shield Advanced.

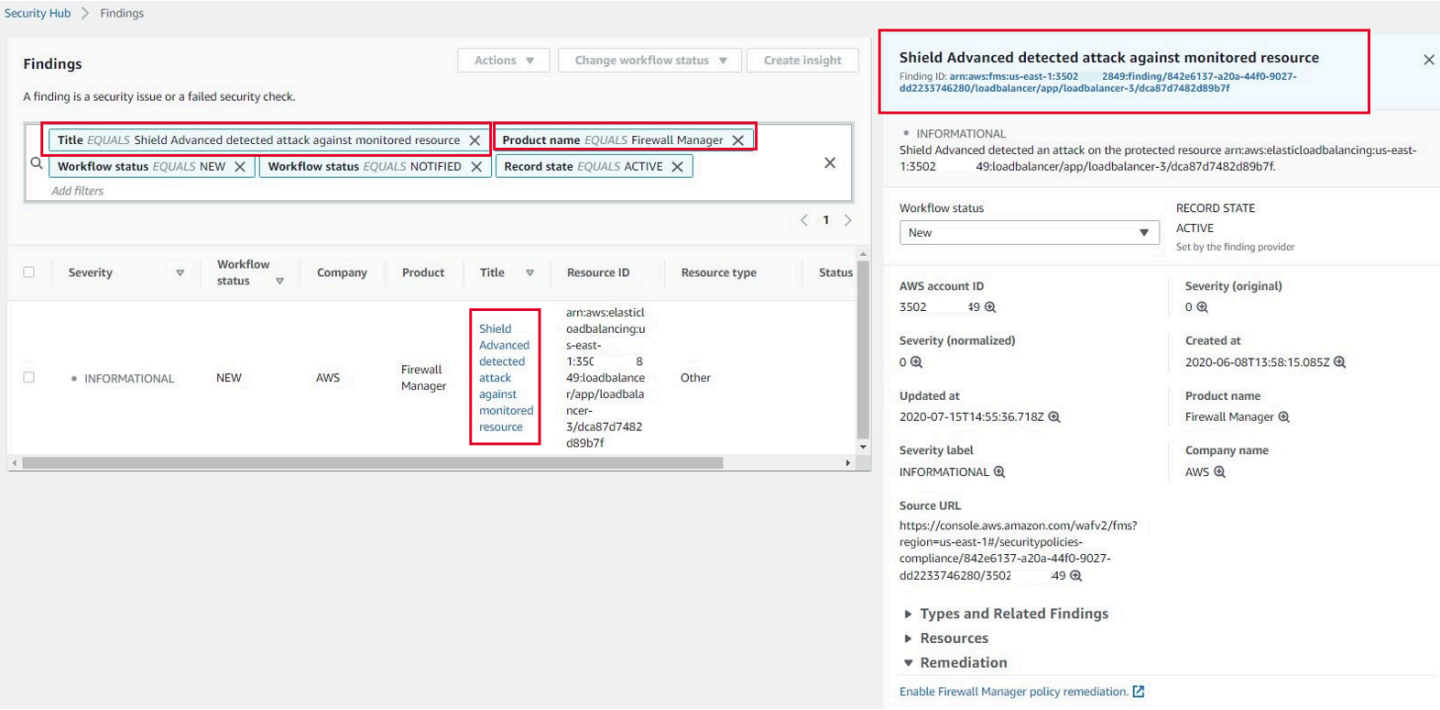
Você pode integrar o Firewall Manager AWS Security Hub para obter um único painel que relata eventos de DDoS detectados pelas descobertas de conformidade do Shield Advanced e do Firewall Manager, quando o Firewall Manager identifica um recurso que está fora de conformidade com sua política de segurança Shield Advanced.

A figura a seguir mostra uma arquitetura típica para monitorar os recursos protegidos do Shield Advanced com o Firewall Manager e o Security Hub.



Ao integrar o Firewall Manager com o Security Hub, você pode visualizar as descobertas de segurança em um único local, junto com outros alertas e informações de status de conformidade dos aplicativos em que você executa na AWS.

A captura de tela a seguir destaca as informações que você pode ver sobre um evento Shield Advanced dentro do console do Security Hub quando você tiver uma integração desse tipo.



Para saber como integrar o Firewall Manager e o Security Hub ao Shield Advanced para centralizar o monitoramento de eventos e conformidade em suas contas protegidas, consulte o blog de AWS segurança Configure o monitoramento centralizado para eventos de DDoS e corrija automaticamente recursos não compatíveis.

Resposta a eventos de DDoS

AWS mitiga automaticamente os ataques de negação de serviço distribuído (DDoS) na rede e na camada de transporte (camada 3 e camada 4). Se você usa o Shield Advanced para proteger suas instâncias do Amazon EC2, durante um ataque, o Shield Advanced implanta automaticamente suas ACLs de rede Amazon VPC na borda da rede AWS . Isso permite que o Shield Advanced forneça proteção contra eventos maiores de DDoS. Para obter mais informações sobre network ACLs, consulte network ACLs.

Para ataques de DDoS na camada de aplicação (camada 7), AWS tentativas de detectar e notificar AWS Shield Advanced os clientes por meio de CloudWatch alarmes. Por padrão, ele não aplica mitigações automaticamente para evitar o bloqueio inadvertido do tráfego válido de usuários.

Para recursos da camada de aplicação (camada 7), você tem as seguintes opções disponíveis para responder a um ataque.

- Fornecer suas próprias mitigações: você pode investigar e mitigar o ataque sozinho. Para mais informações, consulte Mitigação manual de um ataque de DDoS na camada de aplicação.
- Entrar em contato com o suporte: se você é cliente do Shield Advanced, pode entrar em contato com o Centro AWS Support para obter ajuda com as mitigações. Casos críticos e urgentes são encaminhados diretamente a especialistas em DDoS. Para mais informações, consulte Entrando em contato com o centro de suporte durante um ataque de DDoS na camada de aplicação.

Além disso, antes que um ataque ocorra, você pode ativar proativamente as seguintes opções de mitigação:

- Mitigações automáticas nas CloudFront distribuições da Amazon — Com essa opção, o Shield Advanced define e gerencia regras de mitigação para você em sua ACL web. Para obter informações sobre a mitigação automática da camada de aplicação, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.
- Engajamento proativo — Quando AWS Shield Advanced detecta um grande ataque na camada de aplicativos contra um de seus aplicativos, o SRT pode entrar em contato com você de forma proativa. O SRT faz a triagem do incidente de DDoS e cria mitigações do AWS WAF . O SRT entra em contato com você e, com seu consentimento, pode aplicar as regras AWS WAF . Para obter mais informações sobre essa opção, consulte Como configurar o engajamento proativo.

Entrando em contato com o centro de suporte durante um ataque de DDoS na camada de aplicação

Se você for um AWS Shield Advanced cliente, entre em contato com o AWS Support Centro para obter ajuda com as mitigações. Casos críticos e urgentes são encaminhados diretamente a especialistas em DDoS. Com isso AWS Shield Advanced, casos complexos podem ser encaminhados para a AWS Shield Response Team (SRT), que tem profunda experiência em proteger AWS a Amazon.com e suas subsidiárias. Para obter mais informações sobre o SRT, consulte Suporte do Shield Response Team (SRT).

Para obter suporte do Shield Response Team (SRT), entre em contato com a Central AWS Support. O tempo de resposta para seu caso dependerá da gravidade selecionada e dos tempos de resposta, que são documentados na página Plano de suporte da AWS Support.

Selecione as seguintes opções:

- Tipo de caso: suporte técnico

- Serviço: negação de serviço distribuída (DDoS)
- Categoria: Entrada para AWS
- Gravidade: escolha uma opção apropriada

Ao conversar com nosso representante, explique que você é um AWS Shield Advanced cliente que está enfrentando um possível ataque de DDoS. Nosso representante encaminhará sua chamada aos especialistas em DDoS. Se você abrir um caso na Central AWS Support usando o tipo de serviço Distributed Denial of Service (DDoS), poderá falar diretamente com um especialista em DDoS por chat ou telefone. Os engenheiros de suporte de DDoS podem ajudá-lo a identificar ataques, recomendar melhorias em sua AWS arquitetura e fornecer orientação sobre o uso de AWS serviços para mitigação de ataques de DDoS.

Para ataques na camada de aplicação, o SRT pode ajudá-lo a analisar a atividade suspeita. Se você tiver a mitigação automática ativada para seu recurso, o SRT poderá analisar as mitigações que o Shield Advanced está aplicando automaticamente contra o ataque. Em qualquer caso, o SRT pode ajudá-lo a analisar e mitigar o problema. As mitigações recomendadas pelo SRT geralmente exigem que o SRT crie ou atualize listas de controle de acesso à AWS WAF web (ACLs da web) em sua conta. O SRT precisará de sua permissão para fazer esse trabalho.

> **Important**
>
> Recomendamos que, como parte da habilitação AWS Shield Advanced, você siga as etapas Como configurar o acesso para o Shield Response Team (SRT) para fornecer proativamente ao SRT as permissões necessárias para ajudá-lo durante um ataque. Fornecer a permissão antecipadamente ajuda a evitar atrasos no caso de um ataque real.

O SRT ajuda você a fazer a triagem do ataque DDoS para identificar assinaturas e padrões de ataques. Com seu consentimento, o SRT cria e implanta AWS WAF regras para mitigar o ataque.

Você também pode entrar em contato com o SRT antes ou durante um possível ataque para desenvolver e implantar mitigações personalizadas. Por exemplo, se você estiver executando um aplicativo web e precisar apenas das portas 80 e 443 abertas, você pode trabalhar com o SRT para pré-configurar uma web ACL para “permitir” apenas as portas 80 e 443.

Você autoriza e entra em contato com o SRT no nível de conta. Ou seja, se você usar o Shield Advanced em uma política do Firewall Manager Shield Advanced, o proprietário da conta, e não

o administrador do Firewall Manager, deverá entrar em contato com o SRT para obter suporte. O administrador do Firewall Manager poderá autorizar o SRT apenas para contas pertencentes a ele.

Mitigação manual de um ataque de DDoS na camada de aplicação

Se você determinar que a atividade na página de eventos do seu recurso representa um ataque de DDoS, você pode criar suas próprias AWS WAF regras em sua ACL da web para mitigar o ataque. Essa é a única opção disponível se você não for cliente do Shield Advanced. AWS WAF está incluído sem AWS Shield Advanced custo adicional. Para obter mais informações sobre como criar regras na sua web ACL, consulte AWS WAF listas de controle de acesso à web (ACLs da web).

Se você usa AWS Firewall Manager, você pode adicionar suas AWS WAF regras a uma AWS WAF política do Firewall Manager.

Para mitigar manualmente um potencial ataque de DDoS na camada de aplicação

1. Crie declarações de regras em sua web ACL com critérios que correspondam ao comportamento incomum. Para começar, configure-os para contar as solicitações correspondentes. Para obter informações sobre como configurar sua web ACL e declarações de regras, consulte Avaliação de regras da web ACL e do grupo de regras e Testando e ajustando suas AWS WAF proteções.

   > **Note**
   >
   > Sempre teste suas regras primeiro usando inicialmente a ação de regra Count em vez de Block. Assim que estiver certo de que suas novas regras estão identificando as solicitações corretas, você poderá modificá-las para bloquear essas solicitações.

2. Monitore as contagens de solicitações para determinar se você deseja bloquear as solicitações correspondentes. Se o volume de solicitações continuar incomumente alto e você tiver certeza de que suas regras estão capturando as solicitações que estão causando o alto volume, altere as regras em sua web ACL para bloquear as solicitações.
3. Continue monitorando a página de eventos para garantir que seu tráfego seja tratado como você deseja.

AWS fornece modelos pré-configurados para você começar rapidamente. Os modelos incluem um conjunto de AWS WAF regras que você pode personalizar e usar para bloquear ataques comuns baseados na web. Para obter mais informações, consulte Automações de segurança do AWS WAF.

Solicitando um crédito em AWS Shield Advanced

Se você é assinante AWS Shield Advanced e sofre um ataque de DDoS que aumenta a utilização de um recurso protegido do Shield Advanced, você pode solicitar um crédito de serviço do Shield Advanced para cobranças relacionadas ao aumento da utilização, na medida em que não seja mitigado pelo Shield Advanced.

> **Note**
>
> Você pode aplicar quaisquer créditos recebidos por meio desse processo somente ao uso do Shield Advanced. Os créditos Shield Advanced não estão disponíveis para uso com outros serviços.

Os créditos estão disponíveis somente para os seguintes tipos de cobranças:

- Transferência de dados do Shield Advanced
- Solicitações CloudFront HTTP/HTTPS da Amazon
- CloudFront transferência de dados para fora
- Consultas do Amazon Route 53
- AWS Global Accelerator transferência de dados do acelerador padrão
- Unidades de capacidade do balanceador de carga para Application Load Balancer
- Custos de instância para instâncias protegidas do Amazon Elastic Compute Cloud (Amazon EC2) que foram criadas por uma política de ajuste de escala automático em resposta ao ataque

Pré-requisitos para solicitar um crédito

Para estar elegível para o crédito, antes do início do ataque, você deve ter feito o seguinte:

- É preciso ter adicionado a proteção Shield Advanced aos recursos para os quais deseja solicitar um crédito. Os recursos protegidos adicionados durante um ataque não são elegíveis para proteção de custos.

> **Note**
>
> Ativar o Shield Advanced no seu Conta da AWS não ativa automaticamente a proteção Shield Advanced para recursos individuais.

Para obter mais informações sobre como proteger AWS recursos usando o Shield Advanced, consulteAdicionando AWS Shield Advanced proteção aos AWS recursos.

- Para recursos aplicáveis CloudFront e protegidos pelo Application Load Balancer, você deve ter associado uma ACL AWS WAF da web e implementado uma regra baseada em taxa na ACL da web no modo. Block Para obter mais informações sobre regras baseadas em intervalos no AWS WAF , consulte Instrução de regra baseada em intervalos. Para obter informações sobre como associar ACLs da web a AWS recursos, consulteAWS WAF listas de controle de acesso à web (ACLs da web).
- Você deve ter implementado as melhores práticas apropriadas em Práticas recomendadas da AWS para resiliência de DDoS para configurar seu aplicativo de forma que minimize os custos durante um ataque de DDoS.

Como solicitar um crédito

Para se qualificar para um crédito, você deve enviar sua solicitação de crédito dentro do período de 15 dias imediatamente após o mês de cobrança no qual o ataque ocorreu.

Para solicitar um crédito, envie um caso de cobrança pela Central AWS Support. Na sua solicitação, inclua:

- As palavras “Concessão de DDoS” na linha de assunto
- As datas e horários de cada evento ou interrupção de disponibilidade para a qual você está solicitando um crédito
- Os AWS serviços e recursos específicos que foram afetados

Depois de enviar uma solicitação, a AWS Shield Response Team (SRT) validará se ocorreu um ataque de DDoS e, em caso afirmativo, se algum recurso protegido foi escalado para absorver o ataque de DDoS. Se AWS determinar que os recursos protegidos foram escalados para absorver o ataque de DDoS, AWS emitirá um crédito pela parte do tráfego que AWS determina que foi causada pelo ataque DDoS. Os créditos são válidos por 12 meses.

Segurança no uso do AWS Shield serviço

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

> **Note**
>
> Esta seção fornece diretrizes AWS de segurança padrão para o uso do AWS Shield serviço e de seus AWS recursos, como as proteções Shield Advanced.
> Para obter informações sobre como proteger seus AWS recursos usando o Shield e o Shield Advanced, consulte o restante do AWS Shield guia.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto 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. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Shield, consulte Serviços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, como a confidencialidade de seus dados, os requisitos da sua organização, leis e regulamentos aplicáveis.

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

Tópicos

- Validação de conformidade do Shield
- Resiliência no Shield
- Segurança da infraestrutura no AWS Shield

Proteção de dados no Shield

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Shield. 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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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 os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- 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 sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Shield ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

As entidades do Shield, como proteções, são criptografadas em repouso, exceto em determinadas regiões onde a criptografia não está disponível, incluindo China (Pequim) e China (Ningxia). Chaves de criptografia exclusivas são usadas para cada região.

Gerenciamento de identidade e acesso para AWS Shield

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 (fazer login) e autorizado (ter permissões) para usar recursos do Shield. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Shield.

Usuário do serviço: se você usa o serviço Shield para fazer o trabalho, seu administrador fornece as credenciais e as permissões necessárias. À medida que usar mais atributos do Shield para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Shield, consulte Solução de problemas AWS Shield de identidade e acesso.

Administrador do serviço: se você for o responsável pelos recursos do Shield na empresa, provavelmente terá acesso total ao Shield. Cabe a você determinar quais funcionalidades e atributos do Shield os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Shield, consulte Como AWS Shield funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Shield. Para visualizar exemplos de políticas baseadas em identidade do Shield que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar

solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais

temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). 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.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la

para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

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.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade

do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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 Shield funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Shield, saiba quais atributos do IAM estão disponíveis para uso com o Shield.

Recursos do IAM que você pode usar com AWS Shield

Atributo do IAM	Suporte Shield
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como o Shield 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.

Políticas baseadas em identidade para o Shield

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições.

Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para visualizar exemplos de políticas baseadas em identidade do Shield, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

Políticas baseadas em recursos no Shield

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas do Shield

Oferece compatibilidade 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Shield, consulte Ações definidas pelo AWS Shield na Referência de autorização do serviço.

As ações de políticas no Shield usam o seguinte prefixo antes da ação:

```
shield
```

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

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações no Shield que começam com `List`, inclua a seguinte ação:

```
"Action": "shield:List*"
```

Para visualizar exemplos de políticas baseadas em identidade do Shield, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

Recursos de políticas para o Shield

Oferece compatibilidade 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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para obter uma lista dos tipos de recursos do Shield e seus ARNs, consulte Recursos definidos pelo AWS Shield na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Shield. Para permitir ou negar o acesso a um subconjunto de recursos do Shield, inclua o ARN do recurso no elemento `resource` da sua política.

Dentro AWS Shield, os recursos são proteções e ataques. Esses recursos têm ARNs exclusivos associado, conforme mostrado na tabela a seguir.

Nome no AWS Shield console	Nome no AWS Shield SDK/ CLI	Formato do ARN
Evento ou ataque	`AttackDetail`	`arn:aws:shield:: account:attack/ID`
Proteção	`Protection`	`arn:aws:shield:: account:protection/ ID`

Para permitir ou negar o acesso a um subconjunto de recursos do Shield, inclua o ARN do recurso no elemento `resource` da sua política. Os ARNs do Shield têm o seguinte formato:

```
arn:partition:shield::account:resource/ID
```

Substitua as variáveis *`account`*, *`resource`* e *`ID`* por valores válidos. Os valores válidos podem ser os seguintes:

- *`conta`*: O ID do seu Conta da AWS. Você deve especificar um valor.
- *`resource`*: o tipo de recurso do Shield, seja `attack` ou `protection`.
- *`ID`*: o ID do recurso do Shield ou um curinga (`*`) para indicar todos os recursos do tipo especificado associados à Conta da AWS especificada.

Por exemplo, o ARN a seguir especifica todas as proteções da conta `111122223333`:

```
arn:aws:shield::111122223333:protection/*
```

Os ARNs para recursos do Shield têm o seguinte formato:

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Para obter informações sobre os ARNs, consulte Nomes de recurso da Amazon (ARN) na Referência geral da Amazon Web Services.

A seguir, são listados os requisitos específicos dos ARNs dos recursos `wafv2`:

- *`região`*: para os recursos do Shield que você usa para proteger CloudFront as distribuições da Amazon, defina `us-east-1` isso como. Caso contrário, defina isso para a região que você está usando com seus recursos regionais protegidos.
- *`escopo`*: defina o escopo `global` para uso com uma CloudFront distribuição da Amazon ou `regional` para uso com qualquer um dos recursos regionais que oferecem AWS WAF suporte. Os recursos regionais são uma API REST do Amazon API Gateway, um Application Load Balancer, uma API GraphQL AWS AppSync , um grupo de usuários do Amazon Cognito, um AWS App Runner serviço e uma instância de acesso verificado. AWS
- *`resource-type`*: especifique um dos seguintes valores: `attack` para eventos ou ataques, `protection` para proteções.

- *resource-name*: especifique o nome que você deu ao recurso Shield ou especifique um curinga (*) para indicar todos os recursos que atendem às outras especificações no ARN. Você deve especificar o nome do recurso e a ID do recurso ou especificar um caractere curinga para ambos.
- *resource-id*: especifique a ID do recurso Shield ou especifique um curinga (*) para indicar todos os recursos que atendem às outras especificações no ARN. Você deve especificar o nome do recurso e a ID do recurso ou especificar um caractere curinga para ambos.

Por exemplo, o ARN a seguir especifica todas as web ACLscom escopo regional da conta `111122223333` na região `us-west-1`:

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

O ARN a seguir especifica o grupo de regras nomeado `MyIPManagementRuleGroup` com escopo global para a conta `111122223333` na região `us-east-1`:

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Para visualizar exemplos de políticas baseadas em identidade do Shield, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

Chaves de condição de políticas para o Shield

Suporta 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar

vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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 de chaves de condição do Shield, consulte Chaves de condição do AWS Shield na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Shield.

Para visualizar exemplos de políticas baseadas em identidade do Shield, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

ACLs no Shield

Oferece compatibilidade 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Shield

Oferece compatibilidade com ABAC (tags em políticas)	Parcial

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para

permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Shield

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o Shield

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço do Shield

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, 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 um perfil de serviço pode prejudicar a funcionalidade do Shield. Só edite os perfis de serviço quando o Shield orientá-lo a fazê-lo.

Funções vinculadas ao serviço para o Shield

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Shield, consulte Usar funções vinculadas ao serviço para o Shield Advanced.

Exemplos de políticas baseadas em identidade para o AWS Shield

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Shield. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo ACM, incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição do AWS Shield na Referência de autorização do serviço.

Tópicos

- Práticas recomendadas de políticas
- Como usar o console do Shield
- Permitir que os usuários visualizem suas próprias permissões
- Conceda acesso de leitura às suas proteções Shield Advanced
- Conceda acesso somente de leitura ao Shield,, e CloudFront CloudWatch
- Conceda acesso total ao Shield, CloudFront, e CloudWatch

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Shield em sua conta. Essas ações podem incorrer em custos para a 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 mais informações, 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 mais informações 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: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode 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 AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition 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 acionáveis para ajudar você a criar políticas seguras e funcionais. Para mais informações, 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 a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

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

Como usar o console do Shield

Para acessar o AWS Shield console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Shield em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do 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 a operação de API que estiverem tentando executar.

Os usuários que podem acessar e usar o AWS console também podem acessar o AWS Shield console. Nenhuma permissão adicional é necessária.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

Conceda acesso de leitura às suas proteções Shield Advanced

AWS Shield permite acesso a recursos entre contas, mas não permite que você crie proteções de recursos entre contas. Você só pode criar proteções para recursos de dentro da conta que possui esses recursos.

Veja a seguir um exemplo de política que concede permissões para a ação `shield:ListProtections` em todos os recursos. Na implementação atual, o Shield não oferece suporte à identificação de recursos específicos que usam os ARNs do recurso (também chamados de permissões de nível de recurso) para algumas das ações de API. Portanto, você deve especificar um caractere curinga (*). Isso só permite o acesso aos recursos que você pode recuperar por meio da ação `ListProtections`.

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Conceda acesso somente de leitura ao Shield,, e CloudFront CloudWatch

A política a seguir concede aos usuários acesso somente de leitura ao Shield e aos recursos associados, incluindo CloudFront recursos da Amazon e métricas da Amazon CloudWatch . É útil para usuários que precisam de permissão para visualizar as configurações nas proteções e ataques do Shield e monitorar as métricas em CloudWatch. Esses usuários não podem criar, atualizar nem excluir recursos do Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldReadOnly",
                "Effect": "Allow",
                "Action": [
                    "shield:List*",
                    "shield:Describe*",
                    "shield:Get*"
```

```
                ],
                "Resource": "*"
            }
    ]
}
```

Conceda acesso total ao Shield, CloudFront, e CloudWatch

A política a seguir permite que os usuários realizem qualquer operação do Shield, realizem qualquer operação em distribuições CloudFront da web e monitorem métricas e uma amostra de solicitações recebidas. CloudWatch Ela é útil aos usuários que são administradores do Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldFullAccess",
                "Effect": "Allow",
```

```
                "Action": [
                    "shield:*"
                ],
                "Resource": "*"
            }
        ]
}
```

Recomendamos que você configure autenticação multifator (MFA) para os usuários que tiverem permissões administrativas. Para obter mais informações, consulte Como usar dispositivos com autenticação multifator (MFA) com o AWS no Guia do usuário do IAM.

AWS políticas gerenciadas para AWS Shield

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSShieldDRTAccessPolicy

AWS Shield usa essa política gerenciada quando você concede permissão à Shield Response Team (SRT) para agir em seu nome. Essa política dá ao SRT acesso limitado à sua AWS conta, para ajudar na mitigação de ataques de DDoS durante eventos de alta gravidade. Essa política permite que o SRT gerencie suas AWS WAF regras e as proteções do Shield Advanced e acesse seus AWS WAF registros.

Para obter informações sobre como conceder permissão ao SRT para operar em seu nome, consulte Como configurar o acesso para o Shield Response Team (SRT).

Para obter detalhes sobre essa política, consulte AWSShieldDRTAccessPolicyno console do IAM.

AWS política gerenciada: AWSShieldServiceRolePolicy

O Shield Advanced usa essa política gerenciada quando você ativa a mitigação automática de DDoS na camada de aplicação, para definir as permissões necessárias para gerenciar recursos da sua conta. Essa política permite que o Shield Advanced crie e aplique AWS WAF regras e grupos de regras nas ACLs da web que você associou aos seus recursos protegidos, para responder automaticamente aos ataques de DDoS.

Você não pode se vincular AWSShieldServiceRolePolicy às suas entidades do IAM. O Shield anexa esta política a uma função vinculada ao serviço `AWSServiceRoleForAWSShield` que permite que o Shield realize ações em seu nome.

O Shield Advanced permite o uso dessa política quando você ativa a mitigação automática de DDoS da camada de aplicação. Para obter mais informações sobre esta política, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

Para obter informações sobre a função vinculada ao serviço AWSServiceRoleForAWSShield que usa essa política, consulte Usar funções vinculadas ao serviço para o Shield Advanced

Para obter detalhes sobre essa política, consulte AWSShieldServiceRolePolicyno console do IAM.

Atualizações do Shield para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Shield desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos em Histórico do documento.

Política	Descrição de alteração	Data
`AWSShieldServiceRolePolicy` Essa política permite que a Shield acesse e gerencie	Essa política foi adicionada para fornecer ao Shield Advanced as permissões necessárias para a funcional	1º de dezembro de 2021

Política	Descrição de alteração	Data
AWS recursos para responder automaticamente aos ataques de DDoS na camada de aplicação em seu nome. Detalhes no console do IAM: AWSShieldServiceRolePolicy O perfil vinculado ao serviço `AWSServiceRoleForAWSShield` usa essa política. Para mais informações, consulte Usar funções vinculadas ao serviço para o Shield Advanced.	idade automática de mitigação de DDoS na camada de aplicação. Para obter mais informações sobre esse atributo, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.	
O Shield começou a monitorar alterações	A Shield começou a monitorar as mudanças em suas políticas AWS gerenciadas.	3 de março de 2021

Solução de problemas AWS Shield de identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Shield e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Shield
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Shield

Não tenho autorização para executar uma ação no Shield

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 `shield:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `shield:`*`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 uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Shield.

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 erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Shield. 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 acessem meus Conta da AWS recursos do Shield

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o

perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Shield oferece suporte a esses atributos, consulte Como AWS Shield 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Usar funções vinculadas ao serviço para o Shield Advanced

AWS Shield Advanced usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente a um serviço do Shield Advanced. As funções vinculadas ao serviço são predefinidas pelo Shield Advanced 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 Shield Advanced porque você não precisa adicionar as permissões necessárias manualmente. O Shield Advanced define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Shield Advanced pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Shield Advanced, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculada ao serviço para o Shield Advanced

O Shield Advanced usa a função vinculada ao serviço chamada. AWSServiceRoleForAWSShield Essa função permite que o Shield Advanced acesse e gerencie AWS recursos para responder automaticamente aos ataques de DDoS na camada de aplicação em seu nome. Para ter mais informações sobre essa função, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

A função AWSServiceRoleForAWSShield vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `shield.amazonaws.com`

A política de permissões de função denominada AWSShieldServiceRolePolicy permite que o Shield Advanced conclua as seguintes ações em todos os AWS recursos:

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Quando ações são permitidas em todos os AWS recursos, isso é indicado na política como`"Resource": "*"`. Isso significa apenas que a função vinculada ao serviço pode realizar cada ação indicada em todos os AWS recursos que a ação suporta. Por exemplo, a ação `wafv2:GetWebACL` é suportada somente para recursos `wafv2` da web ACL.

O Shield Advanced só faz chamadas de API em nível de atributo para atributos protegidos para os quais você habilitou o atributo de proteção da camada de aplicação e para web ACLs associadas a esses atributos protegidos.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para o Shield Advanced

Não é necessário criar manualmente uma função vinculada a serviço. Quando você ativa a mitigação automática de DDoS na camada de aplicação para um recurso na, na ou na AWS Management Console API AWS CLI, o Shield Advanced cria a AWS função vinculada ao serviço para você.

Se excluir essa função vinculada a serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você habilita a mitigação automática de DDoS na camada do aplicativo para um recurso, o Shield Advanced cria o perfil vinculado ao serviço para você mais uma vez.

Edição de uma função vinculada ao serviço para o Shield Advanced

O Shield Advanced não permite que você edite a função AWSServiceRoleForAWSShield vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Exclusão de uma função vinculada ao serviço para o Shield Advanced

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o Shield Advanced estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Shield Advanced que são usados pelo AWSServiceRoleForAWSShield

Para todos os seus recursos que têm proteções contra DDoS na camada de aplicativo configuradas, desative a mitigação automática de DDoS na camada de aplicativo. Para obter instruções sobre o console, consulte Configurar as proteções contra DDoS na camada de aplicação.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForAWSShield vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas a serviço do Shield Advanced

O Shield Advanced oferece suporte a perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Endpoints e cotas do Shield Advanced.

Como registrar em log e monitorar no Shield

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Shield e de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar seus recursos do Shield e responder a possíveis eventos:

CloudWatch Alarmes da Amazon

Usando CloudWatch alarmes, você observa uma única métrica durante um período de tempo especificado. Se a métrica exceder um determinado limite, CloudWatch envia uma notificação para um tópico AWS Auto Scaling ou política do Amazon SNS. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Shield. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Shield, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Registro de chamadas de API do AWS CloudTrail com.

Validação de conformidade do Shield

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. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os

atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Shield

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 executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

Segurança da infraestrutura no AWS Shield

Como serviço gerenciado, AWS Shield é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Shield pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

AWS Shield Advanced cotas

AWS Shield Advanced tem cotas padrão no número de entidades por região. Você pode solicitar um aumento dessas cotas.

Recurso	Cota padrão
Número máximo de recursos protegidos para cada tipo de recurso que AWS Shield Advanced oferece proteção para, por conta.	1.000
Número máximo de grupos de proteção por conta.	100
Número máximo de recursos protegidos individuais que você pode incluir especificamente em um grupo de proteção. Na API, isso se aplica ao `Members` que você especifica ao definir o grupo de proteção `Pattern` como `ARBITRARY` . No console, isso se aplica aos recursos que você seleciona para o agrupamento de proteção Escolha entre recursos protegidos.	1.000

AWS Firewall Manager

AWS Firewall Manager simplifica suas tarefas de administração e manutenção em várias contas e recursos para uma variedade de proteções AWS WAF, incluindo grupos de segurança e ACLs de rede AWS Shield Advanced da Amazon VPC e o Amazon Route 53 Resolver AWS Network Firewall DNS Firewall. Com o Firewall Manager, você configura suas proteções apenas uma vez e o serviço aplica-as automaticamente em todas as contas e recursos, mesmo quando novos recursos e contas forem adicionados.

O Firewall Manager oferece os seguintes benefícios:

- Ajuda a proteger os recursos em todas as contas
- Ajuda a proteger todos os recursos de um tipo específico, como todas as CloudFront distribuições da Amazon
- Ajuda a proteger todos os recursos com tags específicas
- Adiciona automaticamente proteção aos recursos que são adicionados à sua conta
- Permite que você inscreva todas as contas membros de uma AWS Organizations organização e inscreva automaticamente novas contas dentro do escopo que ingressam na organização AWS Shield Advanced
- Permite aplicar regras de grupo de segurança a todas as contas-membro ou subconjuntos específicos de contas em uma organização do AWS Organizations e aplica automaticamente as regras a novas contas no escopo que ingressam na organização
- Permite que você use suas próprias regras ou compre regras gerenciadas do AWS Marketplace

O Firewall Manager é particularmente útil quando você deseja proteger toda a sua organização ao invés de um pequeno número de contas e recursos específicos, ou se você adiciona frequentemente novos recursos que deseja proteger. O Firewall Manager também fornece monitoramento centralizado de ataques de DDoS em toda a sua organização.

Tópicos

- Trabalhando com AWS Firewall Manager políticas
- Trabalhar com conjuntos de recursos no Firewall Manager
- Visualizando as informações de conformidade de uma AWS Firewall Manager política
- AWS Firewall Manager descobertas
- Segurança no uso do AWS Firewall Manager serviço
- AWS Firewall Manager cotas

AWS Firewall Manager preços

As cobranças incorridas por AWS Firewall Manager são para os serviços subjacentes, como AWS WAF e. AWS Config Para obter mais informações, consulte Preços do AWS Firewall Manager.

AWS Firewall Manager pré-requisitos

Este tópico mostra como se preparar para administrar AWS Firewall Manager. Você usa uma conta de administrador do Firewall Manager para gerenciar todas as políticas de segurança do Firewall Manager da sua organização no AWS Organizations. Exceto onde indicado, execute as etapas de pré-requisito usando a conta que você usará como administrador do Firewall Manager.

Antes de usar o Firewall Manager pela primeira vez, execute as etapas a seguir em sequência.

Tópicos

- Etapa 1: unir e configurar AWS Organizations
- Etapa 2: criar uma conta de administrador AWS Firewall Manager padrão
- Etapa 3: ativar AWS Config
- Etapa 4: para políticas de terceiros, assine o Marketplace AWS e defina as configurações de terceiros
- Etapa 5: Para políticas de Network Firewall e Firewall de DNS, habilite o compartilhamento de recursos
- Etapa 6: Para usar AWS Firewall Manager em regiões que estão desativadas por padrão

Etapa 1: unir e configurar AWS Organizations

Para usar o Firewall Manager, sua conta deve ser membro da organização no serviço AWS Organizations em que você deseja usar suas políticas do Firewall Manager.

> **Note**
>
> Para obter mais informações sobre Organizações, consulte o Guia do usuário do AWS Organizations.

Para estabelecer a AWS Organizations associação e a configuração necessárias

1. Escolha uma conta para usar como administrador do Firewall Manager para a organização em Organizações.
2. Se a conta escolhida ainda não for membro da organização, faça com que ela participe. Siga as orientações em Como convidar um homem Conta da AWS para se juntar à sua organização.
3. AWS Organizations tem dois conjuntos de recursos disponíveis: recursos de faturamento consolidado e todos os recursos. Para usar o Firewall Manager, sua organização precisa estar ativada para todos os atributos. Se a organização estiver configurada somente para o faturamento consolidado, siga a orientação em Ativar todos os atributos na sua organização.

Etapa 2: criar uma conta de administrador AWS Firewall Manager padrão

Esse procedimento usa a conta e a organização que você escolheu e configurou na etapa anterior.

Somente a conta de gerenciamento da organização pode criar contas de administrador padrão do Firewall Manager. A primeira conta de administrador que você cria é a conta de administrador padrão. A conta de administrador padrão pode gerenciar firewalls de terceiros e tem escopo administrativo completo. Quando você define a conta de administrador padrão, o Firewall Manager a define automaticamente como administrador AWS Organizations delegado para o Firewall Manager. Isso permite que o Firewall Manager acesse informações sobre as unidades organizacionais (OUs) na organização. Você pode usar UOs para especificar o escopo das políticas do Firewall Manager. Para obter mais informações sobre como definir o escopo da política, consulte a orientação para os tipos de políticas individuais em Criação de uma AWS Firewall Manager política. Para obter mais informações sobre Organizations e contas de gerenciamento, consulte Gerenciando as AWS contas em sua organização.

Configurações necessárias para a conta de gerenciamento da organização

A conta de gerenciamento da organização deve ter as seguintes configurações para integrar a organização ao Firewall Manager e criar um administrador padrão:

- Ele deve ser membro da organização na AWS Organizations qual você deseja aplicar as políticas do Firewall Manager.

Para definir a conta de administrador padrão

1. Faça login no Firewall Manager AWS Management Console usando uma conta AWS Organizations de gerenciamento existente.
2. Abra o console do Firewall Manager em https://console.aws.amazon.com/wafv2/fmsv2.
3. No painel de navegação, selecione Configurações.
4. Digite o AWS ID da conta que você escolheu usar como administrador do Firewall Manager.

> **Note**
>
> O administrador padrão tem escopo administrativo completo. O escopo administrativo completo significa que essa conta pode aplicar políticas a todas as contas e unidades organizacionais (UOs) da organização, realizar ações em todas as regiões e gerenciar todos os tipos de políticas do Firewall Manager.

5. Escolha Criar conta de administrador para criar a conta.

Para obter mais informações sobre como gerenciar uma conta de administrador do Firewall Manager, consulte Trabalhando com AWS Firewall Manager administradores.

Etapa 3: ativar AWS Config

Para usar o Firewall Manager, é necessário habilitar o AWS Config.

> **Note**
>
> Você incorre em cobranças por suas AWS Config configurações, de acordo com os AWS Config preços. Para obter mais informações, consulte Introdução ao AWS Config.

> **Note**
>
> Para que o Firewall Manager monitore a conformidade com as políticas, AWS Config deve registrar continuamente as alterações de configuração dos recursos protegidos. Na sua AWS

Config configuração, a frequência de gravação deve ser definida como Contínua, que é a configuração padrão.

Para habilitar AWS Config o Firewall Manager

1. Ative AWS Config para cada uma de suas contas de AWS Organizations membros, incluindo a conta de administrador do Firewall Manager. Para obter mais informações, consulte Introdução ao AWS Config.
2. Ative AWS Config para cada um Região da AWS que contenha os recursos que você deseja proteger. Você pode ativar AWS Config manualmente ou usar o AWS CloudFormation modelo “Ativar AWS Config” em Modelos AWS CloudFormation StackSets de amostra.

   Se você não quiser habilitar AWS Config para todos os recursos, deverá habilitar o seguinte de acordo com o tipo de política do Firewall Manager que você usa:

   - Política WAF — Ative o Config para os CloudFront tipos de recursos Distribution, Application Load Balancer ElasticLoadBalancing(escolha V2 na lista), API Gateway, WAF WebACL, WAF Regional WebACL e WAFv2 WebACL. AWS Config Para proteger uma CloudFront distribuição, você deve estar na região Leste dos EUA (Norte da Virgínia). Outras regiões não têm CloudFront como opção.
   - Política Shield — Ative o Config para os tipos de recursos Shield Protection, ShieldRegional Protection, Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL e WAFv2 WebACL.
   - Política de grupo de segurança — ative o Config para os tipos de recursos EC2 SecurityGroup, EC2 Instance e EC2. NetworkInterface
   - Política de ACL de rede — Ative o Config para os tipos de recursos Amazon EC2 Subnet e Amazon EC2 Network ACL.
   - Política de Firewall de Rede — Habilite o Config para os tipos de recursos EC2 VPC NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup, EC2, InternetGateway EC2 e EC2 Subnet. RouteTable
   - Política de DNS Firewall: habilite o Config para o tipo de recurso EC2 VPC.
   - Política de firewall de terceiros — Habilite o Config para os tipos de recursos Amazon EC2 VPC, Amazon EC2, Amazon EC2, Amazon InternetGateway EC2 Subnet e Amazon RouteTable EC2 VPCendpoint.

> **Note**
>
> Se você configurar seu AWS Config gravador para usar uma função personalizada do IAM, precisará garantir que a política do IAM tenha as permissões adequadas para registrar os tipos de recursos necessários da política do Firewall Manager. Sem as permissões adequadas, os recursos necessários podem não ser registrados, o que impede o Firewall Manager de proteger adequadamente os seus recursos. O Firewall Manager não tem visibilidade dessas configurações incorretas de permissão. Para obter informações sobre como usar o IAM com AWS Config, consulte IAM for AWS Config.

Etapa 4: para políticas de terceiros, assine o Marketplace AWS e defina as configurações de terceiros

Preencha os pré-requisitos a seguir para começar a usar as políticas de firewall de terceiros do Firewall Manager.

Pré-requisitos da política do Fortigate Cloud Native Firewall (CNF) as a Service

Para usar o Fortigate CNF para Firewall Manager

1. Assine o serviço Fortigate Cloud Native Firewall (CNF) as a Service no Marketplace. AWS
2. Primeiro, registre um locatário no portal de produtos Fortigate CNF. Em seguida, adicione sua conta de administrador do Firewall Manager sob seu locatário no portal do produto Fortigate CNF. Para obter mais informações, consulte a documentação do Fortigate CNF.

Para obter mais informações sobre como trabalhar com políticas Fortigate CNF, consulte Políticas do Fortigate Cloud Native Firewall (CNF) como serviço.

Pré-requisitos da política do Cloud Next Generation Firewall da Palo Alto Networks

Para usar o NGFW na nuvem da Palo Alto Networks para o Firewall Manager

1. Assine o serviço Pay-As-You-Go Pay-As-You-Go do Palo Alto Networks Cloud Next Generation Firewall no Marketplace. AWS

2. Conclua as etapas de implantação do Palo Alto Networks Cloud NGFW listadas no Deploy Palo Alto Networks Cloud NGFW for AWS com o AWS Firewall Manager tópico no guia de implantação do firewall de próxima geração da Palo Alto Networks Cloud. AWS

Para obter mais informações sobre como trabalhar com as políticas do NGFW na nuvem da Palo Alto Networks, consulte Políticas de NGFW na nuvem da Palo Alto Networks.

Etapa 5: Para políticas de Network Firewall e Firewall de DNS, habilite o compartilhamento de recursos

Para gerenciar as políticas de Firewall Manager, Firewall de Rede e Firewall DNS, você deve habilitar o compartilhamento com AWS Organizations in AWS Resource Access Manager. Isso permite que o Firewall Manager implante proteções em suas contas ao criar esses tipos de política.

Para habilitar o compartilhamento com AWS Organizations o AWS Resource Access Manager

- Siga as orientações em Ativar compartilhamento com AWS Organizations no Guia do usuário AWS Resource Access Manager .

Se você tiver problemas com o compartilhamento de recursos, consulte as orientações em Compartilhamento de recursos para políticas de Network Firewall e Firewall DNS.

Etapa 6: Para usar AWS Firewall Manager em regiões que estão desativadas por padrão

Para usar o Firewall Manager em uma região desativada por padrão, você deve habilitar a Região para a conta de gerenciamento da sua AWS organização e para a conta de administrador padrão do Firewall Manager. Para obter informações sobre regiões desativadas por padrão e como habilitá-las, consulte Gerenciar Regiões da AWS na Referência geral AWS .

Para habilitar uma região desabilitada

- Tanto para a conta de gerenciamento de Organizações, quanto para a conta de administrador padrão do Firewall Manager, siga as orientações em Habilitar uma região na Referência geral AWS .

Agora, você pode configurar o Firewall Manager para começar a proteger seus recursos. Para ter mais informações, consulte Introdução às AWS Firewall ManagerAWS WAF políticas.

Trabalhando com AWS Firewall Manager administradores

Com AWS Firewall Manager você pode ter um ou vários administradores que podem gerenciar os recursos de firewall da sua organização. Se quiser usar vários administradores do Firewall Manager 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 a entidade principal do acesso de privilégio mínimo. Por exemplo, você pode fazer com que um administrador gerencie um conjunto de unidades organizacionais (OUs) para sua organização, enquanto delega a outro administrador o gerenciamento somente de tipos específicos de políticas do Firewall Manager. Para obter mais informações sobre Organizations e contas de gerenciamento, consulte Gerenciando as AWS contas em sua organização.

Para saber o número máximo de administradores que você pode ter por organização, consulte AWS Firewall Manager cotas

Conceitos básicos sobre o uso dos administradores do Firewall Manager

Antes de usar os administradores do Firewall Manager, é necessário atender aos pré-requisitos listados em AWS Firewall Manager pré-requisitos. Nos pré-requisitos, você integrará uma organização ao AWS Organizations Firewall Manager e criará uma conta de administrador padrão para o Firewall Manager. Uma conta de administrador padrão tem a capacidade de gerenciar firewalls de terceiros e tem escopo administrativo completo.

Escopo administrativo

O escopo administrativo define os recursos que o administrador do Firewall Manager pode gerenciar. Depois que uma conta AWS Organizations de gerenciamento integra uma organização ao Firewall Manager, a conta de gerenciamento pode criar administradores adicionais do Firewall Manager com diferentes escopos administrativos. Uma conta AWS Organizations de gerenciamento pode conceder ao administrador um escopo administrativo completo ou restrito. O escopo completo dá ao administrador acesso total a todos os tipos de recursos anteriores. O escopo restrito se refere à concessão de permissão administrativa somente a um subconjunto dos recursos anteriores. Recomendamos que você conceda aos administradores somente as permissões necessárias para realizar as tarefas de suas funções. Você pode aplicar qualquer combinação destas condições de escopo administrativo a um administrador:

- Contas ou OUs em sua organização às quais o administrador pode aplicar políticas.
- Regiões nas quais o administrador pode realizar ações.
- Tipos de política do Firewall Manager que o administrador pode gerenciar.

Perfis de administrador

Há dois tipos de funções de administrador no Firewall Manager: um administrador padrão e administradores do Firewall Manager.

- Administrador padrão - a conta de gerenciamento da organização cria uma conta de administrador padrão do Firewall Manager quando eles integram sua organização ao Firewall Manager enquanto concluem os AWS Firewall Manager pré-requisitos. O administrador padrão pode gerenciar firewalls de terceiros e tem escopo administrativo completo, mas, caso contrário, está no mesmo nível de outros administradores, se você optar por ter vários administradores.
- Administradores do Firewall Manager - um administrador do Firewall Manager pode gerenciar os recursos que a conta de gerenciamento do AWS Organizations designa para eles na configuração do escopo administrativo. Para saber o número máximo de administradores que você pode ter por organização, consulte AWS Firewall Manager cotas. Após a criação de uma conta de administrador do Firewall Manager, o serviço verifica se a conta já é um administrador delegado do Firewall Manager na organização. AWS Organizations Caso contrário, o Firewall Manager chama Organizations para definir a conta como administrador delegado do Firewall Manager. Para obter mais informações, consulte Terminologia e conceitos de Organizations da AWS Organizations no Guia do usuário do AWS Organizations .

Administradores existentes

Se você já é um cliente do Firewall Manager e já definiu um administrador, esse administrador existente será o administrador padrão do Firewall Manager. Não deve haver impactos em seu fluxo existente. Se desejar adicionar mais administradores, você pode fazer isso seguindo os procedimentos deste capítulo.

Criação, atualização e revogação de contas de administrador do Firewall Manager

Os procedimentos nos tópicos a seguir explicam como criar, atualizar e revogar contas de administrador do Firewall Manager. Somente a conta de gerenciamento de uma organização pode

criar e atualizar contas de administrador do Firewall Manager. Somente um administrador individual do Firewall Manager pode revogar sua própria conta de administrador.

Criando a conta de administrador do Firewall Manager

O procedimento a seguir descreve como criar contas de administrador do Firewall Manager usando o console do Firewall Manager.

Para criar a conta de administrador do Firewall Manager

1. Faça login no Firewall Manager AWS Management Console usando uma conta AWS Organizations de gerenciamento existente.
2. Abra o console do Firewall Manager em https://console.aws.amazon.com/wafv2/fmsv2.
3. No painel de navegação, selecione Configurações.
4. Escolha Criar conta de administrador.
5. No painel Detalhes, em ID da conta AWS , digite o AWS ID de uma conta-membro que você gostaria de adicionar como administrador do Firewall Manager.
6. Para Escopo administrativo, selecione uma das seguintes opções:

   - Completo: concede ao administrador a capacidade de aplicar políticas a todas as contas e unidades organizacionais (OUs) da organização, realizar ações em todas as regiões e aplicar todos os tipos de políticas do Firewall Manager, exceto firewalls de terceiros. Somente o administrador padrão pode criar e gerenciar firewalls de terceiros. Tenha cuidado ao conceder esse nível de permissões ao administrador. Considerando o privilégio mínimo, recomendamos conceder ao administrador apenas as permissões necessárias para realizar as tarefas de sua função.
   - Restrito: se estiver aplicando um escopo restrito, em Configurar o escopo administrativo, configure as contas e as unidades organizacionais, as regiões e os tipos de políticas que a conta pode gerenciar.

     Para Contas e unidades organizacionais, escolha as seguintes opções:

     - Se você quiser aplicar políticas a todas as contas ou unidades organizacionais em sua organização, escolha Incluir todas as contas em minha AWS organização.
     - Se você quiser aplicar políticas somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas

na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

- Se você quiser aplicar políticas a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

Em Regiões, escolha uma das seguintes opções:

- Se você quiser permitir que o administrador execute ações em todas as regiões disponíveis, escolha Incluir todas as regiões.
- Se você quiser que o administrador execute ações somente em regiões específicas, escolha Incluir somente as regiões especificadas e, em seguida, especifique as regiões que deseja incluir.

> **Note**
>
> Para incluir uma região que está desativada por padrão, você deve habilitar a região tanto para a conta de gerenciamento AWS Organizations da organização quanto para a conta de administração padrão. Para obter informações sobre como habilitar regiões para uma conta, consulte Habilitar uma região no Referência geral da Amazon Web Services.

Para Tipos de política, escolha as opções da seguinte forma:.

- Se você quiser permitir que o administrador gerencie todos os tipos de política, escolha Incluir todos os tipos de política.
- Se você quiser que o administrador gerencie somente tipos de política específicos, escolha Incluir somente os tipos de política especificados e, em seguida, especifique os tipos de política que você deseja incluir.

7. Escolha Criar conta de administrador para criar a conta de administrador. Após a criação, o Firewall Manager liga AWS Organizations para ver se o administrador já é um administrador delegado da sua organização. Caso contrário, o Firewall Manager designará a conta como administrador delegado. Para obter mais informações sobre administradores delegados em Organizations, consulte Terminologia e conceitos de AWS Organizations no Guia do usuário do AWS Organizations .

Se você aplicar o escopo administrativo restrito, o Firewall Manager avaliará automaticamente quaisquer novos recursos em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente o escopo administrativo à nova conta.

