Guia de implementação

Automações de segurança para AWS WAF

Automações de segurança para AWS WAF: Guia de implementação

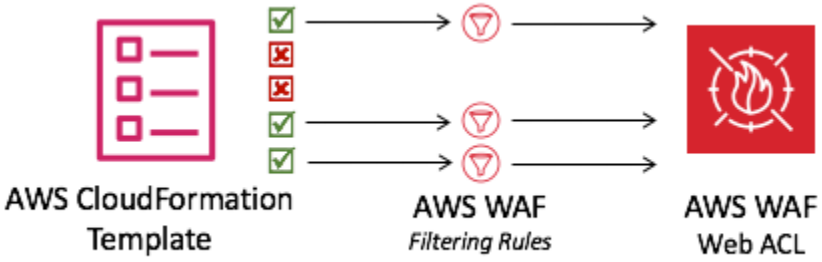
Table of Contents

Implemente automaticamente uma única lista de controle de acesso à web que filtra ataques baseados na web com automações de segurança no AWS WAF

A solução Security Automations for AWS WAF implanta um conjunto de regras pré-configuradas para ajudar você a proteger seus aplicativos contra explorações comuns da web. O serviço principal dessa solução, o AWS WAF, ajuda a proteger os aplicativos da web contra técnicas de ataque que podem afetar a disponibilidade dos aplicativos, comprometer a segurança ou consumir recursos excessivos. Você pode usar o AWS WAF para definir regras de segurança web personalizáveis. Essas regras controlam qual tráfego permitir ou bloquear para aplicativos web e interfaces de programação de aplicativos (APIs) implantados em recursos da AWS, como Amazon CloudFront, Application Load Balancer (ALB). Para obter mais tipos de recursos compatíveis, consulte o AWS WAF no AWS WAF, no AWS Firewall Manager e no AWS Shield Advanced Developer Guide.

Configurar as regras do AWS WAF pode ser desafiador e trabalhoso para organizações grandes e pequenas, especialmente para aquelas que não têm equipes de segurança dedicadas. Para simplificar esse processo, a solução Security Automations for AWS WAF implanta automaticamente uma única lista de controle de acesso à web (ACL) com um conjunto de regras do AWS WAF projetadas para filtrar ataques comuns baseados na web. Durante a configuração inicial do CloudFormation modelo da AWS dessa solução, você pode especificar quais recursos de proteção incluir. Depois de implantar essa solução, o AWS WAF inspeciona as solicitações da web para suas CloudFront distribuições ou ALB (s) existentes e as bloqueia quando aplicável.

Um CloudFormation modelo implanta uma ACL da web com as regras de filtragem do AWS WAF.



Este guia de implementação discute considerações arquitetônicas, etapas de configuração e melhores práticas operacionais para implantar essa solução na nuvem da Amazon Web Services (AWS). Inclui links para CloudFormation modelos que iniciam, configuram e executam os serviços de

segurança, computação, armazenamento e outros serviços da AWS necessários para implantar essa solução na AWS, usando as melhores práticas de segurança e disponibilidade da AWS.

As informações neste guia pressupõem conhecimento prático dos serviços da AWS, como AWS WAF CloudFront, ALBs, e AWS Lambda. Também requer conhecimento básico de ataques comuns baseados na web e estratégias de mitigação.

> **Note**
>
> A partir da versão 3.0.0, essa solução oferece suporte à versão mais recente da API do serviço AWS WAF (AWS WAFV2).

Este guia é destinado a gerentes de TI, engenheiros de segurança, DevOps engenheiros, desenvolvedores, arquitetos de soluções e administradores de sites.

> **Note**
>
> Recomendamos usar essa solução como ponto de partida para implementar as regras do AWS WAF. Você pode personalizar o código-fonte, adicionar novas regras personalizadas e aproveitar mais regras gerenciadas pelo AWS WAF com base nas suas necessidades.

Use esta tabela de navegação para encontrar rapidamente respostas para essas perguntas:

Se você deseja...	Leia…
Conheça o custo da execução dessa solução. O custo total da execução dessa solução depende da proteção ativada e da quantidade de dados ingeridos, armazenados e processados.	Custos
Entenda as considerações de segurança dessa solução.	Segurança
Saiba quais regiões da AWS são compatíveis com essa solução.	Regiões da AWS com suporte

Se você deseja...	Leia…
Visualize ou baixe o CloudFormation modelo incluído nesta solução para implantar automatic amente os recursos de infraestrutura (a “pilha”) dessa solução.	CloudFormation Modelo da AWS
Use o Support para ajudá-lo a implantar, usar ou solucionar problemas da solução.	Suporte
Acesse o código-fonte e, opcionalmente, use o AWS Cloud Development Kit (AWS CDK) para implantar a solução	GitHub repositório

Atributos e benefícios

A solução Security Automations for AWS WAF fornece os seguintes recursos e benefícios.

Proteja seus aplicativos web com grupos de regras do AWS Managed Rules

O AWS Managed Rules para AWS WAF oferece proteção contra vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados. Essa solução inclui grupos de regras de reputação de IP gerenciado pela AWS, grupos de regras de linha de base gerenciados pela AWS e grupos de regras específicos de casos de uso do AWS Managed. Você tem a opção de selecionar um ou mais grupos de regras para sua ACL da web, até a cota máxima da unidade de capacidade da ACL da web (WCU).

Forneça proteção contra inundação de camada 7 com uma regra personalizada predefinida de inundação HTTP

A regra personalizada HTTP Flood protege contra um ataque distribuído Denial-of-Service (DDoS) na camada da web por um período de tempo definido pelo cliente. Você pode escolher uma das seguintes opções para ativar essa regra:

- Regra baseada em taxas do AWS WAF
- Analisador de log Lambda

- Analisador de log Amazon Athena

As opções do analisador de log Lambda ou do analisador de log Athena permitem que você defina uma cota de solicitação menor que 100. Essa abordagem pode ajudar você a não atingir a cota exigida pelas regras baseadas em taxas do AWS WAF. Para obter mais informações, consulte Opções do analisador de registros.

Você também pode aprimorar o analisador de log do Athena adicionando um país e um Uniform Resource Identifier (URI) às condições de filtragem. Essa abordagem identifica e bloqueia ataques de inundação de HTTP que têm padrões de URI imprevisíveis. Para obter mais informações, consulte Usar país e URI no analisador de log HTTP Flood Athena.

Bloqueie a exploração de vulnerabilidades com a regra personalizada predefinida de scanners e sondas

A regra personalizada Scanners & Probes analisa os registros de acesso ao aplicativo em busca de comportamentos suspeitos, como uma quantidade anormal de erros gerados por uma origem. Em seguida, ele bloqueia esses endereços IP de origem suspeitos por um período de tempo definido pelo cliente. Você pode escolher uma dessas opções para ativar essa regra: analisador de log Lambda ou analisador de log Athena. Para obter mais informações, consulte Opções do analisador de registros.

Detecte e desvie a intrusão com a regra personalizada predefinida do Bad Bot

A regra personalizada do Bad Bot configura um endpoint honeypot, que é um mecanismo de segurança destinado a atrair e desviar uma tentativa de ataque. Você pode inserir o endpoint em seu site para detectar solicitações de entrada de raspadores de conteúdo e bots maliciosos. Uma vez detectadas, todas as solicitações subsequentes da mesma origem serão bloqueadas. Para obter mais informações, consulte Incorporar o link Honeypot em seu aplicativo da web.

Bloqueie endereços IP maliciosos com regras personalizadas de listas de reputação de IP predefinidas

A regra personalizada das listas de reputação de IP verifica as listas de reputação de IP de terceiros de hora em hora em busca de novos intervalos de IP a serem bloqueados. Essas listas incluem as

listas Spamhaus Don't Route Or Peer (DROP) e Extended DROP (EDROP), a lista de IP de ameaças emergentes do Proofpoint e a lista de nós de saída do Tor.

Forneça configuração manual de IP com regras personalizadas predefinidas de listas de IPs permitidos e negados

As regras personalizadas das listas de IP permitidos e negados permitem que você insira manualmente os endereços IP que você deseja permitir ou negar. Você também pode configurar a retenção de IP nas listas de IPs permitidos e negados para expirar IPs em um horário definido.

Crie seu próprio painel de monitoramento

Essa solução emite CloudWatch métricas da Amazon, como solicitações permitidas, solicitações bloqueadas e outras métricas relevantes. Você pode criar um painel personalizado para visualizar essas métricas e obter informações sobre o padrão de ataques e a proteção fornecidos pelo AWS WAF. Para obter mais informações, consulte Criar painel de monitoramento.

Casos de uso

Veja a seguir exemplos de casos de uso dessa solução. Você pode personalizar essa solução de maneiras inovadoras que não se limitam a essa lista.

Automatize a configuração das regras do AWS WAF

O AWS WAF protege seu aplicativo web contra ataques comuns; no entanto, configurar as regras do AWS WAF pode ser complicado e demorado. Para ajudá-lo, essa solução implanta automaticamente um conjunto de regras do AWS WAF em sua conta com CloudFormation um modelo. Dessa forma, você não precisa configurar as regras do AWS WAF sozinho e pode começar a usar o AWS WAF mais rapidamente.

Personalize a proteção contra inundação HTTP da camada 7

Essa solução fornece três opções para ativar a proteção HTTP Flood. Você pode selecionar a opção que atenda às suas necessidades para obter proteção contra ataques DDo S. Para obter mais informações, consulte Forneça proteção contra inundação de camada 7 com uma regra personalizada predefinida de inundação HTTP em Recursos e benefícios.

Aproveite o código-fonte para aplicar a personalização ou criar suas próprias automações de segurança

Essa solução fornece um exemplo de como usar o AWS WAF e outros serviços para criar automações de segurança na nuvem da AWS. Seu código-fonte aberto GitHub facilita a aplicação de personalizações ou a criação de suas próprias automações de segurança que atendam às suas necessidades.

Conceitos e definições

Esta seção descreve os principais conceitos e define a terminologia específica dessa solução.

Registros do ALB

Essa solução usa registros para o recurso ALB. A regra de proteção de scanner e sonda nesta solução inspeciona esses registros.

Analisador de log Athena

O Amazon Athena é um serviço de análise interativo e sem servidor que se baseia em estruturas de código aberto, oferecendo suporte a formatos de tabela aberta e de arquivo. Essa solução executa uma consulta programada do Athena para inspecionar os registros do AWS WAF ou ALB CloudFront, se o usuário `yes - Amazon Athena log parser` escolher ativar a regra HTTP Flood Protection ou a regra Scanner & Probe Protection, e pode ser usada para ativar a Bad Bot Protection por meio de detecção que opera por meio de uma cadeia lógica estruturada.

Regra do AWS WAF

Uma regra do AWS WAF define:

- Como inspecionar solicitações web HTTP (S)
- A ação a ser tomada em relação a uma solicitação quando ela atende aos critérios de inspeção

Você define regras somente no contexto de um grupo de regras ou web ACL.

CloudFront logs

Essa solução usa registros para o CloudFront recurso. A regra de proteção de scanner e sonda nesta solução inspeciona esses registros.

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 declaração de regra. Os conjuntos de IP são recursos da AWS.

Analisador de log Lambda

Essa solução executa uma função Lambda invocada por um evento de criação de objetos do Amazon Simple Storage Service (Amazon S3). A função Lambda inicia uma inspeção dos registros do AWS WAF ou ALB se o usuário optar `yes - AWS Lambda log parser` por ativar a Proteção contra Inundação HTTP CloudFront, a Proteção de Scanner e a Proteção de Scanner e pode ser usada para a regra Bad Bot Protection por meio de detecção que opera por meio de uma cadeia lógica estruturada.

Grupos de regras gerenciados

Grupos de regras gerenciadas são coleções de ready-to-use regras predefinidas que os vendedores da AWS e do AWS Marketplace escrevem e mantêm para você. Os preços do AWS WAF se aplicam ao uso de qualquer grupo de regras gerenciadas.

tipo de recurso/endpoint

Você pode associar recursos da AWS à web ACLs para protegê-los. Esses recursos são: ALB CloudFront, AWS AppSync, Amazon Cognito, AWS App Runner e AWS Verified Access. Atualmente, esta solução é suportada pela Amazon CloudFront e pela ALB.

Registros WAF

Essa solução usa registros gerados pelo AWS WAF para os recursos associados à ACL da web. As regras HTTP Flood Protection, Scanner & Probe Protection e Activate Bad Bot Protection desta solução inspecionam esses registros.

WCU

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

ACL da web

Uma ACL da web oferece controle refinado sobre as solicitações HTTP (S) da web às quais seu recurso protegido responde.

> **Note**
>
> Para obter uma referência geral dos termos da AWS, consulte o glossário da AWS.

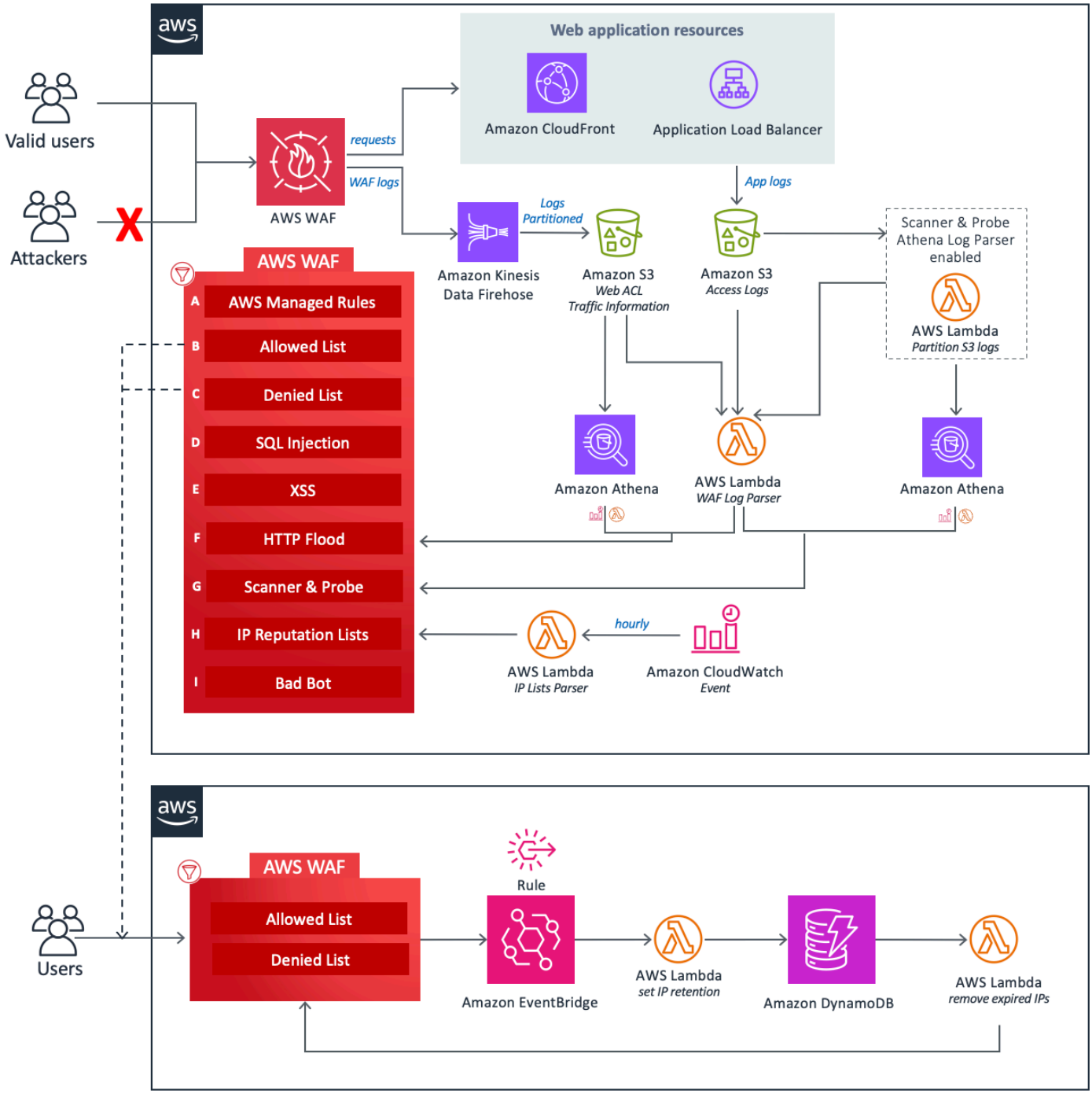
Visão geral da arquitetura

Esta seção fornece um diagrama de arquitetura de implementação de referência para os componentes implantados com essa solução.

Diagrama de arquitetura

A implantação dessa solução com os parâmetros padrão implanta os seguintes componentes em sua conta da AWS.

CloudFormation O modelo implanta o AWS WAF e outros recursos da AWS para proteger seu aplicativo web contra ataques comuns.



No centro do design está uma ACL web do AWS WAF, que atua como ponto central de inspeção e decisão para todas as solicitações recebidas em um aplicativo web. Durante a configuração inicial da CloudFormation pilha, o usuário define quais componentes de proteção devem ser ativados. Cada componente opera de forma independente e adiciona regras diferentes à ACL da web.

