Guia de implementação

Automações de segurança para AWS WAF

Automações de segurança para AWS WAF: Guia de implementação

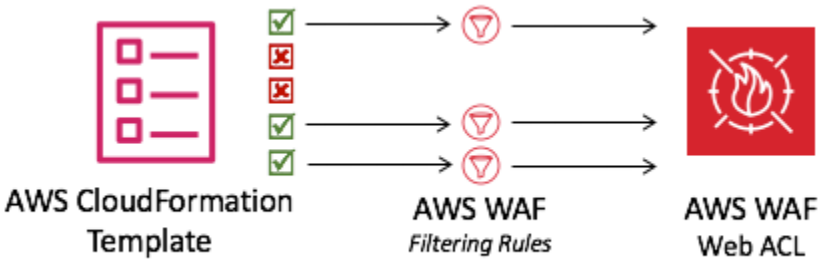
Table of Contents

Implemente automaticamente uma única lista de controle de acesso à web que filtra ataques baseados na web com as automações de segurança ativadas AWS WAF

Data de publicação: setembro de 2016 (última atualização: dezembro de 2024)

A AWS WAF solução Security Automations for implanta um conjunto de regras pré-configuradas para ajudar você a proteger seus aplicativos contra explorações comuns da web. O serviço principal dessa solução, 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 AWS WAF para definir regras de segurança da web personalizáveis. Essas regras controlam qual tráfego permitir ou bloquear para aplicativos web e interfaces de programação de aplicativos (APIs) implantados em AWS recursos como Amazon CloudFront, Application Load Balancer ALB () e Amazon API Gateway. Para obter mais tipos de recursos compatíveis, consulte AWS WAFo AWS WAF, AWS Firewall Manager, e o Guia AWS Shield Advanced do desenvolvedor.

Configurar AWS WAF regras 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 AWS WAF solução Security Automations for implanta automaticamente uma única lista de controle de acesso à web (ACL) com um conjunto de AWS WAF regras projetadas para filtrar ataques comuns baseados na web. Durante a configuração inicial do AWS CloudFormationmodelo dessa solução, você pode especificar quais recursos de proteção incluir. Depois de implantar essa solução, AWS WAF inspeciona as solicitações da web para suas CloudFront distribuições ou ALB distribuições existentes e as bloqueia quando aplicável.



Configuração da AWS WAF web ACL

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. Ele inclui links para CloudFormation modelos que iniciam, configuram e executam os serviços de AWS segurança, computação, armazenamento e outros necessários para implantar essa solução AWS, usando as AWS melhores práticas de segurança e disponibilidade.

As informações neste guia pressupõem conhecimento prático de AWS serviços 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 do AWS WAF serviço API (AWS WAF V2).

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 AWS WAF regras. Você pode personalizar o código-fonte, adicionar novas regras personalizadas e aproveitar mais regras AWS WAF gerenciadas com base em 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 processad os.	Custos
Entenda as considerações de segurança dessa solução.	Segurança

Se você deseja...	Leia…
Saiba quais Regiões da AWS são compatíveis com essa solução.	Suportado Regiões da AWS
Visualize ou baixe o CloudFormation modelo incluído nesta solução para implantar automatic amente os recursos de infraestrutura (a “pilha”) dessa solução.	AWS CloudFormation modelo
Use AWS Support para ajudá-lo a implantar, usar ou solucionar problemas da solução.	AWS Support
Acesse o código-fonte e, opcionalmente, use o AWS Cloud Development Kit (AWS CDK) para implantar a solução	GitHubrepositório

Recursos e benefícios

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

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

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

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

A regra personalizada HTTPFlood 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:

- AWS WAF regra baseada em taxas
- 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 AWS WAF tarifas. 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 HTTP inundação que têm padrões URI imprevisíveis. Para obter mais informações, consulte Use country and URI in HTTP Flood Athena log parser.

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 Don't Route Or Peer (DROP) e Extended DROP (EDROP) do Spamhaus, a lista de IPs do Proofpoint Emerging Threats 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 pela AWS WAF. Para obter mais informações, consulte Criar painel de monitoramento.

Integre-se ao Service Catalog AppRegistry e ao AWS Systems Manager Application Manager

Essa solução inclui um AppRegistry recurso do Service Catalog para registrar o CloudFormation modelo da solução e seus recursos subjacentes como um aplicativo no AWS Service Catalog AppRegistry e no AWS Systems Manager Application Manager. Com essa integração, você pode gerenciar centralmente os recursos da solução.

Casos de uso

Data de publicação: setembro de 2016 (última atualização: maio de 2023)

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 de regras AWS WAF

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

Personalize a proteção HTTP contra inundações da camada 7

Essa solução oferece três opções para ativar a proteção contra HTTP inundações. Você pode selecionar a opção que atenda às suas necessidades para obter proteção contra DDoS ataques. Para obter mais informações, consulte Forneça proteção contra inundação de camada 7 com uma regra personalizada de HTTP inundação predefinida em Características 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 outros AWS WAF serviços para criar automações de segurança no Nuvem 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.

Logs do ALB

Essa solução usa registros para o ALB recurso. 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 abertos de tabela e arquivo. Essa solução executa uma consulta agendada do Athena para inspecionar AWS WAF ou ALB registra se o usuário **`yes - Amazon Athena log parser`** escolher ativar a regra de proteção contra HTTP inundações ou a regra de proteção de scanner e sonda. CloudFront

AWS WAF regra

Uma AWS WAF regra define:

- Como inspecionar HTTP (S) solicitações da web
- 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 da webACL.

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 AWS recursos.

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 Lamba inicia uma inspeção ou ALB registra se o usuário `yes – AWS Lambda log parser` escolher ativar a regra de proteção contra HTTP inundações ou a regra de proteção de scanner e sonda. AWS WAF CloudFront

Grupos de regras gerenciados

Grupos de regras gerenciadas são coleções de ready-to-use regras predefinidas que AWS AWS Marketplace os vendedores escrevem e mantêm para você. AWS WAF O preço se aplica ao uso de qualquer grupo de regras gerenciadas.

tipo de recurso/endpoint

Você pode associar AWS recursos ACLs à web para protegê-los. Esses recursos são CloudFront, API Gateway,, ALB AWS AppSync, Amazon Cognito, AWS App Runner e recursos de acesso AWS verificado. Atualmente, esta solução é suportada pela Amazon CloudFront ALB e.

Logs do WAF

Essa solução usa registros gerados AWS WAF por para os recursos associados à webACL. A regra de proteção contra HTTP inundações dessa solução inspeciona esses registros.

WCU

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

web ACL

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

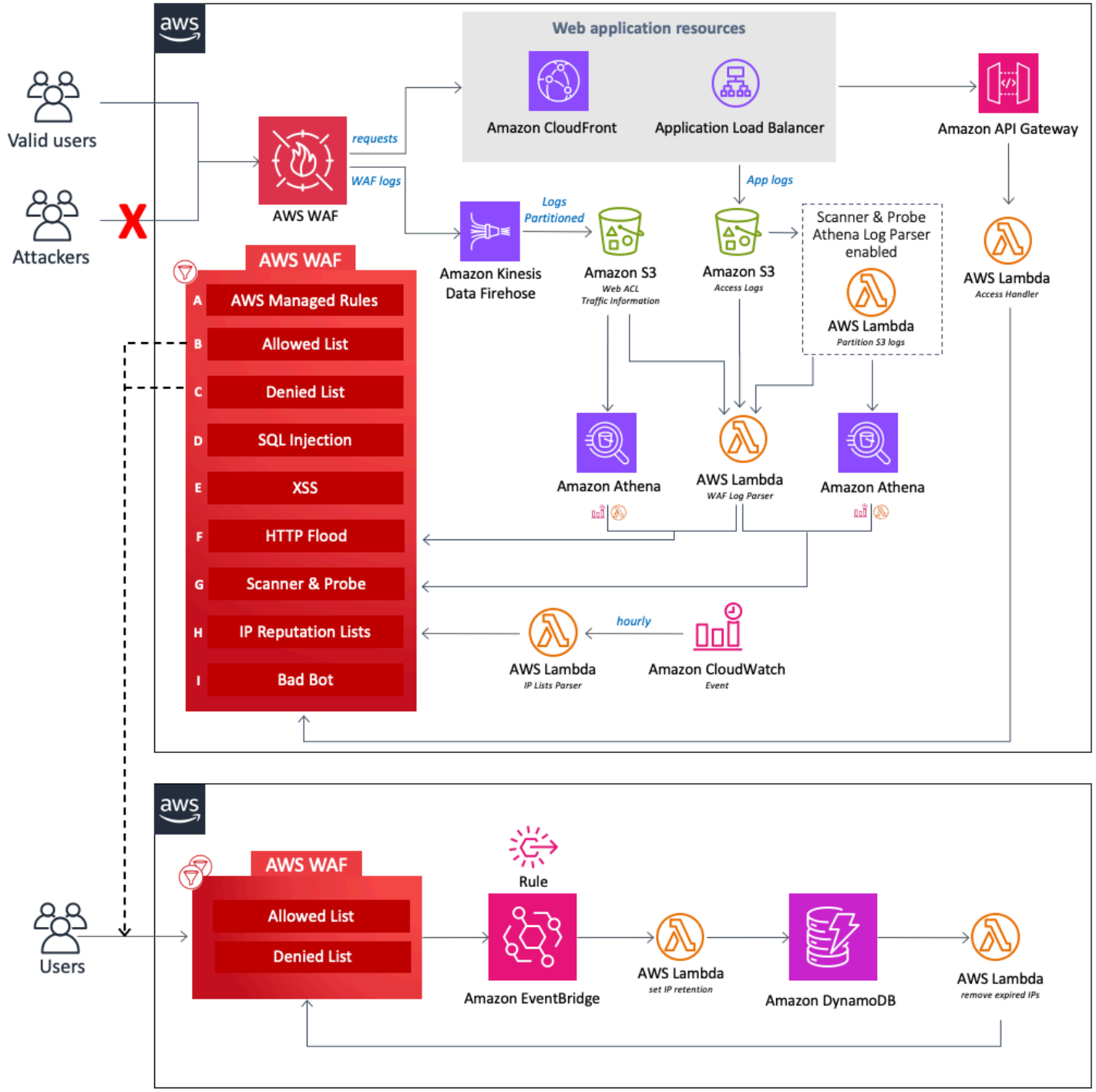
> **Note**
>
> Para obter uma referência geral dos AWS termos, consulte o AWS Glossário.

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 seu. Conta da AWS



Automações de segurança para AWS WAF arquitetura em AWS

No centro do design está uma AWS WAFwebACL, que atua como ponto central de inspeção e decisão para todas as solicitações recebidas em um aplicativo da 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 webACL.