Criando a conta de administrador do Firewall Manager

O procedimento a seguir descreve como atualizar uma conta de administrador do Firewall Manager usando o console do Firewall Manager.

> **Note**
>
> Para atualizar o escopo de um administrador para incluir uma região desativada por padrão, você deve habilitar a região tanto para a conta de gerenciamento AWS Organizations da organização quanto para a conta de administração padrão. Para obter informações sobre como habilitar regiões para uma conta, consulte Habilitar uma região no Referência geral da Amazon Web Services.

Para atualizar uma conta de administrador (console)

1. Faça login no Firewall Manager AWS Management Console usando uma conta AWS Organizations de gerenciamento existente.
2. Abra o console do Firewall Manager em https://console.aws.amazon.com/wafv2/fmsv2.
3. No painel de navegação, selecione Configurações.
4. na tabela de administradores do Firewall Manager, escolha a conta que você gostaria de atualizar.
5. Selecione Editar para alterar os detalhes da conta de administrador. Não é possível alterar o ID da conta.
6. Escolha Salvar para salvar as alterações.

Como revogar uma conta de administrador

O procedimento a seguir descreve como revogar uma conta de administrador do Firewall Manager. Se você for o administrador padrão, antes de poder revogar sua conta, todas as contas de

administrador do Firewall Manager em sua organização devem primeiro revogar suas próprias contas. Para revogar uma conta de administrador, siga o procedimento abaixo

Para revogar uma conta de administrador (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.
2. No painel de navegação, selecione Configurações.
3. No painel Conta de administrador, selecione Revogar conta de administrador para revogar sua conta.

> **Important**
>
> Quando você revogar os privilégios de administrador da conta do administrador atual, todas as políticas do Firewall Manager criadas por essa conta serão excluídas.

Como alterar a conta de administrador padrão

Você só pode designar uma conta em cada organização como a conta de administrador padrão do Firewall Manager. A conta de administrador padrão segue o princípio de primeiro a entrar, último a sair. Para designar uma conta de administrador padrão diferente, cada conta de administrador individual deve primeiro revogar sua própria conta. Em seguida, o administrador padrão existente pode revogar sua própria conta, o que também retirará a organização do Firewall Manager. Quando um administrador revoga sua conta, todas as políticas do Firewall Manager criadas por essa conta serão excluídas. Para designar uma nova conta de administrador padrão, você deve entrar no Firewall Manager com a conta AWS Organizations de gerenciamento para designar uma nova conta de administrador. Para alterar a conta de administrador padrão para uma organização, execute o procedimento a seguir.

A conta de administrador é escolhida por padrão

1. Faça login no Firewall Manager AWS Management Console usando uma conta AWS Organizations de gerenciamento existente.
2. Abra o console do Firewall Manager em https://console.aws.amazon.com/wafv2/fmsv2.

3. No painel de navegação, selecione Configurações.
4. Digite o ID da conta que você escolheu usar como administrador do Firewall Manager.

> **Note**
>
> A conta recebe a permissão para criar e gerenciar as políticas do Firewall Manager em todas as contas da organização.

5. Escolha Criar conta de administrador.
6. Digite o AWS ID da conta que você escolheu usar como administrador do Firewall Manager.

> **Note**
>
> Essa conta tem escopo administrativo completo. O escopo administrativo completo significa que essa conta pode aplicar políticas a todas as contas e unidades organizacionais (UOs) da organização, realizar ações em todas as regiões e gerenciar todos os tipos de políticas do Firewall Manager.

7. Escolha Criar conta de administrador para criar a conta de administrador padrão.

Desqualificando alterações em uma conta de administrador

Algumas alterações em uma conta de administrador podem desqualificá-la de continuar sendo uma conta de administrador.

Esta seção descreve as alterações que podem desqualificar a conta de administrador AWS e como o Firewall Manager lidam com essas alterações.

Conta removida da organização em AWS Organizations

Se a conta do AWS Firewall Manager administrador for removida da organização em AWS Organizations, ela não poderá mais administrar políticas para a organização. O Firewall Manager executa uma das seguintes ações:

- Conta sem políticas: se a conta de administrador do Firewall Manager não tiver políticas do Firewall Manager, o Firewall Manager revogará a conta de administrador.
- Conta com políticas do Firewall Manager — Se a conta do administrador do Firewall Manager tiver políticas do Firewall Manager, o Firewall Manager enviará um e-mail para informá-lo sobre a

situação e fornecer opções que você pode escolher, com a ajuda de seu representante de AWS vendas.

Conta fechada

Se você fechar a conta que está usando para o AWS Firewall Manager administrador, AWS o Firewall Manager lidará com o encerramento da seguinte maneira:

- AWS revoga o acesso do administrador da conta a partir do Firewall Manager e o Firewall Manager desativa todas as políticas que foram gerenciadas pela conta do administrador. As proteções fornecidas por essas políticas são interrompidas em toda a organização.
- AWS retém os dados da política do Firewall Manager da conta por 90 dias a partir da data efetiva do encerramento da conta do administrador. Durante esse período de 90 dias, você pode reabrir a conta fechada.
  - Se você reabrir a conta fechada durante o período de 90 dias, AWS reatribuirá a conta como administradora do Firewall Manager e recuperará os dados da política do Firewall Manager da conta.
  - Caso contrário, ao final do período de 90 dias, excluirá AWS permanentemente todos os dados da política do Firewall Manager da conta.

Introdução às AWS Firewall Manager políticas

Você pode usar AWS Firewall Manager para habilitar vários tipos diferentes de políticas de segurança. As etapas de configuração são um pouco diferentes para cada um.

Tópicos

Introdução às AWS Firewall ManagerAWS WAF políticas

Para usar AWS Firewall Manager para habilitar AWS WAF regras em sua organização, execute as etapas a seguir em sequência.

Tópicos

Etapa 1: Concluir os pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para Etapa 2: criar e aplicar uma AWS WAF política.

Etapa 2: criar e aplicar uma AWS WAF política

Uma AWS WAF política do Firewall Manager contém os grupos de regras que você deseja aplicar aos seus recursos. O Firewall Manager cria uma web ACL do Firewall Manager em cada conta em que você aplica a política. Os gerentes de contas individuais podem adicionar regras e grupos de regras à web ACL resultante, além dos grupos de regras definidos aqui. Para obter informações sobre AWS WAF as políticas do Firewall Manager, consulteAWS WAF políticas.

Para criar uma AWS WAF política do Firewall Manager (console)

Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

1. No painel de navegação, escolha Políticas de segurança.
2. Escolha Criar política.
3. Em Tipo de política, escolha AWS WAF.
4. Para Região, escolha um Região da AWS. Para proteger as CloudFront distribuições da Amazon, escolha Global.

Para proteger recursos em várias regiões (exceto CloudFront distribuições), você deve criar políticas separadas do Firewall Manager para cada região.

5. Escolha Próximo.
6. Em Nome da política, insira um nome descritivo. O Firewall Manager inclui o nome da política nos nomes das web ACLs que ele gerencia. Os nomes da web ACL têm `FMManagedWebACLV2-` seguido do nome da política que você insere aqui, `-`, e do timestamp da criação da web ACL, em milissegundos UTC. Por exemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

   > **Important**
   >
   > Os nomes da web ACL não podem mudar depois da criação. Se você atualizar o nome da sua política, o Firewall Manager não atualizará o nome da web ACL associada. Para que o Firewall Manager crie uma web ACL com um nome diferente, crie uma nova política.

7. Em Regras de política, em Primeiros grupos de regras, escolha Adicionar grupos de regras. Expanda os grupos de regras gerenciadas da AWS . Em Conjunto de regras principais, alterne Adicionar à web ACL. Em AWS Entradas inválidas conhecidas da , alterne Adicionar à web ACL. Escolha Adicionar regras.

   Em Últimos grupos de regras, escolha Adicionar grupos de regras. Expanda os grupos de regras gerenciados da AWS e, para a Lista de reputação de IP da Amazon, alterne Adicionar à web ACL. Escolha Adicionar regras.

   Em Primeiros grupos de regras, selecione Conjunto de regras principais e escolha Mover para baixo. AWS WAF avalia as solicitações da Web em relação ao grupo de regras de entradas inválidas AWS conhecido antes de fazer a avaliação em relação ao conjunto de regras principais.

   Você também pode criar seus próprios grupos de AWS WAF regras, se quiser, usando o AWS WAF console. Quaisquer grupos de regras criados aparecem em Seus grupos de regras na página Descrever política: Adicionar grupos de regras.

   O primeiro e o último grupos de AWS WAF regras que você gerencia por meio do Firewall Manager têm nomes que começam com `PREFMManaged-` ou`POSTFMManaged-`, respectivamente, seguidos pelo nome da política do Firewall Manager e pelo timestamp

de criação do grupo de regras, em milissegundos UTC. Por exemplo, `PREFMManaged-MyWAFPolicyName-1621880555123`.

8. Deixe a ação padrão para a web ACL em Permitir.
9. Deixe a Ação de política como padrão, para não corrigir automaticamente recursos não compatíveis. É possível alterar a opção mais tarde.
10. Escolha Próximo.
11. Em Escopo de política, forneça as configurações para as contas, os tipos de recursos e a marcação que identificam os recursos aos quais deseja aplicar a política. Para este tutorial, mantenha as configurações das Contas da AWS e Recursos e escolha um ou mais tipos de recursos.
12. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
13. Escolha Próximo.
14. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
15. Escolha Próximo.
16. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
17. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente

for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Etapa 3: limpeza

Para evitar cobranças estranhas, exclua políticas e recursos desnecessários.

Para excluir uma política (console)

1. Na página Políticas do Firewall Manager do AWS Firewall Manager , escolha o botão de opção ao lado do nome da política e selecione Excluir.
2. Na caixa de confirmação Excluir, selecione Excluir todos os recursos de política e escolha Excluir novamente.

   AWS WAF remove a política e todos os recursos associados, como ACLs da web, que ela criou em sua conta. As alterações podem levar alguns minutos para serem propagadas em todas as contas.

Introdução às AWS Firewall ManagerAWS Shield Advanced políticas

Você pode usar AWS Firewall Manager para habilitar AWS Shield Advanced proteções em toda a sua organização.

> **Important**
>
> O Firewall Manager não é compatível com o Amazon Route 53 ou AWS Global Accelerator. Se você precisar proteger esses recursos com o Shield Advanced, não poderá usar uma política do Firewall Manager. Em vez disso, siga as instruções em Adicionando AWS Shield Advanced proteção aos AWS recursos.

Para usar o Firewall Manager para habilitar a proteção do Shield Advanced, execute as seguintes etapas em sequência.

Tópicos

- Etapa 1: Concluir os pré-requisitos

- Etapa 2: Criar e aplicar uma política do Shield Advanced
- Etapa 3: (Opcional) Autorizar a equipe de resposta o Shield Response Team (SRT)
- Etapa 4: Configurar notificações e alarmes do Amazon SNS CloudWatch

Etapa 1: Concluir os pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para Etapa 2: Criar e aplicar uma política do Shield Advanced.

Etapa 2: Criar e aplicar uma política do Shield Advanced

Depois de concluir os pré-requisitos, você cria uma política AWS Firewall Manager Shield Advanced. Uma política do Firewall Manager Shield Advanced contém as contas e os recursos que você deseja proteger com o Shield Advanced.

> **Important**
>
> O Firewall Manager não é compatível com o Amazon Route 53 ou AWS Global Accelerator. Se você precisar proteger esses recursos com o Shield Advanced, não poderá usar uma política do Firewall Manager. Em vez disso, siga as instruções em Adicionando AWS Shield Advanced proteção aos AWS recursos.

Criar uma política do Firewall Manager para Shield Advanced (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.

3. Escolha Criar política.
4. Em Tipo de política, escolha Shield Advanced.

   Para criar uma política do Shield Advanced, sua conta de administrador do Firewall Manager deve ser assinante do Shield Advanced. Se você não estiver inscrito, será solicitado a fazê-lo. Para obter mais informações sobre o custo, consulte Definição de preço do AWS Shield Advanced.

   > **Note**
   >
   > Não é necessário inscrever manualmente cada conta de membro no Shield Advanced. O Firewall Manager faz isso por você quando cria a política. Cada conta deve permanecer inscrita no Firewall Manager e no Shield Advanced para continuar protegendo recursos na conta.

5. Para Região, escolha um Região da AWS. Para proteger os CloudFront recursos da Amazon, escolha Global.

   Para proteger recursos em várias regiões (exceto CloudFront recursos), você deve criar políticas separadas do Firewall Manager para cada região.
6. Escolha Próximo.
7. Em Nome, insira um nome descritivo.
8. (Somente região global) Para políticas da região global, você pode escolher se deseja gerenciar a mitigação automática de DDoS da camada de aplicativo do Shield Advanced. Para este tutorial, deixe essa opção na configuração padrão de Ignorar.
9. Em Ação de política, escolha a opção que não corrige automaticamente.
10. Escolha Próximo.
11. Contas da AWS essa política se aplica para permitir que você restrinja o escopo de sua política especificando contas a serem incluídas ou excluídas. Neste tutorial, selecione Incluir todas as contas na minha organização.
12. Escolha os tipos de recurso que você deseja proteger.

    O Firewall Manager não é compatível com o Amazon Route 53 ou AWS Global Accelerator. Se você precisar proteger esses recursos com o Shield Advanced, não poderá usar uma política do Firewall Manager. Em vez disso, siga as orientações do Shield Advanced em Adicionando AWS Shield Advanced proteção aos AWS recursos.

13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
14. Escolha Próximo.
15. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
16. Escolha Próximo.
17. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
18. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Avance para Etapa 3: (Opcional) Autorizar a equipe de resposta o Shield Response Team (SRT).

Etapa 3: (Opcional) Autorizar a equipe de resposta o Shield Response Team (SRT)

Um dos benefícios AWS Shield Advanced é o suporte da Shield Response Team (SRT). Se ocorrer um ataque DDoS, você pode entrar em contato com a Central AWS Support. Se necessário, o Atendimento ao Cliente escalará seu problema para a SRT. A SRT ajuda você a analisar as

atividades suspeitas e auxilia na atenuação do problema. Essa mitigação geralmente envolve a criação ou atualização de AWS WAF regras e ACLs da web em sua conta. O SRT pode inspecionar sua AWS WAF configuração e criar ou atualizar AWS WAF regras e ACLs da web para você, mas a equipe precisa de sua autorização para fazer isso. Recomendamos que, como parte da configuração AWS Shield Advanced, você forneça proativamente ao SRT a autorização necessária. Fornecer a autorização antecipadamente ajuda a evitar atrasos na atenuação no caso de um ataque real.

Você autoriza e entra em contato com o SRT no nível de conta. Ou seja, o proprietário da conta, não o administrador do Firewall Manager, deve executar as seguintes etapas para autorizar a SRT a atenuar ataques em potencial. O administrador do Firewall Manager poderá autorizar a SRT apenas para contas pertencentes a ele. Da mesma forma, somente o proprietário da conta pode entrar em contato com a SRT para obter suporte.

> **Note**
>
> Para usar os serviços da SRT, você deve ser assinante do plano Business Support ou Enterprise Support.

Para autorizar a SRT a atenuar ataques em potencial em seu nome, siga as instruções em Suporte do Shield Response Team (SRT). Você pode alterar o acesso e as permissões da SRT a qualquer momento usando as mesmas etapas.

Avance para Etapa 4: Configurar notificações e alarmes do Amazon SNS CloudWatch .

Etapa 4: Configurar notificações e alarmes do Amazon SNS CloudWatch

Você pode continuar a partir dessa etapa sem configurar notificações CloudWatch ou alarmes do Amazon SNS. No entanto, a configuração desses alarmes e notificações aumenta significativamente sua visibilidade sobre possíveis eventos de DDoS.

Você pode monitorar seus recursos protegidos quanto a possíveis atividades de DDoS usando o Amazon SNS. Para receber notificação de possíveis ataques, crie um tópico do Amazon SNS para cada região.

Para criar um tópico do Amazon SNS no Firewall Manager (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, em AWS FMS, selecione Configurações.
3. Selecione Create new topic (Criar novo tópico).
4. Insira o nome do tópico.
5. Insira um endereço de e-mail de destino para as mensagens do Amazon SNS e, em seguida, escolha Adicionar endereço de e-mail.
6. Selecione Update SNS configuration (Atualizar configuração do SNS).

Configurar CloudWatch alarmes da Amazon

O Shield Advanced registra as métricas de detecção, mitigação e principais colaboradores CloudWatch que você pode monitorar. Para obter mais informações, consulteAWS Shield Advanced métricas. CloudWatch incorre em custos adicionais. Para obter CloudWatch os preços, consulte Amazon CloudWatch Pricing.

Para criar um CloudWatch alarme, siga as instruções em Usando CloudWatch alarmes da Amazon. Por padrão, o Shield Advanced é configurado CloudWatch para alertá-lo após apenas um indicador de um possível evento de DDoS. Se necessário, você pode usar o CloudWatch console para alterar essa configuração e alertá-lo somente após a detecção de vários indicadores.

> **Note**
>
> Além dos alarmes, você também pode usar um CloudWatch painel para monitorar possíveis atividades de DDoS. O painel coleta e processa dados brutos do Shield Advanced como métricas legíveis, quase em tempo real. Você pode usar estatísticas na Amazon CloudWatch para ter uma perspectiva sobre o desempenho do seu aplicativo ou serviço web. Para obter mais informações, consulte O que está CloudWatch no Guia CloudWatch do usuário da Amazon.

Para obter instruções sobre como criar um CloudWatch painel, consulteMonitoramento com a Amazon CloudWatch. Para obter informações sobre as métricas específicas do Shield Advanced que você pode adicionar ao seu painel, consulte AWS Shield Advanced métricas.

Depois de concluir a configuração do Shield Advanced, familiarize-se com suas opções para visualizar eventos em Visibilidade de eventos de DDoS.

Introdução às políticas de grupos de segurança AWS Firewall Manager da Amazon VPC

Para usar AWS Firewall Manager para habilitar grupos de segurança da Amazon VPC em toda a sua organização, execute as seguintes etapas em sequência.

Tópicos

- Etapa 1: Concluir os pré-requisitos
- Etapa 2: Criar um grupo de segurança a ser usado na política
- Etapa 3: Criar e aplicar uma política de grupo de segurança comum

Etapa 1: Concluir os pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para Etapa 2: Criar um grupo de segurança a ser usado na política.

Etapa 2: Criar um grupo de segurança a ser usado na política

Nesta etapa, crie um grupo de segurança que pode ser aplicado em toda a organização usando o Firewall Manager.

> **Note**
>
> Neste tutorial, você não aplicará a política do grupo de segurança aos recursos da organização. Você só criará a política e verá o que aconteceria se aplicasse o grupo de segurança da política aos recursos. É possível fazer isso desabilitando a correção automática na política.

Se você já tiver um grupo de segurança geral definido, ignore esta etapa e vá para Etapa 3: Criar e aplicar uma política de grupo de segurança comum.

Criar um grupo de segurança para usar em uma política de grupo de segurança comum do Firewall Manager

- Criar um grupo de segurança que possa ser aplicado a todas as contas e recursos na organização, seguindo as orientações em Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

  Para obter informações sobre as opções de regras de grupo de segurança, consulte Referência de regras de grupo de segurança.

Você está pronto para ir para Etapa 3: Criar e aplicar uma política de grupo de segurança comum.

Etapa 3: Criar e aplicar uma política de grupo de segurança comum

Depois de concluir os pré-requisitos, você cria uma política de grupo de segurança AWS Firewall Manager comum. Uma política de grupo de segurança comum fornece um grupo de segurança controlado centralmente para toda a AWS organização. Ele também define os recursos Contas da AWS e aos quais o grupo de segurança se aplica. Além das políticas comuns de grupo de segurança, o Firewall Manager oferece suporte às políticas de grupo de segurança de auditoria de conteúdo, a fim de gerenciar as regras de grupo de segurança em uso na organização, e às políticas de grupo de segurança de auditoria de uso, a fim de gerenciar grupos de segurança não utilizados e redundantes. Para ter mais informações, consulte Políticas de grupo de segurança.

Neste tutorial, crie uma política de grupo de segurança comum e defina sua ação para não corrigir automaticamente. Isso permite que você veja qual efeito a política teria sem fazer alterações em sua AWS organização.

Para criar uma política comum de grupo de segurança do Firewall Manager (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Se você não atender aos pré-requisitos, o console exibirá instruções sobre como corrigir os problemas. Siga as instruções e volte a esta etapa para criar uma política de grupo de segurança comum.
4. Escolha Criar política.
5. Em Tipo de política, escolha Grupo de segurança.
6. Em Tipo de política de grupo de segurança, escolha Grupos de segurança comuns.
7. Para Região, escolha um Região da AWS.
8. Escolha Próximo.
9. Em Nome da política, insira um nome descritivo.
10. Em Regras da política é possível escolher como os grupos de segurança dessa política são aplicados e mantidos. Para este tutorial, deixe as opções desmarcadas.
11. Selecione Adicionar grupo de segurança primário, escolha o grupo de segurança criado neste tutorial e selecione Adicionar grupo de segurança.
12. Em Ação da política, selecione Identificar recursos que não estejam em conformidade com as regras da política, mas não corrigir automaticamente.
13. Escolha Próximo.
14. Contas da AWS afetado por essa política permite que você restrinja o escopo de sua política especificando contas a serem incluídas ou excluídas. Neste tutorial, selecione Incluir todas as contas na minha organização.
15. Em Tipo de recurso, escolha um ou mais tipos, de acordo com os recursos que você definiu para sua AWS organização.
16. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

17. Escolha Próximo.
18. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
19. Escolha Próximo.
20. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
21. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política
22. Quando terminar de explorar, se não quiser manter a política criada para este tutorial, escolha o nome da política, selecione Excluir, Limpar recursos criados por esta política e, por fim, selecione Excluir.

Para obter mais informações sobre as políticas de grupo de segurança do Firewall Manager, consulte Políticas de grupo de segurança.

Introdução às políticas de ACL da rede AWS Firewall Manager Amazon VPC

Para usar AWS Firewall Manager para habilitar ACLs de rede em sua organização, execute as etapas desta seção em sequência.

Para obter informações sobre ACLs de rede, consulte Controle o tráfego para sub-redes usando ACLs de rede no Guia do usuário da Amazon VPC.

Tópicos

Etapa 1: Concluir os pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para Etapa 2: criar uma política de ACL de rede.

Etapa 2: criar uma política de ACL de rede

Depois de concluir os pré-requisitos, você cria uma política de ACL de rede do Firewall Manager. Uma política de ACL de rede fornece uma definição de ACL de rede controlada centralmente para toda a organização. AWS Ele também define as sub-redes Contas da AWS e às quais a rede ACL se aplica.

Para obter informações sobre as políticas de ACL de rede do Firewall Manager, consultePolíticas de ACL de rede.

Para obter informações gerais sobre as políticas de ACL de rede do Firewall Manager, consultePolíticas de ACL de rede.

> **Note**
>
> Neste tutorial, você não aplicará sua política de ACL de rede às sub-redes da sua organização. Você apenas criará a política e verá o que aconteceria se aplicasse a ACL de rede da política às suas sub-redes. É possível fazer isso desabilitando a correção automática na política.

Para criar uma política de ACL de rede do Firewall Manager (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Se você não atender aos pré-requisitos, o console exibirá instruções sobre como corrigir os problemas. Siga as instruções e, em seguida, retorne a essa etapa para criar uma política de ACL de rede.
4. Escolha Criar política.
5. Para Região, escolha um Região da AWS.
6. Em Tipo de política, escolha Network ACL.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. Para regras de política de ACL de rede, defina a primeira e a última regras para tráfego de entrada e saída.

   Você define regras de ACL de rede no Firewall Manager da mesma forma que você as define por meio da Amazon VPC. A única diferença é que, em vez de atribuir você mesmo os números das regras, você atribui a ordem para executar cada conjunto de regras e, em seguida, o Firewall Manager atribui os números para você quando você salva a política. Você pode definir até 5 regras de entrada, divididas de qualquer forma entre a primeira e a última, e você pode definir até 5 regras de saída.

   Para obter orientação sobre como especificar regras de ACL de rede, consulte Adicionar e excluir regras de ACL de rede no Guia do usuário da Amazon VPC.

   As regras que você define na política do Firewall Manager especificam a configuração mínima de regras que uma ACL de rede deve ter para estar em conformidade com a política de ACL de rede. Por exemplo, as regras de entrada de uma ACL de rede não podem estar em conformidade com a política, a menos que comecem como as primeiras regras de entrada da política, na mesma ordem em que são especificadas na política. Para ter mais informações, consulte Políticas de ACL de rede.

10. Em Ação da política, selecione Identificar recursos que não estejam em conformidade com as regras da política, mas não corrigir automaticamente.
11. Escolha Próximo.
12. Contas da AWS afetado por essa política permite que você restrinja o escopo de sua política especificando contas a serem incluídas ou excluídas. Neste tutorial, selecione Incluir todas as contas na minha organização.

    O tipo de recurso para uma política de ACL de rede é sempre sub-rede.
13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
14. Escolha Próximo.
15. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
16. Escolha Próximo.
17. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
18. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

19. Quando terminar de explorar, se não quiser manter a política criada para este tutorial, escolha o nome da política, selecione Excluir, Limpar recursos criados por esta política e, por fim, selecione Excluir.

Para obter mais informações sobre as políticas de ACL de rede do Firewall Manager, consulte Políticas de ACL de rede.

Introdução às AWS Firewall ManagerAWS Network Firewall políticas

Para usar AWS Firewall Manager para habilitar um firewall de Firewall de AWS Rede em sua organização, execute as etapas a seguir em sequência. Para obter informações sobre as políticas do Network Firewall do Firewall Manager, consulte AWS Network Firewall políticas.

Tópicos

- Etapa 1: conclua os pré-requisitos gerais
- Etapa 2: crie um grupo de regras do Network Firewall para usar em sua política
- Etapa 3: Criar e aplicar uma política do Network Firewall

Etapa 1: conclua os pré-requisitos gerais

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 2: crie um grupo de regras do Network Firewall para usar em sua política

Para seguir este tutorial, você deve estar familiarizado AWS Network Firewall e saber como configurar seus grupos de regras e políticas de firewall.

Você deve ter pelo menos um grupo de regras no Network Firewall que será usado em sua política do AWS Firewall Manager . Se você ainda não criou um grupo de regras no Network Firewall, faça isso agora. Para obter mais informações sobre o uso do Network Firewall, consulte o Guia do desenvolvedor do AWS Network Firewall.

Etapa 3: Criar e aplicar uma política do Network Firewall

Depois de concluir os pré-requisitos, você cria uma política do AWS Firewall Manager Network Firewall. Uma política de Firewall de Rede fornece um AWS Network Firewall firewall controlado

centralmente para toda a AWS organização. Ele também define os recursos Contas da AWS e aos quais o firewall se aplica.

Para obter informações sobre como o Firewall Manager lida com as políticas do Network Firewall, consulte AWS Network Firewall políticas.

Criar uma política do Network Firewall no Firewall Manager (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Se você não atender aos pré-requisitos, o console exibirá instruções sobre como corrigir os problemas. Siga as instruções e volte a esta etapa para criar uma política do Network Firewall.
4. Escolha Criar política de segurança.
5. Em Tipo de política, escolha AWS Network Firewall.
6. Para Região, escolha um Região da AWS.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. A configuração da política permite que você defina a política de firewall. Esse é o mesmo processo que você usa no AWS Network Firewall console. Você adiciona os grupos de regras que deseja usar em sua política e fornece as ações sem estado padrão. Neste tutorial, configure essa política como você faria com uma política de firewall no Network Firewall.

   > **Note**
   >
   > A correção automática acontece automaticamente para as políticas de Firewall de AWS Firewall Manager Rede, então você não verá a opção de optar por não corrigir automaticamente aqui.

10. Escolha Próximo.
11. Para Endpoints de firewall, escolha Vários endpoints de firewall. Essa opção fornece alta disponibilidade para seu firewall. Quando você cria a política, o Firewall Manager cria uma sub-rede de firewall em cada zona de disponibilidade em que você tem sub-redes públicas para proteger.
12. Para Configuração de rotas do AWS Network Firewall , escolha Monitorar para que o Firewall Manager monitore suas VPCs em busca de violações de configuração de rotas e alerte com sugestões de correção para ajudá-lo a colocar as rotas em conformidade. Opcionalmente, se você não quiser que suas configurações de rota sejam monitoradas pelo Firewall Manager e nem receber esses alertas, escolha Desativado.

    > **Note**
    >
    > O monitoramento fornece detalhes sobre recursos não compatíveis devido à configuração incorreta da rota e sugere ações de correção da API do Firewall Manager. `GetViolationDetails` Por exemplo, o Network Firewall alerta se o tráfego não for roteado pelos endpoints de firewall criados pela sua política.

    > **Warning**
    >
    > Se você escolher Monitorar, não poderá alterá-lo para Desativado no futuro para a mesma política. É necessário criar uma nova política.

13. Em Tipo de tráfego, selecione Adicionar à política de firewall para rotear o tráfego pelo gateway da Internet.
14. Contas da AWS afetado por essa política permite que você restrinja o escopo de sua política especificando contas a serem incluídas ou excluídas. Neste tutorial, selecione Incluir todas as contas na minha organização.

    O Tipo de recurso para uma política do Firewall DNS é sempre VPC.
15. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

16. Escolha Próximo.
17. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
18. Escolha Próximo.
19. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
20. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política
21. Quando terminar de explorar, se não quiser manter a política criada para este tutorial, escolha o nome da política, selecione Excluir, Limpar recursos criados por esta política e, por fim, selecione Excluir.

Para obter mais informações sobre as políticas do Network Firewall do Firewall Manager, consulte AWS Network Firewall políticas.

Introdução às políticas de firewall de AWS Firewall Manager DNS

Para usar AWS Firewall Manager para habilitar o Amazon Route 53 Resolver DNS Firewall em toda a sua organização, execute as seguintes etapas em sequência. Para obter informações sobre as políticas de Firewall DNS do Firewall Manager, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.

Tópicos

Etapa 1: conclua os pré-requisitos gerais

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 2: crie seus grupos de regras do DNS Firewall para usar em sua política

Para seguir esse tutorial, você deve estar familiarizado com o DNS Firewall do Amazon Route 53 Resolver e saber como configurar seus grupos de regras.

Você deve ter pelo menos um grupo de regras no DNS Firewall que será usado em sua política do AWS Firewall Manager . Se você ainda não criou um grupo de regras no DNS Firewall, faça isso agora. Para obter mais informações sobre o Firewall DNS, consulte Firewall DNS do Amazon Route 53 Resolver, no Guia do Desenvolvedor do Amazon Route 53.

Etapa 3: Crie e aplique uma política do DNS Firewall

Depois de concluir os pré-requisitos, você cria uma política de firewall de AWS Firewall Manager DNS. Uma política de firewall de DNS fornece um conjunto de associações de grupos de regras de firewall de DNS controladas centralmente para toda a organização. AWS Ela também define as Contas da AWS e os recursos aos quais o firewall se aplica.

Para obter mais informações sobre como o Firewall Manager gerencia suas associações de grupos de regras do Firewall DNS, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.

Criar uma política de Firewall DNS do Firewall Manager (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.
2. No painel de navegação, escolha Políticas de segurança.

3. Se você não atender aos pré-requisitos, o console exibirá instruções sobre como corrigir os problemas. Siga as instruções e volte a esta etapa para criar uma política de DNS Firewall.
4. Escolha Criar política de segurança.
5. Em Tipo de política, escolha DNS Firewall do Amazon Route 53 Resolver.
6. Para Região, escolha um Região da AWS.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. A configuração da política permite que você defina as associações de grupos de regras do DNS Firewall que você deseja gerenciar a partir do Firewall Manager. Você adiciona os grupos de regras que deseja usar em sua política. Você pode definir uma associação para avaliar primeiro para suas VPCs e outra para avaliar por último. Para este tutorial, adicione uma ou duas associações de grupos de regras, dependendo de suas necessidades.
10. Escolha Próximo.
11. Contas da AWS afetado por essa política permite que você restrinja o escopo de sua política especificando contas a serem incluídas ou excluídas. Neste tutorial, selecione Incluir todas as contas na minha organização.

    O tipo de recurso para uma política do Firewall DNS é sempre VPC.
12. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
13. Escolha Próximo.
14. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
15. Escolha Próximo.
16. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.

17. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

18. Quando terminar de explorar, se não quiser manter a política criada para este tutorial, escolha o nome da política, selecione Excluir, Limpar recursos criados por esta política e, por fim, selecione Excluir.

Para obter informações sobre as políticas do DNS Firewall do Firewall Manager, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.

Introdução às políticas de firewall de próxima geração da AWS Firewall Manager Palo Alto Networks Cloud

Para usar AWS Firewall Manager para habilitar as políticas do Cloud Next Generation Firewall (NGFW) da Palo Alto Networks, execute as seguintes etapas em sequência. Para obter informações sobre as políticas do Cloud NGFW da Palo Alto Networks, consulte Políticas de NGFW na nuvem da Palo Alto Networks.

Tópicos

- Etapa 1: conclua os pré-requisitos gerais
- Etapa 2: preencher os pré-requisitos da política do Cloud NGFW da Palo Alto Networks
- Etapa 3: criar e aplicar uma política do Cloud NGFW da Palo Alto Networks

Etapa 1: conclua os pré-requisitos gerais

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 2: preencher os pré-requisitos da política do Cloud NGFW da Palo Alto Networks

Há algumas etapas obrigatórias adicionais que você deve concluir para usar as políticas do Cloud NGFW da Palo Alto Networks. Essas etapas estão descritas em Pré-requisitos da política do Cloud Next Generation Firewall da Palo Alto Networks. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 3: criar e aplicar uma política do Cloud NGFW da Palo Alto Networks

Depois de concluir os pré-requisitos, você cria uma política de NGFW da AWS Firewall Manager Palo Alto Networks Cloud.

Para obter mais informações sobre as políticas do Firewall Manager para o Cloud NGFW da Palo Alto Networks, consulte Políticas de NGFW na nuvem da Palo Alto Networks.

Para criar uma política do Firewall Manager para o Cloud NGFW da Palo Alto Networks (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Para Tipo de política, escolha Palo Alto Networks Cloud NGFW. Se você ainda não se inscreveu no serviço NGFW Cloud da Palo Alto Networks no AWS Marketplace, você precisará fazer isso primeiro. Para se inscrever no AWS Marketplace, escolha Exibir detalhes do AWS Marketplace.

5. Para Modelo de implantação, escolha o Modelo distribuído ou Modelo centralizado. O modelo de implantação determina como o Firewall Manager gerencia os endpoints da política. Com o modelo distribuído, o Firewall Manager mantém endpoints de firewall em cada VPC que está dentro do escopo da política. Com o modelo centralizado, o Firewall Manager mantém um único endpoint em uma VPC de inspeção.
6. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. Na configuração da política, escolha a política de firewall do Cloud NGFW da Palo Alto Networks para associar a essa política. A lista de políticas de firewall do Cloud NGFW da Palo Alto Networks contém todas as políticas de firewall do Cloud NGFW da Palo Alto Networks que estão associadas ao seu locatário do Cloud NGFW da Palo Alto Networks. Para obter informações sobre como criar e gerenciar políticas de firewall NGFW da Palo Alto Networks Cloud, consulte o tópico Implantar o Palo Alto Networks Cloud NGFW para AWS ver o AWS Firewall Manager tópico no guia de implantação do Palo Alto Networks Cloud NGFW. AWS
10. Para o registro do Palo Alto Networks Cloud NGFW - opcional, opcionalmente, escolha quais tipos de log do Palo Alto Networks Cloud NGFW devem ser registrados para sua política. Para obter informações sobre os tipos de log NGFW do Palo Alto Networks Cloud, consulte Configurar o registro para o Palo Alto Networks Cloud NGFW AWS no guia de implantação do Palo Alto Networks Cloud NGFW. AWS

    Para destino do log, especifique quando o Firewall Manager deve gravar os logs.
11. Escolha Próximo.
12. Em Configurar endpoint de firewall de terceiros, faça o seguinte, dependendo se você está usando o modelo de implantação distribuída ou centralizada para criar seus endpoints de firewall:

    - Se você estiver usando o modelo de implantação distribuído para essa política, em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.
    - Se você estiver usando o modelo de implantação centralizada para essa política, na configuração do endpoint de AWS Firewall Manager , em Configuração da VPC de inspeção, insira a ID da conta da AWS do proprietário da VPC de inspeção e o ID da VPC da inspeção.

- Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.

13. Escolha Próximo.
14. Para o Escopo da política, de acordo com as Contas da AWS às quais esta política se aplica, escolha a seguinte opção:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

    O Tipo de recurso para políticas de Network Firewall é VPC.

15. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

16. Para Conceder acesso entre contas, escolha Baixar modelo de AWS CloudFormation . Isso baixa um AWS CloudFormation modelo que você pode usar para criar uma AWS CloudFormation pilha. Essa pilha cria uma AWS Identity and Access Management função que concede ao Firewall Manager permissões entre contas para gerenciar os recursos NGFW do Palo Alto Networks Cloud. Para obter informações sobre as pilhas, consulte Trabalhar com pilhas no Guia do usuário do AWS CloudFormation .
17. Escolha Próximo.
18. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
19. Escolha Próximo.
20. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.
21. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Para obter mais informações sobre as políticas do Cloud NGFW da Palo Alto Networks para o Firewall Manager, consulte Políticas de NGFW na nuvem da Palo Alto Networks.

Introdução às políticas do AWS Firewall Manager Fortigate CNF

O Fortigate Cloud Native Firewall (CNF) as a Service é um serviço de firewall de terceiros que você pode usar para suas políticas. AWS Firewall Manager Com o Fortigate CNF for Firewall Manager, você pode criar e implantar centralmente os recursos e conjuntos de políticas do Fortigate CNF em todas as suas contas. AWS Para usar AWS Firewall Manager para habilitar as políticas do Fortigate CNF, execute as seguintes etapas em sequência. Para obter mais informações sobre as políticas do Fortigate CNF, consulte Políticas do Fortigate Cloud Native Firewall (CNF) como serviço.

Tópicos

Etapa 1: conclua os pré-requisitos gerais

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 2: concluir os pré-requisitos da política do Fortigate CNF

Há outras etapas obrigatórias que você deve concluir para usar as políticas do Fortigate CNF. Essas etapas estão descritas em Pré-requisitos da política do Fortigate Cloud Native Firewall (CNF) as a Service. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Etapa 3: Criar e aplicar uma política Fortigate CNF

Depois de preencher os pré-requisitos, você cria uma política do AWS Firewall Manager Fortigate CNF.

Para obter mais informações sobre as políticas do Firewall Manager para o Fortigate CNF, consulte Políticas do Fortigate Cloud Native Firewall (CNF) como serviço.

Para criar uma política do Firewall Manager para o Fortigate CNF (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/

fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Fortigate CNF. Se você ainda não se inscreveu no serviço Fortigate CNF no AWS Marketplace, você precisará fazer isso primeiro. Para se inscrever no AWS Marketplace, escolha Exibir detalhes do AWS Marketplace.
5. Para Modelo de implantação, escolha o Modelo distribuído ou Modelo centralizado. O modelo de implantação determina como o Firewall Manager gerencia os endpoints da política. Com o modelo distribuído, o Firewall Manager mantém endpoints de firewall em cada VPC que está dentro do escopo da política. Com o modelo centralizado, o Firewall Manager mantém um único endpoint em uma VPC de inspeção.
6. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
7. Escolha Próximo.
8.
9. Na configuração da política, escolha a política de firewall Fortigate CNF a ser associada a essa política. A lista de políticas de firewall Fortigate CNF contém todas as políticas de firewall Fortigate CNF associadas à sua locação do Fortigate CNF. Para obter informações sobre como criar e gerenciar políticas de firewall do Fortigate CNF, consulte a documentação do Fortigate CNF.
10. Escolha Próximo.
11. Em Configurar endpoint de firewall de terceiros, faça o seguinte, dependendo se você está usando o modelo de implantação distribuída ou centralizada para criar seus endpoints de firewall:

    - Se você estiver usando o modelo de implantação distribuído para essa política, em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você

pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.

- Se você estiver usando o modelo de implantação centralizada para essa política, na configuração do endpoint de AWS Firewall Manager , em Configuração da VPC de inspeção, insira a ID da conta da AWS do proprietário da VPC de inspeção e o ID da VPC da inspeção.
  - Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.

12. Escolha Próximo.
13. Para o Escopo da política, de acordo com as Contas da AWS às quais esta política se aplica, escolha a seguinte opção:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

    O tipo de recurso para as políticas do Fortigate CNF é VPC.

14. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

15. Para Conceder acesso entre contas, escolha Baixar modelo de AWS CloudFormation . Isso baixa um AWS CloudFormation modelo que você pode usar para criar uma AWS CloudFormation pilha. Essa pilha cria uma AWS Identity and Access Management função que concede ao Firewall Manager permissões entre contas para gerenciar os recursos do Fortigate CNF. Para obter informações sobre as pilhas, consulte Trabalhar com pilhas no Guia do usuário do AWS CloudFormation . Para criar uma pilha, você precisará do ID da conta do portal Fortigate CNF.
16. Escolha Próximo.
17. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
18. Escolha Próximo.
19. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Verifique se as Ações da política estão definidas como Identificar recursos que não estão em conformidade com as regras da política, mas não corrigir automaticamente. Isso permite que você revise as alterações que sua política faria antes de ativá-las.

20. Quando estiver satisfeito com a política, escolha Criar política.

    No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Para obter mais informações sobre as políticas Firewall Manager para o Fortigate CNF, consulte Políticas do Fortigate Cloud Native Firewall (CNF) como serviço.

Trabalhando com AWS Firewall Manager políticas

AWS Firewall Manager fornece os seguintes tipos de políticas. Para cada tipo de política, você define:

- AWS WAFpolítica — Suporte ao Firewall Manager AWS WAF e políticas AWS WAF clássicas. Para ambas as versões, defina quais recursos serão protegidos pela política.
  - O tipo de AWS WAF política usa conjuntos de grupos de regras para serem executados primeiro e por último na ACL da web. Em seguida, nas contas em que você aplica a Web ACL, o proprietário da conta pode adicionar regras e grupos de regras para serem executados entre os dois conjuntos.
  - O tipo de política AWS WAF Classic usa um único grupo de regras para ser executado na Web ACL.
- Política Shield Advanced — Esse tipo de política aplica as proteções Shield Advanced em toda a organização para os tipos de recursos que você especificar.
- Política de grupo de segurança da Amazon VPC — Esse tipo de política oferece controle sobre os grupos de segurança que estão em uso em toda a organização e permite aplicar um conjunto básico de regras em toda a organização.
- Política de lista de controle de acesso à rede (ACL) da Amazon VPC — Esse tipo de política oferece controle sobre as ACLs de rede que estão em uso em toda a organização e permite aplicar um conjunto básico de ACLs de rede em toda a organização.
- Política de Firewall de Rede — Esse tipo de política aplica AWS Network Firewall proteção às VPCs da sua organização.
- Política do Firewall DNS do Amazon Route 53 Resolver: essa política aplica proteções do Firewall DNS às VPCs da sua organização.
- Política de firewall de terceiros — Esse tipo de política aplica proteções de firewall de terceiros. Firewalls de terceiros estão disponíveis por assinatura por meio do console do AWS Marketplace no AWS Marketplace.
  - Política NGFW da Palo Alto Networks Cloud — Esse tipo de política aplica as proteções do Cloud Next Generation Firewall (NGFW) da Palo Alto Networks e as pilhas de regras do Palo Alto Networks Cloud NGFW às VPCs da sua organização.

- Política do Fortigate Cloud Native Firewall (CNF) as a Service — Esse tipo de política aplica as proteções do Fortigate Cloud Native Firewall (CNF) as a Service. O Fortigate CNF é uma solução centrada na nuvem que bloqueia ameaças desde o primeiro dia e protege as infraestruturas de nuvem com prevenção avançada de ameaças líder do setor, firewalls inteligentes de aplicativos web (WAF) e proteção de API.

Uma política do Firewall Manager é específica do tipo de política individual. Se pretender impor vários tipos de política entre contas, você poderá criar várias políticas. Você pode criar mais de uma política para cada tipo.

Se você adicionar uma nova conta a uma organização com a qual você criou AWS Organizations, o Firewall Manager aplicará automaticamente a política aos recursos dessa conta que estão dentro do escopo da política.

Configurações gerais para AWS Firewall Manager políticas

AWS Firewall Manager as políticas gerenciadas têm algumas configurações e comportamentos comuns. Para todos, você especifica um nome e define o escopo da política, além de usar a marcação de recursos para controlar o escopo da política. Você pode optar por exibir as contas e os recursos que não estão em conformidade sem tomar medidas corretivas ou corrigir automaticamente recursos não compatíveis.

Para obter informações sobre a política do escopo, consulte AWS Firewall Manager escopo da política.

Criação de uma AWS Firewall Manager política

As etapas para criar uma política variam entre os diferentes tipos de política. Use o procedimento para o tipo de política de que você precisa.

> **Important**
>
> AWS Firewall Manager não é compatível com o Amazon Route 53 ou AWS Global Accelerator. Se você precisar proteger esses recursos com o Shield Advanced, não poderá usar uma política do Firewall Manager. Em vez disso, siga as instruções em Adicionando AWS Shield Advanced proteção aos AWS recursos.

Tópicos

- Criação de uma AWS Firewall Manager política para AWS WAF
- Criação de uma AWS Firewall Manager política para o AWS WAF Classic
- Criação de uma AWS Firewall Manager política para AWS Shield Advanced
- Criar uma política de grupo de segurança comum do AWS Firewall Manager
- Criar uma política de grupo de segurança de auditoria de conteúdo do AWS Firewall Manager
- Criar uma política de grupo de segurança de auditoria de uso do AWS Firewall Manager
- Criando uma política AWS Firewall Manager de ACL de rede
- Criação de uma AWS Firewall Manager política para AWS Network Firewall
- Criação de uma AWS Firewall Manager política para o Amazon Route 53 Resolver DNS Firewall
- Criação de uma AWS Firewall Manager política para o Palo Alto Networks Cloud NGFW
- Criação de uma AWS Firewall Manager política para o Fortigate Cloud Native Firewall (CNF) como serviço

Criação de uma AWS Firewall Manager política para AWS WAF

Em uma AWS WAF política do Firewall Manager, você pode usar grupos de regras gerenciados, que AWS AWS Marketplace os vendedores criam e mantêm para você. Também é possível criar e usar os próprios grupos de regras. Para obter mais informações sobre grupos de regras, consulte AWS WAF grupos de regras.

Se quiser usar seus próprios grupos de regras, crie-os antes da política do Firewall Manager do AWS WAF . Para obter orientações, consulte Gerenciar seus próprios grupos de regras. Para usar uma regra personalizada individual, é necessário definir seu próprio grupo de regras, definir a regra nele e, depois, usar o grupo de regras na política.

Para obter informações sobre AWS WAF as políticas do Firewall Manager, consulteAWS WAF políticas.

Para criar uma política do Firewall Manager para AWS WAF (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha AWS WAF.
5. Para Região, escolha um Região da AWS. Para proteger as CloudFront distribuições da Amazon, escolha Global.

   Para proteger recursos em várias regiões (exceto CloudFront distribuições), você deve criar políticas separadas do Firewall Manager para cada região.
6. Escolha Próximo.
7. Em Nome da política, insira um nome descritivo. O Firewall Manager inclui o nome da política nos nomes das web ACLs que ele gerencia. Os nomes da web ACL têm `FMManagedWebACLV2-` seguido do nome da política que você insere aqui, `-`, e do timestamp da criação da web ACL, em milissegundos UTC. Por exemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.
8. Para a inspeção do corpo da solicitação da web, altere opcionalmente o limite de tamanho do corpo. Para obter informações sobre os limites de tamanho da inspeção do corpo, incluindo considerações de preços, consulte Gerenciando os limites de tamanho da inspeção corporal no Guia do desenvolvedor de AWS WAF .
9. Em Regras de política, adicione os grupos de regras que você AWS WAF deseja avaliar primeiro e por último na ACL da web. Para usar o controle de versão de grupos de regras AWS WAF gerenciados, ative a opção Ativar controle de versão. Os gerentes de contas individuais podem adicionar regras e grupos de regras entre os primeiros e os últimos grupos de regras. Para obter mais informações sobre o uso de grupos de AWS WAF regras nas políticas do Firewall Manager para AWS WAF, consulteAWS WAF políticas.

   (Opcional) Para personalizar como sua web ACL usa o grupo de regras, escolha Editar. A seguir, são mostradas as configurações de personalização comuns:

   - Para grupos de regras gerenciadas, substitua as ações de regra para algumas ou todas as regras. Se você não definir uma ação de substituição para uma regra, a avaliação usará a ação de regra definida dentro do grupo de regras. Para obter mais informações sobre

esta opção, consulte Opções de substituição de ação para grupos de regras no Guia do desenvolvedor AWS WAF .

- Alguns grupos de regras gerenciadas exigem que você forneça configurações adicionais. Consulte a documentação do seu provedor de grupos de regras gerenciadas. Para obter informações específicas sobre os grupos de regras de regras AWS gerenciadas, consulte AWS Regras gerenciadas para AWS WAF o Guia do AWS WAF desenvolvedor.

Ao concluir suas configurações, escolha Salvar regra.

10. Defina a ação padrão para a web ACL. Essa é a ação que o AWS WAF executa quando uma solicitação da web não corresponde a nenhuma das regras na ACL da web. Você pode adicionar cabeçalhos personalizados com a ação Permitir ou respostas personalizadas para a ação Bloquear. Para obter mais informações sobre ações padrão de ACL da web, consulte A ação padrão da web ACL. Para obter informações sobre como configurar solicitações e respostas personalizadas da web, consulte Solicitações e respostas personalizadas da web no AWS WAF.
11. Em Configuração de registro em log, escolha Ativar registro em log para ativar o registro em log. O registro em log fornece informações detalhadas sobre o tráfego que é analisado pela sua web ACL. Escolha o Destino de registro em log e, em seguida, escolha o destino de registro em log que você configurou. Você deve escolher um destino de registro em log cujo nome comece com `aws-waf-logs-`. Para obter informações sobre como configurar um destino de AWS WAF registro, consulteConfigurando o registro em log para uma política AWS WAF.
12. (Opcional) Se você não deseja que determinados campos e seus valores sejam incluídos nos logs, edite esses campos. Selecione o campo para editar e, em seguida, selecione Adicionar. Repita conforme necessário para editar campos adicionais. Os campos editados são exibidos como `REDACTED` nos logs. Por exemplo, se você editar o campo URI, o campo URI nos logs será `REDACTED`.
13. (Opcional) Se você não quiser enviar todas as solicitações para os logs, adicione seus critérios e comportamento de filtragem. Em Filtrar logs, para cada filtro que você deseja aplicar, escolha Adicionar filtro, escolha seus critérios de filtragem e especifique se deseja manter ou eliminar solicitações que correspondam aos critérios. Ao terminar de adicionar filtros, se necessário, modifique o Comportamento de registro de logs padrão. Para obter mais informações, consulte Configuração de registro do Web ACL no AWS WAF Guia do desenvolvedor.
14. Você pode definir uma Lista de domínios de tokens para permitir o compartilhamento de tokens entre aplicativos protegidos. Os tokens são usados pelas Challenge ações CAPTCHA e pelos SDKs de integração de aplicativos que você implementa ao usar os grupos de regras AWS

gerenciadas para controle de AWS WAF fraudes, prevenção de aquisição de contas (ATP) e AWS WAF controle de bots.

