

Guía de implementación

Automatizaciones de seguridad para AWS WAF



Automatizaciones de seguridad para AWS WAF: Guía de implementación

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Información general de la solución	1
Características y ventajas	3
Proteja sus aplicaciones web con los grupos de reglas de AWS Managed Rules	3
Proporcione protección contra inundaciones de nivel 7 con una regla personalizada de inundación HTTP predefinida	3
Bloquee el aprovechamiento de las vulnerabilidades con una regla personalizada predefinida de Scanners & Probes	4
Detecte y desvíe las intrusiones con una regla personalizada predefinida de Bad Bot	4
Bloquee las direcciones IP malintencionadas con listas de reputación de IP predefinidas (regla personalizada)	4
Proporcione una configuración manual de IP con una regla personalizada de listas de IP permitidas y denegadas predefinidas	5
Cree su propio panel de monitoreo	5
Intégrelo con Service Catalog AppRegistry y AWS Systems Manager Application Manager	5
Casos de uso	5
Conceptos y definiciones	6
Información general de la arquitectura	9
Diagrama de arquitectura	9
Consideraciones sobre el diseño de AWS Well-Architected	12
Excelencia operativa	12
Seguridad	13
Fiabilidad	13
Eficiencia del rendimiento	14
Optimización de costos	14
Sostenibilidad	14
Detalles de la arquitectura	15
Los servicios de AWS en esta solución	15
Opciones del analizador de registros	16
Regla basada en la tasa de AWS WAF	16
Analizador de registros Amazon Athena	17
Analizador de registros AWS Lambda	17
Detalles de los componentes	17
Analizador de registros: aplicación	18

Analizador de registros - AWS WAF	19
Analizador de listas de direcciones IP	21
Controlador de acceso	21
Planificación de la implementación	23
Regiones de AWS admitidas	23
Costo	24
Estimación del costo de los troncos CloudWatch	27
Estimación de costes de Athena	28
Seguridad	28
Roles de IAM	29
Datos	29
Capacidades de protección	29
Cuotas	30
Cuotas para los servicios de AWS en esta solución	30
Cuotas de AWS WAF	31
Consideraciones sobre la implementación	31
Reglas de AWS WAF	31
Registro de tráfico de ACL web	31
Gestión sobredimensionada de los componentes de las solicitudes	32
Implementaciones de múltiples soluciones	32
Implementación de la solución	33
Información general del proceso de implementación	33
CloudFormation Plantillas de AWS	34
Pila principal	34
Pila WebACL	34
Pila Firehose Athena	34
Requisitos previos	35
Configure una CloudFront distribución	35
Configure un ALB	35
Paso 1. Lanzar la pila	35
Paso 2. Asocie la ACL web a su aplicación web	74
Paso 3. Configurar registros de acceso web	75
Almacene los registros de acceso a la web de una distribución CloudFront	75
Almacene los registros de acceso a la web desde un Application Load Balancer	75
Supervise la solución	77
Active Application Insights CloudWatch	77

Confirmación de las etiquetas de costos asociadas a la solución	79
Activar las etiquetas de asignación de costos asociadas a la solución	80
AWS Cost Explorer	81
Actualización de la solución	82
Consideraciones sobre la actualización	83
Actualización del tipo de recurso	83
WAFV2 actualizar	83
Personalizaciones durante la actualización de la pila	83
Desinstalar la solución	84
Usa la solución	85
Modifique los conjuntos de IP permitidos y denegados (opcional)	85
Inserte el enlace de Honeypot en su aplicación web (opcional)	85
Cree un CloudFront origen para el punto final de Honeypot	85
Inserte el punto final de Honeypot como un enlace externo	87
Utilice el archivo JSON del analizador de registros Lambda	88
Utilice el archivo JSON del analizador de registros Lambda para la protección contra inundaciones HTTP	88
Utilice el archivo JSON del analizador de registros Lambda para proteger el escáner y la sonda	90
Utilice el país y el URI en el analizador de registros de HTTP Flood Athena	91
Ver las consultas de Amazon Athena	92
Vea las consultas de registro de WAF	93
Vea las consultas del registro de acceso a las aplicaciones	93
Ver cómo añadir consultas de particiones de Athena	94
Configurar la retención de IP en los conjuntos de IP de AWS WAF permitidos y denegados	94
Funcionamiento	95
Active la retención de IP	96
Cree un panel de monitoreo	97
Gestiona los falsos positivos de XSS	98
Solución de problemas	100
Contacto con Support	100
Cree un caso	100
¿Cómo podemos ayudar?	100
Información adicional	100
Ayúdenos a resolver su caso más rápido	101
Resuelva ahora o póngase en contacto con nosotros	101

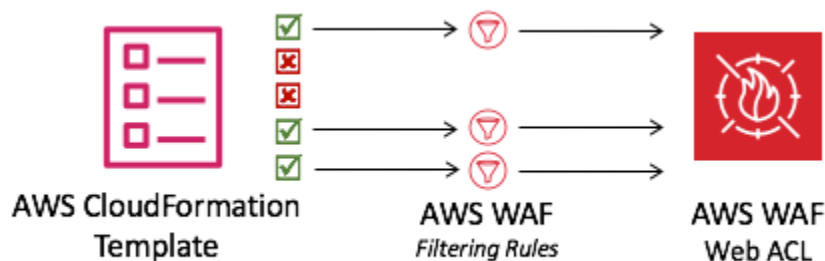
Guía para desarrolladores	102
Código fuente	102
Referencia	103
Recopilación de datos anonimizados	103
Recursos relacionados	104
Documentos técnicos de AWS asociados	104
Publicaciones del blog de seguridad de AWS asociadas	104
Listas de reputación de IP de terceros	105
Colaboradores	105
Revisiones	106
Avisos	107
.....	cviii

Implemente automáticamente una única lista de control de acceso web que filtre los ataques basados en la web con automatizaciones de seguridad en AWS WAF

La solución Security Automations for AWS WAF implementa un conjunto de reglas preconfiguradas para ayudarlo a proteger sus aplicaciones de los ataques web más comunes. El servicio principal de esta solución, [AWS WAF](#), ayuda a proteger las aplicaciones web de las técnicas de ataque que pueden afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos. Puede usar AWS WAF para definir reglas de seguridad web personalizables. Estas reglas controlan qué tráfico se debe permitir o bloquear en las aplicaciones web y las interfaces de programación de aplicaciones (APIs) implementadas en los recursos de AWS, como [Amazon CloudFront](#), [Application Load Balancer](#) (ALB) y [Amazon API Gateway](#). Para ver más tipos de recursos compatibles, consulte [AWS WAF](#) en la Guía avanzada para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield.

Configurar las reglas de AWS WAF puede resultar difícil y engorroso tanto para las organizaciones grandes como para las pequeñas, especialmente para aquellas que no cuentan con equipos de seguridad especializados. Para simplificar este proceso, la solución Security Automations for AWS WAF implementa automáticamente una única lista de control de acceso (ACL) a la web con un conjunto de reglas de AWS WAF diseñadas para filtrar los ataques web más comunes. Durante la configuración inicial de la CloudFormation plantilla de [AWS](#) de esta solución, puede especificar qué funciones de protección desea incluir. Tras implementar esta solución, AWS WAF inspecciona las solicitudes web a sus CloudFront distribuciones o ALB existentes y las bloquea cuando corresponde.

Una CloudFormation plantilla implementa una ACL web con reglas de filtrado de AWS WAF.



Esta guía de implementación analiza las consideraciones arquitectónicas, los pasos de configuración y las mejores prácticas operativas para implementar esta solución en la nube de Amazon Web Services (AWS). Incluye enlaces a CloudFormation plantillas que lanzan, configuran y ejecutan los

servicios de seguridad, computación, almacenamiento y otros servicios de AWS necesarios para implementar esta solución en AWS, utilizando las prácticas recomendadas de AWS en materia de seguridad y disponibilidad.

La información de esta guía presupone un conocimiento práctico de los servicios de AWS CloudFront ALBs, como AWS WAF y AWS [Lambda](#). También requiere conocimientos básicos sobre los ataques y las estrategias de mitigación más comunes basados en la web.

 Note

A partir de la versión 3.0.0, esta solución es compatible con la versión más reciente de la API del servicio WAF (AWS) de [AWS WAFV2](#).

Esta guía está destinada a administradores de TI, ingenieros de seguridad, DevOps ingenieros, desarrolladores, arquitectos de soluciones y administradores de sitios web.

 Note

Recomendamos utilizar esta solución como punto de partida para implementar las reglas de AWS WAF. Puede personalizar el [código fuente](#), añadir nuevas reglas personalizadas y aprovechar más [reglas administradas por AWS WAF](#) en función de sus necesidades.

Utilice esta tabla de navegación para encontrar rápidamente las respuestas a estas preguntas:

Si quiere...	Lea...
Conocer el costo de ejecutar esta solución. El costo total de ejecutar esta solución depende de la protección activada y de la cantidad de datos ingeridos, almacenados y procesados.	Costo
Comprender las consideraciones de seguridad de esta solución.	Seguridad
Conozca qué regiones de AWS son compatibles con esta solución.	Regiones de AWS admitidas

Si quiere...	Lea...
Consulte o descargue la CloudFormation plantilla incluida en esta solución para implementar automáticamente los recursos de infraestructura (la «pila») de esta solución.	CloudFormation Plantilla de AWS
Use Support para ayudarlo a implementar, usar o solucionar problemas de la solución.	Soporte
Acceda al código fuente y, si lo desea, utilice el AWS Cloud Development Kit (AWS CDK) para implementar la solución	GitHub repositorio

Características y ventajas

La solución Security Automations for AWS WAF ofrece las siguientes características y ventajas.

Proteja sus aplicaciones web con los grupos de reglas de AWS Managed Rules

[Las reglas administradas por AWS para AWS WAF](#) proporcionan protección contra las vulnerabilidades comunes de las aplicaciones u otro tráfico no deseado. Esta solución incluye grupos de reglas de [reputación de IP gestionada por AWS](#), [grupos de reglas de referencia gestionados por AWS](#) y [grupos de reglas de casos de uso específicos gestionados por AWS](#). Tiene la opción de seleccionar uno o más grupos de reglas para su ACL web, hasta alcanzar la cuota máxima de unidades de capacidad (WCU) de la ACL web.

Proporcione protección contra inundaciones de nivel 7 con una regla personalizada de inundación HTTP predefinida

La regla personalizada HTTP Flood protege contra un ataque distribuido Denial-of-Service (DDoS) de capa web durante un período de tiempo definido por el cliente. Puede elegir una de estas opciones para activar esta regla:

- Regla basada en la tasa de AWS WAF
- Analizador de registros Lambda

- Analizador de [registros Amazon Athena](#)

Las opciones del analizador de registros Lambda o del analizador de registros Athena permiten definir una cuota de solicitudes inferior a 100. Este enfoque puede ayudarle a no alcanzar la cuota exigida por las normas basadas en las [tarifas](#) de AWS WAF. Para obtener más información, consulte Opciones del [analizador de registros](#).

También puede mejorar el analizador de registros de Athena añadiendo un país y un identificador uniforme de recursos (URI) a las condiciones de filtrado. Este enfoque identifica y bloquea los ataques de inundación HTTP que tienen patrones de URI impredecibles. Para obtener más información, consulte [Usar el país y el URI en el analizador de registros HTTP Flood Athena](#).

Bloquee el aprovechamiento de las vulnerabilidades con una regla personalizada predefinida de Scanners & Probes

La regla personalizada Scanners & Probes analiza los registros de acceso a las aplicaciones en busca de comportamientos sospechosos, como una cantidad anormal de errores generados por un origen. A continuación, bloquea esas direcciones IP de origen sospechosas durante un período de tiempo definido por el cliente. Puede elegir una de estas opciones para activar esta regla: analizador de registros Lambda o analizador de registros Athena. [Para obtener más información, consulte Opciones del analizador de registros](#).

Detecte y desvíe las intrusiones con una regla personalizada predefinida de Bad Bot

La regla personalizada Bad Bot establece un punto final, que es un mecanismo de seguridad destinado a atraer y desviar un intento de ataque. Puedes insertar el punto final en tu sitio web para detectar las solicitudes entrantes procedentes de rastreadores de contenido y bots maliciosos. Una vez detectadas, se bloquearán todas las solicitudes posteriores procedentes de los mismos orígenes. Para obtener más información, consulte [Insertar el enlace de Honeypot en su aplicación web](#).

Bloquee las direcciones IP malintencionadas con listas de reputación de IP predefinidas (regla personalizada)

La regla personalizada de las listas de reputación de IP comprueba cada hora las listas de reputación de IP de terceros para detectar nuevos rangos de IP que bloquear. Estas listas incluyen las listas

Don't Route Or Peer (DROP) y Extended DROP (EDROP) de [Spamhaus](#), la lista de [direcciones IP de Proofpoint Emerging Threats y la lista](#) de nodos de salida de [Tor](#).

Proporcione una configuración manual de IP con una regla personalizada de listas de IP permitidas y denegadas predefinidas

Las reglas personalizadas de las listas de IP permitidas y denegadas le permiten insertar manualmente las direcciones IP que desee permitir o denegar. También puede configurar la [retención de IP en las listas de IP permitidas y denegadas](#) para que caduquen IPs a una hora determinada.

Cree su propio panel de monitoreo

Esta solución emite CloudWatch métricas de [Amazon](#), como solicitudes permitidas, solicitudes bloqueadas y otras métricas relevantes. Puede crear un panel personalizado para visualizar estas métricas y obtener información sobre el patrón de ataques y la protección que proporciona AWS WAF. Para obtener más información, consulte el [panel de monitoreo de Build](#).

Intégrelo con Service Catalog AppRegistry y AWS Systems Manager Application Manager

Esta solución incluye un AppRegistry recurso del [catálogo de servicios](#) para registrar la CloudFormation plantilla de la solución y sus recursos subyacentes como una aplicación tanto en AWS Service Catalog AppRegistry como en [AWS Systems Manager Application Manager](#). Con esta integración, puede administrar de forma centralizada los recursos de la solución.

Casos de uso

A continuación, se muestran ejemplos de casos de uso para usar esta solución. Puede personalizar esta solución de formas innovadoras que no se limitan a esta lista.

Automatice la configuración de las reglas de AWS WAF

AWS WAF protege su aplicación web de los ataques habituales; sin embargo, configurar las reglas de AWS WAF puede resultar complicado y llevar mucho tiempo. Para ayudarle, esta solución implementa automáticamente un conjunto de reglas de AWS WAF en su cuenta con CloudFormation una plantilla. De este modo, no tendrá que configurar las reglas de AWS WAF usted mismo y podrá empezar a utilizar AWS WAF más rápido.

Personalice la capa 7 de protección contra inundaciones HTTP

Esta solución ofrece tres opciones para activar la protección contra inundaciones HTTP. Puede seleccionar la opción que se adapte a sus necesidades para protegerse contra los ataques DDoS. Para obtener más información, consulte [Proporcionar protección contra inundaciones de nivel 7 con una regla personalizada de inundación HTTP predefinida en Características y ventajas](#).

Aproveche el código fuente para aplicar la personalización o crear sus propias automatizaciones de seguridad

Esta solución proporciona un ejemplo de cómo usar AWS WAF y otros servicios para crear automatizaciones de seguridad en la nube de AWS. Su [código fuente abierto](#) le GitHub permite aplicar personalizaciones o crear sus propias automatizaciones de seguridad que se adapten a sus necesidades.

Conceptos y definiciones

En esta sección se describen los conceptos clave y se define la terminología específica de esta solución.

Registros de ALB

Esta solución usa registros para el recurso ALB. La regla de protección de escáneres y sondas de esta solución inspecciona estos registros.

Analizador de registros Athena

Amazon Athena es un servicio de análisis interactivo sin servidor que se basa en marcos de código abierto y admite formatos de archivos y tablas abiertas. Esta solución ejecuta una consulta programada de Athena para inspeccionar los registros de AWS WAF CloudFront o ALB si el usuario así lo `yes - Amazon Athena log parser` decide al activar la regla de protección contra inundaciones HTTP o la regla de protección contra escáneres y sondas.

Regla WAF de AWS

Una regla de AWS WAF define:

- Cómo inspeccionar las solicitudes web HTTP (S)
- La acción que se debe realizar ante una solicitud cuando coincide con los criterios de inspección

Defina las reglas únicamente en el contexto de una ACL web o un grupo de reglas.

CloudFront logs

Esta solución usa registros para el CloudFront recurso. La regla de protección de escáneres y sondas de esta solución inspecciona estos registros.

Conjunto de IP

Un conjunto de direcciones IP proporciona un conjunto de direcciones IP e intervalos de direcciones IP que desea utilizar

juntos en una declaración de reglas. Los conjuntos de IP son recursos de AWS.

Analizador de registros Lambda

[Esta solución ejecuta una función Lambda invocada por un evento de creación de objetos de Amazon Simple Storage Service \(Amazon S3\).](#) La función Lambda inicia una inspección de los registros WAF CloudFront o ALB de AWS si el usuario así lo quiere - `AWS Lambda log parser` decide al activar la regla HTTP Flood Protection o la regla Scanner & Probe Protection.

Grupos de reglas gestionados

Los grupos de reglas gestionados son conjuntos de ready-to-use reglas predefinidas que los vendedores de AWS y AWS Marketplace redactan y mantienen para usted. [Los precios de AWS WAF](#) se aplican al uso de cualquier grupo de reglas administrado.

tipo de recurso/punto final

Puede asociar los recursos de AWS ACLs a la web para protegerlos. Estos recursos son CloudFront API Gateway, ALB, [AWS AppSync](#), [Amazon](#) Cognito, [AWS App](#) Runner y [AWS Verified Access](#). Actualmente, Amazon admite esta solución CloudFront y ALB.

Registros WAF

Esta solución utiliza los registros generados por AWS WAF para los recursos asociados a la ACL web. La regla de protección contra inundaciones HTTP de esta solución inspecciona estos registros.

WCU

AWS WAF utiliza unidades de capacidad de la lista de control de acceso (ACLWCUs) a la web () para calcular y controlar los recursos operativos necesarios para ejecutar las reglas, los grupos de

reglas y la web. ACLs AWS WAF aplica las cuotas de la WCU al configurar los grupos de reglas y la web. ACLs WCUs no afectan a la forma en que AWS WAF inspecciona el tráfico web.

ACL web

Una ACL web le brinda un control detallado sobre las solicitudes web HTTP (S) a las que responde su recurso protegido.

Note

Para obtener una referencia general de los términos de AWS, consulte el [glosario de AWS](#).