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

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

- AWS Regras gerenciadas (A) — Esse componente contém grupos de regras de reputação de AWS Managed Rules IP, grupos de regras de linha de base e grupos de regras específicos para casos de uso. Esses grupos de regras protegem contra a exploração de vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados, incluindo aqueles descritos em OWASPpublicações, sem precisar criar suas próprias regras.
- Listas manuais de IP (B e C) — Esses componentes criam duas AWS WAF regras. 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 AWS WAF IP permitidos e negados.
- SQLInjeção (D) e XSS (E) — Esses componentes configuram duas AWS WAF regras projetadas para proteger contra padrões comuns de SQL injeção ou cross-site scripting (XSS) na URI string de consulta ou no corpo de uma solicitação.
- HTTPFlood (F) — Esse componente protege contra ataques que consistem em um grande número de solicitações de um endereço IP específico, como um DDoS ataque na camada 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 AWS WAF baseada em taxas ou processando AWS WAF registros usando uma função Lambda ou uma consulta do Athena. Para obter mais informações sobre as compensações relacionadas às opções de mitigação de HTTP inundações, 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 Don't Route Or Peer (DROP) e Extended DROP (EDROP) do Spamhaus, a lista de IPs do Proofpoint Emerging Threats e a lista de nós de saída do Tor.
- Bad Bot (I) — Esse componente configura automaticamente um honeypot, que é um mecanismo de segurança destinado a atrair e desviar uma tentativa de ataque. O honeypot dessa solução é um terminal de armadilha que você pode inserir em seu site para detectar solicitações de entrada de raspadores de conteúdo e bots maliciosos. Se uma fonte acessa o honeypot, a função `Access Handler` Lambda intercepta e inspeciona a solicitação para extrair seu endereço IP e, em seguida, a adiciona a uma lista de bloqueio. AWS 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 de design do AWS Well-Architected

Essa solução usa as melhores práticas do AWS Well-Architected Framework, que ajuda os clientes a projetar e operar workloads 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 usa métricas CloudWatch para fornecer observabilidade na infraestrutura, nas funções Lambda, no Amazon Data Firehose, no Gateway, nos buckets do API Amazon S3 e no restante dos componentes da solução.
- Desenvolvemos, testamos e publicamos a solução por meio de um AWS pipeline de integração contínua e entrega contínua (CI/CD). 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 funções 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 AWS sem servidor sempre que possível (por exemplo, Lambda, Firehose, GatewayAPI, 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 AWS serviços que compõem essa solução e os detalhes da arquitetura sobre como esses componentes funcionam juntos.

AWS serviços nesta solução

AWS serviço	Descrição	
AWS WAF	Principal. Implanta uma AWS WAF webACL, AWS Managed Rules grupos de regras, regras personalizadas e conjuntos de IP. Faz AWS WAF API chamadas para bloquear ataques comuns e proteger aplicativos da web.	
Amazon Data Firehose	Principal. Entrega AWS WAF registros para buckets do Amazon S3.	
Amazon S3	Principal. Lojas AWS WAF CloudFront e ALB registros.	
AWS Lambda	Núcleo. 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	

AWS serviço	Descrição	
	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 API Gateway	Suporte. Cria um endpoint de honeypot de bot inválido.	
Amazon SNS	Suporte. Envia notificaç ões por e-mail do Amazon Simple Notification Service (AmazonSNS) para apoiar a retenção de IP nas listas permitidas e negadas.	
AWS Systems Manager (Gerenciador de sistemas)	Suporte. Fornece monitoram ento 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 HTTP contra inundação, scanner e sonda. As seções a seguir explicam cada uma dessas opções com mais detalhes.

AWS WAF regra baseada em taxas

Regras baseadas em tarifas estão disponíveis para proteção HTTP contra inundações. 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, 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 HTTPFlood 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 a execução, o processamento da saída do resultado e a atualização do Athena. 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 regras AWS WAF baseadas em taxas e estiver familiarizado com SQL a implementação de personalizações. Para obter mais informações sobre como alterar a consulta padrão, consulte Exibir consultas do Amazon Athena.

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

AWS Lambda analisador de log

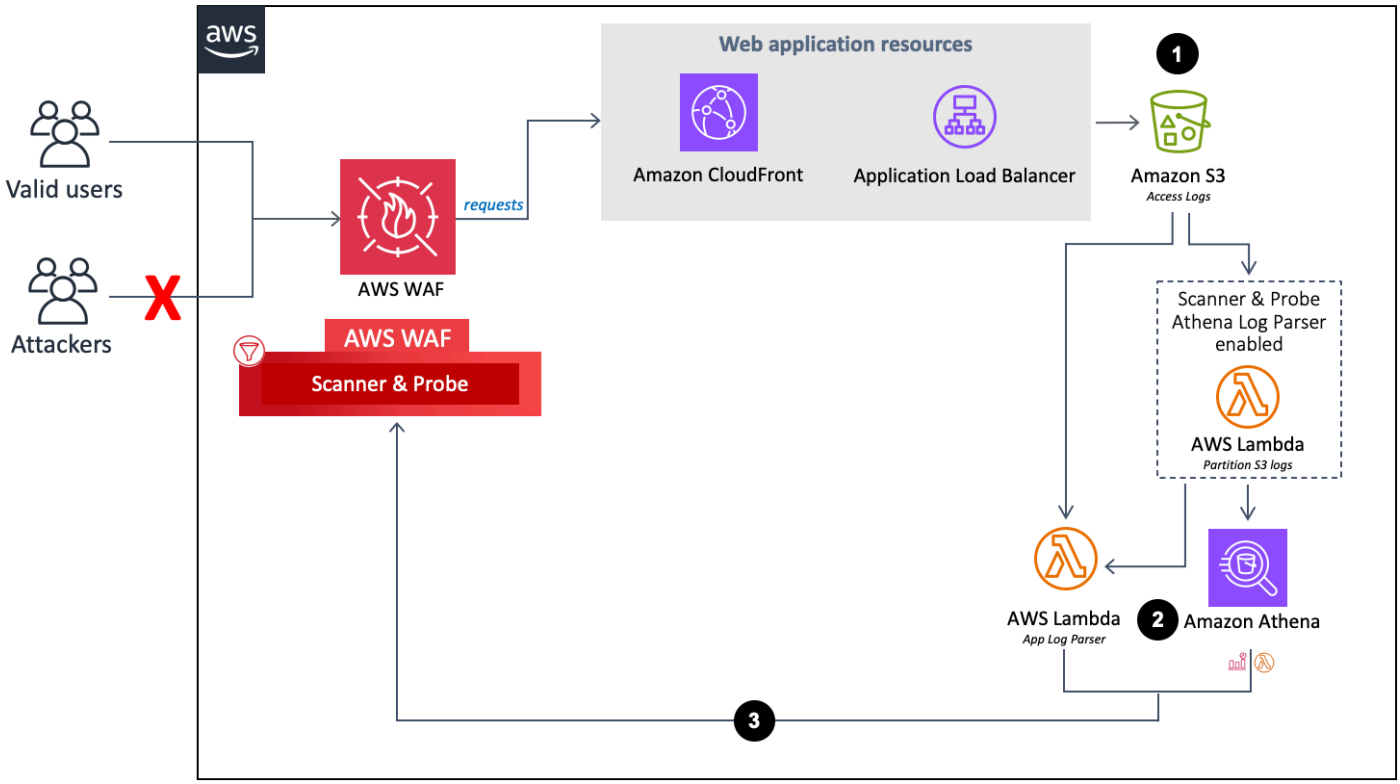
Os parâmetros do modelo Proteção contra HTTP inundações e Proteção de scanner e sonda fornecem a opção AWS Lambda Log Parser. Use o analisador de log Lambda somente quando a regra baseada em AWS WAF taxas e as opções do analisador de log do Amazon Athena não estiverem disponíveis. Uma limitação conhecida 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.

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 AWS WAF bloqueios. 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 registros de aplicativos

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 Activate HTTP Flood Protection e Activate Scanner & Probe Protection, uma função Lambda moverá os registros de acesso de sua pasta original *<customer-bucket>*/AWSLogs para uma pasta recém-particionada quando eles chegarem *<customer-bucket>*/AWSLogs-partitioned/*<optional-prefix>* /year=*<YYYY>*/month=*<MM>* /day=*<DD>*/hour=*<HH>*/ ao Amazon S3.

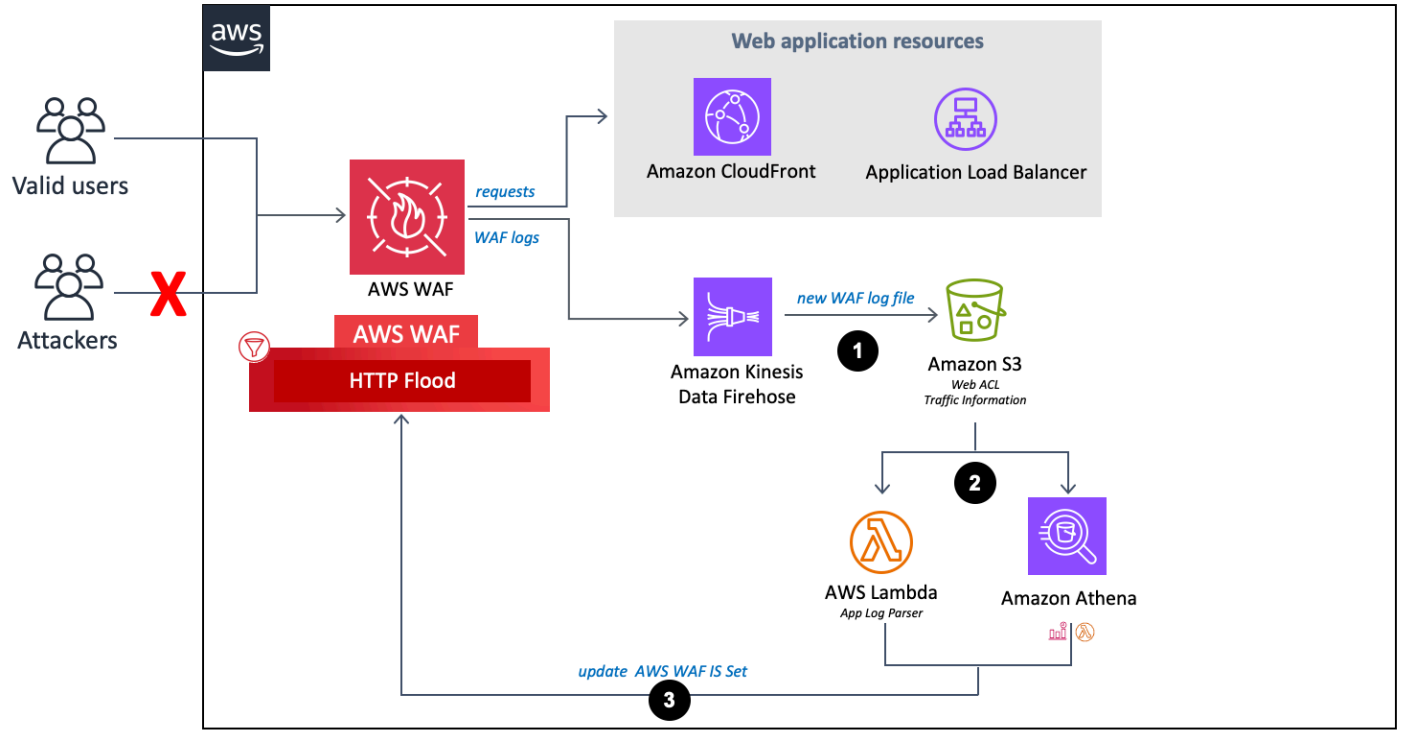
b. (Opcional) Se você selecionar `yes` o parâmetro Manter dados no modelo de localização original do S3, os registros permanecerão no local original e serão copiados para a pasta particionada, duplicando seu armazenamento de registros.

