구현 안내서

에 대한 보안 자동화 AWS WAF

에 대한 보안 자동화 AWS WAF: 구현 안내서

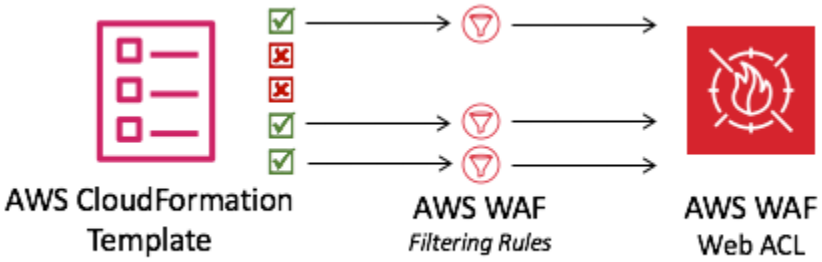
Table of Contents

에서 보안 자동화를 사용하여 웹 기반 공격을 필터링하는 단일 웹 액세스 제어 목록 자동 배포 AWS WAF

게시일: 2016년 9월(마지막 업데이트: 2024년 12월)

AWS WAF 솔루션용 보안 자동화는 일반적인 웹 악용으로부터 애플리케이션을 보호하는 데 도움이 되는 사전 구성된 규칙 세트를 배포합니다. 이 솔루션의 핵심 서비스인는 애플리케이션 가용성에 영향을 미치거나 AWS WAF보안을 손상시키거나 과도한 리소스를 소비할 수 있는 공격 기법으로부터 웹 애플리케이션을 보호하는 데 도움이 됩니다. AWS WAF를 사용하여 사용자 지정 가능한 웹 보안 규칙을 정의할 수 있습니다. 이러한 규칙은 Amazon, Application Load Balancer(APIs) 및 Amazon CloudFront API Gateway와 같은 AWS 리소스에 배포된 웹 애플리케이션 및 애플리케이션 프로그래밍 인터페이스(ALB)를 허용하거나 차단할 트래픽을 제어합니다. 지원되는 리소스 유형에 대한 자세한 내용은 AWS WAF AWS Firewall Manager, 및 AWS Shield Advanced 개발자 안내서AWS WAF의 섹션을 참조하세요.

AWS WAF 규칙을 구성하는 것은 대규모 조직과 소규모 조직, 특히 전용 보안 팀이 없는 조직 모두에게 어렵고 부담스러울 수 있습니다. 이 프로세스를 간소화하기 위해 AWS WAF 솔루션용 보안 자동화는 일반적인 웹 기반 공격을 필터링하도록 설계된 AWS WAF 규칙 집합과 함께 단일 웹 액세스 제어 목록(ACL)을 자동으로 배포합니다. 이 솔루션 템플릿의 초기 구성 중에 포함할 보호 기능을 지정할 AWS CloudFormation 수 있습니다. 이 솔루션을 배포한 후 AWS WAF 는 기존 CloudFront 배포(들) 또는 ALB(들)에 대한 웹 요청을 검사하고 해당하는 경우 차단합니다.



AWS WAF 웹 구성 ACL

이 구현 가이드에서는 Amazon Web Services(AWS) 클라우드에이 솔루션을 배포하기 위한 아키텍처 고려 사항, 구성 단계 및 운영 모범 사례를 설명합니다. 여기에는 AWS 보안 및 가용성 AWS 모범 사례를 사용하여이 솔루션을 배포하는 데 필요한 보안, 컴퓨팅, 스토리지 및 기타 서비스를 시작 AWS, 구성 및 실행하는 CloudFormation 템플릿에 대한 링크가 포함되어 있습니다.

이 안내서의 정보는 AWS WAF CloudFront, ALBs및와 같은 서비스에 대한 AWS 실무 지식을 갖췄습니다AWS Lambda. 또한 일반적인 웹 기반 공격 및 완화 전략에 대한 기본 지식이 필요합니다.

> **Note**
>
> 버전 3.0.0부터이 솔루션은 최신 버전의 AWS WAF 서비스API(AWS WAF V2)를 지원합니다.

이 가이드는 IT 관리자, 보안 엔지니어, 엔지니어, DevOps 개발자, 솔루션 아키텍트 및 웹 사이트 관리자를 대상으로 합니다.

> **Note**
>
> 이 솔루션을 AWS WAF 규칙 구현의 시작점으로 사용하는 것이 좋습니다. 소스 코드를 사용자 지정하고, 새 사용자 지정 규칙을 추가하고, 필요에 따라 더 많은 AWS WAF 관리형 규칙을 활용할 수 있습니다.

이 탐색 테이블을 사용하여 다음 질문에 대한 답을 빠르게 찾을 수 있습니다.

다음을 수행하려는 경우 . . .	읽기 . . .
이 솔루션을 실행하는 데 드는 비용을 파악합니다. 이 솔루션을 실행하는 데 드는 총 비용은 활성화된 보호와 수집, 저장 및 처리된 데이터의 양에 따라 달라집니다.	비용
이 솔루션의 보안 고려 사항을 이해합니다.	보안
이 솔루션에서 지원되는 AWS 리전 를 파악합니다.	지원됨 AWS 리전
이 솔루션에 포함된 CloudFormation 템플릿을 보거나 다운로드하여이 솔루션의 인프라 리소스(“스택”)를 자동으로 배포합니다.	AWS CloudFormation 템플릿

다음을 수행하려는 경우 . . .	읽기 . . .
Support 를 사용하여 솔루션을 배포, 사용 또는 문제를 해결할 수 있습니다.	Support
소스 코드에 액세스하고 선택적으로 AWS Cloud Development Kit (AWS CDK) 를 사용하여 솔루션을 배포합니다.	GitHub 리포지토리

기능 및 이점

AWS WAF 솔루션용 보안 자동화는 다음과 같은 기능과 이점을 제공합니다.

AWS Managed Rules 규칙 그룹으로 웹 애플리케이션 보호

AWS Managed Rules for AWS WAF는 일반적인 애플리케이션 취약성 또는 기타 원치 않는 트래픽에 대한 보호를 제공합니다. 이 솔루션에는 AWS 관리형 IP 평판 규칙 그룹, AWS 관리형 기준 규칙 그룹 및 AWS 관리형 사용 사례별 규칙 그룹이 포함됩니다. 최대 웹 ACL 용량 단위(WCU) 할당량ACL까지 웹에 대해 하나 이상의 규칙 그룹을 선택할 수 있습니다.

사전 정의된 서비스 장애 사용자 지정 규칙을 사용하여 계층 HTTP 7 서비스 장애 방지 제공

HTTP Flood 사용자 지정 규칙은 고객이 정의한 기간 동안 웹 계층 분산 Denial-of-Service(DDoS) 공격으로부터 보호합니다. 다음 옵션 중 하나를 선택하여이 규칙을 활성화할 수 있습니다.

- AWS WAF 속도 기반 규칙
- Lambda 로그 구문 분석기
- Amazon Athena 로그 구문 분석기

Lambda 로그 구문 분석기 또는 Athena 로그 구문 분석기 옵션을 사용하면 요청 할당량을 100 미만으로 정의할 수 있습니다. 이 접근 방식은 속도 기반 규칙에 필요한 AWS WAF 할당량에 도달하지 않는 데 도움이 될 수 있습니다. 자세한 내용은 구문 분석기 옵션 로그를 참조하세요.

필터링 조건에 국가 및 Uniform Resource Identifier(URI)를 추가하여 Athena 로그 구문 분석기를 개선할 수도 있습니다. 이 접근 방식은 예측할 수 없는 URI 패턴이 있는 HTTP홍수 공격을 식별하고 차단합니다. 자세한 내용은 HTTP Flood Athena 로그 구문 분석기URI의 국가 및 사용을 참조하세요.

사전 정의된 스캐너 및 프로브 사용자 지정 규칙을 사용하여 취약성 악용 차단

스캐너 및 프로브 사용자 지정 규칙은 오리진에서 생성된 비정상적인 양의 오류와 같은 의심스러운 동작을 검색하는 애플리케이션 액세스 로그를 구문 분석합니다. 그런 다음 고객이 정의한 기간 동안 의심스러운 소스 IP 주소를 차단합니다. Lambda 로그 구문 분석기 또는 Athena 로그 구문 분석기 중 하나를 선택하여이 규칙을 활성화할 수 있습니다. 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

사전 정의된 잘못된 봇 사용자 지정 규칙을 사용하여 침입 감지 및 편향

잘못된 봇 사용자 지정 규칙은 허니팟 엔드포인트를 설정합니다. 허니팟 엔드포인트는 시도된 공격을 유인하고 편향하기 위한 보안 메커니즘입니다. 웹 사이트에 엔드포인트를 삽입하여 콘텐츠 스크레이퍼 및 잘못된 봇의 인바운드 요청을 감지할 수 있습니다. 감지되면 동일한 오리진의 후속 요청이 차단됩니다. 자세한 내용은 웹 애플리케이션에 Honeypot 링크 포함을 참조하세요.

사전 정의된 IP 평판 목록 사용자 지정 규칙을 사용하여 악성 IP 주소 차단

IP 평판 목록 사용자 지정 규칙은 차단할 새 IP 범위가 있는지 서드 파티 IP 평판 목록을 시간별로 확인합니다. 이러한 목록에는 Spamhaus Don't Route or Peer(DROP) 및 ExtendedDROP(EDROP) 목록, Proofpoint Emerging Threats IP 목록 및 Tor 출구 노드 목록이 포함됩니다.

사전 정의된 허용 및 거부 IP 목록 사용자 지정 규칙을 사용하여 수동 IP 구성 제공

허용 및 거부된 IP 목록 사용자 지정 규칙을 사용하면 허용 또는 거부하려는 IP 주소를 수동으로 삽입할 수 있습니다. 허용 및 거부 IP 목록에서 IP 보존이 설정된 시간에 만료되도록 구성할 수도 IPs 있습니다.

자체 모니터링 대시보드 구축

이 솔루션은 허용된 요청, 차단된 요청 및 기타 관련 지표와 같은 Amazon CloudWatch 지표를 내보냅니다. 사용자 지정 대시보드를 구축하여 이러한 지표를 시각화하고에서 제공하는 공격 및 보호 패턴에 대한 인사이트를 얻을 수 있습니다 AWS WAF. 자세한 내용은 빌드 모니터링 대시보드를 참조하세요.

Service Catalog AppRegistry 및 AWS Systems Manager Application Manager와 통합

이 솔루션에는 솔루션의 CloudFormation 템플릿과 기본 리소스를 Service Catalog AppRegistry AppRegistry 와 AWS Systems Manager Application Manager 모두에 애플리케이션으로 등록하는 AWS Service Catalog 리소스가 포함되어 있습니다. 이 통합을 통해 솔루션의 리소스를 중앙에서 관리할 수 있습니다.

사용 사례

게시일: 2016년 9월(마지막 업데이트: 2023년 5월)

다음은이 솔루션을 사용하기 위한 사용 사례의 예입니다. 이 목록에 국한되지 않는 혁신적인 방식으로 이 솔루션을 사용자 지정할 수 있습니다.

규칙 설정 AWS WAF 자동화

AWS WAF 는 웹 애플리케이션을 일반적인 공격으로부터 보호하지만 AWS WAF 규칙 설정은 복잡하고 시간이 많이 걸릴 수 있습니다. 이 솔루션은 CloudFormation 템플릿으로 계정에 AWS WAF 규칙 세트를 자동으로 배포합니다. 이렇게 하면 AWS WAF 규칙을 직접 구성할 필요가 없으며 더 AWS WAF 빠르게 시작할 수 있습니다.

계층 7 HTTP 서비스 장애 방지 사용자 지정

이 솔루션은 HTTP 서비스 장애 방지를 활성화하는 세 가지 옵션을 제공합니다. DDoS 공격에 대한 보호를 얻기 위해 필요에 맞는 옵션을 선택할 수 있습니다. 자세한 내용은 기능 및 이점에서 미리 정의된 Flood 사용자 지정 규칙을 사용하여 계층 HTTP 7 플러드 보호 제공을 참조하세요.

소스 코드를 활용하여 사용자 지정을 적용하거나 자체 보안 자동화를 구축합니다.

이 솔루션은 AWS WAF 및 기타 서비스를 사용하여에서 보안 자동화를 구축하는 방법에 대한 예를 제공합니다 AWS 클라우드. 의 오픈 소스 코드를 GitHub 사용하면 사용자 지정을 적용하거나 필요에 맞는 자체 보안 자동화를 구축할 수 있습니다.

개념 및 정의

이 섹션에서는 주요 개념을 설명하고이 솔루션과 관련된 용어를 정의합니다.

ALB 로그

이 솔루션은 ALB 리소스에 대한 로그를 사용합니다. 이 솔루션의 스캐너 및 프로브 보호 규칙은 이러한 로그를 검사합니다.

Athena 로그 파서

Amazon Athena는 오픈 소스 프레임워크를 기반으로 구축된 서버리스 대화형 분석 서비스로, 오픈 테이블 및 파일 형식을 지원합니다. 이 솔루션은 예약된 Athena 쿼리를 실행하여 AWS WAF CloudFront, 또는 사용자가 HTTP Flood Protection 규칙 또는 Scanner & Probe Protection 규칙을 활성화할 `yes – Amazon Athena log parser` 때를 선택하는 경우 ALB 로그를 검사합니다.

AWS WAF 규칙

AWS WAF 규칙은 다음을 정의합니다.

- HTTP(S) 웹 요청을 검사하는 방법
- 검사 기준과 일치할 때 요청에 대해 수행할 작업

규칙 그룹 또는 웹의 컨텍스트에서만 규칙을 정의합니다ACL.

CloudFront 로그

이 솔루션은 CloudFront 리소스에 대한 로그를 사용합니다. 이 솔루션의 스캐너 및 프로브 보호 규칙은 이러한 로그를 검사합니다.

IP 세트

IP 세트는 사용하려는 IP 주소 및 IP 주소 범위 모음을 제공합니다.

규칙 문에서 함께. IP 세트는 AWS 리소스입니다.

Lambda 로그 구문 분석기

이 솔루션은 Amazon Simple Storage Service(Amazon S3) 객체 생성 이벤트에서 호출되는 Lambda 함수를 실행합니다. Lamba 함수는의 검사를 시작하거나 AWS WAF CloudFront사용자가 HTTP Flood Protection 규칙 또는 Scanner & Probe Protection 규칙을 활성화할 `yes – AWS Lambda log parser` 때를 선택하는 경우 ALB 로그합니다.

관리형 규칙 그룹

관리형 규칙 그룹은 AWS 및 AWS Marketplace 판매자가 자동으로 작성하고 유지 관리하는 사전 정의된 ready-to-use 규칙의 모음입니다. AWS WAF 요금은 관리형 규칙 그룹의 사용에 적용됩니다.

리소스/엔드포인트 유형

AWS 리소스를 웹과 연결하여 ACLs 보호할 수 있습니다. 이러한 리소스는 API Gateway CloudFront, ALB, AWS AppSync, Amazon Cognito, AWS App Runner 및 AWS Verified Access 리소스입니다. 현재이 솔루션 Amazon은 CloudFront 및를 지원합니다ALB.

WAF 로그

이 솔루션은 웹과 연결된 리소스에 AWS WAF 대해에서 생성된 로그를 사용합니다ACL. 이 솔루션의 HTTP Flood Protection 규칙은 이러한 로그를 검사합니다.

WCU

AWS WAF 는 웹 액세스 제어 목록(ACL) 용량 단위(WCUs)를 사용하여 규칙, 규칙 그룹 및 웹을 실행하는 데 필요한 운영 리소스를 계산하고 제어합니다ACLs.는 규칙 그룹 및 웹WCU을 구성할 때 할당량을 AWS WAF 적용합니다ACLs.가 웹 트래픽을 AWS WAF 검사하는 방법에는 영향을 WCUs 주지 않습니다.

웹 ACL

웹을 ACL 사용하면 보호된 리소스가 응답하는 HTTP(S) 웹 요청을 세밀하게 제어할 수 있습니다.

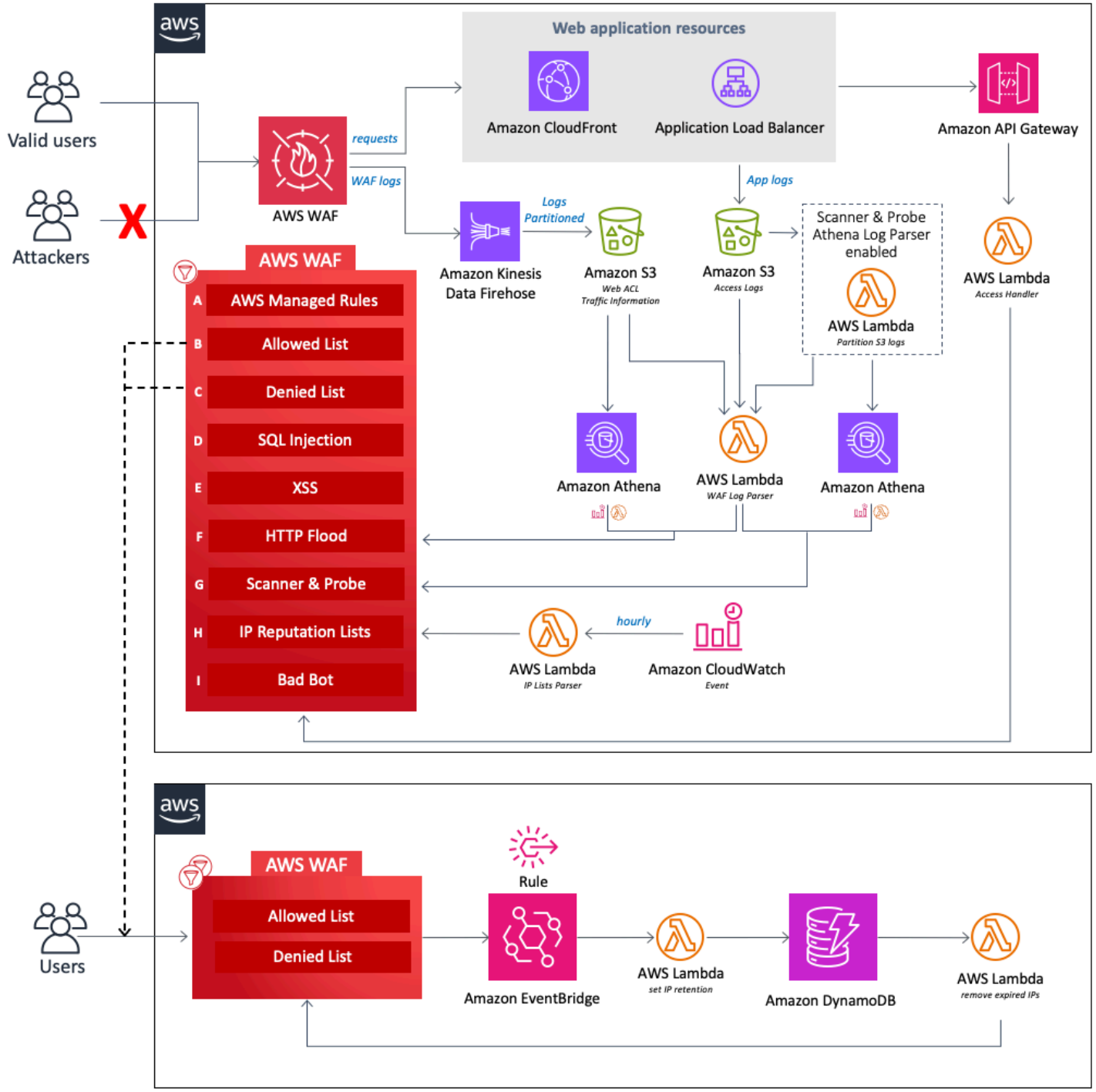
> **Note**
>
> AWS 용어에 대한 일반적인 참조는 AWS 용어집을 참조하세요.

아키텍처 개요

이 섹션에서는 이 솔루션과 함께 배포된 구성 요소에 대한 참조 구현 아키텍처 다이어그램을 제공합니다.

아키텍처 다이어그램

기본 파라미터로이 솔루션을 배포하면에 다음 구성 요소가 배포됩니다 AWS 계정.



