Leitfaden zur Implementierung

Sicherheitsautomatisierungen für AWS WAF

Sicherheitsautomatisierungen für AWS WAF: Leitfaden zur Implementierung

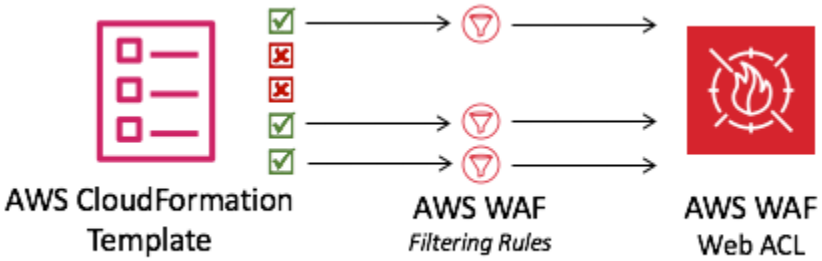
Table of Contents

Stellen Sie mit Security Automations auf AWS WAF automatisch eine einzige Web-Zugriffskontrollliste bereit, die webbasierte Angriffe filtert

Die WAF-Lösung Security Automations for AWS stellt eine Reihe vorkonfigurierter Regeln bereit, mit denen Sie Ihre Anwendungen vor häufigen Web-Exploits schützen können. Der Kernservice dieser Lösung, AWS WAF, schützt Webanwendungen vor Angriffstechniken, die die Verfügbarkeit von Anwendungen beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. Sie können AWS WAF verwenden, um anpassbare Web-Sicherheitsregeln zu definieren. Diese Regeln steuern, welcher Datenverkehr für Webanwendungen und Anwendungsprogrammierschnittstellen (APIs), die auf AWS-Ressourcen wie Amazon CloudFront, Application Load Balancer (ALB) bereitgestellt werden, zugelassen oder blockiert wird. Weitere unterstützte Ressourcentypen finden Sie unter AWS WAF im AWS WAF, AWS Firewall Manager und AWS Shield Advanced Developer Guide.

Die Konfiguration von AWS-WAF-Regeln kann für große und kleine Unternehmen gleichermaßen herausfordernd und belastend sein, insbesondere für Unternehmen, die keine eigenen Sicherheitsteams haben. Um diesen Prozess zu vereinfachen, stellt die Lösung Security Automations for AWS WAF automatisch eine einzige Web Access Control List (ACL) mit einer Reihe von AWS-WAF-Regeln bereit, die darauf ausgelegt sind, gängige webbasierte Angriffe zu filtern. Bei der Erstkonfiguration der CloudFormationAWS-Vorlage dieser Lösung können Sie angeben, welche Schutzfunktionen enthalten sein sollen. Nachdem Sie diese Lösung bereitgestellt haben, überprüft AWS WAF Webanfragen an ihre bestehenden CloudFront Distributionen oder ALB (s) und blockiert sie gegebenenfalls.

Eine CloudFormation Vorlage stellt eine Web-ACL mit AWS-WAF-Filterregeln bereit.



In diesem Implementierungsleitfaden werden architektonische Überlegungen, Konfigurationsschritte und betriebliche Best Practices für die Bereitstellung dieser Lösung in der Amazon Web Services

(AWS) Cloud erörtert. Es enthält Links zu CloudFormation Vorlagen, mit denen die AWS-Sicherheits-, Rechen-, Speicher- und anderen Services gestartet, konfiguriert und ausgeführt werden, die für die Bereitstellung dieser Lösung auf AWS erforderlich sind, wobei die bewährten AWS-Methoden für Sicherheit und Verfügbarkeit verwendet werden.

Die Informationen in diesem Handbuch setzen praktische Kenntnisse über AWS-Services wie AWS WAF, CloudFront ALBs, und AWS Lambda voraus. Außerdem sind Grundkenntnisse gängiger webbasierter Angriffe und Strategien zur Schadensbegrenzung erforderlich.

> **Note**
>
> Ab Version 3.0.0 unterstützt diese Lösung die neueste Version der AWS WAF Service API (AWS WAFV2).

Dieses Handbuch richtet sich an IT-Manager, Sicherheitsingenieure, DevOps Ingenieure, Entwickler, Lösungsarchitekten und Website-Administratoren.

> **Note**
>
> Wir empfehlen, diese Lösung als Ausgangspunkt für die Implementierung von AWS-WAF-Regeln zu verwenden. Sie können den Quellcode anpassen, neue benutzerdefinierte Regeln hinzufügen und je nach Bedarf weitere von AWS WAF verwaltete Regeln nutzen.

Verwenden Sie diese Navigationstabelle, um schnell Antworten auf diese Fragen zu finden:

Wenn du willst.	Lesen.
Informieren Sie sich über die Kosten für den Betrieb dieser Lösung. Die Gesamtkosten für den Betrieb dieser Lösung hängen vom aktiviert en Schutz und der Menge der aufgenomm enen, gespeicherten und verarbeiteten Daten ab.	Kosten
Machen Sie sich mit den Sicherheitsüberleg ungen für diese Lösung vertraut.	Sicherheit

Wenn du willst.	Lesen.
Erfahren Sie, welche AWS-Regionen für diese Lösung unterstützt werden.	Unterstützte AWS-Regionen
Sehen Sie sich die in dieser Lösung enthaltene CloudFormation Vorlage an oder laden Sie sie herunter, um die Infrastrukturressourcen (den „Stack“) für diese Lösung automatisch bereitzustellen.	CloudFormation AWS-Vorlage
Nutzen Sie den Support, um Sie bei der Bereitstellung, Verwendung oder Fehlerbehebung der Lösung zu unterstützen.	Support
Greifen Sie auf den Quellcode zu und verwenden Sie optional das AWS Cloud Development Kit (AWS CDK), um die Lösung bereitzustellen	GitHub Repository

Features und Vorteile

Die WAF-Lösung Security Automations for AWS bietet die folgenden Funktionen und Vorteile.

Schützen Sie Ihre Webanwendungen mit Regelgruppen von AWS Managed Rules

AWS Managed Rules for AWS WAF bietet Schutz vor häufigen Anwendungsschwachstellen oder anderem unerwünschten Datenverkehr. Diese Lösung umfasst AWS Managed IP-Reputationsregelgruppen, AWS Managed-Basisregelgruppen und AWS Managed anwendungsfallspezifische Regelgruppen. Sie haben die Möglichkeit, eine oder mehrere Regelgruppen für Ihre Web-ACL bis zum maximalen WCU-Kontingent (Web ACL Capacity Unit) auszuwählen.

Sorgen Sie mit einer vordefinierten benutzerdefinierten HTTP-Flood-Regel für Hochwasserschutz auf Ebene 7

Die benutzerdefinierte HTTP Flood-Regel schützt für einen vom Kunden definierten Zeitraum vor einem Distributed Denial-of-Service (DDoS) -Angriff auf Webebene. Sie können eine der folgenden Optionen wählen, um diese Regel zu aktivieren:

- Ratenbasierte AWS-WAF-Regel
- Lambda-Protokollparser
- Amazon Athena Athena-Protokollparser

Mit den Optionen Lambda Log Parser oder Athena Log Parser können Sie ein Anforderungskontingent von weniger als 100 definieren. Dieser Ansatz kann dazu beitragen, dass Sie das von den ratenbasierten AWS-WAF-Regeln geforderte Kontingent nicht erreichen. Weitere Informationen finden Sie unter Log-Parser-Optionen.

Sie können den Athena-Protokollparser auch erweitern, indem Sie den Filterbedingungen ein Land und einen Uniform Resource Identifier (URI) hinzufügen. Dieser Ansatz identifiziert und blockiert HTTP-Flood-Angriffe mit unvorhersehbaren URI-Mustern. Weitere Informationen finden Sie unter Land und URI im HTTP Flood Athena-Protokollparser verwenden.

Blockieren Sie die Ausnutzung von Sicherheitslücken mit einer vordefinierten benutzerdefinierten Regel für Scanner & Probes

Die benutzerdefinierte Regel Scanners & Probes analysiert Anwendungszugriffsprotokolle und sucht nach verdächtigem Verhalten, wie z. B. einer ungewöhnlich hohen Anzahl von Fehlern, die durch einen Ursprung verursacht wurden. Anschließend werden diese verdächtigen Quell-IP-Adressen für einen vom Kunden festgelegten Zeitraum gesperrt. Sie können eine der folgenden Optionen wählen, um diese Regel zu aktivieren: Lambda Log Parser oder Athena Log Parser. Weitere Informationen finden Sie unter Log-Parser-Optionen.

Erkennen und verhindern Sie Eindringversuche mit einer vordefinierten, benutzerdefinierten Bad Bot-Regel

Die benutzerdefinierte Bad Bot-Regel richtet einen Honeypot-Endpunkt ein. Dabei handelt es sich um einen Sicherheitsmechanismus, mit dem ein versuchter Angriff verlockt und abgewehrt werden soll.

Sie können den Endpunkt in Ihre Website einfügen, um eingehende Anfragen von Content Scrapern und bösartigen Bots zu erkennen. Sobald sie erkannt wurden, werden alle nachfolgenden Anfragen derselben Herkunft blockiert. Weitere Informationen finden Sie unter Den Honeypot-Link in Ihre Webanwendung einbetten.

Blockieren Sie bösartige IP-Adressen mit vordefinierten IP-Reputationslisten (benutzerdefinierte Regel)

Die benutzerdefinierte Regel für IP-Reputationslisten überprüft stündlich IP-Reputationslisten von Drittanbietern auf neue IP-Bereiche, die gesperrt werden sollen. Zu diesen Listen gehören die Spamhaus-Listen Don't Route Or Peer (DROP) und Extended DROP (EDROP), die Proofpoint Emerging Threats IP-Liste und die Tor-Exit-Knotenliste.

Stellen Sie eine manuelle IP-Konfiguration mit vordefinierten Listen erlaubter und verweigerter IP-Adressen und benutzerdefinierter Regel bereit

Mit den benutzerdefinierten Regeln für Listen zugelassener und verweigerter IP-Adressen können Sie IP-Adressen, die Sie zulassen oder verweigern möchten, manuell einfügen. Sie können die IP-Aufbewahrung auch für Listen mit zulässigen und verweigerten IP-Adressen so konfigurieren, dass sie zu einem bestimmten IPs Zeitpunkt ablaufen.

Erstellen Sie Ihr eigenes Monitoring-Dashboard

Diese Lösung gibt CloudWatchAmazon-Metriken wie zulässige Anfragen, blockierte Anfragen und andere relevante Metriken aus. Sie können ein benutzerdefiniertes Dashboard erstellen, um diese Metriken zu visualisieren und Einblicke in die Angriffsmuster und den Schutz von AWS WAF zu erhalten. Weitere Informationen finden Sie unter Monitoring-Dashboard erstellen.

Anwendungsfälle

Im Folgenden finden Sie Beispiele für Anwendungsfälle für die Verwendung dieser Lösung. Sie können diese Lösung auf innovative Weise anpassen, die nicht auf diese Liste beschränkt ist.

Automatisieren Sie die Einrichtung von AWS-WAF-Regeln

AWS WAF schützt Ihre Webanwendung vor häufigen Angriffen. Die Einrichtung von AWS WAF WAF-Regeln kann jedoch kompliziert und zeitaufwändig sein. Um Ihnen zu helfen, stellt diese Lösung automatisch eine Reihe von AWS-WAF-Regeln mit einer CloudFormation Vorlage in Ihrem Konto

bereit. Auf diese Weise müssen Sie die AWS-WAF-Regeln nicht selbst konfigurieren und können schneller mit AWS WAF beginnen.

Passen Sie den HTTP-Flood-Schutz der Schicht 7 an

Diese Lösung bietet drei Optionen zur Aktivierung des HTTP-Flood-Schutzes. Sie können die Option auswählen, die Ihren Anforderungen entspricht, um sich vor DDo S-Angriffen zu schützen. Weitere Informationen finden Sie unter Funktionen und Vorteile unter Bereitstellen von Layer-7-Hochwasserschutz mit einer vordefinierten benutzerdefinierten HTTP-Flood-Regel.

Nutzen Sie den Quellcode, um Anpassungen vorzunehmen oder Ihre eigenen Sicherheitsautomatisierungen zu erstellen

Diese Lösung bietet ein Beispiel für die Verwendung von AWS WAF und anderen Services zur Erstellung von Sicherheitsautomatisierungen in der AWS-Cloud. Dank des Open-Source-Codes können GitHub Sie bequem Anpassungen vornehmen oder Ihre eigenen Sicherheitsautomatisierungen erstellen, die Ihren Anforderungen entsprechen.

Konzepte und Definitionen

In diesem Abschnitt werden die wichtigsten Konzepte beschrieben und die für diese Lösung spezifische Terminologie definiert.

ALB-Protokolle

Diese Lösung verwendet Protokolle für die ALB-Ressource. Die Regel „Scanner & Probe Protection“ in dieser Lösung überprüft diese Protokolle.

Athena-Protokollparser

Amazon Athena ist ein serverloser, interaktiver Analysedienst, der auf Open-Source-Frameworks basiert und Open-Table- und Dateiformate unterstützt. Diese Lösung führt eine geplante Athena-Abfrage aus, um AWS WAF- oder ALB-Protokolle zu überprüfen CloudFront, wenn der Benutzer dies wünschtyes - `Amazon Athena log parser`, wenn er die HTTP Flood Protection-Regel oder die Scanner & Probe Protection-Regel aktiviert, und kann für die Aktivierung des Bad Bot-Schutzes durch Erkennung verwendet werden, die über eine strukturierte Logikkette funktioniert.

AWS-WAF-Regel

Eine AWS-WAF-Regel definiert:

- Wie überprüft man HTTP (S) -Webanfragen
- Die Aktion, die bei einer Anfrage ergriffen werden muss, wenn sie den Inspektionskriterien entspricht

Sie definieren Regeln nur im Kontext einer Regelgruppe oder Web-ACL.

CloudFront logs

Diese Lösung verwendet Protokolle für die CloudFront Ressource. Die Regel Scanner & Probe Protection in dieser Lösung überprüft diese Protokolle.

IP eingestellt

Ein IP-Set bietet eine Sammlung von IP-Adressen und IP-Adressbereichen, die Sie verwenden möchten

zusammen in einer Regelaussage. IP-Sets sind AWS-Ressourcen.

Lambda-Protokollparser

Diese Lösung führt eine Lambda-Funktion aus, die durch ein Objekt vom Amazon Simple Storage Service (Amazon S3) -Ereignis aufgerufen wird. Die Lambda-Funktion initiiert eine Inspektion der AWS WAF- oder ALB-Protokolle CloudFront, wenn der Benutzer dies `yes - AWS Lambda log parser` bei der Aktivierung von HTTP Flood Protection, Scanner & Probe Protection wünscht. Sie kann für die Regel Bad Bot Protection durch Erkennung verwendet werden, die über eine strukturierte Logikkette funktioniert.

Verwaltete Regelgruppen

Verwaltete Regelgruppen sind Sammlungen vordefinierter ready-to-use Regeln, die Verkäufer von AWS und AWS Marketplace für Sie schreiben und verwalten. Die AWS-WAF-Preise gelten für Ihre Nutzung aller verwalteten Regelgruppen.

Ressourcen-/Endpunkttyp

Sie können AWS-Ressourcen mit dem Internet verknüpfen ACLs , um sie zu schützen. Bei diesen Ressourcen handelt es sich CloudFront um ALB-, AWS AppSync -, Amazon Cognito -, AWS App Runner - und AWS Verified Access-Ressourcen. Derzeit unterstützt Amazon diese Lösung CloudFront und ALB.

WAF-Protokolle

Diese Lösung verwendet von AWS WAF generierte Protokolle für die mit der Web-ACL verknüpften Ressourcen. Die Regeln HTTP Flood Protection, Scanner & Probe Protection und Activate Bad Bot Protection für diese Lösung überprüfen diese Protokolle.

WCU

AWS WAF verwendet die Kapazitätseinheiten () der Web Access Control List (ACLWCUs), um die Betriebsressourcen zu berechnen und zu steuern, die für die Ausführung Ihrer Regeln, Regelgruppen und des Internets ACLs erforderlich sind. AWS WAF setzt WCU-Kontingente durch, wenn Sie Ihre Regelgruppen und das Web konfigurieren. ACLs WCUs haben keinen Einfluss darauf, wie AWS WAF den Webverkehr überprüft.

Web-ACL

Eine Web-ACL gibt Ihnen eine genaue Kontrolle über die HTTP (S) -Webanfragen, auf die Ihre geschützte Ressource reagiert.

> **Note**
>
> Eine allgemeine Referenz zu AWS-Begriffen finden Sie im AWS-Glossar.

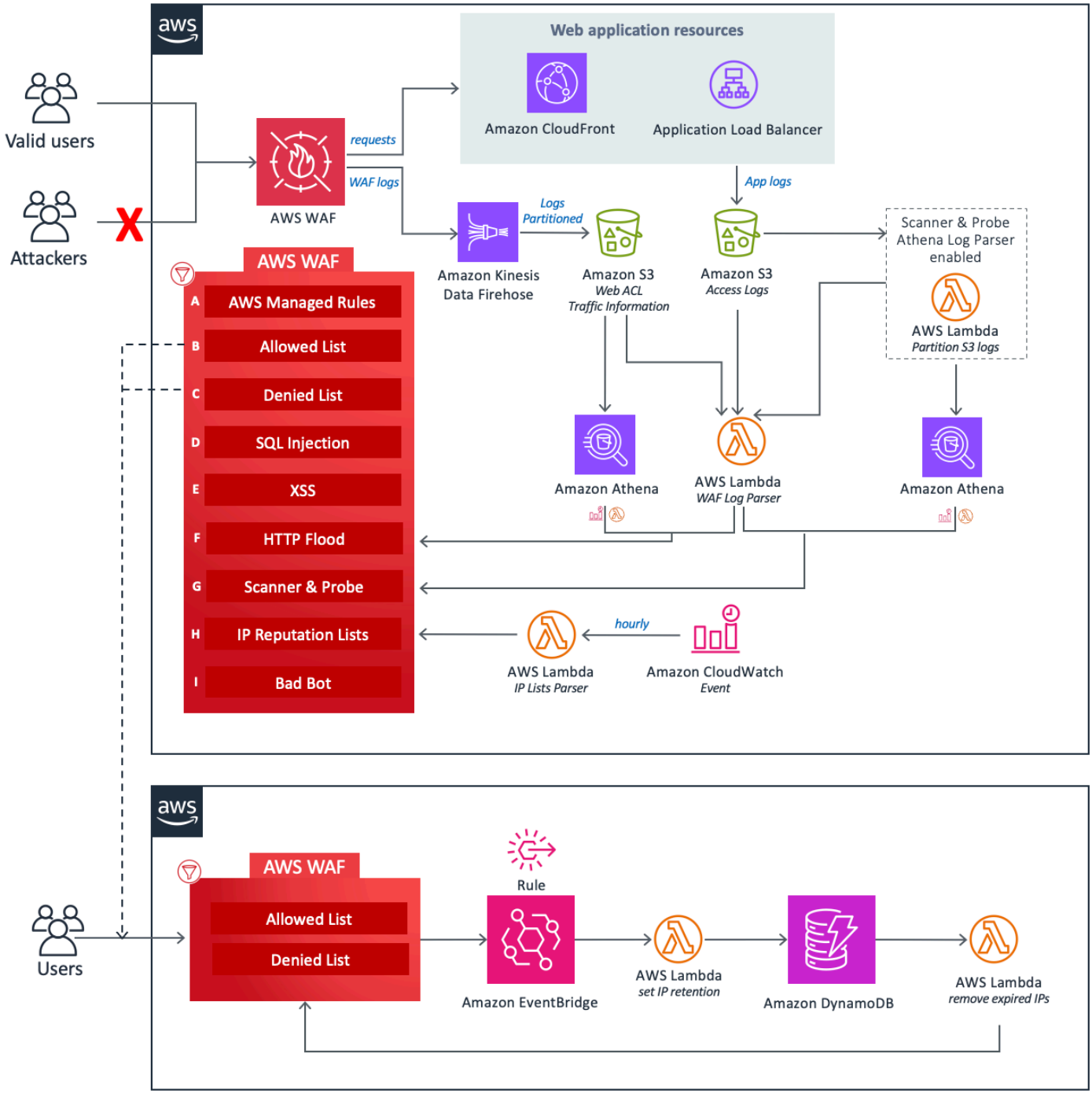
Übersicht über die Architektur

Dieser Abschnitt enthält ein Referenzdiagramm zur Implementierungsarchitektur für die mit dieser Lösung bereitgestellten Komponenten.

Architekturdiagramm

Durch die Bereitstellung dieser Lösung mit den Standardparametern werden die folgenden Komponenten in Ihrem AWS-Konto bereitgestellt.

CloudFormation template stellt AWS WAF und andere AWS-Ressourcen bereit, um Ihre Webanwendung vor häufigen Angriffen zu schützen.