> **Note**
>
> Para o analisador de log Athena, essa solução particiona somente os novos registros que chegam ao seu bucket do Amazon S3 depois que você implanta essa solução. Se você tem registros existentes que deseja particionar, você deve fazer o upload manual desses registros para o Amazon S3 depois de implantar essa solução.

2. Com base na sua seleção dos parâmetros do modelo Ativar a proteção contra HTTP inundações e Ativar a proteção do scanner e da 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. 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 dentro. 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 AWS WAF IP 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` para Ativar Proteção contra HTTP Inundações, essa solução provisiona os seguintes componentes, que analisam AWS WAF os registros para identificar e bloquear as origens que inundam o endpoint com uma taxa de solicitação maior que a cota que você definiu.

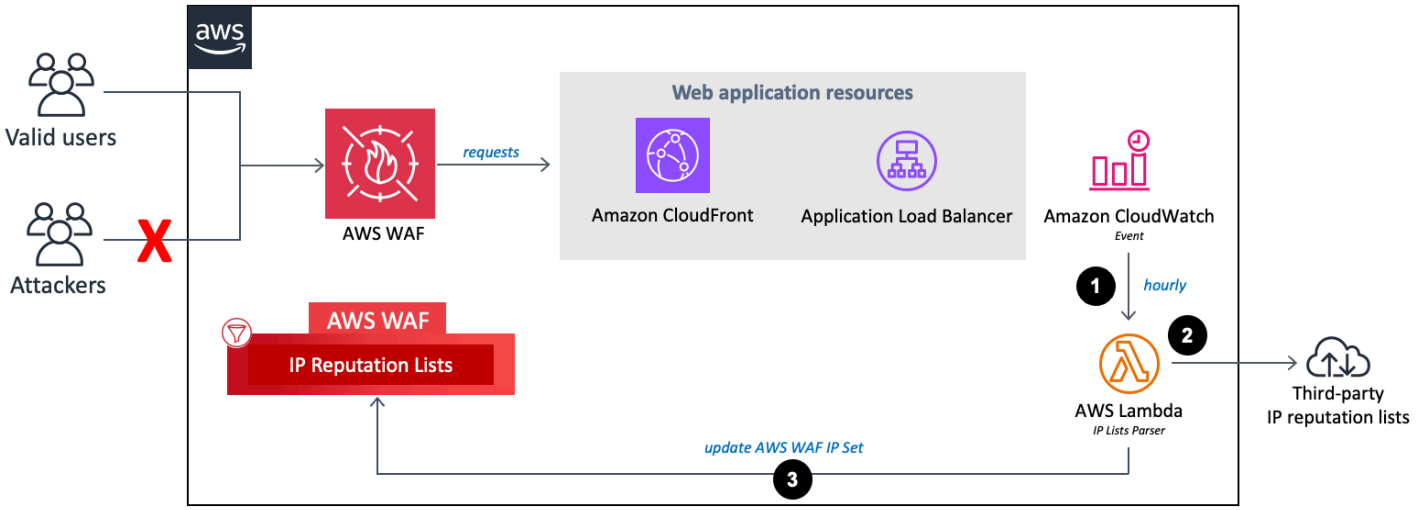


AWS WAF fluxo do analisador de log

1. Quando AWS WAF recebe registros de acesso, ele os envia para um endpoint Firehose. Em seguida, o Firehose 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 a proteção contra HTTP inundações e Ativar a proteção do scanner e da 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 e da sonda é executada e a saída é enviada para. 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 dentro. 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 AWS WAF IP 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.

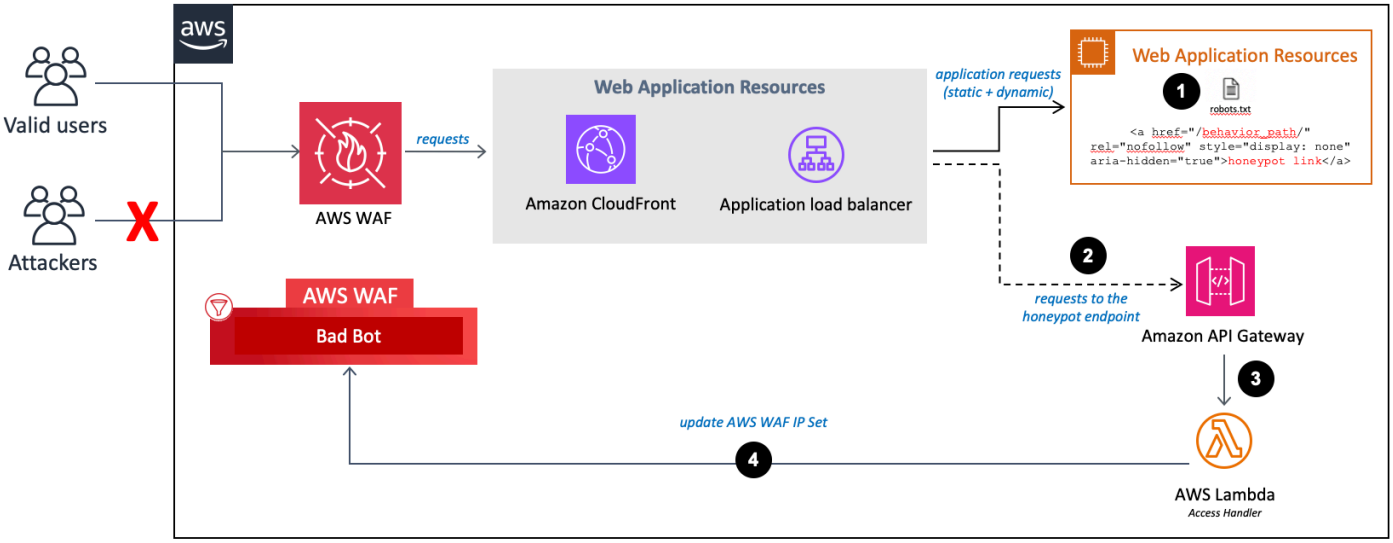


A reputação de IP lista o fluxo do analisador

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:
   - Spamhaus DROP e listas EDROP
   - Lista de IPs de ameaças emergentes da Proofpoint
   - Lista de modos de saída do Tor
3. A função Lambda atualiza a lista de AWS WAF bloqueios com os endereços IP atuais.

Manipulador de acesso

A função `Access Handler` Lambda inspeciona as solicitações para o endpoint do honeypot para extrair o endereço IP de origem.



Access Handler e o endpoint honeypot

1. Incorpore o endpoint do honeypot em seu site e atualize o padrão de exclusão de seus robôs, conforme descrito em Incorporar o link do Honeypot em seu aplicativo da Web (opcional).
2. Quando um raspador de conteúdo ou um bot mal-intencionado acessa o endpoint do honeypot, ele invoca a função Lambda. `Access Handler`
3. A função Lambda intercepta e inspeciona os cabeçalhos da solicitação para extrair o endereço IP da fonte que acessou o endpoint da armadilha.
4. A função Lambda atualiza uma condição de conjunto de AWS WAF IP para bloquear esses endereços IP.

Planeje a implantação

Esta seção descreve o custo, a segurança e outras considerações antes da implantação da solução. the section called “Cotas”

Suportado Regiões da AWS

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 todos Regiões da AWS. Portanto, você deve iniciar essa solução em um Região da AWS local onde esses serviços estejam disponíveis. Para obter a disponibilidade mais atual dos AWS serviços por região, consulte a Lista de Região da AWS todos os serviços.

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Endpoint type				
CloudFront	✓			
Application Load Balancer () ALB	✓			
Ative a HTTP proteção contra inundações				
sim - AWS Lambda analisador de log				✓
sim - Analisador de log Amazon Athena		✓	✓	✓
Ative a proteção do scanner e da sonda				
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 AWS serviços usados durante a execução da AWS WAF solução Security Automations for. O custo total da execução dessa solução depende da proteção ativada e da quantidade de dados ingeridos, armazenados e processados.

Recomendamos criar um orçamento AWS Cost Explorerpara ajudar a gerenciar os custos. Para obter detalhes completos, consulte a página de preços de cada AWS serviço usado 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 AWS gratuito). Os preços estão sujeitos a alterações.

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

AWS serviço	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, 1 milhão de invocações e duração média de 500 milissegundos por execução do Lambda	~$5,40
Amazon API Gateway	1 milhão de solicitações	~$3,40

AWS serviço	Dimensões/mês	Custo [USD]
AWS WAF web ACL	1	$5,00
AWS WAF regra	4	$4,00
AWS WAF pedido	1 milhão	$0,60
Total		~$23,60 por mês

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

AWS serviço	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 de 500 milissegundos por execução do Lambda	~$1,26
Amazon API Gateway	1 milhão de solicitações	~$3,40
Amazon Athena	1,2 milhão de CloudFront acessos de objetos ou 1,2 milhão de ALB solicitações por dia que geram um registro de registro de aproximadamente	~$4,32

AWS serviço	Dimensões/mês	Custo [USD]
	500 bytes por ocorrência ou solicitação	
AWS WAF web ACL	1	$5,00
AWS WAF regra	4	$4,00
AWS WAF pedido	1 milhão	$0,60
Total		~$23,78 por mês

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

AWS serviço	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
Amazon CloudWatch	Eventos 2K	~$0,00
AWS WAF Web ACL	1	$5,00
AWS WAF Regra	2	$2,00
WASWAFpedido	1 milhão	$0,60
Total		~$7,61 por mês

Estimativa de custo dos CloudWatch registros

Alguns AWS serviços 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 nos registros de acesso ao aplicativo AWS WAF ou nos seus buckets 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 HTTPFlood Protection ou Scanner & Probe 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 WAFBlock 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 AWS infraestrutura, as responsabilidades de segurança são compartilhadas entre você AWS e. Esse modelo de responsabilidade compartilhada reduz sua carga operacional porque 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 AWS segurança, visite Nuvem AWS Segurança.

Funções do IAM

Com IAM funções, você pode atribuir acesso, políticas e permissões granulares a serviços e usuários no Nuvem AWS. Essa solução cria IAM funções 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 coletar e roubar conteúdo da web.

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

- AWSRegras gerenciadas — Esse serviço gerenciado fornece proteção contra vulnerabilidades comuns de aplicativos ou outros tráfegos indesejados. Essa solução inclui grupos AWSgerenciados de regras de reputação de IP, grupos de regras de linha de base AWS AWS gerenciados e grupos de regras específicos de casos de uso gerenciados. Você tem a opção de selecionar um ou mais grupos de regras para sua webACL, até a cota máxima de unidade ACL de capacidade da web (WCU).
- SQLinjeção — Os atacantes inserem SQL código malicioso nas solicitações da web para extrair dados do seu banco de dados. Criamos essa solução para bloquear solicitações da web que contêm SQL códigos potencialmente maliciosos.
- XSS— Os invasores 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
- HTTPinundações — servidores Web e outros recursos de back-end correm o risco de DDoS ataques, como HTTP inundações. 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 AWS WAF registros 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 4xx. HTTP Você pode usar esse histórico para ajudar a identificar e bloquear endereços IP de origem maliciosos. Essa solução cria uma função Lambda ou consulta Athena que analisa CloudFront ou ALB acessa automaticamente os registros, conta o número de solicitações inválidas de endereços IP de origem exclusivos por minuto e atualiza 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 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

As service quotas, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para sua conta da Conta da AWS.