Não são permitidos sufixos públicos. Por exemplo, você não pode usar `gov.au` ou `co.uk` como um domínio de token.

Por padrão, AWS WAF aceita tokens somente para o domínio do recurso protegido. Se você adicionar domínios de token nessa lista, AWS WAF aceitará tokens para todos os domínios na lista e para o domínio do recurso associado. Para obter mais informações, consulte AWS WAF configuração da lista de domínios do token Web ACL no AWS WAF Guia do desenvolvedor.

Você só pode alterar o CAPTCHA da web ACL e desafiar os tempos de imunidade ao editar uma web ACL existente. Você pode encontrar essas configurações na página Detalhes da Política do Firewall Manager. Para obter informações sobre essas configurações, consulte Expiração do timestamp: tempos de imunidade AWS WAF do token. Se você atualizar as definições da Configuração de associação, CAPTCHA, Desafio ou Lista de domínios de Token em uma política existente, o Firewall Manager substituirá as web ACLs locais pelos novos valores. No entanto, se você não atualizar as definições de Configurações de associação, CAPTCHA, Desafio ou Lista de domínios de token da política, os valores em suas web ACLs locais permanecerão inalterados. Para obter mais informações sobre esta opção, consulte CAPTCHAe Challenge em AWS WAF no Guia do desenvolvedor AWS WAF .

15. Em Gerenciamento de web ACL, se você quiser que o Firewall Manager gerencie web ACLs não associadas, habilite Gerenciar web ACLs não associadas. Com essa opção, o Firewall Manager cria web ACLs nas contas dentro do escopo da política somente se as web ACLs forem usadas por pelo menos um recurso. Se, a qualquer momento, uma conta entrar no escopo da política, o Firewall Manager criará automaticamente uma web ACL na conta se pelo menos um recurso usar a web ACL. Após a ativação dessa opção, o Firewall Manager executa uma limpeza única das web ACLs não associadas em sua conta. O processo de limpeza pode levar várias horas. Se um recurso deixar o escopo da política depois que o Firewall Manager criar uma web ACL, o Firewall Manager desassociará o recurso da web ACL, mas não limpará a web ACL não associada. O Firewall Manager só limpa web ACLs não associadas quando você habilita antes o gerenciamento de web ACLs não associadas em uma política.
16. Em Ação da política, se quiser criar uma web ACL em cada conta aplicável na organização, mas ainda não aplicar a web ACL a nenhum recurso, escolha Identificar recursos que não estejam em conformidade com as regras de política, mas não corrigir automaticamente e não escolha Gerenciar web ACLs não associadas. É possível alterar essas opções mais tarde.

Se, em vez disso, quiser aplicar automaticamente a política aos recursos existentes no escopo, escolha Auto remediate any noncompliant resources (Corrigir automaticamente quaisquer recursos não compatíveis). Se a opção Gerenciar web ACLs não associadas estiver desativada, a opção Remediar automaticamente qualquer recurso não compatível cria uma web ACL em cada conta aplicável na organização e associa a web ACL aos recursos nas contas. Se a opção Gerenciar web ACLs não associadas estiver ativada, a opção de correção automática de qualquer recurso não compatível somente criará e associará uma web ACL em contas que tenham recursos elegíveis para associação à web ACL.

Ao selecionar Corrigir automaticamente qualquer recurso não compatível, você também pode optar por remover associações de web ACL existentes de recursos dentro do escopo, para as web ACLs que não são gerenciadas por outra política ativa do Firewall Manager. Se você escolher essa opção, o Firewall Manager associará primeiro a web ACL da política aos recursos e, depois, removerá as associações anteriores. Se um recurso tiver uma associação com outra web ACL gerenciada por uma política ativa diferente do Firewall Manager, essa escolha não afetará essa associação.

17. Escolha Próximo.
18. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Para aplicar a política a todas as contas, com exceção de um conjunto específico de contas ou unidades organizacionais (OUs) do AWS Organizations , escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

19. Em Tipo de recurso, escolha os tipos de recurso que você deseja proteger.
20. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
21. Escolha Próximo.
22. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
23. Escolha Próximo.
24. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Criação de uma AWS Firewall Manager política para o AWS WAF Classic

Para criar uma política do Firewall Manager para AWS WAF Classic (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha AWS WAF Classic.
5. Se você já criou o grupo de regras AWS WAF clássico que deseja adicionar à política, escolha Criar uma AWS Firewall Manager política e adicionar grupos de regras existentes. Se você deseja criar um novo grupo de regras, escolha Criar uma política do Firewall Manager e adicione um novo grupo de regras.
6. Para Região, escolha um Região da AWS. Para proteger os CloudFront recursos da Amazon, escolha Global.

   Para proteger recursos em várias regiões (exceto CloudFront recursos), você deve criar políticas separadas do Firewall Manager para cada região.
7. Escolha Próximo.
8. Se você estiver criando um grupo de regras, siga as instruções em Criação de um grupo de regras AWS WAF clássico. Depois de criar o grupo de regras, continue com as etapas a seguir.
9. Insira um nome de política.
10. Se você estiver adicionando um grupo de regras existente, use o menu suspenso para selecionar um grupo de regras para adicionar e escolha Add rule group (Adicionar grupo de regras).
11. Uma política executa duas ações possíveis: Action set by rule group (Ação definida pelo grupo de regras) e Count (Contar). Se você quiser testar a política e o grupo de regras, defina a ação como Count (Contar). Essa ação substitui qualquer ação de bloqueio especificada pelas

regras no grupo. Em outras palavras, se a ação da política for definida como Count (Contar), as solicitações serão apenas contadas, e não bloqueadas. Por outro lado, se você definir a ação da política como Action set by rule group (Ação definida pelo grupo de regras), as ações do grupo de regras serão usadas. Escolha a ação apropriada.

12. Escolha Próximo.
13. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.
14. Escolha o tipo de recurso que você deseja proteger.
15. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

16. Se você deseja aplicar automaticamente a política aos recursos existentes, escolha Create and apply this policy to existing and new resources (Criar e aplicar esta política a recursos novos e existentes).

    Essa opção cria uma web ACL em cada conta aplicável de uma organização da AWS e associa a web ACL aos recursos nas contas. Essa opção também aplica a política a todos os recursos novos que correspondam aos critérios mencionados anteriormente (tipo de recurso e tags). Como alternativa, se você selecionar Criar política mas não aplicá-la a recursos novos ou existentes, o Firewall Manager criará a web ACL em cada conta aplicável da organização, mas não aplicará a web ACL a nenhum dos recursos. Você deverá aplicar a política aos recursos mais tarde. Escolha a opção apropriada.

17. Em Substituir web ACLs associadas existentes, é possível remover quaisquer associações de web ACL atualmente definidas para recursos no escopo e substituí-las por associações às web ACLs que você está criando nessa política. Por padrão, o Firewall Manager não remove associações existentes da web ACL antes de adicionar as novas. Se você quiser remover as existentes, escolha essa opção.

18. Escolha Próximo.

19. Analise a nova política. Para fazer quaisquer alterações, escolha Edit (Editar). Quando estiver satisfeito com a política, escolha Create and apply policy (Criar e aplicar política).

Criação de uma AWS Firewall Manager política para AWS Shield Advanced

Criar uma política do Firewall Manager para Shield Advanced (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Shield Advanced.

   Para criar uma política Shield Advanced, você deve ser assinante do Shield Advanced. Se você não estiver inscrito, será solicitado a fazê-lo. Para obter mais informações sobre o custo, consulte Definição de preço do AWS Shield Advanced.
5. Para Região, escolha um Região da AWS. Para proteger as CloudFront distribuições da Amazon, escolha Global.

   Para opções de região que não sejam Global, para proteger recursos em várias regiões, você deve criar uma política separada do Firewall Manager para cada região.
6. Escolha Próximo.
7. Em Nome, insira um nome descritivo.
8. Somente para políticas de região Global, você pode escolher se deseja gerenciar a mitigação automática de DDoS na camada de aplicativos do Shield Advanced. Para obter informações sobre esse atributo do Shield Advanced, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

   Você pode optar por habilitar ou desabilitar a mitigação automática ou por ignorá-la. Se você optar por ignorá-lo, o Firewall Manager não gerencia a mitigação automática das proteções Shield Advanced. Para obter mais informações sobre essas opções de política, consulte Mitigação automática de DDoS na camada de aplicação.
9. Em Gerenciamento de web ACL, se você quiser que o Firewall Manager gerencie web ACLs não associadas, habilite Gerenciar web ACLs não associadas. Com essa opção, o Firewall Manager cria web ACLs nas contas dentro do escopo da política somente se as web ACLs forem usadas por pelo menos um recurso. Se, a qualquer momento, uma conta entrar no escopo da política, o Firewall Manager criará automaticamente uma web ACL na conta se pelo menos um recurso usar a web ACL. Após a ativação dessa opção, o Firewall Manager executa uma limpeza única das web ACLs não associadas em sua conta. O processo de limpeza pode levar várias horas. Se um recurso deixar o escopo da política após o Firewall Manager criar uma web

ACL, o Firewall Manager não desassociará o recurso da web ACL. Para incluir a web ACL na limpeza única, você deve primeiro desassociar manualmente os recursos da web ACL e depois ativar Gerenciar web ACLs não associadas.

10. Em Ação da política, recomendamos criar a política com a opção que não corrige automaticamente recursos em não conformidade. Ao desativar a remediação automática, você pode avaliar os efeitos da sua nova política antes de aplicá-la. Quando você estiver satisfeito com as alterações, edite a política e altere a ação da política para habilitar a correção automática de recursos não compatíveis.

    Se, em vez disso, quiser aplicar automaticamente a política aos recursos existentes no escopo, escolha Auto remediate any noncompliant resources (Corrigir automaticamente quaisquer recursos não compatíveis). Essa opção aplica as proteções Shield Advanced a cada conta aplicável na AWS organização e a cada recurso aplicável nas contas.

    Somente para políticas de região global, se você escolher Remediar automaticamente quaisquer recursos não compatíveis, também poderá optar por fazer com que o Firewall Manager substitua automaticamente todas as associações existentes de ACL da web AWS WAF clássicas por novas associações às ACLs da web que foram criadas usando a versão mais recente do (v2). AWS WAF Se você escolher essa opção, o Firewall Manager removerá as associações com as web ACLs da versão anterior e criará novas associações com as web ACLs da versão mais recente, depois de criar novas web ACLs vazias em qualquer conta dentro do escopo que ainda não as tenha para a política. Para obter mais informações sobre essa opção, consulte Substitua as ACLs da web AWS WAF clássicas pelas ACLs da web da versão mais recente.

11. Escolha Próximo.

12. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se deseja aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas sob minha organização da AWS .
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades

organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

É possível escolher apenas uma das opções.

Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

13. Escolha o tipo de recurso que você deseja proteger.

    O Firewall Manager não é compatível com o Amazon Route 53 ou AWS Global Accelerator. Se você precisar usar o Shield Advanced para proteger os recursos desses serviços, não poderá usar uma política do Firewall Manager. Em vez disso, siga as orientações do Shield Advanced em Adicionando AWS Shield Advanced proteção aos AWS recursos.

14. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

15. Escolha Próximo.

16. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

17. Escolha Próximo.

18. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Criar uma política de grupo de segurança comum do AWS Firewall Manager

Para obter informações sobre como funcionam as políticas de grupo de segurança comuns, consulte Políticas de grupo de segurança comuns.

Para criar uma política de grupo de segurança comum, você deve ter um grupo de segurança já criado em sua conta de administrador do Firewall Manager que deseja usar como principal para sua política. Você pode gerenciar grupos de segurança por meio da Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon VPC.

Para criar uma política de grupo de segurança comum (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Grupo de segurança.
5. Em Tipo de política de grupo de segurança, escolha Grupos de segurança comuns.
6. Para Região, escolha um Região da AWS.

7. Escolha Próximo.
8. Em Nome da política, insira um nome fácil de lembrar.
9. Em Policy rules (Regras de política), faça o seguinte:

   a. Nas opções de regras, escolha as restrições que você deseja aplicar às regras do grupo de segurança e aos recursos que estão dentro do escopo da política. Se você escolher Distribuir tags do grupo de segurança primário para os grupos de segurança criados por essa política, também deverá selecionar Identificar e relatar quando os grupos de segurança criados por essa política não estiverem em conformidade.

   > **Important**
   >
   > O Firewall Manager não distribuirá tags de sistema adicionadas pelos AWS serviços aos grupos de segurança de réplicas. As tags do sistema começam com o prefixo `aws:`. Além disso, o Firewall Manager não atualizará as tags dos grupos de segurança existentes nem criará novos grupos de segurança se a política tiver tags que entrem em conflito com a política de tags da organização. Para obter informações sobre políticas de tags, consulte Políticas de tags no Guia AWS Organizations do usuário.

   Se você escolher Distribuir referências de grupos de segurança do grupo de segurança primário para os grupos de segurança criados por essa política, o Firewall Manager só distribuirá as referências do grupo de segurança se eles tiverem uma conexão de emparelhamento ativa na Amazon VPC. Para obter informações sobre essa opção, consulte Configurações de regras de política.

   b. Em Grupos de segurança primários, escolha Adicionar grupos de segurança e, em seguida, escolha os grupos de segurança que você deseja usar. O Firewall Manager preenche a lista de grupos de segurança de todas as instâncias do Amazon VPC na conta de administrador do Firewall Manager.

   Por padrão, o número máximo de grupos de segurança primários por política é 3. Para obter mais informações sobre essa configuração, consulte AWS Firewall Manager cotas.

   c. Em Ação de política, recomendamos criar a política com a opção que não corrige automaticamente. Isso permite que você avalie os efeitos de sua nova política antes de aplicá-la. Quando você estiver satisfeito com as alterações, edite a política e altere a ação de política para habilitar a correção automática de recursos não compatíveis.

10. Escolha Próximo.
11. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.
12. Em Tipo de recurso, escolha os tipos de recurso que você deseja proteger.

    Se escolher Instância do EC2, você poderá optar por incluir todas as interfaces de rede elástica em cada instância do Amazon EC2 ou apenas a interface padrão em cada instância. Se você tiver mais de uma interface de rede elástica em qualquer instância do Amazon EC2 no escopo, escolher a opção para incluir todas as interfaces permitirá que o Firewall Manager aplique a política a todas elas. Quando você habilita a correção automática, se o Firewall Manager não puder aplicar a política a todas as interfaces de rede elástica em uma instância do Amazon EC2, ela marcará a instância como não compatível.

13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
14. Em Recursos da VPC compartilhada, se você quiser aplicar a política a recursos em VPCs compartilhadas, além das VPCs que as contas possuem, selecione Incluir recursos de VPCs compartilhadas.
15. Escolha Próximo.
16. Reveja as configurações de política para ter a certeza de que são o que você quer e escolha Criar política.

O Firewall Manager cria uma réplica do grupo de segurança primário em cada instância da Amazon VPC contida nas contas dentro do escopo até a cota máxima suportada da Amazon VPC por conta. O Firewall Manager associa os grupos de segurança de réplica aos recursos que estão dentro do escopo da política para cada conta dentro do escopo. Para obter mais informações sobre como essa política funciona, consulte Políticas de grupo de segurança comuns.

Criar uma política de grupo de segurança de auditoria de conteúdo do AWS Firewall Manager

Para obter informações sobre como as políticas de grupo de segurança de auditoria de conteúdo funcionam, consulte Políticas de grupo de segurança de auditoria de conteúdo.

Para algumas configurações de política de auditoria de conteúdo, você deve fornecer um grupo de segurança de auditoria para o Firewall Manager usar como modelo. Por exemplo, você pode ter um grupo de segurança de auditoria que contém todas as regras que você não permite em nenhum grupo de segurança. Você deve criar esses grupos de segurança de auditoria usando sua conta de administrador do Firewall Manager antes de poder usá-los em sua política. Você pode gerenciar grupos de segurança por meio da Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon VPC.

Para criar uma política de grupo de segurança de auditoria de conteúdo (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Grupo de segurança.
5. Em Security group policy type (Tipo de política de grupo de segurança), escolha Auditing and enforcement of security group rules (Auditoria e imposição de regras de grupo de segurança).
6. Para Região, escolha um Região da AWS.
7. Escolha Próximo.
8. Em Nome da política, insira um nome fácil de lembrar.
9. Para Regras da política, escolha a opção de regras da política gerenciadas ou personalizadas que você deseja usar.

   a. Para Configurar regras de política de auditoria gerenciada, faça o seguinte:

      i. Para Configurar regras de grupo de segurança para auditoria, selecione o tipo de regras de grupo de segurança às quais você deseja que sua política de auditoria se aplique.

      ii. Se você quiser fazer coisas como regras de auditoria com base nos protocolos, portas e configurações de intervalo CIDR dos seus grupos de segurança, escolha Auditar regras de grupos de segurança excessivamente permissivas e selecione as opções desejadas.

      Para a seleção Regra permite todo o tráfego, você pode fornecer uma lista de aplicativos personalizada para designar os aplicativos que você deseja auditar. Para obter informações sobre listas de aplicativos personalizadas e como usá-las em sua política, consulte Listas gerenciadas e Usar listas gerenciadas.

Para seleções que usam listas de protocolos, você pode usar listas existentes e criar novas listas. Para obter informações sobre listas de protocolos e como usá-las em sua política, consulte Listas gerenciadas e Usar listas gerenciadas.

iii. Se você quiser auditar aplicativos de alto risco com base no acesso deles a intervalos de CIDR reservados ou não reservados, escolha Auditar aplicativos de alto risco e selecione as opções desejadas.

As seguintes seleções são mutuamente exclusivas: Aplicativos que podem acessar somente intervalos CIDR reservados e Aplicativos com permissão para acessar intervalos CIDR não reservados. Você pode selecionar no máximo um deles em qualquer política.

Para seleções que usam listas de aplicativos, você pode usar listas existentes e criar novas listas. Para obter informações sobre listas de aplicativos e como usá-las em sua política, consulte Listas gerenciadas e Usar listas gerenciadas.

iv. Use as configurações de Substituição para substituir explicitamente outras configurações na política. Você pode optar por sempre permitir ou sempre negar regras específicas do grupo de segurança, independentemente de elas estarem em conformidade com as outras opções que você definiu para a política.

Para essa opção, você fornece um grupo de segurança de auditoria como modelo de regras permitidas ou negadas. Para Auditar grupos de segurança, selecione Adicionar auditar grupos de segurança e, em seguida, escolha o grupo de segurança que você deseja usar. O Firewall Manager preenche a lista de grupos de segurança de auditoria de todas as instâncias do Amazon VPC na conta do administrador do Firewall Manager. A cota máxima padrão para o número de grupos de segurança de auditoria para uma política é uma. Para obter informações sobre como aumentar a cota, consulte AWS Firewall Manager cotas.

b. Para Configurar regras de política personalizada, faça o seguinte:

i. Nas opções de regras, escolha se deseja permitir somente as regras definidas nos grupos de segurança de auditoria ou negar todas as regras. Para obter informações sobre essa opção, consulte Políticas de grupo de segurança de auditoria de conteúdo.

ii. Para Auditar grupos de segurança, selecione Adicionar auditar grupos de segurança e, em seguida, escolha o grupo de segurança que você deseja usar. O Firewall Manager preenche a lista de grupos de segurança de auditoria de todas as instâncias do

Amazon VPC na conta do administrador do Firewall Manager. A cota máxima padrão para o número de grupos de segurança de auditoria para uma política é uma. Para obter informações sobre como aumentar a cota, consulte AWS Firewall Manager cotas.

iii. Em Ação da política, você deve criar a política com a opção que não corrige automaticamente. Isso permite que você avalie os efeitos de sua nova política antes de aplicá-la. Quando você estiver satisfeito com as alterações, edite a política e altere a ação de política para habilitar a correção automática de recursos não compatíveis.

10. Escolha Próximo.
11. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.
12. Em Resource type (Tipo de recurso), escolha os tipos de recurso que você deseja proteger.

13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
14. Escolha Próximo.
15. Reveja as configurações de política para ter a certeza de que são o que você quer e escolha Criar política.

O Firewall Manager compara o grupo de segurança de auditoria com os grupos de segurança dentro do escopo em sua organização da AWS , de acordo com as configurações de regras de política. Você pode revisar o status da política no console AWS Firewall Manager de políticas. Depois que a política é criada, você pode editá-la e habilitar a correção automática para colocar sua política de grupo de segurança de auditoria em vigor. Para obter mais informações sobre como essa política funciona, consulte Políticas de grupo de segurança de auditoria de conteúdo.

Criar uma política de grupo de segurança de auditoria de uso do AWS Firewall Manager

Para obter informações sobre como as políticas de grupo de segurança de auditoria de uso funcionam, consulte Políticas de grupo de segurança de auditoria de uso.

Para criar uma política de grupo de segurança de auditoria de uso (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Grupo de segurança.
5. Em Tipo de política de grupo de segurança, escolha Auditing and cleanup of unassociated and redundant security groups (Auditoria e limpeza de grupos de segurança redundantes e não associados).
6. Para Região, escolha um Região da AWS.
7. Escolha Próximo.
8. Em Nome da política, insira um nome fácil de lembrar.
9. Em Policy rules (Regras de política), escolha uma ou ambas as opções disponíveis.

   - Se você escolher Grupos de segurança dentro deste escopo de política devem ser usados por pelo menos um recurso, o Firewall Manager removerá os grupos de segurança que ele determinar que não estão sendo utilizados. Quando essa regra é ativada, o Firewall Manager a executa por último quando você salva a política.

     Para obter detalhes sobre como o Firewall Manager determina o uso e o momento da correção, consulte Políticas de grupo de segurança de auditoria de uso.

     > **Note**
     >
     > Ao usar esse tipo de política de grupo de segurança de auditoria de uso, evite fazer várias alterações no status de associação dos grupos de segurança dentro do escopo em um curto espaço de tempo. Isso pode fazer com que o Firewall Manager perca os eventos correspondentes.

     Por padrão, o Firewall Manager considera que os grupos de segurança não estão em conformidade com essa regra de política assim que não são usados. Opcionalmente, você pode especificar por quantos minutos um grupo de segurança pode existir sem uso antes

de ser considerado incompatível, até 525.600 minutos (365 dias). Você pode usar essa configuração para ter tempo de associar novos grupos de segurança aos recursos.

> **Important**
>
> Se você especificar um número de minutos diferente do valor padrão de zero, deverá habilitar relacionamentos indiretos em AWS Config. Caso contrário, suas políticas de grupo de segurança de auditoria de uso não funcionarão conforme o esperado. Para obter informações sobre relacionamentos indiretos em AWS Config, consulte Relacionamentos indiretos AWS Config no Guia do AWS Config desenvolvedor.

- Se você escolher Grupos de segurança dentro deste escopo da política devem ser exclusivos, o Firewall Manager consolidará grupos de segurança redundantes, para que apenas um seja associado aos recursos. Se você escolher essa opção, o Firewall Manager a executará em primeiro lugar quando a política for salva.

10. Em Ação de política, recomendamos criar a política com a opção que não corrige automaticamente. Isso permite que você avalie os efeitos de sua nova política antes de aplicá-la. Quando você estiver satisfeito com as alterações, edite a política e altere a ação de política para habilitar a correção automática de recursos não compatíveis.
11. Escolha Próximo.
12. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

É possível escolher apenas uma das opções.

Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

14. Escolha Próximo.

15. Se você não excluiu a conta de administrador do Firewall Manager do escopo da política, o Firewall Manager solicitará que você faça isso. Fazer isso deixa os grupos de segurança na conta de administrador do Firewall Manager, que você usa para políticas de grupo de segurança comuns e de auditoria, sob seu controle manual. Escolha a opção que deseja nesta caixa de diálogo.

16. Reveja as configurações de política para ter a certeza de que são o que você quer e escolha Criar política.

Se você optar por exigir grupos de segurança exclusivos, o Firewall Manager procurará grupos de segurança redundantes em cada instância da Amazon VPC no escopo. Depois, se optar por exigir que cada grupo de segurança seja utilizado por pelo menos um recurso, o Firewall Manager procurará grupos de segurança que ficaram sem utilização durante os minutos especificados na regra. Você pode revisar o status da política no console AWS Firewall Manager de políticas. Para obter mais informações sobre como essa política funciona, consulte Políticas de grupo de segurança de auditoria de uso.

Criando uma política AWS Firewall Manager de ACL de rede

Para obter informações sobre como as políticas de ACL de rede funcionam, consultePolíticas de ACL de rede.

Para criar uma política de ACL de rede, você deve saber como definir uma ACL de rede para uso com suas sub-redes da Amazon VPC. Para obter informações, consulte Controle o tráfego para sub-redes usando ACLs de rede e Trabalhe com ACLs de rede no Guia do usuário da Amazon VPC.

Para criar uma política de ACL de rede (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Network ACL.
5. Para Região, escolha um Região da AWS.
6. Escolha Próximo.
7. Em Nome da política, insira um nome descritivo.
8. Em Regras de política, defina as regras que você deseja sempre executar nas ACLs de rede que o Firewall Manager gerencia para você. As ACLs de rede monitoram e gerenciam o tráfego de entrada e saída, portanto, em sua política, você define as regras para ambas as direções.

   Em qualquer direção, você define as regras que deseja sempre executar primeiro e as regras que deseja sempre executar por último. Nas ACLs de rede gerenciadas pelo Firewall Manager, os proprietários da conta podem definir regras personalizadas a serem executadas entre a primeira e a última regra.
9. Em Ação de política, se você quiser identificar sub-redes e ACLs de rede não compatíveis, mas ainda não tomar nenhuma ação corretiva, escolha Identificar recursos que não estejam em

conformidade com as regras de política, mas não corrijam automaticamente. É possível alterar essas opções mais tarde.

Se, em vez disso, você quiser aplicar automaticamente a política às sub-redes existentes no escopo, escolha Remediar automaticamente quaisquer recursos não compatíveis. Com essa opção, você também especifica se deve forçar a remediação quando o comportamento de tratamento de tráfego das regras de política entrar em conflito com as regras personalizadas que estão na ACL da rede. Independentemente de você forçar a remediação, o Firewall Manager relata regras conflitantes em suas violações de conformidade.

10. Escolha Próximo.
11. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir somente contas específicas, o Firewall Manager não aplicará a política a nenhuma conta nova e diferente. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.
12. Para Tipo de recurso, a configuração é fixada em Sub-redes.

13. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
14. Escolha Próximo.
15. Reveja as configurações de política para ter a certeza de que são o que você quer e escolha Criar política.

O Firewall Manager cria a política e começa a monitorar e gerenciar as ACLs de rede no escopo de acordo com suas configurações. Para obter mais informações sobre como essa política funciona, consulte Políticas de ACL de rede.

Criação de uma AWS Firewall Manager política para AWS Network Firewall

Em uma política do Network Firewall do Firewall Manager, você usa grupos de regras que gerencia no AWS Network Firewall. Para obter informações sobre como gerenciar seus grupos de regras, consulte grupos de regras do AWS Network Firewall no Guia do desenvolvedor do Network Firewall.

Para obter informações sobre as políticas do Network Firewall do Firewall Manager, consulte AWS Network Firewall políticas.

Para criar uma política do Firewall Manager para AWS Network Firewall (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha AWS Network Firewall.
5. Em Tipo de gerenciamento de firewall, escolha como você gostaria que o Firewall Manager gerenciasse os firewalls da política. Escolha uma das seguintes opções:

   - Distribuído: o Firewall Manager cria e mantém endpoints de firewall em cada VPC que está no escopo da política.
   - Centralizado: o Firewall Manager cria e mantém endpoints em uma única VPC de inspeção.
   - Importar firewalls existentes: o Firewall Manager importa firewalls existentes do Network Firewall usando conjuntos de recursos. Para obter mais informações sobre conjuntos de recursos, consulte Trabalhar com conjuntos de recursos no Firewall Manager.
6. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo. O Firewall Manager inclui o nome da política nos nomes dos firewalls do Network Firewall e das políticas de firewall que ele cria.
9. Na configuração da política de AWS Network Firewall , configure a política de firewall como você faria no Network Firewall. Adicione seus grupos de regras sem estado e com estado e especifique as ações padrão da política. Opcionalmente, você pode definir a ordem de avaliação de regras com estado e as ações padrão da política, bem como a configuração de registro. Para obter informações sobre o gerenciamento de políticas de firewall do Network Firewall, consulte as políticas de firewall do AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

   Quando você cria a política do Network Firewall do Firewall Manager, o Firewall Manager cria políticas de firewall para as contas que estão dentro do escopo. Gerentes de contas individuais podem adicionar grupos de regras às políticas de firewall, mas não podem alterar a configuração que você fornece aqui.
10. Escolha Próximo.
11. Dependendo do tipo de gerenciamento do Firewall que você selecionou na etapa anterior, siga um destes procedimentos:

- Se você estiver usando um tipo de gerenciamento de firewall distribuído, na configuração do endpoint de AWS Firewall Manager em Localização do endpoint do firewall, escolha uma das seguintes opções:
  - Configuração personalizada do endpoint: o Firewall Manager cria firewalls para cada VPC dentro do escopo da política, nas zonas de disponibilidade que você especificar. Cada firewall contém pelo menos um endpoint do firewall.
    - Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.
    - Se você quiser fornecer os blocos CIDR para o Firewall Manager usar nas sub-redes de firewall em suas VPCs, todos eles devem ser blocos CIDR /28. Insira um bloco por linha. Se você os omitir, o Firewall Manager escolherá endereços IP para você dentre aqueles que estão disponíveis nas VPCs.

      > **Note**
      >
      > A correção automática acontece automaticamente para as políticas de Firewall de AWS Firewall Manager Rede, então você não verá a opção de optar por não corrigir automaticamente aqui.

  - Configuração automática de endpoints: o Firewall Manager cria automaticamente endpoints de firewall nas zonas de disponibilidade com sub-redes públicas em sua VPC.
    - Para a configuração Endpoints do firewall, especifique como você deseja que os endpoints do firewall sejam gerenciados pelo Firewall Manager. Recomendamos o uso de vários endpoints para alta disponibilidade.
- Se você estiver usando um tipo de gerenciamento de firewall centralizado, na configuração do endpoint de AWS Firewall Manager , em Configuração da VPC de inspeção, insira a ID da conta da AWS do proprietário da VPC de inspeção e a ID da VPC de inspeção.
  - Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.
  - Se você quiser fornecer os blocos CIDR para o Firewall Manager usar nas sub-redes de firewall em suas VPCs, todos eles devem ser blocos CIDR /28. Insira um bloco por linha. Se você os omitir, o Firewall Manager escolherá endereços IP para você dentre aqueles que estão disponíveis nas VPCs.

> **Note**
>
> A correção automática acontece automaticamente para as políticas de Firewall de AWS Firewall Manager Rede, então você não verá a opção de optar por não corrigir automaticamente aqui.

- Se você estiver usando um tipo de gerenciamento de firewall para importar firewalls existentes, em Conjuntos de recursos, adicione um ou mais conjuntos de recursos. Um conjunto de recursos define os firewalls de Network Firewall existentes pertencentes à sua conta da organização que você deseja gerenciar centralmente nesta política. Para adicionar um conjunto de recursos à política, primeiro você deve criar um conjunto de recursos usando o console ou a PutResourceSetAPI. Para obter mais informações sobre conjuntos de recursos, consulte Trabalhar com conjuntos de recursos no Firewall Manager. Para obter mais informações sobre a importação de firewalls existentes do Network Firewall, consulte importar firewalls existentes.

12. Escolha Próximo.
13. Se sua política usa um tipo de gerenciamento de firewall distribuído, em Gerenciamento de rotas, escolha se o Firewall Manager monitorará e alertará sobre o tráfego que deve ser roteado pelos respectivos endpoints do firewall.

> **Note**
>
> Se você escolher Monitor, não poderá alterar a configuração para Desligado posteriormente. O monitoramento continua até que você exclua a política.

14. Em Tipo de tráfego, adicione opcionalmente os endpoints de tráfego pelos quais você deseja rotear o tráfego para inspeção do firewall.
15. Em Permitir o tráfego necessário entre A-Z, se você habilitar essa opção, o Firewall Manager tratará como roteamento compatível que envia tráfego de uma zona de disponibilidade para inspeção, para zonas de disponibilidade que não têm seu próprio endpoint de firewall. As zonas de disponibilidade que têm endpoints devem sempre inspecionar seu próprio tráfego.
16. Escolha Próximo.
17. Para o Escopo da política, de acordo com as Contas da AWS às quais esta política se aplica, escolha a seguinte opção:

- Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
- Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
- Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

   É possível escolher apenas uma das opções.

   Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

18. O Tipo de recurso para políticas de Network Firewall é VPC.
19. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
20. Escolha Próximo.

21. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
22. Escolha Próximo.
23. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Criação de uma AWS Firewall Manager política para o Amazon Route 53 Resolver DNS Firewall

Em uma política de Firewall DNS do Firewall Manager, você usa grupos de regras que você gerencia no Firewall DNS do Amazon Route 53 Resolver. Para obter informações sobre como gerenciar seus grupos de regras, consulte Gerenciamento de grupos de regras e regras no Firewall DNS no Guia do desenvolvedor do Amazon Route 53.

Para obter informações sobre as políticas de Firewall DNS do Firewall Manager, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.

Para criar uma política do Firewall Manager para o Firewall DNS do Amazon Route 53 Resolver (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Firewall DNS do Amazon Route 53 Resolver .
5. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
6. Escolha Próximo.
7. Em Nome da política, insira um nome descritivo.
8. Na configuração da política, adicione os grupos de regras que você deseja que o Firewall DNS avalie primeiro e por último entre as associações de grupos de regras de suas VPCs. Você pode adicionar até dois grupos de regras à política.

   Quando você cria a política de Firewall DNS do Firewall Manager, o Firewall Manager cria as associações de grupos de regras, com as prioridades de associação que você forneceu, para as VPCs e contas que estão dentro do escopo. Os gerentes de contas individuais podem adicionar associações de grupos de regras entre a primeira e a última associação, mas não podem alterar as associações que você define aqui. Para ter mais informações, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.
9. Escolha Próximo.
10. Para Contas da AWS às quais esta política se aplica, escolha a opção da seguinte maneira:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades

organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

É possível escolher apenas uma das opções.

Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

11. O Tipo de recurso para políticas de Firewall DNS é VPC.
12. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
13. Escolha Próximo.
14. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
15. Escolha Próximo.
16. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das

contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Criação de uma AWS Firewall Manager política para o Palo Alto Networks Cloud NGFW

Com uma política do Firewall Manager para o Firewall de Próxima Geração de Nuvem da Palo Alto Networks (Palo Alto Networks Cloud NGFW), você usa o Firewall Manager para implantar recursos NGFW do Palo Alto Networks Cloud e gerenciar as pilhas de regras do NGFW centralmente em todas as suas contas. AWS

Para obter informações sobre as políticas do Firewall Manager do NGFW na nuvem da Palo Alto Networks, consulte. Políticas de NGFW na nuvem da Palo Alto Networks Para obter informações sobre como configurar e gerenciar o NGFW na nuvem da Palo Alto Networks para o Firewall Manager, consulte o NGFW na nuvem da Palo Alto Networks na documentação da AWS.

Pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Para criar uma política do Firewall Manager para o Cloud NGFW da Palo Alto Networks (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.

4. Para Tipo de política, escolha Palo Alto Networks Cloud NGFW. Se você ainda não se inscreveu no serviço NGFW Cloud da Palo Alto Networks no AWS Marketplace, você precisará fazer isso primeiro. Para se inscrever no AWS Marketplace, escolha Exibir detalhes do AWS Marketplace.
5. Para Modelo de implantação, escolha o Modelo distribuído ou Modelo centralizado. O modelo de implantação determina como o Firewall Manager gerencia os endpoints da política. Com o modelo distribuído, o Firewall Manager mantém endpoints de firewall em cada VPC que está dentro do escopo da política. Com o modelo centralizado, o Firewall Manager mantém um único endpoint em uma VPC de inspeção.
6. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. Na configuração da política, escolha a política de firewall do Cloud NGFW da Palo Alto Networks para associar a essa política. A lista de políticas de firewall do Cloud NGFW da Palo Alto Networks contém todas as políticas de firewall do Cloud NGFW da Palo Alto Networks que estão associadas ao seu locatário do Cloud NGFW da Palo Alto Networks. Para obter informações sobre como criar e gerenciar políticas de firewall NGFW da Palo Alto Networks Cloud, consulte o tópico Implantar o Palo Alto Networks Cloud NGFW para AWS ver o AWS Firewall Manager tópico no guia de implantação do Palo Alto Networks Cloud NGFW. AWS
10. Para o registro do Palo Alto Networks Cloud NGFW - opcional, opcionalmente, escolha quais tipos de log do Palo Alto Networks Cloud NGFW devem ser registrados para sua política. Para obter informações sobre os tipos de log NGFW do Palo Alto Networks Cloud, consulte Configurar o registro para o Palo Alto Networks Cloud NGFW AWS no guia de implantação do Palo Alto Networks Cloud NGFW. AWS

    Para destino do log, especifique quando o Firewall Manager deve gravar os logs.
11. Escolha Próximo.
12. Em Configurar endpoint de firewall de terceiros, faça o seguinte, dependendo se você está usando o modelo de implantação distribuída ou centralizada para criar seus endpoints de firewall:

    - Se você estiver usando o modelo de implantação distribuído para essa política, em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.

- Se você estiver usando o modelo de implantação centralizada para essa política, na configuração do endpoint de AWS Firewall Manager , em Configuração da VPC de inspeção, insira a ID da conta da AWS do proprietário da VPC de inspeção e o ID da VPC da inspeção.
  - Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.

13. Se você quiser fornecer os blocos CIDR para o Firewall Manager usar nas sub-redes de firewall em suas VPCs, todos eles devem ser blocos CIDR /28. Insira um bloco por linha. Se você os omitir, o Firewall Manager escolherá endereços IP para você dentre aqueles que estão disponíveis nas VPCs.

> **Note**
>
> A correção automática acontece automaticamente para as políticas de Firewall de AWS Firewall Manager Rede, então você não verá a opção de optar por não corrigir automaticamente aqui.

14. Escolha Próximo.
15. Para o Escopo da política, de acordo com as Contas da AWS às quais esta política se aplica, escolha a seguinte opção:

- Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
- Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
- Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

É possível escolher apenas uma das opções.

Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.

16. O Tipo de recurso para políticas de Network Firewall é VPC.
17. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.
18. Para Conceder acesso entre contas, escolha Baixar modelo de AWS CloudFormation . Isso baixa um AWS CloudFormation modelo que você pode usar para criar uma AWS CloudFormation pilha. Essa pilha cria uma AWS Identity and Access Management função que concede ao Firewall Manager permissões entre contas para gerenciar os recursos NGFW do Palo Alto Networks Cloud. Para obter informações sobre as pilhas, consulte Trabalhar com pilhas no Guia do usuário do AWS CloudFormation .
19. Escolha Próximo.
20. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
21. Escolha Próximo.
22. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma

política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Criação de uma AWS Firewall Manager política para o Fortigate Cloud Native Firewall (CNF) como serviço

Com uma política do Firewall Manager para o Fortigate CNF, você pode usar o Firewall Manager para implantar e gerenciar os recursos do Fortigate CNF em todas as suas contas. AWS

Para obter informações sobre as políticas Firewall Manager para o Fortigate CNF, consulte Políticas do Fortigate Cloud Native Firewall (CNF) como serviço. Para obter informações sobre como configurar o Fortigate CNF para uso com o Firewall Manager, consulte a Documentação da Fortinet.

Pré-requisitos

Há várias etapas obrigatórias na preparação da conta para o AWS Firewall Manager. Essas etapas estão descritas em AWS Firewall Manager pré-requisitos. Conclua todos os pré-requisitos antes de prosseguir para a próxima etapa.

Para criar uma política do Firewall Manager para o Fortigate CNF (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha Criar política.
4. Em Tipo de política, escolha Fortigate Cloud Native Firewall (CNF) como serviço. Se você ainda não se inscreveu no serviço Fortigate CNF no AWS Marketplace, você precisará fazer isso primeiro. Para se inscrever no AWS Marketplace, escolha Exibir detalhes do AWS Marketplace.

5. Para Modelo de implantação, escolha o Modelo distribuído ou Modelo centralizado. O modelo de implantação determina como o Firewall Manager gerencia os endpoints da política. Com o modelo distribuído, o Firewall Manager mantém endpoints de firewall em cada VPC que está dentro do escopo da política. Com o modelo centralizado, o Firewall Manager mantém um único endpoint em uma VPC de inspeção.
6. Para Região, escolha um Região da AWS. Para proteger recursos em várias regiões, crie políticas separadas para cada região.
7. Escolha Próximo.
8. Em Nome da política, insira um nome descritivo.
9. Na configuração da política, escolha a política de firewall Fortigate CNF a ser associada a essa política. A lista de políticas de firewall Fortigate CNF contém todas as políticas de firewall Fortigate CNF associadas à sua locação do Fortigate CNF. Para obter informações sobre como criar e gerenciar locações do Fortigate CNF, consulte a Documentação da Fortinet.
10. Escolha Próximo.
11. Em Configurar endpoint de firewall de terceiros, faça o seguinte, dependendo se você está usando o modelo de implantação distribuída ou centralizada para criar seus endpoints de firewall:

    - Se você estiver usando o modelo de implantação distribuído para essa política, em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.
    - Se você estiver usando o modelo de implantação centralizada para essa política, na configuração do endpoint de AWS Firewall Manager , em Configuração da VPC de inspeção, insira a ID da conta da AWS do proprietário da VPC de inspeção e o ID da VPC da inspeção.
        - Em Zonas de disponibilidade, selecione em quais zonas de disponibilidade criar endpoints de firewall. Você pode selecionar Zonas de disponibilidade pelo Nome da zona de disponibilidade ou pelo ID da zona de disponibilidade.
12. Se você quiser fornecer os blocos CIDR para o Firewall Manager usar nas sub-redes de firewall em suas VPCs, todos eles devem ser blocos CIDR /28. Insira um bloco por linha. Se você os omitir, o Firewall Manager escolherá endereços IP para você dentre aqueles que estão disponíveis nas VPCs.

> **Note**
>
> A correção automática acontece automaticamente para as políticas de Firewall de AWS Firewall Manager Rede, então você não verá a opção de optar por não corrigir automaticamente aqui.

13. Escolha Próximo.
14. Para o Escopo da política, de acordo com as Contas da AWS às quais esta política se aplica, escolha a seguinte opção:

    - Se você quiser aplicar a política a todas as contas em sua organização, deixe a seleção padrão, Incluir todas as contas em minha AWS organização.
    - Se você quiser aplicar a política somente a contas específicas ou contas que estão em unidades AWS Organizations organizacionais (OUs) específicas, escolha Incluir somente as contas e unidades organizacionais especificadas e, em seguida, adicione as contas e OUs que você deseja incluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.
    - Se você quiser aplicar a política a todas, exceto a um conjunto específico de contas ou unidades AWS Organizations organizacionais (OUs), escolha Excluir as contas e unidades organizacionais especificadas e incluir todas as outras e, em seguida, adicione as contas e OUs que você deseja excluir. Especificar uma UO é equivalente a especificar todas as contas na UO e em qualquer uma das suas UOs filhas, incluindo todas as UOs e contas filhas que forem adicionadas posteriormente.

    É possível escolher apenas uma das opções.

    Depois de aplicar a política, o Firewall Manager avalia automaticamente todas as novas contas em relação às suas configurações. Por exemplo, se você incluir apenas contas específicas, o Firewall Manager não aplicará a política a nenhuma nova conta. Como outro exemplo, se você incluir uma UO, quando adicionar uma conta à UO ou a qualquer uma de suas UOs secundárias, o Firewall Manager aplicará automaticamente a política à nova conta.
15. O Tipo de recurso para políticas de Network Firewall é VPC.

16. Para Recursos, você pode restringir o escopo da política usando marcações, incluindo ou excluindo recursos com as tags que você especificar. Você pode usar inclusão ou exclusão, e não ambas. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.

    Se você inserir mais de uma tag, um recurso deverá ter todas as tags a serem incluídas ou excluídas.

    As tags de recursos só podem ter valores não nulos. Se você omitir o valor de uma tag, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

17. Para Conceder acesso entre contas, escolha Baixar modelo de AWS CloudFormation . Isso baixa um AWS CloudFormation modelo que você pode usar para criar uma AWS CloudFormation pilha. Essa pilha cria uma AWS Identity and Access Management função que concede ao Firewall Manager permissões entre contas para gerenciar os recursos do Fortigate CNF. Para obter informações sobre as pilhas, consulte Trabalhar com pilhas no Guia do usuário do AWS CloudFormation . Para criar uma pilha, você precisará do ID da conta do portal Fortigate CNF.
18. Escolha Próximo.
19. Para tags de política, adicione todas as tags de identificação que você deseja adicionar ao recurso de política do Firewall Manager. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
20. Escolha Próximo.
21. Revise as novas configurações de política e retorne às páginas em que você precise fazer ajustes.

    Quando estiver satisfeito com a política, escolha Criar política. No painel Políticas do AWS Firewall Manager , a política deve estar listada. Provavelmente, indicará Pendente nos títulos das contas e indicará o status da configuração de remediação automática. A criação de uma política pode levar vários minutos. Depois que o status Pendente for substituído por contagens de conta, será possível escolher o nome da política para explorar o status de conformidade das contas e dos recursos. Para obter mais informações, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política

Excluindo uma política AWS Firewall Manager

Você pode excluir uma política do Firewall Manager executando as seguintes etapas.

Para excluir uma política (console)

1. No painel de navegação, escolha Políticas de segurança.
2. Escolha a opção próxima à política que você deseja excluir.
3. Escolha Delete.

> **Note**
>
> Ao excluir uma política de grupo de segurança comum do Firewall Manager, para remover os grupos de segurança de réplica da política, escolha a opção para limpar os recursos criados pela política. Caso contrário, depois que o primário é excluído, as réplicas permanecem e exigem gerenciamento manual em cada instância do Amazon VPC.

> **Important**
>
> Quando você excluir uma política do Firewall Manager Shield Advanced, ela será excluída, mas suas contas permanecerão inscritas no Shield Advanced.

AWS Firewall Manager escopo da política

O escopo da política define onde a política se aplica. Você pode aplicar políticas controladas centralmente a todas as suas contas e recursos em AWS Organizations sua organização ou a um subconjunto de suas contas e recursos. Para obter instruções sobre como estabelecer o escopo da política, consulte Criação de uma AWS Firewall Manager política.

Opções do escopo da política em AWS Firewall Manager

Quando você adiciona uma nova conta ou recurso à sua organização, o Firewall Manager o avalia automaticamente em relação às configurações de cada política e aplica a política com base nessas configurações. Por exemplo, você pode optar por aplicar uma política a todas as contas, exceto aos números de conta em uma lista especificada; você também pode optar por aplicar uma política somente aos recursos que tenham todas as tags em uma lista.

Contas da AWS no escopo

As configurações que você fornece para definir os Contas da AWS afetados pela política determinam em quais contas da sua AWS organização aplicar a política. Você pode optar por aplicar a política de uma das seguintes maneiras:

- A todas as contas da organização
- A apenas uma lista específica de números de contas e unidades organizacionais (OUs) do AWS Organizations incluídas.
- A todas, com exceção de uma lista específica de números de contas e unidades organizacionais (OUs) do AWS Organizations excluídas

Para obter informações sobre AWS Organizations, consulte o Guia AWS Organizations do usuário.

Recursos no escopo

De forma semelhante às configurações para contas em escopo, as configurações fornecidas para recursos determinam quais tipos de recursos no escopo aplicar à política. Você pode escolher uma das seguintes opções:

- Todos os recursos
- Recursos que têm todas as tags especificadas
- Todos os recursos, exceto aqueles que têm todas as tags especificadas

Você só pode especificar tags de recursos com valores não nulos. Se você não fornecer nada para o valor, o Firewall Manager salvará a tag com um valor de string vazio: “”. As tags de recursos só correspondem às tags que têm a mesma chave e o mesmo valor.

Para obter mais informações sobre como marcar seus recursos, consulte Trabalhar com o Tag Editor.

Gerenciamento do escopo da política em AWS Firewall Manager

Quando as políticas estão em vigor, o Firewall Manager as gerencia continuamente e as aplica a novos Contas da AWS recursos à medida que são adicionados, de acordo com o escopo da política.

Como o Firewall Manager gerencia Contas da AWS os recursos

Se uma conta ou recurso sair do escopo por qualquer motivo, AWS Firewall Manager não removerá automaticamente as proteções nem excluirá os recursos gerenciados pelo Firewall Manager, a

menos que você marque a caixa de seleção Remover automaticamente as proteções dos recursos que saem do escopo da política.

> **Note**
>
> A opção Remover automaticamente as proteções dos recursos que saem do escopo da política não está disponível para AWS Shield Advanced nossas políticas AWS WAF clássicas.

Marcar essa caixa de seleção AWS Firewall Manager direciona a limpeza automática dos recursos que o Firewall Manager gerencia para contas quando essas contas saem do escopo da política. Por exemplo, o Firewall Manager desassociará uma web ACL gerenciada pelo Firewall Manager de um recurso protegido do cliente quando esse recurso sair do escopo da política.

Para determinar quais recursos devem ser removidos da proteção quando um recurso do cliente deixa o escopo da política, o Firewall Manager segue estas diretrizes:

- Comportamento padrão:
  - As regras AWS Config gerenciadas associadas são excluídas. Esse comportamento é independente da caixa de seleção.
  - Todas as listas de controle de acesso à AWS WAF web (ACLs da web) associadas que não contêm nenhum recurso são excluídas. Esse comportamento é independente da caixa de seleção.
  - Qualquer recurso protegido que saia do escopo permanece associado e protegido. Por exemplo, um Application Load Balancer ou API do API Gateway associado a uma web ACL permanece associado à web ACL e a proteção permanece em vigor.
- Com a caixa de seleção Remover automaticamente as proteções dos recursos que saem do escopo da política marcada:
  - As regras AWS Config gerenciadas associadas são excluídas. Esse comportamento é independente da caixa de seleção.
  - Todas as listas de controle de acesso à AWS WAF web (ACLs da web) associadas que não contêm nenhum recurso são excluídas. Esse comportamento é independente da caixa de seleção.
  - Qualquer recurso protegido que saia do escopo é automaticamente desassociado e removido da proteção do Firewall Manager quando sai do escopo da política. Por exemplo, para uma política

de grupo de segurança, um acelerador do Elastic Inference ou uma instância do Amazon EC2 é automaticamente desassociada do grupo de segurança replicado quando sai do escopo da política. O grupo de segurança replicado e seus recursos são automaticamente removidos da proteção.