Os componentes dessa solução podem ser agrupados nas seguintes áreas de proteção.

> **Note**
>
> Os rótulos dos grupos não refletem o nível de prioridade das regras do WAF.

- AWS Managed Rules (A) — Esse componente contém grupos de regras de reputação de IP do AWS Managed Rules, grupos de regras básicas e grupos de regras específicos de casos de uso. Esses grupos de regras protegem contra a exploração de vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados, incluindo aqueles descritos nas publicações do OWASP, sem precisar escrever suas próprias regras.
- Listas manuais de IP (B e C) — Esses componentes criam duas regras do AWS WAF. Com essas regras, você pode inserir manualmente os endereços IP que deseja permitir ou negar. Você pode configurar a retenção de IP e remover endereços IP expirados em conjuntos de IP permitidos ou negados usando EventBridge as regras da Amazon e o Amazon DynamoDB. Para obter mais informações, consulte Configurar retenção de IP em conjuntos de IP permitidos e negados do AWS WAF.
- Injeção de SQL (D) e XSS (E) — Esses componentes configuram duas regras do AWS WAF projetadas para proteger contra padrões comuns de injeção de SQL ou cross-site scripting (XSS) no URI, na string de consulta ou no corpo de uma solicitação.
- HTTP Flood (F) - Esse componente protege contra ataques que consistem em um grande número de solicitações de um endereço IP específico, como um ataque na camada DDo S da web ou uma tentativa de login por força bruta. Com essa regra, você define uma cota que define o número máximo de solicitações de entrada permitidas de um único endereço IP em um período padrão de cinco minutos (configurável com o parâmetro Athena Query Run Time Schedule). Depois que esse limite é violado, solicitações adicionais do endereço IP são temporariamente bloqueadas. Você pode implementar essa regra usando uma regra baseada em taxas do AWS WAF ou processando registros do AWS WAF usando uma função Lambda ou uma consulta do Athena. Para obter mais informações sobre as compensações relacionadas às opções de mitigação de inundação HTTP, consulte Opções do analisador de registros.
- Scanner and Probe (G) - Esse componente analisa os registros de acesso ao aplicativo em busca de comportamentos suspeitos, como uma quantidade anormal de erros gerados por uma origem. Em seguida, ele bloqueia esses endereços IP de origem suspeitos por um período de tempo definido pelo cliente. Você pode implementar essa regra usando uma função Lambda ou uma consulta do Athena. Para obter mais informações sobre as vantagens e desvantagens relacionadas às opções de mitigação do scanner e da sonda, consulte Opções do analisador de registros.

- Listas de reputação de IP (H) - Esse componente é a função `IP Lists Parser` Lambda que verifica listas de reputação de IP de terceiros de hora em hora em busca de novos intervalos a serem bloqueados. Essas listas incluem as listas Spamhaus Don't Route Or Peer (DROP) e Extended DROP (EDROP), a lista de IPs do Proofpoint Emerging Threats e a lista de nós de saída do Tor.
- Bad Bot (I) - Esse componente aprimora a detecção de bots incorretos monitorando conexões diretas com um Application Load Balancer (ALB) ou CloudFront Amazon, além do mecanismo de honeypot. Se um bot contorna o honeypot e tenta interagir com o ALB ou CloudFront, o sistema analisa os padrões e registros de solicitações para identificar atividades maliciosas. Quando um bot mal-intencionado é detectado, seu endereço IP é extraído e adicionado a uma lista de bloqueios do AWS WAF para evitar mais acesso. A detecção de bots incorretos opera por meio de uma cadeia lógica estruturada, garantindo uma cobertura abrangente de ameaças:
  - Analisador de log Lambda de proteção contra inundações HTTP — Coleta IPs bots inválidos das entradas de registro durante a análise de inundação.
  - Scanner & Probe Protection Lambda Log Parser — Identifica IPs bots defeituosos nas entradas de registro relacionadas ao scanner.
  - HTTP Flood Protection Athena Log Parser — Extrai bots mal-intencionados dos registros IPs do Athena, usando partições na execução da consulta.
  - Scanner & Probe Protection Athena Log Parser — Recupera bots defeituosos dos registros IPs do Athena relacionados ao scanner, usando a mesma estratégia de particionamento.
  - Detecção de fallback — Se a proteção contra inundação HTTP e a proteção de scanner e sonda estiverem desativadas, o sistema dependerá do analisador Log Lambda, que registra a atividade do bot com base nos filtros de rótulos WAF.

Cada uma das três funções personalizadas do Lambda nesta solução publica métricas de tempo de execução em. CloudWatch Para obter mais informações sobre essas funções do Lambda, consulte Detalhes do componente.

Considerações sobre o design do AWS Well-Architected

Essa solução usa as melhores práticas do AWS Well-Architected Framework, que ajuda os clientes a projetar e operar cargas de trabalho confiáveis, seguras, eficientes e econômicas na nuvem.

Esta seção descreve como os princípios de design e as melhores práticas do Well-Architected Framework beneficiam essa solução.

Excelência operacional

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- A solução envia métricas CloudWatch para fornecer observabilidade na infraestrutura, nas funções Lambda, no Amazon Data Firehose, nos buckets do Amazon S3 e no restante dos componentes da solução.
- Desenvolvemos, testamos e publicamos a solução por meio de um pipeline de integração contínua e entrega contínua (CI/CD) da AWS. Isso ajuda os desenvolvedores a obter resultados de alta qualidade de forma consistente.
- Você pode instalar a solução com um CloudFormation modelo que provisiona todos os recursos necessários em sua conta. Para atualizar ou excluir a solução, você só precisa atualizar ou excluir o modelo.

Segurança

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- Todas as comunicações entre serviços usam as funções do AWS Identity and Access Management (IAM).
- Todas as funções usadas pela solução seguem o acesso com privilégios mínimos. Em outras palavras, eles contêm apenas as permissões mínimas necessárias para que o serviço possa funcionar corretamente.
- Todo o armazenamento de dados, incluindo os buckets do Amazon S3 e o DynamoDB, tem criptografia em repouso.

Confiabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de confiabilidade.

- A solução usa serviços sem servidor da AWS sempre que possível (por exemplo, Lambda, Firehose, Amazon S3 e Athena) para garantir alta disponibilidade e recuperação de falhas no serviço.

- Realizamos testes automatizados na solução para detectar e corrigir erros rapidamente.
- A solução usa funções Lambda para processamento de dados. A solução armazena dados no Amazon S3 e no DynamoDB e, por padrão, persiste em várias zonas de disponibilidade.

Eficiência de desempenho

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de excelência operacional.

- A solução usa uma arquitetura sem servidor para garantir alta escalabilidade e disponibilidade a um custo reduzido.
- A solução aprimora o desempenho do banco de dados ao particionar dados e otimizar a consulta para reduzir a quantidade de dados digitalizados e obter resultados mais rápidos.
- A solução é testada e implantada automaticamente todos os dias. Nossos arquitetos de soluções e especialistas no assunto analisam a solução em busca de áreas para experimentar e melhorar.

Otimização de custo

Esta seção descreve como arquitetamos essa solução usando os princípios e as práticas recomendadas do pilar de otimização do custo.

- A solução usa uma arquitetura sem servidor, e os clientes pagam somente pelo que usam.
- A camada de computação da solução é padronizada para Lambda, que usa um modelo. pay-per-use
- O banco de dados e as consultas do Athena são otimizados para reduzir a quantidade de dados digitalizados, reduzindo assim os custos.

Sustentabilidade

Esta seção descreve como arquitetamos essa solução usando os princípios e as melhores práticas do pilar de sustentabilidade.

- A solução usa serviços gerenciados e sem servidor para minimizar o impacto ambiental dos serviços de back-end.
- O design sem servidor da solução visa reduzir a pegada de carbono em comparação com a pegada de servidores locais em operação contínua.

Detalhes de arquitetura

Esta seção descreve os componentes e os serviços da AWS que compõem essa solução e os detalhes da arquitetura sobre como esses componentes funcionam juntos.

Serviços da AWS nesta solução

Serviço da AWS	Descrição
AWS WAF	Principal. Implanta uma ACL web do AWS WAF, grupos de regras do AWS Managed Rules, regras personalizadas e conjuntos de IP. Faz chamadas de API do AWS WAF para bloquear ataques comuns e proteger aplicativ os web.
Amazon Data Firehose	Principal. Entrega registros do AWS WAF para buckets do Amazon S3.
Amazon S3	Principal. Armazena registros do AWS WAF CloudFront e ALB.
AWS Lambda	Principal. Implanta várias funções do Lambda para oferecer suporte a regras personalizadas.
Amazon EventBridge	Principal. Cria regras de eventos para invocar o Lambda.
Amazon Athena	Suporte. Cria consultas e grupos de trabalho do Athena para dar suporte ao analisador de log do Athena.
AWS Glue	Suporte. Cria bancos de dados e tabelas para dar suporte ao analisador de log Athena.
Amazon SNS	Suporte. Envia notificações por e-mail do Amazon Simple Notification Service (Amazon

Serviço da AWS	Descrição
	SNS) para apoiar a retenção de IP em listas permitidas e negadas.
AWS Systems Manager	Suporte. Fornece monitoramento de recursos em nível de aplicativo e visualização de operações de recursos e dados de custos.

Opções do analisador de log

Conforme descrito na visão geral da arquitetura, há três opções para lidar com as proteções de inundação e scanner e sonda HTTP. As seções a seguir explicam cada uma dessas opções com mais detalhes.

Regra baseada em taxas do AWS WAF

Regras baseadas em taxas estão disponíveis para proteção contra inundação de HTTP. Por padrão, uma regra baseada em intervalo agrega e limita o intervalo das solicitações com base no endereço IP da solicitação. Essa solução permite que você especifique o número de solicitações da web que um IP do cliente permite em um período posterior e continuamente atualizado de cinco minutos. Se um endereço IP violar a cota configurada, o AWS WAF bloqueia novas solicitações bloqueadas até que a taxa de solicitação seja menor que a cota configurada.

Recomendamos selecionar a opção de regra baseada em taxas se a cota de solicitações for superior a 2.000 solicitações por cinco minutos e você não precisar implementar personalizações. Por exemplo, você não considera o acesso estático a recursos ao contar as solicitações.

Você também pode configurar a regra para usar várias outras chaves de agregação e combinações de teclas. Para obter mais informações, consulte Opções e chaves de agregação.

Analisador de log Amazon Athena

Os parâmetros do modelo HTTP Flood Protection e Scanner & Probe Protection fornecem a opção de analisador de log Athena. Quando ativado, CloudFormation provisiona uma consulta do Athena e uma função Lambda programada responsável por orquestrar o Athena para executar, processar a saída do resultado e atualizar o AWS WAF. Essa função Lambda é invocada por um CloudWatch

evento configurado para ser executado a cada cinco minutos. Isso é configurável com o parâmetro Athena Query Run Time Schedule.

Recomendamos selecionar essa opção quando você não puder usar as regras baseadas em taxas do AWS WAF e tiver familiaridade com o SQL para implementar personalizações. Para obter mais informações sobre como alterar a consulta padrão, consulte Exibir consultas do Amazon Athena.

A proteção contra inundação HTTP é baseada no processamento do log de acesso do AWS WAF e usa arquivos de log do WAF. O tipo de log de acesso WAF tem um tempo de atraso menor, que você pode usar para identificar as origens da inundação HTTP mais rapidamente em comparação com o tempo de entrega do log do ALB. CloudFront No entanto, você deve selecionar o tipo de registro CloudFront ou ALB no parâmetro do modelo Activate Scanner & Probe Protection para receber códigos de status de resposta.

> **Note**
>
> Se um bot mal-intencionado contorna o honeypot e interage diretamente com o ALB ou CloudFront, o sistema detecta comportamento malicioso por meio da análise de registros, a menos que o HTTP Flood Protection e o Scanner & Probe Protection não estejam usando o analisador de log Lambda.

Analisador de log AWS Lambda

Os parâmetros do modelo HTTP Flood Protection e Scanner & Probe Protection fornecem a opção AWS Lambda Log Parser. Use o analisador de log Lambda somente quando a regra baseada em taxas do AWS WAF e as opções do analisador de log do Amazon Athena não estiverem disponíveis. Uma limitação conhecida dessa opção é que as informações são processadas dentro do contexto do arquivo que está sendo processado. Por exemplo, um IP pode gerar mais solicitações ou erros do que a cota definida, mas como essas informações são divididas em arquivos diferentes, cada arquivo não armazena dados suficientes para exceder a cota.

> **Note**
>
> Além disso, se um bot mal-intencionado contorna o honeypot e interage diretamente com o ALB ou CloudFront, a detecção depende da opção escolhida do analisador de log para identificar e bloquear efetivamente atividades maliciosas.

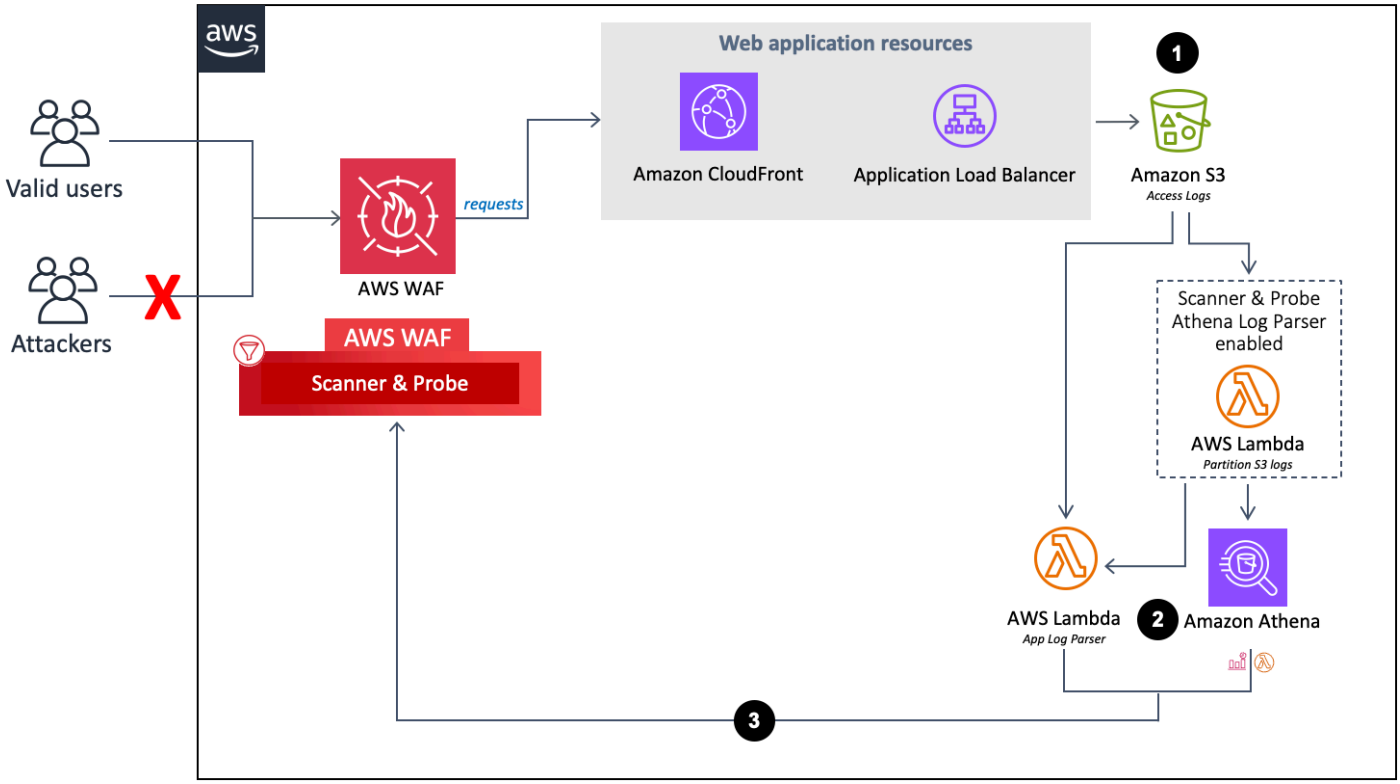
Detalhes do componente

Conforme descrito no diagrama de arquitetura, quatro dos componentes dessa solução usam automações para inspecionar endereços IP e adicioná-los à lista de bloqueios do AWS WAF. As seções a seguir explicam cada um desses componentes com mais detalhes.

Analisador de log - Aplicação

O analisador de log do aplicativo ajuda a proteger contra scanners e sondas.

Fluxo do analisador de log do aplicativo.



1. Quando CloudFront ou um ALB recebe solicitações em nome do seu aplicativo web, ele envia os registros de acesso para um bucket do Amazon S3.
   a. (Opcional) Se você selecionar `Yes - Amazon Athena log parser` os parâmetros do modelo Ativar proteção contra inundação HTTP e Ativar proteção de scanner e sonda, uma função Lambda moverá os registros de acesso de sua pasta original *`<customer-bucket>`* `/AWSLogs` para uma pasta recém-particionada *`<customer-bucket>`* `/AWSLogs-partitioned/` *`<optional-prefix>`* `/year=` *`<YYYY>`* `/month=` *`<MM>`* `/day=` *`<DD>`* `/hour=`*`<HH>`*/após sua chegada ao Amazon S3.

b. (Opcional) Se você selecionar `yes` o parâmetro Manter dados no modelo de localização original do S3, os registros permanecerão no local original e serão copiados para a pasta particionada, duplicando seu armazenamento de registros.

