Guía de implementación

Automatizaciones de seguridad para AWS WAF

Automatizaciones de seguridad para AWS WAF: Guía de implementación

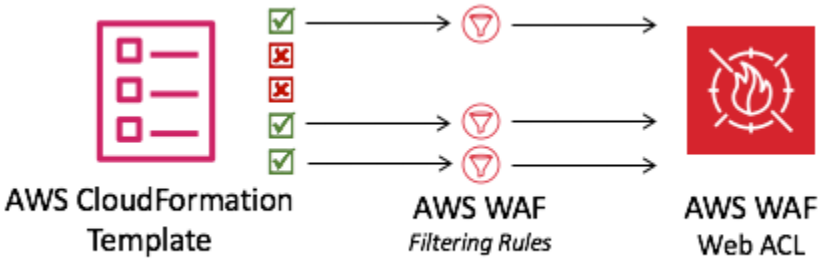
Table of Contents

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

Fecha de publicación: septiembre de 2016 (última actualización: diciembre de 2024)

La AWS WAF solución Security Automations for implementa un conjunto de reglas preconfiguradas para ayudarlo a proteger sus aplicaciones de los ataques web más comunes. El servicio principal de esta solución 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. AWS WAF Puede utilizarlas AWS WAF para definir reglas de seguridad web personalizables. Estas reglas controlan qué tráfico se debe permitir o bloquear hacia las aplicaciones web y las interfaces de programación de aplicaciones (APIs) desplegadas en AWS recursos como Amazon CloudFront, Application Load Balancer (ALB) y Amazon API Gateway. Para obtener más tipos de recursos compatibles, consulte AWS WAFla AWS WAF guía para AWS Shield Advanced desarrolladores y la guía para desarrolladores. AWS Firewall Manager

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



Configuración de la web AWS WAF ACL

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 AWS seguridad, procesamiento, almacenamiento y otros servicios necesarios para implementar esta solución AWS, utilizando las AWS mejores prácticas de seguridad y disponibilidad.

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

> **Note**
>
> A partir de la versión 3.0.0, esta solución es compatible con la última versión del AWS WAF servicio API (AWS WAF V2).

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 AWS WAF reglas. Puede personalizar el código fuente, añadir nuevas reglas personalizadas y aprovechar más reglas AWS WAF administradas 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 coste 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

Si quiere…	Lea…
Conozca cuáles Regiones de AWS son compatibles con esta solución.	Soportado Regiones de AWS
Vea o descargue la CloudFormation plantilla incluida en esta solución para implementar automáticamente los recursos de infraestr uctura (la «pila») de esta solución.	AWS CloudFormation plantilla
Se utiliza Support para ayudarle a implementar, usar o solucionar problemas de la solución.	Support
Acceda al código fuente y, si lo desea, utilícelo AWS Cloud Development Kit (AWS CDK) para implementar la solución	GitHubrepositorio

Características y ventajas

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

Proteja sus aplicaciones web con grupos de Reglas administradas de AWS reglas

Reglas administradas de AWS para brindar AWS WAF protección contra las vulnerabilidades comunes de las aplicaciones u otro tipo de tráfico no deseado. Esta solución incluye grupos de reglas de reputación de IP AWSAWS gestionados, grupos de reglas de referencia gestionados y grupos de reglas AWS gestionados específicos para casos de uso. Tiene la opción de seleccionar uno o más grupos de reglas para su webACL, hasta la cuota máxima de unidades ACL de capacidad web. WCU

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

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

- AWS WAF regla basada en tasas
- 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 requerida por las reglas basadas en tasas. 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 HTTP inundación que tienen patrones impredeciblesURI. Para obtener más información, consulte Usar el país y URI en el analizador de registros HTTP Flood Athena.

Bloquee el aprovechamiento de las vulnerabilidades con una regla personalizada predefinida para 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 que procedan 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)

Las reglas personalizadas de las listas de reputación de IP comprueban 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 de IP manual con una regla personalizada de listas de IP permitidas y denegadas predefinidas

Las reglas personalizadas de las listas de direcciones 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 de control personalizado para visualizar estas métricas y obtener información sobre el patrón de los ataques y la protección que ofrecen. AWS WAF Para obtener más información, consulte el panel de monitoreo de Build.

Integre con Service Catalog AppRegistry y AWS Systems Manager Application Manager

Esta solución incluye un AppRegistry recurso de Service Catalog 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

Fecha de publicación: septiembre de 2016 (última actualización: mayo de 2023)

Los siguientes son 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 AWS WAF reglas

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

Personalice la capa 7: protección contra HTTP inundaciones

Esta solución ofrece tres opciones para activar la protección contra HTTP inundaciones. Puede seleccionar la opción que mejor se adapte a sus necesidades para protegerse contra DDoS los ataques. Para obtener más información, consulte Proporcionar protección contra inundaciones de nivel 7 con una regla personalizada de HTTP inundación 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 utilizar AWS WAF y otros servicios para crear automatizaciones de seguridad en el. 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 utiliza registros para el ALB recurso. 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 AWS WAF inspeccionar o ALB registra si el usuario CloudFront así lo decide `yes - Amazon Athena log parser` al activar la regla de protección contra HTTP inundaciones o la regla de protección de escáneres y sondas.

AWS WAF regla

Una AWS WAF regla define:

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

Las reglas se definen solo en el contexto de un grupo de reglas o una webACL.

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 direcciones 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 AWS recursos.

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 Lamba inicia una inspección o ALB registra los AWS WAF registros si el usuario CloudFront así lo decide `yes – AWS Lambda log parser` al activar la regla de protección contra HTTP inundaciones o la regla de protección de escáneres y sondas.

Grupos de reglas gestionados

Los grupos de reglas gestionados son conjuntos de ready-to-use reglas predefinidas que AWS AWS Marketplace los vendedores redactan y mantienen por ti. AWS WAF Los precios se aplican al uso de cualquier grupo de reglas gestionado.

tipo de recurso/punto final

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

Registros de WAF

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

WCU

AWS WAF utiliza las unidades de capacidad de la lista de control de acceso web (WCUs) para calcular y controlar los recursos operativos necesarios para ejecutar las reglas, los grupos de reglas y la webACLs. ACL AWS WAF aplica WCU cuotas al configurar los grupos de reglas y la webACLs. WCUsno afectan a la forma en que AWS WAF inspecciona el tráfico web.

web ACL

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

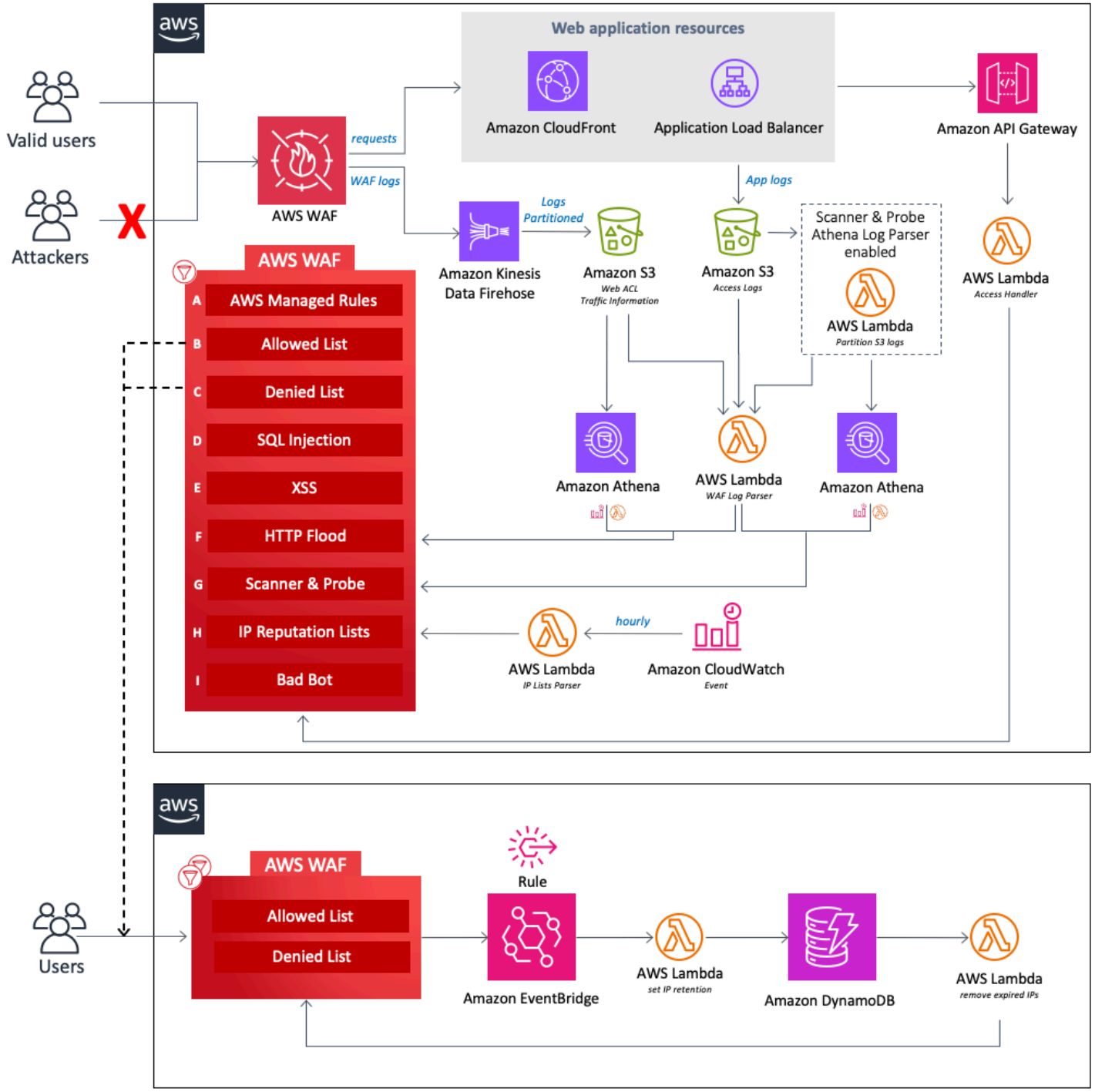
> **Note**
>
> Para obtener una referencia general de AWS términos, consulte el glosario.AWS

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.



Automatizaciones de seguridad para AWS WAF la arquitectura en AWS

En el centro del diseño se encuentra una AWS WAFwebACL, 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 activar. Cada componente funciona de forma independiente y añade reglas diferentes a la webACL.

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

> **Note**
>
> Las etiquetas de grupo no reflejan el nivel de prioridad de las WAF reglas.

- AWS Reglas administradas (A): este componente contiene grupos de reglas de reputación Reglas administradas de AWS IP, grupos de reglas de referencia y grupos de reglas específicos para casos de uso. Estos grupos de reglas protegen contra la explotación de las vulnerabilidades comunes de las aplicaciones u otro tipo de tráfico no deseado, incluidos los que se describen en OWASPlas publicaciones, sin tener que escribir sus propias reglas.
- Listas de IP manuales (B y C): estos componentes crean dos AWS WAF reglas. 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 permitidos y denegados AWS WAF.
- SQLInyección (D) y XSS (E): estos componentes configuran dos AWS WAF reglas diseñadas para proteger contra los patrones comunes de SQL inyección o secuencias de comandos entre sitios (XSS) en la URI cadena de consulta o el cuerpo de una solicitud.
- HTTPInundación (F): este componente protege contra los ataques que consisten en un gran número de solicitudes desde una dirección IP determinada, como un DDoS ataque a una 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 AWS WAF basada en tasas o procesando los AWS WAF registros 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 HTTP inundaciones, 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 esas 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 honeypot 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. 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.