Listas gerenciadas

As listas gerenciadas de aplicativos e protocolos simplificam a configuração e o gerenciamento das políticas do grupo de segurança de auditoria de conteúdo AWS Firewall Manager . Você usa listas gerenciadas para definir os protocolos e aplicativos que sua política permite e proíbe. Para obter informações sobre políticas de auditoria de conteúdo do grupo de segurança, consulte Políticas de grupo de segurança de auditoria de conteúdo.

Você pode usar os seguintes tipos de listas gerenciadas em uma política de grupo de segurança de auditoria de conteúdo:

- Listas de aplicativos e listas de protocolos do Firewall Manager: o Firewall Manager gerencia essas listas.
  - As listas de aplicativos incluem `FMS-Default-Public-Access-Apps-Allowed` e `FMS-Default-Public-Access-Apps-Denied`, que descrevem aplicativos comumente usados que devem ser permitidos ou negados ao público em geral.
  - As listas de protocolos incluem `FMS-Default-Protocols-Allowed`, uma lista de protocolos comumente usados que devem ser permitidos ao público em geral. Você pode usar qualquer lista gerenciada pelo Firewall Manager, mas não pode editá-la nem excluí-la.
- Listas personalizadas de aplicativos e listas de protocolos: você gerencia essas listas. Você pode criar listas de qualquer tipo com as configurações necessárias. Você tem controle total sobre suas próprias listas gerenciadas personalizadas e pode criá-las, editá-las e excluí-las conforme necessário.

> **Note**
>
> Atualmente, o Firewall Manager não verifica as referências a uma lista gerenciada personalizada quando você a exclui. Isso significa que você pode excluir uma lista personalizada de aplicativos gerenciados ou uma lista de protocolos mesmo quando ela estiver sendo usada por uma política ativa. Isso pode fazer com que a política pare de

funcionar. Exclua uma lista de aplicativos ou uma lista de protocolos somente depois de verificar se ela não é referenciada por nenhuma política ativa.

As listas gerenciadas são AWS recursos. Você pode marcar uma lista gerenciada personalizada. Você não pode marcar uma lista gerenciada do Firewall Manager.

Versionamento de listas gerenciadas

As listas gerenciadas personalizadas não têm versões. Quando você edita uma lista personalizada, as políticas que fazem referência à lista usam automaticamente a lista atualizada.

As listas gerenciadas do Firewall Manager têm controle de versão. A equipe de serviço do Firewall Manager publica novas versões conforme o necessário, a fim de aplicar as melhores práticas de segurança às listas.

Ao usar uma lista gerenciada do Firewall Manager em uma política, você escolhe sua estratégia de versionamento da seguinte forma:

- Última versão disponível: se você não especificar uma configuração de versão explícita para a lista, sua política usará automaticamente a versão mais recente. Essa é a única opção disponível no console.
- Versão explícita: se você especificar uma versão para a lista, sua política usará essa versão. Sua política permanece bloqueada para a versão que você especificou até que você modifique a configuração da versão. Para especificar a versão, você deve definir a política fora do console, por exemplo, por meio da CLI ou de um dos SDKs.

Para obter mais informações sobre como escolher a configuração de versão para uma lista, consulte Usar listas gerenciadas em suas políticas de grupo de segurança de auditoria de conteúdo.

Usar listas gerenciadas em suas políticas de grupo de segurança de auditoria de conteúdo

Ao criar uma política de grupo de segurança de auditoria de conteúdo, você pode optar por usar regras de política de auditoria gerenciada. Algumas das configurações dessa opção exigem uma lista gerenciada de aplicativos ou uma lista de protocolos. Exemplos dessas configurações incluem protocolos permitidos em regras de grupo de segurança e aplicativos que podem acessar a Internet.

As restrições a seguir se aplicam a cada configuração de política que usa uma lista gerenciada:

- Você pode especificar no máximo uma lista gerenciada do Firewall Manager para qualquer configuração. Por padrão, você pode especificar no máximo uma lista personalizada. O limite da lista personalizada é uma cota flexível, então você pode solicitar um aumento. Para ter mais informações, consulte AWS Firewall Manager cotas.
- No console, se você selecionar uma lista gerenciada do Firewall Manager, não poderá especificar a versão. A política sempre usará a versão mais recente da lista. Para especificar a versão, você deve definir a política fora do console, por exemplo, por meio da CLI ou de um dos SDKs. Para obter informações sobre o versionamento das listas gerenciadas do Firewall Manager, consulte. Versionamento de listas gerenciadas

Para obter informações sobre como criar uma política de grupo de segurança de auditoria de conteúdo por meio do console, consulte Criar uma política de grupo de segurança de auditoria de conteúdo.

Criar uma lista personalizada de aplicativos gerenciados

Para criar uma lista personalizada de aplicativos gerenciados

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Listas de aplicativos.
3. Na página Lista de aplicativos, escolha Criar lista de aplicativo.
4. Na página Criar lista de aplicativos, dê um nome à sua lista. Não use o prefixo `fms-`, pois ele é reservado para o Firewall Manager.
5. Especifique um aplicativo fornecendo o protocolo e o número da porta ou selecionando um aplicativo no menu suspenso Tipo. Dê um nome à especificação do seu aplicativo.
6. Escolha Adicionar outro conforme necessário e preencha as informações do aplicativo até concluir sua lista.

7. (Opcional) Aplique tags à sua lista.
8. Escolha Salvar para salvar sua lista e retornar à página Listas de aplicativos.

Criar uma lista personalizada de protocolos gerenciados

Para criar uma lista personalizada de protocolos gerenciados

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Listas de protocolos.
3. Na página Listas de protocolos, escolha Criar lista de protocolos.
4. Na página de criação da lista de protocolos, dê um nome à sua lista. Não use o prefixo `fms-`, pois ele é reservado para o Firewall Manager.
5. Especificar um protocolo.
6. Escolha Adicionar outro conforme o necessário e preencha as informações do protocolo até concluir sua lista.
7. (Opcional) Aplique tags à sua lista.
8. Escolha Salvar para salvar sua lista e retornar à página Listas de protocolos.

Visualizar uma lista gerenciada

Para ver uma lista de aplicativos ou uma lista de protocolos

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, selecione Listas de aplicativo ou Listas de protocolos.

   A página exibe todas as listas do tipo selecionado que estão disponíveis para seu uso. As listas gerenciadas pelo Firewall Manager têm um Y na ManagedListcoluna.

3. Para ver os detalhes de uma lista, escolha seu nome. A página de detalhes exibe o conteúdo da lista e todas as tags.

   Nas listas gerenciadas do Firewall Manager, você também pode ver as versões disponíveis selecionando o menu suspenso Versão.

Excluir uma lista gerenciada personalizada

Você pode excluir listas gerenciadas personalizadas. Você pode editar ou excluir listas gerenciadas pelo Firewall Manager.

> **Note**
>
> Atualmente, o Firewall Manager não verifica as referências a uma lista gerenciada personalizada quando você a exclui. Isso significa que você pode excluir uma lista personalizada de aplicativos gerenciados ou uma lista de protocolos mesmo quando ela estiver sendo usada por uma política ativa. Isso pode fazer com que a política pare de funcionar. Exclua uma lista de aplicativos ou uma lista de protocolos somente depois de verificar se ela não é referenciada por nenhuma política ativa.

Para excluir um aplicativo gerenciado personalizado ou uma lista de protocolos

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. Certifique-se de que a lista que você deseja excluir não esteja em uso em nenhuma das suas políticas de grupo de segurança de auditoria fazendo o seguinte:

   a. No painel de navegação, escolha Políticas de segurança.

   b. Na página de políticas do AWS Firewall Manager , selecione e edite seus grupos de segurança de auditoria e remova todas as referências à lista personalizada que você deseja excluir.

      Se você excluir uma lista gerenciada personalizada que está em uso em uma política de grupo de segurança de auditoria, a política que a está usando pode parar de funcionar.

3. No painel de navegação, escolha Listas de aplicativos ou Listas de protocolos, dependendo do tipo de lista que você deseja excluir.
4. Na página da lista, selecione a lista personalizada que você deseja excluir e escolha Excluir.

AWS WAF políticas

Em uma AWS WAF política do Firewall Manager, você especifica os grupos de AWS WAF regras que deseja usar em seus recursos. Quando você aplica a política, o Firewall Manager cria web ACLs em contas dentro do escopo da política, dependendo de como você configura o gerenciamento de web ACLs em sua política. Nas web ACLs criadas pela política, os gerentes de contas individuais podem adicionar regras e grupos de regras, além dos grupos de regras que você definiu por meio do Firewall Manager.

Como o Firewall Manager gerencia as web ACLs

O Firewall Manager cria ACLs da web com base em como você configura a configuração Gerenciar ACLs da web não associadas em sua política ou a `optimizeUnassociatedWebACL` configuração no tipo de SecurityServicePolicyDatadados na API.

Se você habilitar o gerenciamento de web ACLs não associadas, o Firewall Manager só criará web ACLs nas contas dentro do escopo da política somente se as web ACLs forem usadas por pelo menos um recurso. Se, a qualquer momento, uma conta entrar no escopo da política, o Firewall

Manager criará automaticamente uma web ACL na conta se pelo menos um recurso usar a web ACL. Quando você habilita o gerenciamento de web ACLs não associadas, o Firewall Manager executa uma limpeza única das web ACLs não associadas na sua conta. Durante a limpeza, o Firewall Manager ignora todas as web ACLs que você modificou após sua criação, por exemplo, se você adicionou um grupo de regras à web ACL ou modificou suas configurações. O processo de limpeza pode levar várias horas. Se um recurso deixar o escopo da política depois que o Firewall Manager criar uma web ACL, o Firewall Manager desassociará o recurso da web ACL, mas não limpará a web ACL não associada. O Firewall Manager só limpa web ACLs não associadas quando você habilita antes o gerenciamento de web ACLs não associadas em uma política.

Se você não habilitar essa opção, o Firewall Manager não gerenciará web ACLs não associadas, e o Firewall Manager criará automaticamente uma web ACL em cada conta que esteja dentro do escopo da política.

Amostragem e métricas CloudWatch

AWS Firewall Manager permite a amostragem e CloudWatch as métricas da Amazon para as ACLs da web e grupos de regras que ela cria para uma AWS WAF política.

Estrutura de nome da web ACL

Quando o Firewall Manager cria uma web ACL para a política, ele nomeia o `FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`* da web ACL. O timestamp em milissegundos UTC. Por exemplo, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Note**
>
> Se um recurso configurado com mitigação automática avançada de DDoS na camada de aplicação entrar no escopo de uma AWS WAF política, o Firewall Manager não conseguirá associar a Web ACL criada pela AWS WAF política ao recurso.

Grupos de regras em AWS WAF políticas

As ACLs da web gerenciadas pelas AWS WAF políticas do Firewall Manager contêm três conjuntos de regras. Esses conjuntos fornecem um nível mais alto de priorização para as regras e grupos de regras na web ACL:

- Primeiros grupos de regras, definidos por você na AWS WAF política do Firewall Manager. AWS WAF avalia esses grupos de regras primeiro.

- Regras e grupos de regras definidos pelos gerentes de conta nas web ACLs. O AWS WAF avalia quaisquer regras gerenciadas por conta ou grupos de regras a seguir.
- Últimos grupos de regras, definidos por você na AWS WAF política do Firewall Manager. AWS WAF avalia esses grupos de regras por último.

Dentro de cada um desses conjuntos de regras, AWS WAF avalia as regras e os grupos de regras normalmente, de acordo com suas configurações de prioridade dentro do conjunto.

Nos primeiros e últimos conjuntos de grupos de regras da política, é possível adicionar apenas grupos de regras. Você pode usar grupos de regras gerenciados, que as Regras AWS Gerenciadas e AWS Marketplace os vendedores criam e mantêm para você. Também é possível gerenciar e usar seus próprios grupos de regras. Para obter mais informações sobre todas essas ações, consulte AWS WAF grupos de regras.

Se quiser usar seus próprios grupos de regras, crie esses grupos antes de criar a política do Firewall Manager do AWS WAF . Para obter orientações, consulte Gerenciar seus próprios grupos de regras. Para usar uma regra personalizada individual, é necessário definir seu próprio grupo de regras, definir a regra nele e, depois, usar o grupo de regras na política.

O primeiro e o último grupos de AWS WAF regras que você gerencia por meio do Firewall Manager têm nomes que começam com `PREFMManaged-` ou`POSTFMManaged-`, respectivamente, seguidos pelo nome da política do Firewall Manager e pelo carimbo de data/hora da criação do grupo de regras, em milissegundos UTC. Por exemplo, `PREFMManaged-MyWAFPolicyName-1621880555123`.

Para obter informações sobre como AWS WAF avalia solicitações da web, consulteAvaliação de regras da web ACL e do grupo de regras.

Para obter o procedimento para criar uma AWS WAF política do Firewall Manager, consulteCriação de uma AWS Firewall Manager política para AWS WAF.

O Firewall Manager permite a amostragem e CloudWatch as métricas da Amazon para os grupos de regras que você define para a AWS WAF política.

Proprietários de contas individuais têm controle total sobre as métricas e a configuração de amostragem de qualquer regra ou grupo de regras que eles adicionem às web ACLs gerenciadas da política.

Configurando o registro em log para uma política AWS WAF

Você pode ativar o registro centralizado de suas AWS WAF políticas para obter informações detalhadas sobre o tráfego que é analisado pela sua ACL da web em sua organização. As informações nos registros incluem a hora em que AWS WAF recebeu a solicitação do seu AWS recurso, informações detalhadas sobre a solicitação e a ação da regra de que cada solicitação correspondeu de todas as contas dentro do escopo. Você pode enviar seus registros para um stream de dados do Amazon Data Firehose ou para um bucket do Amazon Simple Storage Service (S3). Para obter informações sobre AWS WAF registro, consulte Registrando AWS WAF tráfego de ACL da web o Guia do AWS WAF desenvolvedor.

> **Note**
>
> AWS Firewall Manager suporta essa opção para AWS WAFV2, não para AWS WAF Classic.

Tópicos

Destinos de logs

Esta seção descreve os destinos de registro que você pode escolher para enviar seus registros AWS WAF de políticas. Cada seção fornece orientações para configurar os logs para o tipo de destino e informações sobre qualquer comportamento específico para o tipo de destino. Depois de configurar seu destino de registro, você pode fornecer suas especificações à AWS WAF política do Firewall Manager para começar a fazer login nele.

O Firewall Manager não tem visibilidade das falhas de log depois de criar a configuração de registro em log. É sua responsabilidade verificar se a entrega de logs está funcionando conforme o esperado.

> **Note**
>
> O Firewall Manager não modifica nenhuma configuração de registro em log existente nas contas dos membros da sua organização.

Tópicos

Streams de dados do Amazon Data Firehose

Este tópico fornece informações para enviar seus registros de tráfego de ACL da web para um stream de dados do Amazon Data Firehose.

Quando você ativa o registro no Amazon Data Firehose, o Firewall Manager envia registros das ACLs da web da sua política para um Amazon Data Firehose onde você configurou um destino de armazenamento. Depois de ativar o registro, AWS WAF entrega os registros para cada Web ACL configurada, por meio do endpoint HTTPS do Kinesis Data Firehose, até o destino de armazenamento configurado. Antes de usá-lo, teste seu streaming de entrega para ter certeza de que ele tem throughput suficiente para acomodar os logs da sua organização. Para obter mais informações sobre como criar um Amazon Kinesis Data Firehose e analisar os registros armazenados, consulte O que é o Amazon Data Firehose?

Você deve ter as seguintes permissões para habilitar o registro em log com êxito com um Kinesis:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Quando você configura um destino de registro do Amazon Data Firehose em uma AWS WAF política, o Firewall Manager cria uma ACL da web para a política na conta do administrador do Firewall Manager da seguinte forma:

- O Firewall Manager cria a web ACL na conta do administrador do Firewall Manager, independentemente de a conta estar ou não no escopo da política.
- A web ACL tem o registro em logs ativado, com um nome de log `FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*, em que o timestamp é a hora UTC em que o log foi ativado para a web ACL, em milissegundos. Por exemplo, `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. A web ACL não tem grupos de regras nem recursos associados.
- Você é cobrado pela ACL da web de acordo com as diretrizes AWS WAF de preços. Para obter mais informações, consulte Preços do AWS WAF.

- O Firewall Manager exclui a web ACL quando você exclui a política.

Para obter mais informações sobre funções vinculadas ao serviço e a permissão do `iam:CreateServiceLinkedRole`, consulte Usando funções vinculadas a serviços para AWS WAF.

Para obter mais informações sobre como criar seu stream de entrega, consulte Creating an Amazon Data Firehose Delivery Stream.

Buckets do Amazon Simple Storage Service

Este tópico fornece informações para enviar seus logs de tráfego da web ACL para um bucket do Amazon S3.

O bucket que você escolher como destino de registro em log deve pertencer a uma conta de administrador do Firewall Manager. Para obter informações sobre os requisitos para criar seu bucket do Amazon S3 para requisitos de registro em log e nomenclatura de buckets, consulte Amazon Simple Storage Service no Guia do desenvolvedor AWS WAF .

Consistência eventual

Quando você faz alterações AWS WAF nas políticas configuradas com um destino de registro do Amazon S3, o Firewall Manager atualiza a política do bucket para adicionar as permissões necessárias para o registro. Ao fazer isso, o Firewall Manager segue os modelos de last-writer-wins semântica e consistência de dados que o Amazon Simple Storage Service segue. Se você fizer simultaneamente várias atualizações de políticas em um destino do Amazon S3 no console do Firewall Manager ou por meio PutPolicyda API, algumas permissões podem não ser salvas. Para obter mais informações sobre modelo de consistência de dados do Amazon S3, consulte Modelo de consistência de dados do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Permissões para publicar logs em um bucket do Amazon S3

Configurar o registro de tráfego de ACL da web para um bucket do Amazon S3 em AWS WAF uma política requer as seguintes configurações de permissões. O Firewall Manager atribui automaticamente essas permissões ao seu bucket do Amazon S3 quando você configura o Amazon S3 como seu destino de registro em log para dar ao serviço permissão para publicar registros em log no bucket. Se você quiser gerenciar um acesso mais refinado aos seus recursos de registro em log e do Firewall Manager, você mesmo pode definir essas permissões. Para obter mais informações sobre gerenciamento de permissões, consulte Gerenciamento de acesso para recursos da AWS

no Guia do usuário do IAM. Para obter informações sobre as políticas AWS WAF gerenciadas, consulteAWS políticas gerenciadas para AWS WAF.

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

Para evitar problema de “confused deputy” entre serviços, você pode adicionar as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` e as chaves de contexto à política do seu bucket. Para adicionar essas chaves, você pode modificar a política que o Firewall Manager cria para você ao configurar o destino do registro em log ou, se quiser um controle refinado, pode criar sua própria política. Se você adicionar essas condições à sua política de destino de registro em log, o Firewall Manager não validará nem monitorará as proteções de “confused deputy”. Para obter mais informações sobre o problema de “confused deputy”, consulte O problema de “confused deputy”, no Guia do usuário do IAM.

Quando você adiciona a `sourceAccount` às propriedades `sourceArn` de adição, isso aumenta o tamanho da política do bucket. Se você estiver adicionando uma longa lista de `sourceAccount` às propriedades `sourceArn` de adição, tome cuidado para não exceder a cota de tamanho da política de bucket do Amazon S3.

O exemplo a seguir mostra como evitar o problema de "confused deputy" usando as chaves de contexto de condição globais `aws:SourceArn` e `aws:SourceAccount` na política do seu bucket. *`member-account-id`*Substitua pelos IDs de conta dos membros da sua organização.

```
{
   "Version":"2012-10-17",
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
```

```
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                    "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id-1:*",
                  "arn:aws:logs:*:member-account-id-2:*"
               ]
            }
         }
      }
   ]
}
```

Criptografia no lado do servidor de bucket do Amazon S3

Você pode habilitar a criptografia do lado do servidor do Amazon S3 ou usar uma chave gerenciada pelo AWS Key Management Service cliente em seu bucket do S3. Se você optar por usar a criptografia padrão do Amazon S3 em seu bucket do Amazon S3 AWS WAF para registros, não precisará realizar nenhuma ação especial. No entanto, se você optar por usar uma chave de criptografia fornecida pelo cliente para criptografar seus dados do Amazon S3 em repouso, você deve adicionar a seguinte declaração de permissão à sua política de chaves: AWS Key Management Service