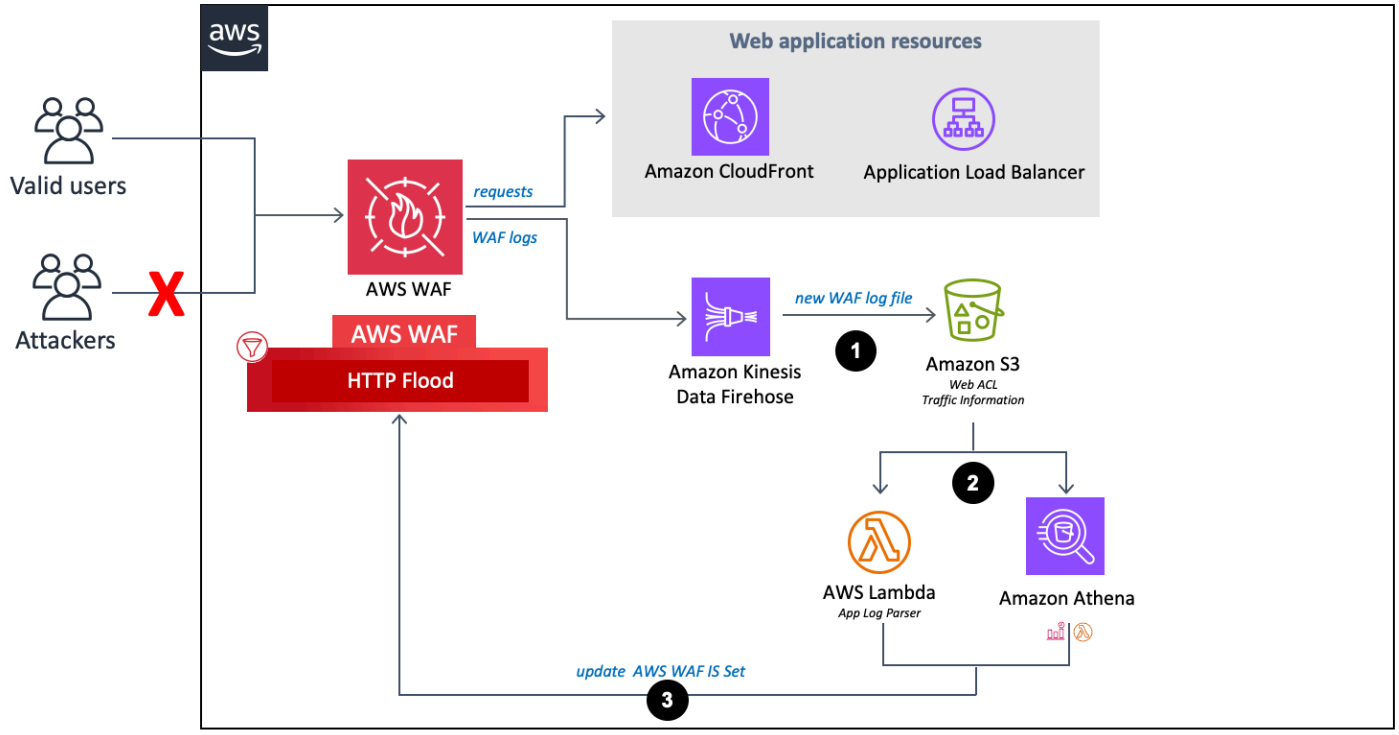
> **Note**
>
> Para o analisador de log Athena, essa solução particiona somente os novos registros que chegam ao seu bucket do Amazon S3 após a implantação dessa solução. Se você tem registros existentes que deseja particionar, você deve carregá-los manualmente para o Amazon S3 depois de implantar essa solução.

2. Com base na sua seleção dos parâmetros do modelo Ativar proteção contra inundação HTTP e Ativar proteção de scanner e sonda, essa solução processa os registros usando uma das seguintes opções:
   a. Lambda — Sempre que um novo log de acesso é armazenado no bucket do Amazon S3, a função `Log Parser` Lambda é iniciada.
   b. Athena — Por padrão, a cada cinco minutos, a consulta Athena do Scanner & Probe Protection é executada e a saída é enviada para o AWS WAF. Esse processo é iniciado por um CloudWatch evento, que inicia a função Lambda responsável por executar a consulta do Athena e envia o resultado para o AWS WAF.
3. A solução analisa os dados de registro para identificar endereços IP que geraram mais erros do que a cota definida. Em seguida, a solução atualiza uma condição de conjunto de IP do AWS WAF para bloquear esses endereços IP por um período de tempo definido pelo cliente.

Analisador de registros - AWS WAF

Se você selecionar `yes - AWS Lambda log parser` ou `yes - Amazon Athena log parser` ativar a proteção contra inundação HTTP, essa solução provisiona os seguintes componentes, que analisam os registros do AWS WAF para identificar e bloquear as origens que inundam o endpoint com uma taxa de solicitação maior do que a cota que você definiu.

Fluxo do analisador de log do AWS WAF.

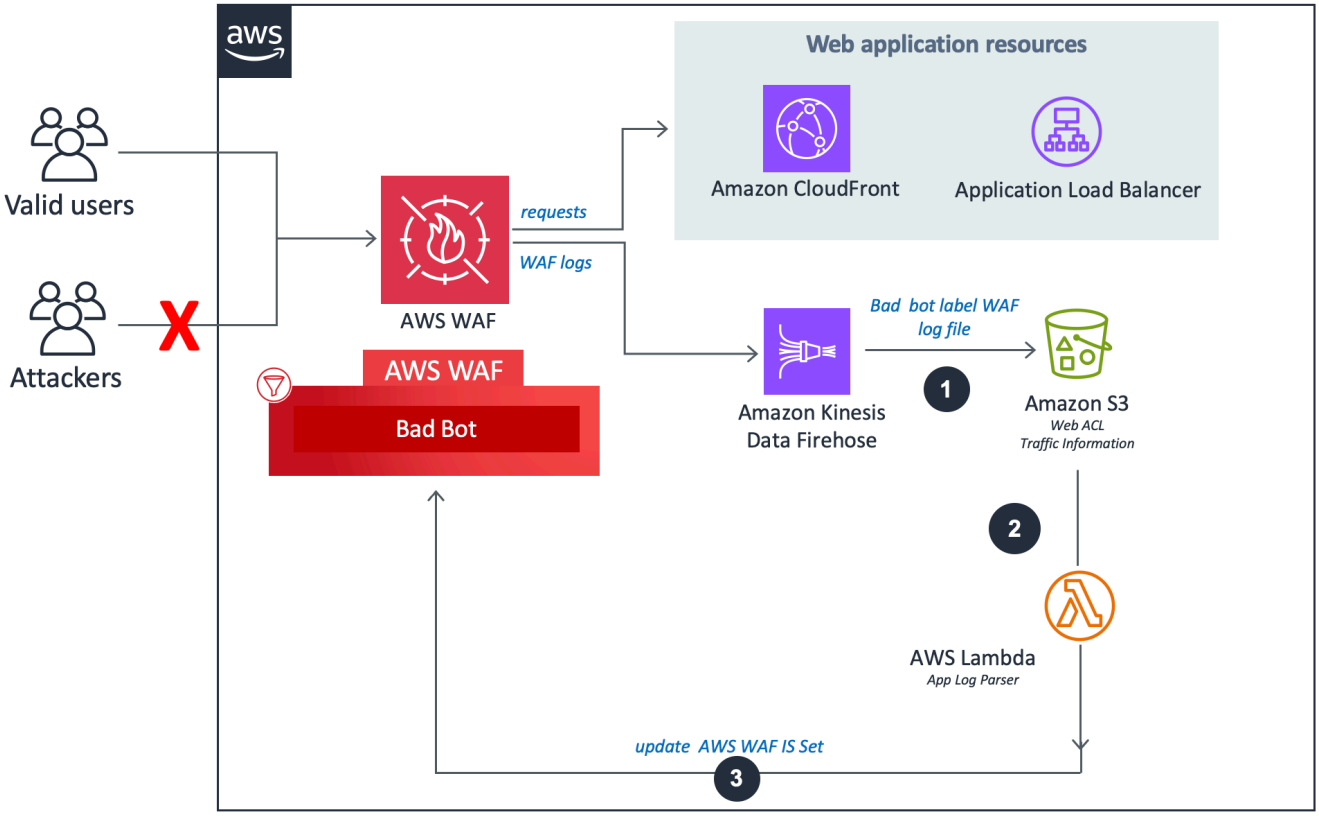


1. Quando o AWS WAF recebe registros de acesso, ele os envia para um endpoint Firehose. O Firehose então entrega os registros em um bucket particionado no Amazon S3 chamado *<customer-bucket>* /AWSLogs/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* / day= *<DD>* /hour= *<HH>* /
2. Com base na sua seleção dos parâmetros do modelo Ativar proteção contra inundação HTTP e Ativar proteção de scanner e sonda, essa solução processa os registros usando uma das seguintes opções:
   a. Lambda: sempre que um novo log de acesso é armazenado no bucket do Amazon S3, a função `Log Parser` Lambda é iniciada.
   b. Athena: Por padrão, a cada cinco minutos, a consulta do scanner e da sonda Athena é executada e a saída é enviada para o AWS WAF. Esse processo é iniciado por um CloudWatch evento da Amazon, que então inicia a função Lambda responsável pela execução da consulta do Amazon Athena e envia o resultado para o AWS WAF.
3. A solução analisa os dados de registro para identificar endereços IP que enviaram mais solicitações do que a cota definida. Em seguida, a solução atualiza uma condição de conjunto de IP do AWS WAF para bloquear esses endereços IP por um período de tempo definido pelo cliente.

Analisador de registros - Bad bot

O analisador de log do Bad bot inspeciona as solicitações para o endpoint do honeypot para extrair o endereço IP de origem.

Fluxo incorreto do analisador de log de bots.

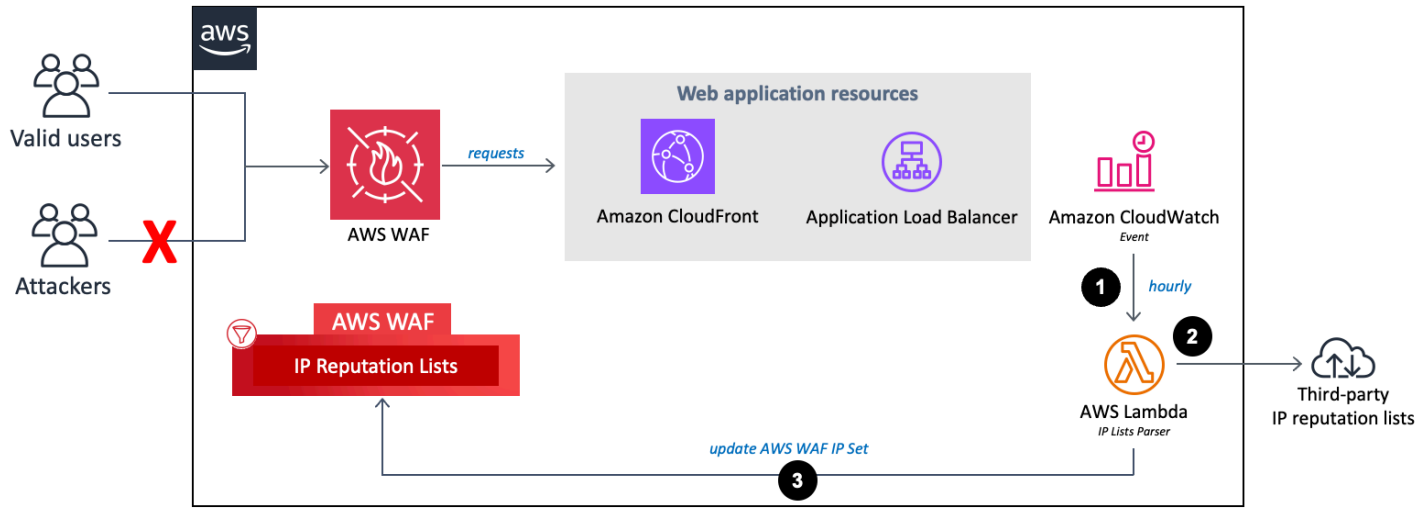


1. Se `Bad Bot Protection` estiver ativado e os recursos HTTP Flood Protection e Scanner & Probe Protection estiverem desativados: o sistema usará o analisador Log Lambda, que registra somente solicitações de bots incorretas com base nos filtros de rótulos WAF.
2. A função Lambda intercepta e inspeciona os cabeçalhos da solicitação para extrair o endereço IP da fonte que acessou o endpoint da armadilha.
3. A solução analisa os dados de registro para identificar endereços IP que enviaram mais solicitações do que a cota definida. Em seguida, a solução atualiza uma condição de conjunto de IP do AWS WAF para bloquear esses endereços IP por um período de tempo definido pelo cliente.

Analisador de listas IP

A função `IP Lists Parser` Lambda ajuda a proteger contra invasores conhecidos identificados em listas de reputação de IP de terceiros.

A reputação do IP lista o fluxo do analisador.



1. Um CloudWatch evento de hora em hora da Amazon invoca a função Lambda`IP Lists Parser`.
2. A função Lambda reúne e analisa dados de três fontes:
   - Listas DROP e EDROP do Spamhaus
   - Lista de IPs de ameaças emergentes da Proofpoint
   - Lista de modos de saída do Tor
3. A função Lambda atualiza a lista de bloqueios do AWS WAF com os endereços IP atuais.

Planeje a implantação

Esta seção descreve o custo, a segurança, as cotas e outras considerações antes da implantação da solução.

Regiões da AWS compatíveis

Dependendo dos valores dos parâmetros de entrada do modelo que você define, essa solução requer recursos diferentes. Esses recursos (listados na tabela a seguir) podem não estar disponíveis em todas as regiões da AWS. Portanto, você deve iniciar essa solução em uma região da AWS onde esses serviços estejam disponíveis. Para obter a disponibilidade mais atual dos serviços da AWS por região, consulte a Lista de serviços regionais da AWS.

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Endpoint type				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
Ative a proteção contra inundação HTTP				
sim - analisador de log AWS Lambda				✓
sim - Analisador de log Amazon Athena		✓	✓	✓
Ative a proteção do scanner e da sonda				

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
sim - Analisador de log Amazon Athena		✓	✓	

> **Note**
>
> Se você escolher `CloudFront` como seu Endpoint, deverá implantar a solução na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

Custo

Você é responsável pelo custo dos serviços da AWS usados ao executar a solução Security Automations for AWS WAF. O custo total da execução dessa solução depende da proteção ativada e da quantidade de dados ingeridos, armazenados e processados.

Recomendamos criar um orçamento por meio do AWS Cost Explorer para ajudar a gerenciar custos. Para obter detalhes completos, consulte a página de preços de cada serviço da AWS que você usou nesta solução.

As tabelas a seguir são exemplos de detalhamento de custos para executar essa solução na região Leste dos EUA (Norte da Virgínia) (excluindo o nível gratuito da AWS). Os preços estão sujeitos a alterações.

Exemplo 1: Ative a proteção de lista de reputação, a proteção contra bots incorretos, o analisador de registros AWS Lambda para proteção contra inundações de HTTP e a proteção de scanners e sondas

Serviço da AWS	Dimensões/mês	Custo [USD]
Amazon Data Firehose	100 GB	~$2,90
Amazon S3	100 GB	~$2,30

Serviço da AWS	Dimensões/mês	Custo [USD]
AWS Lambda	128 MB: 3 funções, 1 milhão de invocações e duração média de 500 milissegundos por execução do Lambda 512 MB: 2 funções, 1 milhão de invocações e duração média de 500 milissegundos por execução do Lambda	~$5,40
ACL da web do AWS WAF	1	$5,00
Regra do AWS WAF	4	$4,00
Solicitação do AWS WAF	1 milhão	$0,60
Total		~$20,60 por mês

Exemplo 2: Ative a proteção da lista de reputação, a proteção contra bots incorretos, o analisador de registros do Amazon Athena para proteção contra inundações de HTTP e a proteção de scanners e sondas

Serviço da AWS	Dimensões/mês	Custo [USD]
Amazon Data Firehose	100 GB	~$2,90
Amazon S3	100 GB	~$2,30
AWS Lambda	128 MB: 3 funções, 1 milhão de invocações e duração média de 500 milissegundos por execução do Lambda 512 MB: 2 funções, 7560 invocações e duração média	~$1,26

Serviço da AWS	Dimensões/mês	Custo [USD]
	de 500 milissegundos por execução do Lambda	
Amazon Athena	1,2 milhão de CloudFront acessos de objetos ou 1,2 milhão de solicitações de ALB por dia que geram um registro de registro de aproximadamente 500 bytes por ocorrência ou solicitação	~$4,32
ACL da web do AWS WAF	1	$5,00
Regra do AWS WAF	4	$4,00
Solicitação do AWS WAF	1 milhão	$0,60
Total		~$20,38 por mês

Exemplo 3: Ativar a retenção de IP para conjuntos de IP permitidos e negados

Serviço da AWS	Dimensões/mês	Custo [USD]
Amazon DynamoDB	1K gravações e 1 MB de armazenamento de dados	~$0,00
AWS Lambda	128 MB: 1 função, 2 mil invocações e duração média de 500 milissegundos por execução do Lambda 512 MB: 1 função, 2 mil invocações e duração média de 500 milissegundos por execução do Lambda	~$0,01

Serviço da AWS	Dimensões/mês	Custo [USD]
Amazon CloudWatch	Eventos 2K	~$0,00
AWS WAF Web ACL	1	$5,00
Regra do AWS WAF	2	$2,00
Solicitação do AWS WAF	1 milhão	$0,60
Total		~$7,61 por mês

Estimativa de custo dos CloudWatch registros

Alguns serviços da AWS usados nessa solução, como o Lambda, geram CloudWatch registros. Esses registros incorrem em cobranças. Recomendamos excluir ou arquivar registros para reduzir o custo. Para obter detalhes sobre o arquivamento de registros, consulte Exportação de dados de log para o Amazon S3 no Guia do usuário do CloudWatch Amazon Logs.