AWS Consideraciones sobre el diseño de Well-Architected

Esta solución utiliza las mejores prácticas de AWS Well-Architected Framework, que ayuda a los clientes a diseñar y operar cargas de trabajo de confianza, 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 las métricas CloudWatch para proporcionar observabilidad en la infraestructura, las funciones de Lambda, Amazon Data Firehose, Gateway, los buckets de API Amazon S3 y el resto de los componentes de la solución.
- Desarrollamos, probamos y publicamos la solución mediante un proceso de integración y entrega AWS continuas (CI/CD). Esto ayuda a los desarrolladores a lograr resultados de alta calidad de forma constante.

- Puede instalar la solución con una CloudFormation plantilla que aprovisione 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 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 servicios AWS sin servidor siempre que es posible (por ejemplo, Lambda, Firehose, GatewayAPI, 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 AWS servicios que componen esta solución y los detalles de la arquitectura sobre cómo funcionan juntos estos componentes.

AWS los servicios de esta solución

AWS servicio	Descripción	
AWS WAF	Principal. Implementa una AWS WAF webACL, Reglas administradas de AWS grupos de reglas, reglas personalizadas y conjuntos de IP. Realiza AWS WAF API llamadas para bloquear ataques comunes y proteger las aplicaciones web.	
Amazon Data Firehose	Principal. Envía los AWS WAF registros a los buckets de Amazon S3.	
Amazon S3	Principal. AWS WAF Almacena CloudFront y ALB registra.	
AWS Lambda	Núcleo. 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	

AWS servicio	Descripción	
	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 con un bot defectuoso.	
Amazon SNS	Admite. Envía notificaciones por correo electrónico de Amazon Simple Notification Service (AmazonSNS) para respaldar 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, hay tres opciones para gestionar las protecciones HTTP contra inundaciones y para los escáneres y las sondas. En las siguientes secciones se explica cada una de estas opciones con más detalle.

AWS WAF regla basada en tasas

Existen reglas basadas en tarifas para la protección HTTP contra inundaciones. 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.

Te 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 necesitas 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 HTTPFlood Protection como Scanner & Probe Protection incluyen 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 cuando no pueda utilizar reglas AWS WAF basadas en tasas y esté familiarizado con SQL la implementación de personalizaciones. Para obtener más información sobre cómo cambiar la consulta predeterminada, consulte Ver consultas de Amazon Athena.

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

AWS Lambda analizador de registros

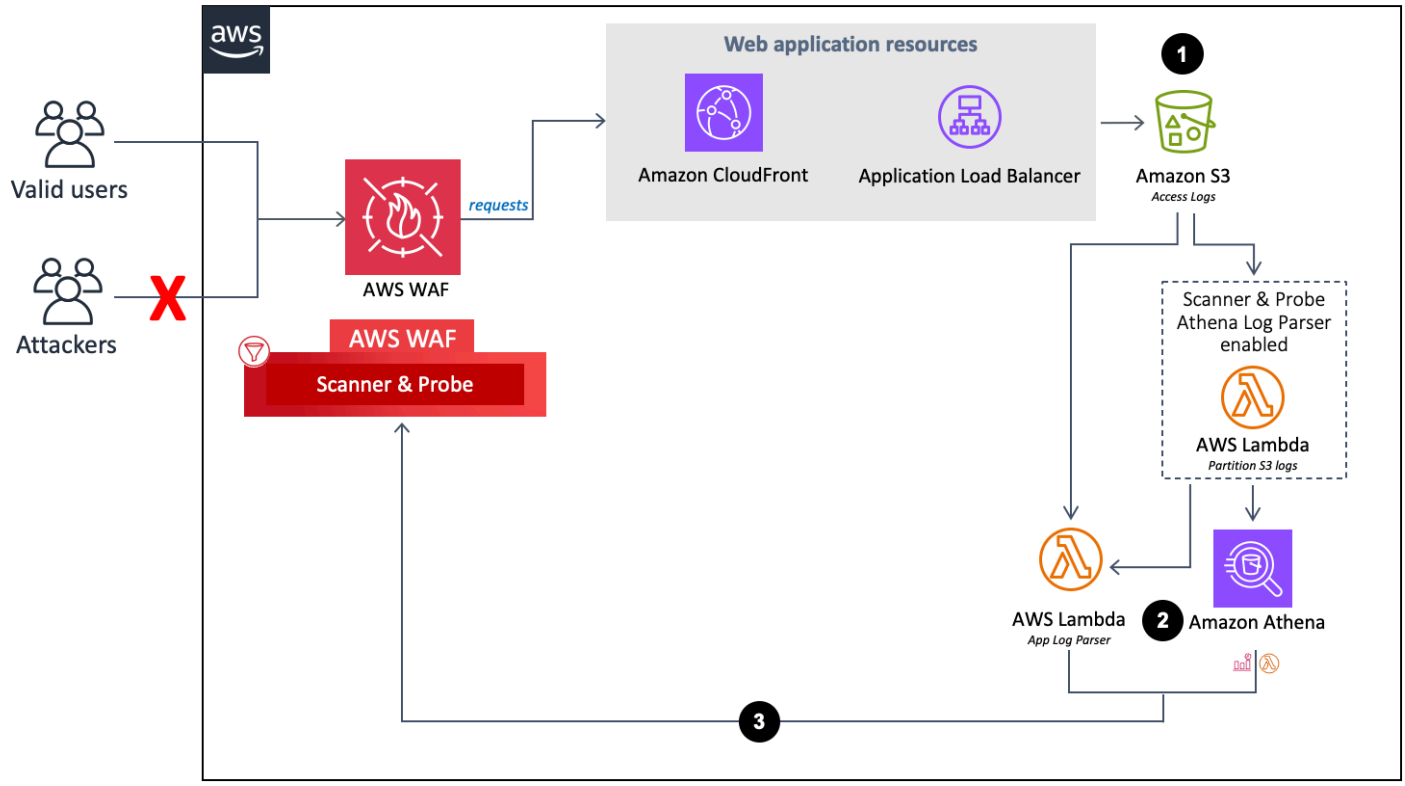
Los parámetros de la plantilla HTTPFlood Protection y Scanner & Probe Protection proporcionan la opción AWS Lambda Log Parser. Utilice el analizador de registros Lambda solo cuando la regla AWS WAF basada en la tasa y las opciones del analizador de registros de Amazon Athena no estén disponibles. Una 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 AWS WAF bloqueados. 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

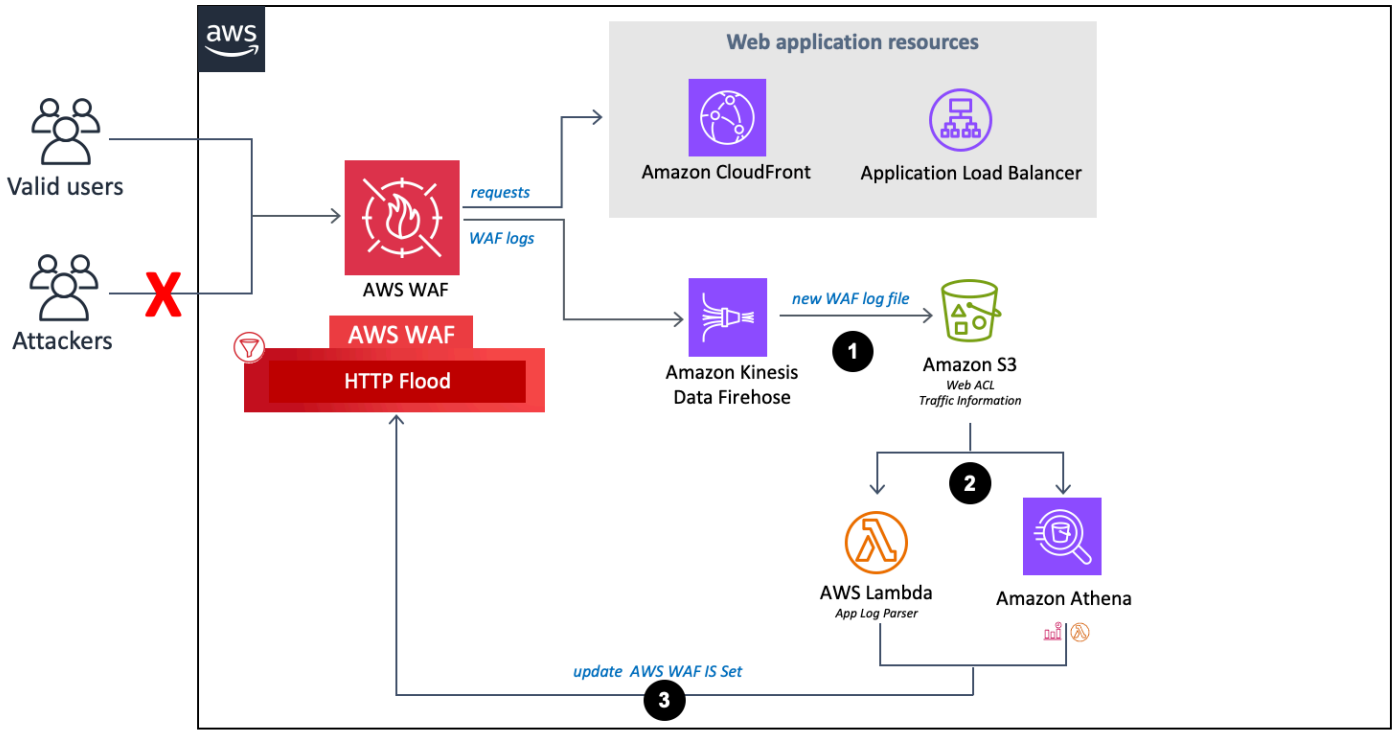
1. Cuando CloudFront o an ALB recibe solicitudes en nombre de su aplicación web, envía los registros de acceso a un bucket de Amazon S3.
   a. (Opcional) Si selecciona los parámetros `Yes - Amazon Athena log parser` de plantilla Activate HTTP Flood Protection y Activate Scanner & Probe Protection, una función de Lambda mueve los registros de acceso de su carpeta original *<customer-bucket>*`/AWSLogs` a una carpeta recién particionada *<customer-bucket>*`/AWSLogs-partitioned/`*<optional-prefix>* `/year=`*<YYYY>*`/month=`*<MM>* `/day=`*<DD>*`/hour=`*<HH>*`/` al llegar a Amazon S3.
   b. (Opcional) Si selecciona el parámetro `yes` de plantilla de ubicación Guardar los datos en el S3 original, 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 HTTPFlood Protection y Activate Scanner & Probe Protection que haya seleccionado, 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 pasa 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 de registro para identificar las direcciones IP que generaron más errores que la cuota definida. A continuación, la solución actualiza una condición de conjunto de AWS WAF IP 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` activa la protección contra HTTP inundaciones, esta solución proporciona los siguientes componentes, que analizan los AWS WAF registros para identificar y bloquear los orígenes que inundan el punto final con una tasa de solicitudes superior a la cuota que usted definió.