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
```

```
            ],
            "Resource": "*"
}
```

Para obter mais informações sobre o uso de chaves de criptografia fornecidas pelo cliente com o Amazon S3, consulte Usando criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-KMS) no Guia do usuário do Amazon Simple Storage Service.

Habilitar o log

O procedimento a seguir descreve como habilitar o registro em log para uma AWS WAF política no console do Firewall Manager.

Para habilitar o registro em log para uma AWS WAF política

1. Antes de habilitar o registro em log, você deve configurar seus recursos de destino de registro em log da seguinte forma:

   - Amazon Kinesis Data Streams — Crie um Amazon Data Firehose usando sua conta de administrador do Firewall Manager. Use um nome que comece com o prefixo `aws-waf-logs-`. Por exemplo, `aws-waf-logs-firewall-manager-central`. Crie o Data Firehose com uma origem PUT e na região em que você está operando. Se você estiver capturando registros para a Amazon CloudFront, crie a mangueira de incêndio no Leste dos EUA (Norte da Virgínia). Antes de usá-lo, teste seu streaming de entrega para ter certeza de que ele tem throughput suficiente para acomodar os logs da sua organização. Para obter mais informações, consulte Criar um fluxo de entrega do Amazon Data Firehose.
   - Buckets do Amazon Simple Storage Service: crie um bucket do Amazon S3 de acordo com as diretrizes do tópico Amazon Simple Storage Service no Guia do desenvolvedor da AWS WAF . Você também deve configurar seu bucket do Amazon S3 com as permissões listadas em Permissões para publicar logs em um bucket do Amazon S3 .

2. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

> **Note**
>
> Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

3. No painel de navegação, escolha Políticas de segurança.
4. Escolha a AWS WAF política para a qual você deseja habilitar o registro. Para obter mais informações sobre registro em log do AWS WAF , consulte Registrando AWS WAF tráfego de ACL da web.
5. Na guia Detalhes da política, na seção Regras da política, escolha Editar.
6. Em Configuração de registro em log, escolha Ativar registro em log para ativar o registro em log. O registro em log fornece informações detalhadas sobre o tráfego que é analisado pela sua web ACL. Escolha o Destino de registro em log e, em seguida, escolha o destino de registro em log que você configurou. Você deve escolher um destino de registro em log cujo nome comece com `aws-waf-logs-`. Para obter informações sobre como configurar um destino de AWS WAF registro, consulteConfigurando o registro em log para uma política AWS WAF.
7. (Opcional) Se você não deseja que determinados campos e seus valores sejam incluídos nos logs, edite esses campos. Selecione o campo para editar e, em seguida, selecione Adicionar. Repita conforme necessário para editar campos adicionais. Os campos editados são exibidos como `REDACTED` nos logs. Por exemplo, se você editar o campo URI, o campo URI nos logs será `REDACTED`.
8. (Opcional) Se você não quiser enviar todas as solicitações para os logs, adicione seus critérios e comportamento de filtragem. Em Filtrar logs, para cada filtro que você deseja aplicar, escolha Adicionar filtro, escolha seus critérios de filtragem e especifique se deseja manter ou eliminar solicitações que correspondam aos critérios. Ao terminar de adicionar filtros, se necessário, modifique o Comportamento de registro de logs padrão. Para obter mais informações, consulte Configuração de registro do Web ACL no AWS WAF Guia do desenvolvedor.
9. Escolha Próximo.
10. Revise suas configurações e escolha Salvar para salvar suas alterações na política.

Como desabilitar o registro

O procedimento a seguir descreve como desabilitar o registro de uma AWS WAF política no console do Firewall Manager.

Para desativar o registro em log de uma AWS WAF política

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha a AWS WAF política para a qual você deseja desativar o registro.
4. Na guia Detalhes da política, na seção Regras da política, escolha Editar.
5. Em Status da configuração de registro em log, escolha Desativado.
6. Escolha Próximo.
7. Revise suas configurações e escolha Salvar para salvar suas alterações na política.

AWS Shield Advanced políticas

Em uma AWS Shield política do Firewall Manager, você escolhe os recursos que deseja proteger. Quando você aplica a política com a correção automática ativada, para cada recurso no escopo que ainda não está associado a uma ACL da AWS WAF web, o Firewall Manager associa uma ACL da web vazia. AWS WAF A web ACL vazia é usada para fins de monitoramento do Shield. Se você então associar qualquer outra web ACL ao recurso, o Firewall Manager removerá a associação vazia da web ACL.

> **Note**
>
> Quando um recurso que está no escopo de uma AWS WAF política entra no escopo de uma política Shield Advanced configurada com mitigação automática de DDoS na camada de aplicação, o Firewall Manager aplica a proteção Shield Advanced somente após associar a Web ACL criada pela política. AWS WAF

Como AWS Firewall Manager gerencia ACLs da web não associadas nas políticas do Shield

Você pode configurar se o Firewall Manager gerencia ACLs da Web não associadas para você por meio da configuração Gerenciar ACLs da Web não associadas na sua política ou da `optimizeUnassociatedWebACLs` configuração do tipo de SecurityServicePolicyDatadados na API. Se você habilitar o gerenciamento de web ACLs não associadas em sua política, o Firewall Manager criará web ACLs nas contas dentro do escopo da política somente se as web ACLs forem usadas por pelo menos um recurso. Se, a qualquer momento, uma conta entrar no escopo da política, o Firewall Manager criará automaticamente uma web ACL na conta se pelo menos um recurso usar a web ACL.

Quando você habilita o gerenciamento de web ACLs não associadas, o Firewall Manager executa uma limpeza única das web ACLs não associadas na sua conta. O processo de limpeza pode levar várias horas. Se um recurso sair do escopo da política depois que o Firewall Manager criar uma web ACL, o Firewall Manager não desassociará o recurso da web ACL. Se você quiser que o Firewall Manager limpe a web ACL, primeiro desassocie manualmente os recursos da web ACL e, em seguida, habilite a opção gerenciar web ACLs não associadas em sua política.

Se você não habilitar essa opção, o Firewall Manager não gerenciará web ACLs não associadas, e o Firewall Manager criará automaticamente uma web ACL em cada conta que esteja dentro do escopo da política.

Como AWS Firewall Manager gerencia as mudanças de escopo nas políticas da Shield

Contas e recursos podem sair do escopo de uma política AWS Firewall Manager do Shield Advanced devido a várias alterações, como alterações nas configurações do escopo da política, alterações nas tags em um recurso e a remoção de uma conta de uma organização. Para obter informações gerais sobre as configurações do escopo da política, consulte AWS Firewall Manager escopo da política.

Com uma política AWS Firewall Manager Shield Advanced, se uma conta ou recurso sair do escopo, o Firewall Manager interrompe o monitoramento da conta ou do recurso.

Se uma conta sair do escopo ao ser removida da organização, ela continuará inscrita no Shield Advanced. Como a conta não faz mais parte da família de faturamento consolidado, a conta terá uma taxa de assinatura pro-rata do Shield Advanced. Por outro lado, uma conta que está fora do escopo, mas permanece na organização, não incorre em taxas adicionais.

Se um recurso sair do escopo, ele continuará protegido pelo Shield Advanced e continuará incorrendo em cobranças de transferência de dados do Shield Advanced.

Mitigação automática de DDoS na camada de aplicação

Ao aplicar uma política do Shield Advanced às CloudFront distribuições da Amazon ou aos Application Load Balancers, você tem a opção de configurar a mitigação automática de DDoS da camada de aplicação do Shield Advanced na política.

Para obter informações sobre a mitigação automática do Shield Advanced, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

A mitigação automática de DDoS da camada de aplicativo Shield Advanced apresenta os seguintes requisitos:

- A mitigação automática de DDoS na camada de aplicação funciona somente com CloudFront distribuições da Amazon e Application Load Balancers.

  Se aplicar sua política Shield Advanced às CloudFront distribuições da Amazon, você pode escolher essa opção para as políticas do Shield Advanced que você cria para a região global. Ao aplicar proteções aos Application Load Balancers, você pode aplicar a política a qualquer região compatível com o Firewall Manager.
- A mitigação automática de DDoS na camada de aplicativo funciona somente com ACLs da web que foram criadas usando a versão mais recente do (v2). AWS WAF

  Por isso, se você tiver uma política que usa ACLs web AWS WAF clássicas, você precisa substituir a política por uma nova política, que usará automaticamente a versão mais recente da AWS WAF, ou fazer com que o Firewall Manager crie uma nova versão de ACLs da web para sua política existente e passe a usá-las. Para obter mais informações sobre essas opções, consulte Substitua as ACLs da web AWS WAF clássicas pelas ACLs da web da versão mais recente.

Configuração de mitigação automática

A opção de mitigação automática de DDoS na camada de aplicativo para as políticas Shield Advanced do Firewall Manager aplica a funcionalidade de mitigação automática do Shield Advanced às contas e recursos dentro do escopo de sua política. Para obter informações sobre esse atributo do Shield Advanced, consulte Mitigação automática de DDoS da camada de aplicação do Shield Advanced.

Você pode optar por ativar ou desativar a mitigação automática do Firewall Manager para CloudFront as distribuições ou os Application Load Balancers que estão no escopo da política, ou pode optar por fazer com que a política ignore as configurações de mitigação automática do Shield Advanced:

- Habilitar: se você optar por habilitar a mitigação automática, você também especifica se as regras de mitigação do Shield Advanced devem contar ou bloquear as solicitações da web correspondentes. O Firewall Manager marcará os recursos dentro do escopo como não compatíveis se eles não tiverem a mitigação automática habilitada ou estiverem usando uma ação de regra que não corresponda à especificada para a política. Se você configurar a política para remediação automática, o Firewall Manager atualizará os recursos não compatíveis conforme o necessário.
- Desabilitar: se você optar por desabilitar a mitigação automática, o Firewall Manager marcará os recursos dentro do escopo como não compatíveis se eles tiverem a mitigação automática habilitada. Se você configurar a política para remediação automática, o Firewall Manager atualizará os recursos não compatíveis conforme o necessário.
- Ignorar: se você optar por ignorar a mitigação automática, o Firewall Manager não considerará nenhuma das configurações de mitigação automática em sua política Shield ao realizar atividades de remediação da política. Essa configuração permite controlar a mitigação automática por meio do Shield Advanced, sem que essas configurações sejam substituídas pelo Firewall Manager. Essa configuração não se aplica a nenhum recurso de Classic Load Balancers ou IPs elásticos gerenciados pelo Shield Advanced, porque o Shield Advanced atualmente não oferece suporte à mitigação automática L7 para esses recursos.

Substitua as ACLs da web AWS WAF clássicas pelas ACLs da web da versão mais recente

A mitigação automática de DDoS na camada de aplicativo funciona somente com ACLs da web que foram criadas usando a versão mais recente do (v2). AWS WAF

Para determinar a versão da web ACL para sua política Shield Advanced, consulte Determinar a versão usada por uma política do Shield Advanced AWS WAF.

Se você quiser usar a mitigação automática em sua política Shield Advanced e sua política atualmente usa ACLs web AWS WAF clássicas, você pode criar uma nova política Shield Advanced para substituir a atual ou usar as opções descritas nesta seção para substituir ACLs da web de versões anteriores por novas ACLs da web (v2) dentro da política atual do Shield Advanced. Novas políticas sempre criam ACLs da web usando a versão mais recente do AWS WAF. Se você substituir a política inteira, ao excluí-la, você também poderá fazer com que o Firewall Manager exclua todas

as web ACLs da versão anterior. O restante desta seção descreve suas opções para substituir as web ACLs dentro de sua política existente.

Quando você modifica uma política existente do Shield Advanced para CloudFront recursos da Amazon, o Firewall Manager pode criar automaticamente uma nova ACL web vazia AWS WAF (v2) para a política, em qualquer conta dentro do escopo que ainda não tenha uma ACL web v2. Quando o Firewall Manager cria uma nova ACL da Web, se a política já tiver uma ACL da Web AWS WAF Clássica na mesma conta, o Firewall Manager configura a nova versão da ACL da Web com a mesma configuração de ação padrão da ACL da Web existente. Se não houver nenhuma ACL da Web AWS WAF Clássica existente, o Firewall Manager define a ação padrão como Allow na nova ACL da Web. Depois que o Firewall Manager criar uma nova web ACL, você poderá personalizá-la conforme necessário por meio do console do AWS WAF .

Quando você escolhe qualquer uma das seguintes opções de configuração de política, o Firewall Manager cria novas web ACLs (v2) para contas dentro do escopo que ainda não as têm:

- Quando você habilita ou desabilita a mitigação automática de DDoS na camada de aplicativo. Somente essa opção faz com que o Firewall Manager crie as novas web ACLs e não substitua nenhuma associação existente de web ACL AWS WAF Classic nos recursos dentro do escopo da política.
- Quando você escolhe a ação política de remediação automática e escolhe a opção de substituir ACLs da web AWS WAF clássicas por ACLs da web AWS WAF (v2). Você pode optar por substituir as web ACLs de versões anteriores, independentemente de suas opções de configuração para mitigação automática de DDoS na camada de aplicativo.

  Quando você escolhe a opção de substituição, o Firewall Manager cria a nova versão das web ACLs conforme necessário e, em seguida, faz o seguinte para os recursos dentro do escopo da política:

  - Se um recurso estiver associado a uma web ACL de qualquer outra política ativa do Firewall Manager, o Firewall Manager deixará a associação de lado.
  - Em qualquer outro caso, o Firewall Manager remove qualquer associação com uma ACL da web AWS WAF clássica e associa o recurso à ACL da web da política AWS WAF (v2).

Você pode optar por fazer com que o Firewall Manager substitua as web ACLs da versão anterior pela nova versão das web ACLs quando quiser. Se você já personalizou as web ACLs AWS WAF Classic da política, você pode atualizar a nova versão das web ACLs para configurações comparáveis antes de escolher que o Firewall Manager execute a etapa de substituição.

Você pode acessar qualquer versão da Web ACL para uma política por meio do console da mesma versão ou Classic. AWS WAF AWS WAF

O Firewall Manager não exclui nenhuma ACLs web AWS WAF clássica substituída até que você exclua a política em si. Depois que as ACLs web AWS WAF clássicas não forem mais usadas pela política, você poderá excluí-las se quiser.

Determinar a versão usada por uma política do Shield Advanced AWS WAF

Você pode determinar qual versão da política AWS WAF do Firewall Manager Shield Advanced usa observando as chaves de parâmetros na regra AWS Config vinculada ao serviço da política. Se a AWS WAF versão em uso for a mais recente, as chaves de parâmetros incluirão `policyId` `webAclArn` e. Se for a versão anterior, AWS WAF Classic, as chaves de parâmetros incluem `webAclId` `resourceTypes` e.

A AWS Config regra lista apenas as chaves das ACLs da web que a política está usando atualmente com recursos dentro do escopo.

Para determinar qual versão da política do AWS WAF Firewall Manager Shield Advanced usa

1. Recupere a ID da política Shield Advanced:

   a. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   b. No painel de navegação, escolha Políticas de segurança.

   c. Escolha a região para a política. Para CloudFront distribuições, isso é`Global`.

   d. Encontre a política que você deseja e copie o valor de sua ID de política.

      ID do exemplo de política: `1111111-2222-3333-4444-a55aa5aaa555`.

2. Crie o nome da AWS Config regra da política anexando o ID da política à string`FMManagedShieldConfigRule`.

   Exemplo de nome de AWS Config regra:`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. Pesquise nos parâmetros da AWS Config regra associada as chaves chamadas `policyId` e`webAclArn`:

a. Abra o AWS Config console em https://console.aws.amazon.com/config/.

b. No painel de navegação, escolha Rules.

c. Encontre o nome da AWS Config regra da política do Firewall Manager na lista e selecione-a. A página da regra é aberta.

d. Em Detalhes da regra, na seção Parâmetros, veja as chaves. Se você encontrar chaves com os nomes `policyId` e `webAclArn`, a política usa web ACLs que foram criadas usando a versão mais recente do AWS WAF. Se você encontrar chaves com o nome `webAclId` `eresourceTypes`, a política usa ACLs da web que foram criadas usando a versão anterior, AWS WAF Classic.

Políticas de grupo de segurança

Você pode usar políticas AWS Firewall Manager de grupo de segurança para gerenciar grupos de segurança da Amazon Virtual Private Cloud para sua organização em AWS Organizations. Você pode aplicar políticas de grupo de segurança controladas centralmente a toda a organização ou a um subconjunto selecionado de suas contas e recursos. Você também pode monitorar e gerenciar as políticas de grupo de segurança que estão em uso na organização com políticas de grupo de segurança de auditoria e uso.

O Firewall Manager mantém continuamente suas políticas e as aplica a contas e recursos à medida que são adicionados ou atualizados em toda a organização. Para obter informações sobre AWS Organizations, consulte o Guia AWS Organizations do usuário.

Para obter mais informações sobre como modificar um grupo de segurança da Amazon Virtual Private Cloud, consulte Grupos de segurança para a sua VPC no Guia do usuário da Amazon VPC.

Você pode usar políticas de grupo de segurança do Firewall Manager para fazer o seguinte em toda a sua organização da AWS :

- Aplique grupos de segurança comuns a contas e recursos especificados.
- Audite as regras de grupo de segurança, para localizar e corrigir regras não compatíveis.
- Audite o uso de grupos de segurança, para limpar grupos de segurança não utilizados e redundantes.

Esta seção aborda como as políticas de grupos de segurança do Firewall Manager funcionam e fornece orientações para usá-las. Para obter os procedimentos de criação de políticas de grupo de segurança, consulte Criação de uma AWS Firewall Manager política.

Políticas de grupo de segurança comuns

Com uma política de grupo de segurança comum, o Firewall Manager fornece uma associação controlada centralmente de grupos de segurança a contas e recursos em toda a sua organização. Você especifica onde e como aplicar a política em sua organização.

Você pode aplicar políticas de grupo de segurança comuns aos seguintes tipos de recursos:

- Instância do Amazon Elastic Compute Cloud (Amazon EC2)
- Interface de rede elástica
- Application Load Balancer
- Classic Load Balancer

Para obter orientação sobre como criar uma política de grupo de segurança comum usando o console, consulte Criar uma política de grupo de segurança comum.

VPCs compartilhadas

Nas configurações de escopo de política para uma política de grupo de segurança comum, é possível optar por incluir VPCs compartilhadas. Essa opção inclui VPCs pertencentes a outra conta e compartilhadas com uma conta dentro do escopo. As VPCs que pertencem a contas no escopo são sempre incluídas. Para obter mais informações sobre VPCs compartilhadas, consulte Como trabalhar com VPCs compartilhadas no Guia do usuário da Amazon VPC.

As seguintes advertências se aplicam à inclusão de VPCs compartilhadas. Essas são uma adição às advertências gerais para políticas de grupo de segurança em Advertências e limitações da política de grupo de segurança.

- O Firewall Manager replica o grupo de segurança primário para as VPCs de cada conta no escopo. Para uma VPC compartilhada, o Firewall Manager replica o grupo de segurança primário uma vez para cada conta no escopo com a qual a VPC é compartilhada. Isso pode resultar em várias réplicas em uma única VPC compartilhada.
- Ao criar uma VPC compartilhada, você só a verá representada nos detalhes da política de grupo de segurança do Firewall Manager depois de criar pelo menos um recurso na VPC que esteja dentro do escopo da política.

- Quando você desabilita VPCs compartilhadas em uma política que tinha VPCs compartilhadas habilitadas, nas VPCs compartilhadas, o Firewall Manager exclui os grupos de segurança de réplica que não estão associados a nenhum recurso. O Firewall Manager mantém os grupos de segurança de réplica restantes no lugar, mas para de gerenciá-los. A remoção desses grupos de segurança restantes requer gerenciamento manual em cada instância da VPC compartilhada.

Grupos de segurança primários

Para cada política de grupo de segurança comum, você AWS Firewall Manager fornece um ou mais grupos de segurança primários:

- Os grupos de segurança primários devem ser criados pela conta de administrador do Firewall Manager e podem residir em qualquer instância da Amazon VPC na conta.
- Você gerencia seus grupos de segurança primários por meio da Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon VPC.
- Você pode nomear um ou mais grupos de segurança como primários para uma política de grupo de segurança do Firewall Manager. Por padrão, o número de grupos de segurança permitidos em uma política é um, mas você pode enviar uma solicitação para aumentá-lo. Para mais informações, consulte AWS Firewall Manager cotas.

Configurações de regras de política

Você pode escolher um ou mais dos seguintes comportamentos de controle de alteração para os grupos de segurança e recursos de sua política de grupo de segurança comum:

- Identifique e relate quaisquer alterações feitas pelos usuários locais para grupos de segurança de réplica.
- Desassocie quaisquer outros grupos de segurança dos AWS recursos que estão dentro do escopo da política.
- Distribua tags do grupo primário para os grupos de segurança da réplica.

> **Important**
>
> O Firewall Manager não distribuirá tags de sistema adicionadas pelos AWS serviços aos grupos de segurança de réplicas. As tags do sistema começam com o prefixo `aws:`. Além disso, o Firewall Manager não atualizará as tags dos grupos de segurança existentes nem

criará novos grupos de segurança se a política tiver tags que entrem em conflito com a política de tags da organização. Para obter informações sobre políticas de tags, consulte Políticas de tags no Guia AWS Organizations do usuário.

- Distribua referências do grupo de segurança do grupo primário para os grupos de segurança de réplica.

  Isso permite que você estabeleça facilmente regras comuns de referência de grupo de segurança em todos os recursos do escopo para instâncias associadas à VPC do grupo de segurança especificado. Quando você ativa essa opção, o Firewall Manager só propaga as referências do grupo de segurança se os grupos de segurança fizerem referência a grupos de segurança pares na Amazon Virtual Private Cloud. Se os grupos de segurança de réplica não referenciarem corretamente o grupo de segurança de mesmo nível, o Firewall Manager marcará esses grupos de segurança replicados como não compatíveis. Para obter informações sobre como referenciar grupos de segurança de mesmo nível na Amazon VPC, consulte Atualizar seus grupos de segurança para referenciar grupos de segurança de mesmo nível no Guia de emparelhamento da Amazon VPC.

  Se você não habilitar essa opção, o Firewall Manager não propagará referências de grupos de segurança para os grupos de segurança de réplica. Para obter informações sobre emparelhamento de VPC na Amazon VPC, consulte o Guia de emparelhamento de VPC da Amazon.

Criação e gerenciamento de políticas

Quando você cria sua política de grupo de segurança comum, o Firewall Manager replica os grupos de segurança primários para cada instância da Amazon VPC dentro do escopo da política e associa os grupos de segurança replicados a contas e recursos que estão no escopo da política. Quando você modifica um grupo de segurança primário, o Firewall Manager propaga a alteração para as réplicas.

Ao excluir uma política de grupo de segurança comum, você pode escolher se deseja limpar os recursos criados pela política. Para grupos de segurança comuns do Firewall Manager, esses recursos são os grupos de segurança de réplica. Escolha a opção de limpeza, a menos que você queira gerenciar manualmente cada réplica individual após a política ser excluída. Para a maioria das situações, escolher a opção de limpeza é a abordagem mais simples.

Como as réplicas são gerenciadas

Os grupos de segurança de réplica nas instâncias da Amazon VPC são gerenciados como outros grupos de segurança da Amazon VPC. Para obter mais informações, consulte Grupos de segurança para sua VPC no Guia do usuário da Amazon VPC.

Políticas de grupo de segurança de auditoria de conteúdo

Use políticas de grupo de segurança de auditoria de AWS Firewall Manager conteúdo para auditar e aplicar ações de política às regras que estão em uso nos grupos de segurança da sua organização. As políticas de grupo de segurança de auditoria de conteúdo se aplicam a todos os grupos de segurança criados pelo cliente em uso na sua AWS organização, de acordo com o escopo definido na política.

Para obter orientação sobre como criar uma política de grupo de segurança de auditoria de conteúdo usando o console, consulte Criar uma política de grupo de segurança de auditoria de conteúdo.

Tipo de recurso do escopo da política

Você pode aplicar políticas de grupo de segurança de auditoria de conteúdo aos seguintes tipos de recursos:

- Instância do Amazon Elastic Compute Cloud (Amazon EC2)
- Interface de rede elástica
- Grupo de segurança da Amazon VPC

Os grupos de segurança serão considerados no escopo da política se estiverem explicitamente no escopo ou se estiverem associados a recursos que estão no escopo.

Opções de regras de política

Você pode usar regras de política gerenciadas ou regras de política personalizadas para cada política de auditoria de conteúdo, mas não ambas.

- Regras de políticas gerenciadas: em uma política com regras gerenciadas, você pode usar listas de aplicativos e protocolos para controlar quais regras o Firewall Manager audita e marca como compatíveis ou não compatíveis. Você pode usar listas gerenciadas pelo Firewall Manager. Você também pode criar e usar suas próprias listas de aplicativos e protocolos. Para obter informações sobre esses tipos de listas e suas opções de gerenciamento para listas personalizadas, consulte Listas gerenciadas.

- Regras de política personalizadas: em uma política com regras de política personalizadas, você especifica um grupo de segurança existente como o grupo de segurança de auditoria para sua política. Você pode usar as regras do grupo de segurança de auditoria como um modelo que define as regras que o Firewall Manager audita e marca como compatíveis ou não compatíveis.

Grupos de segurança de auditoria

Você deve criar grupos de segurança de auditoria usando sua conta de administrador do Firewall Manager antes de poder usá-los em sua política. Você pode gerenciar grupos de segurança por meio da Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon VPC.

Um grupo de segurança que você usa para uma política de grupo de segurança de auditoria de conteúdo é usado pelo Firewall Manager apenas como referência de comparação para os grupos de segurança que estão no escopo da política. O Firewall Manager não o associa a nenhum recurso em sua organização.

A maneira como você define as regras no grupo de segurança de auditoria depende de sua escolha nas configurações de regras de política:

- Regras de política gerenciadas: para configurações de regras de política gerenciadas, você usa um grupo de segurança de auditoria para substituir outras configurações na política, para permitir ou negar explicitamente regras que, de outra forma, poderiam ter outro resultado de conformidade.
  - Se você optar por sempre permitir as regras definidas no grupo de segurança de auditoria, qualquer regra que corresponda a uma definida no grupo de segurança de auditoria será considerada em conformidade com a política, independentemente das outras configurações de política.
  - Se você optar por sempre negar as regras definidas no grupo de segurança de auditoria, qualquer regra que corresponda a uma definida no grupo de segurança de auditoria será considerada em não conformidade com a política, independentemente das outras configurações de política.
- Regras de política personalizadas: para configurações de regras de política personalizadas, o grupo de segurança de auditoria fornece o exemplo do que é aceitável ou não aceitável nas regras de grupo de segurança dentro do escopo:
  - Se você optar por permitir o uso das regras, todos os grupos de segurança no escopo deverão ter somente regras que estejam dentro do intervalo permitido das regras do grupo de segurança

de auditoria da política. Nesse caso, as regras do grupo de segurança da política fornecem o exemplo do que é aceitável fazer.

- Se você optar por negar o uso das regras, todos os grupos de segurança no escopo deverão ter somente regras que não estejam dentro do intervalo permitido das regras do grupo de segurança de auditoria da política. Nesse caso, o grupo de segurança da política fornece o exemplo do que não é aceitável fazer.

Criação e gerenciamento de políticas

Quando você cria uma política de grupo de segurança de auditoria, precisa ter a correção automática desativada. A prática recomendada é rever os efeitos da criação de políticas antes de habilitar a correção automática. Depois de analisar os efeitos esperados, você pode editar a política e habilitar a correção automática. Quando a correção automática está habilitada, o Firewall Manager atualiza ou remove regras que não são compatíveis em grupos de segurança no escopo.

Grupos de segurança afetados por uma política de grupo de segurança de auditoria

Todos os grupos de segurança em sua organização que são criados pelo cliente estão qualificados para estar no escopo de uma política de grupo de segurança de auditoria.

Os grupos de segurança de réplica não são criados pelo cliente e, portanto, não são qualificados para estar diretamente no escopo de uma política de grupo de segurança de auditoria. No entanto, eles podem ser atualizados como resultado das atividades de correção automática da política. O grupo de segurança primário de uma política de grupo de segurança comum é criado pelo cliente e pode estar no escopo de uma política de grupo de segurança de auditoria. Se uma política de grupo de segurança de auditoria fizer alterações em um grupo de segurança primário, o Firewall Manager propagará automaticamente essas alterações para as réplicas.

Políticas de grupo de segurança de auditoria de uso

Use políticas de grupo de segurança de auditoria de AWS Firewall Manager uso para monitorar sua organização em busca de grupos de segurança redundantes e não utilizados e, opcionalmente, realizar a limpeza. Quando você habilita a correção automática dessa política, o Firewall Manager faz o seguinte:

1. Consolida grupos de segurança redundantes, se você tiver escolhido essa opção.
2. Remove grupos de segurança não utilizados, se você tiver escolhido essa opção.

Você pode aplicar políticas de grupo de segurança de auditoria de uso ao seguinte tipo de recurso:

- Grupo de segurança da Amazon VPC

Para obter orientação sobre como criar uma política de grupo de segurança de auditoria de uso usando o console, consulte Criar uma política de grupo de segurança de auditoria de uso.

Como o Firewall Manager detecta e corrige grupos de segurança redundantes

Para que os grupos de segurança sejam considerados redundantes, eles devem ter exatamente as mesmas regras definidas e estar na mesma instância da Amazon VPC.

Para corrigir um conjunto de grupo de segurança redundante, o Firewall Manager seleciona um dos grupos de segurança do conjunto para manter e o associa a todos os recursos associados aos outros grupos de segurança do conjunto. Em seguida, o Firewall Manager desassocia os outros grupos de segurança dos recursos aos quais eles estavam associados, o que os torna inutilizados.

> **Note**
>
> Se você também optou por remover grupos de segurança não utilizados, o Firewall Manager fará isso em seguida. Isso pode resultar na remoção dos grupos de segurança que estão no conjunto redundante.

Como o Firewall Manager detecta e corrige grupos de segurança não utilizados

O Firewall Manager considera que um grupo de segurança não é usado se ambas as afirmações a seguir forem verdadeiras:

- O grupo de segurança não é usado por nenhuma instância do Amazon EC2 ou pela interface de rede elástica do Amazon EC2.
- O Firewall Manager não recebeu um item de configuração dentro do número de minutos especificado no período de tempo da regra de política.

O período de tempo da regra de política tem uma configuração padrão de zero minutos, mas você pode aumentar o tempo até 365 dias (525.600 minutos) para ter tempo de associar novos grupos de segurança aos recursos.

> **Important**
>
> Se você especificar um número de minutos diferente do valor padrão de zero, deverá habilitar relacionamentos indiretos em AWS Config. Caso contrário, suas políticas de grupo de segurança de auditoria de uso não funcionarão conforme o esperado. Para obter informações sobre relacionamentos indiretos em AWS Config, consulte Relacionamentos indiretos AWS Config no Guia do AWS Config desenvolvedor.

O Firewall Manager corrige grupos de segurança não utilizados excluindo-os da sua conta de acordo com suas configurações de regras, se possível. Se o Firewall Manager não conseguir excluir um grupo de segurança, ele o marcará como não compatível com a política. O Firewall Manager não pode excluir um grupo de segurança referenciado por outro grupo de segurança.

O tempo da remediação varia de acordo com o uso da configuração padrão do período de tempo ou de uma configuração personalizada:

- Período de tempo definido como zero, o padrão — Com essa configuração, um grupo de segurança é considerado não utilizado assim que não está sendo usado por uma instância do Amazon EC2 ou por uma interface de rede elástica.

  Para essa configuração de período zero, o Firewall Manager corrige o grupo de segurança imediatamente.
- Período de tempo maior que zero — Com essa configuração, um grupo de segurança é considerado não utilizado quando não está sendo usado por uma instância do Amazon EC2 ou por uma interface de rede elástica e o Firewall Manager não recebeu um item de configuração dentro do número especificado de minutos.

  Para a configuração de período de tempo diferente de zero, o Firewall Manager corrige o grupo de segurança depois que ele permanece no estado não utilizado por 24 horas.

Especificação de conta padrão

Quando você cria uma política de grupo de segurança de auditoria de uso por meio do console, o Firewall Manager escolhe Excluir as contas especificadas e incluir todas as outras automaticamente. O serviço coloca a conta de administrador do Firewall Manager na lista a ser excluída. Esta é a abordagem recomendada e permite que você gerencie manualmente os grupos de segurança que pertencem à conta de administrador do Firewall Manager.

Práticas recomendadas para políticas de grupo de segurança

Esta seção lista recomendações para gerenciar grupos de segurança usando o AWS Firewall Manager.

Excluir a conta de administrador do Firewall Manager

Ao definir o escopo da política, exclua a conta de administrador do Firewall Manager. Quando você cria uma política de grupo de segurança de auditoria de uso por meio do console, essa é a opção padrão.

Comece com a correção automática desabilitada

Para políticas de grupo de segurança de auditoria de conteúdo ou uso, comece com a correção automática desativada. Revise as informações de detalhes da política para determinar os efeitos que a correção automática teria. Quando você estiver satisfeito com as alterações, edite a política para habilitar a correção automática.

Evite conflitos se você também usar fontes externas para gerenciar grupos de segurança

Se você usa uma ferramenta ou serviço diferente do Firewall Manager para gerenciar os grupos de segurança, tenha cuidado para evitar conflitos entre as configurações do Firewall Manager e da sua fonte externa. Se você usa correção automática e as configurações são conflitantes, pode criar um ciclo de correções conflitantes que consomem recursos dos dois lados.

Por exemplo, digamos que você configure outro serviço para manter um grupo de segurança de um conjunto de recursos da AWS e configure uma política do Firewall Manager para manter um grupo de segurança diferente para alguns ou todos os mesmos recursos. Se você configurar um dos lados para não permitir que qualquer outro grupo de segurança seja associado aos recursos no escopo, esse lado removerá a associação de grupo de segurança que é mantida pelo outro lado. Se os dois lados estiverem configurados dessa maneira, você poderá acabar com um ciclo de dissociações e associações conflitantes.

Além disso, por exemplo, você pode criar uma política de auditoria do Firewall Manager para impor uma configuração de grupo de segurança que conflita com a configuração do grupo de segurança do outro serviço. A correção aplicada pela política de auditoria do Firewall Manager pode atualizar ou excluir esse grupo de segurança, deixando-o fora de conformidade para o outro serviço. Se o outro serviço estiver configurado para monitorar e corrigir automaticamente quaisquer problemas encontrados, ele recriará ou atualizará o grupo de segurança, deixando-o novamente fora de conformidade com a política de auditoria do Firewall Manager. Se a política de auditoria do Firewall

Manager estiver configurada para a correção automática, ela atualizará ou excluirá novamente o grupo de segurança externo e assim por diante.

Para evitar conflitos como esses, crie configurações que são mutuamente exclusivas entre o Firewall Manager e quaisquer fontes externas.

Você pode usar a marcação de tags para excluir os grupos de segurança externos da correção automática das suas políticas do Firewall Manager. Para fazer isso, adicione uma ou mais tags aos grupos de segurança ou outros recursos que são gerenciados pela origem externa. Depois, ao definir o escopo da política do Firewall Manager, na especificação dos recursos, exclua aqueles que tenham a tag ou as tags adicionadas.

Da mesma forma, na sua ferramenta ou serviço externo, exclua os grupos de segurança que o Firewall Manager gerencia de qualquer atividade de gerenciamento ou auditoria. Não importe os recursos do Firewall Manager ou use tags específicas do Firewall Manager para excluí-los do gerenciamento externo.

Melhores práticas para políticas de grupo de segurança de auditoria de uso

Siga essas diretrizes ao usar políticas de grupo de segurança de auditoria de uso.

- Evite fazer várias alterações no status de associação de um grupo de segurança em um curto espaço de tempo, como em uma janela de 15 minutos. Isso pode fazer com que o Firewall Manager perca alguns ou todos os eventos correspondentes. Por exemplo, não associe e desassocie rapidamente um grupo de segurança com uma interface de rede elástica.

Advertências e limitações da política de grupo de segurança

Esta seção lista as advertências e limitações do uso das políticas de grupo de segurança do Firewall Manager:

- A atualização de grupos de segurança para interfaces de rede elástica do Amazon EC2 que foram criadas usando o tipo de serviço Fargate não é suportada. No entanto, você pode atualizar grupos de segurança para interfaces de rede elástica do Amazon ECS com o tipo de serviço Amazon EC2.
- O Firewall Manager não oferece suporte a grupos de segurança para interfaces de rede elástica do Amazon EC2 que foram criadas pelo Amazon Relational Database Service.
- A atualização de interfaces de rede elástica do Amazon ECS só é possível para serviços do Amazon ECS que usam o controlador de implantação de atualização contínua (Amazon

ECS). Para outros controladores de implantação do Amazon ECS, como CODE_DEPLOY ou controladores externos, o Amazon ECS atualmente não pode atualizar as interfaces de rede elástica.

- Com grupos de segurança para interfaces de rede elástica do Amazon EC2, as alterações em um grupo de segurança não estão imediatamente visíveis para o Firewall Manager. O Firewall Manager geralmente detecta alterações em algumas horas, mas a detecção pode demorar até seis horas.
- O Firewall Manager não oferece suporte à atualização de grupos de segurança em interfaces de rede elástica para Network Load Balancers.
- Em políticas comuns de grupo de segurança, se uma VPC compartilhada depois tiver o compartilhamento cancelado com uma conta, o Firewall Manager não excluirá os grupos de segurança de réplica na conta.
- Com as políticas de grupo de segurança de auditoria de uso, se você criar várias políticas com uma configuração de tempo de atraso personalizada, todas com o mesmo escopo, a primeira política com constatações de conformidade será a política que relata as descobertas.

Casos de uso da política de grupo de segurança

Você pode usar políticas AWS Firewall Manager comuns de grupos de segurança para automatizar a configuração do firewall do host para comunicação entre instâncias da Amazon VPC. Esta seção lista arquiteturas padrão da Amazon VPC e descreve como proteger cada uma usando políticas de grupo de segurança comuns do Firewall Manager. Essas políticas de grupo de segurança podem ajudá-lo a aplicar um conjunto unificado de regras para selecionar recursos em contas diferentes e evitar configurações por conta no Amazon Elastic Compute Cloud e na Amazon VPC.

Com políticas de grupo de segurança comuns do Firewall Manager, você pode marcar apenas as interfaces de rede elástica do EC2 necessárias para comunicação com instâncias em outra Amazon VPC. As outras instâncias na mesma Amazon VPC são mais seguras e isoladas.

Caso de uso: monitoramento e controle de solicitações para Application Load Balancers e Classic Load Balancers

Você pode usar uma política de grupo de segurança comum do Firewall Manager para definir quais solicitações seus balanceadores de carga dentro do escopo devem atender. Você pode configurar isso por meio do console do Firewall Manager. Somente solicitações que estejam em conformidade com as regras de entrada do grupo de segurança podem alcançar seus balanceadores de carga, e os balanceadores de carga distribuirão somente solicitações que atendam às regras de saída.

Caso de uso: Amazon VPC pública, com acesso à Internet

Você pode usar uma política de grupo de segurança comum do Firewall Manager para proteger uma Amazon VPC pública, por exemplo, para permitir apenas a porta de entrada 443. Isso é o mesmo que permitir apenas tráfego HTTPS de entrada para uma VPC pública. Você pode marcar recursos públicos dentro da VPC (por exemplo, como “PublicVPC”) e definir o escopo da política do Firewall Manager como apenas recursos com essa tag. O Firewall Manager aplica automaticamente a política a esses recursos.

Caso de uso: instâncias da Amazon VPC públicas e privadas

Você pode usar a mesma política de grupo de segurança comum para recursos públicos, conforme recomendado no caso de uso anterior para instâncias da Amazon VPC públicas com acesso à Internet. Você pode usar uma segunda política de grupo de segurança comum para limitar a comunicação entre os recursos públicos e os privados. Marque os recursos nas instâncias públicas e privadas da Amazon VPC com algo como "PublicPrivate" para aplicar a segunda política a eles. Você pode usar uma terceira política para definir a comunicação permitida entre os recursos privados e outras instâncias da Amazon VPC corporativas ou privadas. Para essa política, você pode usar outra tag de identificação nos recursos privados.

Caso de uso: instâncias da Amazon VPC de hub e spoke

Você pode usar uma política de grupo de segurança comum para definir comunicações entre a instância hub da Amazon VPC e as instâncias spoke da Amazon VPC. Você pode usar uma segunda política para definir a comunicação de cada instância spoke da Amazon VPC para a instância hub da Amazon VPC.

Caso de uso: interface de rede padrão para instâncias Amazon EC2

Você pode usar uma política de grupo de segurança comum para permitir apenas comunicações padrão, por exemplo, serviços internos de atualização SSH e Patch/OS, e para impedir outras comunicações inseguras.

Caso de uso: identificar recursos com permissões abertas

Você pode usar uma política de grupo de segurança de auditoria para identificar todos os recursos em sua organização que têm permissão para se comunicar com endereços IP públicos ou que têm endereços IP que pertencem a fornecedores de terceiros.

Políticas da lista de controle de acesso à rede (ACL) da Amazon VPC

Esta seção aborda como as políticas de ACL de AWS Firewall Manager rede funcionam e fornece orientação para usá-las. Para obter orientação sobre como criar uma política de ACL de rede usando o console, consulteCriando uma política de ACL de rede.

Para obter informações sobre as listas de controle de acesso à rede (ACLs) da Amazon VPC, consulte Controle o tráfego para sub-redes usando ACLs de rede no Guia do usuário da Amazon VPC.

Você pode usar as políticas de ACL de rede do Firewall Manager para gerenciar as listas de controle de acesso à rede (ACLs) da Amazon Virtual Private Cloud (Amazon VPC) para sua organização em. AWS Organizations Você define as configurações da regra de ACL de rede da política e as contas e sub-redes nas quais deseja que as configurações sejam aplicadas. O Firewall Manager aplica continuamente suas configurações de política às contas e sub-redes à medida que elas são adicionadas ou atualizadas em toda a organização. Para obter informações sobre o escopo da política e AWS Organizations, consulte AWS Firewall Manager escopo da política e o Guia AWS Organizations do Usuário.

Ao definir uma política de ACL de rede do Firewall Manager, além das configurações padrão da política do Firewall Manager, como nome e escopo, você fornece o seguinte:

- Primeira e última regras para tratamento de tráfego de entrada e saída. O Firewall Manager impõe a presença e a ordem dessas nas ACLs de rede que estão no escopo da política ou relata a não conformidade. Suas contas individuais podem criar regras personalizadas para serem executadas entre a primeira e a última regra da política.
- Se a remediação deveria ser forçada quando a remediação resultaria em conflitos de gerenciamento de tráfego entre as regras na ACL da rede. Isso se aplica somente quando a remediação está habilitada para a política.

Regras e marcação de ACL de rede do Firewall Manager

Esta seção descreve as especificações da regra da política de ACL de rede e as ACLs de rede que são gerenciadas pelo Firewall Manager.

Marcação em uma rede gerenciada (ACL)

O Firewall Manager marca uma ACL de rede gerenciada com uma `FMManaged` tag que tem um valor de`true`. O Firewall Manager só executa a remediação em ACLs de rede que tenham essa configuração de tag.

Regras que você define na política

Na especificação da política de ACL de rede, você define as regras que deseja executar primeiro e último para o tráfego de entrada e as regras que deseja executar primeiro e último para o tráfego de saída.

Por padrão, você pode definir até 5 regras de entrada, para uso em qualquer combinação da primeira e da última regra na política. Da mesma forma, você pode definir até 5 regras de saída. Para obter mais informações sobre esses limites, consulteCotas flexíveis. Para obter informações sobre os limites gerais das ACLs de rede, consulte as cotas da Amazon VPC em ACLs de rede no Guia do usuário da Amazon VPC.

Você não atribui números de regras às regras de política. Em vez disso, você especifica as regras na ordem em que deseja que elas sejam avaliadas, e o Firewall Manager usa essa ordem para atribuir números de regras nas ACLs de rede que ele gerencia.

Além disso, você gerencia as especificações das regras de ACL de rede da política da mesma forma que gerenciaria as regras em uma ACL de rede por meio da Amazon VPC. Para obter informações sobre o gerenciamento de ACLs de rede na Amazon VPC, consulte Controle o tráfego para sub-redes usando ACLs de rede e Trabalhe com ACLs de rede no Guia do usuário da Amazon VPC.

Regras em uma rede gerenciada (ACL)

O Firewall Manager configura as regras em uma ACL de rede que ele gerencia colocando a primeira e a última regras da política antes e depois de qualquer regra personalizada definida por um gerente de conta individual. O Firewall Manager preserva a ordem das regras personalizadas. As ACLs de rede são avaliadas começando com a regra de menor numeração.

Quando o Firewall Manager cria pela primeira vez uma ACL de rede, ele define as regras com a seguinte numeração:

- Primeiras regras: 1, 2,... — Definido por você na política de ACL de rede do Firewall Manager.

  O Firewall Manager atribui números de regras a partir de 1 com incrementos de 1, com as regras ordenadas conforme você as ordenou na especificação da política.
- Regras personalizadas: 5.000, 5.100,... — Gerenciado por gerentes de contas individuais por meio do Amazon VPC.

O Firewall Manager atribui números a essas regras a partir de 5.000 e incrementando em 100 para cada regra subsequente.

- Últimas regras:... 32.765, 32.766 — Definido por você na política de ACL de rede do Firewall Manager.

  O Firewall Manager atribui números de regras que terminam no número mais alto possível, 32766 com incrementos de 1, com as regras ordenadas conforme você as ordenou na especificação da política.

Após a inicialização da ACL de rede, o Firewall Manager não controla as alterações que contas individuais fazem em suas ACLs de rede gerenciadas. Contas individuais podem alterar uma ACL de rede sem tirá-la da conformidade, desde que todas as regras personalizadas permaneçam numeradas entre a primeira e a última regra da política, e a primeira e a última regras mantenham a ordem especificada. Como prática recomendada, ao gerenciar regras personalizadas, siga a numeração descrita nesta seção.

Como o Firewall Manager inicia o gerenciamento de ACL de rede para uma sub-rede

O Firewall Manager inicia o gerenciamento da ACL de rede para uma sub-rede quando associa a sub-rede a uma ACL de rede que o Firewall Manager criou e com a qual marcou como definida. `FMManaged` `true`

A conformidade com uma política de ACL de rede exige que a ACL de rede da sub-rede tenha as primeiras regras da política posicionadas primeiro, na ordem especificada na política, as últimas regras posicionadas por último, em ordem, e quaisquer outras regras personalizadas posicionadas no meio. Esses requisitos podem ser atendidos por uma ACL de rede não gerenciada à qual a sub-rede já esteja associada ou por uma ACL de rede gerenciada.

Quando o Firewall Manager aplica uma política de ACL de rede a uma sub-rede associada a uma ACL de rede não gerenciada, o Firewall Manager verifica o seguinte na ordem, parando quando identifica uma opção viável:

1. A ACL de rede associada já está em conformidade — Se a ACL de rede atualmente associada à sub-rede for compatível, o Firewall Manager deixará essa associação em vigor e não iniciará o gerenciamento da ACL de rede para a sub-rede.

O Firewall Manager não altera nem gerencia uma ACL de rede que não seja de sua propriedade, mas, desde que esteja em conformidade, o Firewall Manager a mantém em vigor e apenas a monitora quanto à conformidade com as políticas.

2. Uma ACL de rede gerenciada compatível está disponível — Se o Firewall Manager já estiver gerenciando uma ACL de rede compatível com a configuração necessária, essa é uma opção. Se a remediação estiver ativada, o Firewall Manager associará a sub-rede a ela. Se a correção estiver desativada, o Firewall Manager marcará a sub-rede como não compatível e oferecerá a substituição da associação de ACL de rede como uma opção de remediação.
3. Crie uma nova ACL de rede gerenciada compatível — Se a correção estiver ativada, o Firewall Manager cria uma nova ACL de rede e a associa à sub-rede. Caso contrário, o Firewall Manager marca a sub-rede como não compatível e oferece as opções de remediação para criar a nova ACL de rede e substituir a associação da ACL de rede.

Se essas etapas falharem, o Firewall Manager reportará a não conformidade da sub-rede.

O Firewall Manager segue essas etapas quando uma sub-rede entra no escopo pela primeira vez e quando a ACL de rede não gerenciada de uma sub-rede está fora de conformidade.

Como o Firewall Manager corrige ACLs de rede gerenciada não compatíveis

Esta seção descreve como o Firewall Manager corrige suas ACLs de rede gerenciadas quando elas não estão em conformidade com a política. O Firewall Manager corrige somente as ACLs de rede gerenciadas, com a `FMManaged` tag definida como. `true` Para ACLs de rede que não são gerenciadas pelo Firewall Manager, consulteGerenciamento inicial de ACL de rede.

A remediação restaura as localizações relativas da primeira, da personalizada e da última regra e restaura a ordenação da primeira e da última regras. Durante a correção, o Firewall Manager não necessariamente moverá as regras para os números de regras que ele usa na inicialização da ACL de rede. Para obter as configurações numéricas iniciais e as descrições dessas categorias de regras, consulteGerenciamento inicial de ACL de rede.

Para estabelecer regras e ordenação de regras compatíveis, o Firewall Manager pode precisar mover as regras dentro da ACL da rede. Tanto quanto possível, o Firewall Manager preserva as proteções da ACL de rede mantendo a ordem de regras compatível existente enquanto faz isso. Por exemplo, ele pode duplicar temporariamente as regras em novos locais e, em seguida, realizar uma remoção ordenada das regras originais, preservando os locais relativos durante o processo.

Essa abordagem protege suas configurações, mas também requer espaço na rede ACL para as regras provisórias. Se o Firewall Manager atingir o limite de regras em uma ACL de rede, ele interromperá a correção. Quando isso acontece, a ACL da rede permanece fora de conformidade e o Firewall Manager relata o motivo.

Se uma conta adiciona regras personalizadas a uma ACL de rede gerenciada pelo Firewall Manager e essas regras interferem na remediação do Firewall Manager, o Firewall Manager interrompe qualquer atividade de remediação na ACL da rede e relata o conflito.

Remediação forçada

Se você escolher a correção automática para a política, você também especifica se deseja forçar a remediação para as primeiras regras ou as últimas regras.

Quando o Firewall Manager encontra um conflito no tratamento do tráfego entre uma regra personalizada e uma regra de política, ele se refere à configuração de remediação forçada correspondente. Se a remediação forçada estiver ativada, o Firewall Manager aplicará a correção, apesar do conflito. Se essa opção não estiver ativada, o Firewall Manager interromperá a correção. Em ambos os casos, o Firewall Manager relata o conflito de regras e oferece opções de remediação.

Requisitos e limitações da contagem de regras

Durante a remediação, o Firewall Manager pode duplicar temporariamente as regras para movê-las sem alterar as proteções que elas fornecem.

Para regras de entrada ou saída, o maior número de regras que o Firewall Manager pode exigir para realizar a correção é o seguinte:

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

As ACLs de rede e as políticas de ACL de rede são limitadas por limites de regras mutáveis. Se o Firewall Manager atingir um limite em seus esforços de remediação, ele para de tentar remediar e relata a não conformidade.

Para abrir espaço para o Firewall Manager realizar suas atividades de remediação, você pode solicitar um aumento de limite. Como alternativa, você pode alterar a configuração na política ou na ACL da rede para reduzir o número de regras usadas.

Para obter informações sobre os limites da ACL de rede, consulte as cotas da Amazon VPC em ACLs de rede no Guia do usuário da Amazon VPC.

Quando a remediação falha

Ao atualizar uma ACL de rede, se o Firewall Manager precisar parar por algum motivo, ele não reverterá as alterações, mas deixará a ACL da rede em um estado provisório. Se você ver regras duplicadas em uma ACL de rede que tem a `FMManaged` tag definida como`true`, o Firewall Manager provavelmente está no meio da correção. As alterações podem ficar parcialmente concluídas por um período, mas devido à abordagem adotada pelo Firewall Manager para remediação, isso não interromperá o tráfego nem reduzirá a proteção das sub-redes associadas.

Quando o Firewall Manager não corrige completamente as ACLs de rede que estão fora de conformidade, ele relata a não conformidade das sub-redes associadas e sugere possíveis opções de correção.

Tentando novamente após a falha na correção

Na maioria dos casos, se o Firewall Manager falhar em concluir as alterações de remediação em uma ACL de rede, ele acabará por tentar a alteração novamente.

A exceção é quando a remediação atinge o limite de contagem de regras de ACL de rede ou o limite de contagem de ACL da rede VPC. O Firewall Manager não pode realizar atividades de remediação que consumam AWS recursos acima de suas configurações de limite. Nesses casos, você precisa reduzir as contagens ou aumentar os limites para continuar. Para obter informações sobre os limites, consulte as cotas da Amazon VPC em ACLs de rede no Guia do usuário da Amazon VPC.

Relatórios de conformidade de ACL de rede do Firewall Manager

O Firewall Manager monitora e relata a conformidade de todas as ACLs de rede conectadas às sub-redes dentro do escopo.

De um modo geral, a não conformidade ocorre em situações como ordenação incorreta de regras ou conflito no comportamento de tratamento de tráfego entre regras de política e regras personalizadas. Os relatórios de não conformidade incluem violações de conformidade e opções de remediação.

O Firewall Manager relata violações de conformidade para uma política de ACL de rede da mesma forma que para outros tipos de política. Para obter informações sobre relatórios de conformidade, consulteVisualizando as informações de conformidade de uma AWS Firewall Manager política.

Não conformidade durante atualizações de políticas

Depois de modificar uma política de ACL de rede, até que o Firewall Manager atualize as ACLs de rede que estão no escopo da política, o Firewall Manager marca essas ACLs de rede como não compatíveis. O Firewall Manager faz isso mesmo que as ACLs da rede possam, estritamente falando, estar em conformidade.

Por exemplo, se você remover as regras da especificação da política, enquanto as ACLs de rede dentro do escopo ainda tiverem as regras extras, suas definições de regras ainda poderão estar em conformidade com a política. No entanto, como as regras extras fazem parte das regras que o Firewall Manager está gerenciando, o Firewall Manager as vê como violações das configurações atuais da política. Isso é diferente de como o Firewall Manager visualiza as regras personalizadas que você adiciona às ACLs de rede gerenciadas pelo Firewall Manager.

Práticas recomendadas para usar as políticas de ACL de rede do Firewall Manager

Esta seção lista recomendações para trabalhar com políticas de ACL de rede e ACLs de rede gerenciadas do Firewall Manager.

Consulte a **`FMManaged`** tag para identificar as ACLs de rede que são gerenciadas pelo Firewall Manager.

As ACLs de rede gerenciadas pelo Firewall Manager têm a `FMManaged` tag definida como. `true` Use essa tag para ajudar a distinguir suas próprias ACLs de rede personalizadas daquelas que você gerencia por meio do Firewall Manager.

Não modifique o valor da **`FMManaged`** tag em uma ACL de rede

O Firewall Manager usa essa tag para definir e determinar seu status de gerenciamento com uma ACL de rede.

Não modifique as associações para sub-redes que tenham ACLs de rede gerenciadas pelo Firewall Manager

Não altere manualmente as associações entre suas sub-redes e quaisquer ACLs de rede gerenciadas pelo Firewall Manager. Isso pode desativar a capacidade do Firewall Manager de gerenciar as proteções dessas sub-redes. Você pode identificar as ACLs de rede que são gerenciadas pelo Firewall Manager procurando as configurações de `FMManaged` tag do`true`.

Para remover uma sub-rede do gerenciamento de políticas do Firewall Manager, use as configurações do escopo da política do Firewall Manager para excluir a sub-rede. Por exemplo, você pode marcar a sub-rede e depois excluir essa tag do escopo da política. Para ter mais informações, consulte AWS Firewall Manager escopo da política.

Ao atualizar uma ACL de rede gerenciada, não modifique as regras gerenciadas pelo Firewall Manager

Em uma ACL de rede gerenciada pelo Firewall Manager, mantenha suas regras personalizadas separadas das regras de política seguindo o esquema de numeração descrito em. Regras e marcação de ACL de rede do Firewall Manager Adicione ou modifique somente regras que tenham números entre 5.000 e 32.000.

Evite adicionar muitas regras aos limites da sua conta

Durante a remediação de uma ACL de rede, o Firewall Manager geralmente aumenta temporariamente a contagem de regras de ACL de rede. Para evitar problemas de não conformidade, verifique se você tem espaço suficiente para as regras que está usando. Para ter mais informações, consulte Como o Firewall Manager corrige ACLs de rede gerenciada não compatíveis.

Comece com a correção automática desabilitada

Comece com a remediação automática desativada e, em seguida, revise as informações detalhadas da política para determinar os efeitos que a remediação automática teria. Quando você estiver satisfeito com as alterações, edite a política para habilitar a correção automática.

Advertências da política de ACL de rede do Firewall Manager

Esta seção lista as advertências e limitações do uso das políticas de ACL de rede do Firewall Manager.

- Tempos de atualização mais lentos do que com outras políticas — O Firewall Manager geralmente aplica políticas de ACL de rede e alterações de políticas mais lentamente do que com outras políticas do Firewall Manager, devido às limitações na taxa na qual as APIs de ACL de rede do Amazon EC2 são capazes de processar solicitações. Você pode notar que as alterações de política demoram mais do que alterações semelhantes em outras políticas do Firewall Manager, especialmente quando você adiciona uma política pela primeira vez.
- Para proteção inicial da sub-rede, o Firewall Manager prefere políticas mais antigas — isso se aplica somente às sub-redes que ainda não estão protegidas por uma política de ACL de rede do Firewall Manager. Se uma sub-rede entrar no escopo de mais de uma política de ACL de rede ao mesmo tempo, o Firewall Manager usará a política mais antiga para proteger a sub-rede.
- Motivos para uma política parar de proteger uma sub-rede — Uma política que gerencia a rede ACL de uma sub-rede retém o gerenciamento até que uma das seguintes situações aconteça:

- A sub-rede sai do escopo da política.
- A política é excluída.
- Você altera manualmente a associação da sub-rede a uma ACL de rede gerenciada por uma política diferente do Firewall Manager e da qual a sub-rede está no escopo.

Excluindo uma política de ACL de rede do Firewall Manager

Quando você exclui uma política de ACL de rede do Firewall Manager, o Firewall Manager altera os valores da `FMManaged` tag para `false` todas as ACLs de rede que está gerenciando para a política.

Além disso, você pode escolher se deseja limpar os recursos criados pela política. Se você escolher limpar, o Firewall Manager tentará as seguintes etapas na ordem:

1. Colocar a associação de volta ao original — o Firewall Manager tenta associar a sub-rede de volta à ACL de rede à qual ela estava associada antes de o Firewall Manager começar a gerenciá-la.
2. Remover a primeira e a última regras da ACL de rede — Se não conseguir alterar a associação, o Firewall Manager tentará remover a primeira e a última regra da política, deixando somente as regras personalizadas na ACL de rede associada à sub-rede.
3. Não faça nada com as regras ou com a associação — Se não puder fazer nenhuma das coisas acima, o Firewall Manager deixa a ACL da rede e sua associação como estão.

Se você não escolher a opção de limpeza, precisará gerenciar manualmente cada ACL de rede após a exclusão da política. Para a maioria das situações, escolher a opção de limpeza é a abordagem mais simples.

AWS Network Firewall políticas

Você pode usar políticas de Firewall de AWS Firewall Manager Rede para gerenciar AWS Network Firewall firewalls para suas VPCs da Amazon Virtual Private Cloud em toda a sua organização em. AWS Organizations Você pode aplicar firewalls controlados centralmente a toda a organização ou a um subconjunto selecionado de suas contas e VPCs.

O Network Firewall fornece proteções de filtragem de tráfego de rede para as sub-redes públicas em suas VPCs. O Firewall Manager cria e gerencia seus firewalls com base no tipo de gerenciamento de firewall definido pela sua política. O Firewall Manager fornece os seguintes modelos de gerenciamento de firewall:

- Distribuído: para cada conta e VPC dentro do escopo da política, o Firewall Manager cria um firewall do Network Firewall e implanta endpoints de firewall em sub-redes de VPC para filtrar o tráfego da rede.
- Centralizado: o Firewall Manager cria um único firewall de Network Firewall em um único Amazon VPC.
- Importar firewalls existentes: o Firewall Manager importa firewalls existentes para gerenciamento em uma única política do Firewall Manager. Você pode aplicar regras adicionais aos firewalls importados gerenciados pela sua política para garantir que seus firewalls atendam aos seus padrões de segurança.

> **Note**
>
> As políticas do Firewall Manager são políticas do Firewall Manager que você usa para gerenciar as proteções do Network Firewall para suas VPCs em toda a organização.
> As proteções do Network Firewall são especificadas em recursos no serviço Network Firewall que são chamados de políticas de firewall.

Para obter mais informações sobre o uso do Network Firewall, consulte o Guia do desenvolvedor do AWS Network Firewall.

As seções a seguir abordam os requisitos para o uso das políticas de Network Firewall do Firewall Manager e descrevem como as políticas funcionam. Para obter o procedimento para criar a política, consulte Criação de uma AWS Firewall Manager política para AWS Network Firewall.

Você deve habilitar o compartilhamento de recursos

Uma política do Network Firewall compartilha grupos de regras do Network Firewall entre as contas da sua organização. Para que isso funcione, você deve ter o compartilhamento de recursos habilitado para AWS Organizations. Para obter informações sobre como habilitar o compartilhamento de recursos, consulte Compartilhamento de recursos para políticas de Network Firewall e Firewall DNS.

Você deve ter seus grupos de regras do Network Firewall definidos

Ao especificar uma nova política de Firewall de Rede, você define a política de firewall da mesma forma que você faz quando está usando AWS Network Firewall diretamente. Você especifica os

grupos de regras sem estado a serem adicionados, as ações sem estado padrão e os grupos de regras com estado. Seus grupos de regras já devem existir na conta de administrador do Firewall Manager para que você possa incluí-los na política. Para obter informações sobre criar grupos de regras do Network Firewall, consulte Grupos de regras do AWS Network Firewall.

Como o Firewall Manager cria endpoints de firewall

O Tipo de gerenciamento de firewall em sua política determina como o Firewall Manager cria firewalls. Sua política pode criar firewalls distribuídos, um firewall centralizado ou você pode importar firewalls existentes:

- Distribuído: com o modelo de implantação distribuído, o Firewall Manager cria endpoints para cada VPC que está dentro do escopo da política. Você pode personalizar a localização do endpoint especificando em quais zonas de disponibilidade criar endpoints de firewall, ou o Firewall Manager pode criar automaticamente endpoints nas zonas de disponibilidade com sub-redes públicas. Se você escolher manualmente as zonas de disponibilidade, terá a opção de restringir o conjunto de CIDRs permitidos por zona de disponibilidade. Se você decidir permitir que o Firewall Manager crie automaticamente os endpoints, você também deverá especificar se o serviço criará um único endpoint ou vários endpoints de firewall em suas VPCs.
  - Para vários endpoints de firewall, o Firewall Manager implanta um endpoint de firewall em cada zona de disponibilidade em que você tem uma sub-rede com um gateway da Internet ou uma rota de endpoint de firewall criada pelo Firewall Manager na tabela de rotas. Essa é a opção padrão para uma política do Network Firewall.
  - Para um único endpoint de firewall, o Firewall Manager implanta um endpoint de firewall em uma zona de disponibilidade única em qualquer sub-rede que tenha uma rota de gateway da Internet. Com essa opção, o tráfego em outras zonas precisa cruzar os limites da zona para ser filtrado pelo firewall.

    > **Note**
    >
    > Para essas duas opções, deve haver uma sub-rede associada a uma tabela de rotas que tenha uma rota IPv4/prefixlist nela. O Firewall Manager não verifica se há outros recursos.

- Centralizado: com o modelo de implantação centralizado, o Firewall Manager cria um ou mais endpoints de firewall em uma VPC de inspeção. Uma VPC de inspeção é uma VPC central em que o Firewall Manager inicia seus endpoints. Ao usar o modelo de implantação centralizado, você também especifica em quais zonas de disponibilidade criar endpoints de firewall. Você não pode

alterar o VPC de inspeção depois de criar sua política. Para usar uma VPC de inspeção diferente, crie uma nova política.

- Importar firewalls existentes: ao importar firewalls existentes, você escolhe os firewalls a serem gerenciados em sua política adicionando um ou mais conjuntos de recursos à sua política. Um conjunto de recursos é uma coleção de recursos, neste caso firewalls existentes no Network Firewall, que são gerenciados por uma conta na sua organização. Antes de usar conjuntos de recursos em sua política, você deve primeiro criar um conjunto de recursos. Para obter mais informações sobre conjuntos de recursos do Firewall Manager, consulte Trabalhar com conjuntos de recursos no Firewall Manager.

  Tenha em mente as seguintes considerações ao trabalhar com firewalls importados:

  - Se um firewall importado não estiver em conformidade, o Firewall Manager tentará resolver automaticamente a violação, exceto nas seguintes circunstâncias:
    - Se houver uma incompatibilidade entre as ações padrão com ou sem estado da política do Network Firewall e do Firewall Manager.
    - Se um grupo de regras em uma política de firewall importado tiver a mesma prioridade que um grupo de regras na política do Firewall Manager.
    - Se um firewall importado usa uma política de firewall associada a um firewall que não faz parte do conjunto de recursos da política. Isso pode acontecer porque um firewall pode ter exatamente uma política de firewall, mas uma única política de firewall pode ser associada a vários firewalls.
    - Se um grupo de regras preexistente pertencente à política de firewall de um firewall importado, que também está especificado na política do Firewall Manager, receber uma prioridade diferente.
  - Se você habilitar a limpeza de recursos na política, o Firewall Manager removerá os grupos de regras que estavam na política de importação do FMS dos firewalls no escopo do conjunto de recursos.
  - Os firewalls gerenciados por um tipo de gerenciamento existente importado pelo do Firewall Manager só podem ser gerenciados por uma política por vez. Se o mesmo conjunto de recursos for adicionado a várias políticas do Network Firewall de importação, os firewalls no conjunto de recursos serão gerenciados pela primeira política à qual o conjunto de recursos foi adicionado e serão ignorados pela segunda política.
  - No momento, o Firewall Manager não transmite configurações de política de exceção de fluxo. Para obter informações sobre políticas de exceção de fluxo, consulte Política de exceção de fluxo no Guia do desenvolvedor do AWS Network Firewall .

Se você alterar a lista de zonas de disponibilidade para políticas usando gerenciamento de firewall distribuído ou centralizado, o Firewall Manager tentará limpar todos os endpoints que foram criados no passado, mas que não estão atualmente no escopo da política. O Firewall Manager removerá o endpoint somente se não houver rotas da tabela de rotas que façam referência ao endpoint fora do escopo. Se o Firewall Manager descobrir que não é possível excluir esses endpoints, ele marcará a sub-rede do firewall como não compatível e continuará tentando remover o endpoint até que seja seguro excluí-lo.

Como o Firewall Manager gerencia suas sub-redes de firewall

As sub-redes de firewall são as sub-redes VPC que o Firewall Manager cria para os endpoints de firewall que filtram seu tráfego de rede. Cada endpoint de firewall deve ser implantado em uma sub-rede VPC dedicada. O Firewall Manager cria pelo menos uma sub-rede de firewall em cada VPC que está dentro do escopo da política.

Para políticas que usam o modelo de implantação distribuído com configuração automática de endpoint, o Firewall Manager cria apenas sub-redes de firewall em zonas de disponibilidade que têm uma sub-rede com uma rota de gateway da Internet ou uma sub-rede com uma rota para os endpoints de firewall que o Firewall Manager criou para sua política. Para obter mais informações, consulte VPCs e sub-redes no Manual do usuário da Amazon VPC.

Para políticas que usam o modelo distribuído ou centralizado em que você especifica em quais zonas de disponibilidade o Firewall Manager cria os endpoints do firewall, o Firewall Manager cria um endpoint nessas zonas de disponibilidade específicas, independentemente de haver outros recursos na zona de disponibilidade.

Ao definir pela primeira vez uma política do Network Firewall, você especifica como o Firewall Manager gerencia as sub-redes do firewall em cada uma das VPCs que estão no escopo. Não é possível alterar essa opção mais tarde.

Para políticas que usam o modelo de implantação distribuído com configuração automática de endpoint, você pode escolher entre as seguintes opções:

- Implante uma sub-rede de firewall para cada zona de disponibilidade que tenha sub-redes públicas. Esse é o comportamento padrão. Isso fornece alta disponibilidade de suas proteções de filtragem de tráfego.
- Implemente uma sub-rede de firewall única em uma zona de disponibilidade. Com essa opção, o Firewall Manager identifica uma zona na VPC que tem a maioria das sub-redes públicas e cria a sub-rede do firewall lá. O endpoint de firewall único filtra todo o tráfego de rede para a VPC. Isso

pode reduzir os custos do firewall, mas não está altamente disponível e exige que o tráfego de outras zonas ultrapasse os limites da zona para ser filtrado.

Para políticas que usam o modelo de implantação distribuído com configuração de endpoint personalizada ou o modelo de implantação centralizado, o Firewall Manager cria as sub-redes nas zonas de disponibilidade especificadas que estão dentro do escopo da política.

Você pode fornecer blocos CIDR da VPC para o Firewall Manager usar nas sub-redes do firewall ou deixar que o Firewall Manager determine os endereços de endpoint do firewall.

- Se você não fornecer blocos CIDR, o Firewall Manager consulta suas VPCs em busca de endereços IP disponíveis para uso.
- Se você fornecer uma lista de blocos CIDR, o Firewall Manager pesquisará novas sub-redes somente nos blocos CIDR que você fornecer. Você deve usar blocos CIDR /28. Para cada sub-rede de firewall criada pelo Firewall Manager, ele percorre sua lista de bloqueios de CIDR e usa a primeira que achar aplicável à zona de disponibilidade e à VPC e que tenha endereços disponíveis. Se o Firewall Manager não conseguir encontrar espaço aberto na VPC (com ou sem a restrição), o serviço não criará um firewall na VPC.

Se o Firewall Manager não conseguir criar uma sub-rede de firewall necessária em uma zona de disponibilidade, ele marcará a sub-rede como não compatível com a política. Enquanto a zona estiver nesse estado, o tráfego da zona deve cruzar os limites da zona para ser filtrado por um endpoint em outra zona. Isso é semelhante ao cenário de sub-rede de firewall única.

Como o Firewall Manager gerencia seus recursos do Network Firewall

Ao definir a política no Firewall Manager, você fornece o comportamento de filtragem de tráfego de rede de uma política de AWS Network Firewall firewall padrão. Você adiciona grupos de regras do Network Firewall sem estado e com estado e especifica ações padrão para pacotes que não correspondem a nenhuma regra sem estado. Para obter informações sobre como trabalhar com políticas de firewall em AWS Network Firewall, consulte as políticas de AWS Network Firewall firewall.

Para políticas distribuídas e centralizadas, quando você salva a política do Network Firewall, o Firewall Manager cria um firewall e uma política de firewall em cada VPC que está dentro do escopo da política. O Firewall Manager nomeia esses recursos do Network Firewall concatenando os seguintes valores:

- Uma string fixa, `FMManagedNetworkFirewall` ou `FMManagedNetworkFirewallPolicy`, dependendo do tipo de recurso.
- Nome da política do Firewall Manager. Esse é o nome que você atribui ao criar a política.
- ID da política do Firewall Manager. Esse é o ID do AWS recurso para a política do Firewall Manager.
- ID da Amazon VPC. Esse é o ID do AWS recurso para a VPC em que o Firewall Manager cria o firewall e a política de firewall.

Veja a seguir um exemplo de nome para um firewall gerenciado pelo Firewall Manager:

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Veja a seguir um exemplo de nome de política de firewall:

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Depois de criar a política, as contas membros nas VPCs não podem substituir suas configurações de política de firewall ou seus grupos de regras, mas podem adicionar grupos de regras à política de firewall que o Firewall Manager criou.

Como o Firewall Manager gerencia e monitora tabelas de rotas da VPC para sua política

> **Note**
>
> Atualmente, o gerenciamento de tabela de rotas não é suportado por políticas que usam o modelo de implantação centralizado.

Quando o Firewall Manager cria seus endpoints de firewall, ele também cria as tabelas de rotas da VPC para eles. No entanto, o Firewall Manager não gerencia suas tabelas de rotas de VPC. Você deve configurar suas tabelas de rotas de VPC para direcionar o tráfego de rede para os endpoints de firewall criados pelo Firewall Manager. Usando os aprimoramentos do roteamento de entrada do Amazon VPC, altere suas tabelas de rotas para rotear o tráfego pelos novos endpoints do firewall. Suas alterações devem inserir os endpoints do firewall entre as sub-redes que você deseja proteger e os locais externos. O roteamento exato que você precisa fazer depende da sua arquitetura e de seus componentes.

Atualmente, o Firewall Manager permite monitorar as rotas da tabela de rotas da VPC para qualquer tráfego destinado ao gateway da Internet que esteja contornando o firewall. O Firewall Manager não oferece suporte a outros gateways de destino, como gateways NAT.

Para obter informações sobre o gerenciamento de tabelas de rotas para sua VPC, consulte Gerenciamento de tabelas de rotas para sua VPC no Guia do usuário da Amazon Virtual Private Cloud. Para obter informações sobre como gerenciar suas tabelas de rotas para o Network Firewall, consulte Configurações da tabela de rotas AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Quando você ativa o monitoramento de uma política, o Firewall Manager monitora continuamente as configurações de rotas da VPC e alerta você sobre o tráfego que ignora a inspeção do firewall dessa VPC. Se uma sub-rede tiver uma rota de endpoint de firewall, o Firewall Manager procurará as seguintes rotas:

- Rotas para enviar tráfego para o endpoint do Network Firewall.
- Rotas para encaminhar o tráfego do endpoint do Network Firewall para o gateway da Internet.
- Rotas de entrada do gateway da Internet para o endpoint do Network Firewall.
- Rotas da sub-rede do firewall.

Se uma sub-rede tiver uma rota de Network Firewall, mas houver roteamento assimétrico no Network Firewall e na tabela de rotas do gateway da Internet, o Firewall Manager reportará a sub-rede como não compatível. O Firewall Manager também detecta rotas para o gateway da Internet na tabela de rotas do firewall que o Firewall Manager criou, bem como na tabela de rotas da sua sub-rede, e as relata como em não conformidade. Rotas adicionais na tabela de rotas de sub-rede do Network Firewall e na tabela de rotas do gateway da Internet também são relatadas como em não conformidade. Dependendo do tipo de violação, o Firewall Manager sugere ações de remediação para que a configuração da rota fique em conformidade. O Firewall Manager não oferece sugestões em todos os casos. Por exemplo, se a sub-rede do seu cliente tiver um endpoint de firewall criado fora do Firewall Manager, o Firewall Manager não sugere ações de correção.

Por padrão, o Firewall Manager marcará qualquer tráfego que cruze o limite da zona de disponibilidade para inspeção como em não conformidade. No entanto, se você optar por criar automaticamente um único endpoint em sua VPC, o Firewall Manager não marcará o tráfego que cruza o limite da zona de disponibilidade como em não conformidade.

Para políticas que usam modelos de implantação distribuídos com configuração de endpoint personalizada, você pode escolher se o tráfego que cruza o limite da zona de disponibilidade a partir

de uma zona de disponibilidade sem um endpoint de firewall é marcado como em conformidade ou em não conformidade.

> **Note**
>
> - O Firewall Manager não sugere ações de remediação para rotas não IPv4, como IPv6 e rotas de lista de prefixos.
> - As chamadas feitas usando a chamada de API `DisassociateRouteTable` podem levar até 12 horas para serem detectadas.
> - O Firewall Manager cria uma tabela de rotas do Network Firewall para uma sub-rede que contém os endpoints do firewall. O Firewall Manager presume que essa tabela de rotas contém somente um gateway da Internet válido e rotas padrão de VPC. Qualquer rota extra ou inválida nessa tabela de rotas é considerada em não conformidade.

Quando você configura sua política do Firewall Manager, se escolher o modo Monitor, o Firewall Manager fornece detalhes de violação e remediação de recursos sobre seus recursos. Você pode usar essas ações de remediação sugeridas para corrigir problemas de rota em suas tabelas de rotas. Se você escolher o modo Desativado, o Firewall Manager não monitorará o conteúdo da tabela de rotas para você. Com essa opção, você mesmo gerencia suas tabelas de rotas da VPC. Para obter mais informações sobre essas violações de recursos, consulte Visualizando as informações de conformidade de uma AWS Firewall Manager política.

> **Warning**
>
> Se você escolher Monitor na configuração de AWS Network Firewall rotas ao criar sua política, não poderá desativá-lo para essa política. No entanto, se você escolher Desativado, poderá ativá-lo mais tarde.

Configurando o registro em log para uma política AWS Network Firewall

Você pode habilitar o registro em log centralizado para suas políticas de Network Firewall para obter informações detalhadas sobre o tráfego em sua organização. Você pode selecionar o registro em log do fluxo para capturar o fluxo de tráfego da rede ou o registro em log de alertas para relatar o tráfego que corresponda a uma regra com a ação da regra definida como `DROP` ou `ALERT`. Para obter mais

informações sobre registro em log AWS Network Firewall , consulte Registrar tráfego de rede do AWS Network Firewall no Guia do desenvolvedor do AWS Network Firewall .

Você envia logs dos firewalls da política do Network Firewall para um bucket do Amazon S3. Depois de ativar o registro, AWS Network Firewall entrega os registros para cada Firewall de Rede configurado atualizando as configurações do firewall para entregar os registros aos buckets selecionados do Amazon S3 com o prefixo reservado AWS Firewall Manager ,. `<policy-name>-<policy-id>`

> **Note**
>
> Esse prefixo é usado pelo Firewall Manager para determinar se uma configuração de registro em log foi adicionada pelo Firewall Manager ou se foi adicionada pelo proprietário da conta. Se o proprietário da conta tentar usar o prefixo reservado para seu próprio registro em log personalizado, ele será substituído pela configuração de registro em log na política do Firewall Manager.

Para obter mais informações sobre como criar um bucket do Amazon S3 e revisar os logs armazenados, consulte O que é o Amazon S3? no Guia do usuário do Amazon Simple Storage Service.

Você deve atender aos seguintes requisitos para habilitar o registro em log:

- O Amazon S3 que você especificar em sua política do Firewall Manager deve existir.
- Você deve ter as seguintes permissões:
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- Se o bucket do Amazon S3 que é seu destino de registro usa criptografia do lado do servidor com chaves armazenadas AWS Key Management Service, você deve adicionar a seguinte política à sua AWS KMS chave gerenciada pelo cliente para permitir que o Firewall Manager faça login no seu grupo de registros de registros: CloudWatch

```
{
    "Effect": "Allow",
    "Principal": {
```

```
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

Observe que somente os buckets na conta de administrador do Firewall Manager podem ser usados para o registro em log central do AWS Network Firewall .

Quando você habilita o registro em log centralizado em uma política de Network Firewall, o Firewall Manager executa as seguintes ações em sua conta:

- O Firewall Manager atualiza as permissões nos buckets do S3 selecionados para permitir a entrega de logs.
- O Firewall Manager cria diretórios no bucket do S3 para cada conta membro no escopo da política. Os logs de cada conta podem ser encontrados em `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`.

Para habilitar o registro em log para uma política de Network Firewall

1. Crie um bucket do Amazon S3 usando sua conta de administrador do Firewall Manager. Para obter mais informações, consulte Criar um bucket no Guia do usuário do Amazon Simple Storage Service.
2. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

3. No painel de navegação, escolha Políticas de segurança.
4. Selecione a política de Network Firewall para a qual você deseja habilitar o registro em log. Para obter mais informações sobre AWS Network Firewall registro, consulte Registro do tráfego de rede AWS Network Firewall no Guia do AWS Network Firewall desenvolvedor.
5. Na guia Detalhes da política, na seção Regras da política, escolha Editar.
6. Para ativar e agregar logs, escolha uma ou mais opções em Configuração de registro em log:
   - Habilitar e agregar logs de fluxo
   - Habilitar e agregar logs de alerta
7. Escolha o bucket do Amazon S3 no qual você quer que seus logs sejam entregues. Você deve escolher um bucket para cada tipo de log habilitado. Você pode usar o mesmo bucket para os dois tipos de log.
8. (Opcional) Se você quiser que o registro em log personalizado criado pela conta do membro seja substituído pela configuração de registro em log da política, escolha Substituir configuração de registro em log existente.
9. Escolha Próximo.
10. Revise suas configurações e escolha Salvar para salvar suas alterações na política.

Para desativar o registro em log de uma política de Network Firewall

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Selecione a política de Network Firewall para a qual você deseja desabilitar o registro em log.
4. Na guia Detalhes da política, na seção Regras da política, escolha Editar.
5. Em Status da configuração de registro em log, desmarque Habilitar e agregar logs de fluxo e Habilitar e agregar logs de alerta, se estiverem selecionados.