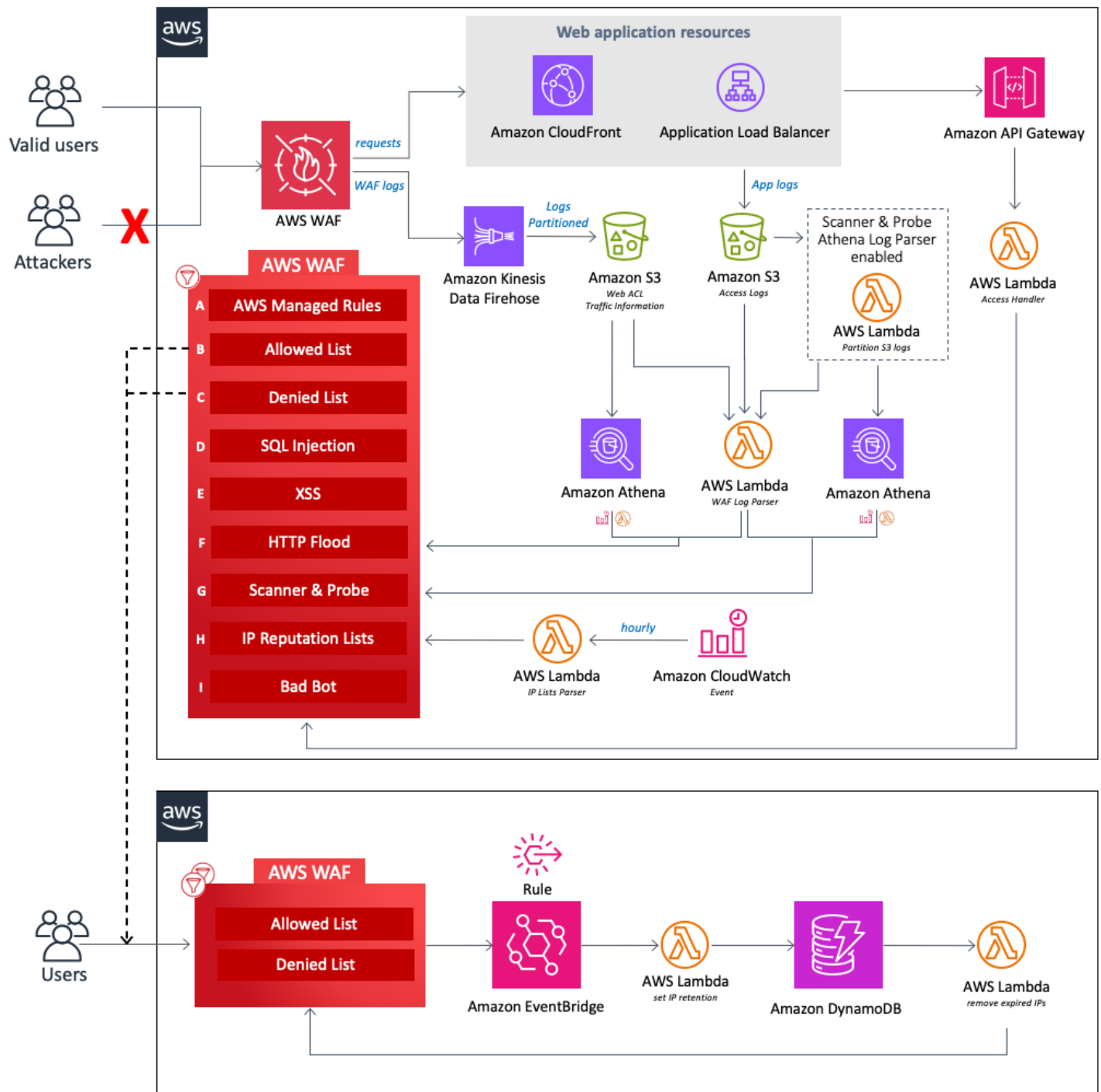
Información general de la arquitectura

En esta sección se proporciona un diagrama de arquitectura de implementación de referencia para los componentes implementados con esta solución.

Diagrama de arquitectura

Al implementar esta solución con los parámetros predeterminados, se implementan los siguientes componentes en su cuenta de AWS.

CloudFormation la plantilla implementa AWS WAF y otros recursos de AWS para proteger su aplicación web de los ataques más comunes.



En el centro del diseño se encuentra una ACL web de [AWS WAF](#), que actúa como punto central de inspección y decisión para todas las solicitudes entrantes a una aplicación web. Durante la configuración inicial de la CloudFormation pila, el usuario define qué componentes de protección debe activar. Cada componente funciona de forma independiente y agrega reglas diferentes a la ACL web.

Los componentes de esta solución se pueden agrupar en las siguientes áreas de protección.

 Note

Las etiquetas de los grupos no reflejan el nivel de prioridad de las reglas de la WAF.

- Reglas administradas por AWS (A): este componente contiene grupos de reglas de [reputación IP](#), [grupos de reglas](#) de [referencia y grupos](#) de [reglas específicos de casos de uso](#) de AWS. Estos grupos de reglas protegen contra la explotación de vulnerabilidades comunes de las aplicaciones u otro tipo de tráfico no deseado, incluidos los que se describen en las publicaciones de [OWASP](#), sin tener que escribir sus propias reglas.
- Listas de IP manuales (B y C): estos componentes crean dos reglas de AWS WAF. Con estas reglas, puede insertar manualmente las direcciones IP que desee permitir o denegar. Puede configurar la retención de IP y eliminar las direcciones IP caducadas de los conjuntos de IP permitidos o denegados mediante EventBridge [las reglas](#) de [Amazon](#) y [Amazon DynamoDB](#). Para obtener más información, consulte [Configurar la retención de IP en conjuntos de IP de AWS WAF permitidos y denegados](#).
- Inyección SQL (D) y XSS (E): estos componentes configuran dos reglas de AWS WAF diseñadas para proteger contra los patrones comunes de inyección de SQL o secuencias de comandos entre sitios (XSS) en el URI, la cadena de consulta o el cuerpo de una solicitud.
- Inundación HTTP (F): este componente protege contra los ataques que consisten en un gran número de solicitudes desde una dirección IP determinada, como un ataque DDoS a la capa web o un intento de inicio de sesión por fuerza bruta. Con esta regla, establece una cuota que define el número máximo de solicitudes entrantes permitidas desde una sola dirección IP dentro de un período predeterminado de cinco minutos (configurable con el parámetro Athena Query Run Time Schedule). Una vez superado este umbral, las solicitudes adicionales de la dirección IP se bloquean temporalmente. Puede implementar esta regla mediante una regla basada en la tasa de AWS WAF o procesando los registros de AWS WAF mediante una función de Lambda o una consulta de Athena. [Para obtener más información sobre las ventajas y desventajas relacionadas con las opciones de mitigación de inundaciones HTTP, consulte las opciones del analizador de registros](#).
- Scanner and Probe (G): este componente analiza los registros de acceso a las aplicaciones en busca de comportamientos sospechosos, como una cantidad anormal de errores generados por un origen. A continuación, bloquea las direcciones IP de origen sospechosas durante un período de tiempo definido por el cliente. [Puede implementar esta regla mediante una función de Lambda o](#)

[una consulta de Athena. Para obtener más información sobre las desventajas relacionadas con las opciones de mitigación del escáner y la sonda, consulte las opciones del analizador de registros.](#)

- Listas de reputación de IP (H): este componente es la función `IP Lists Parser Lambda` que comprueba las listas de reputación de IP de terceros cada hora en busca de nuevos rangos que bloquear. Estas listas incluyen las listas Don't Route Or Peer (DROP) y Extended DROP (EDROP) de Spamhaus, la lista de direcciones IP de amenazas emergentes de Proofpoint y la lista de nodos de salida de Tor.
- Bad Bot (I): este componente configura automáticamente un honeypot, que es un mecanismo de seguridad destinado a atraer y desviar un intento de ataque. El punto de partida de esta solución es un punto de enlace trampa que puedes insertar en tu sitio web para detectar las solicitudes entrantes procedentes de buscadores de contenido y de bots maliciosos. Si una fuente accede al honeypot, la función `Access Handler Lambda` intercepta e inspecciona la solicitud para extraer su dirección IP y, a continuación, la añade a una lista de bloqueados de AWS WAF.

Cada una de las tres funciones Lambda personalizadas de esta solución publica métricas de tiempo de ejecución en CloudWatch. Para obtener más información sobre estas funciones de Lambda, consulte los detalles de los [componentes](#).

Consideraciones sobre el diseño de AWS Well-Architected

Esta solución utiliza las prácticas recomendadas del [AWS Well-Architected Framework](#), que ayuda a los clientes a diseñar y operar cargas de trabajo confiables, seguras, eficientes y rentables en la nube.

En esta sección se describe cómo los principios de diseño y las prácticas recomendadas de Well-Architected Framework benefician a esta solución.

Excelencia operativa

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del [pilar de excelencia operativa](#).

- La solución utiliza métricas CloudWatch para proporcionar observabilidad en la infraestructura, las funciones de Lambda, Amazon [Data Firehose](#), [API Gateway](#), los buckets de Amazon S3 y el resto de los componentes de la solución.

- Desarrollamos, probamos y publicamos la solución mediante una canalización de integración y entrega continuas (CI/CD) de AWS. Esto ayuda a los desarrolladores a conseguir resultados de alta calidad de forma constante.
- Puede instalar la solución con una CloudFormation plantilla que aprovisiona todos los recursos necesarios en su cuenta. Para actualizar o eliminar la solución, solo tiene que actualizar o eliminar la plantilla.

Seguridad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del [pilar de seguridad](#).

- Todas las comunicaciones entre servicios utilizan las funciones de [AWS Identity and Access Management](#) (IAM).
- Todas las funciones que utiliza la solución se basan en el acceso con [privilegios](#) mínimos. En otras palabras, solo contienen los permisos mínimos necesarios para que el servicio pueda funcionar correctamente.
- Todo el almacenamiento de datos, incluidos los buckets de Amazon S3 y DynamoDB, tiene cifrado en reposo.

Fiabilidad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del [pilar de fiabilidad](#).

- La solución utiliza los servicios sin servidor de AWS siempre que es posible (por ejemplo, Lambda, Firehose, API Gateway, Amazon S3 y Athena) para garantizar una alta disponibilidad y recuperación en caso de fallo del servicio.
- Realizamos pruebas automatizadas de la solución para detectar y corregir los errores rápidamente.
- La solución utiliza funciones Lambda para el procesamiento de datos. La solución almacena los datos en Amazon S3 y DynamoDB y, de forma predeterminada, permanece en varias zonas de disponibilidad.

Eficiencia del rendimiento

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del [pilar de eficiencia del rendimiento](#).

- La solución utiliza una arquitectura sin servidor para garantizar una alta escalabilidad y disponibilidad a un coste reducido.
- La solución mejora el rendimiento de la base de datos al particionar los datos y optimizar las consultas para reducir la cantidad de datos escaneados y lograr resultados más rápidos.
- La solución se prueba e implementa automáticamente todos los días. Nuestros arquitectos de soluciones y expertos en la materia revisan la solución en busca de áreas en las que experimentar y mejorar.

Optimización de costos

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del [pilar de optimización de costos](#).

- La solución utiliza una arquitectura sin servidores y los clientes solo pagan por lo que utilizan.
- La capa de cómputo de la solución está predeterminada en Lambda, que usa pay-per-use un modelo.
- La base de datos y las consultas de Athena están optimizadas para reducir la cantidad de datos escaneados y, por lo tanto, reducir los costos.

Sostenibilidad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las mejores prácticas del [pilar de sostenibilidad](#).

- La solución utiliza servicios gestionados y sin servidor para minimizar el impacto medioambiental de los servicios de backend.
- El diseño sin servidores de la solución tiene como objetivo reducir la huella de carbono en comparación con la huella de los servidores locales que funcionan de forma continua.

Detalles de la arquitectura

En esta sección se describen los componentes y los servicios de AWS que componen esta solución y los detalles de la arquitectura sobre cómo funcionan juntos estos componentes.

Los servicios de AWS en esta solución

Servicio de AWS	Descripción
AWS WAF	Principal. Implementa una ACL web de AWS WAF, grupos de reglas de AWS Managed Rules, reglas personalizadas y conjuntos de IP. Realiza llamadas a la API de AWS WAF para bloquear ataques comunes y proteger las aplicaciones web.
Amazon Data Firehose	Principal. Entrega los registros de AWS WAF a los buckets de Amazon S3.
Amazon S3	Principal. Almacena registros de AWS CloudFront, WAF y ALB.
AWS Lambda	Principal. Implementa varias funciones de Lambda para admitir reglas personalizadas.
Amazon EventBridge	Principal. Crea reglas de eventos para invocar Lambda.
Amazon Athena	Admite. Crea consultas y grupos de trabajo de Athena para admitir el analizador de registros de Athena.
AWS Glue	Admite. Crea bases de datos y tablas para soportar el analizador de registros Athena.
Amazon API Gateway	Admite. Crea un punto final de Honeypot defectuoso para bots.

Servicio de AWS	Descripción
Amazon SNS	Admite. Envía notificaciones por correo electrónico del Amazon Simple Notification Service (Amazon SNS) para permitir la retención de IP en las listas permitidas y denegadas.
AWS Systems Manager	Admite. Proporciona monitoreo de recursos a nivel de aplicación y visualización de las operaciones de los recursos y los datos de costos.

Opciones del analizador de registros

Como se describe en la [descripción general de la arquitectura](#), existen tres opciones para gestionar las protecciones de HTTP contra inundaciones y escáneres y sondas. En las siguientes secciones se explica cada una de estas opciones con más detalle.

Regla basada en la tasa de AWS WAF

Las reglas basadas en tarifas están disponibles para la protección contra inundaciones de HTTP. De forma predeterminada, una regla basada en tasas agrega y limita las tasas de las solicitudes en función de la dirección IP de la solicitud. Esta solución le permite especificar el número de solicitudes web que admite la IP de un cliente en un período final de cinco minutos, que se actualiza continuamente. Si una dirección IP supera la cuota configurada, AWS WAF bloquea las nuevas solicitudes bloqueadas hasta que la tasa de solicitudes sea inferior a la cuota configurada.

Recomendamos seleccionar la opción de regla basada en la tasa si la cuota de solicitudes es superior a 2000 solicitudes cada cinco minutos y no necesita implementar personalizaciones. Por ejemplo, no se tiene en cuenta el acceso estático a los recursos al contar las solicitudes.

Puede configurar aún más la regla para que utilice otras claves de agregación y combinaciones de teclas. Para obtener más información, consulte [Opciones y claves de agregación](#).

Analizador de registros Amazon Athena

Tanto los parámetros de la plantilla HTTP Flood Protection como Scanner & Probe Protection proporcionan la opción de analizador de registros Athena. Cuando se activa, CloudFormation aprovisiona una consulta de Athena y una función de Lambda programada responsable de organizar Athena para que ejecute, procese los resultados y actualice AWS WAF. Esta función Lambda se invoca mediante un CloudWatch evento configurado para ejecutarse cada cinco minutos. Esto se puede configurar con el parámetro Athena Query Run Time Schedule.

Recomendamos seleccionar esta opción si no puede utilizar las reglas basadas en tasas de AWS WAF y está familiarizado con SQL para implementar personalizaciones. Para obtener más información sobre cómo cambiar la consulta predeterminada, consulte [Ver consultas de Amazon Athena](#).

La protección contra inundaciones HTTP se basa en el procesamiento de registros de acceso de AWS WAF y utiliza archivos de registro de WAF. El tipo de registro de acceso WAF tiene un tiempo de demora más bajo, que puede utilizar para identificar los orígenes de las inundaciones HTTP con mayor rapidez en comparación con el tiempo de entrega de los CloudFront registros ALB. Sin embargo, debe seleccionar el tipo de registro CloudFront o ALB en el parámetro de plantilla Activar Scanner & Probe Protection para recibir los códigos de estado de respuesta.

Analizador de registros AWS Lambda

Los parámetros de la plantilla HTTP Flood Protection y Scanner & Probe Protection proporcionan la opción AWS Lambda Log Parser. Utilice el analizador de registros Lambda solo cuando las opciones de la regla basada en la velocidad de AWS WAF y del analizador de registros de Amazon Athena no estén disponibles. Una limitación conocida de esta opción es que la información se procesa en el contexto del archivo que se está procesando. Por ejemplo, una IP puede generar más solicitudes o errores que la cuota definida, pero dado que esta información se divide en diferentes archivos, cada archivo no almacena datos suficientes para superar la cuota.

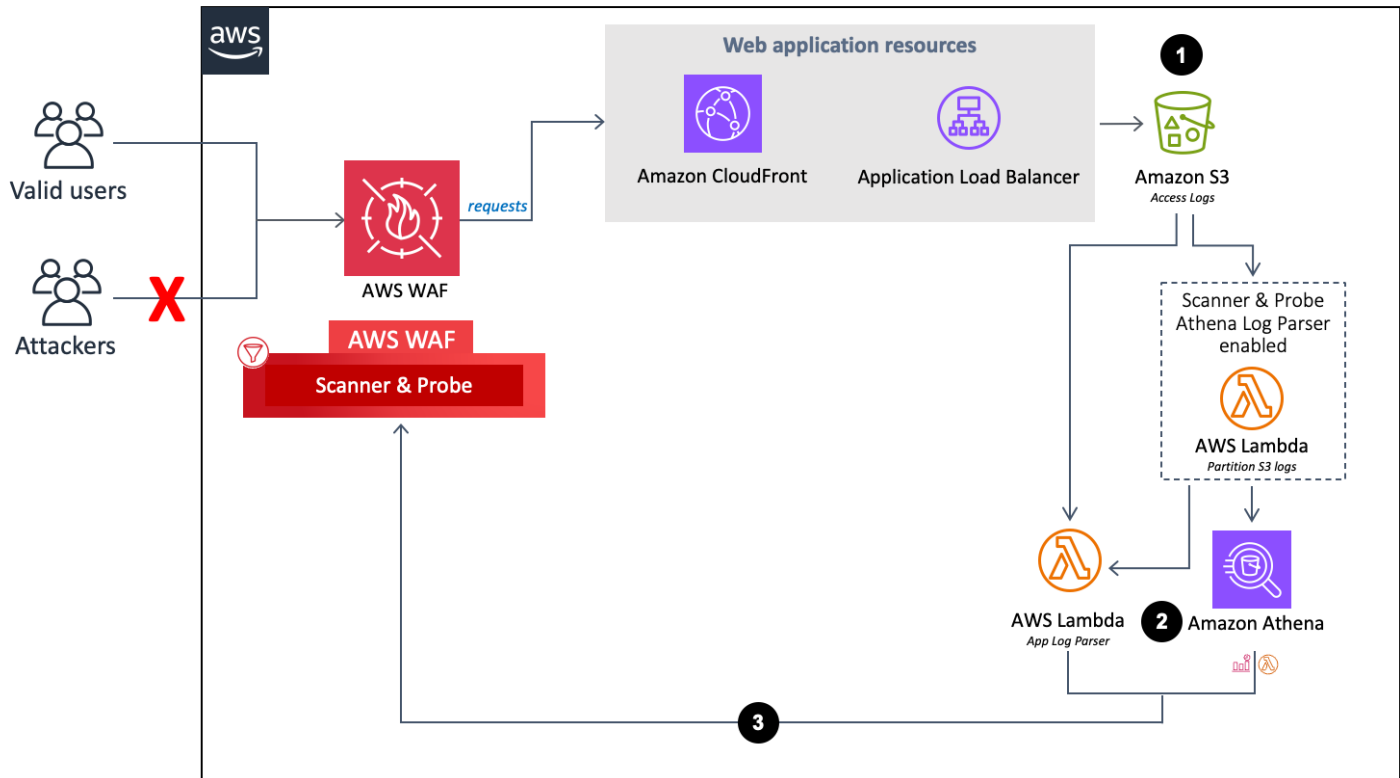
Detalles de los componentes

Como se describe en el [diagrama de arquitectura](#), cuatro de los componentes de esta solución utilizan automatizaciones para inspeccionar las direcciones IP y añadirlas a la lista de bloqueados de AWS WAF. En las siguientes secciones se explica cada uno de estos componentes con más detalle.

Analizador de registros: aplicación

El analizador de registros de aplicaciones ayuda a proteger contra escáneres y sondas.

Flujo del analizador de registros de aplicaciones.