Im Mittelpunkt des Designs steht eine AWS WAF WAF-Web-ACL, die als zentrale Inspektions- und Entscheidungsstelle für alle eingehenden Anfragen an eine Webanwendung fungiert. Bei der Erstkonfiguration des CloudFormation Stacks definiert der Benutzer, welche Schutzkomponenten aktiviert werden sollen. Jede Komponente arbeitet unabhängig und fügt der Web-ACL unterschiedliche Regeln hinzu.

Die Komponenten dieser Lösung lassen sich in die folgenden Schutzbereiche einteilen.

> **Note**
>
> Die Gruppenbezeichnungen spiegeln nicht die Prioritätsstufe der WAF-Regeln wider.

- AWS Managed Rules (A) — Diese Komponente enthält IP-Reputationsregelgruppen von AWS Managed Rules, Basisregelgruppen und anwendungsfallspezifische Regelgruppen. Diese Regelgruppen schützen vor der Ausnutzung häufiger Sicherheitslücken in Anwendungen oder vor anderem unerwünschtem Datenverkehr, einschließlich solcher, die in OWASP-Publikationen beschrieben sind, ohne dass Sie Ihre eigenen Regeln schreiben müssen.
- Manuelle IP-Listen (B und C) — Diese Komponenten erstellen zwei AWS-WAF-Regeln. Mit diesen Regeln können Sie manuell IP-Adressen einfügen, die Sie zulassen oder verweigern möchten. Mithilfe von EventBridgeAmazon-Regeln und Amazon DynamoDB können Sie die IP-Aufbewahrung konfigurieren und abgelaufene IP-Adressen für zulässige oder verweigerte IP-Sets entfernen. Weitere Informationen finden Sie unter Konfiguration der IP-Aufbewahrung für zugelassene und verweigerte AWS-WAF-IP-Sets.
- SQL Injection (D) und XSS (E) — Diese Komponenten konfigurieren zwei AWS-WAF-Regeln, die zum Schutz vor gängigen SQL-Injections- oder Cross-Site-Scripting-Mustern (XSS) in der URI, der Abfragezeichenfolge oder dem Hauptteil einer Anfrage konzipiert sind.
- HTTP Flood (F) — Diese Komponente schützt vor Angriffen, die aus einer großen Anzahl von Anfragen von einer bestimmten IP-Adresse bestehen, wie z. B. einem Web-Layer-S-Angriff oder einem DDo Brute-Force-Anmeldeversuch. Mit dieser Regel legen Sie ein Kontingent fest, das die maximale Anzahl eingehender Anfragen definiert, die von einer einzelnen IP-Adresse innerhalb eines Standardzeitraums von fünf Minuten zulässig sind (konfigurierbar mit dem Parameter Athena Query Run Time Schedule). Wenn dieser Schwellenwert überschritten wird, werden weitere Anfragen von der IP-Adresse vorübergehend blockiert. Sie können diese Regel mithilfe einer ratenbasierten AWS-WAF-Regel oder durch die Verarbeitung von AWS-WAF-Protokollen mithilfe einer Lambda-Funktion oder einer Athena-Abfrage implementieren. Weitere Informationen zu den Kompromissen im Zusammenhang mit den Optionen zur Abwehr von HTTP-Überschwemmungen finden Sie unter Optionen für den Log-Parser.
- Scanner and Probe (G) — Diese Komponente analysiert Anwendungszugriffsprotokolle und sucht nach verdächtigem Verhalten, wie z. B. einer ungewöhnlich hohen Anzahl von Fehlern, die durch einen Ursprung verursacht wurden. Anschließend werden diese verdächtigen Quell-IP-Adressen für einen vom Kunden festgelegten Zeitraum gesperrt. Sie können diese Regel mithilfe

einer Lambda-Funktion oder einer Athena-Abfrage implementieren. Weitere Informationen zu den Kompromissen im Zusammenhang mit den Optionen zur Abwehr von Scannern und Sonden finden Sie unter Optionen für den Log-Parser.

- IP-Reputationslisten (H) — Bei dieser Komponente handelt es sich um die `IP Lists Parser` Lambda-Funktion, die IP-Reputationslisten von Drittanbietern stündlich auf neue Bereiche überprüft, die gesperrt werden sollen. Zu diesen Listen gehören die Spamhaus-Listen Don't Route Or Peer (DROP) und Extended DROP (EDROP), die Proofpoint Emerging Threats IP-Liste und die Tor-Exit-Knotenliste.
- Bad Bot (I) — Diese Komponente verbessert die Erkennung böser Bots, indem sie zusätzlich zum Honeypot-Mechanismus direkte Verbindungen zu einem Application Load Balancer (ALB) oder Amazon CloudFront überwacht. Wenn ein Bot den Honeypot umgeht und versucht, mit ALB oder zu interagieren, analysiert das System Anforderungsmuster und Protokolle CloudFront, um böswillige Aktivitäten zu identifizieren. Wenn ein böser Bot erkannt wird, wird seine IP-Adresse extrahiert und zu einer AWS-WAF-Sperrliste hinzugefügt, um weiteren Zugriff zu verhindern. Die Erkennung bösartiger Bots erfolgt über eine strukturierte Logikkette, die eine umfassende Bedrohungsabdeckung gewährleistet:
  - HTTP Flood Protection Lambda Log Parser — Sammelt schädliche Bot IPs aus Protokolleinträgen während der Hochwasseranalyse.
  - Scanner & Probe Protection Lambda Log Parser — Identifiziert bösartige Bots anhand IPs scannerbezogener Protokolleinträge.
  - HTTP Flood Protection Athena Log Parser — Extrahiert bösartige Bots IPs aus Athena-Protokollen und verwendet dabei Partitionen für den gesamten Abfragelauf.
  - Scanner & Probe Protection Athena Log Parser — Ruft bösartige Bots IPs aus scannerbezogenen Athena-Protokollen ab und verwendet dabei dieselbe Partitionierungsstrategie.
  - Fallback-Erkennung — Wenn sowohl HTTP Flood Protection als auch Scanner & Probe Protection deaktiviert sind, stützt sich das System auf den Log Lambda-Parser, der Bot-Aktivitäten auf der Grundlage von WAF-Labelfiltern protokolliert.

Jede der drei benutzerdefinierten Lambda-Funktionen in dieser Lösung veröffentlicht Laufzeitmetriken auf CloudWatch. Weitere Informationen zu diesen Lambda-Funktionen finden Sie unter Komponentendetails.

Überlegungen zum AWS-Well-Architected-Design

Diese Lösung nutzt die Best Practices des AWS Well-Architected Framework, das Kunden dabei unterstützt, zuverlässige, sichere, effiziente und kostengünstige Workloads in der Cloud zu entwerfen und zu betreiben.

In diesem Abschnitt wird beschrieben, wie die Entwurfsprinzipien und Best Practices des Well-Architected Framework dieser Lösung zugute kommen.

Operative Exzellenz

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers Operational Excellence konzipiert haben.

- Die Lösung nutzt Metriken, CloudWatch um die Infrastruktur, die Lambda-Funktionen, Amazon Data Firehose, Amazon S3 S3-Buckets und die übrigen Lösungskomponenten beobachtbar zu machen.
- Wir entwickeln, testen und veröffentlichen die Lösung über eine AWS-Pipeline für kontinuierliche Integration und kontinuierliche Lieferung (CI/CD). Dies hilft Entwicklern, konsistent qualitativ hochwertige Ergebnisse zu erzielen.
- Sie können die Lösung mit einer CloudFormation Vorlage installieren, die alle erforderlichen Ressourcen in Ihrem Konto bereitstellt. Um die Lösung zu aktualisieren oder zu löschen, müssen Sie nur die Vorlage aktualisieren oder löschen.

Sicherheit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der Sicherheitssäule konzipiert haben.

- Die gesamte dienstübergreifende Kommunikation verwendet AWS Identity and Access Management (IAM) -Rollen.
- Alle von der Lösung verwendeten Rollen folgen dem Zugriff mit den geringsten Rechten. Mit anderen Worten, sie enthalten nur die Mindestberechtigungen, die erforderlich sind, damit der Dienst ordnungsgemäß funktionieren kann.
- Alle Datenspeicher, einschließlich Amazon S3 S3-Buckets und DynamoDB, verfügen über Verschlüsselung im Ruhezustand.

Zuverlässigkeit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der Zuverlässigkeitskomponente konzipiert haben.

- Die Lösung verwendet, wo immer möglich, serverlose AWS-Services (z. B. Lambda, Firehose, Amazon S3 und Athena), um eine hohe Verfügbarkeit und Wiederherstellung nach einem Serviceausfall sicherzustellen.
- Wir führen automatisierte Tests der Lösung durch, um Fehler schnell zu erkennen und zu beheben.
- Die Lösung verwendet Lambda-Funktionen für die Datenverarbeitung. Die Lösung speichert Daten in Amazon S3 und DynamoDB und wird standardmäßig in mehreren Availability Zones gespeichert.

Leistungseffizienz

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers Leistungseffizienz konzipiert haben.

- Die Lösung verwendet eine serverlose Architektur, um eine hohe Skalierbarkeit und Verfügbarkeit bei reduzierten Kosten zu gewährleisten.
- Die Lösung verbessert die Datenbankleistung, indem sie Daten partitioniert und Abfragen optimiert, um den Umfang der Datenscans zu reduzieren und schnellere Ergebnisse zu erzielen.
- Die Lösung wird täglich automatisch getestet und bereitgestellt. Unsere Lösungsarchitekten und Fachexperten überprüfen die Lösung auf Bereiche, in denen experimentiert und verbessert werden muss.

Kostenoptimierung

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren des Pfeilers Kostenoptimierung konzipiert haben.

- Die Lösung verwendet eine serverlose Architektur, und Kunden zahlen nur für das, was sie tatsächlich nutzen.
- Die Rechenschicht der Lösung ist standardmäßig auf Lambda eingestellt, das ein pay-per-use Modell verwendet.
- Die Athena-Datenbank und die Abfragen sind so optimiert, dass weniger Daten gescannt werden müssen und somit die Kosten gesenkt werden.

Nachhaltigkeit

In diesem Abschnitt wird beschrieben, wie wir diese Lösung unter Verwendung der Prinzipien und bewährten Verfahren der Säule Nachhaltigkeit konzipiert haben.

- Die Lösung verwendet verwaltete und serverlose Dienste, um die Umweltbelastung durch die Back-End-Dienste zu minimieren.
- Das serverlose Design der Lösung zielt darauf ab, den CO2-Fußabdruck im Vergleich zu dem Fußabdruck kontinuierlich betriebener Server vor Ort zu reduzieren.

Einzelheiten zur Architektur

In diesem Abschnitt werden die Komponenten und AWS-Services beschrieben, aus denen diese Lösung besteht, sowie die Architekturdetails dazu, wie diese Komponenten zusammenarbeiten.

AWS-Services in dieser Lösung

AWS Service	Description
AWS WAF	Kern. Stellt eine AWS WAF WAF-Web-ACL, Regelgruppen für AWS Managed Rules, benutzerdefinierte Regeln und IP-Sätze bereit. Führt AWS-WAF-API-Aufrufe durch, um häufige Angriffe zu blockieren und Webanwendungen zu schützen.
Amazon Data Firehose	Kern. Liefert AWS-WAF-Protokolle an Amazon S3 S3-Buckets.
Amazon S3	Kern. Speichert AWS WAF CloudFront - und ALB-Protokolle.
AWS Lambda	Kern. Stellt mehrere Lambda-Funktionen zur Unterstützung benutzerdefinierter Regeln bereit.
Amazon EventBridge	Kern. Erstellt Ereignisregeln zum Aufrufen von Lambda.
Amazon Athena	Unterstützend. Erzeugt Athena-Abfragen und Arbeitsgruppen zur Unterstützung des Athena-Protokollparsers.
AWS Glue	Unterstützend. Erstellt Datenbanken und Tabellen zur Unterstützung des Athena-Loggparsers.

AWS Service	Description
Amazon SNS	Unterstützend. Sendet E-Mail-Benachrichtigungen von Amazon Simple Notification Service (Amazon SNS), um die Aufbewahrung von IP-Adressen auf Listen mit erlaubten und verweigerten IP-Adressen zu unterstützen.
AWS Systems Manager	Unterstützend. Bietet Ressourcenüberwachung und Visualisierung von Ressourcenoperationen und Kostendaten auf Anwendungsebene.

Optionen für den Log-Parser

Wie in der Architekturübersicht beschrieben, gibt es drei Optionen für den Umgang mit HTTP-Flood sowie für Scanner- und Probe-Schutzmaßnahmen. In den folgenden Abschnitten wird jede dieser Optionen ausführlicher erläutert.

Preisbasierte AWS-WAF-Regel

Für den HTTP-Hochwasserschutz sind ratenbasierte Regeln verfügbar. Standardmäßig aggregiert und begrenzt eine ratenbasierte Regel Anfragen auf der Grundlage der Anfrage-IP-Adresse. Mit dieser Lösung können Sie die Anzahl der Webanfragen angeben, die eine Client-IP in einem nachfolgenden, kontinuierlich aktualisierten Zeitraum von fünf Minuten zulässt. Wenn eine IP-Adresse das konfigurierte Kontingent überschreitet, blockiert AWS WAF neue blockierte Anfragen, bis die Anforderungsrate unter dem konfigurierten Kontingent liegt.

Wir empfehlen die Auswahl der ratenbasierten Regeloption, wenn das Anforderungskontingent mehr als 2.000 Anfragen pro fünf Minuten beträgt und Sie keine Anpassungen implementieren müssen. Beispielsweise berücksichtigen Sie beim Zählen von Anfragen den statischen Ressourcenzugriff nicht.

Sie können die Regel weiter so konfigurieren, dass sie verschiedene andere Aggregationsschlüssel und Tastenkombinationen verwendet. Weitere Informationen finden Sie unter Aggregationsoptionen und Schlüssel.

Amazon Athena Athena-Protokollparser

Sowohl die Vorlagenparameter HTTP Flood Protection als auch Scanner & Probe Protection bieten die Athena-Log-Parser-Option. Bei Aktivierung werden eine Athena-Abfrage und eine geplante Lambda-Funktion bereitgestellt, CloudFormation die für die Orchestrierung von Athena für die Ausführung, Verarbeitung der Ergebnisausgabe und Aktualisierung von AWS WAF verantwortlich sind. Diese Lambda-Funktion wird durch ein CloudWatch Ereignis aufgerufen, das so konfiguriert ist, dass es alle fünf Minuten ausgeführt wird. Dies ist mit dem Parameter Athena Query Run Time Schedule konfigurierbar.

Wir empfehlen, diese Option zu wählen, wenn Sie die ratenbasierten AWS-WAF-Regeln nicht verwenden können und Sie mit SQL vertraut sind, um Anpassungen zu implementieren. Weitere Informationen zum Ändern der Standardabfrage finden Sie unter Amazon Athena Athena-Abfragen anzeigen.

Der HTTP-Hochwasserschutz basiert auf der Verarbeitung von AWS-WAF-Zugriffsprotokollen und verwendet WAF-Protokolldateien. Der WAF-Zugriffsprotokolltyp hat eine geringere Verzögerungszeit, sodass Sie die Ursprünge von HTTP-Floods im Vergleich zur CloudFront ALB-Protokollzustellungszeit schneller identifizieren können. Sie müssen jedoch im Vorlagenparameter Activate Scanner & Probe Protection den Protokolltyp CloudFront oder ALB auswählen, um Statuscodes für Antworten zu erhalten.

> **Note**
>
> Wenn ein bösartiger Bot den Honeypot umgeht und direkt mit ALB oder interagiert CloudFront, erkennt das System bösartiges Verhalten anhand der Protokollanalyse, es sei denn, sowohl HTTP Flood Protection als auch Scanner & Probe Protection verwenden den Lambda-Protokollparser nicht.

AWS Lambda Lambda-Protokollparser

Die Vorlagenparameter HTTP Flood Protection und Scanner & Probe Protection stellen die AWS Lambda Log Parser-Option bereit. Verwenden Sie den Lambda-Protokollparser nur, wenn die ratenbasierte AWS-WAF-Regel und die Amazon Athena Athena-Protokollparser-Optionen nicht verfügbar sind. Eine bekannte Einschränkung dieser Option besteht darin, dass Informationen im Kontext der verarbeiteten Datei verarbeitet werden. Beispielsweise kann eine IP mehr Anfragen oder Fehler generieren als das definierte Kontingent. Da diese Informationen jedoch in verschiedene

Dateien aufgeteilt sind, speichert jede Datei nicht genügend Daten, um das Kontingent zu überschreiten.

> **Note**
>
> Wenn ein bösartiger Bot den Honeypot umgeht und direkt mit ALB oder interagiert, stützt sich die Erkennung außerdem auf die gewählte Log-Parser-Option CloudFront, um bösartige Aktivitäten effektiv zu identifizieren und zu blockieren.

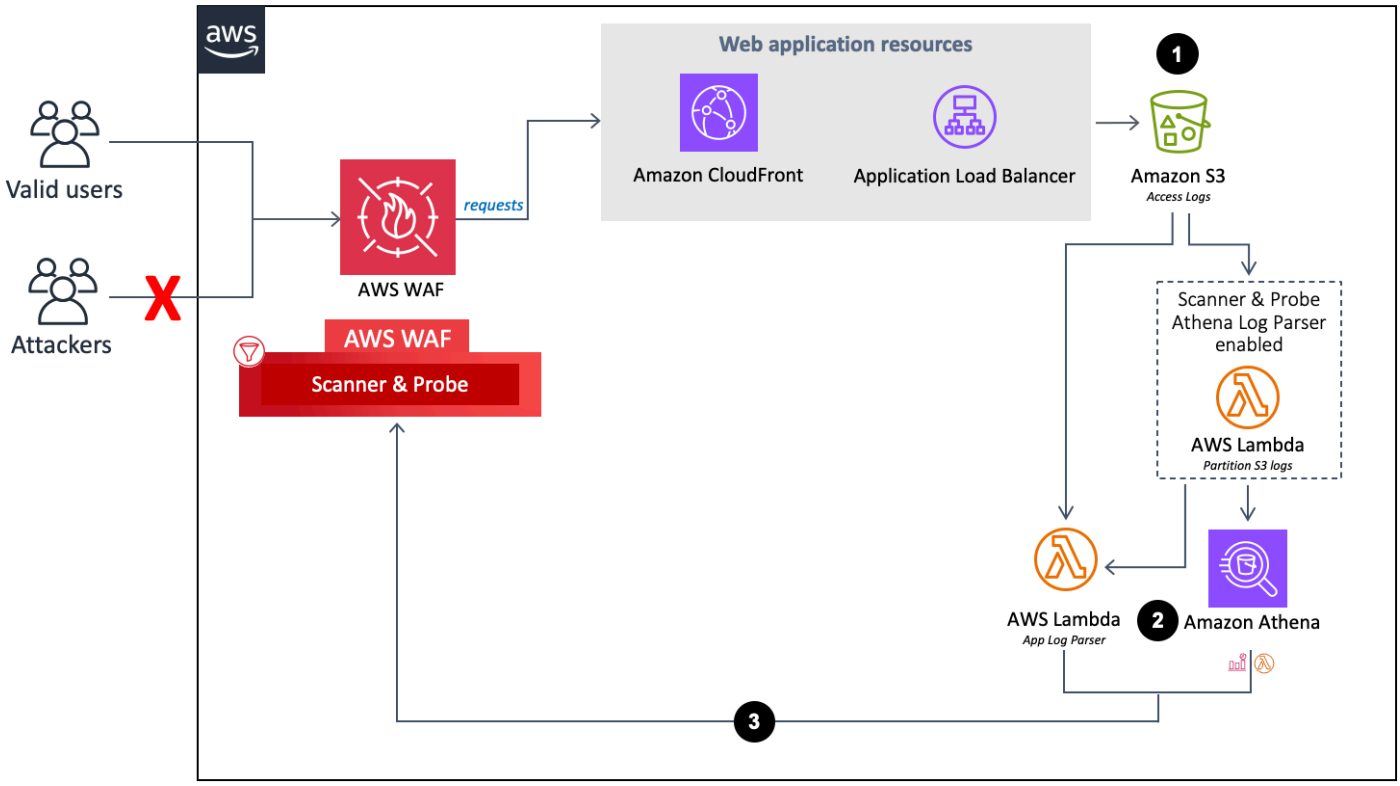
Einzelheiten zu den Komponenten

Wie im Architekturdiagramm beschrieben, verwenden vier der Komponenten dieser Lösung Automatisierungen, um IP-Adressen zu überprüfen und sie der AWS-WAF-Blockliste hinzuzufügen. In den folgenden Abschnitten wird jede dieser Komponenten ausführlicher erläutert.

Log-Parser — Anwendung

Der Anwendungsprotokoll-Parser schützt vor Scannern und Sonden.

Ablauf des Parsers für das Anwendungsprotokoll.