Cotas para AWS serviços nesta solução

Verifique se você tem cota suficiente para cada um dos serviços implementados nessa solução. Sim, para mais informações, consulte AWS Service Quotas. Para ver as cotas de serviço para todos os AWS serviços na documentação sem trocar de página, veja as informações na página Pontos de extremidade e cotas do serviço em vez disso. PDF

AWS WAF cotas

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 AWS WAF cotas. A partir da versão 3.0, essa solução cria dois conjuntos de IP para anexar a cada regra, um para IPv4 e outro paraIPv6.

AWS WAF permite no máximo uma solicitação por segundo, por conta, Região da AWS por API chamada para qualquer pessoa `Create` ou `Update` ação. `Put` Se você fizer essas API chamadas fora da solução, poderá encontrar um problema de API limitação. Para evitar o problema, recomendamos evitar a execução de outros aplicativos que façam essas API chamadas 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.

AWS WAF regras

A web ACL que essa solução gera foi projetada para oferecer proteção abrangente para aplicativos da web. A solução fornece um conjunto AWS Managed Rules de regras personalizadas que você pode adicionar à WebACL. 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 AWS Firewall Manager. Se você quiser usar as regras no Firewall Manager, recomendamos que você aplique personalizações ao código-fonte.

Registro ACL de tráfego na web

Se você criar a pilha em um local Região da AWS diferente do Leste dos EUA (Norte da Virgínia) e definir o Endpoint como`CloudFront`, deverá definir Ativar Proteção contra HTTP Inundações como ou. no `yes - AWS WAF rate based rule`

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

Tratamento de grandes dimensões para componentes de solicitação

AWS WAF não suporta a inspeção de conteúdo superdimensionado para ver o corpo, os cabeçalhos ou os 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 saber 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. 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`— Trate a solicitação da web como se correspondesse à declaração da regra. AWS WAF aplica a ação da regra à solicitação sem avaliá-la de acordo com os critérios de inspeção da regra. 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. AWS WAF continua sua inspeção da solicitação da web usando o resto das regras na webACL, como faria com qualquer regra não correspondente.

Para obter mais informações, consulte Como lidar com componentes de solicitações web de tamanho grande em AWS WAF.

Várias implantações de 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 AWS WAF cotas por conta e por região.

Implante a solução

Essa solução usa modelos e pilhas do AWS CloudFormation para automatizar sua implantação. Os CloudFormation modelos especificam os AWS recursos 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 seu 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 web ACL ao seu aplicativo web

- Associe sua CloudFront (s) distribuição ALB (ões) na web à web ACL 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 sua (s) distribuição ALB (ões) web 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 Logs (`AWS Logs/`prefixo de registro padrão). AWS Consulte o parâmetro Application Access Log Bucket Prefix na Etapa 1. Inicie a pilha para obter mais informações.

AWS CloudFormation modelos

Essa solução inclui um AWS CloudFormation modelo principal 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 AWS WAF web ACL com regras pré-configuradas. Você pode personalizar o modelo com base nas suas necessidades.

Pilha web ACL

aws-waf-security-automations-webacl.template — Esse modelo aninhado provisiona AWS WAF recursos, incluindo uma webACL, IP, conjuntos e outros recursos associados.

Pilha Firehose Athena

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

Pré-requisitos

Essa solução foi projetada para funcionar com aplicativos da web implantados com CloudFront ou umALB. 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 e ALB 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 do

Esse AWS CloudFormation modelo automatizado implanta a solução no Nuvem AWS.

1. Faça login no AWS Management Consolee selecione Launch Solution para iniciar o `waf-automation-on-aws.template` CloudFormation modelo.

Launch solution

2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar essa solução de outra forma Região da AWS, use o seletor de região 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 Regiões da AWS apenas de forma específica. Portanto, você deve iniciar essa solução em um Região da AWS local onde esses serviços estejam disponíveis. Para obter mais informações, consulte Compatível Regiões 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 AWS WAF configuração no campo Nome da pilha. Esse também é o nome da web ACL 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.

Parâmetro	Padrão	Descrição
Nome da stack	*`<requires input>`*	O nome da pilha não pode conter espaços. Esse nome deve ser exclusivo dentro do seu Conta da AWS e é o nome da web ACL que o modelo cria.
Tipo de recurso		
Endpoint	`CloudFront`	Escolha o tipo de recurso que está sendo usado.

Parâmetro	Padrão	Descrição
		Note Se você escolher `CloudFront` como seu endpoint, deverá iniciar a solução para criar WAF recursos na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).
AWS Grupos de regras de reputação de IP gerenciados		

Parâmetro	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 webACL. 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. O necessário WCU é 25. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantaç ão do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	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 WebACL. Esse grupo de regras bloqueia solicitações de serviços que permitem a ofuscação da identidade do espectador. Isso inclui solicitações deVPNs, proxies, nós Tor e provedores de hospedagem. Esse grupo de regras é útil se você quiser filtrar visualizadores que podem estar tentando ocultar a identidade do seu aplicativ o. Bloquear os endereços IP desses serviços pode ajudar a mitigar bots e evasão de restrições geográficas. O necessário WCU é 50. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantaç ão do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
AWS Grupos de regras de linha de base gerenciados		
Ativar a proteção de grupos de regras gerenciados do conjunto de regras principais	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas do Conjunto de Regras Principais à WebACL. Esse grupo de regras oferece proteção contra a exploraçã o de uma ampla variedade de vulnerabilidades, incluindo algumas das vulnerabilidades de alto risco e de ocorrênci a comum. Considere usar esse grupo de regras para qualquer caso de AWS WAF uso. O necessário WCU é 700. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantaç ão do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ativar a Proteção Administrativa Proteção de Grupos de Regras Gerenciadas	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas de Proteção Administrativa à WebACL. 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. O necessário WCU é 100. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ativar entradas incorretas conhecidas e proteção de grupos de regras gerenciadas	no	Escolha ativar o componente projetado `yes` para adicionar o Grupo de Regras Gerenciadas de Entradas Incorretas Conhecidas à WebACL. 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. O necessário WCU é 100. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.
AWS Grupo de regras específicas para casos de uso gerenciados		

Parâmetro	Padrão	Descrição
Ativar a proteção de grupos de regras gerenciados do SQL banco	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas do SQL Banco de Dados à WebACL. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de SQL bancos de dados, como ataques de SQL injeção. Isso pode ajudar a evitar a injeção remota de consultas não autorizadas. Avalie esse grupo de regras para uso se seu aplicativo fizer interface com um SQL banco de dados. Usar a regra personalizada de SQL injeção é opcional se você já tiver um grupo de SQL regras AWS gerenciado ativado. O necessário WCU é 200. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ative a proteção de grupos de regras gerenciados do sistema operacional Linux	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas do Sistema Operacional Linux à webACL. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas do Linux, incluindo ataques de inclusão de arquivos locais () específicos do Linux. 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 no Linux. Você deve usar esse grupo de regras em conjunto com o grupo de regras do sistema POSIX operacional. O necessário WCU é 200. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade.

Parâmetro	Padrão	Descrição
		Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ativar a proteção de grupos de regras gerenciados do sistema POSIX operacional	no	Escolha ativar o componente projetado `yes` para adicionar o Core Rule Set Managed Rule Group Protection à webACL. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades POSIX específicas POSIX e similares a sistemas operacionais, incluindo LFI ataques. 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 POSIX sistema operacional POSIX semelhante. O necessário WCU é 100. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade.

Parâmetro	Padrão	Descrição
		Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ativar a Proteção de Grupo de Regras Gerenciadas do Sistema Operacional Windows	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas do Sistema Operacional Windows à WebACL. 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. O necessário WCU é 200. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade.

Parâmetro	Padrão	Descrição
		Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	Padrão	Descrição
Ativar a proteção de grupos de regras gerenciadas por PHP aplicativos	no	Escolha `yes` ativar o componente projetado para adicionar o Grupo de Regras Gerenciadas por PHP Aplicativos à WebACL. Esse grupo de regras bloqueia padrões de solicitação associados à exploração de vulnerabilidades específicas ao uso da linguagem de PHP programação, incluindo a injeção de funções insegurasPHP. 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 esse grupo de regras se PHP estiver instalado em qualquer servidor com o qual seu aplicativo faça interface. O necessário WCU é 100. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantação do web ACL stack devido ao excesso do limite de capacidade.

Parâmetro	Padrão	Descrição
		Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.
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 WebACL. Esse grupo de regras bloqueia os padrões de solicitação associados à exploração de vulnerabi lidades 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 SQL banco de dados e do PHP aplicativo. O necessário WCU é 100. Sua conta deve ter WCU capacidade suficiente para evitar falhas na implantaç ão do web ACL stack devido ao excesso do limite de capacidade. Para obter mais informações, consulte a lista de grupos de AWS Managed Rules regras.

Parâmetro	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.

Parâmetro	Padrão	Descrição
Nome do bucket do log de acesso ao aplicativo	`<requires input>`	Se você escolheu `yes` o parâmetro Activate Scanner & Probe Protection, insira o nome do bucket Amazon S3 (novo ou existente) no qual você deseja armazenar os registros de acesso para CloudFront sua (s) distribui ção (ões) ALB ou (s). Se você estiver usando um bucket Amazon S3 existente, ele deverá estar localizado no mesmo Região da AWS local 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. **Note** Ative o registro de acesso à CloudFron t web para sua (s) distribuição ALB (ões) web para enviar arquivos de log para esse bucket do Amazon S3. Salve os registros no mesmo prefixo definido na pilha

Parâmetro	Padrão	Descrição
		(`AWS Logs/`prefixo padrão). Consulte o parâmetro Application Access Log Bucket Prefix para obter mais informações.
Prefixo do bucket do log de acesso ao aplicativo	`AWS Logs/`	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 `AWS Logs/` ao seu prefixo, como. `yourprefix/AWSLogs/` Use `AWS Logs/` (padrão) se não houver um prefixo definido pelo usuário. Para desativar essa proteção, ignore esse parâmetro.

Parâmetro	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.

Parâmetro	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 Inundação		

Parâmetro	Padrão	Descrição
Ative a HTTP proteção contra inundações	`yes - AWS WAF rate-based rule`	Selecione o component e usado para bloquear ataques de HTTP inundação . 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 HTTP inundações, insira o máximo de solicitaç ões aceitáveis por cinco minutos, por endereço IP. Se você escolheu `yes - AWS WAF rate-based rule` o parâmetro Ativar proteção contra HTTP inundações, o valor mínimo aceitável é`100`. Se você escolheu `yes - AWS Lambda log parser` ou `yes – Amazon Athena log parser` para o parâmetro Ativar proteção contra HTTP inundações, ele pode ser qualquer valor. Para desativar essa proteção, ignore esse parâmetro.