1. Cuando CloudFront o un ALB recibe solicitudes en nombre de su aplicación web, envía los registros de acceso a un bucket de Amazon S3.
 - a. (Opcional) Si selecciona Yes - Amazon Athena log parser para los parámetros de plantilla Activar HTTP Flood Protection y Activar Scanner & Probe Protection, una función de Lambda mueve los registros de acceso de su carpeta original `<customer-bucket> / AWSLogs` a una carpeta `<customer-bucket> / AWSLogs-partitioned/ <optional-prefix> / year= <YYYY> / month= <MM> / day= <DD> / hour= <HH>` recién particionada o cuando llegan a Amazon S3.
 - b. (Opcional) Si selecciona yes el parámetro de plantilla de ubicación Guardar los datos en la ubicación original de S3, los registros permanecen en su ubicación original y se copian en su carpeta particionada, lo que duplica el almacenamiento de registros.

 Note

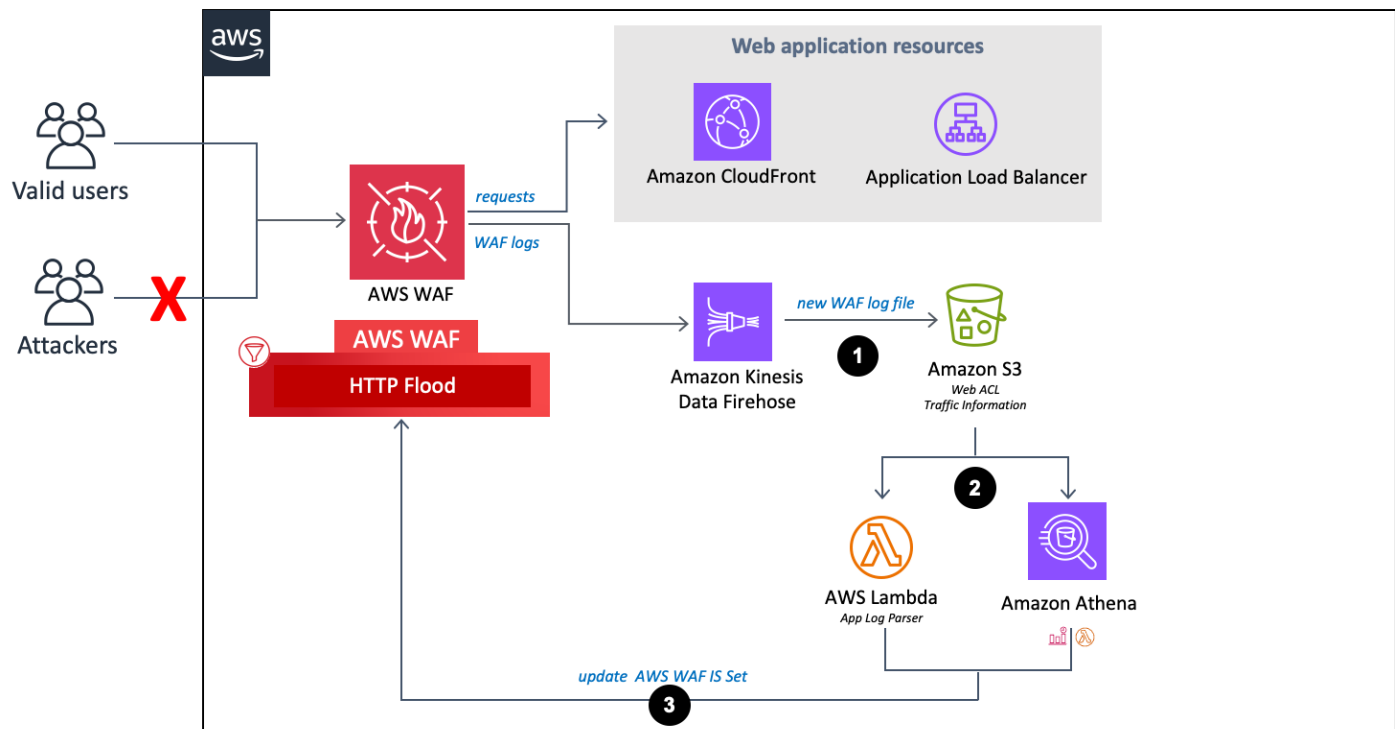
Para el analizador de registros Athena, esta solución solo particiona los registros nuevos que llegan a su bucket de Amazon S3 después de implementar esta solución. Si tiene registros existentes que desea particionar, debe cargarlos manualmente en Amazon S3 después de implementar esta solución.

2. En función de los parámetros de plantilla `Activate HTTP Flood Protection` y `Activate Scanner & Probe Protection`, esta solución procesa los registros mediante uno de los siguientes métodos:
 - a. `Lambda`: cada vez que se almacena un nuevo registro de acceso en el bucket de Amazon S3, se inicia la función `Log Parser Lambda`.
 - b. `Athena`: de forma predeterminada, cada cinco minutos se ejecuta la consulta `Athena de Scanner & Probe Protection` y el resultado se envía a `AWS WAF`. Este proceso se inicia mediante un `CloudWatch` evento que inicia la función `Lambda` responsable de ejecutar la consulta de `Athena` y envía el resultado a `AWS WAF`.
3. La solución analiza los datos del registro para identificar las direcciones IP que generaron más errores que la cuota definida. A continuación, la solución actualiza una condición del conjunto de IP de `AWS WAF` para bloquear esas direcciones IP durante un período de tiempo definido por el cliente.

Analizador de registros - AWS WAF

Si selecciona `yes - AWS Lambda log parser` o `yes - Amazon Athena log parser` selecciona `Activar la protección contra inundaciones HTTP`, esta solución proporciona los siguientes componentes, que analizan los registros de `AWS WAF` para identificar y bloquear los orígenes que inundan el punto final con una tasa de solicitudes superior a la cuota que ha definido.

Flujo del analizador de registros `AWS WAF`.

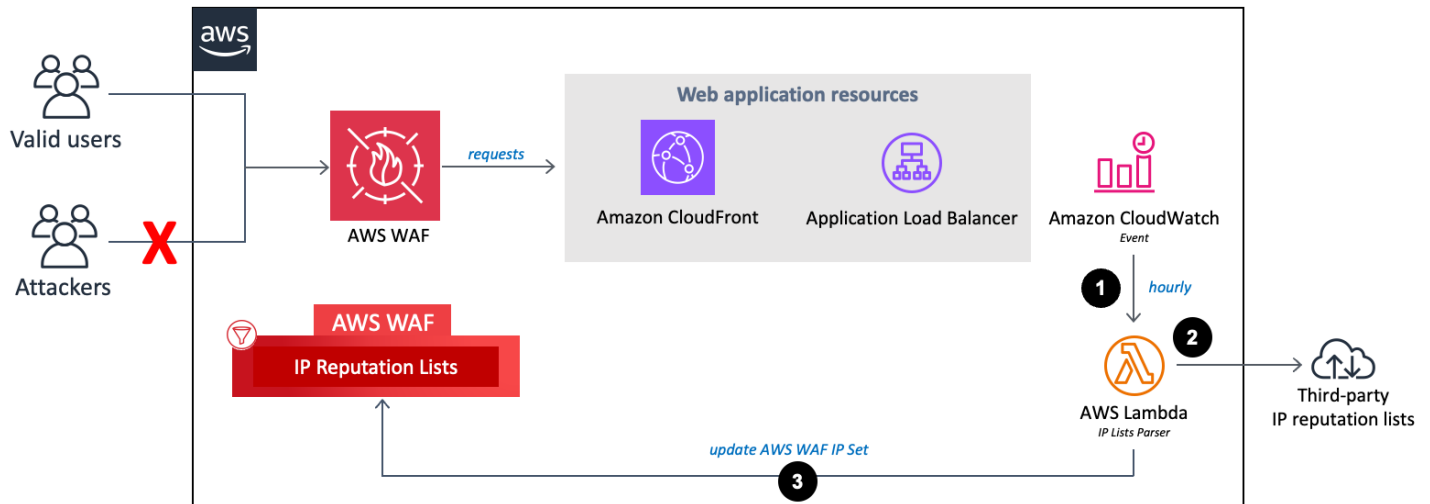


1. Cuando AWS WAF recibe registros de acceso, los envía a un punto final Firehose. A continuación, Firehose entrega los registros a un depósito particionado en Amazon S3 denominado `<customer-bucket>/AWSLogs/<optional-prefix>/year=<YYYY>/month=<MM>/day=<DD>/hour=<HH>/`
2. En función de los parámetros de plantilla Activate HTTP Flood Protection y Activate Scanner & Probe Protection, esta solución procesa los registros mediante uno de los siguientes métodos:
 - a. Lambda: cada vez que se almacena un nuevo registro de acceso en el bucket de Amazon S3, se inicia la función Log Parser Lambda.
 - b. Athena: De forma predeterminada, cada cinco minutos se ejecuta la consulta Athena del escáner y la sonda y el resultado se envía a AWS WAF. Este proceso se inicia mediante un CloudWatch evento de Amazon, que luego inicia la función Lambda responsable de ejecutar la consulta de Amazon Athena y envía el resultado a AWS WAF.
3. La solución analiza los datos de registro para identificar las direcciones IP que enviaron más solicitudes que la cuota definida. A continuación, la solución actualiza una condición del conjunto de IP de AWS WAF para bloquear esas direcciones IP durante un período de tiempo definido por el cliente.

Analizador de listas de direcciones IP

La función `IP Lists Parser Lambda` ayuda a protegerse contra los atacantes conocidos identificados en listas de reputación de IP de terceros.

La reputación de IP enumera el flujo del analizador.

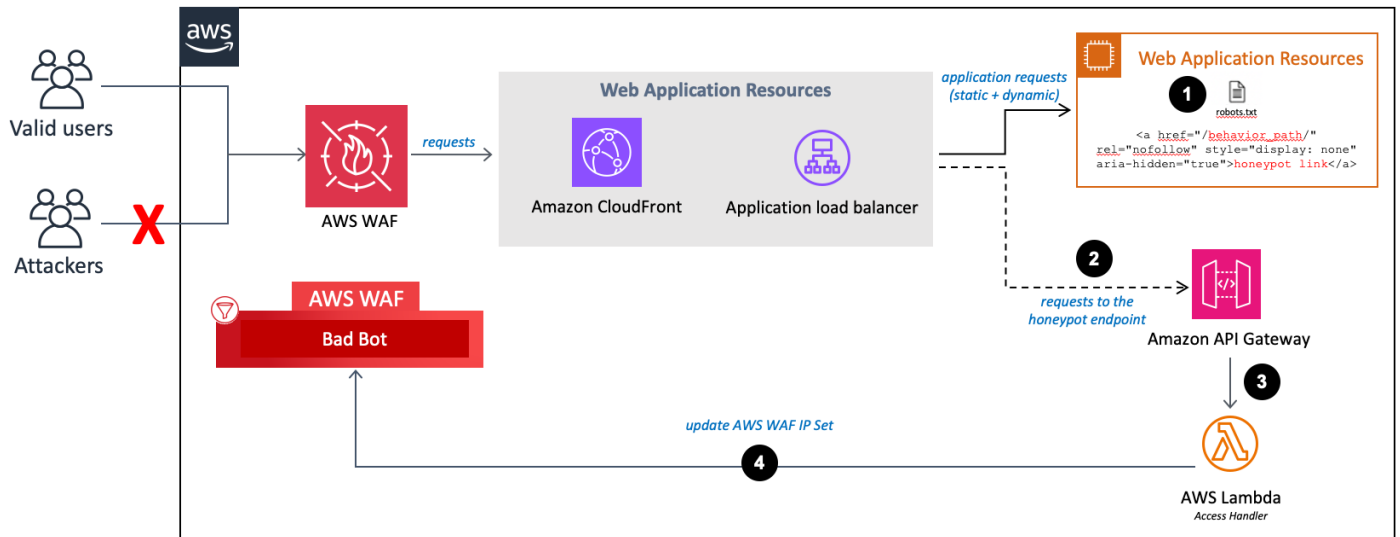


1. Un CloudWatch evento de Amazon cada hora invoca la función `IP Lists Parser Lambda`.
2. La función Lambda recopila y analiza datos de tres fuentes:
 - Listas DROP y EDROP de Spamhaus
 - Lista de direcciones IP de amenazas emergentes de Proofpoint
 - Lista de nodos de salida de Tor
3. La función Lambda actualiza la lista de bloqueados de AWS WAF con las direcciones IP actuales.

Controlador de acceso

La función `Access Handler Lambda` inspecciona las solicitudes al punto final de honeypot para extraer su dirección IP de origen.

El controlador de acceso y el punto final del honeypot.



1. Inserte el punto final de Honeypot en su sitio web y actualice el estándar de exclusión de robots, tal y como se describe en [Insertar el enlace de Honeypot en su aplicación web \(opcional\)](#).
2. Cuando un rastreador de contenido o un bot malicioso accede al punto final del honeypot, invoca la Access Handler función Lambda.
3. La función Lambda intercepta e inspecciona los encabezados de las solicitudes para extraer la dirección IP de la fuente que accedió al punto final de la captura.
4. La función Lambda actualiza una condición de conjunto de IP de AWS WAF para bloquear esas direcciones IP.

Planificación de la implementación

En esta sección se describen el [costo](#), la [seguridad](#), [las cuotas](#) y otras consideraciones antes de implementar la solución.

Regiones de AWS admitidas

Según los valores de los parámetros de entrada de la plantilla que defina, esta solución requiere diferentes recursos. Es posible que estos recursos (que se muestran en la tabla siguiente) no estén disponibles en todas las regiones de AWS. Por lo tanto, debe lanzar esta solución en una región de AWS en la que estén disponibles estos servicios. Para obtener la disponibilidad más reciente de los servicios de AWS por región, consulte la [lista de servicios regionales de AWS](#).

	ACL web de AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Tipo de punto de conexión				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
Active la protección contra inundaciones HTTP				
sí: analizador de registros AWS Lambda				✓
sí: analizador de registros Amazon Athena		✓	✓	✓

	ACL web de AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Active la protección del escáner y la sonda				
sí: analizador de registros Amazon Athena		✓	✓	

Note

Si lo elige CloudFront como punto final, debe implementar la solución en la región EE. UU. Este (Virginia del Norte) (us-east-1).

Costo

Usted es responsable del coste de los servicios de AWS utilizados al ejecutar la solución Security Automations for AWS WAF. El coste total de ejecutar esta solución depende de la protección activada y de la cantidad de datos ingeridos, almacenados y procesados.

Recomendamos crear un [presupuesto](#) a través de [AWS Cost Explorer](#) para ayudar a administrar los costos. Para obtener más información, consulte la página web de precios de cada servicio de AWS que utilizó en esta solución.

Las siguientes tablas son ejemplos de desgloses de costos para ejecutar esta solución en la región EE.UU. Este (Virginia del Norte) (no incluye la capa gratuita de AWS). Los precios están sujetos a cambios.

Ejemplo 1: Activar Reputation List Protection, Bad Bot Protection, AWS Lambda Log Parser para HTTP Flood Protection y Scanner & Probe Protection

Servicio de AWS	Dimensiones/mes	Coste [USD]
Amazon Data Firehose	100 GB	~2,90 \$
Amazon S3	100 GB	~2,30 \$
AWS Lambda	128 MB: 3 funciones, 1 millón de invocaciones y una duración media de 500 milisegundos por ejecución de Lambda 512 MB: 2 funciones, 1 millón de invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	~5,40 \$
Amazon API Gateway	1 millón de solicitudes	~3,40 \$
ACL web de AWS WAF	1	5 DÓLARES
Regla WAF de AWS	4	4,00 DÓLARES
Solicitud de AWS WAF	1M	0,60\$
Total		~23,60 \$ al mes

Ejemplo 2: Activar Reputation List Protection, Bad Bot Protection, Amazon Athena Log Parser para HTTP Flood Protection y Scanner & Probe Protection

Servicio de AWS	Dimensiones/mes	Coste [USD]
Amazon Data Firehose	100 GB	~2,90 \$
Amazon S3	100 GB	~2,30 \$
AWS Lambda	128 MB: 3 funciones, 1 millón de invocaciones y	~1,26 \$

Servicio de AWS	Dimensiones/mes	Coste [USD]
	una duración media de 500 milisegundos por ejecución de Lambda	
	512 MB: 2 funciones, 7560 invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	
Amazon API Gateway	1 millón de solicitudes	~3,40 \$
Amazon Athena	1,2 millones de visitas a CloudFront objetos o 1,2 millones de solicitudes de ALB al día, lo que genera un registro de aproximadamente 500 bytes por visita o solicitud	~4,32 \$
ACL web de AWS WAF	1	5 DÓLARES
Regla WAF de AWS	4	4,00 DÓLARES
Solicitud de AWS WAF	1M	0,60\$
Total		~23,78 \$ al mes

Ejemplo 3: Activar la retención de IP para conjuntos de IP permitidos y denegados

Servicio de AWS	Dimensiones/mes	Coste [USD]
Amazon DynamoDB	1000 escrituras y 1 MB de almacenamiento de datos	~0,00 \$
AWS Lambda	128 MB: 1 función, 2000 invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	~0,01 \$

Servicio de AWS	Dimensiones/mes	Coste [USD]
	512 MB: 1 función, 2000 invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	
Amazon CloudWatch	Eventos 2K	~0,00 \$
ACL web de AWS WAF	1	5,00 DÓLARES
Regla WAF de AWS	2	2,00 DÓLARES
Solicitud de AWS WAF	1M	0,60\$
Total		~7,61 \$ al mes

Estimación del costo de los troncos CloudWatch

Algunos servicios de AWS que se utilizan en esta solución, como Lambda, generan CloudWatch registros. [Estos registros conllevan cargos](#). Recomendamos eliminar o archivar los registros para reducir el coste. Para obtener información detallada sobre el archivo de registros, consulte [Exportación de datos de registro a Amazon S3](#) en la Guía del usuario de Amazon CloudWatch Logs.

Si opta por utilizar el analizador de registros Athena durante la instalación, esta solución programa una consulta para que se ejecute en los registros de acceso a aplicaciones o WAF de AWS de sus buckets de Amazon S3, tal y como están configurados. Se le cobrará en función de la cantidad de datos escaneados por cada consulta. La solución divide los registros y las consultas en particiones para minimizar los costos. De forma predeterminada, la solución mueve los registros de acceso a las aplicaciones de su ubicación original de Amazon S3 a una estructura de carpetas particionada. También puede conservar el original, pero se le cobrará por el almacenamiento de registros duplicados. Esta solución utiliza [grupos de trabajo](#) para segmentar las cargas de trabajo y puede configurarlas para gestionar el acceso a las consultas y los costes. Consulte la [estimación de costes de Athena](#) para ver un ejemplo de cálculo de la estimación de costes. Para obtener más información, consulta los precios de [Amazon Athena](#).

Estimación de costes de Athena

Si utiliza la opción de analizador de registros de Athena mientras ejecuta las reglas HTTP Flood Protection o Scanner & Probe Protection, se le cobrará por el uso de Athena. De forma predeterminada, cada consulta de Athena se ejecuta cada cinco minutos y analiza los datos de las últimas cuatro horas. La solución aplica particiones a los registros y a las consultas de Athena para minimizar los costes. Puede configurar el número de horas de datos que escanea una consulta cambiando el valor del parámetro de plantilla WAF Block Period. Sin embargo, aumentar la cantidad de datos escaneados probablemente aumentará el costo de Athena.

Tip

A continuación se muestra un ejemplo de cálculo del coste CloudFront de los registros:

En promedio, cada CloudFront visita puede generar alrededor de 500 bytes de datos.

Si se reciben 1,2 millones de CloudFront objetos al día, habrá 200 000 (1,2 M/6) visitas cada cuatro horas, suponiendo que los datos se ingieran a un ritmo constante. Tenga en cuenta sus patrones de tráfico reales a la hora de calcular sus costes.