1. Wenn CloudFront oder ein ALB Anfragen im Namen Ihrer Webanwendung empfängt, sendet es Zugriffsprotokolle an einen Amazon S3 S3-Bucket.

   a. (Optional) Wenn Sie `Yes - Amazon Athena log parser` für die Vorlagenparameter Activate HTTP Flood Protection und Activate Scanner & Probe Protection auswählen, verschiebt eine Lambda-Funktion Zugriffsprotokolle von ihrem ursprünglichen Ordner *<customer-bucket>* /AWSLogs in einen neu partitionierten Ordner *<customer-bucket>* /AWSLogs-partitioned/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* /day= *<DD>* / hour=*<HH>*/, sobald sie in Amazon S3 ankommen.

   b. (Optional) Wenn Sie `yes` für den Vorlagenparameter Daten im ursprünglichen S3-Speicherort beibehalten auswählen, verbleiben die Protokolle an ihrem ursprünglichen Speicherort und werden in ihren partitionierten Ordner kopiert, wodurch Ihr Protokollspeicher dupliziert wird.

> **Note**
>
> Für den Athena-Protokollparser partitioniert diese Lösung nur neue Protokolle, die nach der Bereitstellung dieser Lösung in Ihrem Amazon S3 S3-Bucket ankommen. Wenn Sie

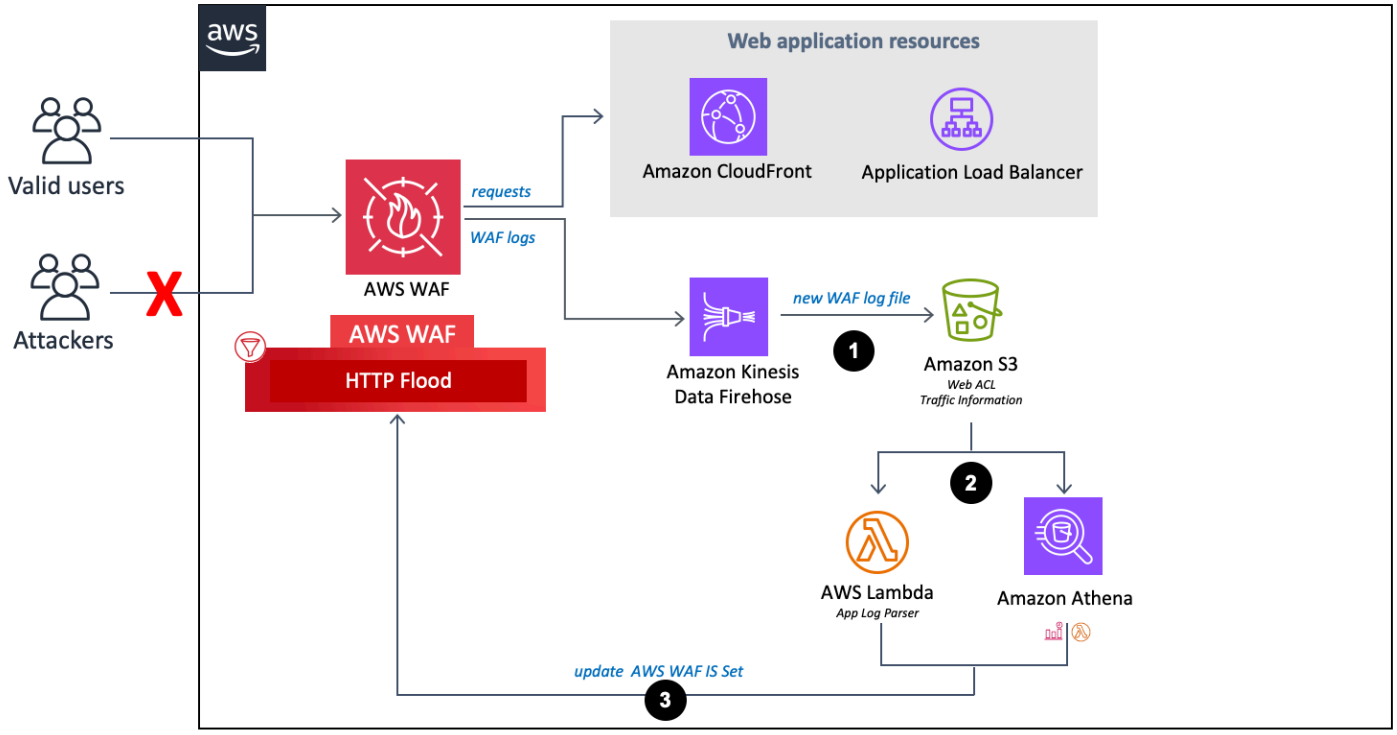
über bestehende Protokolle verfügen, die Sie partitionieren möchten, müssen Sie diese Protokolle nach der Bereitstellung dieser Lösung manuell auf Amazon S3 hochladen.

2. Basierend auf Ihrer Auswahl für die Vorlagenparameter Activate HTTP Flood Protection und Activate Scanner & Probe Protection verarbeitet diese Lösung Protokolle mit einem der folgenden Verfahren:
   a. Lambda — Jedes Mal, wenn ein neues Zugriffsprotokoll im Amazon S3 S3-Bucket gespeichert wird, wird die `Log Parser` Lambda-Funktion initiiert.
   b. Athena — Standardmäßig wird die Scanner & Probe Protection Athena-Abfrage alle fünf Minuten ausgeführt, und die Ausgabe wird an AWS WAF weitergeleitet. Dieser Prozess wird durch ein CloudWatch Ereignis initiiert, das die Lambda-Funktion startet, die für die Ausführung der Athena-Abfrage verantwortlich ist, und das Ergebnis an AWS WAF überträgt.
3. Die Lösung analysiert die Protokolldaten, um IP-Adressen zu identifizieren, die mehr Fehler als das definierte Kontingent generiert haben. Die Lösung aktualisiert dann eine festgelegte AWS-WAF-IP-Set-Bedingung, um diese IP-Adressen für einen vom Kunden definierten Zeitraum zu blockieren.

Protokollparser — AWS WAF

Wenn Sie HTTP Flood Protection aktivieren **`yes - AWS Lambda log parser`** oder `yes - Amazon Athena log parser` auswählen, stellt diese Lösung die folgenden Komponenten bereit, die AWS-WAF-Protokolle analysieren, um Ursprünge zu identifizieren und zu blockieren, die den Endpunkt mit einer Anforderungsrate überfluten, die das von Ihnen definierte Kontingent übersteigt.

Ablauf des AWS WAF WAF-Protokollparsers.

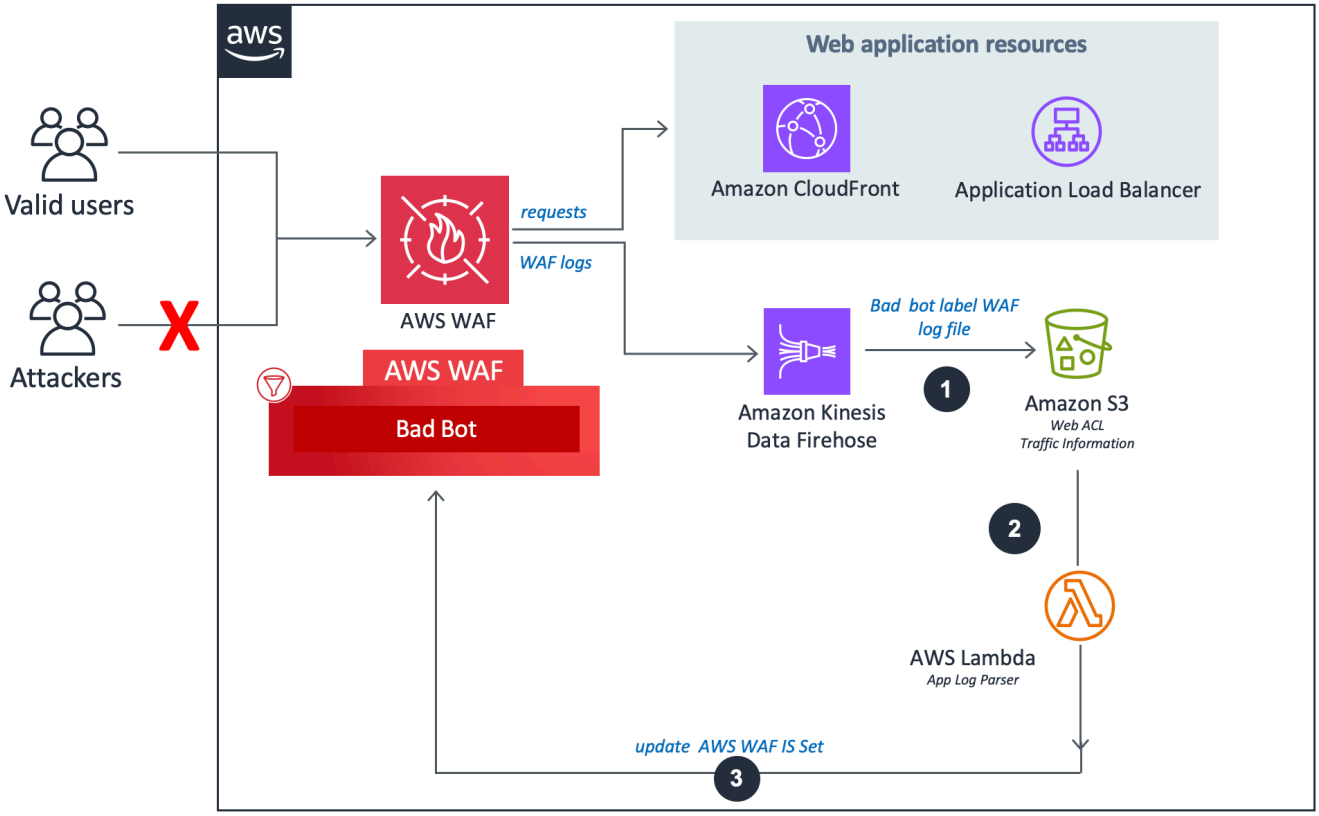


1. Wenn AWS WAF Zugriffsprotokolle empfängt, sendet sie die Protokolle an einen Firehose-Endpunkt. Firehose liefert die Protokolle dann an einen partitionierten Bucket in Amazon S3 mit dem Namen *<customer-bucket>* /AWSLogs/ *<optional-prefix>* /year= *<YYYY>* / month= *<MM>* /day= *<DD>* /hour= *<HH>* /
2. Basierend auf Ihrer Auswahl für die Vorlagenparameter „HTTP Flood Protection aktivieren“ und „Scanner & Probe Protection aktivieren“ verarbeitet diese Lösung Protokolle mit einem der folgenden Verfahren:
   a. Lambda: Jedes Mal, wenn ein neues Zugriffsprotokoll im Amazon S3 S3-Bucket gespeichert wird, wird die `Log Parser` Lambda-Funktion initiiert.
   b. Athena: Standardmäßig werden alle fünf Minuten die Scanner- und Sonden-Athena-Abfrage ausgeführt und die Ausgabe wird an AWS WAF übertragen. Dieser Prozess wird durch ein CloudWatch Amazon-Ereignis initiiert, das dann die Lambda-Funktion startet, die für die Ausführung der Amazon Athena-Abfrage verantwortlich ist, und das Ergebnis in AWS WAF überträgt.
3. Die Lösung analysiert die Protokolldaten, um IP-Adressen zu identifizieren, die mehr Anfragen als das definierte Kontingent gesendet haben. Die Lösung aktualisiert dann eine festgelegte AWS-WAF-IP-Set-Bedingung, um diese IP-Adressen für einen vom Kunden definierten Zeitraum zu blockieren.

Log-Parser — Schlechter Bot

Der Bad Bot Log Parser untersucht Anfragen an den Honeypot-Endpunkt, um deren Quell-IP-Adresse zu extrahieren.

Fehlerhafter Bot-Log-Parser-Flow.

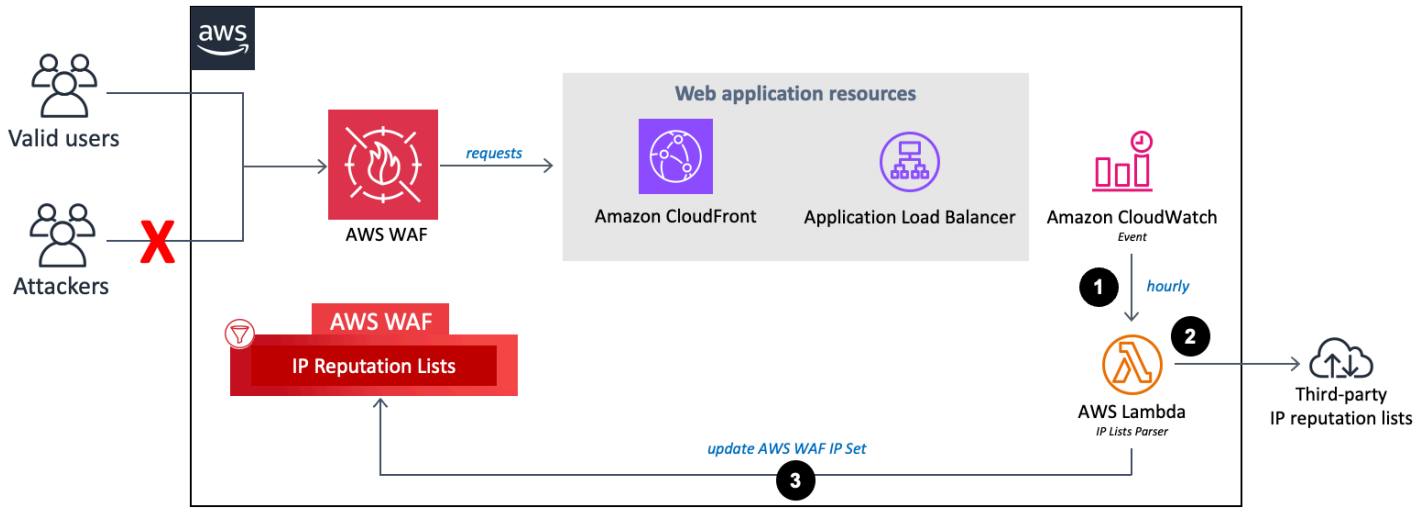


1. Wenn aktiviert `Bad Bot Protection` ist und sowohl die Funktionen HTTP Flood Protection als auch Scanner & Probe Protection deaktiviert sind: Das System verwendet den Log Lambda-Parser, der nur bösartige Bot-Anfragen auf der Grundlage von WAF-Labelfiltern protokolliert.
2. Die Lambda-Funktion fängt Anforderungsheader ab und untersucht sie, um die IP-Adresse der Quelle zu extrahieren, die auf den Trap-Endpunkt zugegriffen hat.
3. Die Lösung analysiert die Protokolldaten, um IP-Adressen zu identifizieren, die mehr Anfragen als das definierte Kontingent gesendet haben. Die Lösung aktualisiert dann eine festgelegte AWS-WAF-IP-Set-Bedingung, um diese IP-Adressen für einen vom Kunden definierten Zeitraum zu blockieren.

Parser für IP-Listen

Die `IP Lists Parser` Lambda-Funktion schützt vor bekannten Angreifern, die in IP-Reputationslisten von Drittanbietern identifiziert wurden.

Die IP-Reputation listet den Parser-Flow auf.



1. Ein stündliches CloudWatch Amazon-Ereignis ruft die `IP Lists Parser` Lambda-Funktion auf.
2. Die Lambda-Funktion sammelt und analysiert Daten aus drei Quellen:
   - DROP- und EDROP-Listen von Spamhaus
   - IP-Liste neuer Bedrohungen von Proofpoint
   - Liste der Tor-Exit-Knoten
3. Die Lambda-Funktion aktualisiert die AWS-WAF-Blockliste mit den aktuellen IP-Adressen.

Planen Sie Ihren Einsatz

In diesem Abschnitt werden die Kosten, die Sicherheit, die Kontingente und andere Überlegungen vor der Bereitstellung der Lösung beschrieben.

Unterstützte AWS Regionen

Abhängig von den von Ihnen definierten Werten für die Eingabeparameter der Vorlage benötigt diese Lösung unterschiedliche Ressourcen. Diese Ressourcen (in der folgenden Tabelle aufgeführt) sind möglicherweise nicht in allen AWS-Regionen verfügbar. Daher müssen Sie diese Lösung in einer AWS-Region starten, in der diese Services verfügbar sind. Die aktuelle Verfügbarkeit von AWS-Services nach Regionen finden Sie in der regionalen AWS-Serviceliste.

	AWS WAF-Web-ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Endpunkttyp				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
Aktivieren Sie den HTTP-Flood-Schutz				
ja — AWS Lambda Lambda-Protokollparser				✓
ja — Amazon Athena Athena-Protokollparser		✓	✓	✓
Aktivieren Sie den Scanner-				

	AWS WAF-Web-ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
und Sondensch utz				
ja — Amazon Athena Athena-Protokollparser		✓	✓	

> **Note**
>
> Wenn Sie sich für Ihren Endpunkt entscheiden`CloudFront`, müssen Sie die Lösung in der Region USA Ost (Nord-Virginia) bereitstellen (`us-east-1`).

Cost (Kosten)

Sie sind für die Kosten der AWS-Services verantwortlich, die beim Betrieb der WAF-Lösung Security Automations for AWS verwendet werden. Die Gesamtkosten für den Betrieb dieser Lösung hängen vom aktivierten Schutz und der Menge der aufgenommenen, gespeicherten und verarbeiteten Daten ab.

Wir empfehlen, über den AWS Cost Explorer ein Budget zu erstellen, um die Kosten besser verwalten zu können. Vollständige Informationen finden Sie auf der Preisseite für jeden AWS-Service, den Sie in dieser Lösung verwendet haben.

Die folgenden Tabellen sind Beispiele für die Aufschlüsselung der Kosten für den Betrieb dieser Lösung in der Region USA Ost (Nord-Virginia) (ohne das kostenlose AWS-Kontingent). Die Preise sind freibleibend.

Beispiel 1: Reputation List Protection, Bad Bot Protection, AWS Lambda Log Parser für HTTP Flood Protection und Scanner & Probe Protection aktivieren

AWS Service	Abmessungen/Monat	Kosten [USD]
Amazon Data Firehose	100 GB	~2,90 $

AWS Service	Abmessungen/Monat	Kosten [USD]
Amazon S3	100 GB	~2,30 $
AWS Lambda	128 MB: 3 Funktionen, 1 Million Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf 512 MB: 2 Funktionen, 1 Million Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf	~5,40 $
AWS WAF WAF-Web-ACL	1	5,00$
AWS-WAF-Regel	4	4,00$
AWS WAF WAF-Anfrage	1 Mio.	0,60$
Gesamt		~20,60 $ pro Monat

Beispiel 2: Reputation List Protection, Bad Bot Protection, Amazon Athena Log Parser für HTTP Flood Protection und Scanner & Probe Protection aktivieren

AWS Service	Abmessungen/Monat	Kosten [USD]
Amazon Data Firehose	100 GB	~2,90 $
Amazon S3	100 GB	~2,30 $
AWS Lambda	128 MB: 3 Funktionen, 1 Million Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf	~1,26 $

AWS Service	Abmessungen/Monat	Kosten [USD]
	512 MB: 2 Funktionen, 7560 Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf	
Amazon Athena	1,2 Mio. CloudFront Objektzugriffe oder 1,2 Mio. ALB-Anfragen pro Tag, wodurch pro Treffer oder Anfrage ein Protokolldatensatz von ~500 Byte generiert wird	~4,32 $
AWS WAF WAF-Web-ACL	1	5,00$
AWS-WAF-Regel	4	4,00$
AWS WAF WAF-Anfrage	1 Mio.	0,60$
Gesamt		~20,38 $ pro Monat

Beispiel 3: Aktivieren Sie die IP-Aufbewahrung für erlaubte und verweigerte IP-Sets

AWS Service	Abmessungen/Monat	Kosten [USD]
Amazon DynamoDB	1.000 Schreibvorgänge und 1 MB Datenspeicher	~0,00 $
AWS Lambda	128 MB: 1 Funktion, 2.000 Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf 512 MB: 1 Funktion, 2.000 Aufrufe und durchschnittliche Dauer von 500 Millisekunden pro Lambda-Lauf	~0,01 $

AWS Service	Abmessungen/Monat	Kosten [USD]
Amazon CloudWatch	2K-Ereignisse	~0,00 $
AWS WAF-Web-ACL	1	5,00$
AWS-WAF-Regel	2	2,00$
WAS WAF-Anfrage	1 Mio.	0,60$
Gesamt		~7,61 $ pro Monat

Kostenschätzung für Logs CloudWatch

Einige in dieser Lösung verwendete AWS-Services, wie Lambda, generieren CloudWatch Protokolle. Für diese Protokolle fallen Gebühren an. Wir empfehlen, Protokolle zu löschen oder zu archivieren, um die Kosten zu senken. Einzelheiten zum Protokollarchiv finden Sie unter Exportieren von Protokolldaten nach Amazon S3 im Amazon CloudWatch Logs-Benutzerhandbuch.