Se você optar por usar o analisador de log Athena na instalação, essa solução agenda uma consulta para ser executada no AWS WAF ou nos logs de acesso ao aplicativo em seu (s) bucket (s) do Amazon S3, conforme configurado. Você é cobrado com base na quantidade de dados verificados por cada consulta. A solução aplica particionamento a registros e consultas para minimizar os custos. Por padrão, a solução move os registros de acesso ao aplicativo de sua localização original no Amazon S3 para uma estrutura de pastas particionadas. Você também pode reter o original, mas será cobrado pelo armazenamento de registros duplicados. Essa solução usa grupos de trabalho para segmentar cargas de trabalho, e você pode configurar ambos para gerenciar o acesso e os custos das consultas. Consulte Estimativa de custo do Athena para obter um exemplo de cálculo de estimativa de custo. Para obter mais informações, consulte os preços do Amazon Athena.

Estimativa de custo de Athena

Se você usar a opção do analisador de log do Athena ao executar as regras HTTP Flood Protection, Scanner & Probe Protection ou Bad Bot Protection, você será cobrado pelo uso do Athena. Por padrão, cada consulta do Athena é executada a cada cinco minutos e verifica as últimas quatro horas de dados. A solução aplica particionamento a registros e consultas do Athena para minimizar os custos. Você pode configurar o número de horas de dados que uma consulta verifica alterando

o valor do parâmetro do modelo WAF Block Period. No entanto, aumentar a quantidade de dados digitalizados provavelmente aumentará o custo do Athena.

> **Tip**
>
> Veja a seguir um exemplo de cálculo CloudFront de custo de registros:
> Em média, cada CloudFront ocorrência pode gerar cerca de 500 bytes de dados.
> Se houver 1,2 milhão de CloudFront objetos atingidos por dia, haverá 200 mil (1,2 M/6) acessos a cada quatro horas, supondo que os dados sejam ingeridos em uma taxa consistente. Considere seus padrões reais de tráfego ao calcular seu custo.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> O Athena cobra $5,00 por TB de dados digitalizados.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> A consulta do Athena é executada a cada cinco minutos, ou seja, 12 execuções por hora.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> Os custos reais variam de acordo com os padrões de tráfego do seu aplicativo. Para obter mais informações, consulte os preços do Amazon Athena.

Segurança

Quando você cria sistemas na infraestrutura da AWS, as responsabilidades de segurança são compartilhadas entre você e a AWS. Esse modelo de responsabilidade compartilhada reduz sua carga operacional porque a AWS opera, gerencia e controla os componentes, incluindo o sistema operacional do host, a camada de virtualização e a segurança física das instalações nas quais os serviços operam. Para obter mais informações sobre a segurança da AWS, acesse AWS Cloud Security.

Perfis do IAM

Com as funções do IAM, você pode atribuir acesso, políticas e permissões granulares a serviços e usuários na nuvem da AWS. Essa solução cria funções do IAM com menos privilégios, e essas funções concedem aos recursos da solução as permissões necessárias.

Dados

Todos os dados armazenados nos buckets do Amazon S3 e nas tabelas do DynamoDB têm criptografia em repouso. Os dados em trânsito com o Firehose também são criptografados.

Capacidades de proteção

Os aplicativos da Web são vulneráveis a uma variedade de ataques. Esses ataques incluem solicitações especialmente criadas para explorar uma vulnerabilidade ou assumir o controle de um servidor; ataques volumétricos projetados para derrubar um site; ou bots e raspadores maliciosos programados para raspar e roubar conteúdo da web.

Essa solução é usada CloudFormation para configurar as regras do AWS WAF, incluindo grupos de regras e regras personalizadas do AWS Managed Rules, para bloquear os seguintes ataques comuns:

- AWS Managed Rules — Esse serviço gerenciado oferece proteção contra vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados. Essa solução inclui grupos de regras de reputação de IP gerenciado pela AWS, grupos de regras de linha de base gerenciados pela AWS e grupos de regras específicos de casos de uso do AWS Managed. Você tem a opção de selecionar um ou mais grupos de regras para sua ACL da web, até a cota máxima da unidade de capacidade da ACL da web (WCU).
- Injeção de SQL - Os atacantes inserem código SQL malicioso em solicitações da web para extrair dados do seu banco de dados. Criamos essa solução para bloquear solicitações da web que contêm código SQL potencialmente malicioso.
- XSS - Os atacantes usam vulnerabilidades em um site benigno como um veículo para injetar scripts maliciosos do site do cliente no navegador da web de um usuário legítimo. Projetamos isso para inspecionar elementos comumente explorados das solicitações recebidas para identificar e bloquear ataques XSS.
- Inundações de HTTP - servidores Web e outros recursos de back-end correm o risco de ataques DDo S, como inundações de HTTP. Essa solução invoca automaticamente uma regra baseada em taxas quando as solicitações da web de um cliente excedem uma cota configurável. Como alternativa, você pode impor essa cota processando os registros do AWS WAF usando uma função Lambda ou uma consulta do Athena.
- Scanners e sondas - Fontes maliciosas escaneiam e investigam aplicativos da Web voltados para a Internet em busca de vulnerabilidades, enviando uma série de solicitações que geram códigos de erro HTTP 4xx. Você pode usar esse histórico para ajudar a identificar e bloquear endereços

IP de origem maliciosos. Essa solução cria uma função Lambda CloudFront ou consulta Athena que analisa automaticamente nossos registros de acesso ao ALB, conta o número de solicitações inválidas de endereços IP de origem exclusivos por minuto e atualiza o AWS WAF para bloquear outras verificações de endereços que atingiram a cota de erro definida.

- Origens conhecidas dos atacantes (listas de reputação de IP) - Muitas organizações mantêm listas de reputação de endereços IP operados por atacantes conhecidos, como spammers, distribuidores de malware e botnets. Essa solução aproveita as informações dessas listas de reputação para ajudá-lo a bloquear solicitações de endereços IP maliciosos. Além disso, essa solução bloqueia invasores identificados por grupos de regras de reputação de IP com base na inteligência interna de ameaças da Amazon.
- Bots e scrapers - Os operadores de aplicativos da web acessíveis ao público precisam confiar que os clientes que acessam seu conteúdo se identificam com precisão e que usam os serviços conforme pretendido. No entanto, alguns clientes automatizados, como raspadores de conteúdo ou bots mal-intencionados, se apresentam erroneamente para contornar as restrições. Essa solução ajuda você a identificar e bloquear bots e raspadores defeituosos.

Cotas

Service quotas, ou limites, representam o máximo de recursos ou operações de serviço permitidos em uma conta AWS.

Cotas para serviços da AWS nesta solução

Verifique se você tem cota suficiente para cada um dos serviços implementados nessa solução. Para obter mais informações, consulte as cotas de serviços da AWS. Para ver as cotas de serviço de todos os serviços da AWS na documentação sem trocar de página, veja as informações na página de endpoints e cotas do serviço no PDF.

Cotas do AWS WAF

O AWS WAF pode bloquear no máximo 10.000 intervalos de endereços IP na notação Classless Inter-Domain Routing (CIDR) por condição de correspondência de IP. Cada lista criada por essa solução está sujeita a essa cota. Para obter mais informações, consulte as cotas do AWS WAF. A partir da versão 3.0, essa solução cria dois conjuntos de IP para anexar a cada regra, um para IPv4 e outro para IPv6.

O AWS WAF permite no máximo uma solicitação por segundo, por conta, por região da AWS para chamadas de API para qualquer indivíduo `Create` ou `Update` ação. `Put` Se você fizer essas chamadas de API fora da solução, poderá encontrar um problema de limitação da API. Para evitar o problema, recomendamos evitar a execução de outros aplicativos que façam essas chamadas de API na mesma conta e região em que essa solução está implantada.

Considerações de implantação

As seções a seguir fornecem restrições e considerações para implementar essa solução.

Regras do AWS WAF

A ACL da web que essa solução gera foi projetada para oferecer proteção abrangente para aplicativos da web. A solução fornece um conjunto de regras gerenciadas da AWS e regras personalizadas que você pode adicionar à ACL da web. Para incluir uma regra, escolha `yes` os parâmetros relevantes ao iniciar a CloudFormation pilha. Consulte a Etapa 1. Inicie a pilha para obter a lista de parâmetros.

> **Note**
>
> A out-of-box solução não é compatível com o AWS Firewall Manager. Se você quiser usar as regras no Firewall Manager, recomendamos que você aplique personalizações ao código-fonte.

Registro de tráfego da Web ACL

Se você criar a pilha em uma região da AWS diferente do Leste dos EUA (Norte da Virgínia) e definir o endpoint como`CloudFront`, deverá definir Ativar proteção contra inundação HTTP como ou. no `yes - AWS WAF rate based rule`

As outras duas opções (`yes - AWS Lambda log parser`e`yes - Amazon Athena log parser`) exigem a ativação dos registros do AWS WAF em uma ACL da web que é executada em todos os pontos de presença da AWS, e isso não é suportado fora do Leste dos EUA (Norte da Virgínia). Para obter mais informações sobre como registrar o tráfego do Web ACL, consulte o guia do desenvolvedor do AWS WAF.

Tratamento de grandes dimensões para componentes de solicitação

O AWS WAF não oferece suporte à inspeção de conteúdo superdimensionado para o corpo, cabeçalhos ou cookies do componente de solicitação da web. Ao escrever uma declaração de regra que inspeciona um desses tipos de componentes de solicitação, você pode escolher uma dessas opções para dizer ao AWS WAF o que fazer com essas solicitações:

- `yes`(continuar) - Inspecione o componente da solicitação normalmente de acordo com os critérios de inspeção da regra. O AWS WAF inspeciona o conteúdo do componente da solicitação que está dentro das limitações de tamanho. Essa é a opção padrão usada na solução.
- `yes - MATCH` - tratar a solicitação da Web como correspondente à instrução de regra. O AWS WAF aplica a ação da regra à solicitação sem avaliá-la de acordo com os critérios de inspeção da regra. Para uma regra com `Block` ação, isso bloqueia a solicitação com o componente de tamanho grande.
- `yes - 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. O 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.

Para obter mais informações, consulte Como lidar com componentes de solicitações web de grande porte no AWS WAF.

Implantações de várias soluções

Você pode implantar a solução várias vezes na mesma conta e região. Você deve usar um nome de CloudFormation pilha exclusivo e um nome de bucket do Amazon S3 para cada implantação. Cada implantação exclusiva incorre em cobranças adicionais e está sujeita às cotas do AWS WAF por conta, por região.

Permissões mínimas de função para implantação (opcional)

Os clientes podem criar manualmente uma função do IAM com as permissões mínimas necessárias para implantação:

- Permissões do WAF

```
        {
```

```
            "Effect": "Allow",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:UpdateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:GetWebACL",
                "wafv2:ListWebACLs",
                "wafv2:CreateIPSet",
                "wafv2:UpdateIPSet",
                "wafv2:DeleteIPSet",
                "wafv2:GetIPSet",
                "wafv2:AssociateWebACL",
                "wafv2:DisassociateWebACL",
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration",
                "wafv2:ListWebACLs",
                "wafv2:ListIPSets",
                "wafv2:ListTagsForResource"
            ],
            "Resource": [
                "arn:aws:wafv2:*:*:regional/webacl/*",
                "arn:aws:wafv2:*:*:regional/ipset/*",
                "arn:aws:wafv2:*:*:global/webacl/*",
                "arn:aws:wafv2:*:*:global/ipset/*"
            ]
        }
```

- Permissões Lambda

```
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*"
```

```
        }
```

- Permissões do Firehose

```
        {
            "Effect": "Allow",
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- Permissões do S3

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
```

```
            "s3:PutBucketLogging",
            "s3:GetBucketLogging"
        ],
        "Resource": "arn:aws:s3:::*"
    }
```

- Permissões do Athena

```
    {
        "Effect": "Allow",
        "Action": [
            "athena:CreateWorkGroup",
            "athena:DeleteWorkGroup",
            "athena:GetWorkGroup",
            "athena:UpdateWorkGroup",
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution"
        ],
        "Resource": "arn:aws:athena:*:*:workgroup/WAF*"
    }
```

- Permissões do Glue

```
    {
        "Effect": "Allow",
        "Action": [
            "glue:CreateDatabase",
            "glue:DeleteDatabase",
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:UpdateDatabase",
            "glue:CreateTable",
            "glue:DeleteTable",
            "glue:GetTable",
            "glue:GetTables",
            "glue:UpdateTable"
        ],
        "Resource": [
```

```
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch Permissões de registros

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream",
                "logs:PutRetentionPolicy",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/*",
                "arn:aws:logs:*:*:log-group:*",
                "arn:aws:logs:*:*:log-group:/aws/kinesisfirehose/*"
            ]
        }
```

- CloudWatch Permissões

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DeleteDashboards",
                "cloudwatch:GetDashboard",
                "cloudwatch:ListDashboards",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        }
```

- Permissões do SNS

```
{
    "Effect": "Allow",
    "Action": [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
    ],
    "Resource": "arn:aws:sns:*:*:*"
}
```

- Permissões do DynamoDB

```
{
    "Effect": "Allow",
    "Action": [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem"
    ],
    "Resource": "arn:aws:dynamodb:*:*:table/*"
}
```

- CloudFormation Permissões

```
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
```

```
            "cloudformation:ListStacks"
        ],
        "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
    }
```

- Permissões de registro de aplicativos do Service Catalog

```
    {
        "Effect": "Allow",
        "Action": [
            "servicecatalog:CreateApplication",
            "servicecatalog:DeleteApplication",
            "servicecatalog:GetApplication",
            "servicecatalog:TagResource",
            "servicecatalog:CreateAttributeGroup",
            "servicecatalog:DeleteAttributeGroup",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:AssociateAttributeGroup",
            "servicecatalog:DisassociateAttributeGroup",
            "servicecatalog:AssociateResource",
            "servicecatalog:DisassociateResource"
        ],
        "Resource": "arn:aws:servicecatalog:*:*:*"
    }
```

- Permissões do X-Ray

```
    {
        "Effect": "Allow",
        "Action": [
            "xray:PutTraceSegments",
            "xray:PutTelemetryRecords"
        ],
        "Resource": "*"
    }
```

- Permissões do IAM

```
    {
```

```
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRoles",
                "iam:PassRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/*"
        }
```

- EventBridge Permissões

```
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:DescribeRule",
                "events:EnableRule",
                "events:ListRules",
                "events:PutRule",
                "events:DeleteRule",
                "events:ListEventSources",
                "events:DescribeEventSource",
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

Implante a solução

Essa solução usa CloudFormation modelos e pilhas da AWS para automatizar sua implantação. Os CloudFormation modelos especificam os recursos da AWS incluídos nessa solução e suas propriedades. A CloudFormation pilha provisiona os recursos descritos nos modelos.

Visão geral do processo de implantação

Antes de iniciar o CloudFormation modelo, revise as considerações de arquitetura e configuração discutidas neste guia. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em sua conta.

Tempo de implantação: Aproximadamente 15 minutos.

> **Note**
>
> Se você já implantou essa solução, consulte Atualizar a solução para obter instruções de atualização.

Pré-requisitos

- Configurar uma CloudFront distribuição
- Configurar um ALB

Etapa 1. Inicie a pilha

- Inicie o CloudFormation modelo em sua conta da AWS.
- Insira valores para os parâmetros necessários: Nome da pilha e Nome do bucket do log de acesso ao aplicativo.
- Revise os outros parâmetros do modelo e ajuste, se necessário.

Etapa 2. Associe a ACL da web ao seu aplicativo da web

- Associe suas distribuições CloudFront web ou ALB (s) à ACL da web que essa solução gera. Você pode associar quantas distribuições ou balanceadores de carga quiser.