의 AWS WAF 아키텍처에 대한 보안 자동화 AWS

설계의 핵심은 AWS WAF 웹 애플리케이션으로 들어오는 모든 요청에 대한 중앙 검사 및 결정 지점 역할을 ACL하는 웹 입니다. CloudFormation 스택의 초기 구성 중에 사용자는 활성화할 보호 구성 요소를 정의합니다. 각 구성 요소는 독립적으로 작동하며 웹에 서로 다른 규칙을 추가합니다ACL.

이 솔루션의 구성 요소는 다음 보호 영역으로 그룹화할 수 있습니다.

> **Note**
>
> 그룹 레이블은 WAF 규칙의 우선 순위 수준을 반영하지 않습니다.

- AWS 관리형 규칙(A) -이 구성 요소에는 IP 평판 규칙 그룹, 기준 규칙 그룹 및 사용 사례별 규칙 그룹이 포함됩니다 AWS Managed Rules . https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html 이러한 규칙 그룹은 자체 규칙을 작성할 필요 없이 일반 애플리케이션 취약성 또는 OWASP 간행물에 설명된 트래픽을 포함한 기타 원치 않는 트래픽의 악용으로부터 보호합니다.
- 수동 IP 목록(B 및 C) - 이러한 구성 요소는 두 가지 AWS WAF 규칙을 생성합니다. 이러한 규칙을 사용하면 허용하거나 거부할 IP 주소를 수동으로 삽입할 수 있습니다. Amazon 규칙 및 Amazon EventBridge DynamoDB를 사용하여 IP 보존을 구성하고 허용 또는 거부된 IP 세트에서 만료된 IP 주소를 제거할 수 있습니다. 자세한 내용은 허용 및 거부 IP 세트에서 AWS WAF IP 보존 구성을 참조하세요.
- SQL 주입(D) 및 XSS (E) - 이러한 구성 요소는 요청의 URI, 쿼리 문자열 또는 본문에서 일반적인 SQL 주입 또는 교차 사이트 스크립팅(XSS) 패턴으로부터 보호하도록 설계된 두 가지 AWS WAF 규칙을 구성합니다.
- HTTP Flood(F) -이 구성 요소는 웹 계층 공격 또는 무차별 포스 로그인 시도와 같이 특정 IP 주소의 많은 요청으로 구성된 DDoS 공격으로부터 보호합니다. 이 규칙을 사용하면 기본 5분 기간 내에 단일 IP 주소에서 허용되는 최대 수신 요청 수를 정의하는 할당량을 설정합니다(Athena 쿼리 실행 시간 일정 파라미터로 구성 가능). 이 임계값을 위반하면 IP 주소의 추가 요청이 일시적으로 차단됩니다. AWS WAF 속도 기반 규칙을 사용하거나 Lambda 함수 또는 Athena 쿼리를 사용하여 AWS WAF 로그를 처리하여이 규칙을 구현할 수 있습니다. HTTP 홍수 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.
- 스캐너 및 프로브(G) -이 구성 요소는 애플리케이션 액세스 로그를 구문 분석하여 오리진에서 생성된 비정상적인 양의 오류와 같은 의심스러운 동작을 검색합니다. 그런 다음 고객이 정의한 기간 동안 의심스러운 소스 IP 주소를 차단합니다. Lambda 함수 또는 Athena 쿼리를 사용하여이 규칙을 구현할 수 있습니다. 스캐너 및 프로브 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.
- IP 평판 목록(H) -이 구성 요소는 서드 파티 IP 평판 목록을 매시간 확인하여 차단할 새 범위를 확인하는 `IP Lists Parser` Lambda 함수입니다. 이러한 목록에는 Spamhaus Don't Route or Peer(DROP) 및 ExtendedDROP(EDROP) 목록, Proofpoint Emerging Threats IP 목록, Tor 출구 노드 목록이 포함됩니다.

- 잘못된 봇(I) -이 구성 요소는 시도된 공격을 유인하고 편향하기 위한 보안 메커니즘인 허니팟을 자동으로 설정합니다. 이 솔루션의 허니팟은 웹 사이트에 삽입하여 콘텐츠 스크레이퍼 및 잘못된 봇의 인바운드 요청을 감지할 수 있는 트랩 엔드포인트입니다. 소스가 허니팟에 액세스하는 경우 `Access Handler` Lambda 함수는 요청을 가로채고 검사하여 IP 주소를 추출한 다음 AWS WAF 블록 목록에 추가합니다.

이 솔루션의 사용자 지정 Lambda 함수 3개 각각은 런타임 지표를에 게시합니다 CloudWatch. 이러한 Lambda 함수에 대한 자세한 내용은 구성 요소 세부 정보를 참조하세요.

AWS Well-Architected 설계 고려 사항

이 솔루션은 고객이 클라우드에서 안정적이고 안전하며 효율적이며 비용 효율적인 워크로드를 설계하고 운영할 수 있도록 지원하는 AWS Well-Architected Framework의 모범 사례를 사용합니다.

이 섹션에서는 Well-Architected Framework의 설계 원칙과 모범 사례가 이 솔루션에 어떤 이점을 제공하는지 설명합니다.

운영 우수성

이 섹션에서는 운영 우수성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 지표를 로 푸시CloudWatch하여 인프라, Lambda 함수, Amazon Data Firehose, API Gateway, Amazon S3 버킷 및 나머지 솔루션 구성 요소에 대한 관찰 가능성을 제공합니다.
- 지속적 통합 및 지속적 제공(CI/CD) 파이프라인을 통해 AWS 솔루션을 개발, 테스트 및 게시합니다. 이를 통해 개발자는 고품질 결과를 일관되게 달성할 수 있습니다.
- 계정에 필요한 모든 리소스를 프로비저닝하는 CloudFormation 템플릿으로 솔루션을 설치할 수 있습니다. 솔루션을 업데이트하거나 삭제하려면 템플릿을 업데이트하거나 삭제하기만 하면 됩니다.

보안

이 섹션에서는 보안 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 모든 서비스 간 통신은 AWS Identity and Access Management (IAM) 역할을 사용합니다.
- 솔루션에서 사용하는 모든 역할은 최소 권한 액세스를 따릅니다. 즉, 서비스가 제대로 작동하는 데 필요한 최소 권한만 포함합니다.
- Amazon S3 버킷 및 DynamoDB를 포함한 모든 데이터 스토리지에는 저장 암호화가 있습니다.

신뢰성

이 섹션에서는 신뢰성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 가능한 경우 AWS 서버리스 서비스(예: Lambda, Firehose, API Gateway, Amazon S3 및 Athena)를 사용하여 서비스 장애로부터 고가용성과 복구를 보장합니다.
- 솔루션에 대한 자동 테스트를 수행하여 오류를 신속하게 감지하고 수정합니다.
- 이 솔루션은 데이터 처리에 Lambda 함수를 사용합니다. 이 솔루션은 Amazon S3 및 DynamoDB에 데이터를 저장하며 기본적으로 여러 가용 영역에 유지됩니다.

성능 효율성

이 섹션에서는 성능 효율성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 서버리스 아키텍처를 사용하여 저렴한 비용으로 높은 확장성과 가용성을 보장합니다.
- 이 솔루션은 데이터를 분할하고 쿼리를 최적화하여 데이터 스캔 양을 줄이고 더 빠른 결과를 달성하여 데이터베이스 성능을 향상시킵니다.
- 솔루션은 매일 자동으로 테스트되고 배포됩니다. 솔루션 아키텍트와 주제 전문가가 솔루션을 검토하여 실험하고 개선할 영역을 찾습니다.

비용 최적화

이 섹션에서는 비용 최적화 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 서버리스 아키텍처를 사용하며 고객은 사용한 만큼만 비용을 지불합니다.
- 솔루션의 컴퓨팅 계층은 pay-per-use 모델을 사용하는 Lambda로 기본 설정됩니다.
- Athena 데이터베이스 및 쿼리는 데이터 스캔 양을 줄이도록 최적화되어 비용을 절감합니다.

지속 가능성

이 섹션에서는 지속 가능성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 관리형 및 서버리스 서비스를 사용하여 백엔드 서비스의 환경 영향을 최소화합니다.

- 이 솔루션의 서버리스 설계는 지속적으로 운영되는 온프레미스 서버의 설치 공간과 비교하여 탄소 발자국을 줄이는 것을 목표로 합니다.

아키텍처 세부 정보

이 섹션에서는이 솔루션을 구성하는 구성 요소 및 AWS 서비스와 이러한 구성 요소가 함께 작동하는 방식에 대한 아키텍처 세부 정보를 설명합니다.

AWS 이 솔루션의 서비스

AWS 서비스	설명	
AWS WAF	Core. AWS WAF 웹ACL, AWS Managed Rules 규칙 그룹, 사용자 지정 규칙 및 IP 세트를 배포합니다. 일반적인 공격을 차단하고 웹 애플리케이션을 보호하기 위해 호출합니다 AWS WAF API.	
Amazon Data Firehose	Core. Amazon S3 버킷에 로그를 전송합니다 AWS WAF .	
Amazon S3	Core. AWS WAF, CloudFront 및 ALB 로그를 저장합니다.	
AWS Lambda	Core. 사용자 지정 규칙을 지원하기 위해 여러 Lambda 함수를 배포합니다.	
Amazon EventBridge	Core. Lambda를 호출하는 이벤트 규칙을 생성합니다.	
Amazon Athena	지원. Athena 로그 파서를 지원하는 Athena 쿼리 및 작업 그룹을 생성합니다.	
AWS Glue	지원. Athena 로그 구문 분석기를 지원하는 데이터베이스와 테이블을 생성합니다.	

AWS 서비스	설명	
Amazon API Gateway	지원. 잘못된 봇 허니팟 엔드포인트를 생성합니다.	
Amazon SNS	지원. Amazon Simple Notification Service(AmazonSNS) 이메일 알림을 전송하여 허용 및 거부 목록에서 IP 보존을 지원합니다.	
AWS Systems Manager	지원. 리소스 운영 및 비용 데이터에 대한 애플리케이션 수준의 리소스 모니터링 및 시각화를 제공합니다.	

로그 구문 분석기 옵션

아키텍처 개요에 설명된 대로 HTTP플러드와 스캐너 및 프로브 보호를 처리하는 세 가지 옵션이 있습니다. 다음 섹션에서는 이러한 각 옵션에 대해 자세히 설명합니다.

AWS WAF 속도 기반 규칙

속도 기반 규칙은 HTTP홍수 방지에 사용할 수 있습니다. 기본적으로 속도 기반 규칙은 요청 IP 주소에 기반하여 요청을 집계하고 속도를 제한합니다. 이 솔루션을 사용하면 클라이언트 IP가 지속적으로 업데이트되는 5분 동안 허용하는 웹 요청 수를 지정할 수 있습니다. IP 주소가 구성된 할당량을 위반하면 는 요청 속도가 구성된 할당량보다 작을 때까지 차단된 새 요청을 AWS WAF 차단합니다.

요청 할당량이 5분당 요청 2,000개를 초과하고 사용자 지정을 구현할 필요가 없는 경우 속도 기반 규칙 옵션을 선택하는 것이 좋습니다. 예를 들어 요청을 계산할 때 정적 리소스 액세스를 고려하지 않습니다.

다양한 기타 집계 키 및 키 조합을 사용하도록 규칙을 추가로 구성할 수 있습니다. 자세한 내용은 집계 옵션 및 키를 참조하세요.

Amazon Athena 로그 구문 분석기

HTTP Flood Protection 및 Scanner & Probe Protection 템플릿 파라미터는 모두 Athena 로그 구문 분석기 옵션을 제공합니다. 활성화되면는 Athena 쿼리와 Athena가 실행, 결과 출력 처리 및 업데이트하도록 조정하는 역할을 하는 예약된 Lambda 함수를 CloudFormation 프로비저닝합니다 AWS WAF. 이 Lambda 함수는 5분마다 실행되도록 구성된 CloudWatch 이벤트에 의해 호출됩니다. 이는 Athena 쿼리 실행 시간 일정 파라미터로 구성할 수 있습니다.

속도 기반 규칙을 사용할 AWS WAF 수 없고에 익숙하여 사용자 지정SQL을 구현할 수 있는 경우이 옵션을 선택하는 것이 좋습니다. 기본 쿼리를 변경하는 방법에 대한 자세한 내용은 Amazon Athena 쿼리 보기를 참조하세요.

HTTP 플러드 보호는 AWS WAF 액세스 로그 처리를 기반으로 하며 WAF 로그 파일을 사용합니다. WAF 액세스 로그 유형은 지연 시간이 더 짧으며, CloudFront 또는 ALB 로그 전송 시간과 비교할 때 HTTP홍수 오리진을 더 빨리 식별하는 데 사용할 수 있습니다. 그러나 응답 상태 코드를 수신하려면 스캐너 및 프로브 보호 활성화 템플릿 파라미터에서 CloudFront 또는 ALB 로그 유형을 선택해야 합니다.

AWS Lambda 로그 구문 분석기

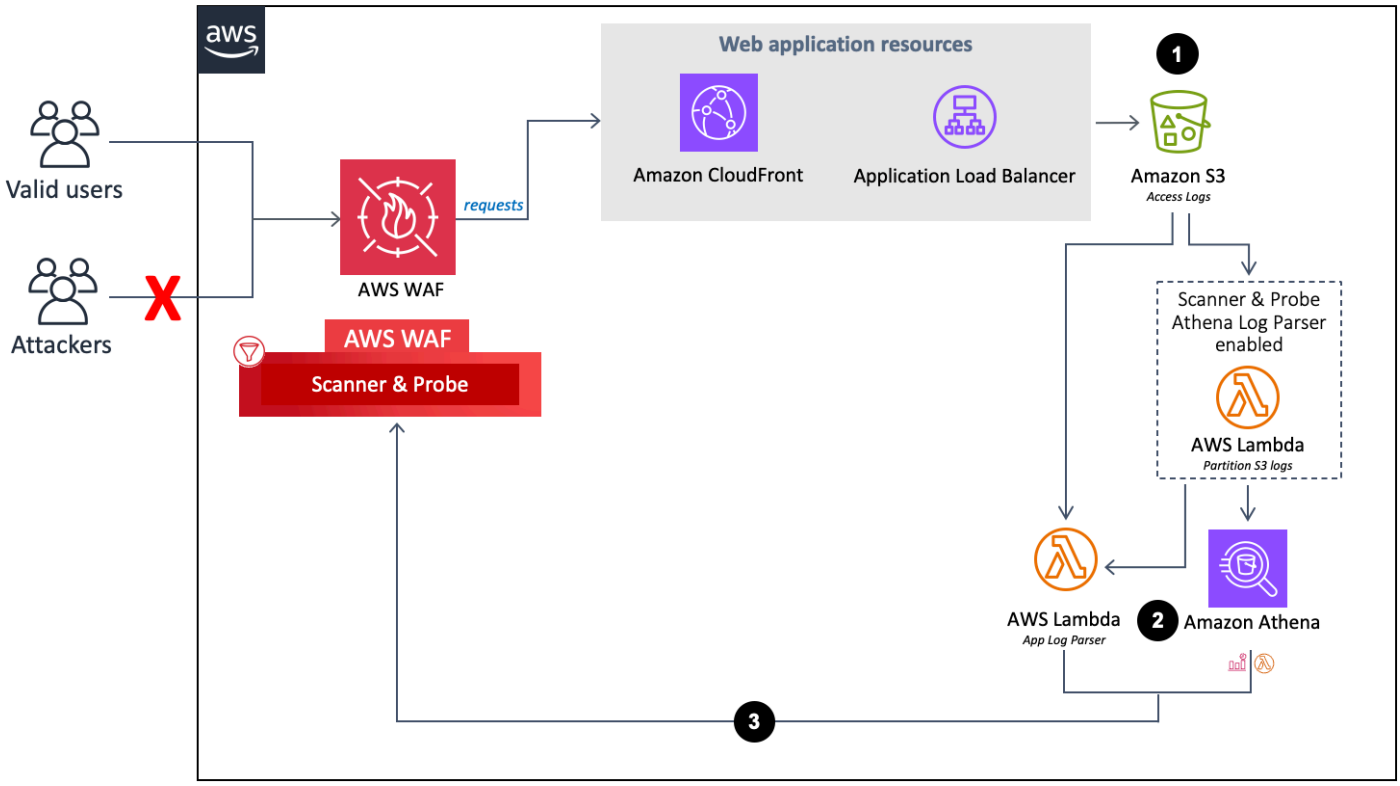
HTTP Flood Protection 및 Scanner & Probe Protection 템플릿 파라미터는 AWS Lambda Log Parser 옵션을 제공합니다. AWS WAF 속도 기반 규칙 및 Amazon Athena 로그 구문 분석기 옵션을 사용할 수 없는 경우에만 Lambda 로그 구문 분석기를 사용합니다. 이 옵션의 알려진 제한 사항은 처리 중인 파일의 컨텍스트 내에서 정보가 처리된다는 것입니다. 예를 들어 IP는 정의된 할당량보다 더 많은 요청이나 오류를 생성할 수 있지만,이 정보는 서로 다른 파일로 분할되므로 각 파일은 할당량을 초과할 만큼 충분한 데이터를 저장하지 않습니다.

구성 요소 세부 정보

아키텍처 다이어그램에 설명된 대로이 솔루션의 구성 요소 중 4개는 자동화를 사용하여 IP 주소를 검사하고 AWS WAF 이를 블록 목록에 추가합니다. 다음 섹션에서는 이러한 각 구성 요소에 대해 자세히 설명합니다.

로그 구문 분석기 - 애플리케이션

Application Log 파서는 스캐너 및 프로브로부터 보호하는 데 도움이 됩니다.



애플리케이션 로그 구문 분석기 흐름

1. CloudFront 또는가 웹 애플리케이션을 대신하여 요청을 ALB 수신하면 액세스 로그를 Amazon S3 버킷으로 전송합니다.

   a. (선택 사항) 템플릿 파라미터`Yes - Amazon Athena log parser`에 대해 HTTP Flood Protection 활성화 및 스캐너 및 프로브 보호 활성화를 선택하면 Lambda 함수는 Amazon S3에 도착할 *<customer-bucket>*/AWSLogs-partitioned/*<optional-prefix>* / year=*<YYYY>*/month=*<MM>* /day=*<DD>*/hour=*<HH>*/ 때 액세스 로그를 원래 폴더에서 새로 분할된 폴더*<customer-bucket>*/AWSLogs로 이동합니다.

   b. (선택 사항) 원본 S3 위치 템플릿에 데이터 유지 파라미터에 `yes` 대해를 선택하면 로그는 원래 위치에 남아 있으며 분할된 폴더에 복사되어 로그 스토리지가 복제됩니다.

> **Note**
>
> Athena 로그 파서의 경우이 솔루션은이 솔루션을 배포한 후 Amazon S3 버킷에 도착하는 새 로그만 분할합니다. 분할하려는 기존 로그가 있는 경우이 솔루션을 배포한 후 Amazon S3에 해당 로그를 수동으로 업로드해야 합니다.

2. 템플릿 파라미터에 대한 선택에 따라이 솔루션은 다음 중 하나를 사용하여 로그를 처리합니다 HTTP.