Wenn Sie sich dafür entscheiden, den Athena-Protokollparser bei der Installation zu verwenden, plant diese Lösung, dass eine Abfrage anhand der AWS WAF- oder Anwendungszugriffsprotokolle in Ihren Amazon S3 S3-Buckets wie konfiguriert ausgeführt wird. Die Gebühren richten sich nach der Menge der bei jeder Abfrage gescannten Daten. Die Lösung partitioniert Protokolle und Abfragen, um die Kosten zu minimieren. Standardmäßig verschiebt die Lösung Anwendungszugriffsprotokolle von ihrem ursprünglichen Amazon S3 S3-Speicherort in eine partitionierte Ordnerstruktur. Sie können auch das Original behalten, der doppelte Protokollspeicher wird Ihnen jedoch in Rechnung gestellt. Diese Lösung verwendet Arbeitsgruppen, um Arbeitslasten zu segmentieren, und Sie können beide konfigurieren, um den Abfragezugriff und die Kosten zu verwalten. Ein Beispiel für eine Berechnung eines Kostenvoranschlags finden Sie unter Kostenvoranschlag von Athena. Weitere Informationen finden Sie unter Amazon Athena Pricing.

Kostenvoranschlag von Athena

Wenn Sie die Athena Log Parser-Option verwenden, während Sie die Regeln HTTP Flood Protection, Scanner & Probe Protection oder Bad Bot Protection ausführen, wird Ihnen die Nutzung von Athena in Rechnung gestellt. Standardmäßig wird jede Athena-Abfrage alle fünf Minuten ausgeführt und scannt die Daten der letzten vier Stunden. Die Lösung wendet Partitionierung auf Protokolle und Athena-Abfragen an, um die Kosten zu minimieren. Sie können die Anzahl der Datenstunden, die

eine Abfrage scannt, konfigurieren, indem Sie den Wert für den Vorlagenparameter WAF Block Period ändern. Eine Erhöhung der Menge der gescannten Daten wird jedoch wahrscheinlich die Athena-Kosten erhöhen.

> **Tip**
>
> Im Folgenden finden Sie ein Beispiel für die Berechnung der CloudFront Protokollkosten:
> Im Durchschnitt kann jeder CloudFront Treffer etwa 500 Byte an Daten generieren.
> Wenn pro Tag 1,2 Millionen CloudFront Objekte getroffen werden, sind es 200.000 (1,2 M/6) Treffer pro vier Stunden, vorausgesetzt, die Daten werden mit einer gleichbleibenden Geschwindigkeit aufgenommen. Berücksichtigen Sie bei der Berechnung Ihrer Kosten Ihre tatsächlichen Verkehrsmuster.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena berechnet 5,00 USD pro TB gescannter Daten.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Die Athena-Abfrage wird alle fünf Minuten ausgeführt, was 12 Durchläufen pro Stunde entspricht.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> Die tatsächlichen Kosten hängen von den Datenverkehrsmustern Ihrer Anwendung ab. Weitere Informationen finden Sie unter Amazon Athena Pricing.

Sicherheit

Wenn Sie Systeme auf der AWS-Infrastruktur aufbauen, werden Sie und AWS gemeinsam für die Sicherheit verantwortlich sein. Dieses Modell der geteilten Verantwortung reduziert Ihren betrieblichen Aufwand, da AWS die Komponenten wie das Host-Betriebssystem, die Virtualisierungsebene und die physische Sicherheit der Einrichtungen, in denen die Services betrieben werden, betreibt, verwaltet und kontrolliert. Weitere Informationen zur AWS-Sicherheit finden Sie unter AWS Cloud Security.

IAM-Rollen

Mit IAM-Rollen können Sie Services und Benutzern in der AWS-Cloud detaillierten Zugriff, Richtlinien und Berechtigungen zuweisen. Diese Lösung erstellt IAM-Rollen mit den geringsten Rechten, und diese Rollen gewähren den Ressourcen der Lösung die erforderlichen Berechtigungen.

Daten

Alle in Amazon S3 S3-Buckets und DynamoDB-Tabellen gespeicherten Daten sind im Ruhezustand verschlüsselt. Daten, die mit Firehose übertragen werden, sind ebenfalls verschlüsselt.

Schutzfunktionen

Webanwendungen sind anfällig für eine Vielzahl von Angriffen. Zu diesen Angriffen gehören speziell gestaltete Anfragen, die darauf abzielen, eine Sicherheitslücke auszunutzen oder die Kontrolle über einen Server zu übernehmen, volumetrische Angriffe, die darauf abzielen, eine Website lahmzulegen, oder bösartige Bots und Scraper, die darauf programmiert sind, Webinhalte zu durchsuchen und zu stehlen.

Diese Lösung konfiguriert AWS-WAF-Regeln, einschließlich Regelgruppen und benutzerdefinierter Regeln für AWS Managed Rules, um die folgenden häufigen Angriffe zu blockieren: CloudFormation

- AWS Managed Rules — Dieser verwaltete Service bietet Schutz vor häufigen Anwendungsschwachstellen oder anderem unerwünschten Datenverkehr. Diese Lösung umfasst AWS Managed IP-Reputationsregelgruppen, AWS Managed-Basisregelgruppen und AWS Managed-Regelgruppen für anwendungsspezifische Anwendungsfälle. Sie haben die Möglichkeit, eine oder mehrere Regelgruppen für Ihre Web-ACL bis zum maximalen WCU-Kontingent (Web ACL Capacity Unit) auszuwählen.
- SQL-Injection — Angreifer fügen bösartigen SQL-Code in Webanfragen ein, um Daten aus Ihrer Datenbank zu extrahieren. Wir haben diese Lösung entwickelt, um Webanfragen zu blockieren, die potenziell bösartigen SQL-Code enthalten.
- XSS — Angreifer nutzen Sicherheitslücken auf einer harmlosen Website, um bösartige Client-Site-Skripte in den Webbrowser eines legitimen Benutzers einzuschleusen. Wir haben dies so konzipiert, dass es häufig untersuchte Elemente eingehender Anfragen untersucht, um XSS-Angriffe zu identifizieren und zu blockieren.
- HTTP-Floods — Webserver und andere Backend-Ressourcen sind dem Risiko von DDo S-Angriffen wie HTTP-Floods ausgesetzt. Diese Lösung ruft automatisch eine ratenbasierte Regel

auf, wenn Webanfragen von einem Client ein konfigurierbares Kontingent überschreiten. Alternativ können Sie dieses Kontingent erzwingen, indem Sie AWS-WAF-Protokolle mithilfe einer Lambda-Funktion oder einer Athena-Abfrage verarbeiten.

- Scanner und Sonden — Böswillige Quellen scannen und untersuchen Internetanwendungen auf Sicherheitslücken, indem sie eine Reihe von Anfragen senden, die HTTP 4xx-Fehlercodes generieren. Sie können diesen Verlauf verwenden, um bösartige Quell-IP-Adressen zu identifizieren und zu blockieren. Diese Lösung erstellt eine Lambda-Funktion oder Athena-Abfrage, die automatisch CloudFront oder ALB-Zugriffsprotokolle analysiert, die Anzahl der fehlerhaften Anfragen von eindeutigen Quell-IP-Adressen pro Minute zählt und AWS WAF aktualisiert, um weitere Scans von Adressen zu blockieren, die die definierte Fehlerquote erreicht haben.
- Bekannte Herkunft der Angreifer (IP-Reputationslisten) — Viele Unternehmen führen Reputationslisten mit IP-Adressen, die von bekannten Angreifern wie Spammern, Malware-Verteilern und Botnetzen betrieben werden. Diese Lösung nutzt die Informationen in diesen Reputationslisten, um Ihnen zu helfen, Anfragen von bösartigen IP-Adressen zu blockieren. Darüber hinaus blockiert diese Lösung Angreifer, die von IP-Reputationsregelgruppen auf der Grundlage interner Bedrohungsinformationen von Amazon identifiziert wurden.
- Bots und Scraper — Betreiber öffentlich zugänglicher Webanwendungen müssen darauf vertrauen können, dass sich die Kunden, die auf ihre Inhalte zugreifen, korrekt identifizieren und dass sie Dienste wie vorgesehen nutzen. Einige automatisierte Clients, wie Content Scraper oder bösartige Bots, geben sich jedoch falsch aus, um Einschränkungen zu umgehen. Diese Lösung hilft Ihnen dabei, bösartige Bots und Scraper zu identifizieren und zu blockieren.

Kontingente

Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto.

Kontingente für AWS-Services in dieser Lösung

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der in dieser Lösung implementierten Services verfügen. Weitere Informationen finden Sie unter AWS-Servicekontingente. Um die Service-Kontingente für alle AWS-Services in der Dokumentation zu sehen, ohne zwischen den Seiten zu wechseln, schauen Sie sich stattdessen die Informationen auf der Seite Service-Endpunkte und Kontingente in der PDF-Datei an.

AWS-WAF-Kontingente

AWS WAF kann pro IP-Übereinstimmungsbedingung maximal 10.000 IP-Adressbereiche in Classless Inter-Domain Routing (CIDR) -Notation blockieren. Jede Liste, die diese Lösung erstellt, unterliegt diesem Kontingent. Weitere Informationen finden Sie unter AWS-WAF-Kontingente. Ab Version 3.0 erstellt diese Lösung zwei IP-Sätze, die an jede Regel angehängt werden, einen für IPv4 und einen für IPv6.

AWS WAF erlaubt maximal eine Anfrage pro Sekunde, pro Konto und AWS-Region für API-Aufrufe an eine Person `Create` oder `Update` Aktion. `Put` Wenn Sie diese API-Aufrufe außerhalb der Lösung tätigen, kann ein Problem mit der API-Drosselung auftreten. Um das Problem zu vermeiden, empfehlen wir, andere Anwendungen, die diese API-Aufrufe tätigen, nicht in demselben Konto und derselben Region auszuführen, in der diese Lösung bereitgestellt wird.

Überlegungen zur Bereitstellung

Die folgenden Abschnitte enthalten Einschränkungen und Überlegungen zur Implementierung dieser Lösung.

AWS-WAF-Regeln

Die Web-ACL, die diese Lösung generiert, wurde entwickelt, um umfassenden Schutz für Webanwendungen zu bieten. Die Lösung bietet eine Reihe von AWS Managed Rules und benutzerdefinierten Regeln, die Sie der Web-ACL hinzufügen können. Um eine Regel einzubeziehen, wählen Sie `yes` beim Starten des CloudFormation Stacks die entsprechenden Parameter aus. Siehe Schritt 1. Starten Sie den Stack für die Liste der Parameter.

> **Note**
>
> Die out-of-box Lösung unterstützt AWS Firewall Manager nicht. Wenn Sie die Regeln in Firewall Manager verwenden möchten, empfehlen wir Ihnen, Anpassungen am Quellcode vorzunehmen.

Protokollierung des Web-ACL-Datenverkehrs

Wenn Sie den Stack in einer anderen AWS-Region als USA Ost (Nord-Virginia) erstellen und den Endpunkt als festlegen`CloudFront`, müssen Sie Activate HTTP Flood Protection auf no oder setzen`yes - AWS WAF rate based rule`.

Die anderen beiden Optionen (`yes - AWS Lambda log parser`und`yes - Amazon Athena log parser`) erfordern die Aktivierung von AWS-WAF-Protokollen auf einer Web-ACL, die an allen AWS-Edge-Standorten ausgeführt wird. Dies wird außerhalb der USA Ost (Nord-Virginia) nicht unterstützt. Weitere Informationen zur Protokollierung von Web-ACL-Verkehr finden Sie im AWS WAF Developer Guide.

Bearbeitung zu großer Mengen von Anforderungskomponenten

AWS WAF unterstützt nicht die Überprüfung übergroßer Inhalte für den Hauptteil, die Header oder Cookies der Webanforderungskomponente. Wenn Sie eine Regelanweisung schreiben, die einen dieser Anforderungskomponententypen untersucht, können Sie eine der folgenden Optionen wählen, um AWS WAF mitzuteilen, was mit diesen Anfragen geschehen soll:

- `yes`(weiter) — Untersuchen Sie die Anforderungskomponente auf normale Weise gemäß den Regelprüfungskriterien. AWS WAF überprüft den Inhalt der Anforderungskomponente, der innerhalb der Größenbeschränkungen liegt. Dies ist die Standardoption, die in der Lösung verwendet wird.
- `yes - MATCH` – Behandeln der Web-Anforderung als übereinstimmend mit der Regelanweisung. AWS WAF wendet die Regelaktion auf die Anfrage an, ohne sie anhand der Prüfkriterien der Regel zu bewerten. Bei einer Regel mit der `Block`-Aktion wird die Anforderung mit der übergroßen Komponente blockiert.
- `yes - NO_MATCH`— Behandeln Sie die Webanfrage so, als ob sie nicht mit der Regelaussage übereinstimmt, ohne sie anhand der Prüfkriterien der Regel zu bewerten. AWS WAF setzt die Prüfung der Webanforderung fort, indem sie die restlichen Regeln in der Web-ACL verwendet, wie dies bei jeder Regel der Fall wäre, die nicht übereinstimmend ist.

Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten in AWS WAF.

Bereitstellungen mehrerer Lösungen

Sie können die Lösung mehrmals im selben Konto und in derselben Region bereitstellen. Sie müssen für jede Bereitstellung einen eindeutigen CloudFormation Stack-Namen und einen Amazon S3 S3-Bucket-Namen verwenden. Für jede einzelne Bereitstellung fallen zusätzliche Gebühren an und unterliegen den AWS-WAF-Kontingenten pro Konto und Region.

Minimale Rollenberechtigungen für die Bereitstellung (optional)

Kunden können manuell eine IAM-Rolle mit den für die Bereitstellung erforderlichen Mindestberechtigungen erstellen:

- WAF-Berechtigungen

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

- Lambda-Berechtigungen

```
        {
            "Effect": "Allow",
            "Action": [
```

```
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*"
        }
```

- Firehose-Berechtigungen

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

- S3-Berechtigungen

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
```

```
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:PutBucketLogging",
                "s3:GetBucketLogging"
            ],
            "Resource": "arn:aws:s3:::*"
        }
```

- Athena-Berechtigungen

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

- Glue-Berechtigungen

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
```

```
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch Protokolliert Berechtigungen

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

- CloudWatch Berechtigungen

```
        {
```

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

- SNS-Berechtigungen

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

- DynamoDB-Berechtigungen

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

- CloudFormation Berechtigungen

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "cloudformation:ListStacks"
            ],
            "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
        }
```

- Registrierungsberechtigungen für Service Catalog-Apps

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

- X-Ray-Genehmigungen

```
        {
            "Effect": "Allow",
            "Action": [
```

```
            "xray:PutTraceSegments",
            "xray:PutTelemetryRecords"
        ],
        "Resource": "*"
    }
```