Etapa 3. Configurar o registro de acesso à web

- Ative o registro de acesso à CloudFront web para suas distribuições web ou ALB (s) e envie arquivos de log para o bucket apropriado do Amazon S3. Salve os registros em uma pasta que corresponda ao prefixo definido pelo usuário. Se nenhum prefixo definido pelo usuário for usado, salve os registros em AWSLogs (`AWSLogs/`prefixo de registro padrão). Consulte o parâmetro Application Access Log Bucket Prefix na Etapa 1. Inicie a pilha para obter mais informações.

CloudFormation Modelos da AWS

Essa solução inclui um CloudFormation modelo principal da AWS e dois modelos aninhados. Você pode baixar os CloudFormation modelos antes de implantar a solução.

Stack principal

aws-waf-security-automations.template - Use esse modelo como ponto de entrada para iniciar a solução em sua conta. A configuração padrão implanta uma ACL web do AWS WAF com regras pré-configuradas. Você pode personalizar o modelo com base nas suas necessidades.

Pilha WebACL

aws-waf-security-automations-webacl.template - Esse modelo aninhado provisiona recursos do AWS WAF, incluindo uma ACL da web, IP, conjuntos e outros recursos associados.

Pilha Firehose Athena

aws-waf-security-automations-firehose-athena.template — Esse modelo aninhado provisiona recursos relacionados ao AWS Glue, Athena e Firehose. Ele é criado quando você escolhe o analisador de log Scanner & Probe Athena ou o analisador de log HTTP Flood Lambda ou Athena.

> **Note**
>
> Os CloudFormation recursos da AWS são criados a partir de construções do AWS Cloud Development Kit (AWS CDK).

Esse CloudFormation modelo da AWS implanta a solução Security Automations for AWS WAF na Nuvem AWS.

Pré-requisitos

Essa solução foi projetada para funcionar com aplicativos web implantados com CloudFront ou com um ALB. Se você ainda não tiver um desses recursos configurado, conclua as tarefas aplicáveis antes de iniciar essa solução.

Configurar uma CloudFront distribuição

Conclua as etapas a seguir para configurar uma CloudFront distribuição para o conteúdo estático e dinâmico do seu aplicativo web. Consulte o Amazon CloudFront Developer Guide para obter instruções detalhadas.

1. Crie uma distribuição de aplicativos CloudFront web. Consulte Criação de uma distribuição.
2. Configure origens estáticas e dinâmicas. Consulte Usando várias origens com CloudFront distribuições.
3. Especifique o comportamento da sua distribuição. Consulte os valores que você especifica ao criar ou atualizar uma distribuição.

> **Note**
>
> Se você escolher `CloudFront` como seu endpoint, deverá criar seus WAFV2 recursos na região Leste dos EUA (Norte da Virgínia).

Configurar um ALB

Para configurar um ALB para distribuir o tráfego de entrada para seu aplicativo web, consulte Create an Application Load Balancer no Guia do usuário para Application Load Balancers.

Etapa 1. Iniciar a pilha

Esse CloudFormation modelo automatizado da AWS implanta a solução na nuvem da AWS.

1. Faça login no AWS Management Console e selecione o `waf-automation-on-aws.template` CloudFormation modelo Launch Solution to Launch.

2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução em uma região diferente da AWS, use o seletor de regiões na barra de navegação do console. Se você escolher `CloudFront` como seu endpoint, deverá implantar a solução na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

> **Note**
>
> Dependendo dos valores dos parâmetros de entrada definidos, essa solução requer recursos diferentes. Atualmente, esses recursos estão disponíveis somente em regiões específicas da AWS. Portanto, você deve iniciar essa solução em uma região da AWS onde esses serviços estejam disponíveis. Para obter mais informações, consulte Regiões compatíveis da AWS.

3. Na página Especificar modelo, verifique se você selecionou o modelo correto e escolha Avançar.
4. Na página Especificar detalhes da pilha, atribua um nome à sua configuração do AWS WAF no campo Nome da pilha. Esse também é o nome da ACL da web que o modelo cria.
5. Em Parâmetros, revise os parâmetros do modelo e modifique-os conforme necessário. Para desativar um recurso específico, escolha none ou no conforme aplicável. Essa solução usa os seguintes valores padrão.

Parameter	Padrão	Descrição
Nome da stack	`[.red]#<requires input>`	O nome da pilha não pode conter espaços. Esse nome deve ser exclusivo em sua conta da AWS e é o nome da

Parameter	Padrão	Descrição
		ACL da web que o modelo cria.
Tipo de recurso		
Endpoint	`CloudFront`	Escolha o tipo de recurso que está sendo usado. NOTA: Se você escolher `CloudFront` como seu endpoint, deverá iniciar a solução para criar recursos WAF na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).
Grupos de regras de reputação de IP gerenciados pela AWS		

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciadas da lista de reputação de IP da Amazon	no	Escolha `yes` ativar o componente projetado para adicionar o Amazon IP Reputation List Managed Rule Group à web ACL. Esse grupo de regras é baseado na inteligência interna de ameaças da Amazon. Isso é útil se você quiser bloquear endereços IP normalmente associado s 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. A WCU necessária é 25. Sua conta deve ter capacidad e de WCU suficiente para evitar falhas na implantaç ão da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informaçõ es, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciadas da lista de IP anônima	no	Escolha ativar o component e projetado `yes` para adicionar o Grupo de Regras Gerenciadas da Lista de IP Anônima à ACL da web. Esse grupo de regras bloqueia solicitações de serviços que permitem a ofuscação da identidade do espectador. Isso inclui solicitações de VPNs, proxies, nós Tor e provedore s 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. A WCU necessária é 50. Sua conta deve ter capacidad e de WCU suficiente para evitar falhas na implantaç ão da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informaçõ es, consulte a lista de grupos

Parameter	Padrão	Descrição
		de regras do AWS Managed Rules.
Grupos de regras básicas gerenciadas pela AWS		
Ativar a proteção de grupos de regras gerenciados do conjunto de regras principais	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas do Conjunto de Regras Principais à ACL da web. Esse grupo de regras oferece proteção contra a exploração de uma ampla variedade de vulnerabilidades, incluindo algumas das vulnerabilidades de alto risco e comuns. Considere usar esse grupo de regras para qualquer caso de uso do AWS WAF. A WCU necessária é 700. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ativar a Proteção Administrativa Proteção de Grupos de Regras Gerenciadas	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas de Proteção Administrativa à ACL da web. Esse grupo de regras bloqueia o acesso externo às 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. A WCU necessária é 100. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciados de entradas inválidas conhecidas	no	Escolha ativar o componente projetado `yes` para adicionar o grupo de regras gerenciadas de entradas incorretas conhecidas à ACL da web. Esse grupo de regras bloqueia o acesso externo às 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. A WCU necessária é 100. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de regras do AWS Managed Rules.
Grupo de regras específicas de casos de uso gerenciados da AWS		

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciadas do banco de dados SQL	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas do Banco de Dados SQL à ACL da web. Esse grupo de regras bloqueia 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. Usar a regra personalizada de injeção de SQL é opcional se você já tiver um grupo de regras SQL gerenciado pela AWS ativado. A WCU necessária é 200. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos

Parameter	Padrão	Descrição
		de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciados do sistema operacional Linux	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas do Sistema Operacional Linux à ACL da web. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas do Linux, incluindo ataques de inclusão de arquivos locais (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. Avalie esse grupo de regras se alguma parte do seu aplicativo for executada no Linux. Você deve usar esse grupo de regras em conjunto com o grupo de regras do sistema operacional POSIX. A WCU necessária é 200. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade.

Parameter	Padrão	Descrição
		Para obter mais informaçõ es, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ative a proteção de grupo de regras gerenciadas do sistema operacional POSIX	no	Escolha ativar o componente projetado `yes` para adicionar o Core Rule Set Managed Rule Group Protection à Web ACL. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas de sistemas operacionais do tipo POSIX e POSIX, incluindo ataques 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. Avalie esse grupo de regras se alguma parte do seu aplicativo for executada em um sistema operacional POSIX ou semelhante ao POSIX. A WCU necessária é 100. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos

Parameter	Padrão	Descrição
		de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ativar a Proteção de Grupo de Regras Gerenciadas do Sistema Operacional Windows	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas do Sistema Operacional Windows à ACL da web. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas do Windows, como 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. A WCU necessária é 200. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade.

Parameter	Padrão	Descrição
		Para obter mais informaçõ es, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Ative a proteção de grupos de regras gerenciados de aplicativos PHP	no	Escolha ativar o componente projetado `yes` para adicionar o PHP Application Managed Rule Group à ACL da web. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas ao uso da linguagem de programação PHP, incluindo a injeção de funções PHP inseguras. 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. A WCU necessária é 100. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos

Parameter	Padrão	Descrição
		de regras do AWS Managed Rules.
Ativar a proteção de grupos de regras gerenciadas por WordPress aplicativos	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas por WordPress Aplicativos à ACL da web. Esse grupo de regras bloqueia os padrões de solicitação associados à exploração de vulnerabilidades específicas dos WordPress sites. Avalie esse grupo de regras se você estiver executando WordPress. Esse grupo de regras deve ser usado em conjunto com os grupos de regras do banco de dados SQL e do aplicativo PHP. A WCU necessária é 100. Sua conta deve ter capacidade de WCU suficiente para evitar falhas na implantação da pilha de ACL da web devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de regras do AWS Managed Rules.

Parameter	Padrão	Descrição
Regra personalizada - Scanners e sondas		
Ative a proteção do scanner e da sonda	`yes - AWS Lambda log parser`	Escolha o componente usado para bloquear scanners e sondas. Consulte Opções do analisador de log para obter mais informações sobre as compensações relacionadas às opções de mitigação.

Parameter	Padrão	Descrição
Nome do bucket do log de acesso ao aplicativo	`[.red]<requires input>`	Se você escolheu `yes` o parâmetro Activate Scanner & Probe Protection, insira o nome do bucket do Amazon S3 (novo ou existente) no qual você deseja armazenar os registros de acesso para CloudFront sua (s) distribui ção (ões) ou ALB (s). Se você estiver usando um bucket Amazon S3 existente , ele deverá estar localizad o na mesma região da AWS em que você está implantan do o modelo. CloudFormation Você deve usar um bucket diferente para cada implantaç ão da solução. Para desativar essa proteção, ignore esse parâmetro . OBSERVAÇÃO: ative o registro de acesso à CloudFront web para suas distribuições web ou ALB (s) para enviar arquivos de log para esse bucket do Amazon S3. Salve os registros no mesmo prefixo definido na pilha (`AWSLogs/`prefixo padrão). Consulte o parâmetro Application Access Log

Parameter	Padrão	Descrição
		Bucket Prefix para obter mais informações.
Prefixo do bucket do log de acesso ao aplicativo	`AWSLogs/`	Se você escolher `yes` o parâmetro Activate Scanner & Probe Protection, poderá inserir um prefixo opcional definido pelo usuário para o bucket de registros de acesso ao aplicativo acima. Se você escolher `CloudFront` o parâmetro Endpoint, poderá inserir qualquer prefixo, como. `yourprefix/` Se você escolher `ALB` o parâmetro Endpoint, deverá acrescentar `AWSLogs/` ao seu prefixo, como. `yourprefix/AWSLogs/` Use `AWSLogs/` (padrão) se não houver um prefixo definido pelo usuário. Para desativar essa proteção, ignore esse parâmetro.

Parameter	Padrão	Descrição
O registro de acesso ao bucket está ativado?	no	Escolha `yes` se você inseriu um nome de bucket do Amazon S3 existente para o parâmetro Application Access Log Bucket Name e se o registro de acesso ao servidor para o bucket já está ativado. Se você escolherno, a solução ativará o registro de acesso ao servidor para seu bucket. Se você escolheu no o parâmetro Activate Scanner & Probe Protection, ignore esse parâmetro.
Limite de erro	`50`	Se você escolher `yes` o parâmetro Activate Scanner & Probe Protection, insira o máximo aceitável de solicitaç ões inválidas por minuto, por endereço IP. Se você escolheu no o parâmetro Activate Scanner & Probe Protection, ignore esse parâmetro.

Parameter	Padrão	Descrição
Mantenha os dados no local original do S3	no	Se você escolher `yes - Amazon Athena log parser` o parâmetro Activate Scanner & Probe Protection, a solução aplica o particionamento aos arquivos de log de acesso ao aplicativo e às consultas do Athena. Por padrão, a solução move os arquivos de log do local original para uma estrutura de pastas particionadas no Amazon S3. Escolha `yes` se você também deseja manter uma cópia dos registros no local original. Isso duplicará seu armazenamento de registros. Se você não escolheu `yes - Amazon Athena log parser` o parâmetro Activate Scanner & Probe Protection, ignore esse parâmetro.
Regra personalizada - HTTP Flood		

Parameter	Padrão	Descrição
Ative a proteção contra inundação HTTP	`yes - AWS WAF rate-based rule`	Selecione o component e usado para bloquear ataques de inundação HTTP. Consulte Opções do analisador de log para obter mais informações sobre as compensações relacionadas às opções de mitigação.
Limite de solicitação padrão	`100`	Se você escolher `yes` o parâmetro Ativar proteção contra inundação HTTP, insira o máximo de solicitaç ões aceitáveis por cinco minutos, por endereço IP. Se você escolher `yes - AWS WAF rate-based rule` o parâmetro Ativar proteção contra inundação HTTP, o valor mínimo aceitável será`10`. Se você escolheu `yes - AWS Lambda log parser` ou `yes - Amazon Athena log parser` para o parâmetro Ativar proteção contra inundação HTTP, ele pode ser qualquer valor. Para desativar essa proteção, ignore esse parâmetro.

Parameter	Padrão	Descrição
Limite de solicitação por país	<optional input>	Se você escolher `yes - Amazon Athena log parser` o parâmetro Activate HTTP Flood Protection, poderá inserir um limite por país seguindo esse formato JSON. `{"TR":50, "ER":150}` A solução usa esses limites para as solicitações originadas dos países especificados. A solução usa o parâmetro Default Request Threshold para as solicitações restantes . OBSERVAÇÃO: Se você definir esse parâmetro, o país será incluído automatic amente no grupo de consulta do Athena, junto com o IP e outros campos opcionais de agrupamento por que você pode selecionar com o parâmetro Agrupar por solicitações no HTTP Flood Athena Query. + Se você optar por desativar essa proteção, ignore esse parâmetro.

Parameter	Padrão	Descrição
Agrupar por solicitações em HTTP Flood Athena Query	`None`	Se você escolher `yes - Amazon Athena log parser` o parâmetro Ativar proteção contra inundação HTTP, poderá escolher um campo agrupado por para contar as solicitações por IP e o campo agrupado selecionado. Por exemplo, se você escolher`URI`, a solução contará as solicitações por IP e URI. Se você optar por desativar essa proteção, ignore esse parâmetro.
Período de bloqueio do WAF	`240`	Se você escolher `yes - AWS Lambda log parser` entre os parâmetros Ativar Proteção de Scanner e Sonda ou Ativar Proteção contra Inundação HTTP, insira o período (em minutos) para bloquear os endereços IP aplicáveis. `yes - Amazon Athena log parser` Para desativar a análise de registros, ignore esse parâmetro.

Parameter	Padrão	Descrição
Cronograma de tempo de execução do Athena Query (minuto)	5	Se você escolher `yes - Amazon Athena log parser` os parâmetros Activate Scanner & Probe Protection ou Activate HTTP Flood Protection, poderá inserir um intervalo de tempo (em minutos) durante o qual a consulta do Athena é executada. Por padrão, a consulta do Athena é executada a cada 5 minutos. Se você optar por desativar essas proteções, ignore esse parâmetro.

Parameter	Padrão	Descrição
Chaves de regras	`IP`	Se você escolheu `yes - AWS WAF rate-based rule` o parâmetro Ativar proteção contra inundação HTTP, configure essa regra para usar várias outras combinações de chaves de agregação. Opções disponíveis: IP (padrão) IP+cabeçalho personalizado (se essa opção for selecionada, `Rule Keys Custom Header` é obrigatório) IP+URI MÉTODO IP+HTTP Para obter mais informações, consulte Opções de agregação com base na taxa de regras do WAF.

Parameter	Padrão	Descrição
Cabeçalho personalizado de chaves de regra	no	Se você escolheu `IP +Custom Header` o parâmetro Rule Keys, insira o nome do cabeçalho personalizado a ser usado para a agregação de solicitações. Para obter mais informações, consulte Opções de agregação com base na taxa do tipo de declaração de regra do WAF.

Parameter	Padrão	Descrição
Limite da janela de tempo (minutos)	5	Limite da janela de tempo em minutos para proteção contra inundação de HTTP. Aplica-se tanto à regra baseada em taxa quanto ao analisador de log lambda. Opções disponíveis: [1, 2, 5, 10]. Se você escolher `yes - AWS WAF rate-based rule` o parâmetro Ativar HTTP Flood Protection, será usado para janelas de tempo de avaliação. Para obter mais informações, consulte a declaração baseada na taxa de ACL na web do WAF. Se você escolher `yes - AWS Lambda log parser` o parâmetro Ativar HTTP Flood Protection, será usado para o período de avaliação, além do período de bloqueio.
Regra personalizada - Bad Bot		
Ative a proteção Bad Bot	`yes`	Escolha `yes` ativar o componente projetado para bloquear bots maliciosos e raspadores de conteúdo.