Parâmetro	Padrão	Descrição
Limite de solicitação por país	<optional input>	Se você escolher `yes - Amazon Athena log parser` o parâmetro Ativar proteção contra HTTP inundações, poderá inserir um limite por país seguindo esse JSON formato. `{"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. **Note** Se você definir esse parâmetro, o país será incluído automaticamente 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 Flood HTTP Athena Query.

Parâmetro	Padrão	Descrição
		Se você optar por desativar essa proteção, ignore esse parâmetro.
Agrupar por solicitações no HTTP Flood Athena Query	`None`	Se você escolher `yes - Amazon Athena log parser` o parâmetro Ativar Proteção contra HTTP Inundações, 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 URI e. Se você optar por desativar essa proteção, ignore esse parâmetro.

Parâmetro	Padrão	Descrição
WAFPeríodo de bloqueio	`240`	Se você escolher `yes - AWS Lambda log parser` entre os parâmetros Ativar Proteção de Scanner e Sonda ou Ativar Proteção contra HTTP Inundaçõe s, 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.
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.
Regra personalizada — Bad Bot		

Parâmetro	Padrão	Descrição
Ative a proteção Bad Bot	`yes`	Escolha `yes` ativar o componente projetado para bloquear bots maliciosos e raspadores de conteúdo.
ARNde uma IAM função que tem acesso de gravação aos CloudWatch registros em sua conta	<optional input>	Forneça uma IAM função opcional ARN que tenha acesso de gravação aos CloudWatch registros em sua conta. Por exemplo: `ARN: arn:aws:iam::account_id:role/myrolename` . Consulte Configurando o CloudWatch registro para um REST API no API Gateway para obter instruções sobre como criar a função. Se você deixar esse parâmetro em branco (padrão), a solução criará uma nova função para você.

Parâmetro	Padrão	Descrição
Limite de solicitação padrão	100	Se você escolher `yes` o parâmetro Ativar proteção contra HTTP inundações, insira o máximo de solicitações aceitáveis por cinco minutos, por endereço IP. Se você escolher `yes - AWS WAF rate-based rule` o parâmetro Ativar proteção contra HTTP inundações, o valor mínimo aceitável é 100. Se você escolheu `yes - AWS Lambda log parser` ou `yes – Amazon Athena log parser` para o parâmetro Ativar proteção contra HTTP inundações, ele pode ser qualquer valor. Para desativar essa proteção, ignore esse parâmetro.
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		

Parâmetro	Padrão	Descrição
Ativar a proteção de SQL injeção	`yes`	Escolha `yes` ativar o componente projetado para bloquear ataques comuns SQL de injeção. Considere ativá-lo se você não estiver usando um conjunto de regras principais AWS gerenciadas ou um grupo de regras de SQL banco de dados AWS gerenciado. Você pode escolher uma das opções `yes` (continuar) ou`yes - NO_MATCH`) AWS WAF para lidar com 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.

Parâmetro	Padrão	Descrição
		Note A CloudFormation pilha adiciona a opção de manuseio de tamanho grande selecionada à regra de proteção de SQL injeção padrão e a implanta na sua. Conta da AWS Se você personalizou a regra fora de CloudFormation, suas alterações serão substituídas após a atualização da pilha.

Parâmetro	Padrão	Descrição
Nível de sensibilidade para proteção contra SQL injeção	`LOW`	Escolha o nível de sensibilidade que você deseja usar AWS WAF para inspecionar ataques de SQL injeção. `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 SQL injeção ou que têm baixa tolerância a falsos positivos. Para obter mais informações, consulte AWS WAF adiciona níveis de sensibilidade às declarações e SensitivityLevelpropriedades da regra de SQL injeção no Guia AWS CloudFormation do usuário. Se você optar por desativar a proteção SQL por injeção, ignore esse parâmetro. **Note** A CloudFormation pilha adiciona o nível de sensibilidade selecionado à regra de proteção de SQL injeção padrão

Parâmetro	Padrão	Descrição
		e o implanta em sua. Conta da AWS Se você personalizou a regra fora de CloudFormation, suas alterações serão substituídas após a atualização da pilha.

Parâmetro	Padrão	Descrição
Ative a proteção de script entre sites	`yes`	Escolha `yes` ativar o componente projetado para bloquear XSS ataques comuns. Considere ativá-lo se você não estiver usando um conjunto de regras principais AWS gerenciad as. Você também pode selecionar uma das opções `yes` (continuar) ou`yes - NO_MATCH`) que deseja AWS WAF processar solicitaç ões 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. **Note** A CloudFormation pilha adiciona a opção de tratamento

Parâmetro	Padrão	Descrição
		de tamanho grande selecionada à regra padrão de script entre sites e a implanta em sua. Conta da AWS Se você personali zou 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 permitido s, 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.

Parâmetro	Padrão	Descrição
Período de retenção (minutos) para o conjunto de IP negado	`-1`	Se você quiser ativar a retenção de IP para o conjunto de IP negado, insira um número (`15`ou mais) como o 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).

Parâmetro	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 IAM recursos e quaisquer recursos adicionais necessários.
9. Escolha Enviar para implantar a pilha.

   Veja o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber um status de CREATE _ COMPLETE em aproximadamente 15 minutos.

> **Note**
>
> Além das funções,, e `Log Parser` `IP Lists Parser`, essa solução inclui `Access Handler` AWS Lambda as funções Lambda `helper` e `custom-resource` Lambda, 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 AWS Lambda console, mas somente as três funções principais da solução estão ativas regularmente. 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, que é o endpoint do honeypot do API Gateway. Lembre-se desse valor porque você o usará no link Incorporar o Honeypot em seu aplicativo da web.

Etapa 2. Associe a web ACL ao seu aplicativo web

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

1. Faça login no console do AWS WAF.
2. Escolha a web ACL que você deseja usar.
3. Na guia Associated AWS resources, escolha Add AWS resources.
4. Em Tipo de recurso, escolha a CloudFront distribuição ouALB.
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 ALB ou envie registros 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 AWS WAF Web ACL, escolha a ACL solução 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 atual. Conta 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(padrãoAWS Logs/).
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 (AmazonEC2).
2. No painel de navegação, selecione Load Balancers.
3. Selecione o do seu aplicativo webALB.
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(padrãoAWS Logs/).
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.

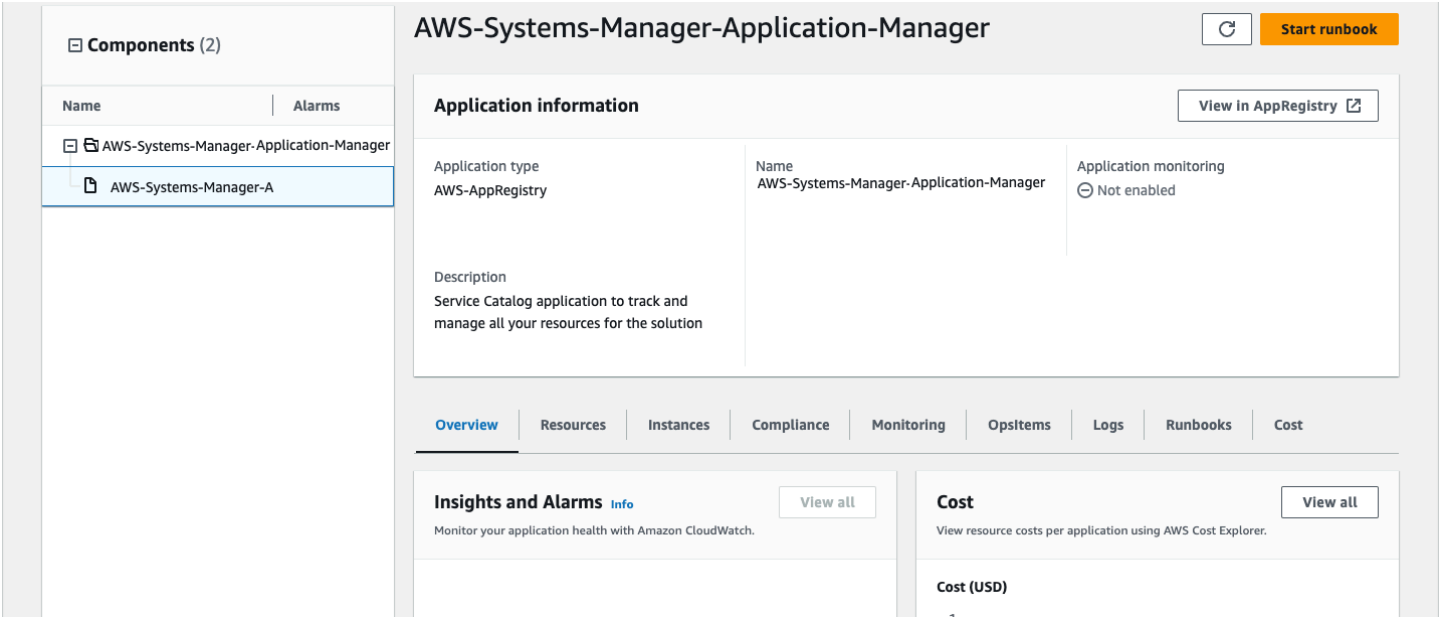
Monitore a solução com AppRegistry

A solução inclui um AppRegistry recurso do Service Catalog para registrar o CloudFormation modelo e os recursos subjacentes como um aplicativo no Service Catalog AppRegistry e no AWS Systems Manager Application Manager.

AWS O Systems Manager Application Manager oferece uma visão em nível de aplicativo dessa solução e de seus recursos para que você possa:

- Monitore seus recursos, custos dos recursos implantados em pilhas e Contas da AWS registros associados a essa solução a partir de um local central.
- Visualize os dados operacionais dos recursos dessa solução no contexto de um aplicativo. Por exemplo, status de implantação, CloudWatch alarmes, configurações de recursos e problemas operacionais.

A figura a seguir mostra um exemplo da visualização do aplicativo para a pilha de soluções no Application Manager.