- IAM-Berechtigungen

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

- EventBridge Genehmigungen

```
    {
        "Effect": "Allow",
        "Action": [
            "events:PutTargets",
            "events:RemoveTargets",
            "events:DescribeRule",
            "events:EnableRule",
            "events:ListRules",
            "events:PutRule",
            "events:DeleteRule",
            "events:ListEventSources",
            "events:DescribeEventSource",
```

```
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

Stellen Sie die Lösung bereit

Diese Lösung verwendet CloudFormation AWS-Vorlagen und -Stacks, um ihre Bereitstellung zu automatisieren. Die CloudFormation Vorlagen spezifizieren die in dieser Lösung enthaltenen AWS-Ressourcen und ihre Eigenschaften. Der CloudFormation Stack stellt die Ressourcen bereit, die in den Vorlagen beschrieben sind.

Überblick über den Bereitstellungsprozess

Bevor Sie die CloudFormation Vorlage starten, sollten Sie sich mit den in diesem Leitfaden erörterten Überlegungen zur Architektur und Konfiguration vertraut machen. Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um die Lösung zu konfigurieren und in Ihrem Konto bereitzustellen.

Zeit für die Bereitstellung: Ungefähr 15 Minuten.

> **Note**
>
> Wenn Sie diese Lösung bereits bereitgestellt haben, finden Sie Anweisungen zum Update unter Lösung aktualisieren.

Voraussetzungen

- Konfigurieren Sie eine CloudFront Distribution
- Konfigurieren Sie ein ALB

Schritt 1. Starten Sie den Stack

- Starten Sie die CloudFormation Vorlage in Ihrem AWS-Konto.
- Geben Sie Werte für die erforderlichen Parameter ein: Stack-Name und Bucket-Name des Application Access Log.
- Überprüfen Sie die anderen Vorlagenparameter und passen Sie ihre Werte bei Bedarf an.

Schritt 2. Ordnen Sie die Web-ACL Ihrer Webanwendung zu

- Ordnen Sie Ihre CloudFront Webdistribution (en) oder ALB (s) der Web-ACL zu, die diese Lösung generiert. Sie können beliebig viele Distributionen oder Load Balancer zuordnen.

Schritt 3. Konfigurieren Sie die Webzugriffsprotokollierung

- Aktivieren Sie die Webzugriffsprotokollierung für Ihre CloudFront Webdistribution (en) oder ALB (s) und senden Sie Protokolldateien an den entsprechenden Amazon S3 S3-Bucket. Speichern Sie Protokolle in einem Ordner, der dem benutzerdefinierten Präfix entspricht. Wenn kein benutzerdefiniertes Präfix verwendet wird, speichern Sie die Protokolle unter AWSLogs (Standard-ProtokollpräfixAWSLogs/). Weitere Informationen finden Sie unter dem Parameter Bucket Prefix für das Anwendungszugriffslog in Schritt 1. Starten Sie den Stack für weitere Informationen.

CloudFormation AWS-Vorlagen

Diese Lösung umfasst eine CloudFormation AWS-Hauptvorlage und zwei verschachtelte Vorlagen. Sie können die CloudFormation Vorlagen herunterladen, bevor Sie die Lösung bereitstellen.

Haupt-Stack

View template

aws-waf-security-automations.template — Verwenden Sie diese Vorlage als Einstiegspunkt, um die Lösung in Ihrem Konto zu starten. Die Standardkonfiguration stellt eine AWS WAF WAF-Web-ACL mit vorkonfigurierten Regeln bereit. Sie können die Vorlage an Ihre Bedürfnisse anpassen.

WebACL-Stapel

View template

aws-waf-security-automations-webacl.template — Diese verschachtelte Vorlage stellt AWS-WAF-Ressourcen bereit, darunter eine Web-ACL, IP, Sets und andere zugehörige Ressourcen.

Firehose Athena Stack

View template

aws-waf-security-automations-firehose-athena.template — Diese verschachtelte Vorlage stellt Ressourcen

zu AWS Glue, Athena und Firehose bereit. Es wird erstellt, wenn Sie entweder den Scanner & Probe Athena-Protokollparser oder den HTTP Flood Lambda- oder Athena-Protokollparser wählen.

> **Note**
>
> CloudFormation AWS-Ressourcen werden aus Konstrukten des AWS Cloud Development Kit (AWS CDK) erstellt.

Diese CloudFormation AWS-Vorlage stellt die WAF-Lösung Security Automations for AWS in der AWS-Cloud bereit.

Voraussetzungen

Diese Lösung ist für die Verwendung mit Webanwendungen konzipiert, die mit CloudFront oder einem ALB bereitgestellt werden. Wenn Sie noch keine dieser Ressourcen konfiguriert haben, führen Sie die entsprechenden Aufgaben aus, bevor Sie diese Lösung starten.

Konfigurieren Sie eine CloudFront Distribution

Gehen Sie wie folgt vor, um eine CloudFront Verteilung für den statischen und dynamischen Inhalt Ihrer Webanwendung zu konfigurieren. Detaillierte Anweisungen finden Sie im Amazon CloudFront Developer Guide.

1. Erstellen Sie eine Verteilung von CloudFront Webanwendungen. Weitere Informationen finden Sie unter Verteilung erstellen.
2. Konfigurieren Sie statische und dynamische Ursprünge. Weitere Informationen finden Sie unter Verschiedene Ursprünge mit CloudFront Distributionen verwenden.
3. Geben Sie das Verhalten Ihrer Distribution an. Weitere Informationen finden Sie unter Werte, die Sie angeben, wenn Sie eine Verteilung erstellen oder aktualisieren.

> **Note**
>
> Wenn Sie `CloudFront` als Endpunkt wählen, müssen Sie Ihre WAFV2 Ressourcen in der Region USA Ost (Nord-Virginia) erstellen.

Konfigurieren Sie ein ALB

Informationen zur Konfiguration eines ALB zur Verteilung des eingehenden Datenverkehrs an Ihre Webanwendung finden Sie unter Erstellen eines Application Load Balancer im Benutzerhandbuch für Application Load Balancers.

Schritt 1. Starten des -Stacks

Diese automatisierte CloudFormation AWS-Vorlage stellt die Lösung in der AWS-Cloud bereit.

1. Melden Sie sich bei der AWS-Managementkonsole an und wählen Sie die `waf-automation-on-aws.template` CloudFormation Vorlage Launch Solution to Launch aus.

   Launch solution

2. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um diese Lösung in einer anderen AWS-Region zu starten, verwenden Sie die Regionsauswahl in der Navigationsleiste der Konsole. Wenn Sie `CloudFront` als Endpunkt wählen, müssen Sie die Lösung in der Region USA Ost (Nord-Virginia) (`us-east-1`) bereitstellen.

   > **Note**
   >
   > Abhängig von den von Ihnen definierten Eingabeparameterwerten benötigt diese Lösung unterschiedliche Ressourcen. Diese Ressourcen sind derzeit nur in bestimmten AWS-Regionen verfügbar. Daher müssen Sie diese Lösung in einer AWS-Region starten, in der diese Services verfügbar sind. Weitere Informationen finden Sie unter Unterstützte AWS-Regionen.

3. Vergewissern Sie sich auf der Seite „Vorlage angeben“, dass Sie die richtige Vorlage ausgewählt haben, und klicken Sie auf Weiter.
4. Weisen Sie auf der Seite „Stack-Details angeben“ Ihrer AWS-WAF-Konfiguration im Feld Stack-Name einen Namen zu. Dies ist auch der Name der Web-ACL, die die Vorlage erstellt.
5. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Um eine bestimmte Funktion zu deaktivieren, wählen Sie none oderno, falls zutreffend. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
Stack name	`[.red]#<requires input>`	Der Stack-Name darf keine Leerzeichen enthalten. Dieser Name muss innerhalb Ihres AWS-Kontos eindeutig sein und ist der Name der Web-ACL, die die Vorlage erstellt.
Ressourcentyp		
Endpunkt	`CloudFront`	Wählen Sie den Typ der verwendeten Ressource aus. HINWEIS: Wenn Sie `CloudFront` als Endpunkt wählen, müssen Sie die Lösung starten, um WAF-Ressourcen in der Region USA Ost (Nord-Virginia) zu erstellen (`us-east-1`).
Regelgruppen für verwaltete AWS-IP-Reputation		

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz von Amazon IP Reputation List	no	Aktivieren Sie die Komponent `eyes`, mit der Amazon IP Reputation List Managed Rule Group zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe basiert auf internen Bedrohung sinformationen von Amazon. Dies ist nützlich, wenn Sie IP-Adressen blockieren möchten, die normalerw eise mit Bots oder anderen Bedrohungen in Verbindung stehen. Das Blockieren dieser IP-Adressen kann dazu beitragen, Bots zu minimieren und das Risiko zu verringern, dass ein schädlicher Akteur eine gefährdete Anwendung entdeckt. Die erforderliche WCU ist 25. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgrup pen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den Schutz für verwaltete Regelgruppen mit anonymer IP-Liste.	no	Aktivieren Sie die Komponente `eyes`, mit der eine verwaltete Regelgruppe mit anonymer IP-Liste zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert Anfragen von Diensten, die die Verschleierung der Identität des Betrachters ermöglichen. Dazu gehören Anfragen von Proxys VPNs, Tor-Knoten und Hosting-Anbietern. Diese Regelgruppe ist nützlich, wenn Sie Betrachter herausfiltern möchten, die möglicherweise versuchen, ihre Identität vor Ihrer Anwendung zu verbergen. Das Blockieren der IP-Adressen dieser Services kann dazu beitragen, Bots und Möglichkeiten zur Umgehung geografischer Einschränkungen zu minimieren. Die erforderliche WCU ist 50. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt.

Parameter	Standard	Beschreibung
		Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.
Von AWS verwaltete Baseline-Regelgruppen		

Parameter	Standard	Beschreibung
Aktivieren Sie den Schutz für verwaltete Regelgruppen im Core Rule Set	no	Wählen `yes` Sie, ob die Komponente aktiviert werden soll, die Core Rule Set Managed Rule Group zur Web-ACL hinzuzufügen. Diese Regelgruppe bietet Schutz vor der Ausnutzung einer Vielzahl von Sicherhei tslücken, einschließlich einiger hochriskanter und häufig auftretender Sicherhei tslücken. Erwägen Sie, diese Regelgruppe für jeden AWS-WAF-Anwendungsfall zu verwenden. Die erforderliche WCU ist 700. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgrup pen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie Admin Protection Managed Rule Group Protection.	no	Aktivieren Sie die Komponente `eyes`, mit der Admin Protection Managed Rule Group zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert den externen Zugriff auf öffentlich zugängliche Verwaltungsseiten. Dies kann nützlich sein, wenn Sie Software von Drittanbietern ausführen oder das Risiko verringern möchten, dass ein schädlicher Akteur administrativen Zugriff auf Ihre Anwendung erhält. Die erforderliche WCU ist 100. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz für bekannte fehlerhafte Eingaben	no	Aktivieren Sie die Komponent `eyes`, mit der die verwaltet e Regelgruppe Known Bad Inputs zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert den externen Zugriff auf öffentlich zugängliche Verwaltungsseiten. Dies kann nützlich sein, wenn Sie Software von Drittanbi etern ausführen oder das Risiko verringern möchten, dass ein schädlicher Akteur administrativen Zugriff auf Ihre Anwendung erhält. Die erforderliche WCU ist 100. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgrup pen von AWS Managed Rules.
Spezifische Regelgruppe für verwaltete AWS-Anwen dungsfälle		

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz für SQL-Datenbanken	no	Wählen `yes` Sie, ob die Komponente aktiviert werden soll, die SQL Database Managed Rule Group zur Web-ACL hinzuzufügen. Diese Regelgruppe blockiert Anforderungsmuster, die mit der Ausnutzung von SQL-Datenbanken in Verbindung stehen, wie z. B. SQL-Injec tion-Angriffe. Dies kann dazu beitragen, das Remote-In jection von nicht autorisie rten Abfragen zu verhinder n. Evaluieren Sie diese Regelgruppe, wenn Ihre Anwendung mit einer SQL-Datenbank verbunden ist. Die Verwendung der benutzerd efinierten SQL-Injection-Rege l ist optional, wenn Sie die von AWS verwaltete SQL-Regelgruppe bereits aktiviert haben. Die erforderliche WCU ist 200. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt.

Parameter	Standard	Beschreibung
		Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz für das Linux-Betriebssystem	no	Aktivieren Sie die Komponent `eyes`, mit der die verwaltete Regelgruppe des Linux-Bet riebssystems zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert Anforderungsmuster im Zusammenhang mit der Ausnutzung von Linux-spe zifischen Sicherheitslücken, einschließlich Linux-spe zifischer LFI-Angriffe (Local File Inclusion). Dies kann dazu beitragen, Angriffe zu verhindern, die Dateiinha lte offenlegen oder Code ausführen, auf den der Angreifer keinen Zugriff haben soll. Evaluieren Sie diese Regelgruppe, wenn ein Teil Ihrer Anwendung unter Linux läuft. Sie sollten diese Regelgruppe in Verbindun g mit der Regelgruppe des POSIX-Betriebssystems verwenden. Die erforderliche WCU ist 200. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund

Parameter	Standard	Beschreibung
		einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz für das POSIX-Betriebssystem	no	Aktivieren Sie die Komponent `eyes`, mit der Core Rule Set Managed Rule Group Protection zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert Anforderungsmuster im Zusammenhang mit der Ausnutzung von Sicherhei tslücken, die für POSIX und POSIX-ähnliche Betriebss ysteme spezifisch sind, einschließlich LFI-Angriffen. Dies kann dazu beitragen, Angriffe zu verhindern, die Dateiinhalte offenlegen oder Code ausführen, auf den der Angreifer keinen Zugriff haben soll. Prüfen Sie diese Regelgruppe, wenn ein Teil Ihrer Anwendung auf einem POSIX- oder POSIX-ähn lichen Betriebssystem läuft. Die erforderliche WCU ist 100. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt.

Parameter	Standard	Beschreibung
		Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den verwaltet en Regelgruppenschutz für das Windows-Betriebssystem	no	Aktivieren `yes` Sie die Komponente, mit der die verwaltete Regelgruppe des Windows-Betriebssystems zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert Anforderungsmuster im Zusammenhang mit der Ausnutzung von Windows-spezifischen Sicherhei tslücken, wie z. B. der Ausführung von PowerShel l Befehlen aus der Ferne. Dadurch kann verhinder t werden, dass Sicherhei tslücken ausgenutzt werden, die es einem Angreifer ermöglichen, nicht autorisie rte Befehle oder bösartigen Code auszuführen. Evaluiere n Sie diese Regelgrup pe, wenn ein Teil Ihrer Anwendung auf einem Windows-Betriebssystem läuft. Die erforderliche WCU ist 200. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund

Parameter	Standard	Beschreibung
		einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den von PHP-Anwendungen verwalteten Regelgruppenschutz	no	Aktivieren Sie die Komponente `eyes`, die entwickelt wurde, um die PHP Application Managed Rule Group zur Web-ACL hinzuzufügen. Diese Regelgruppe blockiert Anforderungsmuster im Zusammenhang mit der Ausnutzung von Sicherheitslücken, die für die Verwendung der Programmiersprache PHP spezifisch sind, einschließlich der Injektion unsicherer PHP-Funktionen. Dadurch kann verhindert werden, dass Sicherheitslücken ausgenutzt werden, die es einem Angreifer ermöglichen, Code oder Befehle, für die er nicht autorisiert ist, aus der Ferne auszuführen. Evaluieren Sie diese Regelgruppe, wenn PHP auf einem beliebigen Server installiert ist, mit dem Ihre Anwendung verbunden ist. Die erforderliche WCU ist 100. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund

Parameter	Standard	Beschreibung
		einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgruppen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Aktivieren Sie den WordPress anwendungsverwalteten Regelgruppenschutz	no	Aktivieren Sie die Komponent `eyes`, mit der die vom WordPress Programm verwaltete Regelgruppe zur Web-ACL hinzugefügt werden soll. Diese Regelgruppe blockiert Anforderungsmuster im Zusammenhang mit der Ausnutzung von spezifisc hen Sicherheitslücken auf WordPress Websites. Evaluieren Sie diese Regelgruppe, wenn Sie sie ausführen WordPress . Diese Regelgruppe sollte in Verbindung mit den Regelgruppen der SQL-Daten bank und der PHP-Anwen dung verwendet werden. Die erforderliche WCU ist 100. Ihr Konto sollte über ausreichende WCU-Kapazität verfügen, um zu verhindern, dass die Bereitstellung des Web-ACL-Stacks aufgrund einer Überschreitung der Kapazitätsgrenze fehlschlägt. Weitere Informationen finden Sie in der Liste der Regelgrup pen von AWS Managed Rules.

Parameter	Standard	Beschreibung
Benutzerdefinierte Regel — Scanner & Probes		
Aktivieren Sie den Scanner- und Sondenschutz	`yes - AWS Lambda log parser`	Wählen Sie die Komponente aus, die zum Blockieren von Scannern und Sonden verwendet wird. Weitere Informationen zu den Kompromissen im Zusammenhang mit den Risikominderungsoptionen finden Sie unter Optionen für die Protokollanalyse.

Parameter	Standard	Beschreibung
Name des Buckets für das Anwendungszugriffsprotokoll	`[.red]<requires input>`	Wenn Sie sich `yes` für den Parameter Activate Scanner & Probe Protection entschieden haben, geben Sie den Namen des Amazon S3 S3-Buckets (neu oder vorhanden) ein, in dem Sie die Zugriffsprotokolle für Ihre CloudFront Distribution (en) oder ALB (s) speichern möchten. Wenn Sie einen vorhandenen Amazon S3 S3-Bucket verwenden, muss er sich in derselben AWS-Region befinden, in der Sie die CloudFormation Vorlage bereitstellen. Sie sollten für jede Lösungsbereitstellung einen anderen Bucket verwenden. Um diesen Schutz zu deaktivieren, ignorieren Sie diesen Parameter. HINWEIS: Aktivieren Sie die Webzugriffsprotokollierung für Ihre CloudFront Webdistribution (en) oder ALB (s), um Protokolldateien an diesen Amazon S3 S3-Bucket zu senden. Speichern Sie Protokolle in demselben Präfix, das im Stack definiert ist (Standard präfix`AWSLogs/`). Weitere

Parameter	Standard	Beschreibung
		Informationen finden Sie im Parameter Bucket Prefix für das Application Access Log.
Bucket-Präfix für das Anwendungszugriffslog	`AWSLogs/`	Wenn Sie sich `yes` für den Parameter Activate Scanner & Probe Protection entschieden haben, können Sie ein optionales benutzerdefiniertes Präfix für den obigen Bucket für die Anwendungszugriffsprotokolle eingeben. Wenn Sie sich `CloudFront` für den Parameter Endpoint entschieden haben, können Sie ein beliebiges Präfix eingeben, z. `yourprefix/` B. Wenn Sie sich `ALB` für den Endpoint-Parameter entschieden haben, müssen Sie `AWSLogs/` an Ihr Präfix Folgendes anhängen, z. B. `yourprefix/AWSLogs/` Verwenden Sie `AWSLogs/` (Standard), wenn es kein benutzerdefiniertes Präfix gibt. Um diesen Schutz zu deaktivieren, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Ist die Bucket-Zugriffspro tokollierung aktiviert?	no	Wählen Sie, yes ob Sie einen vorhandenen Amazon S3 S3-Bucket-Namen für den Parameter Application Access Log Bucket Name eingegeben haben und die Serverzugriffsprotokollieru ng für den Bucket bereits aktiviert ist. Wenn Sie möchtenno, aktiviert die Lösung die Serverzugriffsprotokollierung für Ihren Bucket. Wenn Sie den Parameter Activate Scanner & Probe Protection ausgewählt habenno, ignorieren Sie diesen Parameter.
Schwellenwert für Fehler	50	Wenn Sie den Parameter „Scanner- und Sondensch utz aktivieren“ ausgewähl t habenyes, geben Sie die maximal zulässige Anzahl fehlerhafter Anfragen pro Minute und IP-Adresse ein. Wenn Sie den Parameter „Scanner- und Sondensch utz aktivieren“ ausgewähl t habenno, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Bewahren Sie die Daten am ursprünglichen S3-Speich erort auf	no	Wenn Sie den Parameter Activate Scanner & Probe Protection ausgewählt habenyes - Amazon Athena log parser, wendet die Lösung die Partitionierung auf Anwendungszugriffs-Protokol ldateien und Athena-Abfragen an. Standardmäßig verschieb t die Lösung Protokolldateien von ihrem ursprünglichen Speicherort in eine partition ierte Ordnerstruktur in Amazon S3. Wählen Sie aus, yes ob Sie auch eine Kopie der Protokolle an ihrem ursprüngl ichen Speicherort behalten möchten. Dadurch wird Ihr Protokollspeicher dupliziert. Wenn Sie den Parameter Scanner & Probe Protectio n aktivieren nicht ausgewähl t yes - Amazon Athena log parser haben, ignorieren Sie diesen Parameter.
Benutzerdefinierte Regel — HTTP Flood		

Parameter	Standard	Beschreibung
Aktivieren Sie den HTTP-Flood-Schutz	`yes - AWS WAF rate-based rule`	Wählen Sie die Komponente aus, die zum Blockieren von HTTP-Flood-Angriffen verwendet wird. Weitere Informationen zu den Kompromissen im Zusammenhang mit den Risikominderungsoptionen finden Sie unter Optionen für den Log Parser.

Parameter	Standard	Beschreibung
Standard-Schwellenwert für Anfragen	`100`	Wenn Sie den Parameter „HTTP-Flood-Schutz aktivieren“ ausgewählt haben`yes`, geben Sie die maximal zulässige Anzahl von Anfragen pro fünf Minuten pro IP-Adresse ein. Wenn Sie den Parameter „HTTP-Flood-Schutz aktivieren“ ausgewählt haben`yes - AWS WAF rate-based rule` , ist der zulässige Mindestwert`10`. Wenn Sie `yes - AWS Lambda log parser` oder `yes - Amazon Athena log parser` für den Parameter „HTTP Flood Protection aktivieren“ ausgewählt haben, kann es sich um einen beliebigen Wert handeln. Um diesen Schutz zu deaktivieren, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Schwellenwert für Anfragen nach Land	<optional input>	Wenn Sie sich `yes - Amazon Athena log parser` für den Parameter HTTP Flood Protection aktivieren entschieden haben, können Sie einen Schwellenwert nach Ländern eingeben, der diesem JSON-Format folgt`{"TR":50, "ER":150}` . Die Lösung verwendet diese Schwellen werte für Anfragen, die aus den angegebenen Ländern stammen. Die Lösung verwendet den Parameter Default Request Threshold für die verbleibe nden Anfragen. HINWEIS: Wenn Sie diesen Parameter definieren, wird das Land automatisch in die Athena-Abfragegruppe aufgenomm en, zusammen mit IP und anderen optionalen Gruppieru ngsfeldern, die Sie mit dem Athena-Abfrageparameter Group By Requests in HTTP Flood auswählen können. + Wenn Sie diesen Schutz deaktivieren möchten, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Gruppieren nach Anfragen in HTTP Flood Athena Query	`None`	Wenn Sie den Parameter „HTTP-Flood-Schutz aktiviere n“ ausgewählt haben`yes - Amazon Athena log parser`, können Sie ein Gruppierungsfeld auswählen , um Anfragen pro IP zu zählen, und das ausgewähl te Gruppierungsfeld. Wenn Sie sich beispielsweise dafür entscheiden`URI`, zählt die Lösung die Anfragen pro IP und URI. Wenn Sie diesen Schutz deaktivieren möchten, ignorieren Sie diesen Parameter.
Zeitraum der WAF-Block ierung	`240`	Wenn Sie `yes - Amazon Athena log parser` für die Parameter Scanner- und Sondenschutz aktivieren **`yes - AWS Lambda log parser`** oder HTTP-Flood-Schutz aktivieren die Option oder ausgewählt haben, geben Sie den Zeitraum (in Minuten) ein, in dem die entsprechenden IP-Adressen gesperrt werden sollen. Um die Protokollanalyse zu deaktivieren, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Athena-Abfragelaufzeitplan (Minute)	5	Wenn Sie die Parameter Scanner & Probe Protection aktivieren oder HTTP Flood Protection aktivieren ausgewählt haben`yes - Amazon Athena log parser`, können Sie ein Zeitintervall (in Minuten) eingeben, über das die Athena-Abfrage ausgeführt wird. Standardmäßig wird die Athena-Abfrage alle 5 Minuten ausgeführt. Wenn Sie diese Schutzmaßnahmen deaktivieren möchten, ignorieren Sie diesen Parameter.

Parameter	Standard	Beschreibung