Parameter	Padrão	Descrição
ARN de uma função do IAM que tem acesso de gravação aos CloudWatch registros em sua conta	<optional input>	Forneça um ARN opcional de uma função do IAM que tenha acesso de gravação aos CloudWatch registros em sua conta. Por exemplo: `ARN: arn:aws:iam::account_id:role/myrolename` . Se você deixar esse parâmetro em branco (padrão), a solução criará uma nova função para você.
Regra personalizada - Listas de reputação de IP de terceiros		
Ative a proteção da lista de reputação	`yes`	Escolha `yes` bloquear solicitações de endereços IP em listas de reputação de terceiros (as listas suportadas incluem Spamhaus, Emerging Threats e Tor exit node).
Regras personalizadas antigas		

Parameter	Padrão	Descrição
Ativar a proteção de injeção de SQL	`yes`	Escolha `yes` ativar o componente projetado para bloquear ataques comuns de injeção de SQL. Considere ativá-lo se você não estiver usando um conjunto de regras principais gerenciadas pela AWS ou um grupo de regras do banco de dados SQL gerenciado pela AWS. Você pode escolher uma das opções `yes` (continuar) ou `yes - NO_MATCH`) que deseja que o AWS WAF processe solicitações superdimensionadas que excedam 8 KB (8192 bytes). `yes - MATCH` Por padrão, `yes` inspeciona o conteúdo do componente da solicitação que está dentro das limitações de tamanho de acordo com os critérios de inspeção da regra. Para obter mais informações, consulte Como lidar com componentes de solicitações web de tamanho grande. Escolha no desativar esse recurso. NOTA: A CloudFormation pilha adiciona a opção de tratamento de tamanho grande selecionada à regra

Parameter	Padrão	Descrição
		padrão de proteção por injeção de SQL e a implanta em sua conta da AWS. Se você personalizou a regra fora de CloudFormation, suas alterações serão substituídas após a atualização da pilha.

Parameter	Padrão	Descrição
Nível de sensibilidade para proteção por injeção de SQL	`LOW`	Escolha o nível de sensibilidade que você deseja que o AWS WAF use para inspecionar ataques de injeção de SQL. `HIGH`detecta mais ataques, mas pode gerar mais falsos positivos. `LOW` geralmente é a melhor opção para recursos que já têm outras proteções contra ataques de injeção de SQL ou que têm baixa tolerância a falsos positivos. Para obter mais informações, consulte AWS WAF adiciona níveis de sensibilidade para declarações e SensitivityLevel propriedades de regras de injeção de SQL no Guia CloudFormation do usuário da AWS. Se você optar por desativar a proteção por injeção de SQL, ignore esse parâmetro. NOTA: A CloudFormation pilha adiciona o nível de sensibilidade selecionado à regra padrão de proteção por injeção de SQL e o implanta em sua conta da AWS. Se você personalizou a regra

Parameter	Padrão	Descrição
		fora de CloudFormation, suas alterações serão substituídas após a atualização da pilha.

Parameter	Padrão	Descrição
Ative a proteção de script entre sites	`yes`	Escolha `yes` ativar o componente projetado para bloquear ataques XSS comuns. Considere ativá-lo se você não estiver usando um conjunto de regras principais gerenciado pela AWS. Você também pode selecionar uma das opções `yes` (continuar) ou`yes - NO_MATCH`) que deseja que o AWS WAF processe solicitações superdimensionadas que excedam 8 KB (8192 bytes). `yes - MATCH` Por padrão, `yes` usa a `Continue` opção, que inspeciona o conteúdo do componente da solicitação que está dentro das limitações de tamanho de acordo com os critérios de inspeção da regra. Para obter mais informações, consulte Tratamento de tamanho excessivo para componentes de solicitação. Escolha no desativar esse recurso. NOTA: A CloudFormation pilha adiciona a opção de tratamento de grandes dimensões selecionada à regra padrão de cross-site scripting e a implanta em sua conta da AWS. Se você

Parameter	Padrão	Descrição
		personalizou a regra fora de CloudFormation, suas alterações serão substituídas após a atualização da pilha.
Configurações de retenção de IP permitidas e negadas		
Período de retenção (minutos) para o conjunto de IP permitido	`-1`	Se você quiser ativar a retenção de IP para o conjunto de IPs permitidos, insira um número (`15`ou mais) como período de retenção (minutos). Os endereços IP que atingem o período de retenção expiram e a solução os remove do conjunto de IPs. A solução suporta um período mínimo de retenção de 15 minutos. Se você inserir um número entre `0` e`15`, a solução o tratará como`15`. Deixe-o como `-1` (padrão) para desativar a retenção de IP.

Parameter	Padrão	Descrição
Período de retenção (minutos) para o conjunto de IPs negados	`-1`	Se você quiser ativar a retenção de IP para o conjunto de IP negado, insira um número (`15`ou mais) como período de retenção (minutos). Os endereços IP que atingem o período de retenção expiram e a solução os remove do conjunto de IPs. A solução suporta um período mínimo de retenção de 15 minutos. Se você inserir um número entre `0` e`15`, a solução o tratará como`15`. Deixe-o como `-1` (padrão) para desativar a retenção de IP.
E-mail para receber notificação sobre a expiração dos conjuntos de IP permitidos ou negados	<optional input>	Se você ativou os parâmetros do período de retenção de IP (veja dois parâmetros anteriores) e quiser receber uma notificação por e-mail quando os endereços IP expirarem, insira um endereço de e-mail válido. Se você não ativou a retenção de IP ou deseja desativar as notificações por e-mail, deixe em branco (padrão).

Parameter	Padrão	Descrição
Configurações avançadas		
Período de retenção (dias) para grupos de registros	`365`	Se você quiser ativar a retenção para os grupos de CloudWatch registros, insira um número (1ou mais) como o período de retenção (dias). Você pode escolher um período de retenção entre um dia (`1`) e dez anos (`3650`). Por padrão, os registros expiram após um ano. Defina-o para `-1` manter os registros indefinidamente.

6. Escolha Próximo.
7. Na página Configurar opções de pilha, você pode especificar tags (pares de valores-chave) para recursos em sua pilha e definir opções adicionais. Escolha Próximo.
8. Na página Revisar e criar, revise e confirme as configurações. Selecione as caixas confirmando que o modelo criará recursos do IAM e quaisquer recursos adicionais necessários.
9. Escolha Enviar para implantar a pilha.

   Veja o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status CREATE_COMPLETE em aproximadamente 15 minutos.

> **Note**
>
> Além das funções `Log Parser` e do `IP Lists Parser` AWS Lambda, essa solução inclui as funções `helper` `custom-resource` Lambda e do AWS, que são executadas somente durante a configuração inicial ou quando os recursos são atualizados ou excluídos.
>
> Ao usar essa solução, você verá todas as funções no console do AWS Lambda, mas somente as três funções principais da solução estão regularmente ativas. Não exclua as outras duas funções; elas são necessárias para gerenciar os recursos associados.

Para ver detalhes sobre os recursos da pilha, escolha a guia Saídas. Isso inclui o BadBotHoneypotEndpointvalor. Lembre-se desse valor porque você o usará no link Incorporar o Honeypot em seu aplicativo da web.

Etapa 2. Associe a ACL da web ao seu aplicativo da web

Atualize sua (s) CloudFront distribuição (ões) ou ALB (s) para ativar o AWS WAF e o registro usando os recursos que você gerou na Etapa 1. Inicie a pilha.

1. Faça login no console do AWS WAF.
2. Escolha a ACL da web que você deseja usar.
3. Na guia Associated AWS resources (Recursos associados da AWS) escolha Add AWS resources (Adicionar recursos da AWS).
4. Em Tipo de recurso, escolha a CloudFront distribuição ou o ALB.
5. Selecione um recurso na lista e escolha Adicionar para salvar suas alterações.

Etapa 3. Configurar o registro em log do acesso à web

Configure CloudFront seu ALB para enviar logs de acesso à web para o bucket apropriado do Amazon S3 para que esses dados estejam disponíveis para a função Lambda do Log Parser.

Armazene registros de acesso à web de uma CloudFront distribuição

1. Faça login no CloudFront console da Amazon.
2. Selecione a distribuição do seu aplicativo web e escolha Configurações de distribuição.
3. Na guia Geral, escolha Editar.
4. Para o AWS WAF Web ACL, escolha a solução de ACL da web criada (o parâmetro Stack name).
5. Para Logging, escolha On.
6. Em Bucket for Logs, escolha o bucket do S3 que você deseja usar para armazenar registros de acesso à web. Isso pode ser um bucket S3 novo ou existente que é usado na pilha principal e tem permissão CloudFront para gravar registros. A lista suspensa enumera os buckets associados à conta atual da AWS. Para obter mais informações, consulte Introdução a uma CloudFront distribuição básica no Amazon CloudFront Developer Guide.

7. Defina o prefixo do log como o prefixo usado para implantar a solução.
   Você pode encontrar o prefixo na pilha principal, na guia Parâmetros AppAccessLogBucketPrefixParam(padrãoAWSLogs/).
8. Escolha Yes, edit para salvar as alterações.

Para obter mais informações, consulte Configuração e uso de registros padrão (registros de acesso) no Amazon CloudFront Developer Guide.

Armazene registros de acesso à web a partir de um Application Load Balancer

1. Faça login no console do Amazon Elastic Compute Cloud (Amazon EC2).
2. No painel de navegação, selecione Load Balancers.
3. Selecione o ALB do seu aplicativo web.
4. Na guia Descrição, selecione Editar atributos.
5. Selecione Habilitar logs de acesso.
6. Para localização do S3, digite o nome do bucket do S3 que você deseja usar para armazenar registros de acesso à web. Isso pode ser um bucket S3 novo ou existente que é usado na pilha principal e tem permissão para que o Application Load Balancer grave registros.
7. Defina o prefixo do log como o prefixo usado para implantar a solução.
   Você pode encontrar o prefixo na pilha principal, na guia Parâmetros AppAccessLogBucketPrefixParam(padrãoAWSLogs/).
8. Escolha Salvar.

Para obter mais informações, consulte os registros de acesso do seu Application Load Balancer no Guia do usuário do Elastic Load Balancing.

Atualizar a solução

Se você implantou a solução anteriormente, siga este procedimento para atualizar a CloudFormation pilha da solução para obter a versão mais recente da estrutura da solução. Antes de atualizar a pilha, leia atentamente as considerações sobre a atualização.

1. Faça login no CloudFormation console da AWS.
2. Selecione Pilhas no menu de navegação à esquerda.
3. Selecione sua `aws-waf-security-automations` CloudFormation pilha existente.
4. Selecione Atualizar.
5. Selecione Substituir modelo atual.
6. Em Especificar modelo:
   a. Selecione Amazon S3 URL.
   b. Copie o link da `aws-waf-security-automations.template` AWS CloudFormation.
   c. Cole o link na caixa de URL do Amazon S3.
   d. Verifique se o URL do modelo correto aparece na caixa de texto URL do Amazon S3.
   e. Escolha Próximo.
   f. Escolha Avançar novamente.
7. Em Parâmetros, revise os parâmetros do modelo e modifique-os conforme necessário. Consulte detalhes sobre os parâmetros na Etapa 1. Inicie a pilha.
8. Escolha Avançar.
9. Na página Configurar opções de pilha, selecione Avançar.
10. Na página Revisar, verifique e confirme as configurações.
11. Selecione a caixa reconhecendo que o modelo pode criar recursos do IAM.
12. Escolha Exibir conjunto de alterações e verifique as alterações.
13. Selecione Criar pilha para implantar a pilha.

Você pode ver o status da pilha no CloudFormation console da AWS na coluna Status. Você deve receber o status UPDATE_COMPLETE em cerca de 15 minutos.

Considerações sobre a atualização

As seções a seguir fornecem restrições e considerações para atualizar essa solução.

Atualização do tipo de recurso

Você deve implantar uma nova pilha para atualizar o parâmetro Endpoint depois de criar a pilha. Não altere o parâmetro Endpoint ao atualizar a pilha.

WAFV2 atualização

A partir da versão 3.0, essa solução é compatível com a AWS WAFV2. Substituímos todas as chamadas de API do AWS WAF Classic por chamadas de API WAFV2 da AWS. Isso remove as dependências do Node.js e usa a maior parte do tempo de execução do up-to-date Python. Para continuar usando essa solução com os recursos e melhorias mais recentes, você deve implantar a versão 3.0 ou superior como uma nova pilha.

Personalizações na atualização da pilha

A out-of-box solução implanta um conjunto de regras do AWS WAF com configurações padrão em sua conta da AWS com a pilha. CloudFormation Não recomendamos aplicar personalizações às regras implantadas pela solução. As atualizações do Stack substituem essas alterações. Se você precisar de regras personalizadas, recomendamos criar regras separadas fora da solução.

Atualização do Bad Bot Protection

Na versão 4.1.0, o Access Handler Lambda com API Gateway foi descontinuado e substituído pela funcionalidade de log aprimorada do recurso. `Log parser - Bad bot` Em vez de usar solicitações diretas por meio do API Gateway, a solução agora reutiliza o fluxo de log para detectar bots mal-intencionados.

Implementação anterior:

1. Manipulador de acesso necessário Lambda e API Gateway.
2. Endpoint honeypot usado para tratamento direto de solicitações.
3. É necessário incorporar o endpoint honeypot em sites.

Nova implementação (4.1.0+): O analisador de log do Bad Bot Protection agora:

1. Inspeciona as solicitações para o endpoint do honeypot por meio de registros.
2. Processa solicitações quando o Bad Bot Protection é ativado.
3. Usa o filtro WAF BadBotRuleFilterpara identificar solicitações de bots incorretas.
4. Analisa os dados de registro para identificar endereços IP que excedem as cotas definidas.
5. Atualiza as condições do conjunto de IP do AWS WAF para bloquear endereços identificados.

Essa mudança simplifica a arquitetura, eliminando a funcionalidade duplicada e aproveitando os recursos existentes de processamento de registros.

Atualização do CDK

A partir da versão v4.1.0, essa solução é suportada pelo CDK. Se estiver migrando de uma versão inferior à v4.1.0. Use o novo modelo e atualize a solução no Cloudformation. Em seguida, você pode começar a atualizar a solução localmente por meio de seu terminal usando cdk deploy (consulte o README para obter mais informações). Se você tentar usar o cdk deploy diretamente, poderá ver este erro: Recuo insuficiente na coleta de fluxo

A outra forma de atualizar a solução será usar o modelo fornecido pela solução e acessar a seção Cloudformation do console da AWS, clicar em atualizar a solução e colar o novo modelo lá.

> **Note**
>
> Se você estiver atualizando da versão 3.0 ou 3.1 para a versão 3.2 ou mais recente desta solução e tiver inserido manualmente os endereços IP no conjunto de IP permitido ou negado, correrá o risco de perder esses endereços IP. Para evitar que isso aconteça, faça uma cópia dos endereços IP no conjunto de IP permitido ou negado antes de atualizar a solução. Depois de concluir a atualização, adicione os endereços IP de volta ao conjunto de IPs, conforme necessário. Consulte os comandos get-ip-sete update-ip-setCLI. Se você já estiver usando a versão 3.2 ou mais recente, ignore essa etapa.

Desinstalar a solução

Para desinstalar a solução, exclua as CloudFormation pilhas:

1. Faça login no CloudFormation console da AWS.
2. Selecione a pilha principal da solução. Todas as outras pilhas de soluções serão excluídas automaticamente.
3. Escolha Excluir.

> **Note**
>
> A desinstalação da solução exclui todos os recursos da AWS usados pela solução, exceto os buckets do Amazon S3. Se alguns conjuntos de IP falharem na exclusão devido ao problema de limitação de taxa excedida causado pelas cotas da API AWA WAF, exclua manualmente esses conjuntos de IP e, em seguida, exclua a pilha.

Use a solução

Esta seção fornece instruções detalhadas para usar a solução depois de implantá-la.

Modifique os conjuntos de IP permitidos e negados (opcional)

Depois de implantar a CloudFormation pilha dessa solução, você pode modificar manualmente os conjuntos de IP permitidos e negados para adicionar ou remover endereços IP conforme necessário.

1. Faça login no console do AWS WAF.
2. No painel de navegação esquerdo, escolha Conjuntos de IP.
3. Escolha IP definido para Lista Permitida e adicione endereços IP de fontes confiáveis.
4. Escolha IP definido para Lista negada e adicione os endereços IP que você deseja bloquear.

Incorpore o link do Honeypot em seu aplicativo da web (opcional)

Se você escolheu `yes` o parâmetro Ativar proteção contra bots incorretos na Etapa 1. Inicie a pilha, o CloudFormation modelo cria um ponto final de armadilha para um honeypot de produção de baixa interação. Essa armadilha tem como objetivo detectar e desviar solicitações de entrada de raspadores de conteúdo e bots mal-intencionados. Usuários válidos não tentarão acessar esse endpoint.