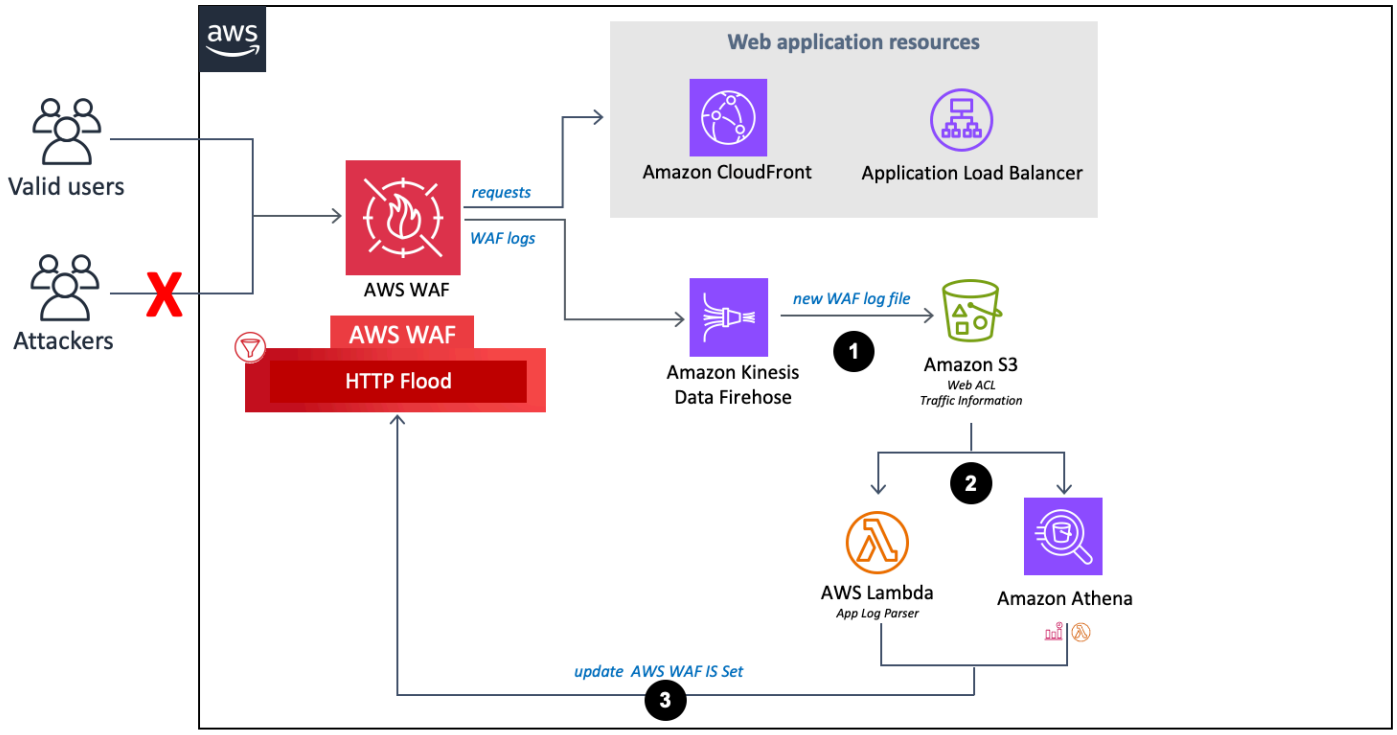
   a. Lambda - 새 액세스 로그가 Amazon S3 버킷에 저장될 때마다 `Log Parser` Lambda 함수가 시작됩니다.

   b. Athena - 기본적으로 5분마다 Scanner & Probe Protection Athena 쿼리가 실행되고 출력이 로 푸시됩니다 AWS WAF. 이 프로세스는 CloudWatch 이벤트에 의해 시작되며, Athena 쿼리 실행을 담당하는 Lambda 함수를 시작하고 결과를에 푸시합니다 AWS WAF.

3. 이 솔루션은 로그 데이터를 분석하여 정의된 할당량보다 더 많은 오류를 생성한 IP 주소를 식별합니다. 그런 다음 솔루션은 AWS WAF IP 세트 조건을 업데이트하여 고객이 정의한 기간 동안 해당 IP 주소를 차단합니다.

로그 구문 분석기 - AWS WAF

서비스 장애 방지 활성화`yes - Amazon Athena log parser`에 대해 `yes - AWS Lambda log parser` 또는를 선택하면이 솔루션은 다음 구성 요소를 프로비저닝합니다.이 구성 요소는 AWS WAF 로그를 구문 분석하여 정의한 할당량보다 큰 요청 속도로 엔드포인트를 플러딩하는 오리진을 식별하고 차단합니다. HTTP

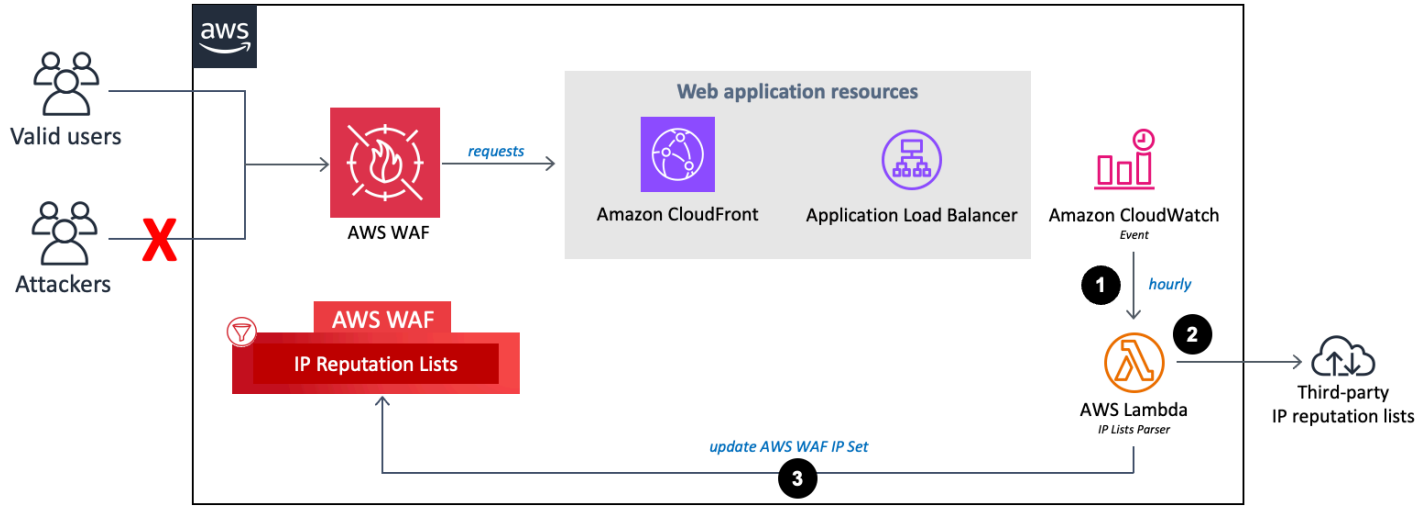


AWS WAF 로그 구문 분석기 흐름

1. AWS WAF 가 액세스 로그를 수신하면 Firehose 엔드포인트로 로그를 전송합니다. 그런 다음 Firehose는 라는 Amazon S3의 분할된 버킷에 로그를 전송합니다. *<customer-bucket>*/AWSLogs/ *<optional-prefix>*/year=*<YYYY>* /month=*<MM>*/day=*<DD>*/hour= *<HH>*/
2. 템플릿 파라미터에 대한 선택에 따라이 솔루션은 다음 중 하나를 사용하여 로그를 처리합니다 HTTP. 홍수 방지 활성화 및 스캐너 및 프로브 보호 활성화:
   a. Lambda: 새 액세스 로그가 Amazon S3 버킷에 저장될 때마다 `Log Parser` Lambda 함수가 시작됩니다.
   b. Athena: 기본적으로 5분마다 스캐너 및 프로브 Athena 쿼리가 실행되고 출력이 푸시됩니다 AWS WAF. 이 프로세스는 Amazon CloudWatch 이벤트에 의해 시작되며, Amazon Athena 쿼리 실행을 담당하는 Lambda 함수를 시작하고 결과를에 푸시합니다 AWS WAF.
3. 이 솔루션은 로그 데이터를 분석하여 정의된 할당량보다 많은 요청을 보낸 IP 주소를 식별합니다. 그런 다음 솔루션은 AWS WAF IP 세트 조건을 업데이트하여 고객이 정의한 기간 동안 해당 IP 주소를 차단합니다.

IP 목록 구문 분석기

`IP Lists Parser` Lambda 함수는 타사 IP 평판 목록에서 식별된 알려진 공격자로부터 보호하는 데 도움이 됩니다.



IP 평판 목록 구문 분석기 흐름

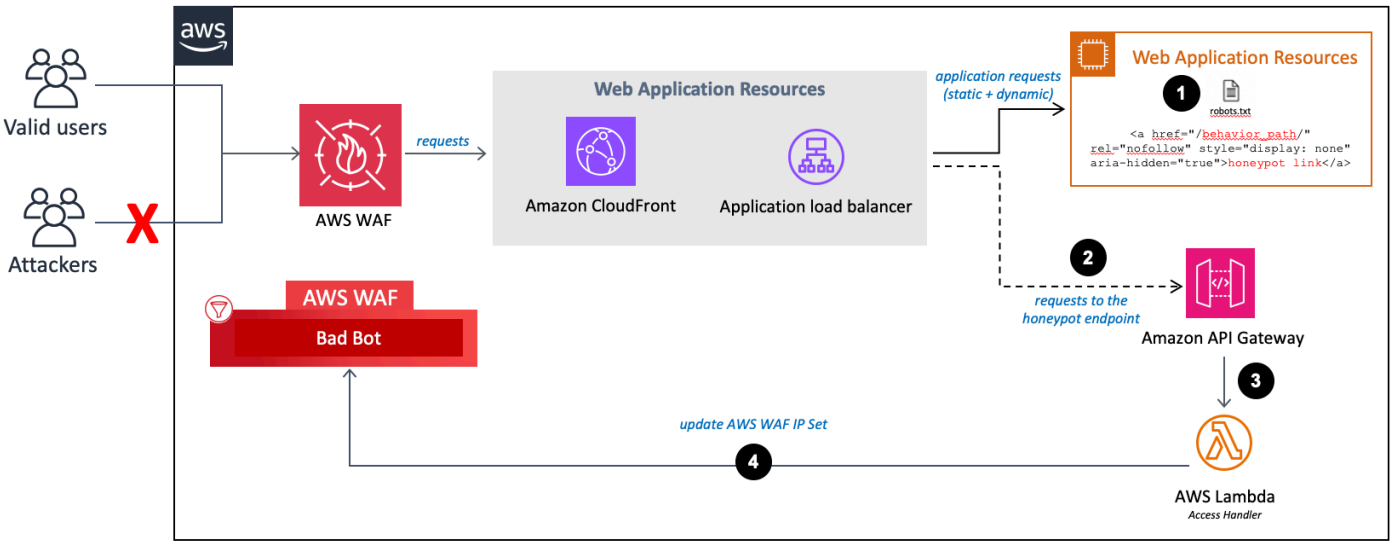
1. 시간당 Amazon CloudWatch 이벤트는 `IP Lists Parser` Lambda 함수를 호출합니다.
2. Lambda 함수는 다음 세 가지 소스에서 데이터를 수집하고 구문 분석합니다.
   - 스팸하우스 DROP 및 EDROP 목록

- Proofpoint 새로운 위협 IP 목록
- Tor 종료 노드 목록

3. Lambda 함수는 AWS WAF 블록 목록을 현재 IP 주소로 업데이트합니다.

액세스 핸들러

`Access Handler` Lambda 함수는 허니팟 엔드포인트에 대한 요청을 검사하여 소스 IP 주소를 추출합니다.



액세스 핸들러 및 허니팟 엔드포인트

1. 웹 애플리케이션에 허니팟 링크 포함(선택 사항)에 설명된 대로 웹 사이트에 허니팟 엔드포인트를 포함시키고 로봇 제외 표준을 업데이트합니다.
2. 콘텐츠 스크레이퍼 또는 잘못된 봇이 허니팟 엔드포인트에 액세스하면 `Access Handler` Lambda 함수를 호출합니다.
3. Lambda 함수는 요청 헤더를 가로채고 검사하여 트랩 엔드포인트에 액세스한 소스의 IP 주소를 추출합니다.
4. Lambda 함수는 AWS WAF IP 설정 조건을 업데이트하여 해당 IP 주소를 차단합니다.

배포 계획

이 섹션에서는 솔루션을 배포하기 전에 발생하는 비용, 보안the section called “할당량”, 및 기타 고려 사항에 대해 설명합니다.

지원됨 AWS 리전

정의한 템플릿 입력 파라미터 값에 따라이 솔루션에는 다양한 리소스가 필요합니다. 이러한 리소스(다음 표에 나열됨)를 전혀 사용하지 못할 수 있습니다 AWS 리전. 따라서 이러한 서비스를 사용할 수 AWS 리전 있는에서이 솔루션을 시작해야 합니다. 리전별 AWS 서비스의 최신 가용성은 AWS 리전 al Services List를 참조하세요.

	AWS WAF 웹 ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
[엔드포인트 유형]				
CloudFront	✓			
Application Load Balancer(ALB)	✓			
HTTP 서비스 장애 방지 활성화				
예 - AWS Lambda 로그 구문 분석기				✓
예 - Amazon Athena 로그 파서		✓	✓	✓
스캐너 및 프로브 보호 활성화				
예 - Amazon Athena 로그 파서		✓	✓	

> **Note**
>
> 엔드포인트CloudFront로를 선택하는 경우 미국 동부(버지니아 북부) 리전()에 솔루션을 배포해야 합니다us-east-1.

비용

AWS WAF 솔루션용 보안 자동화를 실행하는 동안 사용되는 AWS 서비스의 비용은 사용자가 부담해야 합니다. 이 솔루션을 실행하는 데 드는 총 비용은 활성화된 보호와 수집, 저장 및 처리된 데이터의 양에 따라 달라집니다.

비용 관리에 도움이 되도록 abudgetthroughAWS Cost Explorer를 생성하는 것이 좋습니다. 자세한 내용은이 솔루션에서 사용한 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

다음 표는 미국 동부(버지니아 북부) 리전(AWS 프리 티어 제외)에서이 솔루션을 실행하기 위한 비용 내역의 예입니다. 요금은 변경될 수 있습니다.

예제 1: 평판 목록 보호 활성화, 잘못된 봇 보호, HTTP 서비스 장애 방지를 위한 AWS Lambda 로그 파서, 스캐너 및 프로브 보호

AWS 서비스	차원/월	비용 [USD]
Amazon Data Firehose	100GB	~$2.90
Amazon S3	100GB	~$2.30
AWS Lambda	128MB: Lambda 실행당 3개의 함수, 1M 호출 및 평균 500밀리초 기간 512MB: Lambda 실행당 2개의 함수, 1M 호출 및 평균 500밀리초 기간	~$5.40
Amazon API Gateway	1M0만 개의 요청	~$3.40
AWS WAF 웹 ACL	1	$5.00
AWS WAF 규칙	4	$4.00

AWS 서비스	차원/월	비용 [USD]
AWS WAF 요청	100만	$0.60
합계		매월 ~$23.60

예제 2: 평판 목록 보호 활성화, 잘못된 봇 보호, HTTP홍수 방지를 위한 Amazon Athena 로그 파서, 스캐너 및 프로브 보호

AWS 서비스	차원/월	비용 [USD]
Amazon Data Firehose	100GB	~$2.90
Amazon S3	100GB	~$2.30
AWS Lambda	128MB: Lambda 실행당 3개의 함수, 1M 호출 및 평균 500밀리초 지속 시간 512MB: Lambda 실행당 함수 2개, 간접 호출 7560개 및 평균 500밀리초 기간	~$1.26
Amazon API Gateway	1M0만 개의 요청	~$3.40
Amazon Athena	적중 또는 ALB 요청당 약 500바이트 로그 레코드를 생성하는 하루에 120만 건의 CloudFront 객체 적중 또는 120만 건의 요청	~$4.32
AWS WAF 웹 ACL	1	$5.00
AWS WAF 규칙	4	$4.00
AWS WAF 요청	100만	$0.60
합계		매월 ~$23.78

예제 3: 허용 및 거부된 IP 세트에 대한 IP 보존 활성화

AWS 서비스	차원/월	비용 [USD]
Amazon DynamoDB	1K 쓰기 및 1MB 데이터 스토리지	~$0.00
AWS Lambda	128MB: Lambda 실행당 함수 1개, 간접 호출 2K 및 평균 500밀리초 기간 512MB: Lambda 실행당 함수 1개, 간접 호출 2K 및 평균 500밀리초 기간	~$0.01
Amazon CloudWatch	2K 이벤트	~$0.00
AWS WAF 웹 ACL	1	$5.00
AWS WAF 규칙	2	$2.00
WAS WAF 요청	100만	$0.60
합계		매월 ~$7.61

CloudWatch 로그의 비용 추정

Lambda와 같이이 솔루션에 사용되는 일부 AWS 서비스는 CloudWatch 로그를 생성합니다. 이러한 로그에는 요금이 부과됩니다. 비용을 줄이려면 로그를 삭제하거나 보관하는 것이 좋습니다. 로그 아카이브 세부 정보는 Amazon Logs 사용 설명서의 Amazon S3로 로그 데이터 내보내기를 참조하세요 CloudWatch .

설치 시 Athena 로그 파서를 사용하도록 선택한 경우이 솔루션은 Amazon S3 버킷(들)의 AWS WAF 또는 애플리케이션 액세스 로그에 대해 구성된 대로 실행되도록 쿼리를 예약합니다. 각 쿼리에서 스캔한 데이터의 양을 기준으로 요금이 부과됩니다. 이 솔루션은 로그 및 쿼리에 파티셔닝을 적용하여 비용을 최소화합니다. 기본적으로 솔루션은 원래 Amazon S3 위치에서 파티션된 폴더 구조로 애플리케이션 액세스 로그를 이동합니다. 원본을 보존할 수도 있지만 중복 로그 스토리지에 대해서는 요금이 부과됩니다. 이 솔루션은 작업 그룹을 사용하여 워크로드를 분할하며 쿼리 액세스 및 비용을 관리하도

록 둘 다 구성할 수 있습니다. 샘플 비용 견적 계산은 Athena의 비용 견적을 참조하세요. 자세한 내용은 Amazon Athena 요금을 참조하세요.

Athena의 비용 견적

HTTP Flood Protection 또는 Scanner & Probe Protection 규칙을 실행하는 동안 Athena 로그 구문 분석기 옵션을 사용하는 경우 Athena 사용에 대한 요금이 부과됩니다. 기본적으로 각 Athena 쿼리는 5분마다 실행되고 지난 4시간의 데이터를 스캔합니다. 이 솔루션은 로그 및 Athena 쿼리에 파티셔닝을 적용하여 비용을 최소화합니다. WAF 블록 기간 템플릿 파라미터의 값을 변경하여 쿼리가 스캔하는 데이터 시간을 구성할 수 있습니다. 그러나 스캔되는 데이터의 양을 늘리면 Athena 비용이 증가할 수 있습니다.

> **Tip**
>
> 다음은 CloudFront 로그 비용 계산의 예입니다.
> 평균적으로 각 CloudFront 적중은 약 500바이트의 데이터를 생성할 수 있습니다.
> 하루에 120만 개의 CloudFront 객체가 적중되면 데이터가 일관된 속도로 수집된다고 가정할 때 4시간당 200K(120만/6)의 적중이 발생합니다. 비용을 계산할 때 실제 트래픽 패턴을 고려합니다.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena는 스캔한 데이터의 TB당 5.00 USD를 청구합니다.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Athena 쿼리는 5분마다 실행되며, 시간당 12회 실행됩니다.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> 실제 비용은 애플리케이션의 트래픽 패턴에 따라 달라집니다. 자세한 내용은 Amazon Athena 요금을 참조하세요.

보안

AWS 인프라에 시스템을 구축하면 보안 책임이 사용자와 간에 공유됩니다 AWS. 이 공동 책임 모델은 호스트 운영 체제 AWS , 가상화 계층, 서비스가 운영되는 시설의 물리적 보안을 포함한 구성 요소를 운영, 관리 및 제어하기 때문에 운영 부담을 줄입니다. AWS 보안에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요.

IAM 역할

IAM 역할을 사용하면의 서비스 및 사용자에게 세분화된 액세스, 정책 및 권한을 할당할 수 있습니다 AWS 클라우드. 이 솔루션은 권한이 가장 낮은 IAM 역할을 생성하며, 이러한 역할은 필요한 권한을 솔루션의 리소스에 부여합니다.

Data

Amazon S3 버킷 및 DynamoDB 테이블에 저장된 모든 데이터는 저장 시 암호화를 사용합니다. Firehose로 전송 중인 데이터도 암호화됩니다.

보호 기능

웹 애플리케이션은 다양한 공격에 취약합니다. 이러한 공격에는 취약성을 악용하거나 서버를 제어하도록 특별히 설계된 요청, 웹 사이트를 중단하도록 설계된 볼륨 측정 공격, 웹 콘텐츠를 스크레이프 및 도용하도록 프로그래밍된 잘못된 봇 및 스크레이퍼가 포함됩니다.