$[500 \text{ bytes of data}] * [200K \text{ hits per four hours}] = [\text{an average } 100 \text{ MB } (0.0001\text{TB}) \text{ data scanned per query}]$

Athena cobra 5 USD por TB de datos escaneados.

$[0.0001 \text{ TB}] * [\$5] = [\$0.0005 \text{ per query scan}]$

La consulta de Athena se ejecuta cada cinco minutos, lo que equivale a 12 ejecuciones por hora.

$[12 \text{ runs}] * [24 \text{ hours}] = [288 \text{ runs per day}]$

$[\$0.0005 \text{ per query scan}] * [288 \text{ runs per day}] * [30 \text{ days}] = [\$4.32 \text{ per month}]$

Los costos reales varían según los patrones de tráfico de la aplicación. Para obtener más información, consulta los precios de [Amazon Athena](#).

Seguridad

Cuando crea sistemas en la infraestructura de AWS, las responsabilidades de seguridad se comparten entre usted y AWS. Este [modelo de responsabilidad compartida](#) reduce la carga operativa, ya que AWS opera, administra y controla los componentes, incluidos el sistema operativo anfitrión, la capa de virtualización y la seguridad física de las instalaciones en las que operan los

servicios. Para obtener más información sobre la seguridad de AWS, visite [Seguridad en la nube de AWS](#).

Roles de IAM

Con las funciones de IAM, puede asignar acceso, políticas y permisos detallados a los servicios y usuarios de la nube de AWS. Esta solución crea funciones de IAM con los privilegios mínimos y estas funciones otorgan los recursos de la solución con los permisos necesarios.

Datos

Todos los datos almacenados en los buckets de Amazon S3 y en las tablas de DynamoDB tienen cifrado en reposo. Los datos en tránsito con Firehose también están cifrados.

Capacidades de protección

Las aplicaciones web son vulnerables a diversos ataques. Estos ataques incluyen solicitudes especialmente diseñadas para aprovechar una vulnerabilidad o tomar el control de un servidor; ataques volumétricos diseñados para destruir un sitio web; o robots y rastreadores maliciosos programados para extraer y robar contenido web.

Esta solución se utiliza CloudFormation para configurar las reglas de AWS WAF, incluidos los grupos de reglas administradas de AWS y las reglas personalizadas, para bloquear los siguientes ataques comunes:

- Reglas administradas por AWS: este servicio administrado proporciona protección contra las vulnerabilidades comunes de las aplicaciones u otro tráfico no deseado. Esta solución incluye grupos de [reglas de reputación de IP gestionada por AWS](#), [grupos de reglas de referencia gestionados por AWS](#) y [grupos de reglas de casos de uso específicos gestionados](#) por AWS. Tiene la opción de seleccionar uno o más grupos de reglas para su ACL web, hasta alcanzar la cuota máxima de unidades de capacidad (WCU) de la ACL web.
- Inyección de SQL: los atacantes insertan código SQL malicioso en las solicitudes web para extraer datos de la base de datos. Diseñamos esta solución para bloquear las solicitudes web que contienen código SQL potencialmente malicioso.
- XSS: Los atacantes utilizan las vulnerabilidades de un sitio web benigno como medio para introducir scripts maliciosos del sitio del cliente en el navegador web de un usuario legítimo. Lo diseñamos para inspeccionar los elementos más explorados de las solicitudes entrantes a fin de identificar y bloquear los ataques XSS.

- **Inundaciones de HTTP:** los servidores web y otros recursos de back-end corren el riesgo de sufrir ataques DDoS, como las inundaciones de HTTP. Esta solución invoca automáticamente una regla basada en la velocidad cuando las solicitudes web de un cliente superan una cuota configurable. Como alternativa, puede aplicar esta cuota procesando los registros de AWS WAF mediante una función de Lambda o una consulta de Athena.
- **Escáneres y sondeos:** las fuentes malintencionadas escanean e investigan las aplicaciones web con acceso a Internet en busca de vulnerabilidades mediante el envío de una serie de solicitudes que generan códigos de error HTTP 4xx. Puedes usar este historial para identificar y bloquear las direcciones IP de origen malintencionadas. Esta solución crea una función de Lambda CloudFront o una consulta de Athena que analiza automáticamente los registros de acceso a ALB, cuenta el número de solicitudes incorrectas de direcciones IP de origen único por minuto y actualiza AWS WAF para bloquear nuevos escaneos de direcciones que alcanzaron la cuota de error definida.
- **Orígenes conocidos de los atacantes (listas de reputación de IP):** muchas organizaciones mantienen listas de reputación de direcciones IP gestionadas por atacantes conocidos, como remitentes de spam, distribuidores de malware y botnets. Esta solución aprovecha la información de estas listas de reputación para ayudarle a bloquear las solicitudes de direcciones IP malintencionadas. Además, esta solución bloquea a los atacantes identificados por los grupos de reglas de reputación de IP basándose en la inteligencia de amenazas interna de Amazon.
- **Bots y rastreadores:** los operadores de aplicaciones web de acceso público deben confiar en que los clientes que acceden a su contenido se identifican con precisión y utilizan los servicios según lo previsto. Sin embargo, algunos clientes automatizados, como los rastreadores de contenido o los bots maliciosos, se autointerpretan mal para eludir las restricciones. Esta solución le ayuda a identificar y bloquear los robots y rastreadores defectuosos.

Cuotas

Las cuotas de servicio (que también se denominan límites) establecen el número máximo de recursos u operaciones de servicio para su cuenta de AWS.

Cuotas para los servicios de AWS en esta solución

Asegúrese de tener una cuota suficiente para cada uno de los [servicios implementados en esta solución](#). Para obtener más información, consulte las [cuotas de servicio de AWS](#). Para ver las cuotas de servicio de todos los servicios de AWS en la documentación sin cambiar de página, consulte la información en la página de [puntos finales y cuotas del servicio](#) en el PDF.

Cuotas de AWS WAF

AWS WAF puede bloquear un máximo de 10 000 rangos de direcciones IP en la notación de enrutamiento entre dominios sin clase (CIDR) por condición de coincidencia de IP. Cada lista que crea esta solución está sujeta a esta cuota. Para obtener más información, consulte las cuotas de [AWS WAF](#). A partir de la versión 3.0, esta solución crea dos conjuntos de IP para adjuntarlos a cada regla, uno para IPv4 y otro para IPv6.

AWS WAF permite un máximo de una solicitud por segundo, por cuenta y región de AWS para las llamadas a la API dirigidas a cualquier persona Create o Put Update acción. Si realiza estas llamadas a la API fuera de la solución, es posible que se produzca un problema de limitación de la API. Para evitar este problema, te recomendamos que evites ejecutar otras aplicaciones que realicen estas llamadas a la API en la misma cuenta y región en la que se implementa esta solución.

Consideraciones sobre la implementación

En las siguientes secciones, se describen las limitaciones y consideraciones a la hora de implementar esta solución.

Reglas de AWS WAF

La ACL web que genera esta solución está diseñada para ofrecer una protección integral para las aplicaciones web. La solución proporciona un conjunto de reglas administradas por AWS y reglas personalizadas que puede añadir a la ACL web. Para incluir una regla, elija yes los parámetros pertinentes al lanzar la CloudFormation pila. Consulte [el paso 1. Inicie la pila](#) de la lista de parámetros.

Note

La out-of-box solución no es compatible con [AWS Firewall Manager](#). Si desea utilizar las reglas del Firewall Manager, le recomendamos que aplique personalizaciones a su [código fuente](#).

Registro de tráfico de ACL web

Si crea la pila en una región de AWS que no sea EE. UU. Este (Virginia del Norte) y establece el punto de enlace como CloudFront, debe establecer Activate HTTP Flood Protection en no oyes - AWS WAF rate based rule.

Las otras dos opciones (yes - AWS Lambda log parser y yes - Amazon Athena log parser) requieren la activación de los registros de AWS WAF en una ACL web que se ejecute en todas las ubicaciones perimetrales de AWS, y esto no es compatible fuera de EE. UU. Este (norte de Virginia). Para obtener más información sobre cómo registrar el tráfico de ACL web, consulte la guía para [desarrolladores de AWS WAF](#).

Gestión sobredimensionada de los componentes de las solicitudes

AWS WAF no admite la inspección de contenido sobredimensionado para el cuerpo, los encabezados o las cookies del componente de solicitud web. Al escribir una declaración de reglas que inspeccione uno de estos tipos de componentes de solicitud, puede elegir una de estas opciones para indicar a AWS WAF qué hacer con estas solicitudes:

- yes(continuar) - Inspeccione el componente de la solicitud normalmente de acuerdo con los criterios de inspección de la regla. AWS WAF inspecciona el contenido de los componentes de la solicitud que se encuentra dentro de los límites de tamaño. Esta es la opción predeterminada que se utiliza en la solución.
- yes - MATCH: trate la solicitud web como coincidente con la instrucción de regla. AWS WAF aplica la acción de la regla a la solicitud sin evaluarla en función de los criterios de inspección de la regla. En el caso de una regla con Block acción, esto bloquea la solicitud con el componente de sobretamaño.
- yes - NO_MATCH- Considera que la solicitud web no coincide con la declaración de la regla, sin evaluarla según los criterios de inspección de la regla. AWS WAF continúa inspeccionando la solicitud web mediante el resto de las reglas de la ACL web, como haría con cualquier regla que no coincida.

Para obtener más información, consulte [Gestión de componentes de solicitudes web de gran tamaño en AWS WAF](#).

Implementaciones de múltiples soluciones

Puede implementar la solución varias veces en la misma cuenta y región. Debe usar un nombre de CloudFormation pila único y un nombre de bucket de Amazon S3 para cada implementación. Cada implementación única conlleva cargos adicionales y está sujeta a las cuotas de [AWS WAF](#) por cuenta y región.

Implementación de la solución

Esta solución utiliza [CloudFormation plantillas y pilas de AWS](#) para automatizar su implementación. Las CloudFormation plantillas especifican los recursos de AWS incluidos en esta solución y sus propiedades. La CloudFormation pila aprovisiona los recursos que se describen en las plantillas.

Información general del proceso de implementación

Antes de lanzar la CloudFormation plantilla, revise las consideraciones de arquitectura y configuración que se describen en esta guía. Siga las step-by-step instrucciones de esta sección para configurar e implementar la solución en su cuenta.

Tiempo de implementación: aproximadamente 15 minutos.

Note

Si ya implementó esta solución anteriormente, consulte [Actualizar la solución](#) para obtener instrucciones de actualización.

[Requisitos previos](#)

- Configure una CloudFront distribución
- Configure un ALB

[Paso 1. Lanza la pila](#)

- Inicie la CloudFormation plantilla en su cuenta de AWS.
- Introduzca los valores de los parámetros necesarios: el nombre de la pila y el nombre del bucket del registro de acceso a la aplicación.
- Revise el resto de los parámetros de la plantilla y ajústelos si es necesario.

[Paso 2. Asocie la ACL web a su aplicación web](#)

- Asocie sus distribuciones CloudFront web o ALB a la ACL web que genera esta solución. Puede asociar tantas distribuciones o balanceadores de carga como desee.

Paso 3. Configure el registro de acceso a la web

- Active el registro de acceso a la CloudFront web para sus distribuciones web o ALB y envíe los archivos de registro al bucket de Amazon S3 correspondiente. Guarde los registros en una carpeta que coincida con el prefijo definido por el usuario. Si no se utiliza ningún prefijo definido por el usuario, guarde los registros en AWSLogs (prefijo de registro predeterminado). AWSLogs/[Consulte el parámetro Application Access Log Bucket Prefix en el paso 1. Inicie la pila](#) para obtener más información.

CloudFormation Plantillas de AWS

Esta solución incluye una CloudFormation plantilla principal de AWS y dos plantillas anidadas. Puede descargar las CloudFormation plantillas antes de implementar la solución.

Pila principal

View template

[aws-waf-security-automations](#).template: utilice esta plantilla como punto de entrada para lanzar la solución en su cuenta. La configuración predeterminada implementa una ACL web de AWS WAF con reglas preconfiguradas. Puede personalizar la plantilla en función de sus necesidades.

Pila WebACL

View template

[aws-waf-security-automations-webacl](#).template: esta plantilla anidada aprovisiona los recursos de AWS WAF, que incluyen una ACL web, una IP, conjuntos y otros recursos asociados.

Pila Firehose Athena

View template

[aws-waf-security-automations-firehose-athena](#).template: esta plantilla anidada [proporciona recursos relacionados con AWS Glue, Athena y Firehose](#). Se crea al elegir el analizador de registros Athena Scanner & Probe o el analizador de registros HTTP Flood Lambda o Athena.

Requisitos previos

Esta solución está diseñada para funcionar con aplicaciones web implementadas con CloudFront o un ALB. Si aún no ha configurado uno de estos recursos, complete las tareas correspondientes antes de lanzar esta solución.

Configure una CloudFront distribución

Complete los siguientes pasos para configurar una CloudFront distribución para el contenido estático y dinámico de su aplicación web. Consulta la [Guía para CloudFront desarrolladores de Amazon](#) para obtener instrucciones detalladas.

1. Cree una distribución de aplicaciones CloudFront web. Consulte [Creación de una distribución](#).
2. Configure los orígenes estáticos y dinámicos. Consulte [Uso de varios orígenes con CloudFront distribuciones](#).
3. Especifique el comportamiento de su distribución. Consulte los [valores que especifique al crear o actualizar una distribución](#).

Note

Si lo elige CloudFront como punto final, debe crear sus WAFV2 recursos en la región EE.UU. Este (Virginia del Norte).

Configure un ALB

Para configurar un ALB para distribuir el tráfico entrante a su aplicación web, consulte [Create an Application Load Balancer](#) en la Guía del usuario de Application Load Balancers.

Paso 1. Lanzar la pila

Esta CloudFormation plantilla de AWS automatizada implementa la solución en la nube de AWS.

1. Inicie sesión en la [consola de administración de AWS](#) y seleccione la `waf-automation-on-aws.template` CloudFormation plantilla Launch Solution para lanzar.

Launch solution

- La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar esta solución en otra región de AWS, utilice el selector de regiones de la barra de navegación de la consola. Si elige CloudFront como punto final, debe implementar la solución en la región EE.UU. Este (Virginia del Norte) (us-east-1).

 Note

Según los valores de los parámetros de entrada que defina, esta solución requiere diferentes recursos. Actualmente, estos recursos solo están disponibles en regiones específicas de AWS. Por lo tanto, debe lanzar esta solución en una región de AWS en la que estén disponibles estos servicios. Para obtener más información, consulte [Regiones de AWS compatibles](#).

- En la página Especificar plantilla, compruebe que ha seleccionado la plantilla correcta y pulse Siguiente.
- En la página Especificar los detalles de la pila, asigne un nombre a la configuración de AWS WAF en el campo Nombre de la pila. También es el nombre de la ACL web que crea la plantilla.
- En Parámetros, revise los parámetros de la plantilla y modifíquelos según sea necesario. Para excluirse de una función en particular, elija none o no según corresponda. Esta solución utiliza los siguientes valores predeterminados.

Parámetro	Predeterminado/a	Descripción
Nombre de pila	[.red]#<requires input>	El nombre de la pila no puede contener espacios. Este nombre debe ser único en su cuenta de AWS y es el nombre de la ACL web que crea la plantilla.
Tipo de recurso		
Punto de conexión	CloudFront	Elija el tipo de recurso que se va a utilizar. NOTA: Si elige CloudFront como punto final, debe lanzar la solución para crear recursos

Parámetro	Predeterminado/a	Descripción
		de WAF en la región EE.UU. Este (Virginia del Norte) (us-east-1).
Grupos de reglas de reputación IP gestionada por AWS		

Parámetro	Predeterminado/a	Descripción
Activar la protección de grupos de reglas gestionados por listas de reputación IP de Amazon	no	Seleccione yes para activar el componente diseñado para añadir el grupo de reglas gestionado por Amazon IP Reputation List a la ACL web. Este grupo de reglas se basa en la inteligencia de amenazas interna de Amazon. Esto resulta útil si desea bloquear las direcciones IP que suelen estar asociadas a los bots u otras amenazas. El bloqueo de estas direcciones IP puede ayudar a mitigar los bots y a reducir el riesgo de que un actor malintencionado descubra una aplicación vulnerable. La WCU requerida es 25. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionados por listas de direcciones IP anónimas	no	Seleccione yes para activar el componente diseñado para añadir un grupo de reglas gestionado por listas de IP anónimas a la ACL web. Este grupo de reglas bloquea las solicitudes de los servicios que permiten ocultar la identidad del espectador. Estas incluyen solicitudes de proxies VPNs, nodos de Tor y proveedores de alojamiento. Este grupo de reglas resulta útil si desea filtrar los lectores que podrían intentar ocultar su identidad en la aplicación. El bloqueo de las direcciones IP de estos servicios puede ayudar a mitigar los bots y la evasión de restricciones geográficas. La WCU requerida es 50. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Grupos de reglas básicas gestionados por AWS		
Active la protección de grupos de reglas gestionados por el conjunto de reglas principales	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionado por el conjunto de reglas principales a la ACL web. Este grupo de reglas proporciona protección contra la explotación de una amplia gama de vulnerabilidades, incluidas algunas de las de alto riesgo y las que se producen con más frecuencia. Considere la posibilidad de utilizar este grupo de reglas para cualquier caso de uso de AWS WAF. La WCU requerida es 700. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Active Admin Protection (protección gestionada de grupos de reglas)	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionado por Admin Protection a la ACL web. Este grupo de reglas bloquea el acceso externo a las páginas administrativas expuestas. Esto puede resultar útil si ejecuta software de terceros o si quiere reducir el riesgo de que un actor malintencionado obtenga acceso administrativo a la aplicación. La WCU requerida es 100. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionados con entradas incorrectas conocidas	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionadas con entradas incorrectas conocidas a la ACL web. Este grupo de reglas bloquea el acceso externo a las páginas administrativas expuestas. Esto puede resultar útil si ejecuta software de terceros o si quiere reducir el riesgo de que un actor malintencionado obtenga acceso administrativo a la aplicación. La WCU requerida es 100. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.
Grupo de reglas específicas para casos de uso gestionados por AWS		

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionados por bases de datos SQL	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionado por la base de datos SQL a la ACL web. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de bases de datos SQL, como los ataques de inyección de SQL. Este puede ayudar a evitar la inyección remota de consultas no autorizadas. Valore el uso de este grupo de reglas si la aplicación interactúa con una base de datos SQL. El uso de la regla personalizada de inyección de SQL es opcional si ya tiene activado el grupo de reglas SQL gestionado por AWS. La WCU requerida es 200. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos

Parámetro	Predeterminado/a	Descripción
		de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionados por el sistema operativo Linux	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionado del sistema operativo Linux a la ACL web. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de Linux, incluidos los ataques de inclusión de archivos locales (LFI) específicos de Linux. Este puede ayudar a evitar ataques que expongan el contenido de un archivos o que ejecuten código que, en principio, tendría que ser inaccesible para los atacantes. Evalúe este grupo de reglas si alguna parte de su aplicación se ejecuta en Linux. Debe usar este grupo de reglas junto con el grupo de reglas del sistema operativo POSIX. La WCU requerida es 200. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad.

Parámetro	Predeterminado/a	Descripción
		Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules .

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionadas por el sistema operativo POSIX	no	Seleccione activar el componente diseñado y es para añadir la protección de grupos de reglas gestionadas por el conjunto de reglas principales a la ACL web. Este grupo de reglas bloquea los patrones de solicitudes asociados a la explotación de vulnerabilidades específicas de los sistemas operativos POSIX y similares a POSIX, incluidos los ataques LFI. Este puede ayudar a evitar ataques que expongan el contenido de un archivos o que ejecuten código que, en principio, tendría que ser inaccesible para los atacantes. Evalúe este grupo de reglas si alguna parte de la aplicación se ejecuta en un sistema operativo POSIX o similar a POSIX. La WCU requerida es 100. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad.