Schlüssel für Regeln	`IP`	Wenn Sie den Parameter „HTTP Flood Protectio n aktivieren“ ausgewähl t haben`yes - AWS WAF rate-based rule` , konfigurieren Sie diese Regel so, dass sie verschied ene andere Kombinationen von Aggregationsschlüs seln verwendet. Verfügbare Optionen: IP (Standard) IP+Benutzerdefinierter Header (wenn diese Option ausgewählt ist, `Rule Keys Custom Header` ist sie obligatorisch) IP+URI IP+HTTP-METHODE Weitere Informationen finden Sie unter Aggregationsoption en auf Basis der WAF-Regel rate.

Parameter	Standard	Beschreibung
Regelschlüssel, Benutzerdefinierter Header	no	Wenn Sie sich `IP+Custom Header` für den Parameter Rule Keys entschieden haben, geben Sie den Namen des benutzerdefinierten Headers ein, der für die Aggregation von Anfragen verwendet werden soll. Weitere Informationen finden Sie unter Ratenbasierte Aggregationsoptionen für WAF-Regelanweisungen.

Parameter	Standard	Beschreibung
Schwellenwert für das Zeitfenster (Minuten)	5	Zeitfenster-Schwellenwert in Minuten für den HTTP-Hoch wasserschutz. Gilt sowohl für ratenbasierte Regeln als auch für den Lambda-Log-Parser. Verfügbare Optionen: [1, 2, 5, 10]. Wenn Sie den Parameter HTTP aktivieren ausgewähl t haben**`yes - AWS WAF rate-based rule`** , wird Flood Protection für Testzeitf enster verwendet. Weitere Informationen finden Sie unter WAF Web ACL Rate Based Statement. Wenn Sie `yes - AWS Lambda log parser` den Parameter HTTP aktivieren wählen, wird Flood Protectio n zusätzlich zum Blockieru ngszeitraum für den Testzeitr aum verwendet.
Benutzerdefinierte Regel — Bad Bot		
Aktivieren Sie den Schutz vor bösartigen Bots	`yes`	Aktivieren Sie die Komponent `eyes`, die bösartige Bots und Content Scraper blockieren soll.

Parameter	Standard	Beschreibung
ARN einer IAM-Rolle, die Schreibzugriff auf CloudWatch Logs in Ihrem Konto hat	<optional input>	Geben Sie einen optionalen ARN einer IAM-Rolle an, die Schreibzugriff auf CloudWatch Logs in Ihrem Konto hat. Beispiel: `ARN: arn:aws:iam::account_id:role/myrolename` . Wenn Sie diesen Parameter leer lassen (Standard), erstellt die Lösung eine neue Rolle für Sie.
Benutzerdefinierte Regel — IP-Reputationslisten von Drittanbietern		
Aktivieren Sie den Schutz durch Reputationslisten	`yes`	Wählen Sie`yes`, ob Anfragen von IP-Adressen blockiert werden sollen, die auf Reputationslisten von Drittanbietern stehen (zu den unterstützten Listen gehören Spamhaus, Emerging Threats und Tor Exit Node).
Ältere benutzerdefinierte Regeln		

Parameter	Standard	Beschreibung
Aktivieren Sie den SQL-Injection-Schutz	`yes`	Aktivieren `yes` Sie die Komponente, die allgemeine SQL-Injection-Angriffe blockieren soll. Erwägen Sie, es zu aktivieren, wenn Sie keinen von AWS verwalteten Kernregelsatz oder eine von AWS verwaltete SQL-Datenbank-Regelgruppe verwenden. Sie können eine der Optionen (`yes`(fortsetzen) oder`yes - NO_MATCH`) wählen`yes - MATCH`, mit denen AWS WAF übergroße Anfragen verarbeiten soll, die 8 KB (8192 Byte) überschreiten. `yes`Prüft standardmäßig den Inhalt der Anforderungskomponente, der innerhalb der Größenbeschränkungen gemäß den Regelprüfungskriterien liegt. Weitere Informationen finden Sie unter Umgang mit übergroßen Webanforderungskomponenten. Wählen Sie diese Funktion ausno, um sie zu deaktivieren. HINWEIS: Der CloudFormation Stack fügt der standardmäßigen SQL-Injection-Schutzregel die ausgewählte Option zur

Parameter	Standard	Beschreibung
		Handhabung übergroße r Größen hinzu und stellt sie in Ihrem AWS-Konto bereit. Wenn Sie die Regel außerhalb von angepasst haben CloudFormation, werden Ihre Änderungen nach dem Stack-Update überschrieben.

Parameter	Standard	Beschreibung
Sensitivitätsstufe für den SQL-Injection-Schutz	`LOW`	Wählen Sie die Sensitivitätsstufe, die AWS WAF verwenden soll, um nach SQL-Injection-Angriffen zu suchen. `HIGH`erkennt mehr Angriffe, generiert aber möglicher weise mehr Fehlalarme. `LOW` ist im Allgemeinen die bessere Wahl für Ressourcen, die bereits über andere Schutzmaß nahmen gegen SQL-Injection-Angriffe verfügen oder die eine geringe Toleranz für Fehlalarme aufweisen. Weitere Informationen finden Sie unter AWS WAF fügt Sensitivitätsstufen für SQL-Injection-Regelanweisungen und SensitivityLevel Eigenschaften hinzu im CloudFormation AWS-Benutzerhandbuch. Wenn Sie den SQL-Injection-Schutz deaktivieren möchten, ignorieren Sie diesen Parameter. HINWEIS: Der CloudFormation Stack fügt die ausgewählte Sensitivitätsstufe zur standardmäßigen SQL-Injection-Schu

Parameter	Standard	Beschreibung
		tzregel hinzu und stellt sie in Ihrem AWS-Konto bereit. Wenn Sie die Regel außerhalb von angepasst haben CloudFormation, werden Ihre Änderungen nach dem Stack-Update überschrieben.

Parameter	Standard	Beschreibung
Aktivieren Sie den Cross-Site Scripting Protection	`yes`	Wählen Sie`yes`, ob Sie die Komponente aktiviere n möchten, die gängige XSS-Angriffe blockieren soll. Erwägen Sie, es zu aktiviere n, wenn Sie keinen von AWS verwalteten Kernregelsatz verwenden. Sie können auch eine der Optionen (`yes`(fortsetzen), oder`yes - NO_MATCH`) auswählen`yes - MATCH`, mit denen AWS WAF übergroße Anfragen verarbeiten soll, die 8 KB (8192 Byte) überschreiten. `yes`Verwendet standardm äßig die `Continue` Option, die den Inhalt der Anforderu ngskomponente überprüft, der innerhalb der Größenbes chränkungen gemäß den Regelprüfungskriterien liegt. Weitere Informationen finden Sie unter Behandlung von Übergrößen bei Anforderu ngskomponenten. Wählen Sie diese Funktion ausno, um sie zu deaktivie ren. HINWEIS: Der CloudFormation Stack fügt der standardmäßigen Cross-Site-Scripting-Regel die ausgewählte Option für die Bearbeitung von Übergröße

Parameter	Standard	Beschreibung
		n hinzu und stellt sie in Ihrem AWS-Konto bereit. Wenn Sie die Regel außerhalb von angepasst haben CloudFormation, werden Ihre Änderungen nach dem Stack-Update überschrieben.
Zulässige und verweigerte IP-Aufbewahrungseinstellungen		
Aufbewahrungszeitraum (Minuten) für den zulässigen IP-Satz	`-1`	Wenn Sie die IP-Aufbewahrung für den Satz zugelassener IP-Adressen aktivieren möchten, geben Sie eine Zahl (`15`oder mehr) als Aufbewahrungszeitraum (Minuten) ein. IP-Adressen, die den Aufbewahrungszeitraum erreichen, laufen ab, und die Lösung entfernt sie aus dem IP-Set. Die Lösung unterstützt eine Aufbewahrungsfrist von mindestens 15 Minuten. Wenn Sie eine Zahl zwischen `0` und eingeben`15`, behandelt die Lösung sie als`15`. Belassen Sie es auf `-1` (Standard), um die IP-Aufbewahrung zu deaktivieren.

Parameter	Standard	Beschreibung
Aufbewahrungszeitraum (Minuten) für die eingestellte verweigerte IP-Adresse	`-1`	Wenn Sie die IP-Aufbewahrung für den Denied IP-Satz aktivieren möchten, geben Sie eine Zahl (`15`oder mehr) als Aufbewahrungszeitraum (Minuten) ein. IP-Adressen, die den Aufbewahrungszeitraum erreichen, laufen ab, und die Lösung entfernt sie aus dem IP-Set. Die Lösung unterstützt eine Aufbewahrungsfrist von mindestens 15 Minuten. Wenn Sie eine Zahl zwischen `0` und eingeben`15`, behandelt die Lösung sie als`15`. Belassen Sie es auf `-1` (Standard), um die IP-Aufbewahrung zu deaktivieren.

Parameter	Standard	Beschreibung
E-Mail für den Empfang von Benachrichtigungen nach Ablauf der zulässigen oder verweigerten IP-Sets	<optional input>	Wenn Sie die Parameter für den IP-Aufbewahrungsze itraum aktiviert haben (siehe zwei vorherige Parameter) und eine E-Mail-Benachricht igung erhalten möchten, wenn IP-Adressen ablaufen, geben Sie eine gültige E-Mail-Adresse ein. Wenn Sie die IP-Aufbew ahrung nicht aktiviert haben oder E-Mail-Benachricht igungen deaktivieren möchten, lassen Sie das Feld leer (Standard).
Erweiterte Einstellungen		
Aufbewahrungszeitraum (Tage) für Protokollgruppen	365	Wenn Sie die Aufbewahrung für die CloudWatch Protokoll gruppen aktivieren möchten, geben Sie eine Zahl (1oder mehr) als Aufbewahrungszeitr aum (Tage) ein. Sie können einen Aufbewahrungszeitr aum zwischen einem Tag (1) und zehn Jahren (3650) wählen. Standardmäßig laufen Protokolle nach einem Jahr ab. Stellen Sie es auf ein-1, um die Protokolle auf unbestimm te Zeit aufzubewahren.

6. Wählen Sie Weiter aus.
7. Auf der Seite Stack-Optionen konfigurieren können Sie Tags (Schlüssel-Wert-Paare) für Ressourcen in Ihrem Stack angeben und zusätzliche Optionen festlegen. Wählen Sie Weiter aus.
8. Überprüfen und bestätigen Sie auf der Seite Überprüfen und erstellen die Einstellungen. Wählen Sie die Felder aus, um zu bestätigen, dass die Vorlage IAM-Ressourcen und alle zusätzlichen Funktionen erstellt, die erforderlich sind.
9. Wählen Sie Submit, um den Stack bereitzustellen.

   Sehen Sie sich den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status an. Sie sollten in etwa 15 Minuten den Status CREATE_COMPLETE erhalten.

> **Note**
>
> Zusätzlich zu den Lambda-Funktionen `Log Parser` und den `IP Lists Parser` AWS-Lambda-Funktionen umfasst diese Lösung die Funktionen `helper` und `custom-resource` Lambda, die nur während der Erstkonfiguration oder wenn Ressourcen aktualisiert oder gelöscht werden, ausgeführt werden.
> Wenn Sie diese Lösung verwenden, sehen Sie alle Funktionen in der AWS Lambda Lambda-Konsole, aber nur die drei primären Lösungsfunktionen sind regelmäßig aktiv. Löschen Sie die anderen beiden Funktionen nicht. Sie sind für die Verwaltung der zugehörigen Ressourcen erforderlich.

Um Details zu den Stack-Ressourcen zu sehen, wählen Sie die Registerkarte Ausgaben. Dies beinhaltet den BadBotHoneypotEndpointWert. Merken Sie sich diesen Wert, da Sie ihn beim Einbetten des Honeypot-Links in Ihrer Webanwendung verwenden werden.

Schritt 2. Ordnen Sie die Web-ACL Ihrer Webanwendung zu

Aktualisieren Sie Ihre CloudFront Distribution (en) oder ALB (s), um AWS WAF und Logging mithilfe der Ressourcen zu aktivieren, die Sie in Schritt 1 generiert haben. Starten Sie den Stack.

1. Melden Sie sich bei der AWS WAF WAF-Konsole an.
2. Wählen Sie die Web-ACL aus, die Sie verwenden möchten.
3. Wählen Sie auf der Registerkarte Associated AWS resources (Zugeordnete AWS-Ressourcen) Add AWS resources (AWS-Ressourcen hinzufügen).

4. Wählen Sie unter Ressourcentyp die CloudFront Distribution oder ALB aus.
5. Wählen Sie eine Ressource aus der Liste aus und klicken Sie dann auf Hinzufügen, um Ihre Änderungen zu speichern.

Schritt 3. Konfigurieren Sie die Webzugriffsprotokollierung

Konfigurieren Sie CloudFront oder Ihr ALB so, dass Webzugriffsprotokolle an den entsprechenden Amazon S3 S3-Bucket gesendet werden, sodass diese Daten für die Log Parser-Lambda-Funktion verfügbar sind.

Speichern Sie Webzugriffsprotokolle aus einer Distribution CloudFront

1. Melden Sie sich bei der CloudFront Amazon-Konsole an.
2. Wählen Sie den Vertrieb Ihrer Webanwendung und anschließend Vertriebseinstellungen aus.
3. Wählen Sie im Tab General die Option Edit aus.
4. Wählen Sie für AWS WAF Web ACL die erstellte Web-ACL-Lösung aus (den Stack-Name-Parameter).
5. Wählen Sie für Protokollierung On.
6. Wählen Sie für Bucket for Logs den S3-Bucket aus, den Sie zum Speichern von Webzugriffsprotokollen verwenden möchten. Dies kann ein neuer oder ein vorhandener S3-Bucket sein, der im Hauptstapel verwendet wird und über die Berechtigung CloudFront zum Schreiben von Protokollen verfügt. In der Drop-down-Liste sind die Buckets aufgeführt, die dem aktuellen AWS-Konto zugeordnet sind. Weitere Informationen finden Sie unter Erste Schritte mit einer CloudFront Basisdistribution im Amazon CloudFront Developer Guide.
7. Stellen Sie das Protokollpräfix auf das Präfix ein, das für die Bereitstellung der Lösung verwendet wurde. Sie finden das Präfix im Hauptstapel auf der Registerkarte Parameter AppAccessLogBucketPrefixParam(Standard`AWSLogs/`).
8. Wählen Sie Yes, Edit aus, um Ihre Änderungen zu speichern.

Weitere Informationen finden Sie unter Konfiguration und Verwendung von Standardprotokollen (Zugriffsprotokollen) im Amazon CloudFront Developer Guide.

Speichern von Webzugriffsprotokollen von einem Application Load Balancer

1. Melden Sie sich bei der Amazon Elastic Compute Cloud (Amazon EC2) -Konsole an.

2. Klicken Sie im Navigationsbereich auf Load Balancers.
3. Wählen Sie den ALB Ihrer Webanwendung aus.
4. Klicken Sie in der Registerkarte Description (Beschreibung) auf Edit attributes (Attribute bearbeiten).
5. Wählen Sie Enable access logs (Zugriffslogs aktivieren) aus.
6. Geben Sie für den S3-Standort den Namen des S3-Buckets ein, den Sie zum Speichern von Webzugriffsprotokollen verwenden möchten. Dies kann ein neuer oder vorhandener S3-Bucket sein, der im Hauptstapel verwendet wird und über die Berechtigung für Application Load Balancer verfügt, Protokolle zu schreiben.
7. Setzen Sie das Protokollpräfix auf das Präfix, das für die Bereitstellung der Lösung verwendet wurde. Sie finden das Präfix im Hauptstapel auf der Registerkarte Parameter AppAccessLogBucketPrefixParam(Standard`AWSLogs/`).
8. Wählen Sie Speichern.

Weitere Informationen finden Sie unter Access Logs for your Application Load Balancer im Elastic Load Balancing User Guide.

Aktualisieren Sie die Lösung

Wenn Sie die Lösung bereits bereitgestellt haben, gehen Sie wie folgt vor, um den CloudFormation Stack der Lösung zu aktualisieren und die neueste Version des Lösungsframeworks zu erhalten. Lesen Sie sich die Überlegungen zum Update sorgfältig durch, bevor Sie den Stack aktualisieren.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie im linken Navigationsmenü Stacks aus.
3. Wählen Sie Ihren vorhandenen `aws-waf-security-automations` CloudFormation Stack aus.
4. Wählen Sie Aktualisieren.
5. Wählen Sie Aktuelle Vorlage ersetzen aus.
6. Gehen Sie unter Vorlage angeben wie folgt vor:
   a. Wählen Sie Amazon S3 S3-URL aus.
   b. Kopieren Sie den Link der `aws-waf-security-automations.template` AWS CloudFormation.
   c. Fügen Sie den Link in das Amazon S3 S3-URL-Feld ein.
   d. Vergewissern Sie sich, dass die richtige Vorlagen-URL im Textfeld Amazon S3 S3-URL angezeigt wird.
   e. Wählen Sie Weiter aus.
   f. Wählen Sie erneut Next (Weiter).
7. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie nach Bedarf. Weitere Informationen finden Sie in Schritt 1. Starten Sie den Stack, um weitere Informationen zu den Parametern zu erhalten.
8. Wählen Sie Weiter aus.
9. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
10. Überprüfen und bestätigen Sie die Einstellungen auf der Seite Review.
11. Wählen Sie das Kästchen aus, das bestätigt, dass die Vorlage möglicherweise IAM-Ressourcen erstellt.
12. Wählen Sie „Änderungssatz anzeigen“ und überprüfen Sie die Änderungen.
13. Wählen Sie Stack aktualisieren, um den Stack bereitzustellen.

Sie können den Status des Stacks in der CloudFormation AWS-Konsole in der Spalte Status sehen. In etwa 15 Minuten sollte Ihnen der Status UPDATE_COMPLETE angezeigt werden.

Überlegungen zum Update

In den folgenden Abschnitten finden Sie Einschränkungen und Überlegungen zur Aktualisierung dieser Lösung.

Aktualisierung des Ressourcentyps

Sie müssen einen neuen Stack bereitstellen, um den Endpoint-Parameter nach der Erstellung des Stacks zu aktualisieren. Ändern Sie den Endpoint-Parameter nicht, wenn Sie den Stack aktualisieren.

WAFV2 aktualisieren

Ab Version 3.0 unterstützt diese Lösung AWS WAFV2. Wir haben alle API-Aufrufe von AWS WAF Classic durch WAFV2 AWS-API-Aufrufe ersetzt. Dadurch werden Abhängigkeiten von Node.js entfernt und die meiste up-to-date Python-Laufzeit verwendet. Um diese Lösung mit den neuesten Funktionen und Verbesserungen weiterhin verwenden zu können, müssen Sie Version 3.0 oder höher als neuen Stack bereitstellen.

Anpassungen beim Stack-Update

Die out-of-box Lösung stellt eine Reihe von AWS-WAF-Regeln mit Standardkonfigurationen in Ihrem AWS-Konto mit dem CloudFormation Stack bereit. Wir empfehlen nicht, Anpassungen auf die von der Lösung bereitgestellten Regeln anzuwenden. Stack-Updates überschreiben diese Änderungen. Wenn Sie benutzerdefinierte Regeln benötigen, empfehlen wir, separate Regeln außerhalb der Lösung zu erstellen.

Schlechtes Bot-Schutz-Upgrade

In Version 4.1.0 wurde der Access Handler Lambda mit API Gateway als veraltet eingestuft und durch die erweiterte Protokollfunktionalität der Funktion ersetzt. `Log parser - Bad bot` Anstatt direkte Anfragen über API Gateway zu verwenden, verwendet die Lösung jetzt den Protokollstream erneut, um bösartige Bots zu erkennen.

Frühere Implementierung:

1. Erforderlicher Access Handler Lambda und API Gateway.

2. Verwendeter Honeypot-Endpunkt für die direkte Bearbeitung von Anfragen.
3. Erforderliches Einbetten des Honeypot-Endpunkts in Websites.

Neue Implementierung (4.1.0+): Der Bad Bot Protection-Log-Parser jetzt:

1. Überprüft Anfragen an den Honeypot-Endpunkt anhand von Protokollen.
2. Verarbeitet Anfragen, wenn Bad Bot Protection aktiviert ist.
3. Verwendet den WAF-Filter BadBotRuleFilter, um bösartige Bot-Anfragen zu identifizieren.
4. Analysiert Protokolldaten, um IP-Adressen zu identifizieren, die definierte Kontingente überschreiten.
5. Aktualisiert die festgelegten AWS-WAF-IP-Set-Bedingungen, um identifizierte Adressen zu blockieren.

Diese Änderung vereinfacht die Architektur, indem doppelte Funktionen beseitigt und bestehende Funktionen zur Protokollverarbeitung genutzt werden.

CDK-Upgrade

Ab Version v4.1.0 wird diese Lösung von CDK unterstützt. Bei der Migration von einer Version unter v4.1.0. Verwenden Sie die neue Vorlagen- und Aktualisierungslösung in Cloudformation. Anschließend können Sie beginnen, die Lösung lokal über Ihr Terminal mit cdk deploy zu aktualisieren (weitere Informationen finden Sie in der README-Datei). Wenn Sie versuchen, cdk deploy direkt zu verwenden, wird möglicherweise der folgende Fehler angezeigt: Unzureichender Einrückzug in der Flow-Erfassung

Die andere Möglichkeit, die Lösung zu aktualisieren, besteht darin, die von der Lösung bereitgestellte Vorlage zu verwenden und zum Abschnitt Cloudformation der AWS-Konsole zu wechseln, auf Lösung aktualisieren zu klicken und die neue Vorlage dort einzufügen.

> **Note**
>
> Wenn Sie ein Upgrade von Version 3.0 oder 3.1 auf Version 3.2 oder neuer dieser Lösung durchführen und IP-Adressen manuell in den Satz zugelassener oder verweigerter IP-Adressen eingefügt haben, besteht die Gefahr, dass Sie diese IP-Adressen verlieren. Um dies zu verhindern, erstellen Sie vor dem Upgrade der Lösung eine Kopie der IP-Adressen im Satz zugelassener oder verweigerter IP-Adressen. Fügen Sie dann, nachdem Sie das

Upgrade abgeschlossen haben, die IP-Adressen nach Bedarf wieder zum IP-Satz hinzu. Weitere Informationen finden Sie in den Befehlen get-ip-setund update-ip-setCLI. Wenn Sie bereits Version 3.2 oder neuer verwenden, ignorieren Sie diesen Schritt.

Deinstalliere die Lösung

Um die Lösung zu deinstallieren, löschen Sie die CloudFormation Stacks:

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie den übergeordneten Stack der Lösung aus. Alle anderen Lösungsstapel werden automatisch gelöscht.
3. Wählen Sie Löschen aus.

> **Note**
>
> Durch die Deinstallation der Lösung werden alle von der Lösung verwendeten AWS-Ressourcen mit Ausnahme der Amazon S3 S3-Buckets gelöscht. Wenn einige IP-Sets aufgrund eines durch die AWA WAF-API-Kontingente verursachten Problems mit der Geschwindigkeitsüberschreitung nicht gelöscht werden können, löschen Sie diese IP-Sätze manuell und anschließend den Stack.

Benutze die Lösung

Dieser Abschnitt enthält detaillierte Anweisungen zur Verwendung der Lösung nach der Bereitstellung der Lösung.

Ändern Sie die zulässigen und verweigerten IP-Sets (optional)

Nach der Bereitstellung des CloudFormation Stacks dieser Lösung können Sie die zulässigen und verweigerten IP-Sets manuell ändern, um IP-Adressen nach Bedarf hinzuzufügen oder zu entfernen.

1. Melden Sie sich bei der AWS WAF WAF-Konsole an.
2. Wählen Sie im linken Navigationsbereich IP-Sets aus.
3. Wählen Sie IP-Set für die Liste der zugelassenen Geräte und fügen Sie IP-Adressen aus vertrauenswürdigen Quellen hinzu.
4. Wählen Sie IP-Set für die Liste der verweigerten IP-Adressen und fügen Sie IP-Adressen hinzu, die Sie blockieren möchten.

Betten Sie den Honeypot-Link in Ihre Webanwendung ein (optional)

Wenn Sie sich in Schritt 1 `yes` für den Parameter Activate Bad Bot Protection entschieden haben. Wenn Sie den Stack starten, erstellt die CloudFormation Vorlage einen Trap-Endpunkt zu einem Produktions-Honeypot mit geringer Interaktion. Diese Falle dient dazu, eingehende Anfragen von Content-Scrapern und bösartigen Bots zu erkennen und umzuleiten. Gültige Benutzer werden nicht versuchen, auf diesen Endpunkt zuzugreifen.

Diese Komponente verbessert die Erkennung böser Bots, indem sie zusätzlich zum Honeypot-Mechanismus direkte Verbindungen zu einem Application Load Balancer (ALB) oder Amazon CloudFront überwacht. Wenn ein Bot den Honeypot umgeht und versucht, mit ALB oder zu interagieren, analysiert das System Anforderungsmuster und Protokolle CloudFront, um böswillige Aktivitäten zu identifizieren. Wenn ein böser Bot erkannt wird, wird seine IP-Adresse extrahiert und zu einer AWS-WAF-Sperrliste hinzugefügt, um weiteren Zugriff zu verhindern. Die Erkennung bösartiger Bots erfolgt über eine strukturierte Logikkette, die eine umfassende Bedrohungsabdeckung gewährleistet:

- HTTP Flood Protection Lambda Log Parser — Sammelt schädliche Bot IPs aus Protokolleinträgen während der Hochwasseranalyse.

- Scanner & Probe Protection Lambda Log Parser — Identifiziert bösartige Bots anhand IPs scannerbezogener Protokolleinträge.
- HTTP Flood Protection Athena Log Parser — Extrahiert bösartige Bots IPs aus Athena-Protokollen und verwendet dabei Partitionen für den gesamten Abfragelauf.
- Scanner & Probe Protection Athena Log Parser — Ruft bösartige Bots IPs aus scannerbezogenen Athena-Protokollen ab und verwendet dabei dieselbe Partitionierungsstrategie.
- Fallback-Erkennung — Wenn sowohl HTTP Flood Protection als auch Scanner & Probe Protection deaktiviert sind, stützt sich das System auf den Log Lambda-Parser, der Bot-Aktivitäten auf der Grundlage von WAF-Labelfiltern protokolliert.

Verwenden Sie eines der folgenden Verfahren, um den Honeypot-Link für Anfragen aus einer der beiden Distributionen einzubetten. CloudFront

Erstellen Sie einen CloudFront Ursprung für den Honeypot-Endpunkt

Verwenden Sie dieses Verfahren für Webanwendungen, die mit einer CloudFront Distribution bereitgestellt werden. Mit können Sie eine `robots.txt` Datei hinzufügen CloudFront, um Content-Scraper und Bots zu identifizieren, die den Ausschlussstandard von Robots ignorieren. Gehen Sie wie folgt vor, um den versteckten Link einzubetten und ihn dann ausdrücklich in Ihrer `robots.txt` Datei zu verbieten.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie den Stack aus, den Sie in Schritt 1 erstellt haben. Starten Sie den Stack
3. Wählen Sie die Registerkarte Outputs.
4. Kopieren Sie aus dem BadBotHoneypotEndpointSchlüssel die Endpunkt-URL.
   - Der Verhaltenspfad (`/ProdStage`)
5. Binden Sie diesen Endpunkt-Link in Ihren Inhalt ein, der auf den Honeypot verweist. Verstecken Sie diesen Link vor Ihren menschlichen Benutzern. Sehen Sie sich als Beispiel das folgende Codebeispiel an:`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`.
6. Ändern Sie die `robots.txt` Datei im Stammverzeichnis Ihrer Website wie folgt, um den Honeypot-Link ausdrücklich zu verbieten:

```
User-agent: <*>
```

```
        Disallow: /<behavior_path>
```

> **Important**
>
> Es CloudFront ist keine Pfadregistrierung erforderlich, da Anfragen wie folgt lauten: Von WAF blockiert. BadBotRuleFilter Die Lösung wird automatisch in Protokollen erfasst. Wird vom Log-Parser Lambda verarbeitet. Bei diesem vereinfachten Ansatz werden die WAF-Protokolle direkt verwendet, sodass keine zusätzliche Endpunktkonfiguration erforderlich ist, wodurch der Prozess zur Erkennung böser Bots durch Protokollanalyse effizienter wird

> **Note**
>
> Es liegt in Ihrer Verantwortung, zu überprüfen, welche Tag-Werte in Ihrer Website-Umgebung funktionieren. Verwenden Sie es nicht`rel="nofollow"`, wenn es in Ihrer Umgebung nicht beachtet wird. Weitere Informationen zur Konfiguration von Robots-Metatags finden Sie im Google-Entwicklerhandbuch. Ändern Sie die `robots.txt` Datei im Stammverzeichnis Ihrer Website wie folgt, um den Honeypot-Link ausdrücklich zu verbieten:

Betten Sie den Honeypot-Endpunkt als externen Link ein

> **Note**
>
> Diese Regeln verwenden die Quell-IP-Adresse aus dem Ursprung der Webanfrage. Wenn Ihr Datenverkehr über einen oder mehrere Proxys oder Load Balancer läuft, enthält der Ursprung der Webanfrage die Adresse des letzten Proxys und nicht die ursprüngliche Adresse des Clients.

Verwenden Sie dieses Verfahren für Webanwendungen.

1. Melden Sie sich bei der CloudFormation AWS-Konsole an.
2. Wählen Sie den Stack aus, den Sie in Schritt 1 erstellt haben. Starten Sie den Stack.
3. Wählen Sie die Registerkarte Outputs.
4. Kopieren Sie aus dem BadBotHoneypotEndpointSchlüssel die Endpunkt-URL.

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

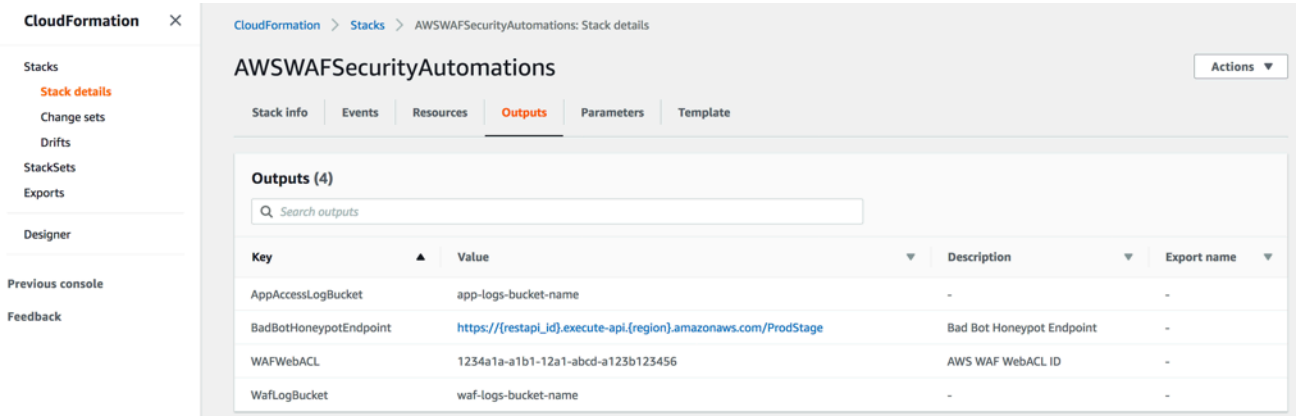
> **Note**
>
> Mit diesem Verfahren werden Roboter angewiesen`rel=nofollow`, nicht auf die Honeypot-URL zuzugreifen. Da der Link jedoch extern eingebettet ist, können Sie keine `robots.txt` Datei hinzufügen, um den Link explizit zu verbieten. Es liegt in Ihrer Verantwortung, zu überprüfen, welche Tags in Ihrer Website-Umgebung funktionieren. Verwenden Sie es nicht`rel="nofollow"`, wenn Ihre Umgebung es nicht beachtet.

Verwenden Sie die JSON-Datei des Lambda-Log-Parsers

Verwenden Sie die Lambda-Log-Parser-JSON-Datei für den HTTP-Flood-Schutz

Wenn Sie sich `Yes - AWS Lambda log parser` für den Vorlagenparameter Activate HTTP Flood Protection entschieden haben, erstellt diese Lösung eine Konfigurationsdatei mit dem Namen `<stack_name>-waf_log_conf.json` und lädt sie in den Amazon S3 S3-Bucket hoch, der zum Speichern der AWS WAF WAF-Protokolldateien verwendet wird. Den Bucket-Namen finden Sie in der WafLogBucketVariablen in der CloudFormation Ausgabe. Die folgende Abbildung zeigt ein Beispiel.

Screenshot, der einen Bildschirm mit der Bezeichnung AWSWAFSecurity Automations zeigt und vier Ausgaben auflistet



Wenn Sie die `<stack_name>-waf_log_conf.json` Datei auf Amazon S3 bearbeiten und überschreiben, berücksichtigt die `Log Parser` Lambda-Funktion die neuen Werte bei der Verarbeitung neuer AWS WAF WAF-Protokolldateien. Im Folgenden finden Sie eine Beispiel-Konfigurationsdatei:

Screenshot einer Beispielkonfigurationsdatei

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

Zu den Parametern gehören die folgenden:

- Allgemeines:
  - Anforderungsschwellenwert (erforderlich) — Die maximal zulässige Anzahl von Anfragen pro fünf Minuten pro IP-Adresse. Diese Lösung verwendet den Wert, den Sie bei der Bereitstellung oder Aktualisierung des CloudFormation Stacks definieren.
  - Sperrzeitraum (erforderlich) — Der Zeitraum (in Minuten), in dem die entsprechenden IP-Adressen gesperrt werden sollen. Diese Lösung verwendet den Wert, den Sie bei der Bereitstellung oder Aktualisierung des CloudFormation Stacks definieren.
  - Ignorierte Suffixe — Anfragen, die auf diesen Ressourcentyp zugreifen, zählen nicht zum Anforderungsschwellenwert. Standardmäßig ist diese Liste leer.
- URI-Liste — Verwenden Sie diese Liste, um einen benutzerdefinierten Schwellenwert für Anfragen und einen Sperrzeitraum für bestimmte URLs Anfragen zu definieren. Standardmäßig ist diese Liste leer.

Wenn WAF-Protokolle in eintreffen WafLogBucket, werden sie von der Lambda-Log-Parser-Funktion unter Verwendung der Konfigurationen in Ihrer Konfigurationsdatei verarbeitet. Die Lösung schreibt das Ergebnis in eine Ausgabedatei mit dem Namen desselben `<stack_name>-`

`waf_log_out.json` Buckets. Wenn die Ausgabedatei eine Liste der als Angreifer identifizierten IP-Adressen enthält, fügt die Lösung sie dem WAF-IP-Set für HTTP Flood hinzu, sodass sie nicht auf Ihre Anwendung zugreifen können. Wenn die Ausgabedateien keine IP-Adressen haben, überprüfen Sie, ob Ihre Konfigurationsdatei gültig ist oder ob das in der Konfigurationsdatei angegebene Ratenlimit überschritten wurde.

Verwenden Sie die Lambda-Log-Parser-JSON-Datei zum Schutz von Scannern und Sonden

Wenn Sie sich `Yes - AWS Lambda log parser` für den Vorlagenparameter Activate Scanner & Probe Protection entschieden haben, erstellt diese Lösung eine Konfigurationsdatei mit dem Namen `<stack_name>-app_log_conf.json` und lädt sie in den definierten Amazon S3 S3-Bucket hoch, der zum Speichern CloudFront von Application Load Balancer Balancer-Protokolldateien verwendet wird.

Wenn Sie `<stack_name>-app_log_conf.json` auf Amazon S3 bearbeiten und überschreiben, berücksichtigt die `Log Parser` Lambda-Funktion die neuen Werte bei der Verarbeitung neuer AWS WAF WAF-Protokolldateien. Im Folgenden finden Sie eine Beispiel-Konfigurationsdatei:

Screenshot der Konfigurationsdatei

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

Zu den Parametern gehören die folgenden:

- Allgemeines:
  - Fehlerschwellenwert (erforderlich) — Die maximal zulässige Anzahl fehlerhafter Anfragen pro Minute und IP-Adresse. Diese Lösung verwendet den Wert, den Sie bei der Bereitstellung oder Aktualisierung des CloudFormation Stacks definiert haben.

  - Sperrzeitraum (erforderlich) — Der Zeitraum (in Minuten), in dem die entsprechenden IP-Adressen gesperrt werden sollen. Diese Lösung verwendet den Wert, den Sie bei der Bereitstellung oder Aktualisierung des CloudFormation Stacks definiert haben.
  - Fehlercodes — Der Rückgabestatuscode wurde als Fehler angesehen. Standardmäßig betrachtet die Liste die folgenden HTTP-Statuscodes als Fehler:`400 (Bad Request)`, `401 (Unauthorized)`403 (Forbidden),`404 (Not Found)`, und`405 (Method Not Allowed)`.
- URI-Liste — Verwenden Sie diese Liste, um einen benutzerdefinierten Schwellenwert für Anfragen und einen Sperrzeitraum für bestimmte Anfragen zu definieren. URLs Standardmäßig ist diese Liste leer.

Wenn Anwendungszugriffsprotokolle in eintreffen AppAccessLogBucket, verarbeitet die `Log Parser` Lambda-Funktion sie anhand der Konfigurationen in Ihrer Konfigurationsdatei. Die Lösung schreibt das Ergebnis in eine Ausgabedatei mit dem Namen `<stack_name>`-app_log_out.json` im selben Bucket. Wenn die Ausgabedatei eine Liste der als Angreifer identifizierten IP-Adressen enthält, fügt die Lösung sie dem WAF-IP-Set für Scanner & Probe hinzu und blockiert sie am Zugriff auf Ihre Anwendung. Wenn die Ausgabedateien keine IP-Adressen haben, überprüfen Sie, ob Ihre Konfigurationsdatei gültig ist oder ob das Ratenlimit gemäß der Konfigurationsdatei überschritten wurde.

Verwenden Sie Land und URI im HTTP Flood Athena Log Parser

Sie können in der Athena-Abfrage nach IPs Land und URI gruppieren, um HTTP-Flood-Angriffe mit unvorhersehbaren URI-Mustern zu erkennen und zu blockieren. Wählen Sie dazu beim Starten des Stacks eine der Optionen (`Country`,`URI`,`Country and URI`) für den Athena-Abfrageparameter Group By Requests in HTTP Flood aus.

Mithilfe des Parameters Schwellenwert für Anfragen nach Land können Sie auch einen Schwellenwert für Anfragen nach Land eingeben. Beispiel, `{"TR": 50,"ER":150}`. Die Lösung verwendet diese Schwellenwerte für Anfragen, die aus diesen angegebenen Ländern stammen. Die Lösung verwendet den Standardschwellenwert für Anfragen aus anderen Ländern.

> **Note**
>
> Wenn Sie einen Schwellenwert nach Ländern definieren, nimmt die Lösung das Land automatisch in die Gruppierungsklausel der Athena-Abfrage auf. Weitere Informationen finden Sie in der Parametertabelle in Schritt 1. Starten Sie den Stack.

Die Lösung zählt den Schwellenwert für Anfragen standardmäßig in einem Zeitraum von fünf Minuten. Dies ist mit dem Parameter Athena Query Run Time Schedule (Minute) konfigurierbar.

> **Note**
>
> Die Athena-Abfrage berechnet den Schwellenwert pro Minute, indem der Anforderungsschwellenwert durch den Zeitraum dividiert wird. Beispiel:
> Schwellenwert für Anfragen (Standardschwellenwert oder Schwellenwert nach Ländern): 100
> Laufzeitplan für Athena Query: 5
> Schwellenwert für Anfragen pro Minute: 20 = 100/5

Amazon Athena Athena-Abfragen anzeigen

Wenn Sie die Vorlagenparameter Activate HTTP Flood Protection oder Activate Scanner & Probe Protection ausgewählt `Yes - Amazon Athena log parser` haben, erstellt und führt diese Lösung Athena-Abfragen für CloudFront ALB (`ScannersProbesLogParser`) oder AWS WAF-Logs (`HTTPFloodLogParser`) aus, analysiert die Ausgabe und aktualisiert AWS WAF entsprechend.

Um die Leistung zu verbessern und die Kosten niedrig zu halten, partitioniert die Lösung Protokolle auf der Grundlage von Zeitstempeln in den Dateinamen. Die Lösung generiert dynamisch Athena-Abfragen zur Verwendung von Partitionsschlüsseln (Jahr, Monat, Tag und Stunde). Standardmäßig werden Abfragen alle fünf Minuten ausgeführt. Sie können ihre Ausführungszeitpläne konfigurieren, indem Sie den Wert des Vorlagenparameters Athena Query Run Time Schedule (Minute) ändern. Bei jedem Abfragelauf werden standardmäßig die Daten der letzten vier bis fünf Stunden gescannt. Sie können die Datenmenge, die eine Abfrage scannt, konfigurieren, indem Sie den Wert des Vorlagenparameters WAF Block Period ändern. Die Lösung platziert Abfragen auch in separaten Arbeitsgruppen, um den Zugriff auf Abfragen und die Kosten zu verwalten.

> **Note**
>
> Stellen Sie sicher, dass Athena für den Zugriff auf den AWS Glue Glue-Datenkatalog konfiguriert ist. Diese Lösung erstellt den Datenkatalog für Zugriffsprotokolle in AWS Glue und konfiguriert eine Athena-Abfrage zur Verarbeitung der Daten. Wenn Athena nicht korrekt konfiguriert ist, wird die Abfrage nicht ausgeführt. Weitere Informationen finden Sie unter Upgrade auf den neuesten AWSAWS Glue-Datenkatalog step-by-step.

Gehen Sie wie folgt vor, um diese Abfragen anzuzeigen:

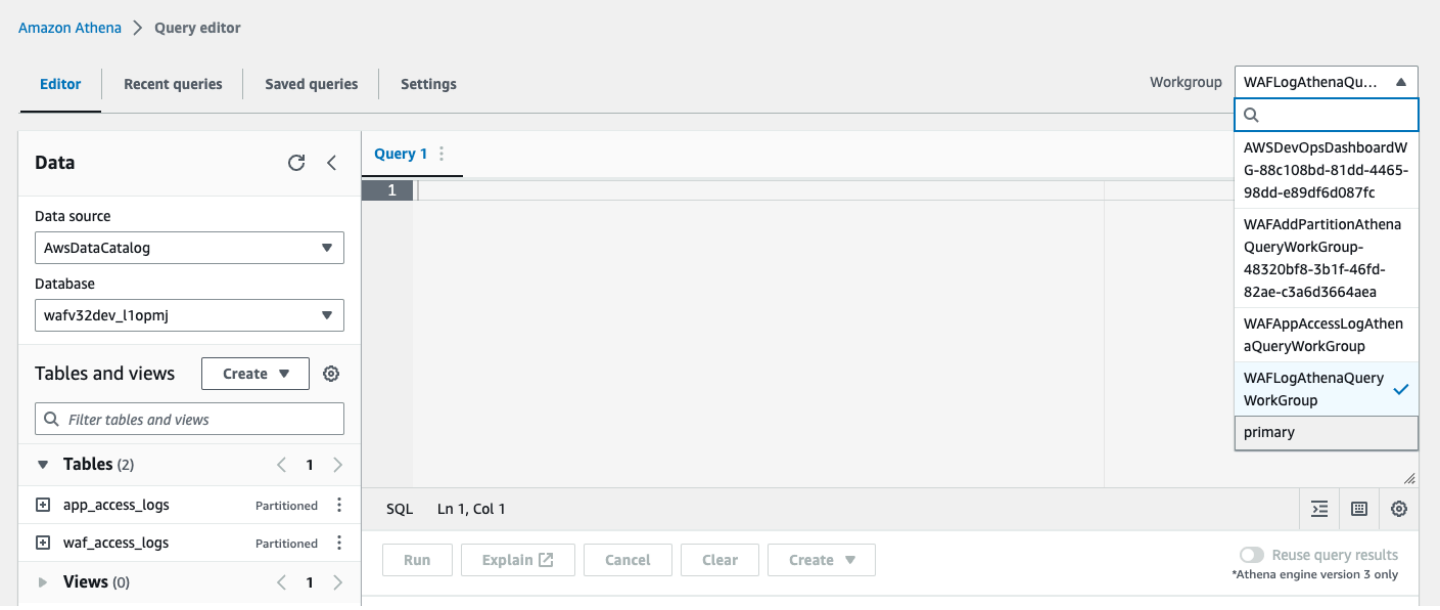
WAF-Protokollabfragen anzeigen

1. Melden Sie sich bei der Amazon Athena Athena-Konsole an.
2. Wählen Sie Abfrage-Editor starten.
3. Wählen Sie die Datenbank für diese Lösung aus.
4. Wählen Sie WAFLogAthenaQueryWorkGroupaus der Drop-down-Liste aus.

> **Note**
>
> Diese Arbeitsgruppe ist nur vorhanden, wenn Sie den Vorlagenparameter „HTTP Flood Protection aktivieren“ ausgewählt `Yes - Amazon Athena log parser` haben.

5. Wählen Sie Switch, um die Arbeitsgruppe zu wechseln.

Screenshot des Athena-Abfrage-Editors, der keine Abfragen zeigt



1. Wählen Sie die Registerkarte Verlauf aus.
2. Wählen Sie SELECT Abfragen aus der Liste aus und öffnen Sie sie.

Abfragen des Anwendungszugriffsprotokolls anzeigen

1. Melden Sie sich bei der Amazon Athena Athena-Konsole an.
2. Wählen Sie die Registerkarte Arbeitsgruppe aus.
3. Wählen Sie WAFAppAccessLogAthenaQueryWorkGroupaus der Liste aus.

> **Note**
>
> Diese Arbeitsgruppe ist nur vorhanden, wenn Sie `Yes - Amazon Athena log parser` für den Vorlagenparameter Activate Scanner & Probe Protection ausgewählt haben.

4. Wählen Sie Arbeitsgruppe wechseln.
5. Wählen Sie die Registerkarte Letzte Abfragen aus.
6. Wählen Sie SELECT Abfragen aus der Liste aus und öffnen Sie sie.

Hinzufügen von Athena-Partitionsabfragen anzeigen

1. Melden Sie sich bei der Amazon Athena Athena-Konsole an.

2. Wählen Sie die Registerkarte Arbeitsgruppe aus.
3. Wählen Sie WAFAddPartitionAthenaQueryWorkGroupaus der Liste aus.

> **Note**
>
> Diese Arbeitsgruppe ist nur vorhanden, wenn Sie `Yes - Amazon Athena log parser` für den Vorlagenparameter Activate HTTP Flood Protection and/or Activate Scanner & Probe Protection ausgewählt haben.

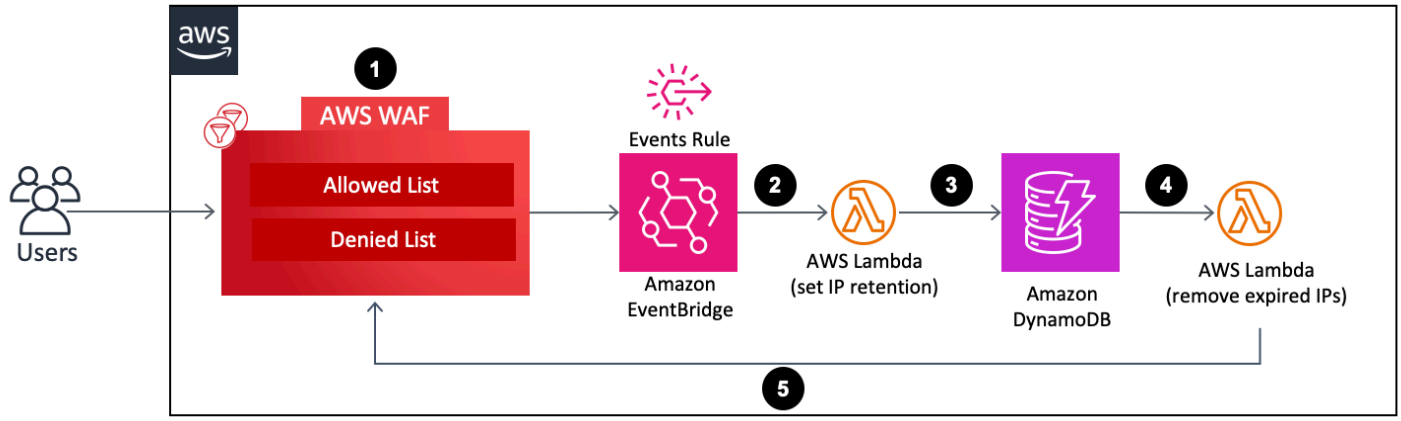
4. Wählen Sie Arbeitsgruppe wechseln aus.
5. Wählen Sie die Registerkarte Verlauf aus.
6. Wählen Sie `ALTER TABLE` Abfragen aus der Liste aus und öffnen Sie sie. Diese Abfragen werden stündlich ausgeführt, um der Athena-Tabelle eine neue stündliche Partition hinzuzufügen.

IP-Aufbewahrung für zugelassene und verweigerte AWS-WAF-IP-Sets konfigurieren

Sie können die IP-Aufbewahrung für zugelassene und verweigerte AWS-WAF-IP-Sets konfigurieren, die die Lösung erstellt. In den folgenden Abschnitten wird erklärt, wie es funktioniert, und es werden die Schritte zur Einrichtung beschrieben.

Funktionsweise

Architekturdiagramm, das die Listen der erlaubten und verweigerten AWS WAF und andere AWS-Ressourcen darstellt



1. Wenn ein Benutzer den WAF-IP-Satz „Zulässig“ oder „Verweigert“ aktualisiert (eine IP-Adresse hinzufügt oder löscht), ruft diese Aktion einen `UpdateIPSet` AWS-WAF-API-Aufruf auf und erzeugt ein Ereignis.
2. Eine EventBridgeAmazon-Ereignisregel erkennt die Ereignisse anhand eines vordefinierten Ereignismusters und ruft eine Lambda-Funktion auf, um die Aufbewahrungsfrist für alle IP-Adressen festzulegen, die nach dem Update im IP-Set vorhanden sind.