이 솔루션은 CloudFormation 를 사용하여 AWS WAF 규칙 AWS Managed Rules 그룹 및 사용자 지정 규칙을 포함한 규칙을 구성하여 다음과 같은 일반적인 공격을 차단합니다.

- AWS 관리형 규칙 -이 관리형 서비스는 일반적인 애플리케이션 취약성 또는 기타 원치 않는 트래픽에 대한 보호를 제공합니다. 이 솔루션에는 AWS 관리형 IP 평판 규칙 그룹, AWS 관리형 기준 규칙 그룹 및 AWS 관리형 사용 사례별 규칙 그룹이 포함됩니다. 최대 웹 ACL 용량 단위(WCU) 할당량 ACL까지 웹에 대해 하나 이상의 규칙 그룹을 선택할 수 있습니다.
- SQL injection - 공격자는 웹 요청에 악성 SQL 코드를 삽입하여 데이터베이스에서 데이터를 추출합니다. 이 솔루션은 잠재적으로 악성 SQL 코드가 포함된 웹 요청을 차단하도록 설계되었습니다.
- XSS - 공격자는 양성 웹 사이트의 취약성을 차량으로 사용하여 합법적인 사용자의 웹 브라우저에 악성 클라이언트 사이트 스크립트를 주입합니다. 이를 통해 일반적으로 탐색되는 수신 요청 요소를 검사하여 XSS 공격을 식별하고 차단할 수 있습니다.
- HTTP 홍수 - 웹 서버 및 기타 백엔드 리소스는 HTTP홍수와 같은 DDoS 공격의 위험이 있습니다. 이 솔루션은 클라이언트의 웹 요청이 구성 가능한 할당량을 초과할 때 속도 기반 규칙을 자동으로 호출합니다. 또는 Lambda 함수 또는 Athena 쿼리를 사용하여 AWS WAF 로그를 처리하여이 할당량을 적용할 수 있습니다.
- 스캐너 및 프로브 - 악성 소스는 HTTP 4xx 오류 코드를 생성하는 일련의 요청을 전송하여 인터넷 연결 웹 애플리케이션의 취약성을 스캔하고 검사합니다. 이 기록을 사용하여 악성 소스 IP 주소를 식별하고 차단할 수 있습니다. 이 솔루션은 Lambda 함수 또는 Athena 쿼리를 생성하여 로그를 자동으로 구문 분석 CloudFront 하거나 ALB 액세스하고, 분당 고유한 소스 IP 주소의 잘못된 요청 수를 계산하고, 정의된 오류 할당량에 도달한 주소의 추가 스캔을 차단 AWS WAF 하도록 업데이트합니다.

- 알려진 공격자 오리진(IP 평판 목록) - 많은 조직이 스팸 메일, 맬웨어 배포자, 봇넷 등 알려진 공격자가 운영하는 IP 주소의 평판 목록을 유지합니다. 이 솔루션은 이러한 평판 목록의 정보를 활용하여 악성 IP 주소의 요청을 차단하는 데 도움이 됩니다. 또한이 솔루션은 Amazon 내부 위협 인텔리전스를 기반으로 IP 평판 규칙 그룹에 의해 식별된 공격자를 차단합니다.
- 봇 및 스크레이퍼 - 공개적으로 액세스할 수 있는 웹 애플리케이션의 운영자는 콘텐츠에 액세스하는 클라이언트가 자신을 정확하게 식별하고 의도한 대로 서비스를 사용한다는 것을 신뢰해야 합니다. 그러나 콘텐츠 스크레이퍼 또는 잘못된 봇과 같은 일부 자동화된 클라이언트는 제한을 우회하기 위해 자신을 잘못 표현합니다. 이 솔루션은 잘못된 봇과 스크레이퍼를 식별하고 차단하는 데 도움이 됩니다.

할당량

서비스 할당량은 AWS 계정계정의 최대 서비스 리소스 또는 작업 수입니다.

이 솔루션의 AWS 서비스에 대한 할당량

이 솔루션에 구현된 각 서비스의 할당량이 충분한지 확인하세요. 자세한 내용은 AWS 서비스 할당량을 참조하세요. 페이지를 전환하지 않고 설명서의 모든 AWS 서비스에 대한 서비스 할당량을 보려면 PDF 대신의 서비스 엔드포인트 및 할당량 페이지에서 정보를 확인합니다.

AWS WAF 할당량

AWS WAF 는 IP 일치 조건당 클래스리스 도메인 간 라우팅(CIDR) 표기법으로 최대 10,000개의 IP 주소 범위를 차단할 수 있습니다. 이 솔루션이 생성하는 각 목록에는이 할당량이 적용됩니다. 자세한 내용은 AWS WAF 할당량을 참조하세요. 버전 3.0부터이 솔루션은 각 규칙에 연결할 두 개의 IP 세트를 생성합니다. 하나는 용IPv4이고 다른 하나는 용입니다IPv6.

AWS WAF 는 개인, 또는 `Update`작업에 AWS 리전 대한 API 호출에 대해 초당, 계정당`CreatePut`, 별로 최대 1개의 요청을 허용합니다. 솔루션 외부에서 이러한 API 호출을 하면 API 제한 문제가 발생할 수 있습니다. 문제를 방지하려면이 솔루션이 배포된 동일한 계정 및 리전에서 이러한 API 호출을 수행하는 다른 애플리케이션을 실행하지 않는 것이 좋습니다.

배포 고려 사항

다음 섹션에서는이 솔루션을 구현하기 위한 제약 조건과 고려 사항을 제공합니다.

AWS WAF 규칙

ACL이 솔루션이 생성하는 웹은 웹 애플리케이션에 대한 포괄적인 보호를 제공하도록 설계되었습니다. 이 솔루션은 웹에 추가할 수 있는 AWS Managed Rules 및 사용자 지정 규칙 세트를 제공합니다ACL. 규칙을 포함하려면 CloudFormation 스택을 시작할 때 관련 파라미터에 yes 대해를 선택합니다. 1단계를 참조하세요. 파라미터 목록에 대한 스택을 시작합니다.

> **Note**
>
> 솔루션은 out-of-box를 지원하지 않습니다AWS Firewall Manager. Firewall Manager에서 규칙을 사용하려면 소스 코드에 사용자 지정을 적용하는 것이 좋습니다.

웹 ACL 트래픽 로깅

미국 동부(버지니아 북부) AWS 리전 이외의에서 스택을 생성하고 엔드포인트를 로 설정하는 경우 HTTP Flood 보호 활성화를 no 또는 로 설정해야 `CloudFront`합니다`yes - AWS WAF rate based rule`.

다른 두 옵션(`yes - AWS Lambda log parser` 및 `yes - Amazon Athena log parser`)은 모든 AWS 엣지 로케이션에서 ACL 실행되는 웹에서 AWS WAF 로그를 활성화해야 하며, 미국 동부(버지니아 북부) 외부에서는 지원되지 않습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 개발자 안내서를 참조하세요.

요청 구성 요소의 크기 초과 처리

AWS WAF 는 웹 요청 구성 요소의 본문, 헤더 또는 쿠키에 대한 크기 초과 콘텐츠 검사를 지원하지 않습니다. 이러한 요청 구성 요소 유형 중 하나를 검사하는 규칙 문을 작성할 때 다음 옵션 중 하나를 선택하여 이러한 요청 AWS WAF 으로 수행할 작업을 지정할 수 있습니다.

- `yes` (계속) - 규칙 검사 기준에 따라 요청 구성 요소를 정상적으로 검사합니다. 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 AWS WAF 검사합니다. 솔루션에 사용되는 기본 옵션입니다.
- `yes - MATCH` - 웹 요청을 규칙 문과 일치하는 것으로 취급합니다.는 규칙의 검사 기준에 따라 평가하지 않고 요청에 규칙 작업을 AWS WAF 적용합니다. `Block` 작업이 있는 규칙의 경우, 이렇게 하면 초과 크기 구성 요소로 요청이 차단됩니다.
- `yes - NO_MATCH` - 규칙의 검사 기준에 대해 평가하지 않고 웹 요청을 규칙 문과 일치하지 않는 것으로 처리합니다.는 일치하지 않는 규칙에 대해와 ACL마찬가지로 웹의 나머지 규칙을 사용하여 웹 요청 검사를 AWS WAF 계속합니다.

자세한 내용은 AWS의 과대 웹 요청 구성 요소 처리를 WAF참조하세요.

여러 솔루션 배포

동일한 계정 및 리전에 솔루션을 여러 번 배포할 수 있습니다. 각 배포에 고유한 CloudFormation 스택 이름과 Amazon S3 버킷 이름을 사용해야 합니다. 각 고유 배포에는 추가 요금이 발생하며 계정당, 리전당 AWS WAF 할당량이 적용됩니다.

솔루션 배포

이 솔루션은 AWS CloudFormation 템플릿 및 스택을 사용하여 배포를 자동화합니다. CloudFormation 템플릿은이 솔루션에 포함된 AWS 리소스와 해당 속성을 지정합니다. 스택은 CloudFormation 템플릿에 설명된 리소스를 프로비저닝합니다.

배포 프로세스 개요

CloudFormation 템플릿을 시작하기 전에이 가이드에서 설명하는 아키텍처 및 구성 고려 사항을 검토하세요. 이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 계정에 배포합니다.

배포 시간: 약 15분.

> **Note**
>
> 이전에이 솔루션을 배포한 경우 업데이트 지침은 솔루션 업데이트를 참조하세요.

사전 조건

- CloudFront 배포 구성
- 구성 ALB

단계 1. 스택 시작

- 에서 CloudFormation 템플릿을 시작합니다 AWS 계정.
- 필요한 파라미터의 값을 입력합니다. 스택 이름 및 애플리케이션 액세스 로그 버킷 이름.
- 다른 템플릿 파라미터를 검토하고 필요한 경우 조정합니다.

2단계. 웹을 웹 애플리케이션ACL과 연결

- CloudFront 웹 배포(들) 또는 ALB(들)을 ACL이 솔루션이 생성하는 웹과 연결합니다. 원하는 만큼 배포 또는 로드 밸런서를 연결할 수 있습니다.

3단계. 웹 액세스 로깅 구성

- 웹 배포(들) 또는 ALB(들)에 대한 CloudFront 웹 액세스 로깅을 활성화하고 로그 파일을 적절한 Amazon S3 버킷으로 전송합니다. 사용자 정의 접두사와 일치하는 폴더에 로그를 저장합니다. 사용자 정의 접두사를 사용하지 않는 경우 로그(기본 AWS로그 접두사)에 로그를 저장합니다AWS Logs/. 1단계의 애플리케이션 액세스 로그 버킷 접두사 파라미터를 참조하세요. 스택을 시작하여 자세한 내용을 확인하세요.

AWS CloudFormation 템플릿

이 솔루션에는 기본 AWS CloudFormation 템플릿 1개와 중첩 템플릿 2개가 포함되어 있습니다. 솔루션을 배포하기 전에 템플릿을 다운로드할 CloudFormation 수 있습니다.

기본 스택

View template

aws-waf-security-automations.template -이 템플릿을 진입점으로 사용하여 계정에서 솔루션을 시작합니다. 기본 구성은 사전 구성된 규칙이 ACL 있는 AWS WAF 웹을 배포합니다. 필요에 따라 템플릿을 사용자 지정할 수 있습니다.

웹ACL 스택

View template

aws-waf-security-automations-webacl.template –이 중첩 템플릿은 웹ACL, IP, 세트 및 기타 관련 AWS WAF 리소스를 포함한 리소스를 프로비저닝합니다.

Firehose Athena 스택

View template

aws-waf-security-automations-firehose-athena.template –이 중첩 템플릿은 , AWS GlueAthena 및 Firehose와 관련된 리소스를 프로비저닝합니다. 스캐너 및 프로브 Athena 로그 파서 또는 HTTP Flood Lambda 또는 Athena 로그 파서를 선택하면 생성됩니다.

사전 조건

이 솔루션은 CloudFront 또는와 함께 배포된 웹 애플리케이션에서 작동하도록 설계되었습니다ALB. 이러한 리소스 중 하나가 아직 구성되지 않은 경우이 솔루션을 시작하기 전에 해당 작업을 완료합니다.

CloudFront 배포 구성

다음 단계를 완료하여 웹 애플리케이션의 정적 및 동적 콘텐츠에 대한 CloudFront 배포를 구성합니다. 자세한 지침은 Amazon CloudFront 개발자 안내서를 참조하세요.

1. CloudFront 웹 애플리케이션 배포를 생성합니다. 배포 생성을 참조하세요.
2. 정적 및 동적 오리진을 구성합니다. CloudFront 배포와 함께 다양한 오리진 사용을 참조하세요.
3. 배포 동작을 지정합니다. 배포를 생성하거나 업데이트할 때 지정하는 값을 참조하세요.

> **Note**
>
> 엔드포인트`CloudFront`로를 선택하는 경우 미국 동부(버지니아 북부) 리전에서 WAFV2 리소스를 생성해야 합니다.

구성 ALB

수신 트래픽을 웹 애플리케이션에 배포ALB하도록를 구성하려면 Application Load Balancer 사용 설명서의 Application Load Balancer 생성을 참조하세요.

단계 1. 스택 시작

이 자동 AWS CloudFormation 템플릿은에 솔루션을 배포합니다 AWS 클라우드.

1. 에 로그인AWS Management Console하고 솔루션 시작을 선택하여 `waf-automation-on-aws.template` CloudFormation 템플릿을 시작합니다.

   Launch solution

2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른에서이 솔루션을 시작하려면 콘솔 탐색 모음에서 리전 선택기를 AWS 리전사용합니다. 엔드포인트`CloudFront`로를 선택하는 경우 미국 동부(버지니아 북부)(`us-east-1`) 리전에 솔루션을 배포해야 합니다.

> **Note**
>
> 정의한 입력 파라미터 값에 따라이 솔루션에는 다양한 리소스가 필요합니다. 이러한 리소스는 현재 특정 에서만 사용할 수 있습니다 AWS 리전 . 따라서 이러한 서비스를 사용할 수 AWS 리전 있는에서이 솔루션을 시작해야 합니다. 자세한 내용은 Supported AWS 리전를 참조하세요.

3. 템플릿 지정 페이지에서 올바른 템플릿을 선택했는지 확인하고 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지의 스택 이름 필드에서 구성에 이름을 할당합니다 AWS WAF . 템플릿이 생성하는 웹의 이름이기도 ACL 합니다.
5. 파라미터에서 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 특정 기능을 옵트아웃하려면 해당하는 no 경우 none 또는를 선택합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

파라미터	기본값	설명
스택 이름	*<requires input>*	스택 이름에는 공백이 포함될 수 없습니다. 이 이름은 내에서 고유해야 하며 ACL 템플릿이 생성하는 웹의 이름 AWS 계정 입니다.
리소스 유형		
Endpoint	`CloudFront`	사용 중인 리소스 유형을 선택합니다. **Note** 엔드포인트`CloudFront` 로를 선택하는 경우 솔루션을 시작하여 미국 동부(버지니아 북부) 리전(`us-east-1`)에서

파라미터	기본값	설명
		WAF 리소스를 생성해야 합니다.
AWS 관리형 IP 평판 규칙 그룹		
Amazon IP 평판 활성화 관리형 규칙 그룹 보호 나열	no	웹에 Amazon IP 평판 목록 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 Amazon 내부 위협 인텔리전스를 기반으로 합니다. 이는 일반적으로 봇 또는 기타 위협과 관련된 IP 주소를 차단하려는 경우에 유용합니다. 이러한 IP 주소를 차단하면 봇을 완화하고 악성 액터가 취약한 애플리케이션을 발견하는 위험을 줄일 수 있습니다. 필수 값은 25WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
익명 IP 목록 관리형 규칙 그룹 보호 활성화	no	웹에 익명 IP 목록 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 최종 사용자 자격 증명의 난독화를 허용하는 서비스의 요청을 차단합니다. 여기에는 VPNs, 프록시, Tor 노드 및 호스팅 공급자의 요청이 포함됩니다. 이 규칙 그룹은 애플리케이션에서 자신의 ID를 숨기려고 하는 최종 사용자를 필터링하려는 경우에 유용합니다. 이러한 서비스의 IP 주소를 차단하면 봇을 완화하고 지리적 제한을 피할 수 있습니다. 필수 값은 50WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.
AWS 관리형 기준 규칙 그룹		

파라미터	기본값	설명
코어 규칙 세트 관리형 규칙 그룹 보호 활성화	no	웹에 코어 규칙 세트 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 고위험 및 흔히 발생하는 취약성 중 일부를 포함하여 광범위한 취약성의 악용으로부터 보호합니다. AWS WAF 모든 사용 사례에 이 규칙 그룹을 사용하는 것이 좋습니다. 필수 값은 700WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
관리자 보호 관리형 규칙 그룹 보호 활성화	no	웹에 Admin Protection 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 노출된 관리 페이지에 대한 외부 액세스를 차단합니다. 서드 파티 소프트웨어를 실행 중이거나, 악성 액터가 애플리케이션에 대한 관리 액세스 권한을 얻게 되는 위험을 줄이려면 이 방법이 유용할 수 있습니다. 필수 값은 100WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
알려진 잘못된 입력 활성화 관리형 규칙 그룹 보호	no	웹에 알려진 잘못된 입력 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 노출된 관리 페이지에 대한 외부 액세스를 차단합니다. 서드 파티 소프트웨어를 실행 중이거나, 악성 액터가 애플리케이션에 대한 관리 액세스 권한을 얻게 되는 위험을 줄이려면 이 방법이 유용할 수 있습니다. 필수 값은 100WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.
AWS 관리형 사용 사례별 규칙 그룹		

파라미터	기본값	설명
SQL 데이터베이스 관리형 규칙 그룹 보호 활성화	no	웹에 SQL 데이터베이스 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 SQL 주입 공격과 같은 SQL 데이터베이스 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 승인되지 않은 쿼리가 원격으로 삽입되는 것을 방지할 수 있습니다. 애플리케이션이 SQL 데이터베이스와 인터페이스하는 경우이 규칙 그룹의 사용을 평가합니다. 이미 AWS 관리형 규칙 그룹이 활성화된 경우 SQL 주입 사용자 지정 SQL 규칙을 사용하는 것은 선택 사항입니다. 필수 값은 200WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
Linux 운영 체제 관리형 규칙 그룹 보호 활성화	no	웹에 Linux 운영 체제 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 Linux 관련 로컬 파일 포함(LFI) 공격을 포함하여 Linux 관련 취약성의 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 Linux에서 실행되는 경우이 규칙 그룹을 평가합니다. POSIX 운영 체제 규칙 그룹과 함께이 규칙 그룹을 사용해야 합니다. 필수 값은 200WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
POSIX 운영 체제 관리형 규칙 그룹 보호 활성화	no	웹에 코어 규칙 세트 관리형 규칙 그룹 보호를 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 LFI 공격을 포함하여 특정 운영 체제 POSIX 및 POSIX유사 운영 체제의 취약성 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 POSIX 또는 POSIX유사 운영 체제에서 실행되는 경우이 규칙 그룹을 평가합니다. 필수 값은 100WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
Windows 운영 체제 관리형 규칙 그룹 보호 활성화	no	웹에 Windows 운영 체제 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 PowerShell 명령의 원격 실행과 같이 Windows 관련 취약성의 악용과 관련된 요청 패턴을 차단합니다. 이를 통해 공격자가 권한이 없는 명령을 실행하거나 악성 코드를 실행할 수 있는 취약성 악용을 방지할 수 있습니다. 애플리케이션의 일부가 Windows 운영 체제에서 실행되는 경우 이 규칙 그룹을 평가합니다. 필수 값은 200WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
PHP 애플리케이션 관리형 규칙 그룹 보호 활성화	no	웹에 PHP 애플리케이션 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 안전하지 않은 PHP 함수 주입을 포함하여 PHP 프로그래밍 언어 사용과 관련된 취약성 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 공격자가 권한이 부여되지 않은 코드나 명령을 원격으로 실행할 수 있는 취약성 악용을 방지할 수 있습니다. 애플리케이션이 인터페이스하는 서버에 PHP이 설치되어 있는 경우이 규칙 그룹을 평가합니다. 필수 값은 100WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.