Parámetro	Predeterminado/a	Descripción
		Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules .

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionados por el sistema operativo Windows	no	Seleccione yes para activar el componente diseñado para agregar el grupo de reglas administrado del sistema operativo Windows a la ACL web. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de Windows, como la ejecución remota de PowerShell comandos. Este puede ayudar a evitar la explotación de vulnerabilidades que permiten a un atacante ejecutar comandos no autorizados o ejecutar código malintencionado. Valore este grupo de reglas si alguna parte de la aplicación se ejecuta en un sistema operativo Windows. La WCU requerida es 200. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos

Parámetro	Predeterminado/a	Descripción
		de reglas de AWS Managed Rules.

Parámetro	Predeterminado/a	Descripción
Active la protección de grupos de reglas gestionadas por aplicaciones PHP	no	Seleccione yes activar el componente diseñado para añadir el grupo de reglas gestionado por aplicaciones PHP a la ACL web. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de vulnerabilidades específicas del uso del lenguaje de programación PHP, incluida la introducción de funciones PHP no seguras. Este puede ayudar a evitar la explotación de vulnerabilidades que permiten a un atacante ejecutar de forma remota código o comandos sin autorización. Evalúe este grupo de reglas si PHP está instalado en cualquier servidor con el que interactúe su aplicación. La WCU requerida es 100. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos

Parámetro	Predeterminado/a	Descripción
		de reglas de AWS Managed Rules .
Active WordPress la protección de grupos de reglas gestionados por aplicaciones	no	Seleccione yes activar el componente diseñado para añadir un grupo de reglas gestionado por WordPress aplicaciones a la ACL web. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de vulnerabilidades específicas de los WordPress sitios. Evalúe este grupo de reglas si está corriendo WordPress . Este grupo de reglas debe usarse junto con los grupos de reglas de la base de datos SQL y de la aplicación PHP. La WCU requerida es 100. Su cuenta debe tener una capacidad de WCU suficiente para evitar que se produzca un error en la implementación de la pila de ACL web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de reglas de AWS Managed Rules.
Regla personalizada: Scanner & Probes		

Parámetro	Predeterminado/a	Descripción
Active la protección del escáner y la sonda	yes - AWS Lambda log parser	Elija el componente utilizado para bloquear los escáneres y las sondas. Consulte las opciones del analizador de registros para obtener más información sobre las ventajas y desventajas relacionadas con las opciones de mitigación.

Parámetro	Predeterminado/a	Descripción
Nombre del depósito de registro de acceso a la aplicación	[.red]<requires input>	Si eligió yes el parámetro Activate Scanner & Probe Protection, introduzca el nombre del bucket de Amazon S3 (nuevo o existente) en el que desea almacenar los registros de acceso de sus CloudFront distribuciones o ALB. Si utiliza un bucket de Amazon S3 existente, debe estar ubicado en la misma región de AWS en la que va a implementar la CloudFormation plantilla. Debe usar un depósito diferente para cada implementación de la solución. Para desactivar esta protección, ignore este parámetro. NOTA: Active el registro de acceso a la CloudFront web en sus distribuciones web o ALB para enviar los archivos de registro a este bucket de Amazon S3. Guarde los registros con el mismo prefijo definido en la pila (AWSLogs/prefijo predeterminado). Consulte el parámetro Application Access Log

Parámetro	Predeterminado/a	Descripción
		Bucket Prefix para obtener más información.
Prefijo del depósito de registro de acceso a la aplicación	AWSLogs/	Si ha elegido yes el parámetro Activar Scanner & Probe Protection, puede introducir un prefijo opcional definido por el usuario para el depósito de registros de acceso a las aplicaciones que aparece arriba. Si ha elegido CloudFront el parámetro Endpoint, puede introducir cualquier prefijo, por ejemplo. <code>yourprefix/</code> Si ha elegido ALB el parámetro Endpoint, debe añadirlo AWSLogs/ a su prefijo, por ejemplo. <code>yourprefix/AWSLogs/</code> Utilice AWSLogs/ (predeterminado) si no hay un prefijo definido por el usuario. Para desactivar esta protección, ignore este parámetro.

Parámetro	Predeterminado/a	Descripción
¿Está activado el registro de acceso al bucket?	no	Elija yes si ha introducido un nombre de bucket de Amazon S3 existente para el parámetro Nombre del bucket del registro de acceso a la aplicación y si el registro de acceso al servidor del bucket ya está activado. Si lo desean, la solución activa el registro de acceso al servidor para su bucket. Si eligió no el parámetro Activar la protección del escáner y la sonda, ignore este parámetro.
Umbral de error	50	Si ha elegido yes el parámetro Activar la protección del escáner y la sonda, introduzca el número máximo de solicitudes erróneas admisibles por minuto y por dirección IP. Si ha elegido no el parámetro Activar la protección del escáner y la sonda, ignore este parámetro.

Parámetro	Predeterminado/a	Descripción
Mantenga los datos en la ubicación original de S3	no	Si ha elegido <code>yes</code> - Amazon Athena <code>log parser</code> el parámetro <code>Activar protección de escáner y sonda</code>, la solución aplica la partición a los archivos de registro de acceso a las aplicaciones y a las consultas de Athena. De forma predeterminada, la solución mueve los archivos de registro de su ubicación original a una estructura de carpetas particionadas en Amazon S3. Elija <code>yes</code> si también desea conservar una copia de los registros en su ubicación original. Esto duplicará tu almacenamiento de registros. Si no eligió <code>yes</code> - Amazon Athena <code>log parser</code> el parámetro <code>Activar la protección del escáner y la sonda</code>, omita este parámetro.
Regla personalizada: HTTP Flood		

Parámetro	Predeterminado/a	Descripción
Active la protección contra inundaciones HTTP	yes - AWS WAF rate-based rule	Seleccione el component e utilizado para bloquear los ataques de inundación HTTP. Consulte las opciones del analizador de registros para obtener más información sobre las ventajas y desventajas relacionadas con las opciones de mitigación.

Parámetro	Predeterminado/a	Descripción
Umbral de solicitud predeterminado	100	Si eligió <code>yes</code> el parámetro <code>Activar la protección contra inundaciones HTTP</code>, introduzca el número máximo de solicitudes aceptables por cada cinco minutos y por dirección IP. Si ha elegido <code>yes</code> - <code>AWS WAF rate-based rule</code> el parámetro <code>Activar la protección contra inundaciones HTTP</code>, el valor mínimo aceptable es <code>100</code>. Si ha elegido <code>yes</code> - <code>AWS Lambda log parser</code> o <code>yes</code> - <code>Amazon Athena log parser</code> el parámetro <code>Activar la protección contra inundaciones HTTP</code>, puede tener cualquier valor. Para desactivar esta protección, ignore este parámetro.

Parámetro	Predeterminado/a	Descripción
Umbral de solicitud por país	<optional input>	Si eligió yes - Amazon Athena log parser el parámetro Activar protección contra inundaciones HTTP, puede introducir un umbral por país siguiendo este formato <code>JSON{"TR":50,"ER":150}</code> . La solución utiliza estos umbrales para las solicitudes originadas en los países especificados. La solución utiliza el parámetro Umbral de solicitud predeterminado para las solicitudes restantes . NOTA: Si define este parámetro, el país se incluirá automáticamente en el grupo de consultas de Athena, junto con la IP y otros campos de grupo opcionales que puede seleccionar con el parámetro Agrupar por solicitudes en HTTP Flood Athena Query. + Si opta por desactivar esta protección, ignore este parámetro.

Parámetro	Predeterminado/a	Descripción
Agrupar por solicitudes en HTTP Flood Athena Query	None	Si eligió yes - Amazon Athena log parser el parámetro Activar la protección contra inundaciones HTTP, puede elegir un campo agrupado por para contar las solicitudes por IP y el campo por grupo seleccionado. Por ejemplo, si lo desea URI, la solución cuenta las solicitudes por IP y URI. Si decide desactivar esta protección, ignore este parámetro.
Periodo de bloqueo del WAF	240	Si ha elegido yes - AWS Lambda log parser los parámetros Activar Scanner & Probe Protection o Activar HTTP Flood Protection, introduzca el período (en minutos) para bloquear las direcciones IP aplicables. yes - Amazon Athena log parser Para desactivar el análisis de registros, ignore este parámetro.

Parámetro	Predeterminado/a	Descripción
Cronograma de tiempo de ejecución de Athena Query (minutos)	5	Si ha elegido yes - Amazon Athena log parser los parámetros Activar Scanner & Probe Protection o Activar HTTP Flood Protection, puede introducir un intervalo de tiempo (en minutos) durante el que se ejecutará la consulta de Athena. De forma predeterminada, la consulta de Athena se ejecuta cada 5 minutos. Si opta por desactivar estas protecciones, ignore este parámetro.
Regla personalizada: Bad Bot		
Activa Bad Bot Protection	yes	Elige yes activar el componente diseñado para bloquear los bots maliciosos y los rastreadores de contenido.

Parámetro	Predeterminado/a	Descripción
ARN de un rol de IAM que tiene acceso de escritura a los CloudWatch registros de su cuenta	<optional input>	Proporcione un ARN opcional de un rol de IAM que tenga acceso de escritura a CloudWatch los registros de su cuenta. Por ejemplo: ARN: <code>arn:aws:iam::account_id:role/myrolename</code> . Consulte Configurar el CloudWatch registro de una API REST en API Gateway para obtener instrucciones sobre cómo crear el rol. Si deja este parámetro en blanco (predeterminado), la solución crea un nuevo rol para usted.

Parámetro	Predeterminado/a	Descripción
Umbral de solicitud predeterminado	100	Si eligió yes el parámetro Activar la protección contra inundaciones HTTP, introduzca el número máximo de solicitudes aceptables por cada cinco minutos y por dirección IP. Si ha elegido yes - AWS WAF rate-based rule el parámetro Activar la protección contra inundaciones HTTP, el valor mínimo aceptable es 100. Si ha elegido yes - AWS Lambda log parser o yes - Amazon Athena log parser ha elegido el parámetro Activar la protección contra inundaciones HTTP, puede tener cualquier valor. Para desactivar esta protección, ignore este parámetro.
Regla personalizada: listas de reputación de IP de terceros		

Parámetro	Predeterminado/a	Descripción
Active la protección de listas de reputación	yes	Elija yes bloquear las solicitudes de direcciones IP incluidas en listas de reputación de terceros (las listas compatibles incluyen Spamhaus, Emerging Threats y Tor exit node).
Reglas personalizadas antiguas		

Parámetro	Predeterminado/a	Descripción
Active la protección contra inyecciones de SQL	yes	Seleccione yes activar el componente diseñado para bloquear los ataques de inyección SQL más comunes. Considere activarlo si no utiliza un conjunto de reglas básicas administradas por AWS o un grupo de reglas de bases de datos SQL administradas por AWS. Puede elegir una de las opciones yes (continuar) oyes - NO_MATCH) si desea que AWS WAF gestione las solicitudes sobredimensionadas que superen los 8 KB (8192 bytes). yes - MATCH De forma predeterminada, yes inspecciona el contenido de los componentes de la solicitud que se encuentra dentro de los límites de tamaño según los criterios de inspección de la regla. Para obtener más información, consulte Gestión de componentes de solicitud es web sobredimensionados. Elija no desactivar esta función. NOTA: La CloudFormation pila añade la opción de gestión de sobredimensionamiento

Parámetro	Predeterminado/a	Descripción
		seleccionada a la regla de protección contra inyecciones de SQL predeterminada y la implementa en su cuenta de AWS. Si ha personalizado la regla fuera de CloudFormation, los cambios se sobrescribirán tras la actualización de la pila.

Parámetro	Predeterminado/a	Descripción
Nivel de sensibilidad para la protección contra inyecciones de SQL	LOW	Elija el nivel de sensibilidad que desee que AWS WAF utilice para inspeccionar los ataques de inyección de SQL. HIGH detecta más ataques, pero podría generar más falsos positivos. Por lo general, LOW es mejor para los recursos que ya tienen otras protecciones contra los ataques de inyección de código SQL o que tienen una baja tolerancia a los falsos positivos. Para obtener más información, consulte AWS WAF añade niveles de sensibilidad para las SensitivityLevel propiedades y las declaraciones de reglas de inyección de SQL en la Guía CloudFormation del usuario de AWS. Si decide desactivar la protección contra las inyecciones de SQL, ignore este parámetro. NOTA: La CloudFormation pila añade el nivel de sensibilidad seleccionado a la regla de protección contra inyección

Parámetro	Predeterminado/a	Descripción
		es de SQL predeterminada y lo implementa en su cuenta de AWS. Si ha personalizado la regla fuera de CloudFormation, los cambios se sobrescribirán tras la actualización de la pila.

Parámetro	Predeterminado/a	Descripción
Active la protección contra secuencias de comandos entre sitios	yes	Seleccione yes activar el componente diseñado para bloquear los ataques XSS más comunes. Considere activarlo si no utiliza un conjunto de reglas básicas administradas por AWS. También puede seleccionar una de las opciones (yes(continuar) o yes - NO_MATCH) si desea que AWS WAF gestione las solicitudes sobredimensionadas que superen los 8 KB (8192 bytes). yes - MATCH De forma predeterminada, yes utiliza la Continue opción, que inspecciona el contenido de los componentes de la solicitud que se encuentra dentro de los límites de tamaño según los criterios de inspección de la regla. Para obtener más información, consulte la sección Gestión del tamaño excesivo de los componentes de la solicitud. Seleccione no desactivar esta función. NOTA: La CloudFormation pila añade la opción de gestión de sobredimensionamiento seleccionada a la regla

Parámetro	Predeterminado/a	Descripción
		predeterminada de secuencia de comandos entre sitios y la implementa en su cuenta de AWS. Si ha personalizado la regla fuera de CloudFormation, los cambios se sobrescribirán tras la actualización de la pila.
Configuración de retención de IP permitida y denegada		
Período de retención (minutos) para el conjunto de IP permitido	-1	Si desea activar la retención de IP para el conjunto de IP permitido, introduzca un número (15 o más) como período de retención (minutos). Las direcciones IP que alcanzan el período de retención caducan y la solución las elimina del conjunto de IP. La solución admite un período de retención mínimo de 15 minutos. Si introduce un número comprendido entre 0 y 15, la solución lo considerará como tal 15. Déjelo como -1 (predeterminado) para desactivar la retención de IP.

Parámetro	Predeterminado/a	Descripción
Período de retención (minutos) para el conjunto de IP denegado	-1	Si desea activar la retención de IP para el conjunto de direcciones IP denegadas , introduzca un número (15o más) como período de retención (minutos). Las direcciones IP que alcanzan el período de retención caducan y la solución las elimina del conjunto de IP. La solución admite un período de retención mínimo de 15 minutos. Si introduce un número comprendido entre 0 y15, la solución lo considerará como tal15. Déjelo como -1 (predeterminado) para desactivar la retención de IP.

Parámetro	Predeterminado/a	Descripción
Correo electrónico para recibir notificaciones sobre la caducidad de los conjuntos de IP permitidos o denegados	<optional input>	Si activó los parámetros del período de retención de IP (consulte los dos parámetros anteriores) y desea recibir una notificación por correo electrónico cuando caduquen las direcciones IP, introduzca a una dirección de correo electrónico válida. Si no has activado la retención de IP o quieres desactivar las notificaciones por correo electrónico, déjala en blanco (opción predeterminada).
Configuración avanzada		
Período de retención (días) para grupos de registros	365	Si desea activar la retención de los grupos de CloudWatch registros, introduzca un número (1o más) como período de retención (días). Puede elegir un período de retención de entre un día (1) y diez años (3650). De forma predeterminada, los registros caducan al cabo de un año. Configúrelo -1 para conservar los registros indefinidamente.

6. Elija Siguiente.

7. En la página Configurar opciones de pila, puede especificar etiquetas (pares clave-valor) para los recursos de la pila y establecer opciones adicionales. Elija Siguiente.
8. En la página Revisar y crear, revise y confirme la configuración. Seleccione las casillas para confirmar que la plantilla creará los recursos de IAM y las capacidades adicionales necesarias.
9. Elija Crear para implementar la pila.

Vea el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 15 minutos.

Note

Además de las funciones y de Access Handler AWS Lambda Log ParserIP Lists Parser, esta solución incluye las funciones y helper custom-resource Lambda, que se ejecutan únicamente durante la configuración inicial o cuando se actualizan o eliminan los recursos.

Al usar esta solución, verá todas las funciones en la consola de AWS Lambda, pero solo las tres funciones principales de la solución están activas de forma regular. No elimine las otras dos funciones; son necesarias para administrar los recursos asociados.

Para ver los detalles sobre los recursos de la pila, selecciona la pestaña Salidas. Esto incluye el BadBotHoneypotEndpointvalor, que es el punto final del honeypot de API Gateway. Recuerde este valor porque lo usará para [incrustar el enlace de Honeypot en su aplicación web](#).

Paso 2. Asocie la ACL web a su aplicación web

Actualice sus CloudFront distribuciones o ALB para activar AWS WAF y el registro con los recursos que generó [en el paso 1. Lance la pila](#).

1. Inicie sesión en la consola [AWS WAF](#).
2. Elija la ACL web que desee usar.
3. En la pestaña Associated AWS resources (Recursos de AWS asociados), seleccione Add AWS resources (Añadir recursos de AWS).
4. En Tipo de recurso, elija la CloudFront distribución o el ALB.
5. Seleccione un recurso de la lista y, a continuación, pulse Añadir para guardar los cambios.

Paso 3. Configurar registros de acceso web

Configure CloudFront o su ALB para que envíe los registros de acceso a la web al bucket de Amazon S3 correspondiente, de modo que estos datos estén disponibles para la función Log Parser Lambda.

Almacene los registros de acceso a la web de una distribución CloudFront

1. Inicia sesión en la [CloudFront consola de Amazon](#).
2. Selecciona la distribución de tu aplicación web y selecciona Configuración de distribución.
3. En la pestaña General, seleccione Edit.
4. Para la ACL web de AWS WAF, elija la solución de ACL web creada (el parámetro del nombre de la pila).
5. En Logging, elija On.
6. En Bucket for Logs, elija el bucket de S3 que desee usar para almacenar los registros de acceso a la web. Puede ser un depósito de S3 nuevo o existente que se utilice en la pila principal y que tenga permiso CloudFront para escribir registros. La lista desplegable enumera los buckets asociados a la cuenta de AWS actual. Para obtener más información, consulta [Cómo empezar con una CloudFront distribución básica](#) en la Guía para CloudFront desarrolladores de Amazon.
7. Establezca el prefijo de registro en el prefijo utilizado para implementar la solución. Puede encontrar el prefijo en la pila principal, en la pestaña Parámetros AppAccessLogBucketPrefixParam(opción predeterminada). AWSLogs/
8. Elija Yes, edit para guardar los cambios.

Para obtener más información, consulte [Configuración y uso de registros estándar \(registros de acceso\)](#) en la Guía para CloudFront desarrolladores de Amazon.

Almacene los registros de acceso a la web desde un Application Load Balancer

1. Inicie sesión en la [consola de Amazon Elastic Compute Cloud \(Amazon EC2\)](#).
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Selecciona el ALB de su aplicación web.
4. En la pestaña Descriptions, elija Edit attributes.
5. Elija Enable access logs.