Esse componente aprimora a detecção de bots incorretos monitorando conexões diretas com um Application Load Balancer (ALB) ou CloudFront Amazon, além do mecanismo de honeypot. Se um bot contorna o honeypot e tenta interagir com o ALB ou CloudFront, o sistema analisa os padrões e registros de solicitações para identificar atividades maliciosas. Quando um bot mal-intencionado é detectado, seu endereço IP é extraído e adicionado a uma lista de bloqueios do AWS WAF para evitar mais acesso. A detecção de bots incorretos opera por meio de uma cadeia lógica estruturada, garantindo uma cobertura abrangente de ameaças:

- Analisador de log Lambda de proteção contra inundações HTTP — Coleta IPs bots inválidos das entradas de registro durante a análise de inundação.
- Scanner & Probe Protection Lambda Log Parser — Identifica IPs bots defeituosos nas entradas de registro relacionadas ao scanner.
- HTTP Flood Protection Athena Log Parser — Extrai bots mal-intencionados dos registros IPs do Athena, usando partições na execução da consulta.

- Scanner & Probe Protection Athena Log Parser — Recupera bots defeituosos dos registros IPs do Athena relacionados ao scanner, usando a mesma estratégia de particionamento.
- Detecção de fallback — Se a proteção contra inundação HTTP e a proteção de scanner e sonda estiverem desativadas, o sistema dependerá do analisador Log Lambda, que registra a atividade do bot com base nos filtros de rótulos WAF.

Use um dos procedimentos a seguir para incorporar o link do honeypot para solicitações de qualquer uma CloudFront das distribuições.

Crie uma CloudFront origem para o endpoint Honeypot

Use esse procedimento para aplicativos web que são implantados com uma CloudFront distribuição. Com CloudFront, você pode incluir um `robots.txt` arquivo para ajudar a identificar raspadores de conteúdo e bots que ignoram o padrão de exclusão de robôs. Conclua as etapas a seguir para incorporar o link oculto e, em seguida, proibi-lo explicitamente em seu arquivo. `robots.txt`

1. Faça login no CloudFormation console da AWS.
2. Escolha a pilha que você construiu na Etapa 1. Inicie a pilha
3. Escolha a guia Outputs.
4. Na BadBotHoneypotEndpointchave, copie o URL do endpoint.
   - O caminho do comportamento (`/ProdStage`)
5. Incorpore esse link de endpoint em seu conteúdo apontando para o honeypot. Oculte esse link de seus usuários humanos. Como exemplo, revise o seguinte exemplo de código:`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`.
6. Modifique o `robots.txt` arquivo na raiz do seu site para proibir explicitamente o link do honeypot, da seguinte forma:

```
User-agent: <*>
        Disallow: /<behavior_path>
```

> **Important**
>
> Nenhum registro de caminho CloudFront é necessário, pois as solicitações são: Bloqueadas pelo WAF BadBotRuleFilter. Solução coletada em registros automaticamente. Processado

pelo analisador de registros lambda. Essa abordagem simplificada usa os registros do WAF diretamente, em vez de exigir configuração adicional de endpoint, tornando o processo de detecção de bots incorretos mais eficiente por meio da análise de registros.

> **Note**
>
> É sua responsabilidade verificar quais valores de tag funcionam no ambiente do seu site. Não use `rel="nofollow"` se seu ambiente não observar. Para obter mais informações sobre a configuração de metatags de robôs, consulte o guia do desenvolvedor do Google. Modifique o `robots.txt` arquivo na raiz do seu site para proibir explicitamente o link do honeypot, da seguinte forma:

Incorpore o endpoint Honeypot como um link externo

> **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.

Use esse procedimento para aplicativos da Web.

1. Faça login no CloudFormation console da AWS.
2. Escolha a pilha que você construiu na Etapa 1. Inicie a pilha.
3. Escolha a guia Outputs.
4. Na BadBotHoneypotEndpointchave, copie o URL do endpoint.

```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> Esse procedimento é usado `rel=nofollow` para instruir os robôs a não acessarem o URL do honeypot. No entanto, como o link é incorporado externamente, você não pode

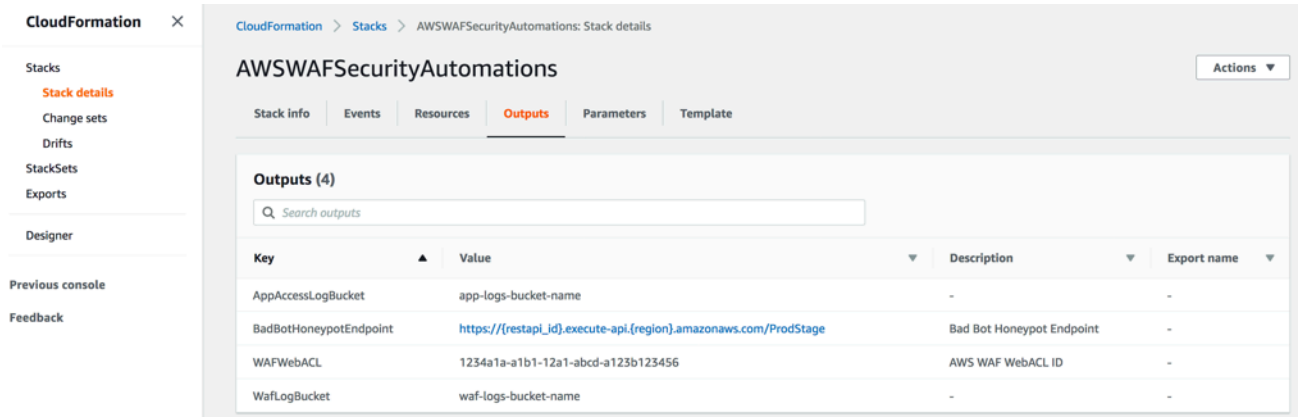
incluir um `robots.txt` arquivo para proibir explicitamente o link. É sua responsabilidade verificar quais tags funcionam no ambiente do seu site. Não use `rel="nofollow"` se seu ambiente não observar.

Use o arquivo JSON do analisador de log Lambda

Use o arquivo JSON do analisador de log Lambda para proteção contra inundação HTTP

Se você escolher o parâmetro `Yes - AWS Lambda log parser` de modelo Activate HTTP Flood Protection, essa solução cria um arquivo de configuração chamado `<stack_name>-waf_log_conf.json` e o carrega no bucket do Amazon S3 usado para armazenar os arquivos de log do AWS WAF. Para encontrar o nome do bucket, consulte a WafLogBucketvariável na CloudFormation saída. A figura a seguir mostra um exemplo.

Captura de tela mostrando uma tela chamada AWSWAFSecurity Automações e listando quatro saídas



Se você editar e sobrescrever o `<stack_name>-waf_log_conf.json` arquivo no Amazon S3, a função `Log Parser` Lambda considera os novos valores ao processar novos arquivos de log do AWS WAF. O exemplo a seguir é um arquivo de configuração de amostra:

Captura de tela de um arquivo de configuração de amostra

```
{
 "general": {
    "requestThreshold": 2000,
    "blockPeriod": 240,
    "ignoredSufixes": [".css", ".js", ".jpg", "png", ".gif"]
  },
 "uriList": {
    "/search": {
        "requestThreshold": 500,
        "blockPeriod": 600
    }
  }
}
```

Os parâmetros incluem o seguinte:

- Geral:
  - Limite de solicitação (obrigatório) - O máximo aceitável de solicitações por cinco minutos, por endereço IP. Essa solução usa o valor que você define ao provisionar ou atualizar a CloudFormation pilha.
  - Período de bloqueio (obrigatório) - O período (em minutos) para bloquear os endereços IP aplicáveis. Essa solução usa o valor que você define ao provisionar ou atualizar a CloudFormation pilha.
  - Sufixos ignorados - as solicitações que acessam esse tipo de recurso não contam para o limite da solicitação. Por padrão, essa lista está vazia.
- Lista de URI - use isso para definir um limite de solicitação personalizado e um período de bloqueio para informações específicas. URLs Por padrão, essa lista está vazia.

Quando os registros do WAF chegarem ao WafLogBucket, eles serão processados pela função do analisador de registros do Lambda usando as configurações em seu arquivo de configuração. A solução grava o resultado em um arquivo de saída nomeado `<stack_name>-waf_log_out.json` no mesmo bucket. Se o arquivo de saída contiver uma lista dos endereços IP identificados como atacantes, a solução os adicionará ao conjunto de IP do WAF para HTTP Flood e eles serão impedidos de acessar seu aplicativo. Se os arquivos de saída não tiverem endereços IP, verifique se o arquivo de configuração é válido ou se o limite de taxa foi excedido de acordo com o arquivo de configuração.

Use o arquivo JSON do analisador de log Lambda para proteção de scanner e sonda

Se você escolher o parâmetro `Yes - AWS Lambda log parser` de modelo Activate Scanner & Probe Protection, essa solução cria um arquivo de configuração chamado `<stack_name>-app_log_conf.json` e o carrega no bucket definido do Amazon S3 usado para CloudFront armazenar os arquivos de log do Application Load Balancer.

Se você editar e sobrescrever `<stack_name>-app_log_conf.json` no Amazon S3, a função `Log Parser` Lambda considera os novos valores ao processar novos arquivos de log do AWS WAF. O exemplo a seguir é um arquivo de configuração de amostra:

Captura de tela do arquivo de configuração