AWS WAF flujo del analizador de registros

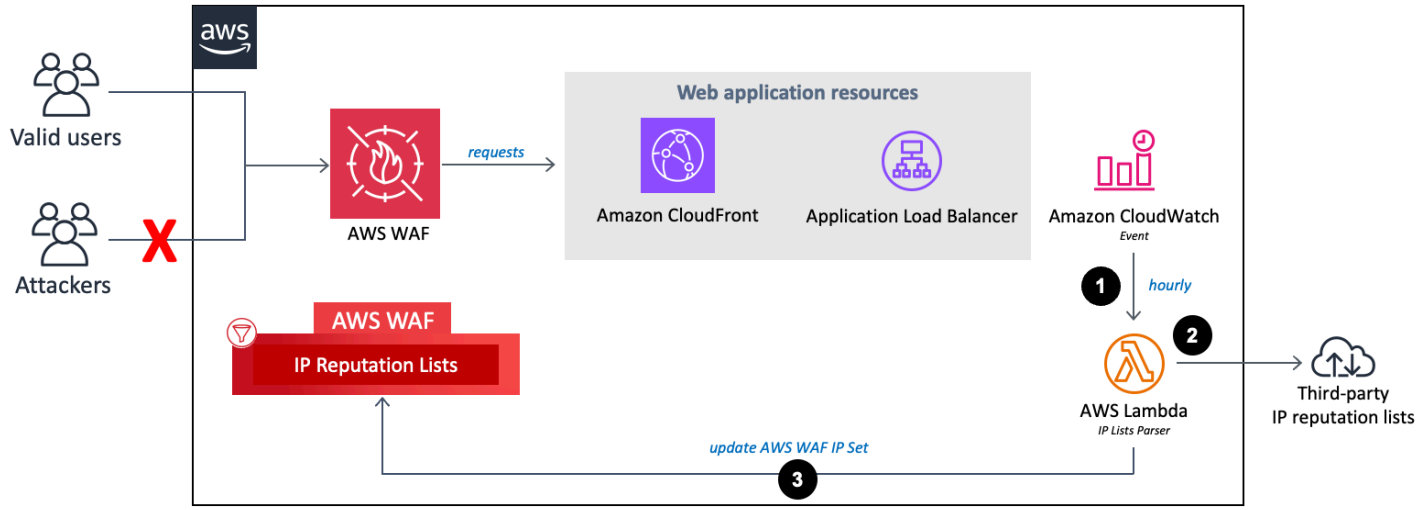
1. Cuando AWS WAF recibe los registros de acceso, los envía a un punto final Firehose. A continuación, Firehose entrega los registros a un depósito particionado en Amazon S3 denominado *<customer-bucket>*/AWSLogs/ *<optional-prefix>*/year=*<YYYY>* / month=*<MM>*/day=*<DD>*/hour= *<HH>*/
2. En función de los parámetros de plantilla Activate HTTPFlood Protection y Activate Scanner & Probe Protection que haya seleccionado, 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. Atenea: De forma predeterminada, cada cinco minutos se ejecuta la consulta Athena del escáner y la sonda y se envía el resultado 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 de conjunto de direcciones AWS WAF IP 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.

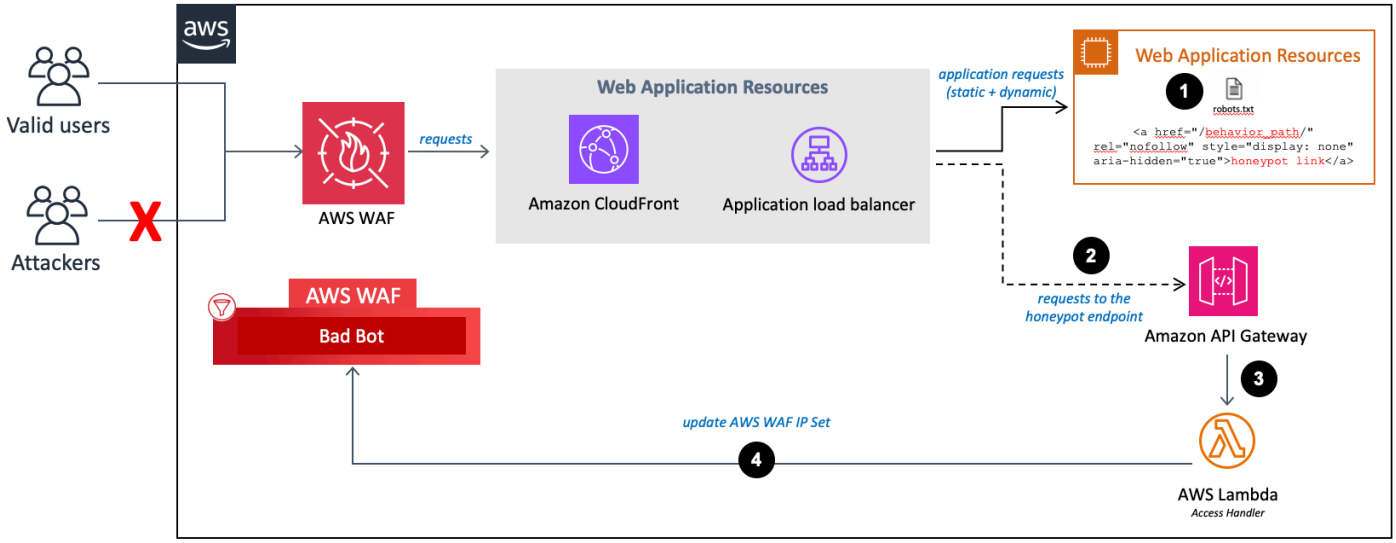


La reputación de IP enumera el flujo del analizador

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:
   - Spamhaus y listas DROP EDROP
   - Lista de direcciones IP de amenazas emergentes de Proofpoint
   - Lista de nodos de salida de Tor
3. La función Lambda actualiza la lista de AWS WAF bloqueados 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 AWS WAF IP para bloquear esas direcciones IP.

Planificación de la implementación

En esta sección se describen el costothe section called “Cuotas”, la seguridad y otras consideraciones antes de implementar la solución.

Soportado Regiones de AWS

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 enumeran en la tabla siguiente) no estén disponibles en todos Regiones de AWS. Por lo tanto, debe lanzar esta solución en un Región de AWS lugar en el que estén disponibles estos servicios. Para obtener la disponibilidad más actualizada de AWS los servicios por región, consulte la lista de Región de AWS todos los servicios.

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Tipo de punto de conexión				
CloudFront	✓			
Application Load Balancer () ALB	✓			
Active la protección HTTP contra inundaciones				
sí, AWS Lambda analizador de registros				✓
sí: analizador de registros Amazon Athena		✓	✓	✓
Active la protección de escáneres y sondas				
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 costo de los AWS servicios 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 AWS Cost Explorerpara ayudar a gestionar los costes. Para obtener más información, consulte la página web de precios de cada AWS servicio 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 AWS gratuita). Los precios están sujetos a cambios.

Ejemplo 1: activar Reputation List Protection, Bad Bot Protection, AWS Lambda Log Parser para proteger contra HTTP inundaciones y Scanner & Probe Protection

AWS servicio	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	~5,40 $

AWS servicio	Dimensiones/mes	Coste [] USD
	milisegundos por ejecución de Lambda	
Amazon API Gateway	1 millón de solicitudes	~3,40 $
AWS WAF web ACL	1	5,00 DÓLARES
AWS WAF regla	4	4,00 DÓLARES
AWS WAF solicitud	1M	0,60$
Total		~23,60 $ al mes

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

AWS servicio	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, 7560 invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	~1,26 $
Amazon API Gateway	1 millón de solicitudes	~3,40 $
Amazon Athena	1,2 millones de visitas a CloudFront objetos o 1,2	~4,32 $

AWS servicio	Dimensiones/mes	Coste [] USD
	millones de ALB solicitudes al día, lo que genera un registro de aproximadamente 500 bytes por visita o solicitud	
AWS WAF web ACL	1	5,00 DÓLARES
AWS WAF regla	4	4,00 DÓLARES
AWS WAF solicitud	1M	0,60$
Total		~23,78 $ al mes

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

AWS servicio	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 512 MB: 1 función, 2000 invocaciones y una duración media de 500 milisegundos por ejecución de Lambda	~0,01 $
Amazon CloudWatch	Eventos 2K	~0,00 $
AWS WAF Web ACL	1	5,00$
AWS WAF Regla	2	2,00 DÓLARES
WASWAFsolicitud	1M	0,60$

AWS servicio	Dimensiones/mes	Coste [] USD
Total		~7,61 $ al mes

Estimación del costo de los troncos CloudWatch

Algunos AWS servicios 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 de Athena durante la instalación, esta solución programa una consulta para que se ejecute en los registros de acceso a las aplicaciones AWS WAF o en los 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 de Protección contra HTTP inundaciones o Protección de escáneres y sondas, 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 WAFBlock 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 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]
```

Athena cobra 5 USD por TB de datos escaneados.

```
[0.0001 TB] * [$5] = [$0.0005 per query scan]
```

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