6. En la ubicación de S3, escriba el nombre del depósito de S3 que desee usar para almacenar los registros de acceso a la web. Puede ser un bucket de S3 nuevo o existente que se utilice en la pila principal y que tenga permiso para que Application Load Balancer escriba registros.
7. Establezca el prefijo de registro como el prefijo utilizado para implementar la solución. Puede encontrar el prefijo en la pila principal, en la pestaña Parámetros AppAccessLogBucketPrefixParam(opción predeterminada). AWSLogs/
8. Seleccione Save.

Para obtener más información, consulte [los registros de acceso de su aplicación Load Balancer](#) en la Guía del usuario de Elastic Load Balancing.

Supervise la solución con AppRegistry

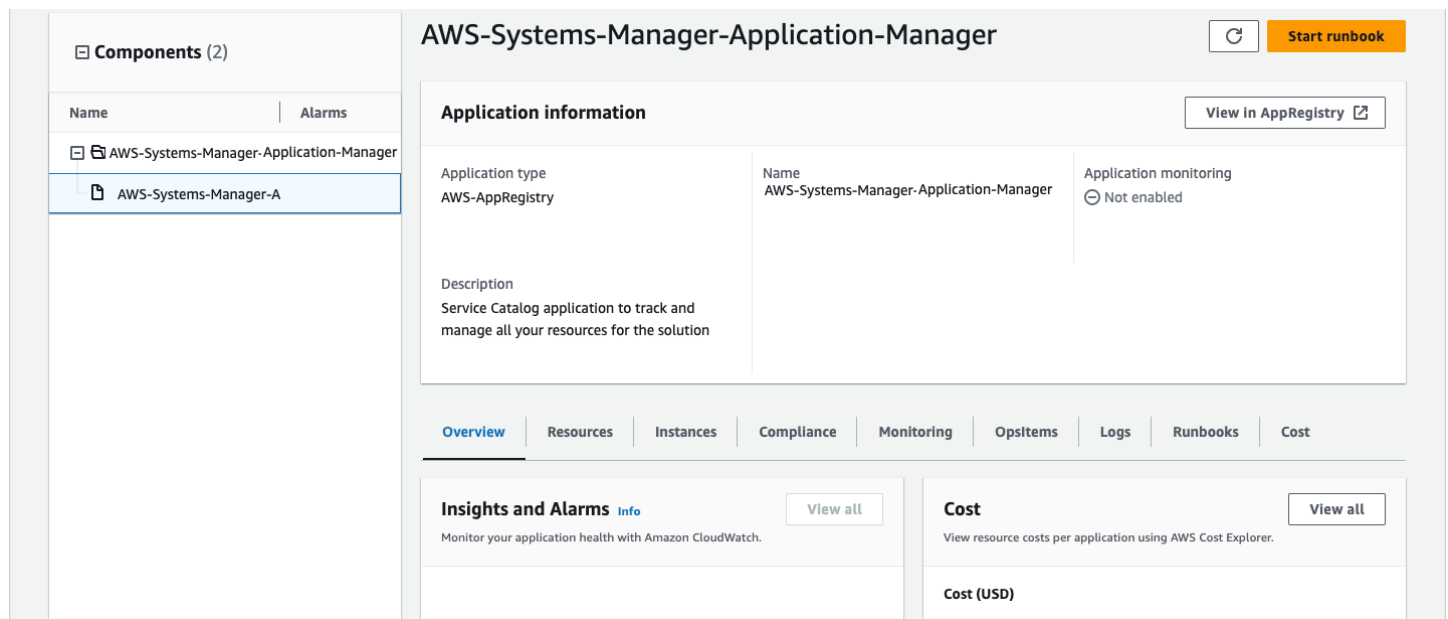
La solución incluye un AppRegistry recurso de Service Catalog para registrar la CloudFormation plantilla y los recursos subyacentes como una aplicación tanto en Service Catalog AppRegistry como en AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager le ofrece una visión a nivel de aplicación de esta solución y sus recursos para que pueda:

- Supervise sus recursos, los costes de los recursos implementados en todas las pilas y cuentas de AWS y los registros asociados a esta solución desde una ubicación central.
- Vea los datos de operaciones de los recursos de esta solución en el contexto de una aplicación. Por ejemplo, el estado de la implementación, CloudWatch las alarmas, las configuraciones de los recursos y los problemas operativos.

En la siguiente figura se muestra un ejemplo de la vista de la aplicación para la pila de soluciones de Application Manager.

Muestra la pila de soluciones en Application Manager



Active Application Insights CloudWatch

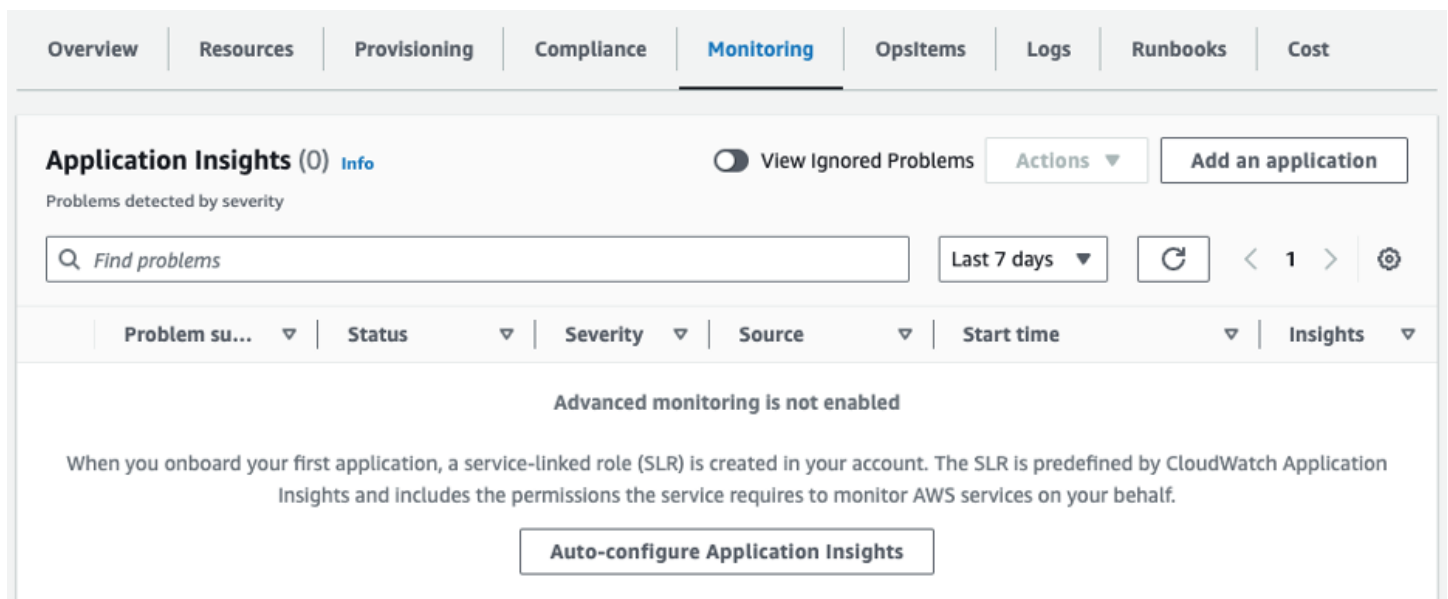
1. Inicie sesión en la [consola de Administrador de aplicaciones](#).

2. En el panel de navegación, elija Administrador de aplicaciones.
3. En Aplicaciones, busque el nombre de la aplicación para esta solución y selecciónela.

El nombre de la aplicación tendrá el registro de aplicaciones en la columna Fuente de la aplicación y tendrá una combinación del nombre de la solución, la región, el identificador de cuenta o el nombre de la pila.

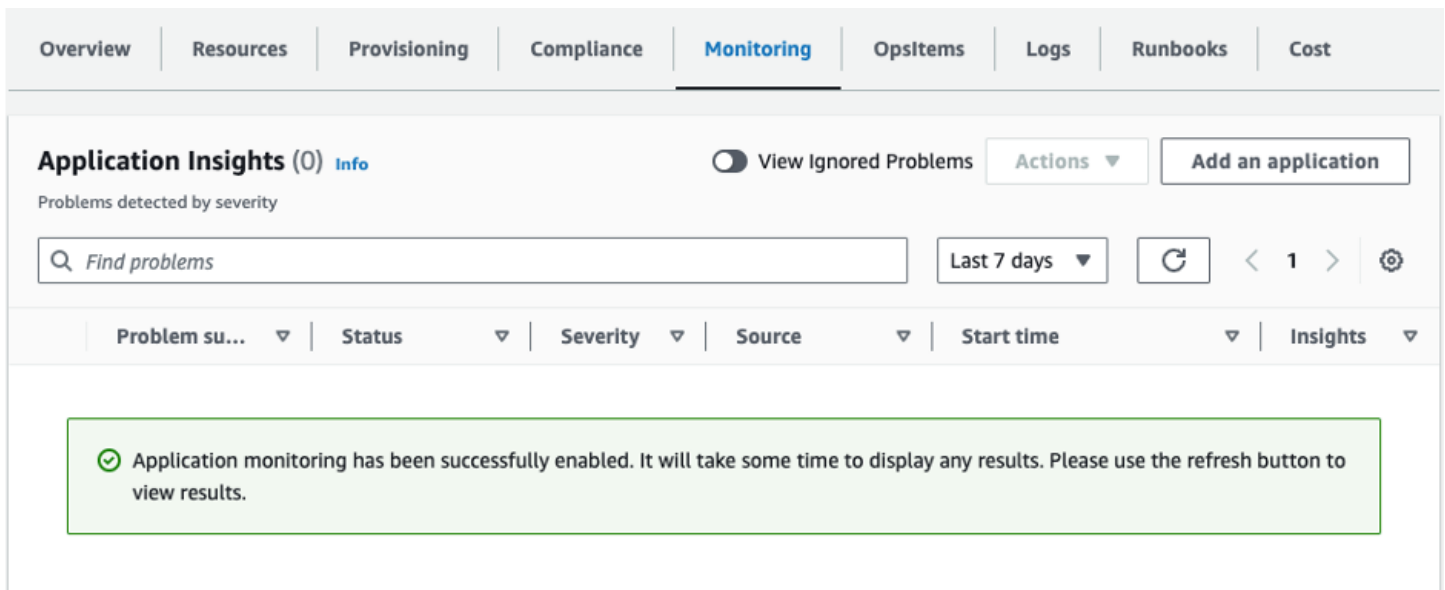
4. En el árbol de componentes, elija la pila de aplicaciones que desee activar.
5. En la pestaña Supervisión, en Application Insights, seleccione Configurar automáticamente Application Insights.

El panel de información de aplicaciones muestra los problemas no detectados y la opción de configuración automática.



Ahora, al estar activada la supervisión de sus aplicaciones, aparece el siguiente cuadro de estado:

El panel de Application Insights muestra un mensaje de activación de la supervisión correcta.



Confirmación de las etiquetas de costos asociadas a la solución

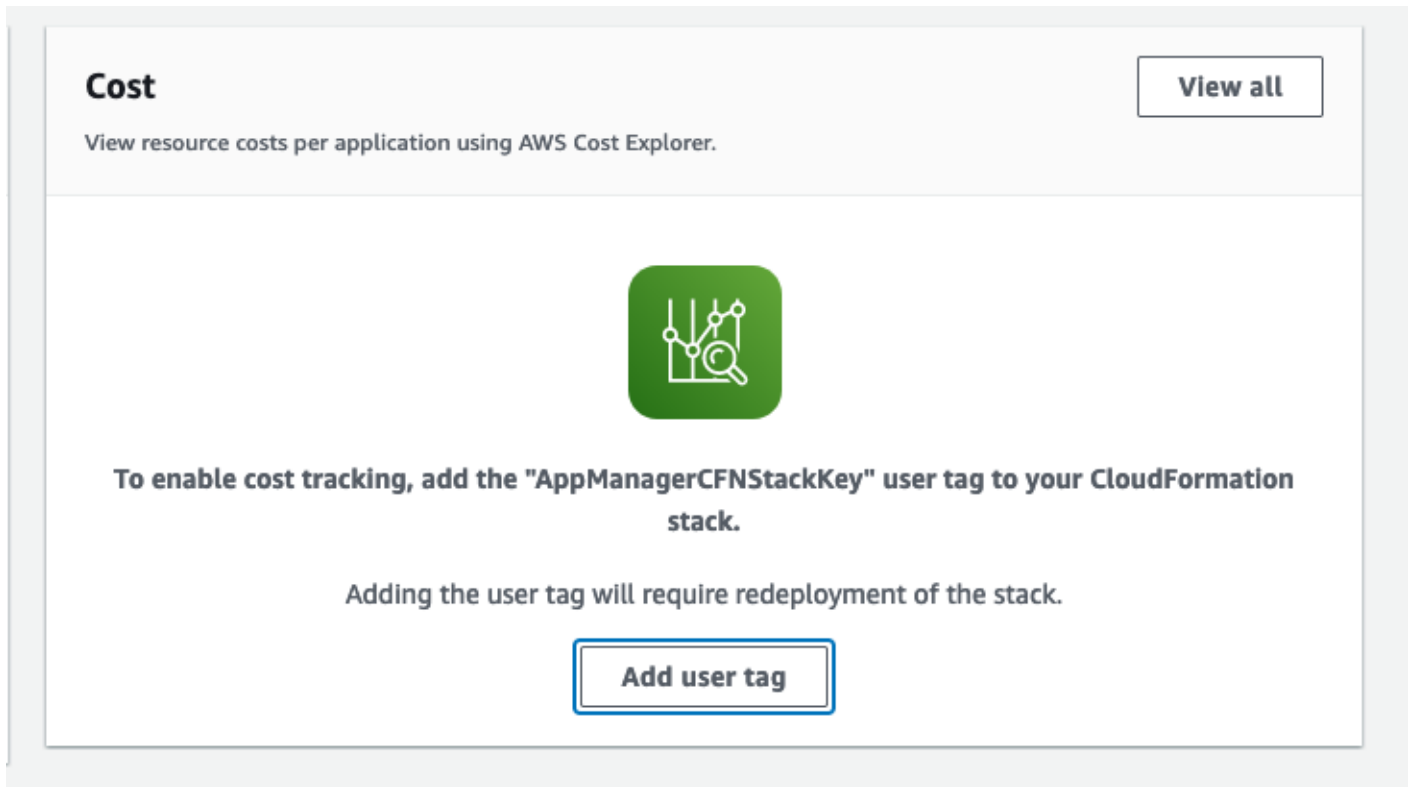
Después de activar Cost Explorer, debe activar las etiquetas de asignación de costos asociadas a esta solución para ver los costos de la solución. Para confirmar las etiquetas de asignación de costos:

1. Inicie sesión en la [consola de Administrador de aplicaciones](#).
2. En el panel de navegación, elija Administrador de aplicaciones.
3. En Aplicaciones, busque el nombre de la aplicación para esta solución y selecciónela.

El nombre de la aplicación tendrá el registro de aplicaciones en la columna Fuente de la aplicación y tendrá una combinación del nombre de la solución, la región, el identificador de cuenta o el nombre de la pila.

4. En la pestaña Descripción general, en Costo, seleccione Agregar etiqueta de usuario.

Captura de pantalla en la que se muestra el coste de la aplicación para añadir etiquetas de usuario



5. En la página Agregar etiqueta de usuario, escriba `confirm` y, a continuación, seleccione Agregar etiqueta de usuario.

El proceso de activación puede tardar hasta 24 horas en completarse y en aparecer los datos de la etiqueta.

Activar las etiquetas de asignación de costos asociadas a la solución

Después de activar Cost Explorer, debe activar las etiquetas de asignación de costos asociadas a esta solución para ver los costos de la solución. Las etiquetas de asignación de costos sólo se pueden activar desde la cuenta de administración de la organización. Para activar las etiquetas de asignación de costos:

1. Inicie sesión en la [consola de AWS Billing and Cost Management y Cost Management](#).
2. En el panel de navegación, seleccione Etiquetas de asignación de costos.
3. En la página de etiquetas de asignación de costes, filtre la etiqueta AppManager CFNStack clave y, a continuación, seleccione la etiqueta de entre los resultados que se muestran.

4. Seleccione Activar.

AWS Cost Explorer

Puede ver un resumen de los costes asociados a la aplicación y a los componentes de la aplicación en la consola de Application Manager mediante la integración con AWS Cost Explorer, que debe activarse primero. Cost Explorer le ayuda a administrar los costos al proporcionarle una visión de los costos y el uso de los recursos de AWS a lo largo del tiempo. Para activar Cost Explorer para la solución:

1. Inicie sesión en la [consola de administración de costos de AWS](#).
2. En el panel de navegación, seleccione Cost Explorer para ver los costos y el uso de la solución a lo largo del tiempo.

Actualización de la solución

Si ya implementó la solución anteriormente, siga este procedimiento para actualizar la CloudFormation pila de soluciones y obtener la versión más reciente del marco de la solución. Antes de actualizar la pila, lea detenidamente [las consideraciones sobre la actualización](#).

1. Inicie sesión en la [CloudFormation consola de AWS](#).
2. Seleccione Stacks en el menú de navegación de la izquierda.
3. Seleccione tu aws-waf-security-automations CloudFormation pila actual.
4. Elija Actualizar.
5. Seleccione Reemplazar la plantilla actual.
6. En Especificar plantilla:
 - a. Seleccione URL de Amazon S3.
 - b. Copia el enlace de aws-waf-security-automations.template [AWS CloudFormation](#).
 - c. Pegue el enlace en el cuadro URL de Amazon S3.
 - d. Compruebe que la URL de la plantilla correcta aparezca en el cuadro de texto URL de Amazon S3.
 - e. Elija Siguiente.
 - f. Vuelva a seleccionar Siguiente.
7. En Parámetros, revise los parámetros de la plantilla y modifíquelos según sea necesario. Consulte el [Paso 1. Lanzar la pila](#) para obtener detalles sobre los parámetros.
8. Elija Siguiente.
9. En la página Configurar opciones de pila, elija Siguiente.
- 10 En la página Revisar, revise y confirme la configuración.
- 11 Seleccione la casilla para confirmar que la plantilla podría crear recursos de IAM.
- 12 Seleccione Ver conjunto de cambios y verifique los cambios.
- 13 Seleccione Crear pila para implementar la pila.

Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debe recibir el estado de UPDATE_COMPLETE en aproximadamente 15 minutos.

Consideraciones sobre la actualización

En las siguientes secciones, se proporcionan restricciones y consideraciones para actualizar esta solución.

Actualización del tipo de recurso

Debe implementar una pila nueva para actualizar el parámetro Endpoint después de crear la pila. No cambie el parámetro de punto final al actualizar la pila.

WAFV2 actualizar

A partir de la versión 3.0, esta solución es compatible con AWS WAFV2. Sustituimos todas las llamadas a la API de [AWS WAF](#) Classic por llamadas a la [API de WAFV2 AWS](#). Esto elimina las dependencias de Node.js y utiliza la mayor parte del tiempo de ejecución de up-to-date Python. Para seguir utilizando esta solución con las funciones y mejoras más recientes, debe implementar la versión 3.0 o superior como una nueva pila.

Personalizaciones durante la actualización de la pila

La out-of-box solución implementa un conjunto de reglas de AWS WAF con configuraciones predeterminadas en su cuenta de AWS con CloudFormation la pila. No recomendamos aplicar personalizaciones a las reglas implementadas por la solución. Las actualizaciones de pila sobrescriben estos cambios. Si necesita reglas personalizadas, le recomendamos que cree reglas independientes fuera de la solución.