```
{
    "general": {
        "errorThreshold": 50,
        "blockPeriod": 240,
        "errorCodes": ["400", "401", "403", "404", "405"]
    },
    "uriList": {
        "/login": {
            "errorThreshold": 5,
            "blockPeriod": 600
        },
        "/api/feedback": {
            "errorThreshold": 10,
            "blockPeriod": 240
        }
    }
}
```

Os parâmetros incluem o seguinte:

- Geral:
  - Limite de erro (obrigatório) - O máximo aceitável de solicitações inválidas por minuto, por endereço IP. Essa solução usa o valor que você definiu ao provisionar ou atualizar a CloudFormation pilha.
  - Período de bloqueio (obrigatório) - O período (em minutos) para bloquear os endereços IP aplicáveis. Essa solução usa o valor que você definiu ao provisionar ou atualizar a CloudFormation pilha.
  - Códigos de erro - Retorne o código de status considerado erro. Por padrão, a lista considera os seguintes códigos de status HTTP como erros: `400 (Bad Request)` `401 (Unauthorized)`403 (Forbidden),404 (Not Found),, 405 (Method Not Allowed) e.

- Lista de URI - Use isso para definir um limite de solicitação personalizado e um período de bloqueio para detalhes específicos URLs. Por padrão, essa lista está vazia.

Quando os registros de acesso ao aplicativo chegam ao AppAccessLogBucket, a função `Log Parser` Lambda os processa usando as configurações em seu arquivo de configuração. A solução grava o resultado em um arquivo de saída chamado `<stack_name>` -app_log_out.json` no mesmo bucket. Se o arquivo de saída contiver uma lista dos endereços IP identificados como atacantes, a solução os adicionará ao conjunto de IP do WAF para Scanner & Probe e os impedirá de acessar seu aplicativo. Se os arquivos de saída não tiverem endereços IP, verifique se o arquivo de configuração é válido ou se o limite de taxa foi excedido de acordo com o arquivo de configuração.

Use o país e o URI no analisador de log Athena de inundação HTTP

Você pode agrupar por IPs junto com o país e o URI na consulta do Athena para detectar e bloquear ataques de inundação de HTTP que tenham padrões de URI imprevisíveis. Para fazer isso, selecione uma das opções (`Country`,`URI`,`Country and URI`) para o parâmetro Agrupar por solicitações no HTTP Flood Athena Query ao iniciar a pilha.

Você também pode inserir um limite de solicitação por país usando o parâmetro Limite de solicitação por país. Por exemplo, .`{"TR": 50,"ER":150}` A solução usa esses limites nas solicitações originadas desses países especificados. A solução usa o limite padrão nas solicitações de outros países.

> **Note**
>
> Se você definir um limite por país, a solução incluirá automaticamente o país na cláusula de agrupamento por consulta do Athena. Para obter mais informações, consulte a tabela de parâmetros na Etapa 1. Inicie a pilha.

Por padrão, a solução conta o limite da solicitação em um período de cinco minutos. Isso é configurável com o parâmetro Athena Query Run Time Schedule (Minute).

> **Note**
>
> A consulta do Athena calcula o limite por minuto dividindo o limite da solicitação pelo período. Por exemplo:
> Limite de solicitação (limite padrão ou limite por país): 100
> Cronograma de execução do Athena Query: 5
> Limite de solicitação por minuto: 20 = 100/ 5

Veja as consultas do Amazon Athena

Se você `Yes - Amazon Athena log parser` selecionou os parâmetros do modelo Activate HTTP Flood Protection ou Activate Scanner & Probe Protection, essa solução cria e executa consultas do Athena para os logs do ALB () CloudFront ou do `ScannersProbesLogParser` AWS WAF (`HTTPFloodLogParser`), analisa a saída e atualiza o AWS WAF adequadamente.

Para melhorar o desempenho e manter os custos baixos, a solução particiona os registros com base nos registros de data e hora nos nomes dos arquivos. A solução gera dinamicamente consultas do Athena para usar chaves de partição (ano, mês, dia e hora). Por padrão, as consultas são executadas a cada cinco minutos. Você pode configurar seus cronogramas de execução alterando o valor do parâmetro do modelo Cronograma de Tempo de Execução (Minuto) do Athena Query. Cada execução de consulta verifica as últimas quatro a cinco horas de dados por padrão. Você pode configurar a quantidade de dados que uma consulta verifica alterando o valor do parâmetro do modelo WAF Block Period. A solução também coloca as consultas em grupos de trabalho separados para gerenciar o acesso e os custos das consultas.

> **Note**
>
> Verifique se o Athena está configurado para acessar o catálogo de dados do AWS Glue. Essa solução cria o catálogo de dados de registros de acesso no AWS Glue e configura uma consulta do Athena para processar os dados. Se o Athena não estiver configurado corretamente, a consulta não será executada. Para obter mais informações, consulte Atualizando para o AWSAWS Glue Data Catalog step-by-step mais recente.

Use o procedimento a seguir para visualizar essas consultas:

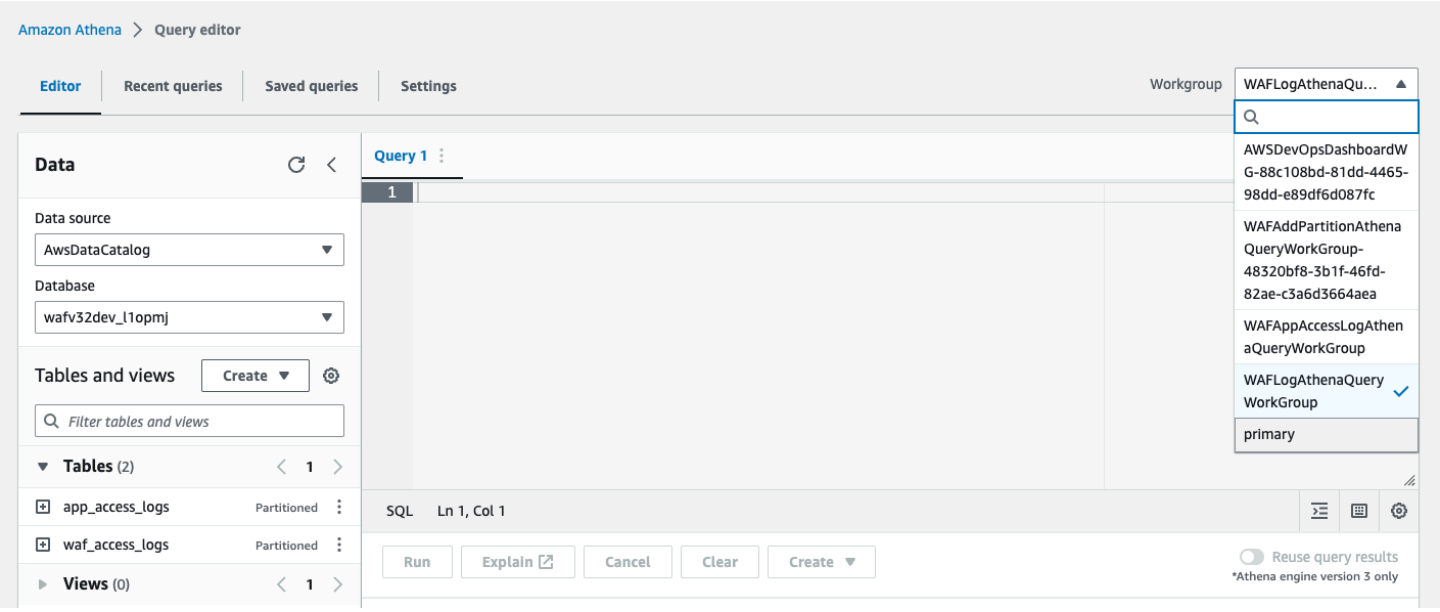
Exibir consultas de log do WAF

1. Faça login no console do Amazon Athena.
2. Escolha Iniciar editor de consultas.
3. Selecione o banco de dados para essa solução.
4. Selecione na WAFLogAthenaQueryWorkGrouplista suspensa.

> **Note**
>
> Esse grupo de trabalho existe somente se você selecionou `Yes - Amazon Athena log parser` o parâmetro do modelo Ativar Proteção contra Inundação HTTP.

5. Escolha Alternar para alternar o grupo de trabalho.

Captura de tela do editor de consultas Athena que não mostra nenhuma consulta



1. Selecione a guia Histórico.
2. Selecione e abra `SELECT` consultas na lista.

Exibir consultas de registros de acesso ao aplicativo

1. Faça login no console do Amazon Athena.

2. Selecione a guia Grupo de trabalho.
3. Selecione WAFAppAccessLogAthenaQueryWorkGroup na lista.

> **Note**
>
> Esse grupo de trabalho existe somente se você selecionou `Yes - Amazon Athena log parser` o parâmetro do modelo Activate Scanner & Probe Protection.

4. Escolha Trocar grupo de trabalho.
5. Selecione a guia Consultas recentes.
6. Selecione e abra `SELECT` consultas na lista.

Visualize a adição de consultas de partição do Athena

1. Faça login no console do Amazon Athena.
2. Selecione a guia Grupo de trabalho.
3. Selecione WAFAddPartitionAthenaQueryWorkGroup na lista.

> **Note**
>
> Esse grupo de trabalho existe somente se você selecionou `Yes - Amazon Athena log parser` o parâmetro do modelo Ativar Proteção contra Inundação HTTP and/or Ativar Scanner e Proteção de Sonda.

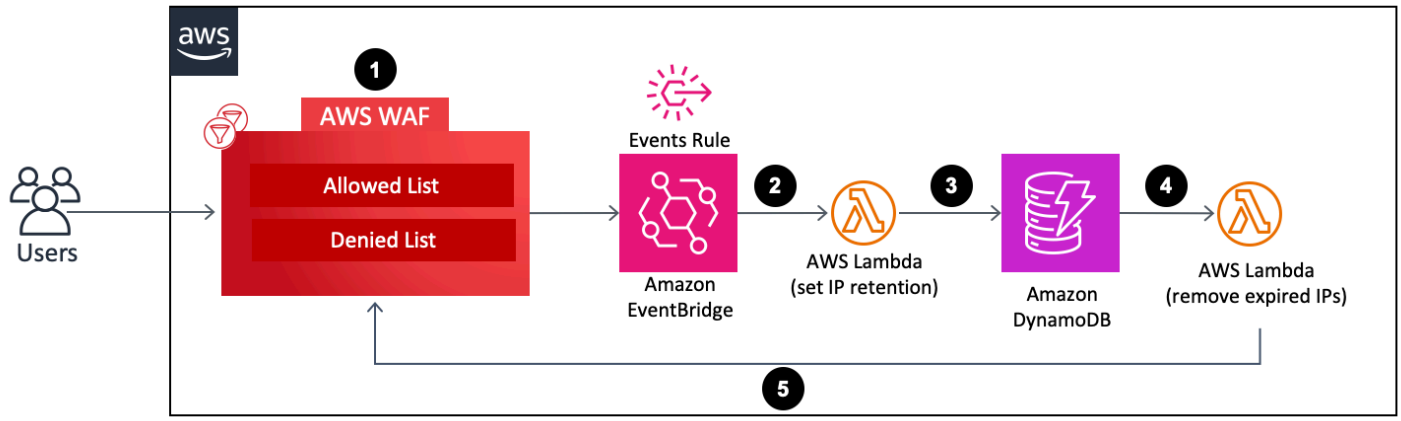
4. Selecione Trocar grupo de trabalho.
5. Selecione a guia Histórico.
6. Selecione e abra `ALTER TABLE` consultas na lista. Essas consultas são executadas a cada hora para adicionar uma nova partição horária à tabela do Athena.

Configurar a retenção de IP nos conjuntos de IP permitidos e negados do AWS WAF

Você pode configurar a retenção de IP nos conjuntos de IP permitidos e negados do AWS WAF criados pela solução. As seções a seguir explicam como ele funciona e fornecem as etapas para configurá-lo.

Como funciona

Diagrama de arquitetura que descreve as listas permitidas e negadas do AWS WAF e outros recursos da AWS



1. Quando um usuário atualiza (adiciona ou exclui um endereço IP) o conjunto de IP do WAF permitido ou negado, essa ação invoca uma chamada da `UpdateIPSet` API do AWS WAF e cria um evento.
2. Uma regra de EventBridge eventos da Amazon detecta os eventos com base em um padrão de eventos predefinido e invoca uma função Lambda para definir o período de retenção de todos os endereços IP que existem no conjunto IP após a atualização.
3. A função Lambda processa os eventos, extrai dados relevantes para a retenção de IP (como nome do conjunto de IP, ID, escopo, endereços IP) e os insere em uma tabela do DynamoDB. Ele também insere um `ExpirationTime` atributo para cada item do DynamoDB. A solução calcula o tempo de expiração adicionando um período de retenção definido pelo usuário ao horário do evento. A tabela tem o DynamoDB Streams e o Time to Live (TTL) ativados. O atributo TTL é`ExpirationTime`.
4. Quando um item atinge o prazo de validade, o TTL é invocado e o DynamoDB exclui o item da tabela após o prazo de expiração. Após a exclusão do item, o item excluído é adicionado ao stream do DynamoDB, que invoca uma função Lambda para processamento posterior.
5. A função Lambda obtém as informações sobre o item excluído do stream do DynamoDB e faz uma chamada à API do AWS WAF para remover os endereços IP expirados incluídos no item do conjunto de IPs de destino do AWS WAF.

Ativar a retenção de IP

Siga estas etapas para ativar a retenção de IP:

1. Na pilha do Cloudformation que você implanta ou atualiza, insira o Período de retenção de IP (minutos) para o Conjunto de IP permitido e o Período de retenção de IP (minutos) para o Conjunto de IP negado. O período mínimo de retenção é de 15 minutos. A solução trata qualquer número entre `0` e `15` como`15`. Para obter mais informações sobre a configuração de implantação, consulte a Etapa 1. Inicie a pilha.
2. Insira um endereço de e-mail se quiser receber uma notificação por e-mail quando endereços IP expirados forem removidos do conjunto de IPs do AWS WAF. Se você optar por receber uma notificação por e-mail, deverá confirmar a assinatura usando o link no e-mail recebido após a implantação bem-sucedida da solução. Para obter mais informações sobre a configuração de implantação, consulte a Etapa 1. Inicie a pilha.
3. Atualize o conjunto de IP do AWS WAF adicionando ou excluindo endereços IP. Isso inicia o processo de retenção de IP e cria um item do DynamoDB, incluindo uma lista de expiração de IP. Essa lista de expiração consiste em endereços IP que existem no conjunto de IPs do AWS WAF após sua atualização.
4. Quando o item do DynamoDB atinge seu prazo de validade e é excluído da tabela, a solução exclui os endereços IP incluídos na lista de expiração de IP do item do conjunto de IP do WAF.

> **Note**
>
> Dependendo do momento em que o DynamoDB exclui um item expirado pelo TTL, a operação real de exclusão de um endereço IP expirado do conjunto de IP do AWS WAF pode variar. A exclusão de TTL do DynamoDB depende principalmente do tamanho e do nível de atividade de uma tabela. Espere um atraso na operação de exclusão do AWS WAF devido ao possível atraso na operação de exclusão do DynamoDB. Em geral, a solução exclui endereços IP expirados do conjunto de IP do AWS WAF logo após a exclusão do TTL do DynamoDB. Para obter mais informações, consulte DynamoDB Time to Live (TTL) no Amazon DynamoDB Developer Guide.

Crie um painel de monitoramento

A AWS recomenda que você configure um sistema de monitoramento de linha de base personalizado para cada endpoint crítico. Para obter informações sobre como criar e usar visualizações métricas personalizadas, consulte CloudWatch Painéis - Criar e usar visualizações de métricas personalizadas e Usar CloudWatch painéis da Amazon.

A captura de tela do painel a seguir mostra um exemplo de um sistema de monitoramento de linha de base personalizado.

Captura de tela do painel CloudFront

O painel exibe as seguintes métricas:

- Solicitações permitidas versus bloqueadas - Mostra se você recebe um aumento no acesso permitido (o dobro do pico normal de acesso) ou no acesso bloqueado (qualquer período que identifique mais de 1.000 solicitações bloqueadas). CloudWatch envia um alerta para um canal do Slack. Você pode usar essa métrica para rastrear ataques DDo S conhecidos (quando as solicitações bloqueadas aumentam) ou uma nova versão de um ataque (quando as solicitações têm permissão para acessar o sistema).

> **Note**
>
> Observação: a solução fornece essa métrica.

- BytesDownloaded vs Uploaded - Ajuda a identificar quando um ataque DDo S tem como alvo um serviço que normalmente não recebe uma grande quantidade de acesso para esgotar os recursos (por exemplo, o envio de informações por um componente de mecanismo MBs de pesquisa para um conjunto de parâmetros de solicitação específico).
- Espalhamento e comprimento da fila do ELB — Ajuda a verificar se um ataque DDo S está causando danos à infraestrutura e se o atacante está contornando a camada CloudFront do AWS WAF e atacando diretamente recursos desprotegidos.
- Contagem de solicitações do ELB - Ajuda a identificar danos na infraestrutura. Essa métrica mostra se o invasor está ignorando a camada de proteção ou se você deve revisar uma regra de CloudFront cache para aumentar a taxa de acertos do cache.
- ELB Healthy Host - Você pode usar isso como outra métrica de verificação de integridade do sistema.
- Utilização da CPU do ASG — ajuda a identificar se o invasor está ignorando o AWS CloudFront WAF e o Elastic Load Balancing. Você também pode usar essa métrica para identificar os danos de um ataque.

Lidar com falsos positivos XSS

Essa solução configura uma regra do AWS WAF que inspeciona elementos comumente explorados das solicitações recebidas para identificar e bloquear ataques XSS. Esse padrão de detecção é menos eficaz se sua carga de trabalho permitir que usuários legítimos componham e enviem HTML, por exemplo, usando um editor de rich text em um sistema de gerenciamento de conteúdo. Nesse cenário, considere criar uma regra de exceção que ignore a regra XSS padrão para padrões de URL específicos que aceitam entrada de rich text e implemente mecanismos alternativos para proteger os excluídos. URLs

Além disso, alguns formatos de imagem ou dados personalizados podem causar falsos positivos porque contêm padrões que indicam um possível ataque de XSS em conteúdo HTML. Por exemplo, um arquivo SVG pode conter uma `<script>` tag. Se você espera esse tipo de conteúdo de usuários legítimos, adapte suas regras de XSS de forma restrita para permitir solicitações de HTML que incluam esses outros formatos de dados.

Conclua as etapas a seguir para atualizar a regra XSS para excluir URLs que aceite HTML como entrada. Consulte o Guia do desenvolvedor do Amazon WAF para obter instruções detalhadas.

1. Faça login no console do AWS WAF.
2. Crie uma correspondência de string ou condição de regex.
3. Defina as configurações do filtro para inspecionar os valores de URI e de lista que você deseja aceitar em relação à regra XSS.
4. Edite a regra XSS dessa solução e adicione a nova condição que você criou.

   Por exemplo, para excluir tudo URLs na lista, escolha o seguinte para Quando uma solicitação:

   - não
   - corresponder a pelo menos um dos arquivadores na condição de correspondência de string
   - Lista de permissões de XSS

Solução de problemas

Se precisar de ajuda com essa solução, entre em contato com o Support para abrir um caso de suporte para essa solução.

Entrar em contato com o Support

Se você tem o AWS Developer Support, o AWS Business Support ou o AWS Enterprise Support, você pode usar o Support Center para obter assistência especializada com essa solução. As seções a seguir dão instruções.

Criar caso

1. Abra o Support Center.
2. Escolha Criar caso.

Como podemos ajudar?

1. Escolha Técnico.
2. Em Serviço, selecione WAF ou AWS WAF.
3. Em Categoria, selecione Automações de segurança do WAF ou Automações de segurança do AWS WAF.
4. Para Severidade, a opção que melhor corresponde ao seu caso de uso.
5. Quando você insere o Serviço, a Categoria e a Gravidade, a interface preenche links para perguntas comuns de solução de problemas. Se você não conseguir resolver sua pergunta com esses links, escolha Próxima etapa: Informações adicionais.

Mais informações

1. Em Assunto, insira um texto resumindo sua pergunta ou problema.
2. Em Descrição, descreva o problema em detalhes.
3. Escolha Anexar arquivos.
4. Anexe as informações de que o Support precisa para processar a solicitação.

Ajude-nos a resolver seu caso com mais rapidez

1. Insira as informações solicitadas.
2. Escolha Próxima etapa: solucione ou entre em contato conosco.

Resolva agora ou entre em contato conosco

1. Analise as soluções Solve now.
2. Se você não conseguir resolver seu problema com essas soluções, escolha Fale conosco, insira as informações solicitadas e escolha Enviar.

Guia do desenvolvedor

Esta seção fornece o código-fonte da solução.

Código-fonte

Visite nosso GitHub repositório para baixar os modelos e scripts dessa solução e compartilhar suas personalizações com outras pessoas.

Os modelos dessa solução são gerados usando o AWS CDK. Consulte o arquivo README.md para obter informações adicionais.

Referência

Esta seção inclui informações sobre um recurso opcional para coletar métricas exclusivas para essa solução, indicadores para recursos relacionados e uma lista dos criadores que contribuíram para essa solução.

Coleta de dados anônima

Essa solução inclui a opção de enviar métricas operacionais para a AWS. Usamos esses dados para entender melhor como os clientes usam essa solução e os serviços e produtos relacionados. Quando ativada, a solução coleta as seguintes informações e as envia para a AWS durante a implantação inicial do CloudFormation modelo:

- ID da solução — O identificador da solução da AWS
- ID exclusivo (UUID) - identificador exclusivo gerado aleatoriamente para cada implantação dessa solução
- Timestamp - Timestamp da coleta de dados
- Configuração da solução - Recursos ativados e parâmetros definidos durante o lançamento inicial
- Ciclo de vida - Por quanto tempo o cliente usou essa solução (com base na exclusão da pilha)
- Dados do analisador de log:
  - O número de endereços IP no conjunto de IP do Scanner & Probe, no conjunto de IP do Bad Bot e no IP HTTP Flood definido para bloquear
  - O número de solicitações processadas e bloqueadas
- IP lista dados do analisador:
  - O número de endereços IP no conjunto de IPs das Listas de Reputação
  - O número de solicitações processadas e bloqueadas
- Dados de retenção de IP - O número de endereços IP expirados que estão sendo removidos do conjunto de IPs permitidos ou negados

A AWS é proprietária dos dados coletados por meio dessa pesquisa. A coleta de dados está sujeita à Política de Privacidade da AWS. Para optar por não usar esse recurso, conclua as etapas a seguir antes de lançar o CloudFormation modelo da AWS.

1. Faça o download `aws-waf-security-automations.template` da AWS CloudFormation em seu disco rígido local.
2. Abra o CloudFormation modelo com um editor de texto.
3. Modifique a seção CloudFormation de mapeamento de modelos a partir de:

```
Solution:
  Data:
   SendAnonymizedUsageData: "Yes"
```

   para:

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. Faça login no CloudFormation console da AWS.
5. Selecione Criar pilha.
6. Na página Criar pilha, seção Especificar modelo, selecione Carregar um arquivo de modelo.
7. Em Carregar um arquivo de modelo, escolha Escolher arquivo e selecione o modelo editado em sua unidade local.
8. Escolha Avançar e siga as etapas na Etapa 1. Inicie a pilha.

Recursos relacionados

Whitepapers associados da AWS

- Melhores práticas da AWS para resiliência DDo de S

Publicações associadas ao blog de segurança da AWS

- Como evitar hotlinking usando AWS WAF, CloudFront Amazon e Referer Checking

Listas de reputação de IP de terceiros

- Site da lista DROP da Spamhaus

- Lista de IPs de ameaças emergentes da Proofpoint
- Lista de modos de saída do Tor

Colaboradores

- Heitor Vital
- Lee Atkinson
- Ben Potter
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- Shu Jackson
- William Quan
- Mykhailo Markhain

Revisões

Visite o CHANGELOG.md em nosso GitHub repositório para acompanhar melhorias e correções específicas da versão.

Avisos

Este guia de implementação é fornecido apenas para fins informativos. Ela representa as ofertas e práticas atuais de produtos da AWS na data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações contidas neste documento e de qualquer uso dos produtos ou serviços da AWS, cada um fornecido “no estado em que se encontra”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria nenhuma garantia, declaração, compromisso contratual, condição ou garantia da AWS, de suas afiliadas, fornecedores ou licenciadores. As responsabilidades e as obrigações da AWS para com os clientes são controladas por contratos da AWS, e este documento não faz parte nem modifica nenhum contrato entre a AWS e seus clientes.

A solução Security Automations for AWS WAF é licenciada sob os termos da Licença Apache Versão 2.0.

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.