```
[12 runs] * [24 hours] = [288 runs per day]
[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]
```

Los costes reales varían en función de los patrones de tráfico de la aplicación. Para obtener más información, consulta los precios de Amazon Athena.

Seguridad

Cuando crea sistemas en una AWS infraestructura, 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 acerca AWS de la seguridad, visite Nube de AWS Seguridad.

Roles de IAM

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

Datos

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

Capacidades de protección

Las aplicaciones web son vulnerables a una variedad de 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 AWS WAF reglas, incluidos grupos de Reglas administradas de AWS reglas y reglas personalizadas, para bloquear los siguientes ataques comunes:

- AWSReglas administradas: 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 AWS AWS gestionados, grupos de reglas de referencia AWS gestionados y grupos de reglas gestionados específicos para casos de uso. Tiene la opción de seleccionar uno o más grupos de reglas para su webACL, hasta la cuota máxima de unidades ACL de capacidad web. WCU
- SQLinyección: los atacantes insertan SQL código malicioso en las solicitudes web para extraer datos de su base de datos. Diseñamos esta solución para bloquear las solicitudes web que contienen SQL códigos potencialmente maliciosos.
- 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 de las solicitudes entrantes que se exploran con más frecuencia a fin de identificar y bloquear los ataques. XSS
- HTTPInundaciones: los servidores web y otros recursos de back-end corren el riesgo de sufrir DDoS ataques, como HTTP las inundaciones. Esta solución invoca automáticamente una regla basada en la tasa cuando las solicitudes web de un cliente superan una cuota configurable. Como alternativa, puede aplicar esta cuota procesando AWS WAF los registros 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 de hasta cuatro veces. HTTP Puedes usar este historial para identificar y bloquear las direcciones IP de origen malintencionadas. Esta solución crea una función Lambda o una consulta de Athena que analiza CloudFront o ALB accede automáticamente a los registros, cuenta el número de solicitudes incorrectas de direcciones IP de origen únicas por minuto y se actualiza AWS WAF para bloquear nuevos escaneos desde 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 los remitentes de correo no deseado, los distribuidores de malware y las 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 que extraen 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

Service Quotas, también denominadas límites, establecen el número máximo de recursos u operaciones de servicio para su cuenta de Cuenta de AWS.

Cuotas de AWS los servicios de esta solución

Asegúrese de tener una cuota suficiente para cada uno de los servicios implementados en esta solución. Para más información, consulte Service Quotas de AWS. Para ver las cuotas de servicio de todos los AWS servicios en la documentación sin tener que cambiar de página, consulte la información en la página de puntos finales y cuotas del servicio, en PDF su lugar.

AWS WAF cuotas

AWS WAF puede bloquear un máximo de 10 000 rangos de direcciones IP en la notación Classless Inter-Domain Routing (CIDR) por condición de coincidencia de IP. Cada lista que cree esta solución está sujeta a esta cuota. Para obtener más información, consulte las AWS WAF cuotas. A partir de la versión 3.0, esta solución crea dos conjuntos de IP para adjuntarlos a cada regla, uno para IPv4 y otro paraIPv6.

AWS WAF permite un máximo de una solicitud por segundo, por cuenta o Región de AWS por API llamada a cualquier persona `Create` o `Update` acción. `Put` Si realizas estas API llamadas fuera de la solución, es posible que te encuentres con un problema de API limitación. Para evitar este problema, te recomendamos que evites ejecutar otras aplicaciones que realicen estas API llamadas en la misma cuenta y región en la que está implementada esta solución.

Consideraciones sobre la implementación

En las siguientes secciones, se describen las restricciones y consideraciones para implementar esta solución.

AWS WAF reglas

La web ACL que genera esta solución está diseñada para ofrecer una protección integral para las aplicaciones web. La solución proporciona un conjunto Reglas administradas de AWS de reglas personalizadas que puede agregar a la webACL. Para incluir una regla, elija `yes` los parámetros relevantes 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 AWS Firewall Manager. Si desea utilizar las reglas del Firewall Manager, le recomendamos que aplique personalizaciones a su código fuente.

Registro del ACL tráfico web

Si crea la pila en un lugar que no Región de AWS sea EE. UU. Este (Virginia del Norte) y establece el punto final como`CloudFront`, debe establecer Activar protección contra HTTP inundaciones en no o`yes - AWS WAF rate based rule`.

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

Manejo de sobredimensionamiento para los componentes de las solicitudes

AWS WAF no permite inspeccionar contenido sobredimensionado para el cuerpo, los encabezados o las cookies del componente de solicitud web. Cuando escribes una declaración de regla que inspecciona uno de estos tipos de componentes de solicitudes, puedes elegir una de estas opciones para indicar AWS WAF qué hacer con estas solicitudes:

- `yes`(continuación): inspeccione el componente de la solicitud normalmente de acuerdo con los criterios de inspección de la regla. AWS WAF inspecciona el contenido del componente 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`— Considera que la solicitud web coincide con la declaración de la 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 el enunciado de la regla, sin evaluarla en función de los criterios de inspección de la regla. AWS WAF continúa inspeccionando la solicitud web utilizando el resto de las reglas de la webACL, como haría con cualquier regla que no coincida.

Para obtener más información, consulte Gestión de componentes de solicitudes web sobredimensionados 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 AWS WAF cuotas por cuenta y por región.

Implementación de la solución

Esta solución utiliza plantillas y pilas de AWS CloudFormation para automatizar su implementación. Las CloudFormation plantillas especifican los AWS recursos 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 una ALB

Paso 1. Lanza la pila

- Lanza la CloudFormation plantilla a tu Cuenta de AWS.
- Introduzca los valores de los parámetros necesarios: nombre de la pila y nombre del depósito de registro de acceso a la aplicación.
- Revise el resto de los parámetros de la plantilla y ajústelos si es necesario.

Paso 2. Asocie la web ACL a su aplicación web

- Asocie su (s) distribución ALB (es) CloudFront web a la web ACL 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 ALB web 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 Logs (prefijo de AWS registro predeterminado). `AWS Logs/` Consulte el parámetro Application Access Log Bucket Prefix en el paso 1. Inicie la pila para obtener más información.

AWS CloudFormation plantillas

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

Pila principal

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

ACLPila web

aws-waf-security-automations-webacl.template: esta plantilla anidada proporciona AWS WAF recursos que incluyen una webACL, una IP, conjuntos y otros recursos asociados.

Pila Firehose Athena

aws-waf-security-automations-firehose-athena.template: esta plantilla anidada proporciona recursos relacionados con Athena y Firehose. AWS Glue Se crea al elegir el analizador de registros Athena Scanner & Probe o el analizador de registros Flood HTTPLambda 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 y distribuir el tráfico entrante a su aplicación web, consulte Create an Application Load Balancer en la Guía del usuario de Application Load Balancers. ALB

Paso 1. Lanzar la pila de

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

1. Inicie sesión en AWS Management Consoley seleccione Launch Solution para lanzar la `waf-automation-on-aws.template` CloudFormation plantilla.

2. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar esta solución en otro lugar Región de AWS, utilice el selector de regiones de la barra de navegación de la consola. Si lo 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 Regiones de AWS solo están disponibles en versión específica. Por lo tanto, debe lanzar esta solución en un Región de AWS lugar donde estén disponibles estos servicios. Para obtener más información, consulte Compatible Regiones de AWS.

3. En la página Especificar plantilla, compruebe que ha seleccionado la plantilla correcta y pulse Siguiente.
4. En la página Especificar los detalles de la pila, asigne un nombre a la AWS WAF configuración en el campo Nombre de la pila. También es el nombre de la web ACL que crea la plantilla.
5. 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	Descripción
Nombre de pila	*<requires input>*	El nombre de la pila no puede contener espacios. Este nombre debe ser único en el tuyo Cuenta de AWS y es el nombre de la web ACL que crea la plantilla.
Tipo de recurso		
Punto de conexión	`CloudFront`	Elija el tipo de recurso que se va a utilizar.

Parámetro	Predeterminado	Descripción
		Note Si lo elige `CloudFront` como punto final, debe lanzar la solución para crear WAF recursos en la región EE.UU. Este (Virginia del Norte) (`us-east-1`).
AWS Grupos de reglas de reputación IP gestionados		

Parámetro	Predeterminado	Descripción