Note

Si está actualizando de la versión 3.0 o 3.1 a la versión 3.2 o posterior de esta solución y ha insertado manualmente las direcciones IP en el [conjunto de IP permitidas o denegadas](#), corre el riesgo de perder esas direcciones IP. Para evitar que eso suceda, haga una copia de las direcciones IP del conjunto de IP permitidas o denegadas antes de actualizar la solución. Luego, después de completar la actualización, vuelva a agregar las direcciones IP al conjunto de IP según sea necesario. Consulte los comandos [get-ip-set](#) y [update-ip-set](#) CLI. Si ya utiliza la versión 3.2 o posterior, ignore este paso.

Desinstalar la solución

Para desinstalar la solución, elimine las CloudFormation pilas:

1. Inicie sesión en la [CloudFormation consola de AWS](#).
2. Seleccione la pila principal de la solución. Todas las demás pilas de soluciones se eliminarán automáticamente.
3. Elija Eliminar.

Note

Al desinstalar la solución, se eliminan todos los recursos de AWS que utiliza la solución, excepto los buckets de Amazon S3. Si algunos conjuntos de direcciones IP no se eliminan debido a un problema de limitación provocado por las [cuotas de las API WAF de AWA](#), elimine esos conjuntos de direcciones IP manualmente y, a continuación, elimine la pila.

Usa la solución

En esta sección se proporcionan instrucciones detalladas para usar la solución después de implementarla.

Modifique los conjuntos de IP permitidos y denegados (opcional)

Tras implementar la CloudFormation pila de esta solución, puede modificar manualmente los conjuntos de IP permitidos y denegados para añadir o eliminar direcciones IP según sea necesario.

1. Inicie sesión en la consola [AWS WAF](#).
2. En el panel de navegación izquierdo, elija IP Sets.
3. Elija el conjunto de direcciones IP en la lista de direcciones permitidas y añada direcciones IP de fuentes confiables.
4. Elija el conjunto de IP para la lista de denegados y añada las direcciones IP que desee bloquear.

Inserte el enlace de Honeypot en su aplicación web (opcional)

[Si eligió yes el parámetro Activar Bad Bot Protection en el paso 1. Al lanzar la pila](#), la CloudFormation plantilla crea un punto final de captura para un honeypot de producción de baja interacción. El objetivo de esta trampa es detectar y desviar las solicitudes entrantes procedentes de rastreadores de contenido y bots maliciosos. Los usuarios válidos no intentarán acceder a este punto final.

Sin embargo, los robots y los rastreadores de contenido, como el malware que busca vulnerabilidades de seguridad y rastrea direcciones de correo electrónico, podrían intentar acceder al punto final trampa. En este escenario, la función `Access Handler Lambda` inspecciona la solicitud para extraer su origen y, a continuación, actualiza la regla de AWS WAF asociada para bloquear las solicitudes posteriores de esa dirección IP.

Utilice uno de los siguientes procedimientos para incrustar el enlace del honeypot para las solicitudes de una CloudFront distribución o de un ALB.

Cree un CloudFront origen para el punto final de Honeypot

Utilice este procedimiento para las aplicaciones web que se despliegan con una CloudFront distribución. Con él CloudFront, puede incluir un `robots.txt` archivo que ayude a identificar los

robots y los rastreadores de contenido que ignoran el estándar de exclusión de robots. Complete los siguientes pasos para incrustar el enlace oculto y, a continuación, prohibirlo explícitamente en su archivo. `robots.txt`

1. Inicie sesión en la [CloudFormation consola de AWS](#).
2. Elija la pila que creó en el [paso 1. Lanza la pila](#)
3. Elija la pestaña Salidas.
4. Desde la `BadBotHoneypotEndpoint`, copia la URL del punto final. Contiene dos componentes que necesita para completar este procedimiento:
 - El nombre del host del punto final (por ejemplo, `xxxxxxxxxx.execute-api.region.amazonaws.com`)
 - El URI de la solicitud (`/ProdStage`)
5. Inicia sesión en la [CloudFront consola de Amazon](#).
6. Elige la distribución que quieres usar.
7. Elija Distribution Settings (Configuración de distribución).
8. En la pestaña Origins (Orígenes), elija Create Origin (Crear origen).
9. En el campo Nombre de dominio de origen, pegue el componente del nombre de host de la URL del punto final que copió en el [paso 2. Asocie la ACL web a su aplicación web](#).
10. En Origin Path, pega la URL de la solicitud que también copiaste en el [paso 2. Asocie la ACL web a su aplicación web](#).
11. Acepte los valores predeterminados para los demás campos.
12. Seleccione Crear.
13. En la pestaña Behaviors (Comportamientos), elija Create Behavior (Crear comportamiento).
14. Cree un nuevo comportamiento de caché y apúntelo al nuevo origen. Puedes usar un dominio personalizado, como un nombre de producto falso que sea similar a otro contenido de tu aplicación web.
15. Inserta este enlace de punto final en tu contenido que apunte al honeypot. Oculta este enlace a tus usuarios humanos. Como ejemplo, consulta el siguiente ejemplo de código:

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

 Note

Es tu responsabilidad comprobar qué valores de etiquetas funcionan en el entorno de tu sitio web. No los utilices `rel="nofollow"` si tu entorno no los respeta. Para obtener más información sobre la configuración de las metaetiquetas de los robots, consulta la [guía para desarrolladores de Google](#).

16 Modifica el `robots.txt` archivo de la raíz de tu sitio web para impedir de forma explícita el enlace del honeypot, de la siguiente manera:

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

Inserte el punto final de Honeypot como un enlace externo

Utilice este procedimiento para las aplicaciones web que se implementan con un ALB.

1. Inicie sesión en la [CloudFormation consola de AWS](#).
2. Elija la pila que creó en el [paso 1. Lance la pila](#).
3. Elija la pestaña Salidas.
4. De la `BadBotHoneypotEndpoint` clave, copia la URL del punto final.
5. Inserte este enlace de punto final en el contenido de su web. Usa la URL completa que copiaste en el [paso 2. Asocie la ACL web a su aplicación web](#). Oculte este enlace a sus usuarios humanos. Como ejemplo, consulta el siguiente ejemplo de código:

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

 Note

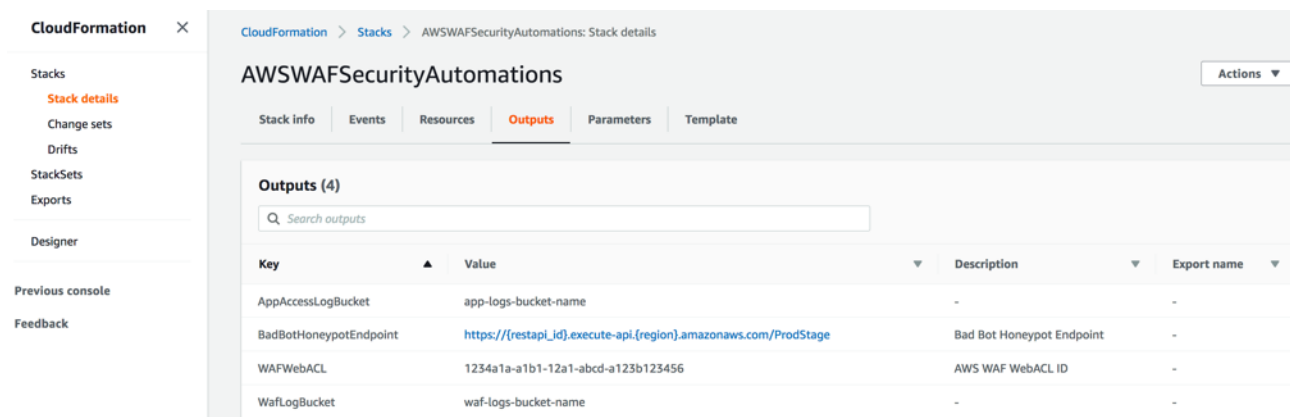
Este procedimiento se utiliza `rel=nofollow` para indicar a los robots que no accedan a la URL del honeypot. Sin embargo, dado que el enlace está incrustado externamente, no puedes incluir un `robots.txt` archivo para rechazar el enlace de forma explícita. Es tu responsabilidad comprobar qué etiquetas funcionan en el entorno de tu sitio web. No las utilices `rel="nofollow"` si tu entorno no las observa.

Utilice el archivo JSON del analizador de registros Lambda

Utilice el archivo JSON del analizador de registros Lambda para la protección contra inundaciones HTTP

Si ha elegido el parámetro Yes - AWS Lambda log parser de plantilla Activar protección contra inundaciones HTTP, esta solución crea un archivo de configuración denominado `<stack_name>-waf_log_conf.json` y lo carga en el bucket de Amazon S3 que se utiliza para almacenar los archivos de registro de AWS WAF. Para encontrar el nombre del bucket, consulte la `WafLogBucket` variable del resultado. CloudFormation En la siguiente figura se muestra un ejemplo.

Captura de pantalla que muestra una pantalla denominada AWSWAFSecurity Automatizaciones y que muestra cuatro salidas



Key	Value	Description	Export name
AppAccessLogBucket	app-logs-bucket-name	-	-
BadBotHoneyPotEndpoint	https://[restapi_id].execute-api.[region].amazonaws.com/ProdStage	Bad Bot HoneyPot Endpoint	-
WAFWebACL	1234a1a-a1b1-12a1-abcd-a123b123456	AWS WAF WebACL ID	-
WafLogBucket	waf-logs-bucket-name	-	-

Si edita y sobrescribe el `<stack_name>-waf_log_conf.json` archivo en Amazon S3, la función Log Parser Lambda tendrá en cuenta los nuevos valores al procesar los nuevos archivos de registro de AWS WAF. A continuación se muestra un ejemplo de archivo de configuración:

Captura de pantalla de un ejemplo de archivo de configuración

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

Los parámetros incluyen los siguientes:

- General:
 - Umbral de solicitudes (obligatorio): el número máximo de solicitudes aceptables por cada cinco minutos y por dirección IP. Esta solución utiliza el valor que defina al aprovisionar o actualizar la CloudFormation pila.
 - Período de bloqueo (obligatorio): el período (en minutos) para bloquear las direcciones IP aplicables. Esta solución utiliza el valor que usted define al aprovisionar o actualizar la CloudFormation pila.
 - Sufijos ignorados: las solicitudes que acceden a este tipo de recurso no se tienen en cuenta para el umbral de solicitudes. De forma predeterminada, esta lista está vacía.
- Lista de direcciones URL: utilícela para definir un umbral de solicitud personalizado y un período de bloqueo para datos específicos URLs. De forma predeterminada, esta lista está vacía.

Cuando los registros WAF lleguen al WafLogBucket, la función de analizador de registros de Lambda los procesará utilizando las configuraciones del archivo de configuración. La solución escribe el resultado en un archivo de salida nombrado `<stack_name>-waf_log_out.json` en el mismo depósito. Si el archivo de salida contiene una lista de las direcciones IP identificadas como atacantes, la solución las añade a la IP de WAF configurada para HTTP Flood y se bloquea el acceso a la aplicación. Si los archivos de salida no tienen direcciones IP, compruebe si el archivo de configuración es válido o si se ha superado el límite de velocidad según el archivo de configuración.

Utilice el archivo JSON del analizador de registros Lambda para proteger el escáner y la sonda

Si ha elegido el parámetro Yes - AWS Lambda log parser de plantilla Activate Scanner & Probe Protection, esta solución crea un archivo de configuración denominado `<stack_name>-app_log_conf.json` y lo carga en el bucket de Amazon S3 definido que se utiliza para almacenar CloudFront los archivos de registro de Application Load Balancer.

Si edita y sobrescribe `<stack_name>-app_log_conf.json` en Amazon S3, la función Log Parser Lambda tendrá en cuenta los nuevos valores al procesar los nuevos archivos de registro de AWS WAF. A continuación se muestra un ejemplo de archivo de configuración:

Captura de pantalla del archivo de configuración

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

Los parámetros incluyen los siguientes:

- General:
 - Umbral de error (obligatorio): el número máximo aceptable de solicitudes incorrectas por minuto y por dirección IP. Esta solución usa el valor que definiste al aprovisionar o actualizar la CloudFormation pila.
 - Período de bloqueo (obligatorio): el período (en minutos) para bloquear las direcciones IP aplicables. Esta solución usa el valor que definiste al aprovisionar o actualizar la CloudFormation pila.
 - Códigos de error: el código de estado devuelto se considera un error. De forma predeterminada, la lista considera errores los siguientes códigos de estado HTTP: 400 (Bad Request) 401 (Unauthorized) 403 (Forbidden), 404 (Not Found), y 405 (Method Not Allowed).

- Lista de URI: utilícela para definir un umbral de solicitud personalizado y un período de bloqueo para datos específicos. URLs De forma predeterminada, esta lista está vacía.

Cuando los registros de acceso a las aplicaciones llegan al AppAccessLogBucket, la función Log Parser Lambda los procesa mediante las configuraciones del archivo de configuración. La solución escribe el resultado en un archivo de salida denominado `<stack_name>-app_log_out.json` en el mismo depósito. Si el archivo de salida contiene una lista de las direcciones IP identificadas como atacantes, la solución las añade al conjunto de IP WAF para Scanner & Probe e impide que accedan a la aplicación. Si los archivos de salida no tienen direcciones IP, compruebe si el archivo de configuración es válido o si se ha superado el límite de velocidad según el archivo de configuración.

Utilice el país y el URI en el analizador de registros de HTTP Flood Athena

Puede agrupar por IPs país y URI en la consulta de Athena para detectar y bloquear los ataques de inundación HTTP que tienen patrones de URI impredecibles. Para ello, seleccione una de las opciones (Country,URI,Country and URI) del parámetro Agrupar por solicitudes en HTTP Flood Athena Query al [lanzar la pila](#).

También puede introducir un umbral de solicitud por país mediante el parámetro Umbral de solicitud por país. Por ejemplo, {"TR": 50, "ER": 150}. La solución utiliza estos umbrales en las solicitudes originadas en estos países específicos. La solución utiliza el umbral predeterminado en las solicitudes de otros países.

Note

Si define un umbral por país, la solución incluye automáticamente el país en la cláusula de agrupamiento por consulta de Athena. [Para obtener más información, consulte la tabla de parámetros del paso 1. Lance la pila.](#)

De forma predeterminada, la solución cuenta el umbral de solicitud en un período de cinco minutos. Esto se puede configurar con el parámetro Athena Query Run Time Schedule (Minute).

Note

La consulta de Athena calcula el umbral por minuto dividiendo el umbral de solicitud por el período de tiempo. Por ejemplo:

Umbral de solicitud (umbral predeterminado o umbral por país): 100

Cronograma de tiempo de ejecución de Athena Query: 5

Umbral de solicitudes por minuto: $20 = 100 / 5$

Ver las consultas de Amazon Athena

Si ha seleccionado Yes - Amazon Athena log parser los parámetros de plantilla Activar HTTP Flood Protection o Activar Scanner & Probe Protection, esta solución crea y ejecuta consultas de Athena para registros de ALB (ScannersProbesLogParser) CloudFront o AWS WAF (HTTPFloodLogParser), analiza el resultado y actualiza AWS WAF en consecuencia.

Para mejorar el rendimiento y mantener los costes bajos, la solución divide los registros en función de las marcas de tiempo de los nombres de los archivos. La solución genera consultas de Athena de forma dinámica para usar claves de partición (año, mes, día y hora). De forma predeterminada, las consultas se ejecutan cada cinco minutos. Puede configurar sus programas de ejecución cambiando el valor del parámetro de plantilla Athena Query Run Time Schedule (Minute). Cada ejecución de consulta escanea los datos de las últimas cuatro o cinco horas de forma predeterminada. Puede configurar la cantidad de datos que escanea una consulta cambiando el valor del parámetro de plantilla WAF Block Period. La solución también coloca las consultas en grupos de trabajo separados para administrar el acceso y los costos de las consultas.

Note

Compruebe que Athena esté configurada para acceder al catálogo de datos de AWS Glue. Esta solución crea el catálogo de datos de registros de acceso en AWS Glue y configura una consulta de Athena para procesar los datos. Si Athena no está configurada correctamente, la consulta no se ejecuta. Para obtener más información, consulte [Actualización al catálogo de datos de AWS Glue más reciente step-by-step](#).

Utilice el siguiente procedimiento para ver estas consultas:

Vea las consultas de registro de WAF

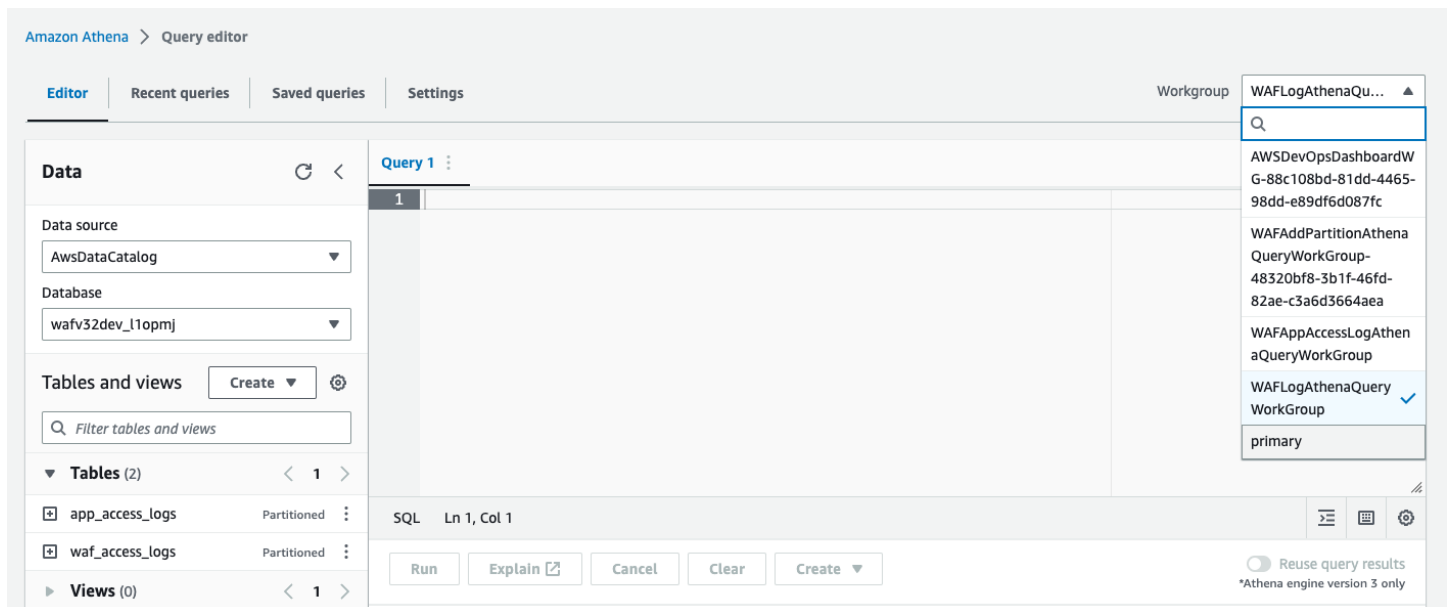
1. Inicia sesión en la consola de [Amazon Athena](#).
2. Elija Iniciar editor de consultas.
3. Seleccione la base de datos para esta solución.
4. Seleccione una opción WAFLogAthenaQueryWorkGroup de la lista desplegable.

Note

Este grupo de trabajo solo existe si seleccionó el parámetro Yes - Amazon Athena log parser de plantilla Activar la protección contra inundaciones HTTP.