파라미터	기본값	설명
WordPress 애플리케이션 관리형 규칙 그룹 보호 활성화	no	웹에 WordPress 애플리케이션 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다ACL. 이 규칙 그룹은 WordPress 사이트별 취약성 악용과 관련된 요청 패턴을 차단합니다. 실행 중인 경우이 규칙 그룹을 평가합니다 WordPress. 이 규칙 그룹은 SQL 데이터베이스 및 PHP 애플리케이션 규칙 그룹과 함께 사용해야 합니다. 필수 값은 100WCU입니다. WCU 용량 제한을 초과하여 웹 ACL 스택 배포가 실패하지 않도록 계정에 충분한 용량이 있어야 합니다. 자세한 내용은 AWS Managed Rules 규칙 그룹 목록을 참조하세요.
사용자 지정 규칙 - 스캐너 및 프로브		
스캐너 및 프로브 보호 활성화	`yes - AWS Lambda log parser`	스캐너와 프로브를 차단하는 데 사용되는 구성 요소를 선택합니다. 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

파라미터	기본값	설명
애플리케이션 액세스 로그 버킷 이름	*<requires input>*	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 CloudFront 배포(들) 또는 (들)에 대한 액세스 로그를 저장하려는 Amazon S3 버킷ALB(신규 또는 기존)의 이름을 입력합니다. 기존 Amazon S3 버킷을 사용하는 경우 CloudFormation 템플릿을 배포 AWS 리전 하는 동일한 위치에 있어야 합니다. 솔루션 배포마다 다른 버킷을 사용해야 합니다. 이 보호를 비활성화하려면이 파라미터를 무시합니다. **Note** 이 Amazon S3 버킷으로 로그 파일을 전송하려면 웹 배포(들) 또는 ALB(들)에 대한 CloudFront 웹 액세스 로깅을 켭니다. 스택에 정의된 것과 동일한 접두사에 로그를 저장합니다(기본 접두사 AWS Logs/). 자세한 내용은 애플리케이션 액세스 로그 버킷 접두사 파라미터를 참조하세요.

파라미터	기본값	설명
애플리케이션 액세스 로그 버킷 접두사	AWS Logs/	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 위의 애플리케이션 액세스 로그 버킷에 대한 선택적 사용자 정의 접두사를 입력할 수 있습니다. 엔드포인트 파라미터에 CloudFront 를 선택한 경우와 같은 접두사를 입력할 수 있습니다yourprefix/ . 엔드포인트 파라미터에 ALB를 선택한 경우와 같은 접두사AWS Logs/에를 추가해야 합니다yourprefix/AWSLogs/ . 사용자 정의 접두사가 없는 경우 AWS Logs/ (기본값)을 사용합니다. 이 보호를 비활성화하려면이 파라미터를 무시합니다.

파라미터	기본값	설명
버킷 액세스 로깅이 켜져 있습니까?	no	Application Access Log Bucket Name 파라미터에 기존 Amazon S3 버킷 이름을 입력했고 버킷에 대한 서버 액세스 로깅이 이미 켜져 yes 있는지 선택합니다. 를 선택하면 솔루션이 버킷no에 대한 서버 액세스 로깅을 켭니다. 스캐너 및 프로브 보호 활성화 파라미터에 no 대해를 선택한 경우이 파라미터를 무시합니다.
오류 임계값	50	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 IP 주소당 분당 허용되는 최대 잘못된 요청을 입력합니다. 스캐너 및 프로브 보호 활성화 파라미터에 no 대해를 선택한 경우이 파라미터를 무시합니다.

파라미터	기본값	설명
원본 S3 위치에 데이터 유지	no	스캐너 및 프로브 보호 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택한 경우 솔루션은 애플리케이션 액세스 로그 파일 및 Athena 쿼리에 파티셔닝을 적용합니다. 기본적으로 솔루션은 로그 파일을 원래 위치에서 Amazon S3의 파티션된 폴더 구조로 이동합니다. 로그의 복사본을 원래 위치에 보관할yes지 여부도 선택합니다. 그러면 로그 스토리지가 복제됩니다. 스캐너 및 프로브 보호 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택하지 않은 경우이 파라미터를 무시합니다.
사용자 지정 규칙 HTTP - 홍수		
HTTP 서비스 장애 방지 활성화	`yes - AWS WAF rate-based rule`	HTTP 홍수 공격을 차단하는 데 사용되는 구성 요소를 선택합니다. 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

파라미터	기본값	설명
기본 요청 임계값	100	서비스 장애 방지 활성화 파라미터에 yes 대해를 선택한 경우 IP 주소당 5분당 허용되는 최대 요청을 입력합니다. HTTP Flood 보호 활성화 파라미터에 yes - AWS WAF rate-based rule 대해를 선택한 경우 허용되는 최소 값은 입니다100. HTTP Flood 보호 활성화 파라미터에 yes – Amazon Athena log parser 대해 yes - AWS Lambda log parser 또는를 선택한 경우 어떤 값이든 될 수 있습니다. HTTP 이 보호를 비활성화하려면이 파라미터를 무시합니다.

파라미터	기본값	설명
국가별 요청 임계값	<선택 사항 입력>	서비스 장애 방지 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택한 경우이 JSON 형식에 따라 국가별 임계값을 입력할 수 있습니다`{"TR":50, "ER":150}` . HTTP 솔루션은 지정된 국가에서 시작된 요청에 대해 이러한 임계값을 사용합니다. 솔루션은 나머지 요청에 대해 기본 요청 임계값 파라미터를 사용합니다. **Note** 이 파라미터를 정의하면 국가가 IP 및 HTTPFlood Athena 쿼리의 요청별 그룹 파라미터를 사용하여 선택할 수 있는 기타 선택적 그룹별 필드와 함께 Athena 쿼리 그룹에 자동으로 포함됩니다. 이 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.

파라미터	기본값	설명
HTTPFlood Athena 쿼리의 요청별 그룹화	None	서비스 장애 방지 활성화 파라미터에 yes – Amazon Athena log parser 대해를 선택한 경우 그룹별 필드를 선택하여 IP당 요청을 계산하고 선택한 그룹별 필드를 계산할 수 있습니다. HTTP 예를 들어, URI를 선택하면 솔루션은 IP 및당 요청을 계산합니다 URI. 이 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.
WAF 차단 기간	240	스캐너 및 프로브 보호 활성화 또는 서비스 장애 방지 활성화 파라미터yes – Amazon Athena log parser에 대해 yes - AWS Lambda log parser 또는를 선택한 경우 기간(분)을 입력하여 해당 IP 주소를 차단합니다. HTTP 로그 구문 분석을 비활성화하려면이 파라미터를 무시합니다.

파라미터	기본값	설명
Athena 쿼리 실행 시간 일정(분)	5	스캐너 및 프로브 보호 활성화 또는 서비스 HTTP 장애 방지 활성화 파라미터yes – Amazon Athena log parser에 대해를 선택한 경우 Athena 쿼리가 실행되는 시간 간격(분)을 입력할 수 있습니다. 기본적으로 Athena 쿼리는 5분마다 실행됩니다. 이러한 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.
사용자 지정 규칙 - 잘못된 봇		
잘못된 봇 보호 활성화	yes	잘못된 봇 및 콘텐츠 스크레이퍼를 차단하도록 설계된 구성 요소를 켜yes려면 선택합니다.
ARN 계정의 로그에 대한 CloudWatch 쓰기 액세스 권한이 있는 IAM 역할의	<선택 사항 입력>	계정의 CloudWatch 로그에 대한 쓰기 액세스 권한이 있는 IAM 역할ARN의 선택 사항을 제공합니다. 예: ARN: arn:aws:iam::account_id:role/myrolename . 역할을 생성하는 방법에 대한 지침은 API GatewayRESTAPI에서에 대한 CloudWatch 로깅 설정을 참조하세요. 이 파라미터를 비워 두면(기본값) 솔루션이 새 역할을 생성합니다.

파라미터	기본값	설명
기본 요청 임계값	100	서비스 장애 방지 활성화 파라미터에 yes 대해를 선택한 경우 IP 주소당 5분당 허용되는 최대 요청을 입력합니다. HTTP Flood 보호 활성화 파라미터에 yes - AWS WAF rate-based rule 대해를 선택한 경우 허용되는 최소 값은 100입니다. HTTP Flood 보호 활성화 파라미터에 yes – Amazon Athena log parser 대해 yes - AWS Lambda log parser 또는를 선택한 경우 모든 값이 될 수 있습니다. HTTP 이 보호를 비활성화하려면이 파라미터를 무시합니다.
사용자 지정 규칙 - 타사 IP 평판 목록		
평판 목록 보호 활성화	yes	타사 평판 목록에 있는 IP 주소의 요청을 차단yes하려면 선택합니다(지원되는 목록에는 스팸하우스, 새로운 위협 및 Tor 종료 노드가 포함됨).
레거시 사용자 지정 규칙		

파라미터	기본값	설명
SQL 주입 보호 활성화	yes	일반적인 SQL 주입 공격을 차단하도록 설계된 구성 요소를 켜yes려면 선택합니다. AWS 관리형 코어 규칙 세트 또는 AWS 관리형 SQL 데이터베이스 규칙 그룹을 사용하지 않는 경우 활성화하는 것이 좋습니다. 8KB(yes8yes - MATCH,192바이트yes - NO_MATCH)를 초과하는 크기 초과 요청을 AWS WAF 처리할 옵션((계속), 또는) 중 하나를 선택할 수 있습니다. 기본적으로는 규칙 yes 검사 기준에 따라 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 검사합니다. 자세한 내용은 초과 크기의 웹 요청 구성 요소 처리를 참조하세요. 이 기능을 비활성화no하려면 를 선택합니다. **Note** CloudFormation 스택은 선택한 크기 초과 처리 옵션을 기본 SQL 주입 보호 규칙에 추가하고에 배포합니다 AWS 계정. 외부에서 규칙을 사용자 지정한 경우 스

파라미터	기본값	설명
		택 업데이트 후 변경 CloudFormation사항을 덮어씁니다.

파라미터	기본값	설명
SQL 주입 방지를 위한 민감도 수준	LOW	SQL 주입 공격을 검사하는 데 AWS WAF 사용할 민감도 수준을 선택합니다. HIGH는 더 많은 공격을 탐지하지만 더 많은 오탐을 생성할 수 있습니다. LOW는 일반적으로 SQL 주입 공격에 대한 다른 보호 기능이 이미 있거나 거짓 긍정에 대한 허용 오차가 낮은 리소스에 더 나은 선택입니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS WAF SQL 주입 규칙 문 및 속성에 대한 민감도 수준 추가를 참조하세요. SensitivityLevel SQL 주입 방지를 비활성화하려면이 파라미터를 무시합니다. **Note** CloudFormation 스택은 선택한 민감도 수준을 기본 SQL 주입 보호 규칙에 추가하고 에 배포합니다 AWS 계정. 외부에서 규칙을 사용자 지정한 경우 스택 업데이트 후

파라미터	기본값	설명
		변경 CloudFormation 사항을 덮어씁니다.

파라미터	기본값	설명
교차 사이트 스크립팅 보호 활성화	yes	일반적인 XSS 공격을 차단하도록 설계된 구성 요소를 켜yes려면 선택합니다. AWS 관리형 코어 규칙 세트를 사용하지 않는 경우 활성화하는 것이 좋습니다. 8KB(yes8yes - MATCH,192바이트yes - NO_MATCH)를 초과하는 크기 초과 요청을 AWS WAF 처리할 옵션((계속), 또는) 중 하나를 선택할 수도 있습니다. 기본적으로는 규칙 검사 기준에 따라 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 검사하는 Continue 옵션을 yes 사용합니다. 자세한 내용은 요청 구성 요소의 크기 초과 처리를 참조하세요. 이 기능을 비활성화no하려면를 선택합니다. **Note** CloudFormation 스택은 선택한 크기 초과 처리 옵션을 기본 교차 사이트 스크립팅 규칙에 추가하고에 배포합니다 AWS 계정. 외부에서 규칙을 사용자 지정한 경우 스택 업데이트 후 변경

파라미터	기본값	설명
		CloudFormation사항을 덮어씁니다.
허용 및 거부된 IP 보존 설정		
허용된 IP 세트의 보존 기간(분)	-1	허용된 IP 세트에 대해 IP 보존을 활성화하려면 보존 기간(15분)으로 숫자(이상)를 입력합니다. 보존 기간에 도달한 IP 주소는 만료되며 솔루션은 IP 세트에서 IP 주소를 제거합니다. 이 솔루션은 최소 15분의 보존 기간을 지원합니다. 0에서 사이의 숫자를 입력하면 15솔루션은 이를 로 취급합니다15. IP 보존을 끄려면 -1 (기본값)으로 둡니다.
거부된 IP 세트의 보존 기간(분)	-1	거부된 IP 세트에 대해 IP 보존을 활성화하려면 보존 기간(15분)으로 숫자(이상)를 입력합니다. 보존 기간에 도달한 IP 주소는 만료되며 솔루션은 IP 세트에서 IP 주소를 제거합니다. 이 솔루션은 최소 15분의 보존 기간을 지원합니다. 0에서 사이의 숫자를 입력하면 15솔루션은 이를 로 취급합니다15. IP 보존을 끄려면 -1 (기본값)으로 둡니다.

파라미터	기본값	설명
허용 또는 거부 IP 세트 만료 시 알림을 수신하기 위한 이메일	<선택 사항 입력>	IP 보존 기간 파라미터(이전 파라미터 2개 참조)를 활성화하고 IP 주소가 만료될 때 이메일 알림을 받으려면 유효한 이메일 주소를 입력합니다. IP 보존을 활성화하지 않았거나 이메일 알림을 끄려면 비워 둡니다(기본값).
고급 설정		
로그 그룹의 보존 기간(일)	365	CloudWatch 로그 그룹에 대해 보존을 활성화하려면 보존 기간(1일)으로 숫자(이상)를 입력합니다. 1일(1)에서 10년() 사이의 보존 기간을 선택할 수 있습니다3650. 기본적으로 로그는 1년 후에 만료됩니다. 로그를 무기한으로 유지-1하려면 로 설정합니다.

6. Next(다음)를 선택합니다.
7. 스택 옵션 구성 페이지에서 스택의 리소스에 대한 태그(키-값 페어)를 지정하고 추가 옵션을 설정할 수 있습니다. Next(다음)를 선택합니다.
8. 검토 및 생성 페이지에서 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스와 필요한 추가 기능을 생성할 것임을 확인하는 상자를 선택합니다.
9. 제출을 선택하여 스택을 배포합니다.

   AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 봅니다. 약 15분 후에 상태가 CREATE_COMPLETE가 됩니다.

> **Note**
>
> 이 솔루션에는 `Log Parser`, `IP Lists Parser`및 `Access Handler` AWS Lambda 함수 외에도 초기 구성 중에만 또는 리소스가 업데이트되거나 삭제될 때만 실행되는 `helper` 및 `custom-resource` Lambda 함수가 포함되어 있습니다.
> 이 솔루션을 사용하면 AWS Lambda 콘솔에 모든 함수가 표시되지만 세 가지 기본 솔루션 함수만 정기적으로 활성화됩니다. 다른 두 함수는 삭제하지 마세요. 연결된 리소스를 관리하는 데 필요합니다.

스택 리소스에 대한 세부 정보를 보려면 출력 탭을 선택합니다. 여기에는 API Gateway 허니팟 엔드포인트인 BadBotHoneypotEndpoint 값이 포함됩니다. 이 값은 웹 애플리케이션의 Honeypot 링크 임베드에 사용되므로 기억하세요.

2단계. 웹을 웹 애플리케이션ACL과 연결

CloudFront 배포(들) 또는 ALB(들)을 업데이트하여 1단계에서 생성한 리소스를 사용하여 활성화 AWS WAF 하고 로깅합니다. 스택을 시작합니다.

1. AWS WAF 콘솔에 로그인합니다.
2. ACL 사용할 웹을 선택합니다.
3. 연결된 AWS 리소스 탭에서 AWS 리소스 추가를 선택합니다.
4. 리소스 유형에서 CloudFront 배포 또는를 선택합니다ALB.
5. 목록에서 리소스를 선택한 다음 추가를 선택하여 변경 사항을 저장합니다.

3단계. 웹 액세스 로깅 구성

CloudFront Log Parser Lambda 함수에이 데이터를 사용할 수 있도록 또는를 구성하여 적절한 Amazon S3 버킷으로 웹 액세스 로그를 ALB 전송합니다.

배포의 CloudFront 웹 액세스 로그 저장

1. Amazon CloudFront 콘솔에 로그인합니다.
2. 웹 애플리케이션의 배포를 선택하고 배포 설정을 선택합니다.
3. General 탭에서 Edit를 선택합니다.

4. AWS WAF 웹 ACL에서 생성된 웹 ACL 솔루션(스택 이름 파라미터)을 선택합니다.
5. [Logging]에서 [On]을 선택합니다.
6. 로그용 버킷에서 웹 액세스 로그를 저장하는 데 사용할 S3 버킷을 선택합니다. 이 버킷은 기본 스택에 사용되고에 로그를 쓸 수 있는 권한이 있는 신규 또는 기존 S3 버킷일 수 CloudFront 있습니다. 드롭다운 목록에는 현재와 연결된 버킷이 나열됩니다 AWS 계정. 자세한 내용은 Amazon CloudFront 개발자 안내서의 기본 CloudFront 배포 시작하기를 참조하세요.
7. 로그 접두사를 솔루션 배포에 사용되는 접두사로 설정합니다. 기본 스택, 파라미터 탭AppAccessLogBucketPrefixParam(기본값)에서 접두사를 찾을 수 있습니다`AWS Logs/`.
8. [Yes, edit]를 선택하여 변경 사항을 저장합니다.

자세한 내용은 Amazon CloudFront 개발자 안내서의 표준 로그(액세스 로그) 구성 및 사용을 참조하세요.

Application Load Balancer의 웹 액세스 로그 저장

1. Amazon Elastic Compute Cloud(AmazonEC2) 콘솔에 로그인합니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. 웹 애플리케이션의를 선택합니다ALB.
4. 설명 탭에서 속성 편집을 선택합니다.
5. [Enable access logs]를 선택합니다.
6. S3 위치에 웹 액세스 로그를 저장하는 데 사용할 S3 버킷의 이름을 입력합니다. 이는 기본 스택에 사용되고 Application Load Balancer가 로그를 작성할 수 있는 권한이 있는 신규 또는 기존 S3 버킷일 수 있습니다.
7. 로그 접두사를 솔루션 배포에 사용되는 접두사로 설정합니다. 기본 스택, 파라미터 탭AppAccessLogBucketPrefixParam(기본값)에서 접두사를 찾을 수 있습니다`AWS Logs/`.
8. 저장(Save)을 선택합니다.

자세한 내용은 Elastic Load Balancing Load Balancing 사용 설명서의 Application Load Balancer에 대한 액세스 로그를 참조하세요.