6. Escolha Próximo.
7. Revise suas configurações e escolha Salvar para salvar suas alterações na política.

Políticas de Firewall DNS do Amazon Route 53 Resolver

Você pode usar políticas de firewall de AWS Firewall Manager DNS para gerenciar associações entre grupos de regras do Amazon Route 53 Resolver DNS Firewall e suas VPCs da Amazon Virtual Private Cloud em toda a sua organização em. AWS Organizations Você pode aplicar políticas de grupo de segurança controladas centralmente a toda a organização ou a um subconjunto selecionado de suas contas e VPCs.

O Firewall DNS fornece filtragem e regulação do tráfego DNS de saída para suas VPCs. Você cria coleções reutilizáveis de regras de filtragem em grupos de regras do Firewall DNS e associa os grupos de regras às suas VPCs. Quando você aplica a política do Firewall Manager, para cada conta e VPC dentro do escopo da política, o Firewall Manager cria uma associação entre cada grupo de regras do Firewall DNS na política e cada VPC que está dentro do escopo da política, usando as configurações de prioridade de associação que você especifica na política do Firewall Manager.

Para obter mais informações sobre o Firewall DNS, consulte Firewall DNS do Amazon Route 53 Resolver, no Guia do Desenvolvedor do Amazon Route 53.

As seções a seguir abordam os requisitos para usar as políticas de Firewall DNS do Firewall Manager e descrevem como as políticas funcionam. Para obter o procedimento para criar a política, consulte Criação de uma AWS Firewall Manager política para o Amazon Route 53 Resolver DNS Firewall.

Você deve habilitar o compartilhamento de recursos

Uma política de firewall DNS compartilha grupos de regras de Firewall DNS entre as contas da sua organização. Para que isso funcione, você deve ter o compartilhamento de recursos ativado com AWS Organizations. Para obter informações sobre como habilitar o compartilhamento de recursos, consulte Compartilhamento de recursos para políticas de Network Firewall e Firewall DNS.

Você deve ter seus grupos de regras do Firewall DNS

Ao especificar uma nova política de Firewall DNS, você define os grupos de regras da mesma forma que você faz quando está usando o Firewall DNS do Amazon Route 53 Resolver diretamente. Seus grupos de regras já devem existir na conta de administrador do Firewall Manager para que você

possa incluí-los na política. Para obter informações sobre a criação de grupos de regras do Firewall DNS, consulte Grupos de regras e regras do Firewall DNS.

Você define as associações de grupos de regras de prioridade mais baixa e mais alta

As associações de grupos de regras do Firewall DNS que você gerencia por meio das políticas do Firewall DNS do Firewall Manager contêm as associações de menor prioridade e as associações de maior prioridade para suas VPCs. Em sua configuração de política, elas aparecem como primeiro e último grupos de regras.

O Firewall DNS filtra o tráfego DNS para a VPC na seguinte ordem:

1. Primeiros grupos de regras, definidos por você na política de Firewall DNS do Firewall Manager. Os valores válidos estão entre 1 e 99.
2. Grupos de regras do Firewall DNS associados por gerentes de contas individuais por meio do Firewall DNS.
3. Últimos grupos de regras, definidos por você na política de Firewall DNS do Firewall Manager. Os valores válidos estão entre 9.901 e 10.000.

Excluir um grupo de regras

Para excluir um grupo de regras de uma política de Firewall DNS do Firewall Manager, você deve executar as seguintes etapas:

1. Remova o grupo de regras da política de Firewall DNS do Firewall Manager.
2. Cancele o compartilhamento do grupo de regras em AWS Resource Access Manager. Para cancelar o compartilhamento de um grupo de regras de sua propriedade, é necessário removê-lo do compartilhamento de recursos. Você pode fazer isso usando o AWS RAM console ou a AWS CLI. Para obter informações sobre como cancelar um compartilhamento de recursos, consulte Atualizar um compartilhamento de recursos AWS RAM no Guia do usuário do AWS RAM .
3. Exclua o grupo de regras usando o console do Firewall DNS ou a AWS CLI.

Como o Firewall Manager nomeia as associações de grupos de regras que ele cria

Quando você salva a política de Firewall DNS, se você habilitou a correção automática, o Firewall Manager cria uma associação de Firewall DNS entre os grupos de regras que você forneceu na política e as VPCs que estão no escopo da política. O Firewall Manager nomeia essas associações concatenando os seguintes valores:

- A string fixa, `FMManaged_`.
- A ID da política do Firewall Manager. Esse é o ID do AWS recurso para a política do Firewall Manager.

Veja a seguir um exemplo de nome para um firewall gerenciado pelo Firewall Manager:

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

Depois de criar a política, se os proprietários da conta nas VPCs substituírem suas configurações de política de firewall ou suas associações de grupos de regras, o Firewall Manager marcará a política como não compatível e tentará propor uma ação corretiva. Os proprietários da conta podem associar outros grupos de regras do Firewall DNS às VPCs que estão no escopo da política do Firewall DNS. Todas as associações criadas pelos proprietários individuais da conta devem ter configurações de prioridade entre a primeira e a última associação do grupo de regras.

Políticas de NGFW na nuvem da Palo Alto Networks

O Cloud Next Generation Firewall (NGFW) da Palo Alto Networks é um serviço de firewall terceirizado que você pode usar para suas políticas. AWS Firewall Manager Com o Palo Alto Networks Cloud NGFW for Firewall Manager, você pode criar e implantar centralmente recursos e pilhas de regras do Palo Alto Networks Cloud NGFW em todas as suas contas. AWS

Para usar o Palo Alto Networks Cloud NGFW com o Firewall Manager, primeiro você assina o serviço Pay-As-You-Go da Palo Alto Networks Cloud NGFW no Marketplace. AWS Depois de se inscrever, você executa uma série de etapas no serviço NGFW na nuvem da Palo Alto Networks para definir sua conta e as configurações do NGFW na nuvem. Em seguida, você cria uma política do Firewall Manager Cloud FMS para implantar e gerenciar centralmente os recursos e regras do Cloud NGFW da Palo Alto Networks em todas as contas em suas organizações. AWS

Para obter o procedimento para criar a política do Firewall Manager, consulte Criação de uma AWS Firewall Manager política para o Palo Alto Networks Cloud NGFW. Para obter informações sobre como configurar e gerenciar o NGFW na nuvem da Palo Alto Networks para o Firewall Manager, consulte o NGFW na nuvem da Palo Alto Networks na documentação da AWS.

Políticas do Fortigate Cloud Native Firewall (CNF) como serviço

O Fortigate Cloud Native Firewall (CNF) as a Service é um serviço de firewall de terceiros que você pode usar para suas políticas. AWS Firewall Manager O Fortigate CNF é um serviço de firewall

de próxima geração que facilita a proteção de suas redes em nuvem e o gerenciamento de suas políticas de segurança. Com o Fortigate CNF for Firewall Manager, você pode criar e implantar centralmente os recursos e conjuntos de políticas do Fortigate CNF em todas as suas contas. AWS

Para usar o Fortigate CNF com o Firewall Manager, primeiro você assina o Fortigate Cloud Native Firewall (CNF) como um serviço no Marketplace. AWS Depois de assinar, você executa uma série de etapas no serviço Fortigate CNF para definir seus conjuntos de políticas globais e outras configurações. Em seguida, você cria uma política do Firewall Manager para implantar e gerenciar centralmente os recursos do Fortigate CNF em todas as contas em suas organizações. AWS

Para o procedimento para criar uma política do Fortigate CNF Firewall Manager, consulte Criação de uma AWS Firewall Manager política para o Fortigate Cloud Native Firewall (CNF) como serviço. Para obter informações sobre como configurar e gerenciar o Fortigate CNF para uso com o Firewall Manager, consulte a Documentação do Fortigate CNF.

Compartilhamento de recursos para políticas de Network Firewall e Firewall DNS

Para gerenciar as políticas de Firewall Manager, Firewall de Rede e Firewall DNS, você deve habilitar o compartilhamento de recursos com o AWS Organizations in AWS Resource Access Manager. Isso permite que o Firewall Manager implante proteções em suas contas ao criar esses tipos de política.

Para ativar o compartilhamento de recursos, siga as instruções em Ativar compartilhamento com AWS Organizations no Guia do usuário de AWS Resource Access Manager .

Problemas com o compartilhamento de recursos

Você pode encontrar problemas com o compartilhamento de recursos, seja ao usá-lo AWS RAM para habilitá-lo ou ao trabalhar em políticas do Firewall Manager que o exijam.

São exemplos desses problemas:

- Quando você segue as instruções para habilitar o compartilhamento, no AWS RAM console, a opção Habilitar compartilhamento com AWS Organizations fica acinzentada e não está disponível para seleção.
- Quando você trabalha no Firewall Manager em uma política que exige compartilhamento de recursos, a política é marcada como não compatível e você vê mensagens indicando que o compartilhamento de recursos ou AWS RAM não está habilitado.

Se você detectar problemas com o compartilhamento de recursos, execute o procedimento a seguir para tentar habilitá-lo.

Tente novamente para habilitar o compartilhamento de recursos

- Tente novamente habilitar o compartilhamento usando uma das seguintes opções:
  - (Opção) Por meio do AWS RAM console, siga as instruções em Ativar compartilhamento com AWS Organizations no Guia AWS Resource Access Manager do usuário.
  - (Opção) Usando a AWS RAM API, chame`EnableSharingWithAwsOrganization`. Veja a documentação em EnableSharingWithAwsOrganization.

Trabalhar com conjuntos de recursos no Firewall Manager

Um conjunto de AWS Firewall Manager recursos é uma coleção de recursos, como firewalls, que você pode agrupar e gerenciar em uma política do Firewall Manager. Os conjuntos de recursos permitem que os membros da sua organização tenham controle granular sobre quais recursos gerenciar em uma política. Para usar conjuntos de recursos, crie um conjunto de recursos no console ou usando a PutResourceSetAPI e adicione o conjunto de recursos à sua política do Firewall Manager.

Você pode criar e gerenciar conjuntos de recursos para os seguintes tipos de recursos e políticas de segurança:

Tipo de recurso	Tipo de política de segurança do Firewall Manager
AWS Network Firewall - firewalls	Política de Network Firewall: use conjuntos de recursos para importar firewalls existentes do Network Firewall. Para obter informações sobre o uso de conjuntos de recursos em uma política do Network Firewall, consulte a etapa Importar firewalls existentes no procedimento Criação de uma AWS Firewall Manager política para AWS Network Firewall.

As seções a seguir abordam os requisitos para criar e excluir conjuntos de recursos.

Tópicos

- Considerações ao trabalhar com conjuntos de recursos no Firewall Manager
- Criar conjuntos de recursos
- Excluir um conjunto de recursos

Considerações ao trabalhar com conjuntos de recursos no Firewall Manager

Preste atenção nas seguintes considerações ao trabalhar com conjuntos de recursos

Referências a recursos inexistentes

Ao adicionar um recurso a um conjunto de recursos, você cria uma referência ao recurso usando um nome do recurso da Amazon (ARN). O Firewall Manager valida se o nome do recurso da Amazon (ARN) está no formato correto, mas não verifica se o recurso referenciado existe. Se o recurso ainda não existir e passar pela validação do ARN, o Firewall Manager incluirá a referência do recurso no conjunto de recursos. Se um novo recurso com o mesmo ARN for criado posteriormente, o Firewall Manager aplicará ao novo recurso os grupos de regras da política associada ao conjunto de recursos.

Recursos excluídos

Quando um recurso em um conjunto de recursos é excluído, a referência ao recurso permanece no conjunto de recursos até ser removida pelo administrador do Firewall Manager.

Recursos pertencentes à conta do membro que sai da AWS Organizations organização

Se uma conta membro sair da organização, qualquer referência aos recursos pertencentes a essa conta membro permanecerá no conjunto de recursos, mas não será mais gerenciada por nenhuma política à qual o conjunto de recursos esteja associado.

Associação a várias políticas

Um conjunto de recursos pode ser associado a várias políticas, mas nem todos os tipos de políticas oferecem suporte a várias políticas que gerenciam o mesmo recurso. Consulte a documentação do seu tipo específico de política para obter informações sobre cenários sem suporte.

Criar conjuntos de recursos

Para criar um conjunto de recursos (console)

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Conjuntos de recursos.
3. Escolha Criar conjunto de recursos.
4. Em Nome do conjunto de recursos, insira um nome descritivo.
5. (Opcional) Insira uma Descrição para o conjunto de recursos.
6. Escolha Próximo.
7. Em Escolher recursos, selecione um ID de conta AWS e selecione Escolher recursos para adicionar os recursos pertencentes e gerenciados por essa conta ao conjunto de recursos. Depois de selecionar os recursos, selecione Adicionar para adicioná-los ao conjunto de recursos.
8. Escolha Próximo.
9. Em Tags do conjunto de recursos, adicione as tags de identificação que você deseja para o conjunto de recursos. Para obter mais informações sobre tags, consulte Trabalhar com o Tag Editor.
10. Escolha Próximo.
11. Analise o novo conjunto de recursos. Para fazer alterações, escolha Editar na área que você deseja alterar. Isso o retorna à etapa correspondente no assistente de criação. Quando estiver satisfeito com o conjunto de recursos, escolha Criar conjunto de recursos.

Excluir um conjunto de recursos

Antes de excluir um conjunto de recursos, ele deve ser desassociado de todas as políticas que o utilizam. Você pode desassociar grupos de recursos na página de detalhes da política usando o console ou com a PutPolicyAPI.

Para excluir um conjunto de recursos (console)

1. No painel de navegação, escolha Conjuntos de recursos.
2. Escolha a opção próxima ao conjunto de recursos que você deseja excluir.
3. Escolha Excluir.

Visualizando as informações de conformidade de uma AWS Firewall Manager política

Esta seção fornece orientação para visualizar o status de conformidade de contas e recursos que estão no escopo de uma AWS Firewall Manager política. Para obter informações sobre os controles em vigor AWS para manter a segurança e a conformidade da nuvem, consulteValidação de conformidade do Firewall Manager.

> **Note**
>
> Para que o Firewall Manager monitore a conformidade com as políticas, AWS Config deve registrar continuamente as alterações de configuração dos recursos protegidos. Na sua AWS Config configuração, a frequência de gravação deve ser definida como Contínua, que é a configuração padrão.

> **Note**
>
> Para manter o estado de conformidade adequado em seus recursos protegidos, evite alterar repetidamente o estado das proteções do Firewall Manager, automática ou manualmente. O Firewall Manager usa as informações de AWS Config para detectar alterações nas configurações dos recursos. Se as alterações forem aplicadas com rapidez suficiente, AWS Config pode perder o controle de algumas delas, o que pode resultar na perda de informações sobre conformidade ou estado de remediação no Firewall Manager.
> Se você perceber que um recurso que você está protegendo com o Firewall Manager tem um status incorreto de conformidade ou remediação, primeiro verifique se não está executando nenhum processo que altere ou redefina as proteções do Firewall Manager e, em seguida, atualize o AWS Config rastreamento do recurso reavaliando as regras de configuração associadas em. AWS Config

Para todas AWS Firewall Manager as políticas, você pode visualizar o status de conformidade de contas e recursos que estão no escopo da política. Uma conta ou recurso está em conformidade com a política do Firewall Manager se as configurações da política estiverem refletidas nas configurações da conta ou do recurso. Cada tipo de política tem seus próprios requisitos de conformidade, que você pode ajustar ao definir a política. Para algumas políticas, você também pode visualizar informações

detalhadas sobre violações dos recursos do escopo, para ajudá-lo a entender e gerenciar melhor seu risco de segurança.

Para visualizar informações de conformidade de uma política

1. Faça login no AWS Management Console usando sua conta de administrador do Firewall Manager e abra o console do Firewall Manager emhttps://console.aws.amazon.com/wafv2/fmsv2. Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

   > **Note**
   >
   > Para obter mais informações sobre a configuração de uma conta de administrador do Firewall Manager, consulte AWS Firewall Manager pré-requisitos.

2. No painel de navegação, escolha Políticas de segurança.
3. Escolha uma política. Na guia Contas e recursos da página de política, o Firewall Manager lista as contas em sua organização, agrupadas segundo as que estão dentro do escopo da política e as que estão fora do escopo.

   O painel Contas dentro do escopo da política lista o status de conformidade de cada conta. O status Conforme indica que a política foi aplicada com sucesso a todos os recursos no escopo da conta. O status Não Conforme indica que a política não foi aplicada a um ou mais recursos no escopo da conta.
4. Escolha uma conta que não esteja em conformidade. Na página da conta, o Firewall Manager lista a ID e o tipo de cada recurso não conforme e o motivo pelo qual o recurso viola a política.

   > **Note**
   >
   > Para os tipos de recursos `AWS::EC2::NetworkInterface` (ENI) e `AWS::EC2::Instance`, o Firewall Manager pode mostrar um número limitado de recursos não conformes. Para listar recursos adicionais não conformes, corrija os que são exibidos inicialmente para a conta.

5. Se o tipo de política do Firewall Manager for uma política de grupo de segurança de auditoria de conteúdo, você poderá acessar informações detalhadas sobre as violações de um recurso.

   Para ver os detalhes da violação, escolha o recurso.

> **Note**
>
> Os recursos que o Firewall Manager considerou não conformes antes da adição da página detalhada de violação de recursos podem não ter detalhes da violação.

Na página de recursos, o Firewall Manager lista detalhes específicos sobre a violação, de acordo com o tipo de recurso.

- **`AWS::EC2::NetworkInterface`** (ENI): o Firewall Manager exibe informações sobre o grupo de segurança com o qual o recurso não está em conformidade. Escolha o grupo de segurança para ver mais detalhes sobre ele.
- **`AWS::EC2::Instance`**: o Firewall Manager exibe a ENI anexada à instância do EC2 que não está em conformidade. Ele também exibe informações sobre o grupo de segurança com os quais os recursos não estão em conformidade. Escolha o grupo de segurança para ver mais detalhes sobre ele.
- **`AWS::EC2::SecurityGroup`**: o Firewall Manager exibe os seguintes detalhes da violação:
  - Regra de grupo de segurança não conforme: A regra que viola, incluindo seu protocolo, intervalo de portas, intervalo de IP CIDR e descrição.
  - Regra referenciada: A regra do grupo de segurança de auditoria que a regra do grupo de segurança que não está em conformidade viola, com seus detalhes.
  - Motivos da violação: Explicação da descoberta de não conformidade.
  - Ação de correção: Ação a ser tomada sugerida. Se o Firewall Manager não conseguir determinar uma ação de correção segura, este campo estará em branco.
- **`AWS::EC2::Subnet`**— Isso é usado para políticas de ACL de rede e Firewall de Rede.

  O Firewall Manager exibe a ID da sub-rede, a ID da VPC e a Zona de Disponibilidade. Se aplicável, o Firewall Manager inclui informações adicionais sobre a violação. O componente de descrição da violação contém uma descrição do estado esperado do recurso, o estado atual de não conformidade e, se disponível, uma descrição do que causou a discrepância.

  Violações do Firewall de Rede

  - Violações do gerenciamento de rotas: Para políticas de Firewall de Rede que usam o modo Monitor, o Gerenciador de Firewall exibe informações básicas da sub-rede, bem como as rotas esperadas e reais na tabela de rotas da sub-rede, do gateway da Internet e da sub-

rede do Firewall de Rede. O Firewall Manager alerta você de que há uma violação se as rotas reais não corresponderem às rotas esperadas na tabela de rotas.

- Ações de remediação para violações do gerenciamento de rotas: Para políticas de Firewall de Rede que usam o modo Monitor, o Firewall Manager sugere possíveis ações de remediação em configurações de rotas que tenham violações.

Por exemplo, digamos que se espera que uma sub-rede envie tráfego pelos endpoints do firewall, mas a sub-rede atual esteja enviando tráfego diretamente para o gateway da Internet. Isso é uma violação do gerenciamento de rotas. A correção sugerida nesse caso pode ser uma lista de ações ordenadas. A primeira é uma recomendação para adicionar as rotas necessárias à tabela de rotas da sub-rede do Firewall de Rede para direcionar o tráfego de saída para o gateway da Internet e direcionar o tráfego de entrada para destinos dentro da VPC para o `local`. A segunda recomendação é substituir a rota do gateway da Internet ou a rota inválida do Network Firewall na tabela de rotas da sub-rede para direcionar o tráfego de saída para os endpoints do firewall. A terceira recomendação é adicionar as rotas necessárias à tabela de rotas do gateway da Internet para direcionar o tráfego de entrada para os endpoints do firewall.

- **`AWS::EC2::InternetGateway`**: Isso é usado para políticas de Firewall de Rede que têm o modo Monitor ativado.
  - Violações do gerenciamento de rotas: O gateway da Internet não está em conformidade se o gateway da Internet não estiver associado a uma tabela de rotas ou se houver uma rota inválida na tabela de rotas do gateway da Internet.
  - Ações de remediação para violações do gerenciamento de rotas: O Firewall Manager sugere possíveis ações de remediação para remediar as violações do gerenciamento de rotas.

  Example 1: Sugestões de violação e remediação do gerenciamento de rotas

  A tabela de rotas não está associada ao gateway da Internet. As ações de correção sugeridas podem ser uma lista de ações ordenadas. A primeira ação é criar uma tabela de rotas. A segunda ação é associar a tabela de rotas ao gateway da Internet. A terceira ação é adicionar a rota necessária à tabela de rotas do gateway da Internet.

  Example 2: Sugestões de violação e remediação do gerenciamento de rotas

  O gateway da Internet está associado a uma tabela de rotas válida, mas a rota está configurada incorretamente. A correção sugerida pode ser uma lista de ações ordenadas. A

primeira sugestão é remover a rota inválida. A segunda é adicionar a rota necessária à tabela de rotas do gateway da Internet.

- **`AWS::NetworkFirewall::FirewallPolicy`**: É usado para políticas de Firewall de Rede. O Firewall Manager exibe informações sobre uma política de firewall do Firewall de Rede que foi modificada de forma a que não esteja em conformidade. As informações fornecem a política de firewall esperada e a política encontrada na conta do cliente, para que você possa comparar nomes e configurações de prioridade de grupos de regras sem estado e com estado, nomes de ações personalizados e configurações padrão de ações sem estado. O componente de descrição da violação contém uma descrição do estado esperado do recurso, o estado atual de não conformidade e, se disponível, uma descrição do que causou a discrepância.
- **`AWS::EC2::VPC`**: É usado para políticas de Firewall DNS. O Firewall Manager exibe informações sobre uma VPC que está no escopo de uma política de firewall DNS do Firewall Manager e que não está em conformidade com a política. As informações fornecidas incluem os grupos de regras esperados que devem ser associados à VPC e os grupos de regras reais. O componente de descrição da violação contém uma descrição do estado esperado do recurso, o estado atual de não conformidade e, se disponível, uma descrição do que causou a discrepância.

AWS Firewall Manager descobertas

AWS Firewall Manager cria descobertas para recursos que estão fora de conformidade e para ataques que ela detecta e para AWS Security Hub os quais os envia. Para obter informações sobre descobertas do Security Hub, consulte Descobertas em AWS Security Hub.

Quando você usa o Security Hub e o Firewall Manager, o Firewall Manager envia automaticamente suas descobertas para o Security Hub. Para obter informações sobre como começar a usar o Security Hub, consulte Como configurar o AWS Security Hub no Guia do usuário do AWS Security Hub.

> **Note**
>
> O Firewall Manager só atualiza as descobertas das políticas que estão sob seu gerenciamento e dos recursos que ele está monitorando.
> O Firewall Manager não resolve as descobertas do seguinte:
>
> - Políticas que foram excluídas.

- Recursos que foram excluídos.
- Recursos que saíram do escopo da política do Firewall Manager, por exemplo, devido a uma alteração na tag ou na definição da política.

Como visualizar minhas descobertas do Firewall Manager?

Para exibir suas descobertas do Firewall Manager no Security Hub, siga as orientações em Trabalhar com descobertas no Security Hub e crie um filtro usando as seguintes configurações:

- Atributo definido como Nome do produto.
- Operador definido como EQUALS.
- Valor definido como `Firewall Manager`. Essa configuração diferencia maiúsculas de minúsculas.

Posso desabilitá-la?

Você pode desativar a integração das AWS Firewall Manager descobertas com o Security Hub por meio do console do Security Hub. Escolha Integrações na barra de navegação e, no painel do Firewall Manager, escolha Desabilitar integração. Para mais informações, consulte o Guia do usuário do AWS Security Hub.

AWS Firewall Manager tipos de descoberta

- AWS WAF conclusões políticas
- AWS Shield Advanced conclusões políticas
- Descobertas de políticas comuns do grupo de segurança
- Descobertas da política de auditoria de conteúdo do grupo de segurança
- Descobertas da política de auditoria de uso do grupo de segurança
- Conclusões da política de Firewall DNS do Amazon Route 53 Resolver

AWS WAF conclusões políticas

Você pode usar AWS WAF as políticas do Firewall Manager para aplicar grupos de AWS WAF regras aos seus recursos no AWS Organizations. Para ter mais informações, consulte Trabalhando com AWS Firewall Manager políticas.

O recurso está ausente da web ACL gerenciada do Firewall Manager.

Um AWS recurso não tem a associação da Web ACL AWS Firewall Manager gerenciada de acordo com a política do Firewall Manager. Você pode habilitar a correção do Firewall Manager na política apropriada.

- Gravidade: 80
- Configurações de status: APROVADO/REPROVADO
- Atualizações: se o Firewall Manager executar a ação de correção, ele atualizará a descoberta e a gravidade diminuirá de `HIGH` para `INFORMATIONAL`. Se você executar a correção, o Firewall Manager não atualizará a descoberta.

A web ACL gerenciada pelo Firewall Manager configurou grupos de regras incorretamente.

Os grupos de regras em uma web ACL que é gerenciada pelo Firewall Manager não estão configurados corretamente, de acordo com a política do Firewall Manager. Isso significa que a web ACL não tem os grupos de regras exigidos pela política. Você pode habilitar a correção do Firewall Manager na política apropriada.

- Gravidade: 80
- Configurações de status: APROVADO/REPROVADO
- Atualizações: se o Firewall Manager executar a ação de correção, ele atualizará a descoberta e a gravidade diminuirá de `HIGH` para `INFORMATIONAL`. Se você executar a correção, o Firewall Manager não atualizará a descoberta.

AWS Shield Advanced conclusões políticas

Para obter informações sobre AWS Shield Advanced políticas, consulte Políticas de grupo de segurança.

O recurso carece da proteção Shield Advanced.

Um AWS recurso que deveria ter a proteção Shield Advanced, de acordo com a política do Firewall Manager, não a tem. Você pode habilitar a correção do Firewall Manager na política, que habilitará a proteção para o recurso.

- Gravidade: 60

- Configurações de status: APROVADO/REPROVADO
- Atualizações: se o Firewall Manager executar a ação de correção, ele atualizará a descoberta e a gravidade diminuirá de `HIGH` para `INFORMATIONAL`. Se você executar a correção, o Firewall Manager não atualizará a descoberta.

O Shield Advanced detectou ataque contra um recurso monitorado.

O Shield Advanced detectou um ataque a um AWS recurso protegido. Você pode habilitar a correção do Firewall Manager na política.

- Gravidade: 70
- Configurações de status: nenhuma
- Atualizações - o Firewall Manager não atualiza essa descoberta.

Descobertas de políticas comuns do grupo de segurança

Para obter informações sobre políticas comuns de grupo de segurança, consulte Políticas de grupo de segurança.

O recurso configurou incorretamente o grupo de segurança.

O Firewall Manager identificou um recurso que está sem as associações de grupo de segurança gerenciadas pelo Firewall Manager que ele deveria ter, de acordo com a política do Firewall Manager. Você pode habilitar a correção do Firewall Manager na política, o que cria as associações de acordo com as configurações de política.

- Gravidade: 70
- Configurações de status: APROVADO/REPROVADO
- Atualizações: o Firewall Manager atualiza essa descoberta.

O grupo de segurança de réplica do Firewall Manager está fora de sincronia com o grupo de segurança primário.

Um grupo de segurança de réplica do Firewall Manager está fora de sincronia com seu grupo de segurança primário, de acordo com a política de grupo de segurança comum. Você pode habilitar a correção do Firewall Manager na política, que sincroniza os grupos de segurança de réplica com o principal.

- Gravidade: 80
- Configurações de status: APROVADO/REPROVADO
- Atualizações: o Firewall Manager atualiza essa descoberta.

Descobertas da política de auditoria de conteúdo do grupo de segurança

Para obter informações sobre políticas de auditoria de conteúdo do grupo de segurança, consulte Políticas de grupo de segurança.

O grupo de segurança não está em conformidade com o grupo de segurança de auditoria de conteúdo.

Uma política de auditoria de conteúdo de grupo de segurança do Firewall Manager identificou um grupo de segurança não compatível. Este é um grupo de segurança criado pelo cliente que está no escopo da política de auditoria de conteúdo e que não está em conformidade com as configurações definidas pela política e pelo grupo de segurança de auditoria. Você pode habilitar a correção do Firewall Manager na política, que modifica o grupo de segurança não compatível para deixá-lo em conformidade.

- Gravidade: 70
- Configurações de status: APROVADO/REPROVADO
- Atualizações: o Firewall Manager atualiza essa descoberta.

Descobertas da política de auditoria de uso do grupo de segurança

Para obter informações sobre políticas de auditoria de uso do grupo de segurança, consulte Políticas de grupo de segurança.

O Firewall Manager encontrou um grupo de segurança redundante.

A auditoria de uso do grupo de segurança do Firewall Manager identificou um grupo de segurança redundante. É um grupo de segurança com regras idênticas definidas como outro grupo de segurança dentro da mesma instância da Amazon Virtual Private Cloud. Você pode habilitar a correção automática do Firewall Manager na política de auditoria de uso, o que substitui grupos de segurança redundantes e com um único grupo de segurança.

- Gravidade: 30

- Configurações de status: nenhuma
- Atualizações - o Firewall Manager não atualiza essa descoberta.

O Firewall Manager encontrou um grupo de segurança não utilizado.

A auditoria de uso do grupo de segurança do Firewall Manager identificou um grupo de segurança não utilizado. É um grupo de segurança que não é referenciado por nenhuma política comum de grupo de segurança do Firewall Manager. Você pode habilitar a correção automática do Firewall Manager na política de auditoria de uso, que remove grupos de segurança não utilizados.

- Gravidade: 30
- Configurações de status: nenhuma
- Atualizações - o Firewall Manager não atualiza essa descoberta.

Conclusões da política de Firewall DNS do Amazon Route 53 Resolver

Para obter mais informações sobre o Firewall DNS, consulte Políticas de Firewall DNS do Amazon Route 53 Resolver.

Falta a proteção do firewall DNS no recurso

Uma VPC não tem uma associação de grupo de regras do Firewall DNS definida na política de Firewall do Firewall Manager DNS. A descoberta lista o grupo de regras especificado pela política.

- Gravidade: 80

Segurança no uso do AWS Firewall Manager serviço

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

> **Note**
>
> Esta seção fornece diretrizes de AWS segurança padrão para o uso do AWS Firewall Manager serviço e de seus AWS recursos, como o Firewall Manager, políticas de firewall de rede e políticas de grupo de segurança.

Para obter informações sobre como proteger seus AWS recursos usando o Firewall Manager, consulte o restante do guia do Firewall Manager.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto 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. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Firewall Manager, consulte Serviços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, como a confidencialidade de seus dados, os requisitos da sua organização, leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Firewall Manager. Os tópicos a seguir mostram como configurar o Firewall 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 Firewall Manager.

Tópicos

Proteção de dados no Firewall Manager

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Firewall 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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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 os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- 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 sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Firewall Manager ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

As entidades do Firewall Manager, como políticas, são criptografadas em repouso, exceto em determinadas regiões onde a criptografia não está disponível, incluindo China (Pequim) e China (Ningxia). Chaves de criptografia exclusivas são usadas para cada região.

Identity and Access Management para AWS Firewall Manager

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 (fazer login) e autorizado (ter permissões) para usar recursos do Firewall Manager. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa o AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz no Firewall Manager.

Usuário do serviço: se você usa o serviço Firewall Manager para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais atributos do Firewall Manager para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Firewall Manager, consulte Solução de problemas AWS Shield de identidade e acesso.

Administrador do serviço: se você for o responsável pelos recursos do Firewall Manager na empresa, provavelmente terá acesso total ao Firewall Manager. Cabe a você determinar quais funcionalidades e atributos do Firewall Manager os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise

as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Firewall Manager, consulte Como AWS Shield funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Firewall Manager. Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Shield.

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários

de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). 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.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

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.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS

Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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 Firewall Manager funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Firewall Manager, saiba quais atributos do IAM estão disponíveis para uso com o Firewall Manager.

Recursos do IAM que você pode usar com AWS Firewall Manager

Atributo do IAM	Suporte ao Firewall Manager
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim

Atributo do IAM	Suporte ao Firewall Manager
Chaves de condição de política (específicas do serviço)	Não
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Parcial
Funções vinculadas a serviço	Sim

Para ter uma visão geral de como o Firewall 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.

Políticas baseadas em identidade para o Firewall Manager

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager, consulte Exemplos de políticas baseadas em identidade para AWS Firewall Manager.

Exemplos de políticas baseadas em identidade para o Firewall Manager

Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager, consulte Exemplos de políticas baseadas em identidade para AWS Firewall Manager.

Políticas baseadas em recursos no Firewall Manager

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de política para o Firewall Manager

Oferece compatibilidade 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Firewall Manager, consulte Ações definidas pelo AWS Firewall Manager na Referência de autorização do serviço.

As ações de política no Firewall Manager usam o seguinte prefixo antes da ação:

```
fms
```