5. Elija Cambiar para cambiar el grupo de trabajo.

Captura de pantalla del editor de consultas de Athena que no muestra consultas



1. Seleccione la pestaña Historial.
2. Seleccione y abra SELECT consultas de la lista.

Vea las consultas del registro de acceso a las aplicaciones

1. Inicia sesión en la consola de [Amazon Athena](#).

2. Seleccione la pestaña Grupo de trabajo.
3. Seleccione WAFAppAccessLogAthenaQueryWorkGroup en la lista.

 Note

Este grupo de trabajo solo existe si seleccionó el parámetro Yes - Amazon Athena log parser de plantilla Activar la protección de escáneres y sondas.

4. Seleccione Cambiar grupo de trabajo.
5. Seleccione la pestaña Consultas recientes.
6. Seleccione y abra SELECT las consultas de la lista.

Ver cómo añadir consultas de particiones de Athena

1. Inicia sesión en la consola de [Amazon Athena](#).
2. Seleccione la pestaña Grupo de trabajo.
3. Seleccione WAFAddPartitionAthenaQueryWorkGroup en la lista.

 Note

Este grupo de trabajo solo existe si ha seleccionado los parámetros Yes - Amazon Athena log parser de plantilla Activar HTTP Flood Protection o Activar Scanner & Probe Protection.

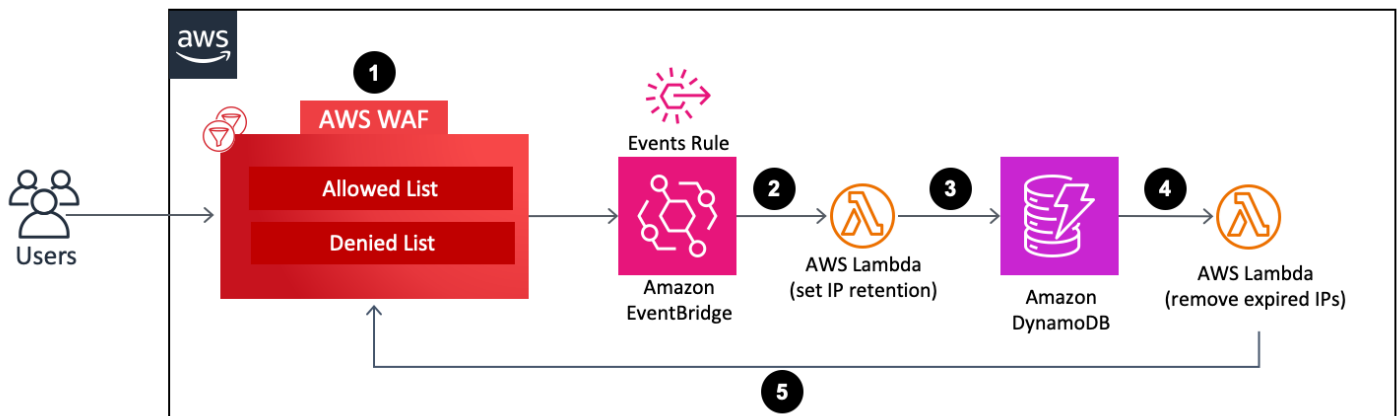
4. Seleccione Cambiar grupo de trabajo.
5. Seleccione la pestaña Historial.
6. Seleccione y abra ALTER TABLE consultas de la lista. Estas consultas se ejecutan cada hora para añadir una nueva partición horaria a la tabla de Athena.

Configurar la retención de IP en los conjuntos de IP de AWS WAF permitidos y denegados

Puede configurar la retención de IP en los conjuntos de IP de AWS WAF permitidos y denegados que cree la solución. En las siguientes secciones se explica cómo funciona y se proporcionan los pasos para configurarlo.

Funcionamiento

Diagrama de arquitectura que muestra las listas de permitidos y denegados de AWS WAF y otros recursos de AWS



1. Cuando un usuario actualiza (añade o elimina una dirección IP) el conjunto de IP de WAF permitidas o denegadas, esta acción invoca una llamada a la API de AWS UpdateIPSet WAF y crea un evento.
2. Una regla de EventBridge eventos de [Amazon](#) detecta los eventos en función de un patrón de eventos predefinido e invoca una función Lambda para establecer el período de retención de todas las direcciones IP que existen en el conjunto de IP después de la actualización.
3. La función Lambda procesa los eventos, extrae los datos relevantes para la retención de IP (como el nombre del conjunto de IP, el ID, el alcance y las direcciones IP) y los inserta en una tabla de DynamoDB. También inserta un ExpirationTime atributo para cada elemento de DynamoDB. La solución calcula el tiempo de caducidad añadiendo un período de retención definido por el usuario a la hora del evento. La tabla tiene [activados DynamoDB Streams](#) y [Time to Live \(TTL\)](#). El atributo TTL es. ExpirationTime
4. Cuando un elemento llega a su fecha de caducidad, se invoca el TTL y DynamoDB lo elimina de la tabla después de esa fecha. Tras la eliminación del elemento, el elemento eliminado se añade al flujo de DynamoDB, que invoca una función Lambda para el procesamiento posterior.
5. La función Lambda obtiene la información sobre el elemento eliminado de la transmisión de DynamoDB y realiza una llamada a la API de AWS WAF para eliminar las direcciones IP caducadas incluidas en el elemento del conjunto de IP de AWS WAF de destino.

Active la retención de IP

Sigue estos pasos para activar la retención de IP:

1. En la pila de Cloudformation que vaya a [implementar](#) o [actualizar](#), introduzca el período de retención de IP (minutos) para el conjunto de IP permitido y el período de retención de IP (minutos) para el conjunto de IP denegado. El período mínimo de retención es de 15 minutos. La solución trata cualquier número comprendido entre 0 y 15 como 15. Para obtener más información sobre la configuración de la implementación, consulte el [paso 1. Lance la pila](#).
2. Introduzca una dirección de correo electrónico si desea recibir una notificación por correo electrónico cuando se eliminen direcciones IP caducadas del conjunto de IP de AWS WAF. Si decide recibir una notificación por correo electrónico, debe confirmar la suscripción mediante el enlace que aparece en el correo electrónico que reciba una vez que la solución se haya implementado correctamente. Para obtener más información sobre la configuración de la implementación, consulte el [paso 1. Lance la pila](#).
3. Actualice el conjunto de IP de AWS WAF añadiendo o eliminando direcciones IP. Esto inicia el proceso de retención de IP y crea un elemento de DynamoDB, que incluye una lista de caducidad de IP. Esta lista de caducidad consta de las direcciones IP que existen en el conjunto de IP de AWS WAF después de actualizarlo.
4. Una vez que el elemento de DynamoDB alcanza su fecha de caducidad y se elimina de la tabla, la solución elimina las direcciones IP incluidas en la lista de caducidad de IP del elemento del conjunto de direcciones IP del WAF.

Note

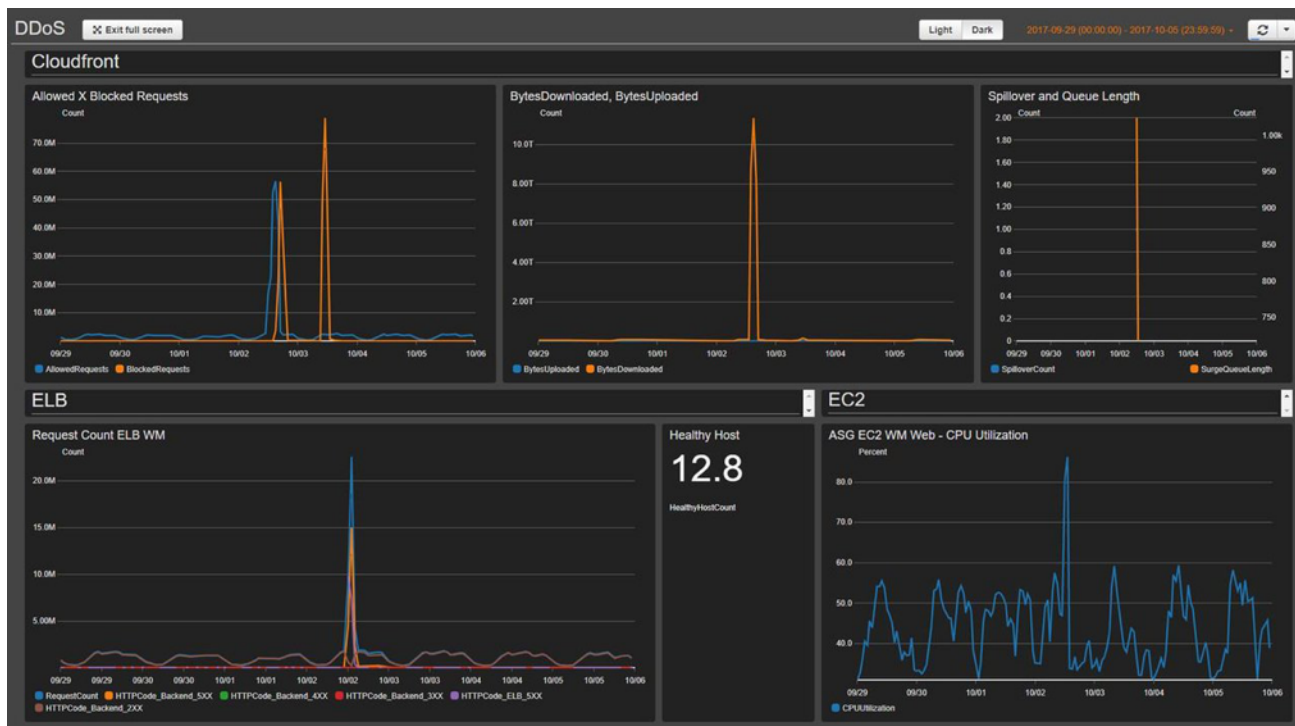
Según el momento en que DynamoDB elimine un elemento caducado por TTL, la operación de eliminación real de una dirección IP caducada del conjunto de IP de AWS WAF puede variar. La eliminación de TTL de DynamoDB depende principalmente del tamaño y el nivel de actividad de una tabla. Se espera un retraso en la operación de eliminación de AWS WAF debido a la posible demora en la operación de eliminación de DynamoDB. En general, la solución elimina las direcciones IP caducadas del conjunto de direcciones IP de AWS WAF poco después de eliminar el TTL de DynamoDB. Para obtener más información, consulte [DynamoDB Time to Live \(TTL\) en la Guía para](#) desarrolladores de Amazon DynamoDB.

Cree un panel de monitoreo

AWS recomienda configurar un sistema de monitoreo de referencia personalizado para cada punto final crítico. Para obtener información sobre la creación y el uso de vistas de métricas personalizadas, consulte [CloudWatch Dashboards: Create & Use Customized Metrics Views](#) y [Using Amazon CloudWatch dashboards](#).

En la siguiente captura de pantalla del panel, se muestra un ejemplo de un sistema de monitoreo de referencia personalizado.

Captura de pantalla del CloudFront panel



El panel muestra las siguientes métricas:

- Solicitudes permitidas o bloqueadas: muestra si recibes un aumento en el acceso permitido (el doble del pico de acceso normal) o en el acceso bloqueado (cualquier período en el que se identifiquen más de 1000 solicitudes bloqueadas). CloudWatch envía una alerta a un canal de Slack. Puedes usar esta métrica para rastrear los ataques DDoS conocidos (cuando aumentan las solicitudes bloqueadas) o una nueva versión de un ataque (cuando las solicitudes pueden acceder al sistema).

 Note

Nota: La solución proporciona esta métrica.

- BytesDownloaded vs Uploaded: ayuda a identificar cuándo un ataque DDoS se dirige a un servicio que normalmente no recibe una gran cantidad de acceso para agotar los recursos (por ejemplo, un componente de un motor MBs de búsqueda que envía información para un conjunto de parámetros de solicitud específico).
- Extensión del ELB y longitud de la cola: ayuda a comprobar si un ataque DDoS está causando daños a la infraestructura y si el atacante está eludiendo la capa de CloudFront AWS WAF y atacando directamente recursos desprotegidos.
- Recuento de solicitudes del ELB: ayuda a identificar los daños en la infraestructura. Esta métrica muestra si el atacante está eludiendo la capa de protección o si se debe revisar una regla de CloudFront caché para aumentar la tasa de aciertos de la caché.
- ELB Healthy Host: puede utilizarla como otra métrica de comprobación del estado del sistema.
- Utilización de la CPU ASG: ayuda a identificar si el atacante está eludiendo CloudFront AWS WAF y Elastic Load Balancing. También puede usar esta métrica para identificar el daño de un ataque.

Gestiona los falsos positivos de XSS

Esta solución configura una regla de AWS WAF que inspecciona los elementos más explorados de las solicitudes entrantes para identificar y bloquear los ataques XSS. Este patrón de detección es menos eficaz si su carga de trabajo permite a los usuarios legítimos redactar y enviar HTML, por ejemplo, mediante un editor de texto enriquecido en un sistema de administración de contenido. En este escenario, considere la posibilidad de crear una regla de excepción que omita la regla XSS predeterminada para patrones de URL específicos que acepten la entrada de texto enriquecido e implemente mecanismos alternativos para proteger a los excluidos. URLs

Además, algunos formatos de imágenes o datos personalizados pueden provocar falsos positivos porque contienen patrones que indican un posible ataque XSS en el contenido HTML. Por ejemplo, un archivo SVG puede contener una etiqueta. `<script>` Si espera que este tipo de contenido provenga de usuarios legítimos, ajuste sus reglas de XSS para permitir solicitudes HTML que incluyan estos otros formatos de datos.

Complete los siguientes pasos para actualizar la regla XSS y excluir las URLs que aceptan HTML como entrada. Consulte la [Guía para desarrolladores de Amazon WAF](#) para obtener instrucciones detalladas.

1. Inicie sesión en la consola [AWS WAF](#).
2. [Cree una coincidencia de cadena o una condición de expresión regular](#).
3. Configure los ajustes del filtro para inspeccionar el URI y enumerar los valores que desee aceptar según la regla XSS.
4. Edite la regla XSS de esta solución y [añada la nueva condición](#) que ha creado.

Por ejemplo, para excluir todos los elementos URLs de la lista, elija lo siguiente para Cuando haya una solicitud:

- no
- coincide con al menos uno de los archivadores en la condición de coincidencia de cadenas
- Lista de permitidos de XSS

Solución de problemas

Si necesita ayuda con esta solución, póngase en contacto con Support para abrir un caso de soporte para esta solución.

Contacto con Support

Si cuenta con [AWS Developer Support](#), [AWS Business Support](#) o [AWS Enterprise Support](#), puede utilizar el Centro de soporte para obtener asistencia de expertos con esta solución. En las siguientes secciones, encontrará instrucciones.

Cree un caso

1. Abra [Support Center](#).
2. Seleccione Crear caso.

¿Cómo podemos ayudar?

1. Elija Técnico.
2. En Servicio, seleccione WAF o AWS WAF.
3. Para la categoría, seleccione Automatizaciones de seguridad de WAF o Automatizaciones de seguridad para AWS WAF.
4. En cuanto a la gravedad, es la opción que mejor se adapte a su caso de uso.
5. Al introducir el servicio, la categoría y la gravedad, la interfaz rellena los enlaces a las preguntas de solución de problemas más frecuentes. Si no puede resolver su pregunta con estos enlaces, seleccione Siguiente paso: información adicional.

Información adicional

1. En Asunto, introduce un texto que resuma tu pregunta o problema.
2. En Descripción, describe el problema en detalle.
3. Selecciona Adjuntar archivos.
4. Adjunte la información que Support necesita para procesar la solicitud.

Ayúdenos a resolver su caso más rápido

1. Introduzca la información solicitada.
2. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.

Resuelva ahora o póngase en contacto con nosotros

1. Revise las soluciones Solve now.
2. Si no puede resolver su problema con estas soluciones, elija Contactar con nosotros, introduzca la información solicitada y pulse Enviar.

Guía para desarrolladores

En esta sección se proporciona el código fuente de la solución.

Código fuente

Visite nuestro [GitHub repositorio](#) para descargar las plantillas y los scripts de esta solución y compartir sus personalizaciones con otras personas.

Referencia

Esta sección incluye información sobre una función opcional para recopilar métricas únicas para esta solución, sugerencias sobre [los recursos relacionados](#) y una [lista de los desarrolladores](#) que han contribuido a esta solución.

Recopilación de datos anonimizados

Esta solución incluye una opción para enviar métricas operativas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. Cuando está activada, la solución recopila la siguiente información y la envía a AWS durante la implementación inicial de la CloudFormation plantilla:

- ID de solución: el identificador de la solución de AWS
- ID único (UUID): identificador único generado aleatoriamente para cada implementación de esta solución
- Marca de tiempo: marca de tiempo de recopilación de datos
- Configuración de la solución: funciones activadas y parámetros establecidos durante el lanzamiento inicial
- Ciclo de vida: cuánto tiempo usó el cliente esta solución (según la eliminación de la pila)
- Registre los datos del analizador:
 - El número de direcciones IP del conjunto de IP de Scanner & Probe y de la IP de inundación HTTP configuradas para bloquear
 - El número de solicitudes procesadas y bloqueadas
- La IP muestra los datos del analizador:
 - El número de direcciones IP del conjunto de direcciones IP de la lista de reputación
 - El número de solicitudes procesadas y bloqueadas
- Acceda a los datos del controlador:
 - El número de direcciones IP del conjunto de direcciones IP de Bad Bot
 - El número de solicitudes procesadas y bloqueadas
- Datos de retención de IP: número de direcciones IP caducadas que se van a eliminar del conjunto de direcciones IP permitidas o denegadas

AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta a la [Política de privacidad de AWS](#). Para excluirse de esta función, complete los siguientes pasos antes de lanzar la CloudFormation plantilla de AWS.

1. Descargue `aws-waf-security-automations.template` [AWS CloudFormation](#) en su disco duro local.
2. Abra la CloudFormation plantilla con un editor de texto.
3. Modifique la sección CloudFormation de mapeo de plantillas desde:

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

a:

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

4. Inicie sesión en la [CloudFormation consola de AWS](#).
5. Elija Crear pila.
6. En la página Crear pila, en la sección Especificar plantilla, seleccione Cargar un archivo de plantilla.
7. En Cargar un archivo de plantilla, seleccione Elegir archivo y después seleccione la plantilla editada de su unidad local.
8. Seleccione Siguiente y siga los pasos del [paso 1. Lance la pila](#).

Recursos relacionados

Documentos técnicos de AWS asociados

- [Prácticas recomendadas de AWS para DDo la resiliencia](#)

Publicaciones del blog de seguridad de AWS asociadas

- [Cómo evitar los enlaces directos mediante AWS WAF, CloudFront Amazon y Referer Checking](#)

Listas de reputación de IP de terceros

- [Sitio web de Spamhaus DROP List](#)
- [Lista de direcciones IP de amenazas emergentes de Proofpoint](#)
- [Lista de nodos de salida de Tor](#)

Colaboradores

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

Revisiones

Fecha de publicación: septiembre de 2016

Visita [ChangeLog.md](#) en nuestro GitHub repositorio para realizar un seguimiento de las mejoras y correcciones específicas de cada versión.

Avisos

Esta guía de implementación se proporciona únicamente con fines informativos. Representa las ofertas y prácticas actuales de los productos de AWS en la fecha de publicación de este documento, que están sujetas a cambios sin previo aviso. Los clientes son responsables de realizar su propia evaluación independiente de la información de este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se proporciona «tal cual» sin garantía de ningún tipo, ya sea expresa o implícita. Este documento no crea ninguna garantía, declaración, compromiso contractual, condición o garantía por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

La solución Security Automations for AWS WAF se licencia según los términos de [la licencia Apache versión 2.0](#).

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.