Activar la protección de grupos de reglas gestionados por listas de reputación IP de Amazon	no	Seleccione `yes` activar el componente diseñado para añadir el grupo de reglas gestionado por Amazon IP Reputation List a la webACL. Este grupo de reglas se basa en la inteligencia de amenazas interna de Amazon. Esto resulta útil si desea bloquear las direccion es 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. El número requerido WCU es 25. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más informaci ón, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas gestionados por listas de direcciones IP anónimas	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por listas de IP anónimas a la webACL. Este grupo de reglas bloquea las solicitudes de los servicios que permiten ocultar la identidad del espectador. Estas incluyen solicitudes de proxiesVPNs, 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. El número requerido WCU es 50. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
AWS Grupos de reglas base gestionados		
Active la protección de grupos de reglas gestionados por conjuntos 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 webACL. 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 usar este grupo de reglas para cualquier caso de AWS WAF uso. El número requerido WCU es 700. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas gestionada por Admin Protection	no	Seleccione `yes` activar el componente diseñado para añadir el grupo de reglas gestionado por Admin Protection a la webACL. 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 administr ativo a la aplicación. El número requerido WCU es 100. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más informaci ón, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas gestionados por entradas incorrectas conocidas	no	Seleccione `yes` activar el componente diseñado para añadir a la web el grupo de reglas gestionadas con entradas incorrectas conocidasACL. 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. El número requerido WCU es 100. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.
AWS Grupo de reglas gestionado para casos de uso específicos		

Parámetro	Predeterminado	Descripción
Active la protección SQL de grupos de reglas administr ados por bases de datos	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por la SQL base de datos a la webACL. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de las SQL bases de datos, como los ataques de SQL inyección. Este puede ayudar a evitar la inyección remota de consultas no autorizadas. Evalúe este grupo de reglas para usarlo si su aplicació n interactúa con una SQL base de datos. El uso de la regla personalizada de SQL inyección es opcional si ya ha activado el grupo de SQL reglas AWS gestionado. El número requerido WCU es 200. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más informaci ón, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas gestionados por el sistema operativo Linux	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por el sistema operativo Linux a la webACL. 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 POSIX operativo. El número requerido WCU es 200. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad.

Parámetro	Predeterminado	Descripción
		Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas administr ada por el sistema POSIX operativo	no	Seleccione `yes` activar el componente diseñado para añadir la protección de grupos de reglas gestionad os por el conjunto de reglas principales a la webACL. Este grupo de reglas bloquea los patrones de solicitud es asociados a la explotaci ón de vulnerabilidades específicas de POSIX los sistemas operativos POSIX similares a ellos, incluidos LFI los ataques. 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 aplicació n se ejecuta en un sistema operativo POSIX o POSIX similar. El valor requerido WCU es 100. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad.

Parámetro	Predeterminado	Descripción
		Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active la protección de grupos de reglas administr ada por el sistema operativo Windows	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por el sistema operativo Windows a la webACL. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotaci ón de vulnerabilidades específicas de Windows, como la ejecución remota de PowerShell comandos. Este puede ayudar a evitar la explotación de vulnerabi lidades que permiten a un atacante ejecutar comandos no autorizados o ejecutar código malintencionado. Valore este grupo de reglas si alguna parte de la aplicació n se ejecuta en un sistema operativo Windows. El número requerido WCU es 200. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más informaci ón, consulte la lista de grupos

Parámetro	Predeterminado	Descripción
		de Reglas administradas de AWS reglas.

Parámetro	Predeterminado	Descripción
Active PHP la protección de grupos de reglas gestionados por la aplicación	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por PHP aplicaciones a la webACL. Este grupo de reglas bloquea los patrones de solicitud asociados a la explotación de vulnerabilidades específicas del uso del lenguaje de PHP programación, incluida la introducción de PHP funciones 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 algún servidor con el que interactúe su aplicación. El valor requerido WCU es 100. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos

Parámetro	Predeterminado	Descripción
		de Reglas administradas de AWS reglas.
Active WordPress la protección de grupos de reglas gestionados por la aplicación	no	Seleccione `yes` activar el componente diseñado para añadir un grupo de reglas gestionado por WordPress aplicaciones a la webACL. 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 SQL de base de datos y PHP aplicaciones. El valor requerido WCU es 100. Su cuenta debe tener la WCU capacidad suficiente para evitar que se produzca un error en la implementación de la ACL pila web si se supera el límite de capacidad. Para obtener más información, consulte la lista de grupos de Reglas administradas de AWS reglas.
Regla personalizada: escáner y sondas		

Parámetro	Predeterminado	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 desventaj as relacionadas con las opciones de mitigación.

Parámetro	Predeterminado	Descripción
Nombre del depósito de registro de acceso a la aplicación	*<requires input>*	Si ha elegido `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. ALB Si utiliza un bucket de Amazon S3 existente, debe estar ubicado en el mismo Región de AWS lugar en el 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. **Note** Active el registro de acceso a la CloudFront web para sus distribuciones web o ALB para enviar los archivos de registro a este bucket de Amazon S3. Guarde los registros con el

Parámetro	Predeterminado	Descripción
		mismo prefijo definido en la pila (prefijo `AWSLogs/` predeterminado). Consulte el parámetro Application Access Log Bucket Prefix para obtener más información.

Parámetro	Predeterminado	Descripción
Prefijo del depósito de registro de acceso a la aplicación	`AWS Logs/`	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. `yourprefix/` Si ha elegido `ALB` el parámetro Endpoint, debe añadirlo `AWS Logs/` a su prefijo, por ejemplo. `yourprefix/AWSLogs/` Utilice `AWS Logs/` (predeter minado) si no hay un prefijo definido por el usuario. Para desactivar esta protección, ignore este parámetro.

Parámetro	Predeterminado	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 deseano, 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	Descripción
Mantenga los datos en la ubicación original de S3	no	Si ha elegido `yes - Amazon Athena log parser` el parámetro Activar protección de escáner y sonda, 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 `yes` si también desea conservar una copia de los registros en su ubicación original. Esto duplicará tu almacenamiento de registros. Si no eligió `yes - Amazon Athena log parser` el parámetro Activar la protección del escáner y la sonda, omita este parámetro.
Regla personalizada: HTTP Inundación		

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

Parámetro	Predeterminado	Descripción
Umbral de solicitud predeterminado	`100`	Si eligió `yes` el parámetro Activar la protección contra HTTP inundaciones, 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 HTTP inundaciones, el valor mínimo aceptable es`100`. Si ha elegido `yes - AWS Lambda log parser` o `yes – Amazon Athena log parser` el parámetro Activar protección contra HTTP inundaciones, puede tener cualquier valor. Para desactivar esta protección, ignore este parámetro.

Parámetro	Predeterminado	Descripción
Umbral de solicitud por país	<optional input>	Si ha elegido `yes - Amazon Athena log parser` el parámetro Activar protección contra HTTP inundaciones, puede introducir un umbral por país siguiendo este JSON formato`{"TR":50, "ER":150}` . 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. **Note** 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 Flood HTTP Athena Query.

Parámetro	Predeterminado	Descripción
		Si decide desactivar esta protección, ignore este parámetro.
Agrupar por solicitudes en HTTP Flood Athena Query	`None`	Si eligió `yes - Amazon Athena log parser` el parámetro Activar la protección contra HTTP inundaciones, 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 opta por desactivar esta protección, ignore este parámetro.
WAFPeriodo de bloqueo	`240`	Si ha elegido `yes - AWS Lambda log parser` `yes - Amazon Athena log parser` los parámetros Activar Scanner & Probe Protection o Activar HTTP Flood Protection, introduzca el período (en minutos) para bloquear las direcciones IP aplicables. Para desactivar el análisis de registros, ignore este parámetro.

Parámetro	Predeterminado	Descripción
Cronograma de tiempo de ejecución de Athena Query (minutos)	`5`	Si ha elegido `yes - Amazon Athena log parser` los parámetros Activar protección de escáner y sonda o Activar protección contra HTTP inundaciones, 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 malicioso s y los rastreadores de contenido.