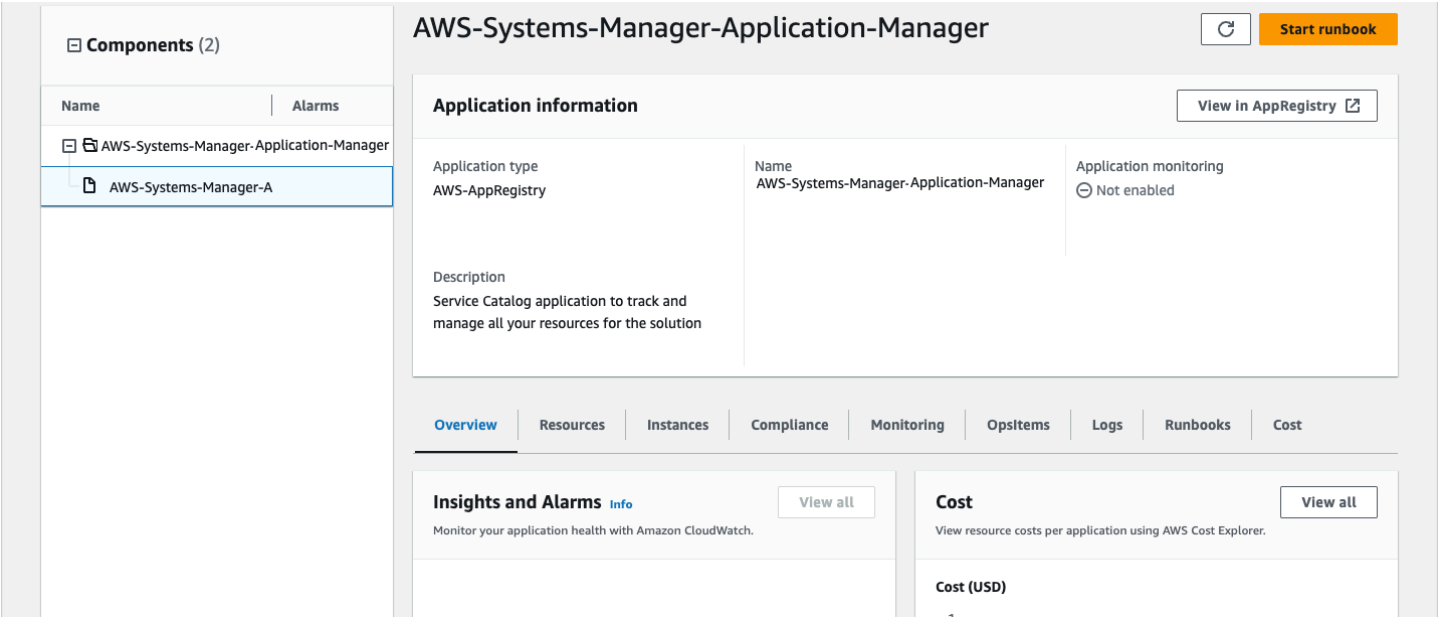
를 사용하여 솔루션 모니터링 AppRegistry

솔루션에는 CloudFormation 템플릿과 기본 AppRegistry 리소스를 Service Catalog AppRegistry 및 AWS Systems Manager Application Manager의 애플리케이션으로 등록하는 Service Catalog 리소스가 포함되어 있습니다.

AWS Systems Manager Application Manager는이 솔루션과 해당 리소스에 대한 애플리케이션 수준 보기를 제공하므로 다음을 수행할 수 있습니다.

- 중앙 위치에서이 솔루션과 연결된 스택 및 로그에 배포된 리소스 AWS 계정, 배포된 리소스의 비용을 모니터링합니다.
- 애플리케이션의 컨텍스트에서이 솔루션의 리소스에 대한 작업 데이터를 봅니다. 예를 들어 배포 상태, CloudWatch 경보, 리소스 구성 및 운영 문제 등이 있습니다.

다음 그림은 Application Manager의 솔루션 스택에 대한 애플리케이션 보기의 예를 보여줍니다.



Application Manager의 솔루션 스택

CloudWatch Application Insights 활성화

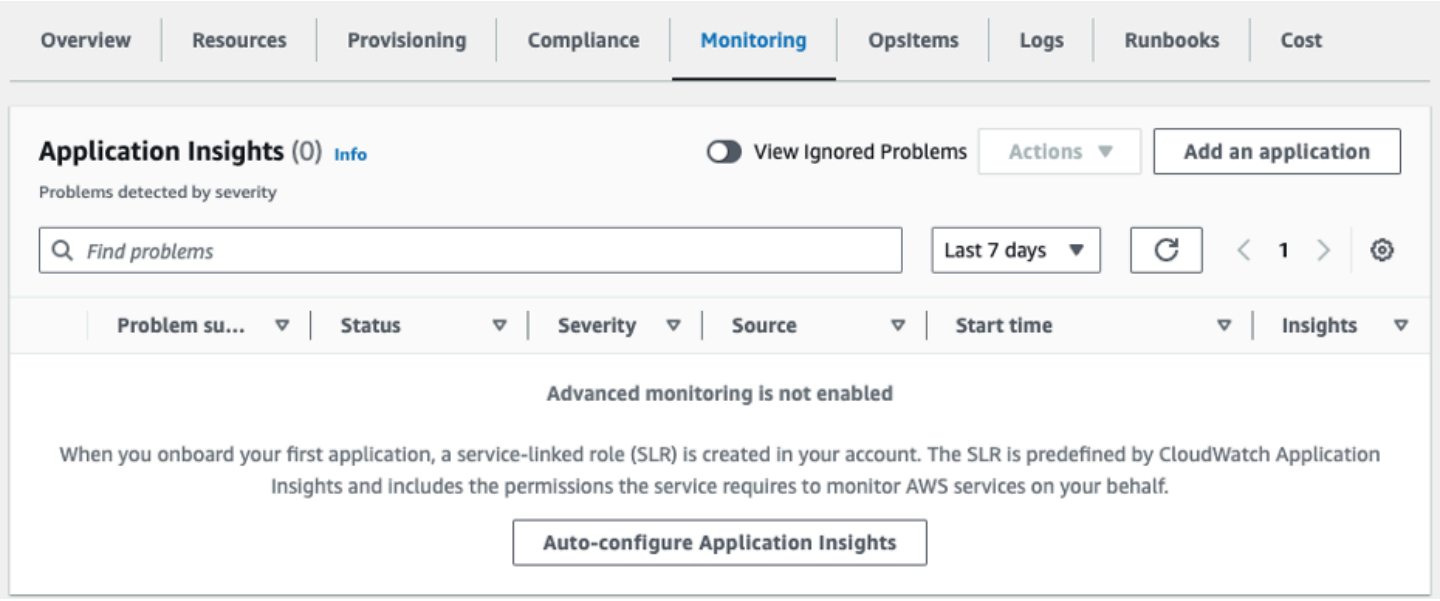
1. Systems Manager 콘솔에 로그인합니다.
2. 탐색 창에서 Application Manager를 선택합니다.

3. 애플리케이션에서이 솔루션의 애플리케이션 이름을 검색하고 선택합니다.

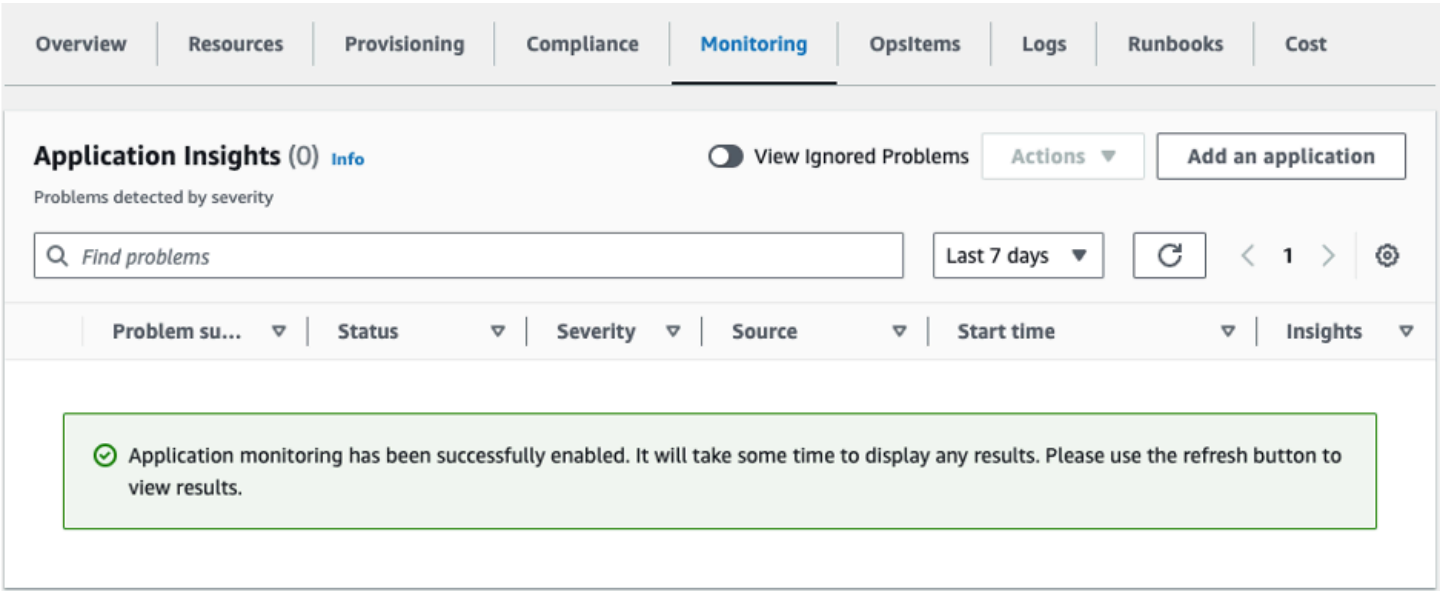
   애플리케이션 이름은 애플리케이션 소스 열에 App Registry가 있고 솔루션 이름, 리전, 계정 ID 또는 스택 이름의 조합이 있습니다.

4. 구성 요소 트리에서 활성화하려는 애플리케이션 스택을 선택합니다.

5. 모니터링 탭의 Application Insights에서 Application Insights 자동 구성을 선택합니다.



이제 애플리케이션 모니터링이 활성화되고 다음 상태 상자가 나타납니다.

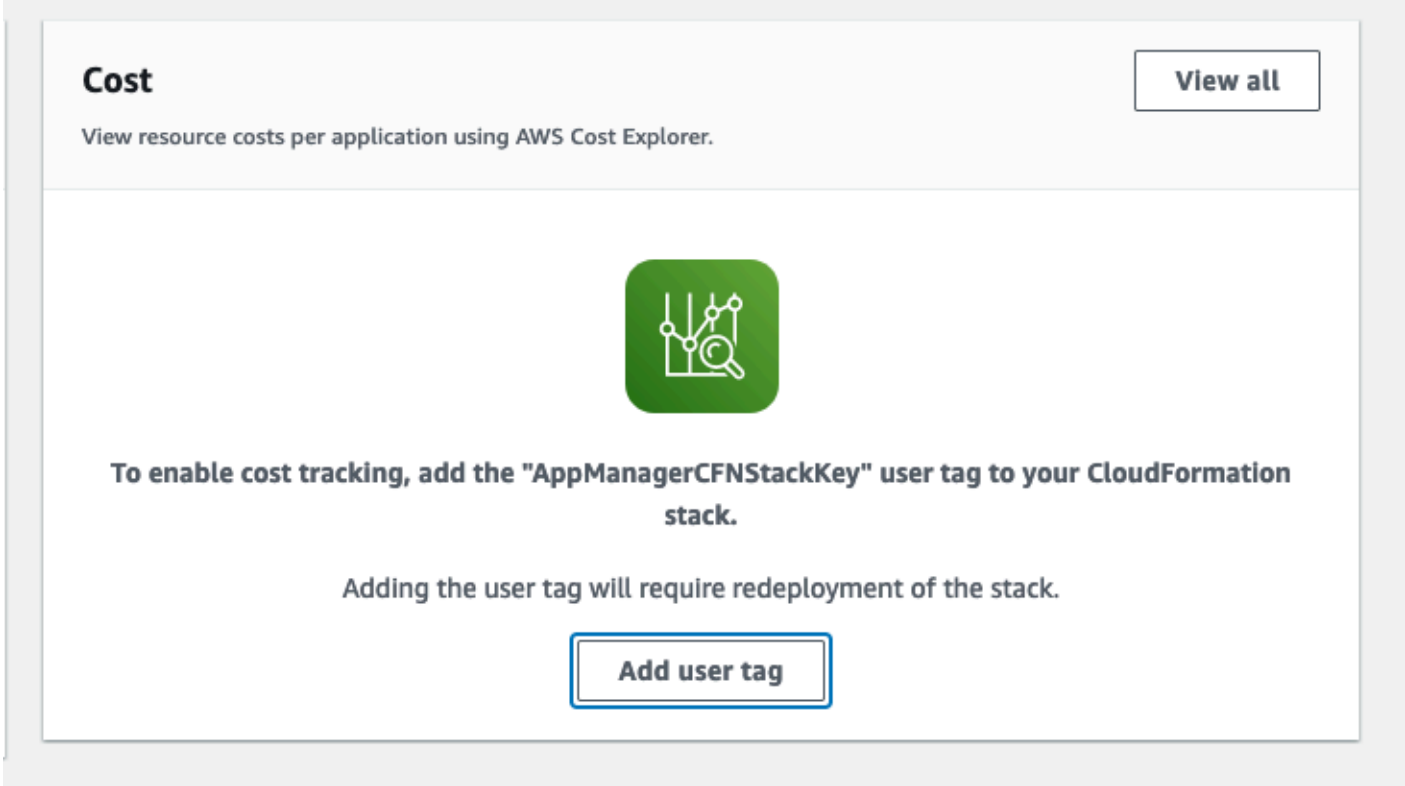


솔루션과 연결된 비용 태그 확인

솔루션과 관련된 비용 할당 태그를 활성화한 후 이 솔루션의 비용을 보려면 비용 할당 태그를 확인해야 합니다. 비용 할당 태그를 확인하려면 다음을 수행합니다.

1. Systems Manager 콘솔에 로그인합니다.
2. 탐색 창에서 Application Manager를 선택합니다.
3. 애플리케이션에서 이 솔루션의 애플리케이션 이름을 선택합니다.

   애플리케이션 이름은 애플리케이션 소스 열에 App Registry가 있고 솔루션 이름, 리전, 계정 ID 또는 스택 이름의 조합이 있습니다.
4. 개요 탭의 비용에서 사용자 태그 추가를 선택합니다.



5. 사용자 태그 추가 페이지에서 `confirm`를 입력한 다음 사용자 태그 추가를 선택합니다.

활성화 프로세스가 완료되고 태그 데이터가 표시되는 데 최대 24시간 정도 걸릴 수 있습니다.

솔루션과 관련된 비용 할당 태그 활성화

Cost Explorer를 활성화한 후 이 솔루션의 비용을 보려면 이 솔루션과 관련된 비용 할당 태그를 활성화해야 합니다. 비용 할당 태그는 조직의 관리 계정에서만 활성화할 수 있습니다. 비용 할당 태그를 활성화하려면 다음을 수행합니다.

1. AWS Billing and Cost Management 및 비용 관리 콘솔에 로그인합니다.
2. 탐색 창에서 비용 할당 태그를 선택합니다.
3. 비용 할당 태그 페이지에서 AppManagerCFNStackKey 태그를 필터링한 다음 표시된 결과에서 태그를 선택합니다.
4. 활성화를 선택합니다.

AWS Cost Explorer

먼저 활성화해야 AWS Cost Explorer하는 와의 통합을 통해 Application Manager 콘솔 내에서 애플리케이션 및 애플리케이션 구성 요소와 관련된 비용의 개요를 볼 수 있습니다. Cost Explorer를 사용하면 시간 경과에 따른 AWS 리소스 비용 및 사용량을 볼 수 있어 비용을 관리하는 데 도움이 됩니다. 솔루션에 대해 Cost Explorer를 활성화하려면 다음을 수행합니다.

1. AWS Cost Management 콘솔에 로그인합니다.
2. 탐색 창에서 Cost Explorer를 선택하여 시간 경과에 따른 솔루션의 비용 및 사용량을 확인합니다.

솔루션 업데이트

이전에 솔루션을 배포한 경우이 절차에 따라 솔루션의 CloudFormation 스택을 업데이트하여 솔루션 프레임워크의 최신 버전을 가져옵니다. 스택을 업데이트하기 전에 업데이트 고려 사항을 주의 깊게 읽어보세요.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 왼쪽 탐색 메뉴에서 스택을 선택합니다.
3. 기존 `aws-waf-security-automations` CloudFormation 스택을 선택합니다.
4. 업데이트를 선택합니다.
5. 현재 템플릿 교체를 선택합니다.
6. 템플릿 지정에서 다음을 수행합니다.
   a. Amazon S3URL를 선택합니다.
   b. 의 링크를 복사합니다`aws-waf-security-automations.template`AWS CloudFormation.
   c. Amazon S3 URL 상자에 링크를 붙여 넣습니다.
   d. Amazon S3 URL텍스트 상자에 올바른 템플릿이 URL 표시되는지 확인합니다.
   e. Next(다음)를 선택합니다.
   f. 다음을 다시 선택합니다.
7. 파라미터에서 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 1단계를 참조하세요. 스택을 시작하여 파라미터에 대한 세부 정보를 확인합니다.
8. Next(다음)를 선택합니다.
9. Configure stack options(스택 옵션 구성) 페이지에서 Next(다음)를 선택합니다.
10. 검토 페이지에서 설정을 검토하고 확인합니다.
11. 템플릿이 IAM 리소스를 생성할 수 있음을 확인하는 상자를 선택합니다.
12. 변경 세트 보기를 선택하고 변경 사항을 확인합니다.
13. 스택 생성을 선택하여 스택을 배포합니다.

콘솔의 상태 열에서 스택 AWS CloudFormation 의 상태를 볼 수 있습니다. 약 15분 후에 상태가 UPDATE_COMPLETE로 표시됩니다.

업데이트 고려 사항

다음 섹션에서는이 솔루션 업데이트에 대한 제약 조건과 고려 사항을 제공합니다.

리소스 유형 업데이트

스택을 생성한 후 엔드포인트 파라미터를 업데이트하려면 새 스택을 배포해야 합니다. 스택을 업데이트할 때 엔드포인트 파라미터를 변경하지 마십시오.

WAFV2 업그레이드

버전 3.0부터이 솔루션은 AWS WAF V2를 지원합니다. 모든 AWS WAF Classic API 호출을 AWS WAF V2 API 호출로 교체했습니다. 이렇게 하면 Node.js에 대한 종속성이 제거되고 대부분의 up-to-date Python 런타임이 사용됩니다. 이 솔루션을 최신 기능 및 개선 사항과 함께 계속 사용하려면 버전 3.0 이상을 새 스택으로 배포해야 합니다.

스택 업데이트 시 사용자 지정

이 out-of-box 솔루션은 CloudFormation 스택을 사용하여 기본 구성의 AWS WAF 규칙 세트를 AWS 계정 에 배포합니다. 솔루션에 의해 배포된 규칙에 사용자 지정을 적용하는 것은 권장하지 않습니다. 스택 업데이트는 이러한 변경 사항을 덮어씁니다. 사용자 지정 규칙이 필요한 경우 솔루션 외부에서 별도의 규칙을 생성하는 것이 좋습니다.

> **Note**
>
> 버전 3.0 또는 3.1에서이 솔루션의 버전 3.2 이상으로 업그레이드하고 허용 또는 거부된 IP 세트에 IP 주소를 수동으로 삽입한 경우 해당 IP 주소가 손실될 위험이 있습니다. 이 문제가 발생하지 않도록 하려면 솔루션을 업그레이드하기 전에 허용 또는 거부된 IP 세트의 IP 주소를 복사합니다. 그런 다음 업그레이드를 완료한 후 필요에 따라 IP 주소를 IP 세트에 다시 추가합니다. get-ip-set 및 update-ip-set CLI 명령을 참조하세요. 버전 3.2 이상을 이미 사용하고 있는 경우 이 단계를 무시하세요.

솔루션 제거

솔루션을 제거하려면 CloudFormation 스택을 삭제합니다.

1. AWS CloudFormation 콘솔에 로그인합니다.

2. 솔루션의 상위 스택을 선택합니다. 다른 모든 솔루션 스택은 자동으로 삭제됩니다.
3. Delete(삭제)를 선택합니다.

> **Note**
>
> 솔루션을 제거하면 Amazon S3 버킷을 제외한 솔루션에서 사용하는 모든 AWS 리소스가 삭제됩니다. AWA WAF API 할당량으로 인한 속도 초과 제한 문제로 인해 일부 IP 세트가 삭제되지 않는 경우 해당 IP 세트를 수동으로 삭제한 다음 스택을 삭제합니다.

솔루션 사용

이 섹션에서는 솔루션을 배포한 후 솔루션을 사용하는 방법에 대한 자세한 지침을 제공합니다.

허용 및 거부된 IP 세트 수정(선택 사항)

이 솔루션의 CloudFormation 스택을 배포한 후 허용 및 거부된 IP 세트를 수동으로 수정하여 필요에 따라 IP 주소를 추가하거나 제거할 수 있습니다.

1. AWS WAF 콘솔에 로그인합니다.
2. 왼쪽 탐색 창에서 IP 세트를 선택합니다.
3. 허용 목록에 대한 IP 세트를 선택하고 신뢰할 수 있는 소스의 IP 주소를 추가합니다.
4. 거부 목록에 대한 IP 세트를 선택하고 차단하려는 IP 주소를 추가합니다.