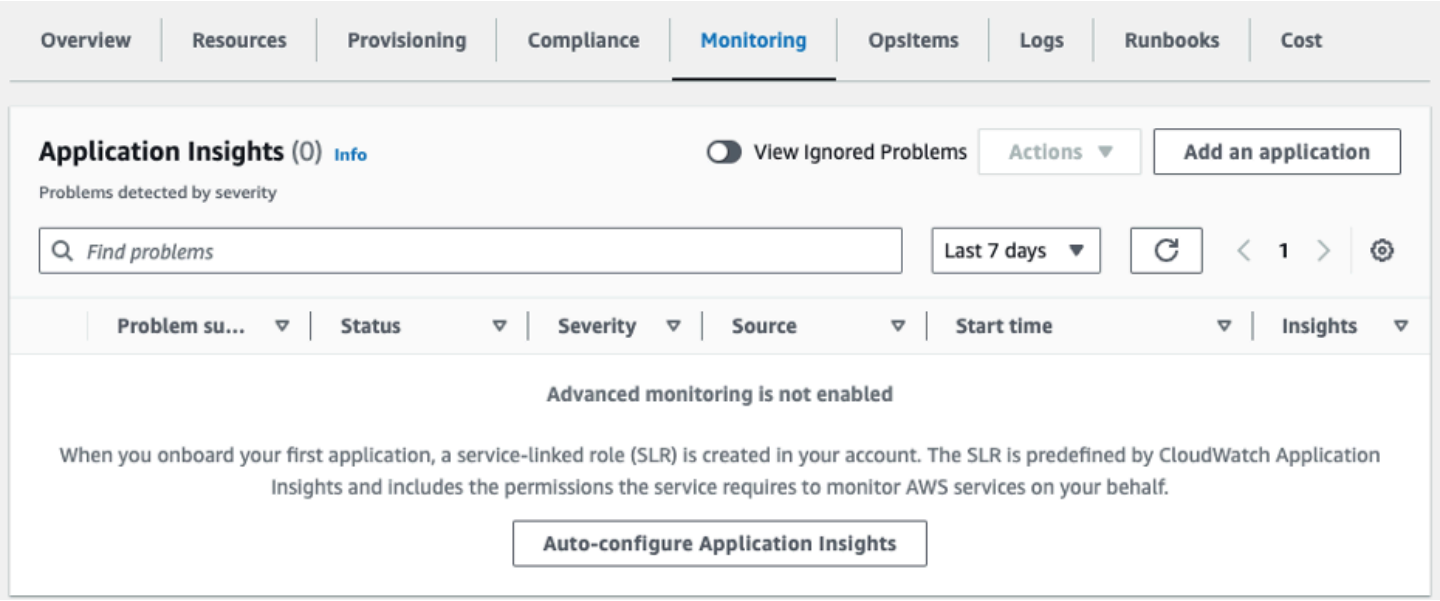
Pilha de soluções no Application Manager

Ative CloudWatch Application Insights

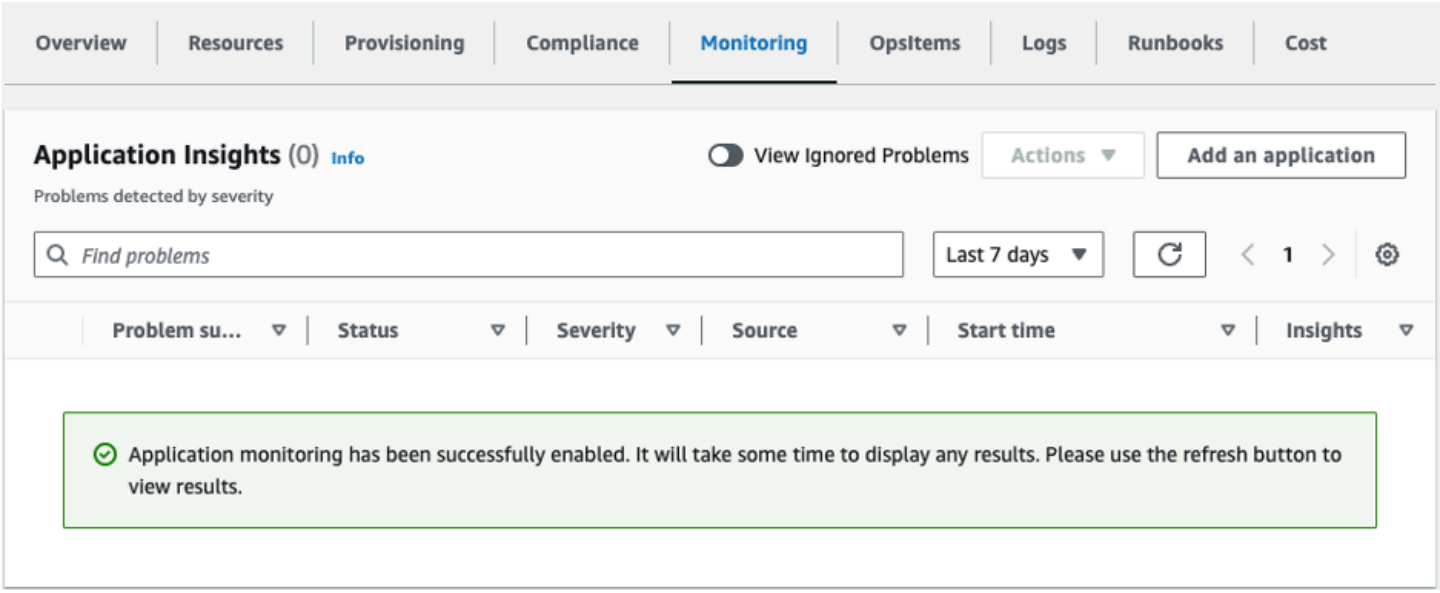
1. Faça login no console do Systems Manager.

2. No painel de navegação, escolha Application Manager.
3. Em Aplicativos, pesquise o nome do aplicativo para essa solução e selecione-o.

   O nome do aplicativo terá Registro do aplicativo na coluna Fonte do aplicativo e terá uma combinação do nome da solução, região, ID da conta ou nome da pilha.
4. Na árvore Componentes, escolha a pilha de aplicativos que você deseja ativar.
5. Na guia Monitoramento, em Application Insights, selecione Configurar automaticamente o Application Insights.



O monitoramento de seus aplicativos agora está ativado e a seguinte caixa de status é exibida:

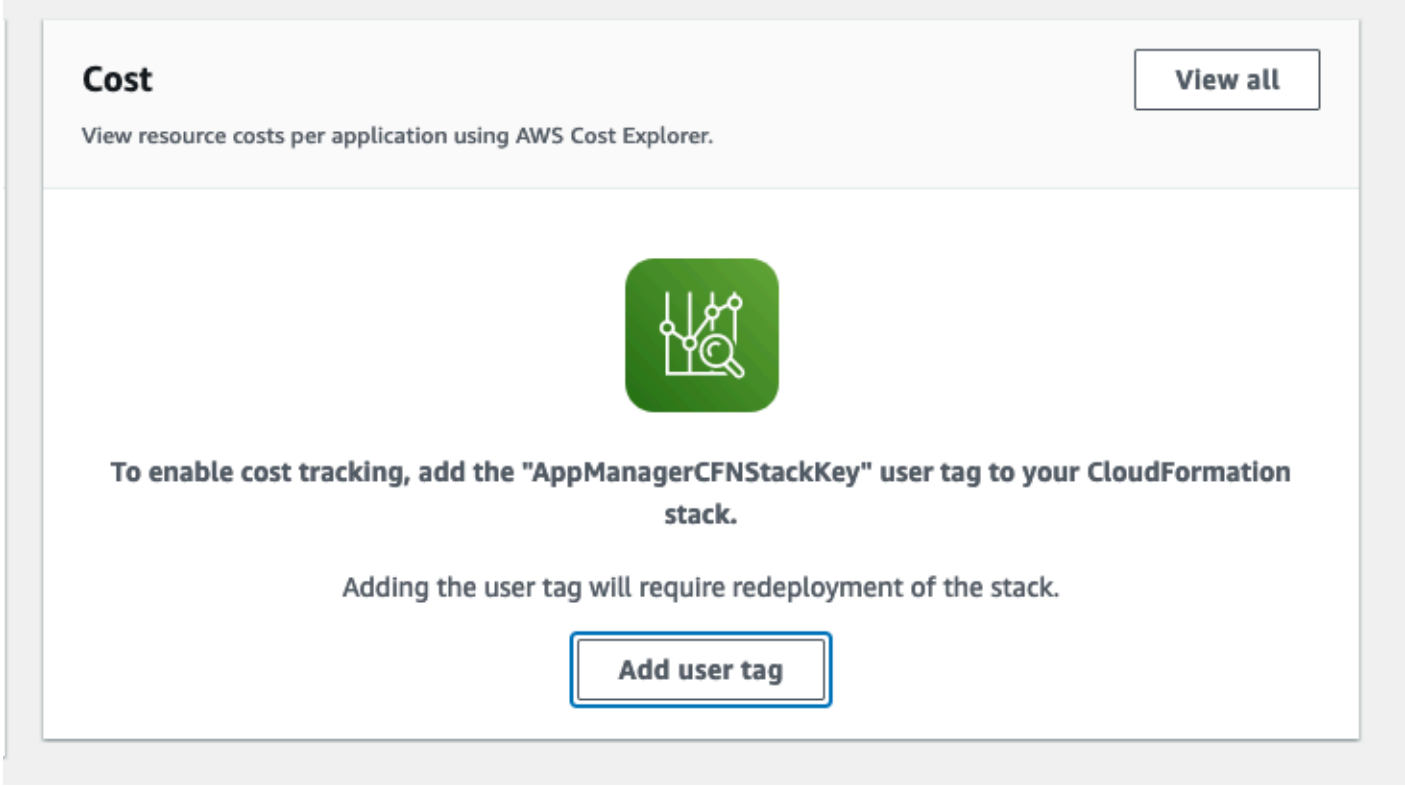


Confirme as tags de custos associadas à solução

Depois de ativar as etiquetas de alocação de custos associadas à solução, você deve confirmar as etiquetas de alocação de custos para ver os custos dessa solução. Para confirmar as tags de alocação de custos:

1. Faça login no console do Systems Manager.
2. No painel de navegação, escolha Application Manager.
3. Em Aplicativos, escolha o nome do aplicativo para essa solução e selecione-o.

   O nome do aplicativo terá Registro do aplicativo na coluna Fonte do aplicativo e terá uma combinação do nome da solução, região, ID da conta ou nome da pilha.
4. Na guia Visão geral, em Custo, selecione Adicionar tag de usuário.



5. Na página Adicionar tag de usuário, insira `confirm` e selecione Adicionar tag de usuário.

O processo de ativação pode levar até 24 horas para que os dados da tag apareçam.

Ative as tags de alocação de custos associadas à solução

Depois de ativar o Cost Explorer, ative as tags de alocação de custos associadas a essa solução para ver os custos dessa solução. As tags de alocação de custos só podem ser ativadas pela conta de gerenciamento da organização. Para ativar as tags de alocação de custos:

1. Faça login no console AWS Billing and Cost Management de gerenciamento de custos.
2. No painel de navegação, selecione Tags de alocação de custos.
3. Na página Tags de alocação de custos, filtre a AppManagerCFNStackKey tag e selecione a tag nos resultados mostrados.
4. Selecione Ativar.

AWS Cost Explorer

Você pode ver a visão geral dos custos associados ao aplicativo e aos componentes do aplicativo no console do Application Manager por meio da integração com AWS Cost Explorer, que deve ser ativada primeiro. O Cost Explorer ajuda você a gerenciar custos fornecendo uma visão dos custos e do uso dos recursos da AWS ao longo do tempo. Ativar o Cost Explorer para a solução:

1. Faça login no Console de Gerenciamento de custos da AWS.
2. No painel de navegação, selecione Cost Explorer para visualizar os custos e o uso da solução ao longo do tempo.

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 console do AWS CloudFormation.
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 S3URL.
   b. Copie o link do `aws-waf-security-automations.template` AWS CloudFormation.
   c. Cole o link na caixa do Amazon S3 URL.
   d. Verifique se o modelo correto URL aparece na caixa de URL texto do Amazon S3.
   e. Escolha Próximo.
   f. Escolha Avançar novamente.
7. Em Parâmetros, revise os parâmetros do modelo e modifique-os conforme necessário. Consulte a Etapa 1. Inicie a pilha para obter detalhes sobre os parâmetros.
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 confirmando que o modelo pode criar IAM recursos.
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 AWS CloudFormation console na coluna Status. Você deve ver um status de UPDATE _ COMPLETE em aproximadamente 15 minutos.