Parámetro	Predeterminado	Descripción
ARNde un IAM rol que tenga acceso de escritura a CloudWatch los registros de tu cuenta	<optional input>	Proporciona un IAM rol opcional que tenga acceso ARN de escritura a CloudWatch los registros de tu cuenta. Por ejemplo: `ARN: arn:aws:iam::account_id:role/myrolename` . Consulte Configurar el CloudWatch registro de un rol REST API 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	Descripción
Umbral de solicitud predeterminado	100	Si eligió `yes` el parámetro Activar la protección contra HTTP inundaciones, 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 HTTP inundaciones, el valor mínimo aceptable es 100. Si ha elegido `yes - AWS Lambda log parser` o `yes – Amazon Athena log parser` el parámetro Activar protección contra HTTP inundaciones, puede tener cualquier valor. Para desactivar esta protección, ignore este parámetro.
Regla personalizada: listas de reputación de IP de terceros		
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).

Parámetro	Predeterminado	Descripción
Reglas personalizadas heredadas		

Parámetro	Predeterminado	Descripción
Active la protección contra SQL inyecciones	`yes`	Seleccione `yes` activar el componente diseñado para bloquear los ataques de SQL inyección más comunes. Considere activarlo si no utiliza un conjunto de reglas básicas AWS gestionadas o un grupo de reglas de SQL bases de datos AWS gestionadas. Puede elegir una de las opciones `yes` (continuar) o `yes - NO_MATCH`) si desea AWS WAF gestionar 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 solicitudes web sobredimensionados. Elija no desactivar esta función.

Parámetro	Predeterminado	Descripción
		Note La CloudForm ation pila añade la opción de gestión de sobredimensionamie nto seleccionada a la regla de protección contra SQL inyeccion es predeterminada y la implementa en la suya. Cuenta de AWS Si has personali zado la regla fuera de CloudFormation, los cambios se sobrescri birán tras la actualiza ción de la pila.

Parámetro	Predeterminado	Descripción
Nivel de sensibilidad para la protección contra SQL inyecciones	`LOW`	Elija el nivel de sensibilidad que desee utilizar AWS WAF para detectar ataques SQL de inyección. `HIGH`detecta más ataques, pero puede generar más falsos positivos. `LOW`suele ser una mejor opción para los recursos que ya cuentan con otras protecciones contra los ataques SQL por inyección o que tienen una baja toleranci a a los falsos positivos. Para obtener más informaci ón, consulte la sección sobre los niveles de sensibilidad adicionales para las instrucci ones y SensitivityLevelpr opiedades de las reglas de SQL inyección en la Guía del AWS CloudFormation usuario.AWS WAF Si decide desactivar la protección contra la SQL inyección, ignore este parámetro. **Note** La CloudFormation pila añade el nivel de

Parámetro	Predeterminado	Descripción
		sensibilidad seleccionado a la regla de protección contra SQL inyecciones predeterminada y lo implementa en la suya. Cuenta de AWS Si has personalizado la regla fuera de CloudFormation, los cambios se sobrescribirán tras la actualización de la pila.

Parámetro	Predeterminado	Descripción
Active la protección contra secuencias de comandos entre sitios	`yes`	Seleccione `yes` activar el componente diseñado para bloquear los ataques más comunesXSS. Considera activarlo si no utilizas un conjunto de reglas básicas AWS gestionadas. También puede seleccionar una de las opciones (`yes`(continua r) o`yes - NO_MATCH`) AWS WAF para gestionar las solicitudes sobredime nsionadas 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. Elija no desactivar esta función. **Note** La CloudForm ation pila añade la

Parámetro	Predeterminado	Descripción
		opción de gestión de sobredimensionamiento seleccionada a la regla predeterminada de secuencias de comandos entre sitios y la implementa en la suya. Cuenta de AWS Si has personalizado la regla fuera de CloudFormation, los cambios se sobrescribirán tras la actualización de la pila.
Configuración de retención de IP permitida y denegada		

Parámetro	Predeterminado	Descripción
Período de retención (minutos) para el conjunto de IP permitido	`-1`	Si desea activar la retención de IP para el conjunto de IP permitido, introduzc a 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 considera rá como tal15. Déjelo como `-1` (predeter minado) para desactivar la retención de IP.

Parámetro	Predeterminado	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 considera rá como tal15. Déjelo como `-1` (predeter minado) para desactivar la retención de IP.

Parámetro	Predeterminado	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 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 Next (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 Next (Siguiente).
8. En la página Revisar y crear, revise y confirme la configuración. Seleccione las casillas para confirmar que la plantilla creará IAM los recursos y las capacidades adicionales necesarias.
9. Elija Crear para implementar la pila.

   Vea el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Deberías recibir un estado de CREATE _ COMPLETE en aproximadamente 15 minutos.

   > **Note**
   >
   > Además de las funcionesLog `Parser`, y`IP Lists Parser`, esta solución incluye `Access Handler` AWS Lambda las funciones `helper` y `custom-resource` Lambda, que se ejecutan solo durante la configuración inicial o cuando se actualizan o eliminan los recursos.
   > Al usar esta solución, verá todas las funciones en la AWS Lambda consola, 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 web ACL a su aplicación web

Actualice sus CloudFront distribuciones para ALB activarlas AWS WAF y registrarlas con los recursos que generó en el paso 1. Lanza la pila.

1. Inicie sesión en la consola de AWS WAF.
2. Elige la web ACL que quieres usar.
3. En la pestaña Recursos de AWS asociados, seleccione Añadir recursos de AWS .
4. En Tipo de recurso, selecciona la CloudFront distribución oALB.
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 envíe ALB los registros de acceso a la web al bucket de Amazon S3 correspondiente para 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 AWS WAF Web ACL, elija la ACL solución 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 cubos asociados al actual. Cuenta de AWS 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). `AWS Logs/`
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 (AmazonEC2).
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Selecciona la de tu aplicación webALB.
4. En la pestaña Descriptions, elija Edit attributes.
5. Elija Enable access registros.

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). `AWS Logs/`
8. Seleccione Guardar.

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

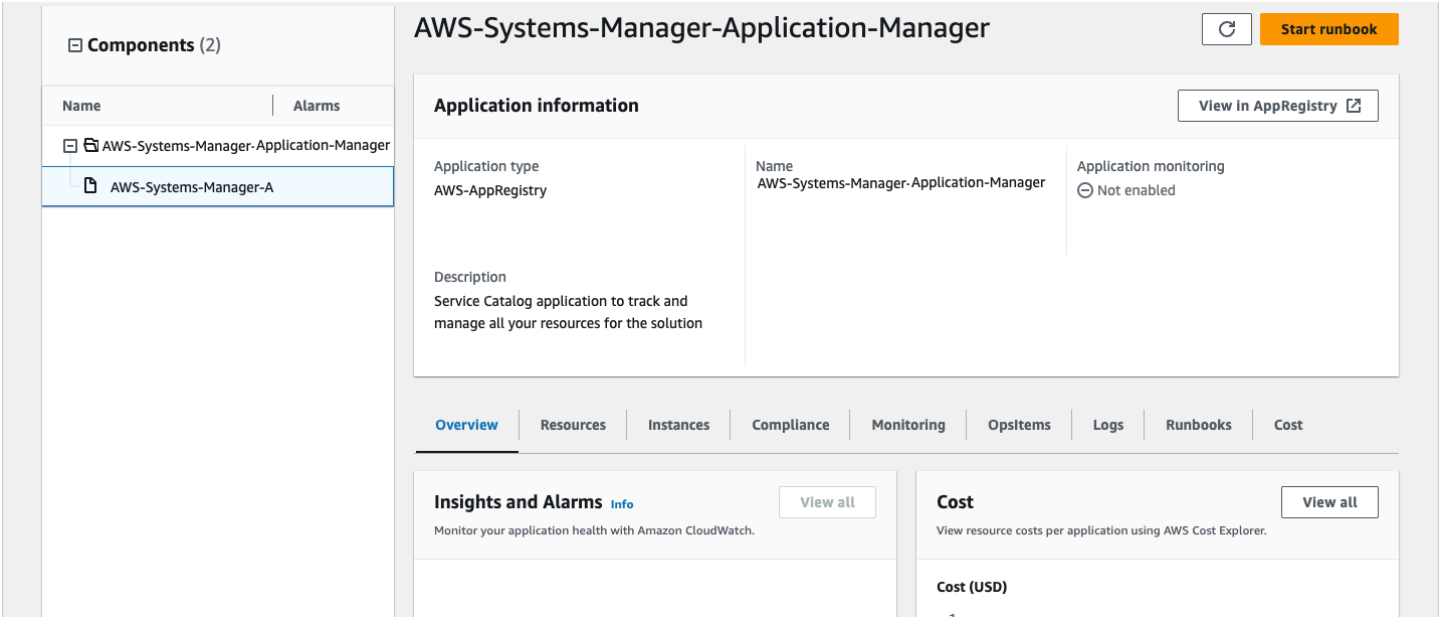
Supervise la solución con AppRegistry

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 costos de los recursos implementados en todas las pilas y Cuentas de AWS 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.



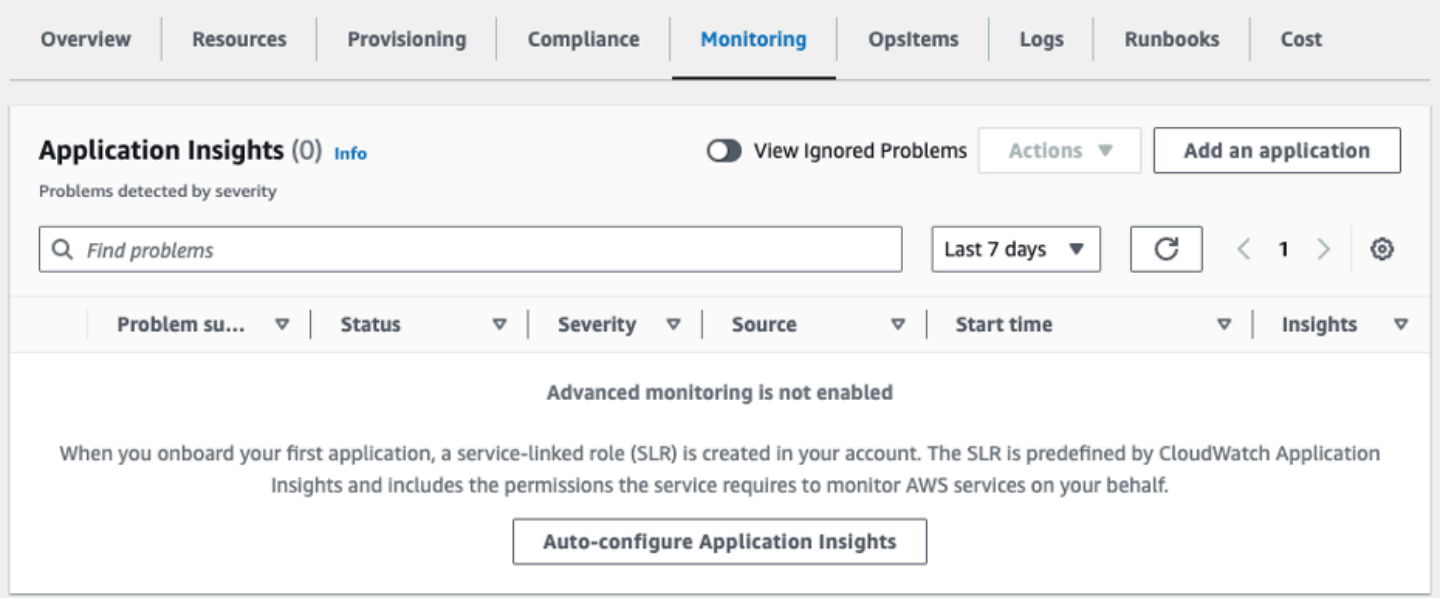
Pila de soluciones en Application Manager

Active CloudWatch Application Insights

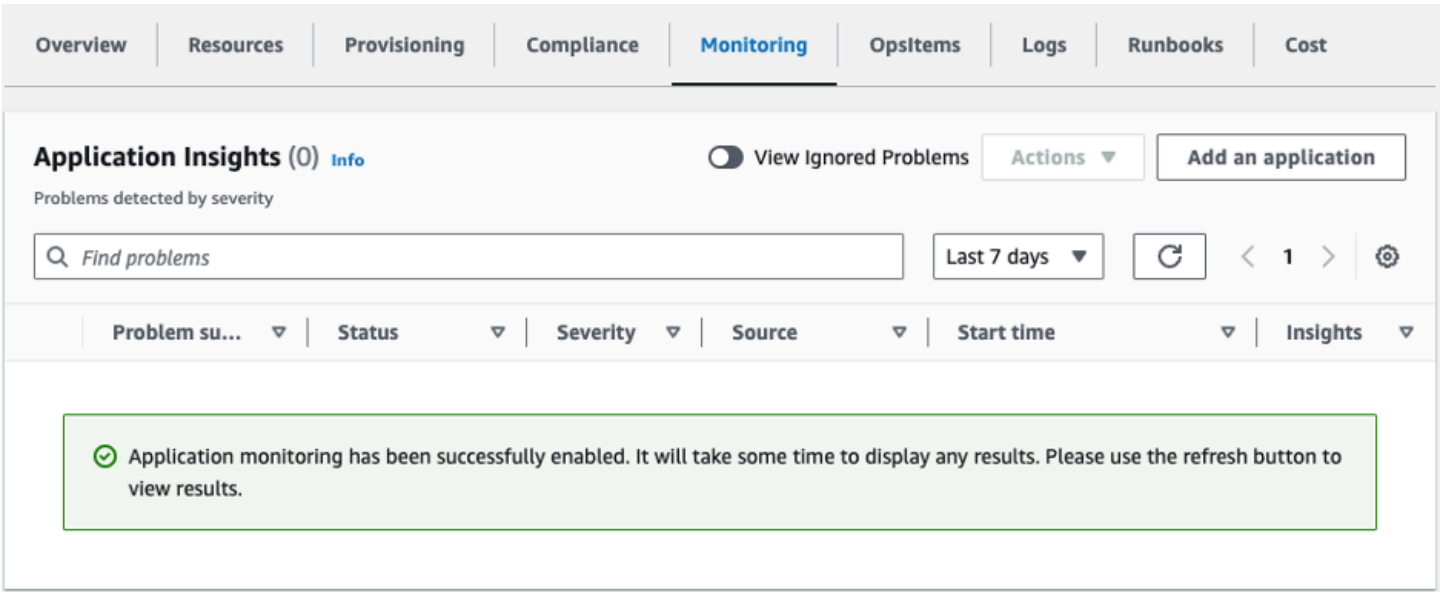
1. Inicie sesión en la consola de Administrador de aplicaciones.

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.



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

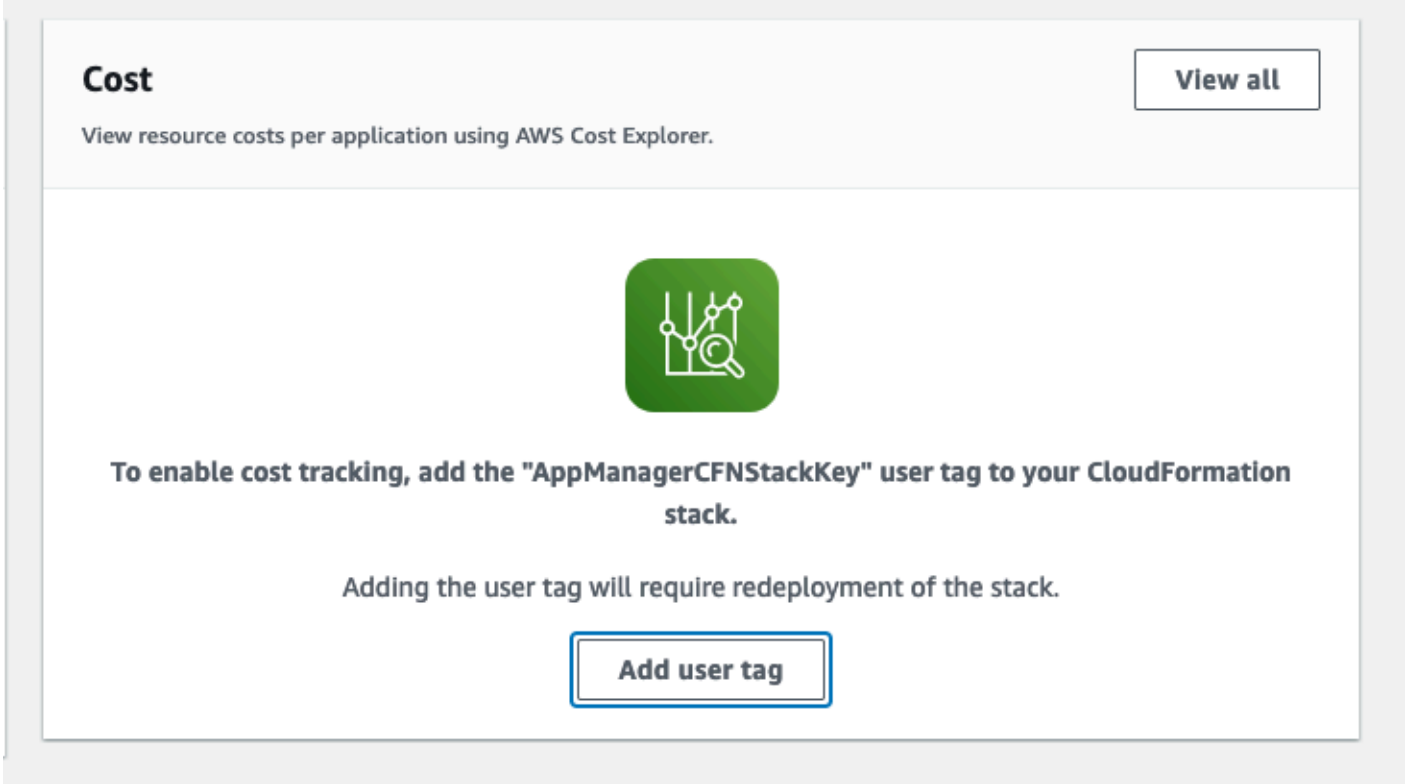


Confirmación de las etiquetas de costos asociadas a la solución

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.



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 AWS Billing and Cost Management y en la consola de administración de costos.
2. En el panel de navegación, seleccione Etiquetas de asignación de costes.
3. En la página Etiquetas de asignación de costos, filtre por la etiqueta AppManagerCFNStackKey y, a continuación, selecciónela 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 sus componentes en la consola de Application Manager mediante la integración con la aplicación AWS Cost Explorer, que debe activarse primero. Cost Explorer lo ayuda a administrar los costos al proporcionarle una vista de los costos y el uso de sus recursos de AWS a lo largo del tiempo. Para activar Cost Explorer para la solución:

1. Inicie sesión en la Consola de administración 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 consola de AWS CloudFormation.
2. Selecciona Stacks en el menú de navegación de la izquierda.
3. Selecciona tu `aws-waf-security-automations` CloudFormation pila actual.
4. Elija Actualizar.
5. Seleccione Reemplazar la plantilla actual.
6. En Especificar plantilla:
   a. Seleccione Amazon S3URL.
   b. Copia el enlace del `aws-waf-security-automations.template` AWS CloudFormation.
   c. Pegue el enlace en la URL casilla de Amazon S3.
   d. Compruebe que la plantilla correcta URL aparece en el cuadro de URL texto de Amazon S3.
   e. Elija Next (Siguiente).
   f. Vuelva a seleccionar Siguiente.
7. En Parámetros, revise los parámetros de la plantilla y modifíquelos según sea necesario. Consulte el paso 1. Inicie la pila para obtener detalles sobre los parámetros.
8. Elija Next (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 IAM recursos.
12. Seleccione Ver conjunto de cambios y verifique los cambios.
13. Seleccione Crear pila para implementar la pila.

Puedes ver el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Deberás ver el estado 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.

WAFV2actualizar

A partir de la versión 3.0, esta solución es compatible con la AWS WAF V2. Sustituimos todas las API llamadas AWS WAF clásicas por APIllamadas AWS WAF V2. 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 AWS WAF reglas con las configuraciones predeterminadas en la Cuenta de AWS CloudFormation 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 update-ip-setCLIcomandos get-ip-sety. Si ya utilizas la versión 3.2 o posterior, ignora este paso.