웹 애플리케이션에 Honeypot 링크 포함(선택 사항)

1단계에서 잘못된 봇 보호 활성화 파라미터yes에 대해를 선택한 경우. 스택을 시작하면 CloudFormation 템플릿이 상호 작용이 적은 프로덕션 허니팟에 트랩 엔드포인트를 생성합니다. 이 트랩은 콘텐츠 스크레이퍼 및 잘못된 봇의 인바운드 요청을 감지하고 전환하기 위한 것입니다. 유효한 사용자는이 엔드포인트에 액세스하려고 시도하지 않습니다.

그러나 보안 취약성을 스캔하고 이메일 주소를 스크레이핑하는 맬웨어와 같은 콘텐츠 스크레이퍼 및 봇은 트랩 엔드포인트에 액세스하려고 할 수 있습니다. 이 시나리오에서 `Access Handler` Lambda 함수는 요청을 검사하여 오리진을 추출한 다음 연결된 AWS WAF 규칙을 업데이트하여 해당 IP 주소의 후속 요청을 차단합니다.

다음 절차 중 하나를 사용하여 CloudFront 배포 또는의 요청에 대한 허니팟 링크를 포함합니다ALB.

Honeypot 엔드포인트의 CloudFront 오리진 생성

CloudFront 배포와 함께 배포된 웹 애플리케이션에이 절차를 사용합니다. 를 사용하면 로봇 제외 표준을 무시하는 콘텐츠 스크레이퍼와 봇을 식별하는 데 도움이 되는 `robots.txt` 파일을 포함할 CloudFront수 있습니다. 다음 단계를 완료하여 숨겨진 링크를 임베드한 다음 `robots.txt` 파일에 명시적으로 허용하지 않습니다.

1. AWS CloudFormation 콘솔에 로그인합니다.

2. 1단계에서 빌드한 스택을 선택합니다. 스택 시작
3. 출력 탭을 선택합니다.
4. BadBotHoneypotEndpoint 키에서 엔드포인트를 복사합니다URL. 여기에는이 절차를 완료하는 데 필요한 두 가지 구성 요소가 포함되어 있습니다.
   - 엔드포인트 호스트 이름(예: `xxxxxxxxxx.execute-api.region.amazonaws.com`)
   - 요청URI(`/ProdStage`)
5. Amazon CloudFront 콘솔에 로그인합니다.
6. 사용할 배포를 선택합니다.
7. Distribution Settings(배포 설정)를 선택합니다.
8. 오리진 탭에서 오리진 생성을 선택합니다.
9. 오리진 도메인 이름 필드에 2단계에서 복사URL한 엔드포인트의 호스트 이름 구성 요소를 붙여 넣습니다. 웹을 웹 애플리케이션ACL과 연결합니다.
10. 오리진 경로에서 2단계에서 복사URL한 요청을 붙여 넣습니다. 웹을 웹 애플리케이션ACL과 연결합니다.
11. 다른 필드의 기본값을 수락합니다.
12. 생성(Create)을 선택합니다.
13. 동작 탭에서 동작 생성을 선택합니다.
14. 새 캐시 동작을 생성하고 새 오리진을 가리킵니다. 웹 애플리케이션의 다른 콘텐츠와 유사한 가짜 제품 이름과 같은 사용자 지정 도메인을 사용할 수 있습니다.
15. 허니팟을 가리키는 콘텐츠에이 엔드포인트 링크를 포함합니다. 인간 사용자로부터이 링크를 숨깁니다. 예를 들어 다음 코드 샘플을 검토합니다.

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

> **Note**
>
> 웹 사이트 환경에서 작동하는 태그 값을 확인하는 것은 사용자의 책임입니다. 환경이 이를 준수하지 않는 `rel="nofollow"` 경우를 사용하지 마십시오. 로봇 메타 태그 구성에 대한 자세한 내용은 Google 개발자 안내서를 참조하세요.

16. 다음과 같이 허니팟 링크를 명시적으로 허용하지 않도록 웹 사이트의 루트에 있는 `robots.txt` 파일을 수정합니다.

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

Honeypot 엔드포인트를 외부 링크로 포함

와 함께 배포된 웹 애플리케이션에이 절차를 사용합니다ALB.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 1단계에서 빌드한 스택을 선택합니다. 스택을 시작합니다.
3. 출력 탭을 선택합니다.
4. BadBotHoneypotEndpoint 키에서 엔드포인트를 복사합니다URL.
5. 웹 콘텐츠에이 엔드포인트 링크를 포함합니다. 2단계에서 복사URL한 전체를 사용합니다. 웹을 웹 애플리케이션ACL과 연결합니다. 인간 사용자로부터이 링크를 숨깁니다. 예를 들어 다음 코드 샘플을 검토합니다.

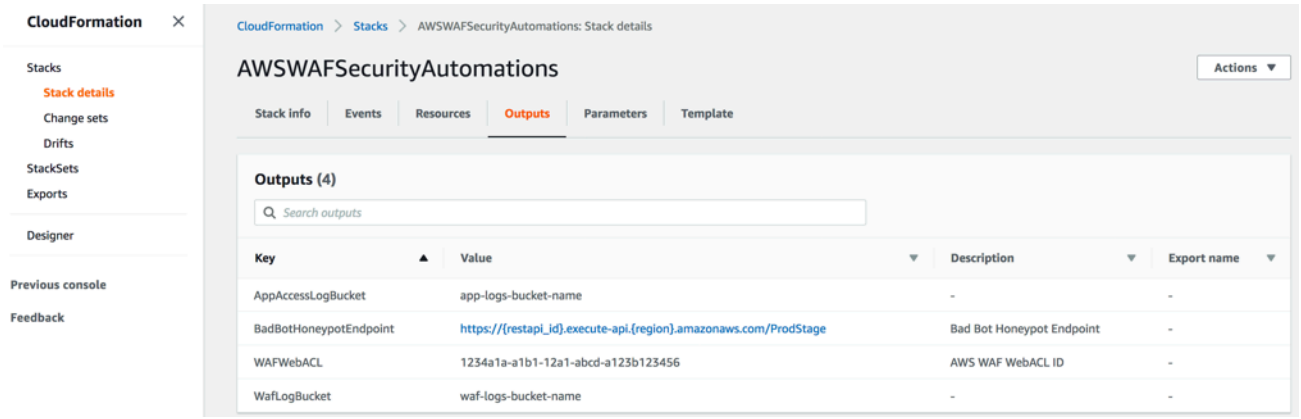
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> 이 절차에서는 `rel=nofollow`를 사용하여 로봇이 허니팟에 액세스하지 않도록 지시합니다URL. 그러나 링크는 외부에 내장되어 있으므로 링크를 명시적으로 허용하지 않는 `robots.txt` 파일을 포함할 수 없습니다. 웹 사이트 환경에서 작동하는 태그를 확인하는 것은 사용자의 책임입니다. 환경이 이를 준수하지 않는 `rel="nofollow"` 경우를 사용하지 마십시오.

Lambda 로그 구문 분석기 JSON 파일 사용

HTTP Flood 보호를 위해 Lambda 로그 구문 분석기 JSON 파일 사용

Flood 보호 활성화 템플릿 파라미터에 `Yes - AWS Lambda log parser` 대해를 선택한 경우 이 솔루션은 라는 구성 파일을 생성하여 AWS WAF 로그 파일을 저장하는 데 사용되는 Amazon S3 버킷에 *<stack_name>*`-waf_log_conf.json` 업로드합니다. HTTP 버킷 이름을 찾으려면 CloudFormation 출력의 WafLogBucket 변수를 참조하세요. 다음 그림은 예를 보여줍니다.



스택 출력

Amazon S3에서 *<stack_name>*-waf_log_conf.json 파일을 편집하고 덮어쓰면 Log Parser Lambda 함수는 새 AWS WAF 로그 파일을 처리할 때 새 값을 고려합니다. 다음은 구성 파일 예제입니다.

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

HTTP 플러드 구성 파일

파라미터에는 다음이 포함됩니다.

- 일반
  - 요청 임계값(필수) - IP 주소당 5분당 허용되는 최대 요청 수입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
  - 차단 기간(필수) - 해당 IP 주소를 차단하는 기간(분)입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.

- 무시된 접미사 -이 유형의 리소스에 액세스하는 요청은 임계값을 요청하는 데 포함되지 않습니다. 기본적으로이 목록은 비어 있습니다.
- URI list -이 옵션을 사용하여 특정에 대한 사용자 지정 요청 임계값 및 차단 기간을 정의합니다URLs. 기본적으로이 목록은 비어 있습니다.

WAF 로그가에 도착하면 구성 파일의 구성을 사용하여 Lambda 로그 구문 분석기 함수에 의해 WafLogBucket처리됩니다. 솔루션은 *<stack_name>*-waf_log_out.json 동일한 버킷에 있는 라는 출력 파일에 결과를 기록합니다. 출력 파일에 공격자로 식별된 IP 주소 목록이 포함되어 있는 경우 솔루션은 이를 HTTP Flood용 WAF IP 세트에 추가하고 애플리케이션에 액세스할 수 없도록 차단합니다. 출력 파일에 IP 주소가 없는 경우 구성 파일이 유효한지 또는 구성 파일에 따라 속도 제한을 초과했는지 확인합니다.

스캐너 및 프로브 보호를 위해 Lambda 로그 구문 분석기 JSON 파일 사용

스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - AWS Lambda log parser` 대해를 선택한 경우이 솔루션은 라는 구성 파일을 생성하여 CloudFront 또는 Application Load Balancer 로그 파일을 저장하는 데 사용되는 정의된 Amazon S3 버킷에 *<stack_name>*-app_log_conf.json 업로드합니다.

Amazon S3에서 *<stack_name>*-app_log_conf.json를 편집하고 덮어쓰면 `Log Parser` Lambda 함수는 새 AWS WAF 로그 파일을 처리할 때 새 값을 고려합니다. 다음은 구성 파일 예제입니다.

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

스캐너 및 프로브 구성 파일

파라미터에는 다음이 포함됩니다.

- 일반

- 오류 임계값(필수) - IP 주소당 분당 허용되는 최대 잘못된 요청 수입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
- 차단 기간(필수) - 해당 IP 주소를 차단하는 기간(분)입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
- 오류 코드 - 오류로 간주되는 Teturn 상태 코드입니다. 기본적으로이 목록은 , `400 (Bad Request)`, `401 (Unauthorized)`, 및 HTTP 상태 코드를 오류로 간주합니다`403 (Forbidden)404 (Not Found)405 (Method Not Allowed)`.

- URI list -이 옵션을 사용하여 특정에 대한 사용자 지정 요청 임계값 및 차단 기간을 정의합니다URLs. 기본적으로이 목록은 비어 있습니다.

애플리케이션 액세스 로그가에 도착하면 `Log Parser` Lambda 함수AppAccessLogBucket는 구성 파일의 구성을 사용하여 이를 처리합니다. 이 솔루션은 *<stack_name>*`-app_log_out.json` 동일한 버킷에 있는 라는 출력 파일에 결과를 기록합니다. 출력 파일에 공격자로 식별된 IP 주소 목록이 포함된 경우 솔루션은 이를 Scanner & Probe용 WAF IP 세트에 추가하고 애플리케이션에 액세스하지 못하도록 차단합니다. 출력 파일에 IP 주소가 없는 경우 구성 파일이 유효한지 또는 구성 파일에 따라 속도 제한을 초과했는지 확인합니다.

HTTP 플러드 Athena 로그 구문 분석기URI에서 국가 및 사용

국가 및 Athena 쿼리URI와 IPs 함께를 그룹화하여 예측할 수 없는 URI 패턴이 있는 HTTP홍수 공격을 탐지하고 차단할 수 있습니다. 이렇게 하려면 스택을 시작할 때 HTTP Flood Athena 쿼리의 요청별 그룹화 파라미터에 대한 옵션(`Country`, `URI`, `Country and URI`) 중 하나를 선택합니다.

국가별 요청 임계값 파라미터를 사용하여 국가별 요청 임계값을 입력할 수도 있습니다. 예: `{"TR": 50,"ER":150}`. 솔루션은 이러한 지정된 국가에서 시작된 요청에 대해 이러한 임계값을 사용합니다. 솔루션은 다른 국가의 요청에 기본 임계값을 사용합니다.

> **Note**
>
> 국가별 임계값을 정의하면 솔루션은 Athena 쿼리 그룹별 절의 국가를 자동으로 포함합니다. 자세한 내용은 1단계의 파라미터 표를 참조하세요. 스택을 시작합니다.

솔루션은 기본적으로 5분 동안 요청 임계값을 계산합니다. 이는 Athena 쿼리 실행 시간 일정(분) 파라미터로 구성할 수 있습니다.

> **Note**
>
> Athena 쿼리는 요청 임계값을 기간으로 나누어 분당 임계값을 계산합니다. 예제:
> 요청 임계값(기본 임계값 또는 국가별 임계값): 100
> Athena 쿼리 실행 시간 일정: 5
> 분당 요청 임계값: 20 = 100/5

Amazon Athena 쿼리 보기

서비스 장애 방지 활성화 또는 스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우이 솔루션은 CloudFront 또는 ALB (`ScannersProbesLogParser`) 또는 AWS WAF 로그()에 대한 Athena 쿼리를 생성 및 실행하고, 출력을 `HTTPFloodLogParser`구문 분석하고, AWS WAF 그에 따라 업데이트합니다. HTTP

성능을 개선하고 비용을 낮게 유지하기 위해 솔루션은 파일 이름의 타임스탬프를 기반으로 로그를 분할합니다. 이 솔루션은 파티션 키(년, 월, 일 및 시간)를 사용하기 위해 Athena 쿼리를 동적으로 생성합니다. 기본적으로 쿼리는 5분마다 실행됩니다. Athena 쿼리 실행 시간 일정(분) 템플릿 파라미터의 값을 변경하여 실행 일정을 구성할 수 있습니다. 각 쿼리 실행은 기본적으로 지난 4~5시간의 데이터를 스캔합니다. WAF 블록 기간 템플릿 파라미터의 값을 변경하여 쿼리가 스캔하는 데이터의 양을 구성할 수 있습니다. 또한이 솔루션은 쿼리 액세스 및 비용을 관리하기 위해 별도의 작업 그룹에 쿼리를 배치합니다.

> **Note**
>
> Athena가에 액세스하도록 구성되어 있는지 확인합니다 AWS AWS Glue Data Catalog. 이 솔루션은에서 액세스 로그 데이터 카탈로그를 생성하고 데이터를 처리하도록 Athena 쿼리를 AWS Glue 구성합니다. Athena가 올바르게 구성되지 않으면 쿼리가 실행되지 않습니다. 자세한 내용은 최신으로 업그레이드를 참조하세요 AWSAWS Glue Data Catalog step-by-step.

다음 절차에 따라 이러한 쿼리를 볼 수 있습니다.

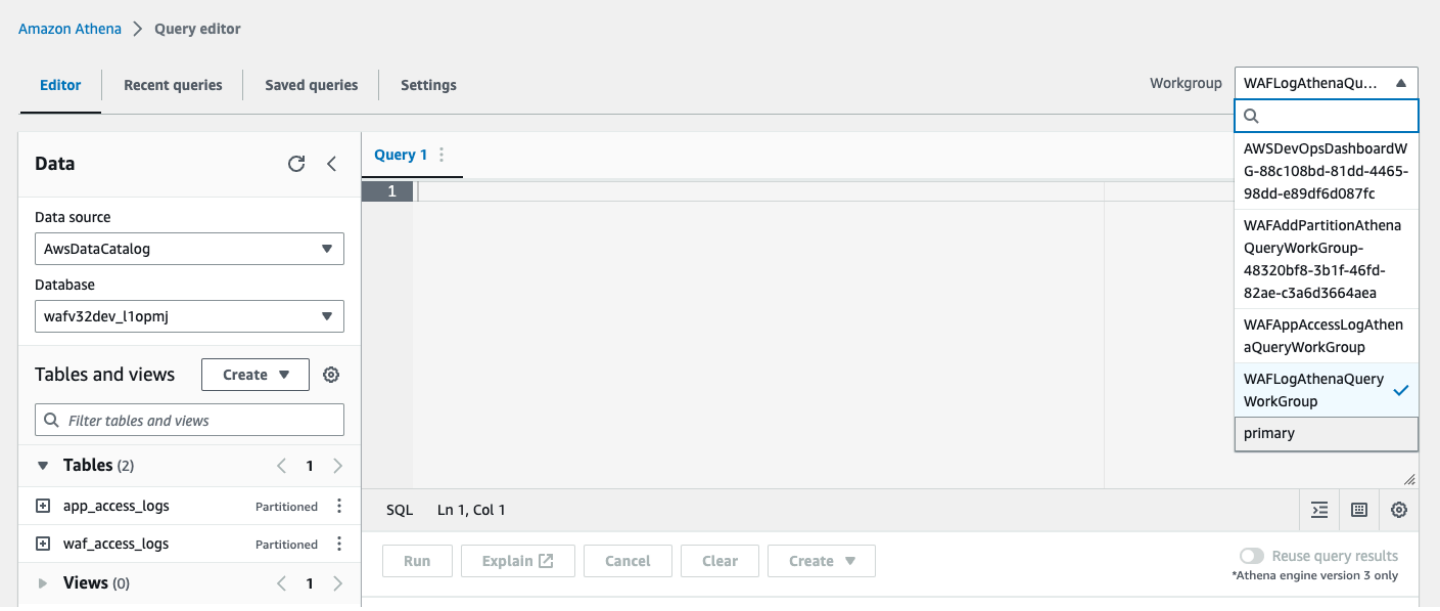
WAF 로그 쿼리 보기

1. Amazon Athena 콘솔에 로그인합니다.
2. 쿼리 편집기 시작을 선택합니다.

3. 이 솔루션의 데이터베이스를 선택합니다.
4. 드롭다운 목록에서 WAFLogAthenaQueryWorkGroup를 선택합니다.

> **Note**
>
> 이 작업 그룹은 Flood 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다. HTTP

5. 전환을 선택하여 작업 그룹을 전환합니다.



6. 기록 탭을 선택합니다.
7. 목록에서 SELECT 쿼리를 선택하고 엽니다.

애플리케이션 액세스 로그 쿼리 보기

1. Amazon Athena 콘솔에 로그인합니다.
2. 작업 그룹 탭을 선택합니다.
3. 목록에서 WAFAppAccessLogAthenaQueryWorkGroup를 선택합니다.

> **Note**
>
> 이 작업 그룹은 스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다.

4. 작업 그룹 전환을 선택합니다.
5. 최근 쿼리 탭을 선택합니다.
6. 목록에서 `SELECT` 쿼리를 선택하고 엽니다.

Athena 파티션 쿼리 추가 보기

1. Amazon Athena 콘솔에 로그인합니다.
2. 작업 그룹 탭을 선택합니다.
3. 목록에서 WAFAddPartitionAthenaQueryWorkGroup를 선택합니다.

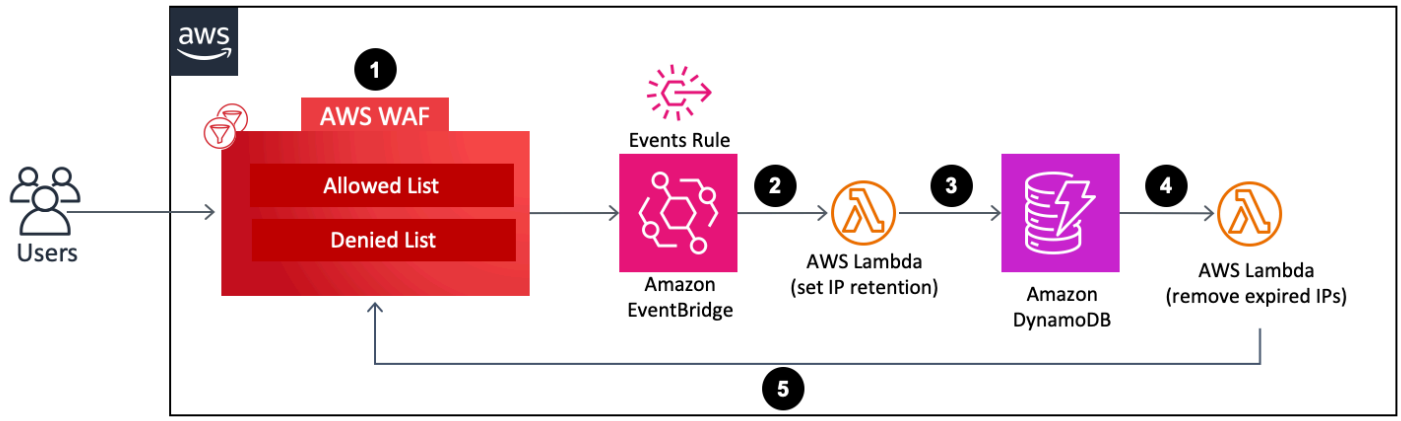
> **Note**
>
> 이 작업 그룹은 HTTP 서비스 장애 방지 활성화 및/또는 스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다.