Considerações de 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.

WAFV2atualização

A partir da versão 3.0, essa solução oferece suporte à AWS WAF V2. Substituímos todas as API chamadas AWS WAF clássicas por APIchamadas AWS WAF V2. 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 AWS WAF regras com configurações padrão em sua Conta da AWS 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.

> **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 IP conforme necessário. Consulte os update-ip-setCLIcomandos get-ip-sete. 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 console do AWS CloudFormation.

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 AWS recursos 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 AWAWAFAPIcotas, 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.

No entanto, raspadores de conteúdo e bots, como malware que verifica vulnerabilidades de segurança e coleta endereços de e-mail, podem tentar acessar o endpoint do trap. Nesse cenário, a função `Access Handler` Lambda inspeciona a solicitação para extrair sua origem e, em seguida, atualiza a AWS WAF regra associada para bloquear solicitações subsequentes desse endereço IP.

Use um dos procedimentos a seguir para incorporar o link do honeypot para solicitações de uma CloudFront distribuição ou de uma. ALB

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 console do AWS CloudFormation.
2. Escolha a pilha que você construiu na Etapa 1. Inicie a pilha
3. Escolha a guia Outputs.
4. Na BadBotHoneypotEndpointchave, copie o endpointURL. Ele contém dois componentes necessários para concluir este procedimento:
   - O nome do host do endpoint (por exemplo,`xxxxxxxxxx.execute-api.region.amazonaws.com`)
   - A solicitação URI (`/ProdStage`)
5. Faça login no CloudFront console da Amazon.
6. Escolha a distribuição que você deseja usar.
7. Escolha Distribution Settings.
8. Na guia Origins (Origens), selecione Create Origin (Criar origem).
9. No campo Nome de domínio de origem, cole o componente do nome do host do endpoint URL que você copiou na Etapa 2. Associe a Web ACL ao seu aplicativo Web.
10. No Origin Path, cole a solicitação URL que você também copiou na Etapa 2. Associe a Web ACL ao seu aplicativo Web.
11. Aceite os valores padrão para os outros campos.
12. Escolha Criar.
13. Na guia Behaviors (Comportamentos), selecione Create Behavior (Criar comportamentos).
14. Crie um novo comportamento de cache e aponte-o para a nova origem. Você pode usar um domínio personalizado, como um nome de produto falso que seja semelhante a outro conteúdo do seu aplicativo web.
15. Incorpore esse link de endpoint em seu conteúdo apontando para o honeypot. Oculte esse link de seus usuários humanos. Como exemplo, analise o seguinte exemplo de código:

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

> **Note**
>
> É sua responsabilidade verificar quais valores de tag funcionam no ambiente do seu site. Não use `rel="nofollow"` se seu ambiente não o observar. Para obter mais informações sobre a configuração de metatags de robôs, consulte o guia do desenvolvedor do Google.