Desinstalar la solución

Para desinstalar la solución, elimine las CloudFormation pilas:

1. Inicie sesión en la consola de AWS CloudFormation.

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 AWS recursos utilizados por 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 AWAWAFAPIlas cuotas, 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 de AWS WAF.
2. En el panel de navegación izquierdo, elija Conjuntos de IP.
3. Elija el conjunto de direcciones IP en la lista de direcciones permitidas y añada direcciones IP de fuentes de confianza.
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 el parámetro `yes` Activar la protección contra bots defectuosos 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, es posible que los robots y los rastreadores de contenido, como el malware que busca vulnerabilidades de seguridad y rastrea direcciones de correo electrónico, intenten acceder al punto final de captura. En este escenario, la función `Access Handler` Lambda inspecciona la solicitud para extraer su origen y, a continuación, actualiza la AWS WAF regla asociada para bloquear las solicitudes posteriores de esa dirección IP.

Utilice uno de los siguientes procedimientos para incrustar el enlace 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 consola de AWS CloudFormation.
2. Elige la pila que creaste en el paso 1. Lanza la pila
3. Elija la pestaña Salidas.
4. Desde la BadBotHoneypotEndpointclave, copia el punto finalURL. Contiene dos componentes que necesita para completar este procedimiento:
   - El nombre del host del punto final (por ejemplo,`xxxxxxxxxx.execute-api.region.amazonaws.com`)
   - La solicitud URI (`/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 del punto final URL que copió en el paso 2. Asocie la Web ACL a su aplicación web.
10. En Origin Path, pega la solicitud URL que también copiaste en el paso 2. Asocie la Web ACL 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 unALB.

1. Inicie sesión en la consola de AWS CloudFormation.
2. Elija la pila que creó en el paso 1. Lanza la pila.
3. Elija la pestaña Salidas.
4. Desde la BadBotHoneypotEndpointclave, copia el punto finalURL.
5. Inserte este enlace de punto final en el contenido de su web. Usa el texto completo URL que copiaste en el paso 2. Asocie la Web ACL a su aplicación web. Oculte este enlace a sus usuarios humanos. Como ejemplo, consulta el siguiente ejemplo de código:

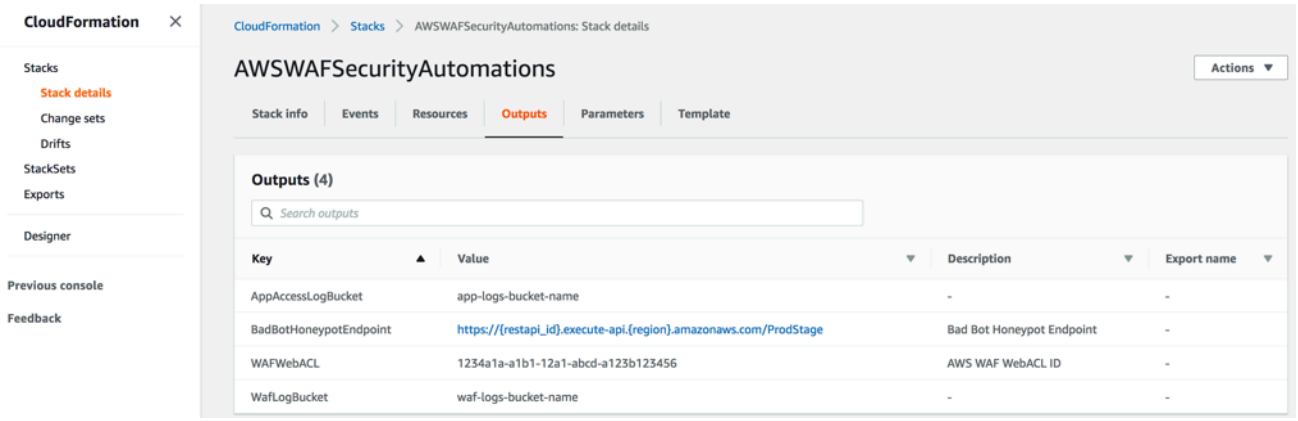
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> Este procedimiento se utiliza `rel=nofollow` para indicar a los robots que no accedan al URL honeypot. Sin embargo, dado que el enlace está incrustado de forma externa, no puedes incluir un `robots.txt` archivo que prohíba explícitamente el enlace. 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 analizador de registros Lambda JSON

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

Si ha elegido el parámetro `Yes - AWS Lambda log parser` de plantilla Activate HTTP Flood Protection, 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 AWS WAF registro. Para encontrar el nombre del bucket, consulte la WafLogBucketvariable del CloudFormation resultado. En la siguiente figura se muestra un ejemplo.



Apila las salidas

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 AWS WAF los nuevos archivos de registro. A continuación se muestra un ejemplo de archivo de configuración:

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

HTTParchivo de configuración de inundación

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 usted define 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 cuentan para el umbral de solicitudes. De forma predeterminada, esta lista está vacía.
- URIlista: utilícela para definir un umbral de solicitud y un período de bloqueo personalizados para fines específicosURLs. De forma predeterminada, esta lista está vacía.

Cuando WAF los registros 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 WAF IP configurada para HTTPFlood 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 JSON archivo 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 AWS WAF los nuevos archivos de registro. A continuación se muestra un ejemplo de archivo de configuración:

Archivo de configuración de escáneres y sondas

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 HTTP estado:`400 (Bad Request)`,`401 (Unauthorized)`, `403 (Forbidden)``404 (Not Found)`, y`405 (Method Not Allowed)`.

- URIlista: 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 cuyo nombre se encuentra *`<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 a la WAF IP configurada para Scanner & Probe e impide que accedan a su 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 analizador de registros Athena por país y URI en caso de HTTP inundación

Puedes agrupar por IPs país y URI en la consulta de Atenea para detectar y bloquear los ataques de HTTP inundación que tienen patrones impredecibles`URI`. 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 solicitudes 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. Lanza 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 los parámetros de plantilla Activar protección contra HTTP inundaciones o Activar protección **`Yes - Amazon Athena log parser`** para escáneres y sondas, esta solución crea y ejecuta consultas de Athena para CloudFront o ALB (`ScannersProbesLogParser`) o AWS WAF logs (`HTTPFloodLogParser`), analiza el resultado y se actualiza en consecuencia. AWS WAF

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 WAFBlock 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 a. AWS AWS Glue Data Catalog Esta solución crea el catálogo de datos de los registros de acceso 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 a la versión más reciente AWSAWS Glue Data Catalog step-by-step.

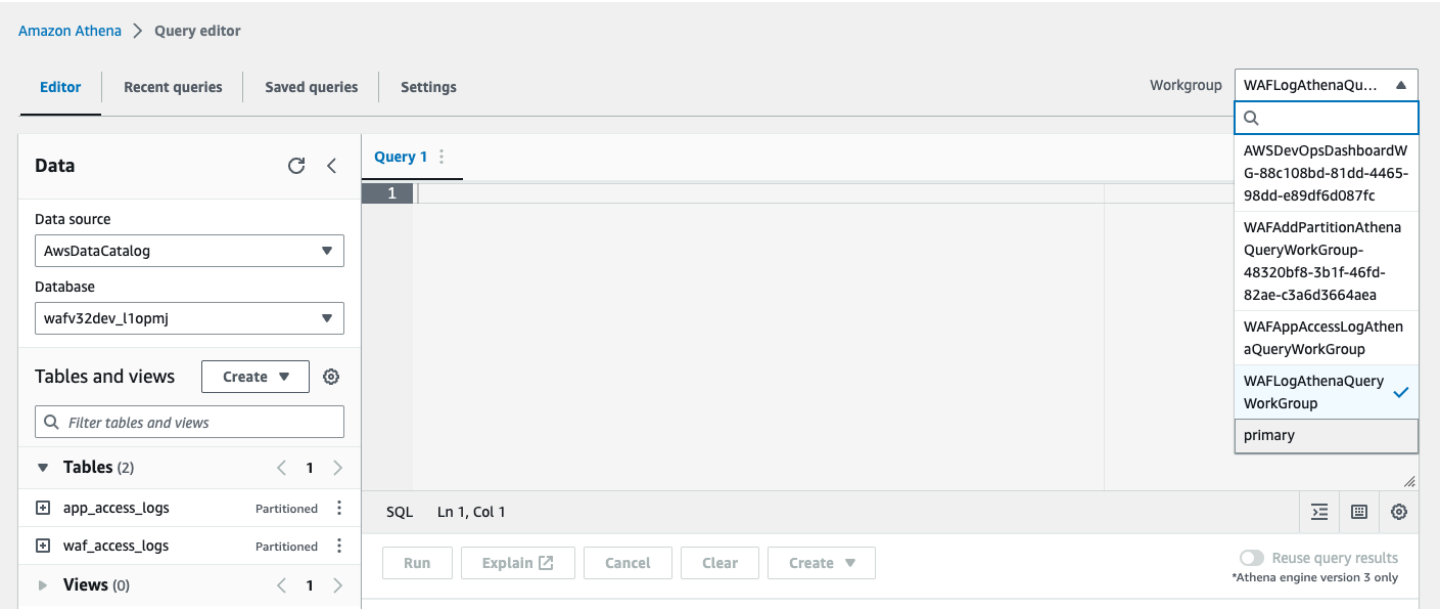
Utilice el siguiente procedimiento para ver estas consultas:

Ver consultas de WAF registro

1. Inicia sesión en la consola de Amazon Athena.
2. Seleccione Iniciar el editor de consultas.
3. Seleccione la base de datos para esta solución.
4. Seleccione una opción WAFLogAthenaQueryWorkGroupde la lista desplegable.

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

5. Elija Cambiar para cambiar el grupo de trabajo.



6. Seleccione la pestaña Historial.
7. 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.

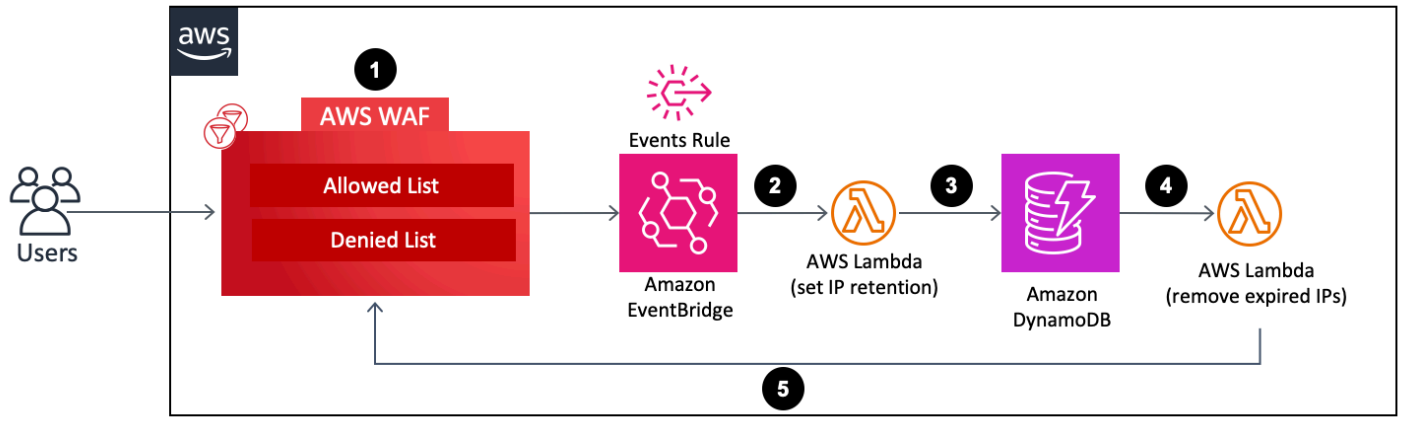
> **Note**
>
> Este grupo de trabajo solo existe si ha seleccionado `Yes - Amazon Athena log parser` los parámetros de plantilla Activar la protección contra HTTP inundaciones o Activar la protección contra escáneres y sondas.

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.

Configure la retención de IP en los conjuntos de AWS WAF IP permitidas y denegadas

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

Funcionamiento



Retención de IP en conjuntos de WAF IP permitidos y denegados

1. Cuando un usuario actualiza (agrega o elimina una dirección IP) el conjunto de WAF IP permitidas o denegadas, esta acción invoca una AWS WAF `UpdateIPSet` API llamada 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 TTL atributo es. `ExpirationTime`
4. Cuando un elemento alcanza su fecha de caducidad, TTL se invoca 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 AWS WAF API llamada para eliminar del conjunto de IP de destino las direcciones IP caducadas incluidas en el elemento. AWS WAF

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. Lanza la pila.
2. Introduzca una dirección de correo electrónico si desea recibir una notificación por correo electrónico cuando las direcciones IP caducadas se eliminen del conjunto de AWS WAF IP. Si decide recibir una notificación por correo electrónico, debe confirmar la suscripción mediante el enlace incluido 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. Lanza la pila.
3. Actualice el conjunto de direcciones AWS WAF IP 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 se compone de las direcciones IP que existen en el conjunto de direcciones AWS WAF IP 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 del conjunto de direcciones IP las direcciones IP incluidas en la lista de caducidad de IP del elemento. WAF

> **Note**
>
> Según el momento en que DynamoDB elimine un elemento caducadoTTL, la operación de eliminación real de una dirección IP caducada del conjunto de IP puede variar AWS WAF . La eliminación de TTL DynamoDB depende principalmente del tamaño y el nivel de actividad de la tabla. Se espera un retraso en la operación de AWS WAF eliminación debido al posible retraso en la operación de eliminación de DynamoDB. En general, la solución elimina las direcciones IP caducadas del conjunto de IP poco después de la AWS WAF eliminación de DynamoDBTTL. 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 básico personalizado para cada punto final crítico. Para obtener información sobre la creación y el uso de vistas de métricas personalizadas,

consulte CloudWatchPaneles: creación y uso de vistas de métricas personalizadas y Uso de CloudWatch paneles de Amazon.

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

El panel muestra las siguientes métricas:

- Solicitudes permitidas o bloqueadas: muestra si recibes un aumento en el número de accesos permitidos (el doble de lo normal) o bloqueados (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 DDoS los ataques 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 En comparación con los archivos subidos: ayuda a identificar si un DDoS ataque 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 envía información para un conjunto de parámetros de solicitud específico).

- ELBExtensión y longitud de la cola: ayuda a verificar si un DDoS ataque está causando daños a la infraestructura y si el atacante está pasando por alto CloudFront la AWS WAF capa y atacando directamente recursos desprotegidos.