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

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "fms:Describe*"
```

Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager, consulte Exemplos de políticas baseadas em identidade para AWS Firewall Manager.

Recursos de política para o Firewall Manager

Oferece compatibilidade 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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para obter uma lista dos tipos de recursos do Firewall Manager e seus ARNs, consulte Recursos definidos pelo AWS Firewall Manager na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Firewall Manager.

Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager, consulte Exemplos de políticas baseadas em identidade para AWS Firewall Manager.

Chaves de condição de política do Firewall Manager

Suporta chaves de condição de política específicas de serviço	Não

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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar

vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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 de chaves de condição do Firewall Manager, consulte Chaves de condição do AWS Firewall Manager na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Firewall Manager.

Para visualizar exemplos de políticas baseadas em identidade do Firewall Manager, consulte Exemplos de políticas baseadas em identidade para AWS Firewall Manager.

ACLs no Firewall Manager

Oferece compatibilidade 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Firewall Manager

Oferece compatibilidade com ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades

e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

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 oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Firewall Manager

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o Firewall Manager

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço do Firewall Manager

Oferece suporte a perfis de serviço	Parcial

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, 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 um perfil de serviço pode prejudicar a funcionalidade do Firewall Manager. Edite os perfis de serviço somente quando o Firewall Manager orientar você a fazê-lo.

Selecionar um perfil do IAM no Firewall Manager

Para usar a ação da `PutNotificationChannel` API no Firewall Manager, você deve escolher uma função para permitir que o Firewall Manager acesse o Amazon SNS para que o serviço possa publicar mensagens do Amazon SNS em seu nome. Para obter mais informações, consulte PutNotificationChannela Referência AWS Firewall Manager da API.

A seguir está um exemplo de configuração de permissão de tópico do SNS. Para usar essa política com seu próprio perfil personalizado, substitua o nome do recurso da Amazon (ARN) `AWSServiceRoleForFMS` pelo ARN `SnsRoleName`.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Para obter mais informações sobre as ações e os recursos do Firewall Manager, consulte o tópico do AWS Identity and Access Management guia Ações definidas por AWS Firewall Manager

Funções vinculadas ao serviço para o Firewall Manager

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS Firewall Manager

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Firewall Manager. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O

administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Firewall Manager, incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição do AWS Firewall Manager na Referência de autorização do serviço.

Tópicos

- Melhores práticas de política
- Usando o console do Firewall Manager
- Permitir que os usuários visualizem suas próprias permissões
- Conceda acesso de leitura aos grupos de segurança do Firewall Manager

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Firewall Manager em sua conta. Essas ações podem incorrer em custos para a 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 obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis 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 atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações 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: você pode adicionar uma condição às políticas para limitar o acesso a ações e atributos. Por exemplo, você pode 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 AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: condições no Manual 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 acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, 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 a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

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

Usando o console do Firewall Manager

Para acessar o AWS Firewall Manager console, você deve ter um conjunto mínimo de permissões. Essas permissões devem autorizar você a listar e visualizar detalhes sobre os recursos do Firewall Manager na sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do 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 a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do Firewall Manager, anexe também o Firewall Manager `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

Conceda acesso de leitura aos grupos de segurança do Firewall Manager

O Firewall Manager permite o acesso a recursos entre contas, mas não permite que você crie proteções de recursos entre contas. Você só pode criar proteções para recursos de dentro da conta que possui esses recursos.

Veja a seguir um exemplo de política que concede permissões para as ações `fms:Get`, `fms:List` e `ec2:DescribeSecurityGroups` em todos os recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS políticas gerenciadas para AWS Firewall Manager

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que

atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: **`AWSFMAdminFullAccess`**

Use a política `AWSFMAdminFullAccess` AWS gerenciada para permitir que seus administradores acessem AWS Firewall Manager recursos, incluindo todos os tipos de política do Firewall Manager. Essa política não inclui permissões para configurar notificações do Amazon Simple Notification Service no AWS Firewall Manager. Para obter informações sobre como configurar o acesso ao Amazon Simple Notification Service, consulte Configurando o acesso ao Amazon Simple Notification Service.

Para ver a lista e os detalhes das políticas, consulte o console do IAM em AWSFMAdminFullAccess. O restante desta seção fornece uma visão geral das configurações de política.

Declarações de permissão

Esta política é agrupada em declarações com base no conjunto de permissões.

- AWS Firewall Manager recursos de política - Permite permissões administrativas completas aos recursos em AWS Firewall Manager, incluindo todos os tipos de política do Firewall Manager.
- Grave AWS WAF registros no Amazon Simple Storage Service - Permite que o Firewall Manager grave e leia AWS WAF registros no Amazon S3.
- Criar função vinculada ao serviço — Permite que o administrador crie uma função vinculada ao serviço, o que permite que o Firewall Manager acesse recursos em outros serviços em seu nome. Essa permissão permite criar a função vinculada ao serviço somente para uso pelo Firewall Manager. Para obter informações sobre como o Firewall Manager usa funções vinculadas ao serviço, consulte. Usar funções vinculadas ao serviço para o Firewall Manager
- AWS Organizations: permite que os administradores usem o Firewall Manager para uma organização no AWS Organizations. Depois de habilitar o acesso confiável para o Firewall Manager em AWS Organizations, os membros da conta de administrador podem ver as descobertas em toda a organização. Para obter informações sobre como usar AWS Organizations com AWS Firewall Manager, consulte Usando AWS Organizations com outros AWS serviços no Guia AWS Organizations do usuário.

Categorias de permissão

A lista a seguir lista os tipos de permissões na política e as permissões que elas fornecem.

- `fms`— Trabalhe com AWS Firewall Manager recursos.
- `wafe` `waf-regional` — Trabalhe com políticas AWS WAF clássicas.
- `elasticloadbalancing`— Associe chamadas AWS WAF da web aos Elastic Load Balancers.
- `firehose`— Visualize informações sobre AWS WAF registros.
- `organizations`— Trabalhe com os recursos da AWS Organizations.
- `shield`— Veja o estado das AWS Shield políticas de assinatura.
- `route53resolver`— Trabalhe com grupos de regras de DNS privado do Route 53 para VPCs em uma política de DNS privado do Route 53 para VPCs.
- `wafv2`— Trabalhe com AWS WAFV2 políticas.
- `network-firewall`— Trabalhe com AWS Network Firewall políticas.
- `ec2`— Veja as zonas e regiões de disponibilidade da política.
- `s3`— Visualize informações sobre AWS WAF registros.

AWS política gerenciada: **`FMSServiceRolePolicy`**

Essa política permite AWS Firewall Manager gerenciar AWS recursos em seu nome no Firewall Manager e em serviços integrados. Esta política é anexada à função vinculada ao serviço `AWSServiceRoleForFMS`. Para obter mais informações sobre a função vinculada ao serviço, consulte Usar funções vinculadas ao serviço para o Firewall Manager.

Para obter detalhes sobre a política, consulte o console do IAM no FMS. ServiceRolePolicy

AWS política gerenciada: AWSFMAdminReadOnlyAccess

Concede acesso somente de leitura a todos os recursos do AWS Firewall Manager.

Para ver a lista e os detalhes das políticas, consulte o console do IAM em AWSFMAdminReadOnlyAccess. O restante desta seção fornece uma visão geral das configurações de política.

Categorias de permissão

A lista a seguir lista os tipos de permissões na política e as informações às quais as permissões permitem acesso somente para leitura.

- `fms`— AWS Firewall Manager recursos.
- `wafe` `waf-regional` — Políticas AWS WAF clássicas.
- `firehose`— AWS WAF troncos.
- `organizations`— Recursos da AWS Organizations.
- `shield`— AWS Shield políticas.
- `route53resolver`— DNS privado do Route 53 para grupos de regras de VPCs em uma política de DNS privado do Route 53 para VPCs.
- `wafv2`— Seus grupos de AWS WAFV2 regras e grupos de regras de regras AWS gerenciadas que estão disponíveis em AWS WAFV2.
- `network-firewall`— grupos de AWS Network Firewall regras e metadados de grupos de regras.
- `ec2`— AWS Network Firewall política de zonas e regiões de disponibilidade.
- `s3`— AWS WAF troncos.

AWS política gerenciada: AWSFMMemberReadOnlyAccess

Concede acesso somente para leitura aos recursos AWS Firewall Manager dos membros. Para ver a lista e os detalhes das políticas, consulte o console do IAM em AWSFMMemberReadOnlyAccess.

Atualizações do Firewall Manager para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Firewall Manager desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do Firewall Manager em Histórico do documento.

Alteração	Descrição	Data
FMS ServiceRolePolicy — Política atualizada	Permissões adicionadas para gerenciar ACLs de rede.	2024-04-22

Alteração	Descrição	Data
	Veja a política atualizada no console do IAM: FMS. ServiceRolePolicy	
FMS ServiceRolePolicy — Política atualizada	Permissões adicionadas que permitem que o Firewall Manager descreva se as AWS Config regras especificadas estão em conformidade. Veja a política atualizada no console do IAM: FMS. ServiceRolePolicy	2023-04-21
FMS ServiceRolePolicy — Política atualizada	Permissões adicionadas que permitem que o Firewall Manager descreva os atributos da instância e da interface de rede do Amazon EC2. Veja a política atualizada no console do IAM: FMS. ServiceRolePolicy	2022-11-15
AWSFMAdminReadOnly Access: política atualizada	Permissões adicionadas para apoiar AWS WAFV2, Shield, Network Firewall, DNS Firewall, grupo de segurança Amazon VPC e políticas. Veja a política atualizada no console do IAM: AWSFMAdmi nReadOnlyAccess.	2022-11-02

Alteração	Descrição	Data
AWSFMAdminFullAccess: política atualizada	Permissões adicionadas para apoiar AWS WAFV2, Shield, Network Firewall, DNS Firewall, grupo de segurança Amazon VPC e políticas. Permissões do Amazon SNS removidas. Veja a política atualizada no console do IAM: AWSFMAdminFullAccess.	2022-10-21
`FMSServiceRolePolicy` — Novas permissões para políticas AWS Firewall Manager de firewall de terceiros	Essa alteração permite que o Firewall Manager crie e exclua os endpoints da VPC do Amazon EC2 associados a uma política de firewall de terceiros.	2022-03-30
`FMSServiceRolePolicy` — Novas permissões para AWS Network Firewall políticas	Foram adicionadas novas permissões para apoiar a implantação de firewalls para políticas de Network Firewall. As novas permissões permitem a recuperação de informações sobre zonas de disponibilidade para contas que estão no escopo de uma política.	2022-02-16

Alteração	Descrição	Data
`FMSServiceRolePolicy` — Novas permissões para AWS Shield políticas	Foram adicionadas novas permissões para recuperar tags para recursos AWS WAF regionais e AWS WAF globais. Foram adicionadas permissões AWS WAF regionais para recuperar ACLs da web usando um ARN de recurso. Foram adicionadas permissões para oferecer suporte à mitigação automática de DDoS na camada de aplicativos do Shield.	2022-01-07
`FMSServiceRolePolicy` — Novas permissões para AWS Shield políticas	Foi adicionada nova permissão para recuperar tags para recursos do Elastic Load Balancing.	2021-11-18
`FMSServiceRolePolicy` — Novas permissões para grupos e AWS Network Firewall políticas de segurança	Foram adicionadas novas permissões para permitir o registro centralizado de AWS Network Firewall políticas. Além disso, permissões do Amazon EC2 somente para leitura foram adicionadas para suportar mudanças no serviço Config que afetam a AWS Firewall Manager forma como consulta recursos para políticas de grupos de segurança.	2021-09-29

Alteração	Descrição	Data
`FMSServiceRolePolicy` — Formatos ARN para recursos AWS WAF	Atualizou o `FMSServiceRolePolicy` para padronizar os formatos de ARN para recursos AWS WAF . Os formatos ARN atualizados são `arn:aws:waf:*:*:*` e `arn:aws:waf-regional:*:*:*` .	2021-08-12
`FMSServiceRolePolicy` — Outras regiões na China	AWS Firewall Manager habilitado `FMSServiceRolePolicy` para as regiões BJS e ZHY na China.	2021-08-12
`FMSServiceRolePolicy` : atualização para a política existente	Foram adicionadas novas permissões para AWS Firewall Manager permitir o gerenciamento do Firewall Amazon Route 53 Resolver DNS. Essa alteração permite que o Firewall Manager configure associações de Firewall DNS Amazon Route 53 Resolver . Isso permite que você use o Firewall Manager para fornecer proteções de Firewall DNS para suas VPCs em toda a organização em AWS Organizations.	2021-03-17
O Firewall Manager começou a rastrear as alterações	O Firewall Manager começou a monitorar as alterações em suas políticas AWS gerenciadas.	2021-03-02

Solução de problemas AWS Firewall Manager de identidade e acesso

Usar as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Firewall Manager e o IAM.

Tópicos

Não tenho autorização para executar uma ação no Firewall Manager

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 `fms:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `fms:`*`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 uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Firewall 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 erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Firewall 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 de fora da minha Conta da AWS acessem meus recursos do Firewall Manager

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Firewall Manager oferece suporte a esses atributos, consulte Como AWS Shield 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Usar funções vinculadas ao serviço para o Firewall Manager

AWS Firewall Manager usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculada diretamente ao Firewall Manager. As funções vinculadas ao serviço são predefinidas pelo Firewall 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 Firewall Manager porque você não precisa adicionar as permissões necessárias manualmente. O Firewall Manager define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Firewall Manager pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

É possível excluir uma função vinculada ao serviço somente depois de excluir os recursos relacionados da função. Isso protege seus recursos do Firewall Manager, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões para funções vinculadas ao serviço para o Firewall Manager

AWS Firewall Manager usa o nome da função vinculada ao serviço AWSServiceRoleForFMS para permitir que o Firewall Manager chame AWS serviços em seu nome para gerenciar políticas de firewall e recursos da AWS Organizations conta. Essa política é anexada à função AWS gerenciada`AWSServiceRoleForFMS`. Para obter mais informações sobre a função gerenciada, consulte AWS política gerenciada: `FMSServiceRolePolicy`.

A função AWSServiceRoleForFMS vinculada ao serviço confia no serviço para assumir a função. `fms.amazonaws.com`

A política de permissões da função permite que o Firewall Manager conclua as seguintes ações nos recursos especificados:

- `waf`- Gerencie ACLs da web AWS WAF clássicas, permissões de grupos de regras e associações de ACLs da web em sua conta.

- `ec2` - Gerencie grupos de segurança em interfaces de rede elásticas e instâncias do Amazon EC2. Gerencie ACLs de rede nas sub-redes da Amazon VPC.
- `vpc` - Gerencie sub-redes, tabelas de rotas, tags e endpoints na Amazon VPC.
- `wafv2`- Gerencie ACLs AWS WAF da web, permissões de grupos de regras e associações de ACLs da web em sua conta.
- `cloudfront`- Crie ACLs da web para proteger as CloudFront distribuições.
- `config`- Gerencie as AWS Config regras de propriedade do Firewall Manager em sua conta.
- `iam`- Gerencie essa função vinculada ao serviço e crie as funções obrigatórias e vinculadas ao serviço AWS WAF Shield se configurar o registro e as políticas do Shield. AWS WAF
- `organization`- Crie uma função vinculada ao serviço de propriedade do Firewall Manager para gerenciar AWS Organizations recursos usados pelo Firewall Manager.
- `shield`- Gerencie AWS Shield proteções e configurações de mitigação L7 para recursos em sua conta.
- `ram`- Gerencie o compartilhamento AWS RAM de recursos para grupos de regras do Firewall DNS e grupos de regras do Firewall de Rede.
- `network-firewall`- Gerencie recursos de propriedade do Firewall Manager e AWS Network Firewall recursos dependentes da Amazon VPC em sua conta.
- `route53resolver` - Gerencie associações de Firewall DNS de propriedade do Firewall Manager em sua conta.

Veja a política completa no console do IAM: FMS. ServiceRolePolicy

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para o Firewall Manager

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você ativa o login do Firewall Manager no AWS Management Console, ou faz uma `PutLoggingConfiguration` solicitação na CLI do Firewall Manager ou na API do Firewall Manager, o Firewall Manager cria a função vinculada ao serviço para você.

Você deve ter a permissão `iam:CreateServiceLinkedRole` para habilitar o registro em log.

Se excluir essa função vinculada a serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você habilita o registro em log do Firewall Manager, o Firewall Manager cria a função vinculada ao serviço novamente.

Editar uma função vinculada ao serviço para o Firewall Manager

O Firewall Manager não permite que você edite a função AWSServiceRoleForFMS 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 obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o Firewall Manager

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço Firewall Manager estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Excluir o perfil vinculado a serviço usando o IAM

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao AWSServiceRoleForFMS serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas ao serviço do Firewall Manager

O Firewall Manager oferece suporte a funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Endpoints e cotas do Firewall Manager.

Prevenção contra o ataque “Confused deputy” entre serviços

O problema de “confused deputy” é uma questão de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que AWS Firewall Manager concedem outro serviço ao recurso. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou estiver especificando vários recursos, utilize a chave de condição de contexto global `aws:SourceArn` com caracteres curingas (`*`) para as partes desconhecidas do ARN. Por exemplo, .`arn:aws:fms:*:`*`account-id`*`:*`

Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões.

O valor de `aws:SourceArn` deve ser a AWS conta do AWS Firewall Manager administrador.

O exemplo a seguir mostra como é possível usar a chave de contexto de condição global `aws:SourceArn` no Firewall Manager, a fim de evitar o problema de “confused deputy”.

O exemplo a seguir mostra como evitar o problema de “confused deputy” usando a chave de contexto de condição global `aws:SourceArn` na política de confiança da função do Firewall Manager. Substitua *`Região`* and *`account-id`* por suas informações.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
```

```
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

Registro e monitoramento no Firewall Manager

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Firewall Manager e de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. AWS fornece várias ferramentas para monitorar os recursos do Firewall Manager e responder a possíveis eventos:

CloudWatch Alarmes da Amazon

Usando CloudWatch alarmes, você observa uma única métrica durante um período de tempo especificado por você. Se a métrica exceder um determinado limite, CloudWatch envia uma notificação para um tópico AWS Auto Scaling ou política do Amazon SNS. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.

AWS CloudTrail Registros

CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Firewall Manager. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Firewall Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Registro de chamadas de API do AWS CloudTrail com.

Validação de conformidade do Firewall Manager

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. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os

atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Firewall Manager

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 executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

Segurança da infraestrutura no AWS Firewall Manager

Como serviço gerenciado, AWS Firewall Manager é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Firewall Manager pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

AWS Firewall Manager cotas

AWS Firewall Manager está sujeito às seguintes cotas (anteriormente chamadas de limites).

AWS Firewall Manager tem cotas padrão que você pode aumentar e cotas fixas.

As políticas de grupo de segurança e as políticas de ACL de rede que são gerenciadas pelo Firewall Manager estão sujeitas às cotas padrão da Amazon VPC. Para obter mais informações, consulte Cotas da Amazon VPC no Guia do usuário da Amazon VPC.

Cada política do Firewall Manager Network Firewall cria um firewall de Network Firewall com uma política de firewall e seus grupos de regras associados. Esses recursos do Network Firewall estão sujeitos às cotas listadas nas cotas do AWS Network Firewall no Network Firewall Developer Guide.

Cotas flexíveis

AWS Firewall Manager tem cotas padrão no número de entidades por região. Você pode solicitar um aumento dessas cotas.

Todos os tipos de políticas

Recurso	Cota padrão por região
Contas por organização em AWS Organizations	Varia. Um convite enviado para uma conta é contabilizado como uma cota. A contagem é revertida

Recurso	Cota padrão por região
	se a conta convidada recusa, a conta de gerenciamento cancela o convite ou a validade do convite expira.
Políticas do Firewall Manager por organização no AWS Organizations.	50. As especificações das regiões `Global` e `US East (N. Virginia) Region` se referem à mesma região, portanto, esse limite se aplica ao total de políticas combinadas para as duas.
Unidades organizacionais no escopo de acordo com a política do Firewall Manager.	20
Contas no escopo de uma política do Firewall Manager se você incluir e excluir explicitamente contas individuais.	200
Contas no escopo de uma política do Firewall Manager se você incluir ou excluir explicitamente contas individuais.	2.500
Tags que incluem ou excluem recursos por política do Firewall Manager.	8
Número de conjuntos de recursos por conta.	20
Número de recursos por conjunto de recursos.	100
Número de recursos definidos por política do Firewall Manager.	5

AWS WAF políticas

Recurso	Cota padrão por região
AWS WAF grupos de regras por conta de administrador do Firewall Manager.	100
AWS WAF Grupos de regras clássicas por conta de administrador do Firewall Manager.	10
Grupos de regras por AWS WAF política.	50

Políticas de grupo de segurança comuns

Recurso	Cota padrão por região.
Grupos de segurança primários por política.	3
Instâncias da Amazon VPC no escopo por política, por conta, incluindo VPCs compartilhadas.	100

Políticas de grupo de segurança de auditoria de conteúdo

Recurso	Cota padrão por região
Grupos de segurança de auditoria por política	1
Aplicativos por lista de aplicativos.	50
Listas personalizadas de aplicativos gerenciados para regras que permitem todo o tráfego.	1
Listas personalizadas de aplicativos gerenciados de acordo com as regras de política.	1
Listas personalizadas de aplicativos gerenciados por conta.	10

Recurso	Cota padrão por região
Protocolos por lista de protocolo.	5
Listas personalizadas de protocolos gerenciados para qualquer configuração em uma política.	1
Listas personalizadas de protocolos gerenciados por conta.	10

Políticas de ACL de rede

Recurso	Cota padrão por região
Número de regras de entrada por política de ACL de rede, usadas para a primeira ou a última regra. Por exemplo, você pode ter 5 primeiras e 0 últimas regras de entrada, ou 2 primeiras e 3 últimas, mas não pode ter 4 primeiras e 2 últimas.	5
Número de regras de saída por política de ACL de rede, usadas para a primeira ou a última regra. Por exemplo, você pode ter 5 primeiras e 0 últimas regras de saída, ou 2 primeiras e 3 últimas, mas não pode ter 4 primeiras e 2 últimas.	5

Políticas de firewall DNS

Recurso	Cota padrão por região
Grupos de regras de firewall de DNS por política de firewall de DNS.	2

Cotas fixas

As seguintes cotas por região relacionadas a não AWS Firewall Manager podem ser alteradas.

Todos os tipos de políticas

Recurso	Cota por região
O número máximo de administradores do Firewall Manager que você pode ter em uma AWS Organizations organização. Você deve ter um administrador padrão e até nove administradores adicionais do Firewall Manager.	10

AWS WAF políticas

Recurso	Cota por região
Total de unidades de capacidade de web ACL (WCU) para os grupos de regras em uma política do AWS WAF .	5.000

AWS WAF Políticas clássicas

Recurso	Cota por região
AWS WAF Grupos de regras clássicos por política.	2:1 grupo de regras criado pelo cliente e 1 grupo de AWS Marketplace regras.
AWS WAF Regras clássicas por grupo de regras AWS WAF clássicas do Firewall Manager.	10

Políticas de auditoria de conteúdo de grupo de segurança

Recurso	Cota por região
Listas de aplicativos gerenciados pelo Firewall Manager para qualquer configuração em uma política.	1
Listas de protocolos gerenciados pelo Firewall Manager para qualquer configuração em uma política.	1

Políticas do Network Firewall

Recurso	Cota por região
Número de VPCs que podem ser corrigidas automaticamente para uma única política.	1.000
O número de CIDRs IPV4 que você pode fornecer para uma única política.	50

AWS Firewall Manager Monitoramento AWS WAF e AWS Shield Advanced

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus serviços.

> **Note**
>
> Para obter informações sobre como monitorar seus recursos do Shield Advanced e identificar possíveis eventos de DDoS usando o Shield Advanced, consulte AWS Shield.

Quando você começar a monitorar esses serviços, crie um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

A próxima etapa é estabelecer uma linha de base de desempenho normal de em seu ambiente, medindo o desempenho em vários momentos e em diferentes condições de carga. À medida que você monitora AWS WAF, o Firewall Manager, o Shield Advanced e os serviços relacionados armazenam dados históricos de monitoramento para que você possa compará-los com os dados de desempenho atuais, identificar padrões normais de desempenho e anomalias de desempenho e criar métodos para resolver problemas.

Pois AWS WAF, você deve monitorar os seguintes itens no mínimo para estabelecer uma linha de base:

- O número de solicitações da web permitidas
- O número de solicitações da web bloqueadas

Tópicos

Ferramentas de monitoramento

AWS fornece várias ferramentas que você pode usar para monitorar AWS WAF AWS Shield Advanced e. É possível configurar algumas dessas ferramentas para realizar o monitoramento, enquanto outras exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Você pode usar as seguintes ferramentas de monitoramento automatizado para observar AWS WAF AWS Shield Advanced e relatar quando algo está errado:

- Painéis de visão geral do tráfego da Web ACL — Acesse os resumos do tráfego da Web que uma ACL da Web avalia acessando a página da ACL da Web no AWS WAF console e abrindo a guia Visão geral do tráfego.

  Os painéis de visão geral do tráfego fornecem resumos quase em tempo real das CloudWatch métricas da Amazon que são AWS WAF coletadas quando avalia o tráfego do seu aplicativo na web. Você pode ver resumos de todo o seu tráfego na web e do tráfego avaliado pelos grupos inteligentes de regras de mitigação de ameaças.

  Para obter mais informações, consulte Painéis de visão geral do tráfego de web ACL ou acesse os painéis no console.
- Amazon CloudWatch Alarms — Observe uma única métrica durante um período de tempo especificado por você e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou uma política do Amazon EC2 Auto Scaling. Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocarão ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para obter mais informações, consulte Monitorando CloudFront atividades usando CloudWatch.

> **Note**
>
> CloudWatch métricas e alarmes não estão habilitados para AWS Firewall Manager.

Você não só pode usar CloudWatch para monitorar AWS WAF as métricas do Shield AdvancedMonitoramento com a Amazon CloudWatch, conforme descrito em, mas também CloudWatch para monitorar a atividade de seus recursos protegidos. Para mais informações, consulte:

- Monitoramento de CloudFront atividades usando CloudWatch o Amazon CloudFront Developer Guide
- Registro em log e monitoramento no Amazon API Gateway no Guia do desenvolvedor do API Gateway
- CloudWatch Métricas para seu Application Load Balancer no Guia do Usuário do Elastic Load Balancing
- Monitorar e registrar em log no Guia do desenvolvedor do AWS AppSync
- Registro e monitoramento no Amazon Cognito no Guia do desenvolvedor do Amazon Cognito
- Visualização de registros do App Runner transmitidos para o CloudWatch Logs e visualização das métricas de serviço do App Runner relatadas CloudWatch no Guia do desenvolvedor AWS App Runner

- Amazon CloudWatch Logs — Monitore, armazene e acesse seus arquivos de log de AWS CloudTrail ou de outras fontes. Para obter mais informações, consulte O que é o Amazon CloudWatch Logs? .
- Amazon CloudWatch Events — Automatize seus AWS serviços e responda automaticamente aos eventos do sistema. Os eventos dos AWS serviços são entregues aos CloudWatch Eventos quase em tempo real, e você pode especificar ações automatizadas a serem tomadas quando um evento corresponde a uma regra que você escreveu. Para obter mais informações, consulte O que é Amazon CloudWatch Events?
- AWS CloudTrail Monitoramento de log — Compartilhe arquivos de log entre contas, monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs, grave aplicativos de processamento de log em Java e valide se seus arquivos de log não foram alterados após a entrega. CloudTrail Para obter mais informações, consulte Registro de chamadas de API do AWS CloudTrail com Trabalhar com arquivos de CloudTrail log no Guia AWS CloudTrail do usuário.

- AWS Config— Visualize a configuração dos AWS recursos em sua AWS conta, incluindo como os recursos estão relacionados entre si e como foram configurados no passado, para que você possa ver como as configurações e os relacionamentos mudam com o tempo.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento AWS WAF AWS Shield Advanced envolve o monitoramento manual dos itens que os CloudWatch alarmes não cobrem. Você pode visualizar o AWS WAF Shield Advanced e outros AWS Management Console painéis para ver o estado do seu AWS ambiente. CloudWatch Recomendamos que você também verifique os arquivos de log quanto aos seus web ACLs e regras.

- Por exemplo, para visualizar o AWS WAF painel:
  - Na guia Solicitações da página AWS WAF Web ACLs, visualize um gráfico do total de solicitações e solicitações que correspondem a cada regra que você criou. Para ter mais informações, consulte Visualizar um exemplo de solicitações da web.
- Veja a página CloudWatch inicial do seguinte:
  - Alertas e status atual
  - Gráficos de alertas e recursos
  - Estado de integridade do serviço

  Além disso, você pode usar CloudWatch para fazer o seguinte:
  - Criar painéis personalizados para monitorar os serviços de seu interesse.
  - Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências.
  - Pesquise e navegue por todas as suas métricas AWS de recursos.
  - Criar e editar alertas para ser notificado sobre problemas.

Monitoramento com a Amazon CloudWatch

Você pode monitorar solicitações da web, ACLs e regras da web usando a Amazon CloudWatch, que coleta e processa dados brutos de AWS WAF e AWS Shield Advanced em métricas legíveis e quase em tempo real. Você pode usar estatísticas na Amazon CloudWatch para ter uma perspectiva sobre o desempenho do seu aplicativo ou serviço web. Para obter mais informações, consulte O que está CloudWatch no Guia CloudWatch do usuário da Amazon.

> **Note**
>
> CloudWatch métricas e alarmes não estão habilitados para o Firewall Manager.

Você pode criar um CloudWatch alarme da Amazon que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alerta observa uma única métrica ao longo de um período especificado por você e realiza uma ou mais ações com base no valor da métrica em relação a um limite especificado ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS ou uma política de Auto Scaling. Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos.

Tópicos

Visualizar métricas e dimensões

As métricas são agrupadas primeiro pelo namespace do serviço e depois pelas várias combinações de dimensões em cada namespace. AWS Firewall Manager não registra métricas.

- O AWS WAF namespace é `AWS/WAFV2`
- O namespace do Shield Advanced é `AWS/DDoSProtection`

> **Note**
>
> AWS WAF relata métricas uma vez por minuto.
> O Shield Advanced relata métricas uma vez por minuto durante um evento e com menos frequência em outras ocasiões.

Use os procedimentos a seguir para visualizar as métricas de AWS WAF AWS Shield Advanced e.

Para visualizar métricas usando o CloudWatch console

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região para aquela em que seus AWS recursos estão localizados. Para CloudFront, escolha a região Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, em Métricas, escolha Todas as métricas e pesquise o serviço na guia Procurar.

Para visualizar métricas usando a AWS CLI

- Para o AWS/WAFV2, em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

  Para o Shield Advanced, em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF métricas e dimensões

AWS WAF relata métricas uma vez por minuto. AWS WAF fornece métricas e dimensões no `AWS/WAFV2` namespace.

Você pode ver informações resumidas das AWS WAF métricas por meio do AWS WAF console, na guia de visão geral do tráfego da ACL da web. Para obter mais informações, acesse o console ou consultePainéis de visão geral do tráfego de web ACL.

Você pode ver as seguintes métricas para ACLs da web, regras, grupos de regras e rótulos.

- Suas regras — As métricas são agrupadas pela ação da regra. Por exemplo, quando você testa uma regra no Count modo, suas correspondências são listadas como `Count` métricas para a Web ACL.
- Seus grupos de regras — As métricas dos seus grupos de regras estão listadas nas métricas do grupo de regras.

- Grupos de regras pertencentes a outra conta — As métricas do grupo de regras geralmente são visíveis somente para o proprietário do grupo de regras. No entanto, se você substituir a ação da regra por uma regra, as métricas dessa regra serão listadas em suas métricas de ACL da web. Além disso, os rótulos adicionados por qualquer grupo de regras são listados em suas métricas de ACL da web

  Os grupos de regras nessa categoria sãoAWS Regras gerenciadas para AWS WAF,AWS Marketplace grupos de regras gerenciados,Grupos de regras fornecidos por outros serviços, e grupos de regras que são compartilhados com você por outra conta.
- Rótulos - Os rótulos que foram adicionados a uma solicitação da web durante a avaliação são listados nas métricas dos rótulos da ACL da web. Você pode acessar as métricas de todos os rótulos, independentemente de terem sido adicionados por suas regras e grupos de regras ou por regras em um grupo de regras de propriedade de outra conta.

Tópicos

ACL da web, grupo de regras e métricas e dimensões de regras

ACL da web, grupo de regras e métricas de regras

Métrica	Descrição
`AllowedRequests`	O número de solicitações da web permitidas. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`BlockedRequests`	O número de solicitações da web bloqueadas. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CountedRequests`	O número de solicitações da web contadas.

Métrica	Descrição
	Critérios de relatório: há um valor diferente de zero. Uma solicitação da web contada é aquela que corresponde a pelo menos uma das regras. A contagem de solicitações é normalmente usada para teste. Estatística válida: soma
`CaptchaRequests`	O número de solicitações da web que tiveram controles de CAPTCHA aplicados. Critérios de relatório: há um valor diferente de zero. Uma solicitação de CAPTCHA na web é aquela que corresponde a uma regra que tem uma configuração de ação CAPTCHA. Essa métrica registra todas as solicitações correspondentes, independentemente de elas terem um token de CAPTCHA válido. Estatística válida: soma
`RequestsWithValidCaptchaTok en`	O número de solicitações da web que tiveram controles de CAPTCHA aplicados e que tinham um token de CAPTCHA válido. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CaptchasAttempted`	O número de soluções que foram enviadas por um usuário final em resposta a um desafio de quebra-ca beça CAPTCHA. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Métrica	Descrição
`CaptchasSolved`	O número de soluções de quebra-cabeça CAPTCHA enviadas que resolveram o quebra-cabeça com sucesso. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`ChallengeRequests`	O número de solicitações da web que tiveram controles de CAPTCHA aplicados. Critérios de relatório: há um valor diferente de zero. Uma solicitação de desafio na web é aquela que corresponde a uma regra que tem uma configuração de ação Challenge. Essa métrica registra todas as solicitações correspondentes, independentemente de elas terem um token de desafio válido. Estatística válida: soma
`RequestsWithValidChallengeToken`	O número de solicitações da web que tiveram controles de desafio aplicados e que tinham um token de desafio válido. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Métrica	Descrição
`PassedRequests`	O número de solicitações aprovadas. Isso é usado somente para solicitações que passam por uma avaliação de grupo de regras sem corresponder a nenhuma das regras do grupo de regras. Critérios de relatório: há um valor diferente de zero. As solicitações passadas são solicitações que não coincidem com nenhuma regra contida no grupo de regras. Estatística válida: soma

ACL da web, grupo de regras e dimensões de regras

Dimensão	Descrição
`Region`	Obrigatório para todos os tipos de recursos protegidos, exceto para CloudFront distribuições da Amazon.
`Rule`	Um dos seguintes: • O nome da métrica da `Rule`. • ALL, que representa todas as regras em um WebACL ou um `RuleGroup` . • `Default_Action` (somente quando combinado com a dimensão `WebACL`), que representa a ação atribuída a qualquer solicitação cuja avaliação não foi terminada por ação de uma regra na ACL da web.
`RuleGroup`	O nome da métrica da `RuleGroup` .
`WebACL`	O nome da métrica da `WebACL`.
`Country`	País de origem da solicitação. Trata-se da designação de dois caracteres do padrão 3166 da Organização

Dimensão	Descrição
	Internacional de Padronização (ISO). Por exemplo, US para os Estados Unidos e UA para a Ucrânia. Se uma solicitação tiver um cabeçalho `X-Forwarded-For` , o AWS WAF o usará para determinar essa configuração. Caso contrário, o AWS WAF usa o país do IP do cliente. Essa determinação é independente de qualquer lógica que você usa em suas regras para determinar o país de origem. AWS WAF determina a localização dos IPs usando bancos de dados MaxMind GeoIP.
`Attack`	O tipo de ataque AWS WAF identificado na solicitação, com base nas regras e grupos de regras que você usa na sua ACL da web. Suas regras e as regras dos grupos básicos de regras AWS gerenciadas podem identificar os tipos de ataque. Por exemplo, as correspondências de regras de cross-site scripting (XSS) identificam os tipos de ataque XSS e as regras baseadas em intervalos identificam os tipos de ataques volumétricos. O tipo de ataque geralmente indica o tipo de regra que encerrou a avaliação da solicitação da web.
`Device`	O tipo de dispositivo do cliente que enviou a solicitação, obtido do cabeçalho `user-agent` da solicitação da web.
`ManagedRuleGroup`	O nome da métrica da `ManagedRuleGroup` .
`ManagedRuleGroupRule`	A regra dentro do `ManagedRuleGroup` que foi correspondida.

Métricas e dimensões do rótulo

Métricas para os rótulos adicionados às solicitações durante a avaliação pelas suas regras e pelos grupos de regras gerenciadas que você usa na sua ACL da web. Para mais informações, consulte Rótulos em solicitações da web.

Para qualquer solicitação da web, AWS WAF armazena métricas para no máximo 100 rótulos. Sua avaliação de ACL da web pode aplicar mais de 100 rótulos e comparar com mais de 100 rótulos, mas apenas os 100 primeiros são refletidos nas métricas.

Métricas de rótulo

Métrica	Descrição
`AllowedRequests`	O número de rótulos em solicitações da web que tiveram a configuração de ação Allow aplicada. Os rótulos podem ter sido adicionados a qualquer momento durante a avaliação da solicitação da web. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`BlockedRequests`	O número de rótulos em solicitações da web que tiveram a configuração de ação Block aplicada. Os rótulos podem ter sido adicionados a qualquer momento durante a avaliação da solicitação da web. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CountedRequests`	O número de rótulos adicionados às solicitações da web pelas regras do grupo de regras que têm uma configuração de ação Count. Essa métrica só está disponível para o proprietário de um grupo de regras, para regras dentro do grupo de regras. Em outros casos, as métricas de rótulo de contagem são agrupadas na ação de encerramento que foi aplicada à solicitação, como Allow ou Block.

Métrica	Descrição
	Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CaptchaRequests`	O número de rótulos em solicitações da web que tiveram uma ação CAPTCHA de encerramento aplicada. Os rótulos podem ter sido adicionados a qualquer momento durante a avaliação da solicitação da web. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`ChallengeRequests`	O número de rótulos em solicitações da web que tiveram uma ação Challenge de encerramento aplicada. Os rótulos podem ter sido adicionados a qualquer momento durante a avaliação da solicitação da web. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`AllowRuleMatch`	O número de regras correspondentes que geraram o rótulo associado e encerraram a avaliação da solicitação com uma Allow ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`BlockRuleMatch`	O número de regras correspondentes que geraram o rótulo associado e encerraram a avaliação da solicitação com uma Block ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Métrica	Descrição
`CountRuleMatch`	O número de regras correspondentes que geraram o rótulo associado e aplicaram uma Count ação. Uma solicitação pode resultar em várias instâncias dessa métrica, se várias regras forem configuradas com o mesmo rótulo e ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CaptchaRuleMatch`	O número de regras correspondentes que geraram o rótulo associado e encerraram a avaliação da solicitação com uma CAPTCHA ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`ChallengeRuleMatch`	O número de regras correspondentes que geraram o rótulo associado e encerraram a avaliação da solicitação com uma Challenge ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`CaptchaRuleMatchWithValidToken`	O número de regras correspondentes que geraram o rótulo associado e aplicaram uma ação sem encerramentoCAPTCHA. Uma solicitação pode resultar em várias instâncias dessa métrica, se várias regras forem configuradas com o mesmo rótulo e ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Métrica	Descrição
`ChallengeRuleMatchWithValidToken`	O número de regras correspondentes que geraram o rótulo associado e aplicaram uma ação sem encerramentoChallenge. Uma solicitação pode resultar em várias instâncias dessa métrica, se várias regras forem configuradas com o mesmo rótulo e ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Dimensões de rótulo

Dimensão	Descrição
`Region`	Obrigatório para todos os tipos de recursos protegidos, exceto para CloudFront distribuições da Amazon.
`WebACL`	O nome da métrica da `WebACL`.
`RuleGroup`	O nome da métrica da `RuleGroup` . Usada para a métrica `CountedRequests` .
`LabelNamespace`	O prefixo do namespace do rótulo que foi adicionado à solicitação.
`Label`	O nome do rótulo que foi adicionado à solicitação.
`Context`	O grupo de regras gerenciadas que serviu como contexto da adição do rótulo. Por exemplo, o contexto para rótulos de gerenciamento de tokens, como `awswaf:managed:token:accepted` é o grupo de regras AWS WAF gerenciadas que usa o gerenciamento de tokens na solicitação, como o Bot Control ou o grupo de regras gerenciadas pelo ATP. Essa dimensão não se aplica a todos os rótulos.

Métricas e dimensões de visibilidade de bots gratuitas

Quando você não usa o Bot Control em sua ACL da web, AWS WAF aplica o grupo de regras gerenciadas do Bot Control a uma amostra de suas solicitações da web, sem custo adicional. Isso pode dar uma ideia do tráfego de bots que está chegando aos seus recursos protegidos. Para obter informações sobre Controle de bots, consulte AWS WAF Grupo de regras do Bot Control.

Métricas de visibilidade de bots gratuitas

Métrica	Descrição
`SampleAllowedRequest`	O número de solicitações de amostra que têm Allow ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`SampleBlockedRequest`	O número de solicitações de amostra que têm Block ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`SampleCaptchaRequest`	O número de solicitações de amostra que têm CAPTCHA ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`SampleChallengeRequest`	O número de solicitações de amostra que têm Challenge ação. Critérios de relatório: há um valor diferente de zero. Estatística válida: soma
`SampleCountRequest`	O número de solicitações de amostra que têm Count ação.

Métrica	Descrição
	Critérios de relatório: há um valor diferente de zero. Estatística válida: soma

Dimensões de visibilidade de bots gratuitas

Dimensão	Descrição
`Region`	Obrigatório para todos os tipos de recursos protegidos, exceto para CloudFront distribuições da Amazon.
`WebACL`	O nome da métrica da `WebACL`.
`BotCategory`	O nome da categoria do bot detectado, com base nos rótulos de solicitação da web.
`VerificationStatus`	O nome do status de verificação do bot detectado, com base nos rótulos de solicitação da web.
`Signal`	O nome dos sinais do bot detectado, com base nos rótulos de solicitação da web.

AWS Shield Advanced métricas

A Shield Advanced publica as métricas de CloudWatch detecção, mitigação e principais colaboradores da Amazon para todos os recursos que protege. Essas métricas melhoram sua capacidade de monitorar seus recursos, possibilitando a criação e configuração de CloudWatch painéis e alarmes para eles.

O console Shield Advanced apresenta resumos de muitas das métricas que ele registra. Para mais informações, consulte Visibilidade de eventos de DDoS.

Se você habilitar a mitigação automática de DDoS na camada de aplicativo para uma proteção na camada de aplicativo,

Locais de relatórios métricos

O Shield Advanced relata métricas na região Leste dos EUA (Norte da Virgínia), `us-east-1` para o seguinte:

- Os serviços globais Amazon CloudFront e Amazon Route 53.
- Grupos de proteção. Para mais informações sobre a proteção de dados nos grupos, acesse AWS Shield Advanced grupos de proteção.

Para outros tipos de recursos, o Shield Advanced relata métricas na região do recurso.

Cronometragem do relatório de métricas

O Shield Advanced reporta métricas para a Amazon CloudWatch sobre um AWS recurso com mais frequência durante eventos de DDoS do que quando nenhum evento está em andamento. O Shield Advanced relata métricas uma vez por minuto durante um evento e, em seguida, uma vez logo após o término do evento.

Enquanto não há nenhum ataque em andamento, o Shield Advanced relata métricas uma vez ao dia, no horário atribuído ao recurso. Esse relatório periódico mantém as métricas ativas e disponíveis para uso em CloudWatch alarmes e painéis personalizados.

Recomendações de alarme

Recomendamos que você crie alarmes para notificá-lo sobre circunstâncias que exijam atenção. Como ponto de partida, você pode criar um alarme para cada recurso protegido que informa quando a métrica `DDoSDetected` de detecção é diferente de zero. Um valor diferente de zero nessa métrica não significa necessariamente que um ataque de DDoS esteja em andamento, mas recomendamos examinar mais de perto o status do recurso quando a métrica estiver nesse estado.

Para floods de solicitações, recomendamos que você crie alarmes para verificações compostas que também considerem fatores como integridade do aplicativo e volume de solicitações da web. Você pode optar por alertar sobre as outras três métricas que relatam o volume de tráfego para várias dimensões do vetor de ataque. Ao considerar a capacidade do seu aplicativo e alertar quando o tráfego estiver se aproximando das limitações do seu aplicativo, você pode criar um conjunto de regras que o notificam conforme necessário, sem muitos ruídos indesejados.

Tópicos

- Métricas de detecção
- Métricas de mitigação

- Métricas dos principais colaboradores

Métricas de detecção

O Shield Advanced fornece as métricas e as dimensões no `AWS/DDoSProtection` namespace.

Métricas de detecção

Métrica	Descrição
`DDoSDetected`	Indica se um evento de DDoS está em andamento para um determinado nome do recurso da Amazon (ARN). Essa métrica tem um valor diferente de zero durante um evento.
`DDoSAttackBitsPerSecond`	O número de bits observados durante um evento de DDoS para um determinado nome do recurso da Amazon (ARN). Esta métrica está disponível apenas para eventos DDoS de camada de rede e transporte (camada 3 e camada 4). Essa métrica tem um valor diferente de zero durante um evento. Unidades: bits
`DDoSAttackPacketsPerSecond`	O número de pacotes observados durante um evento de DDoS para um determinado nome de recurso da Amazon (ARN). Esta métrica está disponível apenas para eventos DDoS de camada de rede e transporte (camada 3 e camada 4). Essa métrica tem um valor diferente de zero durante um evento. Unidades: pacotes

Métrica	Descrição
DDoSAttackRequestsPerSecond	O número de solicitações observadas durante um evento de DDoS para um determinado nome de recurso da Amazon (ARN). Esta métrica está disponível apenas para eventos de DDoS da camada 7. A métrica é relatada apenas para eventos de camada 7 mais significativos. Essa métrica tem um valor diferente de zero durante um evento. Unidades: solicitações

O Shield Advanced publica a métrica DDoSDetected sem nenhuma outra dimensão. As métricas de detecção restantes incluem as dimensões AttackVector que correspondem ao tipo de ataque da lista a seguir:

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood

- `UDPFragment`
- `UDPTraffic`
- `UDPReflection`

Métricas de mitigação

O Shield Advanced fornece métricas e dimensões no `AWS/DDoSProtection` namespace.

Métricas de mitigação

Métrica	Descrição
`VolumePacketsPerSecond`	O número de pacotes por segundo que foram descartados ou aprovados por uma mitigação implantada em resposta a um evento detectado . Unidades: pacotes

Dimensões de mitigação

Dimensão	Descrição
`ResourceArn`	Nome do recurso da Amazon (ARN)
`MitigationAction`	O resultado de uma mitigação aplicada. Os valores possíveis são `Pass` ou `Drop`.

Métricas dos principais colaboradores

O Shield Advanced fornece métricas no `AWS/DDoSProtection` namespace.

Métricas dos principais colaboradores

Métrica	Descrição
`VolumePacketsPerSecond`	O número de pacotes por segundo de um colaborador principal.

Métrica	Descrição
	Unidades: pacotes
`VolumeBitsPerSecond`	O número de pacotes por segundo de um colaborador principal. Unidades: bits

O Shield Advanced publica as métricas dos principais colaboradores por combinações de dimensões que caracterizam os colaboradores do evento. Você pode usar qualquer uma das combinações de dimensões a seguir para qualquer uma das métricas dos principais contribuidores:

- `ResourceArn`, `Protocol`
- `ResourceArn`, `Protocol`, `SourcePort`
- `ResourceArn`, `Protocol`, `DestinationPort`
- `ResourceArn`, `Protocol`, `SourceIp`
- `ResourceArn`, `Protocol`, `SourceAsn`
- `ResourceArn`, `TcpFlags`

Dimensões dos principais contribuidores

Dimensão	Descrição
`ResourceArn`	Nome do recurso da Amazon (ARN).
`Protocol`	Nome do protocolo IP, `TCP` ou `UDP`.
`SourcePort`	Porta TCP ou UDP de origem.
`DestinationPort`	Porta TCP ou UDP de destino.
`SourceIp`	Endereço IP de origem.
`SourceAsn`	Número de sistema autônomo (ASN) da origem.
`TcpFlags`	Uma combinação de sinalizadores presentes em um pacote TCP, separados por um traço (`-`). Os

Dimensão	Descrição
	sinalizadores monitorados são `ACK`, `FIN`, `RST` e `SYN`. Esse valor de dimensão sempre aparece classificado em ordem alfabética. Por exemplo, `ACK-FIN-RST-SYN`, `ACK-SYN` e `FIN-RST`.

AWS Firewall Manager notificações

AWS Firewall Manager não registra métricas, então você não pode criar CloudWatch alarmes da Amazon especificamente para o Firewall Manager. No entanto, você pode configurar notificações do Amazon SNS para alertá-lo para ataques potenciais. Para criar notificações do Amazon SNS no Firewall Manager, consulte Etapa 4: Configurar notificações e alarmes do Amazon SNS CloudWatch .

Registro de chamadas de API do AWS CloudTrail com

AWS WAF, AWS Shield Advanced, e AWS Firewall Manager estão integrados AWS CloudTrail a um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço. CloudTrail captura um subconjunto de chamadas de API para esses serviços como eventos, incluindo chamadas dos consoles AWS WAF Shield Advanced ou Firewall Manager e de chamadas de código para as APIs AWS WAF Shield Advanced ou Firewall 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 WAF Shield Advanced ou o Firewall Manager. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação feita a esses serviços, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando uma atividade de evento suportada ocorre no AWS WAF Shield Advanced ou no Firewall 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 Shield Advanced ou do Firewall Manager, crie uma trilha. AWS WAF 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 do . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

AWS WAF informações em AWS CloudTrail

Todas AWS WAF as ações são registradas AWS CloudTrail e documentadas na Referência da AWS WAF API. Por exemplo, chamadas para `ListWebACL` `UpdateWebACL`, e `DeleteWebACL` geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte CloudTrailUserIdentity Element.

Exemplo: entradas do arquivo de AWS WAF log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. AWS CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por

diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Veja a seguir exemplos de entradas de CloudTrail registro para operações de AWS WAF Web ACL.

Exemplo: entrada de CloudTrail registro para `CreateWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
```

```
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
```

```
}
```

Exemplo: entrada de CloudTrail registro para `GetWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
```

```
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Exemplo: entrada de CloudTrail registro para `UpdateWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
```

```
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


Exemplo: entrada de CloudTrail registro para `DeleteWebACL`


```
{
```

```
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Exemplo: entradas AWS WAF clássicas do arquivo de log

AWS WAF Classic é a versão anterior do AWS WAF. Para mais informações, consulte AWS WAF clássico.

A entrada de log demonstra as operações de `DeleteRule`, `CreateRule`, `GetRule` e `UpdateRule`:


```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
```

```
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
      "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
      "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
```

```
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
```

```
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```

AWS Shield Advanced informações em CloudTrail

AWS Shield Advanced suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Exemplo: entradas do arquivo de log do Shield Advanced

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra as `ListProtections` ações `DeleteProtection` e.


```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
   "eventTime": "2018-01-10T21:31:14Z",
   "eventSource": "shield.amazonaws.com",
   "eventName": "DeleteProtection",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "AWS Internal",
   "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
   "requestParameters": {
     "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
   },
   "responseElements": null,
   "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
   "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
   "eventType": "AwsApiCall",
   "apiVersion": "AWSShield_20160616",
   "recipientAccountId": "123456789012"
 },
 {
```

```
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "12345678909876543212 3",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```


AWS Firewall Manager informações em CloudTrail

AWS Firewall Manager suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel

- GetPolicy
- ListComplianceStatus
- ListPolicies

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Exemplo: entradas do arquivo de log do Firewall Manager

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a ação `GetAdminAccount` -->.

```
{
               "eventVersion": "1.05",
               "userIdentity": {
                              "type": "AssumedRole",
                              "principalId": "123456789098765432123 1",
                              "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                              "accountId": "123456789012",
                              "accessKeyId": "1AFGDT647FHU83JHFI81H",
                              "sessionContext": {
                                             "attributes": {
```

```
                                                                "mfaAuthenticated":
"false",
                                                                "creationDate":
"2018-04-14T02:51:50Z"
                                                            },
                                                    "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
"123456789098765432123 1",
                                                                "arn":
"arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
"123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                      }
                                    },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

Usando a AWS Shield Advanced API AWS WAF and

Esta seção descreve como fazer solicitações à API AWS WAF e ao Shield Advanced para criar e gerenciar conjuntos de partidas, regras e ACLs da web, bem AWS WAF como sua assinatura e proteções no Shield Advanced. Esta seção mostrará os componentes das solicitações, o conteúdo das respostas e a forma de autenticar solicitações.

Tópicos

Usando os AWS SDKs

Se você usa uma linguagem que AWS fornece um SDK para, use o SDK em vez de tentar trabalhar com as APIs. Os SDKs simplificam a autenticação, se integram facilmente ao seu ambiente de desenvolvimento e fornecem acesso fácil aos comandos e ao AWS WAF Shield Advanced. Para obter mais informações sobre os AWS SDKs, consulte Fazer download das ferramentas o tópicoConfigurando sua conta para usar os serviços.

Fazendo solicitações HTTPS para o AWS WAF Shield Advanced

AWS WAF e as solicitações do Shield Advanced são solicitações HTTPS, conforme definido pela RFC 2616. Como qualquer solicitação HTTP, uma solicitação para AWS WAF ou Shield Advanced contém um método de solicitação, um URI, cabeçalhos de solicitação e um corpo de solicitação. A resposta contém um código de status HTTP, cabeçalhos de resposta e, às vezes, corpo da resposta.

URI da solicitação

O URI da solicitação é sempre uma barra individual, `/`.

Cabeçalhos HTTP

AWS WAF e o Shield Advanced exigem as seguintes informações no cabeçalho de uma solicitação HTTP:

Host (obrigatório)

O endpoint que especifica onde seus recursos são criados. Para obter informações sobre endpoints, consulte endpoints de serviço da AWS. Por exemplo, o valor do `Host` cabeçalho AWS WAF para uma CloudFront distribuição é`waf.amazonaws.com:443`.

x-amz-date ou Data (Obrigatório)

A data usada para criar a assinatura contida no cabeçalho `Authorization`. Especifique a data no formato padrão ISO 8601, no horário UTC, como mostrado no exemplo a seguir:

```
x-amz-date: 20151007T174952Z
```

Você deve incluir `x-amz-date` ou `Date`. (Algumas bibliotecas de cliente HTTP não permitem a definição do cabeçalho `Date`). Quando um `x-amz-date` cabeçalho está presente, AWS WAF ignora qualquer `Date` cabeçalho ao autenticar a solicitação.

O registro de data e hora deve estar dentro de 15 minutos da hora do AWS sistema quando a solicitação for recebida. Se não estiver, a solicitação falhará, com o código de erro `RequestExpired`, para impedir que outra pessoa reproduza suas solicitações.

Autorização (obrigatório)

As informações necessárias para solicitar a autenticação. Para mais informações sobre a criação desse cabeçalho, consulte Autenticação de solicitações.

X-Amz-Target (obrigatório)

Uma concatenação de `AWSWAF_` ou `AWSShield_`, a versão da API sem pontuação, um ponto final (`.`) e o nome da operação, por exemplo:

`AWSWAF_20150824.CreateWebACL`

Content-Type (condicional)

Especifica que o tipo de conteúdo é JSON, bem como a versão do JSON, como mostrado no exemplo a seguir:

```
Content-Type: application/x-amz-json-1.1
```

Condição: Obrigatório para solicitações do `POST`.

Content-Length (condicional)

Comprimento da mensagem (sem cabeçalhos) de acordo com a RFC 2616.

Condição: obrigatório se o corpo da solicitação em si contiver informações (a maioria dos toolkits adiciona esse cabeçalho automaticamente).

Veja a seguir um exemplo de cabeçalho para uma solicitação HTTP para criar uma web ACL no AWS WAF:

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

Corpo da solicitação HTTP

Muitas AWS WAF ações da API Shield Advanced exigem que você inclua dados formatados em JSON no corpo da solicitação.

A solicitação do exemplo a seguir usa uma instrução JSON simples para atualizar um `IPSet` para incluir o endereço IP 192.0.2.44 (representado na notação CIDR como 192.0.2.44/32):