16 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>
```

Incorpore o endpoint do Honeypot como um link externo

Use este procedimento para aplicativos web que são implantados com umALB.

1. Faça login no console do AWS CloudFormation.
2. Escolha a pilha que você construiu na Etapa 1. Lance a pilha.
3. Escolha a guia Outputs.
4. Na BadBotHoneypotEndpointchave, copie o endpointURL.
5. Incorpore esse link de endpoint em seu conteúdo da web. Use o completo URL que você copiou na Etapa 2. Associe a Web ACL ao seu aplicativo Web. Oculte esse link de seus usuários humanos. Como exemplo, analise o seguinte exemplo de código:

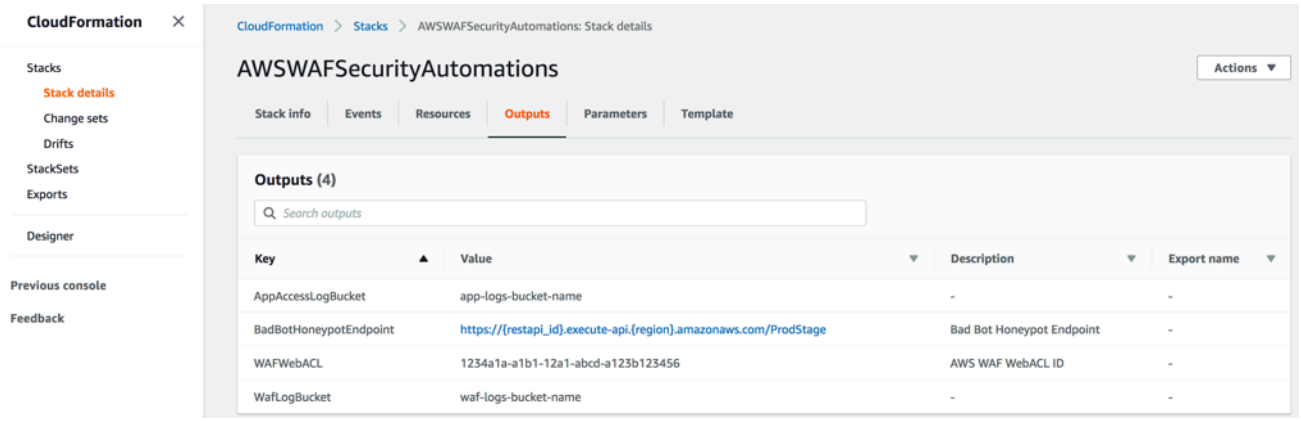
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> Esse procedimento é usado `rel=nofollow` para instruir os robôs a não acessarem o URL 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 o observar.

Use o arquivo do analisador de log Lambda JSON

Use o JSON arquivo do analisador de log Lambda para proteção contra inundações 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 AWS WAF os arquivos de log. Para encontrar o nome do bucket, consulte a WafLogBucketvariável na CloudFormation saída. A figura a seguir mostra um exemplo.



Saídas de pilha

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. AWS WAF O exemplo a seguir é um arquivo de configuração de amostra:

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

HTTParquivo de configuração de inundação

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 endereços IP aplicáveis. Essa solução usa o valor que você define ao provisionar ou atualizar a CloudFormation pilha.
  - Sufixos ignorados — Solicitações que acessam esse tipo de recurso não contam para o limite de solicitações. Por padrão, essa lista está vazia.
- URIlista — 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 WAF os registros chegarem ao WafLogBucket, eles serão processados pela função de 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 WAF IPs do HTTPFlood 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 JSON arquivo do analisador de log Lambda para proteção do scanner e da 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. AWS WAF O exemplo a seguir é um arquivo de configuração de amostra:

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

Arquivo de configuração de scanners e sondas

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 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 HTTP status como erros: `400 (Bad Request)` `401 (Unauthorized)`403 (Forbidden),404 (Not Found),, 405 (Method Not Allowed) e.

- URIlista — Use isso para definir um limite de solicitação personalizado e um período de bloqueio para detalhes específicosURLs. 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 nomeado *`<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 WAF IPs do 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 URI no HTTP flood Athena log parser

Você pode agrupar por país e URI na consulta do Athena para detectar e bloquear ataques de HTTP inundação IPs com padrões imprevisíveis. URI 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. Lance 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 selecionou `Yes - Amazon Athena log parser` os parâmetros do modelo Activate HTTP Flood Protection ou Activate Scanner & Probe Protection, essa solução cria e executa

consultas do Athena para CloudFront or ALB (`ScannersProbesLogParser`) ou AWS WAF logs (`HTTPFloodLogParser`), analisa a saída e atualiza adequadamente. AWS WAF

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 WAFBlock 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. AWS AWS Glue Data Catalog Essa solução cria o catálogo de dados de registros de acesso 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 a versão mais recente AWSAWS Glue Data Catalog step-by-step.

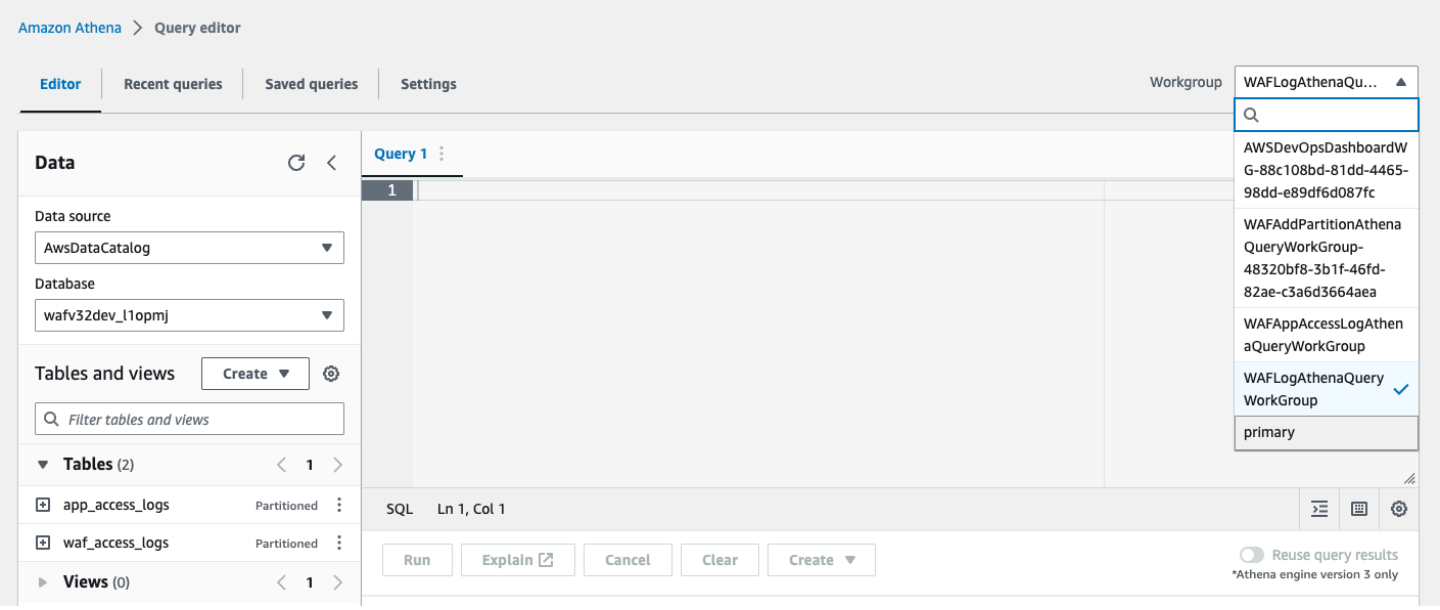
Use o procedimento a seguir para visualizar essas consultas:

Exibir consultas WAF de registro

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 HTTP Inundações.

5. Escolha Alternar para alternar o grupo de trabalho.



6. Selecione a guia Histórico.
7. 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.

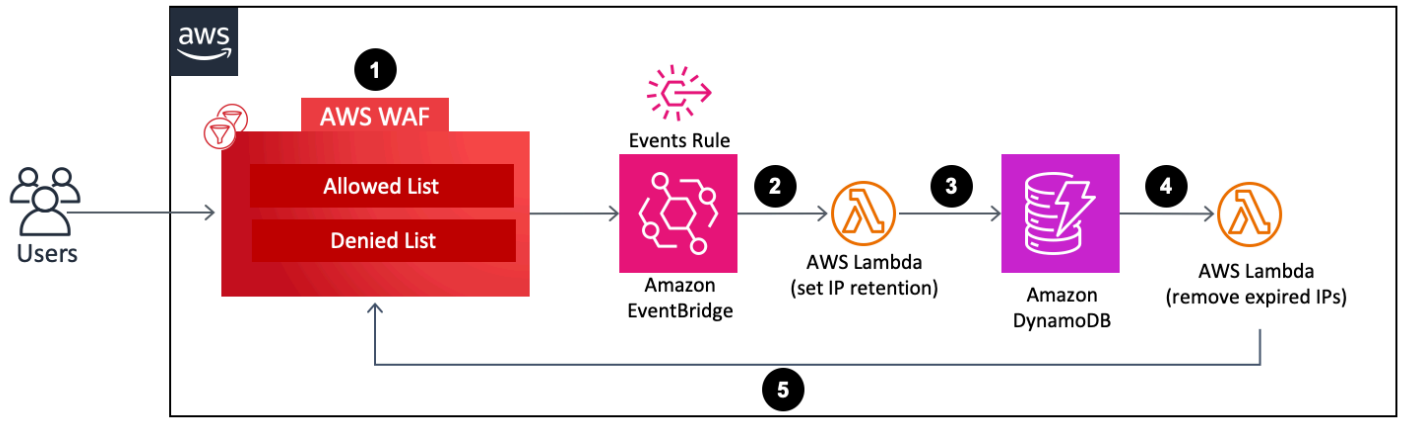
> **Note**
>
> Esse grupo de trabalho existe somente se você selecionou `Yes - Amazon Athena log parser` o parâmetro do modelo Ativar Proteção contra HTTP Inundações e/ou Ativar Proteção de Scanner e Sonda.

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 AWS WAF IP permitidos e negados

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

Como funciona



Retenção de IP em conjuntos de WAF IP permitidos e negados

1. Quando um usuário atualiza (adiciona ou exclui um endereço IP) o conjunto WAF IP permitido ou negado, essa ação invoca uma AWS WAF `UpdateIPSet` API chamada 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 () ativados. TTL O TTL atributo é`ExpirationTime`.
4. Quando um item atinge o prazo de validade, ele 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 AWS WAF API chamada para remover os endereços IP expirados incluídos no item do conjunto de IPs de destino. 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. Lance 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 AWS WAF IPs. 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. Lance a pilha.
3. Atualize o conjunto de AWS WAF IP 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 AWS WAF IP 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 IPs. WAF

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

Crie um painel de monitoramento

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 CloudWatchPainéis — 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.

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 DDoS ataques 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 DDoS ataque 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 específico de parâmetros de solicitação).
- ELBTransbordamento e comprimento da fila — Ajuda a verificar se um DDoS ataque está causando danos à infraestrutura e se o atacante está contornando CloudFront a AWS WAF camada e atacando diretamente recursos desprotegidos.

- ELBContagem de solicitações — 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.
- ELBHost saudável — Você pode usar isso como outra métrica de verificação de integridade do sistema.
- ASGCPUUtilização — Ajuda a identificar se o invasor está ignorando CloudFront, AWS WAF e o Elastic Load Balancing. Você também pode usar essa métrica para identificar os danos de um ataque.

Lidar com XSS falsos positivos

Essa solução configura uma AWS WAF regra 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 escrevam e enviemHTML, 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 XSS regra padrão para URL padrões específicos que aceitam entrada de rich text e implemente mecanismos alternativos para proteger os excluídosURLs.

Além disso, alguns formatos de imagem ou dados personalizados podem causar falsos positivos porque contêm padrões que indicam um possível XSS ataque no HTML conteúdo. Por exemplo, um SVG arquivo pode conter uma `<script>` tag. Se você espera esse tipo de conteúdo de usuários legítimos, adapte suas XSS regras de forma restrita para permitir HTML solicitações que incluam esses outros formatos de dados.

Conclua as etapas a seguir para atualizar a XSS regra e excluir URLs essa aceitação HTML como entrada. Consulte o Amazon WAF Developer Guide 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 URI e listar os valores que você deseja aceitar em relação à XSS regra.
4. Edite a XSSregra 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
- XSSLista de permissões

Solução de problemas

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

Contato AWS Support

Se você tem AWSDeveloper Support, AWS Business Support ou AWSEnterprise 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. Para Serviço, selecione WAFou AWS WAF.
3. Em Categoria, selecione Automações WAFde segurança ou Automações de segurança para. 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 AWS Support necessárias 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 GitHubrepositório para baixar os modelos e scripts dessa solução e compartilhar suas personalizações com outras pessoas.

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 uma opção para a qual enviar métricas operacionais 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 AWS durante a implantação inicial do CloudFormation modelo:

- ID da solução — O identificador da AWS solução
- ID exclusivo (UUID) — Identificador exclusivo gerado aleatoriamente para cada implantação desta 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 e no HTTPFlood IP 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
- Acesse os dados do manipulador:
  - O número de endereços IP no conjunto de IPs do Bad Bot
  - 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

AWS possui os dados coletados por meio desta pesquisa. A coleta de dados está sujeita à AWS Política de Privacidade. Para desativar esse recurso, conclua as etapas a seguir antes de iniciar o AWS CloudFormation modelo.

1. Faça o download `aws-waf-security-automations.template` AWS CloudFormationpara o 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 console do AWS CloudFormation.
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. Lance a pilha.

Recursos relacionados

Documentos AWS técnicos associados

- AWS Melhores práticas para DDoS resiliência

Publicações do blog de AWS segurança associadas

- Como evitar links diretos usando a AWS WAF Amazon e a verificação CloudFront de referências

Listas de reputação de IP de terceiros

- Site da Lista Spamhaus DROP
- 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

Revisões

Data	Alteração
Setembro de 2016	Lançamento inicial
Janeiro de 2017	Esclarecimento sobre os limites de endereço IP nesta solução.
Março de 2017	Orientação adicional sobre a criação de um comportamento de cache; atualizada URLs para postagens no Blog de AWS Segurança.
Junho de 2017	ALBSuporte adicionado e limites atualizados do produto.
30 de novembro de 2017	Foi adicionado suporte a regras baseadas em taxas para proteção contra HTTP inundaçõe s; links adicionais para armazenar registros de acesso a recursos.
Janeiro de 2018	Conteúdo atualizado sobre a disponibilidade regional do AWS WAF para Application Load Balancers.
Dezembro de 2018	Adicionou IPv6 Support, expandiu os CIDR intervalos e adicionou um painel de monitoram ento.
Abril de 2019	AWS WAF integração de registros, integraçã o com o Amazon Athena e adição de um analisador de registros configurável.
Dezembro de 2019	Foram adicionadas informações sobre o suporte para a atualização do Node.js.
Fevereiro de 2020	Correções de erros e atualização do RequestThreshold parâmetro.

Data	Alteração
Junho de 2020	Foi adicionada a otimização de custos do Athena usando particionamento; README instruções atualizadas; corrigiu um possível problema de DoS no cabeçalho Bad Bots. X-Forward-For
Julho de 2020	Atualizado do serviço AWS WAF Classic para o AWS WAF V2. API
Novembro de 2020	Versão de lançamento 3.1.0: esclareci mento sobre as regras de proteção contra HTTP inundações e proteção de scanners e sondas para regiões específicas; substituiu o tipo de caminho S3 pelo estilo hospedado virtualmente; adicionou variável de partição a todasARNs; para obter mais informaçõ es, consulte o arquivo.md no repositório. CHANGELOG GitHub
Setembro de 2021	Versão de lançamento 3.2.0: suporte de retenção de IP adicionado em conjuntos de IP permitidos e negados; correções de bugs. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositór io.
Agosto de 2022	Versão de lançamento 3.2.1: suporte adicionad o ao tratamento de WAF grandes dimensões para componentes de solicitação; suporte adicionado WAF aos níveis de sensibilidade para declarações de regras de SQL injeção. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositór io.

Data	Alteração
Setembro de 2022	Documentação atualizada para personalização fora da CloudFormation pilha da solução.
Dezembro de 2022	Versão de lançamento 3.2.2: integração adicionada com o Service Catalog AppRegistry e o AWS Systems Manager Application Manager. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Dezembro de 2022	Versão de lançamento 3.2.3: adicione região como prefixo ao nome do grupo de atributos do aplicativo para evitar conflito com o nome que começa com. AWS Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Fevereiro de 2023	Versão de lançamento 3.2.4: pytest atualizado e solicitações para mitigar. CVE Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Março de 2023	Documentação atualizada para atualizar a solução da versão 3.0 ou 3.1 para a 3.2 ou mais recente que tenha endereços IP permitidos ou negados.
Abril de 2023	Versão de lançamento 3.2.5: Impacto mitigado causado pelas novas configurações padrão de propriedade de objetos do Amazon S3 (ACLsdesativada) para todos os novos buckets do Amazon S3. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.

Data	Alteração
Maio de 2023	Versão de lançamento 4.0.0: suporte adicionado para novos grupos de AWS Managed Rules regras e regras personalizadas atualizadas. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Maio de 2023	Versão de lançamento 4.0.1: `.gitignore` Arquivo atualizado para resolver o problema de arquivos ausentes. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Setembro de 2023	Versão de lançamento 4.0.2: código refatorado para melhorar a qualidade. Vulnerabilidade corrigida do pacote de solicitações. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Outubro de 2023	Versão 4.0.3: versões atualizadas do pacote para resolver vulnerabilidades de segurança. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Novembro de 2023	Atualização da documentação: Adicionado o AWS Developer Support e mesclado o Contact AWS Support na seção Solução de problemas.
Novembro de 2023	Atualização da documentação: foi adicionada a seção Confirmar as etiquetas de custo associadas à solução na AppRegistry seção Monitorando a solução com o AWS Service Catalog.

Data	Alteração
Abril de 2024	Atualização da documentação: instruções esclarecidas para adicionar um bucket S3 na etapa 3 de implantação.
Setembro de 2024	Versão de lançamento 4.0.4: versões atualizadas do pacote para resolver vulnerabilidades de segurança. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.
Outubro de 2024	Versão de lançamento 4.0.5: Poesia usada para gerenciamento de dependências. O registrador Python nativo foi substituído pelo registrador aws_lambda_powertools. Para obter mais informações, consulte o CHANGELOG arquivo.md no GitHub repositório.
Dezembro de 2024	Versão de lançamento 4.0.6: atualize o lambda para python 3.12. Para obter mais informações, consulte o CHANGELOGarquivo.md no GitHub repositório.

Avisos

Este guia de implementação é fornecido apenas para fins informativos. Representa as ofertas e práticas atuais de AWS produtos 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 de AWS produtos ou serviços, cada um dos quais é fornecido “no estado em que se encontra”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria nenhuma garantia, representação, compromisso contratual, condição ou garantia de suas afiliadasAWS, fornecedores ou licenciadores. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte de, nem modifica, qualquer contrato entre a AWS e seus clientes.

A AWS WAF solução Security Automations for 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.