- ELBRecuento de solicitudes: ayuda a identificar los daños en la infraestructura. Esta métrica muestra si el atacante está eludiendo la capa de protección o si debes revisar una regla de CloudFront caché para aumentar la tasa de aciertos de la caché.
- ELBHost en buen estado: puede utilizarla como otra métrica de comprobación del estado del sistema.
- ASGCPUUtilización: ayuda a identificar si el atacante está pasando por alto CloudFront y Elastic Load Balancing. AWS WAF También puede usar esta métrica para identificar el daño de un ataque.

Gestiona los XSS falsos positivos

Esta solución configura una AWS WAF regla 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 que los usuarios legítimos redacten y envíenHTML, por ejemplo, mediante un editor de texto enriquecido en un sistema de gestión de contenido. En este escenario, considere la posibilidad de crear una regla de excepción que omita la XSS regla predeterminada para URL patrones específicos que acepten la entrada de texto enriquecido e implemente mecanismos alternativos para proteger a los excluidosURLs.

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

Complete los siguientes pasos para actualizar la XSS regla y excluir URLs esa aceptación HTML como entrada. Consulta la Guía para WAF desarrolladores de Amazon para obtener instrucciones detalladas.

1. Inicie sesión en la consola de AWS WAF.
2. Cree una coincidencia de cadenas o una condición de expresión regular.
3. Configure los ajustes del filtro para inspeccionar URI y enumerar los valores que desee aceptar en relación con la XSS regla.

4. Edite la XSSregla de esta solución y añada la nueva condición que ha creado.

   Por ejemplo, para excluir todos los URLs elementos 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
   - XSSLista de permisos

Solución de problemas

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

Contacto Support

Si cuenta con AWSDeveloper Support, AWSBusiness Support o AWSEnterprise Support, puede utilizar el Support Center 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. Para el servicio, seleccione WAFo AWS WAF.
3. En Categoría, seleccione Automatizaciones WAF de seguridad o Automatizaciones de seguridad para. AWS WAF
4. En Gravedad, 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. Adjunta la información Support necesaria 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 GitHubrepositorio 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 a la que enviar las métricas operativas. 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 AWS durante la implementación inicial de la CloudFormation plantilla:

- ID de solución: el identificador de la AWS solución
- ID único (UUID): identificador único generado aleatoriamente para cada implementación de esta solución
- Timestamp: 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 HTTPinundación 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: el número de direcciones IP caducadas que se van a eliminar del conjunto de IP permitidas o denegadas

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

1. `aws-waf-security-automations.template`AWS CloudFormationDescárguela en su disco duro local.
2. Abre 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 consola de AWS CloudFormation.
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. Lanza la pila.

Recursos relacionados

Documentos técnicos AWS asociados

- AWS Mejores prácticas para la resiliencia DDoS

Publicaciones del blog AWS de seguridad asociadas

- Cómo evitar los enlaces directos mediante AWS WAF Amazon y Referer CloudFront 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

Date	Cambio
Septiembre de 2016	Versión inicial
Enero de 2017	Aclaración sobre los límites de direcciones IP de esta solución.
Marzo de 2017	Guía adicional sobre cómo crear un comportamiento de caché; se actualizó URLs para las publicaciones del blog sobre AWS seguridad.
Junio de 2017	Se agregó ALB soporte y se actualizaron los límites de los productos.
Noviembre de 2017	Se agregó compatibilidad con reglas basadas en tasas para la protección contra HTTP inundaciones; enlaces adicionales para almacenar los registros de acceso a los recursos.
Enero de 2018	Se ha actualizado el contenido sobre la disponibilidad regional de AWS WAF los balanceadores de carga de aplicaciones.
Diciembre de 2018	Se agregó IPv6 Support, se ampliaron los CIDR rangos y se agregó un panel de monitoreo.
Abril de 2019	AWS WAF integración de registros, integración de Amazon Athena y se agregó un analizador de registros configurable.
2019 de diciembre de 2019	Se agregó información sobre la compatibilidad con la actualización de Node.js.

Date	Cambio
Febrero de 2020	Se corrigieron errores y se actualizó el RequestThreshold parámetro.
Junio de 2020	Se agregó la optimización de costos de Athena mediante el particionamiento; se actualizaron las README instrucciones; se solucionó un posible problema de DoS en el encabezado de Bad Bots. X-Forward-For
Julio de 2020	Se actualizó del servicio AWS WAF clásico al AWS WAF V2API.
Noviembre de 2020	Versión 3.1.0: aclaraciones sobre las normas de protección contra HTTP inundaciones y protección de escáneres y sondas para regiones específicas; se ha sustituido el tipo de ruta S3 por el de alojamiento virtual; se ha añadido una variable de partición a todas ellasARNs; para obtener más información, consulta el CHANGELOGarchivo.md del repositorio. GitHub
Septiembre de 2021	Versión 3.2.0: Se ha añadido compatibilidad con la retención de IP en los conjuntos de IP permitidos y denegados; se han corregido algunos errores. Para obtener más informaci ón, consulte el CHANGELOGarchivo.md del GitHub repositorio.

Date	Cambio
Agosto de 2022	Versión 3.2.1: se agregó soporte para el manejo de WAF sobredimensionamiento de los componentes de las solicitudes; se agregó soporte para los niveles de WAF sensibili dad para las declaraciones de reglas de SQL inyección. Para obtener más información, consulte el CHANGELOGarchivo.md del repositorio. GitHub
Septiembre de 2022	Se ha actualizado la documentación para la personalización fuera del CloudFormation conjunto de soluciones.
Diciembre de 2022	Versión de lanzamiento 3.2.2: Se agregó la integración con Service Catalog AppRegistry y AWS Systems Manager Application Manager. Para obtener más información, consulte el CHANGELOGarchivo.md del GitHub repositor io.
Diciembre de 2022	Versión 3.2.3: añada una región como prefijo al nombre del grupo de atributos de la aplicació n para evitar conflictos con el nombre que comienza por. AWS Para obtener más información, consulte el CHANGELOG archivo.md del repositorio. GitHub
Febrero de 2023	Versión de lanzamiento 3.2.4: Pytest actualiza do y solicitudes de mitigación. CVE Para obtener más información, consulte el CHANGELOGarchivo.md del repositorio. GitHub

Date	Cambio
Marzo de 2023	Documentación actualizada para actualizar la solución de la versión 3.0 o 3.1 a la 3.2 o posterior que tiene direcciones IP permitidas o denegadas.
Abril de 2023	Versión de lanzamiento 3.2.5: Se ha mitigado el impacto provocado por la nueva configura ción predeterminada de Amazon S3 Object Ownership (ACLsdeshabilitada) para todos los buckets nuevos de Amazon S3. Para obtener más información, consulte el CHANGELOG archivo.md del repositorio. GitHub
Mayo de 2023	Versión 4.0.0: se ha añadido compatibilidad con nuevos grupos de Reglas administradas de AWS reglas y se han actualizado las reglas personalizadas. Para obtener más informaci ón, consulte el CHANGELOGarchivo.md del GitHub repositorio.
Mayo de 2023	Versión 4.0.1: `.gitignore` archivo actualiza do para resolver el problema de la falta de archivos. Para obtener más información, consulte el CHANGELOGarchivo.md del GitHub repositorio.
Septiembre de 2023	Versión de lanzamiento 4.0.2: código refactori zado para mejorar la calidad. Vulnerabi lidad del paquete de solicitudes parcheado . Para obtener más información, consulte el CHANGELOGarchivo.md del GitHub repositor io.

Date	Cambio
Octubre de 2023	Versión 4.0.3: versiones de paquetes actualizadas para resolver las vulnerabilidades de seguridad. Para obtener más información, consulte el CHANGELOGarchivo.md del GitHub repositorio.
Noviembre de 2023	Actualización de la documentación: se agregó AWS Developer Support y se fusionó Contact AWS Support en la sección de solución de problemas.
Noviembre de 2023	Actualización de la documentación: se agregaron las etiquetas de costo de Confirme asociadas a la solución a la AppRegistry sección Supervisión de la solución con AWS Service Catalog.
Abril de 2024	Actualización de la documentación: instrucciones aclaradas para añadir un depósito de S3 en el paso 3 de la implementación.
Septiembre de 2024	Versión de lanzamiento 4.0.4: versiones de paquetes actualizadas para resolver las vulnerabilidades de seguridad. Para obtener más información, consulte el CHANGELOG archivo.md del GitHub repositorio.
Octubre de 2024	Versión de lanzamiento 4.0.5: Se utilizó Poetry para la gestión de dependencias. Se reemplazó el registrador nativo de Python por el registrador aws_lambda_powertools. Para obtener más información, consulte el archivo.md del repositorio. CHANGELOG GitHub

Date	Cambio
Diciembre de 2024	Versión de lanzamiento 4.0.6: actualice la lambda a Python 3.12. Para obtener más información, consulte el CHANGELOG archivo.md del repositorio. GitHub

Avisos

Esta guía de implementación se proporciona únicamente con fines informativos. Representa las ofertas y prácticas de AWS productos actuales a 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 AWS los productos o servicios, 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 sus filialesAWS, 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 AWS WAF solución Security Automations for está licenciada según los términos de la versión 2.0 de la licencia Apache.

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.