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
```

```
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive

{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
}
```

Respostas HTTP

Todas as ações da API All AWS WAF and Shield Advanced incluem dados formatados em JSON na resposta.

A seguir são apresentados alguns cabeçalhos importantes na resposta HTTP e a explicação sobre como você deve lidar com eles em seu aplicativo, se aplicável:

HTTP/1.1

Esse cabeçalho é acompanhado de um código de status. O código de status 200 indica uma operação bem-sucedida.

Tipo: string

x-man- RequestId

Um valor criado por AWS WAF ou Shield Advanced que identifica exclusivamente sua solicitação, por exemplo,. `K2QH8DN0U907N97FNA2GDLL80BVV4KQNS05AEMVJF66Q9ASUAAJG` Se você tiver um problema com AWS WAF, AWS pode usar esse valor para solucionar o problema.

Tipo: string

Content-Length

O comprimento do corpo da resposta, em bytes.

Tipo: string

Data

A data e a hora em que AWS WAF o Shield Advanced respondeu, por exemplo, quarta-feira, 7 de outubro de 2015, 12:00:00 GMT.

Tipo: string

Respostas de erro

Se uma solicitação resultar em erro, a resposta HTTP conterá os seguintes valores:

- Um documento de erro JSON como o corpo da resposta
- Content-Type
- O código de status HTTP 3xx, 4xx ou 5xx aplicável

Veja a seguir um exemplo de um documento de erro de JSON:

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

Autenticação de solicitações

Se você usa uma linguagem que AWS fornece um SDK para, recomendamos que você use o SDK. Todos os AWS SDKs simplificam muito o processo de assinatura de solicitações e economizam uma quantidade significativa de tempo em comparação com o uso da API AWS WAF ou Shield Advanced. Além disso, os SDKs integram-se facilmente com o ambiente de desenvolvimento e fornecem acesso fácil aos comandos relacionados.

AWS WAF e o Shield Advanced exigem que você autentique todas as solicitações enviadas assinando a solicitação. Para assinar uma solicitação, deve calcular uma assinatura digital usando

uma função hash criptográfica que retorna um valor hash baseado na entrada. A entrada inclui o texto da solicitação e a chave de acesso secreta. A função de hash retorna um valor de hash que você inclui na solicitação como sua assinatura. A assinatura é parte do cabeçalho `Authorization` de sua solicitação.

Depois de receber sua solicitação, AWS WAF o Shield Advanced recalcula a assinatura usando a mesma função de hash e entrada que você usou para assinar a solicitação. Se a assinatura resultante corresponder à assinatura na solicitação, AWS WAF ou se o Shield Advanced processar a solicitação. Caso contrário, a solicitação será rejeitada.

AWS WAF e o Shield Advanced oferece suporte à autenticação usando o AWS Signature Version 4. O processo para calcular uma assinatura pode ser dividido em três tarefas:

Tarefa 1: Criar uma solicitação canônica

Crie sua solicitação HTTP em formato canônico, como descrito em Tarefa 1: Crie uma solicitação canônica para o Signature versão 4 no Referência geral da Amazon Web Services.

Tarefa 2: Criar uma string para assinar

Crie uma string que será usada como um dos valores de entrada para sua função hash criptográfica. A string, chamada de string para assinar, é uma concatenação dos seguintes valores:

- Nome do algoritmo hash
- Data da solicitação
- String de escopo de credencial
- Solicitação canonicalizada da tarefa anterior

A string do escopo credencial em si é uma concatenação da data, da região e de informações do serviço.

Para o parâmetro `X-Amz-Credential`, especifique o seguinte:

- O código para o endpoint ao qual você está enviando a solicitação, `us-east-2`
- `waf` para a abreviação do serviço

Por exemplo: .

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

Tarefa 3: Crie uma assinatura

Crie uma assinatura para sua solicitação usando uma função hash criptográfica que aceita duas strings de entrada:

- Sua string para assinar, da Tarefa 2.
- Uma chave derivada. Para calcular a chave derivada, inicie sua chave de acesso secreta e use a string do escopo credencial para criar uma série de códigos de autenticação de mensagem baseados em hash (HMACs).

Informações relacionadas

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

Os seguintes recursos estão disponíveis para AWS WAF AWS Shield Advanced, AWS Firewall Manager e.

- Diretrizes para implementação AWS WAF — Publicação técnica com recomendações atuais de implementação AWS WAF para proteger aplicativos web novos e existentes.
- AWS fóruns de discussão — Um fórum comunitário para discutir questões técnicas relacionadas a este e a outros serviços. AWS
- AWS WAF Fórum de discussão — Um fórum baseado na comunidade para desenvolvedores discutirem questões técnicas relacionadas a. AWS WAF
- Fóruns de discussão do Shield Advanced: um fórum comunitário para desenvolvedores discutirem questões técnicas relacionadas ao Shield Advanced.
- AWS WAF informações do produto — A página principal da Web para obter informações sobre AWS WAF, incluindo recursos, preços e muito mais.
- Informações sobre o produto Shield Advanced: a principal página da web para obter informações sobre o Shield Advanced, incluindo recursos, definições de preços e muito mais.

Os seguintes recursos estão disponíveis para a Amazon web Services.

- Aulas e workshops — Links para cursos especializados e baseados em funções, além de laboratórios individualizados para ajudar a aprimorar suas AWS habilidades e ganhar experiência prática.
- AWS Centro do desenvolvedor — explore tutoriais, baixe ferramentas e saiba mais sobre eventos para AWS desenvolvedores.
- AWS Ferramentas para desenvolvedores — Links para ferramentas de desenvolvedor, SDKs, kits de ferramentas de IDE e ferramentas de linha de comando para desenvolver e gerenciar AWS aplicativos.
- Centro de recursos de introdução — Saiba como configurar seu aplicativo Conta da AWS, participar da AWS comunidade e lançar seu primeiro aplicativo.
- Tutoriais práticos — Siga os tutoriais para iniciar seu step-by-step primeiro aplicativo no. AWS

- AWS Whitepapers — Links para uma lista abrangente de AWS white papers técnicos, abrangendo tópicos como arquitetura, segurança e economia e criados por arquitetos de AWS soluções ou outros especialistas técnicos.
- AWS Support Center — O hub para criar e gerenciar seus AWS Support casos. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e. AWS Trusted Advisor
- AWS Support— A principal página da web com informações sobre AWS Support um one-on-one canal de suporte de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- Entrar em contato:Um ponto central de contato para consultas relativas a faturas da AWS , contas, eventos, uso abusivo e outros problemas.
- AWS Termos do site — Informações detalhadas sobre nossos direitos autorais e nossa marca registrada; sua conta, licença e acesso ao site; e outros tópicos.

Histórico do documento

Esta página lista alterações significativas nesta documentação.

Às vezes, os recursos do serviço são lançados de forma incremental nas AWS regiões em que um serviço está disponível. Atualizamos esta documentação apenas para a primeira versão. Não fornecemos informações sobre a disponibilidade da região nem anunciamos lançamentos subsequentes da região. Para obter informações sobre a disponibilidade de recursos de serviço na região e para assinar notificações sobre atualizações, consulte O que há de novo em AWS? .

Alteração	Descrição	Data
Esclareça como a análise corporal JSON funciona	Cobertura atualizada da inspeção corporal JSON para esclarecer como AWS WAF lida com a análise e o comportamento alternativo da análise corporal.	25 de junho de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	Conjunto de regras do sistema operacional Linux atualizado.	6 de junho de 2024
AWS WAF mudanças de políticas gerenciadas	Atualizado `WAFV2LoggingServiceRolePolicy` e `AWSServiceRoleForWAFV2Logging` para adicionar IDs de declaração (Sids) às configurações de permissões.	3 de junho de 2024
AWS WAF rastreamento gerenciado de alterações de políticas	AWS WAF começou a rastrear as alterações na política gerenciada `WAFV2LoggingServiceRolePolicy` e na função vinculada ao serviço. `AWSServic`	3 de junho de 2024

	`eRoleForWAFV2Loggi ng`	
Regras AWS gerenciadas atualizadas para AWS WAF	Os grupos de regras gerenciadas do Bot Control, ATP e ACFP agora estão versionados e fornecerão notificações do SNS para atualizações de versão, da mesma forma que outras regras gerenciadas com versão. AWS	29 de maio de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do sistema operacion al POSIX,`AWSManage dRulesUnixRuleSet` .	28 de maio de 2024
CAPTCHAe Challenge ações	Foi adicionado um esclareci mento de que os clientes de navegador precisam de HTTPS para executar quebra-cabeças de CAPTCHA e desafios silenciosos.	24 de maio de 2024
Integração com o Amazon Security Lake	Agora você pode usar o Security Lake para coletar dados de tráfego da Web ACL. Para obter informaçõ es, consulte Coleta de dados de AWS serviços no guia do usuário do Amazon Security Lake.	22 de maio de 2024

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	21 de maio de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras gerenciadas para AWS WAF atualizar o grupo de regras do banco de dados SQLi.	14 de maio de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar as entradas inválidas conhecidas e os grupos de regras do sistema operacional POSIX.	8 de maio de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do sistema operacional Windows.	3 de maio de 2024
AWS WAF exemplos de código Kotlin para Android do SDK móvel	Código de exemplo adicionado para integrações Android baseadas em Kotlin.	2 de maio de 2024
AWS WAF métricas, dimensões adicionadas e novas métricas	AWS WAF adicionou uma nova dimensão para as métricas `ManagedRuleSetRule` nas regras e novas métricas para a ação de regra correspondente para as métricas do rótulo.	2 de maio de 2024

AWS Firewall Manager suporta políticas de ACL de rede	O Firewall Manager agora suporta o gerenciamento das listas de controle de acesso à rede (ACLs) da Amazon VPC por meio das políticas de ACL de rede do Firewall Manager.	25 de abril de 2024
AWS Firewall Manager atualizações da política de segurança	Atualizações `FMSServiceRolePolicy` para adicionar permissões para gerenciar ACLs de rede.	22 de abril de 2024
Lista atualizada de métricas de verificação de saúde	Removemos algumas métricas da lista daquelas que são comumente usadas em verificações de saúde.	16 de abril de 2024
Atualizações das políticas de grupo de segurança do Firewall Manager	Atualizamos nossas políticas de grupo de segurança de auditoria de uso e aprimoram os a documentação. Consulte a seção de política de auditoria de uso e as seções sobre melhores práticas e limitações.	2 de abril de 2024
Exemplos de controle de bots atualizados	Foram adicionados exemplos que descrevem o nível de inspeção desejado e exemplos existentes atualizados para refletir as melhores práticas.	27 de março de 2024

Exemplos de ATP atualizados	Foi adicionado um exemplo que descreve a configuração da inspeção de resposta e atualizou os exemplos existentes para refletir as melhores práticas.	27 de março de 2024
Exemplos atualizados de ACFP	Foi adicionado um exemplo que descreve a configuração da inspeção de resposta.	27 de março de 2024
Atualize os limites do fluxo de CloudWatch registros do Amazon Logs	AWS WAF não tem mais limites de ACL por web na publicação de registros em fluxos de registros de CloudWatch registros.	27 de março de 2024
AWS Shield Advanced proteções da camada de aplicação (camada 7)	Orientações gerais e de melhores práticas atualizadas para detecção e mitigação da camada de aplicativos, uso de ACL na web, regras baseadas em taxas e mitigação automática de DDoS na camada de aplicativos.	14 de março de 2024
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras de reputação de IP.	13 de março de 2024
Alterações nos limites de tamanho da inspeção corporal	AWS WAF agora suporta limites maiores de tamanho de inspeção corporal para alguns recursos regionais.	7 de março de 2024

Janela de avaliação configurável para regras baseadas em AWS WAF taxas	Agora você pode configurar a janela de tempo que as regras baseadas em taxas usam para contar as solicitações em 1, 2, 5 ou 10 minutos. O padrão é 5, que era a única opção antes desta versão.	28 de fevereiro de 2024
Informações de registro expandidas para CAPTCHA e Challenge	O nível superior `captchaResponse` e `challengeResponse` os campos agora são preenchidos com a última dessas ações a serem aplicadas a uma solicitação, seja ela encerrada ou não. Antes disso, esses campos eram preenchidos somente para ações de encerramento.	22 de fevereiro de 2024
JavaScript Gerenciamento de chaves da API CAPTCHA	Agora você pode excluir as chaves da API CAPTCHA JS por meio das APIs. AWS WAF	6 de fevereiro de 2024
AWS WAF CAPTCHA puzzles de áudio	A versão em áudio do quebra-cabeça CAPTCHA agora suporta vários idiomas.	6 de fevereiro de 2024
AWS WAF desafio e rotulagem de token CAPTCHA	O gerenciamento de token passou a adicionar rótulos para o token de CAPTCHA e aprimorou a rotulagem de token para o token de desafio.	20 de dezembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras de entradas inválidas conhecidas.	16 de dezembro de 2023

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras de entradas inválidas conhecidas.	14 de dezembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	6 de dezembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Controle de AWS WAF bots.	5 de dezembro de 2023
AWS Config Pré-requisitos atualizados do Firewall Manager	Se você usar uma função personalizada do IAM em vez da função gerenciada do Firewall Manager AWS Config, você deve garantir que sua política de permissão permita que o AWS Config gravador registre os recursos do Firewall Manager.	17 de novembro de 2023
AWS WAF painéis de console	Corrigimos a orientação para visualizar todas as regras e exemplos de solicitações de uma ACL da web no console. AWS WAF	17 de novembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras gerenciadas para AWS WAF atualizar o grupo de regras do Bot Control.	14 de novembro de 2023

AWS WAF console tem novos painéis de ACL da web	A página de ACL da web no AWS WAF console tem novos painéis de visão geral do tráfego da web.	14 de novembro de 2023
Grupo de regras gerenciadas do ATP atualizado	Informações de rótulo corrigidas para as regras `VolumetricIpFailedLoginResponseHigh` e `VolumetricSessionFailedLoginResponseHigh` .	13 de novembro de 2023
Grupo de regras gerenciadas do ACFP atualizado	Informações de rótulo corrigidas para as regras `VolumetricIPSuccessfulResponse` e `VolumetricSessionSuccessfulResponse` .	13 de novembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	2 de novembro de 2023
Mitigação automática de DDoS da camada de aplicação do Shield Advanced	O Shield Avançado passou a manter uma regra baseada em intervalos no grupo de regras de mitigação automática que limita o volume de solicitações de endereços IP conhecidos por serem fontes de ataques de DDoS.	31 de outubro de 2023

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	30 de outubro de 2023
O grupo de regras gerenciadas do Controle de Bots removeu o rótulo de sinal do CSP de solicitação	O grupo de regras gerenciadas do Controle de Bots removeu o rótulo de sinal que indica o provedor de serviços de nuvem (CSP).	28 de outubro de 2023
Rótulo de sinal do grupo de regras gerenciadas do Controle de Bots para o CSP de solicitação	Os rótulos de sinal do grupo de regras gerenciadas do Controle de Bots incluem um rótulo que indica o provedor de serviços de nuvem (CSP).	27 de outubro de 2023
Informações atualizadas de permissões AWS WAF do IAM	Para as AWS WAF ações que gerenciam associações de ACL da web, a seção de ações de política agora lista os requisitos de permissões para cada tipo de recurso de aplicativo da web.	25 de outubro de 2023
Gerenciamento do Firewall Manager de web ACLs modificadas	Quando você habilita o gerenciamento de web ACLs não associadas, o Firewall Manager não inclui as web ACLs modificadas na limpeza única de recursos não usados.	19 de outubro de 2023

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do sistema operacional POSIX, `AWSManagedRulesUnixRuleSet` .	12 de outubro de 2023
AWS WAF dimensões adicionadas às métricas	AWS WAF adicionou novas dimensões para visualizar métricas de ACL da web.	12 de outubro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	11 de outubro de 2023
Atualização da especificação do SDK AWS WAF móvel	Adicionou a operação `storeTokenInCookieStorage` a `WAFTokenProvider` .	11 de outubro de 2023
Regras AWS gerenciadas de implantações de exceções para AWS WAF	AWS As regras AWS WAF gerenciadas lançaram duas versões estáticas do grupo de regras de entradas inválidas conhecidas e atualizaram a versão padrão para apontar para a versão estática mais recente.	4 de outubro de 2023
AWS WAF Transformação de texto de decodificação de entidade HTML	Expandiu a funcionalidade da transformação de texto de decodificação da entidade HTML.	4 de outubro de 2023

Nova opção adicionada à política comum do grupo de segurança do Firewall Manager	O Firewall Manager agora pode distribuir referências de grupos de segurança para grupos de segurança de réplicas.	3 de outubro de 2023
AWS WAF adiciona inspeção da impressão digital JA3	Agora você pode realizar uma correspondência exata com a impressão digital JA3 da solicitação da web, para CloudFront distribuições da Amazon e Application Load Balancers.	26 de setembro de 2023
Atualizações nas configurações das regras de política de grupo de segurança do Firewall Manager	O Firewall Manager agora oferece suporte à referência de grupo de segurança, dos grupos de segurança primários aos grupos de segurança de réplica.	25 de setembro de 2023
Mitigação automática de DDoS da camada de aplicativos Shield Advanced atualizada	O Firewall Manager agora oferece suporte aos recursos do Application Load Balancer para políticas do Shield Advanced configuradas com mitigação automática de DDoS na camada da aplicação.	14 de setembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Controle de AWS WAF bots.	6 de setembro de 2023

AWS WAF Controle de bots	O nível de proteção direciona da do grupo de regras gerenciadas do Controle de Bots agora inspecion a a reutilização de tokens entre endereços IP. Agora, ele também fornece análise opcional de machine learning das estatísticas de tráfego para detectar algumas atividades relacionadas a bots.	6 de setembro de 2023
Atualização da especificação do SDK AWS WAF móvel	Os valores mínimo, máximo e padrão foram reduzidos para `tokenRefreshDelaySec` de mínimo 300, máximo 600 e padrão 300 para mínimo 88, máximo 300 e padrão 88.	5 de setembro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras gerenciadas para AWS WAF atualizar o grupo de regras do AWS WAF Bot Control.	30 de agosto de 2023
Mitigação automática de DDoS da camada de aplicação do Shield Advanced	Foi adicionada orientação AWS CloudFormation para gerenciar as ACLs da web que você usa com a mitigação automática de DDoS na camada de aplicação.	30 de agosto de 2023
Nova opção de política de grupo de segurança da auditoria de conteúdo do Firewall Manager	Foi adicionada uma nova opção para auditar grupos de regras excessivamente permissivos e descrições aprimoradas dos procedime ntos do console.	29 de agosto de 2023

Novo Firewall Manager Shield e opção AWS WAF de política	Se você habilitar o gerenciamento de ACLs da web não associadas no e AWS WAF Shield, o Firewall Manager só criará ACLs da web nas contas dentro do escopo da política somente se as ACLs da web forem usadas por pelo menos um recurso.	9 de agosto de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	26 de julho de 2023
Agregação de regras baseadas em intervalos no caminho do URI	Agora você pode especificar o caminho do URI em suas chaves de agregação personalizadas para regras baseadas em intervalos.	19 de julho de 2023
Nova opção AWS WAF de regra política em AWS Firewall Manager	AWS Firewall Manager adiciona suporte para configurar limites de tamanho de inspeção do corpo AWS WAF da solicitação da web.	18 de julho de 2023

AWS WAF mudanças de políticas gerenciadas	Atualizado`AWSWAFFullAccessPolicy` ,`AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` para adicionar acesso AWS verificado aos tipos de recursos com os quais você pode se proteger AWS WAF.	17 de junho de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para adicionar o grupo de regras`AWSManagedRulesACFPRuleSet` .	13 de junho de 2023
Atualização da prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control	Agora você pode especificar o endpoint de login para o grupo de regras gerenciadas do ATP usando uma expressão regular.	13 de junho de 2023
Novas informações para a API CAPTCHA JavaScript	A nova seção descreve como servir um quebra-cabeça CAPTCHA personalizado ao AWS WAF responder a uma solicitação com um CAPTCHA.	13 de junho de 2023
Novo grupo de regras gerenciadas do ACFP	Use o novo grupo de regras `AWSManagedRulesACFPRuleSet` para detectar e bloquear tentativas fraudulentas de criação de conta.	13 de junho de 2023

Nova prevenção de AWS WAF fraudes na criação de contas de controle de fraudes (ACFP)	Você pode detectar e bloquear tentativas fraudulentas de criação de contas com o novo grupo de regras gerenciadas para prevenção de AWS WAF fraudes na criação de contas (ACFP) do Fraud Control. `AWSManagedRulesACFPRuleSet` Com CloudFront distribuições protegidas, você também pode usar o ACFP para bloquear novas tentativas de criação de conta de clientes que enviaram recentemente muitas tentativas malsucedidas de criação de conta.	13 de junho de 2023
AWS WAF mudanças de políticas gerenciadas	Atualizado `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` para corrigir as configurações de acesso AWS App Runner dos serviços.	6 de junho de 2023
Limitação adicionada para as políticas de grupo de segurança do Firewall Manager	Se uma VPC compartilhada for posteriormente descompartilhada, o Firewall Manager não excluirá os grupos de segurança de réplica na conta associada.	2 de junho de 2023

Novo componente de AWS WAF solicitação: Header order	Agora você pode comparar com uma lista ordenada dos nomes dos cabeçalhos na solicitação.	30 de maio de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	Conjunto de regras do sistema operacional Linux atualizado.	22 de maio de 2023
Atualizou a organização da seção de AWS WAF regras	As listagens de instruções de regras agora estão agrupadas por tipo de declaração.	16 de maio de 2023
Tópico movido: Listagem de endereços IP com intervalo limitado	O tópico para listar endereços IP que estão sendo limitados por uma regra baseada em intervalos agora está no tópico de regras baseadas em intervalos.	16 de maio de 2023
Opções expandidas para regras baseadas em intervalos	Agora você pode limitar os intervalos de solicitações da web com base em chaves de agregação que não sejam endereços IP e pode agregar usando combinações de chaves. Você também pode limitar os intervalos de todas as solicitações que correspon dam a uma instrução de redução de escopo, sem agregação adicional.	16 de maio de 2023

Aumentos da cota do Firewall Manager	Aumentamos o número de políticas do Firewall Manager por organização AWS Organizations de 20 para 50. Aumentamos o número máximo de grupos de segurança primários por política de um para três. O número máximo de WCUs foi alterado de uma cota flexível para uma cota fixa.	5 de maio de 2023
Aumento do máximo de WCUs por grupo de regras	Agora você pode usar até 5.000 unidades de capacidade de web ACL (WCUs) por grupo de regras sem solicitar um aumento do suporte. Este novo limite não pode ser aumentado.	1º de maio de 2023
AWS WAF Localizações de buckets de log do Amazon S3 com prefixos	AWS WAF agora permite prefixos em nomes de bucket de log do Amazon S3.	1º de maio de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	28 de abril de 2023
Foi adicionado suporte para instâncias de acesso AWS verificado ao AWS WAF	Agora você pode associar uma ACL AWS WAF da web a uma instância de acesso verificado. Essa alteração está disponível somente na versão mais recente do AWS WAF e não no AWS WAF Classic.	28 de abril de 2023

Capítulo revisado sobre como trabalhar com vários administradores do Firewall Manager	Agora você pode designar vários administradores do Firewall Manager para criar e gerenciar os recursos de firewall da sua organização.	24 de abril de 2023
AWS Firewall Manager atualização de política gerenciada	Atualizado `FMSServiceRolePolicy` .	21 de abril de 2023
Nova integração de aplicativos JavaScript clientes para CAPTCHA	Agora você pode personalizar o posicionamento e as características do quebra-cabeça CAPTCHA em seus aplicativos JavaScript cliente.	20 de abril de 2023
Integração de aplicativos renomeada para integração de ameaças inteligentes	Renomeamos a funcionalidade existente para integrações de aplicativos clientes para integrações inteligentes de ameaças, para ajudar a distinguir entre ela e a nova integração de aplicativos CAPTCHA para. JavaScript	20 de abril de 2023
Preços variáveis para WCUs de web ACL além de 1.500	O uso de mais de 1.500 unidades de capacidade de web ACL (WCUs) em sua web ACL incorre em custos adicionais, que são ajustados automaticamente à medida que o uso da WCU da web ACL aumenta e diminui. O máximo da web ACL é de 5.000 WCUs.	11 de abril de 2023

Aumento do máximo de WCUs por web ACL	Agora você pode usar até 5.000 unidades de capacidade de ACL Web (WCUs) por grupo de regras sem solicitar um aumento do suporte. Este novo limite não pode ser aumentado.	11 de abril de 2023
Limites de tamanho de inspeção corporal para CloudFront ACLs da web	Para ACLs da web que protegem CloudFront as distribuições da Amazon, você pode aumentar o limite de tamanho da inspeção corporal em até 64 KB na configuração da sua ACL da web.	11 de abril de 2023
Aumento do tamanho da inspeção corporal para CloudFront	O limite máximo de tamanho de inspeção AWS WAF corporal para CloudFront distribuições da Amazon aumentou de 8 KB para 64 KB. O limite de tamanho de inspeção padrão CloudFront é de 16 KB.	11 de abril de 2023

Novas opções AWS WAF de regras de política em AWS Firewall Manager	AWS Firewall Manager adiciona suporte para grupos AWS WAF de regras de prevenção de aquisição de contas (ATP) e regras AWS gerenciadas de controle de AWS WAF bots, destinos de registro do Amazon S3, substituições de ações de regras, ações de regras `Challenge` e listas `CAPTCHA` de domínios de tokens.	7 de abril de 2023
O Firewall Manager oferece suporte a buckets Amazon S3 como destinos de registro para registro AWS WAF	Agora você pode usar os buckets do Amazon S3 como destinos de registro em suas políticas. AWS WAF	7 de abril de 2023
AWS WAF mudanças de políticas gerenciadas	Atualizado `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` para adicionar AWS App Runner serviços aos tipos de recursos com os quais você pode se proteger AWS WAF.	30 de março de 2023

Foi adicionado um aviso sobre o uso de tags nas políticas de grupo de segurança	O Firewall Manager não atualizará as tags dos grupos de segurança existentes nem criará novos grupos de segurança se a política tiver tags que entrem em conflito com a política de tags da organização.	28 de março de 2023
Atualização das informações de perfil de serviço	Atualização de como usar um perfil de serviço com o Firewall Manager.	8 de março de 2023
Informações corrigidas sobre como as regras baseadas em intervalos realizam a limitação de intervalos	Regras baseadas em intervalos com instruções de redução de escopo somente solicitam limites de intervalo que correspondam à instrução de redução de escopo da regra. Estávamos declarando que a limitação se aplicava a todas as solicitações de qualquer endereço IP com intervalo limitado.	1 de março de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do aplicativo PHP.	27 de fevereiro de 2023
Suporte adicionado AWS App Runner para AWS WAF	Agora você pode associar uma AWS WAF Web ACL a um AWS App Runner serviço. Essa alteração está disponível somente na versão mais recente do AWS WAF e não no AWS WAF Classic.	23 de fevereiro de 2023

Atualizou a orientação do IAM para AWS Firewall Manager	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	16 de fevereiro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras `AWSManagedRulesATPRuleSet` para adicionar inspeção de resposta de login em ACLs da web que protegem as CloudFront distribuições da Amazon.	15 de fevereiro de 2023
AWS WAF Controle de fraudes, prevenção de aquisição de contas (ATP), inspeção de resposta de login	Para CloudFront distribuições protegidas, agora você pode usar o ATP para bloquear novas tentativas de login de clientes que enviaram recentemente muitas tentativas de login malsucedidas.	15 de fevereiro de 2023
Regras AWS gerenciadas atualizadas para AWS WAF	Conjunto de regras principais atualizado.	25 de janeiro de 2023
Práticas recomendadas para mitigação de ameaças inteligentes	Foi adicionada uma seção com as melhores práticas para implementar o Controle de Bots, o ATP e outros atributos de mitigação de ameaças inteligentes.	22 de janeiro de 2023

Como inspecionar pseudocabeçalhos HTTP/2	Foi adicionada uma seção que mapeia pseudocabeçalhos HTTP/2 para seus componentes de solicitação da web correspondentes.	20 de janeiro de 2023
Atualizou a orientação do IAM para AWS WAF Classic	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	3 de janeiro de 2023
Atualizou a orientação do IAM para AWS WAF	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	3 de janeiro de 2023
Atualizou a orientação do IAM para AWS Shield	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	3 de janeiro de 2023
Atualização das políticas de Firewall DNS do Amazon Route 53 Resolver	Informações foram adicionadas sobre a exclusão de grupos de regras do Firewall DNS do Amazon Route 53 Resolver.	29 de dezembro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	Atualizou o grupo de regras do sistema operacional Linux.	15 de dezembro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	Conjunto de regras principais atualizado.	5 de dezembro de 2022

O Firewall Manager adiciona suporte às políticas do Fortigate Cloud Native Firewall (CNF) como serviço	O Firewall Manager agora suporta as políticas do Fortigate CNF.	2 de dezembro de 2022
AWS Config Requisito removido para políticas de firewall de DNS	Para políticas de Firewall DNS, agora você só precisa habilitar o Config para o tipo de recurso EC2 VPC.	17 de novembro de 2022
AWS Firewall Manager atualização de política gerenciada	Atualizado `FMSServiceRolePolicy` .	15 de novembro de 2022
Expansão das opções de idioma para o quebra-cabeça AWS WAF CAPTCHA	O quebra-cabeça CAPTCHA agora oferece instruções escritas em vários idiomas. As instruções dentro de cada quebra-cabeça de áudio ainda são fornecidas somente em inglês.	11 de novembro de 2022
Novas cotas do Firewall Manager para conjuntos de recursos	Foram adicionadas novas cotas para conjuntos de recursos.	8 de novembro de 2022
Adicione suporte para conjuntos de recursos	Você pode criar conjuntos de recursos para agrupar recursos gerenciados em uma política do Firewall Manager.	8 de novembro de 2022
Adicionar suporte para importar firewalls do Network Firewall	Agora você pode importar e gerenciar firewalls existente s nas políticas do Network Firewall usando conjuntos de recursos.	8 de novembro de 2022

AWS Firewall Manager atualização de política gerenciada	Atualizado `AWSFMAdminReadOnlyAccess` .	2 de novembro de 2022
A instrução de correspondência geográfica agora adiciona rótulos às solicitações de país e região	Agora você pode gerenciar as origens das solicitações geográficas no nível da região combinando a correspondência geográfica com a correspondência de rótulos.	31 de outubro de 2022
Renomeada a seção de nível superior: proteções gerenciadas	A seção agora se chama mitigação AWS WAF inteligente de ameaças, que se alinha às nossas páginas de marketing.	27 de outubro de 2022
Novo nível de proteção direcionada no grupo de regras gerenciadas do Controle de Bots	O grupo de regras gerenciadas do Controle de Bots agora oferece regras direcionadas e adicionais para a detecção e mitigação de bots sofisticados. Esse nível de proteção está disponível por taxas adicionais.	27 de outubro de 2022
Nova seção sobre AWS WAF tokens	Entenda como AWS WAF usa tokens para mitigação inteligente de ameaças.	27 de outubro de 2022

Observação importante adicionada sobre a atualização das políticas de Network Firewall do Firewall Manager	Quando você atualiza uma política do Firewall Manager, todas as políticas de Network Firewall criadas pela política serão atualizadas com a configuração da política de Network Firewall da política do Firewall Manager.	27 de outubro de 2022
Substituições de ações em grupos de regras	Agora você pode substituir as ações das regras em um grupo de regras por qualquer configuração de ação de regra. Assim como na substituição de ação Count anterior, você pode aplicar suas substituições a todas as regras em um grupo de regras e a regras individuais.	27 de outubro de 2022
AWS WAF nova opção de ação de Challenge regra	Você pode configurar regras para usar um Challenge para verificar se as solicitações estão sendo enviadas pelos navegadores.	27 de outubro de 2022
AWS WAF permite o compartilhamento de tokens em vários aplicativos protegidos	Você pode ativar o uso de tokens em vários aplicativos protegidos configurando uma lista de domínios de tokens para sua web ACL.	27 de outubro de 2022

A especificação de todos os cabeçalhos não faz distinção entre maiúsculas e minúsculas	Alterada a especificação de todos os cabeçalhos para não diferenciar maiúsculas de minúsculas. Isso correspon de ao comportamento do cabeçalho único.	26 de outubro de 2022
AWS Firewall Manager mudanças de políticas gerenciadas	Correções para `AWSFMAdmi nFullAccess` .	21 de outubro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	Conjunto de regras de entradas nocivas conhecidas.	20 de outubro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	Atualizado o grupo de regras de entradas nocivas conhecidas.	5 de outubro de 2022
Atualização da especificação do SDK AWS WAF móvel	Reduziu o valor padrão para `tokenRefreshDelaySec` de 600 (10 minutos) para 300 (5 minutos).	30 de setembro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	Foram corrigidos os nomes dos rótulos fornecidos nesta documentação para os seguintes grupos de regras: sistema operacional POSIX, aplicativo PHP, WordPress aplicativo.	19 de setembro de 2022
Nova opção AWS WAF de regra política em AWS Firewall Manager	AWS Firewall Manager agora oferece suporte a solicitações e respostas personalizadas da Web para ações padrão da Web nas AWS WAF políticas.	9 de setembro de 2022

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: reputação de IP.	30 de agosto de 2022
AWS WAF mudanças de políticas gerenciadas	Atualizado`AWSWAFFullAccessPolicy` ,`AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , e `AWSWAFConsoleReadOnlyAccess` para adicionar grupos de usuários do Amazon Cognito aos tipos de recursos com os quais você pode se proteger. AWS WAF	25 de agosto de 2022
AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP)	Agora você pode usar a funcionalidade de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control com as distribuições da Amazon CloudFront .	24 de agosto de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	22 de agosto de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras:`AWSManagedRulesATPRuleSet` .	11 de agosto de 2022

Foi adicionado suporte para grupos de usuários do Amazon Cognito em AWS WAF	Agora você pode associar uma AWS WAF Web ACL a um grupo de usuários do Amazon Cognito. Essa alteração está disponível somente na versão mais recente do AWS WAF e não no AWS WAF Classic.	11 de agosto de 2022
Foi adicionada uma seção sobre implantações para grupos de regras de regras AWS gerenciadas com versão	Foi adicionada uma nova seção documentando implantações para grupos de regras de regras AWS gerenciadas com versão. A seção inclui informações sobre como as versões padrão são nomeadas durante as implantações de versões candidatas a lançamento.	29 de julho de 2022
Requisitos atualizados para configurar o registro em log para políticas de Network Firewall	Foram adicionados requisitos para políticas do Network Firewall que usam um bucket criptografado do Amazon S3 como destino do log.	26 de julho de 2022
Opção de nível de sensibilidade para instrução de regra de SQLi	Agora você pode aumentar a sensibilidade das instruções de regra de injeção de SQL. Isso não muda o comportamento das instruções existentes, cujo nível de sensibilidade é o padrão de LOW.	15 de julho de 2022

Opção de configuração da política do Network Firewall adicionada	O Firewall Manager agora oferece suporte à ordem de avaliação com estado e às ações padrão nas configura ções da política de firewall do Network Firewall.	14 de julho de 2022
Atualizações nas configura ções das regras de política de grupo de segurança do Firewall Manager	O Firewall Manager agora oferece suporte à distribui ção de tags dos grupos de segurança primários para grupos de segurança de réplica.	7 de julho de 2022
Atualizações do AWS Shield guia	Expandiu as informações no guia do Shield para descrever como o Shield realiza a mitigação de eventos.	24 de junho de 2022
Orientação atualizada para testar e ajustar AWS WAF proteções	A orientação geral para testes e ajustes AWS WAF foi atualizada e agora é um tópico de alto nível.	20 de junho de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Conjunto de regras básicas (CRS).	9 de junho de 2022
Novas orientações sobre o “confused deputy” do Firewall Manager	Foram adicionadas orientaçõ es sobre como evitar o problema do “confused deputy” do Firewall Manager.	1º de junho de 2022

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Conjunto de regras básicas (CRS).	24 de maio de 2022
Novos componentes de AWS WAF solicitação: Headers e Cookies	Agora você pode inspecionar os cookies em uma solicitação da web e inspecionar todos os cabeçalhos em uma solicitaç ão da web, além de apenas um único cabeçalho.	29 de abril de 2022
AWS WAF tratamento de corpos grandes, cabeçalhos e componentes de solicitação de cookies	Agora você pode AWS WAF especificar como lidar com corpos de solicitaç ões, cabeçalhos e cookies grandes dentro das regras que inspecionam esses componentes. As regras que você já criou para inspecionar esses componentes têm um comportamento que correspon de à nova opção Continue de tratamento de tamanhos grandes.	29 de abril de 2022
AWS WAF Alterações na política de log do Amazon S3	A política e o exemplo de permissão de log do Amazon S3 foram atualizados.	12 de abril de 2022

Opção automática de mitigação de DDoS na camada de aplicativo agora disponível com o Application Load Balancer	O Shield Advanced agora oferece suporte à mitigação automática de DDoS na camada de aplicação para AWS Shield Advanced Application Load Balancers, disponibilizando-o para todas as proteções da camada de aplicação. Você pode configurar o Shield Advanced para contar ou bloquear automaticamente as solicitações da web que fazem parte de um ataque de DDoS na camada de aplicação em um recurso protegido.	8 de abril de 2022
Foi adicionado um indicador da configuração da versão padrão atual para grupos de regras gerenciadas	As listas de versões do grupo de regras gerenciadas agora indicam qual versão é a padrão atual.	8 de abril de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Controle de AWS WAF bots.	6 de abril de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	31 de março de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	30 de março de 2022

O Firewall Manager adiciona suporte ao Cloud Next Generation Firewall (NGFW) da Palo Alto Networks	O Firewall Manager agora oferece suporte ao Cloud Next Generation Firewall (NGFW) da Palo Alto Networks.	30 de março de 2022
Adicione suporte para o Palo Alto Networks Cloud NGFW ao AWS Firewall Manager	AWS Firewall Manager agora oferece suporte às políticas do Cloud Next Generation Firewall (NGFW) da Palo Alto Networks.	30 de março de 2022
Atualizações do AWS Shield guia	Expandiu as informaçõ es no guia do Shield para descrever como o Shield realiza a detecção de eventos e fornecer exemplos de arquiteturas resilientes a DDoS.	16 de março de 2022
Atualizações do AWS Shield guia	Expandiu as informações no guia do Shield e melhorou a organização de várias seções. As principais mudanças estão nas seguintes seções do guia Shield: suporte do Shield Response Team (SRT), proteções de recursos em eventos de DDoS e Visibilid ade em AWS Shield Advanced eventos de DDoS.	28 de fevereiro de 2022
O Firewall Manager agora suporta o modelo de implantaç ão centralizada do Network Firewall	Foi adicionado um novo procedimento que explica como configurar políticas que usam modelos de implantação distribuídos e centralizados.	24 de fevereiro de 2022

O Firewall Manager adiciona suporte ao modelo de implantação AWS Network Firewall centralizada	Agora você pode configurar suas AWS Network Firewall políticas para usar o modelo de implantação distribuído ou centralizado. Com o modelo de implantação distribuído, o Firewall Manager cria e mantém endpoints de firewall em cada VPC que está dentro do escopo da política. Com o modelo de implantação centralizado, o Firewall Manager cria e mantém endpoints de firewall em uma única VPC de inspeção.	24 de fevereiro de 2022
Adicione suporte para controle de versão de grupos de regras AWS WAF gerenciados em AWS Firewall Manager	AWS Firewall Manager agora oferece suporte ao controle de versão de grupos de regras AWS WAF gerenciados nas políticas do Firewall Manager AWS WAF .	18 de fevereiro de 2022
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	16 de fevereiro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: listas de reputação de IP.	15 de fevereiro de 2022

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras gerenciadas para AWS WAF adicionar o grupo de regras de prevenção de aquisição de contas (ATP) de controle de AWS WAF fraudes. `AWSManagedRulesATPRuleSet`	11 de fevereiro de 2022
Mudanças na organização do AWS WAF guia	Foi adicionada uma nova seção de nível superior para proteções gerenciadas. A seção CAPTCHA foi movida da seção de regras para a nova seção de proteções gerenciadas. A seção de rótulos foi movida de abaixo das regras para sua própria seção de nível superior.	11 de fevereiro de 2022
AWS WAF integrações de aplicativos clientes	Use AWS WAF JavaScript as APIs do cliente móvel para integrar seus aplicativos cliente aos grupos de regras AWS gerenciadas de mitigação inteligente de ameaças para uma detecção aprimorada.	11 de fevereiro de 2022
AWS WAF Controle de fraudes e prevenção de aquisição de contas (ATP)	Você pode detectar e bloquear tentativas de invasão de contas com o novo grupo de regras gerenciadas para prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control. `AWSManagedRulesATPRuleSet`	11 de fevereiro de 2022

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	28 de janeiro de 2022
AWS WAF mudanças de políticas gerenciadas	`AWSWAFFullAccessPolicy` e `AWSWAFConsoleFullAccess` atualizados para corrigir as permissões de logs.	11 de janeiro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: conjunto de regras principais (CRS), banco de dados SQLi.	10 de janeiro de 2022
O Firewall Manager oferece suporte à mitigação automática de DDoS da camada de aplicativo Shield Advanced	As políticas avançadas do Firewall Manager Shield para CloudFront recursos da Amazon agora incluem suporte para mitigação automática de DDoS na camada de aplicação.	7 de janeiro de 2022
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	7 de janeiro de 2022
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	17 de dezembro de 2021

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	11 de dezembro de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: Entradas inválidas conhecidas.	10 de dezembro de 2021
Nova função AWS Shield Advanced vinculada ao serviço	`AWSServiceRoleForAWSShield` adicionado para oferecer suporte à funcionalidade automática de mitigação de DDoS da camada de aplicativo.	1º de dezembro de 2021
Nova política AWS Shield gerenciada	`AWSShieldServiceRolePolicy` adicionado para oferecer suporte à funcionalidade automática de mitigação de DDoS da camada de aplicativo.	1º de dezembro de 2021

Opção automática de mitigação de DDoS na camada de aplicativo agora disponível com for AWS Shield Advanced CloudFront	O Shield Advanced agora oferece suporte à mitigação automática de DDoS na camada de aplicação para distribuições da Amazon. CloudFront Você pode configurar o Shield Advanced para contar ou bloquear automaticamente as solicitaç ões da web que fazem parte de um ataque de DDoS na camada de aplicação em uma CloudFront distribuição.	1º de dezembro de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: conjunto de regras básicas (CRS), sistema operacional Windows, sistema operacional Linux e listas de reputação de IP.	23 de novembro de 2021
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	18 de novembro de 2021
Opções de registro expandidas para AWS WAF	Agora você pode registrar o tráfego de ACL da web em um grupo de CloudWatch logs do Amazon Logs ou em um bucket do Amazon Simple Storage Service (Amazon S3). Essas opções são adicionais à opção existente de fazer login em um stream de entrega do Amazon Data Firehose.	15 de novembro de 2021

AWS WAF mudanças de políticas gerenciadas	`AWSWAFFullAccessPolicy` e `AWSWAFConsoleFullAccess` atualizados para oferecer suporte a destinos de logs adicionais.	15 de novembro de 2021
AWS WAF nova opção de ação de CAPTCHA regra	Você pode configurar regras para executar um CAPTCHA em solicitações da web e, conforme necessário, enviar um problema de CAPTCHA ao cliente.	8 de novembro de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do conjunto principal de regras (CRS).	27 de outubro de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	Todos os grupos de regras de regras AWS gerenciadas agora oferecem suporte à rotulagem. As descrições das regras incluem as especificações do rótulo.	25 de outubro de 2021
O Firewall Manager oferece suporte à filtragem de logs do Network Firewall	AWS Firewall Manager agora oferece suporte à filtragem de registros para políticas de Firewall de Rede.	4 de outubro de 2021
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	29 de setembro de 2021
Instrução de correspondência de regex adicionada	Agora você pode comparar solicitações da web com uma única expressão regular.	22 de setembro de 2021

Regras baseadas em taxas dentro AWS WAF de grupos de regras	Agora você pode definir regras baseadas em taxas dentro AWS WAF de grupos de regras. Em AWS Firewall Manager, esse recurso é totalmente suportado por AWS WAF políticas.	13 de setembro de 2021
O Firewall Manager oferece suporte à filtragem de AWS WAF registros	AWS Firewall Manager agora oferece suporte à filtragem de registros para AWS WAF políticas.	31 de agosto de 2021
Remova automaticamente as proteções de out-of-scope recursos em AWS Firewall Manager	AWS Firewall Manager permite que você remova automaticamente as proteções dos recursos que estão fora do escopo da política.	25 de agosto de 2021
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	12 de agosto de 2021
Foi adicionado o versionamento aos grupos de regras gerenciadas	Os provedores de grupos de regras gerenciadas agora podem criar versões de seus grupos de regras.	9 de agosto de 2021
Modificar os requisitos AWS Firewall Manager do administrador	Você pode usar a conta de gerenciamento da organização como conta de administrador do Firewall Manager. Isso foi desautorizado.	2 de agosto de 2021

Aumento da cota do Firewall Manager	Aumentou de 10 para 100 o número de instâncias da Amazon VPC que você pode ter no escopo de uma política do Firewall Manager.	28 de julho de 2021
AWS Firewall Manager suporte para monitoramento AWS Network Firewall da tabela de rotas	AWS Firewall Manager agora oferece suporte ao monitoramento de tabelas de rotas e fornece recomendações de ações de remediação aos administradores de segurança para AWS Network Firewall políticas com rotas configuradas incorretamente.	8 de julho de 2021
AWS WAF opções adicionais de transformação de texto	Opções expandidas para transformações de texto, que você pode aplicar aos componentes da solicitação da web antes de inspecioná-los.	24 de junho de 2021
Nomeação modificada para recursos de AWS WAF política do Firewall Manager	A nomenclatura das ACLs da web, dos grupos de regras e do registro que o Firewall Manager gerencia para suas AWS WAF políticas foi alterada.	26 de maio de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para suporte adicional à rotulagem em listas de reputação de IP e sufixos removidos em nomes de regras para a lista de reputação de IP da Amazon.	4 de maio de 2021

Adicionar suporte para administrador AWS Organizations delegado	Quando você define a conta de AWS Firewall Manager administrador, o Firewall Manager agora designa a conta como a administradora AWS Organizations delegada do Firewall Manager. Com essa alteração, ao definir a conta de administrador do Firewall Manager, você deve fornecer uma conta de membro diferente da conta de gerenciamento da organização. Essa alteração não afeta suas configurações existentes.	30 de abril de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras gerenciadas para AWS WAF adicionar o grupo de regras do AWS WAF Bot Control.	1º de abril de 2021
Definir ações de regras individuais para Count em um grupo de regras	Agora você pode definir as ações de regra individuais em um grupo de regras como Count. As informações da substituição existente, que estão no nível do grupo de regras, foram corrigidas.	1º de abril de 2021
Instrução de redução de escopo para grupos de regras gerenciadas	Agora você pode usar uma instrução de redução de escopo com grupos de regras gerenciadas da mesma forma que com uma instrução baseada em intervalo.	1º de abril de 2021

Filtro de log	Agora você pode filtrar o tráfego da web ACL que você registra com base na ação e no rótulo da regra.	1º de abril de 2021
AWS WAF rótulos em solicitações da web	Você pode configurar regras para adicionar rótulos às solicitações da web correspondentes e para corresponder aos rótulos adicionados por outras regras.	1º de abril de 2021
AWS WAF Controle de bots	Você pode monitorar e controlar o tráfego de bots com o novo recurso AWS WAF Bot Control, que combina o grupo de regras gerenciadas do Bot Control com rotulagem de solicitações da web, instruções de redução de escopo e filtragem de registros.	1º de abril de 2021
O Firewall Manager oferece suporte às políticas de Firewall DNS do Amazon Route 53 Resolver	AWS Firewall Manager suporta o gerenciamento central da filtragem de tráfego DNS de saída do Amazon Route 53 Resolver DNS Firewall para suas VPCs.	31 de março de 2021

Tratamento personalizado de solicitações e respostas	Você pode incluir cabeçalhos personalizados para solicitações da web que o AWS WAF não bloqueia e enviar respostas personalizadas para solicitações da web que o AWS WAF bloqueia. Isso está disponível para configurações de ação padrão da web ACL e configurações de ação de regra.	29 de março de 2021
AWS Firewall Manager mudança de política gerenciada	Atualizar para `FMSServiceRolePolicy` .	17 de março de 2021
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os seguintes grupos de regras: conjunto de regras básicas (CRS), proteção administrativa, entradas incorretas conhecidas e sistema operacional Linux.	3 de março de 2021
AWS Shield rastreamento gerenciado de alterações de políticas	A Shield começou a monitorar as mudanças em suas políticas AWS gerenciadas.	3 de março de 2021
AWS Firewall Manager rastreamento gerenciado de alterações de políticas	O Firewall Manager começou a monitorar as alterações em suas políticas AWS gerenciadas.	2 de março de 2021
AWS WAF rastreamento gerenciado de alterações de políticas	AWS WAF começou a rastrear as mudanças em suas políticas AWS gerenciadas.	1º de março de 2021

Inspecione um corpo de solicitação da web como JSON analisado	Foi adicionada a opção de inspecionar o corpo da solicitação da web como JSON analisado e filtrado. Isso é um acréscimo à opção existente de inspecionar o corpo da solicitação da web como texto simples.	12 de fevereiro de 2021
O Firewall Manager oferece suporte a AWS Network Firewall políticas	AWS Firewall Manager suporta o gerenciamento central da filtragem de tráfego de AWS Network Firewall rede para suas VPCs.	17 de novembro de 2020
Adicionar suporte para grupos AWS Shield Advanced de proteção	Agora você pode agrupar seus recursos protegidos em grupos lógicos e gerenciar suas proteções coletivamente.	13 de novembro de 2020
Suporte adicionado AWS AppSync para AWS WAF	Agora você pode associar uma AWS WAF Web ACL à sua API AWS AppSync GraphQL. Essa alteração está disponível somente na versão mais recente do AWS WAF e não no AWS WAF Classic.	1º de outubro de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o conjunto de regras do sistema operacional Windows.	23 de setembro de 2020

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar os conjuntos de regras do aplicativo PHP e do sistema operacional POSIX.	16 de setembro de 2020
AWS Shield Console atualizado	AWS Shield oferece uma nova opção de console, com uma experiência de usuário aprimorada. A orientação do console na documentação é para o novo console.	1.º de setembro de 2020
Atualizações do Firewall Manager nas políticas de grupo de segurança comuns	AWS Firewall Manager políticas comuns de grupos de segurança agora oferecem suporte aos tipos de recursos Application Load Balancers e Classic Load Balancers por meio da implement ação do console. As novas opções estão disponíveis nas configurações do Escopo da política da política comum.	11 de agosto de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o conjunto de regras principais.	7 de agosto de 2020
O Firewall Manager oferece suporte à configuração de AWS WAF registro	AWS Firewall Manager agora oferece suporte à configura ção de registro centralizada para AWS WAF políticas.	30 de julho de 2020

Especifique o local do endereço IP na solicitação da web	Adicionada a opção de usar endereços IP de um cabeçalho HTTP especificado por você, em vez de usar a origem da solicitação da web. Normalmente, o cabeçalho alternativo é `X-Forwarded-For` (XFF), mas é possível especificar qualquer nome de cabeçalho. Você pode usar essa opção para correspon dência de conjuntos de IPs, correspondência geográfica e agregação de contagem de regras baseadas em intervalo s.	9 de julho de 2020
Atualizações do Firewall Manager nas políticas de grupo de segurança de auditoria de conteúdo	AWS Firewall Manager expandiu a funcionalidade para políticas de grupo de segurança de auditoria de conteúdo, incluindo uma opção de regras gerenciadas, que usa listas gerenciadas de aplicativos e protocolos, além de detalhes sobre violações de recursos.	7 de julho de 2020
Listas gerenciadas do Firewall Manager	AWS Firewall Manager agora oferece suporte a listas gerenciadas de aplicativ os e protocolos. O Firewall Manager gerencia algumas listas e você pode criar e gerenciar suas próprias.	7 de julho de 2020

O Firewall Manager oferece suporte a VPCs compartilhadas em políticas comuns de grupo de segurança	AWS Firewall Manager agora oferece suporte ao uso de políticas de grupo de segurança comuns em VPCs compartilhadas. É possível fazer isso além de usá-las nas VPCs pertencentes a contas no escopo.	26 de maio de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	Foi adicionada documentação para cada regra nas Regras AWS gerenciadas para AWS WAF.	20 de maio de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o grupo de regras do sistema operacional Linux.	19 de maio de 2020
Adicione suporte para migrar recursos do AWS WAF Classic para AWS WAF (v2)	Agora você pode usar o console ou a API para exportar seus recursos do AWS WAF Classic para migração para a versão mais recente do AWS WAF.	27 de abril de 2020

Adicionar suporte para unidades AWS Organizations organizacionais no escopo da política	AWS Firewall Manager agora suporta o uso de unidades AWS Organizations organizacionais (OUs) para especificar o escopo da política. Você pode usar OUs para incluir ou excluir contas do escopo, além de incluir ou excluir contas específicas. Especificar uma OU é o mesmo que especificar todas as contas da OU e de todas as suas OUs filhas, incluindo todas as OUs e contas filhas que forem adicionadas posteriormente.	6 de abril de 2020
Adicione suporte para AWS WAF (v2) a AWS Firewall Manager	AWS Firewall Manager agora oferece suporte à versão mais recente do AWS WAF AWS WAF Classic, além da versão anterior.	31 de março de 2020
Atualização das políticas AWS Firewall Manager comuns de grupos de segurança	AWS Firewall Manager A política de grupo de segurança comum agora tem a opção de aplicar a política a todas as interfaces de rede elásticas em suas instâncias do Amazon EC2 dentro do escopo. Você ainda pode optar por aplicar a política somente à interface de rede elástica padrão.	11 de março de 2020

Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para adicionar um grupo de `AWSManagedRulesAnonymousIpList` regras.	6 de março de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS Regras AWS WAF gerenciadas para atualizar o WordPress aplicativo e os grupos de `AWSManagedRulesCommonRuleSet` regras.	3 de março de 2020
Foi adicionada a verificação de saúde do Amazon Route 53 às opções de AWS Shield Advanced proteção	Agora, o Shield Advanced oferece suporte ao uso de associações de verificação de integridade do Amazon Route 53, para melhorar a precisão da detecção e da mitigação de ameaças.	14 de fevereiro de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS O Managed Rules for AWS WAF atualizou o grupo de regras do Banco de Dados SQL para adicionar a verificação do URI da mensagem.	23 de janeiro de 2020

Nova opção de política de grupo de segurança da auditoria de conteúdo do Firewall Manager	O Firewall Manager tem uma nova opção para as políticas de auditoria de uso dos grupos de segurança. Agora você pode definir um número mínimo de minutos em que um grupo de segurança deve permanecer sem uso para que seja considerado incompatível. Por padrão, essa configuração de minutos é zero.	14 de janeiro de 2020
Firewall Manager: nova opção para AWS WAF política	O Firewall Manager tem uma nova opção para AWS WAF políticas. Agora você pode optar por remover todas as associações de web ACL existentes de recursos no escopo antes de associar as novas web ACLs da política a elas.	14 de janeiro de 2020
Regras AWS gerenciadas atualizadas para AWS WAF	AWS O Managed Rules for AWS WAF atualizou as transformações de texto para regras no Conjunto de Regras Básico e nos grupos de regras do Banco de Dados SQL.	20 de dezembro de 2019
AWS Firewall Manager integrado com AWS Security Hub	AWS Firewall Manager agora cria descobertas para recursos que estão fora de conformid ade e para ataques e as envia para AWS Security Hub.	18 de dezembro de 2019

Lançamento da AWS WAF versão 2	Nova versão do guia do AWS WAF desenvolvedor. Você pode gerenciar uma web ACL ou um grupo de regras no formato JSON. Os recursos expandidos incluem instruções de regra lógica, aninhamento de instrução de regra e suporte completo a CIDR para endereços IP e intervalos de endereços. As regras não são mais AWS recursos, mas existem somente no contexto de uma ACL da web ou de um grupo de regras. Para clientes existentes, a versão anterior do serviço agora é chamada de AWS WAF Classic. Nas APIs, SDKs e CLIs, o AWS WAF Classic mantém seus esquemas de nomenclatura e essa versão mais recente do AWS WAF é chamada de “V2" ou “v2" adicionada, dependendo do contexto. AWS WAF não consigo acessar AWS recursos que foram criados no AWS WAF Classic. Para usar esses recursos AWS WAF, você precisa migrá-los.	25 de novembro de 2019
AWS Grupos de regras de regras gerenciadas para AWS WAF	Grupos de regras de regras AWS gerenciadas adicionados. Eles são gratuitos para AWS WAF os clientes.	25 de novembro de 2019

AWS Firewall Manager suporte para grupos de segurança da Amazon Virtual Private Cloud	Adicionado suporte para grupos de segurança da Amazon VPC no Firewall Manager.	10 de outubro de 2019
AWS Firewall Manager suporte para AWS Shield Advanced	Foi adicionado suporte para o Shield Advanced no Firewall Manager.	15 de março de 2019
Tutorial: Criar políticas hierárquicas	Adicionado tutorial sobre criação de políticas hierárquicas no AWS Firewall Manager.	11 de fevereiro de 2019
Controle no nível da regra em de grupos de regras	Agora você pode excluir regras individuais de grupos de AWS Marketplace regras, bem como seus próprios grupos de regras.	12 de dezembro de 2018
AWS Shield Advanced suporte para aceleradores AWS Global Accelerator padrão	O Shield Advanced agora pode proteger aceleradores AWS Global Accelerator padrão.	26 de novembro de 2018
AWS WAF suporte para Amazon API Gateway	AWS WAF agora protege as APIs do Amazon API Gateway.	25 de outubro de 2018
Assistente de introdução avançado AWS do escudo expandido	O novo assistente oferece a oportunidade de criar regras baseadas em tarifas e Amazon CloudWatch Events.	31 de agosto de 2018
AWS WAF registro em log	Habilite o registro em log para obter informações detalhadas sobre o tráfego que é analisado pela web ACL.	31 de agosto de 2018

Suporte para parâmetros de consulta em condições	Ao criar uma condição, agora você pode pesquisar as solicitações de parâmetros específicos.	5 de junho de 2018
Assistente Conceitos básicos do Shield Advanced	Apresenta um novo processo simplificado de assinatura do Shield AWS Advanced.	5 de junho de 2018
Intervalos de CIDR permitidos expandidos	Ao criar uma condição de correspondência de IP, AWS WAF agora oferece suporte a intervalos de endereços IPv4: /8 e qualquer intervalo entre /16 a /32.	5 de junho de 2018

Atualizações anteriores a 2018

A tabela a seguir descreve as alterações importantes em cada versão do Guia do desenvolvedor do AWS WAF antes de junho de 2018.

Alteração	Versão da API	Descrição	Data de lançamento
Atualizar	2016-08-24	AWS Marketplace grupos de regras	Novembro de 2017
Atualizar	2016-08-24	Suporte avançado do Shield para endereços IP elásticos	Novembro de 2017
Atualizar	2016-08-24	Painel de ameaças globais	Novembro de 2017
Atualizar	2016-08-24	Tutorial de site resistente a DDoS	Outubro de 2017

Alteração	Versão da API	Descrição	Data de lançamento
Atualizar	2016-08-24	Condições geográficas e regex	Outubro de 2017
Atualizar	2016-08-24	Regras com base em taxa	Junho de 2017
Atualizar	2016-08-24	Reorganização	Abril de 2017
Atualizar	2016-08-24	Adicionadas informações sobre proteção de DDoS e suporte a Application Load Balancers.	Novembro de 2016
Novos atributos	2015-08-24	Agora você pode registrar todas as suas chamadas de API no AWS WAF through AWS CloudTrail, o AWS serviço que registra as chamadas de API para sua conta e entrega os arquivos de log ao seu bucket do S3. CloudTrail os registros podem ser usados para permitir análises de segurança, rastrear alteraçõe s em seus AWS recursos e auxiliar na auditoria de conformidade. A integração AWS WAF CloudTrail permite determinar quais solicitações foram feitas à AWS WAF API, o endereço IP de origem a partir do qual cada solicitação foi feita, quem fez a solicitação, quando ela foi feita e muito mais. Se você já estiver usando AWS CloudTrail, começará a ver chamadas de AWS WAF API em seu CloudTrai l registro. Se você não CloudTrail ativou sua conta, você pode ativá-la no CloudTrail AWS Management Console. Não há cobrança adicional pela habilitação CloudTrail, mas aplicam-se tarifas padrão para o uso do Amazon S3 e do Amazon SNS.	28 de abril de 2016

Alteração	Versão da API	Descrição	Data de lançamento
Novos atributos	2015-08-24	Agora você pode usar AWS WAF para permitir, bloquear ou contar solicitações da web que parecem conter scripts maliciosos, conhecidos como cross-site scripting ou XSS. Os invasores às vezes inserem scripts mal-intencionados nas solicitações da web na tentativa de explorar as vulnerabilidades das aplicações web. Para ter mais informações, consulte Instrução de regra de ataque de script entre sites.	29 de março de 2016
Novos atributos	2015-08-24	Com esta versão, AWS WAF adiciona os seguintes recursos: • Você pode configurar AWS WAF para permitir, bloquear ou contar solicitações da Web com base nos comprimentos de partes especificadas das solicitações, como cadeias de caracteres de consulta ou URIs. Para ter mais informações, consulte Instrução de regra de restrição de tamanho. • Você pode configurar AWS WAF para permitir, bloquear ou contar solicitações da web com base no conteúdo do corpo da solicitação. Essa é a parte de uma solicitação que contém dados adicionais que você deseja enviar para o seu servidor web na forma de corpo da solicitação HTTP, como dados de um formulário. Esse atributo se aplica às condições de correspondência de string, condições de correspondência de injeção de SQL e as novas condições de restrição de tamanho mencionadas no primeiro marcador. Para ter mais informações, consulte Especificação e tratamento de componentes de solicitações da Web.	27 de janeiro de 2016

Alteração	Versão da API	Descrição	Data de lançamento
Novo recurso	2015-08-24	Agora você pode usar o AWS WAF console para escolher CloudFront as distribuições às quais deseja associar uma Web ACL. Para obter mais informações, consulte Associando ou desassociando uma Web ACL e uma distribuição. CloudFront	16 de novembro de 2015
Versão inicial	2015-08-24	Esta é a primeira versão do Guia do desenvolvedor do AWS WAF .	6 de outubro de 2015

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

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.