4. 작업 그룹 전환을 선택합니다.
5. 기록 탭을 선택합니다.
6. 목록에서 `ALTER TABLE` 쿼리를 선택하고 엽니다. 이러한 쿼리는 매시간 실행되어 Athena 테이블에 새 시간당 파티션을 추가합니다.

허용 및 거부 IP 세트에서 AWS WAF IP 보존 구성

솔루션이 생성하는 허용 및 거부 IP 세트에서 AWS WAF IP 보존을 구성할 수 있습니다. 다음 섹션에서는 작동 방식을 설명하고 설정 단계를 제공합니다.

작동 방법



허용 및 거부 IP 세트의 WAF IP 보존

1. 사용자가 허용 또는 거부 IP WAF 세트를 업데이트(IP 주소 추가 또는 삭제)하면이 작업은 `UpdateIPSet` API 호출을 AWS WAF 호출하고 이벤트를 생성합니다.
2. Amazon EventBridge 이벤트 규칙은 사전 정의된 이벤트 패턴을 기반으로 이벤트를 감지하고 Lambda 함수를 호출하여 업데이트 후 IP 세트에 있는 모든 IP 주소의 보존 기간을 설정합니다.
3. Lambda 함수는 이벤트를 처리하고 관련 데이터를 IP 보존(예: IP 세트 이름, ID, 범위, IP 주소)에 추출하여 DynamoDB 테이블에 삽입합니다. 또한 각 DynamoDB 항목에 대한 `ExpirationTime` 속성을 삽입합니다. 이 솔루션은 이벤트 시간에 사용자 정의 보존 기간을 추가하여 만료 시간을 계산합니다. 테이블에는 DynamoDB 스트림 및 Time to Live(TTL)가 켜져 있습니다. TTL 속성은 입니다`ExpirationTime`.
4. 항목이 만료 시간에 도달하면 TTL가 호출되고 DynamoDB가 만료 시간 후 테이블에서 항목을 삭제합니다. 항목을 삭제하면 삭제된 항목이 DynamoDB 스트림에 추가되어 다운스트림 처리를 위해 Lambda 함수를 호출합니다.
5. Lambda 함수는 DynamoDB 스트림에서 삭제된 항목에 대한 정보를 얻고 AWS WAF API 호출하여 대상 IP 세트에서 항목에 포함된 만료된 AWS WAF IP 주소를 제거합니다.

IP 보존 켜기

다음 단계에 따라 IP 보존을 켭니다.

1. 배포하거나 업데이트하는 Cloudformation 스택에서 허용된 IP 세트의 IP 보존 기간(분)과 거부된 IP 세트의 IP 보존 기간(분)을 입력합니다. 최소 보존 기간은 15분입니다. 솔루션은 `0` ~ 사이의 숫자를 15로 처리합니다15. 배포 구성에 대한 자세한 내용은 1단계를 참조하세요. 스택을 시작합니다.

2. 만료된 IP 주소가 IP AWS WAF 세트에서 제거될 때 이메일 알림을 받으려면 이메일 주소를 입력합니다. 이메일 알림을 받기로 선택한 경우 솔루션이 성공적으로 배포된 후 수신한 이메일의 링크를 사용하여 구독을 확인해야 합니다. 배포 구성에 대한 자세한 내용은 1단계를 참조하세요. 스택을 시작합니다.
3. AWS WAF IP 주소를 추가하거나 삭제하여 IP 세트를 업데이트합니다. 이렇게 하면 IP 보존 프로세스가 시작되고 IP 만료 목록을 포함한 DynamoDB 항목이 생성됩니다. 이 만료 목록은 업데이트 후 IP 세트에 있는 AWS WAF IP 주소로 구성됩니다.
4. DynamoDB 항목이 만료 시간에 도달하고 테이블에서 삭제되면 솔루션은 항목의 IP 만료 목록에 포함된 IP 주소를 WAF IP 세트에서 삭제합니다.

> **Note**
>
> DynamoDB가에 의해 만료된 항목을 삭제하는 시간에 따라 AWS WAF IP 세트에서 만료된 IP 주소의 TTL실제 삭제 작업은 다를 수 있습니다. DynamoDB TTL 삭제는 주로 테이블의 크기 및 활동 수준에 따라 달라집니다. DynamoDB AWS WAF 삭제 작업의 잠재적 지연으로 인해 삭제 작업이 지연될 수 있습니다. 일반적으로 솔루션은 DynamoDB 삭제 직후 IP 세트에서 만료된 AWS WAF IP 주소를 TTL 삭제합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 DynamoDB Time to Live(TTL)를 참조하세요. DynamoDB

빌드 모니터링 대시보드

AWS 에서는 각 중요 엔드포인트에 대해 사용자 지정 기준 모니터링 시스템을 구성할 것을 권장합니다. 사용자 지정 지표 보기 생성 및 사용에 대한 자세한 내용은 CloudWatch 대시보드 - 사용자 지정 지표 보기 생성 및 사용 및 Amazon CloudWatch 대시보드 사용을 참조하세요.

다음 대시보드 스크린샷은 사용자 지정 기준 모니터링 시스템의 예를 보여줍니다.

대시보드에는 다음 지표가 표시됩니다.

- 허용된 요청과 차단된 요청 비교 - 허용된 액세스(정상 피크 액세스의 2배) 또는 차단된 액세스(차단된 요청이 1K000개를 초과하는 모든 기간)가 급증하는지 여부를 표시합니다.는 Slack 채널에 알림을 CloudWatch 보냅니다. 이 지표를 사용하여 알려진 DDoS 공격(차단된 요청이 증가할 때) 또는 새 버전의 공격(요청이 시스템에 액세스할 수 있는 경우)을 추적할 수 있습니다.

  > **Note**
  >
  > 참고: 솔루션은이 지표를 제공합니다.

- BytesDownloaded vs 업로드됨 - DDoS 공격이 일반적으로 배기 리소스에 대한 많은 액세스 권한을 받지 못하는 서비스를 대상으로 하는 시점을 식별하는 데 도움이 됩니다(예: 하나의 특정 요청 파라미터 세트MBs에 대한 정보의 검색 엔진 구성 요소 전송).
- ELB 스필오버 및 대기열 길이 - DDoS 공격으로 인해 인프라가 손상되고 공격자가 CloudFront 또는 AWS WAF 계층을 우회하고 보호되지 않은 리소스를 직접 공격하는지 확인하는 데 도움이 됩니다.
- ELB 요청 수 - 인프라 손상을 식별하는 데 도움이 됩니다. 이 지표는 공격자가 보호 계층을 우회하는지 또는 CloudFront 캐시 규칙을 검토하여 캐시 적중률을 높여야 하는지 여부를 보여줍니다.
- ELB 상태 호스트 - 다른 시스템 상태 확인 지표로 사용할 수 있습니다.

- ASG CPU 사용률 - 공격자가 우회하고 있는지 CloudFront AWS WAF, 그리고 Elastic Load Balancing을 식별하는 데 도움이 됩니다. 이 지표를 사용하여 공격의 피해를 식별할 수도 있습니다.

XSS 오탐 처리

이 솔루션은 일반적으로 탐색되는 수신 요청 요소를 검사하여 XSS 공격을 식별하고 차단하는 AWS WAF 규칙을 구성합니다. 예를 HTML들어 콘텐츠 관리 시스템의 풍부한 텍스트 편집기를 사용하여 합법적인 사용자가를 작성하고 제출할 수 있도록 워크로드가 허용하는 경우이 감지 패턴은 덜 효과적입니다. 이 시나리오에서는 풍부한 텍스트 입력을 허용하는 특정 URL 패턴에 대한 기본 규칙을 우회하는 예외 XSS 규칙을 생성하고 제외된를 보호하기 위한 대체 메커니즘을 구현하는 것이 좋습니다URLs.

또한 일부 이미지 또는 사용자 지정 데이터 형식은 HTML 콘텐츠의 잠재적 XSS 공격을 나타내는 패턴을 포함하므로 오탐을 일으킬 수 있습니다. 예를 들어 SVG 파일에 `<script>` 태그가 포함될 수 있습니다. 합법적인 사용자로부터 이러한 유형의 콘텐츠를 기대하는 경우 이러한 다른 데이터 형식을 포함하는 HTML 요청을 허용하도록 XSS 규칙을 좁히십시오.

다음 단계를 완료하여가 입력HTML으로 수락URLs하는 규칙을 제외하도록 XSS 규칙을 업데이트합니다. 자세한 지침은 Amazon WAF 개발자 안내서를 참조하세요.

1. AWS WAF 콘솔에 로그인합니다.
2. 문자열 일치 또는 정규식 조건을 생성합니다.
3. XSS 규칙에 대해 수락하려는 값을 검사URI하고 나열하도록 필터 설정을 구성합니다.
4. 이 솔루션의 XSS 규칙을 편집하고 생성한 새 조건을 추가합니다.

   예를 들어, 목록에서 모든 URLs를 제외하려면 요청 시에 대해 다음을 선택합니다.

   - 는
   - 문자열 일치 조건에서 하나 이상의 파일러와 일치
   - XSS 허용 목록

문제 해결

이 솔루션에 대한 도움이 필요한 경우 Support 에 문의하여이 솔루션에 대한 지원 사례를 엽니다.

연락처 Support

AWS 개발자 지원, AWS 비즈니스 지원 또는 AWS 엔터프라이즈 지원이 있는 경우 지원 센터를 사용하여이 솔루션에 대한 전문가 지원을 받을 수 있습니다. 이후 단원에서는 그 방법에 대해서 설명합니다.

사례 생성

1. 지원 센터를 엽니다.
2. 사례 생성을 선택합니다.

어떻게 도와드릴까요?

1. 기술을 선택합니다.
2. 서비스에서 WAF 또는를 선택합니다AWS WAF.
3. 범주에서 WAF에 대한 보안 자동화 또는 보안 자동화를 AWS WAF 선택합니다.
4. 심각도의 경우 사용 사례에 가장 적합한 옵션입니다.
5. 서비스, 범주 및 심각도를 입력하면 인터페이스가 일반적인 문제 해결 질문에 대한 링크를 채웁니다. 이러한 링크로 문제를 해결할 수 없는 경우 다음 단계: 추가 정보를 선택합니다.

추가 정보

1. 제목에 질문 또는 문제를 요약하는 텍스트를 입력합니다.
2. 설명에서 문제를 자세히 설명합니다.
3. 파일 연결을 선택합니다.
4. 요청을 처리하는 데 Support 필요한 정보를 연결합니다.

사례를 더 빠르게 해결할 수 있도록 지원

1. 요청된 정보를 입력합니다.

2. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.

지금 해결하거나 문의하기

1. 지금 해결 솔루션을 검토합니다.
2. 이러한 솔루션에서 문제를 해결할 수 없는 경우 문의를 선택하고 요청된 정보를 입력한 다음 제출을 선택합니다.

개발자 안내서

이 섹션에서는 솔루션의 소스 코드를 제공합니다.

소스 코드

GitHub 리포지토리를 방문하여이 솔루션의 템플릿과 스크립트를 다운로드하고 사용자 지정을 다른 사용자와 공유하세요.

레퍼런스

이 섹션에는이 솔루션에 대한 고유한 지표를 수집하기 위한 선택적 기능, 관련 리소스에 대한 포인터, 이 솔루션에 기여한 빌더 목록에 대한 정보가 포함되어 있습니다.

익명화된 데이터 수집

이 솔루션에는 로 운영 지표를 전송하는 옵션이 포함되어 있습니다 AWS. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. 이 기능을 켜면 솔루션은 다음 정보를 수집하여 템플릿을 처음 배포하는 AWS 동안에 전송합니다. CloudFormation

- 솔루션 ID - AWS 솔루션 식별자
- 고유 ID(UUID) -이 솔루션의 각 배포에 대해 무작위로 생성된 고유 식별자
- 타임스탬프 - 데이터 수집 타임스탬프
- 솔루션 구성 - 초기 시작 시 설정된 기능 및 파라미터
- 수명 주기 - 고객이이 솔루션을 사용한 기간(스택 삭제 기준)
- 로그 구문 분석기 데이터:
  - 스캐너 및 프로브 IP 세트의 IP 주소 수와 차단할 HTTP Flood IP 세트의 IP 주소 수
  - 처리 및 차단된 요청 수
- IP는 구문 분석기 데이터를 나열합니다.
  - Reputation Lists IP 세트의 IP 주소 수
  - 처리 및 차단된 요청 수
- 액세스 핸들러 데이터:
  - 잘못된 봇 IP 세트의 IP 주소 수
  - 처리 및 차단된 요청 수
- IP 보존 데이터 - 허용 또는 거부된 IP 세트에서 제거되는 만료된 IP 주소 수

AWS 는이 설문조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인 정보 보호 정책이 적용됩니다. 이 기능을 옵트아웃하려면 AWS CloudFormation 템플릿을 시작하기 전에 다음 단계를 완료합니다.

1. `aws-waf-security-automations.template` AWS CloudFormation를 로컬 하드 드라이브에 다운로드합니다.

2. 텍스트 편집기로 CloudFormation 템플릿을 엽니다.
3. CloudFormation 템플릿 매핑 섹션을 다음에서 수정합니다.

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

변경 후:

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

4. AWS CloudFormation 콘솔에 로그인합니다.
5. 스택 생성을 선택합니다.
6. 스택 생성 페이지, 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
7. 템플릿 파일 업로드에서 파일 선택을 선택하고 로컬 드라이브에서 편집한 템플릿을 선택합니다.
8. 다음을 선택하고 1단계의 단계를 따릅니다. 스택을 시작합니다.

관련 리소스

관련 AWS 백서

- AWS DDoS 복원력 모범 사례

연결된 AWS 보안 블로그 게시물

- AWS WAF, Amazon CloudFront및 참조자 확인을 사용하여 핫링크를 방지하는 방법

타사 IP 평판 목록

- 스팸하우스 DROP 목록 웹 사이트
- Proofpoint 새로운 위협 IP 목록
- Tor 종료 노드 목록

기여자

- 하이터 바이탈
- Lee Atkinson
- 벤 포터
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- 슈 잭슨
- William Quan

개정

날짜	변경 사항
2016년 9월	초기 릴리스
2017년 1월	이 솔루션의 IP 주소 제한에 대한 설명입니다.
2017년 3월 일	캐시 동작 생성에 대한 추가 지침, AWS 보안 블로그 게시물에 URLs 대해 업데이트됨.
2017년 6월	ALB 지원을 추가하고 제품 제한을 업데이트했습니다.
2017년 11월	HTTP 플러드 방지에 대한 속도 기반 규칙 지원 추가, 리소스 액세스 로그 저장에 대한 추가 링크.
2018년 1월	Application Load Balancer용의 리전별 가용성에 AWS WAF 대한 콘텐츠를 업데이트했습니다.
2018년 12월	IPv6 지원, 확장된 CIDR 범위 및 모니터링 대시보드가 추가되었습니다.
2019년 4월	AWS WAF 로그 통합, Amazon Athena 통합 및 구성 가능한 로그 파서를 추가했습니다.
2019년 12월	Node.js 업데이트 지원에 대한 정보가 추가되었습니다.
2020년 2월	버그는 RequestThreshold 파라미터를 수정하고 업데이트합니다.
2020년 6월	파티셔닝을 사용한 Athena 비용 최적화 추가, README 지침 업데이트, 잘못된 봇 X-Forward-For 헤더 내에서 잠재적 DoS 문제 수정.
2020년 7월	AWS WAF Classic에서 AWS WAF V2 서비스로 업그레이드되었습니다API.

날짜	변경 사항
2020년 11월	릴리스 버전 3.1.0: 특정 리전의 HTTP 홍수 방지 및 스캐너 및 프로브 보호 규칙에 대한 설명, S3 경로 유형을 가상 호스팅 스타일로 대체, 모든에 파티션 변수 추가ARNs, 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2021년 9월	릴리스 버전 3.2.0: 허용 및 거부 IP 세트에 대한 IP 보존 지원 추가, 버그 수정. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2022년 8월	릴리스 버전 3.2.1: 요청 구성 요소의 크기 WAF 초과 처리에 대한 지원을 추가하고 주입 SQL 규칙 문에 대한 WAF 민감도 수준에 대한 지원을 추가했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2022년 9월	솔루션 스택 외부에서 사용자 지정을 위한 설명서가 업데이트되었습니다 CloudFormation.
2022년 12월	릴리스 버전 3.2.2: Service Catalog AppRegistry 및 AWS Systems Manager Application Manager와의 통합이 추가되었습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2022년 12월	릴리스 버전 3.2.3: 애플리케이션 속성 그룹 이름에 접두사로 리전을 추가하여 로 시작하는 이름과 충돌하지 않도록 합니다 AWS. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 2월	릴리스 버전 3.2.4: pytest 및 완화 요청을 업그레이드했습니다CVE. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.

날짜	변경 사항
2023년 3월	IP 주소를 허용하거나 거부한 솔루션을 버전 3.0 또는 3.1에서 3.2 이상으로 업그레이드하기 위한 설명서가 업데이트되었습니다.
2023년 4월	릴리스 버전 3.2.5: 모든 새 Amazon S3 버킷에 대한 Amazon S3 객체 소유권의 새 기본 설정(ACLs 비활성화됨)으로 인한 영향을 완화했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 5월	릴리스 버전 4.0.0: 새 AWS Managed Rules 규칙 그룹에 대한 지원을 추가하고 사용자 지정 규칙을 업데이트했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 5월	릴리스 버전 4.0.1: 누락된 `.gitignore` 파일의 문제를 해결하기 위해 파일을 업데이트했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 9월	릴리스 버전 4.0.2: 품질을 개선하기 위해 코드를 리팩터링했습니다. 패치된 요청 패키지 취약성. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 10월	릴리스 버전 4.0.3: 보안 취약성을 해결하기 위해 패키지 버전을 업데이트했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2023년 11월	설명서 업데이트: AWS 개발자 지원을 추가하고 지원 AWS 문의를 문제 해결 섹션에 병합했습니다.

날짜	변경 사항
2023년 11월	설명서 업데이트: AWS 서비스 카탈로그를 사용하여 솔루션 모니터링 섹션에 솔루션과 연결된 비용 태그 확인이 추가되었습니다. AppRegistry
2024년 4월	설명서 업데이트: 배포 3단계에서 S3 버킷 추가 지침을 명확히 했습니다.
2024년 9월	릴리스 버전 4.0.4: 보안 취약성을 해결하기 위해 패키지 버전을 업데이트했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2024년 10월	릴리스 버전 4.0.5: 종속성 관리에 Poetry를 사용했습니다. 기본 Python 로거를 aws_lambda_powertools 로거로 대체했습니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.
2024년 12월	릴리스 버전 4.0.6: lambda를 python 3.12로 업데이트합니다. 자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.

고지 사항

이 구현 가이드는 정보 제공 목적으로만 제공됩니다. 이 문서는이 문서의 발행일 현재 AWS 현재 제품 제공 및 관행을 나타내며, 예고 없이 변경될 수 있습니다. 고객은 본 문서의 정보와 AWS 제품 또는 서비스의 사용에 대해 독자적으로 평가할 책임이 있습니다. 각 정보는 명시적이든 묵시적이든 어떤 종류의 보증도 없이 '있는 그대로' 제공됩니다. 이 문서는 , 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증AWS, 표현, 계약 약정, 조건 또는 보장도 생성하지 않습니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

AWS WAF 솔루션용 보안 자동화는 Apache 라이선스 버전 2.0의 약관에 따라 라이선스가 부여됩니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.