3. Die Lambda-Funktion verarbeitet die Ereignisse, extrahiert relevante Daten für die IP-Aufbewahrung (z. B. IP-Satzname, ID, Bereich, IP-Adressen) und fügt sie in eine DynamoDB-Tabelle ein. Außerdem wird für jedes DynamoDB-Element ein `ExpirationTime` Attribut eingefügt. Die Lösung berechnet die Ablaufzeit, indem sie der Ereigniszeit einen benutzerdefinierten Aufbewahrungszeitraum hinzufügt. In der Tabelle sind DynamoDB Streams und Time to Live (TTL) aktiviert. Das TTL-Attribut ist. `ExpirationTime`
4. Wenn ein Element seine Ablaufzeit erreicht, wird TTL aufgerufen und DynamoDB löscht das Element nach Ablauf der Ablaufzeit aus der Tabelle. Nach dem Löschen des Elements wird das gelöschte Element dem DynamoDB-Stream hinzugefügt, der eine Lambda-Funktion für die Downstream-Verarbeitung aufruft.
5. Die Lambda-Funktion ruft die Informationen über das gelöschte Element aus dem DynamoDB-Stream ab und führt einen AWS-WAF-API-Aufruf durch, um die im Element enthaltenen abgelaufenen IP-Adressen aus dem AWS-WAF-Ziel-IP-Set zu entfernen.

Schalten Sie die IP-Aufbewahrung ein

Gehen Sie wie folgt vor, um die IP-Aufbewahrung zu aktivieren:

1. Geben Sie im Cloudformation-Stack, den Sie bereitstellen oder aktualisieren, den IP-Aufbewahrungszeitraum (Minuten) für den zulässigen IP-Satz und den IP-Aufbewahrungszeitraum (Minuten) für den abgelehnten IP-Satz ein. Die Mindestaufbewahrungsdauer beträgt 15 Minuten. Die Lösung behandelt jede Zahl zwischen `0` und `15` als`15`. Weitere Informationen zur Bereitstellungskonfiguration finden Sie in Schritt 1. Starten Sie den Stack.
2. Geben Sie eine E-Mail-Adresse ein, wenn Sie eine E-Mail-Benachrichtigung erhalten möchten, wenn abgelaufene IP-Adressen aus dem AWS WAF WAF-IP-Set entfernt werden. Wenn Sie eine E-Mail-Benachrichtigung erhalten möchten, müssen Sie das Abonnement über den Link in der E-Mail bestätigen, die Sie nach der erfolgreichen Bereitstellung der Lösung erhalten. Weitere Informationen zur Bereitstellungskonfiguration finden Sie in Schritt 1. Starten Sie den Stack.

3. Aktualisieren Sie den AWS-WAF-IP-Satz, indem Sie IP-Adressen hinzufügen oder löschen. Dadurch wird der IP-Aufbewahrungsprozess initiiert und ein DynamoDB-Element erstellt, einschließlich einer IP-Ablaufliste. Diese Ablaufliste besteht aus IP-Adressen, die nach der Aktualisierung im AWS WAF WAF-IP-Set vorhanden sind.
4. Sobald das DynamoDB-Element seine Ablaufzeit erreicht hat und aus der Tabelle gelöscht wurde, löscht die Lösung die IP-Adressen, die in der IP-Ablaufliste des Elements enthalten sind, aus dem WAF-IP-Set.

> **Note**
>
> Je nachdem, zu welchem Zeitpunkt DynamoDB ein Objekt löscht, dessen TTL abgelaufen ist, kann der tatsächliche Löschvorgang einer abgelaufenen IP-Adresse aus dem AWS-WAF-IP-Set variieren. Das Löschen von DynamoDB-TTL hängt hauptsächlich von der Größe und dem Aktivitätsgrad einer Tabelle ab. Erwarten Sie eine Verzögerung beim AWS-WAF-Löschvorgang aufgrund der möglichen Verzögerung beim DynamoDB-Löschvorgang. Im Allgemeinen löscht die Lösung kurz nach dem Löschen von DynamoDB-TTL abgelaufene IP-Adressen aus dem AWS-WAF-IP-Set. Weitere Informationen finden Sie unter DynamoDB Time to Live (TTL) im Amazon DynamoDB Developer Guide.

Erstellen Sie ein Überwachungs-Dashboard

AWS empfiehlt, für jeden kritischen Endpunkt ein benutzerdefiniertes Basisüberwachungssystem zu konfigurieren. Informationen zum Erstellen und Verwenden von benutzerdefinierten Metrikansichten finden Sie unter CloudWatch Dashboards — Benutzerdefinierte Metrikansichten erstellen und verwenden und CloudWatch Amazon-Dashboards verwenden.

Der folgende Dashboard-Screenshot zeigt ein Beispiel für ein benutzerdefiniertes Basisüberwachungssystem.

Screenshot des CloudFront Dashboards

Das Dashboard zeigt die folgenden Metriken an:

- Zulässige und blockierte Anfragen — Zeigt an, ob Sie einen Anstieg an erlaubten Zugriffen (doppelt so viel wie bei normalen Zugriffen zu Spitzenzeiten) oder blockierten Zugriffen (jeder Zeitraum, in dem mehr als 1.000 blockierte Anfragen identifiziert werden) erhalten. CloudWatch sendet eine Warnung an einen Slack-Channel. Sie können diese Metrik verwenden, um bekannte DDo S-Angriffe (wenn die Anzahl blockierter Anfragen zunimmt) oder eine neue Version eines Angriffs (wenn die Anfragen auf das System zugreifen dürfen) zu verfolgen.

  > **Note**
  >
  > Hinweis: Die Lösung bietet diese Metrik.

- BytesDownloaded vs Uploaded — Hilft zu erkennen, wann ein DDo S-Angriff auf einen Dienst abzielt, der normalerweise keinen großen Zugriff auf ausgelastete Ressourcen erhält (z. B. das Senden MBs von Informationen für einen bestimmten Satz von Anforderungsparametern durch eine Suchmaschinenkomponente).
- ELB-Spillover und Warteschlangenlänge — Hilft zu überprüfen, ob ein DDo S-Angriff die Infrastruktur beschädigt und der Angreifer die AWS-WAF-Ebene CloudFront umgeht und direkt ungeschützte Ressourcen angreift.

- Anzahl der ELB-Anfragen — Hilft bei der Identifizierung von Schäden an der Infrastruktur. Diese Metrik zeigt, ob der Angreifer die Schutzschicht umgeht oder ob Sie eine CloudFront Cache-Regel überprüfen sollten, um die Cache-Trefferquote zu erhöhen.
- ELB Healthy Host — Sie können dies als weitere Metrik zur Systemintegritätsprüfung verwenden.
- ASG-CPU-Auslastung — Hilft zu erkennen CloudFront, ob der Angreifer AWS WAF und Elastic Load Balancing umgeht. Sie können diese Metrik auch verwenden, um den Schaden eines Angriffs zu identifizieren.

Behandeln Sie falsche XSS-Positivmeldungen

Diese Lösung konfiguriert eine AWS-WAF-Regel, die häufig untersuchte Elemente eingehender Anfragen überprüft, um XSS-Angriffe zu identifizieren und zu blockieren. Dieses Erkennungsmuster ist weniger effektiv, wenn Ihr Workload es legitimen Benutzern ermöglicht, HTML zu verfassen und einzureichen, beispielsweise mithilfe eines Rich-Text-Editors in einem Content-Management-System. In diesem Szenario sollten Sie eine Ausnahmeregel erstellen, die die standardmäßige XSS-Regel für bestimmte URL-Muster umgeht, die Rich-Text-Eingaben akzeptieren, und alternative Mechanismen implementieren, um die ausgeschlossenen URLs zu schützen. URLs

Darüber hinaus können einige Bild- oder benutzerdefinierte Datenformate zu Fehlalarmen führen, da sie Muster enthalten, die auf einen möglichen XSS-Angriff in HTML-Inhalten hinweisen. Beispielsweise kann eine SVG-Datei ein `<script>` Tag enthalten. Wenn Sie diese Art von Inhalten von legitimen Benutzern erwarten, passen Sie Ihre XSS-Regeln eng an, um HTML-Anfragen zuzulassen, die diese anderen Datenformate enthalten.

Gehen Sie wie folgt vor, um die XSS-Regel so zu aktualisieren, URLs dass sie diejenigen ausschließt, die HTML als Eingabe akzeptieren. Detaillierte Anweisungen finden Sie im Amazon WAF Developer Guide.

1. Melden Sie sich bei der AWS WAF WAF-Konsole an.
2. Erstellen Sie eine übereinstimmende Zeichenfolge oder eine Regex-Bedingung.
3. Konfigurieren Sie die Filtereinstellungen, um den URI zu überprüfen und Werte aufzulisten, die Sie anhand der XSS-Regel akzeptieren möchten.
4. Bearbeiten Sie die XSS-Regel dieser Lösung und fügen Sie die neue Bedingung hinzu, die Sie erstellt haben.

   Um beispielsweise alle URLs aus der Liste auszuschließen, wählen Sie Folgendes für Wann eine Anfrage aus:

- tut nicht
- entspricht mindestens einem der Filer in der Bedingung für die Übereinstimmung mit der Zeichenfolge
- XSS-Zulassungsliste

Fehlerbehebung

Wenn Sie Hilfe zu dieser Lösung benötigen, wenden Sie sich an den Support, um eine Support-Anfrage für diese Lösung zu eröffnen.

Kontaktieren Sie AWS Support.

Wenn Sie über AWS Business Support+, AWS Enterprise Support oder Unified Operations verfügen, können Sie das AWS Support Center nutzen, um fachkundige Support zu dieser Lösung zu erhalten. In den folgenden Abschnitten finden Sie entsprechende Anweisungen.

Fall erstellen

1. Öffnen Sie das Support Center.
2. Wählen Sie Create case (Fall erstellen) aus.

Wie können wir helfen?

1. Wählen Sie Technisch.
2. Wählen Sie für Service die Option Lösungen aus.
3. Wählen Sie als Kategorie die Option Security Automations for AWS WAF aus.
4. Für Schweregrad die Option, die am besten zu Ihrem Anwendungsfall passt.
5. Wenn Sie den Service, die Kategorie und den Schweregrad eingeben, werden in der Benutzeroberfläche Links zu häufig gestellten Fragen zur Fehlerbehebung angezeigt. Wenn Sie Ihre Frage mit diesen Links nicht lösen können, wählen Sie Nächster Schritt: Zusätzliche Informationen.

Zusätzliche Informationen

1. Geben Sie als Betreff einen Text ein, der Ihre Frage oder Ihr Problem zusammenfasst.
2. Beschreiben Sie unter Beschreibung das Problem detailliert, einschließlich des Namens dieser Lösung und der Version, die Sie verwenden, z. B. in diesem Beispiel: Security Automations for AWS WAF vX.Y.Z.
3. Wählen Sie Dateien anhängen.

4. Fügen Sie die Informationen bei, die der Support zur Bearbeitung der Anfrage benötigt.

Helfen Sie uns, Ihren Fall schneller zu lösen

1. Geben Sie die angeforderten Informationen ein.
2. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).

Löse es jetzt oder kontaktiere uns

1. Sehen Sie sich die Solve Now-Lösungen an.
2. Wenn Sie Ihr Problem mit diesen Lösungen nicht lösen können, wählen Sie Kontakt, geben Sie die angeforderten Informationen ein und klicken Sie auf Absenden.

Entwicklerhandbuch

Dieser Abschnitt enthält den Quellcode für die Lösung.

Quellcode

Besuchen Sie unser GitHub Repository, um die Vorlagen und Skripte für diese Lösung herunterzuladen und Ihre Anpassungen mit anderen zu teilen.

Die Vorlagen dieser Lösung werden mit dem AWS CDK generiert. Weitere Informationen finden Sie in der Datei README.md.

Referenz

Dieser Abschnitt enthält Informationen zu einer optionalen Funktion zum Sammeln einzigartiger Messwerte für diese Lösung, Hinweise auf verwandte Ressourcen und eine Liste der Entwickler, die zu dieser Lösung beigetragen haben.

Anonymisierte Datenerfassung

Diese Lösung beinhaltet eine Option zum Senden von Betriebsmetriken an AWS. Wir verwenden diese Daten, um besser zu verstehen, wie Kunden diese Lösung und die damit verbundenen Services und Produkte nutzen. Wenn sie aktiviert ist, sammelt die Lösung die folgenden Informationen und sendet sie bei der ersten Bereitstellung der CloudFormation Vorlage an AWS:

- Lösungs-ID — Die AWS-Lösungs-ID
- Eindeutige ID (UUID) — Zufällig generierte, eindeutige Kennung für jede Bereitstellung dieser Lösung
- Zeitstempel — Zeitstempel für die Datenerfassung
- Lösungskonfiguration — Beim ersten Start wurden die Funktionen aktiviert und die Parameter wurden festgelegt
- Lebenszyklus — Wie lange hat der Kunde diese Lösung genutzt (basierend auf Stack Delete)
- Parser-Daten protokollieren:
  - Die Anzahl der IP-Adressen im Scanner & Probe-IP-Set, im Bad-Bot-IP-Set und im HTTP-Flood-IP-Set, das blockiert werden soll
  - Die Anzahl der verarbeiteten und blockierten Anfragen
- IP listet Parserdaten auf:
  - Die Anzahl der IP-Adressen im IP-Satz der Reputationslisten
  - Die Anzahl der verarbeiteten und blockierten Anfragen
- IP-Aufbewahrungsdaten — Die Anzahl der abgelaufenen IP-Adressen, die aus dem IP-Satz „Zulässig“ oder „Abgelehnt“ entfernt wurden

AWS ist Eigentümer der im Rahmen dieser Umfrage gesammelten Daten. Die Datenerfassung unterliegt der AWS-Datenschutzrichtlinie. Um diese Funktion zu deaktivieren, führen Sie die folgenden Schritte aus, bevor Sie die CloudFormation AWS-Vorlage starten.

1. Laden Sie `aws-waf-security-automations.template` AWS CloudFormation auf Ihre lokale Festplatte herunter.
2. Öffnen Sie die CloudFormation Vorlage mit einem Texteditor.
3. Ändern Sie den Abschnitt zur CloudFormation Vorlagenzuweisung von:

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

   auf:

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

4. Melden Sie sich in der CloudFormation AWS-Konsole an.
5. Wählen Sie Stack erstellen aus.
6. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus.
7. Wählen Sie unter Vorlagendatei hochladen die Option Datei auswählen und wählen Sie die bearbeitete Vorlage von Ihrem lokalen Laufwerk aus.
8. Wählen Sie Weiter und folgen Sie den Schritten in Schritt 1. Starten Sie den Stack.

Zugehörige Ressourcen

Verwandte AWS-Whitepapers

- Bewährte AWS-Methoden für DDo S-Resiliency

Zugeordnete Blogbeiträge zum Thema AWS-Sicherheit

- So verhindern Sie Hotlinking mithilfe von AWS WAF CloudFront, Amazon und Referer Checking

IP-Reputationslisten von Drittanbietern

- Webseite von Spamhaus DROP List
- IP-Liste neuer Bedrohungen von Proofpoint
- Liste der Tor-Exit-Knoten

Mitwirkende

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

Überarbeitungen

Besuchen Sie CHANGELOG.md in unserem GitHub Repository, um versionsspezifische Verbesserungen und Korrekturen nachzuverfolgen.

Hinweise

Dieser Implementierungsleitfaden dient nur zu Informationszwecken. Es stellt die aktuellen AWS-Produktangebote und -praktiken zum Zeitpunkt der Veröffentlichung dieses Dokuments dar, die sich ohne vorherige Ankündigung ändern können. Kunden sind dafür verantwortlich, die Informationen in diesem Dokument und die Nutzung von AWS-Produkten oder -Services, die jeweils „wie sie sind“ und ohne jegliche ausdrückliche oder stillschweigende Garantie bereitgestellt werden, selbst zu beurteilen. Dieses Dokument stellt keine Garantien, Zusicherungen, vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Die WAF-Lösung Security Automations for AWS ist unter den Bedingungen der Apache License Version 2.0 lizenziert.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.